# 5 Methoden und Hilfsmittel

## 5.1 Vollsicherung und Teilsicherung

Mit dem Begriff „Vollsicherung“ ist gemeint, dass von der gesamten Festplatte oder einem ausgewählten Teil der Festplatte (Partition oder Verzeichnis mit Unterverzeichnissen) ausnahmslos alle Dateien kopiert werden, wobei weder in ältere und neue Dateien unterschieden wird noch in früher bereits gesicherte und noch nie gesicherte Dateien, ohne irgendwelche Ausnahmen. Auch ein Sicherungsauftrag „**alle** Dateien im Ordner Briefe“ oder „**alle** Textdateien vom Dateityp *.doc*“ wäre eine Vollsicherung.

- 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 Wiederherstellungsmethoden.
- Nachteil bei der Sicherung: Der Bedarf an Sicherungsmedien und der Zeitaufwand für die Sicherung sind am größten. Wer immer nur Vollsicherungen erstellt, wird seine Backups aus Speicherplatzmangel oft überschreiben müssen, oder er kann seine Daten nur selten sichern. Beides ist schlecht.

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. Vergleicht man zwei Sicherungen, die 30 Tage auseinanderliegen, steigt die Anzahl der veränderten und neu hinzugekommenen Dateien nicht auf das dreißigfache, denn manche Dateien werden im Laufe des Monats mehrmals verändert. Wenn man nur die Daten sichert, die seit der letzten Vollsicherung hinzugekommen oder geändert worden sind, ist das eine **Teilsicherung**, und zwar eine „Zuwachssicherung“, auch „Inkrementelle Sicherung“ genannt.

Hier stellt sich die Frage: Welche Möglichkeiten gibt es, die veränderten unter der Masse der unveränderten Dateien herauszusuchen? Wenn man nur wenige Dateien zu sichern hat, geht das „von Hand“: Man kann mit einigen Mausklicks auswählen, was gesichert werden soll. Doch wenn man zehntausende Dateien hat, ist es viel zu aufwändig und fehlerträchtig, die veränderten Dateien manuell herauszusuchen. Zum Glück haben die Schöpfer des Dateisystems rechtzeitig daran gedacht und das „Archivbit“ vorgesehen, um das „Heraussuchen“ der veränderten Dateien automatisieren zu können.

## 5.2 Das Archivbit und dessen Nutzung

Jede Datei hat 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. Zwei weitere Attribute sind das „Archivattribut“ und „Versteckt“ (engl. „Hidden“). Klicken Sie mit der rechten Maustaste auf eine beliebige Datei und dann mit der linken Maustaste auf „Einstellungen“. Im unteren Bereich des Fensters finden Sie die Dateiattribute „Schreibgeschützt“ und „Versteckt“, unter „Erweitert“ ist das Attribut „Archiv“ zu finden, wo standardmäßig ein Haken zu sehen ist. Das Betriebssystem setzt den Haken jedesmal automatisch („Datei kann archiviert werden“), wenn eine Datei neu erstellt, verändert, umbenannt oder in ein anderes Verzeichnis verschoben wird. Dieses Archiv-Kennzeichen zeigt den Datensicherungsprogrammen, dass es von der Datei keine aktuelle Sicherung gibt.

Jedes Datensicherungsprogramm kann dieses Bit auswerten und je nach Voreinstellungen das Bit zurücksetzen (den Haken entfernen) oder unverändert belassen. Als Beispiel seien hier die Befehle `xcopy` und `robocopy` genannt, die an der Eingabeaufforderung verwendet werden können (mehr dazu im Kapitel 9.4). Ist der Parameter **`/m`** angegeben, wird das Archivbit nach dem Kopieren gelöscht. Mit dem Parameter **`/a`** wird das Archivbit nach dem Kopieren nicht verändert.

## 5.2.1 Inkrementelle Sicherung

Der ersten inkrementellen Sicherung muss eine Vollsicherung vorangehen, bei der alle kopierten Dateien als gesichert gekennzeichnet worden sind, indem das „Archiv"-Attribut zurückgesetzt (gelöscht) wird. Kommen neue Dateien dazu oder werden Dateien geändert, setzt Windows deren Archivbit. Bei den nachfolgenden „inkrementellen" Sicherungen wird das Archivbit ausgewertet und es werden nur diejenigen Dateien gesichert, die seit der vorhergehenden inkrementellen Sicherung erstellt oder geändert worden sind. Sobald eine Datei gesichert (kopiert) ist, wird deren Archivbit deaktiviert (gelöscht).

Wenn beispielsweise an jedem Montag eine Vollsicherung durchgeführt wird, werden am Dienstag die seit Montag geänderten Dateien gesichert und nun ebenfalls als „gesichert" gekennzeichnet. Am Mittwoch werden die seit der dienstäglichen Sicherung geänderten Dateien gesichert usw. Der Zeit- und Platzbedarf für die Sicherung ist gering. Allerdings ist der Aufwand bei einer Wiederherstellung hoch, denn im Katastrophenfall muss zuerst die letzte Vollsicherung (vom Montag) zurückkopiert werden, anschließend müssen alle folgenden inkrementellen Sicherungen in chronologischer Reihenfolge zurückkopiert werden. Der Bedarf an Datenträgern ist ebenfalls hoch.

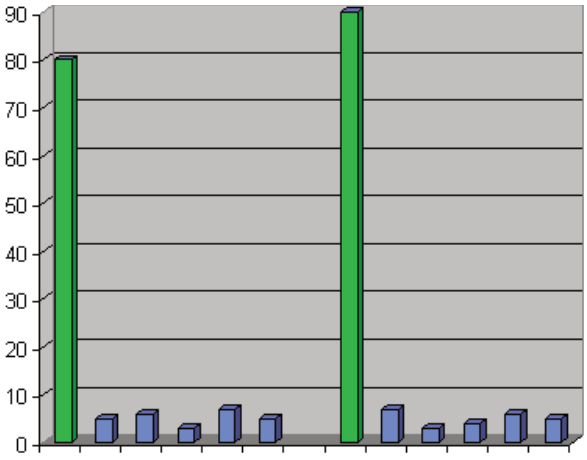


Bild 5.1: Datenmenge bei Inkrementeller Sicherung
Grün: Vollsicherung, blau: Änderungen seit dem Vortag

## 5.2.2 Differenzielle Sicherung

Vor der ersten differenziellen Sicherung wird eine Vollsicherung durchgeführt, bei der alle gesicherten Dateien als „archiviert" gekennzeichnet werden (das „Archiv"-Attribut wird dazu zurückgesetzt). In den folgenden Tagen werden alle Dateien kopiert, die seit der letzten Vollsicherung erstellt bzw. geändert wurden. Das Archiv-Attribut wird dabei nicht geändert.

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

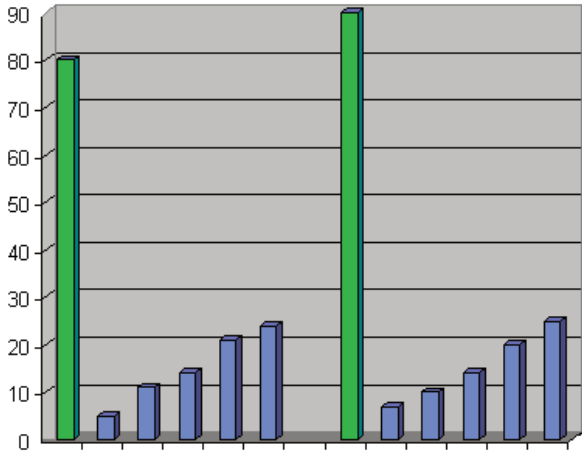


Bild 5.2: Datenmenge bei Differenzieller Sicherung
Grün: Vollsicherung, blau: Änderungen seit Vollsicherung

- Vorteil: Für eine Wiederherstellung werden nur zwei Datenträger benötigt: die letzte Vollsicherung und die letzte Differentialsicherung. Die Wiederherstellung der Daten erfolgt deutlich schneller als bei einer inkrementellen Sicherung.
- Nachteil: Der Zeit- und Platzbedarf für die Sicherung wächst jeden Tag. Je nach Umfang der täglichen Änderungen wird es immer wieder einmal notwendig sein, eine Vollsicherung einzuschieben.

Als Beispiel die Befehle für die Eingabeaufforderung (die in Kapitel 9.4.2 ausführlich erläutert werden):

`xcopy c:\*.* z:\incr\*.* /s /m`

kopiert nur Dateien mit Archivbit, setzt danach das Archivbit zurück (inkrementelle Sicherung).

