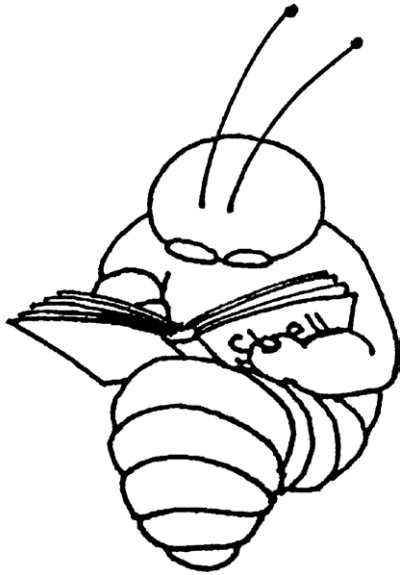
Jürgen Gulbins

Daten- und Dateihandhabung, Dateisysteme sowie Datensicherung (Backup)

Eine Einführung und ein Überblick für Fotografen

Inhaltsverzeichnis



Vorwort

Jürgen Gulbins

Für den Fotografen stehen Fotos im Vordergrund. Da diese heute aber digital gespeichert werden, muss man sich als Fotograf ebenso mit den digitalen Daten beschäftigen.

Bilder und die meisten anderen Informationen werden in Dateien gespeichert und diese wiederum in Ordnern abgelegt. Die Ordner liegen ihrerseits auf Datenträgern wie Magnetplatten, SSDs (*Solid State Disks/ Solid State Drives*), Speicherkarten oder USB-Sticks in Dateisystemen. Diese Speichermedien müssen vor der ersten Nutzung formatiert, eventuell segmentiert (in Partitionen unterteilt) sowie mit einem Dateisystem versehen werden.

Unsere Computersysteme wie Windows, macOS oder Linux nehmen uns viel davon automatisch ab und verstecken viele Details vor dem Benutzer. Zuweilen müssen wir aber doch etwas mehr zu diesen Details wissen – etwa wenn wir einen neuen Datenträger initialisieren möchten oder wenn die Daten automatisch oder explizit verschlüsselt werden sollen.

Auch die Datensicherung – zumeist als *Backup* bezeichnet – verlangt etwas Know-how zu den dafür sinnvollen Techniken. Es erfordert die Wahl eines für den jeweiligen Zweck passenden Verfahrens und schließlich die Wahl eines geeigneten Programms und Datenträgers.

Ich habe versucht, in möglichst verständlicher und übersichtlicher Form einige wesentliche Punkte zu diesen Themenbereichen zusammenzutragen. Ich habe dazu in meinem IT-Know-how gewühlt, recherchiert und viel ausprobiert. Dabei habe ich – wo möglich – etwas vereinfacht und versucht, Struktur in die Vielfalt und die Uneinheitlichkeit der verschiedenen Systeme und Anwendungen sowie in die technischen Begriffe zu bringen. Es werden hauptsächlich die wichtigsten Anwendungsfälle betrachtet und – wo möglich – preiswerte Lösungen gesucht.

Die einzelnen Themen in die richtige Reihenfolge zu bringen hat sich als einigermaßen schwierig erwiesen, da die Techniken und Begriffe ineinander verzahnt sind. Man muss deshalb zuweilen auch einmal etwas weiter hinten nachlesen, um bestimmte Begriffe zu verstehen. Das Inhaltsverzeichnis und der Index sollten Ihnen dabei helfen.

Das Bild von Sandra Petrowitz auf dem Umschlag ist symbolträchtig: Im Normalfall läuft es sich gut und bequem auf dem Sand; passt man aber im Watt nicht auf, holt man sich ohne Orts- und Gezeitenkenntnis schnell nasse Füße und kann im Extremfall auch einmal ganz schön ›absaufen‹.

Dieses E-Book ist relativ umfangreich, erhebt aber keinen Anspruch auf Vollständigkeit. Lassen Sie sich davon nicht abschrecken. Sie müssen und sollen nicht unbedingt alles lesen, sondern können sich die Teile heraussuchen, die Sie benötigen oder die Sie interessieren, und bei Bedarf Details später noch einmal nachlesen. Auch in diesem Fall könnten sich Inhaltsverzeichnis und Index als nützliche Helfer erweisen.

Foto: Sandra Petrowitz

Datenhandhabung und Datensicherung

Shit happens – Mist passiert einfach

Es ist eine Last! Gemeint ist hier die Arbeit mit dem Computer und die damit fast unabdingbar verknüpfte Aufgabe der ständigen Datensicherung – es sei denn, man arbeitet in einem etwas größeren Unternehmen, in dem einem diese Aufgabe von der Systemadministration abgenommen wird und sich diese auch um die Daten auf dem Laptop oder dem Arbeitsplatzrechner kümmert.

Aber hier spreche ich die Fotografen an, die sich in aller Regel um die Sicherung des eigenen Systems und insbesondere um die Sicherung der eigenen Bilder und weiterer zugehöriger Daten kümmern müssen. Ich habe meine Betrachtung in diesem E-Book ausschließlich auf diese konzentriert, auch wenn vieles des Angeführten auch für andere Anwendungen im privaten Bereich oder in kleinen Büros gelten mag.

Wir produzieren fast täglich eine Menge Daten. Ein Teil davon ist nach kurzer Zeit irrelevant und entbehrlich. Einen anderen Teil braucht man etwas länger – etwa eine Woche bis zwei Monate. Weitere Daten möchte man sehr lange aufbewahren, eventuell bis zum eigenen Ende, manches sogar darüber hinaus. Mit größer werdender Datenmenge wachsen auch der Aufwand und die Probleme bzw. Herausforderungen bei der Handhabung der Daten.

Ein Aspekt dabei ist die reine Speicherung. Diese lässt sich für die meisten von uns relativ einfach durch große Speichermedien beheben. So finden wir heute – Mitte 2019 – erschwingliche Plattenlaufwerke bis etwa 12 TB. ›TB‹ steht für Terabyte, was 12.000 GB (Gigabyte) entspricht. Auf die Bilder der hier angesprochenen Fotografinnen und Fotografen angewendet fassen 12 TB grob gerechnet 300.000 Raw-Dateien (mit hoher Auflösung) oder sogar 3,7 Millionen hochauflösende JPEG-Bilder. Nach einer Faustformel schlägt man für eine Bedarfsberechnung etwa 10 % bis 15 % für den Verwaltungsaufwand auf den Speicherplatz auf und braucht darüber hinaus auch immer etwas Reserve.

Mit den steigenden Auflösungen neuerer Kameras erhöht sich natürlich der Speicherbedarf. Belegte meine erste Digitalkamera mit einer Bildauflösung von 1,3 MP (Megapixel) nur etwa 250 KB pro Bild (im JPEG-Format), hat ein Raw-Bild meiner EOS 5D Mk IV mit ›lediglich‹ 30,2 MP im Mittel schon rund 40 MB. Die Bilder aktueller Mittelformatkameras mit 100 Megapixel umfassen im Raw-Format bereits rund 120 MB. Bearbeitete Bilder in TIFF, bei denen man beim Sichern noch die Korrekturebene behält, haben bei mir bereits 1,2 GB – Tendenz steigend.

Die aktuellen Preise von Magnetplatten und SSDs finden Sie in nebenstehender Tabelle.

Nicht jeder hat diese Datenmengen vorliegen, zumindest am Anfang seiner digitalen fotografischen Karriere. Es gilt deshalb, aus Kostengründen die Technik und die Speicherkapazitäten auf den eigenen Bedarf abzustimmen.

Ein zweiter Aspekt ist die Verwaltung bzw. Handhabung einer größeren Datenmenge. Wie strukturiert man im Kleineren (in Ordnern und Unterordnern) die Ablage der Dateien? Ein riesiges Verzeichnis (alle Daten in einem Ordner) ist sowohl technisch ineffizient als auch unübersichtlich und unpraktisch. Also braucht man eine durchdachte Ablagestruktur. Diese will wohlüberlegt und an die eigenen Bedürfnisse und Anwendungen angepasst sein. Sie sollte nachträglich möglichst nicht oder zumindest selten geändert werden, denn eine Umorganisation kostet Zeit, verursacht Aufwand und birgt immer die Gefahr von Fehlern – etwa dass man Daten versehentlich löscht oder falsch einordnet und sie dann nicht mehr oder nur mit erhöhtem Aufwand wiederfindet.

Den Aspekt der Datensicherheit im Sinne eines unberechtigten Zugriffs möchte ich hier zunächst einmal unberücksichtigt lassen.

Tabelle 1: Speicherpreise für Magnetplatten/SSDs

Kapazität	Datenraten	Kosten je Laufw.*
2 TB	ca. 60–90 MB/s	50–100 €
4 TB	ca. 80–100 MB/s	90–200 €
6 TB	ca. 80–120 MB/s	140–280 €
8 TB	ca. 80–130 MB/s	160–360 €
10 TB	ca. 90–180 MB/s	200–450 €
12 TB	ca. 90–200 MB/s	250–550 €
14 TB	ca. 90–220 MB/s	450–600 €
16 TB	ca. 150–250 MB/s	500–700 €
1 TB SSD**	700–1.500 MB/s	120–400 €
2 TB SSD**	500–3.000 MB/s	250–1.000 €
4 TB SSD**	500–3.000 MB/s	450–3.000 €

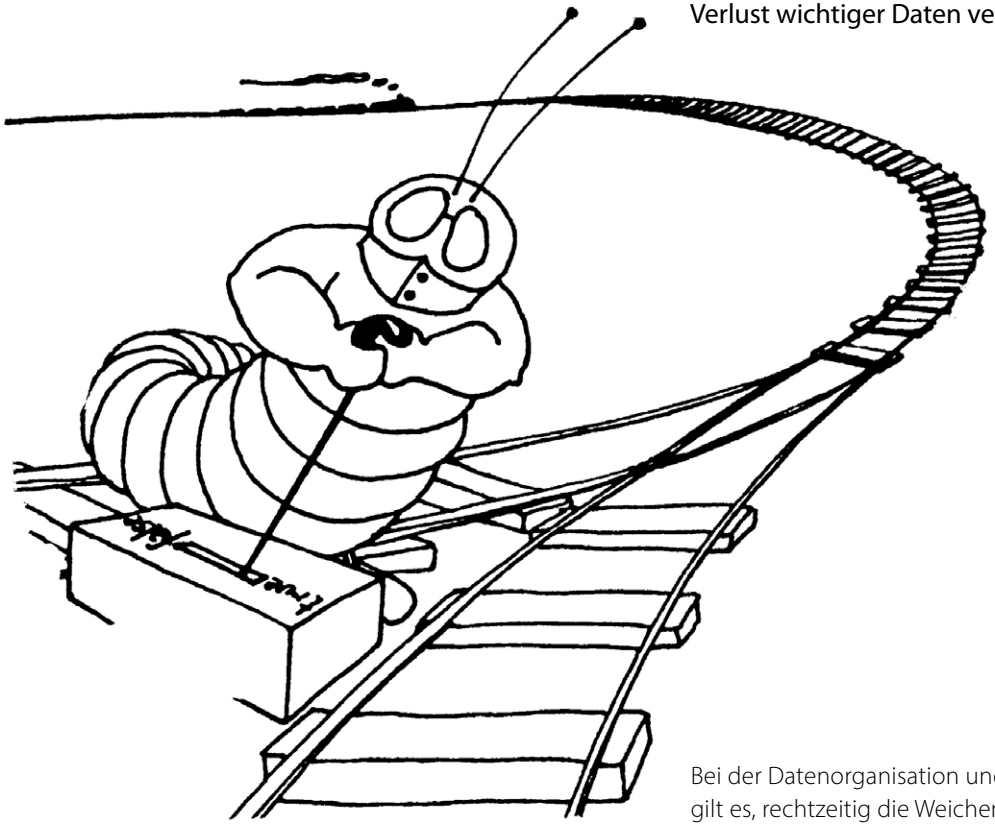
* Die Preise sind inklusive MwSt. und beziehen sich auf ›nackte‹ Laufwerke für Desktop-Rechner. Die Preise für Server-Laufwerke können etwa um den Faktor 1,5 darüber liegen.
** Zu SSDs siehe auch die Beschreibung auf Seite 17.

Ein weiterer Punkt ist der Umstand, dass man seine Daten in bestimmten Abständen durchforsten sollte. Die Aufgabe ist es dabei, nicht mehr benötigte Daten zu löschen und damit den Bestand zumindest etwas zu reduzieren. Beispiele können Bilder von nicht mehr vorhandenen Kunden sein oder Bilder, von denen man bessere Versionen besitzt oder die den eigenen Ansprüchen nicht mehr genügen. Auch ältere Sicherungen gehören dazu, etwa die des Lightroom-Katalogs. Bei diesem Durchforsten stößt man zuweilen aber auch auf Bildjuwelen, die man vergessen hat und unter (neuen) Umständen gut gebrauchen kann. Und zuweilen findet man beim Durchforsten auch Daten – etwa Bilder –, die man falsch eingeordnet hat oder die man nicht mehr nutzen kann, da man die notwendige Anwendung für ihre Nutzung nicht mehr besitzt.

Der Hauptaspekt, den wir in diesem E-Book betrachten, ist der, wie man Datenträger formatiert, partitioniert und mit Dateisystemen versieht und wie man Datensicherungen – *Backups* im Fachjargon – erstellt und handhabt. Auch dafür steigt mit der Datenmenge der technische und zeitliche Aufwand.

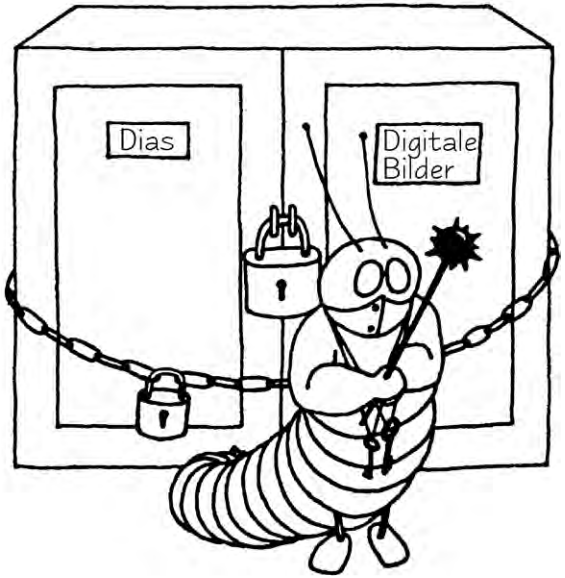
Die Datenvolumina einzelner Datenträger sind zwar kontinuierlich gewachsen – in den letzten 20 Jahren etwa um den Faktor 5 000 000 –, doch die Übertragungsgeschwindigkeit ist nur sehr mäßig gefolgt: Es ist gerade einmal der Faktor 8 in 20 Jahren. Selbst die beeindruckenden, relativ neuen SSDs verbessern dies ›nur‹ um den weiteren Faktor 5 bis 10, aktuell mit Leseraten zwischen 500 MB/s und 3.000 MB/s am oberen Ende. Die Schreibraten liegen etwa 10–15 % niedriger. Und dies setzt bereits voraus, dass die Busse (einfacher: Anschlüsse), mit denen die Datenträger am Rechner angebunden sind, solche Datenraten erlauben, was für ältere Rechner nicht unbedingt gelten muss.

Diese kurze Betrachtung zeigt: Man muss sich selbst als Privatperson bzw. Fotoamateur – und erst recht als professionell agierender Fotograf (oder Fotografin) – Gedanken um seine Datenhandhabung machen, möchte man dafür nicht zu viel Zeit aufwenden. Systematik und ein gut gewähltes Schema bedeuten zu Beginn etwas Aufwand, zahlen sich aber schnell durch eine höhere Effizienz, eine höhere Übersichtlichkeit und am Ende auch durch weniger Handhabungsfehler aus. Es lassen sich so auch Kosten sparen und vor allem der Verlust wichtiger Daten vermeiden.



Bei der Datenorganisation und der Datensicherung gilt es, rechtzeitig die Weichen zu stellen.

Backup – Datensicherung für Fotografen



Für dieses E-Book habe ich einige Grafiken aus meiner EDV-Vergangenheit als UNIX-Spezialist und UNIX-Autor hervorgekramt und ein wenig an die Welt der digitalen Bilder angepasst.

Die Frage ist nicht, **ob** man einmal wertvolle Daten verlieren wird, sondern lediglich: **wann**. Es ist früher oder später unvermeidlich, dass Daten verloren gehen, die man eigentlich noch hätte behalten wollen oder gar dringend braucht. Für den Verlust gibt es viele Gründe; einige davon werde ich noch aufführen. Ich habe wiederholt Erwachsene vor dem Computer weinend erlebt, weil wichtige Daten plötzlich weg waren. Die erste Frage ist dann: »Gibt es eine Datensicherung?« Die zweite Frage, die sich bei positiver Beantwortung ergibt, lautet: »Wo ist das Backup, und wie aktuell ist es?« Und schließlich Frage Nummer drei: »Funktioniert das Zurückholen bzw. Zurückspielen der Daten?«

Jeder, der mit dem Computer arbeitet und dort nützliche, wertvolle oder gar für ihn geschäftskritische Daten hält, muss sich Gedanken zu seiner Datensicherung machen. Die nachfolgend vorgestellten Überlegungen zur Datensicherung gelten für fast alle Bereiche der IT, haben aber natürlich spezifische Ausprägungen für Privatpersonen, kleine Firmen und große Unternehmen. Ich möchte hier dieses Thema aus dem Blickwinkel des Fotografen betrachten, des ambitionierten Amateurs und des Berufsfotografen, der in der digitalen Welt seine Bilder auf dem Computer hat – und zumeist den überwiegenden Teil nur dort.

Dieses Kapitel ist ein leicht überarbeiteter und aktualisierter Auszug aus meinem Buch ›Handbuch Digitale Dunkelkammer‹ (erschienen beim dpunkt-Verlag – vor vielen Jahren).

Datensicherung

Die nachfolgende Diskussion zur Datensicherung mag in Teilen übertrieben klingen, beruht aber auf Erfahrungen. Hier gilt deshalb der Rat: **Sichern** – **Sichern** – **Sichern**, so dass schließlich zumindest drei Exemplare einer jeden Bild- oder wichtigen Arbeitsdatei existieren:

- auf der normalen Arbeitsplatte für die Bearbeitung und für nachfolgende schnelle Zugriffe,
- auf **einem externen, vom Rechner trennbaren Datenträger** wie Festplatte oder Blu-Ray-CD oder auf einem USB-Stick,
- eine weitere (externe) Sicherungskopie an einem anderen Ort (*off-site* gehalten).

Man bezeichnet dies auch als 3-2-1-Konzept, d. h. drei Dateikopien insgesamt – zwei davon im direkten und nahen Zugriff und eine Kopie außer Haus (Abb. 1).

Abb. 1: Von den Daten sollte es nach dem 3-2-1-Konzept drei Kopien geben – eine davon offline außer Haus. Ich empfehle auch, die erste Sicherungskopie nach dem Sichern offline zu schalten, da so Viren und Erpressungs- bzw. Chiffrierungstrojaner nicht darauf zugreifen können.

Gute Bilder, insbesondere im professionellen Bereich, stellen einen erheblichen Wert dar, der über die Zeit bestehen bleibt oder sogar wächst. Aber selbst einem ambitionierten Amateur sollten seine über die Jahre angesammelten Fotos die Zeit, den Aufwand und die Geräte- und Softwarekosten wert sein, die eine gute Datensicherung erfordert. Datenträger – seien es Wechselmedien oder Festplatten – sind so preiswert und handlich geworden, dass man sich diese leisten sollte, selbst im Amateurbereich.

Geht man das Thema *Sichern und Archivieren* etwas systematischer an, so stößt man auf folgende Aspekte, die stark miteinander verzahnt sind:

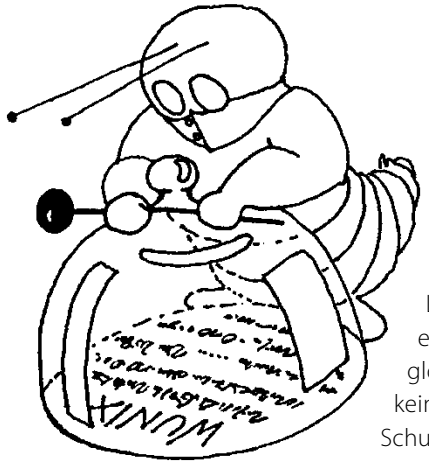
- Welche Risiken bestehen, gegen die ich mich schützen muss?
- Welche Daten sind zu sichern und in welchen zeitlichen Abständen?
- Wie erfolgt die Sicherung – mit welchen Programmen und auf welche Medien?

Die Ausfallrisiken

Die Betrachtung der Ausfallrisiken, d. h. das Nachdenken über ›Was kann passieren?‹, ›Wie wahrscheinlich wird es passieren?‹, ›Was ist der entstehende Schaden?‹, beeinflusst in starkem Maße die nachfolgende Betrachtung und ist das klassische Feld der Risikoanalyse. Eine wirklich detaillierte Erörterung findet man in Peter Kroghs Buch ›Professionelle Bildverwaltung‹. Hier folgt eine zusammengefasste Betrachtung. Ich sehe bei einem Fotografen folgende Verlustrisiken:

A. Datenverlust durch Hardwareausfälle oder Hardwarestörungen
B. Datenverlust durch Virenbefall oder ähnliche Attacken (etwa eine Verschlüsselung durch einen Trojaner bzw. Ransomware)
C. Datenverlust durch menschliche Fehler
D. Datenverlust durch elektronische Störungen (Überspannung, Blitz usw.)
E. Datenverlust durch Diebstahl
F. Datenverlust durch Wasser oder Feuer usw.

Das mag paranoid klingen, aber außer Diebstahl und Feuer habe ich selbst schon alles gehabt, und ich kenne Kollegen, die auch Verlust durch Diebstahl und Feuer erlitten haben. Leider lässt sich auch nicht all diesen Risiken mit den gleichen Mitteln begegnen. Es gilt deshalb, für jedes der Risiken zu überlegen, wie es sich vermeiden bzw. sich die Wahrscheinlichkeit reduzieren



Leider gewährleistet eine einfache Glasglocke über den Daten keinen ausreichenden Schutz!

lässt und wie man den Schaden bei Auftreten beheben kann – was nur bei vorausgegangener Vorsorge gelingt.

Eine wesentliche Frage lautet dabei: »Wie lange kann oder will ich es mir leisten, bei einem Systemausfall keinen regulären Rechnerbetrieb mehr zu haben oder nicht mehr auf meine Daten zurückgreifen zu können?«, beispielsweise bei Ausfall der Systemplatte (mit Betriebssystem und Programmen). Die Antwort hat Einfluss auf die Vorsorgemaßnahmen.

Man kann bei der Systemplatte natürlich das System komplett neu aufsetzen – was bei einem komplexen System mehr als einen Tag kostet. Dies kann erfordern, Lizenzen neu zu beschaffen – beispielsweise Lizenzen, die eine Online-Registrierung erfordern. Habe ich jedoch eine aktuelle Sicherung auf einem separaten Laufwerk, so kann ich in kurzer Zeit einfach durch Austausch der Laufwerke die Arbeit fortsetzen oder – etwas langsamer – durch Austausch des defekten Laufwerks und ein Wiedereinspielen der Daten von einer Sicherung.

So ist erfahrungsgemäß der Ausfall eines Laufwerks (neben Benutzerfehlern) im langjährigen Mittel das häufigste Problem. Das dazu oft genannte Allheilmittel RAID hilft aber nur gegen den Ausfalltyp A. **Alle anderen Verlustarten sind damit nicht abgesichert!**

Hier deshalb eine, wenn auch nur knappe, Betrachtung dieser Risiken und der möglichen Gegenmaßnahmen und Vorsorgen. Bei den Maßnahmen sind drei Aspekte zu betrachten:

- Wie kann ich das Risiko reduzieren und welche Vorsorge muss ich treffen, um die Folgen zu mindern, wenn der Risikofall doch eintritt?
- Wie lange brauche ich später für die Behebung, falls der Schadensfall eintritt?
- Was kostet mich die Vorsorge an Hardware, Lizenzen und anderen Ausgaben – und was kostet mich im Gegenzug ein Schadensfall?

A. Datenverlust durch Hardwareausfall und -störung

Wer kennt es nicht, der länger einen Rechner betreibt: Der Rechner bootet nicht mehr, eine Platte macht komische Geräusche und lässt sich nicht mehr ansprechen. Daneben gibt es viele weitere Komponenten, die ausfallen können (z. B. der Platten-Controller, Kabel, Netzteile…). Ist der Rechner selbst ausgefallen – etwa weil CPU, Speicher oder Platinen defekt sind –, so muss man für ein baldiges Weiterarbeiten auf einen Zweitrechner zurückgreifen können (z. B. einen Laptop) und kann mit etwas Glück die Platte vorübergehend in ein externes Gehäuse einbauen, um vom Ersatzrechner aus Zugriff auf die Daten zu haben.

Handelt es sich um einen Laufwerkausfall, so muss man zwischen dem Ausfall der Systemplatte und der Datenplatte unterscheiden (sofern diese Bereiche sorgfältig getrennt sind, was empfehlenswert ist).

Betrachtet man RAID-Systeme, die zumeist als Erstes genannten Mittel, ist etwas Vorsicht angebracht. RAID hilft nur dann, wenn das richtige RAID-Verfahren eingesetzt wird (siehe dazu die Kästen auf dieser Seite). Es darf nicht RAID 0 sein, sondern muss bei einem Plattenausfall RAID 1, 3, 5 oder RAID 10 sein (es gibt noch weitere Varianten). Aber auch dann hilft RAID nur, wenn lediglich eine Platte ausfällt.[1] Fällt hingegen der RAID-Controller aus und kann kein identischer oder kompatibler Controller beschafft werden, können Sie mit einiger Wahrscheinlichkeit Ihre noch funktionierenden Laufwerke nicht mehr lesen! Abhilfe schafft ein vorsorglich beschaffter Ersatz-RAID-Controller gleichen Typs oder der gleiche Controller aus einem anderen System. Weniger Probleme ergeben sich hier mit einer Software-RAID-Lösung. Auch braucht man beim Ersatz einer defekten RAID-Platte möglichst den gleichen Plattentyp (zumindest aber ein Laufwerk gleicher Größe).

B. Datenverlust durch Virenbefall

Hier besteht die erste Vorsorge natürlich darin, einen Virenscanner einzusetzen und diesen mit aktuellen Virendefinitionen zu versorgen. Damit wird die Gefahr reduziert, aber nicht eliminiert. Eine andere Vorsorge

1 Bei RAID 5 und RAID 10 und bei entsprechender Bestückung darf auch mehr als eine Platte ausfallen.

RAID

Bei den meisten RAID-Lösungen – RAID steht für *Redundant Array of Inexpensive Disks* – werden Daten redundant auf mehrere Platten geschrieben, so dass beim Ausfall einer Platte der Betrieb ohne Unterbrechung weiterlaufen kann. Man braucht dabei der Redundanz wegen mehr Plattenkapazität, um ein bestimmtes Datenvolumen zu speichern (abhängig vom RAID-Verfahren etwa die 1,5- bis 2,0-fache). Tauscht man beim Ausfall einer Platte die defekte Platte aus, so stellt das RAID-System anschließend automatisch den alten Zustand wieder her, was aber eine Weile dauern kann. Dies alles gilt jedoch nicht für RAID-0. Bei RAID-0 werden die Daten über zwei Datenträger (oder mehr) verteilt, um sowohl beim Schreiben als auch beim Lesen eine höhere Performance zu erzielen. Die Datensicherheit sinkt hier (etwa auf die Hälfte)! Für die gängigen RAID-Lösungen sei auf den nebenstehenden Kasten verwiesen.

RAID lässt sich sowohl per Software als auch per Hardware realisieren. Für die Hardware-Variante benötigt man einen RAID-Plattencontroller, was die Kosten erhöht und den Nachteil hat, dass man bei dessen Ausfall oder Migrationen wieder einen kompatiblen Controller benötigt. Dafür kostet er weniger Rechnerleistung und arbeitet schneller. Bei der Software-Lösung muss das Betriebssystem bzw. dessen Plattentreiber die Datenverteilung vornehmen.

Die verschiedenen RAID-Level

RAID 0: Die Daten werden parallel auf mehrere Platten geschrieben (jedoch nicht redundant) und auch parallel wieder gelesen. Dies erlaubt durch die Parallelisierung höhere Übertragungsraten und wird deshalb hauptsächlich für Videobearbeitung eingesetzt. Alle beteiligten Platten werden zu einem großen logischen Laufwerk zusammengefasst. Beim Ausfall einer Platte sind alle Daten im jeweiligen Verbund verloren (minimal 2 Laufwerke).
RAID 1: Alle Daten werden auf mehrere Laufwerke (minimal 2) redundant geschrieben (gespiegelt). Bei Ausfall einer Platte werden die Daten von der anderen Platte gelesen und dorthin geschrieben.
RAID 3: Arbeitet wie RAID 0, schreibt aber zusätzlich Paritätsinformationen auf ein separates Laufwerk, so dass bei Ausfall einer Platte die fehlenden Informationen wiedergewonnen werden können. Es sind minimal 3 Laufwerke erforderlich.
RAID 5: Die Daten werden auf die eingebundenen Laufwerke verteilt; auch die Paritätsinformation wird dabei gleichmäßig verteilt, so dass sowohl ein Geschwindigkeitsvorteil als auch ein Sicherheitsvorteil erzielt wird (es sind minimal 4 Laufwerke erforderlich).
RAID 10: (auch als RAID 0+1 oder RAID 0/1 bezeichnet). Kombiniert die Technik von RAID 0 mit RAID 1. Man erzielt damit höhere Geschwindigkeit und höhere Sicherheit (mindestens 4 Laufwerke).

Eine detaillierte Beschreibung der verschiedenen RAID-Konzepte findet man bei Wikipedia unter [2].

besteht darin, fremde, unbekannte Dateien (und E-Mail-Anhänge) nicht unbedenklich zu öffnen. Die weiteren Vorsorgeschritte sind aber mit denen von Fall C (menschliche Fehler) identisch: Man braucht eine aktuelle Sicherung offline.[1] Statt eines Virenbefalls kann auch Software einmal fehlerhaft sein und Daten zerstören oder unleserlich machen. Vorsorge und spätere Korrekturmaßnahmen sind in beiden Fällen identisch. Sie brauchen dann ein möglichst aktuelles Backup, das zum Fehlerzeitpunkt offline ist, so dass der Fehler nicht (wie etwa bei einem RAID-System) automatisch auf die Sicherungskopie übertragen wird. Bedrohten in der Vergangenheit Viren nur Windows-Systeme, so kommen sie inzwischen auch auf Mac-Systemen vor.

C. Datenverlust durch menschliche Fehler

Dies ist in der Praxis der absolut häufigste Fehler. Sie löschen versehentlich eine Datei (oder ein Verzeichnis oder formatieren die falsche Platte) oder benennen unbemerkt eine Datei um oder verschieben sie, so dass Sie sie danach nicht mehr finden. Hier helfen nur separate Sicherungskopien.

D. Datenverlust durch elektrische Störungen

Spannungsspitzen oder unerwartete Stromausfälle, die zur Beschädigung der Hardware oder (nur) der Dateistruktur führen können, sind häufiger, als man glaubt. Gegen Überspannung kann man mit einem relativ preiswerten Überspannungsschutz vorbeugen[2], gegen Stromausfall durch eine (schon teurere) USV.[3] (Bei Laptop-Systemen mit eigenem Akku kann man auf eine USV verzichten.) Bei Blitzeinschlag in räumlicher Nähe können Überspannungsschutz und USV trotzdem versagen.

Ich selbst betreibe meine Workstation an einer recht kräftigen und etwa 500 Euro teuren USV. Diese schützt weitgehend auch gegen Überspannung und verlängert so potenziell die Lebensdauer der Geräte, da auch viele kleine, kaum bemerkte Spannungsspitzen allmählich die Geräte schädigen können. Bei einem kurzen Stromausfall überbrückt die USV diesen vollständig – je größer und teurer das Gerät, umso länger. Bei längerem Ausfall erlaubt die USV, den Rechner kontrolliert herunterzufahren. Alle zwei bis drei Jahre müssen aber die Akkus der USV ersetzt werden – ein zusätzlicher Kostenfaktor.

Half früher noch ein Burggraben, die eigenen Schätze gegen Feinde zu schützen (wie hier beim Wasserschloss Moyland bei Kleve), gingen doch selbst damit Werte durch Feuer verloren.

E. Datenverlust durch Diebstahl

Als erste Vorsorge gilt es, zunächst eine angemessene Sorgfalt walten zu lassen.[4] Trotzdem ist ein Diebstahl nie auszuschließen. Die nächste Vorsorge besteht ganz trivial in einem aktuellen Backup. Im Falle eines Laptop-Diebstahls auf Reisen reicht eine Sicherungskopie bei einem Online-Service oder zu Hause.

Bei einem Diebstahl im Büro muss eine Sicherungskopie (leider zumeist nicht ganz aktuell) außer Haus vorhanden sein. Beide Maßnahmen decken noch nicht die Sicherung vertraulicher Daten ab. Diese lassen sich nur durch eine Verschlüsselung der Daten schützen (zusätzlich zum Backup bzw. als Teil des Backups).

Überlegen Sie sich im Voraus, woher Sie dann möglichst zügig Ersatz für Ihre gestohlene Hardware bekommen. Eine Elektronikversicherung kann helfen, die

1 ›Offline‹ bedeutet, dass die Platte nicht aktiv oder zumindest nicht im direkten Zugriff des Rechners ist, so dass Viren und andere Fehler nicht auf die Platte übertragen werden können. Dies ist ein wesentliches Sicherungskonzept!

2 Ein reiner Überspannungsschutz kostet etwa 25 bis 70 Euro.

3 USV = ›Unterbrechungsfreie Stromversorgung‹, ein Gerät, welches eine Stromwandlung vornimmt und bei Stromausfall die Versorgung für eine Weile aus einer ständig aufgeladenen Batterie liefert. Die Kosten der USV sind abhängig von der zu erbringenden Leistung und der gewünschten Überbrückungskapazität.

4 Hierzu gehört z. B., bei Abwesenheit Fenster und Türen abzuschließen.

Kosten abzudecken. Achten Sie aber darauf, dass diese auch die Kosten Ihrer mobilen Komponenten (z. B. des Laptops) abdeckt. Die Kosten einer solchen Police liegen etwa bei 1 bis 2 Prozent des versicherten Wertes jährlich.

F. Datenverlust durch Wasser, Feuer und andere Katastrophen

Der Schadensfall ist weitgehend selbsterklärend, die Wahrscheinlichkeit kann individuell stark variieren. So sind beispielsweise Räume im Kellergeschoss stärker durch Wasser gefährdet als höher liegende Räume. Die direkte technische Vorbeugung dürfte ebenso offensichtlich sein – etwa ein Feuer- und Wassermelder. Die Vorbeugung aus Datensicht ist ein möglichst aktuelles Backup aller Daten, das außerhalb gelagert ist.

Einige praktische Maßnahmen

Es erweist sich als praktisch – d. h. es reduziert den Aufwand und vereinfacht die Datensicherung –, wenn man statische (sich seltener ändernde) und sich häufiger ändernde Daten trennt und auf verschiedene Datenträger oder zumindest verschiedene Partitionen eines Datenträgers legt. So spricht aus meiner Erfahrung viel dafür, Systempartition und Datenpartition möglichst sauber zu trennen. Auf der Systempartition liegen dann das Betriebssystem und alle Programme sowie die zum Betriebssystem gehörenden, sich selten ändernden Daten wie etwa Programmbibliotheken, Schriften, Vorlagen, Plug-ins usw.

Gewitter im Anzug: Wenn der Himmel so aussieht, schaltet man den Rechner besser aus und greift zur Kamera.

Alle anderen Daten gehören auf separate Partitionen oder sogar auf ein separates Laufwerk. Dazu zählen auch die typischen Benutzerdaten wie Adressbücher, E-Mails, Terminkalender-Daten und Ähnliches. Natürlich gehören auch die Kataloge von Lightroom und anderen Bildverwaltungen sowie die Caches von Adobe Camera Raw und Bridge und ähnlichen Programmen dazu.

Leider legen sowohl Windows als auch Mac OS X in der Standardkonfiguration diese Daten auf die Systempartition, dort jeweils in benutzerspezifische Verzeichnisse – z. B. in *Dokumente* oder *Bilder*. Auf die Systempartition (das Systemvolume) gehören sie meiner Meinung nach aber nicht. Leider kommen die meisten Rechner vorkonfiguriert mit einer einzigen Partition daher. Hier gilt deshalb, möglichst früh Hand anzulegen und die Daten zu trennen.

Das Systemvolume (ohne die Benutzerdaten) muss man relativ selten sichern. Ich empfehle dies immer, nachdem ein System komplett neu eingerichtet ist, und danach etwa monatlich. Ich sichere zusätzlich immer dann, wenn ein viel benutztes Programm aktualisiert oder ein neues

Programm installiert wurde, das eine Online-Registrierung benötigt oder ein aufwändiges Aufsetzen erfordert.

Eine weitere Trennung kann zwischen wertvollen und weniger wertvollen Daten sinnvoll sein. Die wertvollen wird man unter Umständen häufiger sichern, eventuell verschlüsseln und mehrfache Kopien davon halten.

Die richtige Anbindung/Schnittstelle

Rüsten Sie Ihren Rechner bei Bedarf mit schnellen Schnittstellen aus (oder nach). Diese können das Sichern wesentlich vereinfachen und vor allem beschleunigen. Zu einer Betrachtung der Performance verschiedener Schnittstellen siehe Tabelle 2 auf Seite 15.

Sofern Sie Ihre Daten über LAN (im lokalen Netz) sichern, sollten Sie, wo möglich, Gigabit-LAN einsetzen. Dabei müssen alle Strecken und Komponenten zwischen dem Rechner und dem NAS (*Network Attached Storage* – Netzwerkspeicher) durchgängig die hohe Übertragungsrate unterstützen.

Die Sicherungs- und Wiedereinspielzeit wird im Wesentlichen von vier Faktoren bestimmt:

A. der Lesegeschwindigkeit des zu sichernden Datenträgers,
B. der Schreibgeschwindigkeit des Sicherungsträgers,
C. der dazu eingesetzten Verbindung bzw. des Interfaces (USB in den verschiedenen Generationen, FW, eSATA, Thunderbolt, LAN, …),
D. der Leistung des Rechners – bei NAS auch die des Rechners (Controllers) auf dem NAS.

Welche Daten sind zu sichern?

Diese Frage klingt trivial, wird aber deutlich interessanter, wenn man sie mit dem ›Wann?‹, ›Wie oft?‹, ›Wohin?‹ und dem ›Wie?‹ bzw. ›Womit?‹ verknüpft. Hier hilft das pauschale ›Alles‹ nicht. Man sollte trennen nach den Arbeitsvoraussetzungen. Dabei hilft es, grob mehrere Klassen bzw. Bereiche zu unterscheiden, deren Sicherung unterschiedlich oft und eventuell mit verschiedenen Werkzeugen erfolgen sollte:

1. Betriebssystem und Programme (Systemvolume)
2. Bilder und andere Fotodaten sowie weitere Mediendaten (z. B. Filme)
3. Datenbanken – etwa die Dateien einer Bilddatenbank
4. Arbeitsdaten wie E-Mails, Präsentationen, Office-Dateien…

1. Betriebssystem und Programme

Ein Betriebssystem mit all seinen Programmen, Diensten, Netzwerkeinstellungen, Bibliotheken, Benutzereinstellungen und anderen Hilfsdateien aufzusetzen, ist aufwändig. Hat man diesen Teil, wie zuvor beschrieben, deshalb halbwegs sauber gekapselt, sollte man ihn als Einheit sichern, und zwar so, dass sich das System problemlos und schnell restaurieren lässt – besser noch, dass man gleich von der Sicherung booten und arbeiten kann, auch wenn dies nur für eine Übergangszeit sein mag. Dafür muss das Sicherungsprogramm ausgelegt sein; ebenso muss es eine Sicherung im laufenden Betrieb beherrschen.[1] Wie häufig Sie sichern, hängt von der Änderungshäufigkeit dieses Teils ab. Letzte Updates, die zumindest für das Betriebssystem etwa monatlich erfolgen, können dabei eventuell später nachgeladen werden.

2. Bilder und andere Fotodateien

Was die ›Fotodaten‹ betrifft, gilt es zunächst einmal, alle originären Bilddateien zu sichern, so wie sie aus der Kamera kommen – also die Raw-Dateien oder die JPEGs oder TIFFs aus der Kamera. Vor dem Sichern wird man Bilder häufig zumindest flüchtig mit einem Browser (nach dem Herunterladen auf den Rechner) inspizieren, die unbrauchbaren löschen, die Dateien in konsistenter Weise umbenennen und – soweit notwendig – in die richtige Lage rotieren. Dann ist aber bereits Schluss: Spätestens jetzt wird gesichert – vor jeder weiteren das Original verändernden Bildbearbeitung! Und erst danach kann man mit gutem Gewissen die Daten auf der Speicherkarte der Kamera löschen, die Raw-Daten konvertieren und die Bildbearbeitung starten.[2] Erstellt der

1 Von einer zeitgesteuerten automatischen Sicherung des Betriebssystems rate ich ab, da dabei zu schnell ein fehlerhaftes System die alte Sicherung ersetzt – es sei denn, man hält hier mehrere Versionsstände vor.

2 Einige Downloader sind in der Lage, die Bilder gleich an zwei Stellen parallel abzulegen und damit bereits beim Download eine Sicherungskopie zu erstellen. Hierzu gehören z. B. Lightroom und Downloader Pro. Dies macht den Download zwar etwas langsamer, man befindet sich damit aber auf der sicheren Seite. Ideal ist es, wenn die Dateiumbenennung dabei vor der Sicherung erfolgt.

Downloader eine Sicherungskopie der Kameradaten, so sollte die Sicherungskopie bereits mit den umbenannten Bilddateien erfolgen, so dass die Bilddateien sowohl eindeutige Namen haben (im Gesamtbestand nur genau ein Mal vorkommend) als auch später einfach den Bildern aus dem Arbeitsbereich zugeordnet werden können.

Nun gilt es zu überlegen, was sonst noch alles zu sichern ist. Dazu gehören:

- die Originaldateien (Raws, JPEGs, TIFFs…) – wie bereits geschehen,
- alle fertigen Bilder – TIFFs, PSDs, JPEGs usw. Liegt ein Bild in mehreren unterschiedlichen Formatvarianten vor – etwa als ein Master und eine verkleinerte und komprimierte JPEG-Web-Version –, so sichert man auch diese Varianten, schließlich hat auch die Konvertierung oft etwas Nacharbeit gekostet;
- eventuell alle größeren Zwischenschritte, die Ausgangsbasis für weitere Bearbeitungsvarianten sein könnten. Erfolgen die Korrekturen mit Lightroom und ähnlichen Datenbank-basierten Systemen, so reicht es, die Datenbank (bei Lightroom den Katalog) zu sichern.

Theoretisch kann man aus dem Original das bearbeitete Bild nochmals neu erschaffen, im fertigen Bild kann aber viel Arbeit stecken. Datensicherungsmedien sind inzwischen so preiswert und das Sichern erfolgt (mit guter Vorbereitung) so zügig, dass man lieber etwas zu viel sichert als zu wenig. Wirklich Arbeit macht erst die Organisation.

Editiert man nicht-destruktiv, wie es beispielsweise in ACR, Lightroom oder vielen anderen Raw-Konvertern (auch auf TIFF- und JPEG-Dateien) möglich ist, so gilt es, neben den Bildern selbst auch die zugehörigen Korrektureinstellungen zu sichern – seien es Begleitdaten wie etwa XMP-Dateien bei Adobe Camera Raw oder seien es die Korrektureinstellungen, die wie bei Lightroom in der Bilddatenbank selbst gespeichert werden.

Sicherung für Lightroom ›unterwegs‹

›Unterwegs‹ empfiehlt es sich, die Aufnahmen abends auf den Laptop zu spielen und zumindest flüchtig zu inspizieren. Dann sollte so gesichert werden, dass es (außer der Speicherkarte selbst) zwei Kopien gibt – entweder auf dem Laptop und einem externen Datenträger oder auf zwei externen Datenträgern. Diese sollten bei der Reise (z. B. beim Flug) getrennt aufbewahrt werden. Bei größeren Reisen können Sie so erstellte Kopien, etwa auf einem USB-Stick, auch per Post nach Hause schicken – eine Vorsorge gegen Gepäckverlust und Diebstahl – oder die Daten in einen Online-Speicher stellen (wie etwa Dropbox, Apples iCloud, Microsofts OneDrive oder ein anderer Online-Speicher). Von diesem können Sie später (wieder zu Hause) die Daten bei Bedarf herunterladen und sie im Online-Speicher löschen, um Kosten zu sparen.

3. Datenbanksicherung

Im kommerziellen Umfeld gibt es spezielle Plug-ins zur Datenbanksicherung. Sie sind entweder Teil der Datenbank oder Teil der Sicherungssoftware. Diese Plug-ins gibt es bisher für die meisten der betrachteten Bilddatenbanken aber noch nicht – oder sie sind zu teuer. Die einfachste Lösung besteht deshalb darin, die Datenbanken bzw. die betreffenden Applikationen zu schließen (zu beenden) und erst dann die Dateien der Datenbank zu sichern. Eine Sicherung im laufenden Betrieb und mit den üblichen Sicherungsprogrammen empfiehlt sich nicht – das Ergebnis könnte eine inkonsistente Datenbank sein. (Dieses Problem hatte ich bisher jedoch beim Lightroom-Katalog nie.)

Oft lässt sich erheblich Plattenplatz sparen, wenn die Sicherungsdatei der Datenbank komprimiert wird – bei der Lightroom-Datenbank etwa um den Faktor 3 bis 4! (Ab Lightroom 6 wird das Datenbank-Backup automatisch komprimiert.) Neben den Speicherplatz-Einsparungen kann eine Komprimierung bei schnellen Rechnern sogar die Sicherungszeit verkürzen. Es empfiehlt sich hier auch, mehrere zurückliegende Stände zu halten und dafür öfter zu sichern (und zuweilen ältere Sicherungsstände zu löschen). Bedenken Sie aber, dass – wenn Sie bei Lightroom oder einem anderen Bildverwaltungssystem die Datenbank gesichert haben – die Bilder noch nicht gesichert sind! Diese müssen getrennt gesichert werden, es sei denn, die Bilddatenbank speichert, wie bei dem nicht mehr unterstützten Apple

Aperture möglich, die Bilder selbst auch in der Datenbank.

4. Arbeitsdateien
Hierzu zählen Ihre E-Mails und Terminkalender (sofern sie lokal gehalten werden), Ihre Texte und Präsentationen, an denen Sie aktuell arbeiten, sowie die Bilder (z. B. in Photoshop), die Sie aktuell editieren und ähnliche Daten, die Sie ständig verändern oder aktualisieren.

Hier haben wir die höchste Dynamik bezüglich Änderungen. Deshalb sollte hier täglich gesichert werden (oder an jedem Tag, an dem Sie mit dem Rechner arbeiten). Dies sollte so erfolgen, dass auf mehrere ältere Stände einzelner Dateien zurückgegriffen werden kann. Oft bemerkt man erst recht spät, dass man etwas versehentlich gelöscht hat, einen falschen Weg gegangen ist oder den Vergleich mit einem älteren Stand nochmals benötigt. Abhilfe schafft dabei natürlich eine Versionierung der Dateien, was aber nicht von allen Sicherungsapplikationen angeboten wird – es sei denn, man führt dies manuell aus.

Die Sicherung dieser Daten ist so wichtig, dass sie automatisiert erfolgen sollte – entweder ständig im laufenden Betrieb im Hintergrund, wie es etwa bei Mac OS X *Time Machine* anbietet, oder automatisch zu einem festen Zeitpunkt – etwa nachts, sofern das System nachts durchläuft. Eine weitere Variante ist die automatische Sicherung vor dem Herunterfahren des Systems. Auch dies kann automatisch abends erfolgen und das System anschließend automatisch heruntergefahren werden. Überprüfen Sie aber bei den automatischen Lösungen regelmäßig die Sicherungsprotokolle, damit Sie Probleme rechtzeitig erkennen!

Sicherungsprogramme

Für die Sicherung eines ganzen Volumes (den Daten in einem Dateisystem einer Partition) bzw. einer ganzen Partition setze ich Programme ein, die eine Komplettsicherung durchführen können und bootbare Images[1] erzeugen. (Dies bereitet unter Windows gewisse Probleme; mehr dazu später.) Achten Sie dabei darauf, dass Sie von dem Zieldatenträger (ob intern oder extern) auch wirklich physikalisch booten und Ihr System betreiben können. **Testen Sie dies explizit!**

Das Sicherungsprogramm sollte in der Lage sein, diese Sicherung im laufenden Betrieb vorzunehmen. Unter Mac OS X verwende ich dafür die sehr gute Software *Carbon Copy Cloner* oder alternativ *SuperDuper!*; es gibt aber noch eine ganze Reihe weiterer Programme, die dies können.

Unter Windows nutze ich *Acronis True Image*. Auch hier gibt es eine Reihe weiterer gleichwertiger Programme – etwa das Windows-*Backup* (auf allen neueren Systemen) oder *Drive Snapshot* –, teilweise sogar kostenlos für die private Nutzung. (Später sind noch weitere Backup-Anwendungen aufgeführt.) Man sollte aber

1 Als ›Image‹ wird hier eine Platte oder Partition verstanden.

➜ Bei ständig laufender, inkrementell arbeitender Sicherungssoftware – bei macOS beispielsweise per *Time Machine* – empfiehlt es sich, die Datenbankdateien explizit von der Sicherung auszuklammern. Es werden sonst zu viele und inkonsistente Kopien erstellt, die oft auch noch recht groß sind.

sicherheitshalber eine CD/DVD oder einen USB-Stick haben, von der/dem man booten kann, um ein so erstelltes System-Backup wieder einspielen zu können (eventuell auf ein neues Ersatzlaufwerk), falls die Systemplatte nicht mehr ansprechbar ist und man nicht von einem anderen Laufwerk oder einer anderen Partition booten kann.

Bei diesen Sicherungen ist darauf zu achten, dass so gesichert wird, dass nach dem Austausch oder dem Rückspielen alle notwendigen Lizenzen – beispielsweise die Windows-Lizenz oder die der Adobe Creative Suite bzw. von Photoshop – weiter funktionieren.

Wiederbeschreibbare Datenträger, auf die ich sichere – in aller Regel externe Laufwerke –, werden nach der Sicherung offline gesetzt. Dies verhindert, dass sie durch Viren oder Systemfehler oder Störungen der Varianten B bis E beschädigt werden können.

›Normale Daten‹ habe ich in der Vergangenheit teilweise mit anderen Programmen gesichert. Inzwischen sind aber viele der Sicherungsprogramme in der Lage, sowohl ganze Partitionen (Volumes) zu sichern (in ein bootbares Image) als auch individuelle Verzeichnisse und beides insgesamt sowie inkrementell. Diese Verfahren müssen nicht immer ein gesamtes Volume sichern, sondern brauchen, nachdem einmal eine Grundsicherung erfolgte, nur noch jene Daten zu sichern, die

seit der letzten Sicherung geändert wurden oder neu hinzukamen. Diese Technik wird als ›inkrementelles Sichern‹ bezeichnet. Dabei ist aber darauf zu achten, dass Datenbanken eventuell eine besondere Sicherung benötigen (wenn sie im laufenden Betrieb gesichert werden), damit ein konsistenter Zustand sichergestellt wird. Im einfachsten Fall fährt man eine solche Datenbank herunter. Von meinen Fotowerkzeugen tue ich dies beispielsweise bei Adobe Lightroom, Apple Aperture sowie bei den anderen Bildverwaltungssystemen.

Diese Sicherung erfolgt bei mir primär auf extern angeschlossene Magnetplatten. Infrage kommen hier externe, direkt über USB, FireWire oder eSATA angeschlossene Geräte, NAS- oder SAN-Systeme[1] oder externe File-Server, die praktisch eine Variante von NAS-Systemen darstellen. Theoretisch kommen auch SAN-Systeme in Frage, sind aber für die meisten Fotografen zu teuer und für unsere Zwecke nicht kosteneffizient.

Bei direkt angeschlossenen externen Systemen ist die lange Zeit übliche USB-2-Schnittstelle die langsamste Variante (und war früher beim Mac besonders langsam), FireWire 400 etwas schneller und FireWire 800 spürbar schneller (siehe Tabelle 2). Die bisher schnellsten Varianten bieten die eSATA-Schnittstelle, neuere USB-Varianten – USB 3.0, USB 3.1, USB 3.1 Version 2 (auch als USB 3.2 bezeichnet) – sowie Thunderbolt-Schnittstellen (Version 2 und 3, ab 2020 auch Version 4).

1 NAS = ›Network Attached Storage‹
SAN = ›Storage Area Network‹

Tabelle 2: Reale maximale Übertragungsraten für unterschiedliche Interface-Techniken (Platte zu Platte)

Art	Schreiben	Lesen
USB 2	20–30 MB/s	35–35 MB/s
USB 3.0	60–190 MB/s	80–200 MB/s
USB 3.1	100–500 MB/s	80–700 MB/s
USB 3.2 (3.1 Gen. 2)	200–2.000 MB/s	200–2.500 MB/s
FireWire 400	22–32 MB/s	30–40 MB/s
FireWire 800	30–40 MB/s	40–60 MB/s
SATA/eSATA*	70–250 MB/s	80–600 MB/s
Thunderbolt 2*	700–1.500 MB/s	800–1.500 MB/s
Thunderbolt 3*	800–3.000 MB/s	800–3.500 MB/s
NAS (Gigabit-LAN)	45–90 MB/s	65–100 MB/s

* Die höheren Datenraten erreicht man nur an RAIDs oder SSD-Speichern. Limitierend sind hier der Datenträger und potenziell der Bus, an dem das Laufwerk angeschlossen ist.

USB 2 und FireWire wurden ab 2013 vom schnelleren USB 3 abgelöst – hoffentlich auch an Ihrem Rechner.

NAS-Systeme haben in den letzten Jahren an Geschwindigkeit gewonnen, sind überwiegend aber immer noch um den Faktor 2 bis 3 langsamer als schnelle Direktanschlüsse. NAS-Lösungen erlauben jedoch höhere Kapazitäten pro Einheit (durch Einsatz mehrerer Platten) und einen Betrieb, bei dem mehrere Rechner auf ein NAS zugreifen können.

Für die Kopien, die *off-site,* d. h. außer Haus gehen sollen, verwende ich einfache Plattengehäuse mit (oder ohne) Wechselrahmen, die ich per USB 3, eSATA oder Thunderbolt direkt am Rechner anschließe. Nach dem Bespielen kommt die Platte in eine Schutzhülle und wird bei einem Bekannten gelagert. Solche Kopien erstelle ich (in größeren Abständen) sowohl für die Systemplatte als auch (häufiger) für meine Daten – sowie vor jedem größeren Urlaub, bei dem ich längere Zeit außer Haus bin (Diebstahlgefahr). Als Datenträger verwende ich dabei ganz pragmatisch ältere Platten, die mir für den normalen Betrieb zu langsam und zu klein wurden und die ich deshalb durch neue Laufwerke ersetzt habe. Für ein *Off-site-Backup* sind sie aber immer noch nützlich. Bringe ich einen solchen Datenträger weg, hole ich mir gleichzeitig einen zuvor ausgelagerten zurück, um darauf das nächste Backup zu erstellen. Eine kleine, einfache Buchführung hilft, dabei die Übersicht zu bewahren.

Unterschätzen Sie nicht die Sicherungszeiten bei größeren Datenbeständen. Tabelle 3 auf Seite 16 zeigt die Sicherungszeit für die Vollsicherung eines 2-TB-Volumes mit verschiedenen Techniken (Magnetplatte zu Magnetplatte). Selbst bei einer sehr guten (realistischen) Leistung von 100 MB/s (über viele Dateien hinweg) braucht die Vollsicherung einer 2-TB-Platte viele Stunden – und ein Zurückspielen dauert ebenso lange!

Schnelle SSD-Einheiten mit Datenraten zwischen 500 MB/s und 3.000 MB/s sind für die Systemplatte inzwischen zwar ausgesprochen nützlich und durchaus bezahlbar, als Backup-Medium aber für Fotografen noch zu teuer – auch wenn die Preise für SSDs fast monatlich fallen. Die hohen Datenraten setzen aber für eine optimale Nutzung auch entsprechend schnelle Anbindungen voraus.

Sicherungsmedien

Als Sicherungsmedien verwendet man vorzugsweise Standardmedien, also DVD, BD (Blu-Ray-Disc) oder externe Festplatten. Bänder und magneto-optische Datenträger kommen für Fotografen kaum noch in Frage. Bei den magneto-optischen Datenträgern hinken die Kapazitäten deutlich anderen Datenträgern hinterher. Die Laufwerke sind wie bei Bändern mit hoher Kapazität für den hier beschriebenen Einsatz in der Regel zu teuer.[1]

CDs sind für die heutigen Datenmengen für die Sicherung von Bildern und Datenbanken viel zu klein. Auch DVDs mit einer Kapazität von ca. 4,3 GB (Single Layer) oder 8,4 GB (Double Layer) sind für die meisten Sicherungen nicht ausreichend groß.

Bei der nächsten Generation an optischen Datenträgern hat sich inzwischen zwar der Kampf zwischen Blu-Ray-Discs und HDs zugunsten der Blu-Ray-Technik (BD) entschieden. Aber auch hier sind die Kapazitäten pro Datenträger mit etwa 25 GB bei einlagigen BDs und ca. 50 GB für zweilagige Datenträger recht begrenzt, wenn man an die zu sichernden Datenmengen denkt. Diese liegen eher im Terabyte-Bereich. BD-Schreiblaufwerke liegen inzwischen zwar mit 100 bis 150 Euro (für ein externes Laufwerk) im akzeptablen Preisbereich, die Datenträger sind jedoch mit ca. 3 Euro für einlagige und etwa 5 Euro für zweilagige Datenträger noch recht teuer.

Deshalb ist es heute in den meisten Fällen preiswerter, großvolumige Magnetplatten mit Wechselrahmen (oder auch ohne) direkt in externen Wechsellaufwerkgehäusen einzusetzen, zumal die Übertragungsraten damit deutlich höher sind. Ist einmal Eile geboten, so lassen

1 Ein LTO-4-Laufwerk kostet etwa 4.000 Euro, ein Datenträger dazu mit einer Kapazität von etwa 800 GB ca. 25 Euro. Für diesen Preis bekommen Sie sehr viel Plattenspeicher.

Tabelle 3: Zeitbedarf für die Sicherung einer 2-TB-Platte mit unterschiedlichen Techniken (Platte zu Platte)

USB 2.0	bei 30 MB/s	ca. 18 Std. 33 Min.
USB 3.0	bei 60 MB/s	ca. 9 Std. 17 Min.
USB 3.1/3.2	bei 100 MB/s	ca. 5 Std. 35 Min.
FW 400	bei 38 MB/s	ca. 14 Std. 37 Min.
FW 800	bei 70 MB/s	ca. 8 Std.
Gigabit-NAS	bei 85 MB/s	ca. 6 Std. 33 Min.
eSATA 3G	bei 100 MB/s	ca. 5 Std. 33 Min.
eSATA 6G RAID	bei 120 MB/s	ca. 4 Std. 38 Min.
Thunderbolt 2	bei 150 MB/s	ca. 3 Std. 43 Min.
Internet (Upload)	bei 1 Mbit/s	ca. 232 Tage
Internet (Upload)	bei 10 MBit/s	ca. 23,2 Tage
Internet (Download)	bei 50 MBit/s	ca. 4,6 Tage
Internet (Download)	bei 100 MBit/s	ca. 2,3 Tage

Tabelle 4: ca. Speicherkapazität pro Medium (Stand 2019)

CD	0,6–0,8 GB
DVD	4,3 GB
DVD zweilagig	8,4 GB
Blu-Ray-Disc	25 GB
Blu-Ray zweilagig	50 GB
Magnetplatte 2/2,5“	500 GB–5 TB
Magnetplatte 3,5“	0,5 TB–16 TB
SSD	125 GB–4 TB

◀ Diese relativ preiswerte ICY BOX nimmt sowohl 2"- als auch 3,5"-SATA-Laufwerke auf und hat ein USB-2.0- und ein eSATA-Interface. Ich setze sie ein, um darauf Daten zu sichern, die ich dann außer Haus lagere. Neuere Modelle bieten USB-3.1- und sogar Thunderbolt-Schnittstellen. Es gibt diese Laufwerk-Stationen auch mit zwei getrennten Laufwerkschächten (siehe Abb. 2, Seite 25). Diese können zum Teil Laufwerke autark (ohne Rechner) duplizieren.

▲ Ich verwende für die Platten, die außer Haus gehen, solche Plastikboxen und beschrifte sie entsprechend. Man erhält sie z. B. bei Conrad Electronic.

▲ Dieses Taurus-Gehäuse nimmt zwei SATA-Laufwerke auf (mit je bis zu 4 TB). Es lässt sich so konfigurieren, dass sie im RAID-0, RAID-1 oder im JBOD-Modus arbeiten. Das Gehäuse gibt es mit USB 2, FW400, FW800 und mit 2 SATA-Schnittstellen sowie mit LAN-Interface. Ein interner Ventilator sorgt für ausreichend Kühlung.

sich externe Platten einfach logisch einhängen und bieten dann einen schnellen Datenzugriff.

In den meisten Fällen erweist sich deshalb die extern angeschlossene Magnetplatte (Festplatte) sowohl als schnellste und komfortabelste Lösung für die Datensicherung als auch als preisgünstigste Variante. Hier setze ich (Stand: Mitte 2019) Laufwerke mit einer Kapazität von 6 TB bis 12 TB pro Laufwerk ein. In den kommenden Jahren dürften sich die Kapazitäten weiter nach oben verschieben – 20 TB pro 3,5-Zoll-Laufwerk werden bereits in Aussicht gestellt. Achten Sie aber darauf, welche maximale Plattengröße Ihr System und das externe Gehäuse erlauben – und ob Sie davon booten können, sofern das Laufwerk eine Boot- bzw. Betriebssystem-Partition enthält.

SSD – Solid State Disk

SSDs gehören zu den etwas neueren Speichermedien vom Type Flash-Speicher. Diese haben gegenüber Festplattenlaufwerken den Vorteil, wesentlich schneller zu sein und keine drehenden Teile zu haben. Ihr Stromverbrauch ist damit geringer als bei Festplatten, und sie sind relativ unempfindlich gegenüber Stößen/Erschütterungen.

Der Nachteil von SSDs gegenüber Festplatten ist ihr höherer Preis pro Speichereinheit (z. B. Terabyte) – Tendenz schnell fallend. Die typische Kapazität je Laufwerk/Einheit beträgt 2019 zwischen 250 GB und 4 TB (in dem hier betrachteten Anwendersegment). Ein anderer Nachteil liegt darin, dass die einzelnen Speicherzellen nicht beliebig oft wiederbeschreibbar sind. Ein SSD-Speicher enthält deshalb Reservezellen, die verwendet werden, wenn Zellen ausfallen. Sind diese Reserven erschöpft, ist das Medium nicht weiter beschreibbar. In der Praxis erweist sich dieses Problem aber als geringer, als es sich hier anhören mag.

Das typische Einsatzgebiet für SSDs sind das Betriebssystem-Volume sowie Arbeitsvolumes für die Videobearbeitung. Für das Speichern großer Bildbestände sind SSDs zumeist noch zu teuer. Als Speicher für das Betriebssystem erweisen sich in der Regel Kapazitäten zwischen 500 GB und 1 TB als vollkommen ausreichend – in einer Preisspanne zwischen 80 und 120 Euro in den SATA-Versionen.

Bei der (internen) SSD findet man aktuell drei verschiedene Arten: SSDs mit der klassischen SATA-Schnittstelle (im Format eines 2,5"-Laufwerks), M.2-SATA-SSDs (mit Übertragungsraten bis etwa 1.000 MB/s) sowie schließlich M.2-SSDs mit NVME-Interface. Die SATA-Varianten sind durch das SATA-Interface (SATA-III bzw. SATA-6G)[1] auf etwa 500–550 GB/s beschränkt (theoretisch 600 MB/s). Die NVME-Schnittstelle erlaubt Übertragungsraten bis zu etwa 3.500 MB/s. NVME-Module sind aber auch etwa zwei bis drei Mal teurer als die SATA-Versionen. Die beiden M.2-Arten setzen statt einer klassischen SATA-Schnittstelle passende (unterschiedliche) Steckplätze im Rechner voraus, von denen zumeist nur ein oder zwei Plätze in den typischen Laptops und Workstations vorhanden sind. Die M.2-Riegel haben aktuell Kapazitäten von je 250 GB bis 2 TB. Die beiden schnellen M.2-SSD-Varianten können aber inzwischen auch in entsprechenden externen Gehäusen

1 SATA III (SATA 6G) erlaubt eine maximale Übertragungsrate von 6 Gigabit/s, was theoretisch etwa 600 Megabyte/s entspricht.

Die drei heute typischen Formen von SSDs (von oben nach unten): 2,5"-SATA-SSD, SSD SATA M.2, SSD NVME M.2. Für große File-Server gibt es weitere Bauformen, etwa mit SAS-Interface.

eingesetzt werden. Für große File-Server gibt es weitere Bauformen, die größere Kapazitäten und höhere Transferraten erlauben. Dies ist jedoch nur dann sinnvoll, wenn diese Gehäuse mit entsprechend schnellen Schnittstellen ausgerüstet sind und an einer schnellen Schnittstelle (USB 3.1, Generation 2, USB 4, Thunderbolt 2 oder 3) am Rechner angeschlossen werden können.

Schlussfolgerung zu den Datenträgern: Heute sind Magnetplatten und USB-Sticks (oder SD- oder MicroSD-Speicher höherer Kapazität) für kleinere Datenmengen und externe Festplatten für die Sicherung des Rests für die meisten Fotografen die beste Lösung zur Sicherung und Archivierung der Fotos, und dies möglichst redundant. Dabei dürfte es kein Fehler sein, seine absolut besten Bilder zusätzlich nochmals separat auf einer doppellagigen DVD oder einer Blu-Ray-Disc *off-site* zu halten – im Original und in der optimierten Version.

Natürlich passt man die Plattenkapazitäten an die Größe des eigenen Datenbestands an – jeweils mit 30 % Reserve. Bei den Bilddateien versuche ich, alle Bilder auf einer einzigen Platte unterzubringen statt sie über mehrere Platten zu verstreuen. Das vereinfacht deutlich die Handhabung und Sicherung. Mein Backup-Medium wähle ich in der gleichen Kapazität.

Lagerung der Datenträger und andere Aspekte

Rechnerexterne Datenträger müssen sorgfältig behandelt und richtig gelagert werden. Dabei unterscheiden sich die Ansprüche der unterschiedlichen Datenträgertypen kaum, sieht man einmal davon ab, dass Bänder und Magnetplatten zusätzlich vor Magnetfeldern zu schützen sind. Die wesentlichen Forderungen sind:

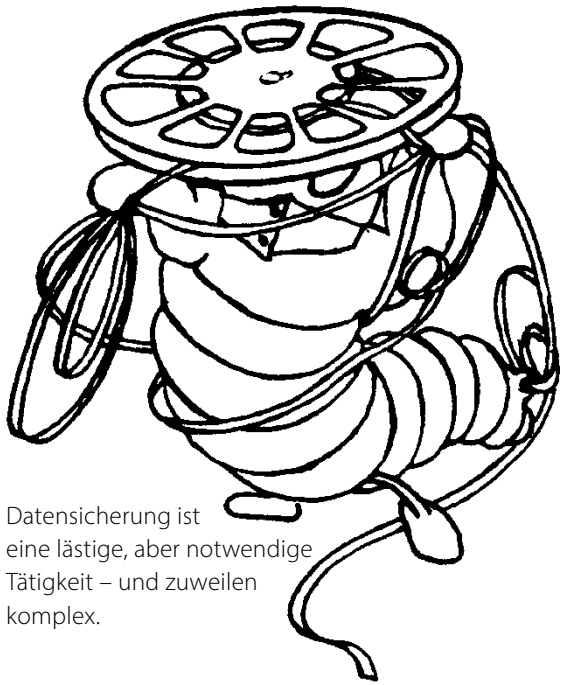
- trockene und staubfreie Lagerung
- mäßige Temperaturen (< 28° C)[1]
- Schutz vor starkem Lichteinfall (insbesondere bei CD/DVD/BD)
- stabile, flache oder senkrechte Lagerung
- Stoßgesicherte Lagerung (insbesondere bei Platten)

Die unabdingbare Beschriftung der Datenträger wurde bereits erwähnt. Benutzen Sie bei CD/DVD/BD dazu geeignete Stifte, die nicht ätzen (zur Sicherheit sollte man nur auf den kleinen inneren Rand des Datenträgers schreiben). Von aufgeklebten Papier-Labels auf CD/DVDs ist dringend abzuraten. Sie können beim Trocknen den Datenträger verziehen und damit beschädigen. DVDs und Blu-Ray-Discs gehören in eine Schutzhülle, und die Schreiboberfläche sollte nicht mit den Fingern berührt werden. Insbesondere DVDs/BDs sollten sorgfältig behandelt und die Schreibfläche nicht angefasst werden. Sie sind der höheren Schreibdichte wegen **wesentlich** empfindlicher als CDs!

Wie bereits erwähnt, empfiehlt es sich bei wertvollen Daten – und eine große, professionelle Fotosammlung gehört dazu – eine Datenträgerkopie an einem anderen, entfernten Ort zu lagern (*off-site*), so dass im Fall eines Brandes oder einer Naturkatastrophe sowie bei Diebstahl noch eine Kopie vorhanden ist.

➜ Die Erfahrung zeigt: Man kauft vorzugsweise die zweitgrößten verfügbaren Kapazitäten, da sie in aller Regel das beste Preis-Leistungs-Verhältnis aufweisen und oft auch eine technisch höhere Zuverlässigkeit bieten. Stand 2019 sind dies bei Festplatten 10-TB- oder 12-TB-Festplatten, sofern man diesen Bedarf hat.

Bei SSDs dürften dies aktuell 1-TB-Modelle sein. Diese Größe würde ich heute auch dann wählen, wenn man für das Betriebssystem mit weniger auskommt. Ist noch ausreichend Speicher frei, so kann man ihn z. B. für den Lightroom-Katalog und Lightroom-/ACR-Caches nutzen, da diese von der höheren Geschwindigkeit profitieren. Bei anderen Anwendungen gibt es ähnliche Speicher, die von schnellen Zugriffen profitieren.



Datensicherung ist eine lästige, aber notwendige Tätigkeit – und zuweilen komplex.

1 Die Haltbarkeit der Daten sinkt bei höheren Temperaturen und bei CDs, DVDs und BDs auch bei stärkerem Lichteinfall steil ab!

Tabelle 5: Übersicht zur Sicherungsstrategie

Datenart	Wann und wie oft?	Womit?	Wohin?	Anmerkung
Systemplatte	Nach dem ersten Aufsetzen, vor jeder großen Änderung, minimal alle 2 Monate	Systemabhängig, z. B. Win: Windows-Backup, Drive Snapshot, Acronis TrueImage; Mac: Carbon Copy Cloner, SuperDuper!, TimeMachine	Auf eigene Partition (bootfähig) auf separatem externem Laufwerk	Überprüfen Sie das Booten oder Wiedereinspielen vom externen Datenträger!
Datenplatte	Abhängig von Änderungen und Wichtigkeit entweder kontinuierlich oder zeitgesteuert oder vor dem Herunterfahren, mindestens einmal pro Woche	Zeitgesteuerte automatische Sicherung (voll und inkrementell), möglichst mit Versionierung	Separate externe Partition, möglichst eine Off-site-Kopie anlegen. Diese darf seltener aktualisiert werden.	Datenbank vor dem Sichern herunterfahren
Datenbanken	Häufig und nach jeder größeren Änderung	Mit Ordner-Synchronisation oder als Teil der Datenplattensicherung	Auf die Sicherung der zugehörigen Datenplatte	Datenbank vor dem Sichern herunterfahren
Spezielle einzelne Ordner	Nach Bedarf oder zeitgesteuert (scheduled)	Bei Bedarf mit Explorer oder Finder, zeitgesteuert mit Ordner-Synchronisation	Separater Datenträger oder auf Platten der normalen Datensicherung	Unwichtige Ordner (z. B. mit temporären Dateien) **nicht** sichern
Laptop	Nach dem Aufsetzen, vor jeder großen Änderung, minimal alle 2 Monate	Wie bei Systemplatte	Wie bei Systemplatte, auf externes, separates Laufwerk (mindestens gleicher Größe)	Platte/Medium sollte bootbar sein
Bilder von Speicherkarte unterwegs	Möglichst bald; Karte erst löschen, wenn mindestens zwei Kopien der Bilder existieren	Downloader; dieser kann evtl. sofort beim Download zusätzliche Kopie erstellen	Laptop + externer Speicher oder Laptop + Speicherkarte	Karte immer in der Kamera formatieren

Überprüfung der Daten

Nach jeder Sicherung – zumindest aber von Zeit zu Zeit – gehören die Daten auf korrekte Übertragung geprüft. Gute Sicherungsprogramme bieten dies als Automatik an. Ein jetzt erkannter Fehler ist sehr einfach zu beheben, ein später erkannter Fehler teilweise schmerzhaft!

Auch später sollten Sie Ihre Daten darauf prüfen, ob sie sich noch fehlerfrei lesen lassen – sowohl den Datenträger mit seinem Dateisystem als auch die Daten bzw. Bilddateien selbst. Dies ist aufwändig, und man macht es nur stichprobenartig von Zeit zu Zeit (etwa einmal im Jahr). Findet man Fehler, so versucht man es mit der zweiten Kopie. Ist diese fehlerfrei lesbar, wird sie sofort nochmals kopiert, und man wirft den defekten Datenträger weg – Geiz ist hier fehl am Platz!

Zur Überprüfung der Konsistenz der einzelnen Bilddateien gibt es einige Hilfsmittel – z. B. den *Integrity-Checker* von Lloyd Chambers [12]. Das Problem liegt nämlich darin, dass eine Datei zwar lesbar sein kann, aus unterschiedlichen Gründen aber trotzdem defekt ist. Dies kann beispielsweise beim Umkopieren passieren.

Umkopieren

Betrachtet man längere Aufbewahrungszeiträume, so muss man daran denken, Daten umzukopieren. Dafür gibt es mehrere Gründe:

- Bei Datenträgern wie Bändern und Magnetplatten ist die Datenpersistenz (Haltbarkeit) begrenzt. Hier spricht also die Datensicherheit für das Umkopieren. Selbst bei CD, DVD und BD sollte man in bestimmten Zeitintervallen zur Sicherheit umkopieren – etwa alle 5 bis 6 Jahre. Für Magnetplatten empfiehlt sich ein Zeitraum von etwa 2 bis 3 Jahren, und zwar immer dann, wenn eine Schnittstelle (wie etwa die inzwischen veraltete PATA-Schnittstelle) ausläuft und kaum noch erhältlich ist. Unter Umständen sind die alten Laufwerke nicht mehr verfügbar. Man denke hier nur an die alten Floppy-Formate oder – wesentlich kürzer – SyQuest-Laufwerke. Es gibt sie heute (nach etwa zwölf Jahren) einfach nicht mehr!
- Sind zwischenzeitlich Datenträger mit mehrfacher Kapazität verfügbar, so lohnt es sich von Zeit zu Zeit, mehrere alte Datenträger auf einen neuen zu-

sammenzukopieren. Weniger Datenträger vereinfachen die Verwaltung und Lagerung. Zugleich erledigt man damit den vorhergehenden Punkt.

- Auch Datenformate überleben sich, wenn auch nur langsam. Aus diesem Grund wird man in größeren Zeitabständen – etwa alle 7 bis 10 Jahre – auch einen Teil seiner Formate konvertieren müssen. Hier sind insbesondere Raw-Dateien kritisch zu betrachten.

  Ein Lösungsansatz könnte hier DNG sein (siehe dazu Fotoespresso 2/2005). Achten Sie darauf, stets einen Konverter für das alte Format zur Verfügung zu haben.

- Sowohl beim Anschluss interner als auch externer Speicher sollte man hochwertige Kabel einsetzen und bei auftretenden Problemen die Kabel überprüfen. Defekte oder schlecht abgeschirmte Kabel sind nicht selten der Grund für Verbindungsprobleme und Übertragungsfehler.

Online-Speicher als Backup?

Ich werde zuweilen gefragt, ob Online-Speicher wie Dropbox, Apples iCloud oder Microsofts OneDrive sich nicht als Backup-Systeme eignen, bieten sie doch oft Automatismen zur Datensicherung. Die Antwort aus meiner Sicht lautet ›**nein**‹ – zumindest nicht für die hier betrachteten Fotografen, seien es Amateure oder Profis. Dafür gibt es mehrere Gründe:

A. Die dort (preiswert) zur Verfügung stehenden Kapazitäten sind zu klein. Bei Microsoft *OneDrive* sind es aktuell 5 GB. Das reicht mit etwas Glück gerade einmal für eine sehr kleine Speicherkarte. Man kann zwar bei den Diensten mehr Speicherplatz kaufen, dann wird es aber teurer (z. B. 50 GB 2 €/Monat).

B. Die Übertragungsraten sind zu langsam und damit die Übertragungszeiten zu lang. Selbst bei einer schnellen DSL- oder Kabelanbindung beträgt die Datenrate im Upload gerade einmal 5 bis 10 MBit bzw. etwa 0,5 bis 1,0 MB/s. Am Beispiel aus Tabelle 3 (Seite 16) würde da die Vollsicherung eines 2-TB-Laufwerks (oder einer Partition) etwa 23,2 Tage dauern (sofern es zu keinem Verbindungsabbruch kommt)! Auch wenn Komplettsicherungen selten erforderlich sein mögen, so dauert bei einem Problem das Rückspielen aller Daten immer noch 2,3 Tage (bei realen maximalen 100 MBit/s bzw. 10 MB/s). In der Regel ist dies deutlich zu lang.

   Anders sieht es aus, wenn man einen solchen Online-Speicher als Backup unterwegs auf einer Reise einsetzen möchte, um eine zweite Sicherungskopie seiner aufgenommenen Fotos zu erstellen. Hier ist das Datenvolumen in der Regel deutlich geringer und man kann – wieder zu Hause – die Daten auf das lokale System herunterladen, sie dort auf Dauer sichern und im Online-Speicher löschen.

   Diese Dienste eigenen sich auch zur Synchronisation kleinerer Datenbestände (E-Mails, Adresslisten, Termine…) zwischen verschiedenen Systemen sowie zum Bildaustausch zwischen unterschiedlichen Plattformen und Parteien.

C. **Gewährleistung!** Lesen Sie einmal in Ruhe und vollständig, welche Garantie der Verfügbarkeit und Datensicherheit Ihnen die genannten Dienste geben. Die Antwort lautet: **keine**. Reicht Ihnen das? (Etwas anderes ist es bei großen kommerziellen Diensten. Diese sind aber deutlich kostspieliger und zielen nicht auf den hier betrachteten Kundenkreis ab.)

D. ›Kein Netzzugriff‹ – keine Verbindung zum Internet – impliziert auch, dass die Sicherungsmöglichkeit oder die Möglichkeit zum Zurückladen gesicherter Daten fehlt.

E. Auch die Vertraulichkeit Ihrer Daten ist in der Cloud bisher eher eine offene als eine geklärte Frage. Insbesondere bei den fast ausschließlich ausländischen Dienstleistern fehlt es hier (aus meiner Sicht) noch an Sicherheit und deren Gewährleistung.

Zusammenfassung

Hier nochmals in aller Kürze meine Empfehlungen zur Datensicherung:

System und Programme: monatliche Sicherung auf bootfähige externe Platten sowie nach jedem größeren Update; jeweils Totalsicherung

Fotodaten: Originale sofort nach Herunterladen auf zweiten Datenträger oder tägliche Sicherung auf einen Near-Line-Speicher (z. B. externe Festplatte oder NAS im direkten Zugriff, ohne dass man explizit den Datenträger einlegen oder anschließen muss).

Arbeitsdateien: Täglich inkrementelle Sicherung mit Halten mehrerer Versionen. Arbeitet man als Amateur oder Profi nicht täglich am Rechner, so sollte die Sicherung zumindest nach jedem Arbeitstag am Rechner erfolgen.

Dazu kommt der regelmäßige Transport einer dritten Kopie zu einer Ablage außer Haus, wobei diese Kopien rotiert werden, sobald aktuellere Kopien vorliegen.

Ergibt sich dies nicht automatisch durch den obigen Ablauf, so sollte man die Daten in größeren Abständen umkopieren. Die Zeiträume dafür haben wir bereits im Abschnitt zum Umkopieren genannt.

Ich habe in diesem Artikel einige Aspekte vereinfacht (z. B. nicht zwischen SATA II und SATA III unterschieden) und Punkte ausgelassen – etwa die der Sicherheit im Sinne der Datenvertraulichkeit. Sowohl Windows als auch Mac OS X bieten integrierte Techniken der Datenverschlüsselung. Dies macht die Systeme aber (abhängig von der dafür verwendeten Technik) langsamer und schafft das Problem der Schlüsselverwaltung und Schlüsselsicherung.

