DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 890 729 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Anleitung Backup-Todsünden – so machen Sie es besser

Diese 20 Fallen sollten Sie vermeiden – so machen Sie es besser

Zu wenige Dateien zu sichern verbietet sich, andererseits sollte das Wiederherstellen zu vieler (Registry-)Daten tabu sein. Wir stellen Ihnen teils ungeahnte Backup-No-Gos vor.
Um den wichtigsten Aspekt dieses Artikels vorwegzunehmen: Der größte Fehler bei der Datensicherung ist, sie aus Bequemlichkeit gar nicht erst zu machen. Kommt es zu einem Verlust wichtiger Dateien, haben Sie dann je nach Art des Verschwindens kaum oder keine Wiederherstellungsoptionen. Darum sei der häufig gegebene Rat an dieser Stelle wiederholt: Sichern Sie Ihre Daten – am besten regelmäßig, eventuell verschlüsselt und/oder komprimiert.
Nun ist diese Weisheit ebenso langweilig wie das Thema Datensicherung an sich: Wer bislang noch keine wichtigen PC-Inhalte verloren hat, muss womöglich erst am eigenen Leib erfahren, was es heißt, dass sie außerhalb des Zugriffs sind – um sich aufzuraffen, es künftig besser zu machen und Backups zu fahren.
Kompliziert muss das nicht sein, denn Automatisierungen übernehmen einen guten Teil der Arbeit. Jetzt sind Sie von Backups womöglich noch immer nicht überzeugt: Daher finden Sie an dieser Stelle "Negativ-Berichterstattung": Im Folgenden lesen Sie, wie es nicht geht. Denn oft finden Leserinnen und Leser – etwa unserer Website – Negatives interessanter als positiv Dargestelltes. Von diesen No-Go-Überschriften leiten wir Handlungsempfehlungen ab, die Sie befähigen, ordentlich zu sichern.
Vielleicht gewinnt das Thema so für Sie an Spannung – und Ihr Datenbestand (nach Lesen der Lektüre) hoffentlich an Schutz. Vorneweg ein Hinweis zur Windows-Systemwiederherstellung: Die ist seit Windows 10 werkseitig deaktiviert, Sie sollten diese Funktion namens Computerschutz einschalten. Das Feature ersetzt keine Backups, ist aber eine sinnvolle Ergänzung.
Empfehlenswerte Backup-Software für Windows:
» Ashampoo Backup Pro 14 – leistungsfähige, dabei noch schlanke Vollversion
» Aomei Backupper – Freeware-Sicherungsprogramm (ohne Verschlüsselung)
» Aomei Backupper Pro – Ein-Jahres-Gratis-Version (mit Verschlüsselung)
» Acronis Cyber Protect Home Office – Backup-Suite mit Virenschutz
» CDBurnerXP – brennt Dateien auf CD-/DVD-Rohlinge
» LCISOCreator – sichert CDs/DVDs auf dem PC im ISO-Format
» Reboot Restore Rx – stellt Windows bei jedem Neustart wieder her
» Ashampoo Backup 2021 – ähnlich Ashampoo Backup Pro 14, legt aber nur Images an
Ashampoo Backup Pro 14 – Kostenlose Vollversion (Top-Empfehlung)
Download

Datensicherung nicht anlegen

Der offensichtlichste Fehler bei Datensicherungen ist, das Thema komplett zu vernachlässigen. Sollten Sie nie Backups anfertigen, sind Ihre Daten bei einem (Ransomware-)Virus-Angriff, einem Hardwareschaden oder bei Diebstahl des Geräts ganz oder teilweise weg.
Zwar sichert Windows mit der Systemwiederherstellung immer mal wieder etwas im Hintergrund, doch betrifft das nur den Systemzustand (Registry, Einstellungen, Programme) – und dank Schattenkopien einige (bearbeitete) Dateien, wobei Sie auf die Berücksichtigung

letzterer keinen Einfluss haben. Es gilt: Selbst ein schlecht gemachtes Backup ist besser als keines.

