

1 Einführung

Haben Sie schon einmal Ihre Daten verloren? Nein, BISHER noch nicht?

Ein kurzer Stromausfall, ein Wackelkontakt oder Verschleiß durch Alterung können Ihre Daten zerstören. Eine Verwechslung beim Aufräumen der Festplatte, eine Fehlbedienung oder einfach nur ein Klick auf das falsche Symbol, schon können Ihre Daten weg sein. Ein Virus könnte Ihre Festplatte löschen oder die Daten unwiderruflich verschlüsseln. Einige der neuesten Notebook-Festplatten löschen sich selbst, wenn die Elektronik „glaubt“, das Notebook wäre gestohlen worden. Es gibt so viele Risiken ... Was tun Sie dagegen?

An der Umfrage einer Computerzeitschrift hatten 6149 Leser aus 128 Ländern teilgenommen. Das Ergebnis:

- 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).

(siehe <http://www.consumerstatistics.org/global-data-backup-survey-results/>)

Nicht nur die 45 % der Datensicherungs-Abstinenzler, sondern auch ein großer Teil der langjährigen Computernutzer sind Anfänger, soweit es die Datensicherung betrifft.

Der Gedanke an einen möglichen Datenverlust wird ebenso verdrängt wie der Gedanke an einen möglichen Autounfall. Vor einem Autounfall kann man sich – zumindest teilweise – durch umsichtiges Verhalten schützen, vor dem finanziellen Schaden schützen Haftpflicht- und Kaskoversicherung. Auch beim Computer kann ein umsichtiges Verhalten und technisches Wissen die Zahl der „Unfälle“ verringern, doch es gibt keine Versicherung, die Sie vor Datenverlusten schützt. Sie haben noch Garantie auf Ihren neuen PC? Wenn die Festplatte defekt ist, bekommen Sie diese vielleicht ersetzt, doch Ansprüche wegen Datenverlusten sind immer ausgeschlossen. Es gibt keinen anderen Weg, als regelmäßig selbst aktiv zu werden. Mit einfachen Mitteln eine regelmäßige Datensicherung zu organisieren, ist weder teuer noch allzu schwierig. Wie das geht, können Sie aus diesem Buch lernen.

Im geschäftlichen Umfeld wird die Datensicherung ernster genommen. Eine Umfrage des Speicherherstellers Buffalo unter Systemadministratoren vom Jahr 2013 hat ergeben, dass 9 % der Firmen stündlich oder öfter die Daten sichern, 68 % täglich und 14 % wöchentlich. Nur 9 % sichern ihre Daten unregelmäßig oder seltener als wöchentlich. Für den Fall eines Datenverlusts befürchten 78 % der Verantwortlichen erhebliche finanzielle Schäden und 69 % befürchten den Verlust von Aufträgen. Laut einer Umfrage von Acronis hatten 31 % der befragten Firmen im Jahr 2018 Ausfallzeiten wegen Datenverlust. Immerhin sichern 86 % der Firmen ihre Daten regelmäßig, davon 26 % täglich, 25 % wöchentlich und 35 % zumindest monatlich.

Dieses Umfrageergebnis betrifft Firmen, die groß genug sind, einen EDV-Fachmann beschäftigen zu können. In den vielen kleinen Betrieben, in denen sich der Chef nebenbei um die EDV kümmert, sieht es schlimmer aus. Und bei den Handwerkern und bei den Selbständigen? Was sie für eine Datensicherung halten, liegt meist viele Monate zurück. Das jedenfalls gestehen sie, wenn sie ihren kaputten PC oder ihr kaputtes Windows zur Reparatur bringen. Und öfters stellt sich heraus, dass unter den gesicherten Daten ausge-rechnet die wichtigsten fehlen. Oder dass statt der Daten nur die Links zu den Daten gesichert worden sind.

Hier ist noch eine interessante Frage. Stellen Sie sich vor, Ihre Wohnung brennt, und Sie können auf der Flucht nur einen einzigen Gegenstand mitnehmen. Der Antivirenspezialist Kaspersky hat deutsche Nutzer gefragt. Immerhin 27 % der Befragten hätten ihr Notebook, Tablet-PC oder Smartphone gerettet, nachzulesen unter <http://www.kaspersky.com/de/news?id=207566626>.

1.1 FACHBEGRIFFE

Die englischen Begriffe „Safety“ und „Security“ werden beide als „**Sicherheit**“ ins Deutsche übersetzt, obwohl sie sehr unterschiedliche Bedeutungen haben. In der Computer-**Security** geht es um den Schutz vor absichtlichen Störungen. Dazu gehören unter anderem Viren, Trojaner, Sabotage, Ausforschung und Datendiebstahl. Dieses Thema wird in meinem Buch „Sicherheit im Internet“ behandelt. Bei „**Safety**“ geht es um den Schutz vor zufälligen Schäden: Übertragungsfehler, defekte Festplatten oder DVDs, falsche Bedienung und versehentliches Löschen, Stromausfälle und Blitzschläge. Da es in diesem Buch nur um „Safety“ geht, wird „Sicherheit“ nur in diesem Sinne gebraucht.

