# Datensicherung für Anfänger

de.wikibooks.org

25. August 2014

# Inhaltsverzeichnis

**Haben Sie schon mal Ihre Daten verloren? Nein, BISHER noch nicht?** Mit einfachen Mitteln eine regelmäßige Datensicherung zu organisieren, ist weder teuer noch schwierig. Dieses Buch ist an den Bedürfnissen von Computerbesitzern mit einem oder wenigen PC ausgerichtet, sollte aber auch für technisch versierte Benutzer hilfreich sein. Das Buch besteht aus drei Teilen. Die Theorie kann für jeden Computernutzer hilfreich sein, ob er nun Windows oder Linux verwendet. Der Rest des Buches ist an Windows-Benutzer gerichtet. Die Beschreibung wichtiger Programme sowie Schritt-für-Schritt-Anleitungen sollen auch und vor allem für Computernutzer mit geringen technischen Kenntnissen verständlich sein.

## 0.1 Datensicherung - ein heikles Thema

Wenn man sicherheitshalber eine Kopie seiner Daten anfertigt, trägt der Vorgang des Kopierens den Namen **Datensicherung**, auch die englische Bezeichnung **Backup** ist gebräuchlich. Mit einer Datensicherung werden Kopien erzeugt, mit denen nach Ausfällen und Datenverlusten ein früher Zustand wiederhergestellt werden kann. Der Vorgang der Rücksicherung wird als **Restore** bezeichnet.

Umgangssprachlich wird mitunter auch der Datenträger mit den kopierten Daten als Datensicherung bezeichnet. "Sicherungskopie" wäre die bessere Bezeichnung dafür. Eine Datensicherung sollte ausreichend häufig und regelmäßig erfolgen. Die Sicherheitskopien müssen unbedingt vollständig sowie kurz- und mittelfristig verfügbar sein. Ältere Versionen können gelöscht und überschrieben werden, eine Langzeitlagerung ist dabei nicht vorgesehen.

Bei der **Datenarchivierung** geht es darum, ausgewählte, wichtige Daten über Jahre, Jahrzehnte und Jahrhunderte sicher aufzubewahren. Die archivierten Daten werden meist von der Festplatte gelöscht. Wegen der begrenzten Lebensdauer von Sicherungsmedien und Technologien müssen die Daten alle paar Jahre überprüft und auf neue Medien umkopiert werden. Einige Aspekte werden in den Kapiteln **Lebensdauer digitaler Daten**[1] und **Lebensdauer von Technologien**[2] behandelt.

Der Übergang von der Datensicherung zur Archivierung ist fließend. Das Finanzamt und die Grundsätze ordnungsgemäßer Buchführung verlangen, dass ausgewählte Daten zehn Jahre lang aufbewahrt werden müssen.

1 Kapitel 14 auf Seite 71
2 Kapitel 15 auf Seite 77

### Ein wenig Statistik

Eine Umfrage [3] unter 6149 Benutzern in 128 Ländern hat ergeben:

- 91% halten Datensicherung für wichtig, aber nur
- 11% sichern Daten regelmäßig (1% täglich, 1% wöchentlich, 9% monatlich).
- 45% haben noch **niemals** Daten gesichert, aber
- 77% haben schon Daten verloren (davon 55% in den letzten beiden Jahren).

### Können Sie diesen Widerspruch verstehen?

Jeder weiß, dass Computer kaputt gehen können. Trotzdem glaubt eine erdrückende Mehrheit der Computernutzer hartnäckig daran, dass eine Störung am High-Tech-Produkt „Computer“ immer nur die Anderen treffen kann. Nicht mal eigene schlechte Erfahrungen können sie dauerhaft von diesem Irrglauben abbringen. Der Gedanke an einen möglichen Datenverlust wird ebenso verdrängt wie der Gedanke an einen möglichen Autounfall. Andererseits zahlen die gleichen Menschen jeden Monat brav ihre Beiträge zu Lebens-, Hausrats- und Kaskoversicherungen, weil sie aus Erfahrung wissen, dass immer mal was schief gehen kann. Leider kann man sich nicht mal fix gegen Datenverlust versichern, Sie müssen regelmäßig selbst aktiv werden. Wie das geht, können Sie aus diesem Buch lernen.

Kategorie:Buch[4]

3 Weltweite Umfrage zu Datensicherung `http://www.consumerstatistics.org/global-data-backup-survey-results/`

4 `http://de.wikibooks.org/wiki/Kategorie%3ABuch`

# 1 Vorwort

Zur Einstimmung auf das Thema einige Fakten:

**Aus den Erfahrungen eines Datenrettungs-Unternehmens:**

Es gibt nur zwei Arten von Daten:

Daten, die gesichert wurden,

und Daten, die *noch nicht* verloren gegangen sind – bis jetzt!

**Aus der Computer-Folklore:**

Datensicherung ist nur ´was für Feiglinge.

**Zitat aus einem Gerichtsurteil:**

Der Datenverlust durch Absturz gehört „zum allgemeinen Risiko eines EDV-Benutzers“, dem durch übliches Anfertigen von Sicherheitskopien zu begegnen sei. [1] [2]

**Die häufigsten Ursachen für Datenverluste:**

- Bedienfehler
- Fehler im Betriebssystem und Anwendungsprogrammen
- Verwendung ungeeigneter Dienst- und Hilfsprogramme
- Viren, Würmer, Trojaner und Hacker-Attacken
- Probleme bei Software-Updates
- Ausfall der Festplatte oder anderer Computer-Komponenten
- Kompatibilitätsprobleme

**Wie schlimm kann der Schaden sein?**

Erkenntnis der Experten von Scotland Yard:

Ein mittleres Unternehmen, das seine Datenbank komplett einbüßt, ist spätestens nach zwei Jahren am Ende.[3]

Statistik des Haftpflichtverbandes der deutschen Industrie:

40% aller Unternehmen, die ihre Daten verlieren, sind nach spätestens zwei Jahren bankrott.[4]

IDC-Studie zur Datensicherheit von 1999:

---

1 Eine aktuelle Datensicherung ist nicht vorhanden `http://www.aufrecht.de/index.php?id=3092`
2 Datensicherung wurde nicht überprüft `http://www.aufrecht.de/index.php?id=3094`
3 IT Sales Week, 10.05.99, S. 24
4 Computer Reseller News, 19.03.07, S. 46

Die Rekonstruktion eines Datenbestandes von 20 MB kostet 17 000 bis 98 000 Dollar und dauert 19 bis 42 Tage.

Versicherungsbedingungen der TELA Versicherung:

Die Versicherung zahlt bei Datenverlusten den nachgewiesenen Aufwand zur Wiederherstellung bzw. zur Neuerfassung der Daten, aber in keinem Fall mehr als 10 000 € pro MByte.

Statistik der Münchner Rückversicherung:

Etwa 40% der Unternehmen, deren Rechenzentrum vernichtet wurde und die keinen Katastrophenplan hatten, eröffneten nicht wieder. 90% derer, die wiedereröffneten, gaben innerhalb der nächsten zwei Jahren auf. Daraus errechnet sich eine „mittelfristige Überlebensrate“ von 6%.

**Preisliste verschiedener Datenrettungsunternehmen:**

- Kroll Ontrack Datenrettung, Tel. 0800 10 12 13 14
- IT-Service24, Tel. 0800 1811 644

Bei physisch beschädigten Festplatten (Kopfaufsetzer o.ä.) kostet die Datenrettung selten weniger als 500 €, meist ein Vielfaches davon.

Preisbeispiele:

- 3,5" Diskette - etwa 40-50 Euro
- SD–Karte, USB-Stick etc. - etwa 70-150 Euro
- Festplatte (logischer Schaden) - etwa 400-700 Euro und
- RAID-System etwa 1300-3000 Euro.

**Kostenloser Ratschlag:** Wenn Ihnen irgend etwas verdächtig vorkommt, sofort die Weiterarbeit einstellen. Nichts speichern und Windows nicht herunterfahren, denn vielleicht startet es nie wieder. Rufen sie einen Experten an und schildern Sie das Problem. Lassen Sie sich nicht von „Fachchinesisch“ einlullen. Fragen Sie nach, bis Sie alles verstanden haben. Zögern Sie nicht, mehrere Meinungen einzuholen. Meiden Sie selbsternannte Experten. Bei den meisten Datenrettungen hat man nur einen Versuch - wenn er misslingt, wird die Situation wirklich schlimm.

**Sind Sie jetzt verunsichert? Das ist sehr gut. Hoffentlich bleibt diese Unsicherheit für immer.**

```
<!-- Erfahrungen eines Datenrettungsunternehmens -->
```

# 2 Was sind Ihre Daten wert?

Ein Nachbar hat Ihr Auto gestreift. Ein Besucher hat Ihr Notebook vom Tisch gestoßen. Können Sie Schadensersatz verlangen? Ja, selbstverständlich. Aber wie sieht es aus, wenn ein Mitarbeiter versehentlich die Kundendatenbank gelöscht hat? Wenn der Computernotdienst Ihre Festplatte gelöscht hat? In welcher Höhe können Sie Schadenersatz verlangen? Das Problem ist, dass Daten nicht körperlich sind, sie haben keinen Materialwert.

Das deutsche Recht sieht zwei Arten von Schadensersatz vor. Primäres Ziel ist die Wiederherstellung (Naturalrestitution), ersatzweise die Schadenskompensation.

### 2.0.1 Kosten der Wiederherstellung

Der Verursacher muss den Schaden selbst beseitigen oder den Geldbetrag zahlen, der zur Wiederherstellung des früheren Zustandes benötigt wird. In der Regel muss die Rechnung eines Datenrettungsunternehmens bezahlt werden oder der Aufwand für die Wiederherstellung von einem Backup-Speicher.

Es kommt vor, dass sich Daten nicht rekonstruieren lassen. Hochzeitsfotos, Manuskripte, technische Zeichnungen und Konstruktionsunterlagen können oft nicht wiederhergestellt werden, wenn kein Backup vorhanden ist. Wenn es aber ohnehin völlig unmöglich ist, die Daten wiederherzustellen, braucht der Versuch nicht unternommen zu werden und dem Verursacher entstehen keine Wiederherstellungskosten.

### 2.0.2 Schadenskompensation

Bei Unmöglichkeit der Wiederherstellung hat der Verursacher den Schaden mit Geld zu kompensieren.

- Es wird ermittelt, wieviel Vermögen der Geschädigte verloren hat.
- Die Arbeitskosten, um die Daten einigermaßen aus der Erinnerung zu rekonstruieren, sind ersatzfähig.
- Personelle und zeitliche Mehraufwendungen wegen gestörter Arbeitsabläufe, z. Arbeitslohn für zeitweilige Hilfskräfte sind ersatzfähig.
- Entgangener Gewinn ist ein ersatzfähiger Schaden.

### 2.0.3 Folgerungen

- Da der Verlust privater Daten nicht zu Gewinnausfällen führt, gehen Privatpersonen fast immer leer aus.

- Wenn durch Ihre Schuld betriebliche Daten verloren gehen, kann das für Sie exorbitant teuer werden.
- Wer es versäumt, für **regelmäßige** Datensicherungen geschäftlich wichtiger Daten zu sorgen, hat eine Mitschuld. Unter Umständen muss er den Schaden vollständig selbst tragen, auch wenn er sehr hoch ist[1].

1 Gerichtsurteil zum Schadenersatz `http://it-vergabe-blog.de/tag/schadensersatz`

# 3 Die Festplatte ist defekt

Die meisten Festplatten werden nach wenigen Jahren zusammen mit dem Computer entsorgt oder gegen größere Platten getauscht, wenn sie voll sind. Deshalb werden Festplatten vom Hersteller nicht für einen langjährigen Einsatz konzipiert und gebaut. Je nach Benutzung (24 oder 8 Stunden täglich) hält eine Festplatte zwei bis fünf Jahre mit erträglicher Wahrscheinlichkeit durch. Natürlich werden auch extrem langlebige und zuverlässige Festplatten gebaut und zu exorbitanten Preisen verkauft, für Server beispielsweise. Warum aber sollte ein Hersteller seine Festplatten für den Massenmarkt mit hohem Aufwand langlebiger machen?

Selbst wenn Sie die Warnzeichen für einen bevorstehenden Ausfall kennen und beachten, eines Tages wird es passieren: Die Festplatte geht kaputt.

> Stellen Sie sich bitte mal vor: Jetzt, in diesem Moment, geht Ihre Festplatte unrettbar kaputt. Wie groß wäre der Schaden? Wie wertvoll sind Ihre Daten?

## 3.1 Verlust der Daten

Beginnen wir mit den Daten, die jeder hat:

- Haben Sie alle Zugangsdaten (DSL, E-Mail, eBay, Messenger, Chat, ...) aufgeschrieben? Auf Papier oder in einer verloren gegangenen Datei? Auch die Daten von allen benutzten Online-Shops?
- Vermutlich haben Sie Dutzende oder Hunderte E-Mails gespeichert. Vielleicht sind auch E-Mails dabei, mit denen Sie Passworte und Zugangskennungen erhalten haben. Habe Sie diese alle ausgedruckt und abgeheftet?
- Wie viele Einträge hat Ihr E-Mail-Adressbuch? Wie aufwändig wäre es, diese Adressen wiederzubeschaffen?
- Wie viele Links hat Ihre Favoritenliste? Wie lange würde es wohl dauern, alle oder wenigstens die wichtigsten davon wiederzufinden?
- Benutzen Sie ein Lohnsteuerprogramm? Wie lange hat die Dateneingabe gedauert?

Wie bitter wäre es für Sie, Fotos und Filme zu verlieren

- von den Urlaubsreisen der letzten Jahre
- von der Hochzeit und anderen Familienfeiern
- von den heranwachsenden Kindern

Sicher haben Sie viele Fotos per E-Mail erhalten, die schwer wiederbeschaffbar sind. Selbst wenn Sie die Originale aller Fotos auf irgendwelchen CDs haben: Wie lange würde es dauern, sie auf die Festplatte zu kopieren, die besten auszusuchen, den Ordnern und den Fotos sinnvolle Namen zu geben und eine „Diashow“ zusammenzustellen?

Eine Sicherheitskopie für eine übliche Datenmenge kostet Sie weniger als einen Euro und das erste Mal weniger als eine Stunde Zeit. Bei einer wohldurchdachten Konzeption dauern die Wiederholungen nur einige Minuten.

## 3.2 Verlust des Betriebssystems

Das Betriebssystem neu installieren zu müssen ist eine langwierige Arbeit. Nicht nur Windows muss installiert werden, sondern auch alle Treiber, alle Updates und alle Anwendungen. Sind Ihre Installations-CDs vollständig und in gutem Zustand? Haben Sie alle Seriennummern, Zugangsdaten und Lizenzen? Vermutlich haben Sie aktuelle Treiber und zahlreiche nützliche Programme im Internet gefunden und installiert. Haben Sie deren Web-Adressen griffbereit? Falls Sie Abonnements von Antiviren- und anderen Programmen über das Internet verlängert haben, wie können Sie die Zahlung nachweisen?

Wenn Sie ein erfahrener Benutzer sind, brauchen Sie mindestens einen Tag für eine Neuinstallation. In den darauffolgenden Tagen werden Sie noch vielen kleine Nachbesserungen vornehmen müssen.

Schätzen Sie jetzt bitte einmal für jeden einzelnen Posten die Stundenzahl und multiplizieren Sie die Summe mit dem Stundensatz Ihres Computerexperten, -händlers oder Ihrem eigenen Stundensatz, um den materiellen Schaden abzuschätzen.

```
<!-- Verlust der Daten -->
```

# 4 Welche Gefahren drohen Ihren Daten

**Ein Defekt der Festplatte ist nur eine von vielen Möglichkeiten, seine Daten zu verlieren.**

## 4.1 Risikofaktor Mensch

- Bedienfehler (versehentliches Löschen einer Datei oder einer Dateiversion),
- Nichtbeachtung der Garantiebedingungen (viele Reparaturbetriebe stellen routinemäßig den Zustand beim Kauf wieder her und löschen dabei Ihre Daten),
- Fehler aus mangelndem Wissen über Computer und Software,
- unberechtigte Benutzer (Haustiere, die über die Tastatur laufen, und Kinder),
- falsche Anwendung von Hilfsprogrammen, vor allem von Partitionierungs-Tools,
- Nichtbeachtung von Warnhinweisen,
- Diebe räumen Ihre Wohnung aus,
- Sie vergessen das Notebook im Taxi oder in der Bahn,
- der Memory-Stick ist nicht mehr zu finden sowie
- „Schabernack“ oder Vandalismus durch Kinder, Kollegen oder Nachbarn beim Blumengießen.

## 4.2 Risiken durch Malware (Schadsoftware)

- Viren, Würmer, Trojaner, Datendiebstahl (Phishing), Hacker-Attacken

## 4.3 Risikofaktor Software

- Fehler im Betriebssystem und Sicherheitslücken,
- inkompatible Programme,
- veraltete Hilfsprogramme,
- fehlerhafte oder unpassende Treiber sowie
- Datenverlust durch ein Update oder durch die Installation eines Servicepacks.

**Der Mensch (als Bediener oder als Programmierer von nützlicher oder schädlicher Software) verursacht statistisch etwa 85% aller Schäden. Es bleiben nur 15%, die auf die technische Umwelt sowie auf Elementarschäden entfallen.**

## 4.4 Risiken durch Umwelt- und andere äußere Einflüsse

**Energieversorgung:**

- Blitzschlag in Strom-, Daten- und Telefonleitungen
- Überspannungen durch Schaltvorgänge des Energieversorgers
- Ausgleichsströme durch falsche Verkabelung

**Flüssigkeiten:**

- Die Waschmaschine in der Wohnung über Ihnen läuft aus.
- Ein Sturm beschädigt das Dach und ein Wolkenbruch folgt.
- Ein „Jahrhundert-Hochwasser“ kann öfter als alle hundert Jahre auftreten.
- Die Feuerwehr löscht einen Brand in der Etage über Ihnen.

**Feuer:**

- Nicht nur die Flammen sind gefährlich. Durch steigende Umgebungstemperatur kann ein eingeschalteter PC überhitzen.
- Aggressive Rauchgase können Leiterzüge zerfressen, Kriechströme verursachen und Kontakte korrodieren lassen.
- Nach dem Löscheinsatz ist die Luftfeuchtigkeit für einige Tage erhöht. Sie lässt Platinen aufquellen und Kontakte korrodieren.

## 4.5 Risiken durch Hardware

- Überhitzung schnell drehender Festplatten,
- Dauerbetrieb von Festplatten, die nicht für Dauerbetrieb ausgelegt sind,
- Vibrationen im Betrieb oder Erschütterungen beim Transport können zu Kopfaufsetzern führen,
- Überhitzung des Prozessors (der sogenannte „plötzliche P4 Tod“ [1]) und andere Elektronik-Ausfälle können zu Schäden am Dateisystem führen.

```
<!-- Risikofaktor Mensch -->
```

**Physikalisch-chemische Vorgänge**

**Durch welche physikalisch-chemischen Vorgänge werden magnetisch gespeicherte Daten zerstört?**

- Das Erdmagnetfeld wirkt zwar schwach, aber ausdauernd auf die Magnetisierung ein.
- Die Magnetfelder benachbarter, unterschiedlich magnetisierter Bits wirken aufeinander ein und schwächen sich gegenseitig:
  - Bei Magnetbändern wirkt die Magnetisierung durch das Trägermaterial hindurch und schwächt die Aufzeichnung ab. Deshalb sollten Magnetbänder jedes Jahr umgewickelt werden und alle zwei bis drei Jahre umkopiert werden.

1 CPU-Ausfall durch langandauernde Überhitzung `http://www.heise.de/ct/hintergrund/meldung/34186`

  - Die Bits auf einer Festplatte sind so winzig und liegen so dicht hintereinander in der Spur, dass sie sich allmählich gegenseitig ummagnetisieren. Es dürfte eine gute Idee sein, eine „abgelagerte“ Festplatte jedes Jahr anzuschließen und zu defragmentieren, um dadurch die Daten neu zu schreiben.
- Wenn eine Festplatte jahrelang nicht benutzt wird, kann das Schmiermittel der Festplattenlager hart werden und verharzen.

**Durch welche physikalisch-chemischen Vorgänge werden Datenträger zerstört?**

- Chemische Prozesse führen zur Zersetzung:
  - Das Trägermaterial zerfällt allmählich. Besonders anfällig ist das für CD/DVD verwendete Polycarbonat.
  - Das Trägermaterial trübt sich ein.
  - Die Klebstoffe zersetzen sich, mit denen die Schichten verklebt sind.
  - Chemische Reaktionen mit der Verpackung der Datenträger [2]
- Auch die Elektronik der Laufwerke ist anfällig:
  - Elektrolytkondensatoren trocknen aus
  - Das BIOS von Festplatten und optischen Laufwerken ist in EPROMs gespeichert, die eine Haltbarkeit in der Größenordnung von zehn Jahren haben, bis die Bits verloren gehen.
  - Energiereiche kosmische Teilchen dringen gelegentlich bis zur Erdoberfläche vor. Hier können sie zu Einzelbit-Datenfehlern führen[3]. Auf hohen Bergen und im Flugzeug ist die Strahlung um ein Vielfaches stärker.
  - Kontakte können durch Korrosion oder nachlassende Federkraft unsicher werden. Ein einziges falsches Bit kann in einem unpassenden Moment in Sekundenbruchteilen die Verwaltungstabellen der Festplatte zerstören, wodurch der gesamte Festplatteninhalt verloren geht.[4]
  - Kontaktprobleme können auch innerhalb der Festplattenelektronik auftreten. [5]

**Softwarefehler der Firmware**

Jede nicht-primitive Software enthält Fehler, auch die Firmware (das BIOS der Festplatte) macht keine Ausnahme. Die Festplatte verwaltet einen eigenen Cache-Speicher. Dazu kommen die S.M.A.R.T. Funktionen, die sehr komplex sind. Die SMART-Software entdeckt und behebt kleine Fehler rechtzeitig und kann bei einer allmählichen Verschlechterung der Festplattenparameter warnen, wenn die Parameter kritisch werden. Leider nimmt mit der Komplexität der Firmware auch deren Ausfallwahrscheinlichkeit zu. Hier einige Fehlerbeschreibungen, die alle auf fehlerhafte Firmware zurückzuführen sind:

- `http://www.dataclinic.co.uk/data-recovery-western-digital-caviar.htm`
- `http://www.dataclinic.co.uk/hard-disk-smooth-l7250.htm`
- `http://www.dataclinic.co.uk/data-recovery-western-digital-wd-series.htm`
- `http://www.dataclinic.co.uk/data-recovery-maxtor-dx541-2b020h1.htm`
- `http://www.dataclinic.co.uk/maxtor-glist-corruption.htm`

2 Bild einer beschädigten CD `http://de.wikipedia.org/wiki/Langzeitarchivierung`

3 Kein Witz! Hochwertige RAM-Prüfgeräte melden das als „atmosphärischen Fehler“

4 Dieser Fehler tritt häufig bei Festplatten in auswechselbaren Schubkästen auf, aber auch ein Wackelkontakt im Datenkabel oder am USB-Stecker kann die Ursache sein.

5 Beispiel: Einige IBM-Festplatten, siehe Abschnitt „Manufacturer: IBM“ in `http://www.acelab.ru/products/pc-en/articles/ModernHDD/005.html`

- http://www.dataclinic.co.uk/data-recovery-maxtor-diamondmax-10.htm

**Absichtliche oder fahrlässige Verstöße gegen Spezifikationen**

- Auf Seagate-Festplatten brannte eine Schutzdiode durch, wenn ein Netzteil zu langsam auf gelegentlich auftretende Überspannungsspitzen reagiert hat. Der Hersteller der Schutzdiode hatte es nicht für möglich gehalten, dass es derart schlechte Netzteile geben könnte. [6]
- Auf zahlreichen Platinen werden Kondensatoren mit ungenügender Spannungsfestigkeit verbaut. Eine um den Mittelwert von 12 Volt schwankende Spannung mit Kondensatoren stabilisieren zu wollen, die maximal mit 12,6 Volt belastet werden dürfen, ist fahrlässig, aber es senkt die Herstellungskosten.
- Der überwiegende Teil der externen Festplatten wird bei mehrstündigem Betrieb zu heiß.
- Bei der Hälfte der untersuchten PCs war die Kühlung des Computers und vor allem der Festplatte ungenügend, obwohl eine geringfügige Änderung am Gehäuse oder eine veränderte Einbauposition der Festplatte die Kühlung deutlich verbessert hätte. Überhitzung ist langfristig der größte Feind der Festplatte.
- Auf zahlreichen Maxtor-Festplatten kam es zu Überhitzungen eines Chips. Nach kurzzeitigen „Aussetzern“ brannte schließlich der Chip durch. [7]

**Umwelteinflüsse**

Wird der Computer, eine externe Festplatte, ein optisches oder magnetisches Laufwerk nach einem längeren Aufenthalt in der Kälte in einen warmen Raum getragen, droht Gefahr:

- Es kann sich Kondenswasser auf der Elektronikplatine bilden, was zu Kriechströmen und Kurzschlüssen führen kann.
- Kondenswasser kann sich sogar im Inneren der Festplatte bilden. [8] Ein Zusammenstoß eines Wassertröpfchens mit dem Lesekopf kann diesen beschädigen.
- Bauteile dehnen sich bei Erwärmung aus, je nach Material unterschiedlich: Kupfer 16, Aluminium 23, Zink 36, Polyethylen 100 bis 250, Porzellan 3 (Angaben in Millionstel der Länge pro °C). Das scheint sehr wenig zu sein. Zum Vergleich: Der Schwenkarm der Festplatte ist etwa zwei Millionen mal länger als der Abstand der Köpfe von der Festplatte. Schon eine kleine Verbiegung kann zu einem Aufsetzen des Kopfes führen.