Zu wenige oder unwichtige Daten sichern

Ein Backup sollte Dateien enthalten, die für Sie 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. Sichern Sie aber nicht zu viel: Riesige Datenmengen verlängern die Backup-Dauer und kosten Zeit bei der Wiederherstellung. Denn Sie rekonstruieren entweder alles oder wählen mühsam mit Häkchen, welche Files zu extrahieren sind.
Unnötig ist es, Windows-eigene Dateien zu sichern. Diese sind über ein Backup nicht schützenswert, da Sie an die Dateien ohnehin wieder gelangen, wenn Sie Ihr System neu installieren. Temporäre Dateien sowie Freeware-Programme, die Sie stets in der neuesten Version nutzen möchten, brauchen Sie ebenso wenig in ein Backup aufzunehmen. Denn Sie laden die Installationsdateien nach einer Windows-Neuinstallation in den aktuellsten Versionen auf Wunsch erneut herunter. Es sei denn, Sie legen 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.

Die besten kostenlosen Backup-Programme

Zu selten sichern

Sicherlich bearbeiten Sie einige Ihrer Dateien besonders oft, etwa Textdokumente. Beispielsweise wöchentlich eine Sicherung davon vorzunehmen, könnte zu wenig sein: Geht Ihre System-SSD kaputt, auf der Ihre Dateien liegen, hätten Sie bei täglicher Bearbeitung im

Beispiel nur sieben Tage alte Kopien. Am besten passen Sie das Intervall Ihrer Backups an Ihre PC-Aktivitäten an – eine Automatisierung erweist sich hier als sinnvoll.
Gängige Backup-Tools bieten in der Regel einen Zeitplaner. Darin geben Sie einen oder mehrere Ordner an: Je nach Verzeichnis erfolgt die Duplizierung in einem bestimmten Zyklus (abhängig davon, welche Relevanz Sie den Ordnerinhalten beimessen).

Sichern in proprietären / kaum verbreiteten Backup-Formaten

Datensicherungs-Programme duplizieren 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 Ihr Backup-Anbieter pleitegeht, bringt er keine neue Version seiner Software mehr heraus. Die Ihnen vorliegende alte Backup-Programmversion könnte aber mit einem künftig erscheinenden Windows 10 oder Windows 11 inkompatibel sein. Microsoft bringt mittlerweile jährlich neue Großversionen von Windows 10 heraus, die Major-Releases von Windows 11 erscheinen von Anfang an im Jahrestakt. User begeben sich mit proprietären Formaten in eine Abhängigkeit, zumal ein Konkurrenz-Backup-Tool Ihre Dateien aus solchen Sicherungsarchiven wohl nicht mehr herausbekommt.
Tipp: Sichern Sie wichtige Dateien in Reinform, also ohne Änderung ihres Formats. Eventuell zippen Sie sie für eine Verkleinerung. Das ZIP-Format erlaubt auch eine Verschlüsselung: Der Windows-Zipper chiffriert zwar nicht, 7-Zip beherrscht das jedoch.

Sichern auf Medien mit ungewisser Zukunft

Vor vielen Jahren waren Notebooks mit optischem CD-/DVD-Laufwerk üblich, heute sind sie nicht mehr allzu verbreitet. Dieses Beispiel unterstreicht, dass Sie nicht auf das falsche Sicherungsmedium setzen sollten: 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, helfen Sie mit einem externen USB-Pendant nach.

Bei Disketten ist die Lage mit dem Auslesen mittlerweile schwieriger. Achten Sie auch auf das Dateisystem: Zu exotisch sollte es nicht sein, formatieren Sie Ihren Sicherungsdatenträger etwa mit NTFS (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. Beachten Sie, dass aber selbst das nicht 100-prozentig zukunftssicher sein muss: Zwar schließen Sie ein externes USB-Auslesegerät an einen künftigen PC an, doch ob es hierfür noch einen Treiber gibt, der mit Ihrem später 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 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). Möchten Sie künftig ein altes Speichermedium an einem neuen Rechner betreiben, finden Sie dafür online eventuell einen Adapter.

