Datensicherung und -wiederherstellung

Stand: 10.08.2023 Quelle: https://www.freiesoftwareog.org

Vorbeugen ist besser als heulen.
Deshalb sind Backups von wichtigen
und (vermeintlich) unwichtigen Dateien Pflicht.

Inhaltsverzeichnis

Allgemeines

Nachfolgend werden zunächst einige grundlegende Fragen angesprochen und geklärt.

Begriffserklärung

Unter Backup versteht man das teilweise oder gesamte Kopieren der in einem Computersystem vorhandenen Daten auf ein alternatives (häufig transportables) Speichermedium.
Zur wiederherstellbaren vollständigen Datensicherung ist die Fixierung aller Werte bzw. Daten notwendig.
Die auf dem Speichermedium gesicherten Daten werden als Sicherungskopie, bzw. „Backup“ bezeichnet.
Das Ziel ist, den Datenverlust bei Systemausfällen zu begrenzen, bzw. ganz zu vermeiden.
Die Wiederherstellung einer Sicherungskopie bezeichnet man als Datenrücksicherung, Restore oder Recovery.

Warum Backups?

Neben dem einleuchtenden Grund, Backups zu machen um Datenverlusten vorzubeugen, gibt es auch andere, z.B. gesetzliche Grundlagen:

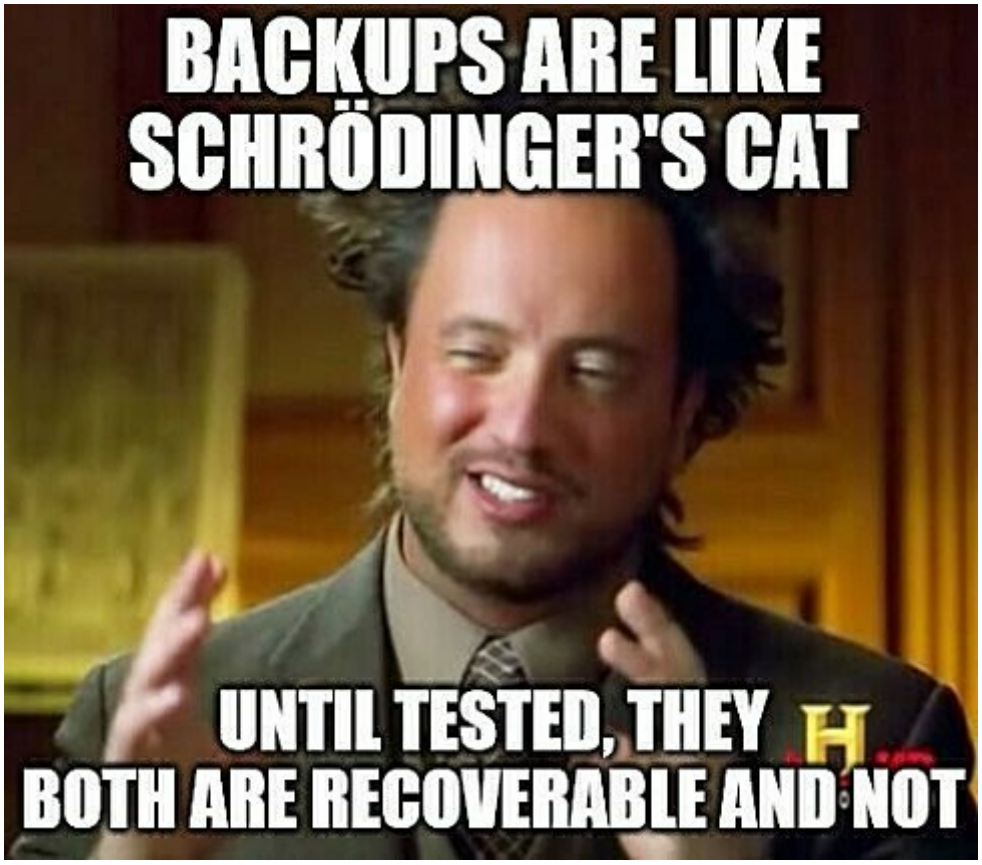
- Basel II: Backup wirkt sich auf die Kreditwürdigkeit eines Unternehmens aus
- ISO/TS 15949: Pflicht!
- Ordnungsgemäße, nachvollziehbare, revisionssichere Buchführung (lt. HGB)

Was kann passieren?

- Menschliches Versagen...
  (Hoppla, Verzeichnis gelöscht, „rm -rf /“)
- Technisches Versagen
  (z.B. Festplattendefekt, Überspannung, Fallschaden, etc.)
- Umweltgefahren
  Blitz/Sturm/Hagel, Feuer/Löschwasser, Erdbeben
- Vandalismus
- Diebstahl

Rücksicherung testen

Der einzig sichere Beweis einer erfolgreichen Datensicherung ist der Nachweis, dass die gesicherten Daten auch vollständig und innerhalb eines angemessenen Zeitraums wiederhergestellt werden können.



Aus diesem Grund müssen unbedingt in regelmäßigen Abständen Rücksicherungstests erfolgen.
Wer hat schon jemals ein „Bare-Metal-Recovery“ versucht?
Hier kann auch mal ein Test mit einer virtuellen Maschine helfen...

Was sollte gesichert werden?

Im Privatbereich geht es meist darum, Korrespondenz, Urlaubsbilder oder digitalisierte Unterlagen zu sichern.
Je nach Datenumfang (z.B. Hobbyfotographen) reicht als Sicherungsmedium eine USB-Festplatte, ergänzt durch das gelegentliche „wegbrennen“ auf DVD oder Blu-Ray (aber Achtung! Medien-Wahl).
Der gemeine Privatanwender wird beim Sichern durch diverse Backup-Programme unterstützt, welche bei großen Distributionen bereits mitgeliefert werden, oder einfach nachzuinstallieren sind.