Ich setze solche Gehäuse für jeweils vier Datenträger (Magnetplatten oder SSDs) für meine Workstation ein. Die Platten sind so einfach austauschbar. Ich betreibe sie als JBODs (Just a Bunch of Disks – Einzellaufwerke). Solche Gehäuse gibt es mit eSata-, USB-3-Schnittstelle, Thunderbolt-2-Schnittstelle (wie hier) und inzwischen auch mit Thunderbolt 3. Die hier gezeigten Gehäuse stammen von der Firma OWC und haben hinten einen ausreichend großen, relativ leisen Lüfter für die Kühlung. Die einzelnen 3,5-Zoll-Platten/2,5-Zoll-SSDs haben alle separate Rahmen, in welche die Datenträger einfach mit Schrauben montiert und mit denen sie in die Backplane des Gehäuses eingeschoben und mit der Schraube oben im Gehäuserahmen fixiert werden. Die Preise solcher Gehäuse für vier oder fünf Laufwerke liegen (leer) zwischen etwa 120 Euro (bei USB 3) und 450 Euro für Thunderbolt 3 (jeweils inkl. MwSt.).

Auch das Thema Datenkomprimierung habe ich bisher ausgelassen. Eine Dateikomprimierung bringt aber zumindest bei den meisten Bildformaten (als Teil der Datensicherung oder des Dateisystems) recht wenig Speicherplatzersparnis, da sich JPEG- und bereits komprimierte TIFF- oder PSD-Dateien kaum weiter komprimieren lassen.

Auch muss man bei der Beschaffung von Speicherlaufwerken darauf achten, ob die Kapazität (jenseits von 2 TB) vom Betriebssystem, den eingesetzten Schnittstellen und bei externen Laufgehäusen vom Controller im Gehäuse unterstützt wird. Liegt die Systemplatte auf dem Laufwerk, muss auch der Boot-Loader, der das Betriebssystem lädt und startet, mit der entsprechenden Plattengröße zurechtkommen. Bei Mac-Systemen ist dies kein Problem, bei modernen Windows-Systemen (etwa mit einem EFI-Loader) auch nicht mehr; ältere PCs können aber Restriktionen hinsichtlich der maximalen Größe von Laufwerken aufweisen.

Wichtig ist sicher, sich mit der Thematik zu befassen, bevor das erste Desaster eintritt. Es gilt, sich ein Sicherungskonzept zu überlegen und es dann konsequent und sehr regelmäßig auszuführen – das Unglück ist sonst programmiert!

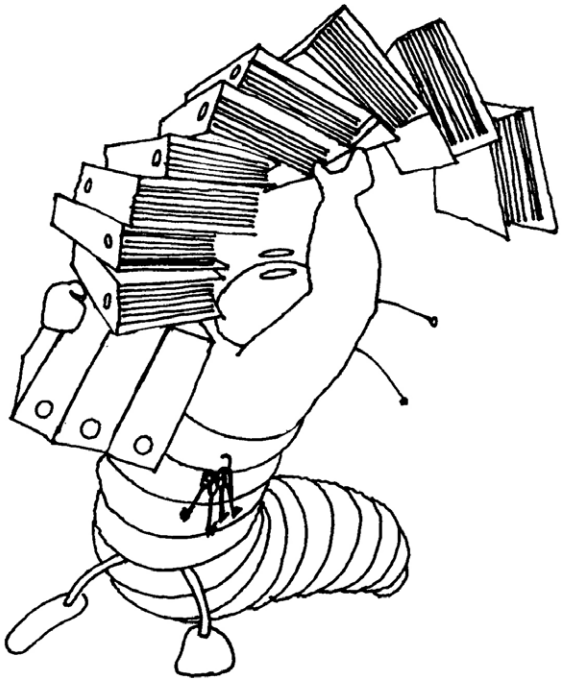
Aufräumen vor dem Sichern?

Man bekommt immer wieder den Ratschlag, vor einer Sicherung das System gründlich aufzuräumen. Für ein gelegentliches Aufräumen spricht aus meiner Sicht viel, insbesondere wenn man ein System auf einen neuen Datenträger migriert, etwa auf eine SSD. Führt man seine Sicherungen aber häufig und möglichst automatisiert durch, was sich dringend empfiehlt, ist ein Aufräumen jedes Mal zuvor eher unrealistisch. Spendieren Sie lieber Ihrem Backup-Medium etwas mehr freien Speicher. Räumen Sie einmal auf, so wird damit – zumindest beim Synchronisieren oder bei der Erstellung einer neuen Vollsicherung – auch Ihre Sicherung ›aufgeräumt‹ und etwas schlanker.

Parallelisierung von Sicherungen

Die meisten der in diesem E-Book angeführten Backup-Lösungen erlauben nur eine sequenzielle Ausführung von Sicherungsaufträgen. In vielen Fällen ist dies akzeptabel und sinnvoll, vor allem dann, wenn Daten oder Volumes von einem Festplattenspeicher oder auf die gleiche Platte gesichert werden. Parallel laufende Auftrage würden nur zu einer ständigen Neupositionierung der Lese-/Schreibköpfe führen und den Sicherungsvorgang damit verlangsamen.

Muss man aber mehrere Quellen von unterschiedlichen Laufwerken oder auf unterschiedliche Plattenlaufwerke sichern, kann eine Parallelisierung sinnvoll sein. In diesem Fall setze ich zwei unterschiedliche Backup-Anwendungen ein und lasse sie – entweder explizit angestoßen oder über eine Zeitsteuerung ausgelöst – zur gleichen Zeit (und damit parallel) laufen. Die Busse moderner Systeme vertragen dieses Vorgehen, ohne dabei zum Engpass zu werden.



Daten, schlecht organisiert, können einem schnell entgleiten!

Man sollte aber nie parallel von der gleichen Quelle oder auf das gleiche Ziel sichern oder synchronisieren!

Terminologie

Die Begriffe, die für unterschiedliche Sicherungstechniken und in den verschiedenen Anwendungen verwendet werden, sind leider nicht ganz einheitlich – in der Praxis sogar recht uneinheitlich. Ich habe deshalb in den nächsten beiden Kapiteln einige Begriffe erläutert und erklärt, was ich unter den Begriffen verstehe.

Zum (vorläufigen) Abschluss:

Aus meiner Sicht gilt: **kein Backup – kein Mitleid!**

Unterschiedliche Backup-Techniken und ihre Terminologie

Es gibt eine Reihe unterschiedlicher Backup-Techniken und leider auch eine uneinheitliche Terminologie. Ich versuche hier, ein wenig Ordnung in die begriffliche Vielfalt zu bringen.

Sichern in spezielle Objekte

Hierbei werden alle zu sichernden Dateien in ein einziges großes ›Objekt‹ gesichert. Dieses Objekt erscheint im Dateisystem als eine große Datei. Auf die darin vorhandenen gesicherten Dateien kann man dann nicht normal mit Anwendungen oder dem Datei-Browser des Systems zugreifen (etwa dem *Finder* unter macOS oder dem *Explorer* unter Windows), sondern benötigt für den Zugriff die spezifische Sicherungs- oder Rückspiel-Anwendung. Bei von *Acronis True Image* erstellten Sicherungsobjekten (mit der Methode *Backup*) ist dies dann beispielsweise wiederum *True Image* bzw. eine Variante davon. Bei Apples *Time Machine*, das ebenfalls ein eigenes Format für das Backup einsetzt, wird *Time Machine* auch für das Restaurieren der Daten verwendet. Ähnliches gilt bei der Microsoft-Anwendung *Sichern und Wiederherstellen (Windows 7)*.

Diese Art der Sicherung hat den Vorteil, dass sich etwas kompaktere Sicherungen ergeben (insbesondere, wenn diese auch noch komprimierte Daten enthalten) und die Sicherung etwas schneller erfolgen kann, da im Ziel nicht viele neue Dateien angelegt werden müssen. Auch ist es effizienter, ein bei der Sicherung entstehendes großes Objekt zu komprimieren als viele kleine einzelne Dateien.

Der offensichtliche Nachteil besteht darin, dass man für einen Zugriff über die spezielle Anwendung gehen muss und eine defekte Platte nicht einfach durch das Sicherungsvolume ersetzt werden kann, sondern erst auf einen anderen Datenträger bzw. dort auf ein Volume zurückgespielt (praktisch entpackt) werden muss, bevor man es normal nutzen kann. Statt ganze Sicherungsobjekte zurückzuspielen, lassen sich in der Regel aber auch einzelne Objekte/Dateien oder ganze Ordner mit Unterordnern aus dem Sicherungsobjekt extrahieren.

Bei dieser Art der Sicherung ist es auch möglich, beim ersten Lauf eine Art Vollsicherung vorzunehmen und anschließend – eventuell in ein neues Sicherungsobjekt – nur noch die Änderungen seit der letzten Sicherung als Inkremente hinzuzufügen.

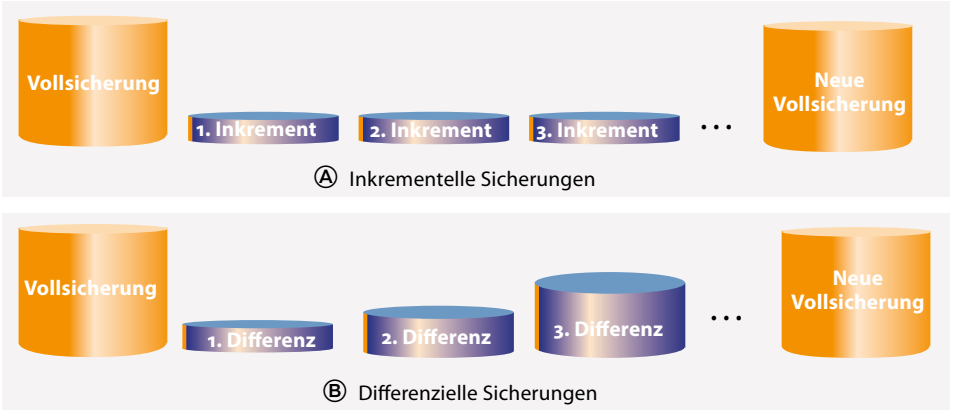


Abb. 1: Bei der ›Inkrementellen Sicherung‹ werden nach der ersten Vollsicherung immer nur noch die Veränderungen zum vorhergehenden Lauf gesichert, bei der ›Differenziellen Sicherung‹ die Veränderungen zur vorhergehenden Vollsicherung.

Inkrementelle Sicherung

Hierbei führt die Backup-Anwendung beim ersten Mal eine vollständige Sicherung durch, sichert aber bei nachfolgenden Läufen (auf das gleiche Zielvolume) nur die seit der letzten Sicherung neu angelegten Dateien/Objekte sowie jene, die geändert wurden. Dies erzeugt in aller Regel sehr viel weniger Datenvolumen und ist deshalb schneller möglich als bei der ersten (Voll-)Sicherung (siehe Abb. 1 Ⓐ).

Sichert das Backup-Programm in spezielle ›Objekte‹, so enthält das neue Inkrement-Objekt nur diese Änderungen. Dies wird beispielsweise von *Acronis True Image* im Standardfall bei der Methode *Backup* genutzt.

Der Nachteil dieser Art der Sicherung besteht darin, dass beim Wiedereinspielen zunächst das Grundobjekt (mit der ersten Komplettsicherung) eingespielt werden muss und danach alle nachfolgenden Inkrement-Sicherungen. Dies kann lange dauern und aufwändig sein und setzt zudem voraus, dass alle zugehörigen Inkremente vorhanden und fehlerfrei sind.

Es empfiehlt sich deshalb bei diesen Anwendungen, von Zeit zu Zeit eine neue Vollsicherung durchzuführen und eventuell die erste alte Vollsicherung sowie die nachfolgenden Inkremente zu löschen.

Differenzsicherung

Bei der Differenzsicherung erfolgt wie bei der inkrementellen Sicherung zunächst eine Vollsicherung. Beim nächsten Lauf werden wie beim inkrementellen Ver-

fahren nur die Unterschiede (die geänderten Dateien) zur Vollsicherung gesichert. Bei der dritten und allen nachfolgenden Sicherungen wird jedoch nicht das Delta zur vorhergehenden, sondern zur letzten Vollsicherung gesichert. Das zu sichernde Datenvolumen ist (nach dem ersten Delta) größer als bei der inkrementellen Sicherung, beim Zurückspielen müssen neben der Vollsicherung aber nur noch die Daten des letzten Differenzlaufs eingespielt werden. Vorhergehende Differenzläufe können gelöscht werden. Abbildung 1 zeigt schematisch die Unterschiede.

Es gibt eine zweite Art der Differenzsicherung, die bei dem in diesem E-Book betrachteten Anwendersegment jedoch keine Rolle spielt. Sie wird dort eingesetzt, wo wirklich große Dateien – etwa sehr große Datenbanken – gesichert werden. Dabei ermittelt die Backup-Software, welche Datenblöcke/Cluster dieser Dateien geändert wurden, und überträgt (oder sichert) nur diese. Dies ist vor allem dann von Vorteil, wenn über (relativ langsame) Netze gesichert wird oder wenn sich bei großen Dateien – etwa den Dateisystem-Dateien virtueller Systeme – oft nur wenige Blöcke ändern. Gleiches gilt, wie erwähnt, für große Datenbankobjekte.

Spiegeln

Beim Spiegeln sorgt die Backup-Anwendung dafür, dass die Objekte (Dateien) im Ziel (bzw. auf dem Backup-Volume) den gleichen Stand wie auf der Quelle haben. Gibt es eine Datei auf der Quelle, die im Ziel noch nicht existiert, wird sie ins Ziel kopiert – möglichst mit allen Attributen (Zugriffsrechte, Erstellungs- und Änderungsdatum, …).

Ist eine Datei in der Quelle neuer als eine gleichnamige Datei auf der Quelle, wird sie durch den neueren Stand ersetzt. Wurde seit der letzten Sicherung eine Datei auf der Quelle gelöscht, wird sie auch im Ziel gelöscht.

Das Spiegeln kann – abhängig vom Backup-Programm – kontinuierlich (bei Änderungen in der Quelle nur mit kleiner Zeitverzögerung) erfolgen oder in bestimmten Zeitintervallen oder nur nach Bedarf.

Datensynchronisierung

Hierbei werden die Daten im Ziel mit den Daten mit den Daten in der Quelle ›synchronisiert‹, d. h. abgeglichen und auf den gleichen Stand gebracht. Dafür gibt es verschiedene Varianten.

Im einfachsten Fall werden Quelle und Ziel miteinander verglichen, und es wird alles, was in der Quelle neuer ist (ein neueres Erstellungs- oder Änderungsdatum hat), auf das Ziel kopiert. Beim Abgleich werden eventuell zusätzlich auch noch die Größen der einzelnen Dateien verglichen, um zu erkennen, ob sie unterschiedlich sind.

Gibt es im Ziel (eine dort anderweitig angelegte) neue oder neuere Datei als in der Quelle, muss per Rückfrage (besser aber per Voreinstellung) festgelegt werden, ob diese gelöscht oder erhalten bleiben soll. Im Standardfall sollte sie gelöscht oder in einen Sonderbereich verschoben werden.

Was aber, wenn in der Quelle Dateien gelöscht wurden, die im Ziel vorhanden sind? Im Standardfall werden diese auch auf dem Ziel gelöscht, um einen Gleichstand zu erreichen.

Bei einigen Anwendungen lassen sich geänderte oder gelöschte Dateien per Option auf dem Ziel-Volume in einen besonderen Bereich verschieben, so dass bei Bedarf noch darauf zugegriffen werden kann. Dies bietet beispielsweise *Carbon Copy Cloner* über eine Einstellung an. Erst wenn der Platz im Ziel knapp wird – bei manchen Programmen wie etwa *Carbon Copy Cloner* lässt sich die Grenze festlegen –, löscht das Sicherungsprogramm im Ziel im Sonderbereich Dateien, um Platz für die neuen Dateien zu erhalten. Für dieses Konzept empfiehlt es sich, das Ziel deutlich größer auszulegen als die Quelle, um auch mehrere alte Stände halten zu können.

Realzeitsynchronisation

Bei der Realzeitsynchronisation werden Dateien gesichert, sobald eine zum Schreiben geöffnete Datei geschlossen wird. Dies stellt sicher, dass geänderte Dateien möglichst bald nach dem Abschluss der Änderung gesichert werden. Es erzeugt aber unter Umständen eine gewisse zusätzliche Systemlast durch den Monitor, der ständig Dateien auf Änderungen überwacht, und

es produziert unter Umständen viele gesicherte Dateiversionen, sofern das Backup-System Versionierung betreibt. Der Zieldatenträger muss hier natürlich permanent angeschlossen/verfügbar sein. Funktional hat die Realzeitsynchronisation gewisse (eingeschränkte) Ähnlichkeiten mit RAID-Lösungen. Ein solche Realzeitsynchronisation wird unter macOS beispielsweise von *FreeFileSync* angeboten und unter Windows von *Personal Backup* und wieder von *FreeFileSync* (zumeist als optionale Komponente).

Backup per direktem Laufwerk-Klonen

Eine schnelle und einfache Backup-Lösung besteht in einem Laufwerk-Cloning, bei dem man eine Harddisk-Docking-Station mit zwei Schächten für Laufwerke einsetzt. In der Regel können solche Stationen sowohl 3,5"- als auch 2,5"-Laufwerke aufnehmen. Hiervon gibt es Versionen, die das Kopieren/Klonen von einem Quell- auf ein Ziellaufwerk selbstständig ohne einen unterstützenden Rechner durchführen können (siehe Abb. 2). Die Kosten solcher Einheiten liegen bei ca. 35–65 Euro.

Voraussetzung ist, dass beide Laufwerke eine SATA-Schnittstelle besitzen und das Ziellaufwerk gleich groß wie oder größer als das Quelllaufwerk ist. Auch die Blockgröße (Sektorgröße, siehe dazu Seite 32) beider Laufwerke muss gleich sein. Zudem müssen beide Laufwerke ›nackt‹ (d. h. ausgebaut) vorliegen. SSDs in M.2-Format (siehe Seite 17) lassen sich damit nicht als Datenträger einsetzen.

Erfolgt das Klonen autark (ohne einen beteiligen Rechner mit entsprechender Software), so erfolgt ein ›dummes‹ Klonen, bei dem einfach Block für Block von der Quelle auf das Ziel kopiert wird – unabhängig von Partitions- und Dateisystemstrukturen.

Eine Anpassung der Partitionsgrößen und anderen Laufwerkparameter (etwa die logische Blockgröße) erfolgt dabei nicht. Ist das Zielvolume größer als das Quellvolume und möchte man den zusätzlichen Platz danach nutzen, muss man mit anderen Mitteln die hinterste Partition später vergrößern oder dort eine zusätzliche Partition anlegen.

Diese Lösungen (blindes Kopieren der Blöcke eines Laufwerks) ist kaum für ein regelmäßiges Backup geeignet, bietet sich für ein schnelles, einfaches Backup von Systemlaufwerken aber an oder um ein System von einer Festplatte auf eine SSD zu migrieren.

Solche Docking-Stationen für SATA-Laufwerke eignen sich auch, um mit entsprechender Backup-Software Sicherungen auf eine ›nackte‹ externe Platte zu machen, die man anschließend offline schaltet und im Schrank oder außer Haus lagern möchte.

Wenn Sie sich eine solche Einheit neu zulegen, sollten Sie ein Gerät wählen, das zumindest USB 3.0, besser noch USB 3.1 oder sogar USB 3.1 Generation 2 bietet – selbst dann, wenn Sie diese Anschlüsse an Ihrem Rechner bisher noch nicht haben. Ihr nächster Rechner wird sicher damit ausgestattet sein, und der Aufpreis ist bei der Anschaffung relativ moderat.

Abb. 2: Eine Harddisk-Docking-Station mit zwei Schächten (beide sowohl für 3,5"- als auch 2,5"-SATA-Laufwerke) erlaubt das autarke Klonen zwischen zwei Harddisk- oder SSD-SATA-Laufwerken. Man kann die beiden Laufwerke aber auch über das Rechner-Interface ansprechen (hier per USB 3.0) und das Sichern oder Klonen mit entsprechender Software vornehmen. Solche Einheiten gibt es von mehreren Firmen.

Laufwerke, Partitionen, Dateisysteme, Volumes

Der Begriff *Laufwerk* sollte zunächst klar sein – es ist ein physikalisches Plattenlaufwerk an einem Rechner. Heute kommen fast ausschließlich Festplattenlaufwerke sowie SSDs (*Solid State Disks*) zum Einsatz. Auch bei SSDs wird der Begriff *Laufwerk* verwendet, obwohl hier nichts mehr ›läuft‹ bzw. sich dreht. Der Begriff *Datenträger* wäre deshalb besser.

Ich gehe nachfolgend zunächst von Laufwerken/SSDs bzw. Datenträgern an Laptops oder in Arbeitsplatzrechnern oder von dort extern angeschlossenen Datenträgern aus und vereinfache ein wenig.

Solche Laufwerke/Datenträger muss man, sofern sie nicht bereits passend vorformatiert sind, zunächst für die Nutzung formatieren (oder umformatieren). Beim Formatieren erhält das Laufwerk eine Art Speicherplatzstrukturierung, *Partitionstabelle* genannt. Eine *Partition* ist dabei ein reservierter Speicherbereich auf dem Datenträger, der in der Partitionstabelle des Datenträgers einen entsprechenden Eintrag hat.

Um eine Partition wirklich als Ablage für Daten/Dateien nutzen zu können, muss man auf der Partition ein *Dateisystem* anlegen. Erst dort hinein können Betriebssystem und Anwendungen Dateien schreiben und von dort lesen. Eine solche mit einem Dateisystem belegte Partition wird als *Volume* bezeichnet.

Für Partitionstabellen gibt es unterschiedliche Formate. Unter Windows ist der Standard inzwischen MBR (*Master Boot Record* mit der *Standard-BIOS-Partitionstabelle,* die maximal vier Partitionen pro Datenträger erlaubt). Moderner ist das Format der GUID-Partitionstabelle (*Global Unique Identifier*), oft mit GPT (*GUID Partition Table*) abgekürzt. In der Welt von macOS ist heute das GUID-Format üblich; unter macOS 9 war es früher das Format *Apple Partition Table*.

Ein Datenträger kann natürlich auch nur eine Partition haben, wie es beispielsweise auf USB-Sticks oder auf den Speicherkarten für Kameras üblich ist (aber nicht erzwungen). Fast immer lässt sich ein physikalisches Laufwerk jedoch in mehrere Partitionen unterteilen. Dies ist dann sinnvoll, wenn das Laufwerk eine größere Datenmenge speichern kann und man seinen Datenbestand unterteilen möchte. Sinnvoll ist eine solche Unterteilung etwa in eine (Betriebs-)Systempartition und in weitere Partitionen (und dort liegende Volumes) für sich häufig verändernde Anwenderdaten.

Ich selbst setze auf meinem Foto-Arbeitsplatzrechner beispielsweise drei Partitionen ein, verteilt über drei Laufwerke:

- Eine Partition ist für das Betriebssystem und sämtliche installierten Programme und Bibliotheken vorgesehen. Dies ist mein Startvolume.

- Eine zweite Partition ist für meine ›Arbeitsdaten‹ reserviert – etwa meine Buchhaltung und die DTP-Dateien meiner Bücher und fotoespresso-Artikel.

- Eine dritte Partition (bei mir auf einem 8-TB-Laufwerk) verwende ich (fast) ausschließlich für meine Bilddateien. Die beschriebene Trennung der Daten hat den Vorteil, dass sie die Sicherung und allgemein die Handhabung vereinfacht.

Auf meinem Arbeitsplatzrechner liegt die Betriebssystem-Partition auf einer SSD (1 TB groß), die nicht weiter partitioniert ist. Die SSD hat den Vorteil, dass das Betriebssystem und die Programme schnell starten. Auch die meisten temporären Dateien, auf welche sie häufig zugreifen, liegen mit auf dieser SSD.

Meine Arbeitsdateien liegen auf einem separaten Plattenlaufwerk, das in zwei Partitionen aufgeteilt ist. Die größere Partition mit 3 TB enthält meine Arbeitsdateien. Dort liegen alle meine Bücher und die zugehörigen DTP- und Bilddateien. Die zweite kleinere Partition dient als Backup-Volume, auf das ich meine Betriebssystem-Partition täglich synchronisiere – also dorthin ein erstes Backup mache. Diese Partition ist wie mein Startvolume 1 TB groß.

Die dritte (Haupt-)Partition für meine Bilddateien, die ich fast vollständig in Lightroom verwalte, ist bei mir 8 TB groß und die einzige Partition auf dem Plattenlaufwerk. (Für diese Kapazität ist mir SSD-Technik bisher zu teuer.)

Viele Fotografen werden mit einer kleineren Kapazität auskommen oder können bei einem großen Laufwerk Arbeitsdateien und Bilddateien entweder auf

zwei getrennten Partionen auf einem größeren Laufwerk ablegen oder sogar in separaten Verzeichnissen (Ordner mit entsprechenden Unterordnern) auf einer Partition halten.

Jede Partition sollte ausreichend Platzreserven für weitere Daten und Datenänderungen haben. Optimal sind 30 %, akzeptabel sind 20 %; kritisch wird es, wenn diese Reserve unter 15 % sinkt. Das (Betriebs-)System kann dann ausgesprochen langsam werden oder sogar wegen Speicherplatzproblemen zum Stillstand kommen oder Fehler melden. (Diese Aussage gilt unabhängig vom eingesetzten Betriebssystem.)

Eine feste Partitionierung wie hier beschrieben ist auf Laptops und Arbeitsplatzrechnern sinnvoll. Sie hat aber den Nachteil, dass man ohne spezielle Hilfsprogramme (auf die ich hier nicht weiter eingehe) bei einem einmal partitionierten Datenträger die Partitionen nicht einfach vergrößern oder verkleinern kann. Damit ergeben sich potenziell Probleme, wenn einmal der Speicherplatz auf einer Partition nicht mehr ausreicht, obwohl andere Partitionen auf dem gleichen Datenträger noch ausreichend freien Platz bieten würden. (Sogenannte ›dynamische Partitionen‹ umgehen dieses Problem.)

Unter neueren macOS-Systemen (ab macOS 10.13) erlaubt das APFS-Dateisystem (eigentlich ist es ein Container-System), in einer statischen Partition mehrere Volumes anzulegen, die sich den Speicherplatz der Partition (des Containers) teilen und dies dynamisch tun. Damit kann bei Bedarf ein Volume innerhalb des Containers mehr Speicher in Anspruch nehmen, wenn ein anderes Volume des Containers den Platz nicht benötigt. Beim Anlegen dieser Volumes lassen sich optional eine minimale Platzreservierung sowie ein Maximum an Speicherverbrauch festlegen.

Es gibt inzwischen auch Lösungen, um dynamische Volumes (Dateisystem-Container) anzulegen, die sich über mehrere Partitionen und sogar mehrere Laufwerke/Datenträger erstrecken können und deren Aufteilung sich auch nachträglich noch ändern lässt. Die Beschreibung dazu würde aber bei weitem den Umfang und die Absicht dieses E-Books sprengen. Diese Technik ist auf Laptops und den typischen Arbeitsplatzrechnern bisher noch nicht üblich und wird primär auf Servern eingesetzt.

Volumes und Datenträger ›auswerfen‹

Mit der Funktion *Auswerfen* wirft man in der Regel einen ganzen Datenträger oder nur eine Partition bzw. das darauf liegende Dateisystem aus, während man mit *Deaktivieren* in der Regel nur ein Volume auf einem Datenträger ausblendet (ein *unmount* darauf ausführt) und es damit für normale Zugriffe nicht mehr verfügbar macht. Beim Auswerfen werden hingegen, so vorhanden, alle Partitionen eines Datenträgers deaktiviert und bei manchen Datenträgern – etwa bei CDs/DVDs und Blu-Rays – der Datenträger auch wirklich physikalisch ausgeworfen bzw. das Laufwerk zur Entnahme geöffnet (nach der vorherigen Deaktivierung). Bei den üblichen externen Platten- und SSD-Einheiten kann man danach den Datenträger entfernen/abstecken/trennen. Vor einem solchen Abziehen/Abstecken sollte man den Datenträger prinzipiell *auswerfen* bzw. alle Volumes darauf *deaktivieren*. Dies stellt sicher, dass im System eventuell noch gepufferte Daten auf das Volume/die Volumes des Datenträgers geschrieben werden und die Volume-Struktur korrekt abgeschlossen wird.

Dateisysteme

Ein *Dateisystem* ist eine weitere Strukturierung des Speicherplatzes, genauer: der Datenblöcke auf einer Partition. Ein spezieller Datenbereich einer Partition dient der ›Buchhaltung‹. Dort ist zunächst die Art des Dateisystems festgehalten – es gibt eine Reihe von Dateisystemformaten. Hier liegt auch eine Liste aller Dateien auf dem Dateisystem, deren Namen, Größen, die Lage der Datenblöcke der Datei (oft in nicht zusammenhängenden Einheiten) sowie die Zugriffsrechte auf die einzelnen Dateien und Ordner (Verzeichnisse). (Der Begriff *Ordner* und *Verzeichnis* bezeichnet die gleiche Art von Objekten.)

Ist auf einer Partition ein Dateisystem angelegt, so muss man dieses Dateisystem noch ›mounten‹ bzw. aktiv schalten, bevor man mit den üblichen Anwendungen darauf zugreifen kann. Dieses Aktivieren oder das ›Mounten‹ erfolgt oft automatisch (etwa beim Systemstart), so dass der Anwender wenig davon mitbe-

kommt. Zuweilen möchte man ein Volume aber explizit deaktivieren – ein *unmount* auf das Volume ausführen. Dies wird teilweise als *Auswerfen* bezeichnet. Man kennt dies vor allem von USB-Sticks und anderen USB-Datenträgern, wo man es unter Windows beispielsweise über die *Auswerfen*-Funktion im Kontextmenü des Finders vornimmt. Unter macOS führt man ein *unmount* (bei im *Finder* selektiertem Volume) über das Kontextmenü (unter der rechten Maustaste) über die Funktion *Auswerfen* aus (es gibt weitere Verfahren).

Zur Erinnerung: Ein *Volume* ist eine *Partition* mit einem angelegten Dateisystem darauf.

Dateisystemarten

Die meisten Betriebssysteme kennen gleich mehrere unterschiedliche Dateisystemarten. Ich beschränke mich hier auf die für den normalen Anwender wichtigsten Varianten (man kann sonst ganze Bücher darüber schreiben). Bei Windows sind dies beispielsweise FAT, FAT32, ExFAT sowie NTFS. macOS wiederum verwendet vorwiegend das Dateisystemformat HFS+ und seit der Version 10.13 (alias High Sierra) auch APFS, kann jedoch auch die verschiedenen FAT-Versionen legen und beschreiben sowie das Windows-Format NTFS lesen, jedoch nicht beschreiben. Mit zusätzlichen Plug-ins – etwa denen der Firma Tuxera [1] – kann macOS auch NTFS beschreiben (und neu anlegen). Linux wiederum hat eine Vielzahl eigener präferierter Dateisystemformate (etwa Ext2, Ext3, Ext4, XFS oder Btrfs), kann

Tabelle 6: Informationen zu unterschiedlichen Dateisystemen unter Windows und macOS

Dateisystem	Gebräuchlich unter	Max. Dateigröße / Volume-Größe	Anmerkungen
FAT[1] **(FAT12)**	MS-DOS	32 MB / 32 MB[7]	Veraltet, noch für Disketten (Floppys) im Einsatz. Dateinamen: 8+3 Zeichen
FAT16[1]	MS-DOS	2 GB / 4 GB[8]	Veraltet
FAT32[1]	MS-DOS, Windows, Kameraspeicherkarten	4 GB /32 GB[6]	Standard für kleinere USB-Sticks und Kameraspeicherkarten. Wird praktisch von allen Systemen unterstützt.
Ex-FAT[1]	Windows, Kameras	16 EB / 16 EB[8]	Standard für USB-Sticks und aktuelle Kameraspeicherkarten. Wird praktisch von allen Systemen unterstützt.
NTFS[2] (Stand 3.1)	Windows 7, 8, 10; kann von **macOS** gelesen werden.	16 EB / 8 PB[8]	Journaling ist der Standard. Empfohlen für Windows-System und Daten. Dateinamen: 255 Zeichen (Dateinamen in Unicode 16); Pfadnamen max. 1024 Zeichen.
HFS+[3] (Stand 2018)	**macOS**; für System- und Daten-Volumes	8 EB / 8 EB	Es gibt das Format auch verschlüsselt. Journaling sollte gewählt werden. Auch mit Verschlüsselung möglich. Dateinamen: 31 (ab Level 2); Dateinamen in Unicode 16.
APFS[4] (Stand 2019)	macOS, iOS, (ab 10.13 für SSDs, ab 10.15 auch für Festplatten)	8 EB / ???	Bisher primär auf Flash-Speicher (SSDs) ausgelegt. Es gibt APFS auch verschlüsselt. APFS erlaubt Schnappschüsse; Journaling ist der Standard. Dateinamen in Unicode 16)
ext2, ext3, ext4	Linux	16 TB / 1 EB	ext4 ist der aktuelle Standard für Linux.
ISO 9660[5] (ISO 9660:1999)	CD, DVD, Blu-Ray Disk. Wird praktisch von allen Systemen unterstützt.	4 GB / ???	Varianten sind das Joliet- und das Rockridge-Format. Wird auch oft als Format für Images verwendet (z. B. für Programmdistributionen). Dateinamen: 31 Zeichen (ab Level 2), 207 Zeichen für Dateipfade

1 Für Details siehe https://de.wikipedia.org/wiki/File_Allocation_Table#exFAT.
2 Für Details siehe https://de.wikipedia.org/wiki/NTFS.
3 Für Details siehe https://de.wikipedia.org/wiki/HFS_(Dateisystem).
4 Für Details siehe https://de.wikipedia.org/wiki/Apple_File_System.
5 Für Details siehe https://de.wikipedia.org/wiki/ISO_9660.
6 32 GB für das Volume gilt für Windows. Dieses Limit lässt sich mit Third-Party-Werkzeugen aufheben (bis zu 16 TB).
7 Bei 8 KB Cluster, 16 MB bei 4 KB Cluster
8 Die maximale Volumegröße ist auch abhängig von der Clustergröße und der jeweiligen Implementierung,
TB Terabyte = 1024 Gigabyte
PB Petabyte = 1024 Terabyte
EB Exabyte = 1024 * 1024 Terabyte
ZB Zetabyte = 1024 * 1024 * 2014 Terabyte

aber sowohl die verschiedenen FAT-Systeme lesen und beschreiben als auch das Windows-NTFS sowie mit bestimmten Erweiterungen das von Apple stammende HFS+. Alle drei Plattformen (Windows, macOS, Linux) beherrschen zusätzlich das ISO-9660-Format, das man überwiegend auf CDs, DVDs und Blu-Rays verwendet und von dem es wiederum eine Reihe von Varianten gibt.

Im Standardfall wird man für SSDs und Plattenlaufwerke unter Windows NTFS (*NT File System*) verwenden. Es ist auch für größere Datenträger ausgelegt und bietet gegenüber FAT und FAT32 viele Vorteile, sollte deshalb im Standardfall für SSDs und größere Plattenlaufwerke verwendet werden. FAT ist ein recht altes Dateisystem und auf Dateigrößen von 4 GB und Datenträgergrößen von maximal 4 TB beschränkt. Man verwendet es heute aber noch in praktisch allen Speicherkarten der Digitalkameras. FAT32 ist eine Erweiterung/Modernisierung von FAT und erlaubt längere Dateinamen (auch in der ISO-8-Kodierung), mehr Dateien pro Datenträger sowie Dateigrößen von mehr als 4 GB und Datenträgergrößen von bis zu 4 TB. Auf größeren Kameraspeicherkarten sollte man heute ExtFAT verwenden, da es große Dateien (> 4 GB) sowie von praktisch allen Betriebssystemen unterstützt wird.

Unter macOS verwendet man auf älteren Systemen für SSDs das HFS+-Format und ab macOS 10.14 (alias Mojave) primär APFS. Ab dem Ende 2019 kommenden macOS 10.15 (alias Catalina) wird APFS (in einer dann weiterentwickelten Version) der Standard für SSDs und Festplatten sein. Die Backup-Programme unter macOS werden dafür (aus verschiedenen Gründen) eine Weiterentwicklung erfahren müssen.

Um auf die Dateien eines Volumes mit den üblichen Anwendungen zugreifen zu können, muss man das Volume aktivieren. Dies wird auch als *mounten* bezeichnet (die Deaktivierung entsprechend als ›*unmounten*‹) Im Standardfall arbeitet man deshalb auf Volumes. Das Betriebssystem mit seinen Treibern verdeckt weitgehend die Unterscheide zwischen den unterschiedlichen Dateisystemarten der Volumes – soweit möglich.

Container

Unter einem *Container* versteht man eine Art virtuellen Datenträger, in dem wiederum mehrere Partitionen/Dateisysteme liegen können. Container werden z. B. unter macOS als eine Art Behälter für APFS-Dateisysteme verwendet. Gegenüber einer normalen Partition liegt hier der Vorteil darin, dass sich Container über mehrere Laufwerke hinweg erstrecken können und die Grenzen (Größen) der darin liegenden Dateisysteme flexibler sind, d. h. sich ohne Neuformatierung verschieben können). Unter anderen Systemen werden diese Container auch (etwas verwirrend) als *Volumes* bezeichnet.

Einige Begriffe bei Datenträgern und Backups

Verschlüsselung

Es wird vielfach empfohlen, Datensicherungen auch gleich zu verschlüsseln, um eine ungewollte Nutzung durch Dritte zu verhindern. Die Verschlüsselung ist jedoch ein etwas komplexes Thema und hat (zumindest) vier zu betrachtende Aspekte:

A. die dafür eingesetzten Techniken (Programme, Verfahren und Schlüssellängen),
B. der Umgang mit den Schlüsseln und deren Sicherung,
C. die Performance-Aspekte,
D. verschlüsseltes System-/Boot-Volume

Eine Verschlüsselung kann sowohl durch die Sicherungsanwendung selbst erfolgen (was z. B. *Acronis True Image* anbietet) oder durch das Betriebssystem, wenn dies für den Zieldatenträger oder das Zielvolume dort aktiviert ist. Eine Verschlüsselung hat Vor- und Nachteile.

Performance-Aspekte der Verschlüsselung

Die Ver- und spätere Entschlüsselung kann sowohl rein per Software erfolgen oder aber Hardware-unterstützt oder rein per Hardware. Bei der reinen Software-Variante kann die Verschlüsselung (und später die Entschlüsselung) den Sicherungsprozess spürbar verlangsamen. Moderne Rechner (CPUs) haben bereits Instruktionen (Befehle auf CPU-Ebene), die die Ver- und Entschlüsselung unterstützen/beschleunigen. Bei den

aufwändigeren neueren Rechnern finden wir zusätzlich spezielle Sicherheitschips, die die Ver- und Entschlüsselung in starkem Maße beschleunigen. Und fast alle modernen SSD-Speicher bieten inzwischen eine Ver- und Entschlüsselung durch den integrierten Controller, was zu kaum spürbaren Zeitverlusten führt.

Verschlüsselung durch Anwendung oder Betriebssystem

Während macOS seit einigen Versionen eine Verschlüsselung (beim Schreiben; beim Lesen die Entschlüsselung) von entsprechend angelegten Dateisystemen anbietet,[1] gibt es dies seit Windows 7 auch unter Windows mit der *BitLocker*-Funktion. Für Windows 7 und 8 wird dies jedoch nur in den Ultimate- und Enterprise-Versionen angeboten, mit Windows 8 und 10 in den Pro-und Enterprise-Versionen, nicht jedoch in den Windows-Home-Systemen.[2] Die Ver- und Entschlüsselung erfolgt unter Windows mit Hilfe des TPM-Moduls (*Trusted Platform Module*), das die Schlüssel verwaltet und die Ver- und Entschlüsselung durchführt.

Der Vorteil ist offensichtlich. Der Nachteil liegt in einem erhöhten Rechenaufwand beim Sichern und beim Zurückspielen. Wie gravierend die Verlangsamung ist, hängt auch von der Leistung Ihres Systems ab. Es gilt dabei zu bedenken, dass sich verschlüsselte Daten kaum komprimieren lassen (sofern die Komprimierung auf den verschlüsselten Daten erfolgen sollte).

Eine ganze Reihe neuer Flash-Speicher bietet eine automatische Verschlüsselung über ihren Controller an. Ein Geschwindigkeitsnachteil ergibt sich dann durch die Ver- und Entschlüsselung kaum.

Daneben brauchen Sie ein gute Schlüsselverwaltung. Geht der Schlüssel verloren, sind ihre verschlüsselten Daten nutzlos. Ist der Schlüssel nicht sicher – wegen der kurze Länge, einem trivialen, leicht erratbaren Passwort oder wegen einer unsicheren Speicherung – so ist Ihre Verschlüsselung ebenso nutzlos oder zumindest geschwächt, abhängig davon, welchen Aufwand der Angreifer betreiben möchte.

In der Regel empfiehlt es sich, vom Schlüssel eine Sicherung zu erstellen und diese wiederum sicher zu lagern. Bei der Windows-BitLocker-Funktion wird der Schlüssel (auch als *Recovery-Key* bezeichnet)[3] auf einem separaten USB-Stick oder auf einer SmartCard gespeichert. Dieses Gerät muss beim Systemstart angeschlossen und sollte zusätzlich über eine PIN gesichert sein. Pro Partition wird ein Schlüssel verwendet und gespeichert.

Wird das Systemvolume verschlüsselt, benutzt das System ein kleines zusätzliches Boot-Volume, von dem zunächst eine Software gebootet wird, die gewisse Konsistenzprüfungen vornimmt (um Manipulationen zu erkennen) und dann den Schlüssel abfragt, um damit auf das verschlüsselte Systemvolume zugreifen zu können. Dies bringt die zusätzliche Komplikation mit sich, dass in dieser Start-Software standardmäßig eine englische Tastatur aktiviert ist, was bei der Wahl des Passworts und dessen Eingabe zu beachten ist. Die Verschlüsselung selbst erfolgt bei BitLocker standardmäßig per AES mit einer Schlüssellänge von 128 oder 256 Bit.

Ein weiterer Nachteil verschlüsselter Daten kann darin liegen, dass beim Umkippen einzelner Bits in den Daten der Rest der Datei (oder zumindest Teile davon) nicht mehr entschlüsselbar ist. Ich selbst verzichte aus diesem Grund auf eine Verschlüsselung meiner Backups. Betrachtet man hingegen moderne SSD-Laufwerke, so kann man dort im Controller die Verschlüsselung durchführen lassen, und zwar ohne große Effizienzverluste. Das Schlüsselproblem bleibt jedoch bestehen.

Daneben bietet nicht jede Backup-Anwendung eine Verschlüsselung an. Insbesondere die Synchronisationsprogramme verzichten aus offensichtlichen Gründen darauf.

1 Man legt dazu ein Dateisystem mit Verschlüsselung an. Siehe dazu Abbildung 6 auf Seite 38.

2 Bei einigen Rechnern, in den Unterlagen kaum zu finden, wird die Verschlüsselung hardwareunterstützt auch in den Installationen von Windows Home angeboten – eine recht unübersichtliche Angelegenheit.

3 Das BitLocker-System verwendet eine asymmetrische Verschlüsselung, bei der ein Schlüssel für die Verschlüsselung und ein ein zweiter Schlüssel für die Entschlüsselung verwendet wird.

Zugriffsrechte (ACLs)

Access Control Lists – kurz ACLs – erlauben es, für Dateien und Verzeichnisse (Ordner) relativ feingliedrig festzulegen, wer was mit bzw. auf dem betreffenden Objekt tun darf. In der Regel sind Zugriffsrechte differenziert (zumindest) nach dem Besitzer (der *Owner* – demjenigen, er die Datei angelegt hat) und einer Gruppe (damit lassen sich Anwender mit ähnlichen Zugriffsrechten gruppieren) sowie in alle anderen Anwender. In der Regel kommen noch die Rechte eines Super-Users (eines Administrators) hinzu. An Funktionen wird unterschieden zwischen *Lesen*, *Schreiben*, *Lesen & Schreiben, Löschen* sowie nach *Ausführen* (interessant für Programme und Skripten). Alle modernen Dateisysteme (NTFS, HFS+, APFS) unterstützen solche ACLs. Bei den einfacheren Systemen (etwa FAT, FAT16 und FAT32 fehlt diese Möglichkeit.

Beim Backup von Dateien, Ordnern und ganzen Dateisystemen möchte man in der Regel diese Zugriffsrechte beim Kopieren übernehmen, was zum Teil aber Administrationsrechte erfordert.

Snapshots/Schattenkopien

Unter einem *Snapshot* versteht man in diesem Zusammenhang eine Funktion, die es erlaubt, den Zustand eines Dateisystems/Volumes auf einem bestimmten Stand einzufrieren. Ein Grund kann sein, dass der aktuelle Stand problemlos gesichert werden soll, ohne dass während der Sicherung neue Schreibvorgänge die gerade zu sichernde Datei ändern. Kommen im laufenden Betrieb neue Schreibvorgänge hinzu, so werden diese in einen neuen Bereich des Volumes geschrieben, was entsprechend freien Speicherplatz voraussetzt. Ein anderer Grund für einen Snapshot kann sein, dass man vor der Installation eines neuen Programms oder eines Updates einen Wiederaufsetzpunkt haben möchte, falls bei der Installation etwas schief geht. Unter Windows werden diese Snapshots als *Volumeschattenkopien* oder nur *Schattenkopien* bezeichnet und stehen unter dem Dateisystem NTFS zur Verfügung. Die meisten Dateisysteme erlauben aber nur eine begrenzte Anzahl solcher Snapshots. Bei NTFS (in der aktuellen Implementierung) sind es maximal 127. Dabei ist zu bedenken, dass jeder Snapshot zusätzlichen Speicherplatz kostet, etwa dadurch, dass von Dateien mehrere Versionen bestehen können – solche vor dem Snapshot und solche, die danach modifiziert wurden.

Das Dateisystem muss solche Snapshots unterstützen. Unter Windows ist dies mit NTFS (in den aktuellen Versionen) möglich, unter macOS erst mit dem neueren APFS. Diese Snapshot-Funktion wird auch von einigen Backup-Anwendungen bei der Erstellung von Backups verwendet.

Versionierung

Unter *Versionierung* versteht man eine Technik, bei der man im Backup mehrere Versionen/Arbeitsstände einer Datei hält statt nur die der letzten Sicherung. Es ist zuweilen ausgesprochen nützlich, wenn man im Backup auf einen früheren Bearbeitsstand zurückgreifen kann – etwa weil die letzte Version durch menschliche oder technische Fehler unbrauchbar wurde oder weil man nochmals auf einen Zwischenstand zugreifen möchte, zum Beispiel bei Bildern oder DTP-Dateien. Betreibt man Versionierung, sollte das Backup-Volume deutlich größer als der aktuell belegte Speicherplatz auf dem Quellvolume sein – der durch die Versionierung potenziell höheren Anzahl von gesicherten Dateien wegen.

Für eine solche Versionierung gibt es unterschiedliche Ansätze. Einer besteht darin, unterschiedliche Zeitebenen in den Backups anzulegen. Dies tut beispielsweise Apples *Time Machine*. Eine andere Lösung besteht darin, statt bei einem späteren Backup eine ältere Dateiversion zu löschen bzw. zu überschreiben, diese in einen speziellen Backup-Bereich zu verschieben und mit einer Versionsnummer oder einem Zeitstempel zu versehen.

Versionierung bieten – zumindest optional – beispielsweise die Backup-Anwendungen *Carbon Copy Cloner*, *FreeFileSync, Time Machine* und *Dateiversionsverlauf* von Windows. Auch die Microsoft-Backup-Anwendung *Backup & Restore* unterstützt dies.

S.M.A.R.T-Status

SMART oder S.M.A.R.T. steht (hier) für ›*Self Monitoring Analysis and Reporting Technology*‹. Damit ist eine Technik gemeint, die Informationen zum Zustand bzw. die

Fehlermeldungen eines Laufwerkes sammelt. Über den SMART-Stataus lässt sich frühzeitig erkennen, wenn ein Laufwerk gehäuft Fehler zeigt, was auf einen baldigen Ausfall hinweisen kann. Die meisten modernen Magnetplatten und SSDs bieten über ihren Controller eine entsprechende Funktion. Es gibt eine ganze Reihe kleiner Dienstprogramme, die den SMART-Status von Laufwerken überwachen und anzeigen. Unter macOS ist es z. B. das *Festplattendienstprogramm* (siehe Abb. 2, Seite 37) – jedoch nur bei direkt angeschlossenen Laufwerken und zumeist nicht, wenn das Laufwerk in einem externen USB-Gehäuse mit eigenem Controller steckt.

Blockgröße und Cluster

Auf den Laufwerken wird die Information in zusammenhängenden Einheiten – *Blöcken* – abgelegt. Beim Lesen und Schreiben auf unterster Treiberebene wird in Einheiten dieser Blöcke geschrieben und gelesen. Lange Zeit war die Standardblockgröße 512 Byte. (Unter Windows wird die Blockgröße teilweise – etwas verwirrend – auch als *Sektorgröße* bezeichnet.) Mit größer werdenden Laufwerken wurde diese Größe auf 4 KB (4096 Byte, zuzüglich Prüfsummen) erhöht. Konnte man früher die Blockgröße beim Low-Level-Formatierung einer Platte noch vorgeben, ist dies heute nicht mehr möglich (oder zumindest dringend davon abzuraten, da die Festplattentechnik zu komplex wurde). Die Laufwerke kommen heute vom Hersteller fest vorformatiert. Weder Windows noch macOS stellen für eine solche Low-Level-Formatierung Programme zur Verfügung. Eine höhere Blockgröße erlaubt auf den Festplattenlaufwerken eine etwas höhere Kapazität (da weniger Platz für die Lücken zwischen den Blöcken verloren geht) und eine etwas höhere Lese- und Schreibgeschwindigkeit. Sie sorgt aber auch für einen etwas höheren Verschnitt. Ist eine kleine Textdatei z. B. 500 Byte groß, so beansprucht sie bei einer Blockgröße von 512 Byte einen 512-Byte-Block, bei einer Blockgröße von 4 K jedoch ebenso einen 4-K-Block. (Einige Dateisysteme versuchen dies zu optimieren, indem sie ›Reste‹ mehrerer ›Dateireste‹ in einen solchen großen Block legen). Eine höhere Blockgröße ist also für viele kleine Dateien suboptimal, für große Dateien – etwa typische Bilddateien – aber gut.

In vielen Fällen möchte man für die Verwaltung belegter und freier Blöcke in einem Dateisystem jedoch mehrere Blöcke in einem sogenannten *Cluster* (*Zuordnungseinheit*) zusammenfassen. Dateisysteme verwalten deshalb Cluster, und beim Anlegen eines Dateisystems (beim Formatieren eines Volumes) kann man bei einigen Anwendungen deshalb die Clustergröße vorgeben – jeweils in einem Vielfachen der Blockgröße. (Für Fotografen und Privatanwender spielt dies nur eine Rolle, wenn man sehr große Datenträger formatiert oder Datenträger für spezielle Zwecke.) So verwendet man (abhängig auch vom eingesetzten Datei- und Betriebssystem) heute Cluster von 512 Byte (was eine 512-Byte-Formatierung voraussetzt) und 64 KB – Letztere hauptsächlich für den Einsatz von großen Datenbanken. Es sind jedoch auch noch größere Clustergrößen möglich. Bei größeren Plattenlaufwerken (ab etwa 4 TB) ist die dort übliche Blockgröße von 4 KB auch die Clustergröße 4 KB.[1] Gibt man unter Windows beim Formatieren einer Partition (z. B. mit der *Datenträgerverwaltung*) für NTFS die Clustergröße nicht explizit an, so wählt die Software eine Clustergröße abhängig von der Größe des Volumes – je größer das Volume, umso größer die Cluster.

MBR und GPT – Partitionstabellen

Formatierte und partitionierte Datenträger haben zumindest auf den ersten physikalischen Blöcken eine sogenannte Partitionstabelle. Diese enthält eine Reihe von Verwaltungsinformationen für den Datenträger sowie die Angabe, wo die erste Partition beginnt und wie groß sie ist (teilweise auch Verweise auf weitere Partitionen). Davon gibt es mehrere Varianten. Am gebräuchlichsten sind *MBR (Master Boot Record)* und *GPT* (*Global Unique Identifier Partition Table*).

MBR ist die recht alte Version einer Partitionstabelle. Sie erlaubt maximal vier Partitionen pro Datenträger – unter Windows sind es (maximal) drei *Primärpartitionen* und eine *Erweiterte Partition*. Eine *Erweiterte Partition* wiederum kann mehrere *logische Laufwerke* (*logical drives*) enthalten. Meines Wissens sind es unter Win-

1 Welche Clustergröße ein Dateisystem hat, lässt sich unter Windows mit folgendem Kommando abfragen:
›fsutil fsinfo ntfsinfo c:‹ . (Ersetzen Sie ›c:‹ durch den Laufwerksbuchstaben des gewünschten Volumes. Dieses Kommando muss mit Administrationsrechten ausgeführt werden.

dows 10 bis zu 255 logische Laufwerke, von denen sich mehrere zu einem Volume zusammenfassen lassen.

Ein solcher virtueller Datenträger darf sich dann auch über mehrere physikalische Festplattenlaufwerke oder SSDs erstrecken. Diese Virtualisierung wird bei Windows durch den *Logical Volume Manager* – kurz LVM – realisiert (und hier nicht weiter beschrieben). Zusätzlich sind die Partitionen eines MBR-Systems auf maximal 2 TB beschränkt.[1] Unter Windows wird für Partitionen auch der (aus meiner Sicht) etwas missverständliche Begriff *Datenträger* verwendet.

Moderner und deutlich flexibler als *MDR* ist *GPT* (oder *GUI Partition Table*). GPT erlaubt, da eine 32-Bit-Struktur eingesetzt wird, sehr viel mehr Partitionen pro Datenträger (in der Windows-Implementierung bis zu 128). Die einzelne Partition (bzw. das Volume darauf) kann auch sehr viel größer sein als bei MBR (selbst bei einer Blockgröße von 512 Byte). Das Limit liegt bei 128 Exabyte ($128*2^6$ Terabyte). Dies ist sehr viel größer als die größten Festplattenlaufwerke, die heute angeboten werden (2019 sind es maximal 20 TB), selbst wenn man mehrere dieser Laufwerke zu einem größeren Volume kombiniert.

Der Boot-Loader des Rechners ist ein Stück Firmware (das BIOS oder das UEFI-System). Er sucht beim Einschalten bzw. beim Booten des Rechners nach einem Boot-Block auf einem der angeschlossenen Laufwerke. Der Boot-Loader lädt diesen Block in den Hauptspeicher und startet das darin vorhandene Miniprogramm, das wiederum ein zweites, etwas mächtigeres Ladesystem (Prográmmchen) enthält. Erst dieses lädt (zumindest unter Windows) das eigentliche Betriebssystem (Windows).

Einige (zumeist ältere) Rechner mit einem älteren BIOS können nur Systeme von einem Laufwerk mit MBR-Partitionstabelle laden. Ist dann einmal ein halbwegs aktuelles Windows gestartet (Windows 7/8/10), so kann dieses auch mit Laufwerken im GPT-Format umgehen. Die Wahl zwischen einer MBR und einer GPT-Struktur kann also durchaus relevant sein. (macOS beherrscht seit langem GPT und handhabt das Booten sehr viel eleganter und flexibler als Windows. Dort sollte man praktisch immer GPT wählen.)

Modernere PCs (und alle Apple-Systeme) verwenden statt des altertümlichen BIOS ein UEFI-Startsystem (auch als *UEFI-BIOS* bezeichnet). Ein UEFI-System (*Unified Extensible Firmware Interface*) kann sowohl von einem MBR- als auch von einem GPT-Datenträger Systeme starten.[2] Im Standardfall setzt man auf diesen Systemen jedoch Laufwerke mit GPT für das Boot-System ein.

Unter halbwegs aktuellen macOS-Systemen haben die normalen Laufwerke – zumindest jene, auf denen sich ein bootfähiges macOS befindet – den Typ GPT.

Universal Restore

Unter Windows wird zuweilen der Begriff *Universal Restore* verwendet. Dies ist beispielsweise bei einer Funktion von *Acronis True Image* der Fall oder beim *AOMEI Backupper* [28]. (Man findet den Begriff auch in einigen Produktbeschreibungen anderer Backup-Anwendungen für Windows-Systeme.) Gemeint ist damit eine Sicherung des Systemlaufwerks, das sich nicht nur auf dem ursprünglichen PC, sondern auch auf einem PC mit geänderter Hardware installieren lässt – etwa wenn das Motherboard des ursprünglichen PCs oder Laptops defekt ist und man seine Systemsicherung auf eine neue Hardware zurückspielen möchte. Das *Universal-Restore*-System enthält dann umfassendere bzw. mehr Treiber für verschiedene Hardware-Komponenten. Sie erlauben auf dem neuen System zumindest das Betriebssystem zu booten und den Bildschirm anzusteuern (oft nur in einer kleinen Auflösung) und bei Bedarf noch fehlende Treiber nachzuladen.

Die Notwendigkeit eines solchen Systems besteht unter macOS kaum, da Apple die Hardware der Systeme sehr viel stärker kontrolliert und die Systeme (macOS) auf praktisch allen Macintosh-Systemen laufen können – zumindest was die Unterstützung der verschiedenen Festplattenlaufwerke und Grafikkarten betrifft. Für wesentlich neuere Hardware benötigt man auch dort eventuell aktualisierte Systeme, die man bei Bedarf aber kostenlos aus dem Apple *APP Store* beim Restaurieren herunterladen kann.

1 Die 2-TB-Beschränkung gilt, sofern das Laufwerk mit 512 Byte großen Blöcken (Segmenten) formatiert ist, was bei den üblichen Laufwerken der Standard ist. Formatiert man das Laufwerke hingegen mit 4-K-Blöcken, so kann ein Laufwerke mit einer MBR-Partitionierung 16 TB nutzen.

2 Einige ältere UEFI-Systeme können ausschließlich von einem Datenträger mit GPT-Tabelle booten.

Der Begriff *Image* hat zahlreiche Bedeutungen. So ist auch ein Bild ein Image. Im Zusammenhang mit Dateisystemen ist damit aber ein ›Objekt‹ bzw. eine (zumeist große) Datei gemeint, die vom Betriebssystem als eine Art virtuelles Volume (virtueller Datenträger) behandelt wird. Es gibt deshalb verschiedene Image-Formate. Diese werden teilweise auch als *virtuelle Laufwerke* bezeichnet (zumeist unter Windows). Ein Beispiel sind ISO-9660-Images. (Es gibt davon eine ganze Reihe von Varianten, darunter das Joliet- und das Rockridge-Format). Sie liegen entweder direkt auf einer CD, DVD oder einer Blu-Ray-Disc oder in einer Datei und können vom Betriebssystem wie ein Volume aktiviert (*gemountet*) werden. Man kann dann darauf durch das dort vorhandene Dateisystem navigieren und einzelne Dateien oder Verzeichnis lesen oder davon kopieren.

Images können aber auch andere Dateisystemformate enthalten. Unter macOS lassen sich mit dem *Festplattendienstprogramm* Images neu anlegen (siehe Seite 36) sowie als Volume mounten und danach darauf zugreifen. Beim Anlegen eines neuen Dateisystem-Images im *Festplattendienstprogramm* kann man angeben, welches Dateisystemformat verwendet und welche Art von Zugriffen möglich sein sollen. Diese Images unter macOS haben dann zunächst den Typus (bzw. die Endung) ›*.dmg*‹ (für *Disk Image*).

Das Image hat teilweise den Charakter eines Datenträgers, kann also mehrere Partitionen haben und unterschiedliche Partitionstabellen. Beim richtigem Typ lässt sich davon booten – etwa um ein kleines Hilfssystem für die Systempflege oder Systemwiederherstellung zu starten oder um ein neues Betriebssystem auf ein vorbereitetes Volume neu aufzuspielen. Das Image bzw. die darauf befindlichen Volumes werden einfach per Doppelklick darauf aktiviert (gemountet). Danach kann mit entsprechenden Rechten und Verfahren darauf zugegriffen werden.

Nach einem Auswerfen verschwindet das Volume (bis zum nächsten Aktivieren) wieder aus den Liste der sichtbaren Volumes (Datenträger).

Auch Windows kennt solche Dateisystem- bzw. Datenträger-Images. Dort wird oft das ISO-9660-Format für die Distribution von Betriebssystemen verwendet. Es gibt aber auch unter Windows eine Vielzahl von Image-Nutzungen. So wird im Standardfall ein Windows-Distributionsmedium als Image ausgeliefert, und das Sichern des Startlaufwerks erfolgt im Standardfall ebenso in einem speziellen Image-Format – etwa bei Verwendung der Windows-Anwendungen *Versionsverlauf* und ›*Sichern und Wiederherstellung (Windows 7)*‹.

Einige Formate für solche Image-Dateien bzw. *virtuellen Laufwerke* kann man unter Windows mit der *Datenträgerverwaltung* (siehe Seite 77) über die Menüfolge Aktion ▸Virtuelle Festplatte erstellen anlegen.

Solche Images sind auch dann praktisch, wenn man eine größere Anzahl von Dateien als Bündel in einer einzigen Datei übertragen möchte oder auf einer CD, DVD oder Blu-Ray-Disk im ISO-9660-Form at weitergeben möchte

Einige Performance-Aspekte

Der freie Speicherplatz auf einem Laufwerk hat Einfluss auf die Performance. Es gilt die Faustformel, dass auf dem Arbeits-Volume (der Partition) immer etwa 20 %, mindestens aber 10 % Platz frei sein sollte, da sonst das Betriebssystem das Dateisystem ständig ›optimieren‹ muss, wenn Dateien gelöscht und neue angelegt werden. Unterhalb von 10 % freiem Platz sinkt die Performance spürbar. Diese Faustformel muss man auf dem Backup-Datenträger nicht unbedingt beachten, da hier weniger/seltener gelöscht und hinzufügt wird, sondern das Medium weitgehend linear beschrieben wird.

Werden die Daten über eine langsame Leitung auf ein entferntes System gesichert, kann es sinnvoll sein, die Daten vor der Übertragung zu komprimieren und komprimiert wieder herunterzuladen und lokal zu dekomprimieren.

Bei Übertragungen über ein externes Netzwerk – typisch über das Internet – ist zu bedenken, dass bei sehr langen Übertragungen (etwa jenseits von etwa zwei Stunden) die Wahrscheinlichkeit für eine temporäre Netzwerkunterbrechung deutlich steigt. Dann ist die Frage, ob die Sicherungssoftware damit fertig wird oder die Sicherung abbricht.

Im Übrigen spielt auch – neben der Anzahl und dem Umfang der zu sichernden Daten – die Lesegeschwindigkeit in der Quelle sowie die Schreibgeschwindigkeit auf dem Ziel und zusätzlich die Anbindung des Ziels eine Rolle. Ein schnelle externe Platte nützt nichts, wenn sie über eine langsame Verbindung (etwa per USB 2) angebunden ist.

Datenträgerhandhabung und Datensicherung unter macOS

Die Datenhandhabung und Datensicherung ist unter macOS (bis einschließlich macOS 10.4 alias Mojave) deutlich einfacher ausführbar als unter Windows. Dies liegt unter anderem daran, dass macOS ein etwas flexibleres Boot-Konzept hat und auch das Systemvolume relativ problemlos im laufenden Betrieb kopiert/gesichert werden kann – auch in der Variante der Erstellung eines Klons des Boot-Volumes –, was mehrere später beschriebene Anwendungen anbieten.

Als Standardwerkzeug wird von Apple für Backups (und das Wiedereinspielen) die Anwendung *Time Machine* kostenlos mitgeliefert. Damit ist es möglich, sowohl das Betriebssystem selbst als auch Benutzerdaten zu sichern. Das Sichern erfolgt auf ein einmal selektiertes Zielvolume in eine spezielle Datei (in einem speziellen Format).

Einige andere Anwendungen (nicht von Apple) führen aus meiner Erfahrung das Sichern flexibler und eleganter durch. Möchte man nur normale Dateien, Ordner oder Dateibäume sichern, findet man auch dazu mehrere Lösungen, teilweise sogar kostenlos. Eine Übersicht dazu finden Sie im Abschnitt ›Datensicherung unter macOS‹ auf Seite 43.

Für die wichtigsten Operationen mit macOS-Datenträgern – Dateisystemprüfung und Dateisystem-Reparatur, Formatieren/Initialisierung von Datenträgern, Partitionen und das Anlegen von Volumes und sogar die Erstellung von System-Klonen – setzt man unter macOS die Anwendung *Festplattendienstprogramm* ein. Dabei täuscht der Name etwas, da die Anwendung auch mit Flash-Speichern wie USB-Sticks und SSDs umgehen und noch einige andere Dinge tun kann. Die Anwendung wird ab Seite 36 beschrieben.

Ein Defragmentieren kann unter macOS aufgrund einer von Windows abweichenden Organisation des Dateisystems entfallen. Auf SSDs sollte es nie ausgeführt werden. Bei SSDs gibt es keine Positionierung der Schreib-/Leseköpfe. Die Defragmentierung würde nur überflüssige Lese-/Schreiboperationen produzieren.

Im Gegensatz zu Windows werden unter macOS Volumes nicht über Laufwerksbuchstaben angesprochen, sondern über Volume-Namen. Dabei sollte man unterschiedlichen Volumes auch unterschiedliche Namen geben (was nicht erzwungen wird). Einige Anwendungen achten aber nicht nur auf den Volume-Namen, sondern zusätzlich auf die Volume-ID, so dass auch zwei Volumes gleichen Namens unterschieden werden.

Neben dem Werkzeug *Festplattendienstprogramm* (von Apple) gibt es eine kleine Anzahl weiterer Anwendungen, die den Umgang mit Datenträgern und Volumes auch in tieferen Ebenen beherrschen und bei Bedarf Korrekturen vornehmen können. Dazu gehört beispielsweise *DiskWarrior* [19] (kostenpflichtig). Die Anwendung *Disk Drill* erlaubt es, gelöschte Dateien zu retten (sofern sie noch nicht überschrieben wurden). Es gibt *Disk Drill* [20] in einer kostenlosen sowie in zwei kostenpflichtigen Versionen (mit jeweils erweiterten Funktionen). Ich musste bisher jedoch sehr selten auf sie zurückgreifen und komme in aller Regel mit dem *Festplattendienstprogramm* aus. Möchte man die Geschwindigkeit unterschiedlicher Datenträger bzw. der Volumes darauf testen, so stehen unter macOS dafür die beiden kostenlosen Programme *Black Magic Speed Test* [15] und *AJA Systemtest* [18] zur Verfügung.

Mit dem im Herbst 2019 erscheinenden macOS 10.15 (Catalina) werden sich eine Reihe von Änderungen ergeben. So wird das Systemvolume *read-only* sein (kein Schreiben erlauben). Benutzerdaten, die im Standardfall bisher auch auf der Systemplatte lagen, liegen dann auf einem separaten Volume (was für den normalen Anwender aber nicht separat erscheint). Dies impliziert wesentliche Änderungen für Backup-Lösungen, die das Systemvolume sichern sollen. Zusätzlich wird APFS, das bisher weitgehend auf Flash-Speicher ausgelegt ist, zum Standarddateisystem – und dies auch für Festplattenspeicher. Bootbare Catalina-Systeme (und neuer) müssen dann auf einem APFS-Volume liegen.

In macOS 10.15 wird *Time Machine* (voraussichtlich) auch auf APFS-Volumes sichern können. Andere Backup-Lösungen werden unter Umständen eine Weile brauchen, bis sie mit den geänderten Rahmenbedingungen umgehen können. Dies dürfte insbesondere für die kostenlosen Anwendungen gelten.

In diesem E-Book werde ich fehlender Erfahrungen wegen nicht weiter auf dieses Thema eingehen, das E-Book später aber aktualisieren.

Festplattendienstprogramm (macOS)

Was Datenträger betrifft, spielt unter macOS das *Festplattendienstprogramm* eine wichtige Rolle. Formatieren (Löschen), Partitionieren und dabei Dateisysteme auf einer Partition anlegen oder die Struktur eines Dateisystems überprüfen und bei Bedarf reparieren – all dies führt man damit durch. Man findet die Anwendung unter */Programme/Dienstprogramme/* auf dem Systemlaufwerk (korrekt: auf dem Systemvolume).

Beim Arbeiten damit sollte man **große Sorgfalt walten lassen**, kann man sich damit doch bei Fehlern die Daten eines Datenträgers und dessen Partitionierung zerstören. Die Anwendung erlaubt nicht nur Datenträger zu initialisieren (mit einer Partitionstabelle zu versehen)[1] und zu partitionieren, sondern auch festzulegen, welche Art Dateisystem man auf die verschiedenen Partitionen legen möchte (sofern man mehrere Partitionen wünscht). Zugleich gibt man hier den Volumes (den Dateisystem-Containern) auch einen Namen. Dabei dürfen mehrere Volumes den gleichen Namen haben, was sich aber definitiv nicht empfiehlt.

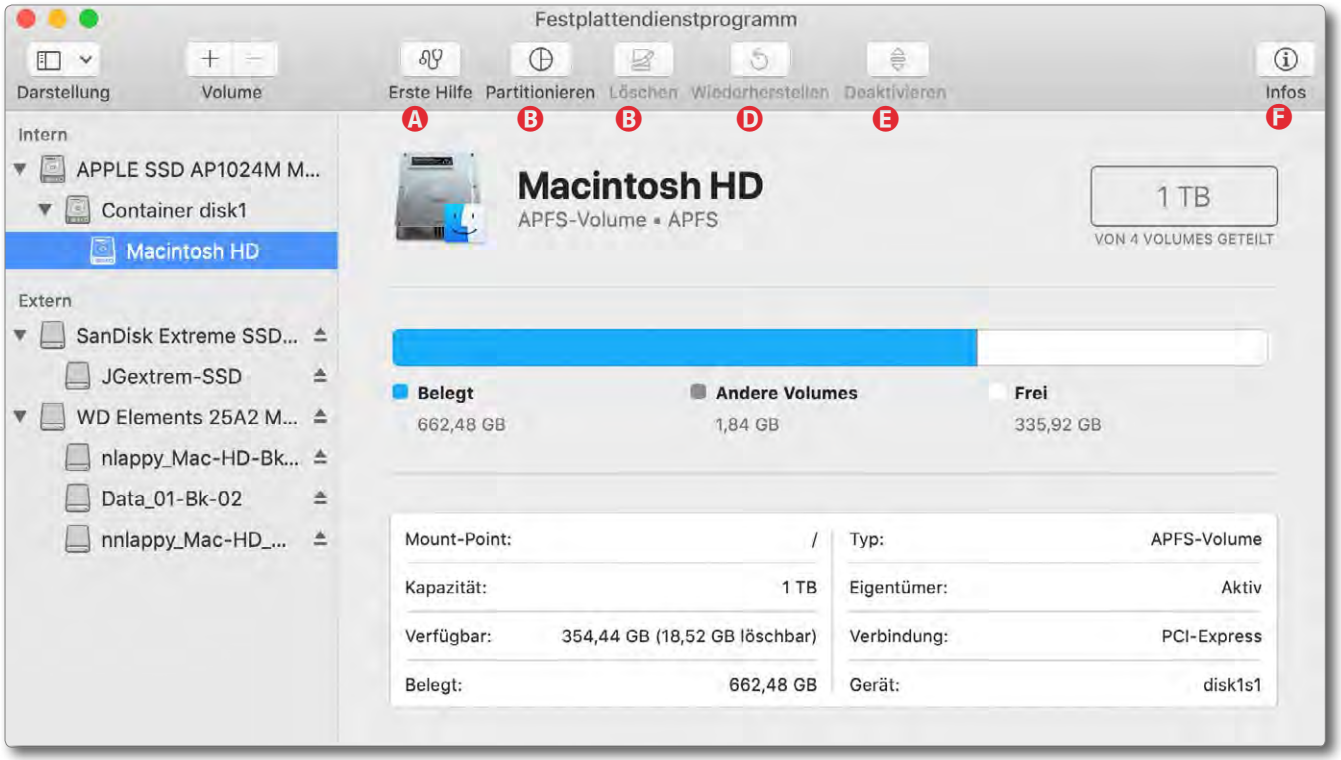


Abb. 1: Das *Festplattendienstprogramm* – hier unter macOS 10.14 – analysiert nach dem Aufruf zunächst die angeschlossenen Laufwerke und zeigt sie zusammen mit ihren Containern (nur bei APFS), Partitionen/Volumes (Letztere eingerückt) an. Selektiert man ein Volume – hier ›Macintosh HD‹ auf dem SSD-Laufwerk ›APPLE SSD …‹ –, so sieht man rechts einige Daten dazu. Die oberste Icon-Leiste zeigt die wesentlichen Funktionen. Sie reichen von *Erste Hilfe* bis hin zum *Deaktivieren* einer Partition oder zum Auswerfen eines ganzen Datenträgers. *Infos* liefert in einem separaten Fenster zahlreiche weitere Informationen zum Datenträger oder zur Partition. Technisch aktuell angeschlossene, aber deaktivierte Datenträger oder Partitionen/Volumes werden zwar angezeigt, sind aber ausgegraut.

Beim Initialisieren eines Datenträgers gibt man über eine Option auch vor, ob ein Booten von einem (oder mehreren) der Partitionen/Volumes möglich sein soll. Dazu muss man natürlich ein zur Hardware passendes Betriebssystem installieren (oder darauf klonen).

Die Anwendung erlaubt auch, einzelne Volumes zu deaktivieren (auszuwerfen bzw. ein *unmount* darauf auszuführen) sowie deaktivierte Volumes zu aktivieren (ein *mount* darauf auszuführen). Daneben kann man hier ein Volume löschen (die Partition bleibt bestehen und ist dann leer) und danach optional ein anderes Dateisystem darauf anlegen.

Beim Start analysiert das *Festplattendienstprogramm* – der englische Name ist *disk utility* – zunächst alle aktuell angeschlossenen Datenträger, Container und Volumes (wie z. B. in Abb. 1). Dies kann etwas dauern.

1 Für den hier als Partitionstabelle bezeichneten Informationsblock (er kann auch mehrere physikalische Blöcke belegen) gibt es unterschiedliche Bezeichnungen und Formate – etwa den von Windows her bekannten MBR (*Master Boot Record*). Unter macOS wird er (zumeist) als *GUID-Partitionstabelle* bezeichnet. In ihm findet man unter anderem eine Datenträger-Identifikation sowie Informationen, wie viele Partitionen auf dem Datenträger liegen und wo sie beginnen. Jede Partition hat einen ›Kopfblock‹, in dem weitere Informationen zur Partition sowie – sofern angelegt – weitere Informationen zum Dateisystem auf der Partition zu finden sind. Ist die Partitionstabelle des Datenträgers beschädigt, sind die Dateien auf den Datenträger kaum noch nutzbar.

Es sei hier angemerkt, dass man beim *Festplattendienstprogramm* im Menüpunkt Hilfe (nicht zu verwechseln mit dem Knopf bzw. der Funktion *Erste Hilfe*) eine recht gute und verständliche Hilfe zu den Funktionen und Begriffen erhält.

Selektiert man statt einer Partition bzw. eines Volumes ein Laufwerk, so zeigt *Festplattendienstprogramm* die Art der Anbindung (z. B. *PCI, SATA, …*), die Art der Partitionstabelle, die Gesamtkapazität, die Anzahl der Partitionen darauf – darunter können sich auch verdeckte Partitionen befinden –, die Art des Datenträgers sowie den internen (macOS-)Gerätenamen. Ein Beispiel ist in Abbildung 2 zu sehen.

Bei den neueren Systemen gibt es statt Partitionen *Container*, die ihrerseits wieder mehrere Volumes vom Typ APFS enthalten können (siehe dazu Seite 29).

Die Funktion *Erste Hilfe* führt eine Dateisystem-Überprüfung der selektierten Partition bzw. des Volumes darauf aus und repariert bei Bedarf und Möglichkeit auch eventuell erkannte Fehler.

Unter *Partitionieren* (Abb. 1 Ⓑ) nimmt man die Aufteilung eines Datenträgers (Laufwerks) in mehrere Bereiche vor – es darf aber auch nur eine einzige Partition sein, wie es bei Kameraspeicherkarten und den meisten USB-Sticks üblich ist.

Mit *Löschen* (Abb. 1 Ⓒ) wird auf dem selektierten Datenträger eine komplett neue Datenträgerstruktur angelegt, was einer Art Basisformatierung entspricht. Damit werden auch alle Daten (Dateien) und alle Partitionsstrukturen gelöscht. Der Datenträger hat damit zunächst nur eine Partition. Beim Löschen kann man vorgeben, welche Basisstrukturierung der Datenträger erhalten soll (siehe Abb. 3 Ⓐ). Dabei werden drei unterschiedliche Schemata angeboten (das, was ich bisher als *Partitionstabelle* bezeichnet habe):

Abb. 2
(Ausschnitt) Hier die Informationen zum ›Datenträger‹ APPLE SSD AP1024M Media‹, einer 1 TB großen SSD direkt am PCI-Express-Bus des Systems mit 3 Partitionen (1 davon verdeckt für Recovery-Funktionen).

A. *GUID-Partitionstabelle* – das Schema für Datenträger für die Benutzung unter aktuellen macOS-Systemen. In der Regel sollte man dieses Schema für die Partitionstabelle verwenden.

B. *Master Boot Record* ist für Windows und DOS-Datenträger vorgesehen. Man verwendet es z. B. standardmäßig für USB-Sticks und Datenträger, die unter Windows eingesetzt werden.

C. *Apple-Partitionstabelle* Dies wird zur Rückwärtskompatibilität mit älteren Systemen angeboten.

Abb. 3: Die Anwendung bietet unter *Schema* drei Arten für die Datenträger-Strukturierung (die Partitionstabelle) an.

Erst nach dem Löschen (dem Formatieren) und damit dem Anlegen einer Partitionstabelle lässt sich der

Datenträger, der zunächst nur eine Partition hat, in mehrere Partitionen unterteilen. Dies ist etwa durch einen Klick auf das +-Zeichen unterhalb des Tortendiagramms möglich. Man selektiert dann nacheinander die einzelnen Elemente (Partitionen) und legt in den Feldern daneben den Partitions- und damit auch den Volume-Namen,[1] unter *Art* die Art des Dateisystems (Abb. 6) auf der Partition sowie schließlich die gewünschte Größe (innerhalb der möglichen Grenzen) fest. Ein Klick auf *Ausführen* führt dann alle notwendigen Operationen durch.

Die Standarddateisystem-Art war bisher HFS+, das hier mit ›*Mac OS Extended*‹ bezeichnet wird. Es werden Varianten angeboten, in deren Volume-Namen die Groß-/Kleinschreibung differenziert wird.

Man kann beim Anlegen wählen, ob die Partition verschlüsselt sein soll. (Dies wird nur angeboten, wenn der Datenträger eine GUID-Partitionstabelle hat.) In diesem Fall muss man einen Schlüssel dazu eingeben (und durch eine zweite Eingabe verifizieren, Abb. 4). macOS kann sich dabei optional das Passwort im eigenen Schlüsselbund merken, so dass bei nächsten Aktivieren (*Mounten*) des Volumes das Passwort nicht erneut eingegeben werden muss (der Anwender muss jedoch angemeldet sein). Ansonsten wird man beim nächsten Aktivieren erneut nach dem Passwort gefragt.

1 Diese Volume-Namen lassen sich später noch ändern – mit entsprechenden Rechten auch im *Finder*.

Abb. 4: Die Eingabe des Passworts muss doppelt erfolgen (um Tippfehler zu erkennen). Zusätzlich lässt sich eine Merkhilfe für das Passwort eingeben.

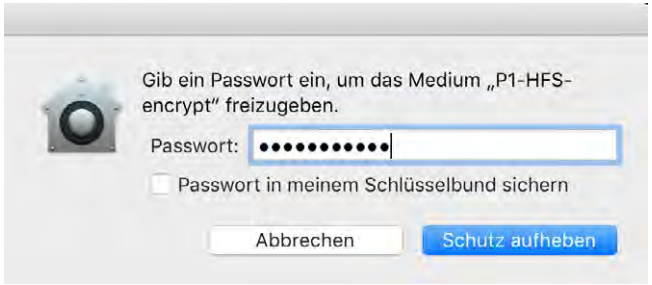


Abb. 5: Wurde das Passwort eines Volumes nicht im Schlüsselbund von macOS hinterlegt, wird beim Aktivieren/Mounten des Volumes nach dem Passwort gefragt.

›Löscht‹ man auf einem Datenträger nur eine einzelne Partition, so gehen (nur) die Daten auf dieser Partition verloren.

Die Dateisystemart *APFS* in ihren verschiedenen Varianten wird erst seit macOS 10.13 (alias High Sierra) angeboten. Ihre Weiterentwicklung ist noch im Gang. Unter iOS, ipadOS, tvOS ist es in deren neueren Versionen das Standard- und einzige Dateisystem.