Wenn man sicherheitshalber eine Kopie seiner Daten anfertigt, trägt der Vorgang des Kopierens den Namen **Datensicherung**, englisch **Backup**. Mit einer Datensicherung werden Kopien erzeugt, mit denen nach einem Datenverlust ein früherer Zustand wiederhergestellt werden kann. Umgangssprachlich wird mitunter auch der Datenträger mit den kopierten Daten als Datensicherung bezeichnet. **Sicherungskopie** oder **Sicherheitskopie** wäre die bessere Bezeichnung dafür.

Datensicherung ist der Oberbegriff für mehrere Verfahren. Die verbreitetsten sind:

- Eine Sicherung „Datei für Datei“ wird im Kapitel 9.4 „Kopierprogramme“ erläutert. Dafür wird der Windows-Explorer genutzt oder einer der Kommandozeilenbefehle `COPY`, `XCOPY` oder `ROBOCOPY`. Vorteil: Verlorene gegangene Dateien oder Ordner sind leicht zu reparieren.
- Das Erstellen eines komprimierten Festplattenabbilds, genannt **Image**, wird in Kapitel 5.4 „Image – das Speicherabbild“ vorgestellt. Vorteil: die Vollständigkeit bei trotzdem geringem Speicherbedarf.
- Wie man eine Bit für Bit identische Kopie der aktiven Festplatte auf einer zweiten Festplatte erstellt (einen **Klon**), lesen Sie in Kapitel 5.6 „Festplatte klonen mit True Image“. Von einer alternden Festplatte können Sie in kurzer Zeit eine funktionierende Kopie erstellen. Allerdings brauchen Sie für jeden Klon eine separate Festplatte.

Der Vorgang der **Rücksicherung** wird englisch als **Restore** bezeichnet. Von dem zur Sicherung verwendeten Verfahren hängt es ab, wie die Rücksicherung durchzuführen ist.

Eine Datensicherung sollte regelmäßig und ausreichend häufig erfolgen. Wenn man eine neue Sicherungskopie erstellt hat, sollte man frühere Kopien nicht übereilt wegwerfen oder überschreiben. Warum? Wenn eine Datei auf der letzten Sicherung nicht mehr lesbar ist, findet man diese Datei vielleicht auf der vorletzten oder vorvorletzten Sicherungskopie. Ob CD, DVD, USB-Speicherstick oder externe Festplatte – **alle** Datenträger haben eine begrenzte, mitunter erschreckend geringe Lebensdauer. Auf eine Haltbarkeit von mehreren Jahren sollte man sich nicht verlassen. Einige Probleme der Langzeitlagerung werden im Kapitel „Lebensdauer digitaler Daten“ behandelt.

Bei der **Datenarchivierung** geht es darum, ausgewählte Daten über Jahre, Jahrzehnte und vielleicht über Jahrhunderte sicher aufzubewahren. Meist wird eine Speicherung gefordert, welche nachträgliche Manipulationen unmöglich macht. Wegen der begrenzten Lebensdauer der Sicherungsmedien und der Technologien sollten die archivierten Daten alle paar Jahre überprüft und auf neue Medien umkopiert werden.

Die meisten Nutzer löschen die archivierten Daten von der internen Festplatte, um Speicherplatz frei zu machen. Doch bevor Sie das tun, sollten Sie für eine zweite Kopie auf einem weiteren Archivmedium sorgen.

Die Abgrenzung zwischen Datensicherung und Archivierung ist fließend. Die Kernfunktion von Backup-Tools ist es, Kopien von aktuellen Systemzuständen zu erstellen. Die Kernfunktion der Archivierung ist es, ausgewählte Daten für lange Zeit sicher aufzuheben.

1.2 WAS SIND IHRE DATEN WERT?

Ein Nachbar hat Ihr Auto gestreift. Ein Besucher hat Ihr Notebook vom Tisch gestoßen. Können Sie Schadenersatz verlangen? Ja, selbstverständlich. Aber wie sieht es aus, wenn Ihr Mitarbeiter aus Versehen 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 Schadenersatz vor. Das primäre Ziel ist die Wiederherstellung (Naturalrestitution), ersatzweise die Schadenskompensation.

1.2.1 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 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 erst unternommen zu werden und dem Verursacher entstehen keine Wiederherstellungskosten.

1.2.2 Schadenskompensation

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

- Es wird ermittelt, wie viel 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. B. der Arbeitslohn für zeitweilige Hilfskräfte, sind ersatzfähig.
- Entgangener Gewinn ist ein ersatzfähiger Schaden.

Folgerungen

- Auch wenn der Verlust privater Daten sehr bitter sein kann – deren Verlust führt nicht zu Gewinnausfällen. Deshalb gehen Privatpersonen fast immer leer aus.
- Wenn durch die Schuld eines Mitarbeiters Firmendaten verloren gehen, kann das teuer für ihn werden. Bei grober Fahrlässigkeit kann es den Mitarbeiter fünf Jahre lang den Teil seines Einkommens kosten, der über der Pfändungsgrenze liegt. Außer: Der Chef trägt die Hauptschuld.
- Wer es als Chef versäumt, für regelmäßige Datensicherungen geschäftlich wichtiger Daten zu sorgen, hat eine Mitschuld. Unter Umständen muss er den Schaden vollständig aus seinem privaten Vermögen bezahlen, auch wenn der Schaden sehr hoch ist.
- Während der Tätigkeit eines IT-Dienstleisters kam es zu einem Serverabsturz mit totalem Datenverlust. Die Schadensersatzklage des betroffenen Unternehmens gegen den IT-Dienstleister wurde vom Obergericht Hamm (Az. 13 U 133/03) abgewiesen. Wer seine Daten nicht täglich teilweise und wöchentlich vollständig sichere, handle grob fahrlässig und „blauäugig“.