Außerdem sollte man nie vergessen,

- dass eine erhöhte Betriebstemperatur die Lebenserwartung der Festplatte verkürzt [9]
- dass sich das Trägermaterial von optischen, magnetischen und anderen Datenträgern bei höherer Lagertemperatur schneller zersetzt
- dass speziell bei externen Festplatten äußere Krafteinwirkungen (Runterfallen etc..) im Betrieb den Datenträger beschädigen könnten

**Spannungsspitzen und Spannungsausfälle**

Einige Beispiele, wodurch gefährliche Überspannungen entstehen können:

---

6 Schutzdiode brennt durch Computerhardware:_HDD:_Probleme:_Seagate#Problem ^{http://de.wikibooks.org/wiki/Computerhardware%3A_HDD%3A_Probleme%3A_Seagate%23Problem}

7 Siehe http://www.dataclinic.co.uk/hard-disk-smooth-l7250.htm

8 Wasserschäden: http://www.datarecovery.org/physical-drive-failure.html

9 Höhere Temperatur erhöht Ausfallrate, siehe Grafik "Temperatur und Ausfallrate" http://www.speicherguide.de/magazin/sata.asp?todo=de&theID=1299&lv=&mtyp=

- Blitzeinschlag
  - in den Blitzableiter des eigenen Hauses oder des Nebenhauses
  - in die Überlandleitung
- Überspannungsspitzen durch Schaltvorgänge auf Hochspannungsleitungen
- Überspannungen auf der Telefon/DSL-Leitung
- Elektrostatische Aufladungen

Selbst ein kurzer Stromausfall von ein 50 bis 100 Millisekunden kann zum Absturz des Computers führen. Wenn der PC zum Zeitpunkt des Stromausfalls mit dem Schreiben auf die Festplatte beschäftigt ist, sind Schäden an einigen oder vielen Dateien wahrscheinlich. Wobei treten solche Unterbrechungen auf?

- Schaltvorgänge des Stromversorgers
- Sicherung „brennt durch“ wegen
  - Überlastung des Stromkreises
  - Anschließen eines defekten Gerätes, z. B. Austausch einer defekten Glühlampe
- Elektrikerarbeiten im Haus

**Chemische Einflüsse**

**Die Chemie magnetischer Datenträger**

Die Magnetschicht besteht aus magnetisierbaren Partikeln, die in eine Polymerschicht eingebettet sind. Als magnetisierbares Material werden $Fe_2O_3$, $CrO_2$, BaFe oder Metallpartikel (MP) verwendet. Für das Trägermaterial wird oft Polyester-Urethan verwendet. Unter Einfluss von Feuchtigkeit zerfällt das Material im sogenannten „Hydrolyse“-Prozess zu Alkohol und Carboxylsäure. Bei 20°C und 30% Luftfeuchtigkeit erreicht der Hydrolyseprozess ein Gleichgewicht, bei dem der Datenträger funktionsfähig bleibt. Bei feuchter Lagerung wird der Datenträger klebrig, der Abrieb verstärkt sich, schließlich löst sich die Schicht ab. Durch lange Lagerung in völlig trockener Wärme kann dieser Schaden teilweise rückgängig gemacht werden. [10]

Aggressive Gase wie Stickoxid, Chlor und Schwefelwasserstoff führen zu Korrosionsschäden an den Magnetpartikeln. Deren Magnetismus lässt nach, wodurch sich die Signalstärke beim Lesen verringert. [11]

**Die Chemie optischer Datenträger**

Als Trägermaterial für CD und DVD wird ein Polycarbonat verwendet. Dieses Material wird selbst bei normaler Lagerung allmählich spröde, es kann zu Ausgasungen kommen. Die Sprödigkeit stört beim Lesen mit geringer Drehzahl wenig, bei hoher Drehzahl kann aber das Material zerreißen. [12]

Ein weiteres Problem ist der bei beschreibbaren Scheiben verwendete Farbstoff. Hauptsächlich verfärbt er sich durch die Hitze des Brenn-Laserstrahls. Allerdings verfärbt er sich auch bei geringeren Temperaturen, wenn auch sehr langsam. Langzeitversuche ergaben eine Vergrößerung der Blockfehlerrate und der Spurstabilität. [13] Mittlerweile verwenden die Her-

10 c't 2000, Heft 24, S. 118
11 Willi Schneider, Langzeitarchivierung von optischen Datenträgern, BSI-Forum 6/97
12 Experiment der „Mythbusters - Die Wissensjäger“ auf RTL2, 2008: Schnelle Laufwerke drehen mit max. 10.000 U/min, DVD zerreißt bei 20.000 U/min
13 Bernd Steinbrink, Bernd Behr, CD-R im Härtetest, c't 9/97, S. 240

steller eine große Anzahl verschiedener Farbstoffverbindungen. Die Stiftung Warentest hat festgestellt, dass die meisten einmal-beschreibbaren Rohlinge eine miserable Lichtbeständigkeit haben, während die RW-Rohlinge höchst empfindlich gegen Wärme und Kälte sind. [14] Die Scheiben im Dunkeln zu lagern sollte kein Problem sein, aber jahreszeitliche Temperaturschwankungen bei der Lagerung lassen sich kaum vermeiden. Deshalb sind die weniger temperaturempfindlichen einmal beschreibbaren Medien besser für eine lange Lagerung geeignet als mehrmals beschreibbare.

**Chemie und die Elektronik**

Bei Fujitsu-Festplatten kam es zu Kurzschlüssen der Elektronik, weil ein Zulieferer ein ungeeignetes Flammschutzmittel verwendet hatte. [15]

Für das Gehäuse des Schaltkreises „Cirrus Logic CL-SH8671-450E“ wurde ein neuartiges Polymer verwendet. Unter erhöhter Temperatur und Feuchtigkeit zersetzte sich ein Teil des Gehäusematerials. Die dabei entstehende Phosphorsäure korrodierte die Kontakte, bis die Festplatte vom BIOS nicht mehr erkannt wurde. Wenn der Fehler auftrat, war die Garantie meist gerade abgelaufen. Durch Reinigen der Kontakte von Chip und Fassung konnten oft die Daten gerettet werden. [16]

**Steck- und Lötverbindungen**

Wo sich Metalle lange Zeit berühren, beginnen Oberflächenatome zu diffundieren. Vermutlich kennen Sie das Problem: Sie ziehen eine Schraube mäßig an, und nach ein paar Monaten oder Jahren sitzt sie fest wie angeschweißt. Im Computer stört es kaum, wenn die Schrauben fest sitzen. Es gibt ein anderes Phänomen: Es bilden sich sogenannte „intermetallische Phasen“, welche den Übergangswiderstand vergrößern.

Steckt man eine Zink- und eine Kohleelektrode in eine leitfähige Lösung, erhält man eine Batterie. Das geht nicht nur mit Zink und Kohle, sondern zwischen beliebigen Metallen [17]. An jeder Lötstelle, aber auch an Schraub- und Steckkontakten, treffen zwei oder drei verschiedene Metalle aufeinander. Wo sich Silber und Gold berühren, entsteht eine Spannung von 0,6 Volt. Zwischen Kupfer und Zinn sind es 0,21 Volt. Sobald Spuren von Feuchtigkeit dazukommen, bildet sich ein galvanisches Element. Der entstehende Stromfluss führt zu einer unabwendbaren Korrosion.

**Thermisch beanspruchte Lötverbindungen**

Die elektronischen Bauteile sind auf Leiterplatinen aufgelötet. Jeder PC hat tausende Lötstellen. Nach dem Einschalten erwärmt sich der PC von 20° auf stellenweise bis 70° C. Die im PC verwendeten Materialien dehnen sich unterschiedlich aus, dabei entstehen mechanischen Belastungen. Große, heiß werdende Widerstände und Leistungshalbleiter (die Spannungsregler im Netzteil und auf der Hauptplatine) sind besonders belastet. Bei herkömmlichem Bleilot gibt es nach zehn bis fünfzehn Jahren die ersten Wackelkontakte (sogenannte „kalte“ Lötstellen), was Ihnen jeder Fernsehmonteur bestätigen kann.

14 http://www.test.de/themen/computer-telefon/test/-DVD-Rohlinge/1359679/1359679/1359772/default.ashx?col=5&col=6&col=7&col=8&col=9

15 Siehe http://www.theregister.co.uk/2002/12/02/pca_publishes_fujitsu_hdd_advisory/ und http://de.wikibooks.org/wiki/Computerhardware:_Festplatte/_Probleme/_Fujitsu#Ursache

16 Siehe den Abschnitt Fujitsu MPG3xxxAT/AH drive family in http://www.acelab.ru/products/pc-en/articles/ModernHDD/005.html

17 http://de.wikipedia.org/wiki/Elektrochemische_Spannungsreihe

Leider gilt seit 2005 in Europa die RoHS-Verordnung, welche die Verwendung von Blei zum Löten verbietet. Es gibt zahlreiche alternative Lötlegierungen, doch keine reicht qualitativ an Bleilot heran. Die meisten bleifreien Lote sind schwierig zu verarbeiten und haben eine schlechte Langzeitstabilität. Ausnahme: Gold-Zinn-Lot ist langzeitstabil, hat aber einen zu hohen Schmelzpunkt, mal abgesehen vom Preis.

Wir müssen also langfristig mit anfälliger werdenden Lötstellen rechnen. Deshalb darf ausnahmsweise für sicherheitsrelevante Anwendungen (medizinische Geräte, Überwachungs- und Kontrollinstrumente, Autoelektronik und das Militär) weiterhin Bleilot verwendet werden.

**Ungeahnte Risiken durch neueste Technologien**

Notebooks werden in einem beträchtlichen Ausmaß verloren oder gestohlen. Um einen Konkurrenten auszuspionieren, braucht man heute nicht mehr in die Firma einzubrechen – einem der Ingenieure nachts das Notebook aus der Wohnung zu stehlen oder es ihm auf dem Parkplatz zu entwenden ist erheblich weniger riskant. Wenn vertrauliche Forschungs- und Finanzunterlagen in die Hände der Konkurrenz gelangen, kann der Schaden gewaltig sein. Deshalb verschlüsseln neuere Notebook-Festplatten sämtliche Daten beim Schreiben und Lesen automatisch. Sofort nach dem Einschalten des Notebooks muss der Schlüssel eingegeben werden. Wer den Schlüssel nicht kennt, kommt nicht an die Daten heran. Theoretisch jedenfalls.

Allerdings verwenden die meisten Benutzer viel zu simple Passwörter, die von Profis in wenigen Minuten oder Stunden zu „knacken“ sind. Die Industrie hat sich auch dagegen etwas einfallen lassen: Bei einigen der neuesten Notebook-Festplatten wird der Schlüssel automatisch gelöscht, wenn das Notebook in falsche Hände fällt. Wenn jemand die Festplatte ausbaut oder der neugierige Sohn ein paar Passwörter durchprobiert, begeht die Festplatte vollautomatisch „Selbstmord“ und der Festplatteninhalt ist weg – unwiderruflich, für immer.

```
<!-- physikalisch-chemische Vorgänge -->
```

# 5 Verlustarten

Welche Methode der Datensicherung schützt gegen welche Risiken?

Die Risiken kann man in drei Gruppen einteilen, die jeweils ganz verschiedene Sicherungsstrategien erfordern.

- **Spektakuläre Ausfälle, die mit Sicherheit sofort bemerkt werden**[1].
  - Der Computer riecht verbrannt, die Festplatte klackert, das Notebook wurde gestohlen. Der Schaden ist meist verheerend.
- **Schwer zu entdeckende, unerwartete Verluste**[2].
  - Sie haben beim Aufräumen ein wenig die Übersicht verloren und versehentlich zu viel gelöscht.
  - Sie suchen eine Datei (oder die DVD mit Ihrer Datensicherung) und können sie nicht finden. Der Schaden ist meist überschaubar, kann Sie aber trotzdem eine Menge Zeit kosten.
- **Unbemerkte Verluste bei der Langzeit-Archivierung**[3].
  - Sie holen eine fünfzehn Jahre alte Foto-CD aus dem Schrank und müssen feststellen, dass sich die Schicht abgelöst hat.
  - Weitaus häufiger: Ihr alter Brenner war nicht mehr im Bestzustand, die zuletzt gebrannten Scheiben lassen sich mit dem neuen Laufwerk nicht lesen.
  - Weniger spektakulär: Ihre neue Software kann die alten Dateien nicht öffnen, und die alte Software lässt sich auf Ihrem neuen Computer nicht installieren.

## 5.1 Spektakuläre Ausfälle

Dass der Computer hinüber ist, wenn ein Blitz in die Stromleitung einschlägt, wird niemanden verwundern. Dass ein Stromausfall zum Datenverlust führen kann, ist ebenfalls vorstellbar. Es gibt unzählige weitere, unerwartete Möglichkeiten, alle seine Daten auf einen Schlag zu verlieren. Das Schicksal ist erfinderisch, in vielen Berufsjahren habe ich so manches erlebt. Ein kleiner Querschnitt, von gewöhnlichen zu extravaganten Vorfällen geordnet:

- Alle Computer der Firma wurden in der Nacht gestohlen.
- Der CIH-Virus löschte die Festplatte.
- Ein Virus verschlüsselte alle Word-Dokumente. Den Schlüssel hätte man angeblich kaufen können.

1 Kapitel 5.1 auf Seite 17
2 Kapitel 5.2 auf Seite 19
3 Kapitel 5.3 auf Seite 20

- Die Benutzung eines ungeeigneten Hilfsprogramms oder dessen fehlerhafte Bedienung war schuld.
- Totalverlust durch falsche Benutzung von Partitionierungssoftware kommt häufig vor.
- Durch das Anstecken eines USB-Sticks änderten sich die den Partitionen zugewiesenen Laufwerksbuchstaben. Das führte zu Verwechslungen.
- Während der Reorganisation der Festplatte mit „Partition Magic“ fiel kurz der Strom aus, die Daten waren verloren. Weitere Stromausfall-Varianten: Das falsche Stromkabel herausgezogen, den falschen Schalter betätigt, über das Kabel gestolpert.
- Im Serverraum fiel die Klimaanlage aus. Der Temperaturanstieg zerstörte mehrere Festplatten.
- Der Reset-Taster, der Netzschalter oder der Schalter der Steckdosenleiste wurde versehentlich betätigt. Außer mit dem Finger passierte es auch mit dem Knie, dem Fuß oder durch Anstoßen mit der Handtasche.
- Ein Kunde kopierte ein Video. Als die Festplatte voll war, wurde wegen eines Programmierfehlers im Dateisystem am Anfang der Festplatte weitergeschrieben. Die Verwaltungstabellen waren verloren und damit der ganze Inhalt der Festplatte.
- Eine harmlos scheinende Installation eines Druckertreibers führte zu einem Serverabsturz. Dabei gingen die Daten des RAID-Systems unrettbar verloren.
- Die neue, schnelle Festplatte wurde in ein zu kleines Gehäuse eingebaut und dieses Gehäuse wurde in einem zu enges Fach unter der Kasse verstaut. Durch Wärmestau war es im PC ständig zu heiß, schon nach sechs Wochen war die Festplatte defekt.
- Vor einer geplanten Neuinstallation hatte der Kunde sorgfältig seine Daten gesichert. Leider hat der Fahrer der Firma den falschen PC zum Händler gebracht.
- Vor einer Neuinstallation sollte die Festplatte formatiert werden. Vorher wurden die Daten auf eine externe Festplatte kopiert, welche üblicherweise für die nächtliche Datensicherung verwendet wird. Die Neuinstallation wurde bis zum Feierabend nicht fertig. Ein Warnhinweis auf der Festplatte unterblieb. Ein uneingeweihter Kollege steckte abends die Festplatte routinemäßig an den Server an, und Nachts wurden die gesicherten Daten überschrieben.
- Der Kunde stellte den PC nach der Reparatur in den Kofferraum und vergaß, die Klappe zu schließen. Beim Anfahren fiel der PC heraus und die Festplatte war hinüber.
- Durch einen Rohrbruch im Steigrohr der Warmwasserheizung wurde der eingeschaltete, unbeaufsichtigte PC besprüht.
- Die Putzfrau zog wahllos irgend einen Stecker heraus, um den Staubsauger anschließen zu können. Leider war es der Stecker des Hauptservers. Ähnliches passierte einem Hausmeister, als er eine Steckdose für die Bohrmaschine brauchte.
- Der Elektriker drehte die falsche Sicherung heraus.
- Der PC stand unter dem offenen Fenster und wurde während eines heftigen Gewitters nass.
- Der Behälter für des Kondenswasser der Klimaanlage wurde nicht rechtzeitig geleert. Das Wasser lief über und tropfte in den darunter stehenden Server.
- Ein Kurzschluss in der Hausstromversorgung zerstörte das Netzteil, welches im Todeskampf die gesamte Elektronik zerstörte. Außer dem CPU-Lüfter hat nichts überlebt.
- Ein Netzwerkkabel zwischen den Etagen verlief im Abstand von 10 Metern parallel zum Blitzableiter. Ein Blitzeinschlag induzierte eine Überspannung im Netzwerkkabel und zerstörte alle direkt angeschlossenen Netzwerkgeräte.

Wenn Sie weitere Horrorgeschichten hören wollen, fragen Sie einen Computerhändler oder Ihre Versicherung.

> Gegen derartige „sofort bemerkbare Schäden“ hilft eine tägliche, stündliche oder permanente Datensicherung, möglichst verbunden mit einer auswärtigen Lagerung der Sicherungsmedien.

## 5.2 Unerwartete Verluste

> Verluste, die erst nach Stunden, Tagen oder Monaten entdeckt werden, sind ein großes, meist unterschätztes Problem. Wie kann es dazu kommen?

Bei einem Windows-Absturz kann es zu Problemen im Dateisystem kommen. Wenn es eine Datei trifft, die gerade in Benutzung war, merkt man das meist nach dem nächsten Start. Manchmal erwischt es zufällige Dateien. Vielleicht merken Sie es ein halbes Jahr später, dass die Datenbank Ihres Lohnsteuerprogramms kaputt ist. Noch schlimmer, wenn die Verwaltungstabellen der Festplatte beschädigt werden. Das passiert häufiger, als man denkt. Wie kann so etwas passieren?

Am Beginn der Festplatte befindet die **F**ile **A**llocation **T**able (FAT) mit der Liste, wo genau sich jedes Stück jeder Datei befindet. Nach jedem Schreibvorgang müssen diese Tabellen entsprechend geändert werden. Die Magnetköpfe müssen dazu jedesmal zeitaufwändig an den Anfang der Festplatte bewegt werden. Im Interesse einer höheren Geschwindigkeit führt Windows diese Schreibvorgänge nicht sofort aus, sondern sammelt die Schreibanforderungen im sogenannten Schreibcache (das ist eine Liste im Arbeitsspeicher). Wenn sich genug Schreibaufträge angesammelt haben, wird die Festplatte auf den neuesten Stand gebracht. Bei einem Absturz unterbleibt die Aktualisierung, und die Verwaltungstabellen der Festplatte stimmen nicht mehr mit deren Inhalt überein. Beim nächsten Start **versucht** Windows das Dateisystem zu reparieren. Das klappt nicht immer. Trümmerstücke, die nicht mehr zusammengefügt werden können, sammelt Windows im Verzeichnis C:\DIR0000 und weiteren Verzeichnissen mit ansteigenden Nummern.

Es gibt aber noch zahlreiche weitere Möglichkeiten, Daten zu verlieren. Einige Beispiele:

- Sie haben beim Aufräumen vor dem Urlaub die Übersicht verloren und löschen versehentlich wichtige Daten.
- Sie tragen irrtümlich falsche Werte in eine Tabelle ein. Wenn Sie es bemerken, ist der Zettel mit den korrekten Werten schon geschreddert.
- Sie löschen oder verändern versehentlich einen Teil eines Dokuments oder Sie löschen versehentlich die falsche Datei. Sie bemerken das erst nach Tagen oder Monaten, wenn Sie die Datei das nächste Mal brauchen.
- Ein Computerschädling ersetzte jeden Tag in einer wichtigen Datei jede tausendste Ziffer „9“ durch die Ziffer „8“. Vermutlich handelte es sich um einen zielgerichteten Angriff gegen die Firma. Was meinen Sie, wie lange es gedauert hat, bis niemand mehr an Tippfehler geglaubt hat?
- Sie haben eine Datei gelöscht, von der Sie sicher waren, sie würde nicht mehr benötigt. Plötzlich wird sie vom Chef oder von der Steuerprüfung benötigt.
- Sie haben einige Dateien auf eine mehrtägige Dienstreise mitgenommen, um daran zu arbeiten. Die in der Firma verbliebene Datei ist zwischenzeitlich von einer Kollegin auf

den neuesten Stand gebracht worden. Zurück von der Reise, kopieren Sie die Datei mit Ihren Änderungen auf den Firmen-PC. Ohne es (zunächst) zu wissen, überschreiben Sie dabei die Arbeit Ihrer Kollegin.
- Ihre Festplatte ist fast voll. Sie haben deshalb einige Dateien ausgelagert und sie dann von der Festplatte gelöscht. Einige Monate sind vergangen, und Sie brauchen eine der ausgelagerten Dateien. Oh weh!
  - Die DVD mit den Daten ist nicht mehr lesbar oder nicht auffindbar.
  - Die Beschriftung ist inkorrekt, die Datei ist nicht drauf.
  - Die Daten waren auf einer externen Festplatte, die inzwischen anderweitig verwendet worden ist.

Ich habe diese Verluste als unauffällig bezeichnet, weil der Zeitpunkt des Verlustes lange zurückliegen kann und meist nicht feststellbar ist.

Was auch passieren kann:

- Eine Woche lang haben Sie an einem Dokument herumgeändert und entscheiden schließlich, dass eine frühere Version die bessere war.

Derartige Verluste treten recht häufig auf, der Schaden ist im Einzelfall meist gering, aber trotzdem ärgerlich. Gegen derartige „schleichende“ Schäden hilft eine häufige, regelmäßige Datensicherung, verbunden mit einer möglichst langen Aufbewahrung der Sicherungsmedien. Idealerweise sollte eine Firma täglich alle Daten sichern und jedes Sicherungsmedium (mindestens) zehn Jahre lang aufbewahren. Privat genügt es möglicherweise, je nach Computernutzung, die Daten einmal wöchentlich zu sichern.

## 5.3 Langzeit-Verluste

Dieses Kapitel ist in Vorbereitung

# 6 Einige Risiken kann man verringern

**Viele Risiken lassen sich durch Vorsicht und Umsicht verringern. Auf dieser Seite geht es um weitere Möglichkeiten, Datenverluste zu vermeiden.**

## 6.1 Stromversorgung

Die Energieversorger müssen manchmal Umschaltungen vornehmen, beispielsweise um Überlandleitungen für Wartungsarbeiten stromlos zu schalten. Jeder Schaltvorgang verursacht eine sehr kurze Spannungsschwankung in den Leitungen. Diese dauert meist weniger als eine halbe Sekunde und wird durch die Pufferkondensatoren des Netzteils abgemildert, das Computernetzteil sollte damit problemlos klar kommen. Wenn der Strom aber eine Sekunde oder länger ausfällt, geht der PC aus und nicht gespeicherte Daten sind verloren.

Gefährlicher ist es, wenn Ihr Wohngebiet von einem großräumigen, länger andauernden Stromausfall betroffen ist. In dem Moment, wenn der Strom wiederkommt, ist der Strombedarf extrem hoch. Beispielsweise laufen sämtliche Kühlschrankmotoren gleichzeitig an. Dieser Motortyp braucht im Anlaufmoment einen vielfach größeren Strom als im Dauerbetrieb. So kommt es zu mehreren Stromstößen, sogenannten „Einschwingvorgängen“, die kurzzeitig mehr als 1000 Volt erreichen können. Dadurch können der PC und andere elektronische Geräte beschädigt werden.

Auch eine durchgebrannte Schmelzsicherung kann zu Problemen führen. Beim Einschrauben der neuen Sicherung gibt es praktisch immer mehrere Stromstöße (Achten Sie mal darauf, wie oft dabei das Licht flackert). Störspannungen können auch durch Blitzschläge entstehen. Nicht nur direkte Blitzschläge sind gefährlich, auch Einschläge in der Nachbarschaft können hohe Störspannungen erzeugen.