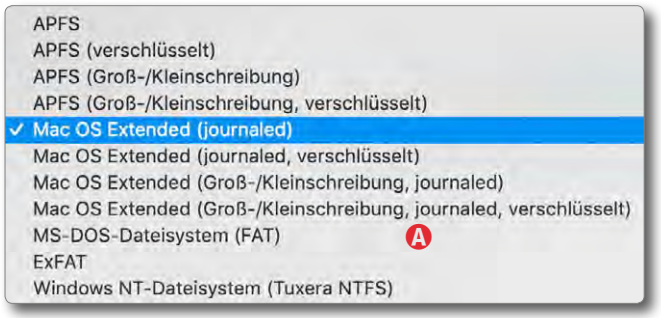


Abb. 6: Dateisystemformate, die unter macOS 10.4.5 angeboten werden. Unter älteren macOS-Versionen fehlen die APFS-Varianten.

Das Dateisystemformat NTFS (Abb. 6 Ⓐ) wird als Dateisystem-Format für neue macOS-Volumes im Standardfall nicht angeboten, wurde hier aber durch die Systemerweiterung der Firma *Tuxera* [1] ermöglicht. macOS kann NTFS-Dateisysteme (auch ohne die *Tuxera*-NTFS-Erweiterung) lesen, nicht jedoch darauf schreiben. Die *Tuxera*-Erweiterung erlaubt es, NTFS-Systeme anzulegen, davon zu lesen (was bereits das macOS-Basissystem erlaubt) und auch darauf zu schreiben.

Der in den Dateisystemen von Abbildung 6 angeführte Zusatz *Journaled* ist eine Funktion, **die die Ro**bustheit des Dateisystems bei Systemabstürzen und Stromausfällen erhöht. Man sollte sie, wo angeboten, wählen.

Eine automatische Komprimierung bietet macOS für seine üblichen Dateisysteme bisher **nicht** an. (Eine Image-Datei lässt sich jedoch komprimiert anlegen und kann nach einem *Mount* (Aktivieren) ›normal‹ gelesen werden.)

Die Funktion *Wiederherstellen* (Abb. 1 Ⓓ) erlaubt es, Daten von einem anderen Datenträger (überschrei-

bend) auf das betreffende Volume zu spielen. Dabei gehen dort eventuell bisher vorhandene Daten verloren!

Beim Anlegen bzw. Neu-Formatieren eines Datenträgers unter macOS sollte man – ob man es aktuell benötigt oder nicht – den Datenträger mit einer GPT-/GUID-Partitionstabelle versehen. Dies erlaubt, gleich oder später ein bootbares Betriebssystem auf eine der Partitionen zu legen. Auch mehrere (bootbare) Systeme dürfen auf mehreren Partitionen liegen. Unter den *Systemeinstellungen* (im Dock) kann man dann unter *Startvolume* (Startvolume) wählen, welches dieser Systeme man beim nächsten Neustart booten möchte. Diese Wahl hat man im Notfall auch, wenn man beim Hochfahren des Systems die ⌥-Taste drückt. In diesem Fall sucht der Startmanager nach erkennbaren Betriebssystempartitionen und lässt einem die Wahl, welches man starten möchte.

Die typischen ›synchronisierenden‹ Backup-Anwendungen unter macOS wie etwa *Carbon Copy Cloner*, *SuperDuper!* oder *FreeFileSync* können selbst die Daten nicht verschlüsseln (chiffrieren). Sollen die Daten auf dem Sicherungs-Volume deshalb verschlüsselt sein, kann man für das betreffende Volume ein verschlüsseltes Dateisystem wählen, muss dies aber bereits beim Anlegen des Dateisystems/Volumes entsprechend einstellen (siehe Abb. 6, Seite 38). Für die Backup-Anwendung ist diese Verschlüsselung dann transparent.

Startvolume wechseln unter macOS

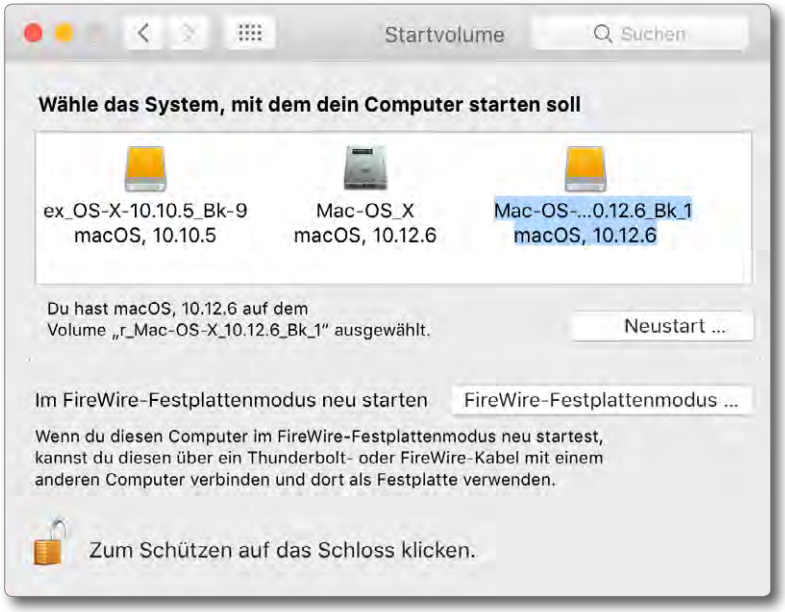


Abb. 7: Unter *Startvolume* lässt sich in den *Systemeinstellungen* von macOS ein neues Startvolume auswählen und per Klick auf Neustart booten. Zuvormuss man (unter Umständen unter Angabe des Administrator-Passworts) das Schloss öffnen bzw. die Funktion ›scharfschalten‹.

Auf Macintosh-Systemen gibt es mit der Änderung des Startvolumes weniger Probleme als unter Windows. Zunächst einmal lässt sich das System-/Startvolume weitgehend problemlos mit den bereits erwähnten Anwendungen sichern und bei Bedarf auch klonen (*Klonen* heißt hier: Sicherung mit Startfähigkeit der Sicherung). Auch ein Start von einem solchen Klon ist möglich – siehe dazu aber die Einschränkung für neuere Macs mit T2-Sicherheitschip, die etwas später beschrieben ist.

Möchte man das System von einem anderen (startfähigen) Volume starten (und kann man die Änderung noch unter einem laufenden System vornehmen), so geht man zunächst in die *Systemeinstellungen* ( ) und aktiviert dort die Funktion *Startvolume* ( ). Darin wählt man nun das Volume mit dem neuen (oder gesicherten) System als Startvolume (Abb. 7). Die Anwendung *Startvolume* ermittelt dabei selbstständig, auf welchen sichtbaren Volumes ein Betriebssystem installiert ist und welche Systemversion es hat. Danach bootet man per Klick auf *Neustart* erneut und läuft dann mit dem gewählten System.

Lässt sich das unter *Startvolume* festgelegte System nicht mehr problemlos starten, so drückt man bei einem Neustart (eventuell erzwungen durch das Aus- und Wiedereinschalten der Netzspannung) die ⌥-Taste. Im dann erscheinenden Boot-Dialog kann man ein Volume mit einer Systemsicherung (oder einem neu eingespielten System) auswählen und das System starten.

Systemstart von externen Laufwerken bei Systemen mit T2-Chip

Bei neueren Macintosh-Systemen, die einen T2-Sicherheitschip besitzen (z. B. beim MacBook Pro ab 2018), verhindert das System (bzw. der Chip) zunächst aus Gründen der Systemsicherheit ein Booten von externen Medien. Möchte man dies trotzdem tun, so ist ein mehrstufiger Prozess erforderlich.

Zunächst bootet man das System neu und drückt dabei die Tastenkombination ⌘-R. Das System mel-

det sich dann im *Wiederherstellungsmodus* (Recovery-Modus) und bietet einige Möglichkeiten der Wiederherstellung mit dem *macOS-Dienstprogramm* (Abb. 8).

Hieraus lässt sich z. B. *Time Machine* für ein Zurückspielen des Systems auf das ursprüngliche Startvolume aufrufen; macOS lässt sich neu installieren, und das *Festplattendienstprogramm* erlaubt es, von einem System-Image oder von einem anderen Volume ein System auf das interne Startvolume zu restaurieren (oder auch nur das Startvolume mit der Funktion *Erste Hilfe*) und – soweit möglich – auch zu reparieren. Ebenso lässt sich damit ein neues Laufwerk formatieren und partitionieren.

Möchte man hingegen wirklich von einem externen Volume ein dort gesichertes System starten, so findet man im Hauptmenü (links oben im Bildschirm) des *macOS-Dienstprogramms* unter *Dienstprogramme* den Eintrag *Startsicherheitsdienstprogramm*. Bevor es startet, muss man das Administrator-Passwort eingeben.

Damit erscheint der Dialog von *Startsicherheitsdienstprogramm* (Abb. 8). Dort lässt sich sowohl die Sicherheit beim Starten ändern als auch ein Starten von einem externen Medium erlauben (Option Ⓐ). Zusätzlich kann man ein Firmware-Passwort setzen oder ändern, das dann beim Booten angegeben werden muss. Für beide Änderungen ist das Administratorpasswort erforderlich.

Nun kann man das *Startsicherheitsdienstprogramm* beenden. Beendet man danach noch das *macOS-Dienstprogramm*, erscheint ein Dialog, in dem man nun

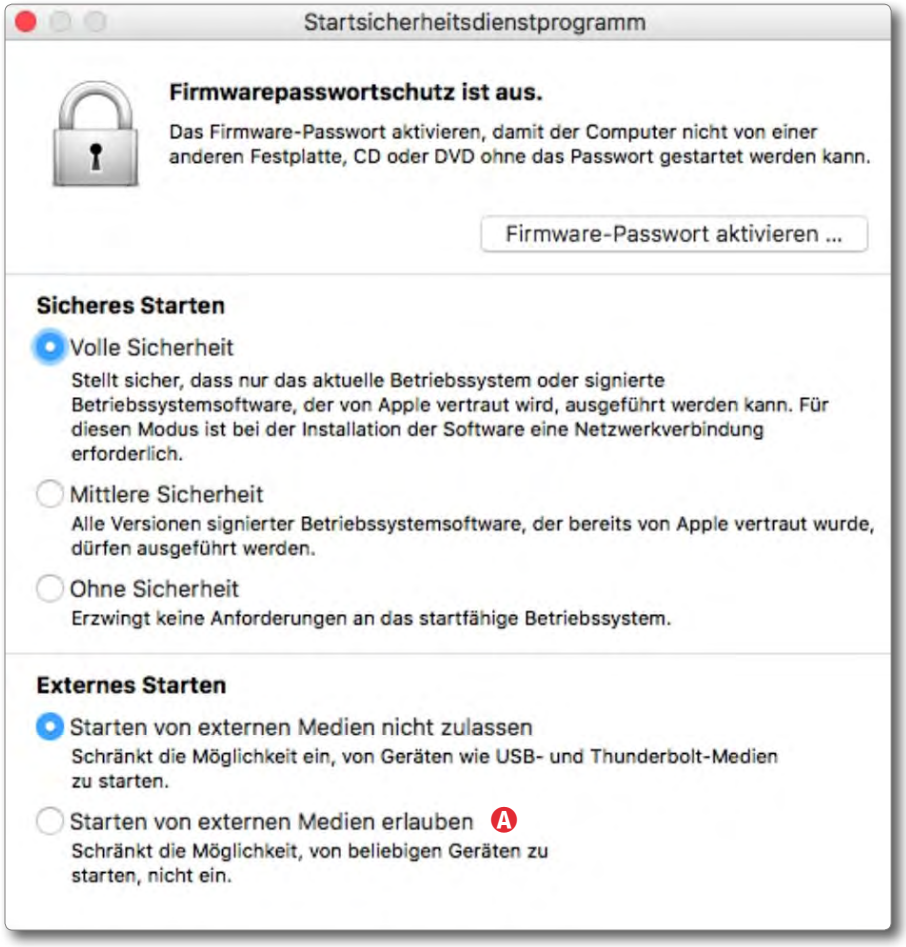


Abb. 8: Im *Startsicherheitsdienstprogramm* kann man die Sicherheitsstufe für den Systemstart ändern und über die Option Ⓐ erlauben, dass das System von einem externen Datenträger gestartet werden kann.

(endlich) das neue (auch externe) Startvolume wählen und danach per Klick auf *Neustart* neu von dort booten kann.

(Weitere Informationen zu diesem ganzen Ablauf finden Sie unter [13].)

Apple Recovery HD

Die *Apple Recovery HD* ist eine in der Regel verdeckte (nicht sichtbare) kleine Partition (etwa 200 GB groß), die ein macOS-Minimalsystem enthält. Ist das System auf dem Mac-Startvolume so defekt, dass es nicht mehr problemlos startet, so kann man (sofern das Problem nicht am Laufwerk selbst liegt) von dieser *Apple Recovery HD* booten und mit den dort vorhandenen Tools das Betriebsystemvolume reparieren oder ein System von einem Sicherungsvolume zurückspielen oder ein neues System aus einer anderen Quelle (etwa dem Internet) installieren.

Drückt man beim Systemstart die Tastenkombination ⌘-R, so meldet sich nach etwas Verzögerung das System dieser *Apple Recovery HD* (sofern auf dem Startvolume vorhanden) im sogenannten *Wiederherstellungsmodus*. Von dort aus lassen sich einige nützliche Funktionen ausführen – etwa das Reparieren des Startvolumes mit dem *Festplattendienstprogramm* oder das Wiedereinspielen eines Time-Machine-Backups oder einer mit anderen Mitteln erstellten Sicherung.

Eine solche *Apple Recovery HD* wird bei der Installation von macOS auf einem ›nackten‹ System oder bei der Neuinstallation eines neuen Betriebssystems auf einem separaten Laufwerk automatisch mit angelegt.

Erstellt man mit *Carbon Copy Cloner* (s. Seite 50) eine Kopie eines macOS-Volumes, so fragt *Carbon Copy Cloner* nach, ob dabei beim ersten Synchronisieren (eigentlich Kopieren) auch eine solche *Recovery HD* erstellt werden soll. Dabei wird effektiv eine verdeckte Partition erstellt und der Platz dafür vom Zielvolume abgezweigt.

macOS-Systemstart in besonderen Modi

Bei einigen Problemen kann es helfen, macOS in speziellen Modi zu starten. Dafür gibt es mehrere Tastatur-Kürzel, die man beim Systemstart drücken kann (sofort nachdem die Hardware-Überprüfung erfolgreich war und der Startton erklingt). Einige dieser Kürzel funktionieren aber nicht, wenn die Tastatur über Bluetooth statt über USB angeschlossen ist, da zu Beginn der Bluetooth-Treiber noch nicht geladen ist:

A. Die ⌥-Taste aktiviert den Startup-Manager. Dieser analysiert zunächst die angeschlossenen Laufwerke und sucht darauf bootfähige Startvolumes, die er anzeigt. Mit den Pfeiltasten navigiert man zu einem geeigneten Volume und startet durch die Eingabetaste (↵) das dort liegende System.

B. Drückt man die ⇧-Taste beim Start, so startet das System des (normalen) Startvolumes im *Sicheren Modus*. Hierbei werden einige Systemerweiterungen, die potenziell Probleme bereiten könnten, nicht automatisch geladen. Dies hilft bei der Analyse von Systemproblemen und deren Behebung (etwa durch das Deinstallieren oder Deaktivieren problematischer Systemerweiterungen).

C. Die ⌘-S-Kombination startet das System (jedoch nur bis macOS 10.13 bzw. *High Sierra*) im Single-User-Modus (*Einzelbenutzermodus*). In ihm werden (ähnlich wie beim *Sicheren Modus*) einige der Betriebssystemerweiterungen nicht geladen, was in manchen Fällen Reparaturarbeiten am System und am Startvolume vereinfachen kann. Hier arbeitet man in aller Regel mit UNIX-Kommandos auf Kommandozeilenebene.

D. ⌘-V aktiviert den *Verbose*-Modus beim Systemstart. In ihm werden die einzelnen Aktionen beim Startvorgang auf dem Bildschirm angezeigt. Dies erlaubt unter Umständen zu erkennen, wo das System bei einem Start Fehler meldet oder hängenbleibt.

E. T startet den Mac im sogenannten *Target-Modus*. Er erlaubt das Startvolume von einem anderen Mac-System zu installieren bzw. zu restaurieren. Dieses zweite System muss über ein Firewire-Kabel oder bei moderneren Systemen über ein Thunderbolt-Kabel angeschlossen sein. Dieser Modus kann nützlich sein, wenn man ein System (ohne dafür einen Datenträger zu haben) neu aufsetzen oder wiederherstellen möchte. (Darauf wird hier nicht weiter eingegangen.)

F. ⌘-R startet das System im *Wiederherstellungsmodus* (*Recovery-Mode)* – korrekt: Es startet ein Minimalsystem von einer sonst nicht sichtbaren Partition mit dem *Apple Recovery HD*-System darauf. Diese Partition sollte auf dem Startvolume (verdeckt) vorhanden sein. Ein solches Recovery-System wird bei neueren macOS-Systeminstallationen automatisch auf den Startvolume mit angelegt (und ist in der

Regel in den meisten Volume-/Partitionsanzeigen nicht sichtbar). Es gibt jedoch einige Hilfsprogramme, mit denen man es auch später noch auf einem bereits formatierten Datenträger unterbringen kann. So ermöglicht es etwa *Carbon Copy Cloner* beim Sichern eines bootbaren Systemvolumes, per Option ein solches Recovery-System (korrekt: ein kleines verdecktes Volume mit einem solchen System) auf dem Ziellaufwerk anzulegen.

In diesem Minimalsystem lassen sich einige bei Startproblemen nützliche Programme ausführen. Zunächst meldet sich dort eine Palette *macOS-Dienstprogramme* und bietet die gezeigten Funktionen an (Abb. 10).

Weitere Funktionen findet man im Hauptmenü (das Menü im Bildschirm links oben in der Kopfzeile) unter Dienstprogramme (Abb. 9). Die Funktionen bzw. Hilfsprogramme sollten offensichtlich sein und sind hier im E-Book separat unter dem entsprechenden Stichwort beschrieben.

Für eine Wiederherstellung aus einem Time-Machine-Backup **muss natürlich ein Backup vorhanden sein** (siehe dazu Seite 45).

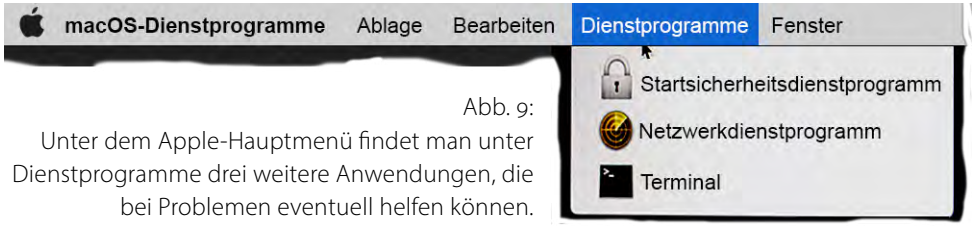


Abb. 9:
Unter dem Apple-Hauptmenü findet man unter Dienstprogramme drei weitere Anwendungen, die bei Problemen eventuell helfen können.

Abb. 10: Im Wiederherstellungsmodus werden einige nützliche Dienstprogramme angeboten, die bei Startproblemen hilfreich sein können.

Zuerst sollte man aber ausprobieren, ob sich die Probleme des Startvolumes mit dem *Festplattendienstprogramm* über die Funktion *Erste Hilfe* beheben lassen (siehe Seite 36). Reicht dies nicht und hat man zu einem früheren Zeitpunkt einen System-Klon erstellt, so lässt sich dieser unter Umständen mit der Funktion *Wiederherstellen* des *Festplattendienstprogramms* zurück- oder auf einen neuen Datenträger spielen und danach booten. Am einfachsten und schnellsten ist aber immer, ein aktuelles System-Klon-Volume zu haben – etwa erstellt mit *Carbon Copy Cloner*, *SuperDuper!* oder mit einer der anderen Anwendungen, die einen bootbaren Klon erstellen können, dieses System zu booten und bei Bedarf von dort aus Reparaturarbeiten vorzunehmen.

Eine weitere Möglichkeit besteht darin, *macOS erneut installieren* zu nutzen, was über das Internet oder von einem USB-Stick möglich ist.

Ansonsten findet man über den Punkt *Online-Hilfe aufrufen* Informationen, die lokal im Recovery-System gespeichert sind (auf Deutsch), oder kann über Safari auch nach Hilfe im Internet recherchieren.

Im **Hauptmenü findet man in diesem speziellen Modus unter** Dienstprogramme die drei Funktionen:

- *Startsicherheitsprogramm* (s. Seite 39),

G. *Netzwerkdienstprogramm* – um Netzwerkeinstellungen vorzunehmen, etwa um ein Betriebssystem aus dem *Apple App Store* herunterladen zu können,

- Aufruf von *Terminal* (das Apple-Kommandozeilenfenster). In der *Terminal*-Anwendung sind eine ganze Reihe von Kommandos auf der macOS/UNIX-Kommandoebene möglich – etwa eine Volume-Überprüfung und -Reparatur mit dem *fsck*-Kommando. Man muss sich dazu jedoch dort gut auskennen – etwas, was den meisten Mac-Anwendern fremd sein dürfte, UNIX- und Linux-Anwendern jedoch bekannt vorkommen sollte und manche Eingriffe ins System erlaubt.

Datensicherung unter macOS

Für die Datensicherung unter macOS gibt es zwar nicht so viele Anwendungen wie unter Windows, einiges ist dafür aber deutlich einfacher. Dies betrifft vor allem die Sicherung des System- bzw. Startvolumes. Dieses lässt sich mit den meisten in diesem Kapitel beschriebenen Anwendungen weitgehend problemlos im laufenden Betrieb sichern und dies auf ein anderes, danach bootbares Volume. (Das betreffende Volume muss dazu natürlich lokal angeschlossen sein.)

Die Backup-Lösungen *Carbon Copy Cloner, SuperDuper!*, *ChronoSync* und *SmartBackup* sind beispielsweise dazu in der Lage. Sie benötigen dafür spezielle Zugriffsrechte, müssen also mit Administratorrechten laufen. Diese Rechte kann man den meisten von ihnen aber bereits bei der Installation geben. Bei anderen (z. B. bei *ChronoSync*) wird das Administratorpasswort beim Aufruf einer entsprechenden Sicherung explizit abgefragt. Das Elegante an diesen Lösungen besteht darin, dass sie nach einer ersten Vollsicherung die Backups per weiterer Synchronisierung aktualisieren können, was sehr viel schneller als ein Voll-Backup ist. Außerdem kann man die Systemkopien so – vorzugsweise zeitgesteuert – mit sehr geringem Aufwand aktualisiert halten. Diese Anwendungen können aber ebenso für Backups ›normaler‹ Dateien bzw. Volumes dienen. Da sie im Zielvolume ›normale‹ Dateien erzeugen, sind auch der Zugriff und das Zurückholen extrem einfach und benötigen in vielen Situationen keine speziellen Programme, wobei man mit den genannten Anwendungen auch zurücksynchronisieren kann. Man kommt hier also mit einer einzigen Backup-Lösung aus (eventuell mit mehreren unterschiedlich konfigurierten Sicherungsaufträgen). Alle genannten Anwendungen erlauben eine automatische, zeitgesteuerte Sicherung.

Es erweist sich auch als praktisch, dass unter macOS mehrere Systemvolumes (bootbare Systeme) nebeneinander (angeschlossen) koexistieren können und man über die Funktion *Startvolume* (wie auf Seite 39 beschrieben) bei Problemen (oder zum Test) von einem anderen als dem aktuellen Startvolume ein System starten kann. (Unter Windows erfordert dies sehr viel mehr Trickserei.)

Mit macOS selbst kommt kostenlos die Backup-Lösung *Time Machine*. Auch damit lässt sich das Betriebssystem sichern, nicht jedoch direkt in ein bootbares Volume. Dies erfordert einen Zwischenschritt über das Zurückspielen aus einem Time-Machine-Backup auf ein anderes Volume oder auf das ursprüngliche Volume – dann aber mit Hilfe eines Notsystems (siehe dazu die Beschreibungen auf den Seiten 41 bis 42). Der Vorteil von *Time Machine* liegt darin, dass die Sicherung optional chiffriert und auch komprimiert sein kann und dass *Time Machine* eine brauchbare Oberfläche für das Restaurieren versionierter Dateistände anbietet.

Auch das zuvor beschriebene *Festplattendienstprogramm* ist in der Lage, einen System-Klon zu erstellen (nachfolgend beschrieben). Zu empfehlen ist diese Lösung jedoch kaum.

Es gibt für macOS außerdem eine Reihe von Lösungen, um ›nur‹ einzelne Ordner(bäume) oder einzelne Dateien zu sichern und zurückzuspielen. Beispiele für kostenfreie Lösungen sind *FreeFileSync* (hier beschrieben bei den Windows-Lösungen ab Seite 100) und *GoodSync Personal* (hier nicht weiter beschrieben).

Ich habe auch das für macOS verfügbare *Acronis True Image* ausprobiert, jedoch keine Vorteile gegenüber den anderen vorgestellten Lösungen gefunden.

Die meisten Anbieter von Enterprise-Lösungen (solchen, für ein größeren Unternehmen) – etwa IBM [35] oder Feeam [30] – unterstützen auch die Datensicherung von Macintosh-Systemen – zumeist mit einem speziellen Mac-Client, der remote (von einem, anderen Rechner aus) angesteuert wird und die Daten auf einen zentralen Server spielt. Auf solche Lösungen geht dieses E-Book jedoch nicht ein.

Ein getrennter Punkt ist die Sicherung von Datenbanken. Dafür gibt es eine Reihe spezieller, hier nicht weiter betrachteter Lösungen. Eine schlichte Lösung besteht darin, die Datenbanken vor der Sicherung herunterzufahren – etwa Lightroom zuvor zu beenden.

Ich selbst habe die kleinere Anzahl von Backup-Lösungen unter macOS nie als Einschränkung empfunden und komme mit den nachfolgend vorgestellten Anwendungen vollkommen aus.

Das Laufwerk – korrekt: das Start-Volume – des macOS-Systems lässt sich mit Hilfe der Anwendung *Festplattendienstprogramm* klonen. Der Vorteil liegt darin, dass man so ohne eine fremde Anwendung relativ einfach einen direkt bootfähigen Klon erzeugen kann.

Der Nachteil gegenüber Backup-Anwendungen wie etwa *Carbon Copy Cloner* oder *SuperDuper!* besteht darin, dass bei jedem dieser Sicherungsläufe das Zielvolume komplett überschrieben und die Quelle komplett neu gesichert wird. Um ein bootfähiges System zu erhalten, muss das Ziellaufwerk eine GUID-Partitionstabelle haben,[1] und die Zielpartition muss ausreichend groß sein, um die Daten der Quelle aufnehmen zu können. Das Klonen erfolgt blockweise und läuft wie folgt ab (unter macOS 10.11 oder neuer):

1. Stellen Sie sicher, dass das Zielvolume auf einem Laufwerk mit einer GUID-Partitionstabelle liegt. Das Zielvolume sollte im Standardfall die Dateisystemart *Mac OS Extended (Journaled)* haben. Überprüfen Sie mit Hilfe des *Festplattendienstprogramms* und seiner Funktion *Erste Hilfe*, dass sowohl das Quellvolume mit dem System als auch das Zielvolume (für den Klon) keine Dateisystemprobleme haben.

2. Selektieren Sie nun im *Festplattendienstprogramm* das Zielvolume und rufen Sie die Funktion *Wiederherstellen* über das Icon im Kopf des Dialogs auf (in Abb. 11 rot markiert).

Abb. 11
Zum Klonen eines Volumes – hier des Startvolumes – verwendet man im *Festplattendienstprogramm* die Funktion *Wiederherstellen*. Zuvor selektiert man dort das Zielvolume und in diesem Fenster das Quellvolume.

3. Im Fenster zu *Wiederherstellen* wählen Sie im Menü Ⓐ das Systemvolume, das geklont werden soll – jenes mit dem zu klonenden macOS darauf. Ein Klick auf den Knopf Ⓑ *Wiederherstellen* startet den Klon-Vorgang.

Nach meiner Erfahrung stößt man bei dieser Technik häufiger auf Probleme, sofern man sie im normalen Betriebssystem-Modus ausführt. Ich empfehle das Klonen deshalb im Wiederherstellungsmodus (siehe dazu die Beschreibung auf Seite 41).

Da hier blockweise geklont wird, ist das Verfahren nicht sehr effizient – sprich langsam –, da offensichtlich auch leere, unbenutzte Blöcke kopiert werden. Ein intelligentes Update nach einer ersten Sicherung wie bei *Carbon Copy Cloner* oder *Superduper!* findet hier nicht statt.

Von einem so erstellten System-Klon lässt sich später booten (siehe die Restriktion bei Mac-Systemen mit dem T2-Sicherheitschip, beschrieben auf Seite 39) oder aber im Wiederherstellungsmodus (siehe Seite 41) auch das Startvolume (oder ein neues Startvolume) von diesem Klon wiederherstellen.

Aus meiner Erfahrung mit mehreren Systemen ist das Klonen eines Systems mit den Anwendungen *Carbon Copy Cloner* (siehe Seite 50) oder *SuperDuper!* (siehe Seite 55) oder *ChronoSync* (siehe Seite 58) sehr viel schneller, transparenter und zuverlässiger als mit dem *Festplattendienstprogramm* oder eine Wiederherstellung aus einem Backup von *Time Machine*.

1 Siehe dazu die Beschreibung des *Festplattendienstprogramms* auf Seite 36.

Time Machine kommt bei macOS seit vielen Versionen automatisch und kostenlos mit. *Time Machine* bietet, einmal korrekt aufgesetzt, eine weitgehend automatische Sicherung von entsprechend ausgewählten Volumes auf zuvor als Ziel- bzw. **Backup-Volume konfigurierten** Volumes. Die gesicherten Daten können optional zusätzlich verschlüsselt werden.

In der Regel sollte das Volume, auf das gesichert wird, deutlich größer als die Summe der zu sichernden Daten sein, da *Time Machine* nach einer ersten Art Vollsicherung ständig in bestimmten Intervallen Änderungen sichert und dabei zunächst ältere Stände erhält. Erst wenn der Platz für weitere Sicherungen nicht mehr ausreicht, werden nach einem bestimmten Schema ältere Versionen automatisch gelöscht. Das Intervall für Sicherungen beträgt standardmäßig eine Stunde. Dabei werden die stündlichen Backups der letzten 24 Stunden gehalten, die täglichen Backups des letzten Monats sowie die wöchentlichen Backups aller vorausgehenden Monate – solange ausreichend Platz auf dem oder den Backup-Volume(s) vorhanden ist.

Time Machine konfigurieren

Zur Konfiguration von *Time Machine* – hier teilweise mit TM abgekürzt – benötigt man (wie üblich) Administrationsrechte bzw. muss das Administrator-Passwort eingeben – etwa zum Öffnen des Schlosses für die Konfiguration (Abb. 1). Aufgesetzt wird *Time Machine* in den Systemeinstellungen unter dem -Icon.

Abb. 1: *Time Machine* konfiguriert man in den Systemeinstellungen und benötigt dazu das Administrator-Passwort. Zunächst muss man die Zielvolumes für *Time Machine* freigeben sowie unter *Volumes auswählen* festlegen, welche Volumes überhaupt automatisch gesichert werden sollen.

Zunächst aber muss man der *Time Machine* Backup-Volumes (zumindest eines) als Ziel für die Backups zuteilen. Dies erfolgt über *Volume auswählen* (Abb. 1) Ⓐ). (Zwar kann man ein Backup-Volume auch für andere Zwecke als das TM-Backup nutzen, dies empfiehlt sich jedoch nicht!) Das Volume sollte ein Dateisystem der Art *Mac OS Extended (Journaled)* oder *Mac OS Extended (Journaled, verschlüsselt)* haben – ansonsten muss es in dieser Art neu formatiert werden (siehe dazu Seite 38). APFS kann in macOS 10.13 (High Sierra) und 10.14 (Mojave) zwar als Quellvolume verwendet werden, aber noch nicht als Zielvolume. Dies dürfte sich mit macOS 10.15 **(Catalina) ändern**, wo APFS der Standard ist (auch für Magnetplatten) und zwingend für Volume mit eine bootbaren System .

Beim Aufsetzen von TM lassen sich bestimmte Daten über den Knopf *Optionen* (Abb. 1 Ⓑ) von

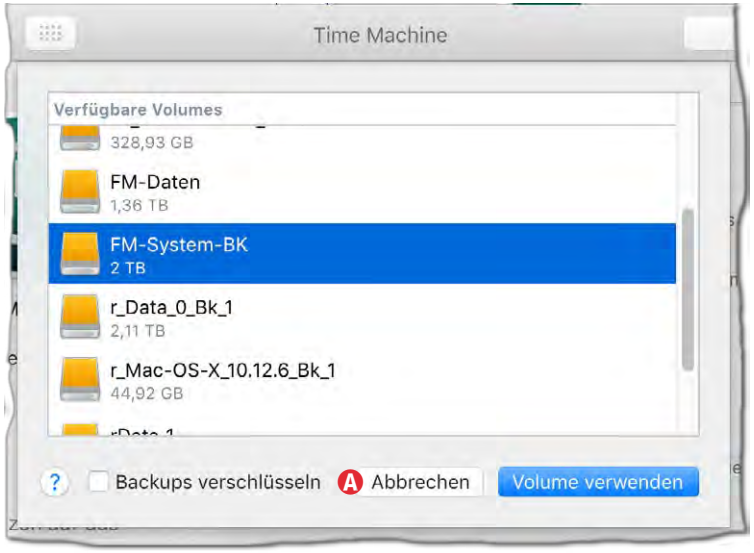


Abb. 2 Fügt man *Time Machine* ein neues Backup-Volume hinzu, kann man vorgeben, dass das Backup verschlüsselt werden soll (Option Ⓐ). Die Verschlüsselung gilt dann aber für alle Zielvolumes!

der Sicherung ausschließen (Abb. 3). Dies ist beispielsweise für Caches und andere temporäre Dateien sinnvoll. Über den Knopf *Optionen* lassen sich auch ganze Volumes von der Sicherung ausnehmen – etwa solche, die man gar nicht oder mit anderen Verfahren sichern möchte.

Hier wäre es zuweilen praktisch, wenn man zunächst nur die Volumes (zusammen mit den Ausnahmen darauf) selektieren könnte, von denen ein TM-Backup erstellt werden soll.

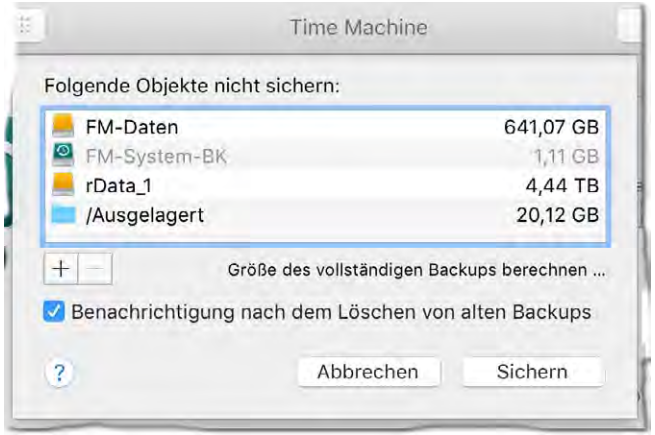


Abb. 3: Es lassen sich einzelne Verzeichnisse, Dateien oder sogar ganze Volumes vom Backup ausschließen.

Auf Laptops lassen sich die automatischen Sicherungen für den Batteriebetrieb ausschließen.

Ob das Backup verschlüsselt wird, legt man beim Hinzufügen eines neuen Backup-Volumes fest siehe

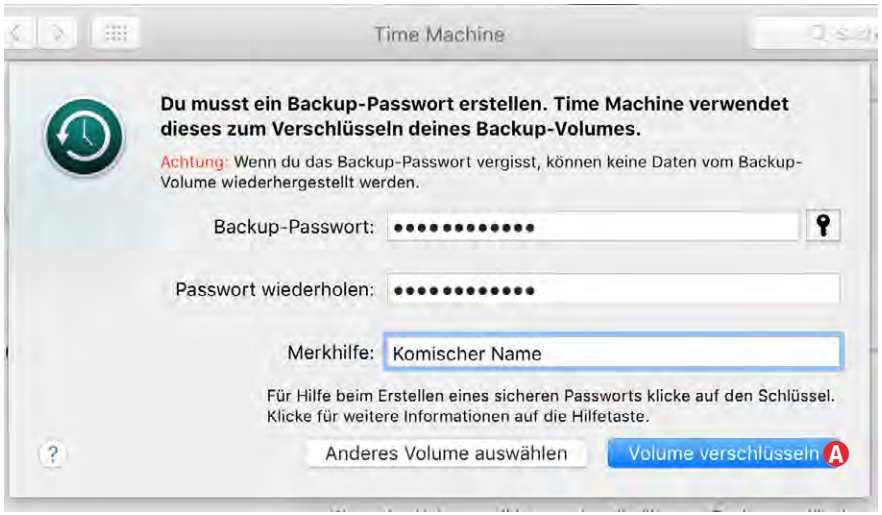


Abb. 4: Soll das Backup auf einem TM-Volume verschlüsselt werden, muss man das Passwort zweimal eingeben und kann optional eine Merkhilfe hinzufügen.

(Abb. 2 Ⓐ). War das Backup auf einem Volume bisher nicht verschlüsselt und soll nun verschlüsselt werden, muss das betreffende Volume zunächst aus der Backup-Liste gelöscht und dann mit der Verschlüsselungsoption neu hinzugefügt werden. Wie bei der Festlegung eines Schlüssels oft üblich, muss man den Schlüssel zweimal eingeben und kann noch eine Merkhilfe dazu angeben. Hat man per Klick auf *Volume verschlüsseln* (Abb. 4 Ⓐ) das Verschlüsseln aktiviert, so dauert es eine Weile, bis *Time Machine* das Volume dafür vorbereitet hat.

Ist *Time Machine* aktiviert und schließt man ein neues Volume am System an, so fragt TM nach, ob dieses Volume (auch) für Backups verwendet werden soll. TM startet nach einer positiven Bestätigung danach automatisch ein (neues) Backup auf dieses neue Zielvolume – und zwar ein Backup aller (entsprechend konfigurierten) Quellvolumes.

TM-Backup-Volumes erhalten in der Volume-Anzeige (z. B. auf dem Desktop) das Icon der *Time Machine* ( ).

Geht man mit dem (normalen) *Finder* auf ein TM-Backup-Volume, so findet man dort ein *Objekt* mit dem Namen *Backups.backupdb* und darunter die gesicherten Volumes, auf die man aber nur mit der TM-Anwendung zugreifen kann.

Dieses Sichern des gesamten Backups in ein einziges Objekt hat einige Nachteile – etwa den, dass das gesamte Backup-Objekt auf einem einzigen Volume liegen muss. Das Zielvolume muss deshalb in der Regel deutlich größer sein als die Summe der zu sichernden Quellvolumes!

Dateien aus einem TM-Backup zurückspielen

Um einzelne Dateien oder ganze Ordnerbäume aus einer TM-Sicherung zurückzuspielen, aktiviert man aus dem Programm-Ordner heraus die Anwendung *Time Machine*. Diese sucht zunächst nach einem TM-Backup-Volume. Die Anwendung zeigt dann eine Art *Finder*-Fenster, hinter dem andere Finder-Fenster gestapelt sind. Vorübergehend wird auf dem Desktop dabei alles andere ausgeblendet. Diese Stapelung zeigt den zeitlichen Verlauf der Sicherungen (Abb. 6). Vorne liegt jeweils die letzte (aktuellste) Sicherung. Geht man mittels

Abb. 5: Das Kontextmenü zu einem in TM selektierten Objekt (hier ›*Disk Doctor.app*‹. Die Funktion *Wiederherstellen* findet man unter dem Fenster (Abb. 6 Ⓑ).

des ^-Symbols rechts des Fensters (Abb. 6 Ⓐ) weiter nach hinten, findet man ältere Sicherungsstände.

Nun navigiert man zu dem Ordner in dieser TM-Ansicht, in dem man (vermutlich versehentlich) Dateien gelöscht hat, und selektiert dort die Datei oder den ganzen Ordner, den man zurückspielen möchte. Im Kontextmenü (rechte Maustaste) werden dann die in Abbildung 5 gezeigten Funktionen angeboten. Möchte man die Datei tatsächlich zurückspielen, so klickt man auf den Knopf *Wiederherstellen* (Abb. 6 Ⓑ), und TM führt die Wiederherstellung durch.

Möchte man hingegen ein ganzes Volume wiederherstellen – eventuell auf ein neues Volume oder sogar auf einen anderen, neuen Mac –, so bootet man das (eventuell neue) System mit gedrückter ⌘-R-Kombination. Es startet damit im Wiederherstellungsmodus. Das TM-Backup-Volume muss dabei bereits angeschlossen sein.

Meldet sich das System dann mit dem *Finder*, so ruft man *Migrationsassistent* (unter *Programme/Dienstprogramme/*) auf (s. Abb. 7) und klickt auf *Fortfahren*.

Im nächsten Fenster (Abb. 8) wählt man die oberste Option *Von einem Mac, Time Machine-Backup oder Startvolume* und klickt wieder auf *Fortfahren*. Im nachfolgenden Fenster wählt man dann das passende *Time-Machine*-Backup-Volume (Abb. 9) und kommt mit *Fortfahren* zu einem Fenster (Abb. 10), in dem man die konkrete Backup-Version auswählt (sofern mehrere vorhanden sind).

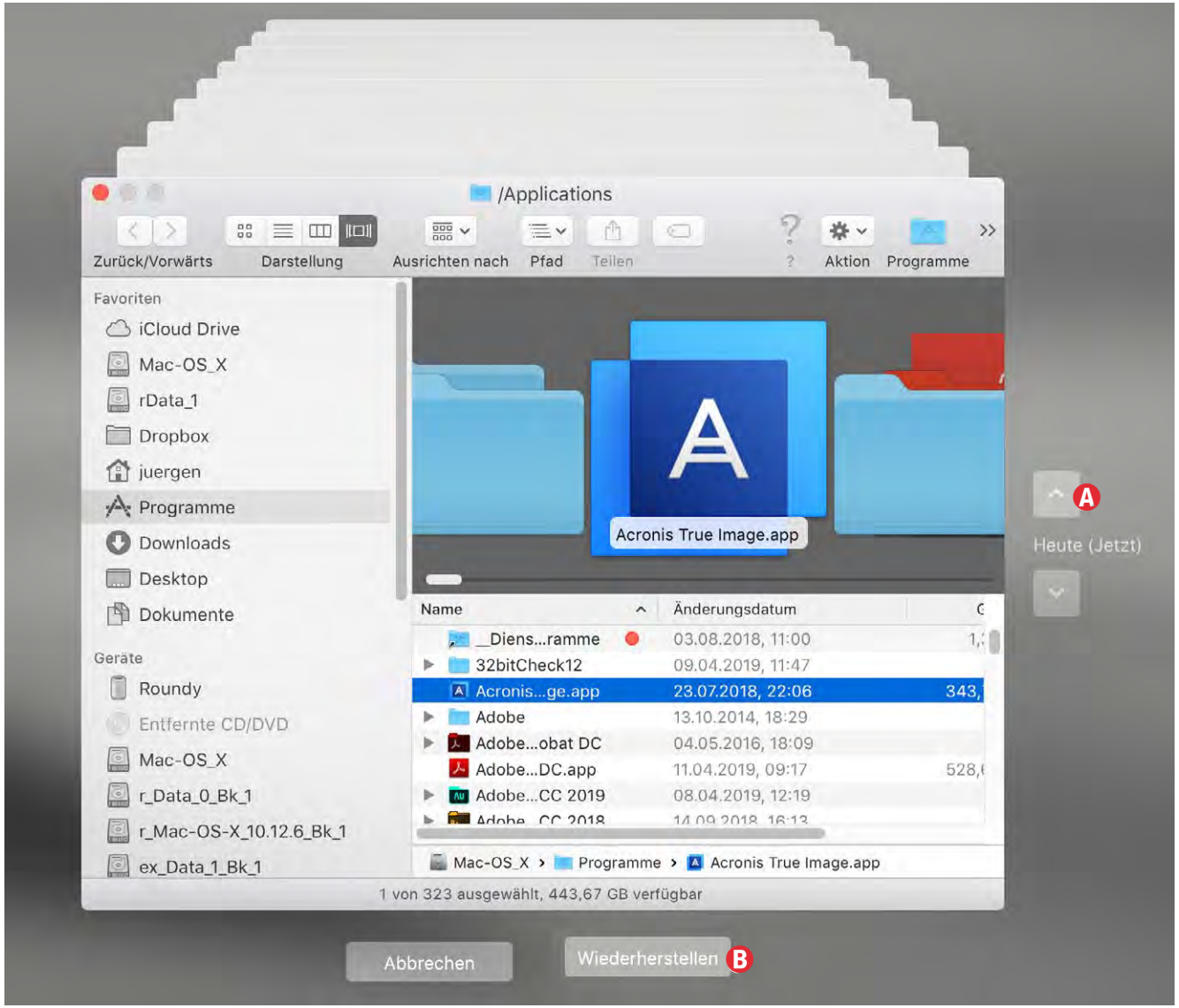


Abb. 6: So etwa sieht das TM-Zeitfenster aus, wenn man Dateien oder ganze Ordner aus einem TM-Backup zurückspielen möchte.

Mit einem weiteren Klick dort auf *Fortfahren* erfolgt schließlich das Einspielen des betreffenden Backups.

Dieser ganze Prozess ist übrigens in der Online-Hilfe der *Time Machine* recht detailliert beschrieben – bei

Abb. 7: Das Laden oder Zurückladen eines mit *Time Machine* erstellten gesamten Backups erledigt man mit dem Programm *Migrationsassistent*.

deutscher Oberfläche in Deutsch (hier könnte sich Microsoft eine Scheibe abschneiden). .

Abb. 9: Hier wählt man, sofern mehrere Sicherungen vorhanden sind, das konkrete Backup, aus dem übertragen werden soll.

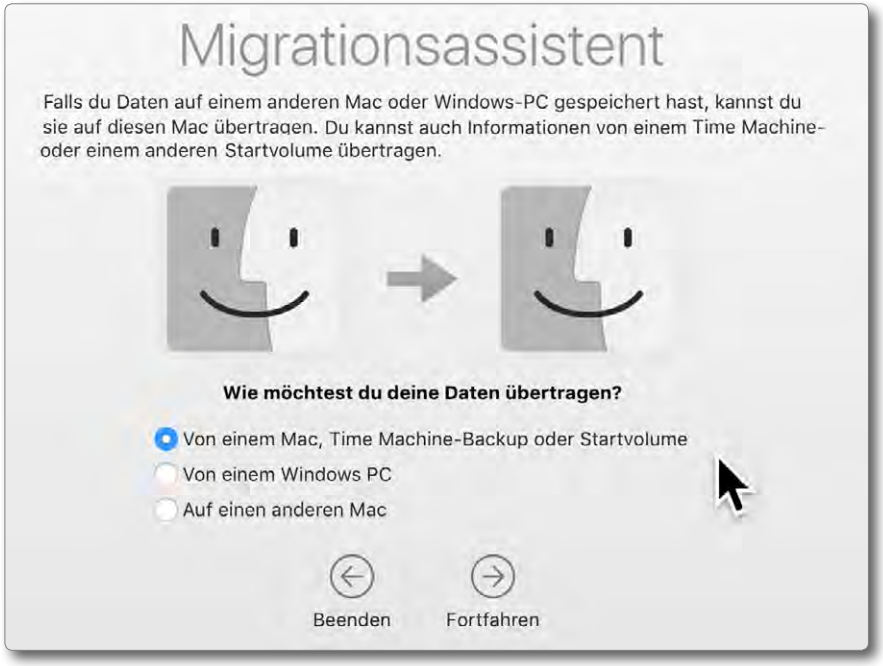


Abb. 8
Der Migrationsassistent bietet mehrere Quellen, von denen man Daten übertragen möchte – in unserem Fall von einem *Time-Machine*-Backup.

Abb. 10
Hier legt man das Volume fest, von dem das *Time-Machine*-Backup geladen werden soll.

Feinsteuerung der Time Machine

Time Machine bietet im Standardfall wenige Eingriffsmöglichkeiten – etwa was die stündlichen Sicherungsintervalle betrifft. Es gibt aber den kleinen kostenlosen *TimeMachineEditor* [9]. Mit ihm lassen sich die Sicherungsintervalle besser kontrollieren (Abb. 11) – etwa Sichern in größeren Intervallen, nur zu bestimmten Zeiten oder nur wenn der Anwender inaktiv ist. Damit diese Steuerung korrekt funktioniert, muss in den *Time Machine*-Einstellungen die Option *Automatische Datensicherung* (Abb. 1 Ⓐ) **deaktiviert** sein. *TimeMachineEditor* stößt dann *Time Machine* für jeden Sicherungslauf explizit an.

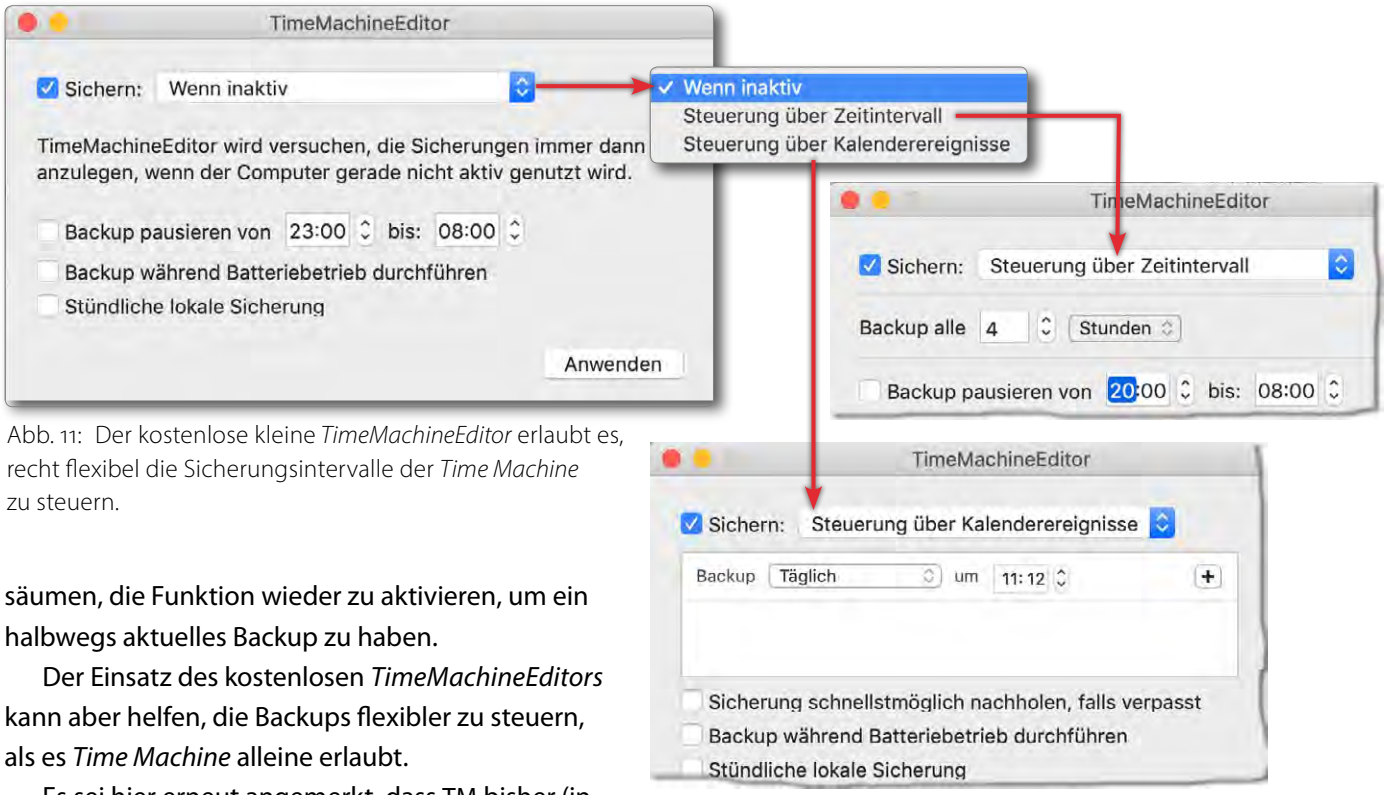


Abb. 11: Der kostenlose kleine *TimeMachineEditor* erlaubt es, recht flexibel die Sicherungsintervalle der *Time Machine* zu steuern.

Nachteile der Time Machine

Time Machine kann durch seine ständigen Aktivitäten eine störende Last im laufenden Betrieb erzeugen. Diese Last betrifft sowohl die Rechenleistung – erhöht, sofern das Backup verschlüsselt wird – als auch die Ein-/Ausgabeleistung. Die Eingriffsmöglichkeiten sind über die normale grafische Oberfläche zudem recht beschränkt. Die Anwendung selbst kann auch bootbaren Backups erstellen (dies geht nur über Zwischenstufen: Quelle per *Time Machine* auf Backup-Volume sichern und später das Backup von dort auf das (oder ein anderes) Boot-Volume restaurieren.

Natürlich kann man *Time Machine* aber jederzeit vorübergehend oder für längere Zeit deaktivieren, um diese Last zu vermeiden, sollte es dann aber nicht versäumen, die Funktion wieder zu aktivieren, um ein halbwegs aktuelles Backup zu haben.

Der Einsatz des kostenlosen *TimeMachineEditors* kann aber helfen, die Backups flexibler zu steuern, als es *Time Machine* alleine erlaubt.

Es sei hier erneut angemerkt, dass TM bisher (inklusive macOS 10.14) zwar die Daten von einem APFS-
Volume sichern kann, jedoch nicht auf ein APFS-, sondern nur auf ein HFS+-Volume! Dieses Volume darf auch über ein Netzwerk angebunden sein – mit gewissen Einschränkungen bei manchen AFP-Implementierungen (*Apple File Protocol*) fremder Anbieter.

Für das Backup normaler Dateien – etwa der eigenen Bilder und des Lightroom-Katalogs, nicht jedoch einer bootfähigen Systempartition – eignet sich auch das kostenlose *FreeFileSync* in der Mac-Version. Eine kurze Anleitung dazu finden Sie auf Seite 100.

Wirklich gut und sehr übersichtlich sind unter macOS daneben die beiden Backup-Lösungen *Carbon Copy Cloner* sowie *SuperDuper!* Beide können bootfähige System-Backups erstellen und sind noch relativ preisgünstig. Beide werden nachfolgend beschrieben.

Zwar gibt es auch unter macOS das von Windows her bekannte *Acronis True Image*; es ist gegenüber den beiden zuvor genannten Anwendungen jedoch teurer, komplexer und weniger elegant.

Es gibt unter macOS außerdem eine kleine Anzahl weiterer, zumeist kostenpflichtiger Backup-Lösungen. Die später noch vorgestellten Varianten sollten aber in aller Regel ausreichen und haben sich bewährt.

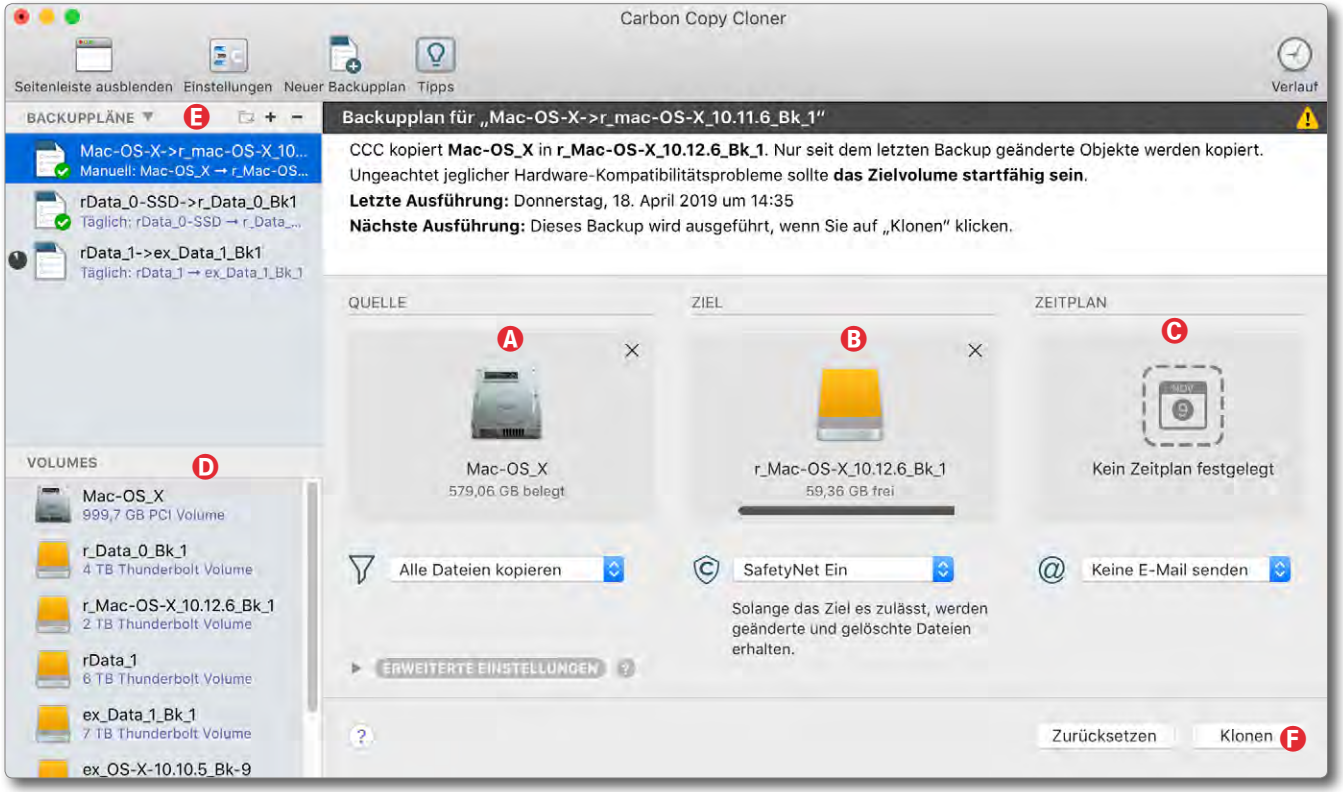


Abb. 1: Carbon Copy Cloner nach dem Start und der Wahl eines Backup-Plans. Oben links sieht man bereits drei Backup-Pläne, die ich aufgesetzt habe und die Backups bzw. Synchronisationen für meine drei wichtigen Partitionen täglich automatisch ausführen.

Unter den aktuellen macOS-Systemen bereitet die Datensicherung deutlich weniger Probleme als unter Windows, insbesondere was die Sicherung des Betriebssystems auf dem Systemlaufwerk betrifft.

MacOS kommt bereits mit einem aus Apples Sicht brauchbaren Sicherungsprogramm: *Time Machine*. Ich selbst kann mich mit dieser (kostenlosen) Anwendung aber aus unterschiedlichen Gründen nicht anfreunden und verwende stattdessen *Carbon Copy Cloner* der Firma Bombich [3]. Das Warum dürfte bei der Beschreibung verständlich werden: Das Programm ist sehr robust, recht funktional und – einmal aufgesetzt – extrem einfach zu bedienen.

Eine Lizenz kostet momentan 37 Euro und kann dafür auf bis zu fünf eigenen Rechnern eingesetzt werden. Auch die Preise für Updates mit neuen Hauptversionsnummern (etwa von 4.x auf 5.x) sind moderat (ca. 50 % des Neupreises). Die Oberfläche unterstützt mehrere Sprachen, darunter auch Deutsch. Hier kurz das Konzept von *Carbon Copy Cloner* (CCC):

- Im Standardfall kopiert – genauer: synchronisiert – man von einem Quellvolume auf ein Zielvolume.

- Dabei lassen sich einzelne Ordner von der Sicherung bzw. Synchronisation ausschließen – etwa temporäre Dateien, Caches und Ähnliches.

- *Synchronisieren* bedeutet hier, dass CCC die Quelle und das Ziel vergleicht und das Ziel auf den Stand der Quelle bringt. Alles, was auf der Quelle neuer als im Ziel ist, wird auf dem Ziel aktualisiert. Synchronisiert man auf ein zunächst leeres Volume, kann dieses Synchronisieren bei vielen Dateien in der Quelle relativ lange dauern – abhängig auch von der Größe der Dateien in der Quelle.

  Bei späteren Läufen werden aber nur noch neue oder geänderte Dateien übertragen, was diese Übertragung erheblich beschleunigt.

  Dateien, die seit der letzten Sicherung auf der Quelle gelöscht wurden, werden im Standardfall auch auf dem Zielvolume gelöscht.

- Optional kann man ›ältere Dateien‹, die auf der Quelle geändert wurden, auch in einen speziellen Bereich des Ziels verschieben lassen, statt sie zu überschreiben – solange auf dem Ziel noch ausreichend Platz ist. Reicht der Platz nicht mehr, werden ›ältere Dateien‹ gelöscht, um Platz zu schaffen.

- CCC nimmt keine eigene Komprimierung vor. Dies hat Vor- und Nachteile. Der Nachteil liegt darin, dass

mehr Platz benötigt wird. Der Vorteil liegt in einer schnelleren Synchronisierung (es muss nicht extra komprimiert werden) und darin, dass die Dateien auf der Quelle und im Ziel in identischer Form vorliegen und zur Nutzung einer Datei auf dem Ziel diese nicht zuvor dekomprimiert werden muss.

- CCC nimmt selbst keine Verschlüsselung vor. Möchte man verschlüsselte Backups haben, muss man auf ein Volume mit verschlüsseltem Dateisystem sichern.

- CCC erlaubt es, das Synchronisieren automatisch zeitgesteuert zu starten. Für die Partition mit meinen Arbeitsdateien tue ich dies z. B. täglich – mit versetzten Zeitpunkten für meine unterschiedlichen Partitionen, um keine zu hohe Systemlast zu erzeugen, die mich beim Arbeiten stört.

- Es gibt eine ganze Reihe weiterer Optionen für die Sicherung. Man findet einige davon in den *Erweiterten Einstellungen* (Abb. 2). Als Beispiele seien genannt:

  – Man kann sich eine E-Mail schicken lassen, die über die Sicherung informiert, optional nur bei aufgetretenen Problemen.

  – CCC führt eine strenge Volume-Erkennung durch; es kopiert damit nur dann, wenn das Zielvolume wirklich genau die Kennung hat wie im Terminplan eingestellt. Damit wird verhindert, versehentlich auf ein Ziel zu kopieren, das nur den gleichen Namen wie das ursprüngliche Ziel hat, nicht aber die gleiche Volume-ID. (Den Buchstabensalat von Windows, bei dem der Laufwerksbuchstabe von Mal zu Mal wechseln kann, gibt es unter macOS nicht.)

  – Man kann Objekte/Dateien und Ordner, die auf der obersten Ebene des Zielvolumes liegen, vor dem Überschreiben schützen.

  – CCC kann versuchen, korrupte Dateien über ein Prüfsummenverfahren auf der Quelle zu erkennen und dann die betreffende Datei erneut zu übertragen. Dies verlangsamt die Synchronisation erheblich, kann aber wertvoll sein.

  – Ist auf dem Ziel eine Datei neuer als in der Quelle, so kann man per Option verhindern, dass diese überschrieben wird.

  – In der Regel werden beim Synchronisieren die Zugriffsrechte und andere Dateiattribute mit in

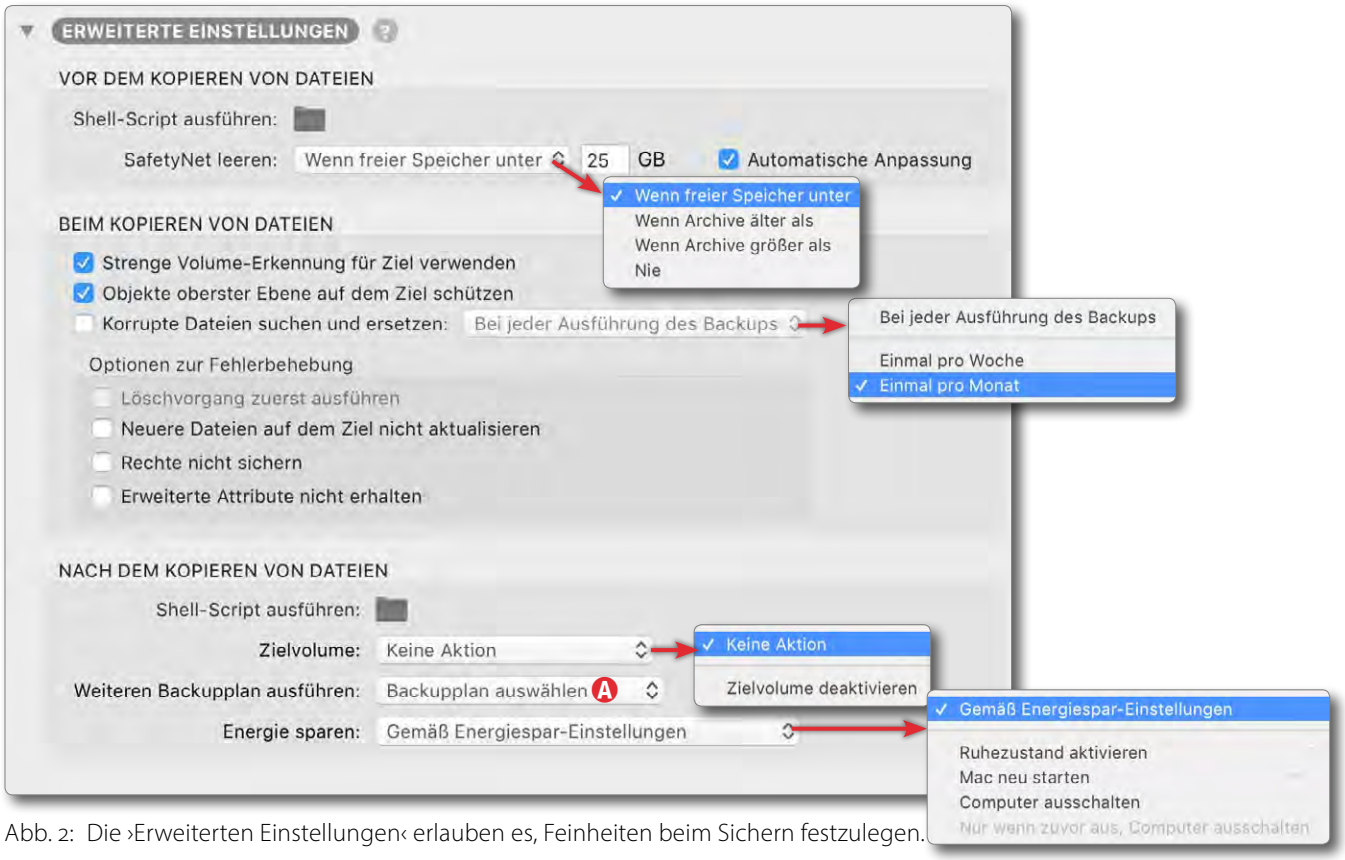


Abb. 2: Die ›Erweiterten Einstellungen‹ erlauben es, Feinheiten beim Sichern festzulegen.

das Ziel übernommen. Dies lässt sich unterdrücken (mir fällt dafür jedoch kein Grund ein).

– Es lässt sich festlegen, was nach dem Sicherungslauf erfolgen soll – etwa das Zielvolume deaktivieren oder den Rechner danach herunterfahren sowie weitere Backup-Pläne anstoßen, etwa um verschiedene Volumes nacheinander zu sichern oder die Dateien von der Quelle gleich auf zwei unterschiedliche Zielvolumes zu sichern.

– Es ist möglich, sowohl vor dem Sichern als auch nach dem Sichern ein Shell-Skript auszuführen – zuvor etwa zum Herunterfahren einer Datenbank oder zum Online-Schalten eines Offline-Datenträgers und danach (wieder optional) zum Offline-Schalten (*unmount*) des gesicherten Laufwerks oder der Partition.

– Einzelne Backup-Pläne lassen sich verketten, so dass man sie (automatisch) nacheinander ausführt, um so etwa eine hohe Ein-/Ausgabelast durch eine parallele Ausführung zu vermeiden.

Ein Klick auf das Tipps-Icon ( ) im Kopf des CCC-Fensters blendet zu allen wesentlichen Bereichen in recht übersichtlicher Weise kleine farbige Tooltips ein (Abb. 5).

Ablauf

Zu Beginn zieht man aus der Liste der aktuell sichtbaren Volumes Ⓓ (Abb. 1) das gewünschte Quellvolume auf *Quelle* (Abb. 1 Ⓐ) – oder klickt dort auf das Quell-Icon und wählt in der dann erscheinenden Liste der verfügbaren Volumes das Quellvolume aus (das gesichert werden soll). Danach wiederholt man dies für das Zielvolume (Abb. 1 Ⓑ), auf das gesichert werden soll. CCC erkennt, wenn beide identisch sind oder das aktive Systemvolume als Ziel gewählt wird, und meldet einen Fehler.

Danach nimmt man die wichtigsten **Sicherungseinstellungen vor, wo**bei hierfür CCC bereits sinnvolle Vorbelegungen vorgenommen hat. Diese Einstellungen ruft man über die beiden Menüs unter der Quelle und dem Ziel auf.

Schließlich legt man unter Zeitplan (Abb. 1 Ⓒ) (Klick auf das -Icon) den gewünschten Startzeitpunkt und das Sicherungsintervall fest. Die Zeitplanung ist recht flexibel, wie die Abbildungen 3 und 4 zeigen. Statt nach einem Zeitplan lässt sich die Synchronisierung per Klick auf *Klonen* (Abb. 1 Ⓕ) auch sofort starten.

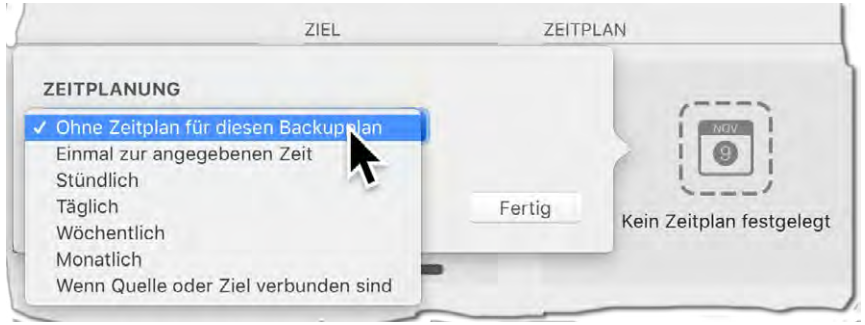


Abb. 3: Unter *Zeitplanung* gibt es mehrere Möglichkeiten.

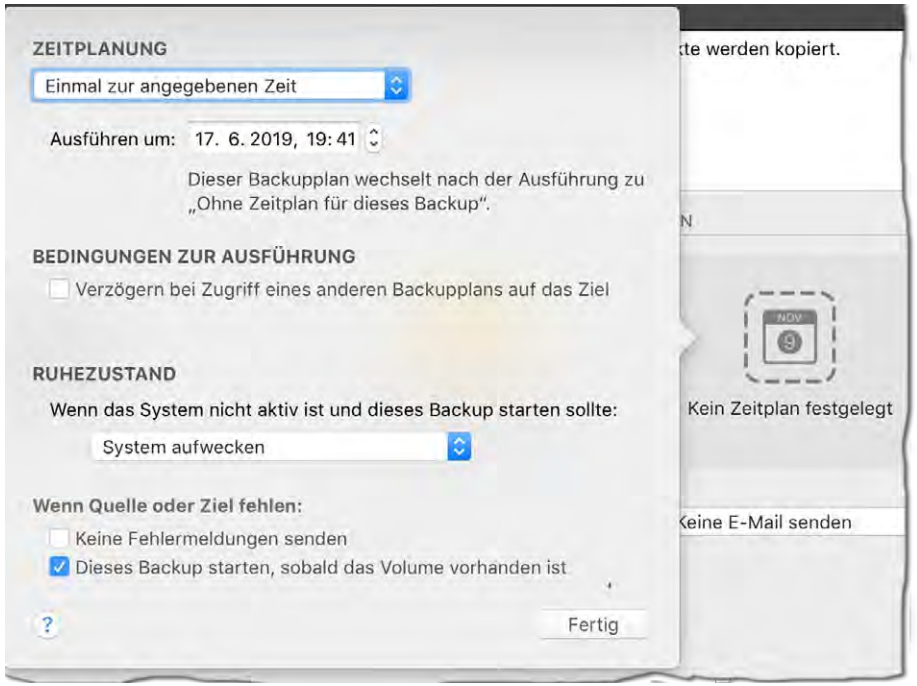


Abb. 4: Wählt man unter *Zeitplanung* die Variante *Einmal zur angegebenen Zeit*, so lassen sich weitere Optionen nutzen, etwa dass das Backup nachgeholt werden soll, sobald das Zielvolume verfügbar wird.

Wählt man im Bereich *Backup-Pläne* (Abb. 1 Ⓔ, Seite 50) einen bereits zuvor angelegten Backup-Plan, so werden dessen Einstellungen direkt in die Quell- und

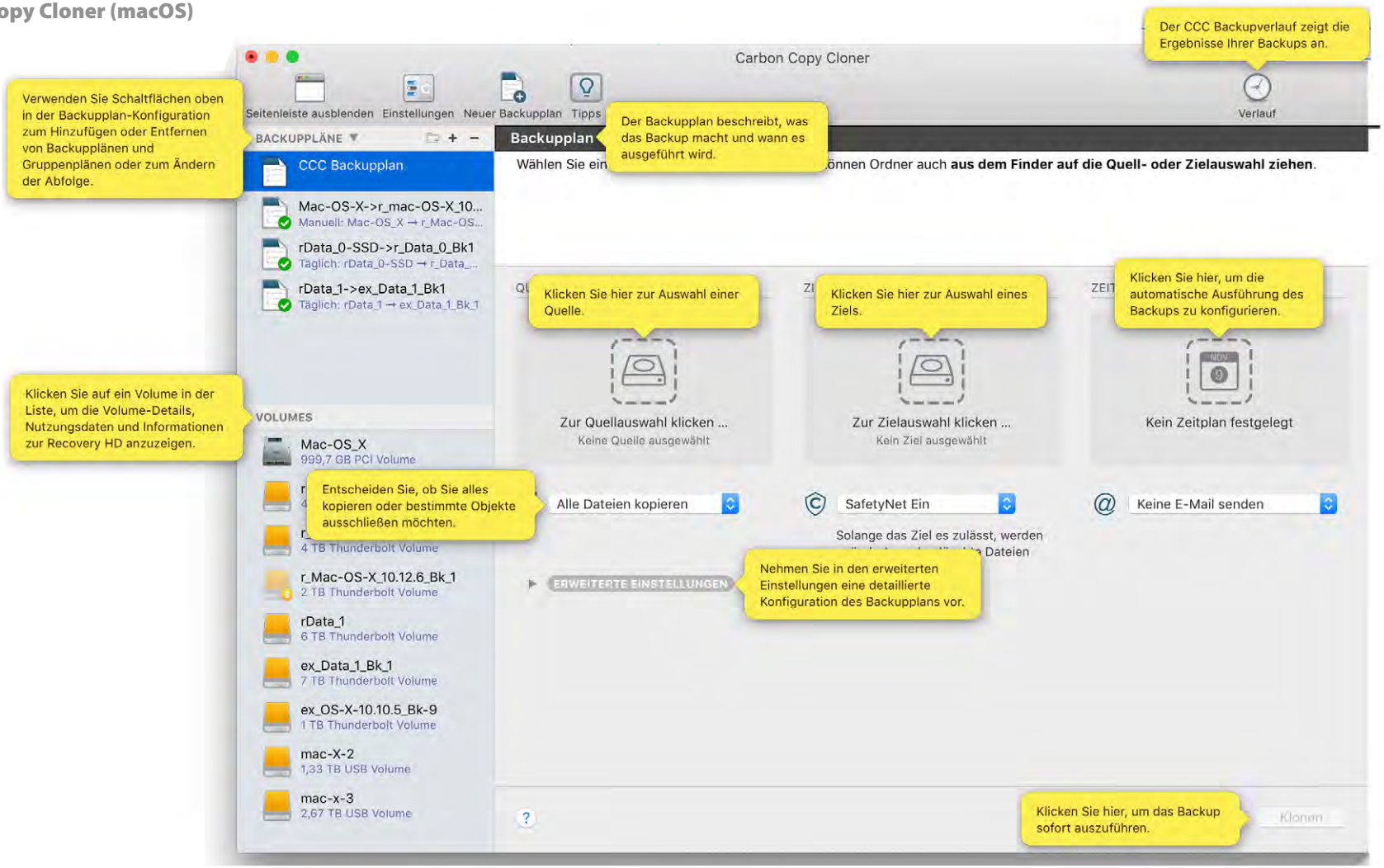


Abb. 5: Ein Klick auf das Tipps-Icon Im Kopf des CCC-Fensters blendet als gelbe Sticker Hinweise zur Funktion der jeweiligen Bereiche ein.

Zielfelder sowie in die dazugehörigen Einstellungen übernommen, können aber für die nächste Sicherung noch modifiziert werden.

CCC liefert im Kopf des Fensters ausreichend Informationen über seine laufende Tätigkeit und meldet zum Schuss den erfolgreichen Abschluss oder gibt einen Hinweis auf aufgetretene Probleme.

Läuft ein automatisch gestarteter Backup-Plan im Hintergrund, ist das CCC-Fenster nicht sichtbar und stört so nicht.

Ist ein im Zeitplaner vorgesehener Sicherungslauf einmal ausgefallen, etwa weil das System ausgeschaltet oder der Datenträger nicht verfügbar (z. B. abgezogen) war, so startet CCC den Sicherungslauf (bei entsprechender Einstellung im Zeitplaner), sobald der Datenträger wieder verfügbar ist.

Eine zeit- und rechenaufwändige Option ist *Korrupte Dateien suchen und ersetzen*. Dabei wird für jede zu sichernde Datei sowohl in der Quelle und nach dem Sichern im Ziel eine Prüfsumme berechnet und dann verglichen. Damit lassen sich Übertragungsfehler oder umgekippte Bits im Backup erkennen, und die Übertragung lässt sich wiederholen. Es empfiehlt sich, dies in bestimmten Intervallen (etwa einmal wöchentlich oder monatlich) zu tun. Entsprechende Einstellungen lassen sich aus dem Menü hinter der entsprechenden Option abrufen (Abb. 2, Seite 51).

Unter *SafetyNet* – die Option unter dem Ziel – versteht man bei CCC die Möglichkeit, Dateien, die im Ziel eigentlich gelöscht oder überschrieben werden (da sie

veraltet sind oder in der Quelle gelöscht wurden), stattdessen in einen separaten Bereich des Zielvolumes zu verschieben, von wo sie bei Bedarf nochmals zurückgeholt werden können. Dies implementiert eine Art Versionierung. Diese Dateien findet man in Zielvolume unter ›_CCC_SafetyNet‹, geordnet nach dem Datum der einzelnen Sicherungsläufe.

Was CCC nicht kann, ist, einen gesamten Datenträger auf einmal zu sichern (sofern dieser mehrere Partitionen hat). Hier muss man für jedes Volume des Datenträgers einen getrennten Sicherungsauftrag aufsetzen und diese Aufträge bei Bedarf verketten (über die Option *Weiteren Backupplan ausführen* (Abb. 2 Ⓐ). Für mich ist dies aber keine ernsthafte Einschränkung.

Zurückspielen gesicherter Dateien

Da die Dateien im Zielvolume als normale Dateien vorliegen, lassen sich einzelne Dateien oder ganze Ordner per Drag & Drop oder per *Kopieren* (bzw. ⌘-C)und einem anschließenden *Einfügen* (per ⌘-V) im *Finder* auf ein anderes Volume oder das ursprüngliche Quellvolume bringen.

Größere Dateimengen lassen sich durch ein Synchronisieren in der anderen Richtung übertragen – vom Backup-Volume auf das ursprüngliche Quellvolume (oder ein anderes Volume). Auf diese Weise lässt sich auch ein korrumpiertes Systemvolume reparieren (jedoch nur bedingt, wenn es das aktive Systemvolume ist).

Resümee

Insgesamt arbeitet CCC vorbildlich und ist aus meiner Sicht sein Geld mehrfach wert. Es bleiben aber kleine Wünsche. So wäre es schön, dass nicht nur die Benutzeroberfläche auf deutschen Systemen in Deutsch erscheint, sondern auch die detaillierte Hilfe vollständig in Deutsch gezeigt würde. Bisher stehen diese Informationen nur in Englisch zur Verfügung.

Die Erläuterungen zu den einzelnen Funktionen sind ausführlich. Für manche Feinheiten muss man sich aber schon einmal in das Handbuch vertiefen, insbesondere dann, wenn man etwas komplexere Szenarien abdecken möchte.

Ich wünschte mir, dass mehr Software eine solche gut gestaltete Oberfläche hätte und auch die komplexeren Funktionen (so man sie benötigt) so gut wie hier beschrieben wären.