1.3 ERFAHRUNGEN UND ZAHLEN

Aus den Erfahrungen von Datenrettungs-Unternehmen:

Es gibt nur zwei Arten von Daten:

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

Backups, die nicht mindestens einmal in einem Test erfolgreich wiederhergestellt wurden, verdienen den Namen „Backup“ nicht.

Backup-Lösungen und -Daten, für die niemand in der Firma direkt verantwortlich ist, sind definitiv schlechte oder unbrauchbare Sicherungen.

Aus der Computer-Folklore:

Datensicherung ist nur etwas für Feiglinge.

Zitat aus einem Gerichtsurteil:

Der Datenverlust durch Absturz gehört „zum allgemeinen Risiko eines EDV-Benutzers“, dem durch das übliche Anfertigen von Sicherheitskopien zu begegnen sei.

Wie schlimm kann der Schaden sein?

Erkenntnis der Experten von Scotland Yard:

Ein mittleres Unternehmen, das seine Daten komplett verliert, ist spätestens nach zwei Jahren am Ende.

Statistik des Haftpflichtverbandes der deutschen Industrie:

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

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 doch noch auf. Daraus errechnet sich eine „mittelfristige Überlebensrate“ von 6 %.

Studie des Recoveringspezialisten Jon W. Toigo:

Nach einem totalen Datenverlust erholen sich 43% der Unternehmen finanziell nie mehr, und 29% der betroffenen Firmen schließen innerhalb von zwei Jahren ihren Betrieb.

Ungefähre Preise der professionellen Datenretter:

Der Aufwand hängt von der Art des Datenträgers ab und natürlich von der zu rettenden Datenmenge. Hier ist eine grobe Abschätzung:

- SD-Karte, USB-Stick etc. – 70 bis 150 Euro
- Magnetische Festplatte bei einem logischen Schaden – 400 bis 700 Euro, bei einem mechanischem Schaden – 1000 Euro oder sehr viel mehr.
- SSD-Festplatte – die Kosten sind hoch und kaum kalkulierbar. Weil das „Wear Leveling“ ständig die Daten umverteilt, um die Speicherzellen gleichmäßig abzunutzen, ist eine Datenrettung schwierig.

Kostenloser Ratschlag:

Wenn Ihnen irgend etwas verdächtig vorkommt, sofort die Weiterarbeit einstellen. Windows nicht herunterfahren, denn vielleicht startet Windows 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. Behalten Sie diesen Moment der Unsicherheit im Gedächtnis.

1.4 FAZIT

Datensicherung ist im Prinzip ganz einfach. Man muss nur die wichtigen Dateien regelmäßig auf einen anderen Datenträger kopieren, den man anschließend an einem sicheren Ort aufbewahrt. Dateien zu kopieren ist ein grundlegender, einfacher Vorgang. Außer dem Windows-Explorer gibt es zahlreiche Dateimanager und Backup-Programme.

Warum also wird es nicht gemacht? Ist es der Glaube, dass ein Datenverlust immer nur die Anderen trifft?

Daten zu sichern bedeutet, Vorsorge zu treffen für ein Ereignis, das höchstwahrscheinlich (in der nahen Zukunft) nicht eintreten wird. Daten zu sichern bedeutet letzten Endes, Zeit zu vergeuden in der schwachen Hoffnung, dass es sich vielleicht irgendwann auszahlt.

Berücksichtigt man diese psychologischen Besonderheiten, folgt daraus:

- Eine wirksame Datensicherung muss vollständig oder weitgehend automatisch funktionieren.
- Niemand sollte gezwungen sein, regelmäßig darüber nachdenken zu müssen, welche Daten gesichert werden müssen und welche nicht.

Was können bzw. müssen Sie tun?

- Sie müssen alle wichtigen Daten mindestens doppelt haben: auf der internen Festplatte und zusätzlich auf DVD oder Speicherstick, im Speicher der Kamera oder auf einer externen Festplatte.
- Verlassen Sie sich nicht auf die Langlebigkeit der Datenträger. Beispielsweise sollten Sie alle zwei bis drei Jahre von Ihren DVDs neue Kopien anfertigen. Testen Sie die neuen Medien. Werfen Sie die alten Medien nicht weg. Vielleicht sind die neuen Rohlinge von minderer Qualität und die alten Kopien überleben länger.
- Bewahren Sie die Datenträger nicht alle an einem Platz auf. Wenn die Feuerwehr in der Etage über Ihnen einen Brand löscht, werden möglicherweise der PC und gleichzeitig alle Ihre Kopien unbrauchbar.
- Verwenden Sie hochwertige Rohlinge. Lagern Sie die DVDs im Dunkeln und kühl (aber nicht im Kühlschrank, dort ist es zu feucht).
- Trauen Sie keiner Reklame, besonders nicht den Prophezeiungen der Hersteller zur Lebensdauer ihrer Medien.