`xcopy c:\*.* z:\diff\*.* /s /a`

kopiert nur Dateien mit Archivbit, ändert dabei das Archivbit nicht (differenzielle Sicherung).

`c:\` ist das zu sichernde Laufwerk, `z:\` ist das Ziellaufwerk, `/s` heißt: Alle Unterordner kopieren.

## 5.2.3 Inkrementell oder differenziell – was ist vorzuziehen?

Das ist ganz klar die differenzielle Sicherung.

- Bei einer Wiederherstellung nach Totalverlust ist der Aufwand an Zeit und Nerven geringer.
- Wenn man eine einzelne verlorene Datei sucht, muss man nur auf zwei Medien nachsehen: Auf der Vollsicherung und der letzten Differenzsicherung.
- Man kann mit weniger Medien auskommen. Zwei abwechselnd verwendete DVD-RWs genügen. Wenn die Wiederherstellung älterer Revisionen von Dateien wichtig ist, nimmt man drei DVDs oder geht zur Drei-Generationen-Sicherung über (Erläuterung folgt).

Unter welchen Bedingungen ist eine inkrementelle Sicherung sinnvoll?

- Wenn die Änderungen seit der Vollsicherung nicht mehr auf einem einzelnen Medium untergebracht werden können.
- Jede differenzielle Sicherung dauert länger als die vorhergehende. Der Zeitaufwand für die Sicherung könnte allmählich unzumutbar werden.

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

- Wenn man viele Revisionen der Dateien gespeichert haben möchte.
- Wenn wenig Zeit für die Sicherung bleibt, z. B. weil das Computersystem möglichst schnell wieder einsatzbereit sein soll.

## 5.2.4 Inkrementell und differenziell gemischt verwendet

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

- Differenzielle Sicherung 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.

### Beispiel für private Nutzung

- Am Jahresende führen Sie eine Vollsicherung durch. Vermutlich hat nur eine externe Festplatte die dafür nötige Kapazität. Weil Datenträger durch lange Lagerung kaputt gehen können, sollten Sie jedes Jahr einen anderen Datenträger verwenden, aber mindestens zwei (oder drei) im Wechsel. Auf einer Festplatte sichern Sie die geraden Jahre, auf der anderen die ungeraden. Besser: die jährliche Vollsicherung auf beide Platten kopieren.
- Täglich, wöchentlich oder in anderen Abständen sichern Sie differenziell. Ein USB-Speicherstick ist wahrscheinlich optimal dafür geeignet. Nutzen Sie nicht die „Jahresfestplatten“ – ständige Benutzung ist auf Dauer nicht ohne Risiko.
- Am Monats- oder Quartalsende eine inkrementelle Sicherung, vielleicht auf DVD **und** sicherheitshalber ein Duplikat auf eine der Jahres-Festplatten? Weil dabei das Archivbit gelöscht wird, wird für die nachfolgenden differenziellen Sicherungen nur wenig Speicherplatz benötigt.

Planen Sie stets mit ein, dass sich im Katastrophenfall vielleicht eins der Backups nicht mehr lesen lässt. Ein defektes Jahres-Backup beispielsweise könnte man aus dem Vorjahres-Backup und dem Hinzufügen von zwölf Monats-Backups rekonstruieren.

### 5.2.5 Sicherung außer der Reihe

Wenn eine außerplanmäßige Vollsicherung gemacht werden soll, z. B. wegen einer geplanten Installation, kann man die Daten auf eine externe Festplatte kopieren. Das geht wesentlich schneller als eine Sicherung auf DVD. Dabei darf aber das Archivbit nicht verändert werden, sonst gerät die nächste reguläre Datensicherung durcheinander.

### 5.2.6 Andere Verfahren

Auf `https://www.oliver-fischer-it.de/reverse-incremental-backup/` wird ein Verfahren „Reverse Incremental Backup" beschrieben. Die Grundidee: Der Datenträger mit der letzten Vollsicherung wird täglich aktualisiert. Die älteren Dateien werden auf einen inkrementellen Tagesdatenträger ausgelagert, bevor sie mit dem neuesten Stand überschrieben werden. Dadurch braucht man im Katastrophenfall nur einen Datenträger mit der ständig aktualisierten Vollsicherung zurückzuspeichern und hat außerdem alle früheren Dateiversionen.

Mir gefällt diese Idee nicht. Erstens wird das wertvollste aller Medien (das mit der Vollsicherung) täglich allerlei Gefahren ausgesetzt (Beschädigung, Erpressungstrojaner, Verwechslung, ...), statt an sicherer Stelle gut verwahrt zu bleiben. Zweitens dauert das Backup länger: Jede geänderte Datei wird zweimal geschrieben (die aktuelle Datei wird auf die Vollsicherung kopiert und deren Vorgängerversion auf das inkrementelle Medium). Und es müssen zwei Datenträger eingelegt werden. Also täglicher doppelter Aufwand, um bei dem (hoffentlich) extrem seltenen Ereignis einer Rücksicherung etwas Zeit zu sparen?

Für Verfahren wie z. B. `https://www.datto.com/de/technologies/`**`inverse-chain-technology`** braucht man eine spezielle Software, die wegen ihres Preises wohl nur für große Firmen sinnvoll sein könnte.

### 5.2.7 Allgemeine Empfehlungen

- Notieren Sie, welche Sicherungen welcher Art wann auf welchen Datenträger gespeichert worden sind. Der sicherste Platz für diese Notizen ist auf Papier. Wenn Sie diese Notizen 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. Haben Sie neue Programme installiert? Haben Sie Ihre Daten anders geordnet?
- Testen Sie zumindest auszugsweise, ob die Daten auf dem Sicherungsmedium tatsächlich fehlerfrei lesbar sind.
- Vertrauen Sie Ihrer Datensicherung nie zu 100 %. Der freie Speicher auf dem Speichermedium könnte aufgebraucht sein, ohne dass Sie es bemerken. Die externe Festplatte könnte kaputt gehen, DVDs können sich als nicht lesbar herausstellen.

Viele Backup-Programme bieten die Möglichkeit, das Backup zu verschlüsseln. Überlegen Sie gut, ob eine Verschlüsselung wirklich notwendig ist. Wenn an einer unverschlüsselten Datei ein paar Bits defekt sind, kann die Datei meist noch genutzt und oft auch repariert werden. Ist eine Datei verschlüsselt, sind Rettungsversuche aussichtslos.

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 fallen aber morgen hühnereigroße Hagelkörner vom Himmel ...

Letztlich kann man eine Datensicherung wie eine Versicherung betrachten: Sie investieren jahrelang Zeit und Geld in die Datensicherung und hoffen dabei, 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.

# 5.3 Drei-Generationen-Sicherung

## 5.3.1 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 vielen 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. Das würde allerdings 365 Datenträger pro Jahr erfordern. Das ist natürlich nicht praktikabel, der Zeit- und Geldaufwand wäre irrsinnig. Wie kann man die Zahl der benötigten Datenträger reduzieren, ohne die Sicherheit wesentlich zu verringern?

## 5.3.2 Das Prinzip der Drei-Generationen-Sicherung

Ein 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 wenn heute die Bänder teilweise durch Festplatten ersetzt werden, bleibt das Prinzip erhalten. Jede Sicherung ist eine Vollsicherung.

- Für die erste Generation verwenden Sie so viele Bänder, wie die Woche Arbeitstage hat. Beschriften Sie diese mit „Montag“, „Dienstag“ usw. In jeder neuen Woche kommen diese Bänder am entsprechenden Tag erneut zum Einsatz.
- Der Freitag ist eine Ausnahme. Sie brauchen fünf Freitagsbänder (denn manche Monate haben fünf Freitage). Beschriften Sie diese mit „Freitag 1. Woche“ usw. und heben Sie diese einen Monat lang bis zum jeweils nächsten Freitag auf. Diese Bänder bilden die zweite Generation. Achten Sie darauf, dass am Freitag eine vollständige Sicherung erfolgt, an den anderen Wochentagen darf es auch eine inkrementelle oder differenzielle Sicherung sein.
- Von jedem Monatsanfang wird eine Sicherung drei Monate lang oder – besser noch – für ein Jahr aufbewahrt. Dafür brauchen Sie drei oder zwölf Bänder. Dies ist die dritte Generation.
- Vernünftigerweise bewahrt man das Jahresabschlussband zehn Jahre auf, das wäre die vierte Generation.