CCC hat gegenüber *Time Machine* zahlreiche Vorteile. So kann es problemlos Sicherungen und Volume-Kopien des aktiven (laufenden) Systemvolumes erstellen – solche, von denen man booten kann. Man muss zwar bei mehreren zu sichernden Volumes getrennte Backup-Aufträge für jedes einzelne zu sichernde Volume erstellen, kann diese Aufträge aber zu einer Auftragskette verknüpfen oder automatisch zeitversetzt (über den Zeitplaner) ablaufen lassen. Dass das Backup-Format als Standard-Volume-Format angelegt wird, erweist sich in der Praxis oft als Vorteil, da man so diese Volumes bei Bedarf aktivieren und ›normal‹ und ohne spezielle Programme darauf zugreifen oder einzelne oder auch mehrere Dateien zurückübertragen kann.

Datensicherung per SuperDuper!

SuperDuper! ist ein weiteres, sehr einfach zu bedienendes Backup-Programm unter macOS. (Das Ausrufezeichen ist Teil des Namens.) Es stammt von der Firma *Shirt Pocket* und ist mit ca. 27 Euro relativ preiswert. Die Oberfläche und das Handbuch sind aber (leider) ausschließlich englisch, jedoch gut verständlich. *SuperDuper!* (hier mit SD abgekürzt) ›synchronisiert‹, erstellt also ›normale‹ Dateien im Ziel und keine ›Backup-Objekte‹. Im Gegensatz zu *FreeFileSync* (siehe Seite 100) lassen sich damit auch Betriebssystem-Partitionen klonen und bootfähige Systeme erstellen. SD läuft auch unter macOS 10.14 (Mojave), kommt mit HFS+- und APFS-Volumes zurecht und kann bei APFS sogar sogenannte *Snapshots* erstellen.

Die Oberfläche ist ausgesprochen übersichtlich, wie Abbildung 1 zeigt. Unter *Copy* Ⓐ wählt man die Quelle aus (nur ganze Volumes), unter *to* Ⓑ das Ziel (wiederum nur ganze Volumes) und unter *using* Ⓒ was alles kopiert werden soll. Was dabei geschieht, wird verständlich (englisch) unter *What's going to happen?* beschrieben. Feinheiten zum Ablauf lassen sich über die Dialoge unter Knopf Ⓓ *Options* einstellen (siehe weiter hinten).

Ein Klick auf *Copy Now* Ⓔ startet den Backup-Vorgang – nach zwei kurzen Rückfragen. Während der Sicherung wird der Fortschritt im Fenster in recht übersichtlicher Art angezeigt (Abb. 3).

Möchte man die Sicherung nicht sofort, sondern später über den *Scheduler* (Zeitplaner) ausführen, klickt man statt auf *Copy Now* auf *Schedule* Ⓕ.

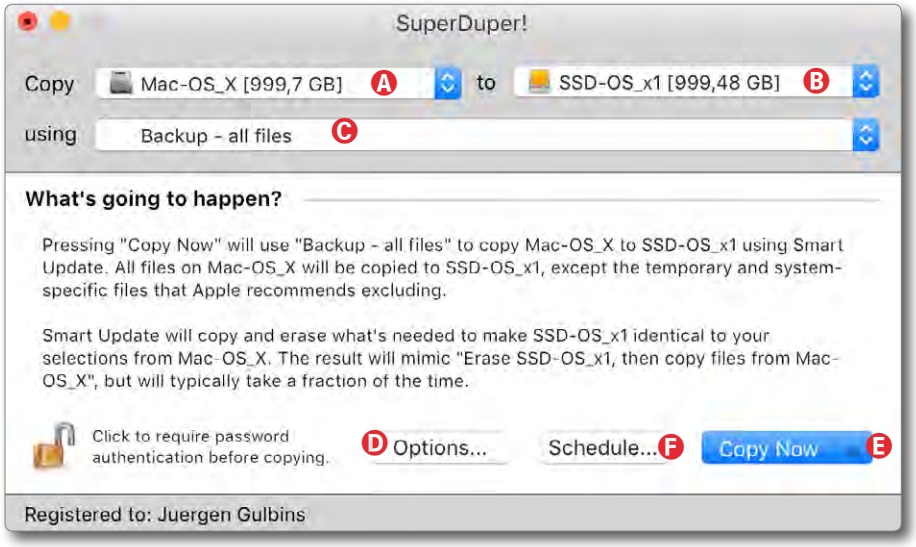


Abb. 1:
Das Startfenster von *SuperDuper!* in der Version 3.2.4. Man sichert die Quelle unter Ⓐ in bzw. auf das Ziel unter Ⓑ. Unter Ⓒ stellt man ein, was kopiert werden soll. Details lassen sich über den *Options*-Knopf Ⓓ einstellen.

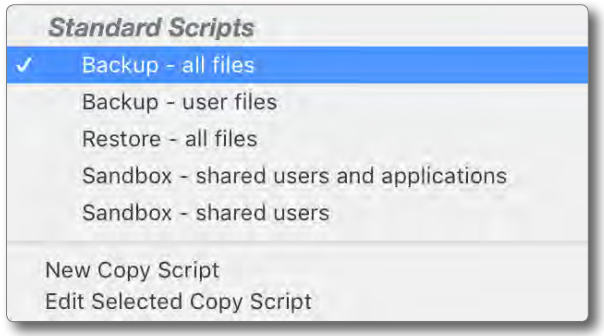


Abb. 2: Hier das Menü Ⓒ (aus Abb. 1) mit den Kopierfunktionen bzw. den dabei verwendeten Skripten.

Zum ›Kopieren‹ werden im Menü Ⓒ die in Abbildung 2 gezeigten Funktionen angeboten. Im Standardfall verwendet man das erste Skript *Backup – all files*. Es lassen sich jedoch auch nur die **Benutzerdateien synchronisieren** (*Backup – user files*) oder sogar eigene Sicherungsskripte erstellen oder die vorhandenen bearbeiten. Mit Backup ist hier gemeint, dass ausschließlich von der Quelle zum Ziel kopiert wird. Beim ersten

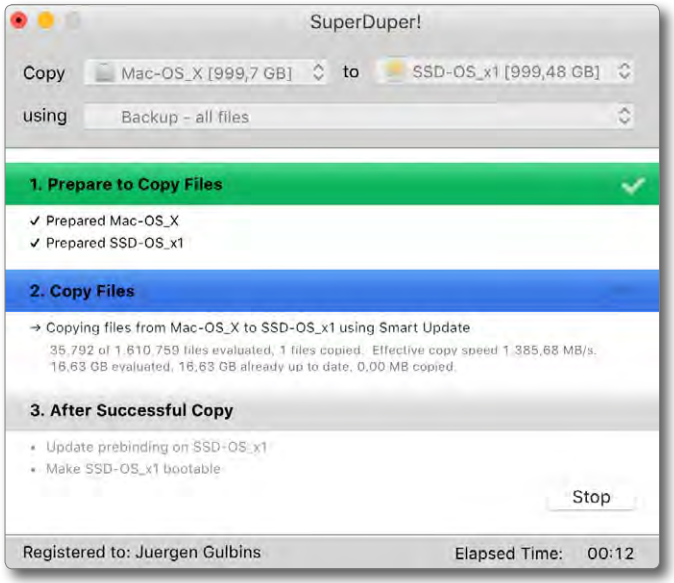


Abb. 3: *SuperDuper!* zeigt während des Backups übersichtlich an, was abläuft.

Sicherungslauf, wenn das Zielvolume noch leer ist (oder ganz andere Dateien enthält), wird eine vollständige Sicherung durchgeführt; bei nachfolgenden

Läufen wird smart gearbeitet, **d. h. es werden nur Dateien kopiert**, die in der Quelle neuer als im Ziel sind. Was auf der Quelle nicht (mehr) vorhanden ist, wird im Ziel bei Bedarf gelöscht. Dateiattribute werden aus der Quelle sauber ins Ziel übernommen. SD erlaubt nur ganze Volumes zu sichern, nicht jedoch lediglich Ordner bzw. einzelne Dateibäume.

Möchte man das Backup zeitgesteuert und automatisch durchführen, so steht dafür der Scheduler zur Verfügung (Abb. 4), den man nach dem Einstellen der Backup-Parameter über den Knopf *Schedule* im Basisfenster (Abb. 1 Ⓕ) aufruft. Ist das Zielvolume zum Backup-Termin nicht verfügbar, so lässt sich hier über die Option *When you connect … to your Macintosh* festlegen, dass das Backup nachgeholt wird, sobald das Zielvolume angeschlossen ist.

In den SD-Voreinstellungen (*Preferences*) lässt sich beispielsweise festlegen, dass von einem Virus-Scanner als Virus markierte Dateien beim Backup nicht berücksichtigt werden (Abb. 6).

Über den Knopf *Options* Ⓓ im Basisfenster (Abb. 1) kommt man zu weitergehenden Einstellungen für den Backup-Vorgang. Sie sind in zwei Reiter unterteilt: *General* und *Advanced*.

Im Reiter *General* (Abb. 7) wählt man im Menü *During copy* die Art der Synchronisation. Im Standardfall setzt man hier *Smart Updates*. Im Menü *On successful completion* (Abb. 7 Ⓕ) legt man fest, was nach einem erfolgreichen Backup geschehen soll (im Standardfall *Do Nothing*). Das Zielvolume lässt sich aber auch automatisch auswerfen (per *Eject*) oder das gesamte System lässt sich herunterfahren mittels *Shut Down Computer*.

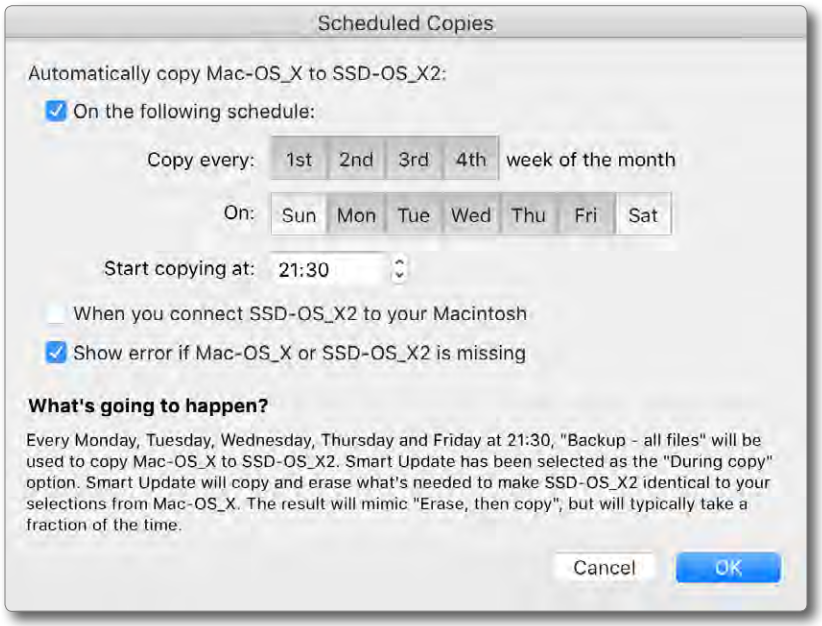


Abb. 4: Im Scheduler lässt sich festlegen, wann ein Backup-Auftrag ausgeführt werden soll. Mit der Option *When you connect … to your Macintosh* lässt sich ein ausgefallener Sicherungslauf nachholen, sobald das betreffende Volume verfügbar wird.

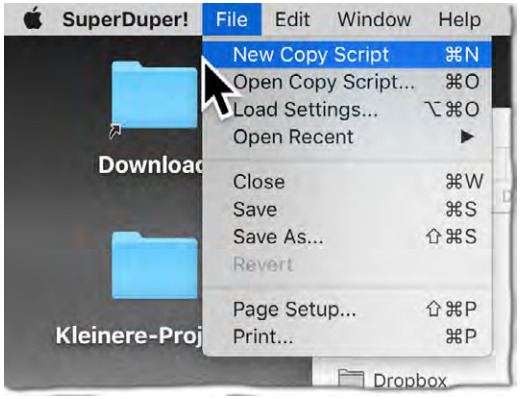


Abb. 5: Im Hauptmenü von SD lassen sich unter *File* neue Backup-Skripten anlegen, solche Skripten öffnen und zuvor gesicherte Einstellungen (*Settings*) abrufen.

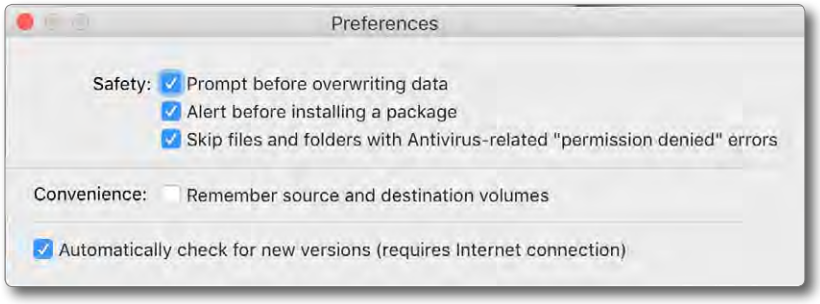


Abb. 6: Einige Voreinstellungen unter SuperDuper! ▸ Preferences

Im Reiter *Advanced* findet man weitere Backup-Einstellungen (Abb. 8). Dort kann man etwa ein Skript festlegen, das vor dem Kopieren ausgeführt wird, und ein weiteres nach dem Kopieren. Die Option *Copy ACLs*

from xxx sollte im Standardfall aktiviert sein, um die Zugriffsrechte aus der Quelle ins Ziel zu übernehmen.

Das Rückspielen von Dateien

Da SD keine Backup-Objekte, sondern normale Dateien auf das Zielvolume legt, lassen sich einzelne Dateien oder ganze Dateibäume einfach von dort zurück auf das Quellvolume (oder ein anderes Volume) kopieren (etwa mit dem *Finder*). Ebenso lässt sich ein ganzes ehemaliges Zielvolume auf ein neues Volume spielen (das ehemalige Zielvolume wird zum Quellvolume). Sie können Dateien aber auch zurücksynchronisieren, indem Sie in den Einstellungen einfach Quelle und Ziel austauschen. SD verhält sich hier sehr ähnlich zu *Carbon Copy Cloner*. Wie bei CCC ist es nicht möglich, im laufenden Betrieb eine vollständige Synchronisation auf das aktive Systemvolume auszuführen – dabei würden laufende Programme und Systemkomponenten überschrieben. Besteht der Bedarf, ein Systemvolume zu restaurieren, so muss man von einem anderen Systemvolume booten und das Restaurieren (Synchronisieren) auf das Volume ausführen, dessen System gerade nicht aktiv ist. Diese Restriktion gilt sowohl für *Carbon Copy Cloner* als auch (in etwas modifizierter Form) für *Time Machine*!

Was *SuperDuper!* nicht kann, ist die Sicherung über Netzwerk (etwa auf ein NAS). Dafür muss man beispielsweise auf *Carbon Copy Cloner* zurückgreifen.

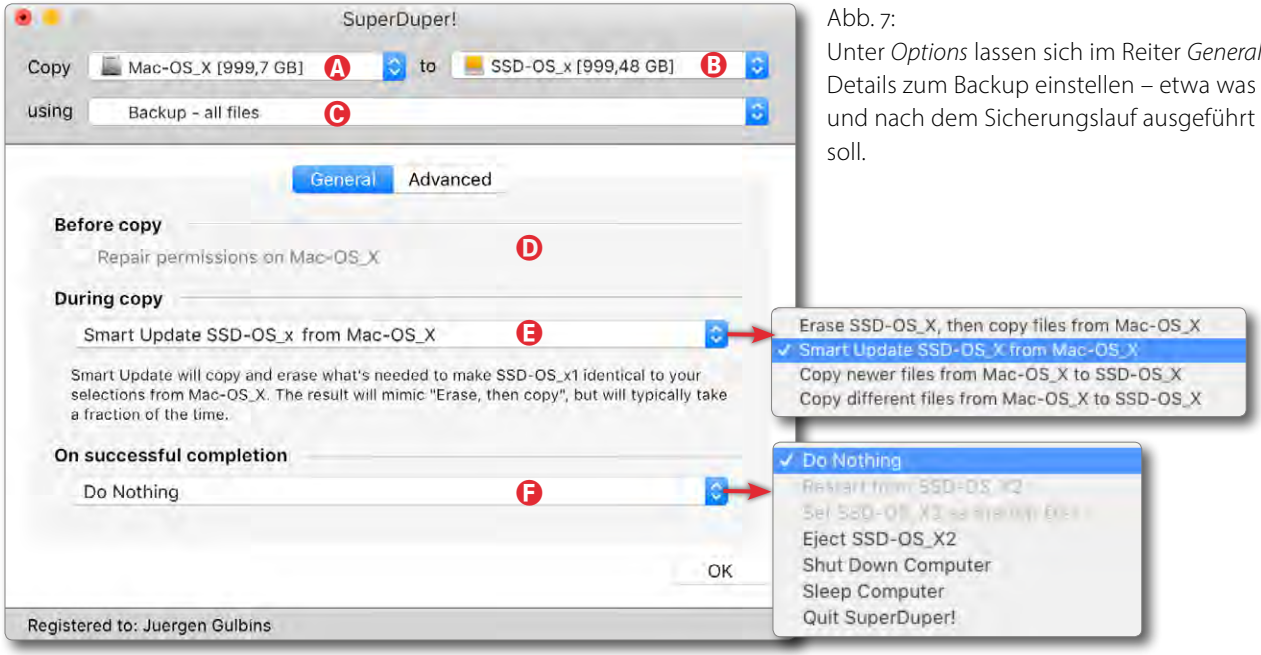


Abb. 7:
Unter *Options* lassen sich im Reiter *General* einige Details zum Backup einstellen – etwa was vor und nach dem Sicherungslauf ausgeführt werden soll.

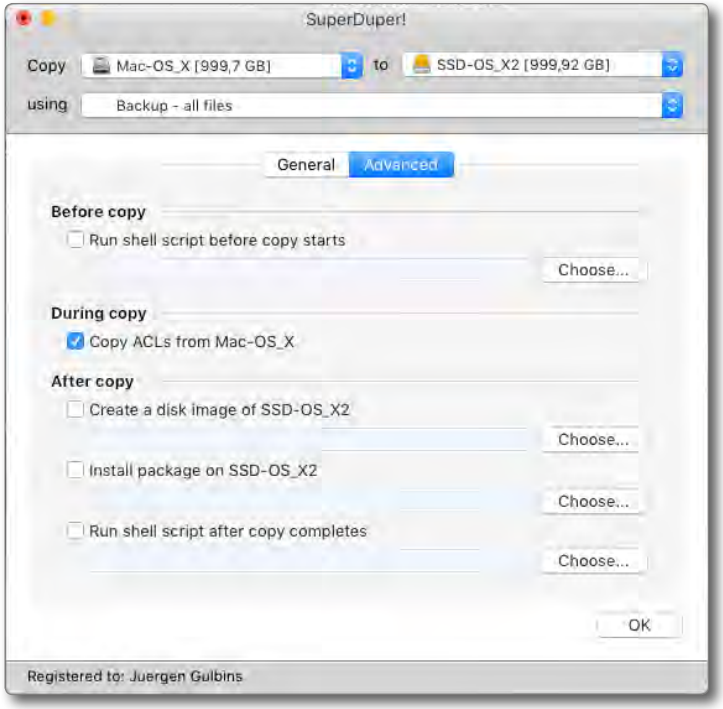


Abb. 8:
Im Reiter *Advanced* findet man weitere Einstellungen zum Backup-Lauf. In der Regel sollte man die ACLs (Zugriffsrechte auf die einzelnen Dateien) aus der Quelle übernehmen.

Zusammenfassung

Insgesamt erweist sich *SuperDuper!* als einfach zu handhabendes, robustes und preiswertes Backup-Programm. Die Updates auf neuere Versionen sind (meines Wissens) bisher kostenlos. Man benötigt aber pro Rechner eine Lizenz. Nachteilig mag für manchen Anwender die englischsprachige Oberfläche sein.

Eine weitere sehr gute und umfassende Lösung für Backups unter macOS ist *ChronoSync* der Firma *Econ Technologies* [6]. Wie mit *Carbon Copy Cloner* und *SuperDuper!* lassen sich damit sehr einfach ganze Volumes sichern bzw. synchronisieren – auch solche mit einem System darauf. Die Kopie ist dann auch bootbar. Es lassen sich aber auch einzelne Ordner (oder mehrere Ordner) sichern bzw. synchronisieren, dies sowohl auf einen lokal angeschlossenen Datenträger (ein Volume) als auch auf andere Systeme (Macs als eine Art Backup-Server), auf NAS oder auf verschiedene Cloud-Speicher.

ChronoSync bietet neben anderen Sprachen auch eine deutsche Oberfläche. Die Einzellizenz kostet etwa 50 USD (im Download); zusammen mit einem *ChronoAgent* beträgt der Preis etwa 60 USD. Der optionale *ChronoAgent* (ca. 11 USD je Rechner) erlaubt es, von einem Mac-Rechner aus die Sicherung für mehrere Rechner zu kontrollieren und auszuführen. Man benötigt dann einen Agent pro Remote-Rechner sowie eine *ChronoSync*-Lizenz auf dem Server (Mac). Bei *ChronoSync* sind auch größere Updates kostenlos!

Eine etwas vereinfachte Version ist *ChronoSync Express* für etwa 28 Euro im *App Store*. Die *Express*-Version kann jedoch keine bootbaren Systeme erzeugen.

Ich beschreibe hier *ChronoSync* in der Version 4.9.3. Sie kann auch mit APFS-Volumes umgehen und bootbare Kopien des Systems erzeugen. Im Ziel werden ›normale‹ Dateien abgelegt mit allen Attributen der Quelldatei.

Abb. 1: Das Organizer-Fenster von *ChronoSync* bietet eine Auftragsübersicht sowie einige Assistenten zum Anlegen neuer Sicherungsaufträge.

Ablauf

Zu Beginn öffnet *ChronoSync* sein Organizer-Fenster (Abb. 1), das im linken Bereich beim ersten Aufruf leer ist. Rechts bietet *ChronoSync* drei Assistenten, die helfen, neue Sicherungsaufträge anzulegen.

Ein *Task-Container* ist ein Sicherungsauftrag, der sich aus mehreren einzelnen Aufträgen zusammensetzt. Auf diese Weise lassen sich Aufträge nacheinander ausführen – z. B. unterschiedliche Quellen auf zugeordnete Ziele oder eine Quelle nacheinander auf mehrere Ziele sichern.

Das Schema ist dabei ähnlich wie bei den meisten Backup-Lösungen, hier unterstützt durch Assistenten:

- Man wählt eine zu sichernde Quelle,
- wählt danach das Ziel, auf das gesichert werden soll,
- und nimmt dann optional Feineinstellungen vor.
- Den Auftrag sichert man nun unter einem beschreibenden Namen.

Mit dem letzten Schritt erscheint der Auftrag im Organizer links in der Auftragsliste. Dort kann man ihn auswählen und unter *Aktion* (Abb. 1 Ⓐ) festlegen, was man damit tun möchte. Im Standardfall ist es *Öffnen & Ausführen*. Ein Doppelklick auf einen Auftrag öffnet dann

zusätzlich das Sicherungsfenster in der Ansicht *Konfiguration* (Abb. 2). Unter Umständen wird man zuvor nach dem Administratorpasswort gefragt, damit privilegierte Operationen durchgeführt werden können (z. B. der Zugriff auf Systemdateien).

Zumeist ist ein Auftrag durch den Assistenten bereits vernünftig konfiguriert. Hier lassen sich aber weitere Einstellungen vornehmen. So kann man im Quellen- und Ziel-Feld unter *Optionen* (©) z. B. vorgeben, dass eine strenge Volume-Identifizierung erfolgen soll und dass das Volume nach erfolgreicher Sicherung automatisch deaktiviert wird (Abb. 3).

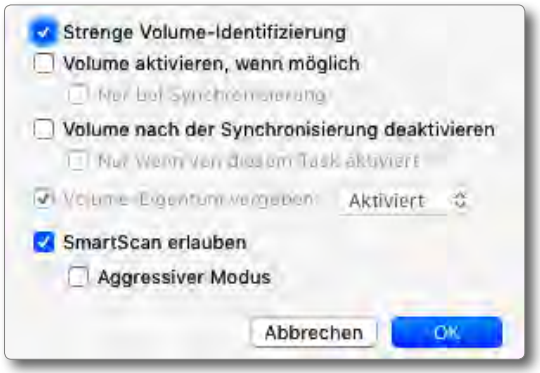


Abb. 3: Die Einstellungen sind unter *Optionen* für die Quelle und das Ziel möglich.

Abb. 2: Im Fenster *Konfiguration* ( ) werden Details zu einem Auftrag angezeigt. Zugleich lassen sich zahlreiche zusätzliche Einstellungen vornehmen.

Ein *SmartScan* – ein vereinfachter und damit schnellerer Vergleich zwischen Quelle und Ziel –ist nur auf direkt fest angeschlossenen Laufwerken möglich und kann den Vergleich spürbar beschleunigen. Ein *SmartScan* ist nicht mit allen einstellbaren Regeln möglich. Mit *Aggressiver Modus* arbeitet *SmartScan* schneller, jedoch auf Kosten von einigen Sicherheitsfunktionen bei der Erkennung von bestimmten Dateisystemereignissen, was dazu führen könnte, dass *SmartScan* einige Änderungen übersieht.

Im Ziel-Panel Ⓑ gibt man unter Ⓓ an, was mit Dateien im Ziel erfolgen soll, die in der Quelle seit dem

letzten Lauf gelöscht wurden. Angeboten wird: *Sofort löschen*, *In den Papierkorb legen* sowie *In das Archiv verschieben* (d. h. in einen verdeckten, normalerweise nicht sichtbaren Ordner ›_*archived items*‹; bei archivierten Dateien werden Versionsnummern an den Dateinamen angehängt).

Unter Ⓔ legt man in der Konfiguration fest, ob Dateien, die seit dem letzten Lauf in der Quelle gelöscht wurden, auch im Ziel zu löschen sind (bzw. optional in das Archiv verschoben werden). Unter Ⓕ definiert man, ob bei Dateien, die in der Quelle neuer als im Ziel sind, die ›alten‹ Zieldateien ins Archiv verschoben werden, bevor die neue Quelldatei ins Ziel kopiert wird.

Sicherungsmodi

Im Konfigurationsfenster (Abb. 2) findet man unter Ⓖ das *Modus*-Menü (Abb. 4). Damit legt man fest, in welcher Richtung gesichert oder synchronisiert wird. Mit *Spiegeln* wird links und rechts ein Gleichstand erzeugt (ohne Archivierung usw.). Bestimmend (die Referenz) ist dabei die durch die gewählte Übertragungsrichtung festgelegte (effektive) Quelle. Der Begriff *blind* impliziert hier, dass eine im Ziel geänderte oder gelöschte Datei **nicht** durch die gleiche Datei aus der Quelle ersetzt wird, sondern erhalten bleibt. Weitere Details dazu findet man in der Online-Hilfe, die man dazu über ? abruft. Man sollte diese wichtigen Einstellungen und die Hilfe zu Beginn sorgfältig studieren.

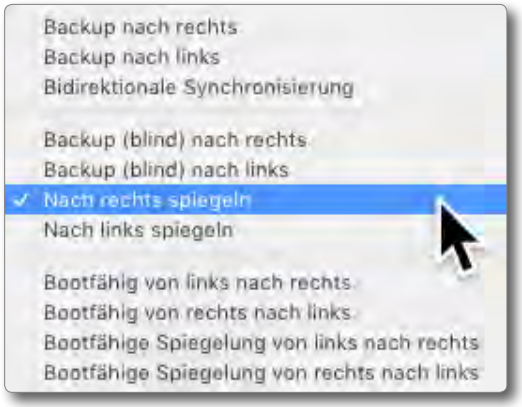


Abb. 4: Das *Modus*-Menü von *ChronoSync* erlaubt verschiedene Übertragungsrichtungen sowie unterschiedliche Arten.

Icons in der Kopfzeile des Konfigurationsfensters

Ein Klick auf das *Sichern*-Icon in der Kopfzeile des Fensters sichert die aktuellen Einstellungen für den Auftrag; *Synchronisieren* () führt die Sicherung/Synchronisierung durch, *Probesync* () führt eine Probe-Synchronisierung durch. Im Ergebnis wird die Anzahl der Abweichungen mit einigen Details aufgelistet.

Validieren () vergleicht die Dateien der Quelle (links) mit jenen im Ziel (rechts) und gibt die Unterschiede aus. Im mit *Validieren* aufgerufenen Dialog lassen sich eine ganze Reihe von Metadaten auswählen, die zum Vergleich herangezogen werden. Das Ergebnis ist eine Liste mit der Anzahl verglichener Dateien, der Anzahl der Unterschiede, mit den gefundenen Waisen (Dateien ohne zugehörigen Eintrag in einem Verzeichnis) und einigem mehr.

Über **>>** kommt man zu weiteren Funktionen – hier *Zur Zeitplanung hinzufügen* () (siehe Seite 62) sowie *Protokoll* (), was das Protokoll des letzen (aktuell gewählten) Sicherungsauftrags anzeigt.

Abb. 5: Das Fenster mit den Optionen hat sieben Reiter.

Die verschiedenen Konfigurations-Panels

Wechselt man per Klick auf *Optionen* (in der Icon-Leiste links) in das Optionen-Fenster, so findet man dort eine Vielzahl von Optionen, untergliedert in die sieben Reiter von Abbildung 5. Um weitere Details zu sehen, klappt man die einzelnen Reiter aus. Auf eine detaillierte Beschreibung der zahlreichen Einstellungen

sei hier verzichtet, zumal die Online-Hilfe wirklich gut ausgebaut ist (und dies auch auf Deutsch). Die Hilfe zu den Punkten eines Reiters ruft man per Klick auf das Icon (?) im Reiter auf.

Im Fenster zu den *Regeln* (per Klick auf) gibt man Regeln für die Dateien an, die für eine Sicherung überprüft werden sollen (Abb. 6). Gibt man hier nichts an, werden alle Dateien als Sicherungskandidaten betrachtet. Die Möglichkeiten sind ausgesprochen vielfältig und reichen von Dateiname, Dateigröße und Änderungsdatum bis hin zu speziellen Dateieigenschaften. Dies erlaubt eine feine Steuerung. Bisher habe ich jedoch keine dieser Einstellungen benötigt.

Unter *Analyse* ( ) findet man einen zweiteiligen Datei-Browser. Selektiert man dort (oben) eine Datei, so zeigt die Anwendung unten deren Status auf der Quelle (links) und im Ziel (rechts) (Abb. 7). Man wird diese Funktion sehr selten benötigen, sie kann bei auftretenden Problemen für eine Analyse jedoch nützlich sein. Die Symbole in der Spalte *Status* signalisieren, ob ein Abgleich noch erforderlich ist.

Im Fenster zu *Archiv* ( ) erhält man eine Archiv-Ansicht (Abb. 8). Sie zeigt jene älteren Dateiversionen, die bei einem Sicherungslauf ins Archiv verschoben wurden, weil sie in der Quelle gelöscht wurden oder dort eine neuere Dateiversion verfügbar war. (Für die Archivierung solcher Dateien müssen aber bei früheren Läu-

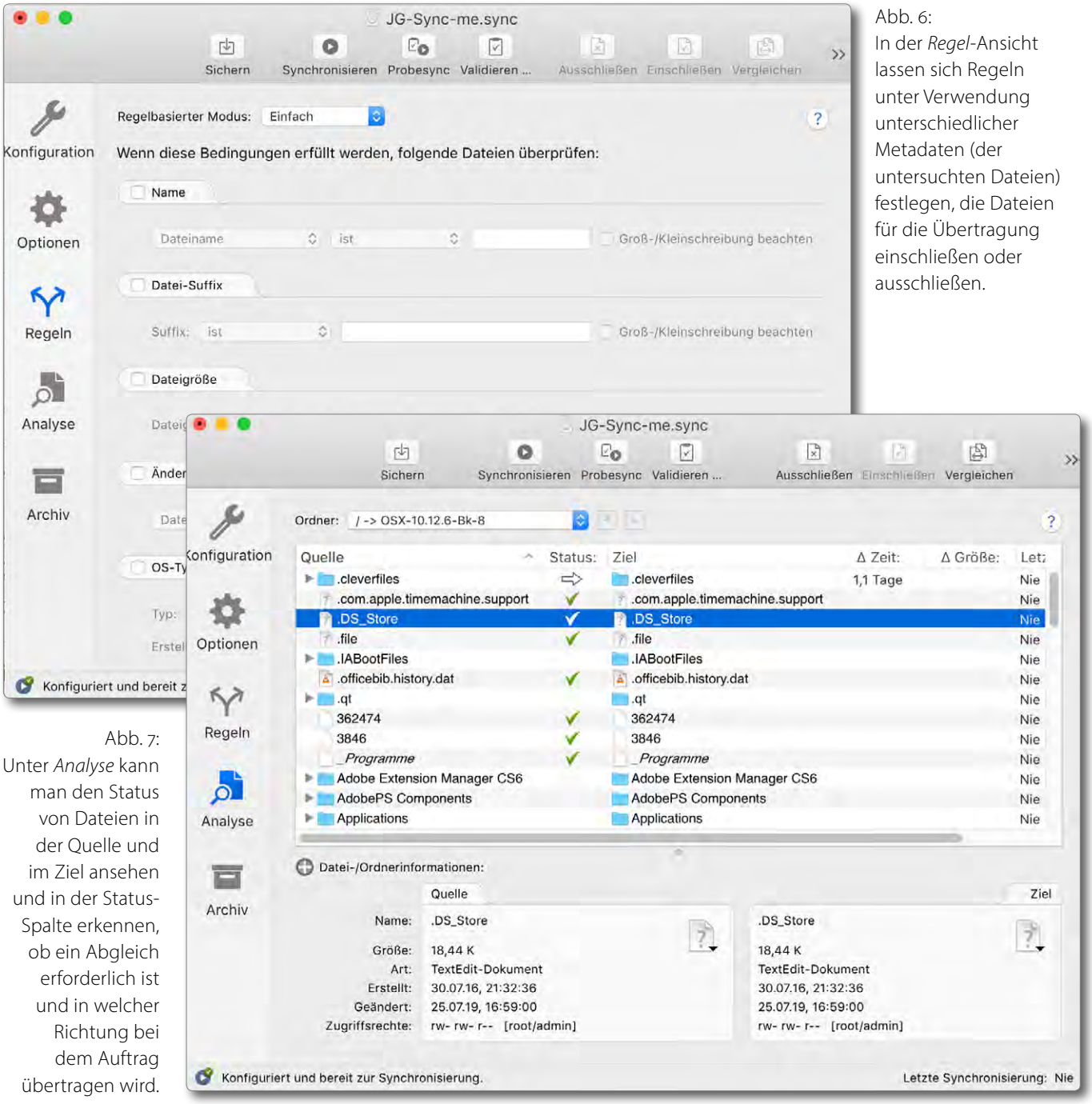


Abb. 6:
In der *Regel*-Ansicht lassen sich Regeln unter Verwendung unterschiedlicher Metadaten (der untersuchten Dateien) festlegen, die Dateien für die Übertragung einschließen oder ausschließen.

Abb. 7:
Unter *Analyse* kann man den Status von Dateien in der Quelle und im Ziel ansehen und in der Status-Spalte erkennen, ob ein Abgleich erforderlich ist und in welcher Richtung bei dem Auftrag übertragen wird.

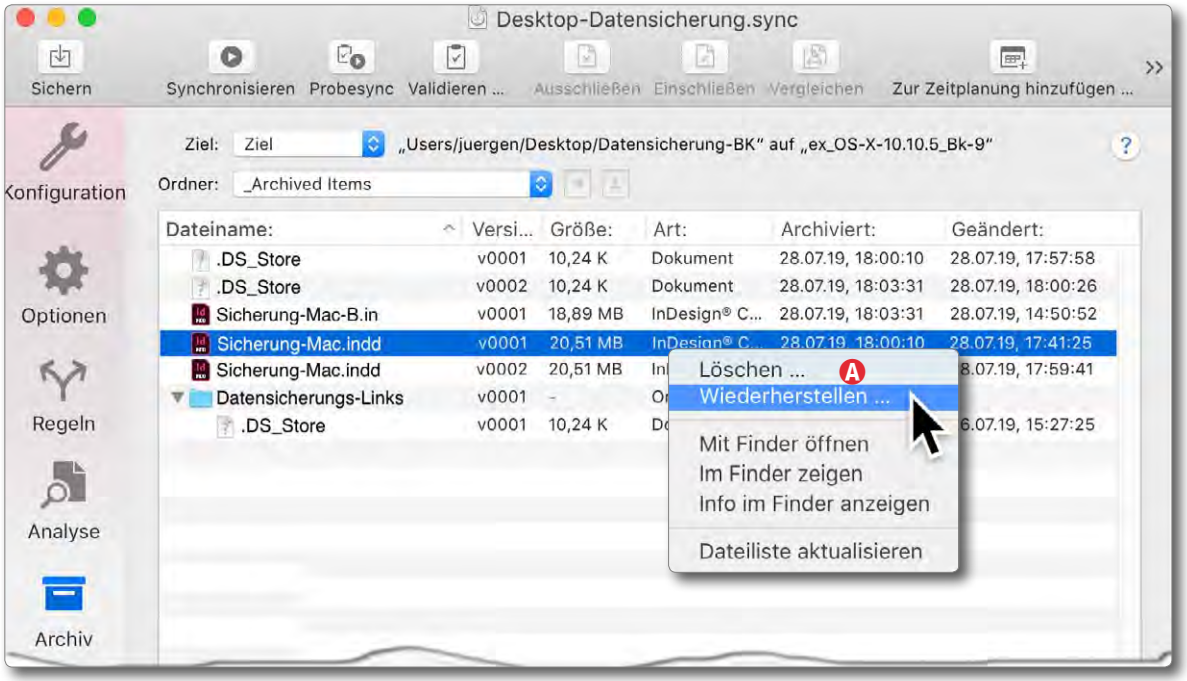


Abb. 8: Hier aus einem anderen Auftrag der Blick ins Archiv. Von der Datei *Sicherung-Mac.indd* liegen zwei Versionen im Archiv vor. Das Kontextmenü Ⓐ bietet Operationen mit den selektierten Dateien an.

Abb. 10: Statt über die Zeit kann man eine Sicherung auch Ereignis-gesteuert planen. Einige Ereignisse lassen sich über *Erweitern für zusätzliche Optionen* Ⓐ noch genauer festlegen.

fen entsprechende Optionen aktiviert sein.) Wählt man in diesem Fenster Dateien aus, so bietet das Kontextmenü (rechte Maustaste) einige Operationen (siehe Abb. 8 Ⓐ) – etwa das Wiederherstellen der selektierten Dateien.

Aufgaben-Planung

Möchte man einen Sicherungslauf nicht sofort, sondern Zeit- oder Ereignis-gesteuert ausführen (und dies regelmäßig), so selektiert man im Organizer einen Auftrag und klickt dort im Fuß auf das -Icon. Alternativ ruft man im Konfigurationsfenster (Abb. 2, eingeblendet eventuell rechts unter >>) die Funktion *Zur Zeitplanung hinzufügen* () auf. Das Fenster für die Zeitplanung hat wiederum drei Reiter, wobei man in den meisten Fällen mit dem Reiter *Einfaches Intervall* auskommt (Abb. 9).

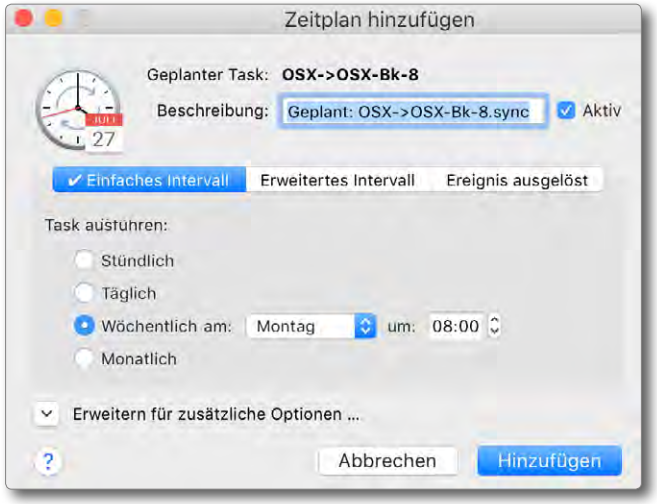


Abb. 9: Fenster für die (einfache) Zeitplanung für einen Auftrag

Für fortgeschrittene Anwender kann aber auch der Reiter *Ereignis ausgelöst* als alternativer Auftrags-Trigger interessant sein (Abb. 10).

Zurückspielen

ChronoSync erzeugt im Ziel kein Image, sondern normale Dateien. Damit lässt sich zunächst mit praktisch allen Programmen auf die gesicherten Dateien zugreifen. (Das betreffende Volume muss dazu natürlich aktiviert sein). Ebenso lässt sich mit dem *Finder* auf die

Dateien zugreifen; bei Bedarf kann man per *Kopieren* und *Einfügen* Dateien auf die Quelle oder an einen anderen Ort übertragen. *ChronoSync* bietet aber auch eine Übertragung vom Ziel (rechts) auf die Quelle (links) an, sofern die Quelle nicht das aktive Systemlaufwerk ist. Diese Funktion findet man im Konfigurationsfenster (Abb. 2 Ⓖ) unter dem *Modus*-Menü mit den Modi in Abbildung 11, die nach links übertragen. Man muss dabei die Art der Übertragung an die Situation anpassen. In diesem Punkt ist *ChronoSync* flexibler als die meisten anderen angeführten macOS-Backup-Lösungen.

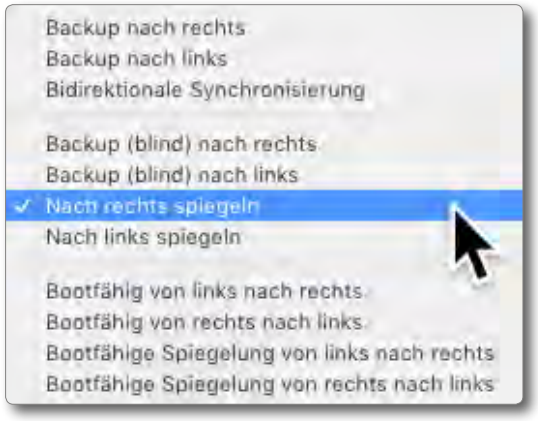


Abb. 11: Das *Modus*-Menü von *ChronoSync* erlaubt verschiedene Übertragungsrichtungen sowie unterschiedliche Arten.

Auch die in Abbildung 8 Ⓐ gezeigte Variante, aus dem Archiv Dateien wiederherzustellen, ist eine Möglichkeit des Zurückspielens.

Remote-Einstellungen

Da *ChronoSync* Sicherungen auch auf remote (andere) Systeme durchführen kann, benötigt man dafür eventuell dort eine Identifikation (einen Login-Namen) sowie ein Passwort. Diese Angaben lassen sich unter den *Voreinstellungen* im Reiter *Verbindungen* vornehmen.

Protokolle

ChronoSync erstellt recht ausführliche Protokolle zu den durchgeführten Sicherungsläufen. Diese lassen sich z. B. im Organizer-Fenster (bei selektiertem Auftrag) per Klick auf das -Icon im Fuß des Fensters abrufen oder alternativ über die Aktion *Protokoll anzeigen* (siehe Seite 58, Abb. 1 Ⓐ).

Zusammenfassung

ChronoSync ist eine ausgereifte Backup-Lösung für macOS. Die Anwendung lässt aus meiner Sicht keine Wünsche offen. Sie lässt sich mittels der Assistenten auch von einem relativ unerfahrenen Anwender nutzen und bietet einem erfahrenen Anwender eine extrem große Flexibilität. Das Handbuch ist ausgezeichnet. Es fehlt aber leider ein Index.

Es gibt wirklich zahlreiche nützliche Kleinigkeiten. So lässt sich beispielsweise die Anzahl der ›archivierten‹ Versionen einer Datei begrenzen oder angeben, ab welchem Alter eine solche Dateiversion automatisch gelöscht wird. Eine andere Option legt fest, dass jede kopierte Datei nochmals überprüft wird.

Der Lizenzpreis von *ChronoSync* mag etwas höher sein als etwa bei *Carbon Copy Cloner* oder *SuperDuper!*, dafür sind aber alle Updates kostenlos.

Hat man mehrere Macintosh-Systeme, so gibt es die Möglichkeit, unter Verwendung von *ChronoAgent* (den ich nicht ausprobiert habe) von einem System aus die Sicherung anderer Systeme anzustoßen und zu überwachen – wenn auch mit (moderaten) Zusatzkosten verbunden.

Ich habe hier mitnichten alle Details beschrieben. Dies würde den Umfang und den Zweck dieses E-Books sprengen. Dafür sollte man auf das recht gute Online-Handbuch (deutschsprachig) zurückgreifen. Man findet sogar einige Video-Tutorials. Diese sind aber englischsprachig.

Die inzwischen kostenlose Backup-Lösung *SmartBackup* [5] habe ich 2019 erst neu entdeckt. Die Anwendung, die man auf der Webseite von *Solesignal Ltd.* findet, ist ausgesprochen übersichtlich gestaltet, wie der Dialog in Abbildung 1 zeigt.

Die Oberfläche dieser schönen Anwendung ist deutsch, die Online-Hilfe aber englisch. Die Anwendung hat funktional sehr viel Ähnlichkeit mit *Carbon Copy Cloner* und *SuperDuper!*, d. h. sie ›synchronisiert‹ einzelne Dateien oder Ordner (mit den dort befindlichen Dateibäumen) oder ganze Volumes von der Quelle ins Ziel. (Ich beschreibe hier Version 4.2.1.)

Ungewohnt ist, dass man zunächst das Ziel angeben muss. Dazu zieht man aus dem *Finder* (oder vom Desktop) den betreffenden Ordner per Drag & Drop auf die Zielfläche Ⓐ. Statt das Ziel dort per Drag & Drop festzulegen, kann man auch auf das (kaum erkennbare) blaue +-Zeichen Ⓑ klicken und das Ziel dann im erscheinenden kleinen Datei-Browser auswählen. Das Ziel kann ein einzelner Ordner sein oder ein ganzes Volume. Die Anwendung zeigt dann an, wie viel freier Speicher noch auf dem Zieldatenträger vorhanden ist.

Erst jetzt lässt sich die Quelle (Datei, Ordner oder Volume) angeben – wieder per Drag & Drop in die Fläche für das Ziel Ⓒ oder durch einen Klick auf das +-Icon Ⓓ. Dabei lassen sich (bei Bedarf) mehrere Quellen angeben. Sie alle landen im Ziel(ordner).

Damit ist man im einfachsten Fall schon fertig und klickt auf *Starten*. Die Anwendung zeigt im Fenster an, was gerade ausgeführt wird. Die Sicherung erfolgt überraschend schnell. Im Fenster erscheint danach auch, wann die letzte Sicherung erfolgte (Abb. 2).

Abb. 1:
Startfenster von *SmartBackup*. Hier zieht man zunächst aus dem *Finder* per Drag & Drop den Zielordner oder das Zielvolume in die Zielfläche Ⓐ (rechts) und danach erst die Quelle in die Fläche für die Quelle links Ⓒ.

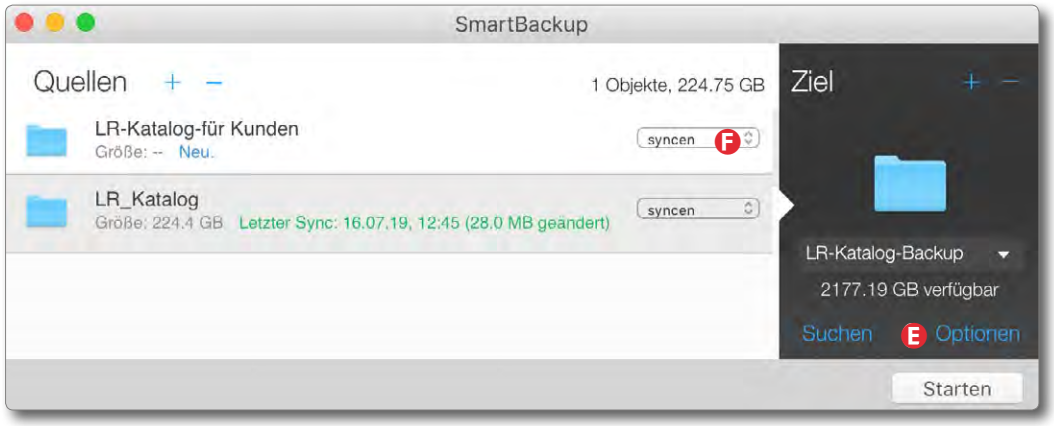


Abb. 2:
Sind das Ziel sowie die Quelle(n) festlegt – hier wurden zwei Quellordner gewählt–, so lassen sich unter *Optionen* Ⓔ Einstellungen für den Sicherungslauf vornehmen (Abb. 3 bis 5).

Sind Ziel und Quelle festgelegt, so erscheint rechts ein Knopf *Optionen* (Abb. 2 Ⓔ). Darüber lässt sich eine Reihe wichtiger Einstellungen für die Sicherungsläufe vornehmen (Abb. 3) – natürlich vor dem Lauf (oder zumindest vor dem nächsten Lauf). Die Einstellungen sind in drei Reiter untergliedert: *Archivieren*, *Erweitert* sowie *Automation*.

Im Reiter *Archivieren* (Abb. 3) legt man fest, was im Ziel mit Dateien erfolgen soll, die in der Quelle gelöscht

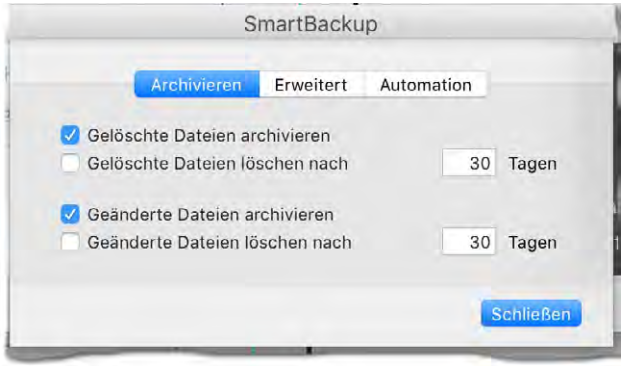


Abb. 3: Unter *Archivieren* wird definiert, was mit in der Quelle seit dem letzten Lauf gelöschten und geänderten Dateien geschehen soll.

oder geändert wurden. Beides kann man (separat) entweder löschen bzw. ersetzen lassen oder ›archivieren‹, d. h. im Ziel in einem Ordner ›*_removed*‹ (für *gelöscht*) bzw. ›*_changed*‹ (für *geändert*) ablegen. Dies erfolgt in nach dem Datum der Sicherungsläufe aufgegliederten Ordnern. Diese Dateien werden (optional) nach einer einstellbaren Anzahl von Tagen gelöscht.

Der Reiter *Erweitert* (Abb. 4) bietet eine Reihe von Optionen. Mit *Tags* sind die farblichen Dateimarkierungen gemeint, die man im *Finder* einem Objekt zuweisen kann. In der Regel kann man für eine schnellere Sicherung auf deren Übertragung verzichten. Die Anzahl der Kopier-Threads gibt an, wie viele parallel laufende Prozesse das Sichern/Kopieren vornehmen sollen. Zwei erweist sich als sinnvolle Voreinstellung. Bei Übertragungen über ein Netzwerk können mehr Threads sinnvoll sein.

Möchte man eine automatische, zeitgesteuerte Sicherung, so aktiviert man im Reiter *Automation* die Option *Aktiviert* (Abb. 5) und gibt an, ob täglich oder wöchentlich gesichert werden soll und um welche Zeit (bei wöchentlicher Sicherung auch an welchem Tag). Die Anwendung läuft dann verdeckt als Hintergrundprozess, erzeugt aber ein Protokoll (siehe Abb. 8). Kommt es bei einem solchen Lauf zu gravierenden Fehlern, wird im Vordergrund eine Fehlermeldung ausgegeben.

Was fehlt, ist die Möglichkeit, mehrere solcher Backup-Aufträge unter einem Namen anzulegen und dann über ein Menü abrufen zu können (wie z. B. in CCC und

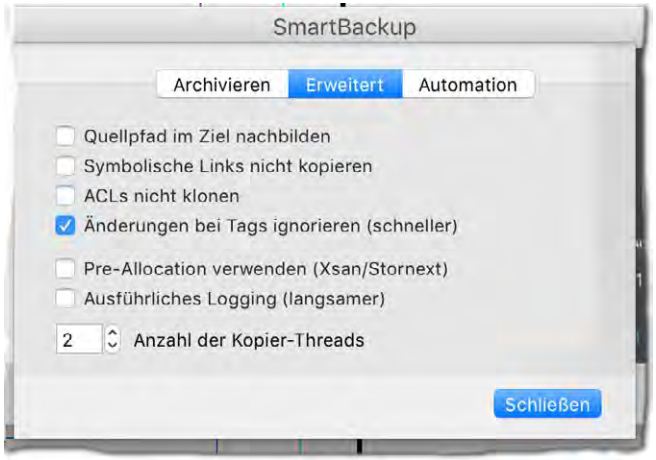


Abb. 4: Hier findet man zusätzliche Optionen für den Sicherungslauf.

Abb. 5: Hier lässt sich eine zeitgesteuerte Sicherung definieren. Sie läuft ohne Fenster im Hintergrund ab.

SuperDuper! möglich). *SmartBackup* merkt sich Sicherungsaufträge aber auf den jeweiligen Zielen in einer verdeckten Datei ›*.smartbackup.conf*‹. Wählt man ein Ziel, so lädt die Anwendung von dort den dorthin zuletzt ausgeführten Auftrag und zeigt ihn an. Dessen Einstellungen lassen sich danach bei Bedarf ändern. Die

Abb. 6: Um ganze Volumes sichern zu können oder Ordner mit speziellen Zugriffsrechten, muss man *SmartBackup* als *SuperUser* starten.

Anwendung kann nur einen solchen Auftrag – den zuletzt aufgesetzten – zeitgesteuert ausführen.

Möchte man ein ganzes Volume sichern, so sind dafür in den meisten Fällen Administratorrechte erforderlich (sicher aber beim Systemvolume). In diesem Fall führt man die Anwendung als SuperUser aus – über das *SmartBackup*-**Hauptmenü und dort über den Menü**punkt *Als SuperUser starten* (Abb. 6). Es wird dann nach dem Administrator-Passwort gefragt. Unten im Fenster wird dies danach mit *SuperUser* signalisiert.

Man kann, wie in Abbildung 2 gezeigt, mehrere Ordner(bäume) als Quellen angeben. Die dortigen Dateibäume werden als Unterordner des Zielordners angelegt. Bei einer erneuten Sicherung lassen sich dann aber einzelne Quellen über das kleine Menü (Abb. 2 Ⓕ) per *überspringen* für den nachfolgenden Lauf überspringen (Abb. 7).

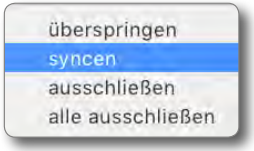


Abb. 7:
Über dieses Menü (siehe Abb. 2 Ⓕ) lassen sich Quellen von der Sicherung ausschließen.

Die Standardfunktion ist das Sichern (*syncen*). Möchte man innerhalb einer Quelle bestimmte Dateien oder Ordner ausschließen, so fügt man sie der Quelle als eigenen Eintrag hinzu und markiert sie per *ausschließen*. Damit fungiert der betreffende Eintrag als eine Art Filter, ist aber nicht ganz so flexibel wie ein Dateinamensmuster (etwa der Art ›*.tmp‹). *Alle ausschließen* überspringt denn nächsten zeitgesteuerten Sicherungslauf.

Zuweilen möchte man verdeckte Ordner (solche, deren Namen mit einem Punkt beginnen), nicht mit sichern. Um diese auszuschließen, klickt man in der Quelle auf das **+**-Zeichen und gibt, wenn der Browser erscheint, ⇧-⌘-. ein. Damit werden auch die verdeckten Dateien und Ordner angezeigt. (Ein zweites ⇧-⌘-. blendet sie wieder aus.) Nun kann man einen verdeckten Ordner auswählen und dann links im Aktionen-Menü (Abb. 7) *ausschließen* einstellen.

SmartBackup erzeugt bei jedem Lauf ein Protokoll, das man per ⌘-1 oder im Hauptmenü über Fenster ▸ Log-Fenster abrufen kann. Das Protokoll enthält eine Zusammenfassung der Vorgänge – auch die älterer Sicherungsläufe (siehe Abb. 8).

Unter macOS 10.14 (Mojave) mit seinen erhöhten Sicherheitsvorkehrungen sollte man *SmartBackup* zunächst manuell erweiterte Zugriffsrechte geben. Dies ist erforderlich, um bootbare Volumes zu erstellen. Die Vergabe geschieht in den *Systemeinstellungen* (z. B. im Dock) unter *Sicherheit* ( ). Dort öffnet man zunächst das Schloss (Administrator-Passwort dazu eingeben), wählt dann in der Liste links *Festplattenvollzugriff*, klickt rechts unter der Liste auf das **+**-Zeichen und wählt dann im erscheinenden Datei-Browser *SmartBackup* (im Ordner *Programme*), um es der Anwendungsliste hinzuzufügen (Abb. 9).

Zurückspielen von Dateien

Da *SmartBackup* wie beispielsweise *Carbon Copy Cloner* im Ziel normale Ordner und Dateien ablegt, lässt sich bei Bedarf auf diese mit den normalen Anwendungen zugreifen oder Dateien und Ordner mit dem *Finder* an eine andere oder die ursprüngliche Stelle kopieren. Bei einer größeren Anzahl wird man aber einen geänderten Sicherungsauftrag vom Ziel in die ursprüngliche Quelle aufsetzen. Dabei lassen sich einzelne Dateien oder Ordner von der Übertragung wie beschrieben ausschließen. Um von einem System-Klon Dateien oder das System auf das Systemlaufwerk zurückzuspielen, muss man zunächst

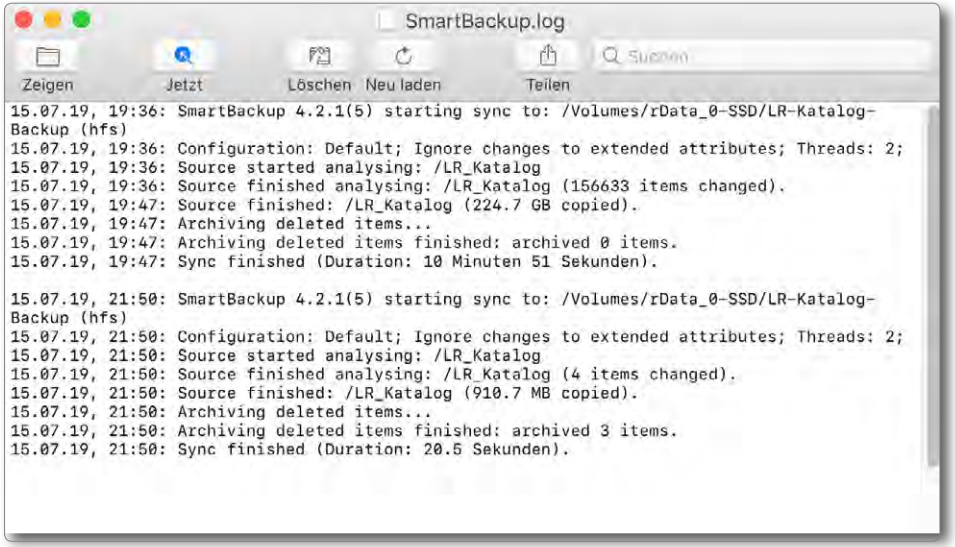


Abb. 8: Das Protokoll listet wesentliche Aktionen der letzten Sicherungsläufe auf.

Abb. 9: Man sollte unter macOS 10.14 *SmartBackup* den *Festplattenvollzugriff* gewähren.

ein anderes System booten und von diesem aus das Rückspielen anstoßen.

SmartBackup bietet auch eine Kommandoschnittstelle, so dass man die Anwendung über ein Skript steuern kann.

Die Anwendung kann unter Mojave auch mit APFS-Dateisystemen als Quelle und Ziel umgehen, kann bisher aber auf einem APFS-Volume noch kein bootbares System erstellen (wohl aber HFS+-Volumes). Dies soll allerdings in Arbeit sein.

Was ebenso fehlt, sind vor und nach dem Sicherungslauf auszuführende Aktionen. Es ist deshalb nicht möglich, mit einem *mount*-Kommando ein Volume vor dem Sicherungslauf explizit zu aktivieren oder nach einem Sicherungslauf den Zieldatenträger per *umount* zu deaktivieren oder das System automatisch herunterzufahren. Auch lassen sich bisher keine Sicherungsaufträge verketten bzw. zu einem größeren Auftrag zusammenfassen.

Resümee

SmartBackup hinterlässt einen guten Eindruck. Es kommt bisher funktional noch nicht ganz an *Carbon Copy Cloner* oder *SuperDuper!* heran, ist dafür aber kostenlos, sehr aufgeräumt und ausgesprochen schnell. Für manchen mag störend sein, dass zwar die Benutzeroberfläche (auf deutschen Systemen) deutsch ist, die Online-Hilfe aber englisch – ebenso das Protokoll (Abb. 8). Das Online-Handbuch selbst ist relativ kurz, beschreibt aber alle Funktionen ausreichend und verständlich.

Es gibt eine Reihe weiterer Anwendungen und Lösungen zur Datensicherung unter macOS. Da wäre beispielsweise das von Windows her bekannte *Acronis True Image*. (Die Version für macOS ist auf der Installations-CD der Windows-Version vorhanden, sie kostet aber eine Lizenz.) Gegenüber den zuvor vorgestellten Lösungen (*Carbon Copy Cloner* und *SuperDuper!*) sehe ich jedoch keinen Vorteil. Auch das zuvor beschriebene *SmartBackup* ist für viele private Einzelanwender eine brauchbare Lösung.

Möchte man ›nur‹ Dateien/Ordner synchronisieren, so kommt das kostenlose Programm *FreeFileSync* [4] in Frage (es ist für Windows ab Seite 100 beschrieben). Was ihm fehlt, ist eine zeit- oder ereignisgesteuerte Ausführung. Es ist auch nicht in der Lage, Systemdateien und die Dateien anderer Anwender zu sichern oder zurückzuspielen – der eingeschränkten Zugriffsrechte wegen.

Eine ähnliche Lösung stellt *GoodSync* [14] dar (auch für Windows verfügbar), von dem es zwar auch eine kostenlose Lösung gibt, die aber so eingeschränkt ist (maximal 100 Dateien pro Lauf, maximal 3 Auftragsdateien), dass man sie nicht empfehlen kann. *GoodSync Personal* (ohne diese Einschränkungen) kostet etwa 50 USD (für drei Rechner). Die Oberfläche ist etwas übersichtlicher als die von *FreeFileSync,* und *GoodSync* bietet sowohl eine Zeit- als auch eine Ereignissteuerung (Benutzeranmeldung/Abmeldung, Laufwerk anschließen, …). Die Benutzeroberfläche ist eine Mischung von Deutsch und Englisch; das Handbuch und die Online-Hilfe sind englisch.

Auch wenn das Spektrum an Lösungen unter macOS sehr viel kleiner als für Windows ist, gibt es doch noch einige weitere Alternativen. Als Beispiel sei *Get Back Pro* [10] erwähnt, eine sehr übersichtliche, relativ preiswerte Lösung, leider nur mit englischer Oberfläche. Als Funktionen werden Archivieren (Synchronisieren mit Versionierung nur in einer Richtung), Synchronisieren sowie das Klonen von Volumes angeboten. *EaseUS ToDo Backup* scheint unter macOS die gleiche Anwendung zu sein. Das kostenlose *SynKron* [11] hingegen ist auf die Synchronisation von Ordnern beschränkt, jedoch mit zahlreichen Konfigurationsmöglichkeiten.

Aus Gründen der Übersichtlichkeit verzichte ich hier darauf, weitere Beispiele zu nennen.

Daneben findet man Lösungen, bei denen die Dateien eines Macintosh von einem Server angestoßen auf einem Fileserver gesichert werden – unter Verwendung lokaler Backup-Clients. Die Firma *Feeam* [30] bietet etwa solche Lösungen (ebenso IBM). Diese sind aber nicht Thema dieses E-Books.

Setzt man *Adobe Lightroom CC* ein, so speichert Lightroom die Bilddateien in der Adobe Cloud (wo sie laut Adobe sicher sind). Dies hat den Vorteil, dass man von verschiedenen Systemen aus recht transparent darauf zugreifen kann. Aber die meisten dieser Cloud-Speicher werden bei einem größeren Bildbestand schnell teuer (siehe nebenstehende Tabelle).

Auch Apple bietet für Bilder, die mit *Apple Fotos* verwaltet werden, eine ähnliche Cloud-Lösung – ebenfalls mit 5 GB kostenlosen Speicher, aber bei großem Volumen mit deutlich steigenden Kosten. Weitere Cloud-basierte Lösungen gibt es von Microsoft, Western Digital, Google, Amazon und einigen mehr.

Tabelle 7: Beispiele zu den Kosten von Cloud-Speicher für Privatanwender (Stand: Mitte 2019)

Anbieter:	Preis pro Jahr:	Anmerkung
Adobe Creative Cloud	144 € / 1 TB	nur für Bilder/Adobe-Dateien
Apple iCloud	120 USD / 2 TB	5 GB für Mac-User frei
Google Drive	100 USD / 1 TB	15 GB frei je Anwender
OneDrive (Microsoft)	120 € / 5 TB	5 GB frei, 84 € für 1 TB
Amazon	100 USD je 1 TB 5 GB frei	zahlreiche weitere Modelle, unbegrenzter Fotospeicher für Prime-User
Carbonite	72 USD	1 Rechner, ohne Limit
Backblaze	60 USD	Ohne Speicherlimit
iDrive	75 USD / 2 TB	pro privatem Rechner
Dropbox (Microsoft)	119 USD / 2 TB	pro Nutzer

Für (private) Einzelrechner noch preiswerte und in der Handhabung relativ transparente Lösungen bieten die amerikanischen Firmen *Carbonite* [31], *iDrive* [32] und *Backblaze* [34]. (Von diesen Firmen gibt es auch kurze, kostenlose Test-Abonnements.) Außerdem gibt es mehrere weitere Anbieter.

Die Cloud-Lösungen – sei es unter Windows oder unter macOS (oder Linux) – betrachte ich derzeit nicht als allgemeine Lösungen, die auch Systemdateien abdecken können (mit Ausnahmen). Eine wirkliche Limitierung ist für die meisten Fotografen mit einer ›normalen‹ Internetanbindung in Deutschland bisher die Übertragungsgeschwindigkeit im Internet bei größeren Volumina. Die Preise werden hier aber weiter fallen und die Übertragungsraten (hoffentlich) steigen.

Tabelle 8: Beispiele für Backup-Lösungen unter macOS

Anwendung	Time Machine	Carbon Copy Cloner	SuperDuper!	ChronoSync	SmartBackup	FreeFileSync
Hersteller	Apple https://www.apple.com	Bomich https://bombich.com/de	Shirt Pocket https://shirt-pocket.com	Econ Technologies https://econtechnologies.com	Solesignal Ltd. https://solesignal.com/smartbackup4/	Open Source https://freefilesync.org
Preis ca.	kostenlos (Teil von macOS)	37 € (für 5 Systeme)	41 € (für 5 Systeme)	60 USD 25 USD (CS Express)	kostenlos	kostenlos
Sicherungsarten:						
– System / bootbar	**+** / per Restore-Funktion	**+ / +**	**+**	**+**	**+**	**– / –**
– Partition/Volume	(+) (alle O. in 1 Objekt)	**+**	**+**	**+**	**+**	**(+)**[1]
– Ordner bzw. Dateibäume	**(+)**	**–**	**–**	**+**	**+**	**+**
– Versionierung	**–**	**+**	**+**	**+**	**+**	**+**
– Realzeitsynchronisiation	**–**	**–**	**–**	**–**	**–**	**+**
– auf Remote-System	**(+)** (nicht empfohlen)	**+**	**+**	**+**	**–**	**–**
– auf Cloud-Speicher	**–**	**–**	**–**	**+**	**–**	**–**
Spezielle Funktionen 1:						
– Skriptsteuerung	**–**	**+**	**+**	**+**	**+**	**+**
– Vorher-/Nachher-Aktion	**–**	**+**	**+**	**+**	**+**	**+**
– Filterfunktionen	**+**	**+**	**+**	**+**	**+**	**+**
– Verschlüsselung	**+**	**–**	**–**	**–**	**–**	**–**
– Komprimierung	**+**	**–**	**–**	**–**	**–**	**–**
Spezielle Funktionen 2:						
– Zeit-gesteuert	**+** (nur stündlich)	**+**	**+**	**+**	**+**	**(+)**
– Ereignis-gesteuert	**–**	**+**	**+**	**+**	**+**	**+**
– Remote-gesteuert	**–**	**–**	**–**	**+** (per *ChronoAgent*)	**–**	**–**
– Server-Lösung	**–**	**–**	**–**	**+** (per *ChronoAgent*)	**–**	**–**
Rückspielen	Time Machine	CCC ⟷, Finder, Direktzugriff auf Dateien/Ordner	SD ⟷, Finder, Direktzugriff auf Dateien/Ordner	CS (interaktiv), CS ⟷, Finder, Direktzugriff auf Dateien	SmartBackup ⟷, Finder/Direktzugriff auf Dateien/Ordner	FreeFileSync ⟷, Finder/Direktzugriff auf Dateien/Ordner
Benutzeroberfläche	DE, EN, FR, …	DE, EN, FR, …		DE, EN, FR, …	DE, EN, FR, …	DE, EN, FR, …
Handbuch/Online-Hilfe	DE, EN, FR, …	(DE), EN			EN	EN
Anmerkungen	Zeitsteuerung erweiterbar durch kostenlosen *TimeMachine Editor*	Sehr guter Support	Eingeschränkte Testversion ohne Zeitlimit	Kostenloses Update lebenslang; Backup für iOS/Android per *InterConneX*	Habe ich noch nicht ausführlich gestestet.	Auch für Windows und Linux verfügbar. (1) bei Volumes eingeschränkte Zugriffsrechte

Disk-Image – Dateisystem in einer Datei (macOS)

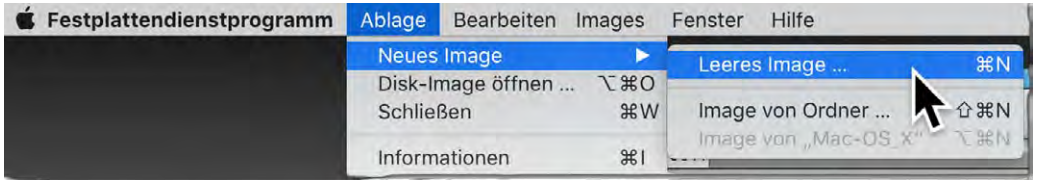


Abb. 10:
Im *Festplattendienstprogranm* lässt sich ein Dateisystem/ Volume in einer Datei neu anlegen.

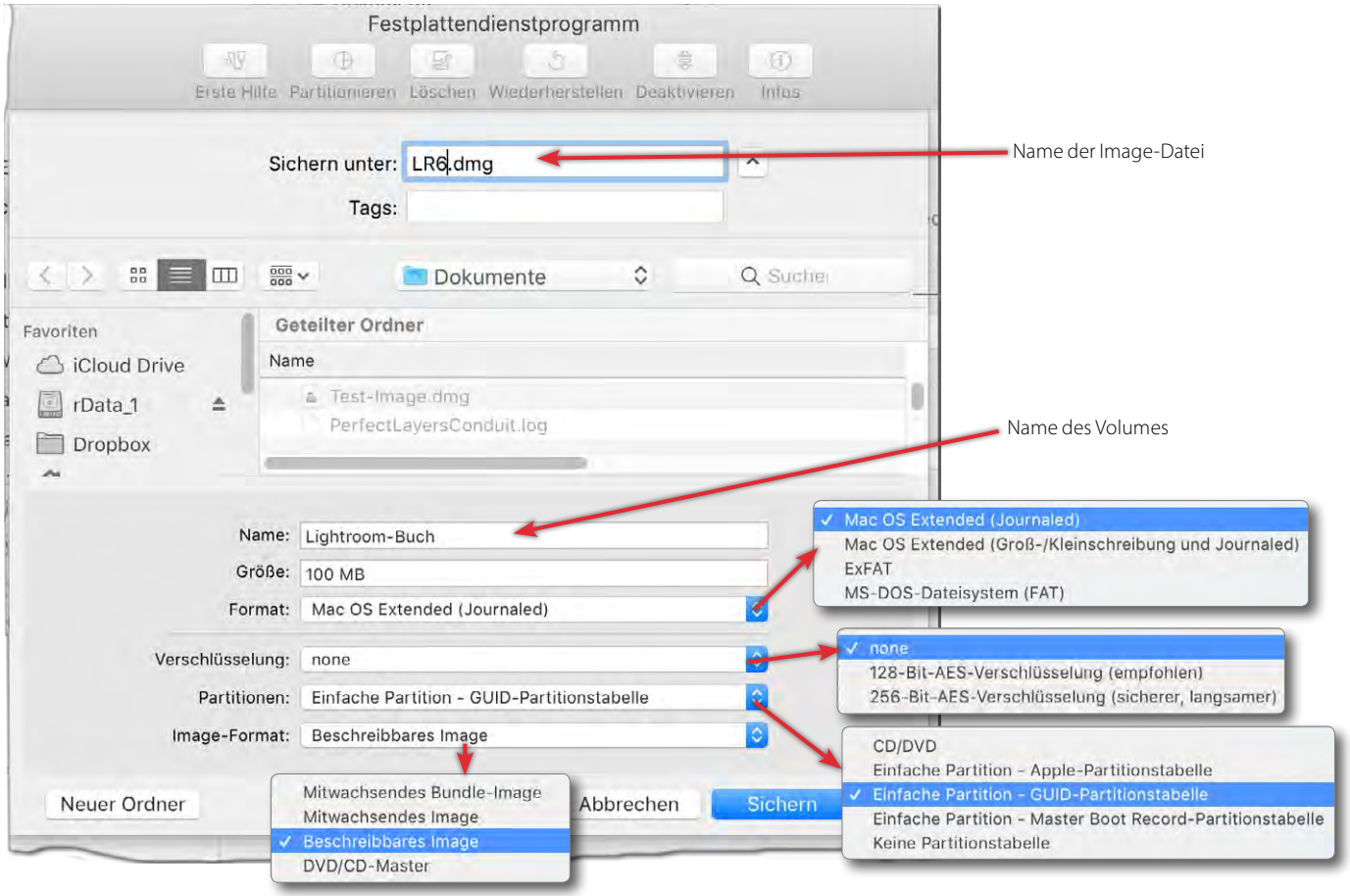


Abb. 11: Ein neues (zunächst leeres) Image legt man im Festplattendienstprogramm über die oben gezeigte Menüfolge an. macOS bietet dazu zahlreiche Details zur Art des Images bzw. des darin angelegten Dateisystems, zur Verschlüsselung, zur Partitionstabelle sowie zum Image-Format.

Apple erlaubt unter macOS ein ganzes Dateisystem in eine Datei zu verpacken. Diese Datei wird als *Image* bezeichnet. Ein solches Image ist zuweilen recht praktisch, lässt sich so doch ein (zumeist kleineres) Dateisystem wie eine einfache Datei kopieren, sichern oder versenden. Um dann wirklich auf den Inhalt des Dateisystems zugreifen zu können, muss man das Image aktivieren bzw. ein *Mount* darauf ausführen. Unter macOS reicht dafür in der Regel ein Doppelklick im Finder auf eine solche Image-Datei. Auch im *Festplattendienstprogramm* lässt sich eine solche Image-Datei über die Menüfolge Ablage ▸Disk-Image öffnen aktivieren. Neue Betriebssysteme werden in der Regel als eine solche Image-Datei verteilt (etwa aus Apples *App Store* heruntergeladen).

Möchte man selbst ein solches Image-Dateisystem anlegen, so nutzt man dazu wieder das *Festplattendienstprogramm*. Dort findet man im Hauptmenü unter Ablage die Funktion Neues Image in den drei Varianten Leeres Image, Image von Ordner sowie Image von „…" (Abb. 10). In Abbildung 11 sieht man die zahlreichen möglichen Einstellungen dazu.

Ist das Image angelegt, aktiviert das *Festplattendienstprogramm* das enthaltene Dateisystem automatisch und zeigt es im Finder an. Bei einem beschreibbaren (zunächst leeren Image) kann man nun darin Dateien und Ordner anlegen oder sie dorthin kopieren. Möchte man das Image wieder zur ›normalen Datei‹ machen und deaktivieren, selektiert man im *Finder* das betreffende Volume und wirft es über das Kontextmenü des *Finders* aus.

Ebenfalls aus dem *Festplattendienstprogramm* lässt sich unter dem Hauptmenü Images (Abb. 12) eine Reihe von Operationen auf eine solche Image-Datei ausführen. So kann man dem Image eine Prüfsumme

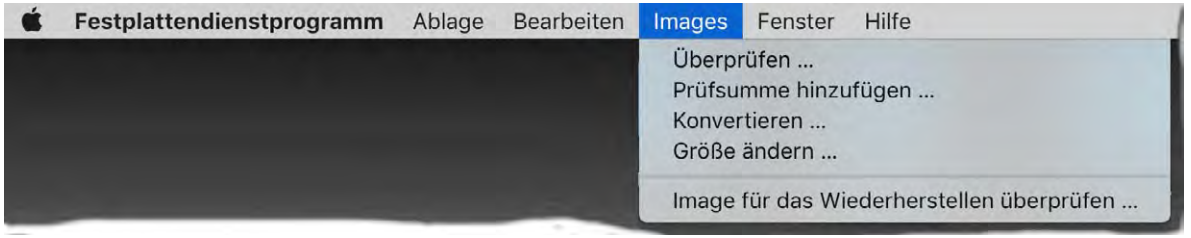


Abb. 12: Das *Festplattendienstprogramm* bietet eine Reihe von Operationen zu einem Image an.

hinzufügen. Anschließend lässt sich mit der Funktion Überprüfen feststellen, ob sich an dem Image etwas geändert hat – etwa durch einen Übertragungsfehler oder durch Manipulation. Ebenso lässt sich die Größe ändern oder das Dateiformat in ein anderes Format konvertieren oder ein bisher unverschlüsseltes Image verschlüsseln oder komprimieren.

Beim Konvertieren wird effektiv der Image-Inhalt in ein neues Image mit dem geänderten Format kopiert. Das ursprüngliche Image bleibt dabei erhalten.

Ein Dateisystem-Image hat die Endung ›.dmg‹ (für *Disk Image*).

Ordnerinhalte in Form eines ›Images‹ verschlüsseln

Das *Festplattendienstprogramm* erlaubt auch ein Image anzulegen, in dem anschließend sowohl ein Ordner selbst als auch die darin liegenden Dateien verschlüsselt liegen.

Der ›Ordner‹ wird dabei wie ein verschlüsselter virtuelles Volume behandelt, so als handle es sich um einen Datenträger. Hat man dieses Volume nach der Eingabe des Passwortes aktiviert, erscheint es als Volume und man kann darauf ganz normal zugreifen. Der Ablauf für die Erstellung:

1. Man ruft das *Festplattendienstprogramm* auf. Dort legt man über Ablage ▸ Neues Image ▸ Leeres Image (oder schneller per ⌘-N) ein neues (Platten-)Image an.

