Alle Windows-Programme aus diesem Beitrag finden Sie **auf der CHIP-DVD**

Daten weg? Nicht mit uns!

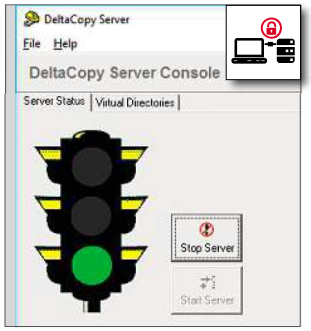
Unser Vier-Stufen-Plan sorgt für eine automatische Sicherung von **Fotos, Dokumenten und Betriebssystem** – lokal, im Heimnetz und in der Cloud. Die passende Software liefern wir auf der CHIP-DVD gleich mit

VON MARKUS MANDAU

Vier Sicherungsstufen

1 > Datenbackup vollautomatisch auf eine interne Zweitplatte mit Aomei Backupper

2 > Systemsicherung auf eine externe Festplatte – ebenfalls mit dem Backupper



3 > Heimnetz regelmäßig auf einem Server oder der NAS sichern

4 > Cloud gezielt mit den wichtigen Daten versorgen und mit BoxCryptor verschlüsseln

Von Urlaubsfotos bis zu geschäftlichen Verträgen – ein immer größerer Teil der für uns wichtigen Daten liegt nur noch elektronisch vor. Was vor zehn Jahren im Leitz-Ordner oder im Fotoalbum schlummerte, landet längst auf der Festplatte. Die digitale Speicherung ist praktisch, denn die Platte bietet viel mehr Platz für Fotos und Dokumente als Wohnzimmerschränke für Ordner und Alben. Die digitale Form der Archivierung verlangt aber nach Planung. Im Gegensatz zur sprichwörtlichen Geduld von Papier, das bei korrekter Lagerung Jahrhunderte überdauert, halten Bits und Bytes längst nicht so lange (siehe rechts). Ihre Ausfallquote steigt nach drei Jahren stark an – ab da droht der Datenverlust.

Regelmäßige Datensicherung

Im Gegensatz zu Papier lassen sich Bits und Bytes ohne großen Aufwand mittels Backup sichern – wenn man es rechtzeitig einrichtet. Zudem sollte sich niemand darauf verlassen, dass die Festplatte keinen Defekt hat oder beim Löschen von Daten keine Fehler passieren. Die professionellen Datenretter von Kroll Ontrack haben die Ursachen von Datenverlusten erfasst. Über die Hälfte geht auf Hardwareschäden zurück und ein Viertel auf menschliches Versagen. All diese Fälle hätten sich mit einem Backup verhindern lassen, das idealerweise regelmäßig und automatisch im Hintergrund stattfindet.

Wir zeigen Ihnen einen Vier-Stufen-Plan, mit dem Sie Ihre Backups ohne Aufwand auf dem neuesten Stand halten. Die Sicherung kann entweder auf einer zweiten lokalen Festplatte stattfinden, im Heimnetz oder in der Cloud. Laut der GfK nutzen immerhin schon 17 Prozent der Deutschen diese Möglichkeit. Die passende Software zum Einrichten der vollautomatischen Datensicherung in allen Szenarien liefern wir auf unserer CHIP-DVD. Bevor wir zur ersten Backup-Stufe kommen, steht noch ein wichtiger Schritt an, die Wahl der richtigen Hardware.

Die richtige Backup-Platte wählen

Jeder gute Backup-Plan beginnt mit einer Festplatte, egal ob es sich um eine NAS im Netzwerk oder einen zusätzlichen internen Datenträger im PC dreht. Letztlich landen alle Sicherungen auf einer Magnetplatte, und die soll trotz vieler Schreib- und Lesezugriffe möglichst lange halten. Man kann dazu normale PC-Platten nehmen, doch wer langfristig denkt oder eine Neuanschaffung plant, hat bessere Alternativen: Die Harddrive-Hersteller bieten seit ein paar Jahren spezielle Medien zur Archivierung an. Die Platten der Serien Red von Western Digital oder NAS von Seagate verwenden die gleichen Elektronikkomponenten wie normale PC-Platten, werden aber von einer Firmware gesteuert, die für den Dauerbetrieb optimiert ist und versucht, die Vibrationen der Platte zu minimieren. Die Lagermechanik ist auf Dauerhaltbarkeit ausgelegt.