Arbeitsdateien

Klassischerweise alles, was der Benutzer über die Zeit selbst „erzeugt“ hat.
Briefe, Kalkulationstabellen, Zeichnungen usw.
Dazu zählen auch Bilder, Musik und Videos.
All diese Dateien „leben“ (falls der Benutzer halbwegs vernünftig arbeitet...) im /home-Verzeichnis (GNU/Linux) bzw. im Benutzerverzeichnis (Windows).
Sie sind meist nach ihrem Zweck benannt, beispielsweise „Dokumente“, „Bilder“, „Videos“, „Musik“...
Also recht einfach zu identifizieren und in eine anstehende Datensicherung zu integrieren.

Lesezeichen des Browsers

Oft übersehen, doch manchmal schmerzlich bereut, ist die Sicherung von Lesezeichen im Browser.
Wie lange hat man wichtige, interessante und hilfreiche Links gesammelt?

Mails und Mailkonteneinstellungen

Genau wie Lesezeichen wird das Mailprogramm meistens übersehen, wenn es um die Sicherung von Daten geht.
Wenn man seine Mails über das Webinterface des jeweiligen Anbieters verwaltet, hat man erstmals nichts zu verlieren.
Verwendet man hingegen einen Mailclient wie beispielsweise Thunderbird, sollte man auch hier ein wenig Sorgfalt in die Sicherungsplanung investieren.
Was würde der Verlust von bestimmten Mails oder dem Adressbuch bedeuten?
Auch hier gibt es einige hilfreiche Anwendungen bzw. Add-Ins, die den Anwender beim Sichern unterstützen.

Programm	Kompatibilität	Typ	Website
Autoarchive Reloaded	GNU/Linux, Windows	Thunderbird Add-On	https://addons.thunderbird.net/de/thunderbird/addon/autoarchivereloaded/
ImportExport Tools NG	GNU/Linux, Windows	Thunderbird Add-On	https://addons.thunderbird.net/de/thunderbird/addon/importexporttools-ng/

Konfigurationsdateien (GNU/Linux)

Im „/home“-Verzeichnis des jeweiligen Benutzers gibt es einige sogenannte „Dot-Dateien bzw. -Verzeichnisse“. Diese sind versteckt und beinhalten Konfigurationesdateien und benutzerspezifische Einstellungen von Anwendungen. Wenn man spezielle Anwendungskonfigurationen erhalten möchte, sollte man diese ebenfalls mitsichern.

Smartphone-Dateien

Oft geht man davon aus, dass Dateien, welche man auf dem Smartphone hat, ja sowieso automatisch über den jeweiligen Cloud-Dienst gesichert werden. Sei es nun Google (Android) oder die iCloud (Apple).
Allerdings spricht nichts dagegen, diese Bewegungsdaten ab und an auch einmal irgendwohin lokal zu speichern. Mal abgesehen davon, dass auch nicht jeder möchte, dass seine Daten (Kontakte, Termine, Notizen, Mails, ...) irgendwo im Wolkenkuckucksheim landen...

Hier bietet sich zum Beispiel eine eigene „Cloud“ an. Mit einem RaspberryPi und der NextCloud.

Datensicherheit und Datenschutz

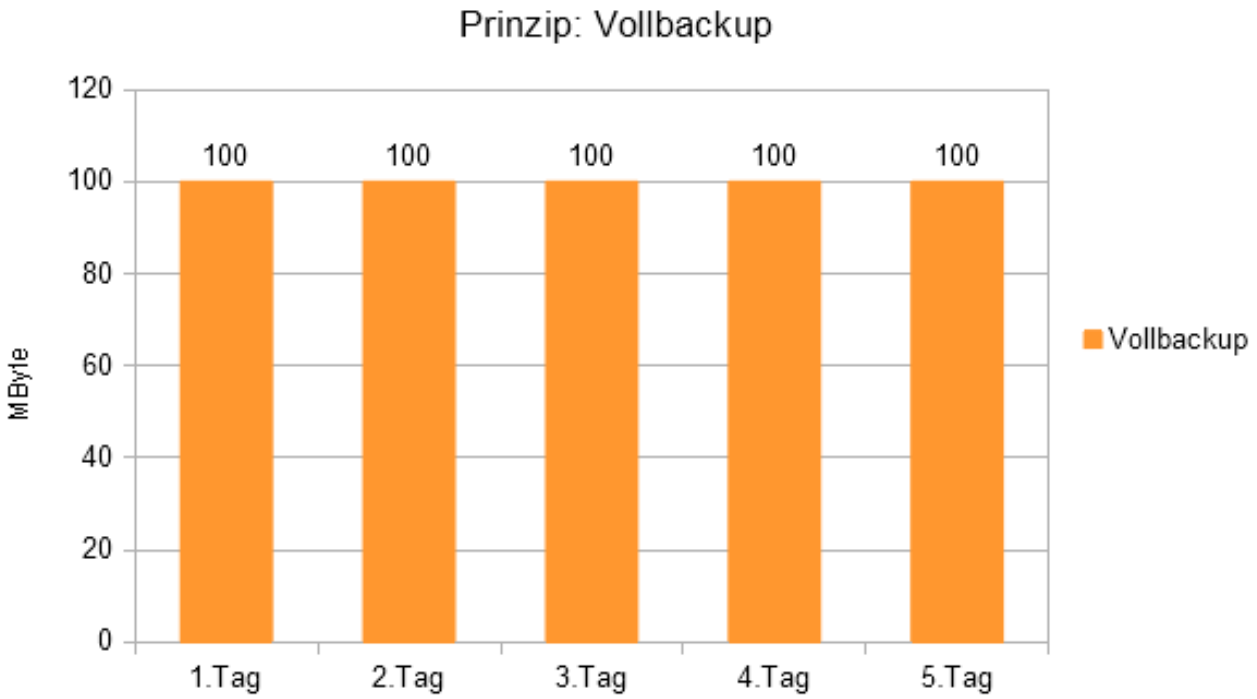
Heutzutage ist es kein Problem, den kompletten Datenbestand der Personalabteilung eines Unternehmens auf einem Datenträger im Zigarettenschachtelformat unterzubringen.
Oder Datenträger mit Sozialversicherungsdaten einer ganzen Stadt werden auf dem Transport verloren.
Die einzige Möglichkeit, den Verlust oder Missbrauch einzugrenzen:
Starke Verschlüsselung der gesicherten Daten!