Deshalb ist es eine gute Idee,

- zum Arbeitsende
- wenn die Sicherung durchgebrannt oder der Strom aus anderem Grund ausgefallen ist
- wenn der Elektriker im Haus ist
- wenn ein schweres Gewitter im Anzug ist
- bevor Sie in Urlaub fahren

den PC (und weitere elektronische Geräte) vom Stromnetz zu trennen.

Den Telefonstecker oder den DSL-Anschluss können Sie gleich mit herausziehen.

Wenn Sie sich angewöhnen, PC, Bildschirm und Lautsprecher (aber nicht den Tintendrucker![1]) mittels schaltbarer Steckdosenleiste bei jedem Arbeitsschluss vom Stromnetz zu nehmen, können Sie mindestens 30 € pro Jahr sparen und schützen außerdem Ihren PC vor Überspannungen.

## 6.2 RAID

Der Begriff RAID steht für eine Technologie, bei der mehrere Festplatten zu einem Verband zusammengeschaltet werden. Für den privaten Bereich sind vor allem RAID-0 und RAID-1 interessant. Bei RAID-0 werden die Daten auf zwei oder mehr Festplatten möglichst gleichmäßig verteilt. Mehrere gleichzeitig arbeitende Festplatten bewältigen in der Summe eine erheblich größere Datenmenge pro Sekunde, was besonders für Videoschnitt-PCs interessant ist. Das Risiko eines Datenverlustes steigt: Wenn eine der Festplatten des Verbandes ausfällt, kann man mit den Fragmenten auf den restlichen Festplatten nichts mehr anfangen.

Das Verfahren RAID-1 ist auch unter der Bezeichnung „Spiegelung“ bekannt. Es werden zwei identische Festplatten benutzt und alle Daten werden gleichzeitig auf beide Festplatten geschrieben. Bei Ausfall einer der Festplatten sind die Daten nicht verloren, es kann sogar ohne Unterbrechung weitergearbeitet werden. Das ist nützlich für Firmen, wo ein Ausfall wichtiger Computer zu kostspieligen Betriebsstörungen führen kann. Allerdings sollte man bedenken, dass ein RAID-System nicht vor Viren und Bedienfehlern schützt. Es schützt auch nicht davor, dass durch einen Fehler im Netzteil oder einen Blitzeinschlag in der Nähe beide Festplatten gleichzeitig durchbrennen. Ohnehin gehen die meisten Daten durch andere Ursachen verloren, weniger als 10% aller Datenverluste werden durch einen Festplattenausfall verschuldet. Die Wahrscheinlichkeit, dass die Hauptplatine kaputt geht, ist weitaus höher. Ein neueres Modell oder gar die Platine eines anderen Herstellers kommen eventuell mit der Datenstruktur Ihres RAID-Systems nicht zurecht. Insoweit ist ein RAID-System kein Ersatz für eine Datensicherung. Eine regelmäßige Sicherung auf DVD oder ein anderes Medium ist unbedingt notwendig!

Um die Festplatten „zusammenzuschalten“, ist spezielle Hardware notwendig. Auf vielen modernen Hauptplatinen ist ein einfacher RAID-Controller integriert. Für professionelle Lösungen gibt es RAID-Controller als Steckkarte, die mehrere tausend Euro kosten können.

Wenn Sie beispielsweise vier Festplatten mit Daten haben, würden Sie weitere vier Festplatten für deren Spiegelung brauchen. Das ist teuer. Wenn Sie eine Hauptplatine mit integriertem RAID-5-Controller haben oder einen speziellen RAID-Controller kaufen, kommen Sie statt mit vier mit nur einer einzigen zusätzlichen Festplatte aus, ohne Sicherheit zu verlieren. Bei „RAID-5“ wird zu einer Anzahl von Festplatten nur eine einzige zusätzliche Platte hinzugefügt. Der Controller sorgt für eine solche Verteilung der Daten auf die Platten, dass bei Ausfall einer beliebigen Festplatte die Daten verfügbar bleiben.

Für noch höhere Ansprüche gibt es „RAID-6“. Dabei werden zwei Reservefestplatten verwendet, so dass selbst bei Ausfall beliebiger zwei Festplatten weitergearbeitet werden kann. Bei

1 Das Ausschalten des Druckers erhöht die Kosten `http://de.wikibooks.org/wiki/Computerhardware:_Drucker:_Tintendrucker#Drucker_nicht_ausschalten.2C_um_Tinte_zu_sparen`

RAID-10 können die Platten zu mehreren Gruppen mit unterschiedlicher Ausfallsicherheit zusammengeschaltet werden.

**Nachteil:**

- Man braucht einen speziellen Festplattencontroller, der **sehr teuer** sein kann. Deshalb sind RAID-5-Lösungen (und höher) vor allen in Servern zu finden.

**Vorteile:**

- Da sich die Leseanforderungen auf mehrere Festplatten verteilen, steigt der Datendurchsatz des Systems deutlich an. Je mehr Festplatten, desto schneller.
- An einfachere Controller können bis zu 15 Festplatten angeschlossen werden, teure Modelle können 45 Platten ansteuern. Es können mehrere Controllerplatinen in einem PC betrieben werden.
- Wenn der Speicherplatz knapp wird, ergänzt man den RAID-Verband um eine oder mehrere zusätzliche Festplatten. Der Controller kann die vorhandenen Daten bei laufendem Betrieb umverteilen. Einige Stunden später steht die größere Kapazität zur Verfügung.
- Weil RAID mit weniger Festplatten auskommt als eine Spiegelung, wird Energie gespart.

Ein RAID-System schützt **nur** vor dem Ausfall einer Festplatte und der damit zusammenhängenden Betriebsunterbrechung. Die meisten Daten gehen durch andere Ursachen verloren, weniger als 10% aller Datenverluste werden durch einen Festplattenausfall verschuldet. Insoweit ist ein RAID-System kein Ersatz für eine Datensicherung. Eine regelmäßige Sicherung auf Band oder ein anderes Medium ist unbedingt notwendig!

Der erste von mir verkaufte RAID-Controller kostete 4500 DM. Zehn Festplatten waren angeschlossen, das System war unglaublich schnell. Ich werde nie den Tag vergessen, an dem der Lüfter des RAID-Controllers ohne jedes Warnsignal ausfiel. Der Controller hatte zwar einen eigenen Piepser für Fehlermeldungen, aber die Funktion des Lüfters wurde nicht elektronisch überwacht. Jedenfalls überhitzte sich die CPU des Controllers, und die Verwaltungstabellen der Festplatten wurden beschädigt. Alle Daten waren rettungslos verloren! Ohne die Bandsicherung der letzten Nacht hätte ich wohl mein Testament schreiben müssen, bevor mich der Inhaber der betroffenen Firma erschießt.

Wenn eine der Festplatten eines RAID-Verbandes ausgefallen ist, ersetzt man sie einfach durch eine neue. Je nach Hardware darf das im laufenden Betrieb erfolgen, oder man muss den PC kurz herunterfahren. Der Controller integriert die neue Festplatte automatisch, d. h. er verteilt sämtliche Daten neu. Dabei gibt es eine wenig bekannte Gefahr:

- Alle Platten des Verbundes sind möglicherweise im Abstand weniger Minuten vom Fließband gelaufen. Sie sind deshalb mechanisch sehr ähnlich und haben etwa die gleiche Lebenserwartung. Während des Betriebes hatten sie immer die gleiche Belastung auszuhalten. Nach dem Ausfall der ersten Festplatte könnten die nächsten bald nachfolgen!
- Die Festplatten eines RAID-Systems sind im Normalbetrieb relativ wenig beansprucht, denn die Leseanforderungen werden nahezu gleichmäßig auf alle Platten verteilt. Nach dem Einsetzen der Ersatzfestplatte ändert sich das: Der RAID-Controller wird stundenlang mit Höchstlast laufen müssen, um die Daten umzustrukturieren und die neue Platte zu integrieren. Noch nie zuvor sind Ihre Festplatten derart beansprucht, derart heiß geworden! Das führt nicht selten zum Ausfall einer weiteren Festplatte, siehe vorherigen Hinweis. Besonders häufig sind derartige Pannen bei Plattenspiegelungen von S-ATA-

Festplatten in Heimcomputern. Die hier üblicherweise verwendeten Festplatten sind nicht für derartige lang andauernde Belastungen konzipiert.

Deshalb sollten Sie **zuerst** eine komplette Sicherung durchführen und erst danach die Festplatte auswechseln.

## 6.3 Gespiegelte Server

Wenn die CPU oder das Netzteil ausfällt, nützen Ihnen gespiegelte Festplatten oder ein RAID-System gar nichts. In solchen Fällen können gespiegelte Server eingesetzt werden. Dabei sind zwei meist identische PCs mit einer Spezialsoftware über eine schnelle Netzwerkverbindung zusammengeschaltet, so dass sämtliche Eingaben gleichzeitig an beide PC gehen und sie die gleichen Daten verarbeiten. Nur einer der Server, der primäre, gibt die Daten an die Benutzer aus. Wenn der primäre Server ausfällt, übernimmt der andere Server innerhalb einiger Sekunden und wird zum neuen primären Server.

Wenn der ausgefallene Server repariert und wieder hochgefahren ist, holt er sich von dem in Betrieb gebliebenen Server die aktuellen Daten und steht nun als Ersatzserver zur Verfügung.

Bei allerhöchsten Anforderungen an die Ausfallsicherheit werden gespiegelte Rechenzentren eingesetzt. Für den Fall von Überschwemmungen, Erdbeben und Terroranschlägen sollte das Ersatz-Rechenzentrum viele Kilometer entfernt sein.

## 6.4 Wo sollten die Datenträger gelagert werden?

Welches Medium Sie auch immer verwenden, achten Sie darauf, dass möglichst viele der Sicherungsmedien räumlich weit entfernt vom PC gelagert werden. Was nützt Ihnen eine Sicherung, wenn sie zusammen mit dem PC bei einem Diebstahl mitgenommen oder durch Brand oder Hochwasser zerstört wird?

Die privaten Daten auf einer DVD können Sie vielleicht einem Freund oder Verwandten zur Aufbewahrung geben. Eine DVD luftdicht verpackt im Keller zu lagern ist auch eine brauchbare Idee (wenn der nicht überschwemmungsgefährdet ist). Allerdings sollte man in beiden Fällen über eine Verschlüsselung nachdenken.

Für eine Firma ist ein anderes Gebäude oder ein Platz auf der anderen Seite einer Brandschutztür optimal. Der Chef oder der mit der Datensicherung beauftragte Mitarbeiter könnten die Daten nach Hause mitnehmen.

Die Sicherheitskopien im Tresor der Firma vor Unbefugten zu schützen ist eine gute Idee. Das schützt aber nicht vor allen Gefahren. Bei einem Brand sind die Kopien gefährdet. Übliche Tresore sind dafür gebaut, Papier zu beschützen. Papier entzündet sich erst bei 185 °C. Polycarbonat, das Trägermaterial von DVDs und Magnetbändern, hat sich bei dieser Temperatur bereits verformt. Mehr als 125 °C verträgt es nicht. [2]

2 `http://de.wikipedia.org/wiki/Polycarbonate` zulässige Temperatur 125 °C

Was kann man tun? Lagern Sie nicht alle Kopien im Tresor. Stellen Sie eine wärmedämmende Box für die Datenträger in den Tresor. Es gibt spezielle Datenträgertresore, in denen Ihre Daten ein Feuer überstehen können.

Bedenken Sie, dass Sie nach einem Brand oder Einbruch eventuell tagelang keinen Zugang zu ihren Räumen mit den möglicherweise unversehrten Datenträger haben, solange die Spurensicherung am Werk ist.

Wenn Sie Bänder verwenden, droht eine andere Gefahr: Was ist, wenn Ihr Bandgerät defekt ist? Wenn das Bandgerät samt Server gestohlen oder verbrannt ist, woher bekommen Sie ein neues Bandgerät zum Einlesen der Bänder? Sie sollten sich fragen

- Wie viele Tage würde es dauern, ein Ersatzgerät zu beschaffen?
- Wie exotisch ist Ihr Bandgerät? Wäre es überhaupt wiederbeschaffbar?
- Sie haben jemanden gefunden, der das gleiche Bandgerät benutzt und es Ihnen im Notfall leihen würde. Würde das Ersatzgerät Ihre Bänder lesen können? **Haben Sie das getestet?**

Besprechen Sie das Thema mit Ihrem Hardware-Händler. Vielleicht können Sie mit einem anderen Kunden Ihres Händlers vereinbaren, die Bandgeräte im Störfall gegenseitig auszuleihen. Testen Sie mit wenigsten einem Band, ob das fremde Gerät Ihr Band lesen kann. Wenn Sie Pech haben, ist Ihr Bandgerät schlecht justiert und liest nur die selbst beschriebenen Bänder.

An diese Stelle passt ein unter Administratoren gebräuchlicher Witz: **„Unsere Backups waren in Ordnung, nur die Rücksicherung hat nicht geklappt!“**

```
<!-- Stromversorgung, RAID -->
```

# 7 Der Unterschied zwischen Daten- und Systemsicherung

Mit einem Backup können zwei verschiedene Ziele erreicht werden, die genau unterschieden werden müssen: Systemsicherung oder Datensicherung.

## 7.1 Datensicherung

Eine **Daten**sicherung bewahrt die Ergebnisse Ihrer Arbeit vor Verlust: Dokumente, Fotos, Zeichnungen. Die einzelnen Dateien sind meist nicht groß: Für 400 Fotos, 250 MP3-Dateien oder den Inhalt eines 10 m hohen Bücherstapels genügt ein Gigabyte. Bei vernünftiger Organisation reicht die Speicherkapazität einer CD oder DVD für ein Daten-Backup aus. Eine häufige Sicherung sollte deshalb kein Problem sein.

## 7.2 Systemsicherung

Eine Systemsicherung ermöglicht eine schnelle Wiederherstellung der Arbeitsfähigkeit, wenn das Betriebssystem Schaden genommen hat. Dabei sind vier Probleme zu überwinden.

1. Einige Dateien sind ständig in Benutzung, als Beispiele seien die Registry, die Benutzereinstellungen und die Auslagerungsdatei genannt. Es ist nicht ohne weiteres möglich, diese Dateien zu kopieren, und mit den Windows-Bordmitteln gelingt das schon gar nicht.
2. Auch wenn Sie dem PC eine Pause gönnen, ist Windows nicht untätig. Die Speicherbelegung wird optimiert (Auslagerungsdatei), im Internet wird nach Updates gesucht, und einige Anwenderprogramme speichern von Zeit zu Zeit ihren aktuellen Zustand. Während der Dauer einer Systemsicherung (üblicherweise mehr als 15 Minuten) werden einige der bereits kopierten Dateien verändert. Im Ergebnis enthält die Systemsicherung Bestandteile, die nicht zueinander passen.
3. Es würde nicht genügen, alle Dateien zu kopieren und sie bei Bedarf zurückzukopieren. Einige Dateien müssen sich an einer präzise definierten Stelle der Festplatte befinden, sonst startet das Betriebssystem nicht. Ein Kopierbefehl kann das nicht sichern.
4. Auch wenn Windows nicht mehr starten kann, muss das Zurückkopieren möglich sein.

Daraus ergeben sich drei Bedingungen:

1. Das Sichern und Zurückkopieren muss nicht Datei für Datei, sondern Sektor für Sektor erfolgen. Jeder Sektor muss genau an die ursprüngliche Position zurück.

2. Das Backup-Programm muss von CD startfähig sein. Dadurch werden die Probleme mit ständig benutzten und geänderten Dateien gelöst: Wenn Windows nicht gestartet werden muss, sind alle Dateien unbenutzt.
3. Aus 1. und 2. folgt: Das Backup-Programm muss mit jeder gängiger Hardware zurechtkommen, denn es muss ohne Treiberunterstützung auskommen.

Ein weiteres Problem ist, dass ein Backup-Medium mit hoher Kapazität benötigt wird. Windows XP plus einige Anwendungen belegt reichlich 10 GB, Windows 7 etwa 20 GB und mehr. Durch die Komprimierung werden etwa 30% Speicherplatz gespart. Das ist immer noch zu viel für eine einzelne DVD. Eine Systemsicherung ist deshalb relativ aufwändig.

## 7.3 Vergleich

Wenn das Betriebssystem beschädigt oder infiziert ist und Sie eine Systemsicherung haben, können Sie den PC schon nach einer halben Stunde wieder benutzen. Wenn Sie Daten auf der Systempartition haben, die Sie seit dem letzten Systembackup verändert haben, dauert es ein wenig länger. Wenn Sie kein Systembackup haben, brauchen Sie „nur“ Windows und alle Ihre Anwendungen erneut installieren, Updates installieren und das System an Ihre Bedürfnisse anpassen. Das dauert zwar einen ganzen Arbeitstag oder mehr, aber es ist keine Katastrophe. Deshalb braucht eine Systemsicherung nur in größeren Abständen durchgeführt werden, vorzugsweise nach der Installation neuer Programme oder nach anderen größeren Änderungen am Betriebssystem.

Wenn Sie jedoch keine Datensicherung haben, ist Ihre Arbeit weg. Für immer.

Wenn Ihre letzte Datensicherung einen Monat alt ist, müssen Sie die Arbeit des gesamten zurückliegenden Monats noch einmal wiederholen.

# 8 Drei-Generationen-Sicherung

## 8.1 Tägliche Sicherung

Gegen Festplattenausfälle hilft eine regelmäßige, ausreichend häufige Datensicherung. Wenn man jedesmal ein anderes Sicherungsmedium nimmt und die Medien anschließend möglichst lange aufbewahrt, hat man sich auch gegen die unauffälligen, „schleichenden“ Schäden geschützt. In Firmen ist es üblich, an jedem Arbeitstag ein Backup zu erstellen, von denen einige zehn Jahre lang aufbewahrt werden, um gesetzliche Vorgaben zu erfüllen.

> Es wäre ein nahezu ideales Verfahren der Datensicherung, jeden Tag den gesamten Festplatteninhalt zu sichern und jedes Sicherungsmedium (mindestens) zehn Jahre lang aufzubewahren.

Jeden Datenträger aufzuheben würde allerdings 365 Datenträger pro Jahr erfordern. Das ist natürlich kaum praktikabel, der Aufwand ist sehr hoch, so wiegen z.B. (unverpackte) DVDs für 10 Jahre knapp 60kg. Wie kann man die Zahl der benötigten Datenträger verringern, ohne die Sicherheit wesentlich zu verringern?

## 8.2 Sicherung hochverfügbarer Systeme

Für manche Anwendungen reicht es nicht aus, die Daten nur einmal täglich zu sichern. Stellen Sie sich das Chaos vor, wenn das weltweite Flug-Reservierungssystem ausfällt und alle Buchungen der letzten Stunden verloren sind! Für derartig kritische Anwendungen reicht nicht mal eine stündliche Sicherung. Es wäre absolut ideal, wenn jede Datei unmittelbar nach jeder Änderung gesichert wird. Alle diese „Schnappschüsse“ werden aufbewahrt. Dieses Verfahren heißt „**C**ontinuous **D**ata **P**rotection (CDP)“. Im Recovery-Fall kann der Zustand des Datenträgers auf jeden beliebigen Zeitpunkt zurückgesetzt werden.

Wenn Datenverluste von einigen Minuten zugelassen werden können, kann das „NCDP“-Verfahren verwendet werden. **N**ear **C**ontinuous **D**ata **P**rotection sichert den Datenbestand in größeren Zeitabständen, beispielsweise stündlich oder alle fünf Minuten. Dazwischenliegende Zeitpunkte lassen sich nicht wiederherstellen, aber in vielen Fällen stört das nicht.

Beide Verfahren (CDP und NCP) erfordern allerdings einen gewaltigen Aufwand und sind für Privatanwender und die meisten Firmen nicht praktikabel. Deshalb beschränken wir die weiteren Betrachtungen auf eine maximal tägliche Datensicherung.

## 8.3 Das Prinzip der Drei-Generationen-Sicherung

**Magnetbänder**

Eine jahrzehntelang bewährtes Verfahren beruht auf dem „Drei-Generationen-Prinzip“, das oft auch als „Großvater-Vater-Sohn-Prinzip“ bezeichnet wird. Seit Jahrzehnten werden die Daten in den Rechenzentren der Welt nach diesem Prinzip auf Magnetbänder gesichert, auch heute noch.

Für die erste Generation verwenden Sie fünf bis sieben Bänder, für jeden Tag der Woche eins. Beschriften Sie diese mit „Montag“, „Dienstag“ usw. In jeder weiteren Woche kommen diese Bänder erneut zum Einsatz.

Der Freitag ist eine Ausnahme. Sie brauchen fünf Freitagsbänder, die Sie am Besten mit „Freitag 1. Woche“ usw. beschriften und einen Monat lang aufheben. Diese Bänder bilden die zweite Generation. Achten Sie darauf, dass am Freitag eine vollständige Sicherung erfolgt, an den anderen Tagen darf es auch eine inkrementelle oder differenzielle Sicherung sein.

Von jedem Monatsanfang wird eine Sicherung drei Monate lang oder - besser noch - für ein ganzes Jahr aufbewahrt. Dafür brauchen Sie drei oder zwölf Bänder. Dies ist die dritte Generation.

Vernünftigerweise bewahrt man das Band mit dem Jahresabschluss noch zehn Jahre auf, das wäre die vierte Generation.

**Insgesamt benötigen Sie etwa zwanzig Bänder für das erste Jahr und eins für jedes Folgejahr. Berücksichtigt man den Verschleiß, werden pro Jahr vier weitere Bänder benötigt.**

**Optische Medien**

Anstelle von Bändern können natürlich auch andere Sicherungsmedien verwendet werden, beispielsweise DVDs[1]. Für die tägliche und wöchentliche Sicherung verwenden Sie zweckmäßigerweise mehrfach beschreibbare DVDs. Jedes Brennprogramm bietet einen Dateivergleich nach dem Brennen an. Nutzen Sie diese Funktion zumindest hin und wieder, um unzuverlässige DVD rechtzeitig aussondern zu können.

Für die Monats-CDs sollten Sie zu hochwertigeren einmal- oder mehrfach-beschreibbaren Scheiben greifen. Immerhin müssen diese Datenträger ein Jahr lang aufgehoben werden.

Für die Jahressicherungen sind hochwertige DVD-R[2] mit UV-Schutz empfehlenswert. Wenn Ihr Brenner damit umgehen kann, sollten Sie zu DVD-RAM[3] greifen. DVD-RAM haben die besten Fehlerkorrekturmechanismen und sind darüber hinaus die einzigen optischen Scheiben, für die in der Spezifikation eine Mindesthaltbarkeit gefordert ist: Sie müssen mindestens 30 Jahre haltbar sein.

Möglicherweise ist es ratsam, für die Monatssicherungen grundsätzlich einmal-beschreibbare Scheiben zu verwenden. Stellen Sie die geringen Preise für DVD-R ins Verhältnis zum Aufwand, die DVD-RW[4] vor Gebrauch zu löschen. Für die Sicherheit und die Langzeitlagerung ist es ohnehin besser, alle Monate aufzubewahren. Die Jahressicherungen können dann entfallen.

1 http://de.wikipedia.org/wiki/DVD
2 http://de.wikipedia.org/wiki/DVD-R
3 http://de.wikipedia.org/wiki/DVD-RAM
4 http://de.wikipedia.org/wiki/DVD-RW

Es ist immer empfehlenswert, mindestens zwei **verschiedene** DVD-Fabrikate zu verwenden. So sind Sie selbst dann noch auf der sicheren Seite, wenn eine Charge einen versteckten Fehler hat und sämtliche DVDs einer Spindel nach einigen Monaten nicht mehr lesbar sind. Wenn Sie mehr als einen DVD-Brenner haben, sollten Sie hin und wieder den anderen Brenner verwenden. Vielleicht ist Ihr bevorzugter Brenner nicht mehr präzise justiert? Vielleicht produziert er seit Monaten DVDs, die außer ihm kein anderes Gerät lesen kann? Sie sollten von Zeit zu Zeit mit einer Ihrer DVDs ausprobieren, ob sie sich in einem anderen Laufwerk lesen lässt.

Ja, ja, ich weiß, das ist paranoid. Aber wenn es um die Sicherheit geht, sollte man wenigstens zeitweise ein wenig paranoid sein.

## 8.4 Die Protokollierung

Jede durchgeführte Datensicherung sollte protokolliert werden. Das Protokoll sollte enthalten:

- Datum, evtl. Uhrzeit
- Bezeichnung des Datenträgers, sofern nicht offensichtlich
- Art der Sicherung: Voll, differenziell oder inkrementell
- Eventuelle Auffälligkeiten
- Irgendeine Angabe, die einen Vergleich mit Vortagen ermöglicht, z. B. Anzahl der gesicherten Dateien, benötigte Zeit oder benötigter Speicherplatz. Wenn die Datensicherung funktioniert, sollten diese Zahlen allmählich wachsen, außer jemand hat „groß aufgeräumt“.