Wenn Ihre Daten verloren scheinen, können Sie sich an ein Datenrettungslabor wenden, das mit hoher Wahrscheinlichkeit Ihre Daten wiederherstellen kann. Allerdings kostet das einige bis viele hundert Euro. Ihre Daten rechtzeitig zu duplizieren, kommt Sie erheblich günstiger.

1.5 DATENSICHERUNG MIT 20 KLICKS

Jaja, ich weiß, es gibt zahlreiche Anleitungen „Datensicherung mit drei Klicks“ im Internet. Glaubt irgend jemand, dass drei Klicks tatsächlich genügen? Nun, es ist üblich geworden, in der Werbung schamlos zu lügen. Doch wenn Sie dieses Buch bis zum Ende lesen, können Sie eine individuelle Sicherung einrichten, die tatsächlich mit **einem** Doppelklick oder automatisch gestartet werden kann. Doch jetzt beginnen wir mit Ihrer ersten Datensicherung.

Kaufen Sie eine externe Festplatte (2000 GB für 60 €) oder einen USB-Speicherstick (128 GB für 20 €). Stecken Sie die externe Festplatte (oder den USB-Stick) an einen USB-3-Anschluss. Wenn Sie das erstmals machen, dauert es 10 bis 20 Sekunden, bis der PC in der rechten unteren Ecke des Bildschirms meldet „Neue Hardware gefunden, Treiber werden installiert“ oder „Installieren von Gerätetreibersoftware“ (Win7). Windows 10 öffnet für etwa fünf Sekunden ein Mitteilungsfenster mit dem Label des Datenträgers und der Aufforderung, „Wählen Sie eine Aktion für Wechseldatenträger aus“. Klicken Sie schnell darauf.

Das war der erste Klick.

Falls Sie eine Meldung sehen „Dieses Gerät könnte eine höhere Leistung erzielen ...“, sollten Sie sich die Zeit nehmen, den Stick auszuwerfen und andere USB-Anschlüsse ausprobieren. Ob die Daten mit 480 oder 5000 Mbit/s übertragen werden, macht einen enormen Zeitunterschied aus. Die schnelleren Anschlüsse mit USB 3.0 und höher sind 9-polig und meist blau oder rot, USB 2.0 Anschlüsse sind 4-polig und meist schwarz.

Falls Sie rechtzeitig auf „Wählen Sie eine Aktion für Wechseldatenträger aus“ geklickt haben, öffnet Windows ein Fenster wie das nebenstehende. Im oberen Teil des Fensters steht der Name des Datenträgers (hier: USB_8_GB), den Sie sich merken bzw. auf den Speicher aufkleben sollten. Hier wird auch der Laufwerksbuchstabe angezeigt, der dem Datenträger zugewiesen wurde. **Nehmen wir an, es ist E:**. Hinweis: Der zugewiesene Laufwerksbuchstabe kann morgen ein anderer sein, je nachdem, welche weiteren Geräte angesteckt sind. An einem anderen PC kann der Laufwerksbuchstabe ebenfalls ein anderer sein.

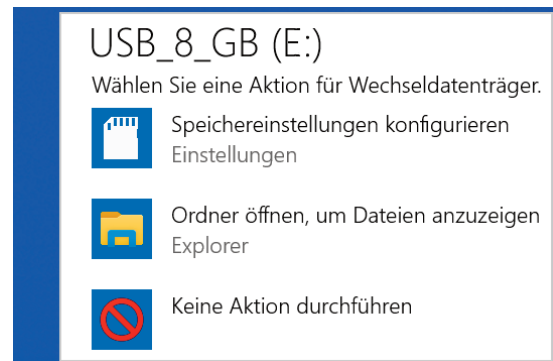


Bild 1.1: Aktion auswählen

Klick 2: Klicken Sie auf „Ordner öffnen, um Dateien anzuzeigen“. Der Windows Explorer zeigt Ihnen im rechten Fenster Teil den Inhalt des eingesteckten Datenträgers. Bei einem neuen Datenträger ist der Ordner leer.

Klick 3 und 4: Rechtsklick in das leere Fenster, Linksklick auf „Neu“ → „Ordner“. Geben Sie dem „neuen Ordner“ einen Namen, z. B. „2020-06-30“.