Backup-Methoden

Es gibt verschiedene Methoden, wie man eine Datensicherung angehen kann. Einige davon werden nachfolgend erläutert.

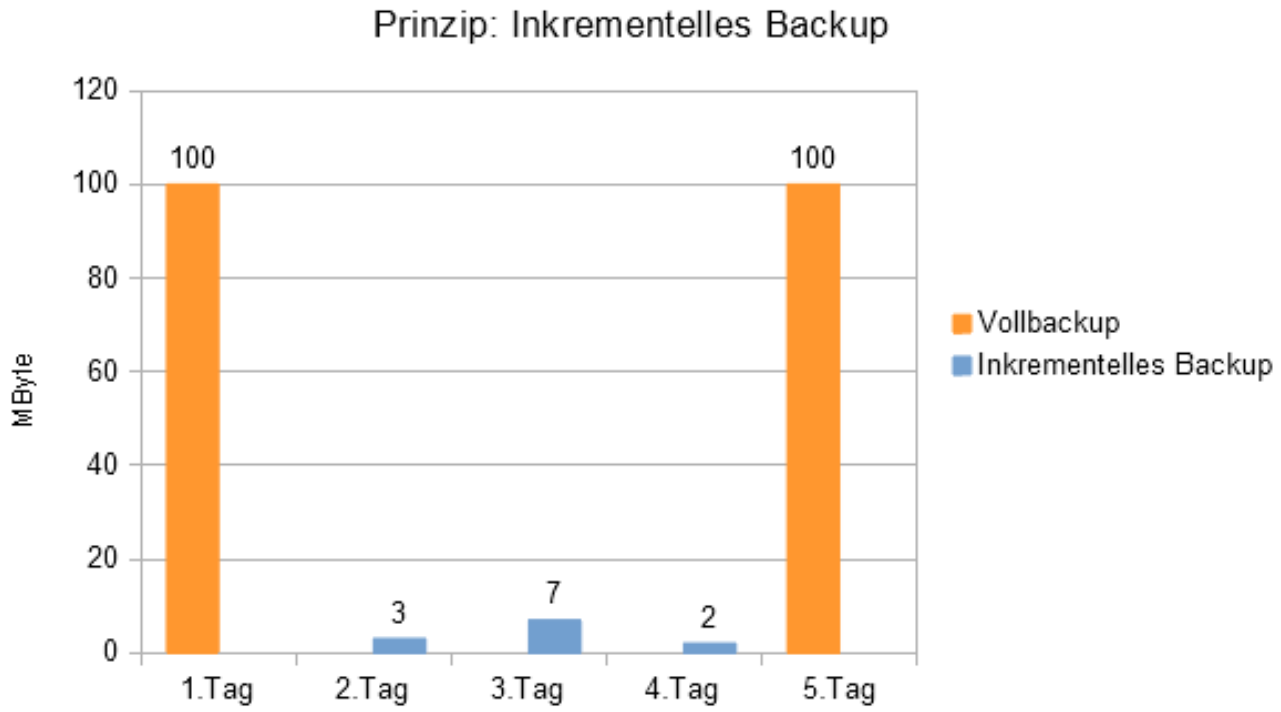
Vollständiges Backup

Eine vollständige Datensicherung bezeichnet die Sicherung aller Daten, unabhängig vom Datum ihrer letzten Sicherung.