Zudem sollen die Speichermedien leise und stromsparend laufen. Insgesamt versprechen die Hersteller für NAS-Platten eine um 35 Prozent höhere Lebensdauer im Vergleich zu den PC-Pendants, die auf Performance getrimmt sind. Dabei kommt es gerade bei NAS-Systemen nicht auf Höchstgeschwindigkeit an, denn die Netzwerkschnittstelle gibt das Tempo vor. So dreht die Red-Serie nur mit 5.900 Umdrehungen, was für den Datentransfer im Heimnetz ausreicht. Das reduziert nochmals Energieverbrauch und Wärmeentwicklung. Die NAS-Serie von Seagate läuft mit 7.200 Umdrehungen, was sie als Zweitplatte im PC empfiehlt.

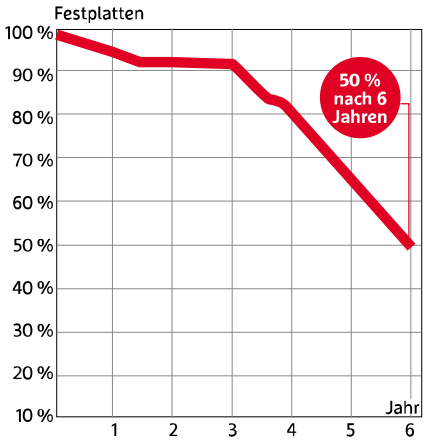
Steht die Hardware, kann man sich an die Einrichtung des Backups machen. In der ersten Stufe beschreiben wir, wie man mit unserer Vollversion Aomei Backupper Professional ein regelmäßig laufendes Datenbackup aufsetzt. Danach gehen wir zur Systemsicherung auf einem externen Medium über. In Stufe drei erfolgt die Sicherung im Netzwerk und zum Schluss die Einrichtung einer verschlüsselten Cloudanbindung.

Datensicherung in vier Stufen

Mit unseren vier Stufen haben wir die grundsätzlichen Backup-Möglichkeiten einzeln abgedeckt. Zur doppelten Absicherung der Daten können Sie verschiedene Stufen kombinieren – was sich →

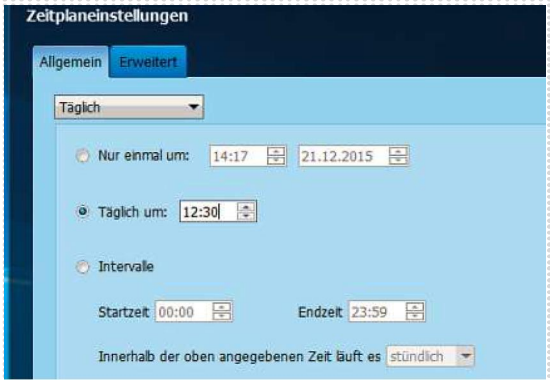
Ausfallquote für Magnetplatten

Die Frage lautet nicht ob, sondern wann: Beim Cloudanbieter Backblaze fällt nach sechs Jahren jede zweite Festplatte aus

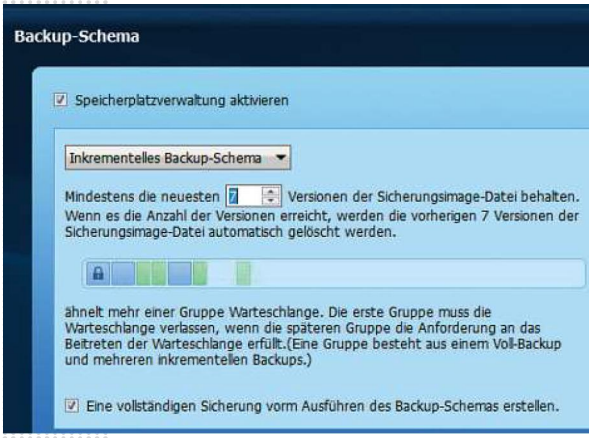


Fotos v. li. n. re., o. n. u.: iStockphoto/mamanamsai2, pixdeluxe; 123rf/Denis Tevekov; iStockphoto/OlegGr, Gordana Sermek, mamanamsai2, roundhill; Simon Kirsch; iStockphoto/LDProd; 123rf/Kristina Afanasyeva; iStockphoto/DmitriMaruta, Geber86, debibishop, mamanamsai2, ArtMarie; Fotolia/Gina Sanders; iStockphoto/mamanamsai2; Fotolia/Falko Matte; iStockphoto/CatherinePro; Fotolia/demarco; iStockphoto/mamanamsai2; 123rf/Yuri Arcurs; iStockphoto/angelhell; 123rf/Sebastian Duda; iStockphoto/mamanamsai2, ArtMarie; Fotolia/Thomas Kleber; iStockphoto/swissmediavision, mamanamsai2, Robert Ingelhart, mseidelch, mamanamsai2, Teresa Guerrero

