Digitale Daten mit Backups vor Verlust schützen

Vorsorge

Von Klaus Fritzsche

Jedem PC-Nutzer ist sicherlich bewusst, dass Daten verloren gehen können, sei es durch Hardwarepannen oder durch die eigene Schusseligkeit. Eine regelmäßige Datensicherung ist deshalb essentiell, um im Fall der Fälle kein Desaster zu erleben.

Eine erfolgreiche Datensicherung hängt an vielen Komponenten – Hardware, Software, Backup-Medien – aber auch die Art der Dateiablage auf der oder den Festplatten im PC haben Einfluss. Nachfolgend sollen ein paar Grundlagen der Datensicherung vermittelt werden.

Regelmäßig!

Sicherlich weiß jeder Computernutzer, dass die darauf befindlichen Daten einer gewissen Gefährdung unterliegen, sei es durch den Defekt einer Festplatte, durch das versehentliche Löschen von Dateien oder sonstigem Malheur. Ebenso klar dürfte sein, dass die Daten deshalb regelmäßig gesichert werden müssen, um einem Verlust vorzubeugen.

Aber – Hand aufs Herz – die Datensicherung (häufig als Backup bezeichnet) ist lästig und mit Arbeit verbunden. Es ist deshalb sinnvoll, das Backup zu einem regelmäßigen Ritual zu machen, so ähnlich wie das Zähneputzen, das ja auch irgendwie der Vorsorge dient.

Für die innere Akzeptanz der Datensicherung ist es ungemein hilfreich, wenn die Prozedur so einfach wie möglich ist und am besten weitgehend automatisch abläuft.

Die wesentlichen Fragen zur Datensicherung sind, *was, wie* und *wohin* gesichert werden soll.

Was wird gesichert?

Grundsätzlich gibt es im Computer zwei Arten von Daten: Das Betriebssystem mit den installierten Programmen einerseits und die Daten des Benutzers andererseits.

Betriebssystem

Das Betriebssystem und die Programme sind relativ statisch. Änderungen ergeben sich im Wesentlichen bei der Installation neuer Programme und beim Einspielen von Updates. Alle diese Daten liegen auf der sogenannten Systempartition der Festplatte. Zu Schaden kommen kann die Systempartition nicht nur durch Hardware-Defekte, sondern auch durch Schadsoftware. Generell kann die Systempartition durch Neuinstallieren des Betriebssystems und der Programme wieder hergestellt werden. Weil das aber recht langwierig sein kann, lohnt es sich, zumindest alle paar Monate eine System-Sicherung zu machen. Dafür gibt es Programme, welche die gesamte Systempartition auf ein anderes Speichermedium kopieren, z. B. DriveSnapshot (näheres am Ende des Artikels).

Daten

Die Daten des Benutzers sind Dokumente wie Texte und Grafiken, Bilder, Videos, Musik, AV-Projekte und alles Mögliche andere. Die Daten sind viel dynamischer als das Betriebssystem, bei der täglichen Arbeit kann sich viel ändern. Vor allem alle selbst erstellten Daten, also die eigenen Texte und Fotos bedürfen einer Sicherung, denn sie waren mit Arbeit verbunden oder sind erst gar nicht erneut herzustellen, wie z. B. die Urlaubsbilder. Aus der persönlichen Arbeitswut ergibt sich die Häufigkeit der Sicherung. Im Privathaushalt mag eine wöchentliche Sicherung ein geeigneter Kompromiss aus Sicherheit, Aufwand und Platzbedarf sein.

Wichtige Daten sollten mindestens zweifach, besser dreifach gespeichert sein. Außer auf dem Arbeits-PC sind die Daten also auf mindestens einem Backup-Medium vorhanden. Wenn z. B. die Speicherkarte einer Kamera ausgelesen wird, sollte diese erst gelöscht werden, wenn die Bilder auf den PC und auf eine weitere Festplatte überspielt wurden.

Eine übersichtliche Struktur der vielen Datenordner dient dem leichteren Zurechtfinden wie auch der leichteren Anlage der Datensicherung. Umgekehrt, wenn Bilder und andere Daten auf der ganzen Festplatte unsortiert verstreut liegen, wird die Einrichtung einer Datensicherung unnötig schwierig.