Insgesamt benötigen Sie 21 Bänder für das erste Jahr und eins für jedes Folgejahr, und hin und wieder müssen die verschlissenen Tagesbänder ersetzt werden.

## 5.3.3 Drei-Generationen-Sicherung mit optischen Medien

Privat kann man Bänder durch DVDs ersetzen und wahrscheinlich die tägliche Sicherung weglassen. Für die wöchentliche Sicherung verwenden Sie zweckmäßigerweise mehrfach beschreibbare DVDs oder USB-Sticks. Jedes Brennprogramm bietet einen Dateivergleich nach dem Brennen an. Nutzen Sie diese Funktion wenigstens hin und wieder, um unzuverlässige DVDs rechtzeitig aussondern zu können.

Für die Jahressicherungen sind hochwertige DVD-R mit UV-Schutz empfehlenswert. Wenn Ihr Brenner damit umgehen kann, sollten Sie zu DVD-RAM 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. Noch besser, wenn auch etwas teurer, sind die M-Disk, siehe Kapitel 6.3.4 über langlebige Medien.

Für die Monats-DVDs sollten Sie nicht zu den billigsten Scheiben greifen. Immerhin müssen diese Datenträger ein Jahr lang aufgehoben werden. Einmalbeschreibbare Scheiben sind vorzuziehen. Stellen Sie die geringen Preise für DVD-R (etwa 25 Cent) ins Verhältnis zum Aufwand, eine DVD-RW vor jedem Gebrauch löschen zu müssen. Für die Sicherheit und die Langzeitlagerung ist es ohnehin besser, alle jemals erstellten Monatssicherungen mehrere Jahre aufzubewahren. Die Jahressicherungen können dann entfallen.

Es ist ratsam, DVDs von verschiedenen DVD-Herstellern im Wechsel zu verwenden. So sind Sie selbst dann noch auf der sicheren Seite, wenn eine Charge einen versteckten Fehler hat und sämtliche Rohlinge 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 Lieblings-Brenner nicht mehr präzise justiert? Vielleicht produziert er seit Monaten DVDs, die außer von Ihrem Brenner von keinem anderen Gerät gelesen werden können? Sie sollten von Zeit zu Zeit mit einer Ihrer Sicherungs-DVDs ausprobieren, ob sie sich im Laufwerk eines anderen PC lesen lässt.

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

### 5.3.4 Drei-Generationen-Sicherung mit Festplatten

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 anstelle der Magnetbänder 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 die Änderungen automatisiert werden können, wird in den Kapiteln 10 „Anleitung für lokale Sicherung“ sowie 11.6 „Dokumente täglich automatisch sichern“ gezeigt.

### 5.3.5 Deduplizierung

Durch tägliche Vollsicherungen wird bald der Speicherplatz knapp. Für Firmen kann es sinnvoll sein, eine hohe dreistellige Summe für eine Deduplizierungssoftware wie z. B. „Acronis Deduplication“ auszugeben. Diese Software durchsucht das Backup nach identischen Dateien. Wenn beispielsweise der Chef ein Rundschreiben an alle Mitarbeiter schickt, wird es im Postfach jedes Mitarbeiters gespeichert. Solche und andere mehrfach vorhandene Dokumente werden durch Verweise auf das erste Vorkommen ersetzt und die Duplikate gelöscht. Es kann sogar nach identischen Teilen von Dokumenten gesucht werden. Der Briefkopf einer Firma beispielsweise kommt in vielen Dokumenten vor. Wenn das Programm die Sicherungen unterschiedlicher Tage vergleicht, findet es noch mehr Duplikate, weil sich aufeinanderfolgende Sicherungen meist nur in wenigen Dateien unterscheiden. Der Speicherbedarf für die Backups sinkt durch Deduplikation typischerweise auf fünf bis zehn Prozent. In „Windows Server“ ab der Version 2012 ist die Funktion der Deduplizierung bereits integriert.

### 5.3.6 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 schnellen Vergleich mit früheren Tagen ermöglicht, z. B. die Anzahl der gesicherten Dateien, die benötigte Zeit oder der benötigte Speicherplatz. Wenn die Datensicherung funktioniert, sollten diese Zahlen allmählich wachsen. Wenn nicht, suchen Sie nach der Ursache. Vielleicht hat jemand „groß aufgeräumt"? Oder die Daten in einen Bereich verschoben, der (bisher noch) nicht gesichert wird?

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, 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.

## 5.4 Image – Das Speicherabbild

### 5.4.1 Ein Speicherabbild – was ist das?

Ein Speicherabbild (engl. „Image") ist eine 1:1 Kopie einer oder mehrerer Partitionen der Festplatte. Ein Image enthält Informationen über das Dateisystem und die Struktur des Datenträgers, einschließlich Master Boot Record. Betriebssystem, Programme und Daten werden einschließlich ihrer Position auf der Festplatte gesichert. Kopiert man das Image auf eine Festplatte zurück, entsteht ein exaktes Abbild, Bit für Bit identisch mit dem Original. Welche Vorteile hat ein Image?

Bei der klassischen Datensicherung wird Datei für Datei gesichert. Wenn die Festplatte 10 000 Dateien in 555 Ordnern enthält, so hat auch die Kopie 10 000 Dateien in 555 Ordnern. Einer der Vorteile dieser klassischen Datensicherung ist, dass man eine verlorene Datei ganz leicht wiederfinden kann, da die Namen der Ordner und Dateien auf Original und Kopie übereinstimmen. Das Verfahren hat aber auch Nachteile:

- Das komplette Betriebssystem kann auf diese klassische Weise weder gesichert noch wiederhergestellt werden. Das hat mehrere 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 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 (Inhaltsverzeichnisse und Belegungstabellen) auf dem Ziellaufwerk geändert werden. Wenn viele kleine Dateien zu sichern sind, werden diese Verwaltungstabellen sehr umfangreich. Wenn die Verwaltungstabellen nicht mehr in den Arbeitsspeicher passen, müssen sie immer wieder auf Festplatte ausgelagert und erneut eingelesen werden. Der Zeitbedarf für das Kopieren geht drastisch in die Höhe, auf das Zehnfache oder mehr. Eventuell steht so viel Zeit nicht zur Verfügung.

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 von einem USB-Speicherstick gestartet. Das Image-Programm braucht also nicht installiert zu werden. Dadurch ist eine Sicherung selbst dann noch möglich, wenn das Betriebssystem defekt ist und nicht mehr hochfährt.

2. In manchen Fällen kann oder darf der PC nicht heruntergefahren werden. Ein Image bei laufendem Betrieb beherrschen nur wenige Programme. Es wird ein „Schattenkopie“ genanntes Verfahren genutzt, das nur mit den Professional-Versionen von Windows möglich ist. Mit Datenbanken funktioniert das mitunter nicht ohne Zukauf von Spezialmodulen. Bei der Entscheidung für ein Backup-Programm sollte man dessen 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 das Rücksichern) meist viel schneller als das Kopieren vieler Einzeldateien. Der größte Vorteil aber ist die Möglichkeit, ein funktionsfähiges Betriebssystem zu sichern, welches nach einer Rücksicherung sofort starten kann. Ohne ein solches Image müsste man zuerst das Betriebssystem samt Treibern installieren, dann das Backup-Programm, und nun erst könnte man die Daten wiederherstellen. Anschließend müssten noch Sicherheitsupdates und Anwendungen installiert werden. Das würde viele Stunden dauern, oft mehr als einen Tag.

Nach einem Datenverlust oder wenn man seine alte Festplatte gegen eine größere wechseln möchte, ist es sehr praktisch, vorher ein Image erstellt zu haben. Das Image wird auf die neue Festplatte ausgepackt, was typischerweise 15 bis 30 Minuten dauert. Anschließend ist das Betriebssystem einsatzfähig, ohne das irgendwelche Anpassungen vorgenommen werden müssen.

In der Standardeinstellung komprimiert das Image-Programm die Daten. In zwei Fällen kann es sinnvoll sein, die Komprimierung abzuschalten: wenn wegen einer leistungsschwachen CPU die Komprimierung zu lange dauert oder wenn die Daten bereits komprimiert sind. Bilder (.jpg), Audios (.mp3) und Videos (.avi, .mpeg u. a.) sind bereits hoch komprimiert und der Versuch, sie noch weiter zu komprimieren, dauert sehr lange und bringt häufig einen „Gewinn“ von weniger als einem Prozent. Eine „typische“ Systempartition schrumpft durch die Komprimierung etwa auf drei Viertel.