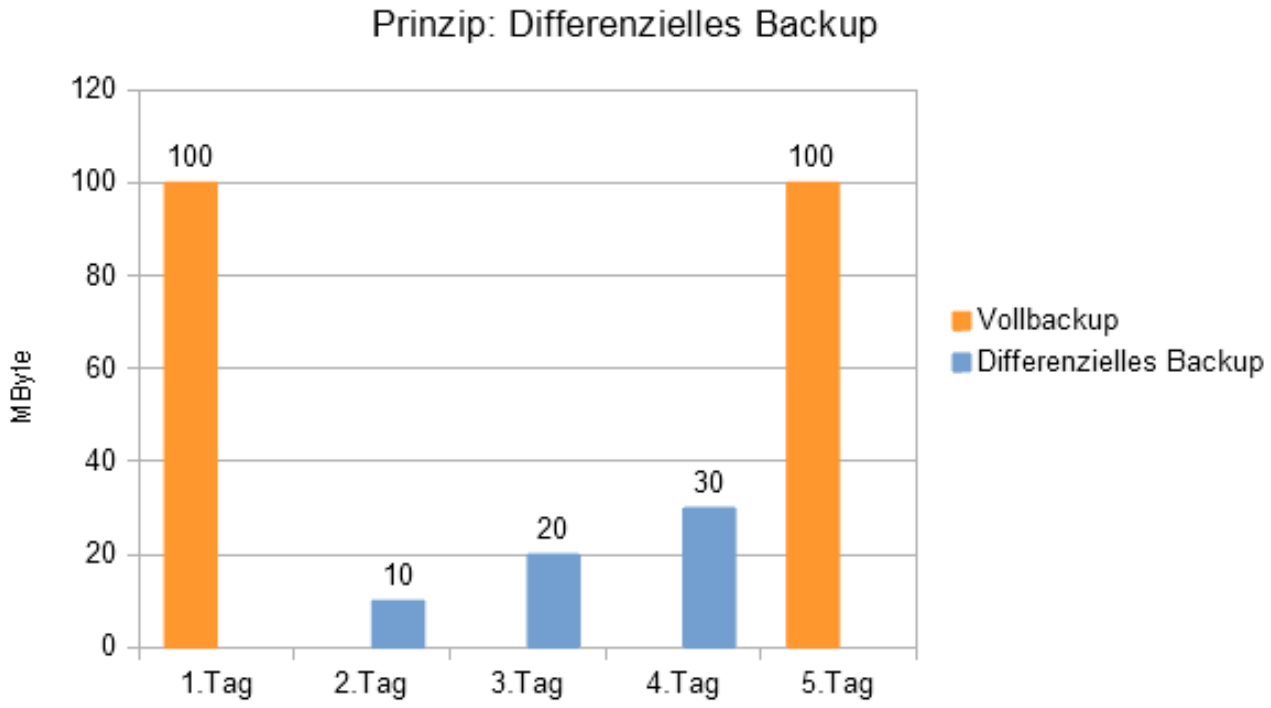
Inkrementelles Backup

Bei der inkrementellen Sicherung werden immer nur die Dateien gespeichert, die seit der letzten inkrementellen Sicherung oder (bei der ersten inkrementellen Sicherung) seit der letzten Komplettsicherung geändert wurden oder neu hinzugekommen sind.
Es wird also immer auf der letzten inkrementellen Sicherung aufgesetzt.
Die Vorteile sind eine geringere zu sichernde Datenmenge und schnellere Datensicherung.
Der Nachteil ist ein relativ großer Aufwand bei der Wiederherstellung von Daten, da mehrere Sicherungen hintereinander eingespielt werden müssen.
Für die Rücksicherung benötigt man also das Vollbackup sowie alle inkrementellen Backups bis zum Zeitpunkt des Ausfalls.



Differenzielle Sicherung

Bei der sogenannten differenziellen Sicherung werden alle Daten, die seit der letzten Komplettsicherung geändert wurden oder neu hinzugekommen sind, gespeichert.
Es wird also immer wieder auf der letzten Komplettsicherung aufgesetzt, wobei gegenüber einer neuen Vollsicherung Speicherplatz und Zeit gespart werden kann.
Für die Rücksicherung benötigt man das Vollbackup sowie die letzte differentielle Sicherung.



Fortschreitende inkrementelle Sicherung

Es werden ausschließlich und beliebig oft nur veränderte oder neu hinzugekommene Dateien gesichert
Eine vollständige Sicherung wird nur implizit im Rahmen der Einrichtung des Sicherungsbetriebs gemacht
Beim Wiederherstellen bietet das Datensicherungsprogramm virtuell zusammengesetzte Vollsicherungen zur Auswahl an
Das verbindet die Vorteile der Vollsicherung (einfache Handhabung) mit inkrementeller Sicherung (kleine Datenmengen)
Ein Nachteil ist die Komplexität des Werkzeugs, da es sich um ein datenbankbasiertes Datensicherungsprogramm handelt.

Beispiele:

Die Wiederherstellungskonsole von Windows und TimeShift in Linux Mint

Methode: Großvater – Vater – Sohn

Eine Großvater-Vater-Sohn Datensicherung, auch Generationenprinzip genannt, ist ein altbekanntes Verfahren zur Datensicherung.
Dabei wird von dem Datenbestand ständig ein dreifaches Backup verschiedenen Alters (Großvater, Vater, Sohn) von einem Datenträger gemacht.
Veränderungen und Verluste von Daten können somit rekonstruiert werden.
Sind die Sohn-Daten beschädigt, werden sie aus den Vater-Daten wieder erzeugt und die Vater-Daten gegebenenfalls aus den Großvater-Daten.
Siehe auch: https://de.wikipedia.org/wiki/Generationenprinzip

Methode: 3-2-1-Regel

Ein wichtiger Begriff im Zusammenhang mit der Datensicherungsstrategie ist die 3-2-1-Backup-Regel. Diese goldene Regel der Datensicherung besagt, dass es zu sämtlichen Daten mindestens drei (aktuelle) Versionen bzw. Kopien geben sollte. Wobei eine der Versionen das eigentliche „Original" der Daten ist, mit dem der Benutzer arbeitet. Zusätzlich zu den Originaldaten sollte es also zwei Kopien geben, die auf zwei unterschiedlichen Medientypen erfolgen und von denen mindestens eines an einem Ort außerhalb des Arbeitsumfeldes aufbewahrt wird.
Definition: Drei Backups, zwei Medientypen, eines extern aufbewahrt

Der alternative Aufbewahrungsort, als fester Bestandteil der 3-2-1-Regel, sichert beim Ausfall des „Primärstandortes" den Benutzer zusätzlich ab. Ein Brand, eine unerwartete Überschwemmung, wie sie im vergangenen Jahr auftrat – all das kann Anlass für einen Datenverlust sein.