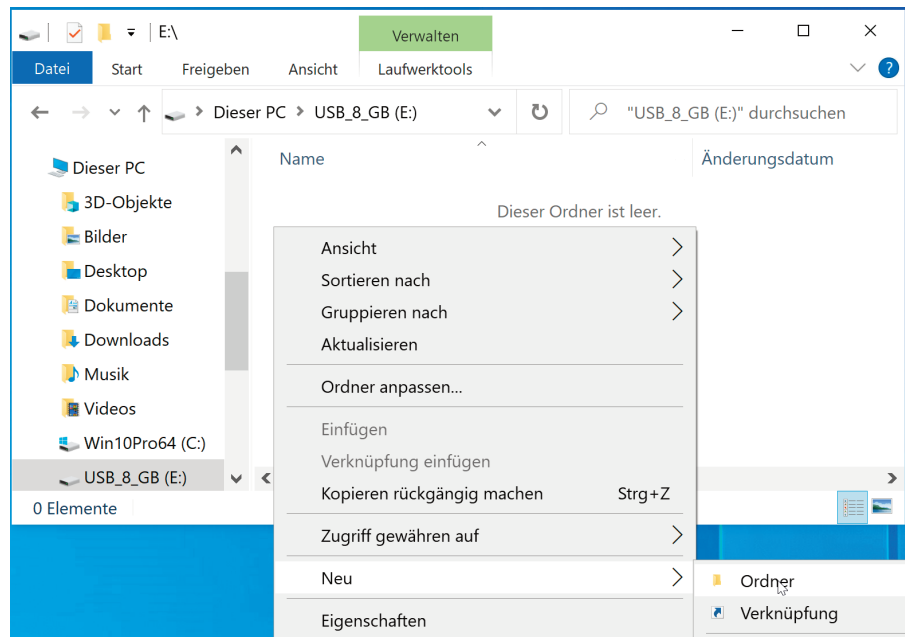


Bild 1.2: Neuen Ordner für Backup anlegen

Klick 5: Doppelklick auf den neuen Ordner. Er ist noch leer, wie im Bild 1.3.

Klick 6: Verschieben Sie das Fenster in die Nähe des rechten Bildschirmrandes, damit in der linken Bildschirmhälfte Platz bleibt, um ein weiteres Explorer-Fenster für die Auswahl der Daten zu öffnen.

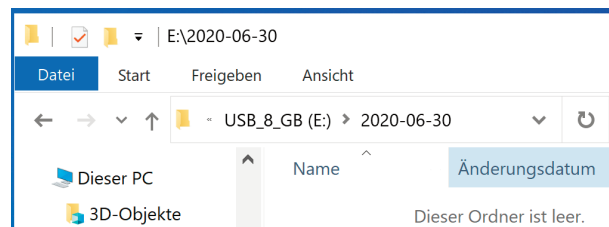


Bild 1.3: Der neue Backup-Ordner ist noch leer

Klick 7 und 8: Rechtsklick auf den Start-Button“. Im Kontextmenü klicken Sie auf „Explorer“. Es öffnet sich ein zweites Fenster mit dem Windows Explorer.

Klick 9: Klicken Sie im soeben geöffneten, linken Explorerfenster auf „Dieser PC“.

In der rechten Fensterhälfte werden Ihnen die wichtigsten Datenordner angezeigt.

Klick 10-14: Nun müssen Sie die zu sichernden Ordner markieren.

Halten Sie die Strg-Taste bis auf weiteres gedrückt und klicken Sie nacheinander auf Bilder, Desktop, Dokumente, Musik und Videos. Falls Sie 3D-Objekte haben, klicken Sie auch darauf. Lassen Sie jetzt erst die Strg-Taste los. Die fünf wichtigsten Ordner sind jetzt markiert, wie in Bild 1.4.

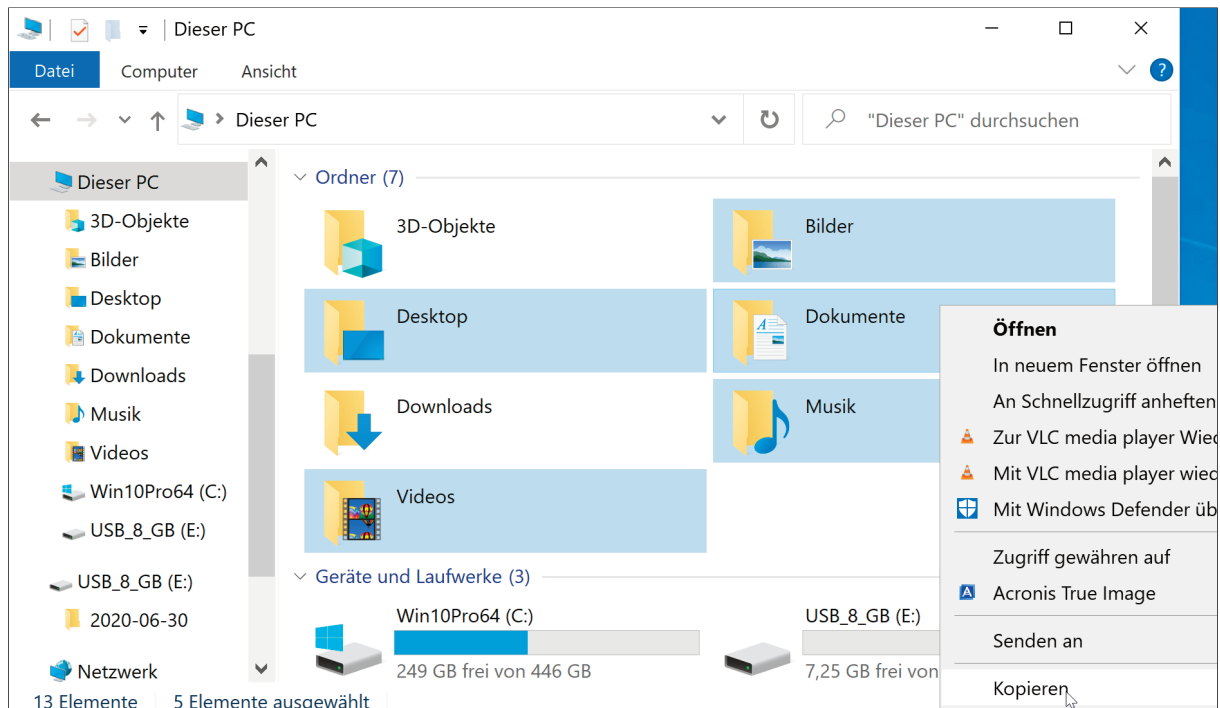


Bild 1.4: Die wichtigsten Ordner sind markiert und das Kontextmenü ist geöffnet

Klick 15: Rechtsklick auf einen beliebigen der markierten Ordner, es öffnet sich das Kontextmenü wie in Bild 1.4 rechts unten gezeigt.