Ein Image-Programm sichert normalerweise nur die belegten Sektoren der Partition, doch es besteht die Möglichkeit eines „forensischen Backups“, bei dem auch die „leeren“ Bereiche der Partition gesichert werden. Wann ist das sinnvoll?

Ein Trojaner oder ein Saboteur könnte Dateien löschen, um seine Spuren zu verwischen. Wenn eine Datei gelöscht wird, markiert Windows deren Sektoren als ungenutzt und streicht den Dateinamen aus dem Dateiverzeichnis. Doch tatsächlich bleiben die Daten in den nunmehr freigegebenen Sektoren erhalten, bis sie vielleicht irgendwann von einer anderen Datei überschrieben werden. Diese Dateireste können mit Datenrettungsprogrammen wiederhergestellt werden. In Spezialfällen (z. B. zu Beweiszwecken oder vor einem Datenrettungsversuch) können die vermeintlich „gelöschten“ Sektoren in die Sicherung eingeschlossen werden. Die Image-Datei wird dadurch sehr groß, auch wenn beim Erstellen des Images die Komprimierung eingeschaltet ist.

Beim Erstellen eines Images können die Daten in Portionen gewünschter Größe aufgeteilt werden, zum Beispiel in Portionen von der Größe einer DVD (4,7 GB). Bei Bedarf können die einzelnen Dateien im Nachhinein von der Backup-Festplatte auf DVD kopiert werden.

Das Archiv kann mit einem Passwort geschützt werden.

Auf den meisten Notebooks und Komplettsystemen hat der Hersteller ein Image bereitgestellt. Es wird auf der Festplatte in einem versteckten Bereich bereitgehalten. Manchmal wird der Benutzer in den ersten Tagen nach dem Kauf aufgefordert, eine Imagedatei selbst zu erstellen und auf DVD zu brennen.

Das dazu benötigte Image-Programm wird entweder auf einer sogenannten „Recovery-CD“ mitgeliefert oder es ist im BIOS oder auf einer versteckten Partition enthalten und kann mit einer Tastenkombination gestartet werden. Achtung! Beim Recovery-Vorgang werden wahrscheinlich Ihre Daten gelöscht!

## 5.4.2 Für welche Sicherungen ist ein Image geeignet?

Bei der Sicherung kompletter Festplatten sind Geschwindigkeit, Komprimierung, Verschlüsselung und die Unabhängigkeit vom Zustand des Betriebssystems die großen Vorteile eines Image-Programms. Ihre größte Stärke spielen Image-Programme 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 nach den Änderungen der günstigste Zeitpunkt. Ein Image bringt Ihnen die folgenden Vorteile:

- Wenn die Installation fehlschlägt, können Sie einfach zum unbeschädigten Windows zurückkehren.
- Wenn Ihr System durch Schadsoftware oder eine Fehlbedienung beschädigt ist, kann es leicht auf eine frühere lauffähige Version zurückgesetzt werden.
- Sie haben eine Sicherung derjenigen Dateien, die von anderen Sicherungen möglicherweise nicht erfasst werden (Datenbanken oder ständig in Benutzung befindliche Dateien).

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, selbst bei Software von Testsiegern. Geradezu haarsträubend 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 jedoch die Festplatte auf klassische Weise Datei für Datei kopiert hat, verliert man bei einem zufälligen Fehler nur eine Datei, die man mit etwas Glück in einer etwas älteren Sicherung wiederfinden kann.

Für eine langfristige Archivierung Ihrer Daten ist ein Image aus einem weiteren Grund denkbar ungeeignet. Jeder Software-Hersteller speichert die Sicherung in einem eigenen, „proprietären“ Dateiformat. Wer weiß, ob Ihr Image-Programm unter der Windows-Version von 2020 noch lauffähig ist? Vielleicht gibt es bald keine Updates mehr, weil der Hersteller von der Konkurrenz aufgekauft wird? Die Festplattenhersteller haben die Datenstrukturen umgestellt. Neue Festplatten haben eine Sektorgröße von 4096 statt 512 Byte. Statt der uralten MBR-Partitionstabelle kommt weitgehend die neuere **G**UID **P**artition **T**able (GPT) zum Einsatz. Ob sich wohl ein älteres Image auf die neu strukturierten Festplatten zurücksichern lässt?

## 5.4.3 Vorsicht beim Rücksichern eines Images!

Windows startet nicht mehr oder ist von hartnäckigen Trojanern befallen? Sie wollen die Systempartition auf einen älteren, funktionierenden Zustand zurücksetzen? Beim Rücksichern müssen Sie sehr aufmerksam sein, um keinen Schaden anzurichten.

Beim Rücksichern einer Partition werden die aktuellen Daten der Partition **zuverlässig und endgültig** mit den alten Daten überschrieben. „Endgültig“ bedeutet, dass nicht mal die professionellen Datenretter helfen könnten. Haben Sie alle Ihre Dateien gesichert, die seit dem Tag der Erstellung des letzten Images geändert worden sind? Wenn Sie diesbezüglich nicht sicher sind oder nicht wissen, wo Ihre Daten sind, sollten Sie ein Backup oder ein Image des beschädigten Betriebssystems erstellen, bevor Sie das fehlerfreie ältere Image zurücksichern. Im Image des beschädigten Betriebssystems können Sie später alle Dateien finden, die Sie vielleicht noch brauchen.

Das Image-Programm ordnet den Partitionen mitunter andere Laufwerksbuchstaben zu als das Betriebssystem. Beispielsweise könnte Ihre Datenpartition, die Sie immer unter Laufwerk D: gefunden haben, nun unter Laufwerk C: zu finden sein, stattdessen hat das Betriebssystem den Buchstaben D: bekommen. Falls Sie nun eine solche Änderung übersehen und das Image des Betriebssystems nach C: zurücksichern, stellt es sich im Nachhinein heraus, dass Sie damit Ihre Daten vernichtet haben. Machen Sie sich deshalb die kleine Mühe und geben Sie jeder Partition schon bei ihrer Erstellung einen sinnvollen Namen. Verschaffen Sie sich vor dem Start des Image-Programms einen Überblick über Größe und Namen aller Partitionen mit einem Partitionsmanager oder mit dem Windows Explorer.

### Eine Sicherung teilweise zurückholen

Ein Image-Programm kann aus einem Image einzelne Dateien oder Verzeichnisse zurückzuholen. Sie können wählen, ob Sie diese an den ursprünglichen Speicherort zurückkopieren wollen oder Sie können ein anderes Zielverzeichnis wählen. Kopieren Sie möglichst nicht in das ursprüngliche Verzeichnis zurück! Wenn dabei etwas schiefgeht, wissen Sie nicht nur, dass Ihr Backup nichts getaugt hat, Sie haben auch eventuell vorhandene, noch intakte Dateien überschrieben.

## 5.4.4 Welche Image-Programme gibt es?

Etwa ein Dutzend Image-Programme haben eine nennenswerte Verbreitung. Acronis True Image, Paragon Drive Backup und Norton Ghost kosten jeweils 30 bis 50 Euro. Sie sind relativ übersichtlich und haben eine deutsche Bedienoberfläche. DriveImage XML, Partimage, Clonezilla, Partclone, Aomei Data Backupper und DiscWizard von Seagate sind kostenlos. Manchmal findet man zeitlich begrenzte Versionen der Bezahl-Programme im Internet und in Fachzeitschriften. Für die Sicherung bei laufendem Betrieb kann man Symantec Active System Recovery verwenden, das allerdings etwa 500 Euro kostet.

### Beispiel: Acronis True Image

Eins der besten Image-Programme ist Acronis True Image. Es gibt diverse Mietversionen für 50 Euro und mehr pro Jahr. Uns genügt eine „Dauerlizenz“, die für einen PC einmalig 30 Euro kostet, für drei PCs 50 Euro. Auf `www.acronis.de` können Sie eine 30-Tage-Testversion kostenlos herunterladen. Es lassen sich Partitionen, ganze Festplatten oder ausgewählte Ordner sichern, auch inkrementell. Aus einem Backup der Festplatte oder Partition kann man komplette einzelne Ordner oder Dateien zurückzusichern. Sie können Sicherungen automatisch nach einem Zeitplan durchführen lassen. Von Jahr zu Jahr fügt Acronis neue Funktionen hinzu. In der Premium-Edition (jährlich 125 Euro) sind 1TB Speicher in der Acronis Cloud inbegriffen.

