Inhaltsverzeichnis

6

Dias, CDs, Papierdokumente: Wann lohnt es sich, Analoges zu digitalisieren?

52

Wie können Sie all Ihre Dateien im Blick behalten und strukturiert speichern?

70

Betrüger sind leider einfallsreich. Auf welche Links sollten Sie niemals klicken?

88

Wie kreieren Sie ein gutes Passwort und was bietet sogar noch mehr Schutz?

136

Ab in die Cloud: Bei welchen Cloudanbietern sind Ihre Daten gut aufgehoben?

151

Bloß keine Panik! Wie können Sie Ihre Daten retten, notfalls sogar ohne Backup?

3 Ziehen Sie das gescannte Bild mit dem Text in das Fenster auf dem Bildschirm.

4 Wählen Sie unten die Sprache des Textes aus und klicken Sie dann auf *OCR starten*.

5 Die Webseite macht jetzt eine durchsuchbare PDF-Datei aus dem Bild. Der Text wird dabei erkannt.

6 Klicken Sie auf *Vorschau*, um eine Voransicht angezeigt zu bekommen und den Text daraus direkt kopieren zu können, oder auf *Download*, um die PDF-Datei herunterzuladen und den Text später daraus weiterzuverwenden.

Bilder und Dias scannen

Auch für Papierfotos und Dias ist der Scanner das Gerät der Wahl. Ein Foto sollte mindestens mit einer Auflösung von 300 dpi gescannt werden, wenn Sie es später wieder drucken möchten. Diese Auflösung reicht aus, wenn es in derselben Größe wie das Original ausgedruckt werden soll. An einem Beispiel: Ein 10 mal 15 Zentimeter großes Papierbild lässt sich mit 300 dpi gescannt in 10 mal 15 Zentimetern gut ausdrucken. Sollten Sie hingegen einen Ausdruck in der Größe 20 mal 30 Zentimeter planen, dann muss beim Scannen als Auflösung 600 dpi eingestellt werden. Doppelte Größe, doppelte Auflösung. Das ist allerdings nicht endlos fortführbar: Über 1200 dpi hat das Original einfach keine zusätzlichen Bildinformationen mehr, die der Scanner aufnehmen kann. Soll das Bild auf einer Internetseite verwendet werden, reicht im Normalfall eine Auflösung von 72 dpi.

Bei Dias – die bei vielen von uns noch kistenweise auf dem Dachboden verstauben – kommt eine weitere Herausforderung auf Sie zu: Ein Dia ist darauf ausgelegt, in einem Projektor an die Wand geworfen zu werden. Ein normaler Scanner kann aus einem Dia kein Bild extrahieren. Dafür gibt es spezielle Diascanner oder Aufsätze auf bestehende Scanner. Dasselbe gilt für Negative von Fotos. Hier sollten Sie überlegen, ob es sich für Sie lohnt, sich ein solches Gerät anzuschaffen. Wenn die Digitalisierung Ihrer Negativ- oder Diasammlung nicht eine einmalige Sache ist, ist es oft sinnvoller, dies einen Dienstleister machen zu lassen.

Scannen – so wird's gemacht

Zu Ihrem Scanner bekommen Sie eine CD (oder einen Download) mit der zugehörigen Software. Installieren Sie diese und schauen Sie im Handbuch nach, wie Sie die Scanfunktion starten. Meist geht es so:

1 Wählen Sie das *Scanprofil* aus (meist stehen Foto und Dokumente zur Wahl).

2 Die *Auflösung* (in dpi) wird durch die Auswahl des Scanprofils meist schon vorausgefüllt, Sie können sie auch manuell anpassen.

3 Schwarz-Weiß-Dokumente nehmen weniger Speicherplatz weg als farbige. Wählen Sie das Ausgabeformat also mit Bedacht!

Info

Onlinedienste? Vertrauenssache Eine Betrachtung, die Sie durch dieses Buch begleiten wird: Wenn Sie Daten nicht lokal speichern oder verarbeiten, dann geben Sie wissentlich Ihre Informationen an Dritte, die Sie nicht kennen. Gerade bei Diensten, die unbekannter sind, sollten Sie abwägen, ob das wirklich eine gute Idee ist. Je vertraulicher die Informationen sind, desto eher sollte die Antwort auf diese Frage „Nein" lauten.