Trennung

Aufgrund der Unterschiede von Betriebssystem und Daten, was die Änderungshäufigkeit angeht und die Art der Wiederherstellung (als Ganzes hier und dateiweise dort) ist es sinnvoll, unterschiedliche Sicherungsmethoden zu verwenden. Das setzt allerdings voraus, dass Daten auf einer anderen Festplatten-Partition abgelegt sind als das Betriebssystem. Sonst würden bei einer Wiederherstellung des Betriebssystems aus einer Datensicherung, die vielleicht schon etliche Wochen alt ist, auch die Daten mit dem alten Stand überschrieben.

Wie wird gesichert?

Für die Datensicherung gibt es verschiedene Methoden, die sich im Platzbedarf und der Komplexität unterscheiden.

Bei einer **Synchronisation** werden neue Dateien (seit dem letzten Backup) dazu kopiert, geänderte Dateien werden überschrieben und inzwischen gelöschte Dateien von der Backup-Platte ebenfalls entfernt. Diese Art des Backups ist schnell und braucht am wenigsten Platz auf der Backup-Platte. Alle Dateien sind 1:1 auf dem Backup-Medium zu finden. Nachteilig ist jedoch, dass aus Versehen gelöschte Dateien auch auf der Backup-Platte gelöscht werden.

Wenn dieser Nachteil vermieden werden soll, müssen die vorherigen Backup-Daten erhalten bleiben. Das funktioniert mit einer sogenannten **Versionierung**. Dazu wird

für jedes Backup ein Ordner mit dem aktuellen Datum angelegt und dort hinein werden die Daten kopiert. Dafür gibt es wiederum mehrere Methoden, die bei manchen Backup-Programmen wählbar sind:

Komplettsicherung: Der komplette Datenbestand wird auf die Backup-Platte kopiert. Das wird bei der Erstsicherung und dann in größeren Abständen durchgeführt.

Differentielles Backup: Nach dem ersten Backup werden bei den folgenden Backups nur alle neuen und geänderten Dateien (im Vergleich zur letzten Komplettsicherung) kopiert. Für die Wiederherstellung muss also auf das letzte Komplettbackup und die letzte differentielle Sicherung zugegriffen werden.

Inkrementelles Backup: Hier werden nur alle neuen und geänderten Dateien (im Vergleich mit dem letzten inkrementellen Backup) kopiert. Das beansprucht weniger Platz als das differentielle Backup, aber die Wiederherstellung wird komplizierter, denn es muss auf die letzte Komplettsicherung und auf alle danach erfolgten inkrementellen Backups zugegriffen werden.

Wenn der Platzverbrauch des Backups nicht ausufern soll, müssen alte Kopien auch regelmäßig wieder gelöscht werden. Bis zu welchem Alter Backups aufbewahrt werden, hängt vom persönlichen „Sicherheitsbedürfnis“ ab.

Es ist möglicherweise sinnvoll, für verschiedene Daten auch verschiedene Verfahren anzuwenden. Für das Bildarchiv, das leicht einige hundert Gigabyte groß sein kann, mag eine Synchronisation ausreichen. Für Textdokumente, an denen intensiv gearbeitet wird, mag eine stündliche Sicherung mit Versionierung angemessen sein.

Wohin wird gesichert?

Ein Backup-Medium sollte in erster Linie ein zuverlässiger Datenspeicher sein. Geschwindigkeit, günstiger Preis und einfache Handhabung sind weitere Kriterien.

Sehr wichtig ist, dass das Backup-Medium nur während des Backups mit dem PC verbunden ist und ansonsten an einem sicheren Ort verstaut ist. Das erfordert zwar ein paar Handgriffe mehr vor und nach der Datensicherung und verhindert auch eine vollständige Automatisierung der Sicherung, verringert aber die Gefahr von Datenverlust. Sollte ein Verschlüsselungstrojaner auf den PC gelangen, würde der die Daten einer direkt angeschlossene Backup-Platte ebenso unbrauchbar machen wie die auf PC-internen Laufwerken.

Dennoch kann auch mit fest verbundenen Backup-Medien gearbeitet werden, dann muss aber der Zugriff durch ein Protokoll (mit Benutzername und Passwort) geschützt sein, wie z. B. FTP, SSH oder WebDAV. Das geht, wenn das Backup-Ziel nicht eine einfache Festplatte ist, sondern ein Server mit entsprechenden Diensten, z. B. in der Cloud oder in einem lokales NAS (Näheres weiter unten). Wer für den Internetzugang eine Fritz-Box betreibt, kann deren eingebautes NAS nutzen, es braucht lediglich eines nicht zu kleinen USB-Sticks, der in die Box gesteckt wird.