Sofern Sie True Image nur zum Erstellen von Images und zum Klonen nutzen wollen, sollten Sie das Programm von DVD booten. Eine Installation von True Image brauchen Sie nur, wenn Sie die Backup-Funktion nutzen wollen. Dann können Sie die Bedienersprache auf Deutsch umstellen, und Sie können aus einem Image einzelne Dateien und Ordner extrahieren, ohne das ganze Image auspacken zu müssen.

Beachten Sie: Die nachfolgenden und weitere Anleitungen können Sie ausführlicher und aktueller auf `https://www.eifert.net` unter „Hilfen“ → „Datensicherung“ finden.

### Anleitung: Image erstellen mit Acronis True Image

Booten Sie von der Acronis-DVD. In einem Auswahlmenü können Sie wählen:

1: Acronis True Image

2: Acronis System Report

c: Continue booting

Je nachdem ob Sie im UEFI- oder im Legacy-Modus gebootet haben, müssen Sie die „1“ drücken oder auf den ersten Menüpunkt klicken, um ins Hauptmenü („Home“) zu kommen.

What would you like to do? (Was wollen Sie tun)? Im Abschnitt „Back Up“ stehen „My Disks“ oder „Files & Folders“ zur Wahl.

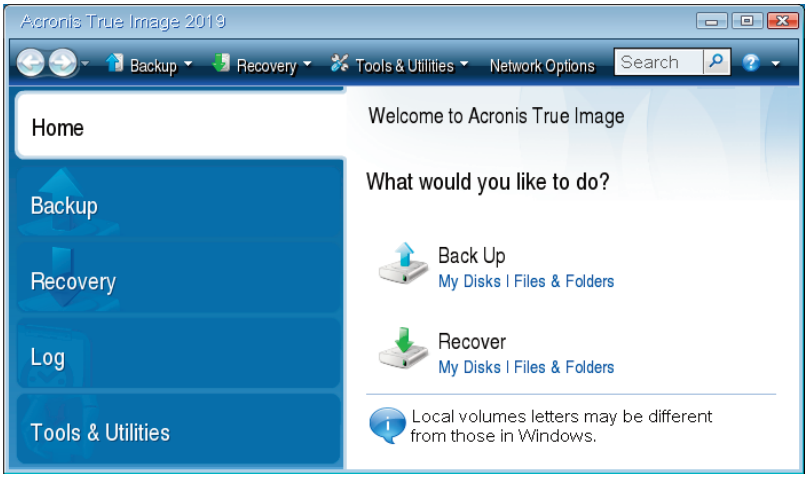


Bild 5.3: Acronis True Image Hauptmenü

Mit letzterem können Sie einzelne Ordner und Dateien sichern – das würde mit dem Explorer oder mit ROBOCOPY besser gehen. Wählen Sie „My Disks“, um komplette Partitionen zu sichern.

Nachdem Sie „My Disks“ gewählt haben, werden in der rechten Fensterhälfte die Partitionen der Festplatten gezeigt (Bild 5.4). Wenn mehrere Festplatten im PC stecken, muss vermutlich „Festplatte 1“ als die zu sichernde Festplatte ausgewählt werden. Beachten Sie die Warnung „Local volume letters may be different from those in Windows“ (Die Laufwerksbuchstaben können andere sein als unter Windows) in Bild 5.3. Orientieren Sie sich keinesfalls an den Laufwerksbuchstaben, sondern an Größe und Bezeichnung (Label) der Partitionen. Wählen Sie die zu sichernden Partitionen aus. Setzen Sie einen Haken vor Partition C:. Sie muss mit „Primär“ gekennzeichnet sein. Wenn eine kleine Startpartition von etwa 100 MB dabei ist, die als „Primär, Active“ oder „System-reserviert“ gekennzeichnet ist, enthält diese den Bootmanager. Diese kleine Partition sollte auf jeden Fall ein Teil von jeder Sicherung werden. „Size to back up“ nennt den für die ausgewählten Partitionen maximal notwendigen (unkomprimierten) Speicherplatz.

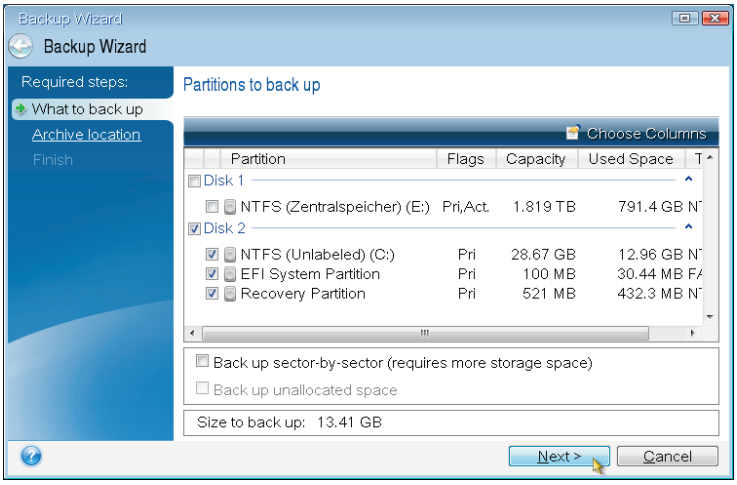


Bild 5.4: Image: Auswahl Quelle

Bei „Back up sector-by-sector (requires more storage space)“ sowie „Back up unallocated space“ keinen Haken setzen. Jeden Sektor (einschließlich die vom Betriebssystem gelöschten und die nie benutzten Sektoren) zu speichern ist nicht nötig, außer bei forensischen Untersuchungen und vor dem Versuch einer Datenrettung. Klicken Sie auf „Next“.

Im Fenster „Target backup archive“ (Bild 5.5) ist „Create new backup archive“ (neues Backup erstellen) vorgewählt. Sie könnten auch „Add to existing backup archive“ (ein vorhandenes Archiv auf den neuesten Stand bringen) wählen. Das kann sinnvoll sein, wenn Sie auf dem Sicherungsmedium nicht genug Platz haben für ein neues komplettes Image.

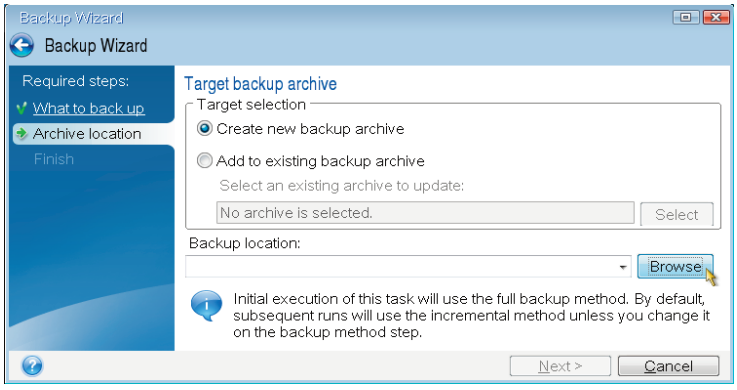


Bild 5.5: Neues Backup oder vorhandenes Image updaten

Klicken Sie auf „Browse“ (Durchsuchen), um ein Laufwerk und einen Ordner auszuwählen, wohin das Backup gespeichert werden soll.

Im Bild 5.6 wählen Sie ein Laufwerk mit einer Partition mit genügend freiem Platz. Sie können auch die externe Festplatte oder den DVD-Brenner auswählen.

Legen Sie dann den „Filename“ fest: Entweder Sie klicken auf „Generate name“ und bekommen den Namen „MeinBackup“ vorgeschlagen, oder Sie tippen einen frei gewählten Dateinamen in das Feld. Die Dateierweiterung `.tib` wird automatisch erstellt.

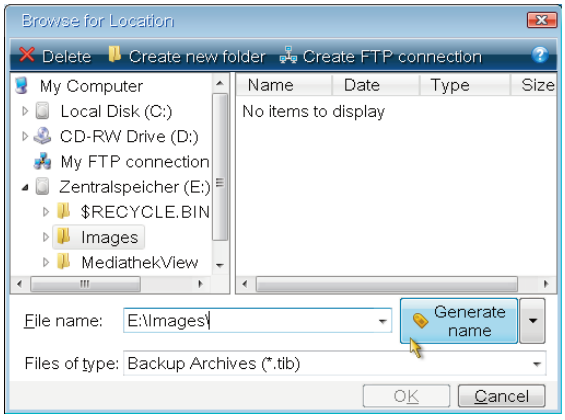


Bild 5.6: Ordner für Image auswählen

Empfehlung: Beginnen Sie den Namen mit „Datum-Computername“, z. B. `2020-09-28-Notebook` oder mit „Computername-Datum“. Beim Datum ist die Reihenfolge `jjjj-mm-tt` zu empfehlen, weil dann die Sicherungen auf dem Backup-Medium chronologisch sortiert angezeigt werden. Dann „OK“.