Dateien suchen und finden

Fast alle Dateien befinden sich auf einem Datenträger, der auf Ihrem Rechner verfügbar ist. Externe Festplatten müssen natürlich angeschlossen sein, aber auch verbundene Netzlaufwerke sind im Explorer unter Windows beziehungsweise dem Finder unter macOS sicht- und zugreifbar. Auch Clouddateien werden in der Regel synchronisiert und haben damit eine Entsprechung auf der lokalen Festplatte.

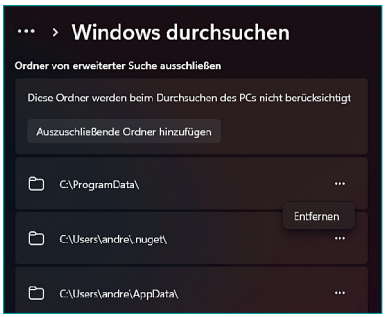
Wichtig: die Suchvorbereitung

Die Art, wie die Betriebssysteme die Suche effizienter machen, ist vergleichbar mit einer Bibliothek: Die einzelnen Bücher sind schon nach einem ausgeklügelten System in unterschiedlichen Räumen, Regalen und Fächern sortiert und ordentlich mit Schildern an den Regalböden gekennzeichnet. Sie gehen in den Raum mit den Reisebüchern, dann ans Regal „Schweden“ und suchen dort nach dem Bildband über schwedische Sehenswürdigkeiten. Den finden Sie nicht. Aber warum? Bevor Sie lange rätseln, gehen Sie zur Bibliothekarin. Die wird Ihnen ohne großes Nachdenken sagen, dass Sie das gewünschte Buch nicht bei „Reise“, sondern bei „Architektur“ finden. Das funktioniert aber nur, weil die Bibliothekarin sich lange und ausführlich mit den einzelnen Büchern beschäftigt hat. Sie hat quasi einen Bücherlageplan im Kopf.

→ **Die Indizierung erstellt den Lageplan**

Ein „Bücherlageplan“ hat seine Entsprechung auf Ihrem Rechner. Die Suche nach Dateien wäre nicht so effizient, wenn Windows oder macOS immer wieder die gesamte Festplatte neu durchsuchen müssten. Stattdessen läuft automatisch ein vorgelagerter Suchprozess: die Indizierung.

Bei Windows Ordner für die Indizierung auswählen



Windows durchsucht die Standardspeicherorte und legt die Informationen zu den Dateien in einer Datenbank ab. Auf diese hat die Suchfunktion dann Zugriff. Legen Sie deshalb alle für Sie relevanten Ordner fest, besonders wenn Sie nicht die Standardordnerstruktur von Windows verwenden:

1 Geben Sie im Suchfeld in der Taskleiste „Systemsteuerung“ ein und starten Sie die Systemsteuerung durch einen Klick auf den Eintrag.

2 Klicken Sie oben rechts auf *Anzeige* und auf *Große Symbole*.

3 Im Detailbereich klicken Sie dann auf *Indizierungsoptionen*.

4 Windows zeigt die aktuell indizierten Laufwerke und Verzeichnisse an. Klicken Sie auf *Ändern*, unter *Ausgewählte Orte ändern* lassen sich dann Ordner ab- oder anwählen, die indiziert werden sollen.

5 Beim nächsten Indizierungslauf indiziert Windows die aktualisierten Verzeichnisse und findet über die Suche Dateien auch in diesen neuen Ordnern.

Indizierung in macOS verwalten

Beim Mac heißt die Indizierung Spotlight. Im Gegensatz zu Windows läuft die automatisch über die gesamte Festplatte. Das ist nicht immer so gewünscht, denn das Durchsuchen dauert schon einen gewissen Zeitraum und aufgrund der Systemstruktur von macOS gibt es viele Dateien zu durchsuchen. Sie können an zwei Stellen auf die Indizierung einwirken. Gehen Sie in die *Einstellungen* von macOS und suchen Sie nach *Spotlight* oder klicken Sie auf *Siri & Spotlight*.

Im Standard stellt Ihnen MacOS Dateien aller halbwegs sinnvollen Dateitypen im Suchergebnis dar. Manche davon wollen Sie gegebe-

Alles kann passieren!