Festplatten

Die externe (Magnet-)Festplatte mit USB3-Anschluss bietet einen günstigen Preis pro Gigabyte und ist ein recht langlebiger und zuverlässiger Datenspeicher. Am besten hält man zwei oder drei solcher Festplatten vor, die dann abwechselnd benutzt werden. Wenn eine davon außer Haus oder zumindest im Keller gelagert wird, sind die Daten auch gegen elementare Schäden wie Blitzschlag und Feuer ganz gut geschützt.

Es sei noch festgehalten, dass Festplatten Verschleißteile sind. Ein regelmäßiger Austausch hilft auch, das Ausfallrisiko zu verringern. Drei bis vier Jahre bei täglicher Nutzung sollte eine Festplatte zuverlässig funktionieren. Nach dieser Zeit ist ohnehin oft ein größeres Modell fällig …

Backup-Platten, die immer nur kurzzeitig in Betrieb sind, haben natürlich eine wesentlich länger Lebensdauer.

Cloud

Die „Cloud“, also ein Webdienst im Internet, hat einige Vorteile: die Daten sind physisch sicher aufgehoben und ein Zugriff im Prinzip jederzeit möglich. Aber natürlich gibt es auch Nachteile: Wer noch nicht im Glasfaser-Zeitalter angekommen ist, muss insbesondere für den Upload etwas mehr Zeit einplanen. Und Speichergrößen, die auch für ein Bild- und/oder Videoarchiv groß genug sind, gehen ins Geld. Von daher ist die Cloud eher für die „kleinen“ Daten wie Texte und Projektdateien geeignet. Dafür reicht eventuell sogar ein kostenlos angebotener Cloudspeicher wie z. B. die Magenta-Cloud. Doch Obacht: gerade bei kostenlosen Lösungen sollte man genau hinschauen, wo die Daten gespeichert werden. Manche Datenspeicher sind in den USA und da wollen wir unsere Daten vielleicht nicht haben. Generell empfiehlt es sich, alle Dateien in der Cloud nur verschlüsselt abzulegen, damit der Cloud-Betreiber oder Behörden keinen Zugriff haben. Ein dauerhaft gesperrter Account, weil der Betreiber Bilder von nackten Kindern zu erkennen glaubte, ist schon vorgekommen.

NAS-Geräte

NAS-Geräte (Network Attached Storage) sind eigenständige Geräte mit einer oder mehreren Festplatten, die über ein Netzwerk mit in der Regel mehreren PCs verbunden sind. Sie sind sozusagen eine hausinterne Cloud, und sie dienen in erster Linie als zentraler Datenspeicher, aber auch als Medienserver für Musik und Video. NAS-Geräte sind typischerweise ständig in Betrieb und von daher kein sicheres Backup-Medium (außer, der Zugriff ist z. B. via FTP gesichert).

Protokolle (FTP, SSH, WebDAV)

Mit Protokoll ist hier gemeint, dass für den Zugriff auf den externen Speicher (in der Cloud oder im NAS) eine Anmeldung mit Nutzernamen und Passwort erforderlich ist. Das schützt die Daten vor unbefugtem Zugriff.

Wichtig: Cloud- und NAS-Speicher (auch der USB-Stick an der Fritz-Box) lässt sich meistens auch so konfigurieren, dass er über einen Laufwerksbuchstaben direkt vom PC angesprochen werden kann (also ohne Protokoll). Das ist zwar komfortabel, es ist für Backup-Speicher aber ein No-Go, denn ein Verschlüsselungstrojaner hätte dann ebenso einfach Zugriff auf die Backup-Daten.