Welchen Sinn hat die Protokollierung?

- Sie hilft dabei, Unregelmäßigkeiten zu entdecken.
- Sie hilft Ihnen zu bestimmen, welche Dateiversionen auf welchem Datenträger sind. Das ist ganz besonders wichtig, wenn Sie die Datensicherung nicht täglich vornehmen.
- Sie hilft Ihnen, die zu einer inkrementellen Sicherung zugehörige vorangehende Vollsicherung zu ermitteln.
- Sie führt Ihnen selbst (und eventuell Ihrem Chef) vor Augen, wie zuverlässig Sie die Sicherungen vornehmen.

# 9 Vergleich von Backup-Geräten

**Welche Geräte kann man benutzen, um eine Datensicherung durchzuführen?**

## 9.1 DVD

Einen Brenner hat ja wohl fast jeder, und Rohlinge sind billig. Problematisch ist der hohe Arbeitszeitaufwand: Das Brennprogramm starten, Rohling einlegen, zu sichernde Dateien auswählen, Brennvorgang starten und überwachen. Später das Programm beenden, die DVD beschriften und einlagern. Die Hersteller der Brennprogramme bieten keine praktikable Möglichkeit an, das Brennen von Routinesicherungen zu automatisieren. Allerdings ist das kein Grund, auf jegliche Datensicherung zu verzichten. Von Zeit zu Zeit das Brennprogramm zu starten, den Ordner „Dokumente und Einstellungen“ in das Fenster des Brennprogramms zu ziehen und ein paar mal auf „Weiter“ zu klicken, dauert nicht mal zwei Minuten. Damit sind Eigene Dateien, Desktop und die Favoriten des Internet Explorers gesichert. Das ist zwar nicht alles, aber ein großer Teil Ihrer Daten.

Ein weiterer Nachteil ist die Kapazität, die im Vergleich zur Festplatte gering ist. Zur Sicherung eines frisch installierten Windows mit ein paar Anwendungen werden zwei bis drei DVDs gebraucht. Die Daten „von Hand“ auf mehrere DVDs aufzuteilen, ist nicht praktikabel, zumal der Windows Explorer das Kopieren abbricht, sobald er auf eine in Benutzung befindliche Datei trifft. Die Verwendung eines Image-Programms löst das Problem der Aufteilung der Daten und der benutzten Dateien. Das Problem mit der Kapazität aber bleibt. Kein vernünftiger Mensch wird regelmäßig Daten sichern, wenn er dafür zehn DVDs braucht.

Wenn man nur eine kleine Datenmenge zu sichern hat (beispielsweise eine Zuwachssicherung), kann die Verwendung einer CD-ROM sinnvoll sein. Sie sind billiger als DVD-Rohlinge und etwas sicherer, weil die Daten weniger dicht gepackt sind.

## 9.2 BD (Blu-ray)

Die Kapazität ist zwar größer, aber für heute übliche Datenmengen immer noch nicht groß genug. Zudem ist ein BD-Brenner deutlich teurer als eine externe Festplatte.

## 9.3 Die eigene Festplatte

Auf den ersten Blick klingt es verblüffend, die eigene Festplatte für eine Datensicherung benutzen zu wollen. Was ist, wenn die Festplatte kaputt geht? Dagegen hilft nur eine Datensicherung auf ein externes Medium. Weil aber die kleinen Unfälle weitaus häufiger sind als ein Festplattenausfall, gibt es zwei wichtige Anwendungen für die interne Festplatte:

- Wenn man sicherheitshalber ein Image seines Betriebssystems auf DVD brennt oder auf einer Partition seiner Festplatte aufbewahrt, kann man jederzeit eine unbeschädigte Version seines Betriebssystems wiederherstellen. Das Erstellen eines Images erfordert nur wenige Minuten Arbeit, erspart aber viele Stunden, wenn eine Neuinstallation notwendig werden sollte. Optimalerweise enthält das Image keine Daten, nur Programme, so dass man bei einem Festplattenausfall nur Arbeitszeit verliert.
- Die eigene Festplatte kann man verwenden, um den Zustand wichtiger Dokumente für einige Tage zurück aufzubewahren. Das kann man automatisieren (siehe das Kapitel über zyklische Sicherung), oder man macht vor größeren Aktionen vorsorglich eine Kopie.

## 9.4 Festplatte eines anderen PC

Wenn Sie zwei oder mehr über ein Netzwerk verbundene PCs haben, ist eine erstklassige Datensicherung ohne irgendeine Investition möglich. Kopieren Sie einfach die zu sichernden Daten auf den jeweils anderen PC! Dieses Verfahren basiert auf der Erkenntnis, dass die Festplatte der meisten PC zu weniger als einem Fünftel belegt ist. Folglich ist ein genügend großer Bereich frei, um die Datensicherung eines anderen PC unterzubringen. Dazu müssen die Festplatten geeignet partitioniert sein. Richten Sie auf dem ersten PC eine Partition für die Sicherung des zweiten PC ein und umgekehrt.

Jetzt brauchen Sie nur noch eine Stapeldatei auf jedem PC, die mit dem Befehl XCOPY oder ROBOCOPY das Kopieren übernimmt. Diese Batch-Datei lassen Sie vom PC täglich automatisch ausführen. Wählen Sie dafür einen geeigneten Zeitpunkt. Es muss ein Zeitpunkt sein, wann mit hoher Wahrscheinlichkeit beide PC eingeschaltet sind und wenn der Leistungsabfall während der Sicherung nicht stört. Wenn Sie den Beginn der Sicherung auf den Beginn der Frühstücks- oder Mittagspause legen, verpassen Sie den Anfang der Pause nicht.

In manchen Firmen kommt ein Backup-PC zum Einsatz, der keine andere Aufgabe hat, als die Datensicherungen aller anderen PC zu speichern. Als Backup-PC kann durchaus ein älterer, leistungsschwacher PC verwendet werden, wichtig ist nur dessen Festplattenkapazität. Wenn dieser PC zeitgesteuert hochgefahren und nach der Sicherung automatisch heruntergefahren wird, ist der Energieverbrauch gering.

| **Vor- und Nachteile** | | Kommentare |
|---|---|---|
| Hardware | keine Kosten | |
| Software | keine Kosten | So schwierig ist eine Batchdatei nicht, und manuell geht es auch |
| Automatisierbar | ja | Ein Eintrag im Taskplaner ist nicht schwer |
| Einmaliger Zeitaufwand | 30 Min | um eine Stapeldatei zu schreiben und zu testen |

| **Vor- und Nachteile** | | Kommentare |
|---|---|---|
| Täglicher Zeitaufwand | 1 Min | für eine gelegentliche Kontrolle |
| Externe Gefahren | groß | Durch Feuer oder Diebstahl gehen vermutlich beide PC verloren |

## 9.5 Datensicherung über das Internet

Die Idee hört sich modern an. Bei manchen Anbietern kostet es nicht mal was, eine Kopie seiner privaten Daten im Internet zu hinterlegen.

- Bei www.xdrive.com bekommen Sie kostenlos 5 GB Speicherplatz.
- Auch bei www.divshare.com gibt es 5 GB gratis. Ausführbare Dateien dürfen nicht hochgeladen werden. Per E-Mail können Sie Bekannten Ihre Dateien zugänglich machen. Ein Passwortschutz ist möglich.

Ein Backup bei diesen Anbietern erfordert viele Klicks und ist deshalb für eine routinemäßige Datensicherung nicht geeignet.

Es gibt aber noch weitere Probleme.

- Ein Problem ist die geringe Datenübertragungsrate. In der Upstream-Richtung (vom Computer zum Internet) ist die Datenübertragung langsam. Eine DSL-2000-Leitung beispielsweise überträgt in der Upstream-Richtung maximal 384 kbit/s, DSL-6000 und höher kommen nicht über 1000 kbit/s. Pro Nacht lassen sich typischerweise 0,5 bis 2 Gigabyte sichern. Die Übertragungsrate schwankt stark: Das Internet ist unterschiedlich schnell. Wenn die zu sichernden Dateien durchschnittlich klein sind, läuft die Übertragung langsam, bei großen Dateien geht es schneller.
- Die Telekom trennt jede Nacht die DSL-Verbindung für ein paar Sekunden, auch bei anderen Anbietern können kurze Unterbrechungen auftreten. Wenn Sie keine Spezialsoftware haben, welche die Verbindung wiederherstellt, war's das für diese Nacht.
- Wenn eine VPN-Verbindung (eine verschlüsselte Verbindung) benutzt wird, muss sie sich automatisch aufbauen lassen. Die Übertragung muss automatisch starten. Dazu ist vermutlich Spezialsoftware nötig.
- Wenn man ganz konsequent nur die geänderten Daten überträgt, können sich trotz der geringen Übertragungskapazität im Verlauf von Monaten größere Datenmengen auf der entfernten Festplatte ansammeln. Wie lange würde es im Schadensfall dauern, den gesamten Datenbestand über das Internet zurückzukopieren? Bei einem Experiment dauerte es 30 Nächte, 35 GB von einer Festplatte über das Internet zu sichern. Für die Rücksicherung steht zwar die höhere Downloadrate zur Verfügung, trotzdem hätte die Rücksicherung selbst im 24-Stunden-Betrieb mehrere Tage gedauert. Können Sie sich im Notfall derart lange Wartezeiten leisten?
- Weil die Sicherung die gesamte Bandbreite der Internetverbindung benötigt, würde sie tagsüber die Arbeit sehr behindern. Deshalb ist die Sicherung nur nach Arbeitsschluss sinnvoll.
- Möglicherweise sind einige Dateien so groß, dass sie sich nicht in einer Nacht übertragen komplett lassen. Dann müssen Sie ein Backup-Programm benutzen, welches den sogenannten „Restartable Mode“ beherrscht: Nach einem Abbruch muss das Kopieren an der unterbrochenen Stelle fortgesetzt werden können.

In welchen Fällen ist die Sicherung über das Internet sinnvoll? Die geringe Datenmenge, die sich in einer Nacht übertragen lässt, passt locker auf einen USB-Stick. Bei Bedarf eine (mehrfach beschreibbare) DVD zu brennen geht schneller, eine externe Festplatte oder ein externes Bandgerät sind bequemer zu benutzen. Den PC am Abend bzw. die ganze Nacht eingeschaltet zu lassen, kostet Sie eine Menge Energie, und der Verschleiß des Computers steigt. Die Festplatte bekommt nie Zeit zum Abkühlen.

Am sinnvollsten scheint die Internetsicherung zu sein, wenn

- eine Sicherheitskopie der wichtigsten Daten außer Haus gelagert werden soll und sich niemand die Mühe machen will, täglich einen Datenträger nach Hause mitzunehmen oder in den Keller bzw. den Safe zu schaffen,
- die Sicherung erst Nachts erfolgen darf, weil einzelne Mitarbeiter länger arbeiten als der Datensicherungsbeauftragte oder weil die Daten z. B. von einer Filiale oder externen Mitarbeitern noch spät benutzt werden
- eine Energieersparnis nicht eintritt, weil der PC ohnehin nie abgeschaltet wird
- die Daten einer Filiale zur Zentrale übertragen werden, wo sie anschließend der Firmenleitung zur Verfügung stehen
- es nicht wünschenswert ist, dass jeden Abend der letzte Mitarbeiter einen Datenträger mitnehmen muss, denn
  - der Datenträger könnte auf dem Weg verloren gehen und in falsche Hände geraten
  - der jeweils letzte Mitarbeiter soll vertrauliche Daten nicht in die Hände bekommen
  - es könnte vergessen werden

### 9.5.1 Datensicherheit

In den Rechenzentren der großen Anbieter werden hochwertige RAID-Systeme eingesetzt, so dass auch bei Ausfall mehrerer Festplatten keine Daten verloren gehen. Teilweise werden gespiegelte Server eingesetzt oder ein räumlich entferntes Zweitrechenzentrum, so dass auch bei Ausfall eines Servers oder des ganzen Rechenzentrums Ihre Daten verfügbar bleiben. Außerdem werden regelmäßig Backups durchgeführt. Ihre Daten sind also sehr sicher. So steht es jedenfalls in der Reklame.

Allerdings sind Zweifel angebracht. Wie oft wird ein Backup durchgeführt? Auch die ausgereifteste Infrastruktur kann nicht vor **allen** menschlichen und technischen Fehlern schützen. Nehmen wir Amazon als Beispiel. Amazon ist ein bedeutender Anbieter von Online-Speicherplatz. Im April 2011 verloren zahlreiche Kunden ihre auf den Amazon-Servern gespeicherten Daten. Der Analyst Henry Blodget meint dazu, *dass Amazon (so wie andere Cloud-Anbieter auch) seine Kunden mit dem Versprechen regelmässiger Backups in falscher Sicherheit wiege. Oft würden die zu sichernden Dateien bei genauerem Hinsehen nur irgendwo auf dem gleichen Server oder im gleichen Server-Raum kopiert - mit einer echten Disaster-Recovery-Strategie habe das wenig gemein.* [1]

Doch Amazon traf es am 7. August 2011 erneut. Der Strom fiel aus und die Notstromgeneratoren funktionierten nicht. Die Sicherheitskopien waren teilweise unbrauchbar: Die Backup-Software erwies sich als fehlerhaft. Nach 68 Stunden hatten 85% der Kunden ihre

1 Datenverlust bei Amazon `http://www.computerworld.ch/news/it-services/artikel/amazon-datenverlust-durch-ec2-crash-56420/`

Daten zurück, am vierten Tag 98%. Kunden, die ihre Daten mehrere Tage nicht benutzen konnten, durften den Amazon-Service 10 Tage lang gratis nutzen. 30 Tage Gutschrift erhielten die Kunden, deren Daten verloren gegangen sind. Es ist vorbildlich, dass Amazon einen Bericht über den Vorfall im Internet veröffentlicht hat, damit die Branche daraus lernen kann. *„The human checks in this process failed to detect the error. … We learned a number of lessons from this event.“* [2]

Um die Rechenzentren ausfallsicher zu machen, ist ein überaus komplexes Zusammenwirken von Hard- und Software notwendig. Bei der benötigten Hardware handelt es sich oft um Prototypen, und die Sicherheitssoftware enthält Fehler wie jede andere Software auch. Wenn es zu einem Problem kommt, ist dieses meist so komplex, dass es zu mehrtägigen Ausfällen kommt.

### 9.5.2 Datenschutz

- Sie wissen nicht, in welchem Land die Server mit Ihren Daten stehen und welche Datenschutzgesetze dort anwendbar sind. Und was die Provider mit Ihren Daten machen, erfahren Sie nicht.
  - In den USA behalten sich einige Anbieter vor, Ihre Daten zu sichten, um Raubkopien oder "anstößige" Daten zu entfernen.
  - In vielen Ländern haben Geheimdienste und Polizei Zugriff.
  - Google durchsucht E-Mails, Dokumente und Tabellen, z. B. um passende Werbung einblenden zu können.
  - Die Daten sollten über eine sichere Verbindung übertragen werden, damit niemand die Verbindung abhören kann (VPN).
  - Es gibt auch positive Ausnahmen. Alle Server von Strato stehen in Deutschland und unterliegen den relativ strengen deutschen Datenschutzgesetzen. Strato sichert zu, die Daten niemals weiterzugeben.
- Kontodaten und jegliche Passwörter sollte man nicht im PC speichern, und irgendwohin übertragen sollte man sie schon gar nicht!
- Deshalb sollten wichtige Daten bereits vor der Übertragung verschlüsselt werden, denn es ist bedenklich, seine wichtigsten, vertraulichen Daten einer unbekannten Firma anzuvertrauen. Es sollte eine exzellente Verschlüsselung mit einem sicheren Passwort sein, denn der Empfänger Ihrer Daten (oder deren Dieb) hat alle Zeit der Welt, den Code zu entschlüsseln.

### 9.5.3 Datendiebstahl

Die Server der großen Firmen und der Internetprovider sind bevorzugtes Angriffsziel von Hackern. Ein erfolgreicher Einbruch in ein Rechenzentrum hebt das Prestige eines Hackers unter seinen Kumpeln, außerdem kann es finanziell sehr lukrativ sein, die gefundenen Daten zu verwerten. Es vergeht kein Monat, ohne dass einige namhafte Firmen gezwungen sind zuzugeben, dass Daten gestohlen wurden. Eine kleine Auswahl aus den zweiten Quartal 2011:

2 Erneut Datenverlust bei Amazon (engl. Originalbericht) `http://aws.amazon.com/de/message/2329B7/`

- 2011/04: Amazon, Ashampoo, Sony Playstation;
- 2011/05: Mindfactory, Planet4one, Lockheed Martin, Adcell, Citibank;
- 2011/06: Acer, Sony Pictures, Neckermann, Google Mail, Nitendo).
- Selbst die Sicherheitsspezialisten sind nicht sicher.
  - Die US-Sicherheitsfirma Barracuda Networks wurde im April 2011 gehackt[3].
  - Im Juni 2011 wurden die Firma RSA gehackt. RSA verwaltet die Sicherheitsschlüssel von Regierungen, Rüstungsfirmen, Geheimdiensten und Großkonzernen. Die gestohlenen Schlüssel wurden u. a. benutzt, um der Rüstungsfirma Lockheed Martin Konstruktionsunterlagen zu entwenden. RSA musste etwa 40 Millionen Kunden empfehlen, ihre Passwörter zu wechseln [4].

Wenn Sie eine Suchmaschine nach "Datendiebstahl 2011" fragen, finden Sie noch mehr Beispiele.

Aber das ist nur die Spitze des Eisberges. Fragen Sie sich mal:

- Wie viele Firmen haben nicht gemerkt, dass Daten gestohlen wurden?
- Wie viele Firmen haben zwar es gemerkt, aber geben es aus Angst vor Imageschaden nicht zu (bzw. geben es erst zu, wenn die Beweise unübersehbar sind?)

3 Sicherheitsfirma Barracuda Networks gehackt `http://www.heise.de/security/meldung/Datendiebstahl-bei-Netzwerk-Sicherheitsfirma-1226365.html`

4 Sicherheitsspezialist RSA gehackt `http://article.wn.com/view/2011/06/07/Millionenfacher_Austausch_von_PasswortSchl_sseln/`

| **Einige Anbieter von Online-Backup-Speicherplatz** | | | | | |
|---|---|---|---|---|---|
| **Anbieter** | Adresse | Server in | gratis | 20 GB | 100 GB |
| Dropbox[5] | dropbox.com | USA | 2 GB | | 199$ |
| GMX[6] | gmx.net | USA | | | |
| Windows Live SkyDrive[7] | windowslife.de | Irland | 25 GB | - | |
| Amazon Cloud Drive[8] | amazon.com/clouddrive | USA | 5 GB | - | 100 $ |
| Strato HiDrive[9] | strato.de | DE | - | 24 € | 48 € |
| F-Secure[10] | | | | | |
| Norton 360[11] | | | | | |

5 http://de.wikibooks.org/wiki/Datensicherung%2F%20Werkzeuge%2F%20Online-Backup%2F%20Dropbox

6 http://de.wikibooks.org/wiki/Datensicherung%2F%20Werkzeuge%2F%20Online-Backup%2F%20GMX

7 http://de.wikibooks.org/wiki/Datensicherung%2F%20Werkzeuge%2F%20Online-Backup%2F%20Windows%20Live

8 http://de.wikibooks.org/wiki/Datensicherung%2F%20Werkzeuge%2F%20Online-Backup%2F%20Amazon

9 http://de.wikibooks.org/wiki/Datensicherung%2F%20Werkzeuge%2F%20Online-Backup%2F%20Strato

10 http://de.wikibooks.org/wiki/Datensicherung%2F%20Werkzeuge%2F%20Online-Backup%2F%20F-Secure

11 http://de.wikibooks.org/wiki/Datensicherung%2F%20Werkzeuge%2F%20Online-Backup%2F%20Norton%20360

### 9.5.4 E-Mail

Im studentischen Bereich hat es sich bewährt, Daten zu sichern, indem man sie häufig per E-Mail an sich selbst schickt und weniger häufig an einige seiner Freunde. Die zu sichernde Datenmenge ist meist winzig und die Daten sind nicht im geringsten Geheim. Typischerweise betrifft dies Examensarbeiten von wenigen Megabyte Größe, die mit der Abgabe beim Prüfungsamt sowieso öffentlich einsehbar werden. Schön an diesem Verfahren ist vor allem, dass die Daten auch bei einem Zimmerbrand oder bei starken Unwetter in auf das Zimmer hernieder stürzende Baukräne oder einem anderen Totalausfall des PC gesichert sind. Durch den Versand an viele Adressaten stellt auch der Ausfall eines Providers kein Problem da.

## 9.6 Externe Festplatte

Die ist wenigstens groß genug, und man kann sie vom PC trennen. Manchen Festplatten liegt ein Datensicherungsprogramm bei, ansonsten kann eine Stapeldatei mit XCOPY oder ROBOCOPY verwendet werden.

Kein anderes Medium sichert die Daten schneller. Genug Platz hat die Festplatte meist auch. Wenn man eine Datei verloren hat, ist sie auf der externen Festplatte leicht aufzufinden.

Allerdings sind externe Festplatten weniger sicher als allgemein angenommen. Die Erschütterungen beim Umhertragen sind nachteilig. Die Gefahr, während des Betriebes an die Festplatte anzustoßen, muss vermutlich berücksichtigt werden. Wenn man die Datensicherung auf das Arbeitsende verschiebt - wer schaltet hinterher die Platte aus, damit sie nicht überhitzt?

Auch wenn die Festplatte intakt bleibt, können Daten verloren gehen. Denken Sie **ausnahmslos immer** daran, die Festplatte abzumelden, bevor Sie den USB-Stecker herausziehen? Ein Wackelkontakt kann alle Daten in Sekundenbruchteilen vernichten.

**Eine Festplatte reicht nicht!**

Wenn Sie eine einzige Festplatte als alleiniges Backup-Gerät einsetzen, reicht das nicht. Nehmen wir an, Sie machen an jedem Abend ein Backup. Am Montagabend sind die Daten auf dem PC und auf der externen Festplatte noch OK. Im Laufe des Dienstags beschädigen Sie unbemerkt eine Datei oder Sie löschen einen Ordner durch einen falschen Klick. Das ist nicht schlimm, die Sicherung vom Montag ist ja noch OK. Wenn Sie jedoch den Fehler im Laufe des Dienstags nicht bemerken und die Sicherung immer ins gleiche Verzeichnis der Festplatte speichern, werden Sie am Abend das einzige intakte Backup überschreiben und die Daten sind endgültig weg. Deshalb sollten Sie das Backup jedes neuen Tages in ein neues Verzeichnis schreiben, damit der Vortag erhalten bleibt.

Auch damit sind Sie noch nicht auf der sicheren Seite. Was passiert bei einer Virusinfektion? Auf eine externe Festplatte kann der Virus überspringen und auch ein Softwarefehler kann das Ende aller Daten bedeuten. Bei Benutzung von Bändern oder DVDs besteht diese Gefahr nicht, denn sie werden nach dem Beschreiben herausgenommen.

Unter anderem deshalb hat sich das Großvater-Vater-Sohn-Prinzip bewährt. Mit Festplatten kann man die gleiche Sicherheit erreichen, wenn man zwanzig davon verwendet oder wenigstens zwei bis drei, die nach einem durchdachten Plan reihum verwendet werden.

Freilich ist das teuer. Wenn Sie mit nur einer Festplatte auskommen müssen, sollten Sie hin und wieder eine weitere Sicherung auf DVD oder einen USB-Stick dazwischenschieben.

| **Vor- und Nachteile** | | Kommentare |
|---|---|---|
| Hardware | etwa 100€ | pro Festplatte |
| Software | keine Kosten | So schwierig ist eine Batchdatei nicht, und manuell geht es auch |
| Automatisierbar | nein | Das An- und Abstecken der Platte lässt sich nicht automatisieren |
| Einmaliger Zeitaufwand | 30 Min | um eine Stapeldatei zu schreiben |
| Täglicher Zeitaufwand | 3+3 Min | Anstecken, bis Ende der Sicherung warten, deaktivieren, wegräumen |
| Externe Gefahren | gering | wenn die Platte weit entfernt vom PC gelagert wird |

Empfehlungen:

- Benutzen Sie mindestens zwei externe Festplatten im Wechsel.
- Lassen Sie die Festplatte nicht dauernd eingeschaltet, sonst überhitzt sie.
- Lagern Sie die Festplatte über Nacht auswärts, im Safe oder zumindest etwas entfernt.

## 9.7 USB-Stick

Die Kapazität ist geringer und der Anschaffungspreis auch, alle anderen Eigenschaften sind denen einer „Externen Festplatte“ vergleichbar.