Dass die Daten auf zwei unterschiedlichen Medientypen (also beispielsweise in der Cloud, auf Festplatte, SSD-Speicher, Magnetband oder auch auf optischen Datenträgern wie DVDs oder Blu-Rays) abgelegt werden sollten, hat mit der Wahrscheinlichkeit eines Ausfalls zu tun.
Mit jeder Backup-Kopie sinkt das Ausfallrisiko enorm: Mit der 3-2-1-Regel liegt das Risiko eines Datenverlusts bei 1:10.000.
Im Vergleich dazu: Bei nur einer einzigen Version beträgt dieses Risiko 1:100.
Sogar im Worst-Case-Szenario, in dem zwei Speichermedien parallel ausfallen, garantiert die dritte Kopie die Datensicherheit.

Siehe auch: https://de.wikipedia.org/wiki/Toleranzmanagement#Die_3-2-1-Regel

Backup-Medien

Zumindest einen kurzen Gedanken sollte man auch an das zu wählende Medium für eine Datensicherung verschwenden.
Immerhin hängt daran die Zukunft einer eventuell notwendigen Rücksicherung.

CDs, DVDs, BluRays

Es gibt verschiedene Studien, welche zusammengenommen nicht sehr hilfreiche Werte nennen: Von wenigen Monaten bis zu mehreren Jahren...

Die Qualität der Sicherung hängt vom Brenner, Rohling und lesendem Laufwerk ab.
Wichtig bei der Verwendung dieser Medien sind regelmäßige Tests bzw. das gelegentliche Umkopieren.

USB-Sticks, Festplatten, Bänder

USB-Sticks sind relativ sicher, die Haltbarkeit ist durch die Natur des Mediums begrenzt. Bei Defekt gibt es nur sehr eingeschränkte Möglichkeiten der Wiederherstellung.
USB-Festplatten sind sehr sicher als Backup-Ziel.
Genau wie (Magnet-) Bänder, welche jedoch im Privatbereich überhaupt nicht verbreitet sind, beziehungsweise nach kurzer Zeit schon wieder verschwunden waren (Ditto, 1996).

SSDs

Mittlerweile sind SSD-Speicher (extern/intern) auch für den Normalgebrauch recht erschwinglich (z.B. 1TB ab ca. 60€, Stand: 17.06.23).
SSDs sind sehr sicher, die Haltbarkeit der Daten jedoch nicht ganz so.

Lagerung von Backup-Medien

Auch für die Lagerung des entsprechenden Mediums gibt es einige Dinge zu beachten. Zum Beispiel die USB-Sicherungsplatte nicht am Rechner angeschlossen lassen, Bänder bei konstanter Temperatur und trocken lagern (möglichst in einem anderen Brandabschnitt), oder in einem feuerfesten Tresor, bzw. überhaupt einem abgeschlossenen Tresor.
Man könnte eine externe Sicherheitskopie auch in einem Bankschließfach lagern. Diese kosten etwa 30,00€ im Jahr.
Billiger fährt man mit der Lagerung bei einem Bekannten, und ein Grund auf ein Bier vorbei zu kommen...

Lifecycle-Management

Wie sieht es aus technischer Sicht mit der Lesbarkeit des gewählten Backup-Mediums aus?
Vor 8 Jahren waren noch Zip- und LS120-Laufwerke verfügbar...
Auch interessant: Optische Laufwerke werden immer seltener...
Vorschlag:
Neben dem regelmäßigen Umkopieren sollte auch ein Medienwechsel geprüft werden. Eventuell ist etwas Neues auf dem Vormarsch.

Fehler bzw. Missverständnisse

Gar keine Datensicherung machen

Der offensichtlichste Fehler bei Datensicherungen ist, dieses Thema komplett zu vernachlässigen oder zu ignorieren.
Fertigt man nie Backups an, sind die Daten bei einem (Ransomware-)Virus-Angriff, einem Hardwareschaden oder bei Diebstahl des Geräts ganz oder teilweise weg.

Zu wenige oder unwichtige Daten sichern

Ein Backup sollte Dateien enthalten, die für einen von hohem Wert sind.
Um das Prozedere schneller durchzuführen, ist mancher Nutzer geneigt, nur das absolut Nötige zu berücksichtigen: also Dateien, deren Verlust einen finanziellen, existenziellen oder enormen emotionalen Schaden verursachen würde (Steuererklärungen, Familienfotos, ...). Doch auch Dateien, deren Verschwinden zwar nicht dramatisch, aber doch ärgerlich ist, gehören in ein Backup. Hier wären z.B. Lesezeichen oder Kontakte im Mailprogramm zu nennen.
Man sollte aber auch nicht zu viel sichern: Riesige Datenmengen verlängern die Backup-Dauer und kosten Zeit bei der Wiederherstellung.
Denn man rekonstruiert entweder alles oder wählt mühsam mit Häkchen, welche Dateien zu extrahieren sind.
Unnötig ist es, Betriebssystem-eigene Dateien zu sichern. Diese sind über ein Backup nicht schützenswert, da man bei einer Neuinstallation ohnehin wieder an diese Dateien gelangt. Ausnahmen bilden hier in speziellen Fällen die oben erwähnten „Dot-Dateien“ in GNU/Linux.
Temporäre Dateien sowie Programme, die man stets in der neuesten Version nutzen möchte, braucht man ebenso wenig in ein Backup aufzunehmen. Diese können nach einer Neuinstallation des Betriebssystems in den aktuellsten Versionen auf Wunsch erneut installiert werden. Es sei denn, man legt Wert auf eine bestimmte ältere Version, die die großen Download-Portale in der Regel nicht unbegrenzt lange vorrätig halten. Portable Anwendungen lassen sich wiederum in Form ihrer (entpackten) Dateien sichern, da bei ihnen eine Installation unnötig ist.