Im Hauptmenü des Aomei Backuppers wählen Sie den Sicherungstyp, den Sie anlegen möchten



Im Scheduler definieren Sie die Backup-Frequenz – beispielsweise stündlich, täglich oder wöchentlich



Das Backup-Schema erlaubt eine Kombination aus Sicherungsmethoden, etwa eine Frequenz aus Vollbackup und inkrementeller Sicherung

Backup-Methoden

> Inkrementell Nach einem einmaligen Vollbackup werden immer nur die Änderungen im Vergleich zum letzten Schnappschuss gesichert.
> Differentiell Es werden bei jedem Schnappschuss jeweils alle Änderungen zum Vollbackup gespeichert.

besonders für die Stufen 1 und 3 anbietet: Das Backup von Dateien auf einer internen zweiten Festplatte lässt sich im Heimnetz spiegeln. Auch eine einmalige Systemsicherung sollte man zusätzlich auf einem anderen PC oder einer NAS ablegen. Neben den Windows-Rechnern halten auch Smartphones immer mehr wichtige Daten vor. Hier lohnt sich ein separates Backup in der Cloud oder auf einem PC im Heimnetz. Dafür stehen neben Services von Apple und Google eine Reihe von Apps bereit (siehe Seite 33).

Stufe 1: Datenbackup

Bevor es an das Backup geht, empfiehlt es sich, eine eigene Partition für die Originaldaten anzulegen. Falls auf der Systempartition mal etwas schiefgeht, wird der Datenbestand davon nicht tangiert. Allgemein geht es beim Datenbackup um eine Sicherung in regelmäßigen Intervallen und eine gewisse Effizienz. Damit der Platz auf dem Backup-Medium nicht durch unnötige Redundanz verschwendet wird, bieten entsprechende Programme eine inkrementelle Sicherung an, die nach einem ersten Gesamtbackup pro Snapshot nur die Änderungen des Datenbestands sichert. Die Frequenz dieser Sicherungen wird über einen Scheduler festgelegt. Diese Aufgabe lässt sich zwar auch mit Windows-Bordmitteln angehen, aber eine spezielle Software wie Aomei Backupper Professional verfügt über mehr Funktionen und Komfort.

Datensicherung einrichten

Der Backupper läuft unter Windows 7, 8 sowie 10 und bietet nach dem Start links ein Übersichtsfenster mit den Programmfunktionen. Zum Einrichten einer regelmäßigen Sicherung des Datenbestands kommen Sie über den Punkt »Backup«, gefolgt von der Option »Dateisicherung«. Der Backupper legt für die Sicherung eine Image-Datei an. Dazu bestimmen Sie zunächst unter Punkt »1« die Ordner, die Sie regelmäßig sichern möchten. Da man sie nur einzeln hinzufügen kann, lohnt es sich, den Datenbestand entsprechend zu organisieren, also Fotos, Filme und Dokumente jeweils in einem eigenen Ordner abzulegen – die Unterverzeichnisse nimmt der Backupper mit. Bei der Auswahl unter »Datei-Einschlussmaske« wählen Sie die Dateitypen, die Sie sichern wollen. »Systemdateien und -ordner« gehören ausgeschlossen, sonst speichert das Programm auch Files, die Windows automatisch anlegt wie Thumbs.db, das die Vorschaubilder in Foto-Ordnern enthält.

Nun geht es darum, wie der Backupper sichern soll. In den »Optionen« bietet sich die AES-Verschlüsselung an. Das ist für Familienfotos oder große Videodateien weniger sinnvoll als etwa für die Unterlagen fürs Finanzamt. Daher sollten Sie für vertrauliche Dokumente eine separate, verschlüsselte Sicherung anlegen. Unter »Kompression« bietet der Backupper an, die Daten zu zippen. Office-Dokumente und E-Books lassen sich gut komprimieren. Wer nur JPEGs, MP3-Files und Filme sichert, gewinnt nichts. Hier sollten Sie mehrere Sicherungen je nach Dateityp anlegen. Das betrifft auch Scheduling: Der »Zeitplan« legt fest, auf welche Weise und wie oft die Software ein Backup anlegt. Als Grundeinstellung für Office-Dateien, die man häufig editiert, empfiehlt sich eine tägliche Sicherung. Multimedia-Dateien, auf die Sie nur sporadisch zugreifen, brauchen Sie diese hohe Frequenz nicht zu gönnen.

