



Backup

Um ein Backup kommt man nicht herum, will man vor verlorenen Notebooks, Virenbefall und unachtsamer Löscherei gefeit sein. Einige Fragen erreichen uns immer wieder aufs Neue – hier beantworten wir sie.

Von Jan Schübler

Die Grundregel: 3-2-1

? 3-2-1? Wie bitte?

! Die 3-2-1-Regel besagt, dass es von wichtigen Dateien stets mindestens drei Exemplare inklusive des Originals gibt, dass diese drei Exemplare auf mindestens zwei verschiedenen Medientypen gesichert sind und dass eine der Sicherungskopien außer Haus gelagert wird – Letzteres, um Diebstahl, Wohnungsbrand und Ähnlichem vorzuzukommen.

In der Praxis kann das zum Beispiel so aussehen, dass Sie erstens alle wichtigen Dateien auf Ihrem PC vorhalten, zweitens regelmäßig ein Backup auf einer externen Festplatte speichern und drittens Ihre Daten in einen vertrauenswürdigen Cloudspeicher synchronisieren.

Bedenken Sie außerdem, dass Backup-Medien nicht dauerhaft mit dem PC verbunden sein dürfen. Verbinden Sie sie stattdessen nur zum Zweck der Datensicherung und klemmen Sie sie danach gleich wieder ab. Denn der beste Backup-Speicher bringt Ihnen nichts, wenn er am PC hängt, während ein Erpressungstrojaner all Ihre Dateien kapert und das Backup dabei gleich mitnehmen kann.

Pro-Tipp: Erweitern Sie die 3-2-1-Regel zur 3-2-1-0-Regel. Achten Sie darauf, null proprietäre oder undokumentierte Speicherformate zu verwenden (siehe auch weiter unten: Hard- und Software).

Ist das nötig?

? Ehrlich, ich bin so faul. Muss ich wirklich ein Backup haben?

! Diese Frage können Sie selbst am besten beantworten: Stellen Sie sich einfach vor, die Festplatte oder SSD in Ihrem PC ginge von jetzt auf gleich kaputt oder Ihr Smartphone ginge auf der nächsten

Reise über Bord. Alles an Daten, was Sie nicht noch irgendwo anders gesichert haben, wäre dann futsch. Wäre die einzige Sorge, die Sie danach haben, bloß der Verlust der teuren Hardware? Wenn ja, brauchen Sie wohl wirklich kein Backup. Ansonsten gilt: kein Backup – kein Mitleid.

Kaputtes Acronis-Archiv

? Ich nutze Acronis True Image und bin nun auf eine Wiederherstellung angewiesen – doch ich bekomme stets nur die Fehlermeldung, das Backup sei defekt. Der Acronis-Support erweist sich als unfähig, mir zu helfen. Und nun?

! Von solchen Problemen hören wir ab und zu – eine fertige Lösung haben wir für so etwas leider nicht und würden, beträfe es uns, auch zunächst per Google recherchieren und Supportforen durchstöbern müssen.

Erfahrungen wie Ihre sind allerdings ein perfektes Beispiel für ein generelles Problem: Nutzt ein Hersteller ein proprietäres Speicherformat, stehen Sie im Zweifelsfall im Regen, wenn ein Archiv beschädigt ist oder irgendein skurriles Kompatibilitätsproblem mit einer neuen Softwareversion auftritt.

Hard- und Software

? Gibt es bestimmte Backup-Programme, die Sie empfehlen können?

! Ja. Wir erachten es für hilfreich, ein Speicherformat zu verwenden, mit dem Sie sich nicht von einem einzelnen Softwarehersteller abhängig machen. So vermeiden Sie, dass künftige Kompatibilitätsprobleme oder kryptische Fehlermeldungen beim Wiederherstellen zur Stolperfalle werden.

Daraus lassen sich durchaus ein paar Empfehlungen ableiten. Für Backups der



Syncthing ist ein P2P-Programm, das sich hervorragend zur Datensicherung eignet – kostenlos und quelloffen.

kompletten Windows-Systempartition auf eine externe Festplatte erweist sich etwa seit Jahren das von uns entwickelte Skript `c't-WIMage` als robust (siehe ct.de/wimage). Es sichert in WIM-Abbilddateien, die sich mit jedem Windows lesen lassen. Der eigentliche Charme des Tools besteht aber darin, dass die Wiederherstellung eines WIMage-Backups mittels der regulären Windows-Setup-Umgebung geschieht. Geht Ihr PC kaputt, können Sie die Sicherung ohne Treibermäzchen auch auf einem neuen Rechner wiederherstellen – denn das Zurückspielen regelt die Windows-Setup-Umgebung.

Um Ordner und Dateien zu sichern, eignet sich etwa `Duplicati` [1], das auf quelloffene Speicherformate setzt, sodass sich Archive im Notfall auch ohne die Software auslesen lassen. Eine Empfehlung wert sind außerdem Peer-to-Peer-Synchronisierer (P2P) wie `Syncthing` oder `Resilio Sync`. Sie halten Ordnerinhalte zwischen mehreren Rechnern und auch Smartphones und Tablets synchron. In [2] finden Sie eine Anleitung zum Bau eines Backup-Speichers, der einen Raspberry Pi mit externer Festplatte als Grundlage verwendet und in [3] Tipps für ein universelles Familienbackup mit `Resilio Sync`.

Beim Kauf von Speichermedien sollten Sie USB-Sticks meiden und externen Festplatten und SSDs den Vorzug geben – letztere sind im Regelfall einfach langlebiger. Gegen den Einsatz eines USB-Sticks, etwa um die wichtigsten Dokumente im Notfall schneller griffbereit zu haben, spricht natürlich trotzdem nichts.