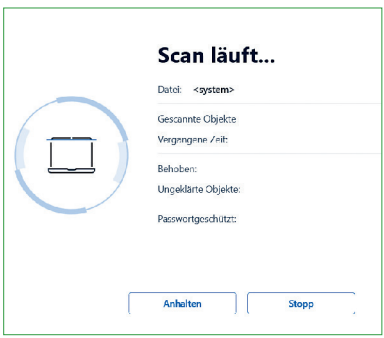
Fehlender Überblick ist ein wichtiges Stichwort – leider auch im Hinblick auf die unzähligen Gefahren, in denen Ihre Daten potenziell schweben. Lassen Sie sich nicht verunsichern: Viele Szenarien sind unwahrscheinlich. Wahr ist aber auch: Je unwahrscheinlicher ein Szenario ist, desto weniger bereiten wir uns darauf vor. Das führt schnell dazu, dass der Schaden höher ist, weil auch die einfachsten Schutzmechanismen nicht aktiv sind. Wir zeigen Ihnen, was alles passieren kann und wie Sie sich schützen können.

Malware – die (un)bekannte Gefahr

Wenn man über Gefahren für PCs und Smartphones spricht, kommt man an einem Thema nicht vorbei: Viren. Trojaner, Würmer, Ransomware, die Namen und Wirkungen sind vielfältig. Das Ergebnis aber ist meist das Gleiche: Durch Malware beziehungsweise Schadprogramme verlieren Sie wertvolle Daten. Und im schlimmsten Fall sind diese auch nicht wiederherstellbar: Wenn der Virus schon im System war, ist das Backup gegebenenfalls auch virenbelastet und nicht wiederherstellbar.

Der klassische Computervirus

Computerviren sind aus einer gut gemeinten Forschungsidee entstanden: dem Prozess der Replikation, also der Selbstvervielfältigung. In der Natur weit verbreitet sorgt er dafür, dass Ökosysteme und Arten überleben können. Wie so oft in der Computerei versuchte man, dies am Computer nachzustellen. Die anfänglichen Programme sollten zwischen Rechnern in einem Netzwerk hin- und herspringen können. Heute ist das anders: Computerviren haben echte Schadfunktionen, die in den allermeisten Fällen alles andere als lustig sind. Daten werden gelöscht, verschlüsselt, verändert, und Sie müssen irgendwie damit leben.



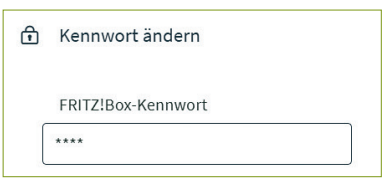
so gut wie alle Programme und Dienste bieten die Anpassung der Privatsphäre-Einstellungen an. Wer kann welche Daten sehen? Was bleibt an Spuren auf Ihrem Rechner zurück? Wie genau Sie diese Einstellungen vornehmen, ist je nach Dienst oder Programm unterschiedlich, doch zumindest bei den bekannten Plattformen sind diese Einstellungen relativ verständlich und übersichtlich gestaltet. Viele Tipps zu diesem Thema können Sie außerdem in unserem Buch „Spurlos im Internet“ nachlesen.

Passwörter: Trügerischer Schutz

Zum kleinen Einmaleins der Datensicherheit gehören Passwörter: Selbstverständlich sind Ihre Konten passwortgeschützt! Vielleicht fühlen Sie sich deshalb sicher. Diese Einschätzung war einmal richtig, aber das ist leider schon viele Jahre her. Durch die technischen Möglichkeiten, die Cyberkriminellen mittlerweile zur Verfügung stehen, ist ein Passwort nur noch eine von mehreren Schutzschichten. Und schon beim Passwort gibt es einiges zu beachten.

Standardpasswörter ändern

Im Netzwerk befindliche Geräte verfügen in der Regel über eine Weboberfläche, in der Sie Einstellungen vornehmen können. Diese wird immer mit einem Standardpasswort gesichert, das entweder im Handbuch steht (für alle Exemplare dieses Geräts identisch) oder auf dem Typenaufkleber an der Hardware. In jedem Fall gilt: Ein solches Passwort sollten Sie umgehend ändern. Andernfalls machen Sie es Krimi-



nellen wirklich sehr leicht: Da das Standardpasswort für alle Geräte eines Modells gleich ist, kann jeder sie im Internet finden, darauf zugreifen und sie übernehmen.