Backup-Schema wählen

Unter »Erweitert« geht es darum, die Methode festzulegen. Voreingestellt ist »Inkrementelles Backup«. Das ist platzsparend, klappt aber nur reibungslos, wenn alle inkrementellen Sicherungen heil bleiben. Geht eine kaputt, lassen sich die Änderungen nicht mehr zurückverfolgen. Das »differentielle Backup« speichert alle Änderungen zum Vollbackup jeweils aufs Neue. Das bringt mehr Ausfallsicherheit, verbraucht aber Platz. Den optimalen Mix bietet ein Backup-

Zur Systemsicherung muss man im Backupper die Windows-Partition markieren. Die Voreinstellungen in den »Optionen« passen meistens

Bevor der Backupper das System-Image zurückspielt, gibt er eine Übersicht über anstehende Operationen

Linux oder Windows PE – der Backupper unterstützt beide Möglichkeiten beim Erzeugen eines Rettungssystems

»Schema«, das man im Hauptmenü auswählt. Aktiviert man die »Aufgabenplanung«, macht die Software unter »inkrementelles Backup-Schema« in regelmäßigen Intervallen eine Vollsicherung und löscht alle alten Speicherpunkte. So kann man jeden Tag eine inkrementelle Sicherung anlegen und nur einmal pro Woche ein Komplett-Backup.

Achtung! Alte Versionen, etwa eines Word-Dokuments, bleiben so nur eine Woche erhalten. Im Hauptmenü gibt man einen Zielort an, mit »Starten« gehts los.

Zum Wiederherstellen einer Datensicherung gehen Sie auf »Recovery« und aktivieren eine Sicherung. Im nächsten Fenster wählen Sie den Schnappschuss aus, woraufhin der Backupper das Image in einem Explorer-Fenster öffnet. Dort setzen Sie ein Häkchen vor die Dateien, die Sie zurückhaben wollen. Dann wählen Sie beispielsweise »Am ursprünglichen Speicherort wiederherstellen« und »Existierende Dateien ersetzen«, wenn Sie eine alte Version wiederherstellen wollen. Mit einem Klick auf »Start« erledigt das Programm diese Aufgabe.

Stufe 2: Systemsicherung

Im Gegensatz zum regelmäßigen Backup muss man eine Systemsicherung nur sporadisch anlegen. Seit Windows 7 ist ein Neuaufsetzen des Systems sowieso nur erforderlich, wenn viel schiefgeht, etwa ein Malwarebefall, der sich nicht so einfach wieder beheben lässt. Neben dem Image mit der gesicherten Systempartition benötigt man zudem ein bootbares Rettungsmedium, auf dem ein Notfallsystem läuft. Das kommt zum Einsatz, falls Windows gar nicht mehr hochfährt. Das eigentliche Image gehört auf eine zweite Festplatte. Da es sich um eine einmalige Sicherung handelt, empfiehlt sich dafür eine externe USB-Platte.

System-Image anlegen

Im Hauptmenü des Backuppers steht unter dem Punkt »Backup« die »Systemsicherung« für Windows zur Verfügung. Dort markieren Sie die Windows-Partition. In den »Optionen« steht unter »intelligente Sektoren« neben der Sicherung der mit Daten belegten auch eine Sicherung aller Sektoren zur Wahl. Letztere lohnt sich bei einer Systemsicherung nicht – es sei denn, man will die Image-Datei später einmal nach schon gelöschten Daten durchsuchen, die sich in diesen leeren Sektoren befinden. Unter »VSS« hat der Backupper den Volume Shadow Copy Service von Windows automatisch aktiviert. Er erlaubt das Anlegen einer Sicherung im laufenden Betrieb. Ansonsten wäre der Zugriff auf zentrale Systemdateien wie die Registry schwierig.