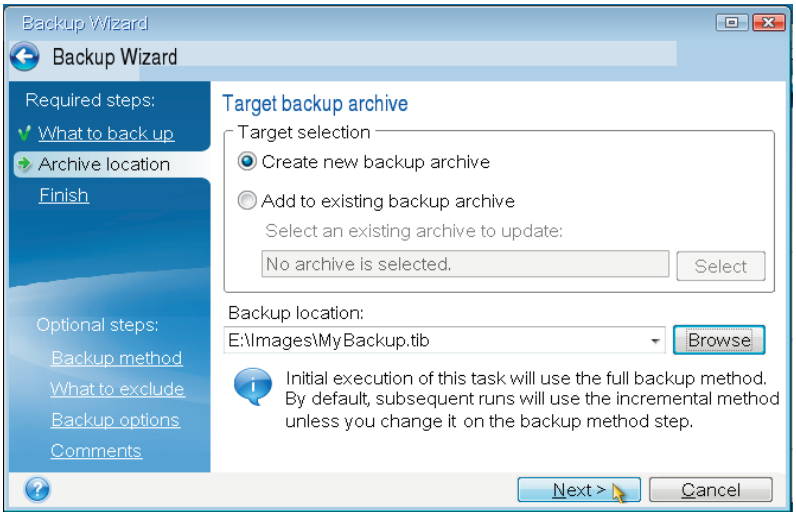


Bild 5.7: Image: Neu oder nur Update eines älteren Images

Nach „Next“ wird eine Zusammenfassung (Summary) wie in Bild 5.8 angezeigt. Klicken Sie nach einer sorgfältigen Überprüfung auf „Proceed“ (Ausführen).

Im Fenster „Operating Progress“ (Bild 5.9) wird der Fortschritt und die geschätzte Restzeit („Time left“) angezeigt. In der ersten Minute ist die geschätzte Zeit sehr hoch, danach wird die Schätzung einigermaßen realistisch (mit einer optimistischen Tendenz). Die Sicherung dauert meist 10 bis 30 Minuten, selten mehr als eine Stunde. Auf jeden Fall sollten Sie die Restzeit-Prognose im Auge behalten.

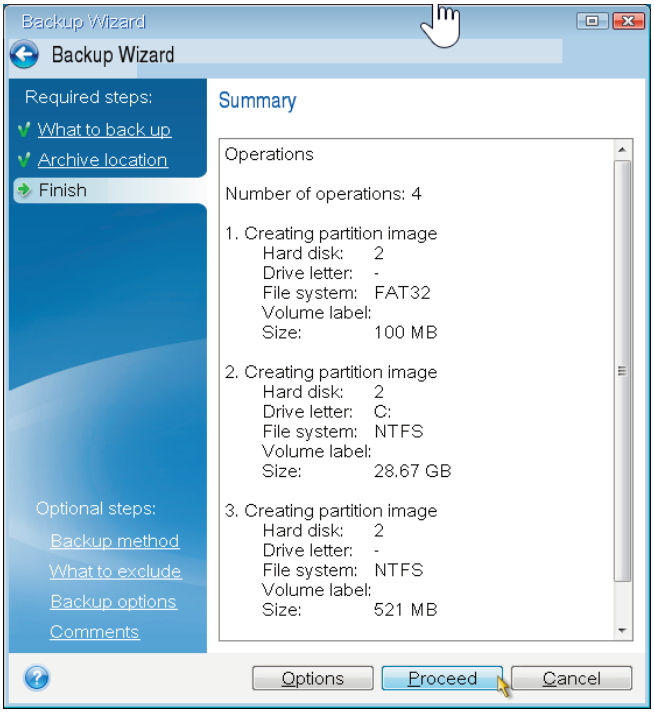


Bild 5.8: Zusammenfassung der Planung

Tipp: Beobachten Sie den Verlauf. Wenn sich die prognostizierte Restdauer plötzlich verdoppelt, ist Acronis auf einen Bereich der Festplatte gestoßen, wo für zahlreiche Sektoren vielfache Leseversuche nötig waren. Acronis nimmt nun an, dass auch der Rest der Festplatte so problematisch ist. Wenn nicht, geht die Zeitprognose langsam wieder nach unten – bis zum nächsten geschwächten Bereich.

Ein kleiner Teil der Schwankungen hängt davon ab, ob gerade große oder viele kleine Dateien kopiert werden. Bei einer älteren Festplatte, besonders bei Notebooks, sind kleinere Schwankungen normal. Wenn Acronis gerade große Dateien kopiert, werden mehr Byte pro Sekunde kopiert als bei vielen kleinen Dateien. Doch wenn sich Prognosezeiten verdreifachen, vielleicht gar mehrmals, sollten Sie über den Kauf einer neuen Festplatte oder zumindest über eine regelmäßigere Datensicherung nachdenken.

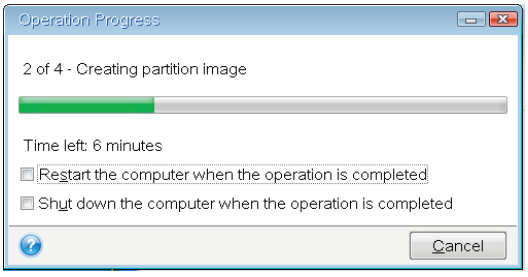


Bild 5.9: Fortschrittsanzeige und Zeitprognose

Wundern Sie sich nicht, wenn gegen Ende des Kopiervorganges die Restzeitschätzung ständig zu kurz ist. Das hängt mit den mechanischen Eigenschaften der Festplatte zusammen: Je weiter der Magnetkopf nach innen wandert, desto kleiner wird die Länge der Spuren und damit die Datenmenge pro Spur und desto weniger Daten werden pro Umdrehung gelesen bzw. geschrieben.

Auf meiner Webseite `https://eifert.net` unter „Hilfen“ → „Datensicherung“ ist die Beschreibung noch ausführlicher.

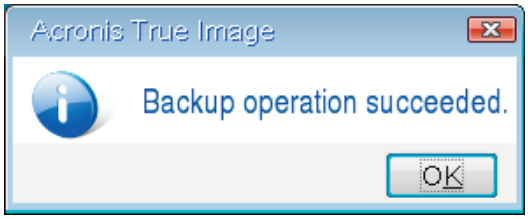

Bild 5.10: Erfolgsmeldung

### Festplatte duplizieren

Ein Hinweis: Unter dem Menüpunkt „Tools & Utilities“ finden Sie „Clone Disk“. Damit können Sie eine komplette Festplatte auf eine neue, größere Festplatte zu kopieren und dabei neue Partitionsgrößen festlegen. Am Ende dieses Kapitels (5.6 Festplatte klonen mit Acronis True Image“) ist das genauer beschrieben.

## 5.4.5 Die Grenzen von Image-Programmen

Sie haben einen neuen PC gekauft. Sie haben das Image vom alten PC auf den neuen PC zurückgesichert bzw. die Festplatte geklont, doch auf dem neuen PC startet Windows nicht. Warum?

Während der Neuinstallation von Windows verwendet das Betriebssystem eigene, universelle Treiber, die mit jedem Chipsatz zurechtkommen. Allerdings nutzen diese Treiber die Leistungsfähigkeit moderner Chipsätze nur zu einem geringen Teil. Deshalb werden bei einer Treiberinstallation die Festplatten-Universaltreiber durch Treiber ersetzt, die für den verwendeten Chipsatz optimiert sind und mit jedem anderen Chipsatz (dem von der neuen Hauptplatine) nicht funktionieren.

Wenn die Hauptplatine des neuen PC einen anderen Chipsatz als der alte PC hat (was zu 99 % sicher ist), sehen Sie beim Hochfahren eine Fehlermeldung (meist einen Blue Screen). Das gleiche Problem haben Sie, wenn die Hauptplatine defekt ist und gegen eine neuere ausgewechselt werden musste. Sie müssten also die alten Festplattentreiber gegen die zur neuen Hauptplatine passenden auswechseln. Zur Treiberinstallation müsste sich Windows aber starten lassen. Wenn aber Windows abstürzt, noch bevor Sie auf die Festplatte zugreifen konnten? Dann haben Sie ein Problem.