Zu selten sichern

Sicherlich bearbeitet man einige Dateien besonders oft, etwa Textdokumente. Beispielsweise wöchentlich eine Sicherung davon vorzunehmen, könnte zu wenig sein: Geht die System-SSD kaputt, auf der diese Dateien liegen, hätte man bei täglicher Bearbeitung im Beispiel nur sieben Tage alte Kopien. Am besten passt man das Intervall des Backups an die eigenen PC-Aktivitäten an – eine Automatisierung erweist sich hier als sinnvoll.
Gängige Backup-Tools bieten in der Regel einen Zeitplaner.
Darin gibt man einen oder mehrere Ordner an: Je nach Verzeichnis erfolgt die Duplizierung in einem bestimmten Zyklus (abhängig davon, welche Relevanz man den Ordnerinhalten beimisst).

Sichern in proprietären Formaten

Datensicherungs-Programme kopieren Dateien oft nicht in Reinform, sondern in speziellen Formaten – erkennbar an den Backup-Dateiendungen.
Es findet dabei quasi eine Umwandlung statt. Auf lange Sicht ist das Sichern in proprietären Formaten unklug: Wenn der Backup-Anbieter pleitegeht, bringt er keine neue Version seiner Software mehr heraus. Die vorliegende alte Backup-Programmversion könnte aber mit einem künftig erscheinenden Betriebssystem inkompatibel sein. User begeben sich mit proprietären Formaten in eine Abhängigkeit, zumal ein Konkurrenz-Backup-Tool die Dateien aus solchen Sicherungsarchiven wohl nicht mehr herausbekommt.
Tipp: Man sichert wichtige Dateien in Reinform, also ohne Änderung deren Formate. Dies geschieht durch einfaches, klassisches Kopieren von A nach B. Eventuell packt man sie für eine Verkleinerung. Das ZIP-Format erlaubt beispielsweise auch eine Verschlüsselung.

Sichern auf Medien mit ungewisser Zukunft

Vor vielen Jahren waren Notebooks und Desktop-PCs mit optischem CD- und DVD-Laufwerken üblich, heute sind sie nicht mehr allzu verbreitet. Dieses Beispiel unterstreicht, dass man nicht auf das falsche Sicherungsmedium setzen sollte: Für eines, das heute noch aktuell ist, gibt es in einigen Jahren womöglich keine Lesegeräte mehr. Fehlt in einem PC oder Notebook ein Laufwerk für optische Medien, kann man immerhin (noch) mit einem externen USB-Pendant arbeiten.

Bei Disketten ist die Lage mit dem Auslesen mittlerweile schwieriger. Man sollte auch auf das verwendete Dateisystem achten: Zu exotisch sollte es nicht sein, man formatiert den Sicherungsdatenträger etwa mit NTFS oder ext4 (statt zum Beispiel mit exFAT).
Neben einem Datensicherungsmedium und einem darauf befindlichen Backup sollte zu einer guten Sicherungsausstattung ein Lesegerät gehören – und zwar ein externes. Beide Hardwareteile lassen sich an einem sicheren Ort (wie einem Tresor) deponieren. Man sollte allerdings bedenken, dass selbst das nicht 100-prozentig zukunftssicher sein muss: Zwar schließt man ein externes USB-

Auslesegerät an einen künftigen PC an, doch ob es hierfür noch einen Treiber gibt, der mit dem in Zukunft genutzten Betriebssystem kompatibel ist, steht in den Sternen. Auch ob klassische USB-(A-)Buchsen eine Zukunft haben, ist fraglich; der verdrehsichere USB-C-Stecker mit seiner davon abweichenden Bauform ist seit längerem im Aufwind.

Damit sich Daten in einigen Jahrzehnten noch auslesen lassen, sollten Paranoiker am besten auch einen alten Computer aufbewahren (samt darauf installiertem „Betriebssystem von damals“; anschluss- und treibertechnisch sollte so der Backup-Zugriff gewährleistet sein). Möchte man künftig ein altes Speichermedium an einem neuen Rechner betreiben, findet man dafür online eventuell einen Hardware-Adapter.

Mit jeder „Heft-DVD“ das Backup-Programm wechseln

In Computerzeitschriften finden sich auf der (Online-)Heft-CD oder DVD immer mal wieder Backup-Programme. Manchmal ist das kostenfreie Software (Freeware/Open Source) in anderen Fällen handelt es sich um sonst kostenpflichtige Produkte, die hier in einer (leicht veralteten) Gratis-Version bereitstehen. Man sollte dem Drang wiederstehen, die Sicherungssoftware quasi ständig zu wechseln.
Andernfalls müsste man Sicherungen oft von Neuem anlegen, da meist die eine Software das Format der anderen nicht unterstützt – der zeitliche Sicherungsaufwand nimmt so unnötig zu.

Datensicherung ohne Virenschutz (Windows)

Wer regelmäßig Datensicherungen anlegt, kommt womöglich auf die Idee, ohne einen Virenschutz zu arbeiten. Letzterer ist ohnehin als Systembremse verschrien. Dies erfolgt beispielsweise nach dem Motto: Wenn ein Schädling auf den PC gelangt, ist mir das herzlich egal – weil ohnehin alle zerstörten Dateien aus einer Sicherung rettbar sind. Fakt ist aber, dass Virenschutz und Backup einander nicht ersetzen, sondern beide wichtig sind; sie ergänzen sich und sind Teil einer ganzheitlichen Sicherungsstrategie.