## 9.8 Bandgerät

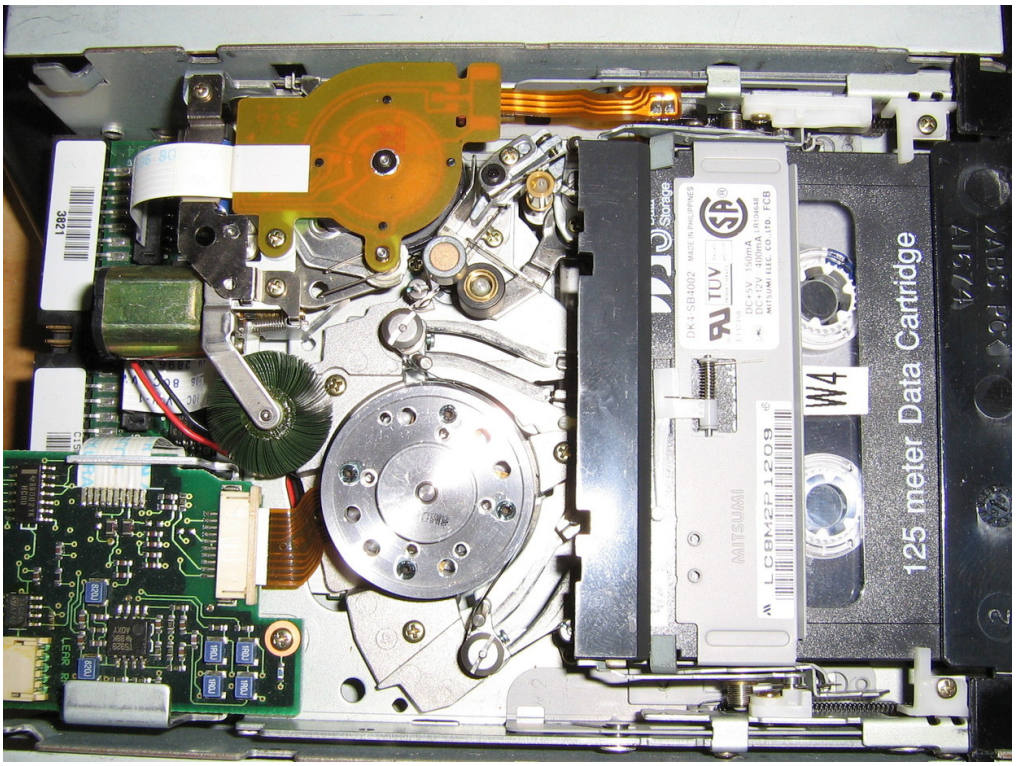


**Abb. 1**

Bandgeräte sind sehr teuer, trotzdem sind sie für eine professionelle Datensicherung kaum entbehrlich. DVDs haben einfach nicht genug Kapazität, und das Brennen lässt sich kaum automatisieren. Dazu kommt der hohe Zeitaufwand. Um 100 GB Daten zu sichern, müsste jemand fast den ganzen Tag bzw. die Nacht 22 DVDs wechseln und beschriften. 100 GB auf Band zu sichern kann zwar einige Stunden dauern, muss aber nicht beaufsichtigt werden. Mehr noch: Sogenannte „Tape Libraries“ (Bandroboter) können eine Woche lang automatisch die Bänder wechseln.

Die aktuelle Technologie heißt "LTO Ultrium" und wird von IBM, HP und Quantum gemeinsam ständig weiterentwickelt. Die Partner wollen alle zwei Jahre eine neue Laufwerksgeneration mit verdoppelter Kapazität und anderthalbfacher Transferrate vorstellen. Unternehmen müssen immer größere Datenmengen speichern und archivieren, und am preiswertesten geht das mit Bandgeräten.

| **Typ** | | Kapazität | Datenrate | Zeit zum Vollschreiben | Zeit für 5 GB |
|---|---|---|---|---|---|
| LTO | Linear Tape Open Version Ultrium 7[12] | 6400 GB | 315 MB/s | 5,6 h | 16 sek |
| AIT | Advanced Intelligent Tape[13] | 400 GB | 7 MB/s | 16 h | 12 min |
| DLT | Digital Linear Tape[14] | 300 GB | 11 MB/s | 8 h | 8 min |
| DVD | 8x (zum Vergleich) | 4,7 GB | 7 MB/s | 12 min | 13 min |

12 http://de.wikipedia.org/wiki/Linear_Tape_Open
13 http://de.wikipedia.org/wiki/Advanced%20Intelligent%20Tape
14 http://de.wikipedia.org/wiki/Digital%20Linear%20Tape

## 9.9 Externes RAID-System

In manchen Firmen sind die zu sichernden Datenmengen so groß, dass sie nicht auf ein Band passen. Nacheinander mehrere Bänder einzulegen scheidet aus: Es wäre zu teuer, mitten in der Nacht einen Mitarbeiter zum Bandwechsel in die Firma zu schicken. Theoretisch könnte sich die Firma einen Bandroboter anschaffen, der die Bänder automatisch wechselt. Praktisch scheitert die Sicherung auf mehrere Bänder oft aus einem profanen Grund: Die Nacht ist zu kurz, denn Bandgeräte sind relativ langsam. Es dauert meist länger als eine Stunde, ein Band vollzuschreiben. Eine Umfrage der Zeitschrift „Computer Reseller News“ zeigte, dass ein Drittel der mittelständigen Betriebe es nicht schaffen, im verfügbaren Zeitrahmen alle ihre Daten zu sichern.

Einen möglichen Ausweg stellen sogenannte „Appliances“ dar. Das sind Computersysteme, die auf das Speichern von großen Datenmengen spezialisiert sind. Die Daten werden auf eine größere Anzahl von Festplatten verteilt, die als RAID-5-System arbeiten, manchmal auch im RAID-6-Modus (das heißt, es dürfen zwei Platten gleichzeitig ausfallen, ohne dass Daten verloren gehen). Diese Appliances werden an das Netzwerk angeschlossen und sinnvollerweise in einen Raum gestellt, der weit genug vom Server entfernt ist.

## 9.10 NAS

Network Attached Storage, abgekürzt NAS, ist ein Netzwerkspeicher für die gemeinsame Nutzung durch mehrere PC. Die kleineren Geräte mit einer Festplatte sind nicht viel größer als ein dickes Buch. Es handelt es sich um einen kleinen Fileserver, oft mit dem Betriebssystem Linux. Weil es sich um PCs ohne Ein- und Ausgabegeräte handelt, werden sie über den Webbrowser eines der angeschlossenen PC konfiguriert. NAS haben außer einem Einschalter keine Bedienelemente.

NAS werden üblicherweise als gemeinsamer Datenspeicher eingesetzt. Der Benutzer kann seine Dateien in Ordnern oder Partitionen ablegen. Es können Zugriffsrechte vergeben werden. Es spricht nichts dagegen, die lokalen Daten der angeschlossenen PCs auf dem NAS abzulegen. Bedenken Sie aber:

- Im Unterschied zu externen Festplatten sind NAS für den Dauerbetrieb konzipiert. Man muss sie nach der Datensicherung nicht abmelden und ausstöpseln. Dieser Vorteil ist zugleich ein Nachteil: Wenn ein Virus einen der PC befällt und dessen Daten verschlüsselt oder löscht, macht er das vermutlich auch mit allen Backups auf dem NAS.
- Einige professionellere Geräte haben mehrere Festplatten, die meist als RAID-Verbund geschaltet sind (beim RAID-Verfahren werden Festplatteninhalte doppelt gespeichert, so dass selbst beim Ausfall einer der Festplatten keine Daten verloren gehen). Gegen Viren oder versehentliches Löschen von Dateien helfen die doppelten Festplatten allerdings nicht. Einige NAS verwenden ein proprietäres (herstellereigenes) Speicherformat, so dass nach einem Defekt an der Geräteelektronik die unversehrten Festplatten möglicherweise nicht ausgelesen werden können.
- Wohin werden die gemeinsamen Daten der NAS gesichert? Vielleicht auf eine freie große Partition eines der angeschlossenen PC?

## 9.11 Deduplizierung

In jedem Backup gibt es große Mengen an ähnlichen Dateien, sowohl vom gleichen Tag als auch von verschiedenen Tagen.

1. Wenn Sie regelmäßig Vollsicherungen machen, haben Sie jede Menge identischer Dateien.
2. Wenn Sie beispielsweise eine E-Mail an mehrere Kollegen versenden, möglicherweise mit Anhang, gibt es identische Dateien in mehreren Briefkästen. Auch auf anderem Wege werden Dateien kopiert.
3. Viele Dokumente sind abschnittsweise identisch. Beispielsweise werden Briefe, Rechnungen und andere Dokumente oft aus Standardbausteinen zusammengesetzt oder ein früheres Dokument wird als Vorlage genommen und leicht verändert.
4. Wenn Sie regelmäßig an einer Datei arbeiten, werden Sie vermutlich nur Teile der Datei ändern, während weite Bereiche unverändert bleiben. Sicherungen unterschiedlicher Tage haben also gemeinsame Bestandteile.

Das amerikanische Unternehmen Data Domain hat das Verfahren der Deduplizierung entwickelt und patentiert. Die mehrfach enthaltenen Abschnitte werden ermittelt und nur einmal gespeichert, in alle anderen Dateien wird der betreffende Abschnitt durch einen Verweis auf diesen Dateibaustein ersetzt. Im Ergebnis schrumpft der Speicherbedarf der Backups auf ein Bruchteil. Es gibt das Online- und das Offline-Verfahren:[15]

- Online-Deduplizierung, „Inline“: Das Speichergerät sucht bereits während des Backups nach Dubletten. [16]
- Offline, „Post-processing“: Im Zeitraum zwischen den Sicherungen versucht die CPU des Backup-PCs ständig, weitere identische Bytefolgen zu ermitteln.

## 9.12 Vergleichende Betrachtung für Firmen

Firmen sichern ihre Daten in der Nacht. Deshalb kommen nur solche Lösungen in Frage, bei denen die komplette Sicherung auf ein Medium passt. Das Wechseln der Datenträger erfolgt am nächsten Tag. Das muss mit möglichst wenig Zeitaufwand erfolgen und ohne Fachwissen möglich sein, beispielsweise durch den Pförtner auf dem nächtlichen Rundgang oder morgens durch die Reinigungskraft.

Bandgeräte, sogenannte „Streamer“, sind immer noch weit verbreitet. Die Bandgeräte sind zwar teuer, aber die Bänder sind billig. Bänder sind unempfindlich, problemlos zu wechseln und zu transportieren.

Ersetzt man die zwanzig Bänder, die für eine Drei-Generationen-Sicherung nötig sind, durch zwanzig externe Festplatten, erreicht man das gleiche Maß an Sicherheit. Um die Festplatte vor dem Auswechseln vom System abmelden zu können, muss man als Administrator angemeldet sein - ein ernstes Sicherheitsrisiko. Zudem sind 20 Festplatten im Wechselrahmen vermutlich teurer als der Gesamtpreis von Bandgerät plus 20 Bändern. Trotzdem sind die festplattenbasierten Lösungen im Vormarsch.

15 Deduplizierung `http://www.searchstorage.de/index.cfm?pid=4963&pk=170116`
16 w:Deduplizierung ^{`http://de.wikipedia.org/wiki/Deduplizierung`}

- Die Sicherung wird wesentlich schneller abgeschlossen.
- Im Katastrophenfall braucht man kein Bandgerät heranschaffen und auf dem Ersatzserver installieren, denn die externe Festplatte mit dem Backup kann problemlos an jeden PC angeschlossen werden.
- Die Rücksicherung von Festplatte ist einige Stunden früher als von Band beendet, so dass die Firma früher arbeitsfähig wird.
- Die Datenmengen auf Firmenservern wachsen von Jahr zu Jahr in einem so schnellen Tempo, dass die Entwicklung größerer, schnellerer Bandgeräte nicht mitkommt.

Die Bedeutung der Festplatten-„Appliances“ nimmt zu. Eine ausgereifte Software macht das Wechseln von Datenträgern unnötig. Das spart Arbeitszeit, und der Serverraum kann verschlossen bleiben, denn niemand braucht mehr zum Bandwechsel hinein.

# 10 Vollsicherung

Mit den Begriffen „Vollsicherung“ und „Teilsicherung“ ist nicht gemeint, die gesamte Festplatte zu sichern. Gemeint ist, dass von einem ausgewählten Teil der Festplatte (Partition oder Verzeichnis mit Unterverzeichnissen) alle Dateien kopiert werden, ohne in ältere und neue Dateien zu unterscheiden.

Bei einer Vollsicherung werden alle vorhandenen Daten kopiert: Neue und uralte Dateien, früher bereits gesicherte Dateien und neue, noch nie gesicherte Dateien, ohne irgendwelche Ausnahmen.

Vorteil bei der Sicherung: Es wird keine Datei vergessen.

Vorteil bei der Wiederherstellung: Alle Dateien liegen komplett vor und können leicht gefunden werden. Es ist die schnellste der Methoden.

Nachteil bei der Sicherung: Der Bedarf an Sicherungsmedien und der Zeitaufwand für die Sicherung sind am größten. Wer ausschließlich Vollsicherungen erstellt, wird gezwungen sein, seine Backups nur wenige Tage aufzubewahren oder seine Daten nur selten zu sichern. Beides ist schlecht.

# 11 Teilsicherung

Wenn die Daten nicht komplett auf ein einziges Medium passen, wird eine Vollsicherung derart aufwändig, dass sie viel zu selten durchgeführt wird. Eigentlich ist es ja Unsinn, Dateien erneut zu sichern, von denen es bereits eine Kopie gibt. Führt man die Datensicherung täglich durch, beträgt der Unterschied zweier aufeinander folgender Datensicherungen nur wenige Prozente. Liegt ein Abstand von 30 Tagen zwischen zwei Sicherungen, steigt der Unterschied keinesfalls auf das dreißigfache, weil viele Dateien täglich verändert werden.

Welche Möglichkeiten gibt es, die veränderten unter der Masse der unveränderten Dateien herauszusuchen? Wenn man nur wenige Dateien zu sichern hat, kann man mit ein paar Mausklicks auswählen, was gesichert werden soll. Unter zehntausenden Dateien die zu sichernden Dateien herausfinden ist allerdings viel zu aufwändig und fehlerträchtig. Das „Heraussuchen“ muss automatisierbar sein. Zum Glück haben die Programmierer rechtzeitig daran gedacht und das „**Archivbit**“ vorgesehen.

## 11.1 Das Archivbit

Jede Datei hat in zahlreiche Eigenschaften: Name, Typ, Länge, Datum und Uhrzeit. Zusätzlich verfügt jede Datei über einige Attribute, von denen das „Read Only“ („Nur Lesen“) das bekannteste ist. Ein weiteres Attribut ist das „Archivattribut“. Klicken Sie mit der rechten Maustaste auf eine beliebige Datei und dann mit der linken Maustaste auf „Einstellungen“. In der rechten unteren Ecke finden Sie das Dateiattribut „Archiv“. Normalerweise ist dort immer ein Haken zu sehen. Das Betriebssystem setzt den Haken jedesmal, wenn die Datei verändert, umbenannt oder in ein anderes Verzeichnis verschoben wird. Jede neu erstellte Datei erhält ebenfalls den Haken. Dieses Kennzeichen zeigt den Datensicherungsprogrammen, dass die Datei gesichert werden muss.

Jedes Datensicherungsprogramm kann dieses Bit auswerten. Je nach Voreinstellungen kann ein Backup-Programm das Bit zurücksetzen (den Haken entfernen) oder belassen.

Wie benutzen Datensicherungsprogramme dieses Attribut?

## 11.2 Inkrementelle Sicherung

Bei einer vorangehenden Vollsicherung werden alle kopierten Dateien als gesichert gekennzeichnet, indem das „Archiv“- Attribut zurückgesetzt (gelöscht) wird. Bei einer inkrementelle Sicherung werden nur diejenigen Dateien gesichert, die seit der letzten Vollsicherung oder einer vorhergehenden inkrementellen Sicherung erstellt oder geändert worden sind. Während der inkrementellen Sicherung wird das Attribut-Archiv deaktiviert (entfernt).

Wenn beispielsweise am Montag eine Vollsicherung erfolgte, werden am Dienstag die seit Montag geänderten Dateien gesichert. Am Mittwoch werden die seit Dienstag geänderten Dateien gesichert usw.

Vorteil: Zeit- und Platzbedarf für die Sicherung ist gering.

Nachteil: Hoher Wiederherstellungsaufwand, denn im Katastrophenfall müssen zuerst die letzte Vollsicherung und anschließend **alle nachfolgenden** inkrementellen Sicherungen zurückkopiert werden.

## 11.3 Differenzielle Sicherung

Bei einer vorangehenden Vollsicherung müssen alle kopierten Dateien als gesichert gekennzeichnet werden, indem das „Archiv"- Attribut zurückgesetzt (gelöscht) wird. Alle Dateien, die nach dem Zeitpunkt der letzten Vollsicherung erstellt bzw. geändert werden, bekommen vom Betriebssystem das Archiv-Attribut gesetzt. Die Anzahl der gekennzeichneten Dateien wächst von Tag zu Tag. Die differenzielle Sicherung erfasst alle Dateien mit Archivattribut, ändert aber das Archivbit nicht.

Wenn beispielsweise am Montag eine Vollsicherung erfolgte, werden am Dienstag die Veränderungen seit Montag gesichert, am Mittwoch die Änderungen von Montag bis Mittwoch usw.

Vorteil: Der Zeit- und Platzbedarf für die Sicherung ist anfangs gering. Für eine Wiederherstellung werden nur die letzte Vollsicherung und die letzte Differentialsicherung benötigt.

Nachteil: Der Zeit- und Platzbedarf für die Sicherung wächst jeden Tag mehr. Je nach Umfang der täglichen Änderungen wird immer wieder mal eine Vollsicherung notwendig.

## 11.4 Inkrementell oder differenziell - welche ist vorzuziehen?

Das ist ganz klar die differenzielle Sicherung.

- Bei einer Wiederherstellung nach einem Totalverlust ist der Aufwand an Zeit und Nerven geringer.
- Wenn man eine einzelne verlorene Datei sucht, muss man nur auf zwei Medien nachsehen.
- Wenn man mehrfach beschreibbare Medien verwendet, braucht man weniger davon. Zwei abwechselnd verwendete DVD-RW genügen. Wenn die Wiederherstellung älterer Revisionen von Dateien wichtig ist, nimmt man drei Bänder oder geht zur Drei-Generationen-Sicherung über (Erläuterung folgt).

Unter welchen Bedingungen ist ein Wechsel zur inkrementellen Sicherung sinnvoll?

- Wenn die Änderungen nicht mehr auf ein einzelnes Medium passen.
- Wenn der wachsende Zeitaufwand für die Sicherung unzumutbar wird.

Unter welchen Bedingungen ist die inkrementelle Sicherung von Anfang an besser?

- Man möchte viele Revisionen der Dateien gespeichert haben.

- Die verwendeten Medien sind teuer und nur einmal verwendbar, deshalb soll die zu sichernde Datenmenge klein sein.

## 11.5 Gemischte Verwendung

Falls Sie es schaffen, dabei die Übersicht zu behalten, ist folgendes Vorgehen sinnvoll:

- Beginn mit einer vollständigen Sicherung.
- Differenzielle Sicherungen durchführen, solange die Änderungen auf ein einzelnes Medium passen.
- Eine inkrementelle Sicherung einschieben. Sicherheitshalber sollten Sie diese Zwischenstand-Sicherung zweimal durchführen, um bei zufälligen Schäden am Datenträger nicht ohne Daten dazustehen.
- Ab dem Datum der inkrementellen Sicherung wird, ausgehend vom erreichten Stand, wieder differenziell gesichert.
- Von Zeit zu Zeit eine Vollsicherung, z. B. zum Jahresende.

### 11.5.1 Beispiel

Die Medien könnten folgendermaßen beschriftet sein:

| **Nr** | Typ | Beschriftung |
|---|---|---|
| 1 | Voll | Vollsicherung vom 1.1.2010 |
| 2 | Diff | Änderungen seit 1.1.2010 (bis tt.mm.jjjj) |
| 3 | Ink | Änderungen vom 1.1.2010 bis 1.4.2010 |
| 4 | Diff | Änderungen seit 1.4.2010 (bis tt.mm.jjjj) |
| 5 | Ink | Änderungen vom 1.4.2010 bis 1.7.2010 |
| 6 | Diff | Änderungen seit 1.7.2010 (bis tt.mm.jjjj) |
| 7 | Ink | Änderungen vom 1.7.2010 bis 1.10.2010 |
| 8 | Diff | Änderungen seit 1.10.2010 (bis tt.mm.jjjj) |
| 9 | Ink | Änderungen vom 1.10.2010 bis 1.1.2011 |
| 10 | Voll | Vollsicherung vom 1.1.2011 |
| 11 | Diff | Änderungen seit 1.1.2011 (bis tt.mm.jjjj) |

Die in den Schritten 1, 3, 5, 7 und 9 benutzten Medien müssen mindestens so lange aufbewahrt werden, bis wieder einmal eine Vollsicherung durchgeführt wird. Wenn auch nur eins dieser Medien fehlerhaft ist, lassen sich Ihre Daten nicht vollständig wiederherstellen. Deshalb sollten Sie jedes dieser Medien sicherheitshalber doppelt haben oder eine Kopie davon auf eine externe Festplatte schreiben.

Die in den Schritten 2, 4, 6, 8 und 11 verwendeten Medien werden vor jeder Benutzung gelöscht. Sie könnten mit einer einzigen DVD-RW auskommen, die Sie das ganze Jahr täglich benutzen. Besser und nicht viel teurer wäre es, 5 DVD-RW zu verwenden, die mit Mo, Di, Mi, Do, Fr beschriftet werden und am jeweiligen Wochentag zum Einsatz kommen.

Angenommen, am 3.10.2010 geht die Festplatte kaputt. Auf die neue Festplatte müssten Sie die Daten in folgender Reihenfolge aufspielen: 1, 3, 5, 7, 8.

Angenommen, am 3.1.2011 geht die Festplatte kaputt. Auf die neue Festplatte müssten Sie die Daten in folgender Reihenfolge aufspielen: 10, 11. Falls das Medium mit der Vollsicherung vom 1.1.2011 defekt ist, könnten Sie notfalls 1, 3, 5, 7, 9, 11 aufspielen. Das dauert zwar länger, doch das Resultat ist das gleiche.

### 11.5.2 Durchführung

Sie müssen die „Eingabeaufforderung“ starten und die Befehle eintippen.

Das Beispiel geht von folgenden Annahmen aus:

- Das zu sichende Verzeichnis oder Laufwerk wird mit QUELLE bezeichnet. Ersetzen Sie QUELLE beispielsweise durch "C:", "C:\USERS", "C:\Dokumente und Einstellungen" o. ä.
- Mit ZIEL wird der Datenträger bezeichnet, auf den die Sicherung erfolgt. Das kann ein Stick, eine externe Festplatte oder ein Laufwerk mit DVD-RAM sein. Ersetzen Sie ZIEL beispielsweise durch "R:", "R:\2010", "R:\2010-11" o. ä.

Erläuterungen zu den Befehlen:

- Für eine Vollsicherung müssen nacheinander zwei Befehle ausgeführt werden: Der Befehl ATTRIB setzt das Archivbit für alle Dateien, dadurch lässt der anschließende XCOPY-Befehl keine Datei aus.
- Die Parameter /S /C bewirken, dass Unterverzeichnisse kopiert werden und bei Fehlern der Kopiervorgang nicht abgebrochen wird.
- /M bedeutet: Alle Dateien mit gesetztem Archivbit kopieren, anschließend das Archivbit zurücksetzen.
- /A bedeutet: Alle Dateien mit gesetztem Archivbit kopieren, das Archivbit nicht verändern.
- Wenn ein Dateiname Leerzeichen enthält bzw. enthalten kann, muss er von Anführungszeichen eingeschlossen werden.

| **Variante mit XCOPY-Befehl** | |
|---|---|
| **Nr** | Befehl |
| 1,10 | `ATTRIB "QUELLE\*.*" +A`<br>`XCOPY "QUELLE*.*" ZIEL*.* /S /C /M` |
| 2,4,6,8,11 | `XCOPY "QUELLE*.*" ZIEL*.* /S /C /A` |
| 3,5,7,9 | `XCOPY "QUELLE*.*" ZIEL*.* /S /C /M` |

- /MIR bedeutet, dass alle Unterverzeichnisse im Ziel in exakte Übereinstimmung mit der Quelle gebracht werden.
- /R:1 /W:1 bedeutet, dass bei Fehlern nach einer **W**artezeit von 1 Sekunde ein Wiederholungsversuch (**R**etry) unternommen wird.

| **Variante mit ROBOCOPY-Befehl** | |
|---|---|
| **Nr** | Befehl |
| 1,10 | `ATTRIB "QUELLE\*.*" +A`<br>`ROBOCOPY "QUELLE*.*" ZIEL*.* /MIR /R:1 /W:1 /M` |
| 2,4,6,8,11 | `ROBOCOPY "QUELLE*.*" ZIEL*.* /MIR /R:1 /W:1 /A` |

| **Variante mit ROBOCOPY-Befehl** | |
|---|---|
| **Nr** | Befehl |
| 3,5,7,9 | `ROBOCOPY "QUELLE*.*" ZIEL*.* /MIR /R:1 /W:1 /M` |

## 11.6 Sicherung außer der Reihe

Wenn wegen einer bevorstehenden Installation sicherheitshalber eine außerplanmäßige (Voll-)Sicherung gemacht werden soll, kann man die Daten auf eine externe Festplatte kopieren. Das geht wesentlich schneller als eine Sicherung auf Magnetband oder gar auf DVD. Dabei darf aber das Archivbit nicht verändert werden, sonst gerät die reguläre Datensicherung durcheinander.