Separate Passwörter statt Masterpasswort

Aus Gründen der Bequemlichkeit liegt nichts näher, als sich ein gutes Passwort auszudenken und dieses für verschiedene Konten zu nutzen – vergleichbar mit einem Generalschlüssel. Der Schlüsselbund wird kleiner, lässt sich komfortabler mitnehmen, keine ständige Suche nach dem richtigen Schlüssel. Mit dem Verlust des Generalschlüssels sind potenziell allerdings sämtliche Türen gefährdet! Übertragen auf die Passwörter: Sämtliche Zugänge zu Ihren Konten wären bei einem solchen Masterpasswort in Gefahr.

Prüfen Sie: Wurde Ihr Passwort schon geknackt?

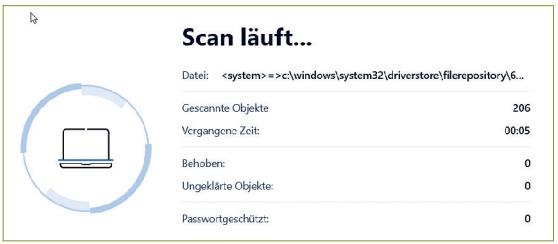
Meist erfahren Sie von einem kompromittierten Passwort erst zu spät. Kontrollieren Sie daher regelmäßig, ob Ihre E-Mail-Adresse und zugehörige Passwörter durch ein Datenleck bekannt wurden. Dazu gibt es die Webseite haveibeenpwned.com, die die Daten der meisten Datenlecks überprüft.

1 Geben Sie Ihre E-Mail-Adresse (oder Handynummer) ein und klicken Sie auf: *pwned?*

Info

Komplexität versus Komfort bei Passwörtern

Nicht selten begegnen einem folgende Passwort-Maximen: hohe Komplexität und häufiger Wechsel. Was zunächst vernünftig klingt, birgt zugleich ein Risiko: Je komplexer und je häufiger der Wechsel, desto eher müssen Sie sich Ihre Passwörter notieren. Das bedeutet jedoch, dass die Passwörter auch außerhalb Ihres Kopfes existieren – an einem Ort, auf den Fremde eventuell zugreifen können.



platte sind oder die eines Programmes wie beispielsweise einer Buchhaltungssoftware: Backups sind eine der wichtigsten Maßnahmen, um Ihre Daten verfügbar zu halten (siehe ab Seite 145).

Synchronisation macht es noch einfacher

Ein klassisches Backup ist der Definition nach eine Einwegsicherung: Die Daten werden vom Original- auf ein Sicherungslaufwerk kopiert. Das gibt Ihnen die Sicherheit, dass Daten im Falle eines Verlustes des Originallaufwerks noch vorhanden beziehungsweise wiederherstellbar sind. Sie können allerdings nur die Originaldatei verändern, sonst haben Sie schnell unterschiedliche Dateistände. Einfacher ist es, wenn Sie Daten zwischen all den Geräten, auf denen Sie darauf zugreifen können und müssen, live synchronisieren lassen (siehe Seite 147).

Backups regelmäßig prüfen

Mit einem Backup können Sie sich ziemlich sicher fühlen, dass Ihre Daten auch den Katastrophenfall überleben. Vorausgesetzt, dass

Info

Tracker verwenden Wenn Sie einen wichtigen Datenträger mitnehmen müssen, können Sie sich zumindest dagegen schützen, dass Sie ihn irgendwo vergessen: Tracker wie die Airtags von Apple zeichnen über ein Netzwerk anonym die Position eines Gegenstandes auf und teilen Ihnen diese auf Anfrage mit. So hat schon manch ein vergessener oder verlorener Gegenstand ohne Datenverlust wieder zu seinem rechtmäßigen Besitzer gefunden.

Sie das Backup weit genug weg vom Originalgerät aufbewahren, sodass nicht ein und dieselbe Katastrophe Original und Backup vernichtet. Nicht wenige Benutzer hatten schon ein böses Erwachen, wenn sie ihre Daten aus dem Backup wiederherstellen wollten und dabei feststellen mussten, dass das Backup defekt war. Und zwar weil es schon bei der Erstellung mit einer Fehlermeldung abgebrochen war, da die Festplatte, auf der es vor Jahren erstellt worden war, zu lange unbenutzt gelegen hat. Darum: Überprüfen Sie regelmäßig die Integrität Ihrer Backups.