Es gibt drei Möglichkeiten in dieser Situation:

- Erstellen Sie eine „Acronis Universal Restore“ DVD und nehmen Sie damit die Rücksicherung auf eine andere Hardware vor. Der Erfolg hängt davon ab, wie stark sich die neue Hardware von der alten unterscheidet. Nach meinen Erfahrungen klappt das etwa bei zwei Drittel der Hardware-Paarungen.
- Wenn Ihr alter PC noch funktioniert, können Sie versuchen, den Festplattentreiber zu entfernen und durch den Windows-Standardtreiber zu ersetzen. Das ist nicht einfach und eventuell verlieren Sie dadurch den Zugriff auf Ihre Festplatte. Wenn es gelingt, können Sie ein neues Image erstellen und es auf dem neuen PC ausprobieren.
- Wenn Ihr alter PC noch funktioniert, stellen Sie fest, ob beide PCs einen PCI- oder PCI-Express-Steckplatz gemeinsam haben. Besorgen Sie eine PCI- bzw. PCIe-Karte mit Festplattenanschluss.
    - Bauen Sie diese Erweiterungskarte in den alten PC ein und installieren Sie die zugehörigen Treiber.
    - Schließen Sie nun die Festplatte mit dem Betriebssystem des alten PC an diese Karte an und testen Sie, ob der PC ganz normal hochfährt.
    - Bestücken Sie die nun die neue Hauptplatine bzw. den neuen PC mit der zusätzlichen Steckkarte.
    - Stecken Sie die Festplatte vom alten PC zunächst an den Anschluss der zusätzlichen Karte.
    - Starten Sie Windows. Da die Treiber der Erweiterungskarte bereits installiert sind, sollte es keine Probleme geben.
    - Installieren Sie nun die Treiber für den Chipsatz der neuen Hauptplatine / des neuen PC.
    - Nun können Sie die Festplatte von der zusätzlichen Steckkarte an den Anschluss der Hauptplatine umstecken. Die Zusatzkarte wird nicht mehr benötigt und kann ausgebaut werden.
    - Bei Bedarf können Sie noch die Festplatte auf eine größere kopieren.

Beachten Sie die ausführlichere Anleitung im Buch „Computerhardware für Fortgeschrittene“ und auf `eifert.net` unter „Hilfen“ → „Hardware“ → „Hauptplatine auswechseln“.

Wenn all das nicht geht, bleibt Ihnen nur noch, die Betriebssystempartition zu löschen und Windows neu zu installieren. Anschließend installieren Sie alle Treiber und alle Ihre Anwendungen erneut. Kopieren Sie die Daten vom Backup zurück und verknüpfen Sie diese mit den Anwendungen.

### 5.4.6 Ein einziges defektes Bit kann Ihr Backup vernichten

Bei allen Vorteilen ist ein Image eine riskante Art der Datensicherung. In einer einzigen großen Datei werden tausende kleine Dateien zusammengefasst. Wenn ein Teil der Datei nicht mehr oder nicht richtig gelesen werden kann, bekommen Sie die Meldung „Die Image-Datei ist beschädigt“ und es ist sehr wahrscheinlich, dass auch professionelle Datenretter scheitern werden.

Auf jeder Festplatte gibt es einige Stellen, die ein geschwächtes Lesesignal liefern. Bei der Herstellung gibt es Unterschiede in der Beschichtung mit dem Magnetmaterial. Dazu kommt die Abnutzung, z. B. durch leichte Kopfaufsetzer. Selbst bei fabrikneuen Festplatten wird eins von tausend Bits falsch gelesen. Die interne Fehlerkorrektur kann fast alle Fehler korrigieren. Hersteller Seagate gibt für Standardfestplatten eine verbleibende Fehlerhäufigkeit von 1 Bit pro $10^{14}$ an. Das entspricht einem Fehler in 24 Stunden, wenn die Festplatte ununterbrochen Daten liest. Die meisten Fehler sind zwar temporär, doch einige sind hartnäckig. Wenn von den zehntausenden einzelnen Dateien einer Windows-Partition eine nicht lesbar ist, ist das meist nicht schlimm: Falls Windows diese Datei vermisst, kann sie meist durch den **S**ystem**F**ile**C**heck repariert werden (mit `sfc /scannow` an der Eingabeaufforderung). Doch sobald das Image-Programm einen nicht lesbaren Sektor in der Image-Datei findet, bricht es ab und damit sind alle im Image gespeicherten Dateien gleichzeitig unbrauchbar.

Das gleiche Problem haben alle Programme, mit denen viele Dateien zu einer Datei zusammengefasst werden: Winzip und ähnliche, TrueCrypt und VeraCrypt. Generell steigt das Risiko, wenn Dateien komprimiert werden. Der Vorteil der Speicherplatzeinsparung wird durch höheres Risiko erkauft.

Das Risiko von Datenverlusten können Sie mit jeder Art von Verschlüsselung noch weiter steigern.

## 5.5 Recovery

Liegt Ihrem PC eine Systemwiederherstellungs-DVD, engl. Recovery-DVD oder Recovery-Disc bei? Mit einer funktionierenden Recovery-CD sind Sie alle Sorgen los – und Ihre Daten möglicherweise auch.

Der Hersteller hat den Auslieferungszustand des PC in einer komprimierten Datei, einem „Image“, auf der Recovery-DVD und / oder in einer versteckten Partition auf der Festplatte gespeichert. Damit lässt sich der Zustand des PC beim Kauf wiederherstellen – allerdings ohne Ihre Daten. Einige Recovery-Programme warnen Sie vor dem bevorstehenden Datenverlust, manche bieten Ihnen sogar die Auswahl, ob Sie Ihre Daten behalten wollen oder nicht. Aber auch bei der Auswahl „Daten behalten“ werden meist nur die Daten in den Ordnern „Eigene Dateien“ geschützt. Ordner an anderen Orten werden möglicherweise gelöscht. Manche Hersteller legen Ihre Daten in einer komprimierten Datei ab und Sie müssen erst die Anleitung suchen, wie Sie nach der Neuinstallation Ihre Daten auspacken können.

Es ist sogar bei einzelnen Notebook-Modellen passiert, dass alle Partitionen der Festplatte gelöscht wurden, um die ursprüngliche Partitionierung wiederherzustellen. So wie gekauft – ohne Kompromisse.

Es ist also auf jeden Fall ratsam, alle bzw. wenigstens die wichtigsten Daten auf ein externes Medium zu sichern. Wenn Ihre Festplatte geteilt ist, werden möglicherweise auch die Daten auf D: und weiteren Partitionen gelöscht.

Nachdem Sie Ihre Daten gesichert haben, können Sie die Wiederherstellung starten.

### Windows 8 und 10

Wenn Sie zu Beginn des Startvorgangs die Taste F8 drücken, finden Sie unter „Computerreparaturoptionen“ das **Win**dows **R**ecovery **E**nvironment (WinRE). Falls Windows nicht mehr startet, kann man alternativ von der Windows Installations-DVD starten. Nachdem Sie die Installationssprache bestätigt haben, finden Sie im nächsten Fenster die „Computerreparaturoptionen“ mit den Recovery-Optionen.

Das Recovery Environment bietet zwei Möglichkeiten:

- Beim „Originaleinstellung wiederherstellen“ kann man wählen, ob nur die Systempartition oder alle Partitionen gelöscht werden sollen. Anschließend hat man ein neu installiertes Windows.
- Beim „PC auffrischen“ erfolgt keine Neuinstallation. Es werden „nur“ die Systemdateien ersetzt, wobei die installierten Apps und Ihre Daten erhalten bleiben. Sie benötigen dafür einen Windows-8-Installationsdatenträger sowie das Passwort eines Benutzers mit Administratorrechten.

Nur noch wenige Notebooks und PCs werden mit einer Installations-DVD oder Recovery-DVD ausgeliefert. Doch mit Windows 8 und 10 kann man einen Minimal-Ersatz selbst erstellen. Geben Sie an der Eingabeaufforderung den Befehl „recoverydrive.exe“ ein. Stecken Sie einen 8 GB großen USB-Speicherstick ein (Achtung! Wird gelöscht!). Mit diesem Stick können Sie später, wenn es notwendig wird, Windows reparieren oder den Neuzustand wiederherstellen. Mehr finden Sie auf `eifert.net` unter Hilfen → Datensicherung.

## 5.6 Festplatte klonen mit Acronis True Image

Booten Sie von der Acronis-DVD. Im Hauptmenü (Bild 5.3) wählen Sie „Tools & Utilities“ (Extras und Werkzeuge) → „Clone Disk“ (Laufwerk klonen), siehe Bild 5.12.