Die eigentliche Systemsicherung wirft man im Hauptmenü nach der Angabe eines Zielpfades per »Start« an. Das Fenster zeigt den Fortschritt an und Sie können dort einstellen, dass der Backupper die »Sicherungsintegrität nach dem Abschluss« überprüft. Damit checkt die Software, ob das Systemimage Fehler enthält. Das dauert ein paar Minuten.

Rettungsmedium erzeugen

Wenn Windows nicht mehr hochfährt oder der Umzug auf eine neue Festplatte ansteht, benötigt man ein Notfallsystem. Diese Aufgabe sollte man direkt nach dem Anlegen des System-Images angehen. Im Backupper findet sich diese Funktion unter »Werkzeuge« mit einem Klick auf »Bootfähiges Medium erstellen«. Als Medium empfiehlt sich in der Regel ein USB-Stick. Im nächsten Schritt →

Alternative: Personal Backup

Die umfangreiche Freeware finden Sie zum Download auf chip.de. Sie sichert auch Dokumente, die gerade geöffnet sind

bietet das Programm zwei Optionen: ein Linux- oder ein Windows-basiertes System. Wer mit der Windows-Welt vertraut ist, nimmt »WindowsPE«. Soll es auf BIOS-Rechnern starten, wählt man den »Legacy-Boot-Modus«. Ansonsten kommt der neuere »UEFI-Boot-Modus« zum Einsatz. Stecken Sie den USB-Stick ein und definieren Sie ihn als Zielmedium, den Rest erledigt der Backupper. Wenn Sie vom Stick booten, fährt WindowsPE hoch und öffnet den Backupper auf dem Rettungsmedium. Das Aufspielen des System-Images läuft dann wie gehabt.

System-Image zurückspielen

In einem funktionierenden Windows können Sie aus dem Backupper heraus die Systempartition wiederherstellen. Dazu gehen Sie im Hauptmenü auf »Restore« und wählen die Systemsicherung aus. Nun fragt das Programm, ob man eine Systemwiederherstellung durchführen will, was man mit »Ok« bestätigt. Danach zeigt es an, welche Aktionen durchgeführt werden. Beim Neustart bootet der Backupper noch vor Windows und spielt die gesicherte Systempartition automatisch wieder auf. Noch ein Tipp: Zum Umzug auf eine andere Festplatte sollten Sie zuvor die Funktion »Universal Restore« aktivieren. Sie sorgt dafür, dass Windows auch auf der neuen Platte startet.

Stufe 3a: Server im Heimnetz

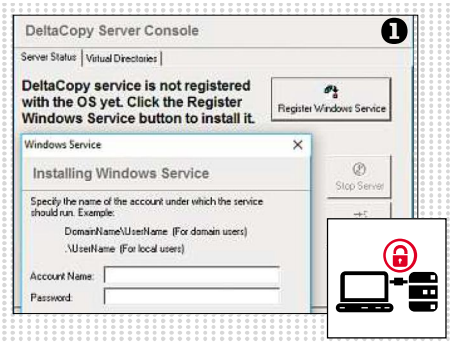
Die interne Datensicherung auf einer zweiten Festplatte bietet sich zwar für den PC an, doch schon beim Notebook wird das schwierig. Oft fehlt im Gerät der Platz für ein zweites Speichermedium. In dem Fall sollte man auf ein Daten-Backup im Heimnetz ausweichen. Als Gegenstelle zum Notebook benötigt man entweder eine NAS (Network Attached Storage) oder einen alten Windows-PC, den man als Datenserver einsetzt. Wir zeigen beide Optionen und beginnen mit der Netzwerksicherung auf einem anderen Rechner. Dabei hat sich rsync bewährt. Bei rsync handelt es sich sowohl um ein Verbindungsprotokoll als auch um eine Synchronisations- und Sicherungssoftware. rsync stammt ursprünglich aus der Unix-Welt, läuft inzwischen aber auf allen möglichen Plattformen. Die Windows-Software DeltaCopy hat rsync integriert und bietet eine Benutzeroberfläche – sonst lässt sich rsync auch in Windows nur über die Kommandozeile bedienen.