Dateien in kaum verbreiteten Formaten sichern

Einige Dateiformate fristen ein Nischendasein, bei denen es in Zukunft möglicherweise schwerfällt, geeignete Software zum Öffnen derart gespeicherter Files aufzutreiben. Solche Programme könnten aus dem Web verschwinden (etwa da deren Anbieter die Server-Gebühren nicht mehr bezahlen wollen) oder inkompatibel zum in x Jahren aktuellen (Microsoft-)Betriebssystem sein.
Sichern Sie Dateien am besten in bekannten Formaten, die einen hohen Verbreitungsgrad haben. Bei Bildern empfehlen sich JPEG, TIFF und RAW, bei Musik MP3 und WAV. Bei Dokumenten sollten Sie auf DOCX und PDF setzen, unpraktikabel sind Microsofts Nischen-PDF-Alternativen XPS und OXPS.

Alle 30 Tage das Backup-Tool wechseln

In Computerzeitschriften finden Sie auf der (Online-)Heft-CD/-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. Widerstehen Sie dem Drang, Ihre Sicherungssoftware quasi ständig zu wechseln.
Andernfalls müssten Sie Ihre Sicherungen oft von Neuem anlegen, da meist die eine Software das Format der anderen nicht unterstützt – der zeitliche Sicherungsaufwand nimmt so unnötig zu.

Daten sichern ja, Virenschutz nein

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 Sie ein externes Laufwerk nach dem Backup nicht vom PC getrennt haben. Doch selbst wenn Schädlinge Ihre Datensicherungen nicht im Zugriff haben: Der Verzicht auf einen Virenschutz öffnet Erpressern Tür und Tor. So könnten sie sensible Dateien von Ihrem 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 Acronis True Image (neuerdings: Cyber Protect Home Office) seit geraumer Zeit auch eine Virenschutz-Funktion enthält.
Wir testeten den Acronis-Schutz mit dem Eicar-Testvirus und einem echten Trojaner; beide Dateien erkannte die Automatik und verschob sie in Quarantäne. Wie sinnvoll solche Features sind und ob eine schlankere Backup-Lösung wie Ashampoo Backup Pro 14 nicht besser wäre, muss jeder für sich abwägen.

Verseuchtes Windows sichern

Eins-zu-eins-Kopien von Dateien erlauben eine simple Wiederherstellung, mit Images hingegen sichern Sie wahlweise Dateien oder sogar ganze Betriebssysteme. Ein (mutmaßlich) verseuchtes Windows sollten Sie jedoch nicht in einen Sicherungsdatensatz schreiben: Denn nach der Wiederherstellung mithilfe eines Bootmediums hätten Sie wieder ein potenziell unsicheres System. Ebenso sollten Sie kein Windows vollständig sichern, das unter Datenmüll leidet. Räumen Sie es zuvor manuell oder mit Tuning-Tools auf.
Eine Ausnahme beim Sichern eines verseuchten Betriebssystems: Hat ein Verschlüsselungs-Trojaner zugeschlagen und gibt es kein Entschlüsselungs-Tool für Ihre verlorenen Daten, bewahren Sie eine Kopie des Systems auf, bis so ein Tool bereitsteht. Das wenden Sie dann auf Ihre Systemkopie an und dechiffrieren so die befallenen Files.

Programmdateien stumpf sichern

Sichern Sie installierte Programme nicht in Form ihrer Dateien, andernfalls wären sie nach dem Kopieren in ein frisches Windows wohl nicht mehr funktionsfähig. Denn zu ihnen gehören auch Registry-Einträge, die Sie bei einem reinen Datei-Backup nicht erwischen. Sichern Sie stattdessen die Installationsdateien Ihrer Anwendungen und installieren Sie sie darüber neu. Eine Ausnahme bilden portable Applikationen: Die kommen ohne Registry-Einträge aus und liegen rein in Dateiform vor. Auch ausschließlich Verknüpfungen sollten Sie nicht sichern: Diese verweisen nur auf EXE-/Batch-Dateien und sind keine vollwertige Software (was schon anhand des bytegroßen Umfangs erkennbar ist).

Backup auf demselben Speicher

Sichern Sie Dateien nicht auf dem Laufwerk, auf dem sie liegen: 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 Ihre Files weg sind – beide Gefahrenquellen betreffen immer alle Partitionen.
Ein weiterer Tipp: Fertigen Sie Sicherungen von Backup-Speichern an, auch sie könnten kaputtgehen. Bequeme Backups sind am PC ebenso wie bei NAS-Netzwerkspeichern mit einem RAID möglich, das redundant Daten auf mehrere Festplatten kopiert.