Nach einer Wartezeit müssen Sie zwischen automatischem oder manuellem Modus wählen. Weil ich keinem Programm blind vertraue, bevorzuge ich den manuellen Modus: Wenn sich die Automatik irrt, könnte der „Inhalt“ der leeren Festplatte auf die volle Platte kopiert werden. Lieber wähle ich Quell- und Ziellaufwerk selbst aus.

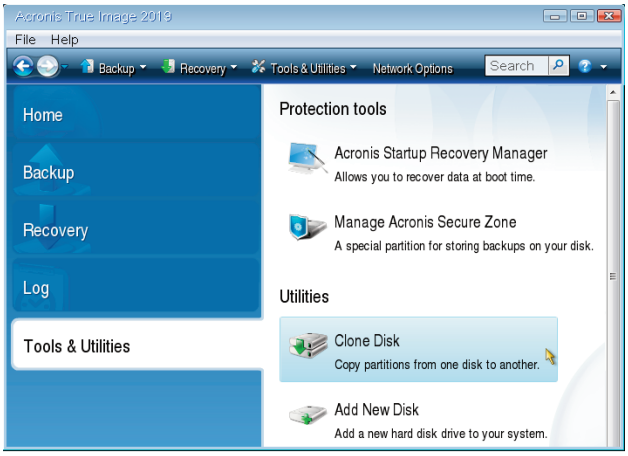

Bild 5.12: Menü Klonen

Bild 5.13 zeigt das Auswahlfenster für das Quelllaufwerk (source hard disk).

Damit Ihnen kein Fehler unterläuft, haben Sie zwei Hilfen: Am unteren Rand wird die aktuelle Belegung der ausgewählten Festplatte angezeigt. Und wenn Sie mit der rechten Maustaste auf ein Laufwerk klicken und dann auf „Disk properties“, sehen Sie genaue Angaben zum Laufwerk, bis zur Kopf- und Zylinderanzahl.

Nach „Next“ und einer Wartezeit, die einige Minuten betragen kann, wählen Sie das Ziellaufwerk (target hard disk), siehe Bild 5.14. Die aktuelle Belegung des Ziels wird auch hier angezeigt.

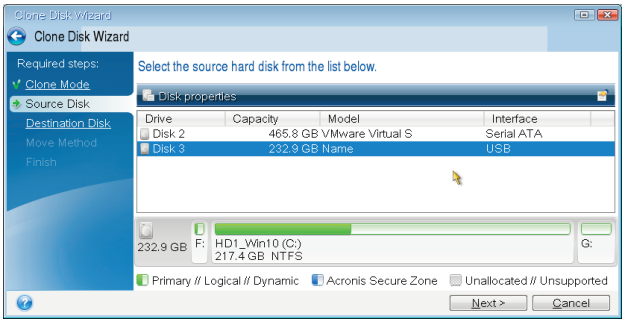

Bild 5.13: Klonen: Auswahl Quelle

Nach „Next“ wird Ihnen möglicherweise eine Warnung wie in Bild 5.15 angezeigt: Immer dann, wenn es auf der Ziel-Festplatte bereits Partitionen gibt. Bestätigen Sie mit „OK“.

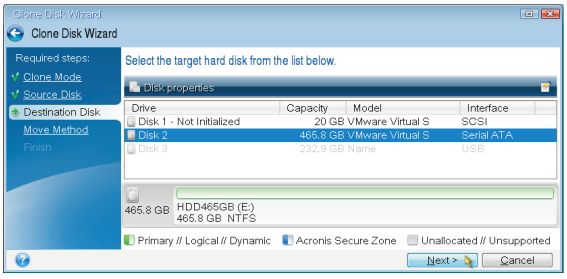


Bild 5.14: Klonen: Auswahl Ziel

Als nächstes (Bild 5.16) können Sie wählen:

- „As is“ (identisch kopieren) bedeutet, dass die Partitionsgröße beim Kopieren nicht verändert wird. Auf der neuen, größeren Platte bleibt der Teil ungenutzt, der die Kapazität der alten Festplatte übersteigt.
- „proportional anpassen“ ist meist die bessere Option. Alle Partitionen werden um den gleichen Faktor vergrößert, damit die Kapazität der Festplatte voll genutzt wird.
- „manuell“ ist etwas aufwändig, aber erlaubt Ihnen, für jede Partition die optimale neue Größe einzustellen.

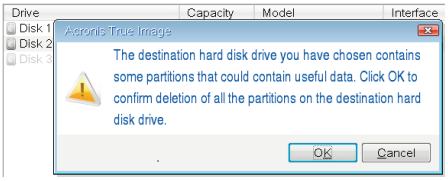


Bild 5.15: Klonen: Warnung

Auf Bild 5.17 wird zur Kontrolle die Belegung der Ziel-Festplatte vor und nach dem Kopieren gezeigt. Wenn alles richtig ist, klicken Sie auf „Proceed“ (Ausführen).

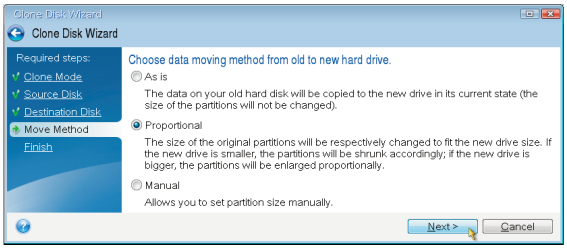


Bild 5.16: Anpassung der Partitionsgrößen

Wenn die Quell-Festplatte eine MBR-Partitionstabelle hat und die Ziel-Festplatte größer als 2047 GB ist, wird Acronis das Partitionsschema in GPT (**G**UID **P**artition **T**able) umwandeln. Bei kleineren Ziel-Festplatten bleiben die MBR-Partitionen erhalten („`disk´s layout will remain MBR`“) oder auch nicht – ich konnte noch keine Gesetzmäßigkeit finden, wann eine Umwandlung erfolgt und wann nicht.

Beachten Sie, dass der PC ein UEFI-BIOS haben muss, um große Festplatten verwalten zu können. Mehr dazu siehe Kapitel 7.

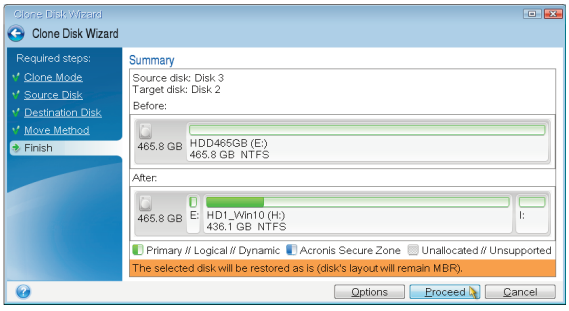


Bild 5.17: Vorschau der Planung

Bild 5.18 zeigt den Fortschritt und die Restzeitprognose. Wenn Ihr Computer weniger als 5000 Euro gekostet hat, sollten Sie die geschätzte Restzeit vervierfachen, um eine realistische Wartezeit zu erhalten.

Sie können wählen, ob der Computer zum Abschluss heruntergefahren (shut down) oder neu gestartet werden soll. Ich empfehle, den Computer erst dann neu zu starten, wenn eine der beiden Festplatten entfernt ist. Wenn Windows beim Start zusätzliche Partitionen findet und die alten Partitionen unter anderen Laufwerksbuchstaben einsortiert werden, könnte Windows beschädigt werden.

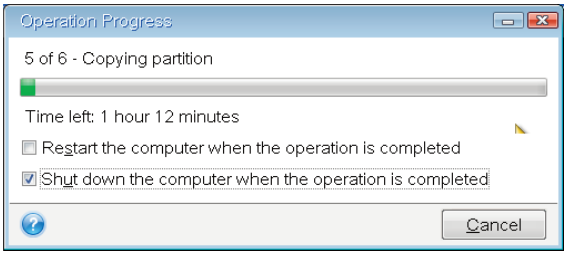


Bild 5.18: Fortschrittsabzeige

Wenn Acronis in Bild 5.13 die neue Festplatte nicht findet, muss sie möglicherweise „initialisiert“ werden. Falls das nicht automatisch geschieht, gehen Sie im Acronis-Hauptmenü auf „Tools & Utilities“ (Extras und Werkzeuge) → „Add new drive“ (Neues Laufwerk hinzufügen). Markieren Sie die neue Festplatte, „Weiter“.

Eine wesentlich ausführlichere Anleitung finden Sie auf `eifert.net` unter Hilfen → Datensicherung.