Klick 16: Klicken Sie im Kontextmenü auf „Kopieren“.

Klick 17: Im rechten Teil des Bildschirms ist noch das Explorerfenster zu sehen, dass den leeren Backup-Ordner zeigt. Ein Rechtsklick in das Fenster (z. B. direkt auf den Schriftzug „Dieser Ordner ist leer“) öffnet das Kontext-Menü.

Klick 18: Linksklick auf „Einfügen“. Das Kopieren beginnt jetzt.

Bei eventuellen Meldungen „Es befindet sich bereits eine Datei desselben Namens an diesem Ort“ setzen Sie einen Haken in der linken unteren Ecke bei „Vorgang für die nächsten ... Konflikte wiederholen“ und dann wählen Sie „Kopieren und ersetzen“.

Warten Sie nun das Ende des Kopiervorgangs ab. Prüfen Sie stichprobenartig, ob Ihre wichtigsten Dateien erfolgreich kopiert worden sind.

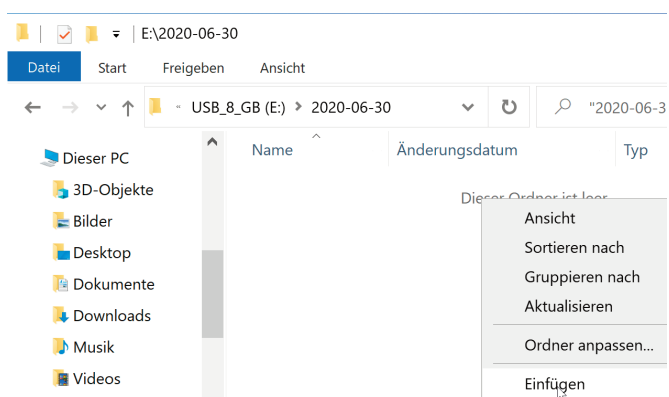


Bild 1.5: Kontextmenü des Backup-Ordners

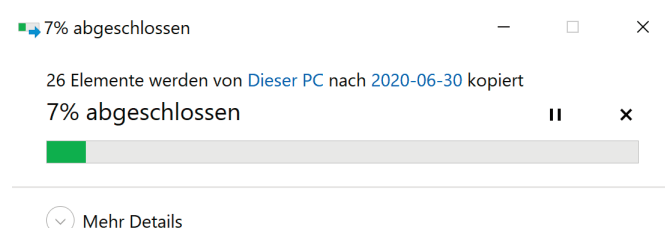


Bild 1.6: Fortschrittsanzeige

Klick 19 und 20: Damit das Backup nicht durch Bedienfehler oder einen bössartigen Trojaner beschädigt wird, sollten Sie den USB-Backup-Speicher nicht dauerhaft am PC angeschlossen lassen.

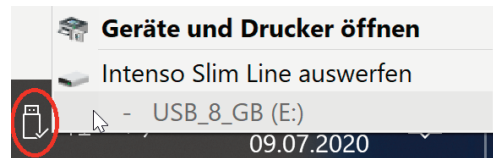


Bild 1.7: USB-Speicher auswerfen

Klicken Sie auf das Symbol für „Hardware auswerfen“ (im rechten Teil der Taskleiste, im Bild 1.7 rot markiert) und danach auf die Bezeichnung des Speichers (es könnten ja mehrere USB-Speicher angesteckt sein).

Nach der Meldung „Hardware kann jetzt entfernt werden“ können Sie den USB-Speicher herausziehen.

Falls Sie den PC herunterfahren wollen, können Sie auf das „Hardware auswerfen“ verzichten und den USB-Speicher nach dem Herunterfahren herausziehen.

Ergänzende Hinweise

- Markieren Sie keine versteckten Links wie z. B. „Anwendungsdaten“ oder „Eigene Dateien“, denn das sind nur für ältere Programme eingerichtete Weiterleitungen auf die neuen Ordnerbezeichnungen „AppData“ und „Dokumente“.
- Den Ordner „Downloads“ brauchen Sie nicht sichern. Normalerweise befinden sich dort nur Dateien, die Sie jederzeit wieder aus dem Internet herunterladen können (meist in einer neueren Version).
- Für Videos sowie Bilder- und Musiksammlungen wird wohl auf einem USB-Speicherstick der Platz nicht ausreichen.
- Einige wenige Programme legen Daten nicht in den Benutzer-Unterordnern ab. Was tun? Siehe Kapitel „Daten ordnen“.
- Falls Sie Ihre E-Mails nicht auf dem Server des Anbieters (z. B. web.de oder gmx.net) lagern, müssen Sie vielleicht Teile des unsichtbaren Ordners „Anwendungsdaten“ bzw. „AppData“ sichern.
- Die obige Anleitung gilt für einen PC mit vorinstalliertem Windows, bei dem es für Betriebssystem, Programme und Daten nur eine einzige Partition gibt. Falls Sie Daten in weiteren Ordnern oder Partitionen haben, müssen Sie diese ebenfalls sichern.