## 11.7 Allgemeine Empfehlungen

- Notieren Sie, welche Sicherungen welcher Art wann auf welchen Datenträger gespeichert worden sind. Am besten auf Papier. Wenn Sie das in eine Datei schreiben, sollten Sie dafür sorgen, dass diese Datei auf keiner Sicherheitskopie fehlt.
- Kontrollieren Sie von Zeit zu Zeit, ob immer noch alle wichtigen Daten gesichert werden. Passen Sie Ihre Datensicherung an neue Programme und andere Veränderungen an.
- Testen Sie zumindest auszugsweise, ob die Daten auf dem Sicherungsmedium tatsächlich fehlerfrei lesbar sind.
- Vertrauen Sie Ihrer Datensicherung nie zu 100%. Bänder oder DVDs können sich als nicht lesbar herausstellen.

Es gibt keine allgemeingültigen Empfehlungen, wie häufig und wie umfangreich eine Datensicherung sein sollte. Es ist wie bei der Kasko-Versicherung vom Auto: Möglicherweise zahlen Sie viele Jahre ein, ohne etwas herauszubekommen. Vielleicht kommt aber morgen ein Hagelschlag ...

Letztlich kann man eine Datensicherung wie eine Versicherung betrachten: Sie investieren jahrelang Zeit und Geld in der Hoffnung, dass der Schaden nie eintritt. Bisher hatten Sie Glück, vielleicht bleibt es eine lange Zeit so, aber gewiss nicht für immer. Vergleichen Sie den Aufwand zwischen den Kosten (materiellen und ideellen) des seltenen Ereignisses „Datenverlust“ und dem regelmäßigen vorbeugenden Aufwand und entscheiden Sie dann über Umfang und Häufigkeit.

```
<!-- Das Archivbit -->
```

## 11.8 Eine Festplatte statt vieler Bänder

Auf dieser Seite geht es um die Möglichkeit, ein Bandgerät und viele Bänder durch eine einzige Festplatte zu ersetzen und trotzdem auf frühere Versionen einer Datei zurückgreifen zu können.

Ein großes Plus der Drei-Generationen-Sicherung ist die Möglichkeit, auf tage-, wochen- und monatealte Versionen einer Datei zurückgreifen zu können. Wenn Sie eine externe Festplatte verwenden, ist vermutlich Platz für viele Sicherungen. Wenn Sie Ihre Dateien jeden Tag in ein anderes, neu angelegtes Verzeichnis sichern, können Sie bald auf viele frühere Dateiversionen zurückgreifen.

Allerdings müssen Sie

- jeden Tag ein neues Zielverzeichnis anlegen
- jeden Tag den Namen des neuen Zielverzeichnisses in den Befehl eintragen, mit dem die Datensicherung erfolgt.

Diese tägliche Änderung manuell durchzuführen ist natürlich völlig unakzeptabel. Wie könnte man das automatisieren?

## 11.9 In den Beispielen verwendete Bezeichnungen und Annahmen

| | |
|---|---|
| C: | Das Laufwerk mit dem Betriebssystem |
| Q: | Das **Quellen**-Laufwerk mit den zu sichernden Daten |
| Z: | Das **Ziel**-Laufwerk, wohin die Daten gesichert werden |
| DVD: | Der Laufwerksbuchstabe Ihres Brenners |

Für diesen Zweck ist eine der Windows-Variablen gut geeignet. Windows stellt die Variable **%DATE%** zur Verfügung, die während der Ausführung durch das aktuelle Datum in der Form `tt.mm.jjjj` ersetzt wird. Mit einem einfachen DOS-Befehl

```
md  \%DATE%
```

kann man jeden Tag ein neues Verzeichnis erstellen. Probieren Sie es einfach mal aus: Öffnen Sie ein DOS-Fenster (Start-Ausführen-cmd-OK), tippen Sie den Befehl ein und überzeugen Sie sich, dass im aktuellen Laufwerk ein neues Verzeichnis entstanden ist! Wenn Sie anschließend den Befehl

```
xcopy  Q:\*.doc  \%DATE%\*.doc /s
```

eintippen und Enter drücken, werden alle Ihre Word-Dokumente in ein Datumsverzeichnis kopiert.

Nachteil dieses Verfahrens: Pro Jahr würden 365 Kopien entstehen, die wohl kaum auf die Festplatte passen würden. Eine Möglichkeit wäre es, länger zurückliegende Sicherungen zu löschen. Das müsste aber automatisch geschehen, sonst taugt das ganze Konzept nichts.

Eine sinnvolle Möglichkeit wäre es, nur ein Teil des Datums zu verwenden. Wenn man vom Datum nur die beiden Ziffern des Tages verwendet, erhält man jeden Tag ein neues Verzeichnis, insgesamt 31 Verzeichnisse pro Monat. Am entsprechenden Tag des nächsten Monats würden die im Vormonat kopierten Daten überschrieben werden. Dadurch bliebe einerseits der Platzbedarf in Grenzen, andererseits kann man bis zu 31 Tage rückwärts jeden Tag rekonstruieren. Das sollte wohl für alle praktisch relevanten Fälle ausreichen.

Für die meisten Anwender würde es genügen, den Datenstand der letzten zehn Tage rekonstruieren zu können. Auch das ist problemlos möglich. Dafür braucht man die Einer-Ziffer des Tages. Die Variable %DATE:~1,1% liefert diese eine Ziffer. Mit den folgenden Befehlen

```
md  \%DATE:~1,1%

xcopy  Q:\*.doc  z:\%DATE:~1,1%\*.doc  /s
```

erfolgt die Sicherung am 1., 11., 21. und 31. Tag des Monats in das Verzeichnis mit dem Namen "1". Am 2., 12. und 22. Tag des Monats erfolgt die Sicherung in das Verzeichnis mit dem Namen "2" usw.

Weil Verzeichnisnamen, deren Namen nur aus einer Ziffer besteht, verwirrend wären, ändern wir das Programm etwas ab:

```
md  \Tag_x%DATE:~1,1%

xcopy  Q:\*.doc  z:\Tag_x%DATE:~1,1%\*.doc  /s
```

erfolgt die Sicherung am 1., 11., 21. und 31. Tag des Monats in das Verzeichnis mit dem Namen "Tag_x1". Am 2., 12. und 22. Tag des Monats erfolgt die Sicherung in das Verzeichnis mit dem Namen "Tag_x2" usw.

# 12 Image

## 12.1 Ein Speicherabbild - Was ist das?

Ein Speicherabbild (engl. Image) ist eine 1:1 Kopie einer oder mehrerer Partitionen der Festplatte. Betriebssystem, Programme und Daten werden einschließlich ihrer Position auf der Festplatte gespeichert. Kopiert man das Image auf eine Festplatte zurück, entsteht ein exaktes Abbild, Bit für Bit identisch mit dem Original.

Nach einem Datenverlust oder wenn man seine alte Festplatte gegen eine größere wechseln möchte ist es sehr praktisch, ein Image zu haben. Das Image wird mit einem geeigneten Programm auf die neue Festplatte kopiert, und das Betriebssystem ist ohne jede Anpassung sofort einsatzfähig. Das Rückkopieren dauert je nach Datenmenge typischerweise 15 bis 30 Minuten.

Das ist ein gewaltiger Zeitvorteil. Bei einer „normalen“, dateiweisen Datensicherung muss zuerst das Betriebssystem samt Treibern installiert werden, anschließend die Anwendungen und viele Sicherheitsupdates. Das dauert mehrere Stunden, oft mehr als einen Tag. Erst wenn das Datensicherungsprogramm installiert worden ist, kann begonnen werden, die Daten zurückzusichern.

Bei der klassischen Datensicherung wird Datei für Datei gesichert. Wenn die Festplatte 10.000 Dateien enthält, so hat auch die Kopie 10.000 Dateien. Einer der Vorteile dieser klassischen Datensicherung ist, dass man eine verlorene Datei ganz leicht wiederfinden kann. Das Verfahren hat aber auch Nachteile:

- Das Betriebssystem kann auf diese Weise weder gesichert noch wiederhergestellt werden. Das hat zwei Ursachen:
  - Einige Dateien des Betriebssystems sind ständig in Benutzung, wie z. B. die Dateien der Registry. In Benutzung befindliche Dateien lassen sich nicht kopieren, außer mit teuren Spezialprogrammen.
  - Einige Dateien müssen sich an einer genau definierten Stelle der Festplatte befinden, wie z. B. einige Startdateien und die Auslagerungsdatei. Mit einem Kopierbefehl ist es aber nicht möglich, eine Datei an eine bestimmte Position der Festplatte zu kopieren.
- Nach dem Kopieren jeder einzelnen Datei müssen die Verwaltungstabellen (Inhaltsverzeichnis und Belegungstabellen) auf dem Ziellaufwerk geändert werden. Wenn viele kleine Dateien zu sichern sind, werden diese Tabellen sehr umfangreich. Wenn die Verwaltungstabellen nicht mehr in den Arbeitsspeicher passen, werden sie immer wieder auf Festplatte ausgelagert und wieder eingelesen. Der Zeitbedarf für das Kopieren geht drastisch in die Höhe, auf das Zehnfache oder mehr. Eventuell steht so viel Zeit nicht zur Verfügung.

Diese Probleme lassen sich mit der Technologie eines **Speicherabbildes** (engl.: **Image**) lösen. Bei einem Image wird neben den Dateien deren Struktur und Anordnung mitkopiert.

In der Regel erfolgt das Kopieren Sektor für Sektor, unabhängig von der Verzeichnisstruktur der Partition.

Wie wird das Problem der ständig in Benutzung befindlichen Dateien gelöst? Es gibt zwei Möglichkeiten:

1. Windows wird heruntergefahren, dann wird das Image-Programm direkt von CD oder Stick gestartet. Das Image-Programm braucht also nicht installiert werden. Dadurch ist eine Sicherung selbst dann noch möglich, wenn das Betriebssystem defekt ist und nicht mehr hochfährt.
2. In manchen Fällen kann oder soll der PC nicht heruntergefahren werden. Ein Image bei laufendem Betrieb beherrschen nur wenige Programme. Es wird ein Verfahren „Schattenkopie“[1] genutzt, mit dem sich auf Windows-Servern die Registry und andere ständig benutzte Dateien sichern lassen. Mit Datenbanken anderer Hersteller funktioniert das mitunter nicht ohne Zukauf von Spezialmodulen. Bei der Entscheidung für ein Programm sollte man den Leistungsumfang sehr genau prüfen.

Für den Privatanwender kommt üblicherweise nur das erste Verfahren in Frage. Soll ein Image automatisch in regelmäßigen Abständen erstellt werden, bleibt nur das zweite Verfahren.

Zum Kopieren werden schnelle Hardwarefunktionen verwendet, dadurch geht das Erstellen (und auch das Rücksichern) meist viel schneller als das dateiweise Kopieren. Der größte Vorteil aber ist die Möglichkeit, ein funktionsfähiges Betriebssystem zu sichern, welches nach einer Rücksicherung sofort startbereit ist. Einige weitere Vorteile eines Images sind:

- Die Daten können in Portionen gewünschter Größe aufgeteilt werden, beispielsweise in Portionen von 4,7 GB. Bei Bedarf können sie leicht auf DVD archiviert werden.
- Die Daten werden standardmäßig komprimiert, jedoch kann die Komprimierung abgeschaltet werden.
- Das Archiv kann mit einem Password geschützt werden.
- Nicht benutzte Sektoren werden in der Standardeinstellung nicht gesichert, aber in Spezialfällen (z. B. vor einem Datenrettungsversuch oder zu Beweiszwecken) ist es möglich.

## 12.2 Für welche Sicherungen ist ein Image geeignet?

Bei der Sicherung kompletter Festplatten sind Geschwindigkeit, Komprimierung, Verschlüsselung und Unabhängigkeit vom Zustand des Betriebssystems die großen Vorteile eines Imageprogramms. Ihre größte Stärke spielten Imageprogramme bei der Sicherung des Betriebssystems aus.

Je nach Ihrer Arbeitsweise kann ein monatliches Image des Betriebssystems sinnvoll sein, oder einmal pro Quartal. Wenn Sie größere Änderungen am Betriebssystem planen, ist davor und eventuell zusätzlich danach der günstigste Zeitpunkt. Ein Image bringt Ihnen Vorteile:

- Wenn die anschließende Installation fehlschlägt, können Sie einfach zu einem unbeschädigten Windows zurückkehren.

1 `http://de.wikipedia.org/wiki/Volume%20Shadow%20Copy%20Service`

- Wenn Ihr System durch Schadsoftware oder eine Fehlbedienung beschädigt ist, kann es leicht auf eine lauffähige Version zurückgesetzt werden.
- Sie haben eine Sicherung derjenigen Dateien, die von anderen Sicherungen möglicherweise nicht erfasst werden.

Allerdings sollte ein Image niemals Ihre einzige Datensicherung sein. Ein einziges defektes Bit kann das gesamte Archiv unbrauchbar machen. Auch wenn das Archiv auf einer eigentlich zuverlässigen Festplatte abgelegt ist, passiert es mitunter, dass sich eine Archivdatei nicht öffnen lässt. Das Internet ist voll von solchen Leidensberichten[2], selbst bei Testsieger-Programmen. Geradezu verheerend riskant ist es, ein Archiv auf mehrere DVDs zu verteilen. Wenn nur eine der DVDs einen Lesefehler hat, sind auch die restlichen DVDs wertlos. Wenn man die Festplatte auf klassische Weise Datei für Datei kopiert, verliert man bei einem zufälligen Fehler nur eine Datei, die man möglicherweise in einer älteren Sicherung finden kann.

Für eine sichere Archivierung Ihrer Daten ist ein Image aus einem weiteren Grund denkbar ungeeignet. Die Sicherung erfolgt in einem proprietären (herstellereigenem) Dateiformat. Wer weiß, ob Ihr Image-Programm unter Windows 8 und 9 noch lauffähig ist.

## 12.3 Teilsicherungen

Ein Imageprogramm kann statt einer kompletten Partition auch nur ausgewählte Verzeichnisse kopieren. Viel interessanter ist die Möglichkeit, aus einem vollständigen Image einzelne Dateien oder Verzeichnisse zurückzuholen. Sie können wählen, ob Sie an den ursprünglichen Speicherort zurückkopieren wollen oder Sie können ein anderes Zielverzeichnis wählen. Kopieren Sie keinesfalls in das ursprüngliche Verzeichnis zurück, denn wenn dabei etwas schief geht, wissen Sie nicht nur, dass Ihr Backup nichts getaugt hat, sondern Sie sind vermutlich auch die noch intakten Daten los.

## 12.4 Forensisches Backup

Beim Löschen einer Datei wird nur der Dateiname gelöscht und der von der Datei belegte Speicherplatz wird als „frei“ markiert. Die eigentlichen Daten sind nicht gelöscht, sie sind lediglich nicht mehr ohne weiteres auffindbar. Diese als frei markierten Bereiche werden vom Imageprogramm in der Standardeinstellung nicht gesichert. In der Regel gibt es eine Betriebsart „Forensik“ o.ä., bei der auch die als unbenutzt deklarierten Bereiche gesichert werden. Ein solches Backup ist nützlich, wenn man nach einem Zwischenfall die Schuldfrage klären will.

2 Image lässt sich nicht zurücksichern `http://www.computerbild.de/download/review/Acronis-True-Image-Home-2011-2511794.html`

## 12.5 Welche Image-Programme gibt es?

„Drive Image“ von der Firma PowerQuest war das erste Programm dieser Art. Nachdem die Firma Powerquest von Symantec aufgekauft wurde, heißt das Programm jetzt „Symantec ImageCenter“. Weitere bekannte Programme sind Norton Ghost und Acronis True Image. Mitunter gibt es zeitlich begrenzte Versionen im Internet und in Fachzeitschriften. „Active System Recovery“ von Symantec beherrscht die Sicherung bei laufendem Betrieb.

## 12.6 Zurücksichern

Das **Sichern** von Daten ist ungefährlich, selbst wenn Sie Fehler machen. Schlimmstenfalls sichern Sie die falschen Daten oder zu wenig Daten. Beim **Rücksichern** können Sie allerdings Schaden anrichten.

1. Das Image-Programm ordnet den Partitionen mitunter andere Laufwerksbuchstaben zu als das Betriebssystem. Das kann dazu führen, dass Sie beim Rücksichern irrtümlich die falsche Partition überschreiben. Geben Sie deshalb den Partitionen im Vorfeld sinnvolle Namen. Verschaffen Sie sich vor dem Start des Image-Programms einen Überblick über Größe und Namen aller Partitionen.
2. Haben Sie **alle** Dateien gesichert, die seit dem Erstellen des Images geändert worden sind? Beim Rücksichern werden alle neueren Daten zuverlässig und endgültig mit den alten Daten überschrieben. Wenn Sie diesbezüglich nicht sicher sind, erstellen Sie ein Image der kaputten Partition. Darin können Sie nötigenfalls alle Dateien finden, die Sie vielleicht noch brauchen.

**Achtung!**
Sichern Sie die auf Laufwerk C: verstreuten Daten, bevor Sie die Partition auf einen früheren Zustand zurücksetzen!

# 13 Daten sinnvoll ordnen

## 13.1 Programme und Daten trennen

Festplatten sind Datenspeicher mit einem gewaltigen Fassungsvermögen. Heutige Festplatten fassen einige hundert DVDs. Um derartige Datenmengen besser ordnen zu können, kann die Festplatte in Bereiche, sogenannte Partitionen unterteilt werden. Bei den meisten PCs wird diese Möglichkeit allerdings nicht genutzt.

Wenn man die Festplatte in mindestens zwei Partitionen teilt – die erste Partition für das Betriebssystem, der Rest für die Daten –, und die Daten auf die zweite Partition verlagert, kann man Übersichtlichkeit, Geschwindigkeit und Sicherheit gewinnen. Außerdem wird die Datensicherung erleichtert. Betrachten wir, wieso.

### 13.1.1 Mehr Übersicht

Zu diesem Thema gibt es nicht viel zu sagen. Kaum jemand steckt Schriftstücke (= Dokumente) zwischen die Bücher (= Programme). Normalerweise ist es sinnvoll, Bücher und Dokumente getrennt aufzubewahren.

### 13.1.2 Mehr Geschwindigkeit

Wieso gewinnt man Geschwindigkeit durch Partitionierung der Festplatte?

Windows protokolliert ständig viele Vorgänge und Veränderungen (Logbücher, Registry, Wiederherstellungspunkte u. a.). Mehr als 90 Prozent aller Festplattenzugriffe betreffen das Schreiben von Protokolldateien sowie das Lesen von Dateien des Betriebssystems und der installierten Programme, weniger als 10% entfallen auf Lesen und Schreiben von Daten. Ein Beispiel dazu: Wenn Sie eine Word-Datei anklicken, braucht der PC einige Sekunden, bis Word geöffnet ist. Maximal 100 ms davon hat der PC für das Lesen der Word-Datei gebraucht, die vielen anderen Zugriffe dienen zum Lesen der benötigten Programmdateien.

Wenn Windows freien Platz für irgendeine Datei benötigt, wird die Festplatte, am Anfang beginnend, nach der ersten freien Lücke durchsucht. Dorthin wird die Datei gespeichert. Wird durch das Löschen einer Datei Platz frei, kommt die nächste Datei dort hin. Im Laufe der Zeit werden Programme und Daten vermischt und weiträumig über den gesamten belegten Bereich verteilt.

Wenn man nun beispielsweise von einer 400 GB Festplatte die ersten 20 GB für die Systempartition mit Windows und anderer Software reserviert und den großen Rest von 380 GB für Daten verwendet, entfallen 90% der Zugriffe auf einen kompakten Bereich von 5% der Festplattenfläche. Nun muss man wissen, dass die Magnetköpfe für kurze Bewegungen nur 2

bis 3 Millisekunden benötigen, ein Spurwechsel von ganz außen (wo die Programme sind) bis zu den mittleren Spuren dauert 15 – 20 ms, bis nach ganz innen 20 – 25 ms - die zehnfache Zeit wie im Nahbereich!

Durch die Partitionierung der Festplatte können also 90% der Festplattenzugriffe in weniger als 3 ms erfolgen. Dabei gilt: Je voller die Festplatte wird, desto größer ist der Geschwindigkeitsvorteil. Zugegeben, es gibt nur einen geringen Vorteil, solange die Festplatte fast leer ist, aber sie wird ja nicht immer leer bleiben. Bei einer halb vollen, partitionierten Festplatte wird die Festplatte im statistischen Mittel um 20% bis 30% schneller.

Werden durch eine Unterteilung möglicherweise Daten langsamer gelesen? Nein. Selbst wenn es so wäre: Sogar der langsamste Computer kann die Daten um Größenordnungen schneller liefern, als Sie diese anhören oder betrachten können. Wartezeiten entstehen nur dadurch, dass Windows die zum Betrachten der Daten benötigten Programme laden und konfigurieren muss. Genau das wird durch eine sinnvolle Partitionierung beschleunigt.

### 13.1.3 Mehr Sicherheit

Der Schreibvorgang einer Datei besteht aus mindestens vier Etappen: Die Belegungstabelle durchsucht, um freiem Speicherplatz für die Datei zu finden. Die Datei wird dorthin geschrieben, das Inhaltsverzeichnis wird aktualisiert und die Belegungstabelle der Festplatte wird ergänzt. Wenn der PC wegen einer Störung den Vorgang nicht abschließen kann, ist mindestens eine Datei oder ein Verzeichnis beschädigt. Beim nächsten Start des PCs sehen Sie die Meldung

```
Eine Datenträgerüberprüfung ist geplant

Festplatten müssen überprüft werden
```

Zu diesen Abstürzen kommt es durch Inkompatibilitäten, Programmfehler, Updates und Bedienungsfehler. Windows versucht eine automatische Reparatur. Manchmal gelingt die Reparatur nicht oder nur teilweise. Eventuell entstehen Dateitrümmer, die in Verzeichnissen mit den Namen „C:\File0001“, „C:\File0002“ usw. abgelegt werden. Schäden an den Verwaltungstabellen des Dateisystems treten glücklicherweise nur selten auf. Im schlimmsten Fall ist die Partition kaputt und alle darauf befindlichen Daten sind verloren.

Wenn die Platte jedoch in Betriebssystem- und Datenpartition unterteilt war, geht fast immer nur die Partition mit dem Betriebssystem kaputt, während die Daten auf den restlichen Partitionen erhalten bleiben. Schlimmstenfalls muss man „nur“ Windows neu installieren.

Die Partitionierung hat einen weiteren Vorteil: Veränderungen am Betriebssystem werden weniger riskant. Die Installation eines Treibers oder eines Programms kann Windows beschädigen. Kleine Verbesserungen, Reparaturen oder die Beseitigung von Schadsoftware können zu Problemen führen. Das Betriebssystem legt zwar von Zeit zu Zeit Wiederherstellungspunkte an, um nach einem Fehler zu einem früheren, fehlerfreien Zustand zurückkehren zu können, aber die Rückkehr klappt nicht immer. Deshalb ist es vor Installationen und nichttrivialen Reparaturen ratsam, vorher eine Kopie (ein Image) des Betriebssystems anzufertigen. Wenn die Festplatte unterteilt ist, braucht nur die kleine Betriebssystem-Partition gesichert werden. Ein bis zwei DVD reichen dafür aus. Noch bequemer und sehr viel schneller (nur

etwa 10 Minuten) geht es, wenn man das Image der Systempartition auf der Datenpartition ablegen kann.

Wenn die Festplatte nicht unterteilt ist, sind die Dateien des Betriebssystems mit den Daten vermischt. Es bleibt kein anderer Weg, als den gesamten Inhalt der Festplatte zu sichern. Wie viel wäre das bei Ihnen? Auf DVD sichern ist unsinnig, denn mit weniger als einem halben Dutzend DVD kommen Sie nicht aus. Sie brauchen also eine externe Festplatte und eine Stunde Zeit, denn so lange könnte es dauern. Das Zurückkopieren (wenn der erste Reparaturversuch fehlschlägt) dauert genau so lange.