→ Endstation Festplatte? Vorsicht!

Festplatten wie auch SSDs sollten nicht monate- und jahrelang unbenutzt in einem Tresor liegen, sondern immer mal wieder angeschlossen werden. Und wenn Sie es ganz sicher machen wollen: Erstellen Sie nicht nur ein Backup, sondern verwenden Sie abwechselnd verschiedene Datenträger.

Ordnung ist das halbe Leben …

… doch das Genie beherrscht das Chaos. Das alte Sprichwort mag richtig sein, jede Anwenderin hat ihre eigene Ordnung und Struktur, um Sachen abzulegen. Das lässt sich für Ihre Daten recht komfortabel mit Ordnerstrukturen auf Ihren Festplatten und USB-Sticks erreichen. Aber diese Daten wollen auch geschützt sein: Wenn Ihr Schreibtisch voller Dokumente und Datenträger ist, gegebenenfalls noch an einem offen zugänglichen Ort, dann birgt das Gefahren, dass ein Unbefugter diese liest oder eine Festplatte einsteckt. Aber auch, dass Sie sich irgendwann nicht mehr erinnern, wo Sie einen USB-Stick oder eine Rechnung hingelegt haben.
Vielleichte wäre sogar die sogenannte Clean Desk Policy etwas für Sie: Wenn Sie Ihren Arbeitsplatz verlassen, dann räumen Sie alle Unterlagen weg. Lassen Sie Ihre Datenträger nicht auf dem Tisch liegen, sondern schließen Sie sie ein oder legen sie zumindest an einen Ort, an dem Sie sie wiederfinden.

► Bei Windows wie MacOS fehlt das Schloss-Symbol neben dem WLan-Namen.

Wenn Sie sich also entscheiden, das WLan zu verwenden, dann achten Sie auf folgende Dinge:

► Achten Sie auf eine verschlüsselte Verbindung zu Webseiten, die Sie an dem https:// (statt http://) der Internetadresse oder dem Schloss in der Adresszeile Ihres Browsers erkennen.

► Schalten Sie das WLan nur bei Bedarf ein.

► Übertragen Sie hierüber möglichst keine sensiblen Daten.

► Verwenden Sie ein VPN, um den Internetverkehr zu verschlüsseln (siehe nächste Seite).

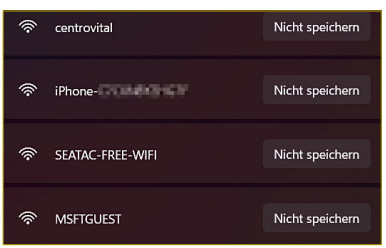
Aufräumen der WLan-Liste

Über die Monate und Jahre sammelt sich in Ihrer WLan-Liste eine schier unüberschaubare Menge von WLans, mit denen sich Ihr Rechner verbunden hat – und sich auch wieder verbinden würde, wenn Sie ihn ließen. Es ist daher sehr sinnvoll, wenn Sie die Liste der gespeicherten WLans kontrollieren und die nicht wirklich benötigten löschen. Das geht so:

Windows:

1 Öffnen Sie die *Einstellungen* von Windows, klicken Sie dann links in der Übersicht auf *Netzwerk und Internet*.

2 Klicken Sie auf *WLan*, dann zeigt Windows die gespeicherten/bekannten WLans an.



3 Klicken Sie neben allen WLans, die Sie nicht mehr speichern wollen, auf *Nicht speichern*.

4 Windows löscht die Zugangsdaten zu diesen WLans. Sie können sich nach wie vor damit verbinden, müssen nur manuell die Zugangsdaten eingeben, die Verbindung läuft nicht mehr automatisch.

MacOS:

1 Öffnen Sie die *Einstellungen* von MacOS, klicken Sie dann links in der Übersicht auf *Netzwerk*.