Schadprogramme greifen womöglich auf Backups zu: Bei auf der internen Platte abgelegten Backups gelingt das leicht. Außerdem attackiert manche Malware Inhalte, die auf verbundenen externen Sicherungsmedien liegen: Es genügt bereits, wenn ein externes Laufwerk nach dem Backup nicht vom PC getrennt wird. Doch selbst wenn Schädlinge die Datensicherungen nicht im Zugriff haben: Der Verzicht auf einen Virenschutz öffnet Erpressern Tür und Tor. So könnten sie sensible Dateien vom PC abgreifen und „Schutzgeld“ verlangen, wenn sie diese nicht an andere Menschen weiterleiten sollen.
Der Fachbegriff dafür lautet Ranshameware (das englische „shame“ steht für Scham, „ware“ kürzt Software ab). Das ist eine neue Form von Ransomware.

Ein aktuell gehaltener Virenschutz hätte die verantwortliche Malware-Infektion abwenden können, ein Backup leistet das nicht. Wobei verschiedene proprietäre Backup-Systeme mittlerweile auch eine Virenschutz-Funktion enthalten.

Verseuchtes Windows sichern

Eins-zu-eins-Kopien von Dateien erlauben eine simple Wiederherstellung, mit Images (oder Abbildern) hingegen sichert man wahlweise Dateien oder sogar ganze Betriebssysteme. Ein (mutmaßlich) verseuchtes Windows sollte jedoch nicht in einen Sicherungsdatensatz geschrieben werden: Denn nach der Wiederherstellung mithilfe eines Bootmediums hätte man wieder ein potenziell unsicheres System. Ebenso sollte man kein Windows vollständig sichern, das unter Datenmüll leidet. Zuvor sollte man es manuell oder mit Tuning-Tools aufräumen.
Eine Ausnahme beim Sichern eines verseuchten Betriebssystems: Hat ein Verschlüsselungs-Trojaner zugeschlagen und gibt es kein Entschlüsselungs-Tool für die verlorenen Daten, bewahrt man eine Kopie des Systems auf, bis so ein Tool eventuell bereitsteht. Das wendet man dann auf diese Systemkopie an und dechiffriert so die befallenen Dateien.

Programmdateien sichern

Man sollte installierte Programme nicht in Form ihrer Dateien sichern, da diese nach dem Zurückspielen in ein frisches Windows wohl nicht mehr funktionsfähig wären. Denn zu ihnen gehören auch Registry-Einträge und eventuelle Konfigurationsdateien, die man bei einem reinen Datei-Backup nicht erwischt. Stattdessen sichert man eventuell vorhandene Installationsdateien dieser Anwendungen und installiert sie darüber neu.
Eine Ausnahme bilden portable Applikationen: Die kommen ohne Registry-Einträge aus und liegen rein in Dateiform vor. Auch ausschließlich Verknüpfungen sollte man nicht sichern: Diese verweisen nur auf ausführbare Dateien (EXE-/Batch-Dateien) und sind keine vollwertige Software (was schon anhand des bytegroßen Umfangs erkennbar ist).

Backup auf dem gleichen Speichermedium

Dateien sollten niemals auf dem Laufwerk, auf dem sie liegen gesichert werden: Eine Duplizierung auf eine Extra-Partition ist zwar gut, eine Ergänzung und noch dazu besser ist jedoch das Anlegen von Kopien auf einem externen Speichermedium. Das Sichern auf demselben Speicher ist nicht optimal, weil ein Defekt oder ein Diebstahl der Platte zur Folge hat, dass die Dateien weg sind – beide Gefahrenquellen betreffen immer alle Partitionen.
Ein weiterer Tipp: Man sollte auch Sicherungen vom eigentlichen Backup-Speicher anfertigen (Backup des Backups), da auch sie kaputtgehen könnten.

Sicherungsdatenträger angeschlossen lassen

Da Schädlinge wie Verschlüsselungs-Trojaner mitunter externe Backup-Medien befallen, sollte man daran denken, eine Sicherungsplatte oder einen USB-Stick nach erledigtem Sicherungsauftrag zu trennen.

Backup-Medien nur an einem Ort aufbewahren

Brennt es oder gibt es einen Wasserschaden, ist es gut, wenn sich Backup-Medien außer Haus befinden. So könnte man beispielsweise zwei Backup-Festplatten verwenden und lagert die zweite bei einem Verwandten/Bekannten/Nachbarn (sogenannte Georedundanz bzw. 3-2-1-Regel).

Tipp:

Selbst wenn man der anderen Person vertraut: Verschlüsselt man seine Sicherung, braucht man kein mulmiges Gefühl zu haben, wenn andernorts beispielsweise ein Einbrecher den USB-Datenträger stiehlt.

Passwort des verschlüsselten Backups vergessen

Gute Backup-Programme bieten an, zu sichernde Dateien zu verschlüsseln. Einher geht damit in der Regel die Wahl eines Passworts und teils eines Chiffrier-Algorithmus. Von Letzterem gibt es verschiedene Bit-Stärken. Sollte man sein Passwort vergessen, sperrt man sich selbst aus: Zwar befinden sich die gesicherten Dateien noch als Originale unverschlüsselt auf der PC-Platte. Doch wenn diese abraucht oder Daten aus anderen Gründen verloren gehen, ist man auf das Backup angewiesen – und könnte es ohne das Passwort allenfalls mit Bruce-Force-Knackmethoden entschlüsseln. Selbst Datenrettungslabore dürften in solchen Fällen meist machtlos sein.