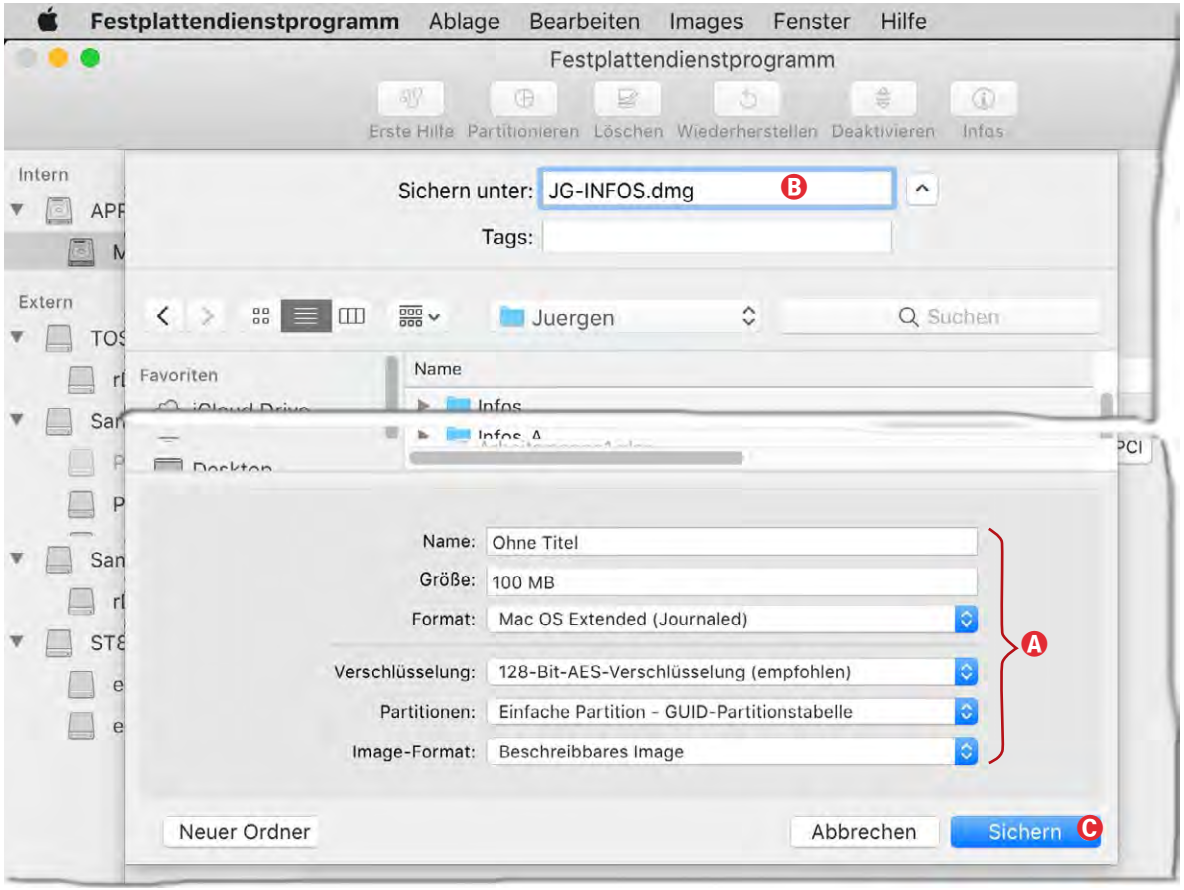


Abb. 13: Mit dem *Festplattendienstprogramm* kann man eine Art virtuellen Datenträger – ein Image – in einer Datei anlegen. Wählt man unter *Verschlüsselung* eine Verschlüsselungsart, so wird der Inhalt des ›Datenträgers‹ verschlüsselt.

2. Dort gibt man im unteren Bereich Ⓐ
   - dem Volume einen Namen,
   - legt die *Größe* fest (das *Festplattendienstprogramm* wird beim späteren Anlegen die gesamte angegebene Größe reservieren),
   - wählt ein (Dateisystem-)*Format* (empfohlen wie gezeigt),
   - eine Verschlüsselung (die 256-Bit-Schlüssel-Variante erfordert etwas mehr Rechenaufwand, ist aber sicherer).

3. Im erscheinenden Dialog gibt man ein frei wählbares Passwort ein (das muss ein zweites Mal wiederholt werden). Klickt man im Dialog dazu auf das ?-Icon, zeigt die Anwendung in einem weiteren Fenster die Stärke des gewählten Passwortes und schlägt selbst ein Passwort vor, das man aber nicht nutzen muss.

4. Jetzt legt man die Partitionsart fest (in der Regel wie in Abb. 13 gezeigt) und legt über das *Image-Format* fest, dass es ein *Beschreibbares Image* sein soll …

5. … navigiert unter Ⓑ zum vorgesehenen Ablageort und gibt dem virtuellen Datenträger, der in Wirklichkeit in der Datei (auf einem anderen Volume) liegt, einen Datenträgernamen.

6. Schließlich klickt man auf *Sichern* (Abb. 13 Ⓒ).

Das Anlegen des Images kann eine Weile dauern. Ist es angelegt, so wird es von macOS automatisch aktiviert und im Finder angezeigt.

Man kann nun dort ganz normal Dateien und Ordner (oder ganze Dateibäume) anlegen oder kopieren – bis zur Grenze des verfügbaren Platzes im Image. Für Anwendungen, die darauf arbeiten, ist der Zugriff transparent.

Benötigt man den Zugriff auf den Datenträger (das Image) nicht mehr, selektiert man es und wirft es über das Kontextmenü (unter der rechten Maustaste) aus. Es verschwindet damit vom Desktop und im Finder. Fährt man das System herunter, erfolgt das Auswerfen automatisch. Nach einem erneuten Systemstart wird das so erstellte Image **nicht** wieder automatisch aktiviert.

Möchte man auf die Dateien erneut zugreifen, so navigiert man mit dem Finder zum entsprechenden Image und führt einen Doppelklick darauf aus oder öffnet es über die *Öffnen*-Funktion des Finders.

macOS verlangt nun nach dem Passwort (Abb. 14), öffnet damit das Image und zeigt es gleich im Finder an. Hat man vor der Eingabe noch die Option *Passwort in Schlüsselbund sichern aktiviert*, merkt sich das System das Passwort im Schlüsselring des Anwenders, so dass das Image beim nächsten explizit angestoßenen *Öffnen* sich das Passwort automatisch von dort holt und nicht nachfragen muss.

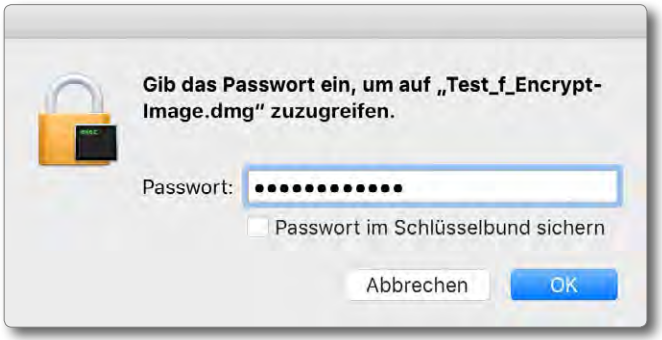


Abb. 14: Beim Öffnen eines verschlüsselten Images wird nach dem Passwort gefragt.

Die Image-Datei kann man natürlich kopieren oder versenden und auch auf einem anderen Mac öffnen, braucht dort aber wieder das richtige Passwort.

Verschlüsseltes Image von einem Ordner

Statt wie beschrieben ein neues Image anzulegen, kann man auch eine bereits existierenden Ordner in ein solches Image legen.

Dazu nutzt man wieder das Festplattendienstprogramm, öffnet diese Mal aber über Ablage ▸ Neues Image ▸ Image von Ordner (oder per ⇧-⌘-N) einen bereits vorhandenen Ordner (in dem die zu schützenden Dateien bereits liegen). Man navigiert im Browser-Fenster der Anwendung zum Ordner, selektiert ihn und klickt auf *Öffnen*.

Im neuen Fenster gibt man dem neu zu erstellenden Image einen Namen (als Endung wird automatisch ›.dmg für *Disk Image* angehängt). Unten im Fenster legt man unter Verschlüsselung fest, wie verschlüsselt werden soll (gar nicht, mit 128-Bit- oder mit 256-Bit-AES-Verschlüsselung) sowie ob zusätzlich komprimiert werden soll.

Ganzes Volume verschlüsseln (macOS)

Nun klickt man auf den Knopf *Sichern*, um den ganzen Vorgang anzustoßen.

Die Anwendung führt die Abläufe nun aus und legt das Ergebnis fertig ab. Das Original bleibt dabei vorhanden und sollte nach der Operation gelöscht werden, sofern die unverschlüsselten Daten darin auch lokal vertraulich bleiben sollen.

Die Objekte im erzeugten Image sind hier nach dem erneuten Öffnen des Images schreibgeschützt, und es können keine neue Dateien hinzugefügt werden. Das Image lässt sich aber als Ganzes löschen.

Lagert man ein Backup außer Haus oder lokal auf einem separaten Datenträger, so möchte man dessen Inhalt eventuell verschlüsseln, um Fremden (etwa bei Diebstahl) keinen Einblick auf die gesicherten Daten zu geben. Viele der hier für macOS beschriebenen Backup-Lösungen können das Backup jedoch nicht selbst verschlüsseln. Diese Aufgabe kann man aber macOS überlassen, indem man das Volume verschlüsselt, auf das man sichert. Dazu wählt man beim Anlegen des Volumes ein verschlüsseltes Dateisystemformat (siehe Abb. 15). Die verschlüsselten Varianten werden jedoch nur angeboten, wenn man für die Partitionstabelle das Format *GUID-Partitionstabelle* gewählt hat.

Unter macOS 10.4 (alias Mojave) ist *verschlüsselt* der Standard für SSD-Volumes (korrekt: für Volumes auf SSD-Datenträgern). Dabei wird zumindest bei von Apple stammenden SSDs die Verschlüsselungsfunktion des SSD-Controllers genutzt, so dass durch die Verschlüsselung keine zusätzliche CPU-Last entstehet.

Wird das Systemvolume verschlüsselt, so wird für das Volume das Administrator-Passwort als Passwort gewählt. Das Volume wird beim Start des Systems entsperrt bzw. korrekt: beim Login. Wird das Volume an einem anderen Rechner angeschlossen, muss dort für den Zugriff das Passwort explizit eingegeben werden (es sei denn, man hat dort bereits das Passwort zum Volume im Apple-Schlüsselbund hinterlegt).

Möchte man bei Backup-Lösungen, die selbst keine Verschlüsselung anbieten – etwa *Carbon Copy Cloner*

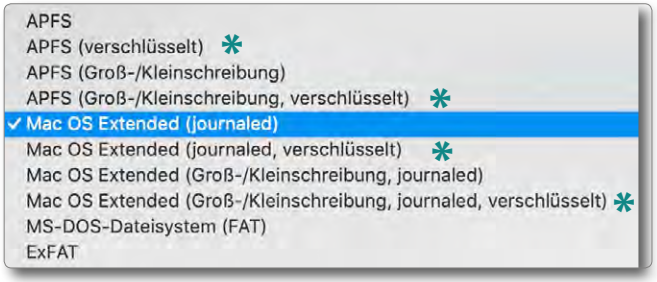


Abb. 15: Ab macOS 10.14 (Mojave) werden die vier mit ✻ markierten verschlüsselten Dateisystemvarianten angeboten. In früheren Systemen entfallen die beiden APFS-Versionen.

oder *SuperDuper!* – das Backup verschlüsselt anlegen, so wählt man als Zielvolume einfach ein Volume mit einem verschlüsselten Dateisystem.

Die Verschlüsselung eines Volumes hat natürlich auch den Vorteil, dass bei einem Rechnerdiebstahl der Volume-Inhalt auch dann nicht ausgelesen werden kann, wenn der Dieb den Datenträger ausbaut und an einem anderen Rechner mit Administratorrechten versucht, die Daten auszulesen. Dies gilt natürlich nur, solange er nicht an das Passwort zum Volume gelangt.

Fällt eine Festplatte aus, so kann dies viele Gründe haben. So kann der Motor nicht mehr starten oder der Controller defekt sein oder es kann wegen eines sogenannten *Head Crashs* sein, dass einzelne oder viele Blöcke nicht mehr lesbar sind.

Bei extern angeschlossenen Laufwerken sollte man aber zunächst die Kabel zum Laufwerk überprüfen und probeweise einmal austauschen.

Datenträger und Datensicherung unter Windows 10

Windows 10 ist heute die beste Wahl für ein Windows-System für Fotografen – sei es die Standard- oder die Pro-Version. Ein Umstieg von Windows 7 auf Windows 10 ist mittelfristig kaum vermeidbar. Ich beschränke mich hier deshalb auf die Beschreibung der Anwendungen und Funktionen unter Windows 10, wobei der größte Teil des Gesagten ebenso für Windows 7 und Windows 8 zutrifft.

Gegenüber macOS ergeben sich eine ganze Reihe von Unterschieden. Dies betrifft sowohl die Standard-Dateisystemformate als auch die meisten Anwendungen und Sicherungsschemata. Obwohl Windows bei Dateisystemen verschiedene Formate unterstützt (z. B. FAT12, FAT16, FAT32, ExFAT, NTFS), ist NTFS das Standardformat sowohl für die Systemplatte als auch für die zusätzlichen normalen weiteren Datenlaufwerke (Partitionen/Volumes). Die neueren Server-Versionen von Windows bieten daneben noch das hier nicht weiter erwähnte ReFS (*Resilient File System*), welches moderner und nochmals robuster als NTFS ist und auf Server und sehr große Dateisysteme abzielt. Ein einzelnes ›Dateisystem‹ kann dabei mehrere physikalische Laufwerke überspannen. Es erlaubt Dateigrößen bis zu 16 Exabyte und Dateisystemgrößen von (eher theoretischen) 4 ZB (Zetabyte, dies entspricht ca. 4.096 Exabyte).

Die mit Windows 10 mitgelieferten Backup-Lösungen – *Dateiversionsverlauf* und ›*Sicherung und Wiederherstellung (Windows 7)*‹ – sind leider unbefriedigend dokumentiert, eingeschränkt in Funktion und Konfiguration und etwas versteckt und in den Details recht unübersichtlich. Man findet deshalb wirklich zahlreiche Alternativen, was den Markt aber verwirrend und den Vergleich etwas schwierig gestaltet.

Dateiversionsverlauf dient primär dazu, die Standard-Benutzerverzeichnisse auf der Systemplatte zu sichern (siehe die Beschreibung auf Seite 89), während *Sichern und Wiederherstellung (Windows 7)* sowohl das System selbst sichern kann als auch Benutzerdaten. *Sichern und Wiederherstellung (Windows 7)* ist immer noch Teil von Windows 10 und funktioniert dort problemlos, auch wenn Microsoft die Weiterentwicklung dafür offiziell eingestellt hat.

Eine Art Sicherungsmechanismus sind Windows' Wiederaufsetzpunkte (beschränkt auf das System). Dazu protokolliert Windows verdeckt Änderungen, die bei System-Updates sowie bei der Installation von Treibern und Anwendungen vorgenommen werden, und erstellt zuvor eine Volume-Schattenkopie. Dies erlaubt bei neu auftretenden Problemen das System auf einen Stand vor der Update-Operation zurückzusetzen. Auf den Umgang mit diesen Wiederaufsetzpunkten, etwas verwirrend auch als *Computerschutz* bezeichnet, geht die Beschreibung ab Seite 113 ein.

Eine Hässlichkeit besteht unter Windows darin, dass sich das System im laufenden Betrieb nicht ohne Weiteres sichern bzw. klonen lässt. Dies liegt unter anderem an den zahlreichen offenen (geöffneten) Dateien, die dabei für den Zugriff anderer Anwendungen teilweise blockiert sind. Einige Anwendungen umgehen das Problem, indem sie vor der Sicherung eine Schattenkopie (Snapshot) des Systemvolumes anlegen und dann diese Snapshot-Daten sichern, während das System in neuen Datenblöcken weiterarbeiten kann.

Das allgemeine Sicherungskonzept unter Windows geht deshalb in den meisten Fällen von einer Aufteilung zwischen (Betriebs-)Systemkomponenten und Anwenderdaten aus. Hier trifft man immer wieder auf die Aussage, dass es reicht, die Anwenderdaten zu sichern, da sich das Betriebssystem und die Anwendungen einfach erneut installieren lassen. Ich betrachte diese Aussage als veraltet und als Unsinn. Ein komplettes System neu aufzusetzen ist relativ zeitaufwändig – insbesondere dann, wenn man zahlreiche lizenzpflichtige Anwendungen installiert hat, etwa MS Office, Adobe Lightroom, Teile der Adobe Application Suite, Capture One oder andere spezielle Anwendungen. Auch Fonts (Schriften) und Farbprofile gehören dazu. Eine vollständige Neuinstallation setzt auch entsprechende Datenträger mit dem Betriebssystem und den Anwendungen voraus oder alternativ einen schnellen Internet-Zugang sowie unter Umständen das nachträgliche Einspielen mehrerer Updates.

Aus meiner Sicht empfiehlt es sich deshalb, einen möglichst aktuellen Klon des Systems zu haben – in der Regel mit dem Inhalt des Volumes ›C\‹: sowie eventuell der speziellen Partitionen für ein Windows-Recovery (Wiederherstellen) und für eine Windows-Reparatur.

Entsprechend der oben erwähnten Teilung der Daten in Betriebssystem (sowie installierten Anwendungen) und Benutzer- und Anwendungsdaten, die prinzipiell nicht falsch ist und auch in diesem E-Book empfohlen wird, muss man unter Windows zwei Gruppen von Backup-Lösungen unterschieden: solche, die einen System-Klon erstellen, und solche, die nur die Anwenderdaten sichern (oder synchronisieren oder spiegeln). Einige Backup-Lösungen können beides.

Bei den meisten System-Klon-Lösungen besteht das Konzept darin, das System (korrekt: das Systemvolume) in einem besonderen Format zu sichern und es später bei Bedarf aus dieser Sicherung auf das ursprüngliche oder ein neues Laufwerk zurückzuspielen. Da der Klon in den meisten Fällen nicht direkt bootbar ist, erstellt man für den Fall, dass das System-Volume selbst kein operables System mehr enthält, eine Art bootbares Minimalsystem (oft auf einer CD/DVD oder einem USB-Stick), das man dann bootet und von dem aus man das Zurückspielen ausführt, um danach dieses restaurierte System zu booten. (Im Prinzip geht Time Machine unter macOS ähnlich vor, dort gibt es aber elegantere Lösungen.)

Unter Windows besteht dieses bootbare Minimalsystem zumeist aus einem *Windows PE* (oder *WinPE, Windows Preinstallation Environment*), eventuell ergänzt um zusätzliche Werkzeuge. Die *WinPE*-Partition benötigt etwa 200 MB (etwas größer ist besser). Mit den Werkzeugen dieser Minisysteme lassen sich bei Bedarf Reparaturarbeiten am eigentlichen Boot-System durchführen, Laufwerke partitionieren, ein neues System installieren oder ein System-Backup zurückspielen. So erlaubt beispielsweise *Acronis True Image* (siehe Seite 94), eine Boot-CD oder einen USB-Boot-Stick (mit Windows PE darauf) zu erstellen, der auch eine vereinfachte Version von *True Image* enthält und das Wiedereinspielen eines Backups ermöglicht. Einige Backup-Lösungen verwenden statt *WinPE* ein kleines Linux-System.

Meine Meinung dazu: Elegant geht anders. Diese Kritik gilt aber nicht den Windows-Backup-Programmen, sondern dem nun wirklich veralteten Boot-Verfahren von Windows. Wir zahlen hier den Preis für eine weitreichende Rückwärtskompatibilität. Auch müsste man dem aktuellen UEFI-System etwas mehr Speicher und etwas mehr ›Intelligenz‹ mitgeben. Dass es auch anders geht, zeigen macOS, Linux und viele andere Systeme.

Eine recht brauchbare Lösung zum Klonen des Betriebssystems auf ein Backup-Laufwerk lässt sich mit der *Free*-Version von *EaseUS Partition Master* erzielen (siehe Seite 120). Nach dem Einstellen von Quell- und Ziellaufwerk muss das System neu gestartet werden und aktiviert dabei einen speziellen, minimalen Windows-Modus. Dieser klont dann das System und kann dabei offensichtlich problemlos auf die Dateien des Startlaufwerks zugreifen, da dort zu diesem Zeitpunkt keine Dateien offen oder gesperrt sind. Nach der Fertigstellung wird wieder das normale System gestartet (gebootet). Eine ähnliche Funktion bietet *MiniTool Partition Wizard*, beschrieben auf Seite 118.

VSS – Volume Shadow Copy Service (nicht für Laien)
Windows bietet bereits seit Version 7 für NTFS-Volumes die Erstellung von Snapshots (Schattenkopien) an. Dabei wird das aktuelle Dateisystem praktisch eingefroren (nach einer Vorbereitung, bei der offene Dateien zuerst geschlossen und kopiert werden). Alle weiteren Schreiboperationen erfolgen (auf Blockebene) danach in einem neuen Datenbereich innerhalb des Volumes. Die Implementierung wurde seither weiterentwickelt, und die Funktion steht ebenso für das ReFS-System zur Verfügung.

Die eigentliche Durchführung wird von einem Systemdienst erbracht, dem VSS (*Virtual Shadow Copy Service*). Anwendungen können diese Funktion in Anspruch nehmen – etwa eine Backup-Anwendung, z. B. um Systemdateien im laufenden Betrieb zu sichern, also auch Dateien/Objekte, die gerade geöffnet sind. Dabei müssen auch andere gerade aktive Prozesse mitspielen, etwa Datenbanken. Die Schattenkopien kann die Anwendung dabei von einzelnen Dateien oder vom ganzen Volume erstellen lassen. Das Ganze ist ein komplexer Prozess und beeinflusst auch (temporär) die Performance des Systems. Eine Windows-Funktion, die solche Schattenkopien verwendet, ist das Setzen von Wiederherstellungspunkten (siehe Seite 113). Aber auch einige Backup-Lösungen nutzen diese Funktion. Da sie aber komplex, kaum rückwärtskompatibel und nur auf NTFS- und ReFS-Volumes möglich ist, sind es wenige. Für weitere Informationen zu Windows VSS sei hier auf [39] verwiesen.

Datenträgerverwaltung unter Windows

Wesentliche Funktionen mit Datenträgern führt man unter Windows (7, 8, 10) mit der Anwendung *Datenträgerverwaltung* aus. Sie lässt sich auf unterschiedlichen Wegen aufrufen. Eine Variante funktioniert so: Per ⊞–R (Windows-Taste + R) ruft man den Kommandozeilendialog auf und gibt dort *diskmgmt.msc* ein.

Damit startet die *Datenträgerverwaltung*. Sie zeigt nach kurzer Zeit die aktuell sichtbaren Datenträger mit deren Partitionen und Volumes an. Nicht alle hier angezeigten Volumes müssen auch im *Explorer* sichtbar sein. So zeigt z. B. im Normalfall der Explorer auf dem Boot-Datenträger weder die *EFI-Systempartition* noch die OEM-Partition *WinRE DRV* an.

Mit der Datenträgerverwaltung lassen sich neue (oder vorhandene) Datenträger neu formatieren; dabei kann man angeben, ob ein ExFAT- oder ein NTFS-Volume angelegt werden soll. Bei einem neu angelegten Volume lässt sich auch die automatische Komprimierung aktivieren.

Die Anwendung erlaubt ebenso, eine Partition bzw. die darauf liegenden Volume zu verkleinern oder – sofern dahinter noch nicht zugewiesener Speicherplatz auf dem Datenträger vorhanden ist – zu erweitern. Löscht man ein Volume, so gehen (natürlich) alle dort vorhandenen Daten verloren.

Für die meisten Operationen selektiert man mit der Maus den betreffenden Datenträger oder eine Partition darauf und ruft die Funktion über das Kontextmenü unter der rechten Maustaste auf (siehe Abb. 2).

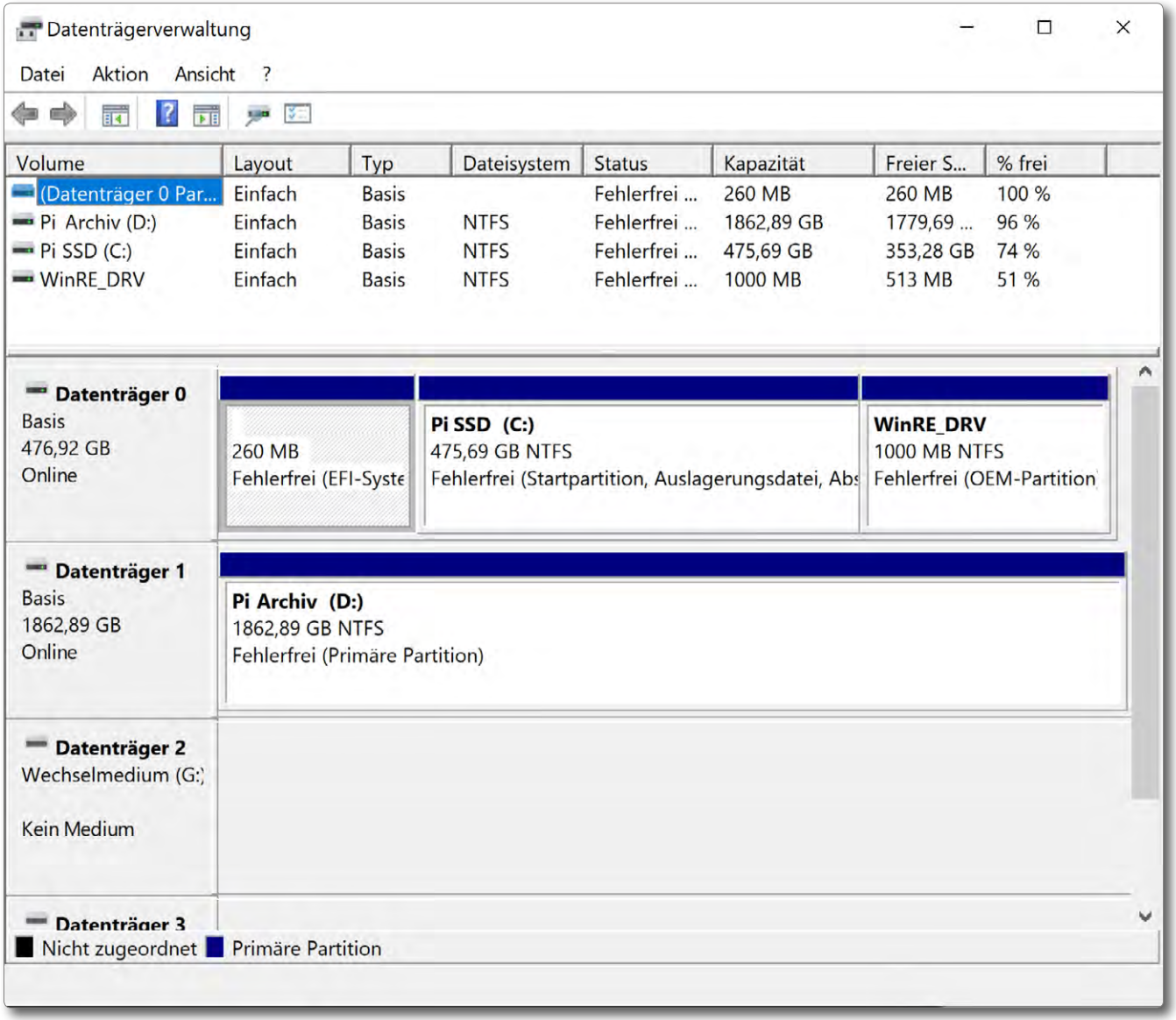


Abb. 1: Die *Datenträgerverwaltung* unter Windows 10, hier mit drei sichtbaren Datenträgern mit mehreren Partitionen und Volumes. Teilweise muss man in der Datenträgerliste erst nach unten scrollen, um einen gesuchten Datenträger zu sehen. Das aktuell selektierte Volume ist grau umrandet (hier das erste auf *Datenträger 0*) und etwas schwer zu erkennen.

Eine weitere nützliche Funktion, die sich hier auf einem Volume ausführen lässt, ist die, dem Volume einen festen Laufwerkbuchstaben zuzuordnen. Dazu selektiert man das Volume und ruft über die rechte Maustaste das Kontextmenü auf (Abb. 2), wo man die Funktion *Laufwerkbuchstaben und -pfad ändern* wählt. Im nachfolgenden kleinen Dialog (Abb. 3) gibt man dem Volume den gewünschten Buchstaben. Dies verhindert, dass sich der Laufwerkbuchstabe ändert, wenn ein externer Datenträger beim nächsten Mal aktiviert wird und andere Volumes bereits aktiviert sind. Ohne diese Maßnahme findet beispielsweise Lightroom Bilder, die auf externen Datenträgern liegen, oft nicht mehr, da die betreffenden Volumes mit den Bildern andere Laufwerkbuchstaben erhalten, wenn sie in unterschiedlicher zeitlicher Reihenfolge aktiviert werden. Es empfiehlt sich dabei, die Laufwerksbuchstaben von hinten (mit ›Z‹ beginnend) zu vergeben.

Beim Formatieren eines Volumes (Abb. 3) lässt sich nicht nur gleich ein Volume-Name und die Dateisystemart festlegen, sondern optional auch die *Größe der Zuordnungseinheit* (eine Art virtuelle Blockgröße). Bei Volumes primär für Bilddateien kann eine Größe von 4 K bis 8 K kleine Vorteile mit sich bringen (der Standard sind 512 Byte). Eine Komprimierung von Bilddaten lohnt hingegen kaum.

Es gibt eine Reihe weiterer Funktionen in der *Datenträgerverwaltung*. So kann man beispielsweise Volumes

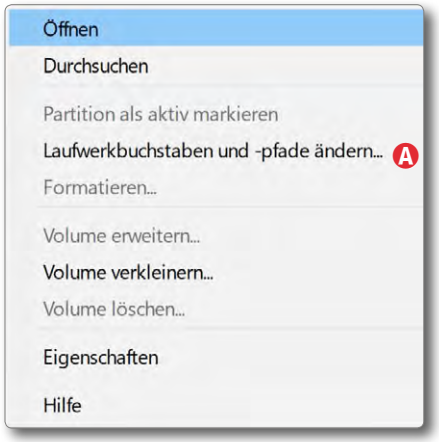


Abb. 2 Kontextmenü zu einem selektierten Volume in der Windows-Datenträgerverwaltung

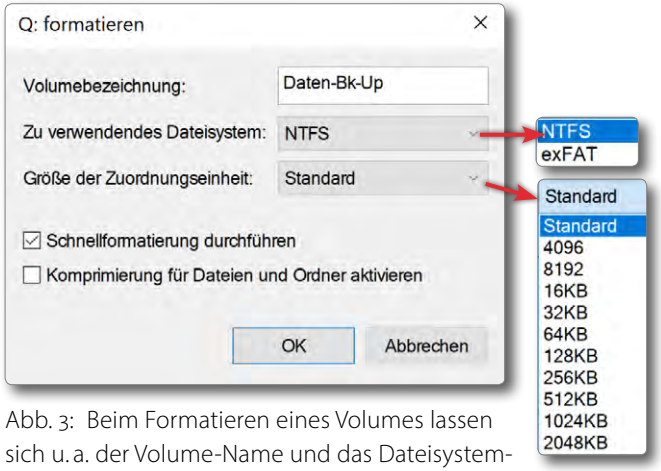


Abb. 3: Beim Formatieren eines Volumes lassen sich u. a. der Volume-Name und das Dateisystemformat sowie die Clustergröße (*Zuordnungseinheit*) vorgeben.

über mehrere Datenträger hinweg anlegen und so ein größeres Volume schaffen. Die dafür notwendigen Erläuterungen gehen aber über den Rahmen dieses E-Books hinaus.

Wie unter macOS (dort mittels *Festplattendienstprogramm*) lässt sich auch bei dieser Anwendung (unter dem Menüpunkt Aktion ›Virtuelle Festplatte erstellen) eine Art virtuelles Volume anlegen, das in einer Datei abgelegt wird. Auf diesem ›Datenträger‹ muss man anschließend über die *Datenträgerverwaltung* ein Volume anlegen, um ihn sinnvoll nutzen zu können.

Etwas inkonsistent führt man ein Auswerfen, Bereinigen oder das Formatieren nicht hier in der *Datenträgerverwaltung* durch, sondern aktiviert diese Funktionen im *Explorer* über das Kontextmenü. Das Formatieren lässt sich hingegen sowohl in der *Datenträgerverwaltung* als auch über den *Explorer* aufrufen.

Das unter Windows bei Magnetplatten zuweilen sinnvolle Defragmentieren von Volumes aktiviert man hingegen wieder an anderer Stelle. Beim Defragmentieren versucht Windows, die einzelnen Datenblöcke einer Datei in aufeinander folgende Plattenblöcke zu legen. Damit wird das Lesen und Schreiben solcher Daten potenziell etwas schneller, da zwischendurch die Schreib-/Leseköpfe nicht neu positioniert werden müssen.

SSDs und andere Flash-Speicher defragmentiert man prinzipiell nicht, da dies keine Geschwindigkeitsvorteile mit sich bringt und nur unnötige Schreibvorgänge initiiert.

Um den Dialog zum Defragmentieren zu finden, geben Sie im Windows-Suchfenster ›defrag‹ ein und klicken dann auf den Eintrag *Apps: Laufwerk defragmentieren und optimieren*. Das erscheinende Dialogfenster zeigt den Defragmentierungszustand Ihrer Volumes (Abb. 4) und erlaubt es, ein Volume auszuwählen, zu *analysieren* sowie zu *optimieren*.

Da eine Defragmentierung zeitaufwändig sein kann, lohnt es sich, vor einem solchen Lauf das Volume zu analysieren und nur dann zu defragmentieren, wenn eine nennenswerte Fragmentierung vorliegt. Bei Backup-Laufwerken bzw. Volumes kann man auf eine Defragmentierung zumeist vollständig verzichten.

Es gibt für Windows eine ganze Reihe von Anwendungen, die ähnliche Funktionen wie die *Datenträgerverwaltung* anbieten, teilweise mit deutlich erweiterten Funktionen. Einige davon – etwa *Smart Defrag* – sind kostenlos, andere kostenpflichtig (etwa *Acronis Disk Director*). Aus meiner Erfahrung recht gute Anwendungen für den Umgang mit Datenträgern sind auch *EasyUS Partition Master* [25] (siehe Seite 120) sowie *Partition Wizard* der Firma *Mini Tool* [27] (siehe Seite 118), von denen es jeweils kostenlose Versionen sowie Pro-Versionen mit erweitertem Funktionsumfang gibt. Für komplexere Operationen empfehle ich die Pro-Version von *EasyUS Partition Master* (für etwa 45 Euro), die neben verschiedenen Partition-Operationen auch das Klonen von Partitionen – auch von Systempartitionen – sowie das Migrieren des Systems auf andere Systeme unterstützt.

Ebenso findet man weitere Anwendungen, die eine Defragmentierung von Volumes anbieten (z. B. die kostenlose Version von *EasyUS Partition Master*). Eigentlich reichen hier aber die kostenlosen Werkzeuge von Windows und deren automatische Anwendung.

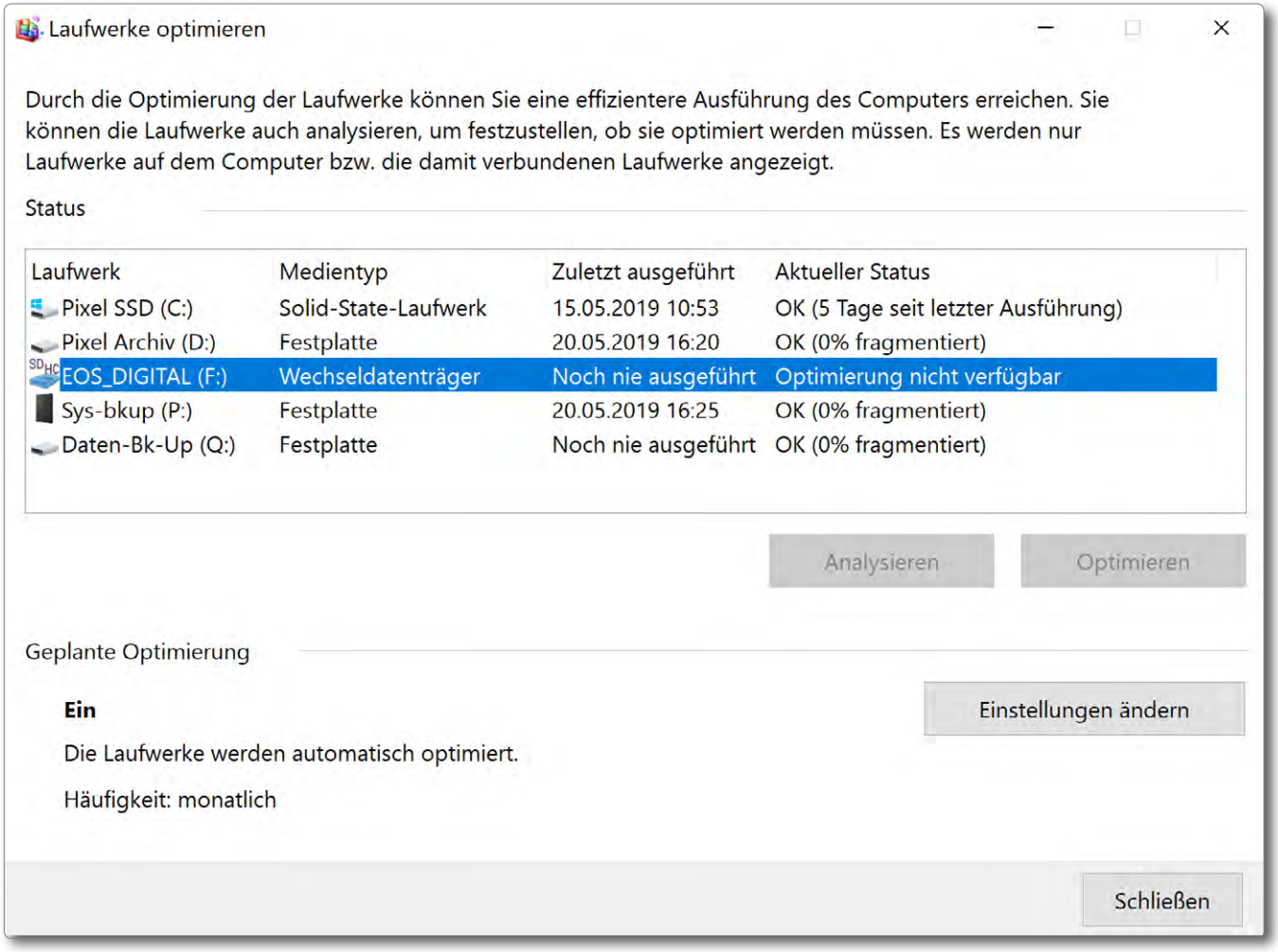


Abb. 4: Die Funktion *Analysieren* ermittelt den Grad der Fragmentierung eines Volumes, während *Optimieren* das Volume bei Bedarf defragmentiert, was bei starker Fragmentierung eine Weile dauern kann. Im Standardfall erfolgt das Optimieren in regelmäßigen Abständen automatisch (nur bei NTFS-Systemen). Auch die Einstellungen dazu lassen sich hier ändern.

Windows-Systemstart im ›abgesicherten Modus‹

Wie bei macOS ist es zuweilen notwendig, das Windows-System in einem besonderen Modus zu starten, um darin besser gewisse Korrekturen vornehmen zu können. Unter Windows ist das der *abgesicherte Modus*. Startet man in diesem Modus, so wird ein Großteil der Startobjekte nicht geladen, und viele Systemdienste bleiben deaktiviert. Dies vereinfacht die Reparatur und Korrektur problematischer Komponenten.

Per ⊞-I (Windows-Taste + I) öffnet man dazu die Windows-Einstellungen. Dort geht man auf *Update + Sicherheit* und wählt in der linken Spalte *Wiederherstellung*. Scrollt man dort nach unten, so findet man *Erweiterter Start* und darunter den Knopf *Jetzt neu Starten*.

Nach dem Neustart wählt man im Bildschirm (Abb. 1) *Problembehandlung* (und bestätigt dies mit der Eingabetaste), um im nächsten Bildschirm (Abb. 2) *Erweiterte Optionen* zu wählen. Im darauf folgenden Bildschirm (Abb. 3) wählt und aktiviert man *Starteinstellungen*.

Abb. 3: Unter *Erweiterte Optionen* wählt man *Starteinstellungen*.

Abb. 1:
Nach dem ersten Neustart erscheint dieser Bildschirm (hier wie in den nachfolgenden Bildschirmen stark beschnitten).

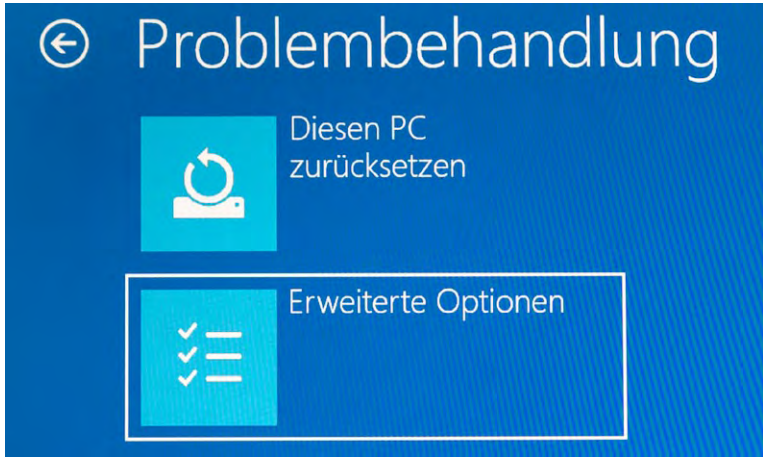


Abb. 2:
Hier wählt man *Erweiterte Optionen*.

Im nächsten Bildschirm (Abb. 4) – er ist rein informativ – klickt man auf *Neu starten*. Nach dem Neustart erscheint der Bildschirm von Abbildung 5. Hier wählt man über die Tastatur 4 oder 5, abhängig davon, ob man neben den Basisfunktionen auch die Netzwerktreiber benötigt, um bei Bedarf Komponenten aus dem Internet herunterladen zu können.

Im abgesicherten Modus (mit schwarzem Bildschirmhintergrund) funktioniert Ihre Bluetooth- oder **Funkmaus nicht mehr; der Bluetooth-Treiber ist nicht gela**den. Sie benötigen deshalb hier eine USB-Maus. Gleiches gilt für eine Bluetooth-Tastatur.

Hier kann man nun Reparaturarbeiten vornehmen, etwa Treiber neu installieren oder das System auf einen älteren Stand zurücksetzen oder eine problematische neue Software deinstallieren. Unter Umständen hilft es auch, das Dateisystem eines Laufwerks zu überprüfen.

Dazu wählt man im *Finder* das betreffende Laufwerk aus, aktiviert im Kontextmenü *Eigenschaften*, wechselt dort auf den Reiter *Tools*, um schließlich unter *Fehlerüberprüfung* den Knopf *Prüfen* einzusetzen. Damit wird überprüft, ob das Volume Dateisystemfehler aufweist, die (sofern möglich) auch gleich behoben werden.

Auch einige Funktionen auf Kommandozeilenebene können für die Stabilisierung des Systems hilfreich sein Ein Beispiel dafür ist *fsutil* (siehe Seite 123) oder das Kommando *chkdsk* (*check disk*), um Volumes auf Dateisystemfehler zu überprüfen und diese zu beheben. *chkdsk* ist etwas mächtiger als die zuvor erwähnte Dateisystemprüfung unter den *Eigenschaften* des Volumes.

Funktioniert im abgesicherten Modus das System problemlos, so kann man davon ausgehen, dass ein Treiber oder eine andere Komponente Probleme bereitet. In diesem Fall sollte man das System auf einen früheren Stand zurücksetzen (wie auf Seite 113 beschrieben) oder die zuletzt installierte Software deinstallieren.

Um zurück in den normalen Windows-Modus zu kommen, starten Sie einfach das System neu.

Abb. 4: Als einzige Funktion (außer dem Schritt zurück) findet man *Neu starten*.

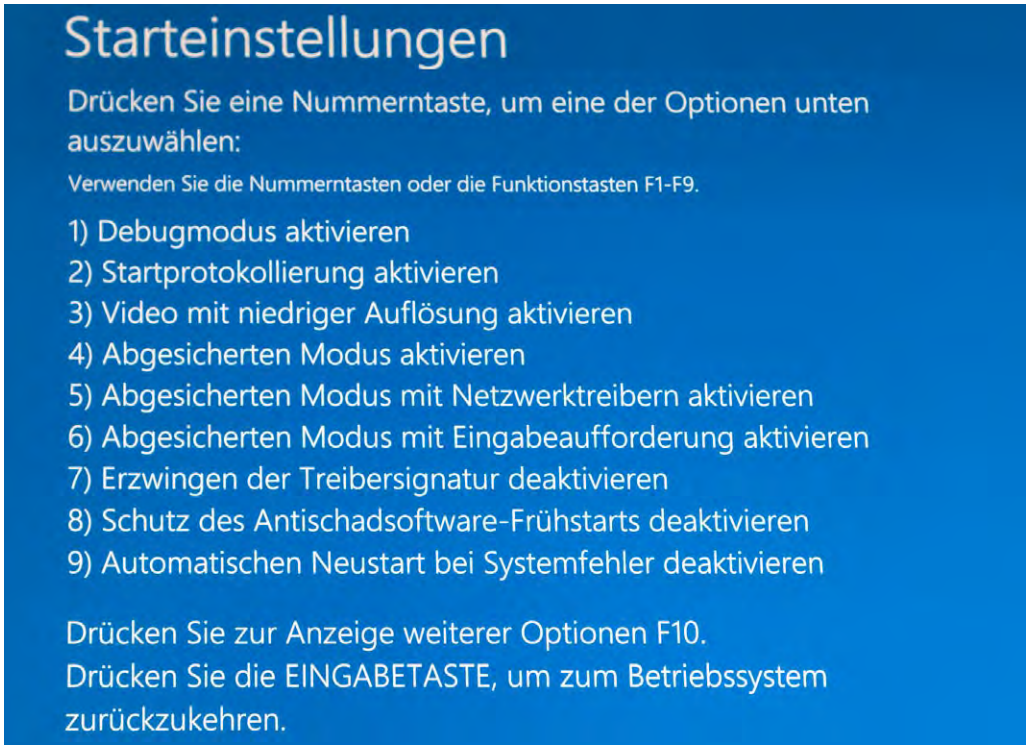


Abb. 5: Hier endlich ist es möglich, mit den Tasten 4 oder 5 den *Abgesicherten Modus* für den nächsten Start zu aktivieren.

Sicherungsanwendungen unter Windows 10

Einige wesentliche Punkte zu diesem Thema wurden bereits zu Beginn des Windows-Kapitels angesprochen. Die Datensicherung unter Windows erweist sich bisher als deutlich komplexer als unter macOS. Dies betrifft insbesondere die Sicherung bzw. das Kopieren der Systempartitionen. Bei den meisten Sicherungslösungen muss man deshalb unterschiedliche Arten der Sicherung betrachten:

A. Sicherung des Betriebssystems (Windows) und der installierten Anwendungen,
B. Sicherung der Benutzerdaten,
C. Sicherung von Datenbanken (hier nicht weiter diskutiert).

Manche Backup-Lösungen bieten beide Funktionen (z. B. *Acronis True Image* oder *AOMEI Backupper*), aber mit unterschiedlichen Programm-Modulen. Die meisten Lösungen für die Systemsicherung sichern das System in eine spezielle Image-Datei und können später aus diesem Image das System unter Nutzung eines Hilfssystems – auch als Reparaturdatenträger bezeichnet (z. B. *WindowsPE*), das zu diesem Zweck gebootet werden muss – auf den alten oder einen neuen Datenträger wieder herstellen (siehe dazu das Schemabild in Abbildung 1). Oft werden dann beim Sichern auch wirklich nur Systemdateien und die installierten Programme gesichert, nicht aber die auf dem Startlaufwerk liegenden Benutzerdateien. Manche dieser Lösungen sind leider nicht in der Lage, nach einer ersten Vollsicherung am System vorgenommene Änderungen in die Sicherung zu synchronisieren, sondern können Änderungen nur als getrennte Inkremente abspeichern. Dann lohnt es sich, nach einigen inkrementellen Sicherungen erneut eine Vollsicherung durchzuführen, um im Fall eines erforderlichen Zurückspielens nicht nacheinander die Vollsicherung und danach alle Inkremente einspielen zu müssen. Gerade beim Klonen des Systems können die meisten Anwendungen nur relativ zeitaufwändige Komplettsicherungen durchführen.

Andere Backup-Anwendungen sichern nur die Benutzerdateien, nicht aber die Systemdateien (mit den installierten Anwendungen und Treibern). Dies gilt beispielsweise für die Microsoft-Anwendung *Dateiversionsverlauf* (in der Standardkonfiguration) oder die kostenlosen Anwendungen *FreeFileSync, SyncBackFree* oder *Personal Backup*. Insbesondere zum Sichern der Benutzerdaten (der ›normalen‹ Dateien) gibt es eine Vielzahl kostenloser und kostenpflichtiger Anwendungen, von denen hier im E-Book nur einige als Beispiele beschrieben werden, ohne damit eine Qualitätsbewertung vornehmen zu wollen. Das kostenpflichtige *Acronis True Image* erledigt beides.

Wie unter macOS *Time Machine* als Teil des Systems kostenlos mitgeliefert wird, so werden bei den neueren Windows-Versionen zwei Anwendungen kostenlos mitgeliefert: *Dateiversionsverlauf* (englisch: *File History*) und *Sichern und Wiederherstellung (Windows 7)* (englisch: *Backup & Recovery*). *Dateiversionsverlauf* dient dazu, Benutzerdateien zu sichern und dabei eine Versionierung zu betreiben, so dass sich auch ältere Versionen einer bearbeiteten Datei wieder herstellen lassen.

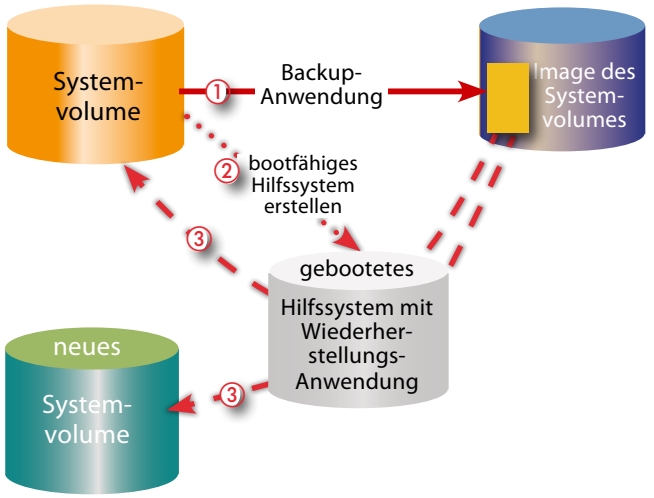


Abb. 1: Schema für die Sicherung des Systems als Image auf ein anderes Volume und das Zurückladen auf das ursprüngliche oder ein neues Systemvolume unter Verwendung eines zuvor einmal erstellten Hilfssystems bzw. Reparaturdatenträgers (z. B. WinPE) auf einem bootbaren Medium (CD/DVD, USB-Stick, USB-Laufwerk)

Zusätzlich findet man in Windows 10 eine Funktion, um einen Reparaturdatenträger zu erstellen, mit dessen Hilfe man bei massiven Boot-Problemen ein zuvor als Image gesichertes System wiederherstellen kann (siehe Seite 83).

Möchte man mit kostenlosen, komfortablen Werkzeugen auskommen, so sollte man zwei Werkzeuge einsetzen – eines für die Sicherung des Systems (z. B. Windows-*Systemabbild* oder *MiniTool Partition Wizard*) und ein zweites für die normalen Dateien des Benutzers (etwa *Personal Backup*).

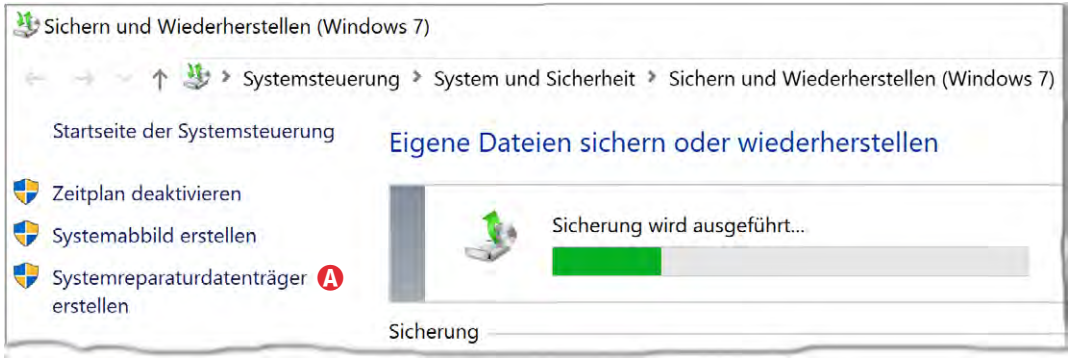


Abb. 1: Zur Erstellung eines Systemreparaturdatenträgers gehen Sie über *Einstellungen → Update und Sicherheit → Sicherung → Sichern und Wiederherstellen (Windows 7)*.

Wie erwähnt benötigt man zuweilen ein kleines System, das man booten kann, um damit gewisse Reparaturabeiten an einem defekten System durchzuführen. Dafür findet man unter Windows eine Vielzahl sowohl kostenloser als auch kostenpflichtiger Anwendungen. *AOMEI Backupper* [28] ist ein Beispiel dafür, gut und (in der *Free-Edition*) kostenlos. Auch *Acronis True Image* (siehe Seite 94) erlaubt es, ein solches Hilfssystem zu erstellen (auf CD/DVD oder auf einem USB-Stick), ist aber kostenpflichtig. Die meisten dieser Anwendungen können ein solches Minisystem (einen *Reparaturdatenträger*) sowohl auf einer CD/DVD erstellen als auch auf einem ausreichend großen USB-Stick (hier reicht fast immer ein Stick mit 16 GB).

Aber auch unter Windows 10 (ich nehme an, auch Windows 7 und 8) gibt es ein solches Tool, wobei dieses jedoch die Erstellung nur auf einer CD/DVD erlaubt. Die Handhabung ist dafür ausgesprochen einfach.

Man kommt zu dem Werkzeug über *Einstellungen → Update und Sicherheit → Sicherung → Zu Sichern und Wiederherstellen (Windows 7) wechseln*. Dort findet man links (Abb. 1 Ⓐ) den Knopf *Systemreparaturdatenträger erstellen*. Ein Klick darauf öffnet das Fenster von Abbildung 2, wo man das passende CD/DVD-Laufwerk auswählt. Darin sollte eine leere beschreibbare CD oder DVD liegen.

Ein Klick auf *Datenträger erstellen* legt dieses bootbare Minisystem auf der CD/DVD an. Beschriften Sie im Nachgang, wie von der Anwendung empfohlen (Abb. 3), diese CD mit ›*Reparaturdatenträger Windows 10*‹ (bzw. Ihrer aktuellen Windows-Version). In der Regel reicht eine CD mit 700 MB Kapazität. Schöner und aktueller wäre es, wenn man den Reparaturdatenträger auch auf einem USB-Stick erstellen könnte.

Unter Änderung der Boot-Reihenfolge im BIOS oder UEFI (beides Boot-Systeme für ein Betriebssystem) des Rechners beim Systemstart bootet man dann bei Bedarf dieses Reparatursystem und nimmt Reparaturarbeiten vor. Es lässt sich **z. B. das Systemlaufwerk** auf Fehler überprüfen (und hoffentlich reparieren) oder ein System aus einem früher erstellten Systemabbild restaurieren.

Einige der anderen Anwendungen, die ein solches Boot-Hilfssystem erstellen, so etwa *Acronis True Image* oder *EaseUS Partition Master,* packen auch gleich eine eigene Komponente in dieses System. Dies bietet beim Wiedereinspielen zumeist etwas mehr Möglichkeiten.

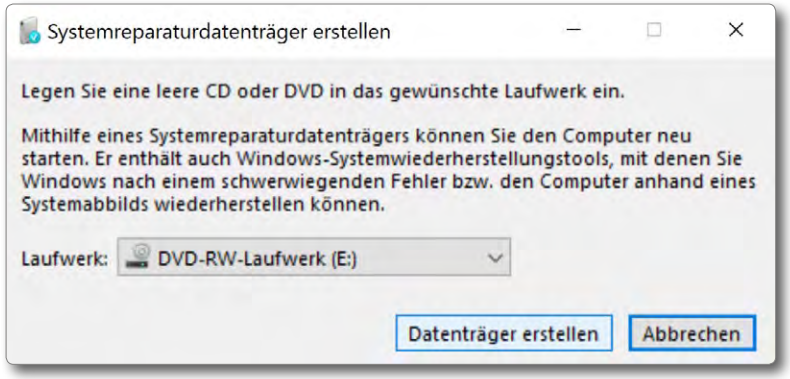


Abb. 2: Wählen Sie hier den CD/DVD-Brenner, in dem eine leere beschreibbare CD oder DVD für das Reparatursystem liegt.

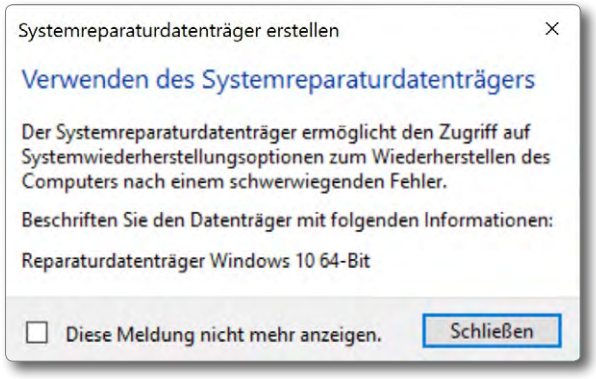


Abb. 3: Zum Schluss wirft man die CD aus und sollte sie dann wie hier vorgeschlagen beschriften. Ich selbst füge noch ein Erstellungsdatum hinzu und eine Angabe, zu welchem System der Datenträger gehört.

Es ist für einen Notfall vorteilhaft, ein Systemabbild Ihres Arbeitssystems zu haben, so dass Sie bei einem Laufwerkproblem das System bootfähig auf ein Ersatzlaufwerk spielen können, ohne Windows und die ganzen installierten Anwendungen neu installieren und eventuell mehrere Updates fahren zu müssen. Dafür gibt es zahlreiche Lösungen. Eine finden wir auch als Windows-Komponente (in Windows 7, 8, 10).

Die Funktion dazu erreicht man wieder über *Einstellungen → Update und Sicherheit → Sicherung → Zu Sichern und Wiederherstellen (Windows 7) wechseln*. Dort finden Sie links (Abb. 1 Ⓐ) den Knopf *Systemabbild erstellen*. Ein Klick darauf ruft den Dialog von Abbildung 3 auf, in dem man wählt, auf welchem Laufwerk das Abbild erstellt werden soll. Wählt man ein Festplattenlaufwerk (korrekt: ein entsprechendes Volume), so wird dort eine Datei mit dem Namen *WindowsImageBackup* erstellt. Auf dem Medium muss natürlich ausreichend Speicherplatz vorhanden sein. Der Bedarf ist abhängig davon, welche Partitionen Sie beim Sichern mit einschließen. DVDs sind der Größenbeschränkung wegen unpraktisch (ich hätte für meinen kaum gefüllten Laptop etwa 13 DVDs benötigt). Die zu sichernden Laufwerke legt man im nächsten Dialog fest (Abb. 3). Bei mir hat Windows automatisch (und nicht änderbar) die *EFI_Systempartition* sowie die *WinRE_DRV*-Partition

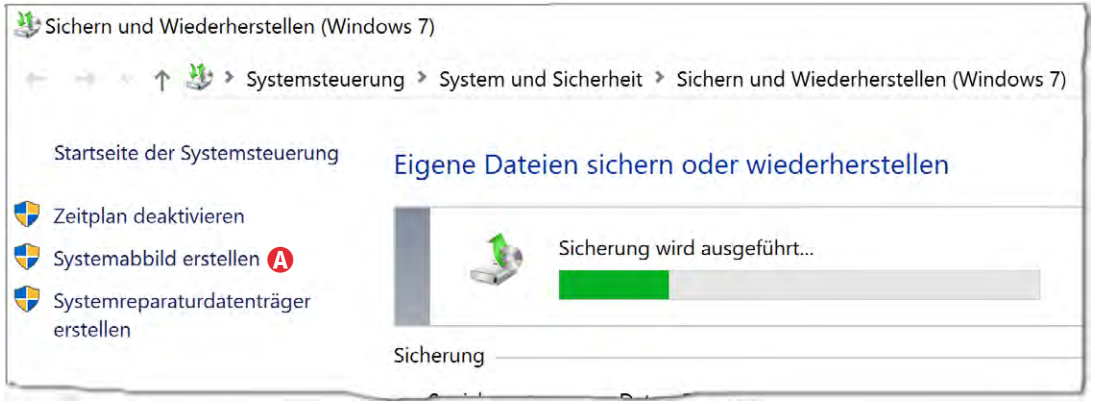


Abb. 1: Zur Erstellung eines Systemabbilds geht man unter Windows 10 über *Einstellungen → Update und Sicherheit → Sicherung → Sichern und Wiederherstellen (Windows 7)*.

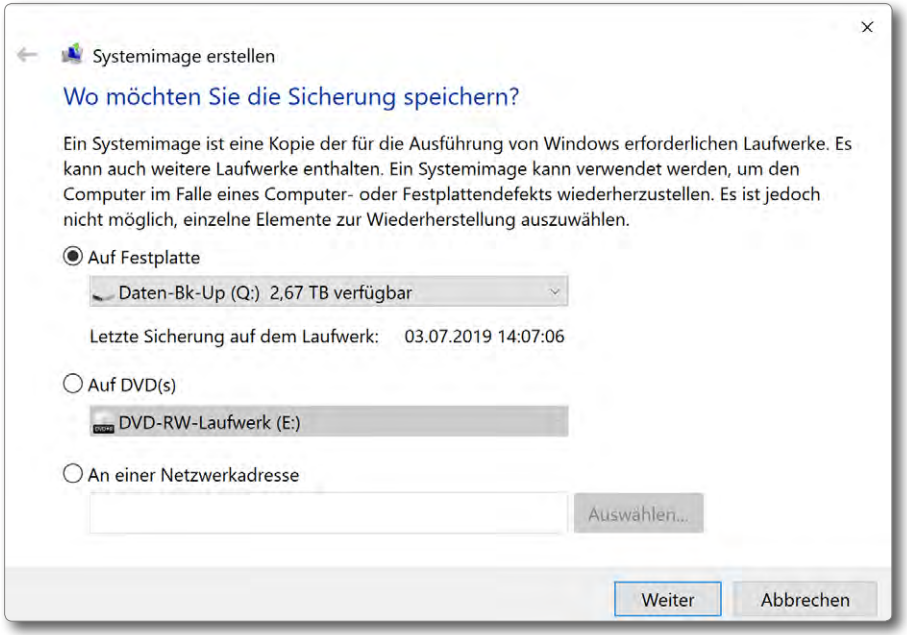


Abb. 2: Zunächst wählt man das Ziel für das Systemabbild – es kann ein Volume auf einer Festplatte sein, eine DVD oder ein Netzwerk-Laufwerk.

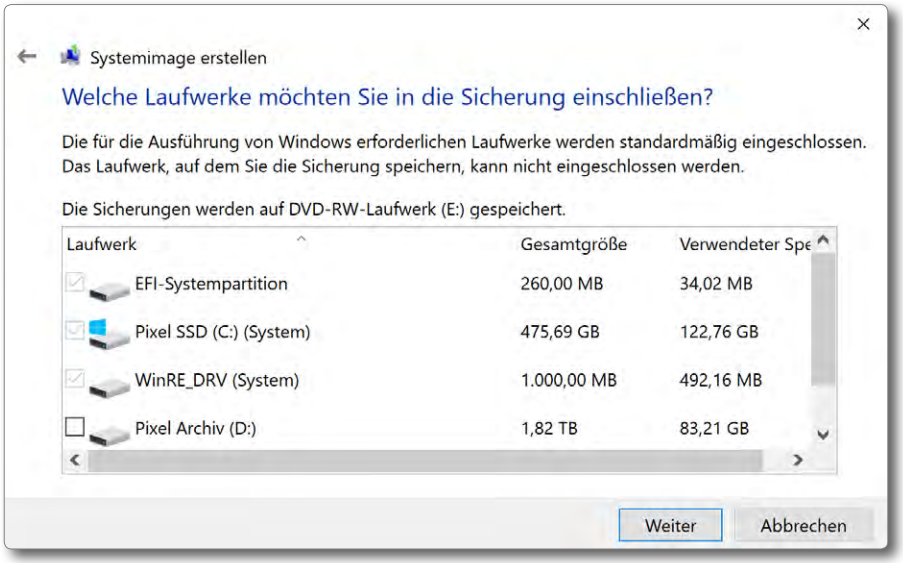


Abb. 3: Hier legt man fest, welche Partitionen im Abbild enthalten sein sollen.

(eine verdeckte Partition auf dem C-Laufwerk, die eine Windows-Recovery-Funktion bietet) sowie schließlich die Partition (das Volume) C mit eingeschlossen. Weitere Partitionen lassen sich einschließen. In der Regel ist das allerdings überflüssig, da man typische Datenpartitionen (bzw. die dort vorhandenen Dateien) besser mit anderen Mitteln sichert und bei Bedarf restauriert.

Ein Klick auf *Weiter* zeigt die Sicherungseinstellungen nochmals an und weist darauf hin, dass ein früheres Backup und andere Daten auf dem gewählten Datenträger automatisch und ohne Rückfrage überschrieben werden (Abb. 4).

Ein Klick auf *Sicherung starten* beginnt die Erstellung, zeigt dabei einen Fortschrittsbalken (Abb. 5) und bringt nach Abschluss die Erfolgsmeldung. Schließlich wird noch nachgefragt, ob man auch gleich einen Systemreparaturdatenträger erstellen möchte (siehe dazu den Abschnitt auf Seite 83).

Die erstellte Sicherung mit dem Namen *Windows-ImageBackup* enthält einen Ordner mit dem Namen des gesicherten Systems. Möchte man darauf zugreifen, so erscheint zunächst aber eine Warnung, in der man den Zugriff bestätigen muss.

Aus diesem Backup lassen sich mit normalen Mitteln **keine** einzelne Dateien extrahieren, sondern sie können nur als Gesamtheit mithilfe eines Reparaturdatenträgers (den man zuvor booten muss) zurückgespielt werden – auf den ursprünglichen Datenträger oder auf einen neuen Datenträger. Dies ist, verglichen mit anderen Lösungen, etwa *Acronis True Image*, eine unschöne Begrenzung. Bei *True Image* lässt sich zwar das System nur mit einem dafür gebooteten Hilfssystem komplett auf das Systemvolume zurückspielen, es lassen sich bei Bedarf aber zumindest einzelne Komponenten aus dem Image noch extrahieren.

Spielt man das Systemabbild wieder ein, hat man das System einschließlich der Benutzereinstellungen sowie alle zusätzlich installierten Anwendungen auf den Stand zurückgesetzt, zu dem das Abbild erstellt wurde. Man sollte deshalb in regelmäßigen Abständen ein solches Abbild erstellen – jedes Mal nach einem System-Update – und eventuell zusätzlich noch eine etwas ältere Version haben.

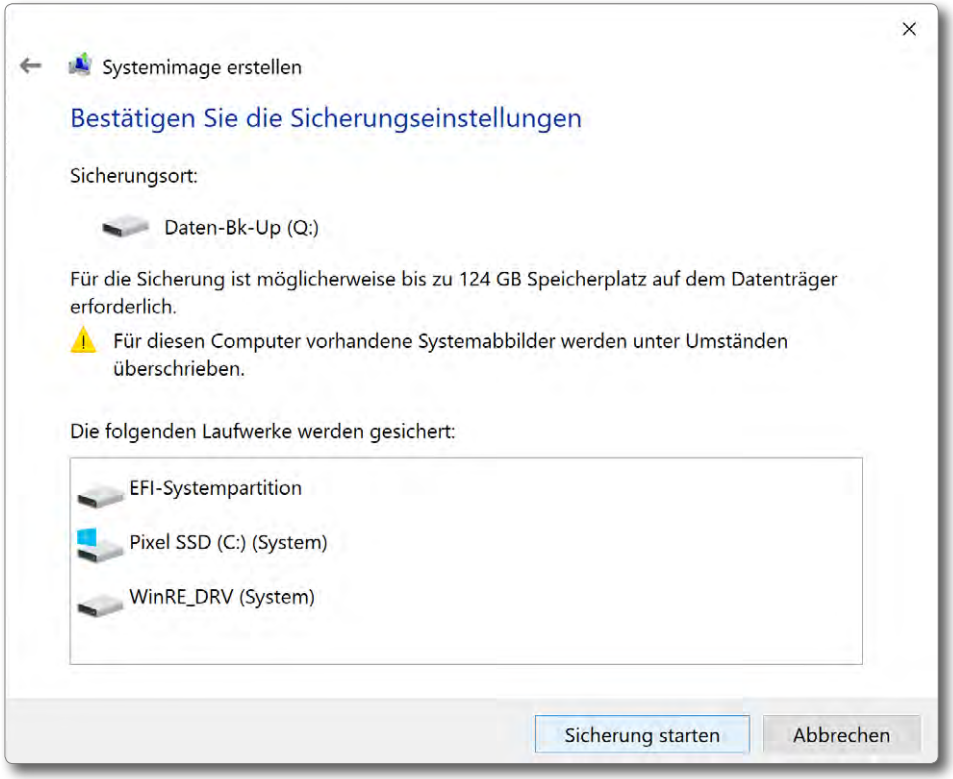


Abb. 4: Hier können Sie die Einstellungen nochmals überprüfen.

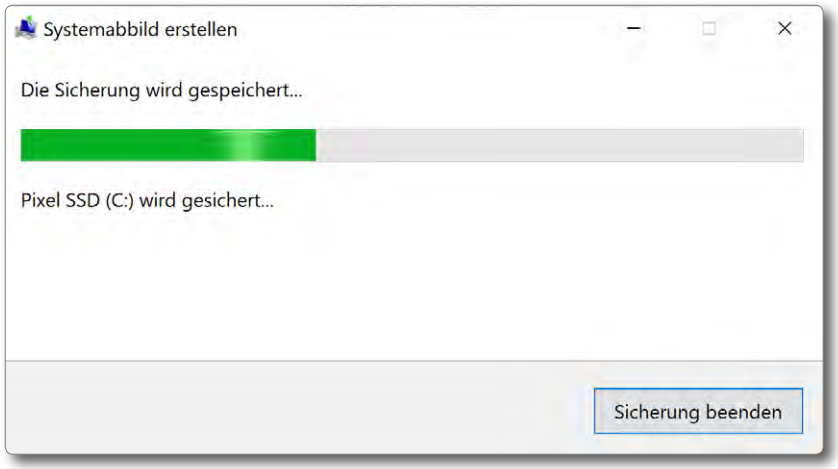


Abb. 5: Die Funktion zeigt an, wie weit die Sicherung fortgeschritten ist.

Datensicherung per ›Dateiversionsverlauf‹

Windows kommt seit Windows 8 mit der Anwendung *Dateiversionsverlauf* einher. Sie erlaubt die Sicherung von Dateien und Verzeichnissen, nicht jedoch (in der Standardkonfiguration) des (Betriebs-)Systems. Die Anwendung hat einige Ähnlichkeit mit *Time Machine* von macOS und führt eine Versionierung durch, d. h. sichert mehrere Versionsstände von Dateien. Die Microsoft-Dokumentation zur Anwendung ist leider recht mager. Der englische Name der Anwendung ist *File History*.

Man erreicht die Funktion über *Einstellungen* → *Update und Sicherheit* → *Sicherung*. Dort findet man zwei Anwendungen: *Dateiversionsverlauf* und (unter Windows 10 darunter) ›*Sicherung und Wiederherstellung (Windows 7)*‹ (Abb. 1). Hier zunächst die Beschreibung zum *Dateiversionsverlauf*.

Die Anwendung sichert in der Standardkonfiguration nur Benutzerdaten und überprüft nach einer ersten Art Vollsicherung in einstellbaren Intervallen, welche Dateien und Ordner neu hinzugekommen sind und welche geändert wurden, um diese dann ebenfalls zu sichern. Es erfolgt dabei eine Art Versionierung. Gesichert wird in ein spezielles Zielverzeichnis *FileHistory* (den Namen kann man nicht ändern). Alle gesicherten Daten müssen auf das eingestellte Zielvolume passen.

Ganz zu Beginn muss man zunächst per Klick auf das +-Icon Ⓐ angeben, wohin gesichert werden soll. Dies tut man in der erscheinenden Laufwerkliste. Dazu muss man wissen, dass die Sicherung (zunächst) nicht

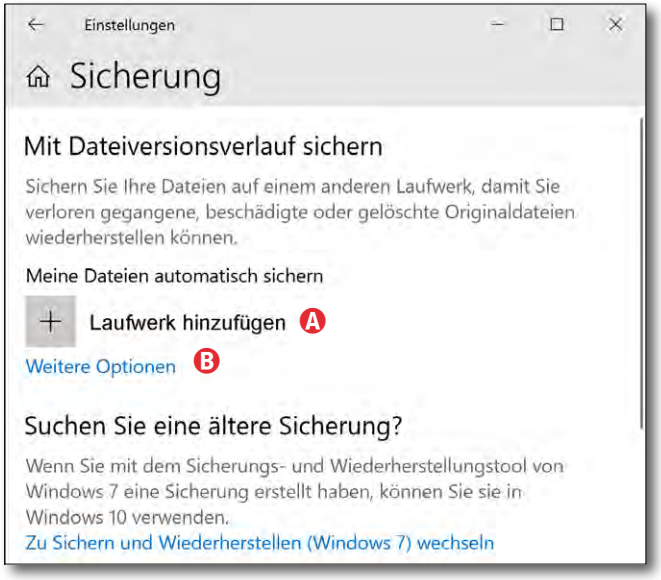


Abb. 1: Nach viel Klicken erreicht man über *Einstellungen* → *Update und Sicherheit* → *Sicherung* dieses Panel.

das ganze Laufwerk (das Volume) in Anspruch nimmt oder neu formatiert, sondern dort eine Datei namens *File History* anlegt. In diese (Image-)Datei wird hineingesichert – auch bei späteren Sicherungsläufen. Das Zielvolume sollte natürlich auf einem anderen physikalischen Laufwerk liegen als die zu sichernden Daten.

Danach erscheint statt des +-Icon ein Schalter, den man auf *Ein* oder *Aus* stellen kann (Abb. 2.

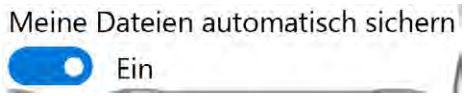


Abb. 2: Nach der ersten Konfiguration sieht der Kopf so aus.

Bevor man die Anwendung über den Schalter auf *Ein* stellt, sollte man über *Weitere Optionen* Ⓑ einige Einstellungen vornehmen. Dazu gehört das Sicherungsintervall (Abb. 3 Ⓒ). In der Regel kann man es auf *Täglich*

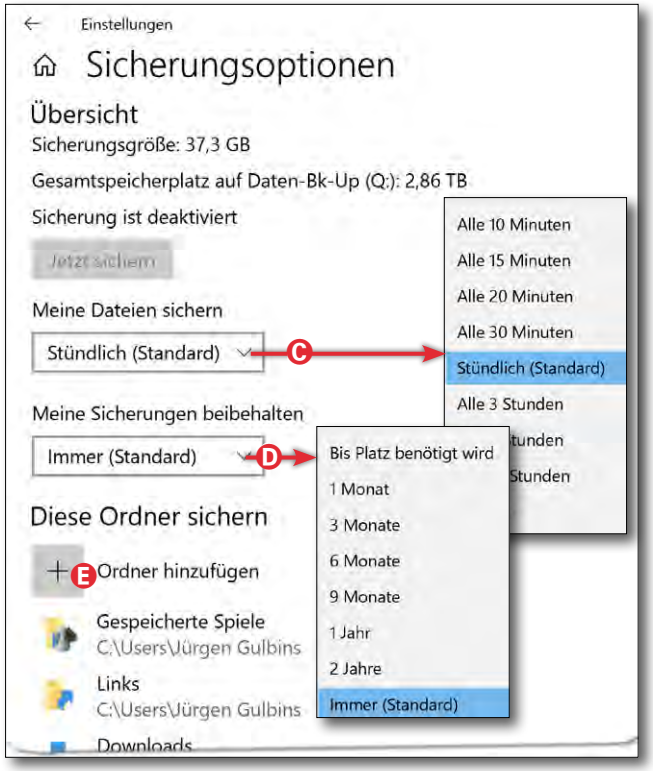


Abb. 3: Unter den *Sicherungsoptionen* finden wir das Sicherungsintervall, die Aufbewahrungsdauer gesicherter Dateien sowie die zu sichernden Ordner.

setzen (riskiert dann aber die Arbeit eines Tages).

Unter Ⓓ legt man fest, wie lange die verschiedenen Versionsstände erhalten werden sollen. Die Vorbelegung für Ⓓ ist *Immer*, was zunächst sinnvoll ist.

Danach sollte man sich unter Ⓔ die Ordner ansehen, die gesichert werden. Da Microsoft sehr großzügig in den Panels mit Platz umgeht, muss man dazu in der Regel nach unten scrollen. Die Anwendung sichert im Standardfall nur die üblichen Benutzerdaten, die sie auf dem C-Laufwerk unter dem Verzeichnis des Anwenders annimmt (etwa *Dokumente, Eigene Aufnahmen, Musik,*

Bilder, Videos). Windows nennt diese *Bibliotheken*.

Möchte man einen der aufgelisteten Ordner von der Sicherungsliste ausschließen, so klickt man zunächst auf den Eintrag und danach auf den damit erscheinenden Knopf *Entfernen*.

Es lassen sich weitere Ordner hinzufügen. Dies erfolgt per Klick auf das +-Icon (Abb. 3 Ⓔ). Diese Ordner dürfen auch auf anderen Laufwerken liegen.

Weiter unten in dieser Liste findet man auch eine Komponente *Diese Ordner ausschließen*. Dort lassen sich, wie zuvor beschrieben, Ordner hinzufügen oder löschen. Einzelne Dateien lassen sich aber weder ein- noch ausschließen. Ebenso gibt es keine Filterfunktion, mit der man per Namensmuster (in der Art: ›*.tmp‹)[1] Dateien von der Sicherung ausschließen kann.

Der Ablageort bzw. das Zielvolume lässt sich auch später noch ändern, allerdings etwas umständlich. Dazu muss man zunächst die automatische Sicherung deaktivieren und warten, bis der aktuelle Sicherungslauf beendet ist. Dann fährt man in der Sicherungsliste nach unten bis zu *Laufwerk nicht mehr verwenden*. Dann geht man in die übergeordnete Ansicht (Abb. 1) und klickt dort unter *Laufwerk hinzufügen* auf das +-Icon, um ein neues Ziellaufwerk festzulegen.

Recht weit unten in der Scroll-Liste findet man einen Punkt *Verwandte Einstellungen*. Klickt man dort auf *Siehe weitere Einstellungen*, so erhält man eine Art Übersicht

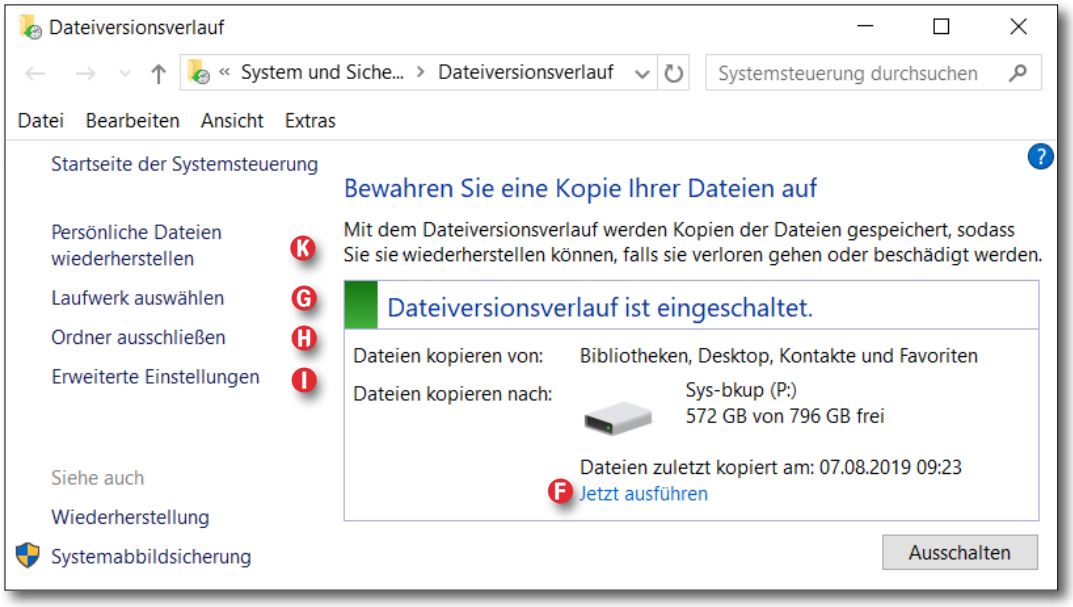


Abb. 4:
Fenster zu *Erweiterte Einstellungen*. Hier lassen sich etwas kompakter als im Fenster von Abbildung 3 Einstellungen vornehmen. Zusätzlich stehen hier weitere Funktionen zur Verfügung.