Sicherungsmedium angeschlossen lassen

Da Schädlinge wie Verschlüsselungs-Trojaner mitunter externe Backup-Medien befallen, denken Sie daran, eine Sicherungsplatte oder einen USB-Stick nach erledigtem Sicherungsauftrag zu trennen. Ziehen Sie den Speicher ab oder klicken Sie auf "Hardware sicher entfernen" im Infobereich (Symbol neben der Windows-Uhr). Sicherer ist das physische Entfernen, bequemer das softwarebasierte via Mausklick. Wer es nerdig mag, der nutzt das portable sync.exe aus der Sysinternals Suite und trennt Sicherungslaufwerke darüber mittels Tastaturbefehl über die Kommandozeile.

Backup-Medien nur an einem Ort aufbewahren

Brennt es oder gibt es einen Wasserschaden, ist es gut, wenn sich Backup-Medien außer Haus befinden. Verwenden Sie etwa zwei Backup-Festplatten und lagern Sie die zweite bei einem Verwandten (Georedundanz, 3-2-1-Regel).
Selbst wenn Sie der anderen Person vertrauen: Verschlüsseln Sie Ihre Sicherung, brauchen Sie kein mulmiges Gefühl zu haben, wenn andernorts beispielsweise ein Einbrecher Ihren USB-Datenträger stiehlt.

Passwort von verschlüsseltem Backup 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. Sollten Sie Ihr Passwort vergessen, sperren Sie sich selbst aus: Zwar befinden sich Ihre gesicherten Dateien noch als Originale unverschlüsselt auf der PC-Platte. Doch wenn diese abraucht oder Daten aus anderen Gründen verloren gehen, sind Sie auf Ihr Backup angewiesen – und können es ohne das Passwort allenfalls mit Bruce-Force-Knackmethoden entschlüsseln. Selbst Datenrettungslabore dürften in solchen Fällen meist machtlos sein.

Windows-10-/-11-eigenes Windows-7-Backup nutzen

In der Systemsteuerung von Windows 10/11 gibt es einen Backup-Bereich namens "Sichern und Wiederherstellen (Windows 7)". Die Funktion sichert Dateien und erstellt Images. Berichten zufolge ist sie unzuverlässig. Greifen Sie lieber etwa zum Aomei Backupper (Freeware, siehe Aomei-Backupper-Testbericht).

Windows in die Cloud sichern

Manche Backup-Software sichert Daten in die Cloud und bietet an, auch Windows dort zu speichern. Sinnvoll erscheint das nicht: Der Gratis-Speicherplatz von Webdiensten reicht dafür meist nicht – sodass Sie bezahlen müssen. Günstiger: Kaufen Sie sich eine Backup-Festplatte und sichern Sie darauf Windows. Das geht zudem schneller, da die Übertragung per USB rasanter ist als per DSL-Upload. Wenn Sie Cloud-Backups anfertigen, verschlüsseln Sie sie vor dem Hochladen mit 7-Zip oder Boxcryptor.

Registry vollständig sichern

Sichern Sie die Windows-Registry (etwa per Registry-Editor) nicht komplett, sonst drohen nach der Wiederherstellung Probleme. Eine importiere ältere Registry (oder gar von einem fremden PC) passt meist nicht.
Wer die Registry sichern will, sollte Teilbereiche duplizieren und zurückspielen oder das ganze Betriebssystem als Image aufbewahren.

Synchronisieren statt klassischem Backup

Manche Menschen verwenden die Begriffe Backup und Synchronisieren synonym, penibel betrachtet ist das aber nicht dasselbe: So sichern Sie bei einem Backup Daten, wobei beim Synchronisieren dasselbe zu passieren scheint. 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 das File am anderen Ort entfernen, sollte es dort abgelegt sein; so sind die Inhalte zwar "synchron", doch vernichtet der Abgleich bisweilen ungewollt Daten.
Tipp: Nutzen Sie eine Synchronisations-Software zusätzlich zu einem Backup-Tool. Wenn Sie nur synchronisieren wollen, um Daten zu sichern, stellen Sie sicher, dass keine Datenlöschung stattfindet; hierfür kontrollieren Sie die Konfiguration Ihrer Sync-Lösung (und testen das Prozedere mit Dummy-Dateien, bevor Sie es auf Ihre echten Files anwenden).