Synchronisieren statt Backup

Manche Menschen verwenden die Begriffe Backup und Synchronisieren synonym, penibel betrachtet ist das aber nicht dasselbe: So sichert man bei einem Backup Daten, und beim Synchronisieren scheint ja dasselbe zu passieren.
Der Unterschied ist, dass letztgenannte Methode noch weitere Spielarten kennt: Sie hievt nicht nur Dateien von A (etwa einer SSD) nach B (etwa eine Sicherungs-Festplatte), sondern auch von B nach A.
Es kann eine Synchronisierung von einer Richtung in die andere oder sogar eine Zwei-Wege-Synchronisierung in einem Rutsch stattfinden. Nun ist das Sichern im Beispiel von einer HDD auf eine SSD auch ein Backup. Nur löscht eine Synchronisation je nach Einstellung der genutzten Software dabei womöglich auch Dateien: Fehlt in einem (Wurzel-)Verzeichnis der ausgewählten Sync-Orte eine Datei, kann eine Syncing-Software die Datei am anderen Ort entfernen, sollte es dort abgelegt sein; so sind die Inhalte zwar „synchron“, doch vernichtet der Abgleich bisweilen ungewollt Daten.

Tipp:

Man nutzt eine Synchronisations-Software zusätzlich zu einem Backup-Tool.

Wenn man nur synchronisieren will, um Daten zu sichern, stellt man sicher, dass keine Datenlöschung stattfindet; hierfür kontrolliert man die Konfiguration der jeweiligen Sync-Lösung (und testet das Prozedere mit Dummy-Dateien, bevor man es auf echte Dateien anwendet).

Backup nicht verifizieren

Gute Datensicherungs-Software bietet eine Funktion, um angelegte Backups zu verifizieren. Damit prüfet man sie auf Datenfehler. Wenn eine Sicherung beschädigt ist, erkennt und meldet dies das Sicherungsprogramm idealerweise. Angenommen, man ändert mit einem Hex-Editor auch nur ein Bit einer Image-Datei, würde zum Beispiel Aomei Backupper Pro darauf reagieren und die Verifikation scheitert. Man sollte die Wiederherstellbarkeit zusätzlich in der Praxis testen: Nur so hat man Gewissheit.

Backup auf SSDs

Eine SSD als Datenlager für Backups einzusetzen, ist möglich, aber aus Preis-Leistungs-Sicht nicht ideal; Festplatten bieten mehr Kapazität für das gleiche oder weniger Geld. Wem das Preis-Leistungs-Verhältnis bei SSDs egal ist, der verwendet seinen Speicher entsprechend für Sicherungen. Da es den Flash-Speichern an festplattenüblichen mechanischen Bauteilen mangelt, könnten Daten auf SSDs sogar recht sicher lagern. Das gilt vor allem, wenn das Speichern allzu großer Datenmengen ausbleibt; diese sorgen nämlich für Verschleiß.
Das perfekte Backup-Medium stellen SSDs allerdings trotz theoretischer Vorteile nicht dar, da ihnen ohne Stromzufuhr Datenverlust droht.
Bei einer Raumtemperatur von 30 Grad halten SSDs bei Lagerung gemäß JEDEC-Spezifikation die Daten zumindest ein Jahr (sogenannte Retentions-Zeit). Für den professionellen Einsatz ausgelegte Enterprise-SSDs sind keine bessere Wahl: JEDEC spezifiziert für sie nur ein dreimonatiges Beibehalten der gespeicherten Daten ohne Stromzufuhr (bei 40 Grad Raumtemperatur).

Dateibackup (Werkzeuge und Anwendungen)

Wenn es „nur“ um einzelne Dateien geht und nicht um das Gesamtsystem, kommt man mit einem einfachen Dateibackup gut klar.

Werkzeuge zur Dateisicherung (Desktop, Notebook)

Programm	Kompatibilität	Typ	Website
Duplicati	GNU/Linux	Anwendung	https://www.duplicati.com/
FreeFileSync	GNU/Linux Windows	Anwendung	https://freefilesync.org/
TrayBackup	GNU/Linux	Anwendung	https://www.traybackup.de/
Mailstore Home	Windows	Anwendung	https://www.mailstore.com/de/produkte/mailstore-home/

Werkzeuge zur Dateisicherung (Smartphones, Tablets)

Die immer größer werdenden Speicher unserer kleinen Begleiter verführen dazu, Unmengen an Dateien (vorzugsweise Bilder) auf ihnen zu lagern. Diese werden bei Backup-Strategien oft vergessen oder zumindest vernachlässigt.

Programm	Kompatibilität	Typ	Website
MyPhoneExplorer	Windows	Anwendung	https://www.fjsoft.at/de/
Titanium Backup	Android	App	Play Store
NeoBackup	Android	App	F-Droid

Und natürlich kann man auch den Clouds der großen Anbieter „entkommen“, wenn man sich eine eigene Wolke Zuhause hält.
Beispielsweise in Form eines RaspberryPi und der Open Source Lösung „NextCloud“.
Damit synchronisiert man seine Smartphone-Daten auf den eigenen (NextCloud)Server.
Ganz nach dem Motto: „Meine Daten gehören mir und ich habe auch die Hoheit darüber.“

Systembackup (Werkzeuge und Anwendungen)

Unter einem Systembackup oder Image versteht man die Komplettsicherung des installierten Betriebssystems.

Werkzeuge zur Image- oder Abbilderstellung

	Kompatibilität	Typ	Website
Clonezilla	GNU/Linux	Live-System	https://draugeros.org/go/
RedoRescue	GNU/Linux	Live-System	https://batocera.org/
Ping	GNU/Linux	Live-System	http://www.lakka.tv/
TimeShift	GNU/Linux	Anwendung	https://github.com/linuxmint/timeshift

Eigene Notizen