2 Klicken Sie dann auf WLan, dann auf *weitere Optionen*. Nun zeigt MacOS die gespeicherten/bekannten WLans an.

3 Um ein WLan zu löschen, klicken Sie es an und dann auf das *Minus*-Zeichen unten an der Liste der WLans.

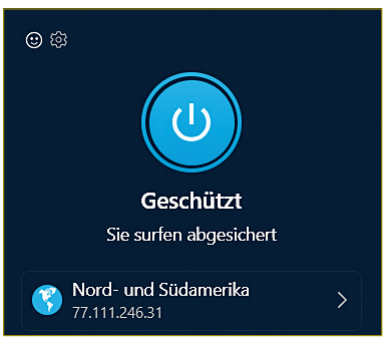
4 MacOS löscht die Zugangsdaten zu diesen WLans. Sie können sich weiterhin damit verbinden, müssen nur manuell die Zugangsdaten eingeben, die Verbindung läuft nicht mehr automatisch.

Ein VPN verwenden

Besonders, wenn Sie vertrauliche Informationen übertragen oder die Verbindung selbst nicht sicher ist – wie es bei einem offenen WLan der Fall ist – ist es empfehlenswert, ein VPN zu verwenden. Dieses Virtual Private Network baut innerhalb des WLans einen eigenen Tunnel auf, in dem die Daten sicher verschlüsselt werden. Wenn ein Unbefugter ins WLan kommt, dann benötigt er zusätzlich noch den Verschlüsselungscode des VPNs.

VPN im Browser

Falls Sie fürchten, dass das viel zu kompliziert sei, können wir Sie beruhigen: Das geht schon mit sehr einfachen Mitteln. Beispielsweise wenn Sie statt Ihres Standard-Browsers Opera (opera.com) verwenden. Der kostenlose Browser hat in der Windows-Version nämlich ein kostenloses VPN integriert.



1 Laden Sie Opera herunter und installieren Sie den Browser.

2 Nach dem Durchführen der ersten Konfigurationsschritte finden Sie links von der Adresszeile von Opera eine kleine Schaltfläche *VPN*. Ein Klick darauf verschlüsselt die Verbindung .

Die Antivirensoftware

Wir haben zuletzt 2023 Antivirenprogramme getestet, mit einem sehr erfreulichen Gesamtergebnis: Antivirenprogramme schützen gut, oft sogar sehr gut. Daher lautet der erste Rat: Wenn Sie schon eines der von uns geprüften Programme haben und damit zufrieden sind, behalten Sie es! Denn jedes Jahr die Software zu wechseln, ist fehlerträchtig. Welche Programme wir getestet haben und alle Details zum Test erfahren Sie hier: test.de/Antivirenprogramme.
Falls Sie sich ein Antivirenprogramm neu anschaffen möchten, gibt unser Test ebenfalls Orientierung. Testsieger für Windows-Rechner sind Avast One Individual, Bitdefender und F-Secure. Für MacOS-Geräte liegen Bitdefender und F-Secure vorn.

→ **Ein Antivirenprogramm gehört auf jeden Rechner!**
Eine Software gegen Viren und andere Malware schützt nicht nur die Lauffähigkeit Ihres Rechners, sondern auch gleichzeitig die Dateien darauf. Viren sorgen unter anderem auch dafür, dass Dateien verändert oder gelöscht werden!

Der Windows Defender

Microsoft setzt schon seit vielen Jahren den hauseigenen Defender als vorinstallierte Antivirenlösung von Windows ein. Der Vorteil: Im Hintergrund wird die Schwarmintelligenz der Windows-Rechner verwendet. Ein Sicherheitsereignis, das auf einem Rechner stattfindet, kann Zufall sein. Bei einer Vielzahl von Rechnern lässt das eher darauf schließen, dass sich gerade eine neue Malware verbreitet, die vielleicht noch nicht alle Virenscanner erkennen.
Unser Test zeigt jedoch, dass andere Programme bessere Erkennungsraten haben. Der Windows Defender erhielt lediglich das Testurteil befriedigend, er landet damit am Ende des Testfelds. Etwas häufiger als andere Schutzprogramme meckert er unbescholtene Dateien als vermeintliche Gefahren an.