**Zusammenfassung:** Wie kommt also der Gewinn an Sicherheit zustande?

- Wenn Schäden an einer Partition auftreten, betrifft das fast immer die Systempartition. Die Datenpartition(en) bleiben intakt.
- Der anfälligste Teil der Festplatte - das Betriebssystem - lässt sich mit geringem Aufwand sichern, denn es passt meist auf ein bis zwei DVDs. Noch bequemer ist es, wenn Sie das Image auf die Datenpartition der Festplatte oder auf eine externe Festplatte schreiben können. Es wird Ihnen leicht fallen, die Systempartition öfter zu sichern.

### 13.1.4 Datensicherung mit weniger Aufwand

Bei den meisten PCs belegt das Betriebssystem weniger als 15 GByte, dann reichen zwei DVD für ein Image aus. Andererseits schafft es kaum ein Privatanwender, mit seiner Hände Arbeit mehr Dateien zu erstellen, als auf eine einzige DVD passen. Nehmen wir mal an, Ihr Betriebssystem passt auf zwei DVD und alle wichtigen Daten auf eine DVD.

Wenn die Festplatte nicht unterteilt ist, hat ein Normalanwender zwei Möglichkeiten, seine Daten zu sichern:

1. Er sucht die auf der Festplatte verteilten Verzeichnisse zeitaufwändig zusammen und brennt sie auf eine DVD.
2. Er sichert die gesamte Festplatte. Dafür werden mehrere DVD benötigt, es dauert entsprechend lange.

Wenn jedoch die Daten auf die Datenpartition verlagert sind, sollten auf C: keine Daten mehr sein.

1. Folglich ist es nicht zwingend nötig, die Betriebssystempartition zu sichern. Wenn die Festplatte versagt, baut man eine neue ein und installiert das Betriebssystem und die Anwendungen neu.
2. Für die Datensicherung wird nur eine DVD benötigt. Das Brennen geht schnell.

Man kann sich und andere relativ leicht zu einer Datensicherung überreden, wenn es nur einen Rohling und zwei Minuten Zeit kostet. Ein paar Klicks und eine Kaffee- o.a. Pause, und man ist fertig. Wenn mehrere DVD zu brennen sind, steigt nicht nur der Materialaufwand, sondern vor allem der Zeitbedarf. Jede Viertelstunde die DVD wechseln und den PC eine Stunde lang nicht sinnvoll nutzen zu können, ist lästig.

```
<!-- Programme und Daten trennen -->
```

### 13.1.5 Die Einteilung der Festplatte ändern

Möglicherweise haben Sie nun beschlossen, Ihre Festplatte zu partitionieren. Wie macht man das?

„Partition Magic“ von der Firma Powerquest war das erste Programm, mit dem Partitionen ohne Datenverlust verändert werden konnten. Präziser formuliert: Wenn alles optimal klappt, gehen die Daten dabei nicht verloren. Inzwischen gibt es weitere Programme, zum Beispiel

- MS-Diskmanager (erst ab Vista)
- Acronis Disk Director Suite
- Paragon Partition Manager
- Partition Commander
- Ranish Partition Manager
- Smart FDISK
- GDisk

Diese Programme kosten meist weniger als 50 Euro, teilweise gibt es die Programme als funktionsfähige Demo im Internet oder als Beilage von Fachzeitschriften. Einige dieser Partitionierprogramme können keine Festplatten bearbeiten, auf denen ein (Windows-) Serverbetriebssystem installiert ist. Für die Umgestaltung von Server-Festplatten gibt es spezielle Serverversionen mit Preisen im hohen dreistelligen Bereich.

Alle Programme sind angeblich „ganz leicht“ zu bedienen. Sie sollten sich von so einer Behauptung nicht beruhigen lassen, sondern – im Gegenteil – warnen lassen. Haben Sie jemals in der Computerbranche eine Werbung gesehen, in der ein Produkt als „schwierig zu bedienen“ und „gefährlich“ angepriesen worden wäre?

Da das Partitionieren nur selten durchgeführt wird, ist es schwer, darin Routine zu bekommen.

Es sollte Ihnen zu denken geben, dass Sie in jeder Anleitung aufgefordert werden, vor der Partitionierung unbedingt Ihre Daten zu sichern. Dadurch trifft den Hersteller keine juristische Verantwortung, wenn beim Partitionieren etwas schief geht. Nehmen Sie die Datensicherung ernst. Erschreckend viele Leute, die sich auszukennen glaubten, haben bei den ersten Versuchen mit einer Partitionierungssoftware ihre Daten verloren.

**Achtung!**

Bearbeiten Sie nie eine Partition mit wichtigen Daten ohne vorherige Datensicherung!
Selbst bei fehlerfreier Verwendung eines Partitionsmanagers kann es leicht zum Totalschaden kommen.
Bei einem Stromausfall oder einer anderen Störung sind die Daten hoffnungslos verloren!

Wie man es die Partitionierung ändert, können Sie im Abschnitt **Werkzeuge** lesen:

- Partitionieren mit PQMAGIC[1]
- Partitionen mit MS Disk Manager einrichten[2]

Es gibt zahlreiche weitere Programme zum Partitionieren der Festplatte, darunter auch kostenlose.

```
<!-- Wie ändert man Einteilung HDD? -->
```

## 13.2 Die Datenpartition noch weiter unterteilen

Sie haben gelesen, dass die Zweiteilung der Festplatte in System- und Datenpartition mehr Sicherheit, Übersichtlichkeit und Geschwindigkeit bringt. Außerdem werden Reparaturen am Betriebssystem erleichtert, und die Datensicherung wird erleichtert.

Aus dem Blickwinkel der Datensicherung ist jedoch eine weitere Unterteilung der Daten sinnvoll. Der Grund dafür ist, dass es unterschiedliche Datentypen gibt und für jeden Typ eine andere Sicherungsstrategie optimal ist. Manche Daten sollten häufig gesichert werden, bei anderen darf es seltener sein. Betrachten wir die Unterschiede:

- Die größte Sicherungshäufigkeit sollte auf Textdateien und andere **selbst erstellte, oft veränderte**, besonders wichtige Daten entfallen. Sinnvoll ist sowohl eine tägliche Sicherung als auch die Möglichkeit, auf Sicherungen von Vortagen zurückgreifen zu können.
- Sammlungen nicht-selbsterstellter Daten, die wiederbeschaffbar sind oder auf die man notfalls verzichten kann, z. B. MP3. Deren Sicherung ist solange kein Problem, wie die Datenmenge auf eine DVD passt. Wenn der Umfang größer wird, gibt es mehrere Möglichkeiten:
  - Die Sicherung nur selten vornehmen und akzeptieren, dass Sie im Schadensfall einen möglicherweise großen Teil der Daten verlieren
  - Das Archivbit ausnutzen, um nach einer Vollsicherung zukünftig inkrementelle Sicherungen vorzunehmen
  - Dateien trennen nach schwer und leicht wiederbeschaffbaren Dateien und zukünftig nur die schwer beschaffbaren Dateien sichern.
  - Nur noch die kleinen Dateien sichern, die großen weglassen. Im Verlustfall ist es weniger aufwändig, eine große statt zehn kleine Dateien wiederfinden zu müssen.
- Kauf-DVD und -CD, die aus Komfortgründen auf die Festplatte kopiert worden sind. Man sichert nicht deren Kopie als Teil der gesamten Festplatte, sondern macht eine 1:1 Kopie vom Original.
- Fotos und andere selbst erstellte nicht-kleine Daten. Wenn Sie die Fotos nicht bearbeiten, brauchen Sie frühere Versionen nicht sichern, denn es gibt sie nicht. Eine Sicherung ist besonders nach wichtigen Ereignissen (Urlaub) sinnvoll. Wenn die Datenmenge nicht mehr auf eine DVD passt, kann man einen Teil archivieren oder man sichert zukünftig nur die Veränderungen. Fotos lassen sich chronologisch sinnvoll ordnen. Wenn man den PC privat

1 http://de.wikibooks.org/wiki/Datensicherung%2F%20Werkzeuge%2F%20PQMAGIC
2 http://de.wikibooks.org/wiki/Datensicherung%2F%20Werkzeuge%2F%20MS%20Disk%20Manager

und geschäftlich nutzt, kann man getrennte Bereiche für Privates und Geschäftliches vorsehen.

Um die Datenarten zu trennen, gibt es zwei Möglichkeiten:

- getrennte Partitionen
- Unterverzeichnisse

Möglicherweise ist es am Besten, eine Grobeinteilung in Partitionen vorzunehmen und eine vielleicht später notwendige feinere Unterteilung mit Unterverzeichnissen vorzunehmen.

Ganz bestimmt ist es sinnvoll, MP3-Dateien, Filme und andere sehr große Dateien in einer Archiv-Partition oder in speziellen Partitionen zu sammeln. Außerdem kommt auch alles andere ins Archiv, was man notfalls wiederbeschaffen oder erneut aus dem Internet herunterladen kann. Dadurch wird die Datenpartition relativ klein und man kann sie mit nur geringem Zeitaufwand regelmäßig auf CD oder DVD brennen. Die Archivpartition wird nur selten gesichert, wenn überhaupt.

Wie viele Partitionen Sie auch einrichten - jede Einteilung ist besser als gar keine Unterteilung der Daten. Ohne Aufteilung muss man bei jeder Datensicherung jedes einzelne Verzeichnis mit unersetzlichen Daten finden und zum Brennauftrag hinzufügen. Die Gefahr ist groß, etwas zu vergessen, und der Aufwand ist typischerweise so hoch, dass die meisten Leute erfahrungsgemäß viel zu selten oder nie ihre Daten sichern. Welche Unterteilung für Ihre Festplatte sinnvoll ist, hängt von sehr vielen Bedingungen und Einschränkungen ab. Lassen Sie sich beraten!

Beispielhafte Einordnung einiger Datentypen:

| **Typ** | Eigenschaften | typische Menge | wie häufig sichern |
|---|---|---|---|
| Office, E-Mail | häufig verändert | 1 DVD reicht | täglich, Versionierung nötig |
| Fotosammlung | unveränderlich, nur Zuwachs | wenige DVD | gelegentlich den Zuwachs sichern |
| eigene Videos | unveränderlich, nur Zuwachs | viele DVD | manuell thematisch sichern |
| MP3-Sammlung | unveränderlich, nur Zuwachs | viele DVD | gelegentlich den Zuwachs sichern |
| Spielfilm-Sammlung | unveränderlich | zu viel | nicht sichern, weil wiederbeschaffbar |

Beim Festlegen der Größe der Partitionen kann es sinnvoll sein, sich an der Kapazität einer DVD zu orientieren. Dann ist eine Sicherung auf DVD jederzeit problemlos möglich.

Überlegen Sie, welche der nachfolgenden Partitionen Sie einrichten wollen:

- Systempartition C: mit 20 bis 40 GByte. Dort ist Platz für das Betriebssystem und alle Programme.
- Datenpartition mit 5 bis 20 GB für wichtige, veränderliche Daten.
- Eventuell Spezialpartitionen, z. B. für Fotos oder MP3-Dateien
- Archivpartition für wichtige Daten, die nie oder nur sehr selten verändert werden
- Kopien-Partition für Daten, die wiederbeschaffbar sind

- Reserve-Partition, etwas größer als die Systempartition. Ein bis zwei Images der Systempartition sollten hineinpassen.

Bringt das Aufsplitten Ihrer Daten auch Nachteile mit sich?

- Nein, denn die Datensicherung wird übersichtlicher.
- Ja, denn man muss sich Gedanken über seine Daten machen und die Daten sinnvoll aufteilen.
- Ja, denn man muss möglicherweise hin und wieder die Größe der Partitionen anpassen, wenn man das Wachstum der Datenmengen falsch eingeschätzt hat.

Falls Sie nun beschlossen haben, Ihre Daten auf mehrere Partitionen aufzuteilen - wie macht man das?

Am einfachsten ist es natürlich, gleich beim Einrichten der Festplatte die Partitionen anzulegen. Andernfalls müssen vorhandene Partitionen verändert werden.

```
<!-- Datenpartition weiter unterteilen -->
```

## 13.3 Prioritäten setzen

Die Daten passen nicht auf das Sicherungsmedium. Was kann man tun?

**Wie kann man den Aufwand verringern, ohne große Abstriche an der Sicherheit zuzulassen?**

1. Daten nach Wichtigkeit sortieren
2. Aktuelle Daten von den alten Daten trennen
3. Veränderliche Daten von den unveränderlichen Daten trennen
4. Die Häufigkeit der Datensicherung reduzieren

Betrachten wir nacheinander diese Methoden.

### 13.3.1 Daten nach Wichtigkeit sortieren

Die Wichtigkeit von Daten kann man nach verschiedenen Kriterien beurteilen:

- Wie viel Arbeit wurde für die Erstellung der Daten aufgewendet?
- Ist es überhaupt möglich, die Daten wiederherzustellen?
- Wenn es möglich ist: Wie schwierig wäre es, die Daten wiederherzustellen?

In selbst erstellten Texten und anderen Office-Dokumenten steckt in der Regel viel Arbeit. Wenn Sie das Dokument ausgedruckt und abgeheftet haben, ist es im Prinzip wiederherstellbar, wenn auch mit beträchtlichem Aufwand. Wenn kein Ausdruck existiert, ist es nicht wiederherstellbar.

Verloren gegangene Fotos können in der Regel nicht ersetzt werden, ein Verlust könnte emotional schwerwiegend sein.

Downloads können meist mit einem erträglichen Aufwand erneut heruntergeladen werden.

Das Betriebssystem und die Programme sollten vorrätig oder leicht beschaffbar sein. Eine Neuinstallation kann zwar aufwändig sein, ist aber nicht allzu schwierig.

### 13.3.2 Aktuelle Daten von den alten Daten trennen

Die Zahl der auf Ihrer Festplatte gespeicherten Dokumente wächst von Jahr zu Jahr. Entsprechend wächst der Zeitaufwand für eine komplette Datensicherung sowie der Speicherplatzbedarf. Ein gelegentliches Aufräumen (Löschen) alter Dateien mildert das Problem, behebt es aber nicht. Andererseits können Sie pro Tag nur eine begrenzte Menge an Dokumenten bearbeiten. Ein immer größer werdender Teil der gespeicherten Dokumente ist schon „seit Ewigkeiten“ nicht mehr verändert worden. Typischerweise sind deutlich weniger als 10% der Daten in den letzten 30 Tagen verändert worden. Die Aufteilung der Daten in aktuelle, die häufig gesichert werden, sowie alte Daten, die nur selten gesichert werden brauchen, ist eine der möglichen Lösungen des Problems.

Wie trennt man diese Daten? Manuell oder automatisch?

- XCOPY, ROBOCOPY und andere Dienstprogramme können Dateien abhängig von ihrem Alter kopieren. Beispielsweise kann man alle Dateien, die älter als drei Jahre sind, an einen anderen Speicherort verlagern. Beim Kopieren entsteht am neuen Speicherort die gleiche Verzeichnisstruktur wie am alten Ort. Diese Methode ist nicht allzu schwierig und erfordert kaum Zeitaufwand. Die Methode hat aber schwere Mängel:
  1. Dateien, die thematisch zusammengehören, werden auseinander gerissen. Findet man eine Datei im bisherigen Verzeichnis nicht mehr, muss man aufwändig in ein anderes Verzeichnis wechseln.
  2. In der täglichen Arbeit werden Dateien und Verzeichnisse umbenannt, verschoben und anders geordnet. Im Laufe der Jahre ändert sich die Verzeichnisstruktur und wird der früheren Struktur immer unähnlicher. Dadurch wird das Wiederfinden alter Dateien zunehmend schwieriger.
- Besser, wenn auch aufwändiger, ist die manuelle Methode. Abgeschlossene Vorgänge, alte Rechnungen und Steuererklärungen, Kündigungen und Bestellungen, abgeschlossenen Briefwechsel und ähnliches kann man von Zeit zu Zeit auf eine andere Partition verschieben, die weniger oft gesichert wird. Am früheren Speicherort hinterlässt man eine Verknüpfung zum neuen Speicherort, dadurch können die Daten jederzeit leicht wiedergefunden werden.

### 13.3.3 Veränderliche Daten von den unveränderlichen Daten trennen

Manche Daten werden nach dem erstmaligen Speichern nicht verändert. Dazu gehören E-Mails, PDF-Dokumente, ZIP-Archive, MP3-Dateien und Downloads. Es ist sinnvoll, diese Dateien von Anfang an separat anzuordnen. Bei diesen Daten braucht man keine früheren Versionen

### 13.3.4 Häufigkeit der Datensicherung reduzieren

Manche Datenarten werden nicht jeden Tag verändert. Ein typisches Beispiel sind Fotos. Fotos werden in der Regel nicht bearbeitet, Veränderungen bestehen meist nur im Hinzufügen neuer Fotos. In den meisten Fällen werden neue Fotos nicht jeden Tag hinzugefügt, sondern in mehrtägigen Abständen. Es genügt vollauf, Fotos an den Tagen nach Veränderungen zu sichern.

```
<!-- Häufige Sicherungen schützen vor kleinen Unfällen -->
```

### 13.3.5 Häufige Sicherungen schützen vor kleinen Unfällen

Die von Ihnen häufig bearbeiteten Dateien sollten Sie vor den kleinen Alltagspannen schützen, indem Sie diese täglich oder zumindest öfter sichern, und zwar jedes Mal in ein anderes Verzeichnis. Weil dabei nur wenige Dateiarten gesichert werden brauchen, ist der Zeitaufwand und der Speicherbedarf gering. Es ist nicht mal eine externe Festplatte notwendig, für diese Art der Sicherung genügt eine separate Partition oder ein Verzeichnis auf der internen Festplatte.

Wichtig ist dabei, dass diese Sicherung automatisch oder mit einem einzigen Klick gestartet werden kann, ohne dass weitere Eingaben gefordert sind. An dieser Hürde scheitern die manche Datensicherungsprogramme. Die Sicherung wird immer öfter weggelassen, wenn sie zu zeitaufwändig ist. Erfahrungsgemäß wird nach einem Vierteljahr kaum noch daran gedacht, die Daten zu sichern.

### 13.3.6 Gelegentliche Sicherungen zum Schutz vor Katastrophen

Hier geht es vor allem darum, nach einem Defekt der Festplatte oder ähnlichen Katastrophen nicht ohne Daten dazustehen. Die Daten müssen unbedingt auf eine andere Festplatte (eine externe oder die eines anderen PCs) oder auf einen (optischen) Datenträger gesichert werden.

# 14 Lebensdauer digitaler Daten

Sie möchten im Alter die Musik hören können, nach der Sie in der Jugend getanzt haben? Ihr Hochzeitsfoto und den Film, als Ihr Kind die ersten Schritte machte, möchten Sie ein halbes Jahrhundert später Ihren Enkeln und Urenkeln zeigen können?

**Sie haben ein Problem.**

Die digitale Welt wird vermutlich noch lange eine Welt der flüchtigen Informationen bleiben. Die beliebten Datenträger CD und DVD werden innerhalb weniger Jahre unbrauchbar. Selbst bei optimaler Einlagerung verlieren Festplatten und Magnetbänder die Magnetisierung. Externe Festplatten haben eine erschreckend hohe Ausfallrate. Die Haltbarkeit der Daten auf USB-Sticks ist nicht groß, Datenverluste sind häufig. In fünfzig Jahren wird der Großteil der heutigen Daten verloren, „in den Wind geschrieben“ sein. [1].

**Nicht nur Sie haben ein Problem.**

- 10 bis 20% der NASA-Datenbänder von der 1976er Viking-Mission zum Mars haben signifikante Fehler. [2]

Das bedeutet: Digitale Informationen bleiben nur dann erhalten, wenn sie oft genug kopiert werden.

Bei Dokumenten von besonderer Wichtigkeit sollte man über eine zusätzliche nicht-digitale Kopie nachdenken. Papier und andere nicht-digitale Medien sind relativ lange haltbar und überstehen ein halbes oder ganzes Jahrhundert in brauchbarer Qualität. Selbst wenn zahlreiche kleine Beschädigungen auftreten, bleibt ein Text, Bild oder Musikstück noch verwendbar. Im Unterschied dazu kann schon ein einziges falsches Bit eine Datei für normale Nutzung unbrauchbar machen.

Ein klassisches Schwarz-Weiß-Foto auf gutem Fotopapier hat eine gute Haltbarkeit. Farbfotos auf hochwertigem Material haben eine brauchbare Haltbarkeit. Bedingung ist aber, dass sie im Dunkeln und nicht warm gelagert werden.

In der ersten Hälfte des 20. Jahrhunderts waren die meisten Papiersorten säurehaltig und sind deshalb nur sehr begrenzt haltbar. Heutige Papiere sind weitgehend säurefrei. Für die Archivierung sollte man gezielt nach hochwertigen Materialien suchen. Papyrus ist sehr lange haltbar, aber heute wohl nicht mehr zu bekommen.

Ein weiteres Problem ist die Tintenqualität. Viele Tinten enthalten Eisen, welches verrostet und Löcher in das Papier frisst. Hochwertiges Papier, mit einem Laserdrucker bedruckt, hat eine sehr gute Chance auf Langlebigkeit. Einige Hersteller von Tintendruckern machen Langzeittests mit ihrer Tinte und erreichen ebenfalls eine recht hohe Haltbarkeit.

---

1 `http://www.longnow.org/views/essays/articles/writtenonwind.php`
2 Nach: c't 2000, Heft 24, S. 114

Eins haben Fotos, Papier, Magnetbänder und optische Datenträger gemeinsam: Wärme und Licht verkürzen die Haltbarkeit drastisch, direkte Sonneneinstrahlung wirkt geradezu verheerend. Die Verwendung billiger Materialien reduziert ebenfalls die Haltbarkeit.

## 14.1 Kopieren, Kopieren, Kopieren ...

Es gibt nur zwei bewährte Verfahren, um Informationen dauerhaft haltbar zu machen.

Die erste Methode wurde bereits von den Pharaonen verwendet. Sauber in Granit gemeißelt und vor Umwelteinflüssen gut geschützt (z. B. im Inneren einer Pyramide) bleibt die Information nahezu ewig erhalten, zumindest einige tausend Jahre.

Die zweite bewährte Methode wurde Jahrtausendelang von Priestern und Mönchen benutzt und ist im Computer-Zeitalter aktueller denn je: Ganze Bibliotheken wurden wieder und wieder und wieder präzise abgeschrieben. Die Kopien wurden weiträumig in Europa verteilt. So haben einige von der ungeheuren Anzahl dieser Kopien alle Kriege, Feuersbrünste, Naturkatastrophen sowie den „Zahn der Zeit“ überlebt.

In Ermangelung an Granit und Zeit bleibt für den Alltagsgebrauch nur die zweite Methode und hieraus resultierend folgende Möglichkeiten:

- Differenzielle und inkrementelle Backups von Daten
- Spiegelungen von Datenträgern via Software und Hardware (Raid)
- Regelmäßiges Überspielen der Daten auf aktuelle Speichermedien, alte Speichermedien aufbewahren
- Datenträger an verschiedenen Orten lagern.

Selbst die Methode des ständigen Kopierens kann einem Datenverlust nicht per se vorbeugen. Selbst wenn ein Backup oder eine Kopie vorhanden ist, so kann es vorkommen, dass Daten falsch gespeichert wurden und die Integrität des Datenträgers somit nicht mehr gewährleistet ist. Die jahrtausende alte Methode ist unbestritten deutlich sicherer, da sich mit ihrer Hilfe eine fast 100 prozentige Datenintegrität realisieren lässt.

**Nur kopierte Daten sind sichere Daten.**

## 14.2 Statistiken zur Lebensdauer von Datenträgern

## 14.3 Wie hoch ist die Lebensdauer meiner Daten?

Möglicherweise haben Sie hier eine Statistik erwartet, wie lange durchschnittlich eine CD, eine DVD oder ein USB-Stick lesbar bleiben. Doch so eine Statistik habe ich nicht. Eine dreitägige Suche im Internet hat nichts vertrauenswürdiges ergeben. Wahrscheinlich wird es so eine Statistik nie geben. Warum?

Die Hersteller testen die Lebensdauer ihrer Medien unter Prüfbedingungen, von denen sie glauben bzw. spekulieren, dass eine einmonatige Lagerung bei erhöhter Temperatur einer Alterung von 10 Jahren unter Normalbedingungen entspricht. Es gibt aber nicht allzu viele zehn Jahre alte Exemplare, an denen man überprüfen könnte, ob die zehn Jahre früher gemachten Spekulationen über deren Haltbarkeit zutreffen.