Backup nicht verifizieren

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

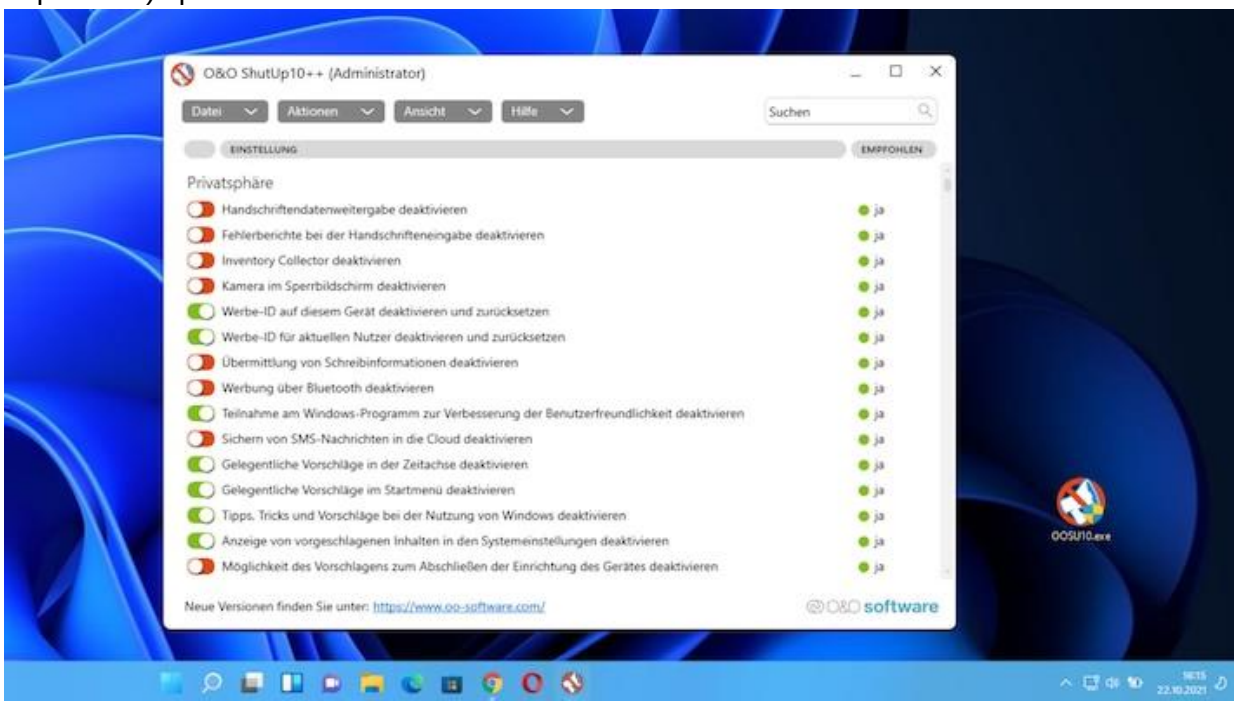
Backup auf SSDs und diese stromlos lagern

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 ihre Daten zumindest ein Jahr (sogenannte Retentions-Zeit; weitere Infos liefert das verlinkte JEDEC-PDF). 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).
» SSD-Todsünden: Vorsicht vor diesen 27 unverzeihlichen Fehlern

Die besten Datensicherungs-Programme

Womöglich empfinden Sie jegliche Programme, mit denen sich Daten sichern lassen, als nervig. Streng genommen sind jedoch nicht die Programme, sondern die Backups selbst lästig. Entsprechende Sicherungs-Hilfetools vereinfachen das Prozedere oft sogar. Lediglich schlecht gemachte Backup-Tools (wie Toucan) strapazieren mit nervtötender Bedienung das Gemüt mehr als nötig. Wenn Sie dem Genre Backup-Software dennoch keine Chance geben wollen, etwa um eine (minimale) PC-Belastung und eine Einarbeitung in die Bedienerführung