Info

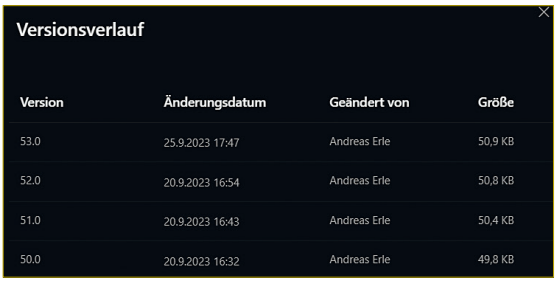
Spezialfall Kaspersky Vor dem Hintergrund des Krieges in der Ukraine haben wir entschieden, für die Antivirenprogramme des russischen Anbieters Kaspersky keine Qualitätsurteile zu vergeben. Zwar hat sich nach unseren Testergebnissen an der Schutzwirkung der Programme nichts geändert. Dennoch ist nicht auszuschließen, dass die russische Regierung Druck auf den Anbieter ausübt, um Änderungen an der Software zu erreichen, die sich negativ auf deren Funktionsweise auswirken. Kaspersky hat das uns gegenüber zurückgewiesen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt seit März 2022 vor Kaspersky-Produkten und rät, andere Antivirensoftware zu nutzen.

Eine Schwäche betrifft den Phishing-Schutz: Einen Phishing-Schutz integriert der Defender nur in den „hauseigenen" Browser Microsoft Edge, nicht aber in Google Chrome. Wenn Sie den Defender nutzen möchten, sollten Sie ihn daher mit Microsoft Edge kombinieren. Alternativ können Sie zum Beispiel den Browser Firefox mit integriertem Phishing-Schutz nutzen.

Vor dem Hintergrund unserer Testergebnisse ist eine separate Antivirensoftware also durchaus sinnvoll. Im Standard deaktiviert Windows den Windows Defender, wenn Sie eine separate Antivirensoftware installiert haben. Sie können ihn aber mit einigen Optionen trotzdem verwenden, Windows sorgt dann selbst dafür, dass die die anderen Programme potenziell störenden Funktionen nicht aktiviert werden:

1 Öffnen Sie die *Einstellungen* von Windows, klicken Sie dann links in der Übersicht auf *Datenschutz und Sicherheit*.

2 Klicken Sie links in der Leiste auf die Option *Viren- und Bedrohungsschutz*.



Papierkorb

Ein weiteres Risiko bei der Nutzung von Clouddiensten ist das Löschen von Dateien: Auf einem Gerät gelöscht, wird die Datei überall sonst auch gelöscht. Für einige Zeit haben Sie aber auch hier noch eine Sicherung: den Papierkorb auf dem Cloudserver. Um daraus eine Datei wiederherzustellen, gehen Sie wie im Folgenden beschrieben vor:

1 Rufen Sie Webseite Ihres Clouddienstes auf und melden Sie sich mit Ihren Kontoinformationen an.

2 Suchen Sie links in der Liste den Ordner *Papierkorb* und klicken Sie darauf.

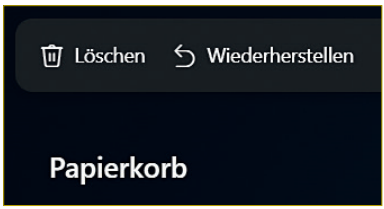
3 Markieren Sie die Datei, die Sie vor der Löschung retten wollen, mit einem Klick, dann klicken Sie darüber auf *Wiederherstellen*.

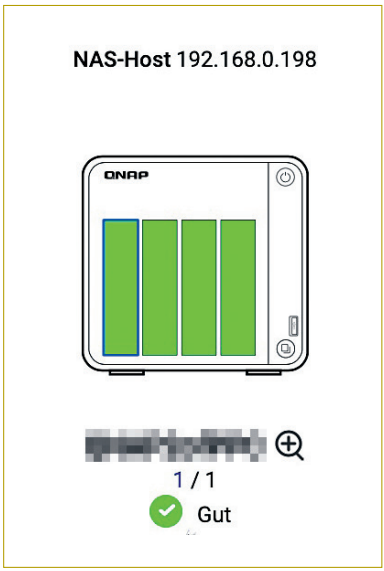
Netzwerkfestplatten als Backup-Medium

Netzwerkspeicher – oft „NAS“ genannt („network-attached storage“) – hängen am heimischen Router und dienen im lokalen Netzwerk als zentraler Speicher für Musik, Fotos, Videos und Dokumente jeglicher Art. Die Konfiguration ist für den Normalanwender mithilfe der entsprechenden Einrichtungsdialoge durchaus machbar und die Datensicherung mittels der entsprechenden Synchronisationssoftware (siehe Seite 147) dann nur noch ein weiterer Schritt.