(Abb. 4). Hier sieht man das Datum der letzten Sicherung und kann die Sicherung sofort anstoßen (Ⓕ). Unter Ⓖ lässt sich auch ein abweichendes Ziellaufwerk auswählen; man kann Ordner von der Sicherung ausschließen (Ⓗ) sowie *Erweiterte Einstellungen* (Ⓘ) vornehmen. Damit werden lediglich die Einstellungen in einer anderen Form präsentiert (Abb. 5). Daneben lässt sich die Sicherung *bereinigen*. Ein Dialog erlaubt dann festzulegen,

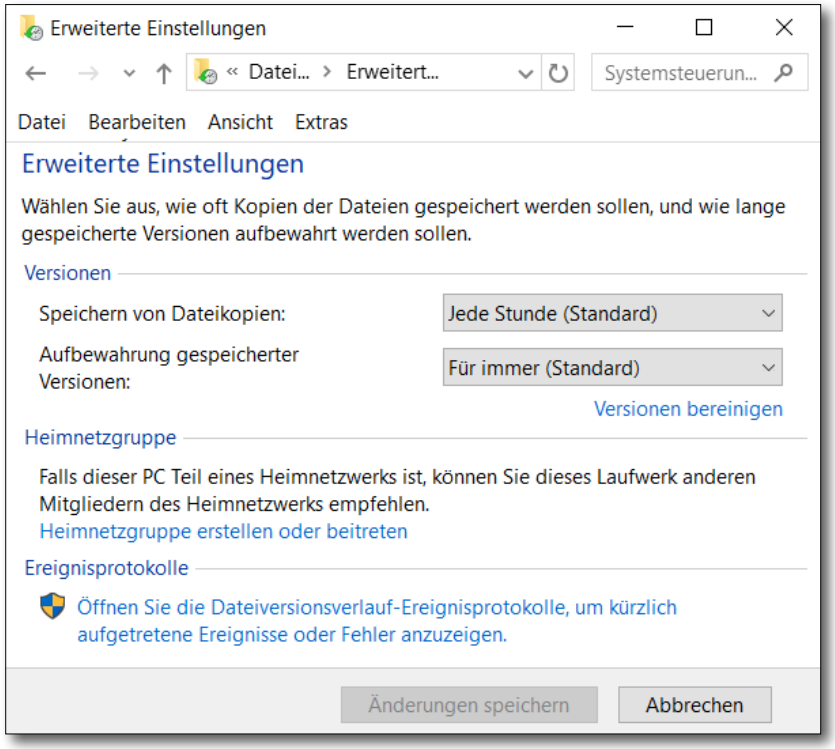


Abb. 5:
Erweiterte Einstellungen zeigt einige Einstellungen in kompakter Form und erlaubt es, das Protokoll der letzten Sicherungen abzurufen. Unter *Versionen bereinigen* lassen sich ältere Versionsstände löschen, um Speicherplatz zu sparen.

1 Das Namensmuster ›*.tmp‹ besagt, dass *alle* (dafür steht das ›*‹) Dateien mit der Endung ›.tmp‹ auf das Muster passen.

welche älteren Versionsstände gelöscht werden sollen (etwa älter als ein Jahr). Zusätzlich kann man in diesem Fenster das Ereignisprotokoll der letzten Sicherungen abrufen.

Zurückspielen gesicherter Dateien

Möchte man nur einzelne Dateien extrahieren, so navigiert man auf dem Sicherungsvolume mit dem *Explorer* auf den Ordner *File History* und dort unter dem Ordner *Data* zu dem gewünschten Ordner, um per Kopieren & Einfügen die gewünschten Dateien oder Ordner an eine andere Stelle zu übertragen. Offensichtlich beherrscht der Explorer dieses Sicherungsformat. Es ist auf diese Weise jedoch etwas schwierig, bestimmte Versionsstände einer Datei zu finden.

Möchte man hingegen mehrere oder alle gesicherten Dateien zurückspielen oder sucht man nach einer bestimmten älteren Version einer gesicherten Datei, so verwendet man dafür wieder *Dateiversionsverlauf*. Dort nutzen Sie die Funktion *Persönlichen Dateien wiederherstellen* (Ⓚ) im Fenster von Abbildung 4. Nach kurzer Zeit erscheint ein Fenster, etwa wie in Abbildung 6.

Hier gibt man im Suchfeld Ⓐ den Namen der gewünschten Datei ein oder verwendet die Pfeile nach links und rechts, um die verschiedenen Versionen der Ordner und Dateien zu durchsuchen. Das angeschnittene Fenster links signalisiert, dass es noch einen früheren Sicherungsstand gibt, ein angeschnittenes Fenster rechts einen späteren Stand.

Im zentralen Fenster wählt man die Objekte aus, die man am ursprünglichen Ort wiederherstellen möchte. Ein Klick auf den *Wiederherstellen*-Knopf führt die Operation aus. Möchte man die ausgewählten Objekte an anderer Stelle wiederherstellen, so bietet das Kontextmenü zum -Knopf Ⓓ die Option *Wiederherstellen in* und gestattet den neuen Ablageort festzulegen.

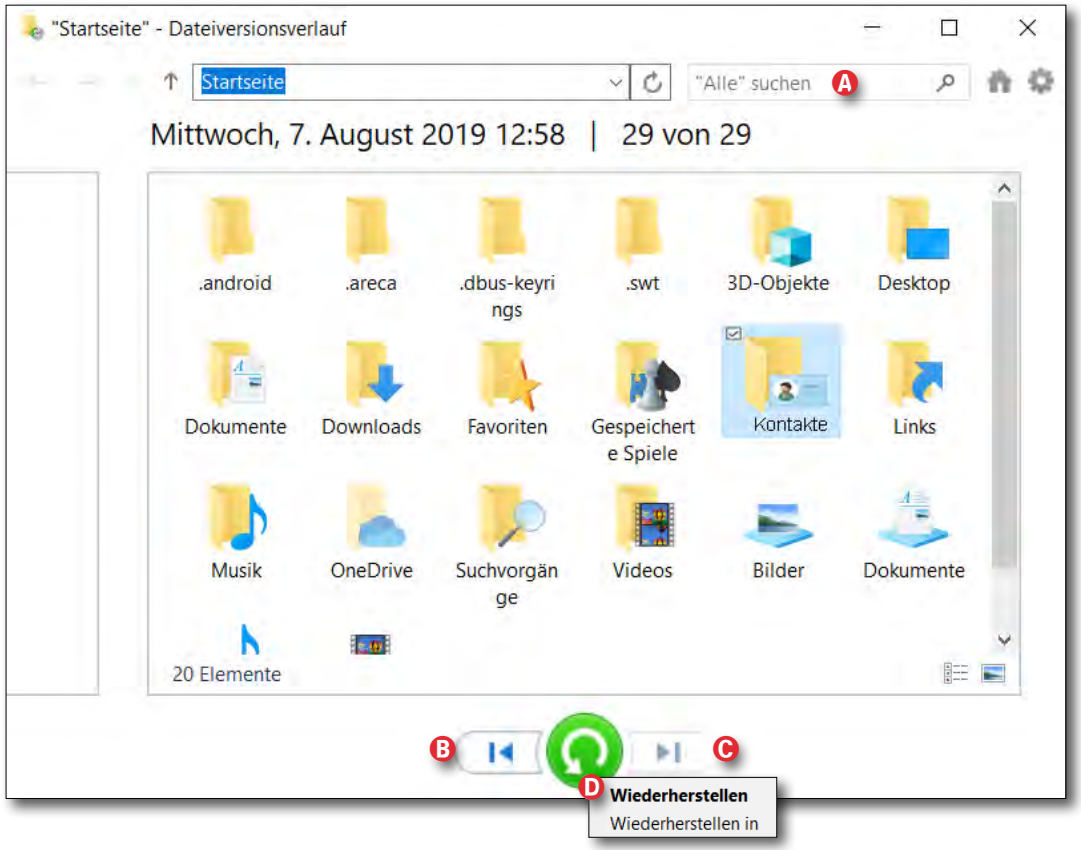


Abb. 6: Man kann in diesem Wiederherstellungsfenster mit dem Rollbalken sowie den Pfeilen navigieren. Das angeschnittene Fenster links signalisiert, dass es noch frühere Versionen gibt. Knopf Ⓑ führt zur ältesten Sicherung, Knopf Ⓒ zur neuesten. Hat man im Fenster Objekte für die Wiederherstellung selektiert (hier *Kontakte*), so führt ein Klick auf die Wiederherstellung an den ursprünglichen Ort durch. Das Kontextmenü zu erlaubt eine Wiederherstellung an einem anderen Ablageort.

Zusammenfassung

Kennt man andere Backup-Anwendungen, so muss man – ohne ein Microsoft-Bashing zu betreiben – leider feststellen, dass es **Microsoft gelungen ist, eine durchaus funktionale Anwendung** mit einer umständlichen und intransparenten Oberfläche zu versehen, mit unübersichtlicher Konfiguration, verteilt über uneinheitliche Dialoge. Es fehlen nützliche Funktionen – etwa Filter, die unter Verwendung von Namensschemata erlauben, bestimmte Dateien ein- oder auszuschließen. Auch die Robustheit bei Problemen und die Art der Fehlermeldungen lassen zu wünschen übrig.

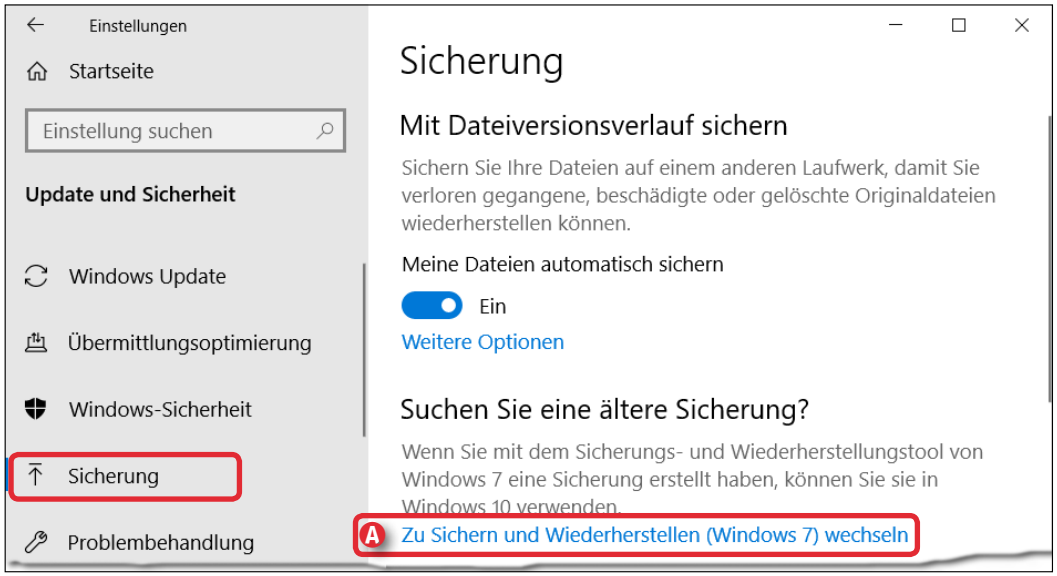


Abb. 1: Unter den Windows-*Einstellungen* findet man unter *Update und Sicherheit* und dort wiederum unter *Sicherung* die Funktion ›*Zu Sichern und Wiederherstellen (Windows 7) wechseln*‹.

Eine weitere Sicherungsanwendung von Windows 10 (auch unter Windows 7 und 8 verfügbar) ist die Anwendung mit dem langen Namen ›*Sichern und Wiederherstellung (Windows 7)*‹. Microsoft hat die Weiterentwicklung abgekündigt, ohne bisher einen richten Ersatz dafür anzubieten. Ich werde den langen Namen nachfolgend mit ›SuWW7‹ abkürzen.

Man findet die Anwendung im Windows-Startmenü unter *Einstellungen* → *Update und Sicherheit* → *Sicherung*. Dort findet man (wie zuvor bei *Dateiversionsverlauf* beschrieben) zwei Anwendungen: *Dateiversionsverlauf* und (unter Windows 10 darunter) ›*Zu Sichern und Wiederherstellen (Windows 7) wechseln*‹. Hier betrachte ich Letztere (Abb. 1 Ⓐ).

Ein Klick darauf bringt uns ins Fenster von Abbildung 2, wo wir per Klick auf *Sicherung einrichten* Ⓑ die Details für die Sicherung festlegen können.

Es erscheint zunächst ein Dialog, in dem man das Ziellaufwerk für die Sicherung wählt (auf einen Screenshot des Dialogs sei an dieser Stelle verzichtet). Windows zeigt dabei den gesamten Speicher der einzelnen Laufwerke als auch den jeweils noch vorhandenen freien Speicher. Das gewählte Laufwerk sollte eines sein, das auf einem anderen physikalischen Datenträger liegt (nicht nur auf einer anderen Partition) als das Systemlaufwerk und die eventuell weiteren zu sichernden Laufwerke. Der (hier nicht gezeigte) Dialog dazu weist nochmals explizit darauf hin. (Bei all diesen Änderungen dauert es einen Augenblick, bis Windows die Einstellungsdialoge anzeigt.) Die Daten dieser Sicherungen (aller Läufe) landen auf dem eingestellten Laufwerk in einer Datei, die den Namen Ihres Rechners trägt.

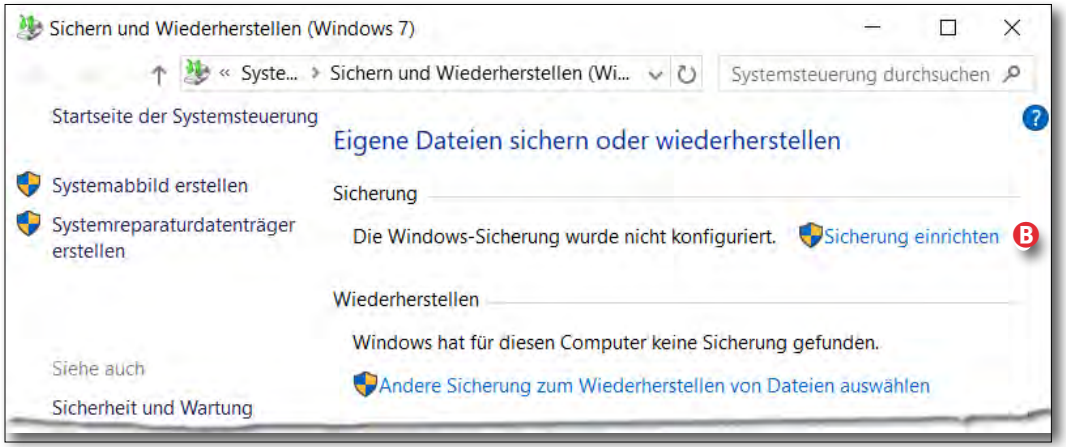


Abb. 2 Ist *Sichern und Wiederherstellen (Windows 7)* wie hier noch nicht konfiguriert, so nimmt man die Einstellungen per Klick auf Knopf Ⓑ vor.

Zusätzlich gilt es im nachfolgenden Schritt festzulegen, welche Daten gesichert werden sollen – entweder die durch Windows ausgewählten, wobei damit auch

ein Systemimage gesichert wird (Abb. 3 Ⓒ), oder man führt als Benutzer die Auswahl selbst durch (Ⓓ). In letzterem Fall kann man Order aus der Voreinstellungsliste löschen und eigene hinzufügen. Auch hier wird die Option angeboten, ein Systemabbild (als Image-Datei) anzulegen. Dieses wird (wie unter Ⓒ) separat auf dem Zieldatenträger unter *WindowsImageBackup* abgelegt.

Möchte man später ein anderes Ziellaufwerk verwenden und damit eine neue Sicherung erstellen, so ist dies über den Knopf *Einstellungen ändern* im Basispanel möglich (Abb. 6 Ⓗ).

Vor dem Sichern der Einstellung für die nachfolgenden Sicherungsläufe zeigt Windows nochmals ein Fenster mit den bisherigen Einstellungen (Abb. 4).

Der Knopf *Zeitplan ändern* Ⓔ führt zum Zeitplan für die (automatischen) Sicherungen (Abb. 5). Man hat die Wahl zwischen *Täglich*, *Wöchentlich* und *Monatlich* und kann noch die Uhrzeit für die automatische Sicherung einstellen – bei *Wöchentlich* zusätzlich den Wochentag und bei *Monatlich* den Tag des Monats. (Es ist jedoch auch möglich, auf die Automatik zu verzichten und die Sicherungen jeweils explizit anzustoßen, z. B. über den Knopf *Jetzt sichern* von Abbildung 6.)

Zurück im Dialog von Abbildung 4 sichert man die Einstellungen per Klick auf *Einstellungen speichern und Sicherung ausführen* (Ⓕ). Die erste Sicherung wird damit automatisch gestartet.

Nach dem ersten Sicherungslauf sieht das Fenster zu *Sichern und Wiederherstellen (Windows 7)* etwa wie in

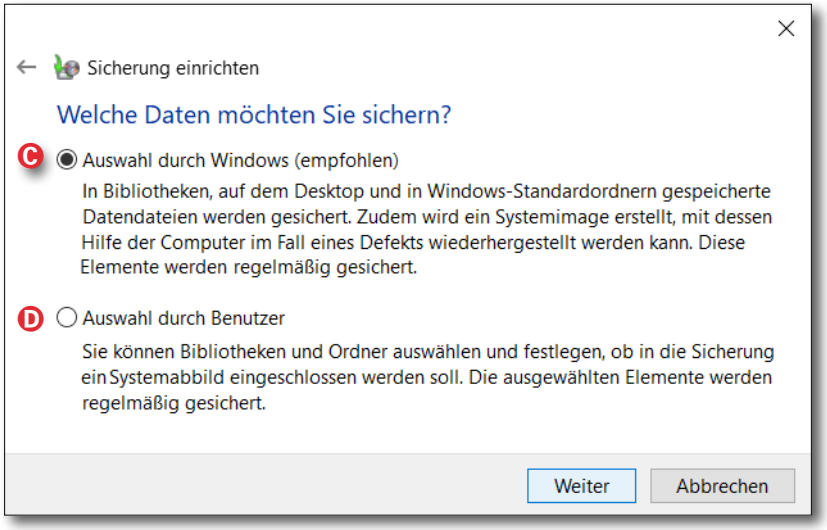


Abb. 3: Hier kann man Windows die Auswahl der zu sichernden Daten überlassen – oder man legt sie selbst fest.

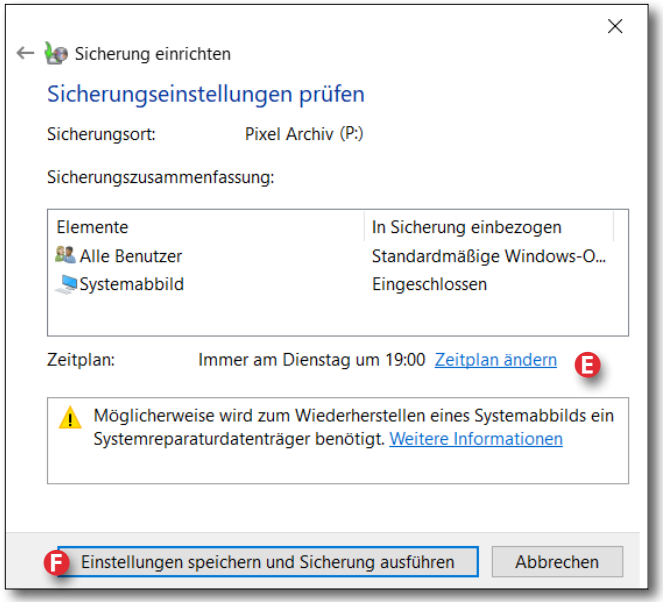


Abb. 4: Prüfen Sie hier nochmals einige Einstellungen und aktivieren Sie unter Ⓜ die Sicherungsintervalle.

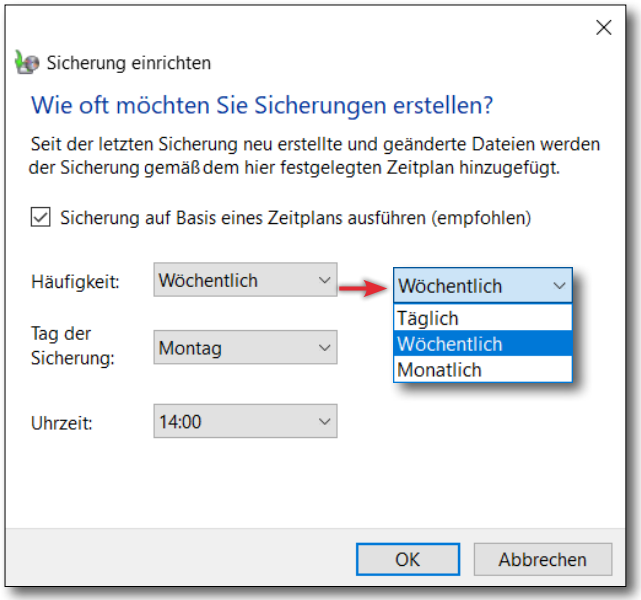


Abb. 5: Zeitplan für die Ausführung der Sicherung

Abbildung 6 aus. Hier ist erkennbar, wann der letzte Sicherungslauf erfolgte und für wann der nächste vorgesehen ist.

Mit dem Knopf Ⓖ *Speicherplatz verwalten* erhält man detaillierte Informationen zum Speicher, der durch die Sicherung beansprucht wird (Abb. 7), getrennt nach den reinen Daten (Datendateispeicherung) und nach dem *Systemabbild* (sofern dessen Sicherung auch eingestellt war). Unter *Sicherungen anzeigen* Ⓘ zeigt Windows die inzwischen durchgeführten Sicherungsläufe an. Dabei lässt sich ein Lauf auswählen und über den Knopf *Löschen* entfernen, um Speicherplatz zu sparen. Mittels *Einstellungen ändern* (Abb. 7 Ⓙ) ist es möglich, ältere Systemabbilder zu löschen – sofern die Erstellung von Systemabbildern aktiviert wurde –, wiederum um Speicherplatz zu sparen.

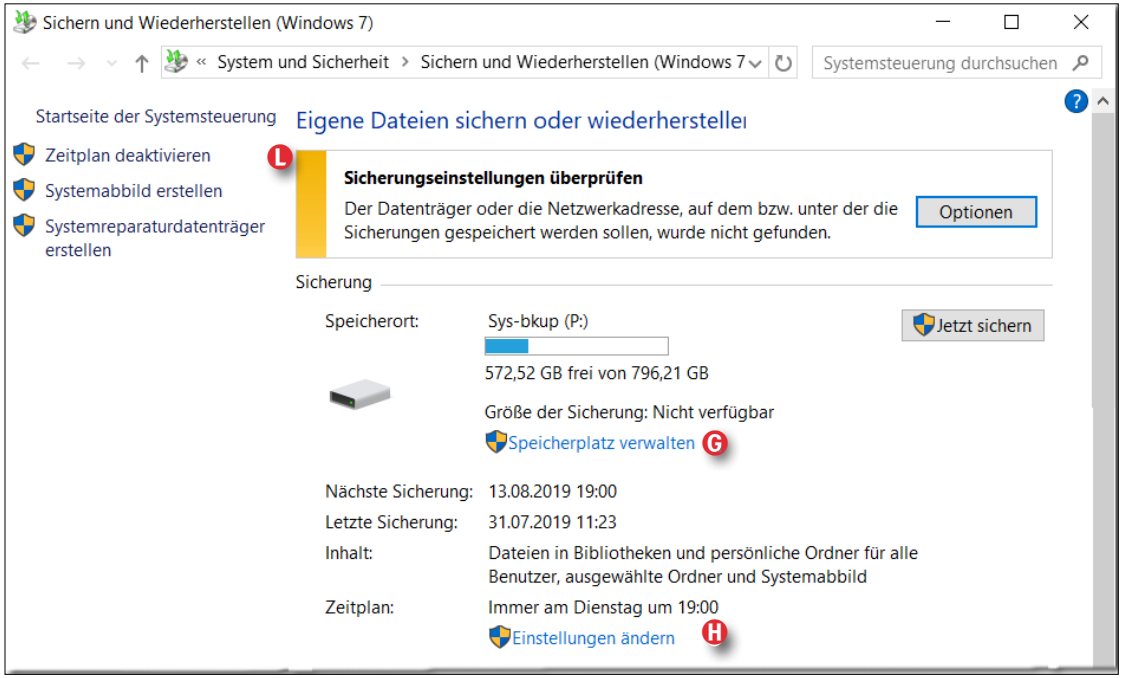


Abb. 6:
Der obere Teil der Informationen und Einstellungen zu SuWW7

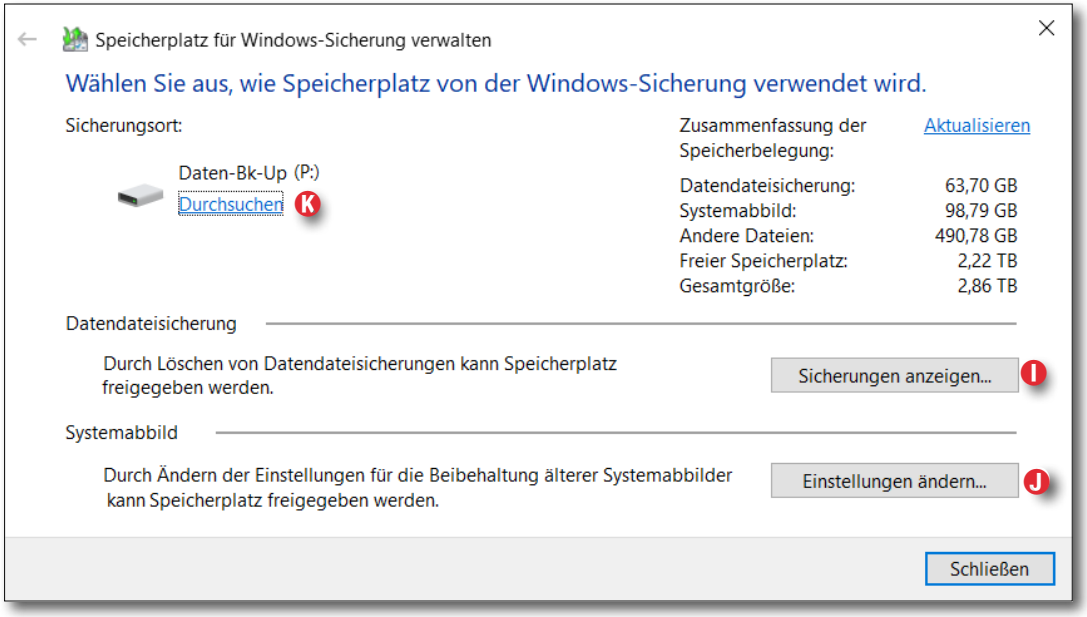


Abb. 7:
Das Fenster zeigt unter *Datensicherung* zunächst, wie viel Platz die Sicherungen bisher in Anspruch nehmen. Hier wählt man das Ziellaufwerk für die Sicherung und kann sich unter Ⓕ die Sicherungsliste anzeigen lassen und ältere Sicherungen löschen, um Speicherplatz zu sparen.

Wiederherstellen der Daten

Möchte man Daten wiederherstellen, so muss man unter *Sichern und Wiederherstellung* weiter nach unten scrollen, um den Block *Wiederherstellen* zu sehen (Abb. 8). (Alternativ geht man in Abbildung 7 auf *Durchsuchen* (Ⓚ) und wählt im Browser-Fenster die Datei mit dem Sicherungsimage. Im erscheinen Dialog (siehe Abb. 11, Seite 93) werden ebenso die nachfolgend angeführten drei Varianten angeboten.) Dort finden wir drei Funktionen: *Eigene Dateien wiederherstellen* Ⓘ und *Dateien für alle Benutzer wiederherstellen* Ⓚ sowie *Andere Sicherung zum Wiederherstellen von Daten*

auswählen Ⓛ. (Diese Funktionen sind nur aktivierbar, wenn aktuell keine Sicherung läuft.)

Mit einem Klick auf Ⓘ (*Eigene Dateien wiederherstellen*) erscheint ein Dialog (Abb. 9), in dem man nach Dateien oder Ordnern sucht, die man wiederherstellen möchte. Dazu kann man mit *Suchen* arbeiten. Es erscheint dafür ein eigenes Suchfenster, aus dessen Trefferliste man Objekte übernehmen kann. Alternativ verwendet man *Nach Dateien suchen* oder *Nach Ordner suchen* und navigiert in deren Browser-Fenster im Bestand der gesicherten Objekte zu den gewünschten Dateien oder Ordnern.

Eine Funktion, alle gesicherten Dateien für eine Wiederherstellung auszuwählen, habe ich nicht gefunden, es mag sie aber in den etwas unübersichtlichen Dialogen/Panels geben.

Wurden mehrere Sicherungsläufe durchgeführt (im Standardfall ist automatisch der letzte Lauf ausgewählt), lässt sich auch ein bestimmter Sicherungslauf über das Datum unter dem Knopf *Anderes Datum auswählen* (Abb. 9 Ⓜ) für eine Wiederherstellung aussuchen.

Hat man alle gewünschten Objekte in die Wiederherstellungsliste von Abbildung 9 übernommen, so kommt man per *Weiter* zum nächsten Dialog (Abb. 10).

Darin hat man die Wahl, ob die zuvor ausgewählten Objekte an den ursprünglichen Speicherort zurück- oder an eine neue Stelle gespeichert werden sollen. Ein Klick auf *Wiederherstellen* führt die Operation schließlich durch.

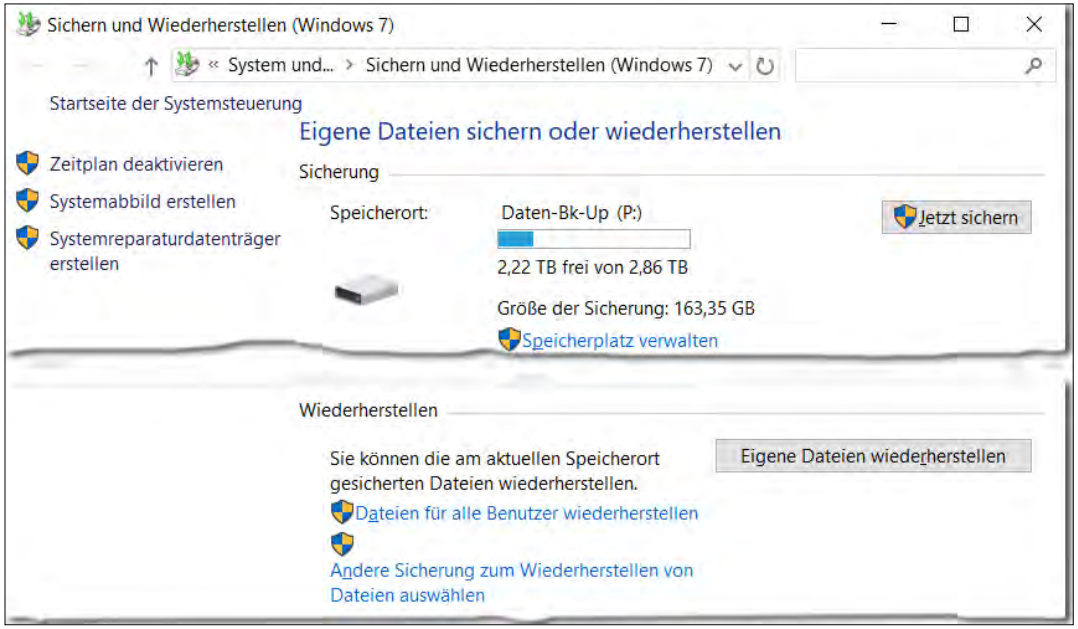


Abb. 8:
Scrollt man im Basispanel nach unten, erscheint der Block *Wiederherstellen*.

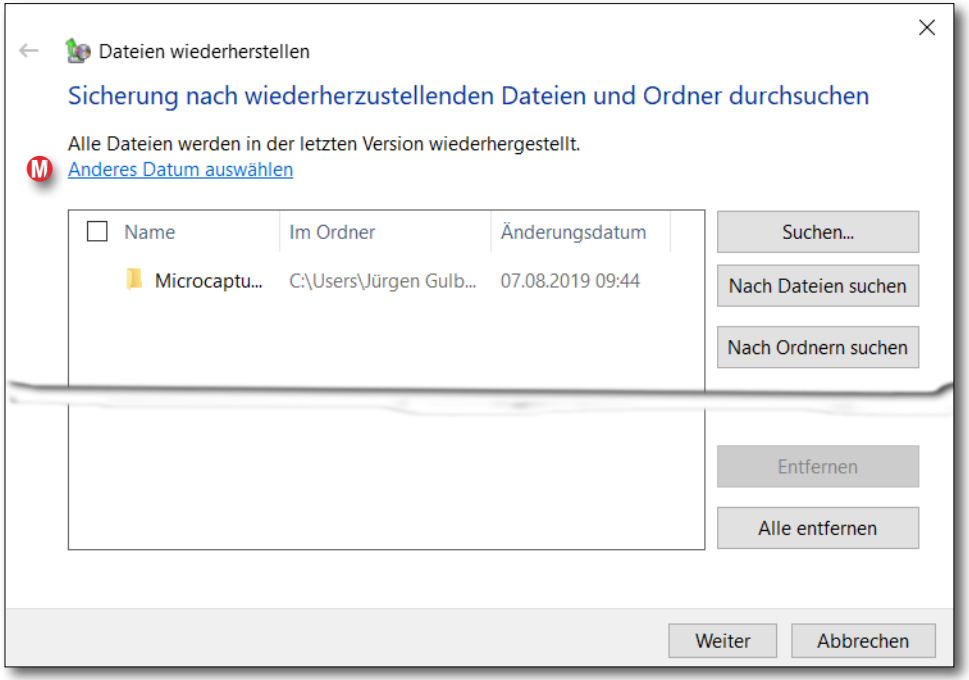


Abb. 9:
Hier sucht oder navigiert man zu den Dateien oder Ordnern, die man zurückspielen möchte, und übernimmt sie in diese Liste.

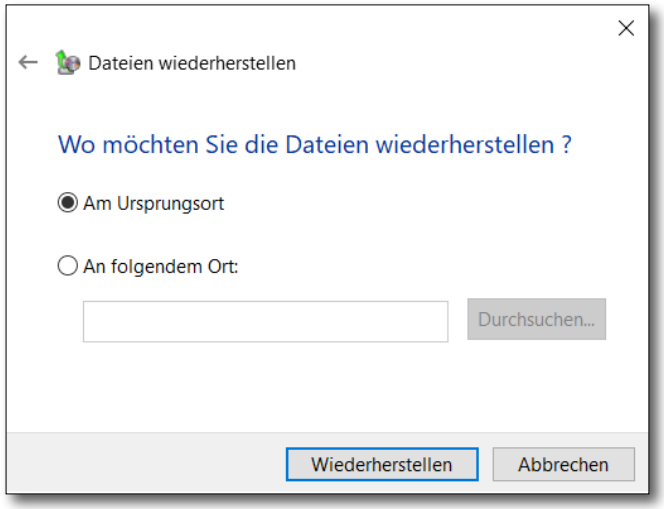


Abb. 10: Die zuvor ausgewählten Objekte werden im Standardfall an den Ursprungsort zurückgeschrieben. Man kann aber auch ein neues Ziel angeben.

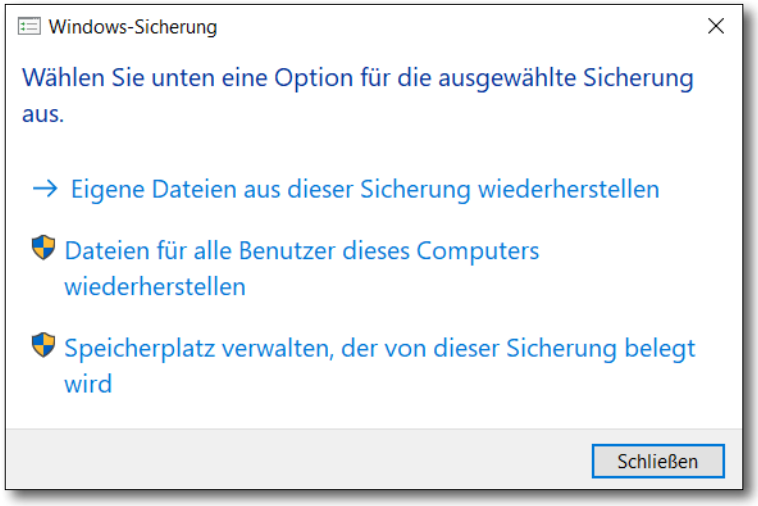


Abb. 11: Für das Zurückspielen gesicherter Objekte werden dem Benutzer drei Optionen geboten. Dieser Dialog erscheint auch, wenn man im *Explorer* einen Doppelklick auf eine Image-Datei ausführt, die mit *Sichern und Wiederherstellen (Windows 7)* erstellt wurde.

Zusammenfassung

Was eine etwas unübersichtliche Konfiguration der Anwendung betrifft, gilt die gleiche Kritik wie für *Dateiversionsverlauf*. Nicht selten muss man suchen und ausprobieren, um eine einmal vorgenommene Einstellung später zu ändern.

Einmal aufgesetzt, läuft die Anwendung aber unauffällig und funktional, und sie ist, wie erwähnt, wie *Dateiversionsverlauf* kostenloser Bestandteil von Windows (7, 8, 10). Es könnte jedoch passieren, dass *Sichern und Wiederherstellen (Windows 7)* in einer der nächsten Funktions-Updates von Windows 10 entfällt.

Literaturempfehlung

Es gibt ein wirklich breites Spektrum an Literatur zu den zuvor beschriebenen Systemdetails und dazu, was man tun kann, wenn Windows nicht wie erwartet funktioniert. Mir selbst hat dabei ein kleines, relativ preiswertes Büchlein von Wolfram Gieseke geholfen [40]. Es trägt den Titel ›*Der Windows 10 Pannenhelfer*‹.

Datensicherung per Acronis True Image (Windows)

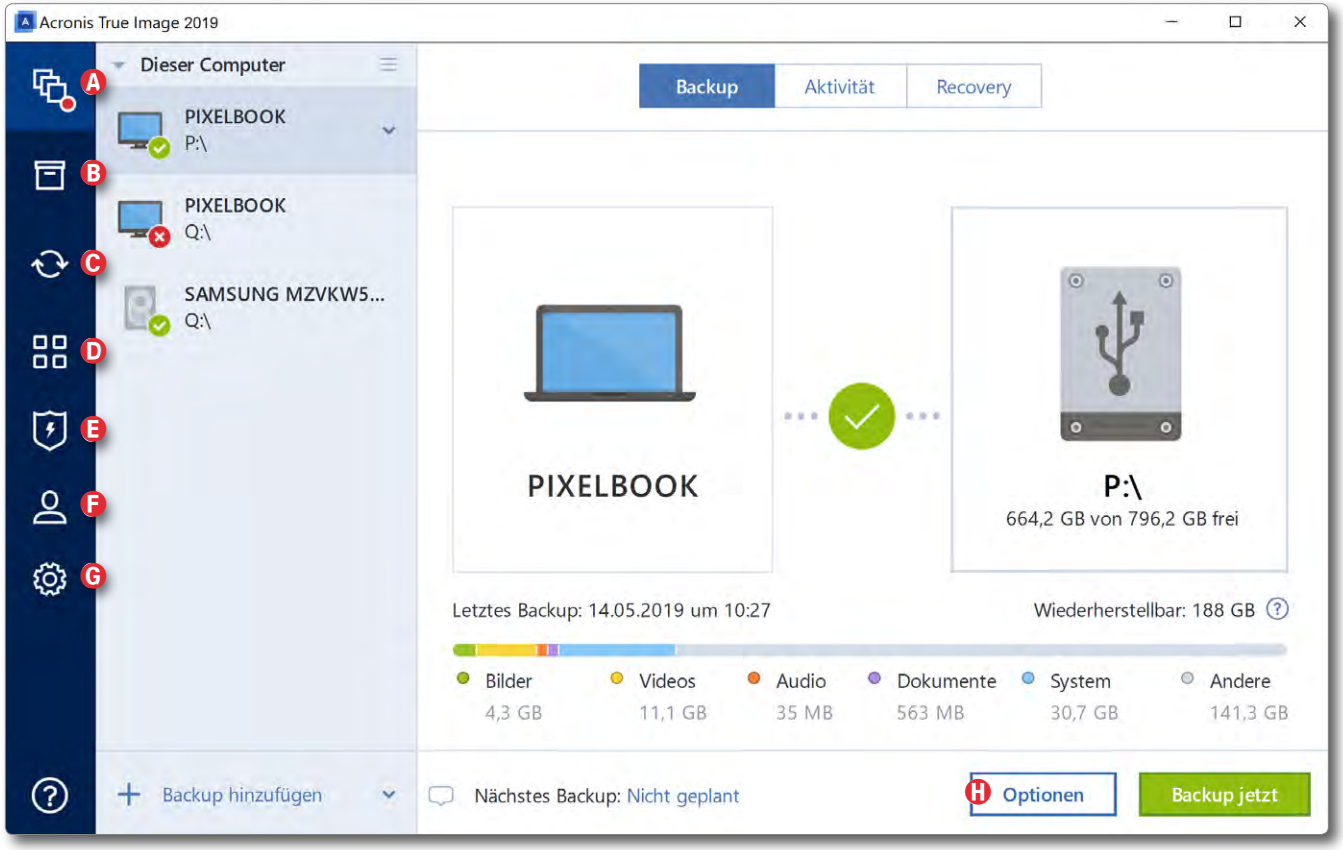


Abb. 1: *Acronis True Image* – hier in der Version 2019 – bietet sehr viele Funktionen in einem Paket. Oft benötigt man davon nur einen kleinen Teil. Die Basisfunktion ist aber die Erstellung von Backups sowie das Wiedereinspielen.

Was die Datensicherung betrifft, ist die Anwendung *True Image* der Firma Acronis [6] ein echtes Allround-Programm. Es erlaubt in der 2018- und 2019-Version eine ganze Reihe verschiedener Dinge:

A. Erstellung eines System-Klons bzw. eines Backups auf ein anderes Volume (ein lokal angeschlossenes Volume, ein NAS-Volume oder in die Cloud)

B. Archivieren. Darunter wird hier verstanden, große und alte (lange nicht genutzte) Dateien auf einen anderen Datenträger auszulagern.

C. Dateien über die *Acronis Cloud* zwischen verschiedenen Systemen (PCs, Smartphones, Tablets) auszutauschen – hier als *Synchronisieren* bezeichnet. Dafür stehen auch spezielle iOS- und Android-Apps zur Verfügung.

D. Eine Reihe von *Extras,* etwa die Erstellung eines Laufwerk-Klons oder die Funktion der Systembereinigung. Eine wichtige Funktion erlaubt (mit dem *Rescue Media Builder*) die Erstellung eines Boot-Mediums (auf CD/DVD, USB-Stick oder USB-Laufwerk), das es bei einem defekten System ermöglicht, eine Art Not- bzw. Hilfssystem zu booten, von dem aus man Acronis-Sicherungen auf das eigentliche Boot-System zurückspielen oder auf einen neuen Windows-Boot-Datenträger bringen kann. Man sollte nach der Erstellung eines solchen Boot-Mediums dieses testen und sich mit dem Wiedereinspielen vertraut machen.

E. *Acronis Active Protection* – eine Art Malware-Erkennung (Erkennung von bösartigen Modulen), die sich im System verankert und fortlaufend aktualisiert wird.

F. *Konto*-Verwaltung – Verwaltung Ihres Acronis-Kontos

G. *Einstellungen* erlaubt z. B. die Sprache der Oberfläche oder den Speicherort von *Mobile Backups* (Sicherung der Daten ihrer Android- und iOS-Geräte) einzustellen.

Jährlich kommen neue (kostenpflichtige) Versionen von *True Image* auf den Markt, jedes Mal mit mehr oder weniger großen Verbesserungen. Häufig reicht aber auch eine etwas ältere Version, die dann online zumeist preisgünstiger zu haben ist. (Der Preis für die 2019-Ein-

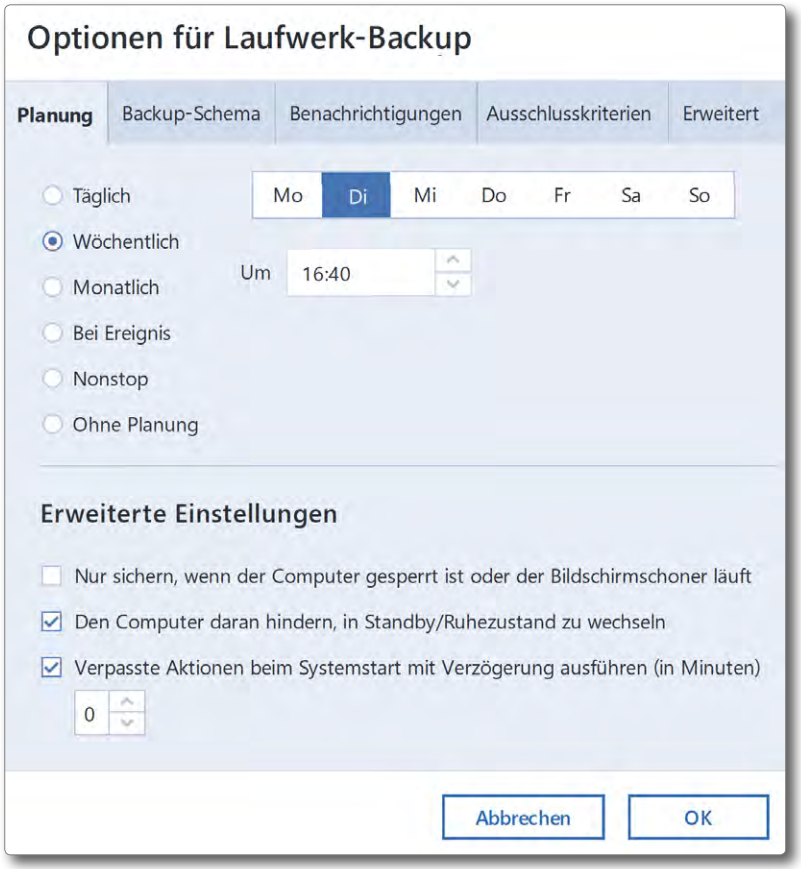


Abb. 2: Unter den *Optionen* (Abb. 1 Ⓗ) findet man eine ganze Reihe von Reitern mit weiteren Einstellungen zu den Backups. Im Reiter *Planung* legt man fest, wann *True Image* jeweils automatisch eine Sicherung erstellt.

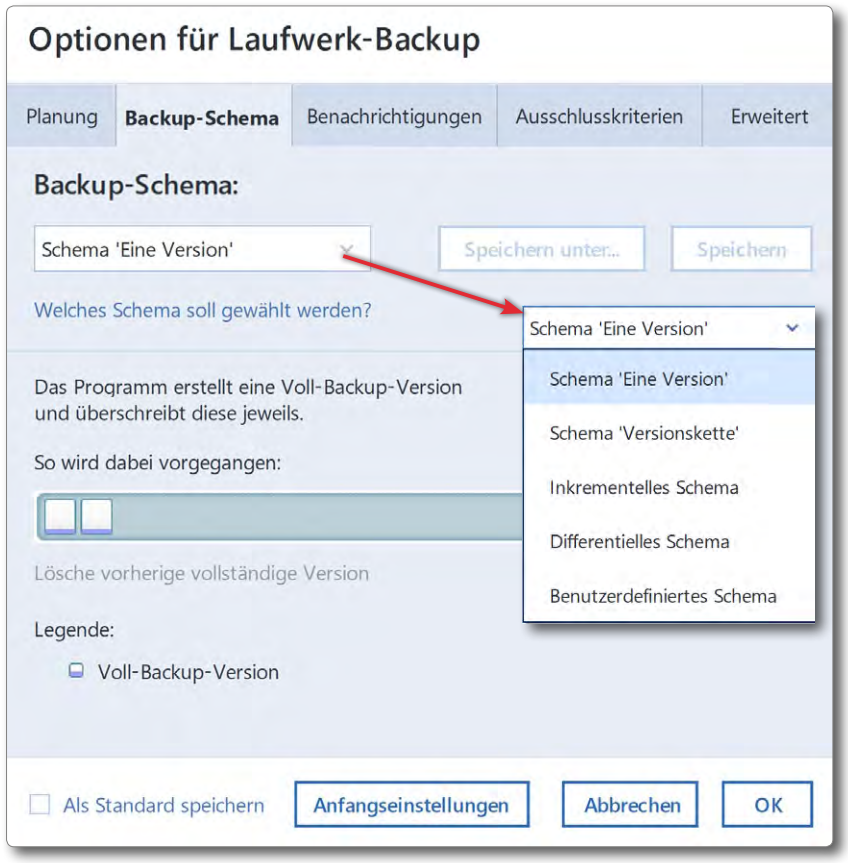


Abb. 3: Für ein Laufwerk-Backup bietet *True Image* verschiedene Schemata.

zellizenz liegt bei ca. 35 Euro, für eine 3er-Lizenz bei etwa 51 Euro).

True Image sichert in der Regel ganze Laufwerke mit allen darauf befindlichen Partitionen/Volumes. Es lassen sich jedoch auch einzelne Verzeichnisse damit sichern. Im Standardfall sichert *True Image* auf dem Zielvolume ähnlich wie *Time Machine* unter macOS alles in eine einzelne Datei – korrekt: in ein spezielles Backup-Objekt. Diese Datei trägt (ohne dass man einen explizi-ten Namen vorgibt, was aber möglich ist) den Namen des Rechners sowie die Art der Sicherung und schließlich die Endung ›.tib‹.

Ablauf

Zunächst verwendet man für ein einfaches Backup das oberste Icon (Abb. 1 Ⓐ), wählt dort das zu sichernde Quelllaufwerk und danach das Zielvolume. Darunter erhält man bereits Informationen zu den zu sichernden Daten und dazu, wie viel Speicher auf dem Zielvolume noch frei ist.

In *Optionen* (Abb. 1 Ⓗ) findet man unter dem Reiter *Planung* (Abb. 2) Einstellungen für eine automatische Backup-Aktivierung – täglich, wöchentlich (und an welchen Tagen), monatlich, bei bestimmten Ereignissen, eine Nonstop-Aktualisierung (in fünfminütigem Abstand) oder auf explizite Anforderung. Hier bleiben wenig Wünsche offen.

Eine ereignisgesteuerte Sicherung kann bei einer Benutzer-An- oder Abmeldung erfolgen, vor dem Herunter- oder nach dem Herauffahren des Systems oder wenn ein Backup-Volume angeschlossen wird.

Unter dem Reiter *Backup-Schema* (immer noch unter den Optionen für das Laufwerk-Backup) findet man verschiedene Backup-Schemata (Abb. 3). Verwendet man die *Versionskette* oder ein *Inkrementelles Schema*, so lässt sich festlegen, nach wie vielen Inkrementen eine neue Komplettsicherung erfolgen soll. Die Legende zeigt dazu, welche Backups schon erstellt wurden. Ich selbst verwende das Schema *Eine Version*, so dass ein einfaches und schnelles Zurückspielen möglich ist. Bei *Differentielles Schema* werden die Änderungen zur letzten Vollsicherung gesichert.

Unter *Benachrichtigungen* (Abb. 4) lässt sich einstellen, wann und wie man bei Problemen oder bei einem normalen Backup über den Vorgang informiert wird – etwa per E-Mail an eine vorgebbare E-Mail-Adresse.

Der Reiter *Ausschlusskriterien* (Abb. 5) gestattet es, bestimmte Arten von Dateien sowie einzelne Dateien und Dateibäume von der Sicherung auszuschließen. So werden im Standardfall die Inhalte der Papierkörbe ausgeschlossen, ›.tmp‹- sowie einige Cache-Dateien nicht gesichert. Auch die Auslagerungsdatei (*Swapfile.sys*) braucht im Normalfall nicht gesichert zu werden, da sie nach dem nächsten Systemstart neu gefüllt wird.

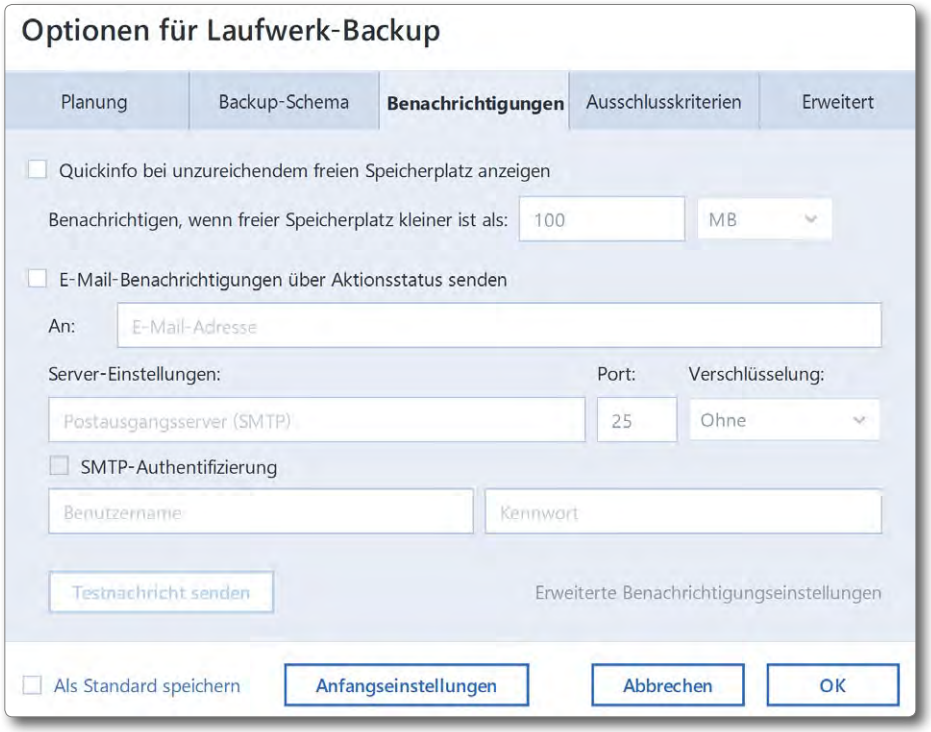


Abb. 4: Hier stellen Sie ein, wie Sie über einen Sicherungslauf informiert werden.

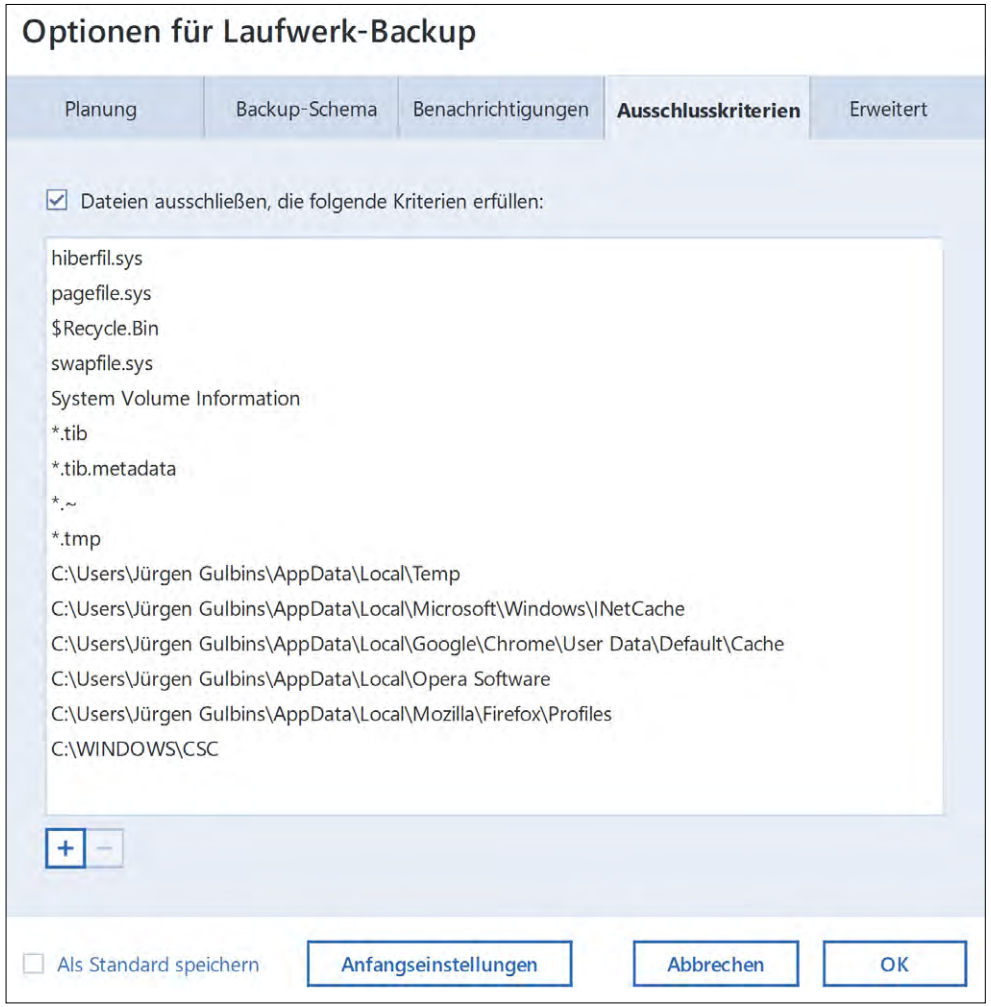


Abb. 5: Unter den *Ausschlusskriterien* legen Sie fest, welche Dateiarten und konkrete Dateien nicht gesichert werden sollen. Die Vorbelegung ist für das C-Laufwerk bereits sinnvoll gesetzt.

Das Panel *Erweitert* bietet eine ganze Reihe von Optionen (Abb. 6), unter *Backup-Schutz* beispielsweise, ob das Backup verschlüsselt werden soll (und mit welchem Passwort). Hier ist es auch möglich, eine Validierung des Backups zu initiieren und festzulegen, ob das System nach Abschluss des Backups automatisch heruntergefahren werden soll. Unter *Erweitert* lässt sich auch gleich eine zweite Backup-Kopie erstellen (hier als *Reservekopie* bezeichnet) – vorzugsweise auf einen weiteren Datenträger.

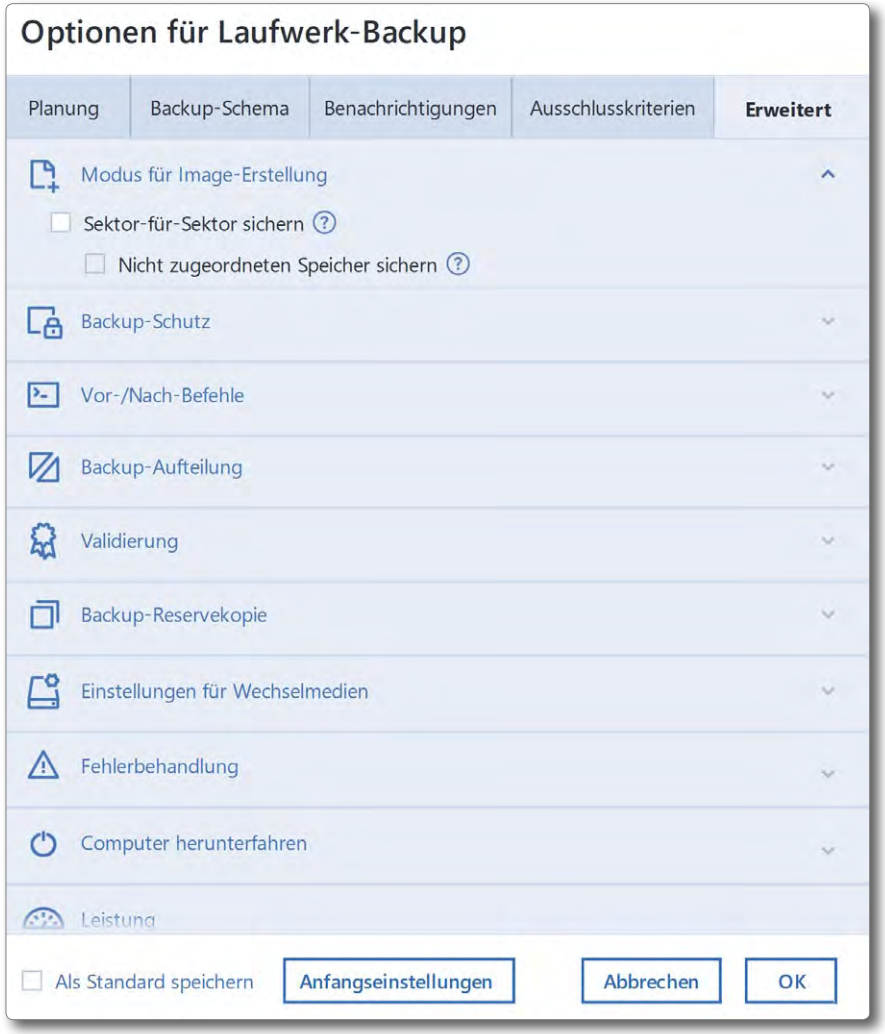


Abb. 6: *Erweitert* bietet eine ganze Reihe weiterer Einstellungen für das Fine-Tuning des Backups. Es lohnt sich, die einzelnen Optionen genauer zu studieren. Es bleiben wenige Wünsche offen.

Hier sind auch (per Skripts) Operationen vor und nach einem Backup einstellbar. Bei einem aufgetretenen Fehler lässt sich sogar automatisch ein weiterer Back-up-Lauf starten. Wie bei *Carbon Copy Cloner* lassen sich Befehle eintragen, die vor und nach einem Backup-Lauf auszuführen sind (was etwas Know-how im Scripting voraussetzt).

Acronis hat für all diese Optionen sinnvolle Vorbelegungen, die für den Standardfall bereits passen sollten, sich aber noch anpassen lassen.

Im Basisfenster zu *Backup* findet man unter dem Reiter *Aktivität* eine Art Protokoll der letzten Aktivitäten und Sicherungsläufe (Abb. 7). Hier findet man unten auch, für wann der nächste Sicherungslauf geplant ist.

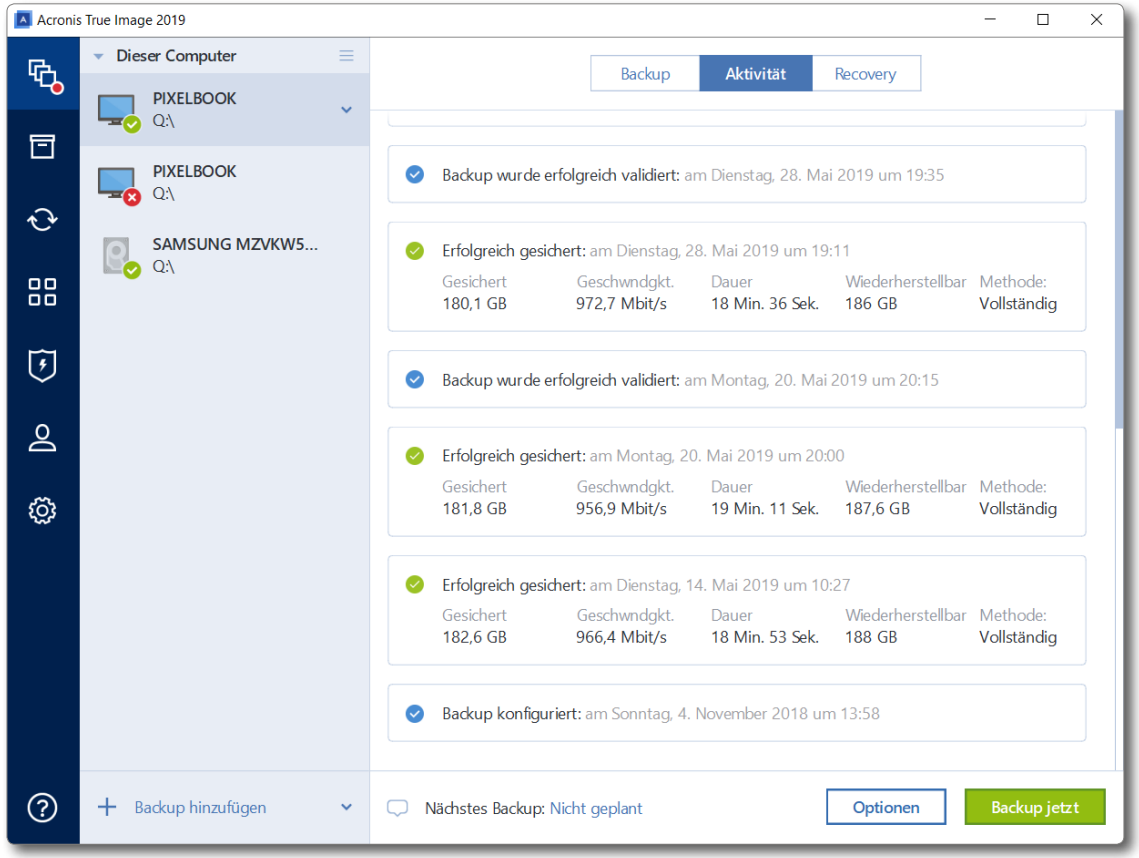


Abb. 7: Im Basisfenster zu *Backup* findet man unter *Aktivitäten* eine Art Protokoll zu den Sicherungsläufen.

Daten zurückspielen

Für das Zurückspielen von Daten aus einem *True-Image*-Backup gibt es mehrere Techniken, deren Einsatz man auf den jeweiligen Bedarf abstimmt. Da *True Image* ein spezielles Backup-Format verwendet, ist der direkte Zugriff und das Kopieren bzw. Übertragen auf das Quell- oder ein anderes Volume nicht mit dem *Explorer* oder ähnlichen Anwendungen möglich, sondern man benötigt *True Image*-Werkzeuge.

Ist das Backup-Image nicht verschlüsselt und komprimiert und möchte man nur einige einzelne Dateien extrahieren, so kann man auch auf die Datei eines Voll-Backups gehen – sie hat die Endung ›*.tib*‹ – und sie per Doppelklick öffnen. Ein weiterer Doppelklick auf das erscheinende Objekt öffnet nun die einzelnen gesicherten Objekte bzw. Ordner. Darin kann man – wir befinden uns sich immer noch im *Explorer* von Windows – zum Ordner navigieren, der das oder die gesuchten Dateien enthält, und von dort die Dateien über das Kontextmenü *Öffnen* oder *Kopieren* – oder man ›kopiert‹ sie per Drag & Drop auf ein anderes Laufwerk.

Möchte man hingegen das gesamte Backup zurückspielen, so wählt man im Basisfenster zu *Backup* den Reiter *Recovery* (Abb. 8).

Dort sucht man unter Ⓐ zunächst die gewünschte Sicherung bzw. den Sicherungsstand. Nun kann man entweder alles zurückspielen oder selektiert im Fenster Ⓑ (und eventuell Ⓒ) die Verzeichnisse (oder nur die Dateien), die man wiederherstellen möchte. Natürlich

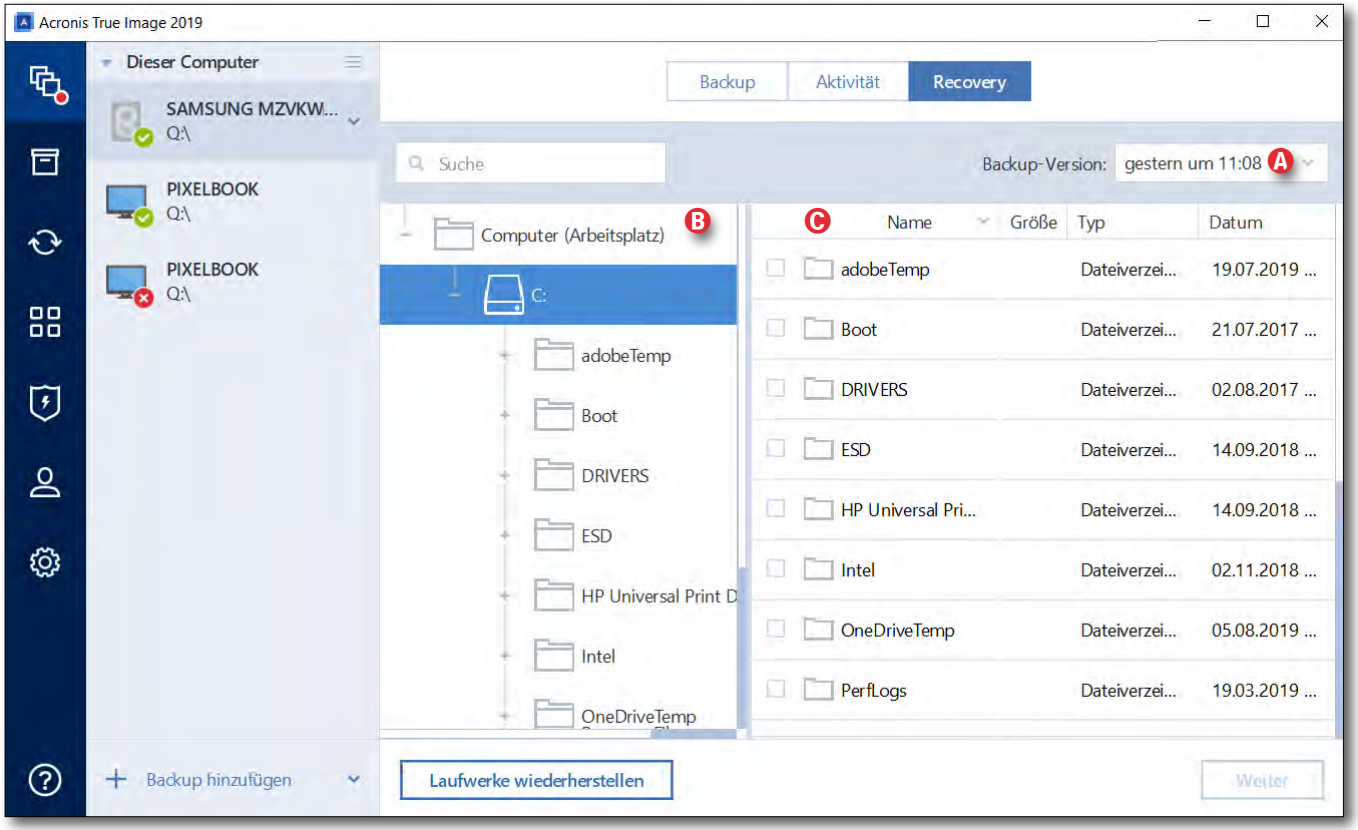


Abb. 8: Zum Zurückspielen ganzer Sicherungen/Laufwerke verwendet man die *Recovery*-Funktion von *True Image*.

kann man dabei Systemkomponenten eines gerade aktiven (laufenden) Systems **nicht** überschreiben. Sind wirklich wesentliche Teile des Betriebssystems wiederherzustellen, so ist dies im normalen Betrieb nicht möglich. Dafür muss man zunächst ein Hilfssystem booten – hier als *Rescue Media* bezeichnet – das man zuvor in ›guten Zeiten‹ angelegt haben sollte. Dieses mit *True Image* angelegte *Rescue Media*-System enthält auch eine Version von True Image. Mit dessen Hilfe lasse sich dann Systemkomponenten auf das ursprüngliche (oder ein neues) Systemlaufwerk (das zu diesem Zeitpunkt nicht als System aktiv ist) zurückspielen.

Unkritische Komponenten, etwa einzelne Benutzerdateien oder -verzeichnisse, kann man jedoch auswählen und auf *Weiter* klicken. Man wird dann in wenigen Schritten durch den Wiederherstellungsprozess (das *Recovery*) geleitet. Dabei kann man noch einige Recovery-Optionen setzen – etwa dass das Backup vor der

Wiederherstellung validiert und/oder dass das Dateisystem nach der Wiederherstellung geprüft werden soll.

Es ist etwas verwirrend, dass hier statt der deutschen Namen für Verzeichnisse die englischen Datei- oder Verzeichnisnamen angezeigt werden (etwa *Pictures* statt *Bilder* und *Users* für das Verzeichnis *Benutzer*).

Erstellt man mit *True Image* unter der Funktion *Extras* (Abb. 1 Ⓓ, Seite 94) mit der Funktion R*escue Media Builder* ein WinPE-Boot-Medium, so befindet sich darauf auch eine Acronis-Version, die es erlaubt, ein System-Backup (durch Acronis) auf das ursprüngliche oder ein neues Systemlaufwerk zu spielen. Für den Fall, dass ein System nicht mehr bootfähig ist, stellt dies eine Möglichkeit dar, das defekte System zu reparieren.

Zusammenfassung

Insgesamt erweist sich *True Image* als gut durchdacht, hat zahlreiche Einstellungen für besondere Fälle und zumeist sinnvolle Vorbelegungen.

Angesichts der vielen Möglichkeiten, die manchen Anwender zumindest anfänglich etwas verwirren könnten, sollte man sich Zeit nehmen, um all die Optionen zu studieren. Obwohl Acronis jährlich neue Versionen mit mehr oder weniger relevanten Verbesserungen auf den Markt bringt, kann man in den meisten Fällen mit einer Version zwei oder sogar drei Jahre auskommen, ohne ein kostenpflichtiges Update vorzunehmen.

Verwendet man *Acronis True Image* zum Sichern seines (Betriebs-)Systems – darin liegen seine eigentlichen Stärken –, so sollte man zu Beginn auf jeden Fall einen Boot-Stick oder eine Boot-CD/DVD erstellen.

Dies erfolgt unter dem *Extras*-Icon von Abb. 1 Ⓓ mit der Funktion *Rescue Media Builder* (unter Nutzung von *WindowsPE*). Der Vorgang ist recht einfach. Man muss lediglich eine beschreibbare (noch leere) CD oder DVD zur Verfügung stellen (und entsprechend im Dialog wählen) oder einen ausreichen großen (ca. 16 GB) USB-Stick. Dieser sollte als ExtFat formatiert sein. Sein eventuell vorhandener Inhalt geht verloren und wird mit dem *Rescue Media*-System überschrieben.

Um Sicherungen auf einem anderen Rechner, eventuell mit abweichender Hardware, einspielen zu können, verwendet man statt des *Rescue Media Builders* die Acronis-Funktion *Universal Restore*.

Im Notfall, wenn sich das System nicht mehr problemlos starten lässt, kann man dann dieses Medium booten. (Dazu muss man in aller Regel den Boot-Prozess unterbrechen und das erwähnte Medium als Boot-Laufwerk einstellen.) Auf dem Medium (*Rescue Media* oder *Universal Restore*) findet man dann auch eine vereinfachte Version von *True Image*, die das Restaurieren von Dateien oder eines ganzen Systems erlaubt – etwa auch auf ein Ersatzlaufwerk.

Eine Alternative ist das *Acronis Survival Kit*. Die Erstellung findet sich ebenfalls unter *Extras* (in Abb. 1 Ⓓ). Das Survival Kit enthält drei wesentliche Dinge: ein bootfähiges Minisystem sowie Acronis und schließlich die gesicherten Daten des ursprünglichen Systems. Dafür benötigt man in aller Regel ein externes USB-Laufwerk.

Auch das Klonen eines Laufwerks ist eine der zahlreichen Funktionen von *Acronis True Image*. Handelt es sich dabei um das Systemlaufwerk, so kann man es bei Bedarf einsetzen, um das ursprüngliche Systemlaufwerk bei einem Defekt zu ersetzen. Oder man verwendet es, um ein System von einem Festplattenlaufwerk auf eine SSD zu migrieren.

Wie üblich habe ich hier nur eine Art Überblick über die zahlreichen Funktionen von *Acronis True Image* und deren Optionen gegeben und viele Details ausgelassen. Das recht gute (deutschsprachige) Online-Handbuch erläutert aber den Rest. Zusätzlich findet man einige Video-Tutorials unter der Programmhilfe, von denen aber die meisten in Englisch sind.

Kostenlos, recht funktional und zudem (auch) mit deutscher Oberfläche ist *FreeFileSync* [4], ein Open-Source-Programm. Diese Anwendung, die für Windows, macOS sowie Linux zur Verfügung steht, erlaubt Ordner und einzelne Dateien zu ›synchronisieren‹. Die Anwendung kann jedoch nur recht eingeschränkt den Inhalt ganzer Volumes klonen (es fehlen ihr dabei oft die entsprechenden Zugriffsrechte); und sie kann keine bootbare Partitionen/Volumes erstellen. Beschrieben wird hier Version 10.13 unter Windows 10.

Ich liefere eine vereinfachte Beschreibung und lasse viele weitere Möglichkeiten aus – etwa die *Realzeitsynchronisation*, die eine ständige Synchronisierung im laufenden Betrieb erlaubt (was in einem gewissen Umfang einem RAID 1 gleichkommt, wenn auch mit etwas mehr Verzögerung).

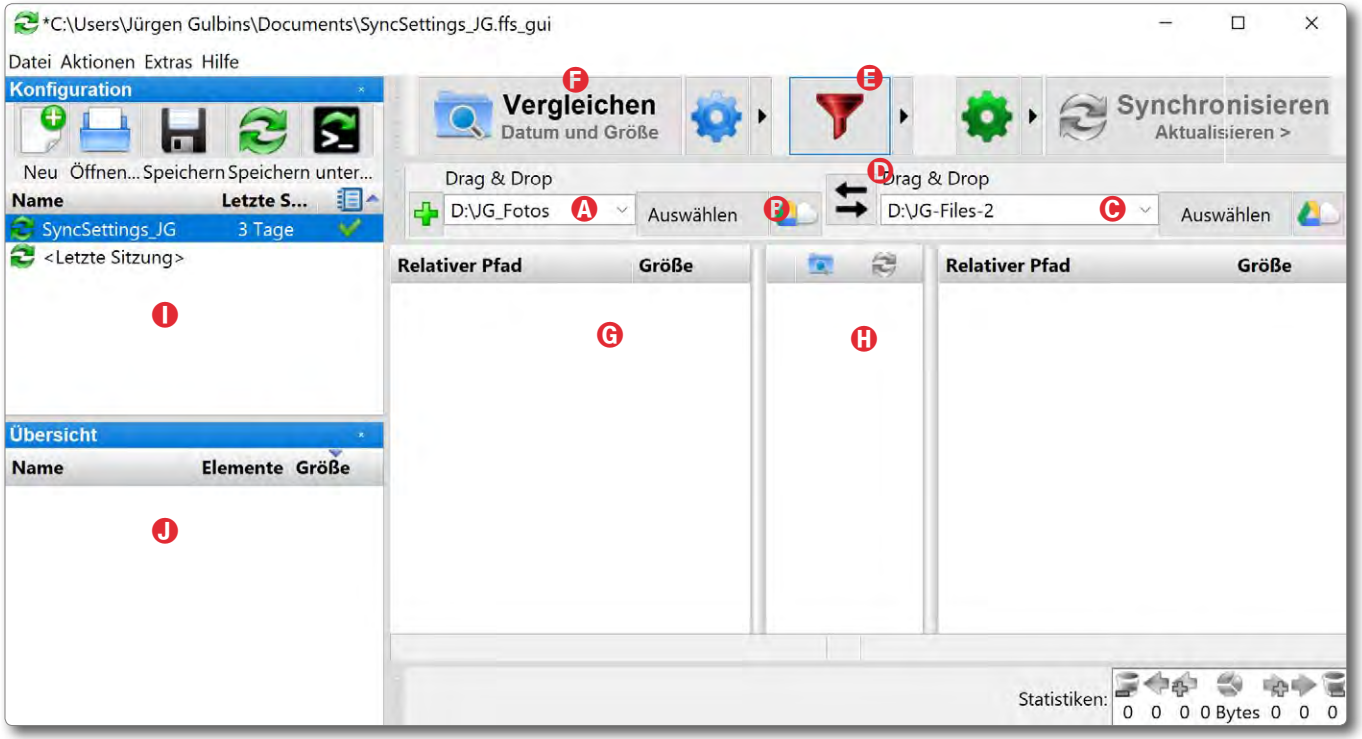


Abb. 1: Das Fenster von *FreeFileSync*. Unter Ⓐ legt man die Quelle fest, unter Ⓒ das Ziel und unter Ⓓ die Richtung oder Richtungen zum Synchronisieren. Unter Ⓔ lässt sich im *Filter* festlegen, welche Dateien beim Abgleich ignoriert werden sollen.

FreeFileSync (hier teils mit FFS abgekürzt) ist zum Synchronisieren sowohl einzelner Dateien als auch ganzer Ordner (Ordnerbäume) gedacht. Der Inhalt ganzer Volumes lässt sich nur dann sichern, wenn dafür die Zugriffsrechte des aufrufenden Anwenders ausreichen – was für ein aktives Startvolume nicht der Fall ist. Dafür benötigt man andere Anwendungen wie etwa *Acronis True Image* und erweiterte Zugriffsrechte (die *True Image* beim Programmstart jeweils anfordert und vom Anwender bestätigen lässt). FFS überträgt die Daten als einzelne Dateien auf das Zielvolume. Man kann also dort direkt und ohne eine spezielle Anwendung darauf zugreifen. Im Standardfall werden auch die Zugriffsrechte und das Erstellungs- und Änderungsdatum dieser Dateien mit übernommen.

Die Oberfläche von *FreeFileSync* ist zwar deutsch (bzw. zeigt sich auf einem deutschen Windows standardmäßig als Deutsch und lässt sich unter Extras ▸ Sprache auf eine ganze Reihe weiterer Sprachen umstellen), die Online-Hilfe mit den detaillierten Funktionsbeschreibungen ist aber (leider) in Englisch.

Ablauf

Nach dem Start von FFS wählt man im FFS-Fenster zunächst unter Ⓐ die Quelle, die man sichern/synchronisieren möchte. Dies ist sowohl per Drag&Drop aus dem Explorer heraus möglich als auch über einen kleinen Datei-Browser, den man über den Knopf Ⓑ *Auswählen* aufruft. Ein Klick auf das Cloud-Icon erlaubt den Zugriff auf einen Online-Speicher – etwa Google Drive oder einen Speicher, auf den man per FTP oder SFTP zugreift (man muss dann natürlich ein Benutzerkonto und eventuell ein Passwort dafür angeben). Als Nächstes wählt man unter Ⓒ in gleicher Art das Ziel aus.