RAID-Systeme

RAID-Systeme werden typischerweise in NAS-Geräten verwendet. Ein RAID-System verbindet mehrere Festplatten zu einem Verbund. Dabei kann je nach Konfiguration ein schnellerer Datenzugriff und/oder eine

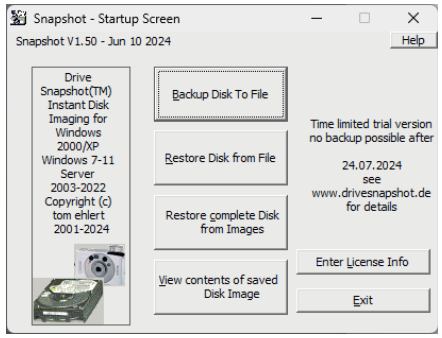
redundante (mehrfache) Speicherung der Daten im Vordergrund stehen. Mit einer Datensicherung hat RAID dennoch nichts zu tun. Es geht dabei ausschließlich um die Verfügbarkeit des Festplattenspeichers: Bei Ausfall einer Platte kann trotzdem weitergearbeitet werden. In Firmen ist das wichtig. Im privaten Umfeld erkauft man sich diesen Vorteil mit einigen Nachteilen aufgrund der höheren Komplexität. Eine Fehlbedienung oder ein Defekt des RAID-Controller-Chips sind zusätzliche Risiken, die zum kompletten Datenverlust führen können. Zudem ist eine Datenwiederherstellung auf einer getauschten Platte ein besonderer Stress für die noch intakte Platte und ein Ausfall auch dieser nicht so unwahrscheinlich. Die Daten auf einem RAID-System müssen deshalb genauso gesichert werden wie bei einfachen Festplatten.

Programme

Eine Sicherung von Hand ist mühsam und fehleranfällig. Es gibt bewährte Programme für die Datensicherung. Exemplarisch seien hier zwei Programme genannt, die sich über Jahre bewährt haben.

Man kommt nicht darum herum, sich vor der ersten Benutzung eines Backup-Programmes mit der Konfiguration auseinanderzusetzen und einige Tests zu machen, denn es gibt allerhand Einstellmöglichkeiten. Wichtig ist auch eine Kontrolle, ob das Backup so funktioniert hat, wie man es geplant hat. Das muss zumindest am Anfang und später stichprobenartig erfolgen.

DriveSnapshot ist ein Programm für die Sicherung ganzer Partitionen, es kostet einmalig 39 Euro, kann aber 30 Tage lang kostenfrei getestet werden. Nach dem



Das Programm DriveSnapshot sichert komplette Festplatten-Partitionen

Testzeitraum ist eine Wiederherstellung weiterhin unbegrenzt möglich, lediglich die Sicherung funktioniert nicht mehr. Die Programmoberfläche ist Englisch, auf der Downloadseite steht jedoch ein ausführliches deutsches Handbuch als PDF zur Verfügung.

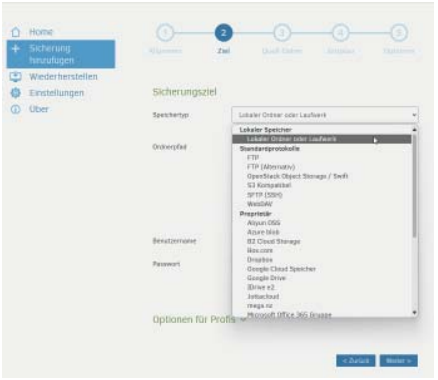
Außer einer kompletten Wiederherstellung kann die Sicherungsdatei auch als virtuelles Laufwerk geöffnet werden und es können dann einzelne Dateien aus der Sicherung entnommen werden.

Duplicati 2.0 ist ein Programm für die Sicherung von Einzeldateien bzw. Verzeichnissen. Dieses Programm ist für die private Nutzung kostenlos. Bedient wird es über einen Webbrowser. Es können mehrere Sicherungs-Jobs angelegt werden. Darin wird jeweils definiert, welche Verzeichnisse zu sichern sind, wohin gesichert wird (z. B. externe Festplatte oder NAS via Protokoll), außerdem Verzeichnisse oder Dateitypen, die von der Sicherung ausgenommen werden sollen (z. B. temporäre Daten), und auch ein Zeitplan ist individuell einstellbar. Auf Wunsch werden die Daten verschlüsselt, bevor sie aufs Backup-Medium kopiert werden.

Duplicati 2.0 ist ein Browserbasiertes Programm für die Sicherung von Verzeichnissen

Oben: Im Hauptmenü werden die konfigurierten Sicherungen aufgelistet

Über den Menüpunkt „Sicherung hinzufügen“ werden in mehreren Schritten Allgemeines, das Sichrungsziel und die zu sichernden Verzeichnisse festgelegt (unten und rechts)



Downloadlinks

DriveSnapshot: drivesnapshot.de
Duplicati 2.0: duplicati.com