Windows-eigene Sicherung

? Was spricht eigentlich gegen die auch in Windows 11 nach wie vor enthaltene Funktion „Sichern und Wiederherstellen (Windows 7)“?

! In erster Linie die miserablen Erfahrungen, von denen uns Leser seit vielen Jahren immer wieder berichten. Zwar lassen sich Backups damit problemlos erstellen, doch scheitert die Wiederherstellung bemerkenswert oft – an skurrilen Problemen wie einer veränderten Partitionierung oder minimal veränderter Hardware. Weil die Verlässlichkeit des Wiederherstellungsvorgangs absolut essenziell ist, können wir daher nur raten: Finger weg. Microsoft hat die Funktion ohnehin

längst als „deprecated“ gekennzeichnet, also als veraltet.

Wichtige Handgriffe

? Ich habe ein Backup erstellt. Jetzt ist alles fein, oder?

! Nein, noch nicht. Es mag etwas penibel klingen, aber um auf der sicheren Seite zu sein, müssen Sie auch testen, ob sich das Backup im Fall der Fälle wiederherstellen lässt. Geht es um ein Backup von Ordnern und Dateien, ist das recht einfach: Holen Sie stichprobenartig einige Dateien aus der Sicherung heraus und probieren Sie, ob sie sich öffnen lassen.

Um die Funktionsfähigkeit eines kompletten Systemabbaus zu prüfen, müssten Sie es streng genommen einmal zurückspielen, zum Beispiel auf einen Testrechner oder auf eine unbenutzte Festplatte oder SSD, die Sie zu dem Zweck temporär in Ihren PC einbauen. Das ist ein gewisser Aufwand – ist Ihnen das zu viel, prüfen Sie wenigstens, ob Sie die Wiederherstellungsumgebung starten und das Backup zum Zurückspielen auswählen können. In `c't-WIMage` klicken Sie sich beispielsweise bis zu dem Punkt durch, an dem das Setup Sie fragt, auf welcher Partition Ihr Windows landen soll und brechen den Vorgang dann ab. Bedenken Sie aber: Dass das Backup funktionsfähig ist, ist damit zwar sehr wahrscheinlich, aber nicht bewiesen.

Fotos von Android sichern

? Ich fotografiere viel mit meinem Android-Handy und möchte die Fotos auch gerne unterwegs schon sichern können, aber nicht immer gleich alles in die Google-Cloud schieben – zumal der Speicherplatz immer ratzfatz zur Neige geht.

! Dafür gibt es mehrere Lösungen. Eine, die datenschutztechnisch und in puncto Komfort hervorragend abschneidet, ist ein Cloudspeicher mit Ende-zu-Ende-Verschlüsselung wie `Tresorit` oder `YourSecureCloud`. Der Nachteil: Die Abos dafür sind teils etwas, teils deutlich teurer als die Speichererweiterungs-Abos für Google Drive, Microsoft OneDrive & Co.

Auch in diesem Fall empfehlen wir darüber hinaus einen Backup-Speicher auf Basis von `Syncthing` als Alternative. Es synchronisiert Ihre Daten via Internet,

braucht aber keinen Cloudspeicher dafür und auf Wunsch speichert es auch einen Versionsverlauf Ihrer Dateien [2].

Voll vs. inkrementell vs. differenziell

? Mein Backuptool spricht von inkrementellen, differenziellen und vollen Backups. Was hat es damit auf sich?

! Bei einem Vollbackup wird bei jedem erneuten Backupvorgang eine vollständige Sicherung aller zu sichernden Daten erzeugt. Das ist platztechnisch ineffizient: Sichern Sie rund 200 GByte an Daten, ist eine 1-TByte-Festplatte nach vier bis fünf Backups voll – mit Datenkompression vielleicht ein paar mehr.

Bei einem differenziellen Backup wird nur einmal ein Vollbackup erzeugt. Danach vergleicht die Backup-Software nur noch, welche der Daten sich im Vergleich zu diesem vollständigen Abbild geändert haben oder neu hinzugekommen sind und sichert die in einem Differenzabbild. Zum Wiederherstellen der jüngsten Sicherung braucht man also zwei Archive – Vollbackup plus jüngstes Differenzabbild.

Inkrementelle Backups sind die platzsparendste Variante. Sie wenden das Prinzip differenzieller Backups wiederum auf die Differenzabbilder an. Die Software erstellt zunächst ein Vollbackup und danach inkrementelle Abbilder. Zum Wiederherstellen der jüngsten Datensicherung sind also das volle Abbild plus *alle* seitdem erstellen Inkremente nötig, da jedes einzelne jeweils auf das vorige aufbaut.

Der Nachteil der Platzspartechniken: Ist ein relativ frühes Teilarchiv beschädigt, lassen sich meist auch die darauf aufbauenden inkrementellen Backup-Sätze nicht mehr gebrauchen. Aus diesem Grund kombinieren die meisten Tools die Verfahren und erstellen beispielsweise bei jedem zehnten Backup-Vorgang ein Vollbackup und dazwischen differenzielle oder inkrementelle Datensätze. (js@ct.de)

Literatur

- [1] Ronald Eikenberg, `Backups überall, Daten schnell und einfach mit Duplicati 2.0 sichern`, c't 24/2019, S. 160
- [2] Jan Schüßler, `Ding zum Sichern, Plattform-unabhängiges Backup mit Syncthing`, c't 14/2021, S. 140
- [3] Axel Vahldiek, `Alle in einem, Emotet-sicheres Familien-Backup`, c't 10/2020, S. 26

Backup-Tools: ct.de/y1fb