Unter Ⓔ lassen sich Filterregeln vorgeben (Abb. 2). Man nutzt dies, um bestimmte Dateien oder Dateitypen – definiert durch ein Namensmuster – von der Synchronisierung auszuschließen, etwa den Papierkorb *(\$Recycle.Bin\)*. FFS kommt hier bereits mit einigen

sinnvollen Vorbelegungen einher, die sich aber ergänzen oder ändern lassen.

Als Nächstes klickt man auf Ⓕ *Vergleichen*. FFS vergleicht damit die Dateien in der Quelle mit jenen des Ziels (unter Berücksichtigung der Ausschlüsse durch den Filter) und listet das Ergebnis in den Feldern Ⓖ, Ⓗ und Ⓘ auf (Abb. 3). Die Symbole in der Spalte Ⓗ zeigen, in welche Richtung synchronisiert wird (dies ist auch abhängig von den Einstellungen unter *Synchronisieren*).

Grüne Pfeile signalisieren, dass die betreffende Datei zum ersten Mal übertragen wird; graue Pfeile zeigen, dass es sich um eine erneute Synchronisation handelt. Selbst das zu übertragende Datenvolumen wird angezeigt. Es lassen sich dann hier (optional) noch einzelne Dateien von der Übertragung ausschließen. Dies erfolgt, indem man per Klick auf das Übertragungshäkchen **neben der Datei die Übertragung deaktiviert**.

Synchronisationsfunktionen stehen unter dem -Icon zur Verfügung (oder über F8). Sie legen fest, in welcher Richtung synchronisiert (übertragen) wird. Mit *Spiegeln* wird ausschließlich von der Quelle (im Feld Ⓐ/Ⓖ) zum Ziel (im Feld Ⓒ/Ⓘ) übertragen. Bei *Zwei Wege* wird jeweils in beiden Richtungen synchronisiert, wobei die neuere Datei die ältere (oder noch nicht vorhandene) ersetzt. Mit *Aktualisieren* werden links vorhandene neue Dateien und dort geänderte Dateien in das Ziel übertragen.

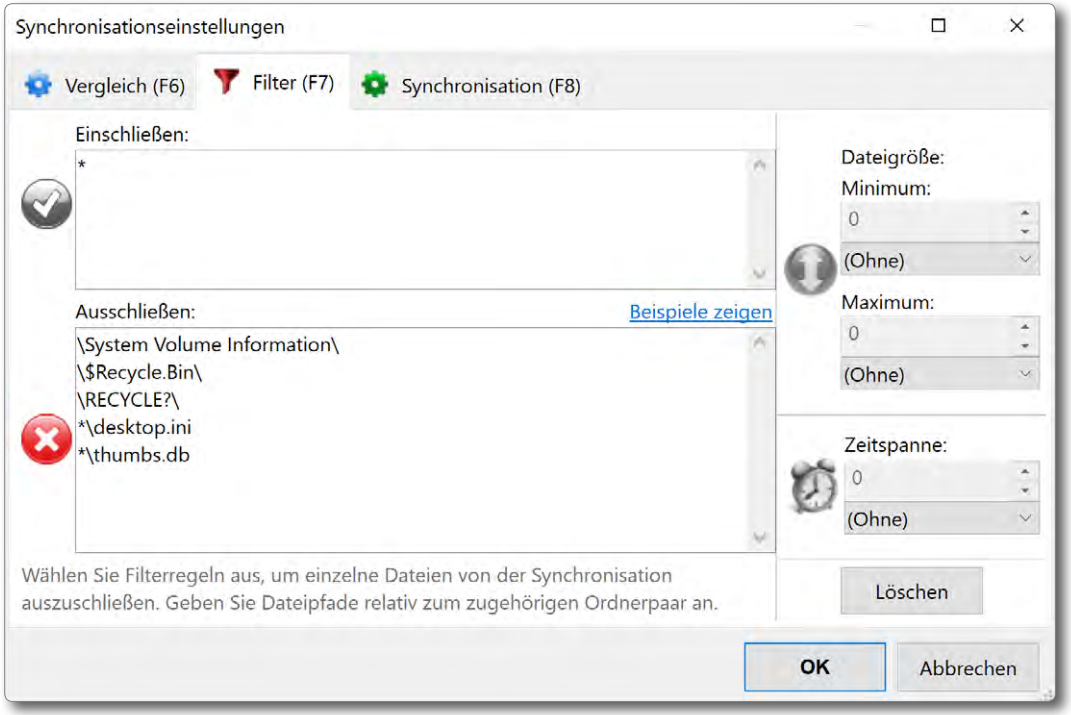


Abb. 2: Unter *Filter* geben Sie an, welche Dateien gesichert werden sollen – * bedeutet ›alles‹ – und welche ausgeschlossen werden.

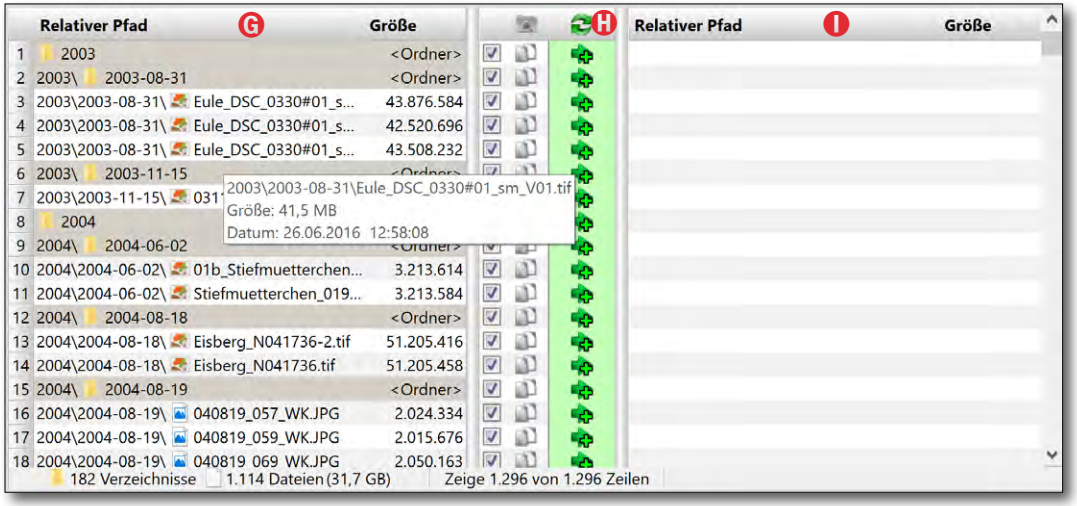


Abb. 3: Nach dem Vergleich findet man unter Ⓖ die Dateien, die von der Quelle (links) zum Ziel Ⓘ (oder umgekehrt) übertragen werden. Unter Ⓗ findet man die Übertragungsrichtung.

Muss eine Datei ersetzt/überschrieben werden, so lässt sich hier angeben, ob sie im Papierkorb landen, gleich ganz (permanent) gelöscht und ob eine Versionierung stattfinden soll. Zusätzlich lässt sich hier im Reiter *Synchronisieren* vorgeben, was nach Abschluss der Synchronisierung erfolgen soll – etwa den Rechner herunterfahren.

Geht man auf die einzelnen Icons, so liefert FFS dazu einen kleinen Tooltipp. Mit OK schließt man dieses Einstellungsfenster.

Zurück im Hauptfenster (Abb. 1) startet ein Klick auf das Synchronisieren-Icon oder F9 schließlich den Datenabgleich (die Synchronisation).

Hat man einen Synchronisationsauftrag zusammengestellt und möchte diesen häufiger ausführen, was für ein regelmäßiges Backup etwa des eigenen Bildbestands typisch ist, so sollte man über das Speichern-Icon (oder per Strg-S) den Auftrag unter einem sinnträchtigen Namen als Sicherungsauftrag mit allen Einstellungen speichern.

Legt man diese Auftragsdatei auf dem Desktop ab – sinnvoller noch in einem Unterordner des Desktops[1] –, so lässt sich *FreeFileSync* per Doppelklick auf diese Auftragsdatei starten und mit den eingestellten Parametern ausführen.

1 Es empfiehlt sich, die Anzahl der Objekte auf dem Desktop gering zu halten. Dies sorgt nicht nur für mehr Übersicht, sondern trägt auch zu einer höheren Geschwindigkeit des Systems bei.

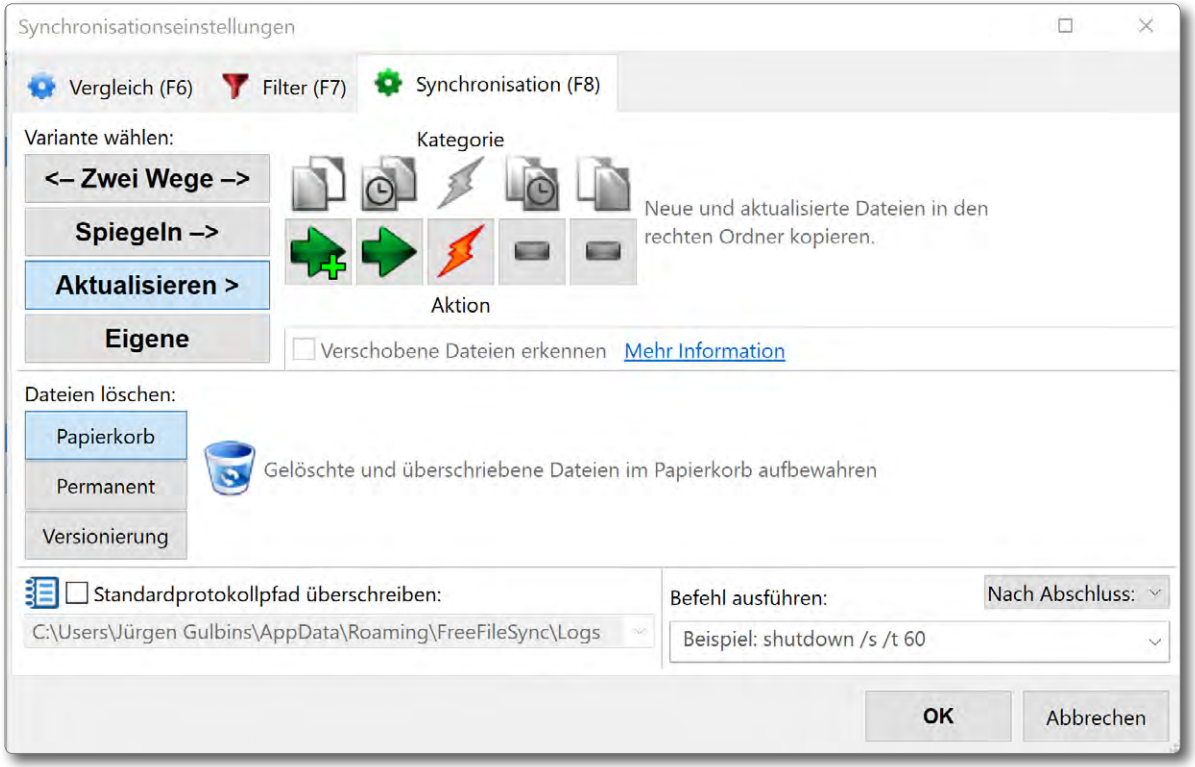


Abb. 4: Unter dem Reiter *Synchronisation* legt man fest, wie der Datenabgleich erfolgen soll und wie zu löschende oder zu ersetzende Dateien behandelt werden sollen.

Für die Prüfung der Objekte in Quelle und Ziel lässt sich unter den Vergleichseinstellungen, die man z. B. über F6 oder das -Icon aufruft, festlegen, ob das Änderungsdatum zusammen mit der Dateigröße, nur die Dateigröße oder – relativ aufwändig – der gesamte Dateiinhalt herangezogen (verglichen) werden soll. In aller Regel nimmt man *Datum und Größe*.

Viele der Funktionen/Operationen von FFS lassen sich sowohl über das Hauptmenü unter *Aktionen* anstoßen als auch per Klick auf ein betreffendes Icon und alternativ auch per Funktionstasten (sofern diese nicht vom Betriebssystem anderweitig belegt sind). So zeigt F4 das letzte Protokoll, F5 ruft den Vergleich auf, F6 zeigt die Vergleichseinstellungen, F7 die Filtereinstellungen, F8 die Synchronisationseinstellungen – und F9 startet das Synchronisieren.

Bei länger laufenden Operationen wird der Fortgang in der Titelleiste des Hauptfensters angezeigt und über ein eigenes Fenster mit dem Fortschritt (Abb. 5), das man aber ausblenden kann. Darin lässt sich der Vorgang auch anhalten (Klick auf *Pause*) und später wieder fortsetzen oder ganz abbrechen.

Eine weitere Möglichkeit zur Steuerung von FFS sind Shell-Skripte. Sie erfordern aber etwas Know-how zu

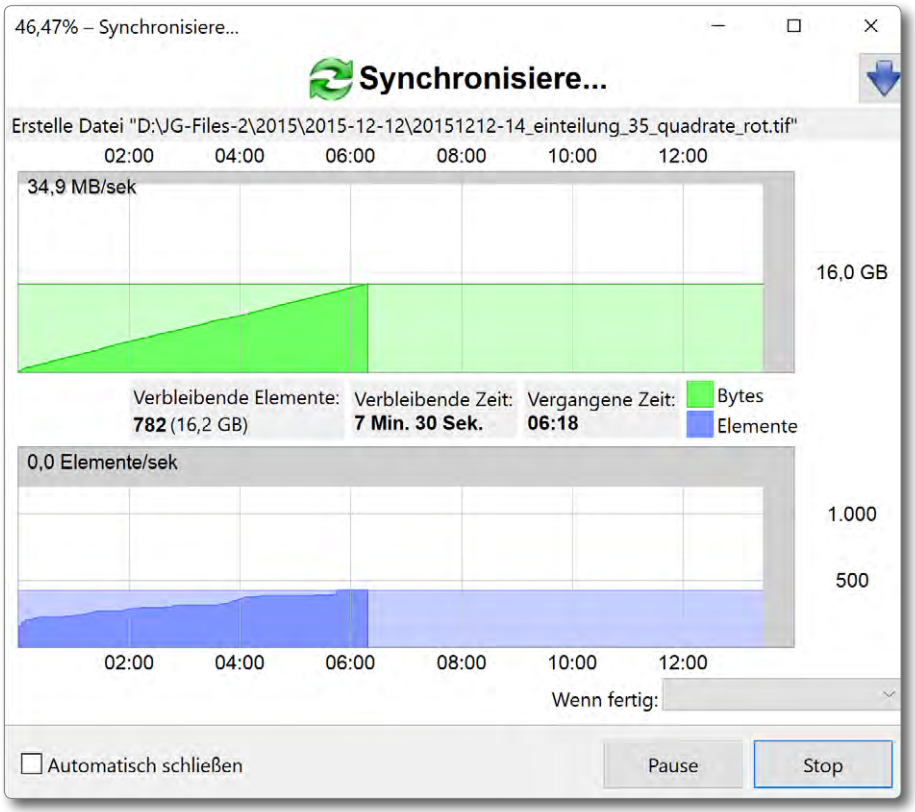


Abb. 5: Während des Synchronisationslaufs zeigt ein Fenster den Fortschritt an mit einer Abschätzung, wie lange der Datenabgleich noch laufen wird.

Skripten und Kommandozeilen. Für einen Systemadministrator mit entsprechenden Kenntnissen ist diese Technik jedoch praktisch. Auch diese Schnittstelle ist brauchbar beschrieben, jedoch nur in Englisch.

Daten zurückspielen

Da FFS die Dateien einzeln und ohne spezielles Format im Ziel ablegt (unverschlüsselt und unkomprimiert), kann man auch mit normalen Mitteln darauf zugreifen – entweder direkt auf dem Zielvolume oder indem man einzelne Dateien oder ganze Dateibäume im *Explorer* (bzw. unter macOS mit dem Finder) vom Zielvolume auf das Quellvolume kopiert, sollten einmal einzelne Dateien oder Verzeichnisse versehentlich gelöscht worden sein.

Möchte man mehr als ein paar Dateien (zurück-)übertragen, so lässt sich ebenso ›rückwärts synchronisieren‹, also vom ehemaligen Sicherungsziel zur ehemaligen Sicherungsquelle. Dies ist vollständig oder – mit entsprechend angepassten Einstellungen – auch nur partiell möglich. Im einfachsten Fall schaltet man die Synchronisation dann auf *Zwei Wege*. Alternativ vertauscht man Quelle und Ziel, z. B. per Klick auf das Icon im Hauptfenster.

Über das -Icon lässt sich ein Sicherungsauftrag auch als Batchauftrag sichern (Abb. 6), den man dann entweder wieder per Doppelklick aktiviert oder den man dem Windows-Taskplaner zur einmaligen oder wiederholten Ausführung übergibt; man muss sich dann aber ein wenig mit dem Windows-**Taskplaner** beschäftigen. Andere Anwendungen wie *Acronis True*

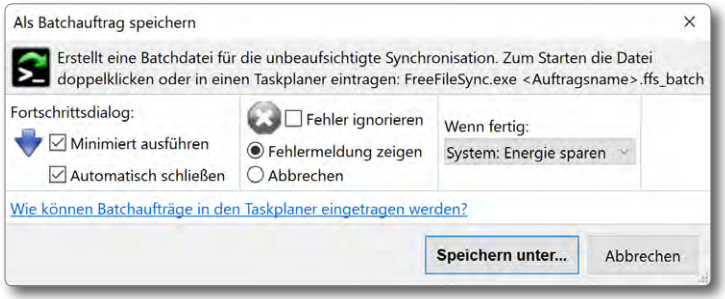


Abb. 6: Beim Speichern als Batchauftrag lässt sich ein Lauf auch ohne Fenster ausführen.

Image oder *Carbon Copy Cloner* und *SuperDuper!* (Letztere beide auf dem Mac) lösen dies eleganter.

Man kann *FreeFileSync* auch dazu nutzen, um zwei Verzeichnisse zu vergleichen. Man verwendet dann lediglich die Funktion *Vergleichen,* verzichtet auf die Synchronisation und erhält eine Liste von Unterschieden, die sich ausgeben lässt.

Wie bei den anderen Backup-Anwendungen habe ich auch hier nur die Basisfunktionen und nicht alle Feinheiten beschrieben. Es sollte jedoch erkennbar sein, was die Vorteile von *FreeFileSync* sind und was man damit tun kann.

Wer *FreeFileSync* in einem Videotutorial vorgeführt sehen möchte, findet eines unter YouTube hier: https://www.youtube.com/watch?v=wpzuBbrFI6E&app=desktop

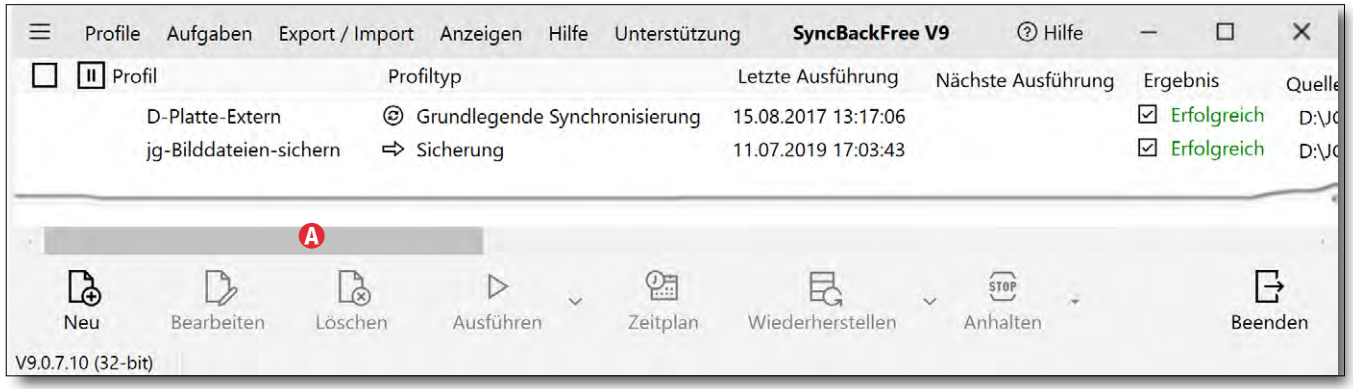


Abb. 1: Das Startfenster von *SyncBackFree*, hier bereits mit zwei definierten Aufträgen. Zieht man den Scrollbalken Ⓐ nach rechts, werden weitere Informationen sichtbar – etwa von wo nach wo gesichert wird.

Ein weiteres recht schönes und ebenfalls kostenloses Werkzeug zur Datensicherung unter Windows ist *SyncBackFree* der Firma *2BrightSparks* [21]. Die Anwendung gibt es in drei Versionen:

- *SyncBackFree* (kostenlos sowohl für den privaten als auch für den kommerziellen Einsatz),
- *SyncBackSE* (ca. 44 Euro) sowie
- *SyncBackPro* (ca. 61 Euro).

Während *SyncBackFree* offensichtlich eine 32-Bit-Version ist (die aber unter 64-Bit-Windows problemlos arbeitet), gibt es *SyncBackSE* und *SyncBackPro* sowohl als 32- als auch als 64-Bit-Software (zum gleichen Preis). Die SE-Version und Pro-Versionen bieten jeweils erweiterte Funktionen, etwa die Sicherung aktuell geöffneter oder ›gelockter‹ Dateien unter Verwendung von VSS (siehe dazu Seite 76). Beide Versionen dürfen für den genannten Preis auf bis zu fünf Systemen installiert werden. Alle Versionen können Sicherungen auch über ein Netzwerk hinweg vornehmen. Alle drei Versionen unterstützen Windows 7, 8 und 10. Für die meisten Fotografen dürfte *SyncBackFree* ausreichen, dessen Version 9 ich hier in einer Kurzform beschreibe. Die Oberfläche ist deutsch, die Online-Hilfe leider nur englisch.

Die Funktion von *SyncbackFree* besteht darin, Dateien bzw. den Dateibaum eines Ordners zu sichern (zu synchronisieren), nicht hingegen ganze Laufwerke oder Volumes. Möchte man beispielsweise all seine Bilddateien mit *SyncBack* sichern, so ist es vorteilhaft, wenn die Bilder möglichst alle in einem einzigen Dateibaum oder in einer kleinen Anzahl von Dateibäumen liegen. (Gleiches gilt übrigens auch beim Einsatz von *FreeFileSync*.)

SyncBack arbeitet mit den Rechten des Anwenders und kann deshalb nicht ohne weiteres Dateien anderer Anwender sichern (sofern deren Ordner und Dateien nur dem Besitzer Zugriffsrechte erteilen). Die Anwendung bietet sowohl einen einfachen als auch einen Expertenmodus an (zu wählen unter dem ☰-Icon im Fenster links oben). Ich beschreibe hier den einfachen Modus.

Zum Sichern der Lightroom-Daten (der Bibliotheken und der Dateibäume mit den Bildern) oder ähnlicher fotografischer Anwendungen sowie anderer üblicher Benutzerdaten unter Windows (7/8/10) ist *SyncBackFree* sehr gut geeignet – hier der prinzipielle Ablauf.

1. Zunächst erstellt man – per Klick auf das Neu-Icon (Abb. 1 in der Fußzeile) ein sogenanntes *Profil* und gibt ihm einen beschreibenden Namen. Im Profiltyp wird festgelegt, wie gesichert werden soll. Für das Sicherungsverfahren gibt es drei Varianten:
   - *Sichern* kopiert (nur) von der Quelle ins Ziel;
   - *Synchronisieren* (Abgleich von Quelle und Ziel);
   - *Spiegeln* (Abgleich, so dass das Ziel der Quelle entspricht; in der Quelle gelöschte Dateien werden auch im Ziel gelöscht).

2. Dabei gibt man im nächsten Schritt sowohl die Quelle als auch das Ziel an sowie ob lokal oder über Netz gesichert wird (sowohl bei der Quelle als auch beim Ziel) – es können also auch Daten von Remote-Systemen gesichert werden.

3. Hat man das Profil gesichert, so lässt es sich auswählen und damit (optional) ein Testlauf ausführen. Passt dessen Ergebnis, führt man den eigentlichen Sicherungslauf aus. Dabei wird ein Protokoll erstellt, das sich später über *Aufgaben* abrufen lässt.

4. Ist die erste Sicherung erfolgreich, sollte man für den nächsten Lauf per Klick auf das Zeitplan-Icon die Zeitplanung für den nächsten Lauf vornehmen.

Es gibt zwei Arten von Profilen: ein normales Profil sowie ein Gruppenprofil. In einem Gruppenprofil lassen sich mehrere normale Profile aufnehmen; sie werden dann automatisch nacheinander abgearbeitet.

SyncbackFree bietet bereits in der Free-Version eine zeitgesteuerte Ausführung, was eine automatische Sicherung erlaubt. Dies ist selbst dann möglich, wenn der Anwender zu diesem Zeitpunkt nicht angemeldet ist. Man muss dazu aber das Benutzerpasswort im Profil hinterlegen, was ein gewisses Sicherheitsrisiko darstellt.

Wie viele andere Backup-Lösungen erstellt *SyncBackFree* bei Ausführung ein Protokoll. Um es anzuzeigen, wählt man im Hauptfenster zunächst den betreffenden Auftrag, klickt dann auf *Aufgaben* und wählt im erscheinenden Fenster (Abb. 2) *Protokoll anzeigen*.

Abb. 2: Unter *Aufgaben* findet man das Anzeigen des letzten Protokolls.

Die Funktionen zum Öffnen der Quelle oder des Ziels öffnen den *Explorer* mit dem betreffenden Verzeichnis in der Ansicht. So lassen sich dort einzelne Dateien oder Ordner löschen, kopieren, verschieben …

Daten/Dateien wiederherstellen

Da *SyncBackFree* im Ziel normale Dateien und Ordner ablegt, lässt sich auch normal darauf zugreifen. Möchte man mehrere Dateien restaurieren, so selektiert man den Auftrag und ruft *Wiederherstellen* auf (zu finden in der Fußzeile des Hauptfensters). Dort werden über das kleine Menü drei Varianten angeboten:

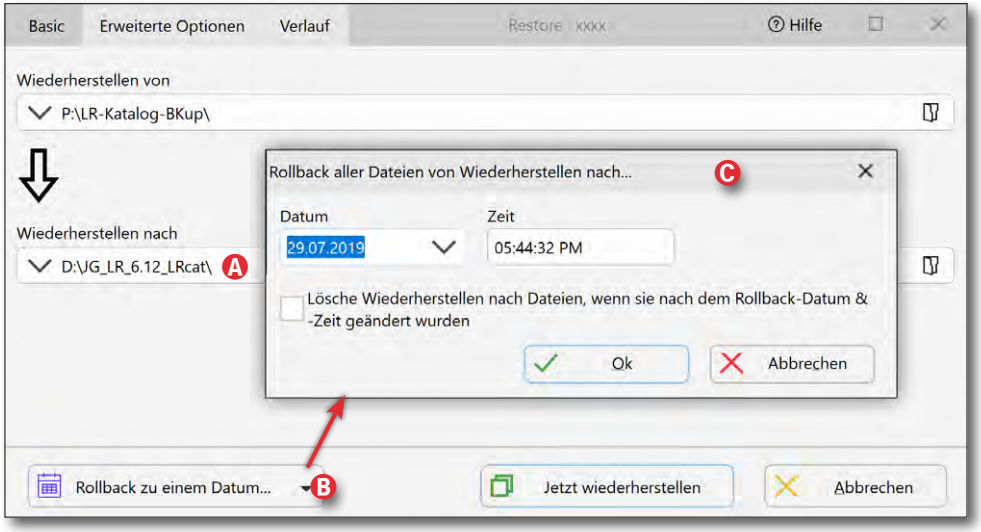


Abb. 3: Im Wiederherstellungs-/Restore-Fenster lässt sich unter Ⓐ das Zielverzeichnis ändern sowie unter *Rollback zu einem Datum* Ⓑ ein Wiederherstellungszeitpunkt auswählen Ⓒ.

Das Wiederherstellungsfenster (Abb. 3) erlaubt im unteren Bereich das (Wiederherstellungs-)Ziel zu ändern, so dass es möglich ist, die Wiederherstellung an einem anderen Ort durchzuführen.

Da *SyncBackFree* auch eine Versionierung betreibt, erlaubt das **Wiederherstellungsfenster, die Wiederherstellung** auf den Stand eines bestimmten Datums (des entsprechenden Sicherungslaufs) zu bringen. Diese Funktion wählt man über den Kopf *Rollback zu einem Datum* Ⓑ und erhält dann ein Auswahlfenster (wie in Abbildung 3 gezeigt).

Zusammenfassung

SyncBackFree ist eine einfache, aber übersichtliche und funktionale Anwendung, die ihre Aufgaben problemlos und sauber ausführt und zusätzlich eine nette kleine Wiederherstellungsfunktion bietet. Einige Menüs und Angaben und Pop-up-Meldungen sind leider nicht vollständig ins Deutsche übersetzt (was aber funktional kaum stört), und die Online-Hilfe würde man sich auch noch in Deutsch wünschen.

Datensicherung per Personal Backup

Der Name *Personal Backup* mag täuschen; es handelt sich um eine originäre deutsche Implementierung von Dr. J. Rathlev. Sie ist kostenlos einsetzbar (auch im kommerziellen Bereich), und dies nicht nur auf normalen PCs (unter Windows), sondern auch auf Windows-Servern. *Personal Backup* [29] gibt es als 32- und als 64-Bit-Version. Es unterstützt auch ältere Windows-Systeme, ist aber für Windows 7, 8 und 10 optimiert.

Die Anwendung ist auf die Sicherung von normalen Ordnern (Verzeichnissen) ausgelegt und nicht auf die des Betriebssystems, kann aber auch mit Administrationsrechten laufen. *Personal Backup* ist gut durchdacht und wird ständig gepflegt. Es kann die Sicherung sowohl auf lokale Datenträger ablegen als auch im Netz etwa auf ein NAS oder einen entfernten FTP-Server.

Die Dateien werden abhängig von den Einstellungen als einzelne Dateien abgelegt oder als ZIP-Archiv. Die Sicherung lässt sich sowohl explizit anstoßen als auch Zeit- oder Ereignis-gesteuert ausführen. Die Konfigurationsmöglichkeiten sind ausgesprochen vielfältig und bieten hohe Flexibilität. Assistenten helfen aber bei Bedarf bei der Erstellung der Sicherungsaufträge.

Zusatzmodule vereinfachen die Sicherung von *Thunderbird*-E-Mails oder können Ordner auf Veränderungen überwachen (mit dem Modul *Backup Monitor*), um dann eine automatische Sicherung anzustoßen.

Auch hier erstellt man zunächst per Klick auf *Neu* einen Sicherungsauftrag, unterstützt durch einen Assistenten (Abb. 2) – wahlweise für Anfänger oder für Fortgeschrittene. In ihm legt man zunächst das Zielverzeichnis für die Sicherung fest und danach die Quelle. Es dürfen auch mehrere Quellverzeichnisse sein, die dann in mehreren Zielverzeichnissen abgelegt werden – optional getrennt nach den Laufwerken der Quellen. Voreingestellt sind die üblichen Benutzer-Ver-

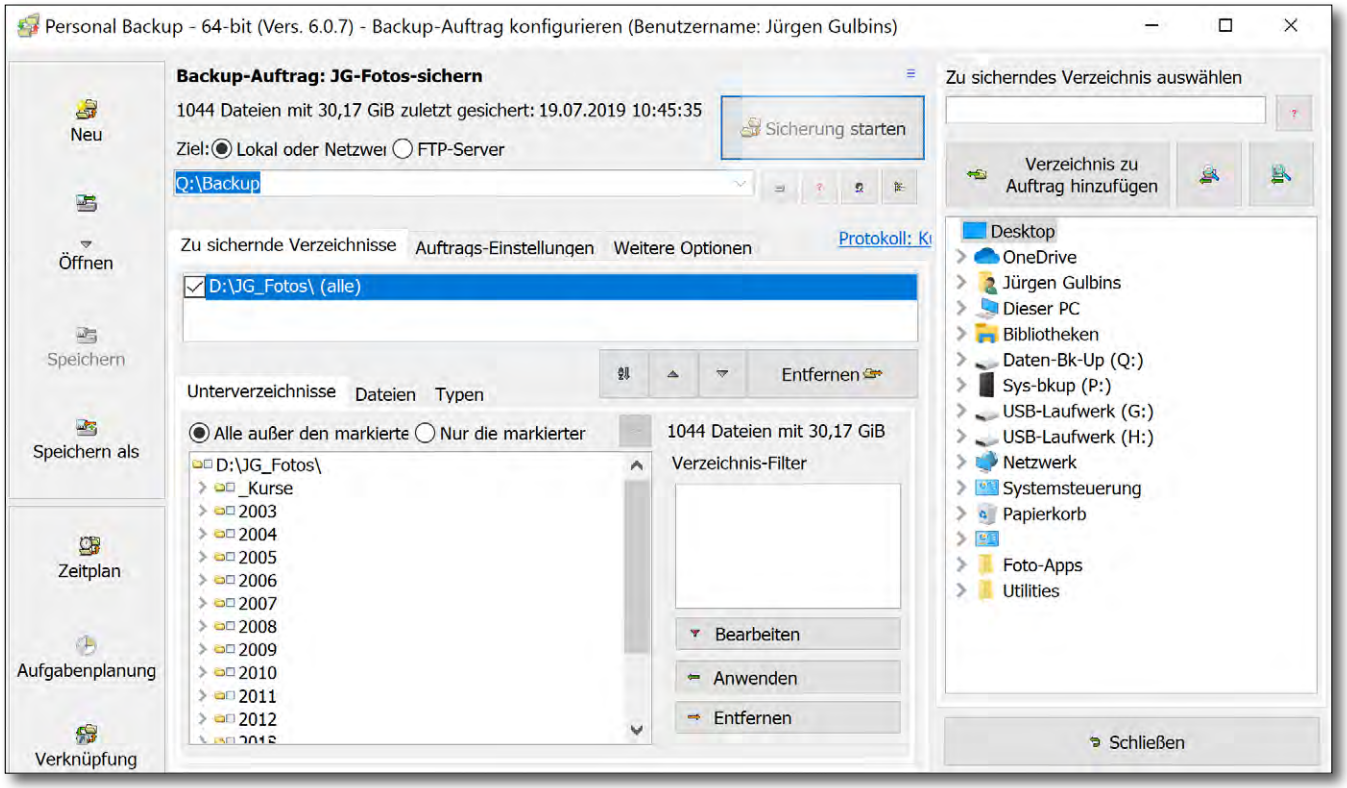


Abb. 1: Mein erster Sicherungsauftrag, erstellt mit dem Assistenten (für Anfänger)

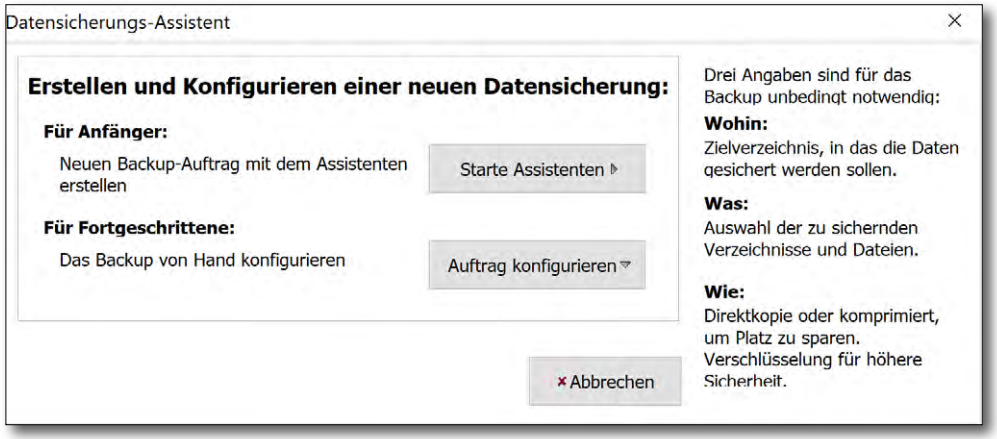


Abb. 2: Assistenten erleichtern die Erstellung von Sicherungsaufträgen.

zeichnisse (teilweise auch als *Bibliotheken* bezeichnet) auf dem C-Laufwerk (*Dokumente*, *Bilder*, *Musik*, *Videos*, …). Man kann davon einzelne (oder alle) deaktivieren und andere Quellen hinzufügen.

Im Assistenten legt man ebenso fest, wie die Sicherung abgelegt wird (Abb. 3): als Einzeldateien oder als ZIP-Archiv. Aber auch die Einzeldateien lassen sich komprimieren und optional (wie das ZIP-Archiv) verschlüsseln.

Danach gibt man noch an, wie der Auftrag ausgeführt werden soll – explizit aufgerufen oder Zeit-gesteuert. (Dies lässt sich später noch ändern.) Zum Schluss versieht man den Auftrag mit einem sinnträchtigen Namen. Die Auftragsübersicht (ähnlich wie in Abb. 1) zeigt nochmals die wesentlichen Elemente des Auftrags. Hier sind noch Änderungen/Ergänzungen möglich – z. B. **einzelne Verzeichnisse aus der Quelle** markieren und rechts mit dem Knopf von der Sicherung ausschließen. Es ist hier auch möglich, einen Zeitplan für die Ausführung zu erstellen oder zu ändern.

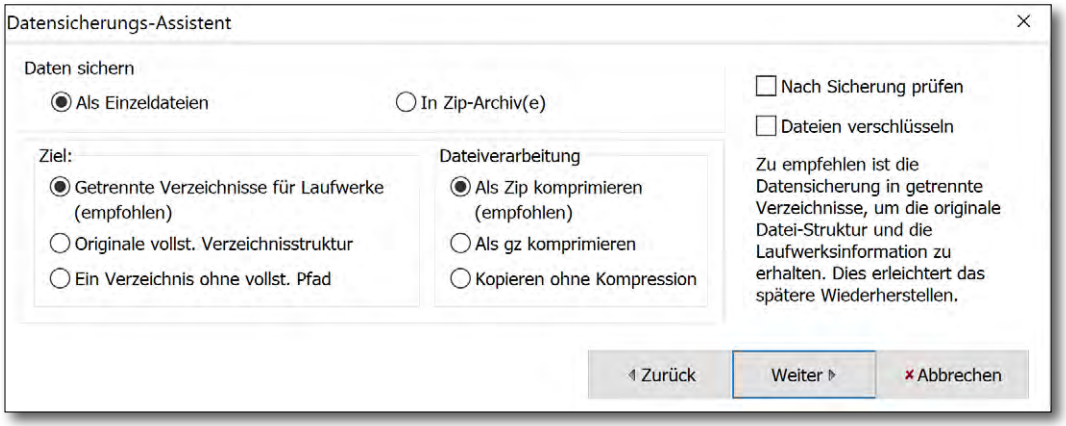


Abb. 3:
Hier legt man fest, wie die gesicherten Dateien im Ziel abgelegt werden und ob sie zusätzlich verschlüsselt und optional nach der Sicherung nochmals geprüft werden.

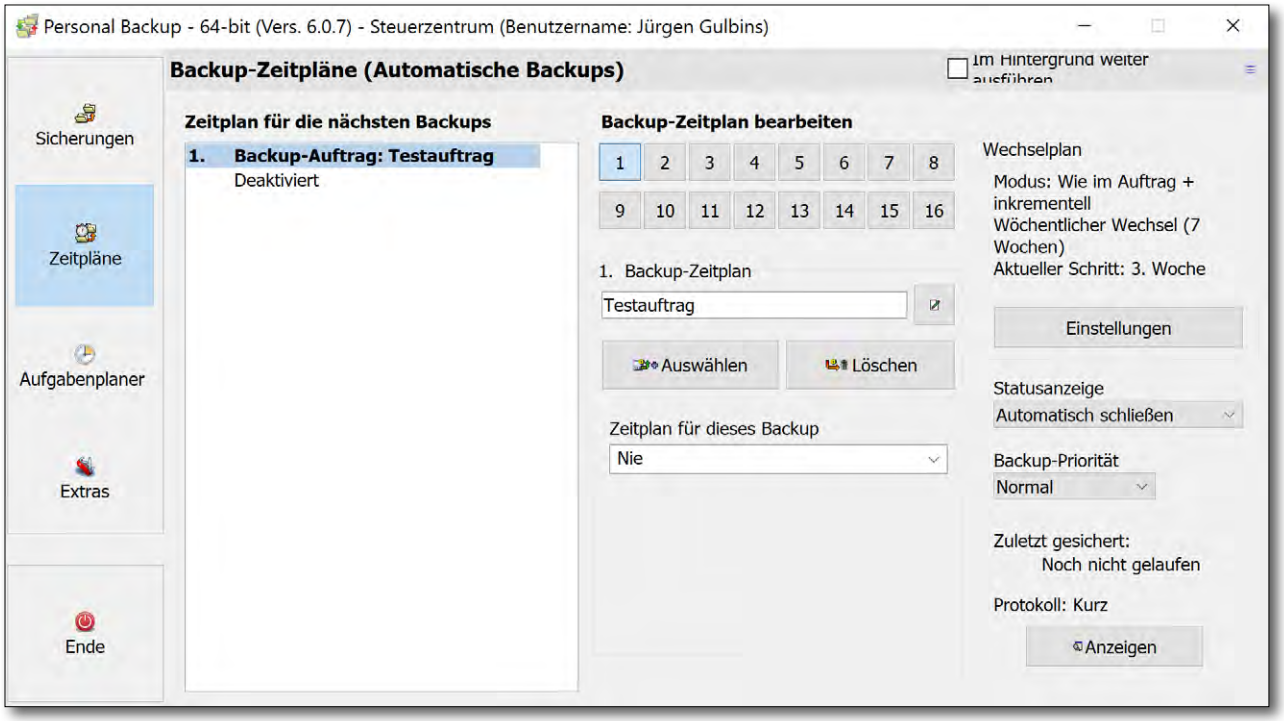


Abb. 4: Für automatisch ausgeführte Backups muss man Zeitpläne erstellen.

Zeitplaner

Hat man nicht gleich bei der Auftragserstellung einen Zeitplan erstellt, so lässt sich dies nachholen. Dazu wählt man im Hauptfenster den Auftrag und ruft über die Funktion *Zeitpläne* (links im Fenster) den Zeitplaner auf (Abb. 4).

Wesentliche Einstellungen nimmt man über den Knopf *Einstellungen* vor (Abb. 5). Die Möglichkeiten sind hier so vielfältig, dass man Details dazu im Online-Handbuch studieren sollte. *Personal Backup* erlaubt (pro Sicherungsauftrag) bis zu 16 Zeitpläne mit unterschiedlichen Einstellungen. In der Regel kommt man aber mit einer kleinen Anzahl aus – etwa einen für eine Vollsicherung und weitere für inkrementelle Backups.

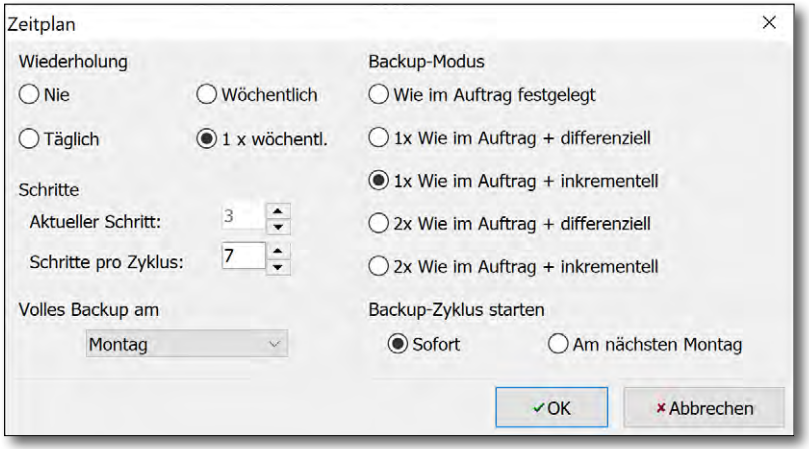


Abb. 5: Im Zeitplan legt man nicht nur die Zeitpunkte fest, sondern auch die Art der Sicherung zu dem betreffenden Zeitplan, etwa ein Voll-Backup gefolgt von *n* inkrementellen oder differenziellen Sicherungen.

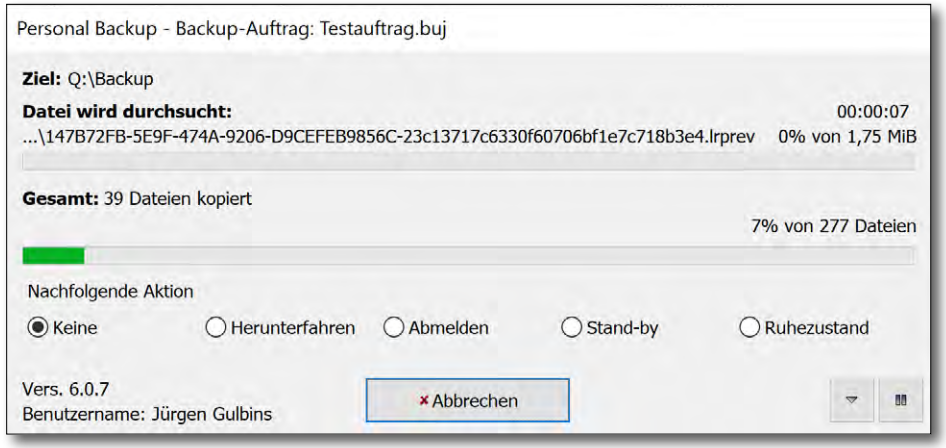


Abb. 6: Während des Laufs zeigt *Personal Backup* den Fortschritt und erlaubt noch festzulegen, was nach dem Lauf passieren soll.

Ein *differenzielles Backup* sichert jeweils alle Änderungen gegenüber der letzten Vollsicherung, ein *inkrementelles* seit dem letzten Sicherungslauf.

Bei Bedarf konfiguriert man dann den Auftrag über zahlreiche Optionen detailliert – etwa über die Filter, mit denen man (Quell-)Dateien in die Sicherung ein- oder von ihr ausschließt oder was die Ablage im Ziel betrifft (ZIP-Archiv oder normale Dateien/Ordner). Die Aufträge können mit einem beschreibenden Kommentar versehen werden.

Schließlich startet man über *Sicherung starten* den Auftrag, und sei es auch nur für einen Testlauf. Die Option *Im Hintergrund ausführen* (zu finden in der Kopfzeile links in der Auftragsübersicht) sorgt dafür, dass der Auftrag im Hintergrund läuft und nur dann ein Fenster erscheint, wenn Probleme auftreten und die Anwendung nachfragt, wie sie gelöst werden sollen.

Fortschrittsfenster

Das Fortschrittsfenster während der Auftragsausführung ist informativ (Abb. 6). Dort kann man (auch nachträglich) nochmals festlegen, was nach Fertigstellung des Auftrags erfolgen soll – von *Nichts* bis zum *Herunterfahren* des Rechners.

Daten wiederherstellen

Die Wiederherstellung der Daten ist natürlich abhängig, davon, wie man gesichert hat. Besteht die Sicherung aus normalen einzelnen Ordnern und Dateien, unkomprimiert und unverschlüsselt, so navigiert man einfach in das betreffende Verzeichnis und kann dort wie in der Quelle auf die Dateien zugreifen – direkt oder kopieren (z. B. mit dem *Explorer*). Sind sie als einzelne Dateien komprimiert, kann man sie zuvor per Doppelklick dekomprimieren; sind sie verschlüsselt, muss man sie unter Angabe des Schlüssels zuvor entschlüsseln.

Sollen mehr Dateien/Verzeichnisse wiederhergestellt werden, so legt man dafür einen eigenen Auftrag an (unter *Extras* per Klick auf *Restore* oder per Strg-R und dann auf *Neu*). Man erhält dann ein Auftragsfenster (Abb. 7), in dem man die Details für die Wiederherstellung festlegt. Dabei ist auch ein von der ursprünglichen Quelle abweichendes Verzeichnis als Ziel für die Wiederherstellung konfigurierbar. Die Optionen in diesem Fenster sind wahrlich vielfältig und dürften die meisten Situationen und Bedürfnisse abdecken.

Zusammenfassung

Dafür, dass *Personal Backup* kostenlos ist und gut gepflegt wird, bietet es sehr viel, läuft zügig, ist sehr gut dokumentiert und hat eine Reihe von Zusatzmodulen,

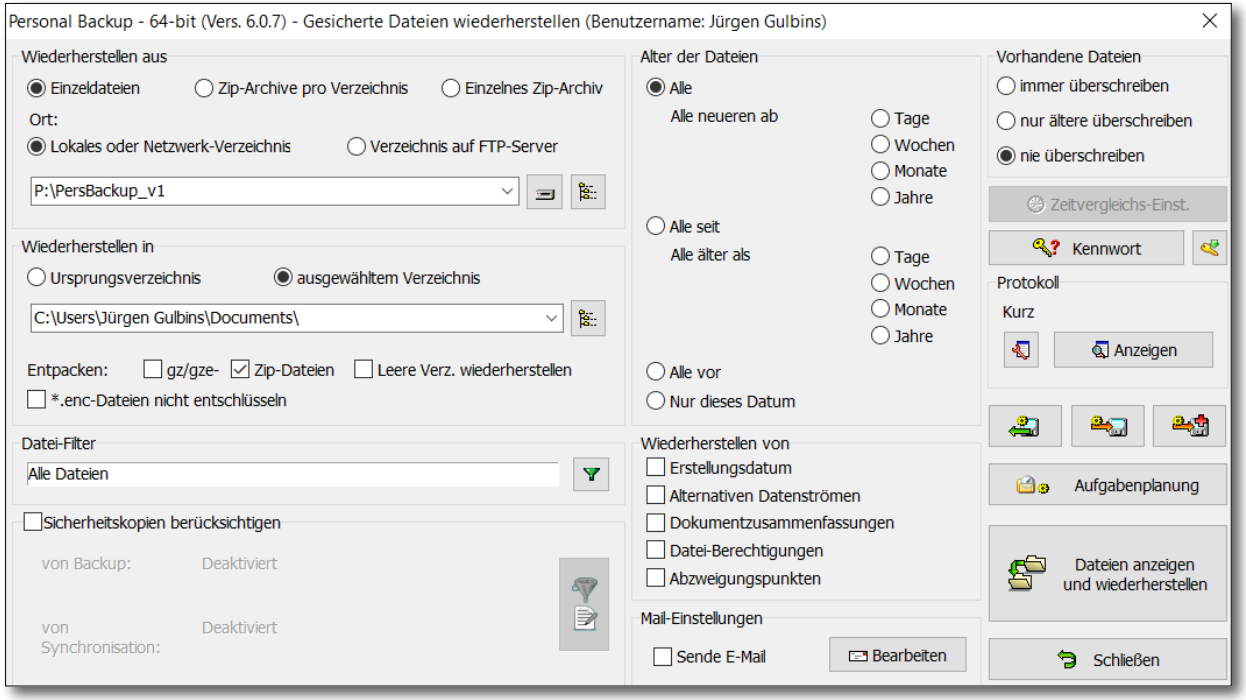


Abb. 7: Hier legt man die Details für den Auftrag zu einer Wiederherstellung fest.

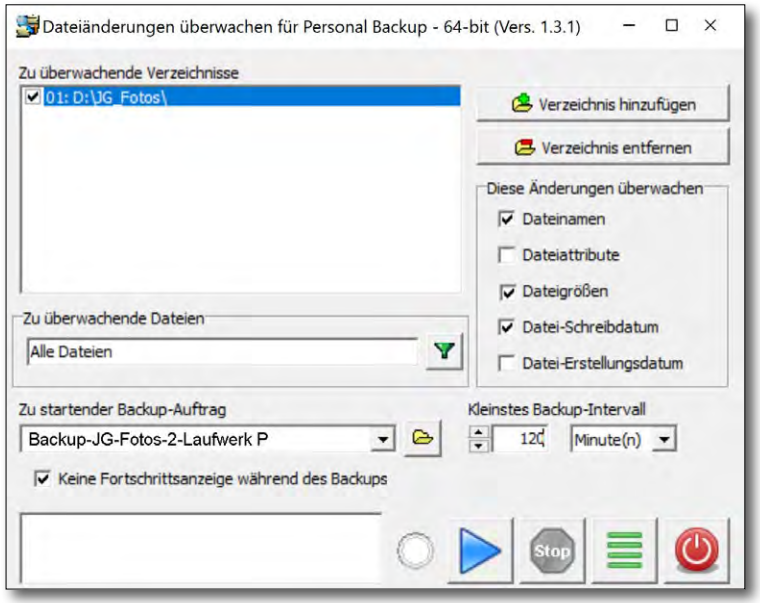


Abb. 8: Im *Personal Monitor* kann man Verzeichnisse überwachen lassen und bei Änderungen einen Sicherungsauftrag anstoßen.

etwa um *Thunderbird*-E-Mails zu sichern oder *Personal Backup Starter*, der die Anwendung unter einem anderen Benutzerkonto ausführt.

Das Modul *Backup Monitor* erlaubt Verzeichnisse zu überwachen und bei Änderungen (die man genauer spezifizieren kann) einen zugeordneten Sicherungsauftrag anzustoßen (Abb. 8).

Selbst der Detaillierungsgrad des Protokolls lässt sich konfigurieren sowie wann alte Protokolle automatisch gelöscht werden sollen.

Die Anwendung erlaubt sogar eine Liste mit Dateiendungen zu definieren (eine sinnvolle Basisliste ist bereits vorhanden), damit bestimmte Dateiarten von der Komprimierung bei der Sicherung ausgeschlossen werden – etwa bereits komprimierte JPEG- und ZIP-Dateien.

Statt eines **Laufwerksbuchstabens lässt sich in Aufträgen** (über das -Icon im Fenster mit den Aufträgen) auch ein Datenträgername verwenden, was oft die bessere Technik ist, aber voraussetzt, dass man diese Namen an die Sicherungsdatenträger vergibt und ein sauberes Namensmanagement betreibt (einen Datenträgernamen genau ein Mal vergibt).

Die Assistenten erlauben es auch einem unerfahrenen Anwender, seine Sicherungen zu konfigurieren. Auf Wunsch klinkt sich *Personal Backup* in das Kontextmenü des *Explorers* ein, so dass man dort direkt für einem selektierten Ordner ein Backup starten kann. (Bei Bedarf lässt sich zuvor ein entsprechender Sicherungsauftrag interaktiv erstellen.)

Tooltips verraten für viele der Icons deren Funktion. Die Online-Hilfe wird wie in vielen Anwendungen über F1 aufgerufen. (Über F2 erhält man einige weitere Informationen.) Die meisten Funktionen lassen sich statt über Menüs oder Icons auch über Tastaturkürzel aufrufen (beschrieben in der Online-Hilfe).

Der Entwickler hat bei der Programmierung wirklich an vieles gedacht und vieles umgesetzt.

Wie bei den anderen Backup-Programmen habe ich hier nur einen Ausschnitt aus den Möglichkeiten gezeigt; das Handbuch erläutert vieles detaillierter und gibt auch sinnvolle Empfehlungen.

Was bisher vorgestellt wurde, ist nur ein kleiner Ausschnitt der Anwendungen zur System- und Datensicherung. Es gibt davon für Windows wirklich zahlreiche – auch für unterschiedliche Anwendungsbereiche wie privater Nutzer, kleines oder größeres Unternehmen (Enterprise). Die bisher vorgestellten Lösungen wenden sich primär an den privaten oder einzelnen Anwender mit einem System oder einer kleinen Anzahl von Systemen. Dafür gibt es sicher eine große zweistellige Anzahl von Applikationen. Abgesehen von den kostenlosen Open-Source-Versionen findet man Anwendungen, die von kommerziellen Firmen in ›kleiner Version‹ kostenlos angeboten werden, um den Anwender später eventuell zur erweiterten kostenpflichtigen Version zu verleiten. Nur wenige der kostenlosen Versionen bedienen auch Windows-Server-Systeme. Dafür muss man in der Regel die kostenpflichtigen Pro- oder sogar die Enterprise-Versionen einsetzen. Vorteilhaft ist es, wenn die Anwendungen die Funktion von Schattenkopien (bei NTFS- und ReFS-Systemen) beherrschen.

Andere Anforderungen ergeben sich, wenn man eine größere Anzahl von Systemen verwalten und sichern möchte oder die Daten auf einem Windows-Server.[1] Dann lohnt sich schnell eine Server-Struktur, bei der ein zentrales System die Sicherungen vornimmt und überwacht. Dafür werden in der Regel auf den Einzelsystemen kleine Clients installiert, die von einer zentralen Backup-Anwendung angestoßen werden und ihre Daten zum zentralen Backup-Server schicken. Die meisten dieser Lösungen sind relativ komplex und in der Regel auch recht kostenintensiv, entlasten aber den einzelnen Anwender von dem Backup-Problem. Für einige der in diesem E-Book angesprochenen Lösungen gibt es solche (kostenpflichtigen) Server-Versionen.

Auch der kostenlose *AOMEI Backupper* [28] bietet (mit einer deutschen Oberfläche) die Möglichkeit, sowohl ein Backup des Systems in eine Image-Datei auszuführen (und zurückzuspielen) als auch einen Klon des Systems auf einem anderen Laufwerk zu erstellen, von dem man später booten kann (das ursprüngliche Systemlaufwerk muss dazu entfernt werden). Dies ist beispielsweise nützlich, um ein Windows-System auf eine SSD zu übertragen.

Die dritte Funktion besteht darin, Benutzerdaten zu sichern – in ein Backup-Image (eine einzelne große Datei) oder aber als viele ›normale Dateien‹ zu synchronisieren. Auch hier möchte die Firma *AOMEI* den Anwender mit seiner kostenlosen Lösung zum Kauf der etwa 40 Euro teuren Pro-Version verleiten, die aber recht gute Bewertungen bekommt.

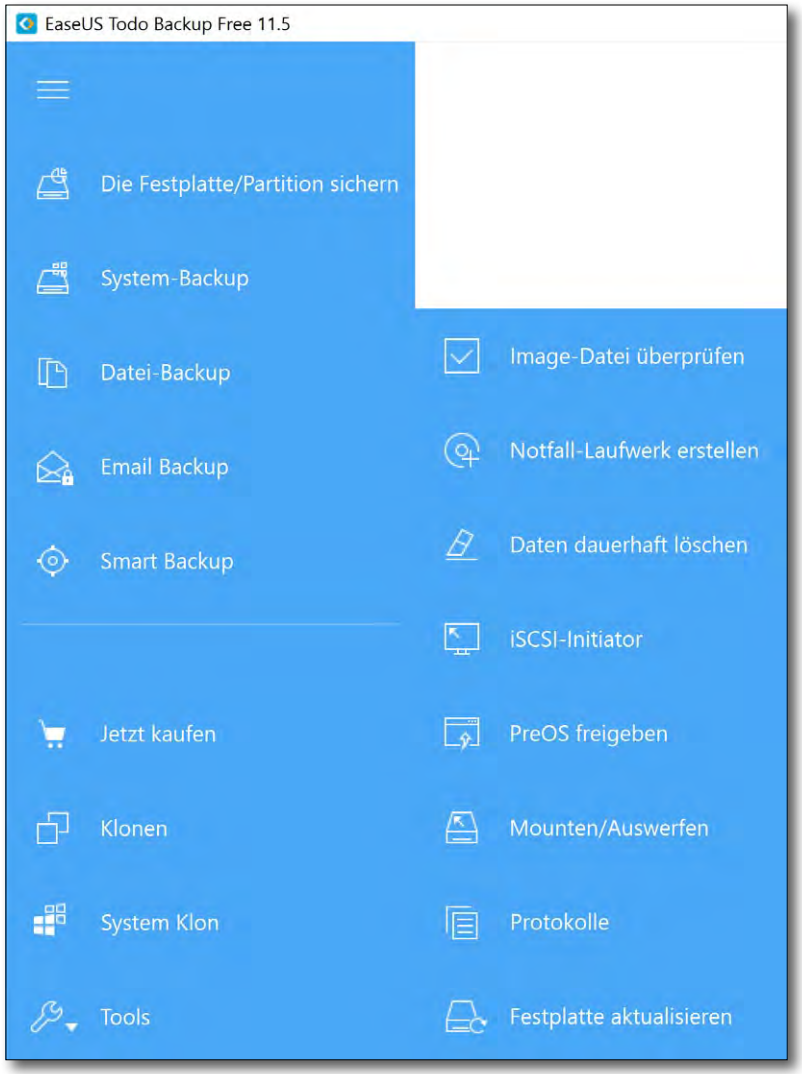


Abb. 9: *EaseUS Todo Backup* bietet in seiner *Home-Edition* ein breites Spektrum an Backup-Funktionen, viele davon bereits in der kostenlosen *Free*-Edition.

1 Die meisten kostenlosen Backup-Lösungen schließen das Sichern von Windows-Server-Versionen aus.

Die Firma *EaseUS*, von der auch der *EaseUS Partition Manager* stammt, bietet mit *EaseUS Todo Backup* [25] ein (in der *Free*-Version kostenloses) Backup-Programm mit deutscher Oberfläche. Abbildung 9 zeigt die vielfältigen Möglichkeiten der Anwendung, wobei man bei genauerem Hinschauen feststellt, dass einige davon die mit 27 Euro relativ preisgünstige *Home-Edition* erfordern. Die Updates der *Home-Edition* sind in diesem Preis auf Dauer kostenlos enthalten.

Die englische Firma *Macriumsoftware* bietet unter dem Label *Macrium Reflect 7* [33] ein recht breites Spektrum von Backup-Lösungen für Windows an, vom kostenlosen *Reflect 7 Free* bis hin zur Enterprise-Lösung *Reflect 7 Deployment Kit*. Wie viele dieser Lösungen kann *Reflect 7* (bereits in der Free-Version) sowohl einen Boot-Stick für den Notfall erstellen als auch das System in eine Image-Datei sichern (und später restaurieren) als auch einzelne Dateien und Ordner sichern – und dies auch Zeit-gesteuert.

Eine recht ausgeklügelte Backup-Anwendung (kostenlos und *Open Source*) für Benutzerdateien ist *Areca Backup* [38]. Es gibt eine deutsche Oberfläche, die Online-Hilfe ist jedoch englisch. Die Konfigurationsmöglichkeiten und Filter (zum Ein- und Ausschließen von Dateien für die Sicherung) sind beeindruckend. Es gibt einige optional Plug-ins zu *Areca Backup* – etwa *ArecaVSS*,[1] das erlaubt, die Windows-Schattenkopie-Funktion (kurz VSS für *Volume Shadow Copy Service*) für Sicherungen nutzen. Daneben gibt es Plug-ins für Datenübertragungen per FTP/FTPs- sowie dem SFTP-Protokoll zu Remote-Systemen. *Areca Backup* kann jedoch nicht das Betriebssystem sichern und wiederherstellen.

NAS-Systeme (*Network Attached Systems*) lassen sich mit den meisten Backup-Anwendungen nicht nur als Ziel für die Sicherung einsetzen, sondern die meisten davon bringen auch Clients (Programme) mit, welche auf den verschiedenen Plattformen, die Zugriff auf das NAS haben, auch automatisch Backups ausführen.

Datenbanksicherung

Ein spezielles Problem stellt die Sicherung von Datenbanken dar – und viele E-Mail-Systeme haben im normalen Windows-Betrieb eine Datenbank für die E-Mails ständig offen. Manche Backup-Anwendungen haben deshalb spezielle Module zur Sicherung solcher Datenbanken, etwa denen von *Thunderbird, Outlook* oder *Sharepoint*. Diese Möglichkeit findet man (fast nur) in den kommerziellen Backup-Lösungen, teilweise mit optionalen Zusatzmodulen. Dieses Thema sprengt aber den Rahmen dieses E-Books, und mir fehlt dazu auch die Erfahrung. Eine relativ simple Lösung besteht jedoch darin, die Datenbank vor der Sicherung herunterzufahren, sie während der laufenden Sicherung nicht zu benutzen oder die Datenbank-Datei in die Sicherung einzuschließen.

1 Das *ArecaVSS*-Plug-in erfordert aber eine 4 Euro teuere Lizenz je System.

Tabelle 9: Beispiele für Backup-Lösungen unter Windows

Anwendung	Dateiversionsverlauf	Sichern und Wiederherstellen (Windows 7)	Acronis True Image	Personal Backup	FreeFileSync	SyncBackFree
Hersteller	Microsoft Teil von Windows 10	Microsoft Teil von Windows 10	Acronis www.acronis.com/de-de/	Dr. Jürgen Rathlev http://personal-backup.rathlev-home.de	Open Source https://freefilesync.org	2BrightSparks Pte. Ltd. https://www.2brightsparks.com
Preis ca.	kostenlos (Teil von Windows)	kostenlos (Teil von Windows)	35 € für 1 PC (51 € für 3 PCs)	kostenlos	kostenlos	kostenlos
Sicherungsarten:						
– System / bootbar	(+) nach Restore-Funkt.	(+) nach Restore-Funkt.	**+ /** (+) per Klon	–	**– / –**	**– / –**
– Partition/Volume	(+) alles in 1 Image	(+) alles in 1 Image	+	–	(+)[1]	(+)[1]
– Ordner bzw. Dateibäume	+	+	+	+	+	+
– Versionierung	+	+	+	+	+	+
– auf Remote-System	(+) auf Netzwerklaufw.	(+) auf Netzwerklaufw.	+	+	+	+
– auf Cloud-Speicher	(+) in OneDrive-Cloud	–	**(+)** in Acronis-Cloud	–	–	–
Spezielle Funktionen 1:						+
– Skriptsteuerung	–	–	+	+	+	+
– Vorher-/Nachher-Aktion	–	–	+	+	+	+
– Filterfunktionen	–	–	+	+	+	+
– Verschlüsselung	–	–	+	+	–	–
– Komprimierung	–	–	+	+	–	+ (einzeln und als 1 Image)
– Realzeitsynchronisation	–	–	(+) 5-Minuten-Intervall	(+) per Backup Monitor	+ (per RealTimeSync)	–
Spezielle Funktionen 2:						
– Zeit-gesteuert	+ (nur stündlich)	+	+	+	(+)[2]	+
– Ereignis-gesteuert	–	+	+	–	+	+
– Remote-gesteuert	–	+	–	–	–	–
– Server-Lösung	–	–	–	–	–	–
Rückspielen	über Wiederherstellungsfunktion	über Wiederherstellungsfunktion	einzelne Dateien direkt, mehr/alle per Restore-Funktion	einzelne Dateien direkt, per Wiederherstellen-Auftrag	FreeFileSync ⟷, Explorer / Direktzugriff auf Dateien/Ordner	SyncBackFree ⟷, Explorer /Direktzugriff auf Dateien/Ordner
Benutzeroberfläche	DE, EN, FR, …	DE, EN, FR, …	DE, EN, FR, …	DE, EN, …	DE, EN, FR, …	DE, EN, …
Handbuch/Online-Hilfe	DE, EN, FR, …	(DE), EN	DE, EN, FR, …	DE, EN, …	EN	DE, EN, …
Anmerkungen	Konfiguration über viele Panels verteilt	Konfiguration über viele Panels verteilt, Support von MS abgekündigt	Sehr verbreitet mit vielen Funktionen und sehr stabil	Sehr umfangreich konfiguierbar	Auch für macOS und Linux verfügbar. (1) Bei Volumes eingeschränkte Zugriffsrechte. (2) über den Windows-Sheduler	(1) Bei Volumes eingeschränkte Zugriffsrechte

Umgang mit Wiederherstellungspunkten

Während Apple unter macOS bisher keine grafische Oberfläche für den Umgang mit Snapshots für APFS-Volumes zur Verfügung stellt, gibt es unter Windows 10 für NTFS-Volumes dafür Werkzeuge, wobei Snapshots hier als *Volumeschattenkopien* bezeichnet werden; ein Anwendungsbereich dafür sind *Wiederaufsetzpunkte* – primär für das Betriebssystem. (Es sei hier angemerkt, dass die nachfolgende Beschreibung nur für Windows 10 gilt, da es zu vorhergehenden Versionen einige Änderungen gab.)

Um überhaupt Schattenkopien für ein Volume zu ermöglichen, muss es sich um ein NTFS-**Volume handeln**. Die Erstellung von Wiederherstellungspunkten von bestimmten Ständen des installierten Betriebssystems zu einem bestimmten Zeitpunkt – hier als *Wiederaufsetzpunkte* bezeichnet – unter Verwendung von Schattenkopien ist dabei eine Nutzung des Windows-Schattenkopie-Services (abgekürzt VSS – *Volume Shadow Copy Service*). Die Funktion zum Anlegen von Wiederaufsetzpunkten muss aber aktiviert sein.

Diese Funktion ist für das Systemvolume im Standardfall aktiv, jedoch für keine weitere Partition (Volume). Wiederherstellungspunkte werden vom System praktisch vor jedem Betriebssystem-Update sowie vor der Installation neuer Treiber geschaffen – und zusätzlich in bestimmten Intervallen (leider ist nicht angegeben, wie oft). Erst diese Wiederherstellungspunkte erlauben es, bei Problemen auf einen vorhergehenden Stand des Betriebssystems, installierter Anwendungen und Systemeinstellungen zurückzugehen.

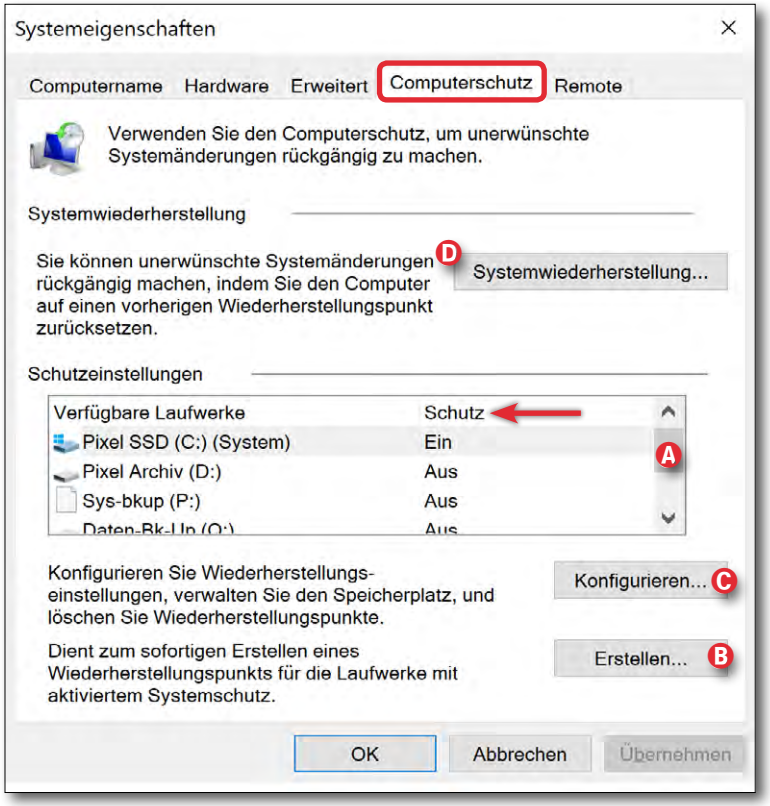


Abb. 1: Unter *Systemeigenschaften* sieht man, ob für ein Volume die Schattenkopie-Funktion alias *Computerschutz* aktiviert ist.

Aus diesen Schattenkopien lassen sich unter Umständen versehentlich gelöschte oder defekte Dateien wiederherstellen. (**Man sollte dies aber nicht als Ausrede nutzen, keine getrennten Sicherungen herzustellen!**)

Um zu sehen, ob für ein Laufwerk die Schattenkopien-Funktion aktiviert ist, ruft man *Systemeigenschaften* auf. Dazu gibt man ⊞-R (Windows-Taste + R gleichzeitig) ein und im erscheinenden Kommandofenster ›*sysdm.cpl*‹. Unter *Systemeigenschaften* geht man auf den Reiter *Computerschutz* (Abb. 1). Der *Schutz*-Status eines Laufwerks zeigt an, ob der Mechanismus der

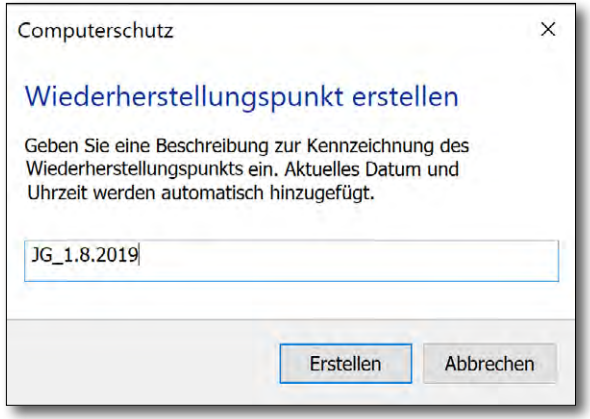


Abb. 2: Es ist sinnvoll, dem Wiederherstellungspunkt einen erklärenden Namen zu geben.

Schattenkopien aktiviert (*Ein*) ist oder deaktiviert (*Aus*) ist.

Ist der Mechanismus aktiv, so kann man per *Erstellen* Ⓑ auf dem ausgewählten Volume eine neue Schattenkopie – hier als *Wiederherstellungspunkt* bezeichnet – anlegen und der Kopie einen beschreibenden Namen geben (Abb. 2). Datum und Uhrzeit werden dabei automatisch zum Wiederaufsetzpunkt vermerkt.

Möchte man für ein Volume Wiederaufsetzpunkte aktivieren (oder deaktivieren), so wählt man in der Scroll-Liste von Abbildung 1 Ⓐ das betreffende Volume und klickt auf *Konfigurieren* Ⓒ. Damit erscheint der Dialog von Abbildung 3, in dem man Wiederaufsetzpunkte – hier als *Computerschutz* bezeichnet – aktivieren oder deaktivieren kann. Hier legt man ebenso fest, wie viel Prozent des gesamten Speicherplatzes des Volumes Schattenkopien maximal einnehmen dürfen. Bei Bedarf werden dann beim Anlegen eines neuen Wiederaufsetzpunkts die jeweils ältesten Kopien automatisch gelöscht. Fünf bis etwa zehn Prozent erweisen

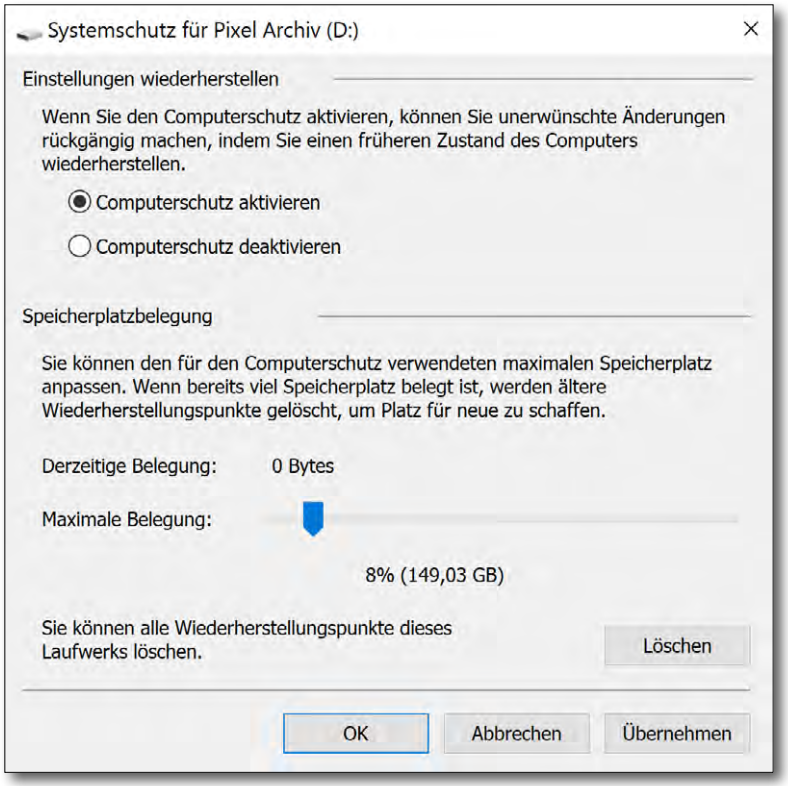


Abb. 3: Hier aktiviert oder deaktiviert man den *Computerschutz* eines Laufwerks und legt auch die prozentuale maximale Größe fest, die die Schattenkopien einnehmen dürfen.

sich als sinnvoll. Der aktuell verwendete Speicher wird ebenfalls angezeigt. Hier lassen sich auch alle Wiederherstellungspunkte eines Volumes (nach Rückfrage) löschen, was Speicher freigibt. Das Löschen nur einzelner älterer Wiederherstellungspunkte des Platzgewinns wegen ist leider nicht möglich. Nach dem Löschen ist das Volume auf dem Stand vor dem Löschen, hat aber die alten Stände verloren und kann nicht mehr darauf zurückgesetzt werden. Das Löschen ist für einzelne Volumes möglich. Ein solches Löschen alter Wiederherstellungspunkte kann auch vor dem Migrieren/Kopieren eines Systems oder eines anderen Volumes auf einen anderen Datenträger (z. B. eine *SSD*) sinnvoll sein. Eine andere Art des Löschens kann darin bestehen, die *Maximale Belegung* zu verkleinern (zumindest vorübergehend).

Ein Wiederherstellungspunkt kostet auf der Systemplatte etwa 300–350 MB.

Systemwiederherstellung

Möchte man das System auf einen älteren Stand zurücksetzen, findet man die Funktion dazu im Fenster zu den *Systemeigenschaften* unter *Systemwiederherstellung* (Abb. 1 Ⓓ). Dabei fällt auf, dass man hier zwar auch ein Volume in der Liste wählen kann, das kein Systemvolume ist, mit *Systemwiederherstellung* wird aber auch das System auf den gewählten Wiederherstellungspunkt zurückgesetzt – die Benutzerdateien auf dem Systemlaufwerk bleiben dabei unverändert.

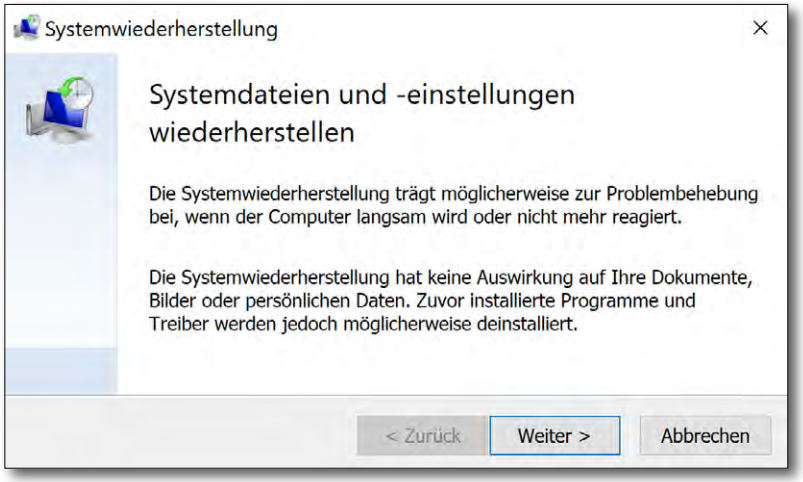


Abb. 4: Informationen des Systems zur Wiederherstellung

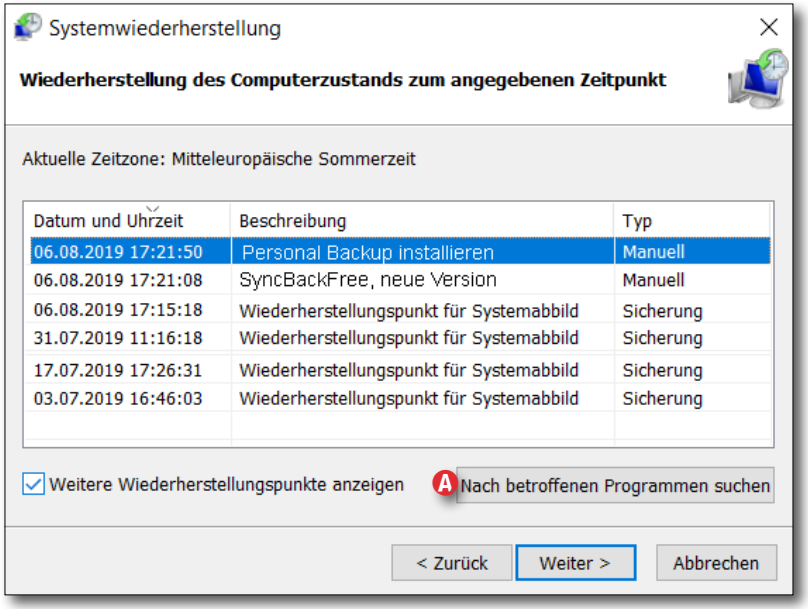


Abb. 5: Hier wählt man den gewünschten Wiederaufsetzpunkt.

Es erscheint zunächst die Information von Abbildung 4. Mit *Weiter* zeigt die Systemwiederherstellung die Wiederherstellungspunkte für das Systemlaufwerk und die anderen Laufwerke mit solchen Punkten (Abb. 5). Man selektiert dort den gewünschten Punkt und kann sich über den Knopf Ⓐ noch die von dieser Wiederherstellung betroffenen Programme anzeigen lassen. Mit *Weiter* erscheint eine letzte

Warnung, dass eine einmal angestoßene Wiederherstellung nicht mehr gestoppt und nicht mehr rückgängig gemacht werden kann. Bestätigt man dies erneut mit *Weiter*, wird die Wiederherstellung angestoßen. Sie kann eine Weile dauern. Danach wird das System neu gestartet.