Hier noch ein paar Tipps, wie man mehrere Dateien markiert.

- Die Tastenkombination Strg-A markiert alle Dateien und alle Unterordner des aktuellen Ordners. Wenn Sie die Markierung aller Einträge wieder aufheben wollen, klicken Sie auf irgendeine Datei.
- Wenn Sie eine zusammenhängende Gruppe markieren wollen, klicken Sie auf den ersten Eintrag, drücken Sie auf die Umschalttaste, klicken Sie auf den letzten Eintrag und lassen Sie die Umschalttaste los.
- Mit gedrückter Strg-Taste kann man nacheinander mehrere einzelne Dateien markieren. Klickt man auf eine bereits markierte Datei, wird die Markierung aufgehoben.

1.6 DATENSICHERUNG AUF DVD

Erstaunlich viele Computerbesitzer haben noch nie eine Daten-CD oder -DVD gebrannt. Zugegeben, unter Windows XP war das nicht einfach. Man musste ein Brennprogramm kaufen oder finden und installieren. Doch seit Windows Vista ist ein einfaches Brennprogramm im Betriebssystem enthalten.

Sie können auch ein kostenloses Brennprogramm installieren, z. B. den „CDBurnerXP“ oder „Deep Burner Free“, den es sogar als portable Version gibt. Eine Anleitung zur Benutzung finden Sie auf eifert.net unter „Hilfen“ → „Datensicherung“.

DVD-Rohlinge bekommen Sie in fast jedem Supermarkt. Bevorzugen Sie den Typ DVD-R (einmal beschreibbar) oder DVD-RW (mehrfach beschreibbar), vermeiden Sie DVD+R und DVD+RW. Sowohl DVDs mit Kauf-Software als auch DVDs in Zeitschriften werden in einem Format gepresst, das nur mit DVD-R und DVD-RW kompatibel ist und sich auf DVD+R nicht duplizieren lässt.

Eigentlich ist es einfach: Markieren Sie die Ordner oder die Dateien, die gesichert werden sollen, z. B. wie in Bild 1.4 (zwei Seiten zurück) gezeigt und erklärt. Klicken Sie dann mit der rechten Maustaste auf einen der markierten Ordner. Es öffnet sich das Kontextmenü. Klicken Sie auf „Eigenschaften“. Geben Sie Windows etwas Zeit, die Dateien zu zählen. Die „Größe auf Datenträger“ darf 4,7 GB nicht überschreiten, sonst passt die Datenauswahl nicht auf eine DVD. Auf eine CD passen knapp 0,7 GB.

Wenn Sie eine geeignete Zusammenstellung von Ordnern haben, klicken Sie erneut mit der rechten Maustaste auf einen der markierten Ordner, dabei bleiben die von Ihnen vorgenommenen Markierungen erhalten. Bewegen Sie im Kontextmenü den Mauszeiger auf „Senden an“ und weiter auf „DVD“, den vermutlich letzten Eintrag. Falls Sie ein Brennprogramm wie „CDBurnerXP“ oder „Deep Burner Free“ installiert haben, können Sie die markierten Ordner auch an das Brennprogramm senden. Nun werden Sie aufgefordert, einen leeren Datenträger einzulegen.

Windows 7 und 10 fragen, wie der Datenträger verwendet werden soll. Antworten Sie „mit einem CD/DVD-Player“. Hier können Sie ein Label für die CD/DVD vergeben (maximal 11 Zeichen lang). Vielleicht sehen Sie eine Meldung „Es befindet sich bereits eine Datei gleichen Namens an diesem Ort.“ Dabei geht es um die „desktop.ini“. Jeder Ordner enthält diese normalerweise unsichtbare Datei, in der das Aussehen des Ordners gespeichert ist (große oder kleine Symbole, Sortierung nach Dateinamen oder nach Datum usw.). Diese Datei braucht nicht gesichert zu werden, wählen Sie „Nicht kopieren“. Suchen Sie im oberen Teil des Explorerfensters nach „Brennen“ und klicken Sie darauf.

Prüfen Sie die frisch gebrannte DVD, ob die Dateien lesbar sind. Probieren Sie, ob die DVD auch in einem anderen Laufwerk lesbar ist, z. B. am Computer von Freunden.

1.7 DATENSICHERUNG MIT WINDOWS-BORDMITTELN

1.7.1 Sichern und Wiederherstellen

Windows 7

Das Backup-Programm finden Sie über „Start“ → „Alle Programme“ → „Wartung“ → „Sichern und Wiederherstellen“.

Windows 10

Das Programm von Windows 7 funktioniert auch unter Windows 10. Schreiben Sie „Systemsteuerung“ in das Suchfeld („Zur Suche Text hier eingeben“) und drücken Sie Enter. Stellen Sie „Anzeige“ (rechts oben) auf „Kategorie“. Unter „System und Sicherheit“ finden Sie „Sichern und Wiederherstellen (Windows 7)“.