Einfache oder doppelte Sicherheit?

Die NAS-Systeme verschiedener Hersteller unterscheiden sich in ihren Grundfunktionen nur an wenigen Stellen. Ein Faktor aber hat einen spürbaren Einfluss auf die Sicherheit: Die einfachen NAS-Systeme verwenden eine einzige Festplatte, höherwertige Systeme gleich zwei oder vier Datenträger. Damit können Sie zwar auch die Speicherkapazität Ihres NAS erhöhen, häufiger werden die zusätzlichen Festplatten aber für Sicherheitskopien verwendet. Die Daten werden gespiegelt, sodass sie beim Ausfall eines Datenträgers immer noch vorhanden sind – ein Backup fürs Backup sozusagen.





Verbinden des NAS mit heimischem PC oder Mac

Vereinfacht gesagt sind Netzwerkfestplatten kleine Server, die ein eigenes Betriebssystem und eine eigene Konfigurationsoberfläche haben. Über einen Webbrowser rufen Sie diese auf und richten dann alle Funktionen ein. Was hilft es Ihnen aber, wenn Sie Ihre Datensicherungen auf der Netzwerkfestplatte ablegen wollen? Dazu müssen diese als Laufwerk im Explorer oder Finder vorhanden sein. Das geht entweder über die Apps der Hersteller oder mit Bordmitteln.

Am Beispiel der QNAP-NAS:

1 Installieren Sie das kostenlose Tool QFinder von der Herstellerwebseite. Dieses wird für Windows und MacOS angeboten.

2 Nach der Installation durchsucht es das Netzwerk nach verfügbaren NAS und zeigt diese in einer Übersicht an.

3 Klicken Sie das gewünschte NAS einmal mit der rechten Maustaste an, dann auf *Netzlaufwerk verbinden* und auf *OK*.

Schon zu spät? Hilfe im Verlustfall

Sie wissen nun, was Sie tun können, um Ihre Daten bestmöglich zu schützen. Was aber, wenn es schon zu spät ist? Oder wenn trotz aller Schutzmaßnahmen doch etwas schiefgeht? Eine Festplatte ist defekt, die Aktentasche verloren, kurz: Ihre Daten – und vielleicht mehr – sind weg. Das Wichtigste: Geraten Sie nicht in Panik! Auch jetzt können Sie noch einiges tun, um Ihre Daten zu retten.

Verlorene Daten retten

Hilfe, die Daten sind weg! Häufig liegt das daran, dass Sie Daten versehentlich gelöscht haben oder dass diese durch einen Datenträgerdefekt nicht mehr verfügbar sind. Nun geht es darum, die Dateien schnell wieder verfügbar zu machen, sprich: die Daten irgendwie zu retten. Wie kann das gelingen?

Wiederherstellung aus einem Backup

Wenn Sie bereits regelmäßig Backups angelegt haben, können Sie zunächst einmal tief durchatmen. Wahrscheinlich können Sie Ihre Daten wiederbekommen. Aber bevor Sie jetzt direkt ein Backup einspielen, sollten Sie ein paar Vorbereitungen treffen:

- **Das richtige Backup:** Wenn Sie mehrere Backups gemacht haben, dann verschaffen Sie sich einen Überblick und suchen Sie sich den aktuellen Stand heraus.
- **USB-Anschluss testen:** Haben Sie die Möglichkeit, probieren Sie den USB-Anschluss Ihres Rechners mit einem andren USB-Stick aus, um sicherzustellen, dass dieser funktioniert.
- **Virenscan:** Führen Sie einen aktuellen Virenscan auf Ihrem Rechner durch. Denn sollte Virenbefall Ursache des Datenverlusts sein, wäre es denkbar ungünstig, Sie würden den Virus auf den Backup-Datenträger spielen und eventuell auch das Backup verlieren.
- **Erst noch ein Backup:** Wenn Sie auf Nummer sicher gehen wollen, machen Sie von den Dateien, die Sie mit dem Backup überschreiben, vorher ein Backup. Oft passiert es, dass manche Dateien auf der Festplatte aktueller waren als die im Backup.