zu vermeiden, sollten Sie zumindest wichtige Dateien hin und wieder manuell sichern. Hierzu reicht der Windows Explorer aus. Für kleine Mengen eignet sich ein schnell angesteckter und schnell abgezogener, einfach mitnehmbarer sowie gut in der Schublade verstaubarer USB-Stick. Für größere Datenmengen kommen hochpreisige USB-Sticks infrage; ein besseres Preis-Leistungs-Verhältnis haben externe Festplatten. Schneller als diese, jedoch teurer (und wie USB-Sticks Flash-basiert) sind externe (USB-)SSDs.
Sind Sie nicht abgeneigt, Tools für Datensicherungen zu verwenden, finden Sie im Folgenden Helfer, von denen Sie einen der Allrounder downloaden. Oder Sie picken sich mehrere Tools heraus, von denen sich einige auf bestimmte Aufgaben (wie Browser-Einstellungen duplizieren) spezialisiert haben:



Mehr Sicherheit für Windows 10/11

Für Profis: Das hält Windows für manuelle Backups bereit

Sie sind von Datensicherungs-Tools nicht überzeugt, wollen aber hin und wieder ein manuelles Backup über sich ergehen lassen? Ein bisschen mehr Komfort als beim Datenkopieren über den Windows Explorer wäre schön? In dem Fall hilft Ihnen eine systemeigene Funktion: Mit einem Registry-Hack programmieren Sie quasi ein eigenes Backup-Tool. Es basiert auf Windows-Mechanismen und ist daher schlank sowie im Ressourcenverbrauch genügsam. Damit vervielfältigen Sie schützenswerte Files über ihr Kontextmenü mit nur zwei Klicks. Ellenlanges Herumklicken im Registry-Editor ersparen Sie sich dank eines komplexen Geheimbefehls: Mit diesem tweaken Sie die Windows-Registry in null Komma nichts. Das nötige Win-R-Dialogfenster-Kommando finden Sie im Artikel "Windows-Explorer-Backup: Einfach per Kontextmenü und NTBackup".
Der genannte Sicherungsbefehl ist nicht der einzige, der das Betriebssystem aufwertet. Darüber hinaus gibt es unzählige Systemkommandos mehr, mit denen Sie per Copy & Paste zeitsparend in die Registry eingreifen. Eine Liste mit Empfehlungen haben wir in einem gesonderten Beitrag zusammengestellt: "Windows: Registry-Tweaks, die neue Funktionen und mehr Speed bringen". Tweaks, die unter Windows 11 nicht anschlagen, machen Sie

funktionsfähig, indem Sie beim neuesten Betriebssystem mit dem Tool "Winaero Tweaker" die Windows-10-Taskleiste reaktivieren.
Haben Sie noch CDs/DVDs, dürfte hierfür der portable LCISOCreator das beste Backup-Tool sein. Eine Anleitung hält der Ratgeber "CD-Image-Backup: Mit LCISOCreator – CD-/DVD-Image erstellen" bereit.

Robocopy, CMD-Backup und Speed-Tweaks/-Tools

Für Datensicherungen und Synchronisierungen hat Windows das Kommandozeilen-Tool Robocopy im Portfolio. Das ist in Profi-Gefilden angesiedelt, hilfreiche Tipps geben wir Ihnen hier:
» Datensicherung: So kopieren Sie Filme und Fotos auf externe Festplatten
» Backup über die Kommandozeile: Datensicherung für Profis
Mit Tricks kopieren Sie Dateien schneller und sind so zügiger mit Backups fertig. Wollen Sie den Turbogang einlegen, lesen Sie den Artikel "Dateien schneller kopieren: Mit Registry-Hack, MFT und dem Tool TeraCopy". Das Anlegen von Ordnern ist bei Datensicherungen häufig wichtig, da es eine bessere Übersicht schafft. Müssen Sie viele Verzeichnisse erzeugen, sind Ihnen unsere Anregungen beim flotten Generieren der Dateien-Behälter behilflich: "Windows: Ordner schneller anlegen mit Bordmitteln und Gratis-Tools".

Quelle: https://www.computerbild.de/artikel/cb-Tipps-Software-Backup-Todsuenden-Diese-Fallen-sollten-Sie-vermeiden-16226223.html