Die Firma Sandisk hat im September 2011 einen Speicherstick „Sandisk Memory Vault mit Chronolock-Technologie“ herausgebracht, *der die kostbarsten Erinnerungen in Originalqualität bis zu 100 Jahre speichern kann* (siehe `http://sandisk.de/misc/preserve)`. **Kann**, wohlgemerkt. Auf `http://forums.sandisk.com/t5/Memory-Vault/Technology-amp-Life-Testing/td-p/245746` ist genau beschrieben, wie die Haltbarkeit ermittelt wurde. 30 Sticks wurden 336 Stunden (das sind 14 Tage, nicht gerade lange) bei 125 °C getestet. Daraus wurde eine Lebensdauer von 104 Jahren mit der Arrhenius-Gleichung[3] ermittelt. Ein Faktor dieser Gleichung ist die Boltzmann-Konstante[4], welche die Entropie (die Alterungsgeschwindigkeit des Universums) beschreibt. Es ist anzunehmen, dass alle Hersteller diese Gleichung benutzen. Irgendwie leuchtet es mir nicht ein, dass sich die vielfältigen Ursachen, die zu einem Ausfall führen können, mit einer einzigen Formel berücksichtigen lassen. Dass man *nur* 30 Sticks *nur* 14 Tage lang getestet hat, verstärkt mein Vertrauen auch nicht.

Fachzeitschriften testen die Medien ebenfalls. Diese Tests sind recht gründlich und die Ergebnisse sind nicht durch Herstellerinteressen verfälscht. Aber auch die Fachzeitschriften arbeiten mit Vermutungen, wie man aus einige Tage andauernden Tests Rückschlüsse auf mehrere Jahre ableiten kann. Eine glaubwürdige Statistik setzt voraus, dass die Medien zehn Jahre lang unter reproduzierbaren, typischen Bedingungen benutzt und aufbewahrt worden sind. Was sind aber typische Bedingungen? Eine Aussage des Herstellers, dass die Lagerung bei 10 °C eine zehnjährige Haltbarkeit sichert, nützt Ihnen gar nichts - oder kennen Sie jemanden, des sich eine Klimakammer zugelegt hat, um die CDs entsprechend der Herstellervorschrift lagern zu können?

Wenn ein Hersteller nach zehn Jahren eine Statistik erstellen würde, wie viele seiner Datenträger überlebt haben - was würde es ihm oder Ihnen nützen? Die Fertigungstechnologie ist inzwischen mehrmals umgestellt worden, die alten Erkenntnisse sind auf die gegenwärtige Produktion kaum anwendbar.

Wenn es zuverlässige Daten über mittlere Haltbarkeit gäbe - was würden sie Ihnen nützen? Kein Hersteller wird Ihnen jemals **garantieren**, dass sein Datenträger drei Jahre hält. Wenn Sie Pech haben, ist er schon am nächsten Tag kaputt.

Eine Angabe „mehr als 95% der DVD halten mindestens drei Jahre“ würde Ihnen wenig nützen. Selbst wenn diese Behauptung stimmt, wissen Sie nicht, ob Sie eine von den 5% oder von den 95% gekauft haben.

Wenn ein Hersteller seine DVD mit der Aufschrift „Drei Jahre garantierte Haltbarkeit“ bedrucken würde - was würde es Ihnen nutzen, wenn Sie im Garantiefall nach dem Ausfüllen und Einschicken einer Schadensmeldung kostenlos einen neuen Rohling bekämen? Auf den Kosten einer Datenrettung bleiben Sie sitzen.

3 `http://de.wikipedia.org/wiki/Arrhenius-Gleichung`
4 `http://de.wikipedia.org/wiki/Boltzmann-Konstante`

Die Lebensdauer der Daten hängt **ganz entscheidend** von der richtigen Lagerung ab. Lagern Sie alle Ihre DVD stehend, im Dunkeln, bei einer Temperatur unter 25 °C und einer Luftfeuchtigkeit von maximal 80%? Eine DVD im Hochsommer auf dem Tisch am Fenster eine Woche lang liegen gelassen - das kann's schon gewesen sein.

Der Zufall ist nicht zu unterschätzen. Von der gesamten Kapazität einer Daten-CD entfallen 47% auf die Daten und 53% auf Zusatzinformationen für Fehlerkorrektur, Codierung und Synchronisation. Eine CD kann daher eine Unmenge kleiner Kratzer verkraften. Allerdings kann unter unglücklichen Umständen ein einziger Kratzer die CD unlesbar machen. Besonders kritisch sind kreisförmige Kratzer.

DVDs verwenden ein besseres Fehlerkorrekturverfahren als CDs. Andererseits sind die Strukturen einer DVD viel feiner. Die empfindliche Schicht kann zwar nicht zerkratzt werden, denn bei einer DVD liegt sie mittig. Trotzdem sind oberflächliche Kratzer gefährlich, weil sie den Laserstrahl zerstreuen.

In einem Punkt stimmen die Tests überein: Die Verwendung von Markenware im Vergleich zu No-Name-Material erhöht die Lebensdauer drastisch (ich spekuliere mal: auf das zwei- bis dreifache). Von den Markendisketten aus den Jahren ab 1973 sind zwei Drittel noch problemlos und vollständig lesbar, von den Billigdisketten ist etwa jede zehnte noch lesbar. Allerdings kann auch einem Markenhersteller eine Charge misslingen.

Im übrigen gilt Murphys Gesetz[5]: Je wertvoller die Daten, desto wahrscheinlicher gehen sie verloren.

## 14.4 Welche Medien sind für die Langzeitarchivierung zu empfehlen?

*Wann immer irgendwo ein Test von CD-/DVD-Rohlingen durchgeführt wird, kommt dabei ein niederschmetterndes Ergebnis raus. Rohlinge sind eher Datensärge als Datenspeicher. Bereits ein frisch gebrannter Rohling kann nach kurzer Zeit Müll sein, noch kritischer sieht die Sache bei der Lebenserwartung aus.* (Zitat aus www.nickles.de[6]

Andererseits sind DVDs die mit Abstand preiswertesten Datenträger.

- Blu-ray Disks sind ein relativ neues Medium, zu dem wenig Langzeiterfahrungen vorliegen. Die Hersteller suchen noch nach den besten Mischungen für die Aufnahmeschicht.
- Auf zweilagige DVD sollte man verzichten. Die Justierung des Lasers auf die zweite Schicht ist nicht unproblematisch, es ist mit höheren Fehlerraten zu rechnen.
- Bei DVD-RW muss die Laserleistung wesentlich genauer als bei DVD-R auf die Eigenschaften der Aufnahmeschicht justiert werden. *Fast alle DVD-Brenner, die wir in den vergangenen Jahren getestet haben, produzierten mit RW-Medien inakzeptabel hohe Fehlerraten, sodass wir von ihrem Einsatz zur Archivierung abraten.* (c't 16/08[7].

5 http://de.wikipedia.org/wiki/Murphys%20Gesetz

6 Rohlinge sind eher Datensärge als Datenspeicher http://www.nickles.de/c/s/praxis-cd-dvd-rohlinge-qualitaet-pruefen-und-daten-retten-529-1.htm

7 Archiv-DVDs im Langzeittest http://www.heise.de/ct/artikel/Silberne-Erinnerungen-291658.html

- DVD-RAM haben angeblich eine Haltbarkeit von 30 Jahren, aber es scheint keinen Prüfbericht eines unabhängigen Labors zu geben, der das bestätigen würde.

Man sollte also einlagige DVD-R oder DVD+R verwenden. Eine unvollständige Liste empfehlenswerter Fabrikate mit überdurchschnittlicher Haltbarkeit:

- Kodak produziert "goldene DVD" mit einer angeblichen Haltbarkeit von 100 Jahren.
- Verbatim bietet DVD-R "Archival Grade" an.
- Die "Scratchproof DVD-R von TDK hat eine besonders kratzfeste Schutzschicht.

## 14.5 Ist die DVD noch in einem guten Zustand?

Mit „Nero DiscSpeed“ oder „Nero CD-DVD-Speed“ kann man den Alterungsgrad der Aufzeichnung ermitteln. In einer Grafik werden leicht beschädigte Sektoren gelb und unlesbare Sektoren rot angezeigt. Wenn Sie Gelb oder Rot sehen, sollten Sie eine Kopie anfertigen. Sogar bei roten Sektoren gelingt das Kopieren manchmal. Bei wichtigen DVDs sollte man die erste Überprüfung sofort nach dem Brennen vornehmen.

Manchen Brennern legt der Hersteller ein Programm zur Qualitätsmessung bei. Plextor-Brennern liegt oft „PlexTools“ bei, K-Probe gibt es zu Lite-On-Laufwerken dazu.

Das einfachste Mittel, um die Lesbarkeit der Daten zu testen: Kopieren Sie die Daten in ein temporäres Verzeichnis der Festplatte. Wenn das nicht mehr vollständig gelingt, sollten Sie wenigstens den Rest der Daten auf eine neue DVD retten.

## 14.6 Wann sollte man die Daten auf ein neues Medium umkopieren?

Rechtzeitig bevor die DVD versagt, auch wenn man nicht weiß, wann das sein wird. Sie sollten von allen wichtigen Daten eine Kopie haben. Wenn die Daten der einen DVD nicht vollständig lesbar sind, können Sie die fehlenden Dateien von der zweiten DVD ergänzen.

### Einige Meinungen zur Haltbarkeit von Medien

- `http://www.techwriter.de/thema/lebensda.htm`
- Haltbarkeit der Trägermedien[8]

8 `http://de.wikipedia.org/wiki/Langzeitarchivierung%23Haltbarkeit_der_Tr.C3.A4germedien`

# 15 Lebensdauer von Technologien

## 15.1 Die Lebensdauer von Speichertechnologien

Zu einer Speichertechnologie gehören Datenträger, Laufwerk, PC und Software. Die Speichertechnologien wechseln schnell. Die ersten PC-Diskettenlaufwerke hatten 1981 eine Kapazität von 160 kByte, dann stiegen die Kapazitäten auf 180, 320, 360, 720, 1200, 1440 und 2880 kByte. Heute sind Disketten ungebräuchlich geworden, die meisten neuen PCs werden ohne Diskettenlaufwerk ausgeliefert. Haben Sie schon alle Ihre Disketten weggeworfen? Im gleichen Zeitraum wechselte das Aufzeichnungsverfahren der Festplatten von FW, MFM zu RLL. Die ST506-Festplattencontroller wurden durch IDE, eIDE, P-ATA und S-ATA abgelöst, wobei es auch noch SCSI, SAS und FC gibt. Ein ähnliches Änderungstempo liegt auch bei anderen Speichertechnologien vor. Mit Blu-ray-Laufwerken, der neuesten optischen Speichertechnologie, sind erst etwa 10% aller PC ausgerüstet, während Samsung daran glaubt, dass Blu-ray schon in fünf bis zehn Jahren wieder vom Markt verschwunden sein wird. [1]

Das bedeutet, dass man nach jeweils fünf bis zehn Jahren beginnen muss, seine Daten zu sichten und sie auf modernere Speichermedien zu übertragen, damit sie - hoffentlich - ein weiteres Jahrzehnt überleben können.

## 15.2 Die Lebensdauer von Kodierungen

Ein weiteres Problem ist die verwendete Codierung. Hieroglyphen und Keilschrift sind nur schwer zu entziffern. Mit digitalen Codierungen steht es viel viel viel schlimmer. 1982 war ein geniales Textprogramm namens „WordStar“ allgegenwärtig. 1991 wurde dessen Weiterentwicklung eingestellt, weil das Programm „Word Perfect“ klar überlegen war. Bald danach war auch „Word Perfect“ vergessen. Beginnend 1996 konnte das damals aktuelle WinWord das WordStar-Textformat nicht mehr lesen. Wollte man alte mit WordStar geschriebene Texte heute lesen, bliebe nur, WordStar zu installieren. Das ist fast unmöglich. Wer hat noch lesbare Installationsdisketten? Hat Ihr PC noch ein 5,25" Diskettenlaufwerk? Vermutlich lässt es sich auch nicht nachträglich einbauen, denn die meisten modernen PCs haben keine BIOS-Unterstützung mehr für 5,25" Laufwerke. Selbst wenn Sie Laufwerk und Installationsdisketten haben: Verträgt sich WordStar mit dem Windows-Betriebssystem? Auch mit den zukünftigen 64-Bit-Systemen? Letztlich bleibt nur die Konvertierung in „Handarbeit“. Leider ist die Konvertierung eines WordStar-Textes extrem schwierig, fast so langwierig wie ihn neu zu tippen.

1 `http://www.pocket-lint.co.uk/news/news.phtml/17399/18423/samsung-blu-ray-5-years-left.phtml` Interview mit dem „director of consumer electronics“ von Samsung UK

Ein anderes Beispiel: Das Einsteiger-Officeprogramm „MS Works“ ist „nur“ etwa zehn Jahre alt. Versuchen Sie mal, einen mit MS Works geschriebenen Text mit dem Programm Word zu öffnen! Es ist nicht unmöglich, aber für den „Normalbenutzer“ schwierig. Mit Works-Tabellen und -Datenbanken ist es keinesfalls einfacher...

In wie vielen Jahren wird es vermutlich schwierig werden, einen mit Word geschriebenen Text mit eingebetteten Bildern und Grafiken zu öffnen? Word 5.0 beispielsweise hat ein Jahr-2000-Problem.

In wie vielen Jahren wird man kein Betriebssystem mehr finden können, auf dem sich Word installieren lässt?

Es gibt eine kaum überschaubare Zahl von Codierungen für Videos (Codecs), Musik und Fotos. Ständig werden neue, bessere entwickelt, andere werden ungebräuchlich. Wie viele von ihnen werden überleben? Wird sich ein Programmierer die Mühe machen, auch noch das älteste, inzwischen total ungebräuchliche Format in seinen neuen Player zu integrieren? Wohl kaum. Das gleiche Problem gibt es mit den zahllosen Programmen zur Datenkompression. Es werden nur wenige überleben.

Archivar ist ein Ausbildungsberuf, denn sachkundiges Archivieren ist komplizierter, als nur Kopien in ein Regal zu stellen und sie bei Bedarf wiederzufinden. Wobei das Wiederfinden vermutlich das größte Problem ist. Wenn Ihre Daten überleben sollen, müssen Sie Zeit und Gedanken darauf verwenden.

## 15.3 Empfehlungen

- Den größten Einfluss auf die Haltbarkeit haben schonender Umgang und sachgemäße Lagerung.
- Kaufen Sie hochwertige Datenträger und Geräte.
- CDs sind etwas zuverlässiger als DVDs, weil DVDs die fünffache Datendichte haben, ohne dass die Codierung mehr Redundanz beinhaltet.
- DVD-RAM sind die zuverlässigsten optischen Medien: Sie haben ein gutes Defektmanagement. Im Unterschied zu allen anderen optischen Medien gibt es eine Spezifikation, die eine mindest dreißigjährige Haltbarkeit fordert.
- Einmal-beschreibbare optische Datenträger sind etwas langlebiger als mehrfach-beschreibbare, wenn sie im Dunkeln gelagert werden.
- Benutzen Sie Medien verschiedener Hersteller, um bei einem Chargenfehler nicht alle Kopien gleichzeitig zu verlieren.
- Benutzen Sie nur die gebräuchlichsten Dateiformate. Konvertieren sie gegebenenfalls veralternde Dateiformate in aktuellere.
- Vergleichen Sie gleich nach dem Kopieren jede Kopie mit dem Original.
- Führen Sie einen Katalog oder ein Verzeichnis, welche Daten sich auf welchen Medien befinden.
- Mustern Sie die weniger guten Fotos aus. Wenn man fünf gute Fotos hat, wozu weitere zwanzig weniger gute aufbewahren?
- Mustern Sie uninteressant gewordene Daten aus. Sie werden auch im Rentenalter weder Zeit noch Lust haben, zehntausend Fotos zu betrachten. Ihre Enkel werden vermutlich noch weniger Lust dazu haben.

- Ein einzelner Bitfehler kann eine einzelne Datei unbrauchbar machen. Wenn Sie viele Dateien zu einer Archivdatei zusammenfassen und komprimieren, gehen durch einen einzigen Bitfehler möglicherweise alle darin enthaltenen Dateien verloren. [2] ***Komprimieren Sie deshalb die Daten nicht.***

2 Warum komprimierte Daten anfälliger für Fehler sind, ergibt sich daraus, dass wenn es innerhalb dieser Daten zu Fehlern kommt, diese beim Decodieren Folgefehler nach sich ziehen. Einige Bytes Veränderung machen ein Archiv unbrauchbar. Bei einer reinen Huffmancodierung fängt sich der Code wieder, wenn er zufällig auf ein gültiges Codewort trifft und es kommt zu einem Bündelfehler, alle Wörterbuchbasierenden Verfahren (LZ...) führen zu erheblich entstellenden Byte und Bündelfehlern. -- ThePacker ^{`http://de.wikibooks.org/wiki/Benutzer%3AThePacker`} 21:57, 28. Jul. 2008 (CEST)

# 16 Quellen

# 17 Lizenz

Siehe http://de.wikipedia.org/wiki/Wikipedia:Lizenzbestimmungen

# 18 Autoren

| Edits | User |
|---|---|
| 4 | Dirk Huenniger[1] |
| 7 | Heuler06[2] |
| 1 | JARU[3] |
| 4 | Juetho[4] |
| 629 | Klaus Eifert[5] |
| 11 | ThePacker[6] |
| 6 | Uncopy[7] |

1 http://de.wikibooks.org/wiki/Benutzer:Dirk_Huenniger
2 http://de.wikibooks.org/wiki/Benutzer:Heuler06
3 http://de.wikibooks.org/wiki/Benutzer:JARU
4 http://de.wikibooks.org/wiki/Benutzer:Juetho
5 http://de.wikibooks.org/wiki/Benutzer:Klaus_Eifert
6 http://de.wikibooks.org/wiki/Benutzer:ThePacker
7 http://de.wikibooks.org/wiki/Benutzer:Uncopy

# Abbildungsverzeichnis

- GFDL: Gnu Free Documentation License. http://www.gnu.org/licenses/fdl.html
- cc-by-sa-3.0: Creative Commons Attribution ShareAlike 3.0 License. http://creativecommons.org/licenses/by-sa/3.0/
- cc-by-sa-2.5: Creative Commons Attribution ShareAlike 2.5 License. http://creativecommons.org/licenses/by-sa/2.5/
- cc-by-sa-2.0: Creative Commons Attribution ShareAlike 2.0 License. http://creativecommons.org/licenses/by-sa/2.0/
- cc-by-sa-1.0: Creative Commons Attribution ShareAlike 1.0 License. http://creativecommons.org/licenses/by-sa/1.0/
- cc-by-2.0: Creative Commons Attribution 2.0 License. http://creativecommons.org/licenses/by/2.0/
- cc-by-2.0: Creative Commons Attribution 2.0 License. http://creativecommons.org/licenses/by/2.0/deed.en
- cc-by-2.5: Creative Commons Attribution 2.5 License. http://creativecommons.org/licenses/by/2.5/deed.en
- cc-by-3.0: Creative Commons Attribution 3.0 License. http://creativecommons.org/licenses/by/3.0/deed.en
- GPL: GNU General Public License. http://www.gnu.org/licenses/gpl-2.0.txt
- LGPL: GNU Lesser General Public License. http://www.gnu.org/licenses/lgpl.html
- PD: This image is in the public domain.
- ATTR: The copyright holder of this file allows anyone to use it for any purpose, provided that the copyright holder is properly attributed. Redistribution, derivative work, commercial use, and all other use is permitted.
- EURO: This is the common (reverse) face of a euro coin. The copyright on the design of the common face of the euro coins belongs to the European Commission. Authorised is reproduction in a format without relief (drawings, paintings, films) provided they are not detrimental to the image of the euro.
- LFK: Lizenz Freie Kunst. http://artlibre.org/licence/lal/de
- CFR: Copyright free use.

- EPL: Eclipse Public License. `http://www.eclipse.org/org/documents/epl-v10.php`

Copies of the GPL, the LGPL as well as a GFDL are included in chapter Licenses[8]. Please note that images in the public domain do not require attribution. You may click on the image numbers in the following table to open the webpage of the images in your webbrower.

8 Kapitel 19 auf Seite 91

| | | |
|---|---|---|
| 1 | Adlerweb[9] Original uploader was Adlerweb[10] at de.wikipedia[11] | |

9 http:////de.wikipedia.org/wiki/Benutzer:Adlerweb
10 http:////de.wikipedia.org/wiki/User:Adlerweb
11 http://de.wikipedia.org

# 19 Licenses

## 19.1 GNU GENERAL PUBLIC LICENSE

Version 3, 29 June 2007



Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow. TERMS AND CONDITIONS 0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion. 1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work. 2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary. 3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures. 4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee. 5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

* a) The work must carry prominent notices stating that you modified it, and giving a relevant date. * b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices". * c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it. * d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate. 6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

* a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange. * b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge. * c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b. * d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements. * e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying. 7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

* a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or * b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or * c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or * d) Limiting the use for publicity purposes of names of licensors or authors of the material; or * e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or * f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way. 8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10. 9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so. 10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it. 11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law. 12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from

conveying the Program. 13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such. 14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License “or any later version” applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version. 15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION. 16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. 17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.> Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short notice like this when it starts in an interactive mode:

<program> Copyright (C) <year> <name of author> This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, your program's commands might be different; for a GUI interface, you would use an “about box”.

You should also get your employer (if you work as a programmer) or school, if any, to sign a “copyright disclaimer” for the program, if necessary. For more information on this, and how to apply and follow the GNU GPL, see <http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License. But first, please read <http://www.gnu.org/philosophy/why-not-lgpl.html>.

# 19.2 GNU Free Documentation License

Version 1.3, 3 November 2008

Copyright © 2000, 2001, 2002, 2007, 2008 Free Software Foundation, Inc. <http://fsf.org/>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. 0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "freeïn the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference. 1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Versionöf the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A SSecondary Sectionïs a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The Ïnvariant Sectionsäre certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Textsäre certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent"copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparentïs called Öpaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page"means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page"means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

The "publisher"means any person or entity that distributes copies of the Document to the public.

A section Ëntitled XYZ"means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as Äcknowledgements", "Dedications", Ëndorsements", or "History".) To "Preserve the Titleöf such a section when you modify the Document means that it remains a section Ëntitled XYZäccording to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License. 2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies. 3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document. 4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

* A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission. * B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement. * C. State on the Title page the name of the publisher of the Modified Version, as the publisher. * D. Preserve all the copyright notices of the Document. * E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices. * F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below. * G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice. * H. Include an unaltered copy of this License. * I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "Historyîn the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence. * J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "Historyßection. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission. * K. For any section Entitled Äcknowledgementsör "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein. * L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles. * M. Delete any section Entitled Ëndorsements". Such a section may not be included in the Modified Version. * N. Do not retitle any existing section to be Entitled Ëndorsementsör to conflict in title with any Invariant Section. * O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled Ëndorsements", provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version. 5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "Historyîn the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled Äcknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled Ëndorsements". 6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document. 7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an ãggregateïf the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate. 8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled Äcknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title. 9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, or distribute it is void, and will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, receipt of a copy of some or all of the same material does not give you any rights to use it. 10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License ör any later versionäpplies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation. If the Document specifies that a proxy can decide which future versions of this License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Document. 11. RELICENSING

"Massive Multiauthor Collaboration Site"(or "MMC Site") means any World Wide Web server that publishes copyrightable works and also provides prominent facilities for anybody to edit those works. A public wiki that anybody can edit is an example of such a server. A "Massive Multiauthor Collaboration"(or "MMC") contained in the site means any set of copyrightable works thus published on the MMC site.

"CC-BY-SA"means the Creative Commons Attribution-Share Alike 3.0 license published by Creative Commons Corporation, a not-for-profit corporation with a principal place of business in San Francisco, California, as well as future copyleft versions of that license published by that same organization.

Ïncorporate"means to publish or republish a Document, in whole or in part, as part of another Document.

An MMC is ëligible for relicensingïf it is licensed under this License, and if all works that were first published under this License somewhere other than this MMC, and subsequently incorporated in whole or in part into the MMC, (1) had no cover texts or invariant sections, and (2) were thus incorporated prior to November 1, 2008.

The operator of an MMC Site may republish an MMC contained in the site under CC-BY-SA on the same site at any time before August 1, 2009, provided the MMC is eligible for relicensing. ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

Copyright (C) YEAR YOUR NAME. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with ... Texts."line with this:

with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.

# 19.3 GNU Lesser General Public License

GNU LESSER GENERAL PUBLIC LICENSE

Version 3, 29 June 2007



Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General Public License, supplemented by the additional permissions listed below. 0. Additional Definitions.

As used herein, “this License” refers to version 3 of the GNU Lesser General Public License, and the “GNU GPL” refers to version 3 of the GNU General Public License.

“The Library” refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

An “Application” is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library. Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.

A “Combined Work” is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the “Linked Version”.

The “Minimal Corresponding Source” for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The “Corresponding Application Code” for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work. 1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL. 2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

* a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or * b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

* a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License. * b) Accompany the object code with a copy of the GNU GPL and this license document.

4. Combined Works.

You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:

* a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License. * b) Accompany the Combined Work with a copy of the GNU GPL and this license document. * c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document. * d) Do one of the following: o 0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source. o 1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version. * e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

* a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License. * b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License “or any later version” applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.