Ab hier geht es unter Windows 7 und 10 identisch weiter

Als Erstes müssen Sie die „Sicherung einrichten“. Wählen Sie das externe Laufwerk. Anschließend müssen Sie auswählen, welche Daten Sie sichern wollen. Die „Auswahl durch Windows“ ist vielleicht ausreichend.

Das Programm legt einen Ordner mit dem Netzwerknamen des PCs an und darin einige Protokolldateien, Unterordner sowie komprimierte ZIP-Dateien. Die erste Sicherung ist eine Vollsicherung, alle zukünftigen Sicherungen erfassen nur veränderte Dateien. Mit dem Windows-Backup kann man relativ übersichtlich die benötigten Dateien zurückkopieren.

1.7.2 Dateiversionsverlauf von Windows 10

Sie benötigen eine externe Festplatte mit genügend freiem Speicherplatz. Bei der ersten Benutzung des Dateiversionsverlaufs wird eine Vollsicherung vom Desktop und von allen Bibliotheken erstellt. Der „Dateiversionsverlauf“ legt dazu auf dem Sicherungsdатenträger einen Ordner „FileHistory“ an. Beachten Sie: Selbst erstellte Ordner werden ignoriert, wenn man sie nicht zu einer Bibliothek hinzufügt.

Der Befehl, mit dem man Dateien oder Ordner wiederherstellt, heißt „filehistory.exe“ und er ist an der Eingabeaufforderung einzugeben. Beachten Sie auch: Wenn Sie die entsprechende Option nicht abschalten, werden alle USB-Speichersticks und alle angeschlossenen externen Festplatten ebenfalls gesichert. Da wird die Backup-Festplatte schnell voll sein ...

In der Standardeinstellung werden die Daten jede Stunde aktualisiert. Will man die Sicherungsfestplatte nicht ständig eingeschaltet lassen (was u. a. wegen Verschleiß und Wärmeentwicklung nicht zu empfehlen ist), muss sie mindestens für eine Stunde eingeschaltet sein, damit wenigstens einmal täglich eine Aktualisierung erfolgt. Insgesamt ist das ein Verfahren, das für Power-User und Firmen-PCs zusätzlich zu einem Backup sinnvoll sein kann. Für Anwender, die ihren PC nur gelegentlich für eine meist kurze Zeit einschalten, betrachte ich eine solche Backup-Lösung schlichtweg als ungeeignet.

1.8 WARUM SOLLTEN SIE DEN REST DES BUCHES LESEN?

Weil die in den Abschnitten 1.5 und 1.7 beschriebenen Datensicherungen nicht berücksichtigen, welche Arten von Daten Sie haben, wird Ihre Backup-Festplatte schnell voll sein. Zum Einen, weil es sich bei einem großen Teil der gesicherten Daten um temporäre oder anderweitig überflüssige Dateien handelt. Zweitens: Wenn Sie Ihre Daten öfter sichern, werden viele Daten dabei sein, die unnötig oft gesichert werden. Wie viele immer gleiche Kopien Ihrer Fotos möchten Sie auf Ihrer externen Festplatte haben? Wenn Sie sich die Mühe machen, Ihre Datensicherung individuell anzupassen, sparen Sie langfristig eine Menge Zeit und Geld.

1.9 AKTUALITÄT

Sind Sie erstaunt, dass noch Anleitungen zu Windows 7 enthalten sind? Es gibt noch eine Menge Computer mit diesen alten Betriebssystemen, nicht nur in Industriesteuerungen und Geldautomaten. Manche ältere Programme funktionieren nicht mit Windows 10. Für ältere Notebooks und Peripheriegeräte gibt es keine Treiber mehr. Und wer mit dem PC nie ins Internet geht, könnte sogar mit Windows XP noch gut zurechtkommen. Jedenfalls ist auch ein älterer Computer bestens als Backup-PC geeignet, um die Daten aller anderen Computer einzusammeln und zu sichern.

Im Buch sind zahlreiche Verweise auf Internetseiten enthalten, und in meinen „Weblinks zum Buch Datensicherung für Anfänger“ (<https://eifert.net/project/dasi-links/>) finden Sie noch mehr zum Thema. Alle Links wurden vor der Drucklegung überprüft. Doch das World Wide Web ist höchst dynamisch. Webseiten können verschwinden oder sie werden geändert. Der Autor übernimmt keine Verantwortung für den Inhalt der verlinkten Webseiten.

Auch die Anleitungen im Buch werden regelmäßig überprüft. Allerdings gibt es ständig Updates von den Softwareproduzenten, wobei sich manchmal auch die Bedienung ändert. Besonders intensiv wird Windows 10 mit jedem halbjährlichem Update umgestaltet. Kürzlich ist die „Eingabeaufforderung“ zugunsten der „Power Shell“ aus der Zubehörgruppe verschwunden, doch über die Suchfunktion mit der Eingabe von „cmd“ ist die Eingabeaufforderung noch immer nutzbar.

Wenn etwas nicht wie beschrieben funktioniert, finden Sie im Buch oft ein alternatives Verfahren. Vielleicht gibt es schon eine neuere oder bessere Beschreibung auf eifert.net → „Hilfen“ → „Datensicherung“?

Ich würde mich sehr freuen, wenn Sie mir Unstimmigkeiten und Verbesserungsvorschläge mitteilen würden!