Leider können auf die gezeigte Weise andere Volumes nicht separat auf einen früheren Stand gebracht werden. Diese Funktion hier ist eben sehr stark auf eine Systemwiederherstellung ausgelegt.

Eine abweichende Art, das Systemvolume auf einen früheren Stand zu bringen, ist folgende: Zunächst selektiert man im *Explorer* das Systemlaufwerk und geht dort im Kontextmenü ganz unten auf *Eigenschaften*. (Abb. 6). Im *Eigenschaften*-Fenster wählt man den Reiter *Vorgängerversionen*. Nach einem Augenblick listet das Fenster die verfügbaren Versionen auf, zeigt jedoch keine manuell gesetzten Wiederherstellungspunkte. Selektiert man hier einen Zeitpunkt, so lässt sich über das Kontextmenü die Funktion *Wiederherstellen* aufrufen (Abb. 7).

Es gibt noch eine Reihe weiterer Verfahren, um das System bei Problemen auf einen früheren (hoffentlich stabileren) Stand zurückzusetzen – etwa unter den (Windows-)*Einstellungen* → *Update und Sicherheit* → *Wiederherstellung*.

Auch die Windows-Funktion *Dateiversionsverlauf* (Seite 86) scheint Wiederherstellungspunkte zu setzen. Es führen eben viele (verschiedene) Wege nach Rom.

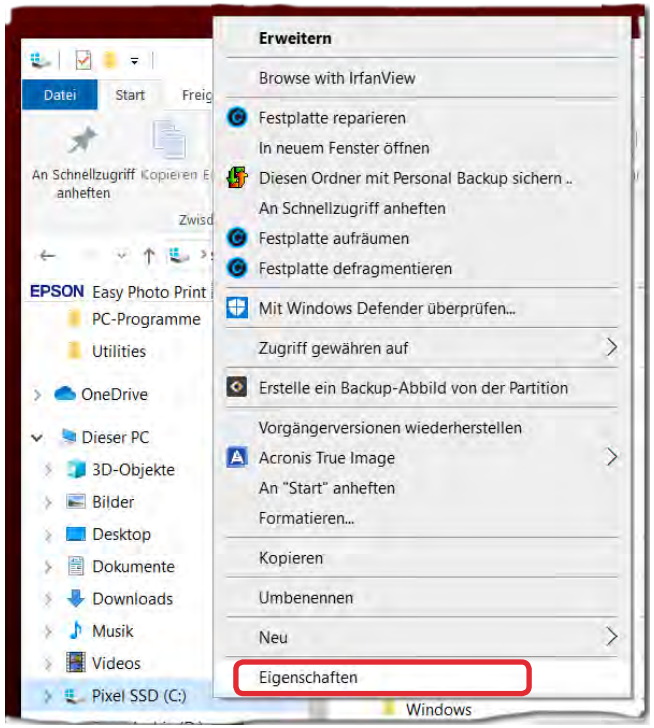


Abb. 6: Wählt man im *Explorer* das Systemvolume und aktiviert im Kontextmenü *Eigenschaften*, so kommt man zu Abb. 7.

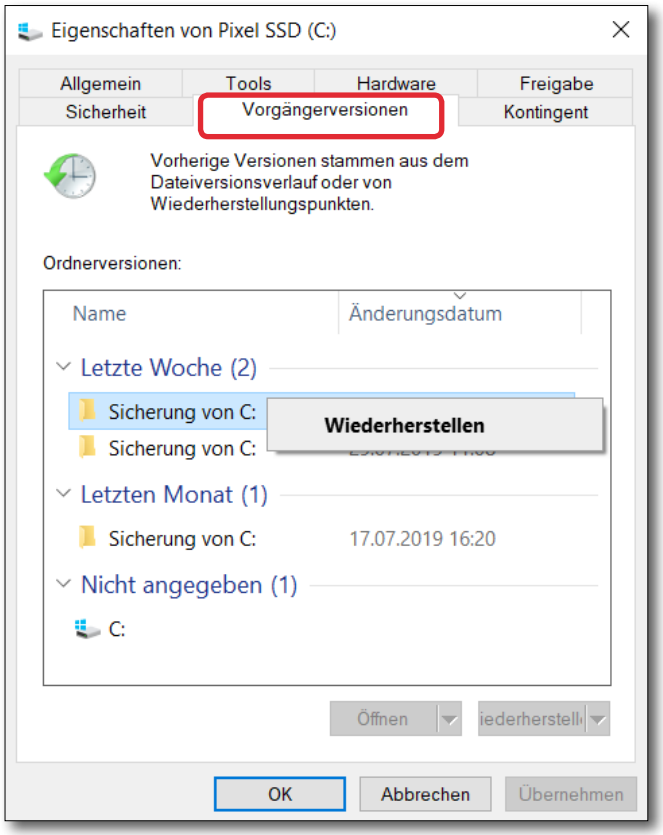


Abb. 7: Beim Systemvolume – hier C: – zeigt *Vorgängerversionen* die Wiederherstellungspunkte des Systems. Per Kontextmenü lässt sich eine Wiederherstellung auf den gewählten Zeitpunkt anstoßen.

Wiederherstellung einzelner Dateien

Obwohl möglich, stellt Windows in der Home- oder in der Pro-Version selbst meines Wissens keine Anwendung zur Verfügung, um gelöschte oder beschädigte Dateien aus einer älteren Schattenkopie wieder herzustellen. (Unter Windows Server scheint es dafür Funktionen zu geben). Diese Aufgabe lässt sich aber mit der Anwendung *ShadowExplorer* durchführen. Sie wird auf Seite 122 beschrieben.

Es gibt einige kleine Anwendungen, die ich bei der Systempflege meiner Windows-Rechner und beim Umgang mit Datenträgern nützlich oder informativ gefunden habe. Die Mehrzahl von ihnen ist kostenlos – zumindest für den privaten Einsatz.

CrystalDiskInfo

CrystalDiskInfo [26] liefert zu angeschlossenen Laufwerken eine ganze Reihe nützlicher Informationen (Abb. 1), etwa die Seriennummer, die Anschlussart, einige technische Daten; auch der S.M.A.R.T.-Status sowie die Temperatur des Laufwerks wird angezeigt (soweit auslesbar).

CrystalDiskMark

CrystalDiskMark [26] erlaubt die Lese- und Schreibgeschwindigkeit von Datenträgern zu testen – mit mehreren unterschiedlichen Zugriffsarten (Blockgrößen und sequenziellen oder zufälligen Zugriffen).

Beim Test muss man ein wenig Geduld aufbringen, da mit den Standardeinstellungen die einzelnen Tests fünf Mal durchlaufen und die Ergebnisse gemittelt werden (was sinnvoll ist). Die Anzahl der Durchläufe lässt sich unter Abbildung 2 Ⓑ ändern.

Zuweilen erhält man damit überraschende Ergebnisse und kann mit diesem Wissen sein System so optimieren, dass man eine bessere Performance erhält – etwa, wenn man bestimmte Dateien (z. B. den Lightroom-Katalog) auf einen schnelleren Datenträger legt.

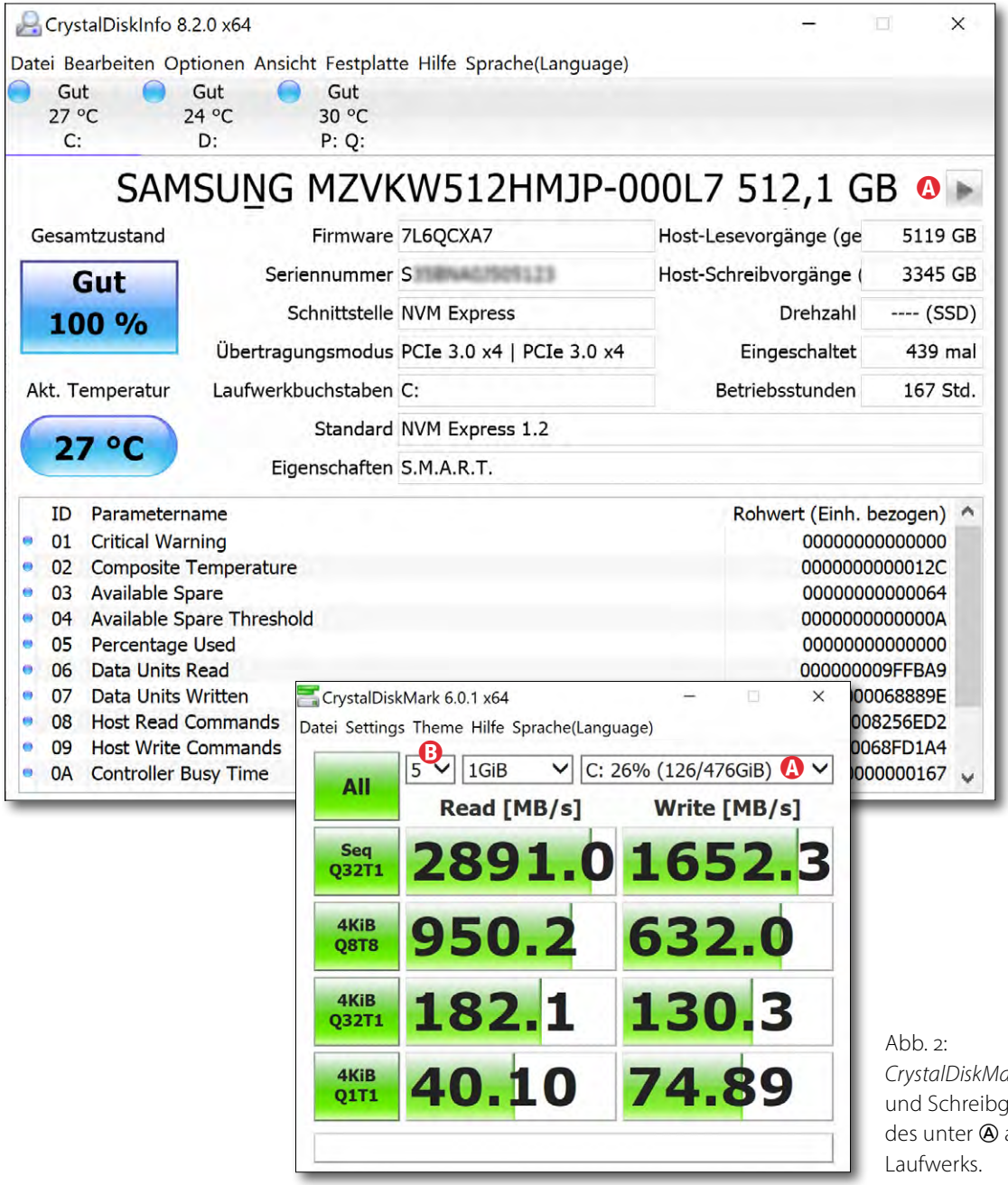


Abb. 1
CrystalDiskInfo zeigt zum unter Ⓐ ausgewählten Laufwerk – hier die SSD meines Windows-Laptops – eine Reihe nützlicher Informationen.

Abb. 2:
CrystalDiskMark misst die Lese- und Schreibgeschwindigkeit des unter Ⓐ ausgewählten Laufwerks.

SiSoftware Sandra Lite

Die Anwendung *SiSoftware Sandra Lite* der Firma SiSoftware [23] liefert zu Ihrem Rechner sehr detaillierte Informationen (Abb. 3) – etwa welchen CPU-Typ das System hat, mit wie vielen Kernen und Threads, wie die Grafikkarte aussieht oder welche Speicherriegel verbaut sind. Untergliedert in verschiedene Kacheln bzw. Themenbereiche liefert die Anwendung eine Vielzahl von weiteren Informationen. Deren Interpretation erfordert ein wenige Hardware-Know-how, kann im Einzelfall jedoch nützlich sein, etwa um zu sehen, ob man den Rechner noch mit weiteren (Haupt-) Speicherriegeln ausbauen kann. Auch einige Sensoren – etwa zur aktuellen CPU-Temperatur –lassen sich damit auslesen und die Daten anzeigen. Zu vielen der Komponenten wird der Hersteller genannt, was nützlich sein kann, um Treiberaktualisierungen zu finden.

Die Daten lassen sich als Berichte in verschiedenen Formaten abspeichern. Außerdem kann man mit dem Werkzeug verschiedene Benchmark-Tests durchführen.

Diese Anwendung benötigt man selten, aber wenn, dann kann sie nützlich sein. Als Fotograf kommt man fast immer mit der hier gezeigten kostenlosen Lite-Version aus. Einige Funktionen sind bei ihr deaktiviert. Im nebenstehenden Bild sind sie ausgegraut.

Eigentlich bräuchte man zu dem Werkzeug ein ganzes Buch – in der Regel kommt man aber mit den Online-Hilfen (in Deutsch), ein wenig Intuition und Erfahrung sowie ein bisschen Ausprobieren zu den gewünschten Informationen.

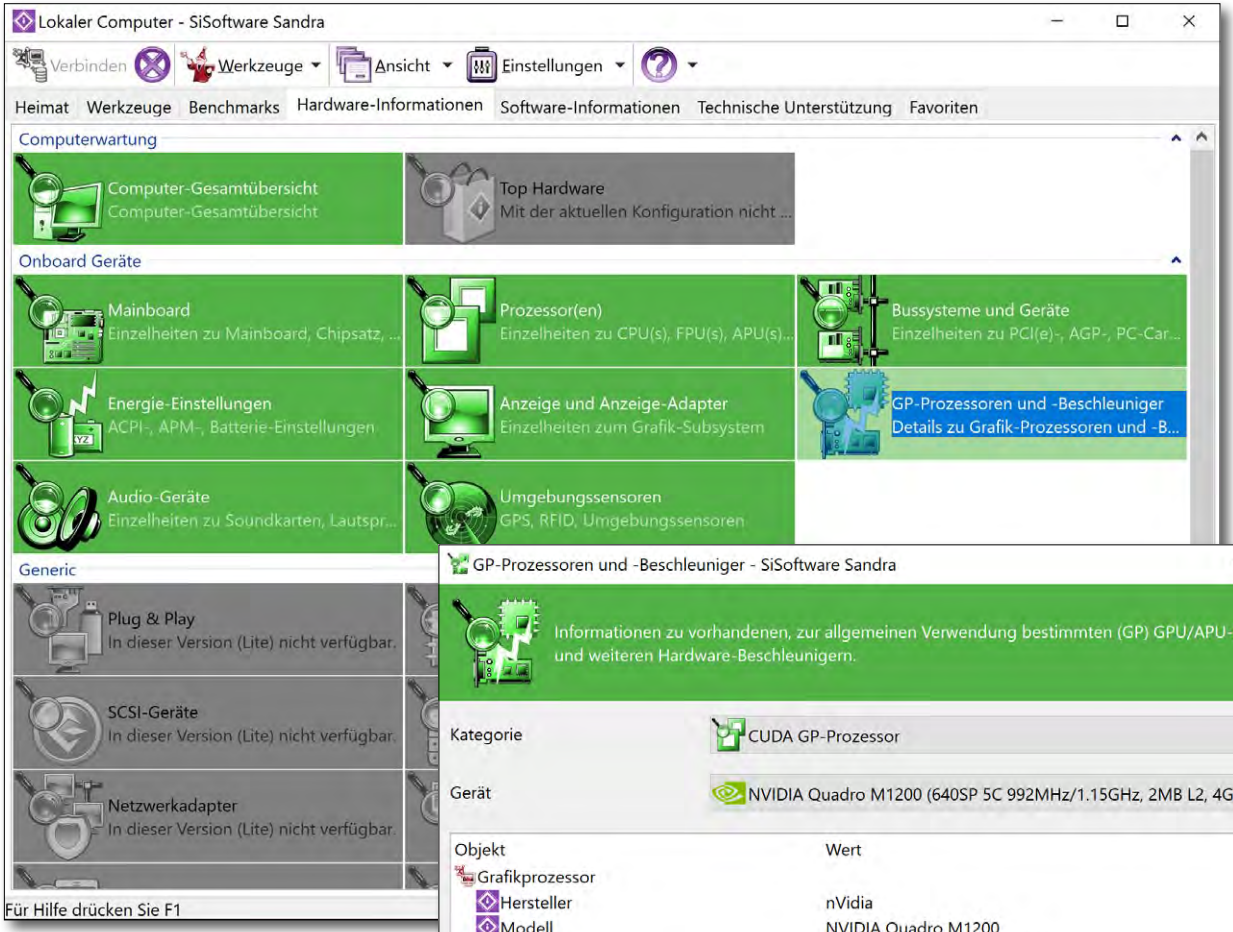


Abb. 3: ▲ *SiSoftware Sandra* liefert sehr detaillierte Informationen zu Ihrem Rechner, aufgeteilt in zahlreiche Rubriken. Ein Doppelklick auf eines der Felder zeigt dann die Einzelheiten, wie nebenstehend in Abbildung 4 zu sehen zum Grafikprozessor meines Laptops.

Eine kompaktere Alternative zu *Sandra Lite* ist das kostenlose *CPU-Z* [24] (englischsprachig).

Abb. 4: Hier die Information zu meiner Grafikkarte (Ausschnitt)

MiniTool Partition Wizard

MiniTool Partition Wizard [27] ist eine – in der Lite-Version kostenlose – Werkzeugsammlung mit deutscher Oberfläche (Abb. 5). Hier findet man Werkzeuge zur Daten- und Partitionswiederherstellung, zum Klonen von Datenträgern und Kopieren von Partitionen, zum Benchmarken von Laufwerken sowie zur Datenträger- und Partitionsverwaltung. Ein Klick auf eines der Panels ruft das betreffende Werkzeug auf.

Der *Partition Wizard* ist eine gute Alternative zur *Datenträgerverwaltung* von Windows und umfasst mehr Funktionen (Abb. 5) und zeigt, wenn man *Datenträger- & Partitionsverwaltung* (Abb. 5 Ⓐ) aktiviert, mehr Informationen als die *Datenträgerverwaltung*, wie bereits Abbildung 6 erkennen lässt. Es werden auch mehr Funktionen als in dem Windows-Tool angeboten. Der *Partition Wizard* bietet links gleich eine ganze Reihe von Assistenten für spezielle Operationen.

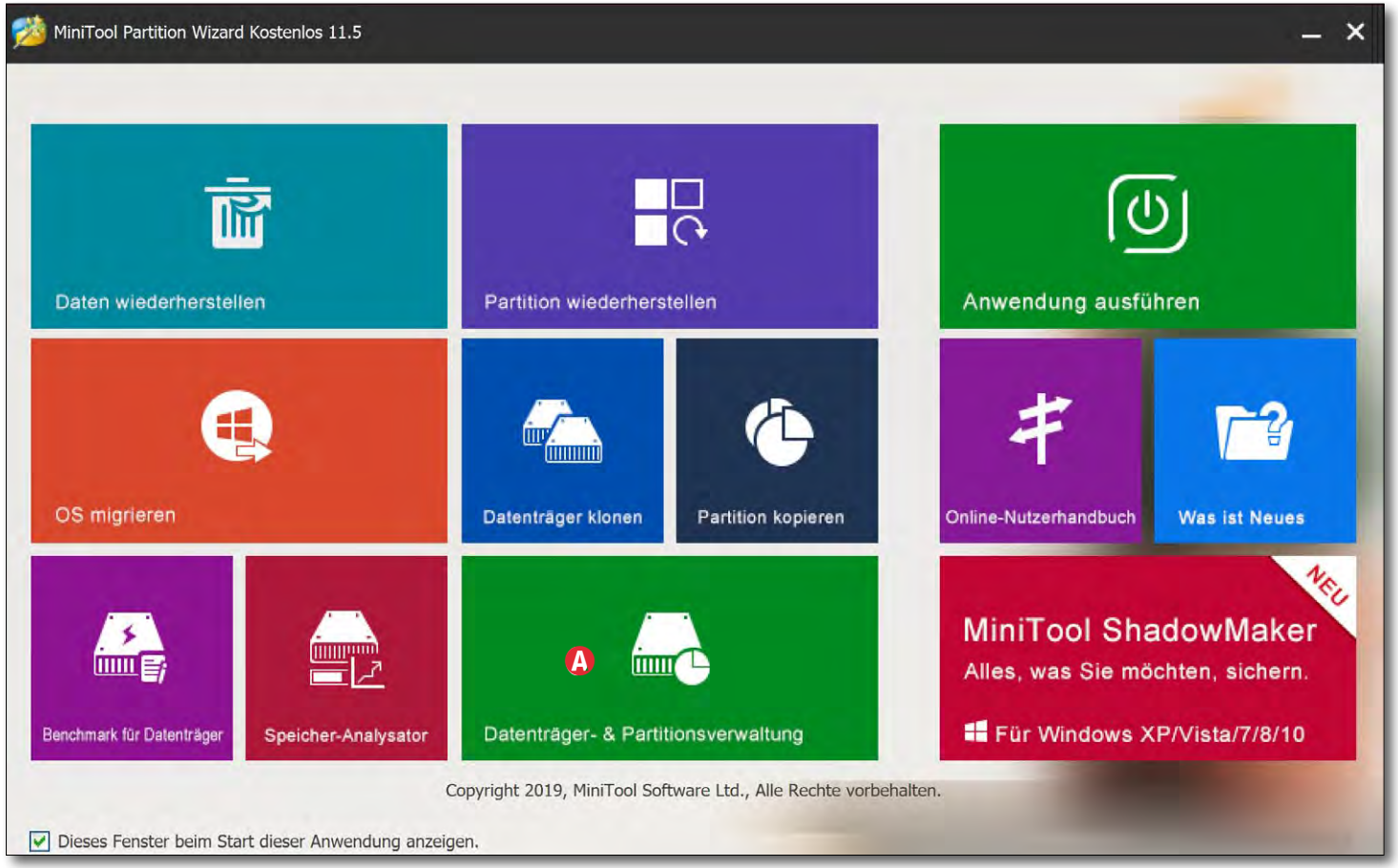


Abb. 5: *MiniTool Partition Wizard* ist eine Werkzeugsammlung verschiedener Tools zur Handhabung von Laufwerken und Partitionen. Aus diesem Panel ruft man per Klick die verschiedenen Werkzeuge auf.

Das Migrieren des Betriebssystems auf eine andere Festplatte oder eine SSD ist nur ein Beispiel dafür. Es entsteht dabei ein Klon auf ›intelligente Weise‹. Der Vorteil beim Migrieren besteht darin, dass der Zieldatenträger auch kleiner als das Quelllaufwerk sein darf (sofern die Daten alle darauf passen), was häufig der Fall ist, wenn man das System von einer Magnetplatte auf eine wesentlich schnellere SSD migriert. (Zuvor lohnt es sich aber, das System aufzuräumen – etwa mit der Windows-Funktion *Systembereinigung*.)

Auch die Überprüfung und Fehlerbehebung einer Partition – korrekt: des Dateisystems auf der Partition – wird angeboten. Ebenso kann man ein Laufwerk partitionieren und die Partitionen ›formatieren‹ (mit einem Dateisystem belegen). Wir finden hier auch zahlreiche Funktionen zu Partitionen, die man zwar selten benötigt, die im Einzelfall aber praktisch sein können – etwa das Aufteilen einer Partition, das Verkleinern und Vergrößern, die Anzeige der Block-/Sektorengröße und der Clustergröße sowie das Ändern der Clustergröße einer Partition. Man kann bei Bedarf sogar ein FAT-Dateisystem in ein NTFS (und umgekehrt) konvertieren.

Selbst ein Oberflächentest ist möglich, um defekte Blöcke zu finden und auszublenden. Da er nur die Blöcke liest, aber nicht beschreibt, ist er nicht destruktiv. Viele dieser mit *Partition Wizard* möglichen Operationen setzen aber einiges an Know-how und große Sorgfalt voraus.

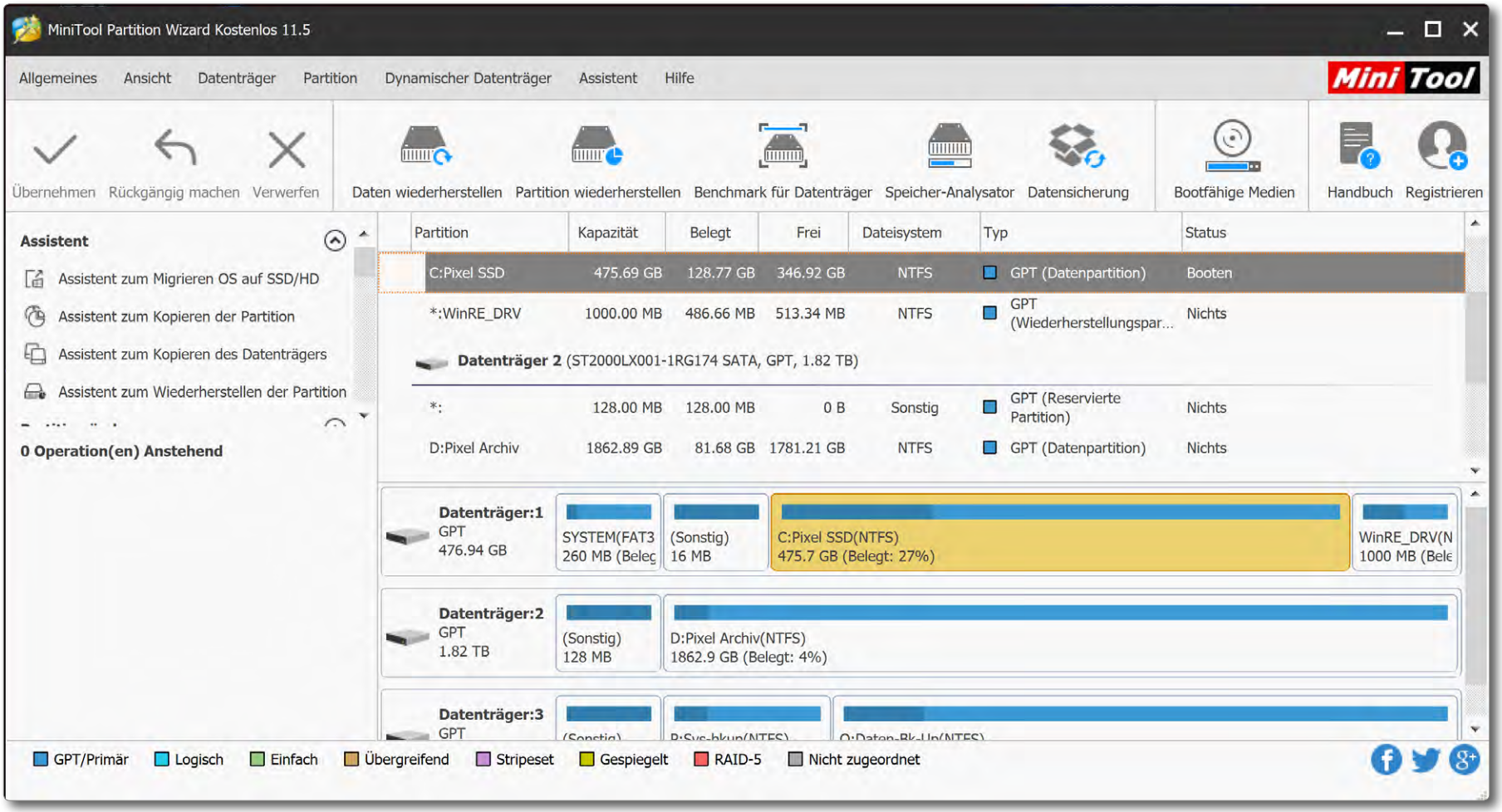


Abb. 6: Die Funktion *Datenträger- & Partitionsverwaltung* von *MiniTool Partition Wizard* zeigt mehr Informationen als die *Datenträgerverwaltung* von Windows und bietet eine ganze Reihe weiterer Funktionen an – etwa einen *Benchmark für Datenträger* oder die Sicherung von Datenträgern.

Einige der angezeigten Funktionen sind jedoch nicht in der kostenlosen Lite-Version enthalten, sondern setzen die kostenpflichtige Pro- oder gar die Server-Edition voraus. So ruft die Funktion *Datensicherung* in der Kopfleiste beispielsweise die Anwendung *MiniTool ShadowMaker Pro* auf (eine andere, kostenpflichtige Anwendung). Für die einfachen Operationen kommt man aber vollkommen mit der kostenlosen Version aus. Hierzu gehören beispielsweise Partitions-Informationen auslesen, Datenträger partitionieren, Partitionen verkleinern oder vergrößern, ein System auf SSD migrieren, Benchmark für Datenträger. Die (kostenlose) Funktion *Speicher-Analysator* zeigt in drei unterschiedlichen Ansichten die Speicherbelegung des gewählten Volumes mit der absoluten Größe und in Prozent die Dateien und Verzeichnisse auf dem Volume. So findet man relativ schnell die ›Speicherfresser‹.

Nicht nur die Oberfläche des gesamten Werkzeugs präsentiert sich in Deutsch, sondern auch das relativ ausführliche Benutzerhandbuch.

EaseUS Partition Master

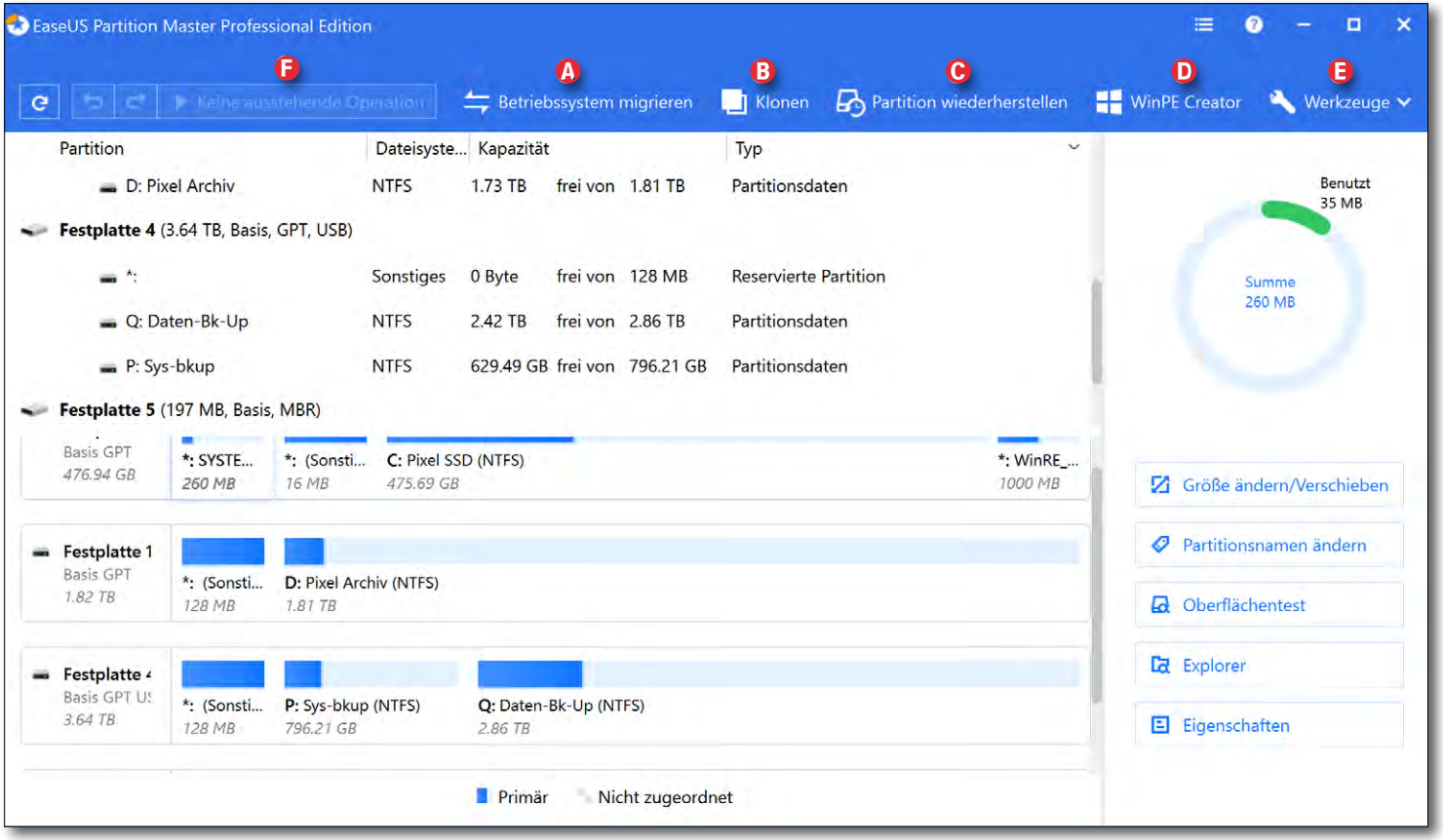


Abb. 7: *EaseUS Partition Master* ist ein weiteres Werkzeug zur Erstellung und Bearbeitung von Partitionen, bietet unter *Werkzeuge* (Ⓔ) aber eine Menge weiterer Funktionen – etwa das Klonen einer einzelnen Partition oder einer ganzen Festplatte oder SSD.

Für einige Operationen ist *EaseUS Partition Master* [25] eine Alternative zur Windows-*Datenträgerverwaltung* oder zum zuvor angesprochenen *MiniTool Partition Wizard*. *EaseUS Partition Master* erlaubt in seiner kostenlosen Version nicht nur Laufwerke zu formatieren/partitionieren, sondern zeigt auch deren Partitionierung an und ob das Laufwerk eine MBR- oder GPT-Strukturierung hat (Abb. 7). Zusätzlich bietet es Funktionen zur Sicherung und zum Klonen von Laufwerken und Partitionen. Wie beim *MiniTool Partition Wizard* gibt eine Reihe von Funktionen, für die man die kostenpflichtige Pro-Version benötigt.

Ich beschränke mich hier auf die Beschreibung der Funktionen zum Umgang mit Partitionen bei der kostenlosen Version.

Die üblichen Operationen – Formatieren und Partitionieren eines Datenträgers, Partitionsnamen ändern, Vergrößern oder Verkleineren von Partitionen – werden hier sehr ähnlich durchgeführt wie mit der Windows-*Datenträgerverwaltung*.

Partition Master erlaubt unter der Funktion *WinPE Creator* (Ⓓ) die sehr einfache Erstellung eines Boot-Mediums mit *WinPE* darauf. Dies kann auf einer CD/DVD oder einem USB-Stick erfolgen oder man kann ein entsprechendes ISO-Image erstellen (eine Datei auf einem Volume). Verwendet man einen USB-Stick, so wird dieser zuvor neu formatiert – alle dort vorhandenen Daten gehen dabei verloren. Die Funktion führt den Anwender in einfachen Schritten durch den Prozess. **Man muss aber darauf achten, den richtigen Zieldatenträger auszuwählen!**

Auch die Funktion *Betriebssystem migrieren* (Ⓐ) erweist sich als nützlich, wenn man das Systemlaufwerk auf ein anderes Laufwerk oder sogar auf einen anderen Rechner übertragen möchte. Nach der Basiskonfiguration für diese Operation wird der aktuelle Rechner neu gestartet. Ein Minimalsystem führt dann die eigentliche Operation durch, was eine Weile dauern kann.

Oberflächentest

Selektiert man ein Laufwerk in der Liste oben, so bieten das Kontextmenü (Abb. 9) oder die Funktionsliste rechts dazu einen *Oberflächentest* an. Dieser testet das fehlerfreie Lesen jeden einzelnen Blocks des Laufwerks und zeigt das Ergebnis grafisch an. Ein solcher Test ist sowohl bei neuen Platten vor deren erster Nutzung

sinnvoll als auch dann, wenn Zweifel an der Fehlerfreiheit einer Platte aufkommen.[1] Der Test nimmt allerdings – abhängig von der Größe des Datenträgers – einige Zeit in Anspruch. Das Ergebnis wird grafisch angezeigt (Abb. 8).

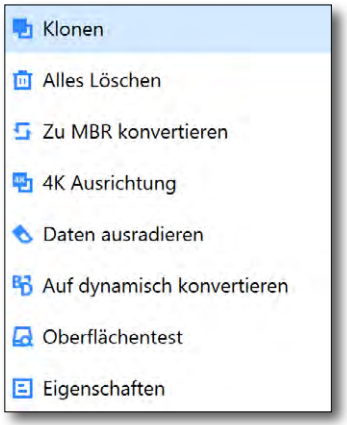


Abb. 9: Kontextmenü zu einem selektierten Laufwerk bzw. einer selektierten Partition

Unter den Werkzeugen (Abb. 7 Ⓔ) findet man drei weitere Funktionen:

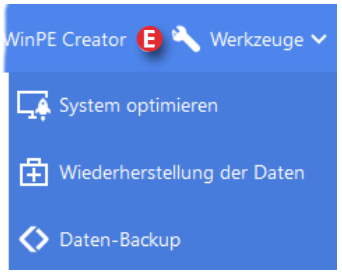


Abb. 10: Kontextmenü zu einem selektierten Laufwerk bzw. einer selektierten Partition

1 Eine sehr ähnliche Funktion bietet das ebenso kostenlose Programm *HDDScan* [37] an.

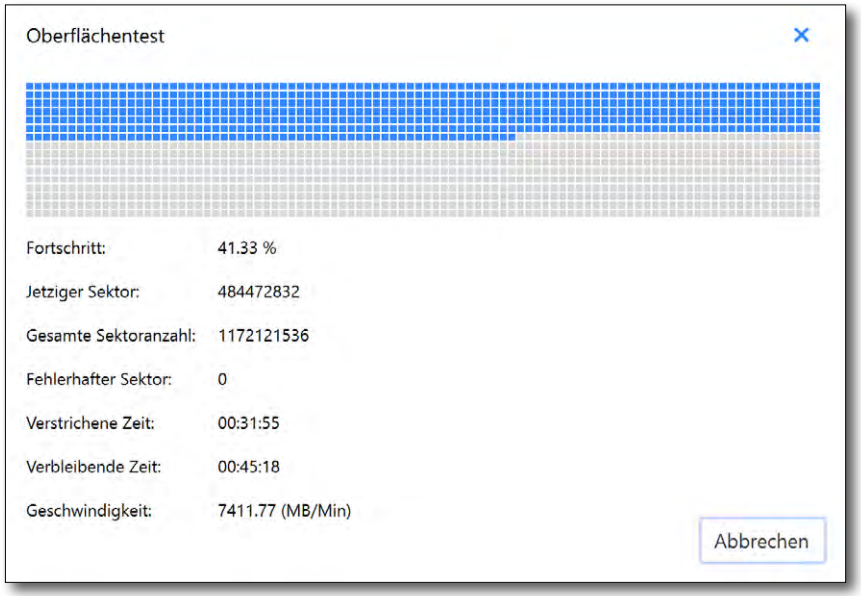


Abb. 8: Der Oberflächentest gibt Aufschluss darüber, ob sich alle Blöcke der Platte fehlerfrei lesen lassen.

Die Funktion *System optimieren* ruft ein spezielles Modul (einen separaten Prozess) auf, um verschiedene Optimierungen durchzuführen, etwa *Jung-Dateien aufräumen*. *Große Dateien aufräumen* startet die Suche nach und die (eventuelle) Bereinigung großer Dateien, und unter *Disk optimieren* findet man Funktionen zur Analyse und Defragmentierung von Laufwerken.

Daten-Backup ruft die Anwendung *EaseUS Todo Backup Free* auf – ein weiteres Tool, um Backups zu erstellen (von dem es natürlich auch eine *Pro*-Version gibt, deren Kauf hier beim Aufruf angeboten wird). Man muss es bei Bedarf zunächst herunterladen.

Auch *Datenwiederherstellung* ruft ein separates Werkzeug auf (*EaseUS Data Recovery Wizard*), das es erlaubt, gelöschte Dateien (soweit nicht bereits überschrieben) oder Dateien von einem defekten Medium – z. B. einer Kamera-Speicherkarte – zu retten.

Zusammenfassung

EaseUS Partition Master hat einen reichen Funktionsumfang – selbst in der kostenlosen Version. Es gibt aber eine Reihe kleiner Macken. So werden in der Anzeige einige wichtigen Angaben abgeschnitten (zumindest bei deutscher Oberfläche, wie in Abbildung 7 unten bei ›Festplatte 2‹ zu sehen).

Auch ist nicht deutlich erkennbar, welche angezeigten Funktionen bereits in der *Free*-Version und welche nur in den kostenpflichtigen Versionen (*Pro* und *Server*) zur Verfügung stehen. Um dies zu erfahren, muss man in die Vergleichsübersicht der Firma gehen (hier).

Ein wirkliches Manko der Anwendung besteht darin, dass – zumindest in der Free-Version – die Online-Hilfe nur umständlich erreichbar ist. Man wird dazu auf die Produktseite von *EaseUS* geführt, muss einige Dinge bestätigen und kommt erst dann an die gewünschte Information. Und dass bei einigen der Funktionsaufrufe einem jedes Mal ein Upgrade auf die Pro-Version oder der Kauf einer anderen Funktion nahegelegt wird, ist zwar nachvollziehbar, oft aber einfach nur lästig.

Die im Startfenster angebotenen Funktionen Ⓐ (*Betriebssystem migrieren*), Ⓑ (*Klonen*) und Ⓔ (*WinPE Creator*) erweisen sich aber für die angesprochenen Aufgaben als nützlich. Wie war das mit dem geschenkten Gaul?

ShadowExplorer

Leider verzichtet Windows (wie auch macOS) bisher auf eine komfortable grafische Oberfläche, um aus einer Volume-Schattenkopie (siehe Seite 113) einzelne Dateien oder Ordner zu extrahieren, um versehentlich gelöschte oder defekte Dateien zu ersetzen.

ShadowExplorer [22] setzt hier an. Es erlaubt, in den Schattenkopien eines NTFS-Volumes zu browsen und einzelne Dateien oder Ordner zu exportieren. (**Diese Möglichkeit macht aber in keinem Fall Sicherungen überflüssig!**)

Damit dies überhaupt möglich ist, muss das betreffende Volume (wie auf Seite 113 beschrieben) ein NTFS-Volume sein, der Computerschutz muss für das Volume aktiviert und Schattenkopien müssen zuvor einmal erstellt sein.

Den kostenlosen *ShadowExplorer* gibt es sowohl in einer Version für eine normale Installation als auch als portable Version, die man auf einem USB-Stick hält und die keine explizite Installation erfordert. Diese Variante ist für Systemadministratoren gedacht, die einem Anwender bei defekten oder verlorenen Dateien helfen müssen. Die Oberfläche ist zwar englisch, aber so einfach, dass man auch ohne große Englischkenntnisse damit zurechtkommen dürfte.

Nach dem Aufruf scannt die Anwendung zunächst die vorhandenen Volumes auf Schattenkopien. Unter dem Menü Ⓐ findet man die

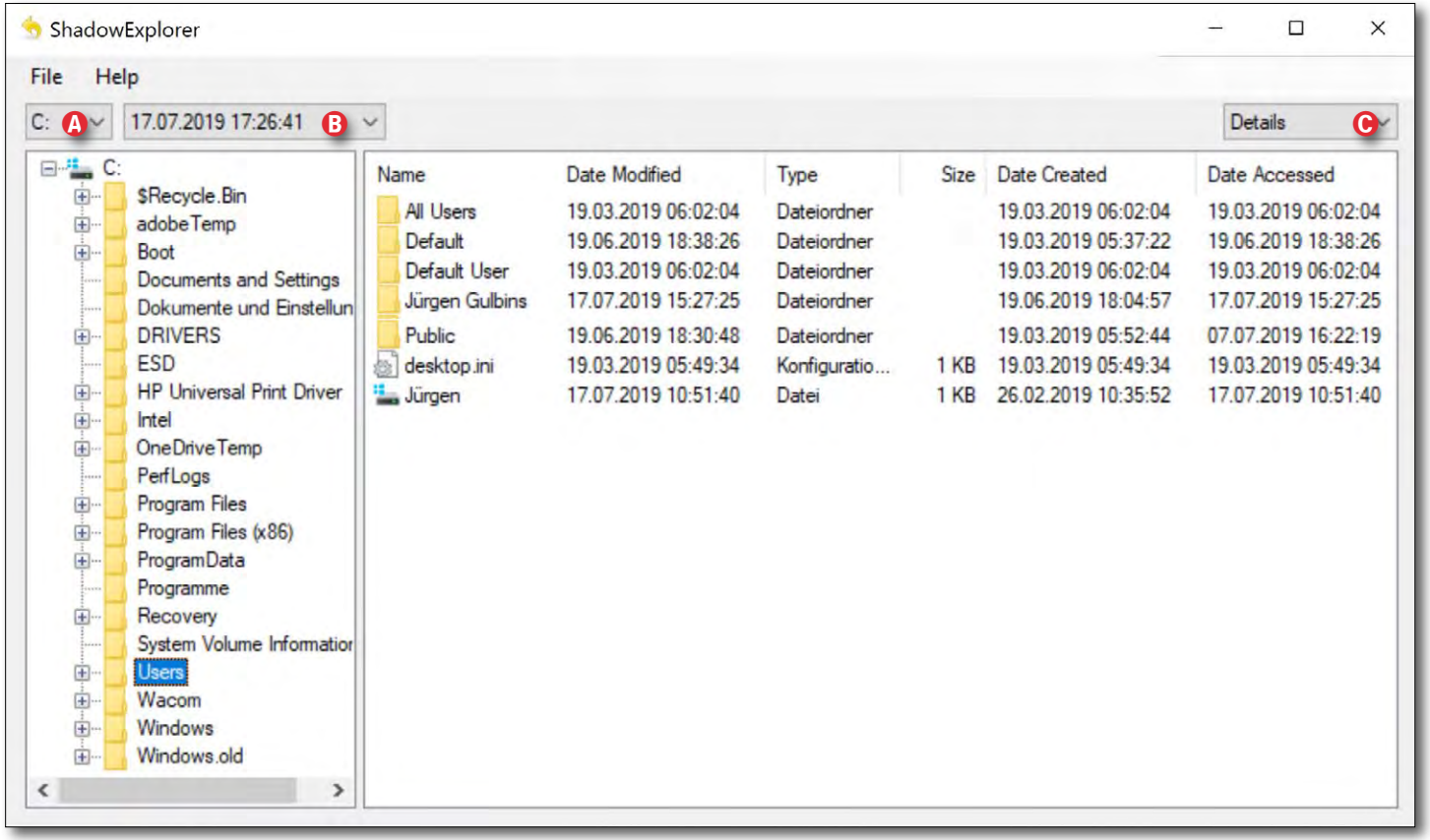


Abb. 11: *ShadowExplorer*-Fenster. Es zeigt hier den Inhalt der Laufwerks C:\ Ⓐ mit der Schattenkopie vom 17.07.2019 Ⓑ und rechts die Dateien und Ordner des links gewählten Ordners *Users*. Als Ansichtsoption wurde unter © *Details* gewählt.

Laufwerke (Volumes). Hat ein Laufwerk keine Schattenkopien, sind die beiden Listenfenster leer. Findet man in der rechten Liste Einträge, ist es praktisch, in der linken Liste über das kleine +-Zeichen das Volumeverzeichnis auszuklappen und zunächst in dieser Liste den gewünschten Ordner auszuwählen.

Oben, im Menü Ⓑ, findet man die Schattenkopien des Volumes. Hier wählt man die gewünschte Version (den Zeitpunkt) aus. Von den Darstellungsoptionen © habe ich *Details* als am informativsten empfunden.

Es empfiehlt sich, den Raum für die linke Liste mit der Maus etwas breiter zu ziehen und in dieser Liste zu navigieren, bis man rechts die gewünschte Datei oder das gesuchte Verzeichnis findet.

Diese selektiert man und ruft über das Kontextmenü (rechte Maustaste) die Funktion *Export* auf. Im Datei-Browser, der nun erscheint, gibt man ein Zielverzeichnis vor und kann dafür optional einen neuen Ordner anlegen. Ein Klick auf *OK* führt den Export dann durch. Das war schon alles – einfach, zuweilen aber nützlich.

Ich breche hier ein wenig mit der Beschreibung und den Anwendungen. *fsutil* ist keine Windows-Anwendung mit grafischer Oberfläche, sondern ein Kommando auf Kommandoebene. *fsutil* liefert eine ganze Reihe von Informationen zu einem Dateisystem bzw. Volume und erlaubt einige Operationen auf einem angegebenen Volume. **Letztere sollte man nur ausführen, wenn man weiß, was man tut.** Für viele der Funktionen benötigt man Administrationsrechte.

Für die Eingabe gibt man zunächst im Windows-Suchfenster (zumeist unten links) *cmd* ein, um das Kommadofenster zu erhalten. Von dort aus lässt sich das *fsutil*-Kommando aufrufen.

›**fsutil fsInfo drives**‹ listet alle aktuell aktiven Laufwerke (Volumes) auf (Abb. 12 Ⓐ).

›**fsutil fsInfo ntfsInfo P:**‹ liefert sehr detaillierte Informationen vom Volume *P* (Abb. 12 Ⓑ).

›**fsutil volume dismount P:**‹ deaktiviert beispielsweise das angegebene Volume (Abb. 12 Ⓒ).

›**fsutil fsInfo drivetype G:**‹ gibt Auskunft über den Laufwerkstyp des angegebenen Volumes/Laufwerks (Abb. 12 Ⓓ).

Ich möchte hier nicht die vollständige Syntax und alle Möglichkeiten des Kommandos beschreiben, sondern mich auf wenige Funktionen beschränken.

›**fsutil**‹ ohne weitere Parameter aufgerufen liefert eine kurze Übersicht zu den verfügbaren Funktionen, ohne aber weitere Informationen zu den einzelnen Funktionen bzw. deren weitere Parameter zu geben.

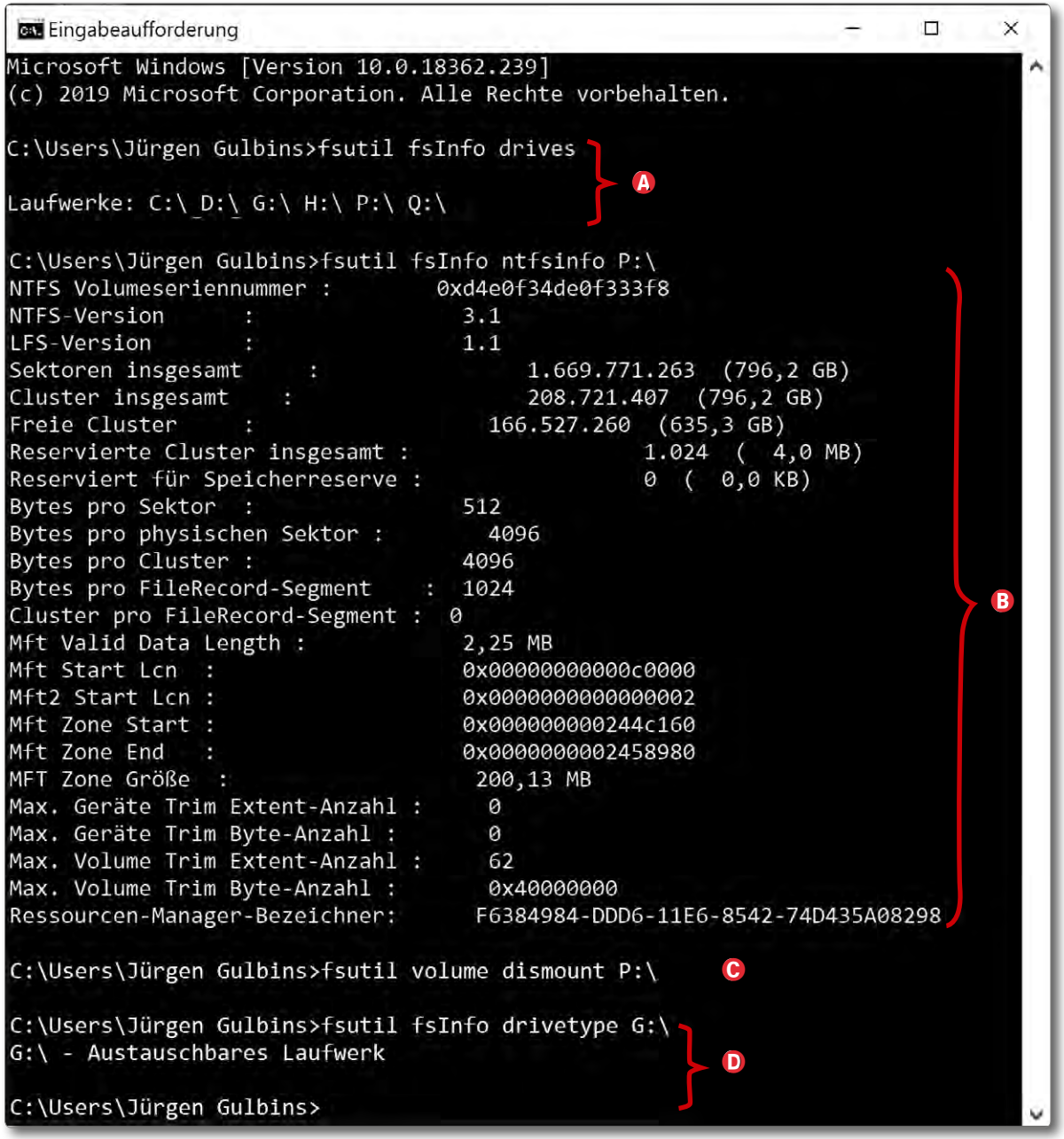


Abb. 12: Vier Beispiele für Informationen, die *fsutil* liefern kann.

God's Mode

Programmierer haben verrückte Ideen, so auch bei dem hier vorgestellten *God's Mode*; frei übersetzt und ein bisschen blasphemisch der *Gottes-Modus*. Gemeint ist damit ein Ordner mit einem sehr speziellen Namen auf dem Desktop. Ist er vorhanden, so findet man darin an einer Stelle eine Vielzahl von Verwaltungs- und Einstellungsfunktionen.

Dazu legt man einfach auf dem Desktop einen neuen Ordner mit folgendem eigenartigen Namen an: **›GM.{ED7BA470-8E54-465E-825C-99712043E01C}‹** (ohne die kleinen spitzen Klammern, wohl aber mit den geschweiften Klammern). Den Namensteil vorne (hier ›GM‹) können Sie frei wählen. Der Name wird auf dem Desktop übrigens nicht angezeigt, dafür aber folgendes Icon:  . Was aber bewirkt dieser eigenartige Modus?

Ein Klick auf den Ordner zeigt eine ganze Reihe von für die Systemverwaltung erforderlichen Funktionen/Programmen, die man damit im direkten Zugriff hat, was oft praktisch ist. Abbildung 13 präsentiert nur einen kleinen Ausschnitt. Ein langes Suchen und Navigieren über viele Panels kann damit entfallen. Scrollen Sie in dieser Ordneransicht einmal nach unten, um zu sehen, was man Ihnen hier alles kompakt liefert – bei mir sind es 216 Elemente.

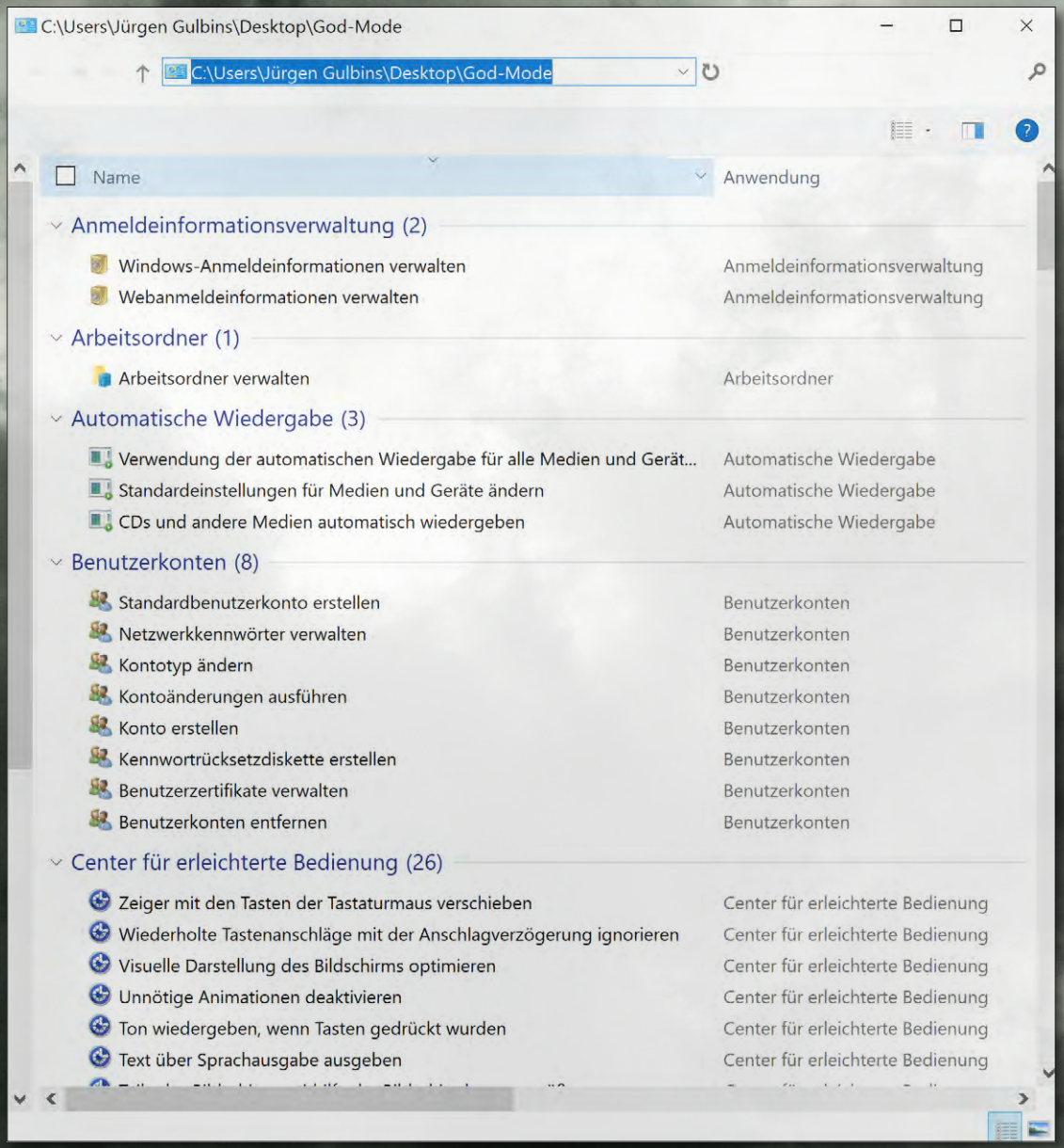


Abb. 13: Ausschnitt der Funktionen und Programme, die wir kompakt auf dem Windows-Desktop finden in dem Ordner mit der eigenartigen Endung ›.{ED7BA470-8E54-465E-825C-99712043E01C}‹ und dem Icon  .

Schlussbemerkung

Die in diesem E-Book behandelten Themen sind vielfältig, teilweise komplex und darüber hinaus einem ständigen Wandel unterworfen. Trotzdem muss man sich auch als normaler PC-Anwender – z. B. als Fotograf – in einem gewissen Umfang damit auseinandersetzen, auch wenn man im täglichen Betrieb über längere Phasen nicht damit konfrontiert wird, abgesehen von einer praktisch immer erforderlichen Datensicherung. Lassen Sie sich also nicht allzu sehr von der Komplexität verunsichern. Ziel des E-Books ist es, Ihnen sinnvolle und hoffentlich hilfreiche Informationen und Hinweise an die Hand zu geben und nicht, Sie mit unnötigen Informationen und Begriffen zu erschlagen. Lassen Sie sich im Bedarfsfall von einem Bekannten bei den komplexeren Themen helfen.

Es bleiben aus meiner Sicht zum Schluss folgende Ratschläge:

- Lesen Sie sich die Beschreibungen hier bei Interesse und Bedarf mehrmals durch.

- Arbeiten Sie bei den hier behandelten Themen sehr sorgfältig und immer ohne Hast.

- Seien Sie bei der Beschaffung von Datenträgern nicht zu knausrig, was die Kapazität betrifft, die Qualität und die Geschwindigkeit der Laufwerke. Geben Sie auch für Backup-Anwendungen lieber ein paar Euro mehr aus, um stabile, aktuelle, robuste und gute bedienbare Software zu bekommen.

- Automatisieren Sie Ihre Sicherungsläufe (zeitgesteuert) und überprüfen Sie von Zeit zu Zeit, ob Fehler aufgetreten sind. Spielen Sie ebenso gelegentlich zum Test Daten zurück.

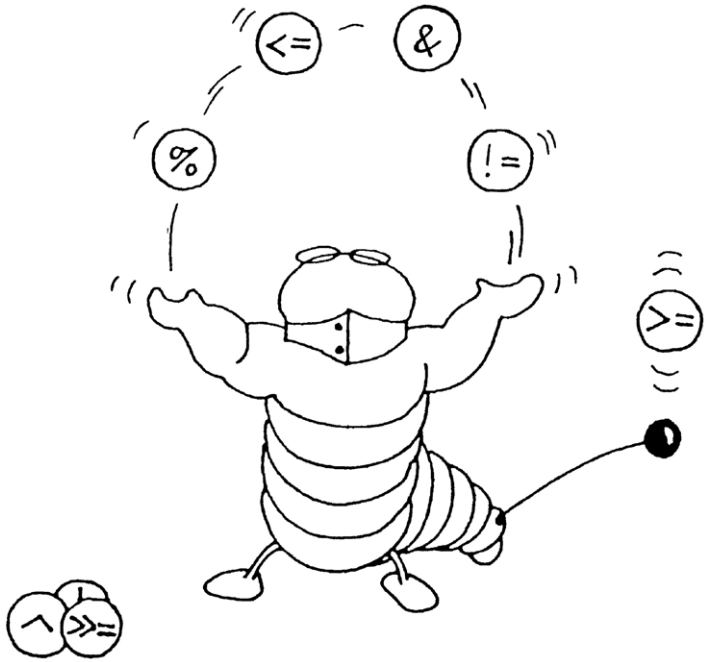
- Üben Sie das Zurückspielen, **bevor** es zu einem Bedarfsfall dafür kommt. Im Bedarfsfall sollte der Ablauf bekannt sein.

- Versuchen Sie alles so einfach wie möglich zu halten – Komplexität reduziert die Übersicht und erhöht die Wahrscheinlichkeit von Handhabungsfehlern.

Der Fluch der kostenlosen Software/Downloads

Ich habe hier versucht, die Kosten für Software sinnvoll gering zu halten, und deshalb eine ganze Reihe durchaus guter kostenloser Software aufgeführt. Und gegen diese möchte ich nicht argumentieren. Einige der Programme versuchen beim Download jedoch, Ihnen weitere ›kostenlose Anwendungen‹ mit auf den Rechner zu packen – verstärkt im Windows-Umfeld. Einige der kostenlosen Zusätze verankern sich recht tief im System. Man sollte bei Downloads deshalb sehr sorgfältig darauf achten, die Zusätze beim Herunterladen zu vermeiden.

Andere kostenlose Anwendungen versuchen Ihnen bei jedem Aufruf eine erweiterte, kostenpflichtige Pro-Version aufzudrängen. Dies ist oft lästig; benötigt man das Programm selten, ist es tolerier- und ignorierbar. Zuweilen lohnt sich aber auch ein kostenpflichtiges Update/Upgrade auf die kostenpflichtigen Versionen, sofern man die Anwendung häufig einsetzt und die funktionalen Erweiterungen ausreichende Vorteile bieten.



Nach einiger Zeit und mit etwas Übung sollte Ihnen der Umgang mit Datenträgern, Dateisystemen und Sicherungen leichtfallen, und Sie sollten sich sicher darin fühlen. Unter Umständen hilft ein Spickzettel – oder dieses E-Book.

Eine letzte Anmerkung

Natürlich bin auch ich nicht perfekt. Sollte ich falsche Informationen veröffentlicht oder etwas nicht richtig verstanden oder dargestellt haben, so wäre ich dankbar für Hinweise. Sollten Sie für bestimmte Aufgaben bessere Lösungen finden oder andere Erfahrungen machen, so würde ich mich über einen Bericht oder Korrekturen oder ein Telefongespräch von Ihrer Seite freuen.

Quellen und Programme

[1] Die Firma *Tuxera* bietet eine Reihe von Produkten, um Dateisysteme fremder Betriebssysteme anlegen, davon lesen und darauf schreiben zu können. So erlaubt die Systemerweiterung *Tuxera NTFS,* unter macOS auf Windows-NTFS-Systeme zugreifen zu können. *Tuxera HFS+* und *Tuxera APFS* erlauben wiederum, von Windows (7, 8, 10) aus auf die Dateisysteme HFS+ bzw. APFS von Apple zugreifen zu können, wobei von einem APFS-Volume bisher nur gelesen werden kann.
https://www.tuxera.com

[2] Eine recht detaillierte, verständliche Beschreibung der verschiedenen RAID-Techniken mit Angaben zur Mindestanzahl von Laufwerken und zur Ausfallwahrscheinlichkeit (totaler Datenverluste) findet man bei Wikipedia:
https://de.wikipedia.org/wiki/RAID

[3] Die Firma *Bombich* entwickelt und vertreibt (ausschließlich über das Internet) die Anwendung *Carbon Copy Cloner* – ein sehr gutes Backup-Programm für macOS. Es kann auch bootfähige System-Klone erzeugen (siehe Seite 50). Beim Schreiben des Artikels ist CCC 5.1.8 die aktuellste Version. Es steht eine 30-tägige Testversion zum Download zur Verfügung:
https://bombich.com/de

[4] *FreeFileSync* ist ein kostenloses Open-Source-Programm zum Datenabgleich zwischen einer Quelle und einem Ziel (siehe Seite 100). Die Quelle können einzelne Dateien, ganze Ordner oder sogar ein ganzes Volume sein. Da die Anwendung mit normalen Benutzerrechten läuft, kann sie jedoch nur Dateien und Ordner übertragen (und bei Bedarf löschen), auf die der aufrufende Anwender Zugriffsrechte hat. Deshalb lassen sich damit keine System-Klone erstellen. Das Programm steht für Windows, macOS sowie für verschiedene Linux-Distributionen zur Verfügung.

Beim Download muss man darauf achten, nicht ungewollt weitere angebotene Anwendungen mit herunterzuladen: https://freefilesync.org

[5] Die Firma *Solesignal Ltd.* bietet mit *SmartBackup* ein recht schönes, übersichtliches und kostenloses Werkzeug zur Datensicherung unter macOS (inkl. 10.14) an – zur Sicherung und Synchronisierung (siehe Seite 64). Die Oberfläche ist (auch) deutsch, alle Hilfedateien jedoch englisch:
https://solesignal.com/smartbackup4/

[6] *ChronoSync* ist eine wirklich gute Backup-Software für macOS. Es stammt von der Firma *Econ Technologies*, hat (auch) eine deutschsprachige Oberfläche und kann sowohl einzelne (und mehrere) Ordner als auch ganze Volumes sichern (synchronisieren) und bootfähige System-Klone erzeugen. Das Backup kann sowohl Zeit- als auch Ereignis-gesteuert erfolgen (siehe Seite 58). Neben *ChronoSync* bietet Econ das etwas vereinfachte und etwas billigere *ChronoSync Express* an.
https://www.econtechnologies.com

[7] *Acronis True Image* ist eine der Standard-Anwendungen zur Erstellung von System-Klonen und zum Backup ganzer Laufwerke (inklusive aller dort vorhandenen Partitionen/Volumes) unter Windows. Die Anwendung verwendet im Standardfall ein spezielles Backup-Format, in dem Dateien komprimiert und verschlüsselt werden können. Die Anwendung erlaubt in einer eigenen Funktion das komplette oder selektive Zurückspielen (siehe Seite 94). Es gibt eine funktional etwas reduzierte Version auch für macOS.
https://www.acronis.com/de-de/

[8] *SuperDuper!* der Firma *Shirt Pocket* ist ein recht schönes Backup-Werkzeug für macOS. Es ist mit 27 Euro relativ preiswert, erlaubt ein bequemes Synchronisieren von Daten und kann auch Backups bzw. Klone der System-Partition erstellen (siehe Seite 55). Es kommt dabei sowohl mit HFS+- als auch (seit Version 3.2.4) mit APFS-Volumes zurecht. Es kann bei APFS-Systemen auch Snapshots erstellen. Man kann das Programm kostenlos herun-

terladen und mit dieser Testversion System-Clones erstellen (ohne Zeitlimit). Es hat eine englische Oberfläche. https://www.shirt-pocket.com

[9] Der kostenlose *TimeMachineEditor* (beschrieben auf Seite 49) erlaubt es, die Sicherungsintervalle von Apples *Time Machine* flexibel zu steuern: https://tclementdev.com/timemachineeditor/

[10] *Get Back Pro* der Firma *Belight Software* ist mit etwa 20 USD eine relativ preiswerte Backup-Lösung für macOS, leider nur mit englischer Oberfläche, aber sehr übersichtlich gestaltet. Sie bietet für die Datensicherung eine Archivierung (in eine Art Image-Datei) sowie eine Synchronisierung von Quelle und Ziel. Sie kann auch ganze Volumes klonen und dabei bootfähige Systeme erzeugen: https://www.belightsoft.com/products/getbackup/

[11] *SynKron* ist ein kostenloses Programm zur Synchronisation von Ordnern unter macOS, Linux und Windows. Neben der englischen gibt es auch eine deutsche Oberfläche. Die Anwendung ist jedoch nicht in der Lage, einen bootfähigen Klon der Systemplatte zu erstellen. Die ›portable‹ Version kann ohne Installation von einem USB-Stick herunter benutzt werden. http://synkron.sourceforge.net

[12] Lloyd Chambers bietet auf seiner Webseite diglloyd.com verschiedene Tools an, darunter die *diglloydTools* mit dem *IntegrityChecker*, der es erlaubt, die Integrität von Dateien mittels Prüfsummen zu überprüfen: https://macperformanceguide.com

[13] Auf dieser Apple-Support-Seite finden Sie Informationen zum *Startsicherheitsdienstprogramm* von macOS (bei Systemen mit einem T2-Sicherheitschip): https://support.apple.com/de-de/HT208198

[14] Die Firma *GoodSync* bietet verschiedene Backup-Lösungen auch mit deutscher Oberfläche an, angefangen von einer kostenlosen Version für eine private Nutzung über *GoodSync* für OS-Server und ein Backup-Kontrollzentrum und dies für unterschiedliche Plattformen (macOS, Windows, Linux/Unix): https://www.goodsync.com/de/

[15] *Black Magic Speed Test* ist ein kostenloses Programm, das es erlaubt, die Geschwindigkeit verschiedene Datenträger zu testen und zu vergleichen: https://apps.apple.com/de/app/blackmagic-disk-speed-test/id425264550?mt=12

[16] Die Firma *MiniTool Software Ltd.* bietet mit dem Programm *MiniTool ShadowMaker* ein für den privaten Anwender kostenloses Werkzeug an (auch mit deutscher Oberfläche), um Windows-Systeme zu klonen – etwa von einer Betriebssystem-Partition auf eine andere Platte oder auf eine SSD. Das Ziellaufwerk darf dabei sogar kleiner als das Quelllaufwerk sein, muss aber natürlich ausreichend Platz für alle Daten der Quelle bieten. Es gibt auch eine kostenpflichtige Pro-Version. Auch die Anwendung *MiniTool Partition Wizard* für die Formatierung von Laufwerken in einer kostenlosen und einer erweiterten kostenpflichtigen Version kann von Interesse sein. Eine Kurzbeschreibung von *MiniTool Partition Wizard* finden Sie auf Seite 118. https://www.partitionwizard.com

[17] Die Firma *Siber Systems* bietet mit *GoodSync* eine recht schöne Backup- und Synchronisationslösung für Windows und macOS. Von *GoodSync* gibt es mehrere Versionen: *GoodSyncFree*, die kostenlose Version (allerdings mit unschönen Einschränkungen), *GoodSync SE* sowie *GoodSync Pro* – jeweils mit zunehmenden Funktion. Die Version *GoodSync Connect* erlaubt Sicherungen auch auf iOS- und Android-Systemen. Die Version *GoodSync2Go* (für Windows) bietet (mit einigen Einschränkungen) Backup- und Synchronisationsfunktionen, ohne dass das Programm installiert werden muss – es kann von einem USB-Stick aus gefahren werden: https://www.goodsync.com/de/

[18] *AJA Systemtest* erlaubt sowohl unter macOS als auch unter Windows verschiedene Benchmarks zu fahren und das System zu testen – auch hinsichtlich der Datenträgergeschwindigkeit: https://www.sir-apfelot.de/festplatten-benchmark-tool-aja-system-test-4937/

[19] *DiskWarrier* ist ein Programm der Firma *Alsoft* unter macOS, das defekte Datenträgerstrukturen reparieren kann. Man braucht in der Regel bei einem Update des Betriebssystems auch ein Update der Anwendung: www.alsoft.com/DiskWarrior/

[20] *Disk Drill* ist eine Anwendung der Firma *508 Software LLC,* die dabei hilft, gelöschte Dateien wiederherzustellen (sofern sie nicht bereits überschrieben sind). Es gibt die Anwendung in einer kostenlosen sowie in zwei kostenpflichtigen Versionen: https://www.cleverfiles.com/de/pro.html

[21] Die Firma *2BrightSparks* bietet eine Reihe von Backup-Software für Windows an, darunter das kostenlose *SyncBackFree* (siehe dazu Seite 104) sowie die kostenpflichtigen Versionen *SyncBackSE* und *SyncBackPro*. https://www.2brightsparks.com/freeware/

[22] *ShadowExplorer* ist eine kostenlose Anwendung für Windows, die es erlaubt, in Schattenkopien des Systems zu navigieren und von dort Dateien und Ordner zu extrahieren, um versehentlich gelöschte oder defekte Dateien zu ersetzen (siehe dazu die Beschreibung auf Seite 122): https://www.shadowexplorer.com

[23] Die Firma *SiSoftware* bietet mit *SiSoftware Sandra Lite* eine kostenlose Version an, die sehr viel Informationen zur verbauten Hardware (und in Teilen auch zur installierten Software) Ihres Rechners liefert – und dies ohne Werbung und andere Störungen. Die Oberfläche ist (auch) in Deutsch (siehe Seite 117): https://www.sisoftware.co.uk/download-buy/

[24] *CPU Z* liefert wie *Sandra Lite* eine Menge Informationen zur Hardware (CPU, CPU-Caches, GPU, Mainboard, Memory Slots, …) eines Rechners in recht kompakter Form (mit englischer Oberfläche): https://www.cpuid.com

[25] *EaseUS Partition Partition Master* der Firma *EaseUS* ist ein Partitions-Manager (siehe Seite 120) (auch mit deutschsprachiger Oberfläche), der neben dem Formatieren und Partitionieren von Datenträgern auch verschiedene Backup-Funktionen bietet (einige Funktionen nur mit der ca. 54 € teuren Pro-Version). Mit *EaseUS ToDo Backup Pro* steht mit englischer Oberfläche eine Backup-Lösung auch unter macOS zur Verfügung. https://www.easeus.de/

[26] *CrystalDiskInfo* und *CrystalDiskMark* sind zwei kleine Anwendungen für Windows, die auch eine deutsche Oberfläche aufweisen. *CrystalDiskInfo* liefert eine Menge Informationen zu Ihren angeschlossenen Laufwerken; *CrystalMarkInfo* führt Messungen zur Lese- und Schreibgeschwindigkeit des ausgewählten Laufwerks durch (siehe auch Seite 116). Die Standard-Ausgaben beider Module sind für die private Nutzung kostenlos. Daneben gibt es kostenpflichtige Pro-Versionen. https://crystalmark.info/en/software/

[27] Die Firma *Mini Tool* bietet eine Reihe nützlicher Werkzeuge zum Umgang mit Laufwerken an. Dazu gehört z. B. *MiniTool Partition Wizard*, das es in drei Versionen gibt. Die Lite-Version ist dabei kostenlos. Die Pro-Version für etwa 40 USD und die Ultimate-Version für etwa 100 USD bieten funktionale Erweiterungen. Ein anderes Werkzeug der gleichen Firma ist *ShadowMaker* zur Datensicherung, ein weiteres *MiniTool Power Data Recovery*, um Daten von einem defekten Laufwerk zu retten – sowohl für Windows als auch für macOS und sowohl in einer kostenlosen als auch in einer mächtigeren Pro-Version. https://www.minitool.com

[28] Die Firma *AOMEI* hat ein ganzes Repertoire von Backup-Lösungen im Angebot, darunter den *AOMEI Backupper* in verschiedenen Versionen, etwa die kostenlose *Standard*-Version. Sie erlaubt Windows-Systeme zu sichern (in ein Image), zu klonen sowie Benutzerdateien zu sichern (synchronisieren). Wie (fast) üblich gibt es noch Pro-, Server- und Technician-Versionen mit jeweils erweiterten Funktionen und zu höheren Preisen: https://www.aomei.de

[29] *Personal Backup* ist eine kostenlose, recht ausgereifte Backup-Lösung für Verzeichnisse/Dateien unter Windows (7/8/10) von Dr. Jürgen Rathlev (beschrieben auf Seite 106). Die Anwendung kann jedoch kein bootfähiges Backup der Systempartition erstellen. Die deutschsprachige Dokumentation ist vorbildlich: http://personal-backup.rathlev-home.de

[30] Die Firma *Veeam* bietet ein breites Spektrum vom Backup-Lösungen an bis hin zu Dienstleistungen im Bereich Cloud-basierter Backups. Die meisten der Lösungen zielen auf mittlere und größere Unternehmen mit zahlreichen Rechnern ab. Leider sind die Oberflächen aber englischsprachig. https://www.veeam.com/vm-backup-recovery-replication-software.html

[31] Die US-Firma *Carbonite* bietet einen noch relativ preiswerten Cloud-Server für Backups, der Daten verschiedener Betriebssysteme relativ transparent mittels entsprechender Clients sichert und zurückspielen kann: https://www.carbonite.com/backup-software/

[32] Die Firma *iDrive* bietet eine relativ transparente Cloud-basierte Backup-Lösung (auch für unterschiedliche Plattformen) in verschiedenen Modellen an: https://www.idrive.com/

[33] Die englische Firma *Macriumsoftware* bietet unter dem Label *Macrium Reflect 7* ein recht breites Spektrum von Backup-Lösungen für Windows an, vom kostenlosen *Reflect 7 Free* bis hin zur Enterprise-Lösung *Reflect 7 Deployment Kit*. Die Oberfläche ist englisch und es ist eine Registrierung erforderlich: https://www.macrium.com/reflectfree

[34] *Backblaze* ist ein weiterer US-Anbieter für Cloud-basierte Backup-Lösungen mit einem für Privatanwender recht attraktiven Preis (ohne Speicherlimit). Unterstützt werden Clients für verschiedene Betriebssysteme (Windows, macOS). Im Notfall kann man sich statt einer Online-Wiederherstellung die Daten (kostenpflichtig) auch auf einer Festplatte zuschicken lassen: https://www.backblaze.com

[35] *IBM* bietet im Enterprise-Bereich verschiedene Backup-Lösungen an, darunter auch *Backup and Recovery* für macOS. Die große Lösung mit eigenem Archiv-Server, früher als *Tivoli Storage Manager* bezeichnet, heißt nun *IBM Spectrum Protect for Workstations*: https://www.ibm.com/de-de/marketplace/data-protection-and-recovery/specifications

[36] Microsoft *OneDrive* ist ein Cloud-Speicher, auf den man recht transparent von unterschiedlichen Plattformen (Windows, macOS, iOS, Android, …) aus zugreifen kann. Aktuell sind dort 5 GB kostenlos. Weiterer Speicher lässt sich anmieten: https://onedrive.live.com/about/de-de/

[37] *HDDScan* ist eine kleine kostenlose Software (mit englischer Oberfläche), um einen Festplattenoberflächen-Scan von Datenträgern durchzuführen. Damit wird überprüft, ob alle Blöcke fehlerfrei gelesen werden können. Optional kann auch ein fehlerfreies Schreiben getestet werden. Dies überschreibt aber den vorhandenen Inhalt! https://hddscan.com

[38] *Areca Backup* ist eine kostenlose, Open-Source-basierte Lösung zur Sicherung und zum Wiedereinspielen von Benutzerdaten mit zahlreichen

Möglichkeiten und einigen Plug-ins:
http://www.areca-backup.org/

[39] Folgender Artikel gibt eine kurze, relativ verständliche Einführung zu dem Mechanismus von *Snapshots* (*Schattenkopien*) unter Windows und deren Funktion bei VSS-basierten Backups:
https://www.computerweekly.com/de/definition/VSS-basiertes-Backup

[40] Wolfgang Gieseke: *Der Windows 10 Pannenhelfer.* Es gibt das Büchlein mit 177 Seiten als gedruckte Ausgabe oder als Kindle-Edition (nochmals kostengünstiger).
ISBN: 978-3-7392-4567-6 (Printausgabe), 2016
BoD – Books on Demand, Norderstedt

Index

Tabellenverzeichnis