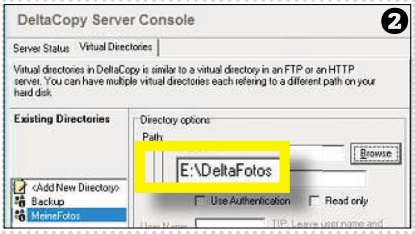
Backup-Server aufsetzen

DeltaCopy besteht aus zwei Teilen, Server und Client. Bei der Installation werden automatisch beide ins System eingespielt, auch wenn man jeweils nur eine Komponente verwendet. Zuerst sollten Sie den Serverteil auf dem alten Windows-Rechner aufsetzen, der zur Datensicherung im Netzwerk dient. Dazu starten Sie das Programm direkt nach dem letzten Installationsschritt und klicken auf »Register Windows Service«, um DeltaCopy als Windows-Dienst zu aktivieren. Nun geben Sie die Zugangsdaten des Windows-Kontos ein, mit dem Sie sich normalerweise im Betriebssystem anmelden. Am Ende spuckt DeltaCopy eine Erfolgsmeldung aus und wird normalerweise über

DeltaCopy: Server einrichten

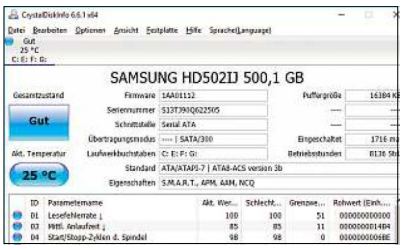
Zunächst melden Sie DeltaCopy als Systemdienst an. Dazu benötigt man die Daten für das eigene Windows-Konto ❶. Danach geben Sie das Zielverzeichnis an, in das DeltaCopy später die Daten sichern soll ❷



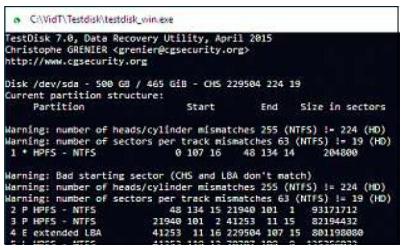


»Start Server« aktiviert. Erhält man stattdessen die Fehlermeldung „Could not start the service", ist ein Zwischenschritt notwendig: Gehen Sie in die »Systemsteuerung | Verwaltung« von Windows und öffnen Sie dort über »Dienste« den Eintrag zum »DeltaCopy Server«. Unter dem Reiter »Anmelden« wählen Sie die Option »Lokales Systemkonto«. Gehen Sie nun zu DeltaCopy zurück und betätigen Sie wieder »Start Server«. Nun springt die Ampel im DeltaCopy-Fenster auf Grün, der Server läuft. Jetzt muss man im entspre-

Analyse- und Rettungstools für die Festplatte



> Crystal DiskInfo liest die SMART-Werte von Festplatten aus. Die „Self-Monitoring, Analysis and Reporting Technology" soll rechtzeitig vor einem Harddrive-Crash warnen. Das Tool zeigt auch an, wie viele Arbeitsstunden die Platte schon hinter sich hat und wie oft sie eingeschaltet wurde.



> TestDisk analysiert den logischen Aufbau der Festplatte und zeigt Fehler beim Aufbau der Partitionen an. Diese kann TestDisk in vielen Fällen beheben – auch wenn die Aktion für ungeübte User nicht trivial ist. Ebenfalls im Bundle dabei ist PhotoRec, eine Datenrettung für gelöschte Fotos.

> Recuva spürt gelöschte und schon aus dem Papierkorb entfernte Dateien auf und stellt sie wieder her. Dazu untersucht es gelöschte Einträge in der Partitionstabelle. Im Deep-Scan-Modus kämmt das Tool auch gelöschte Festplattensektoren durch. Das dauert länger, liefert aber bessere Ergebnisse.

DeltaCopy: Client konfigurieren

Im Client erstellt man ein Profil mit der IP-Adresse des Servers ❶ und testet, ob das klappt. Dann geben Sie die Verzeichnisse an, die DeltaCopy sichern soll und erstellen im Scheduler ❷einen Zeitplan

So viel NAS ist sinnvoll

> Zur Datensicherung reicht eine 2-Bay-NAS ohne Schnickschnack wie die unten vorgestellten Geräte. Dafür sollte man etwas mehr Geld in ein gut gepflegtes Betriebssystem investieren, wie es Qnap und Synology bieten.

	Disk Station DS214	Turbo Station TS-231
Hersteller	Synology	Qnap
Preis	ca. 230 Euro	ca. 170 Euro
Transferrate Lesen	97,0 MBit/s	107,1 MBit/s
Transferrate Schreiben	93,9 MBit/s	94,3 MBit/s
Leistungsaufnahme Standby	8,3 Watt	7,6 Watt
Leistungsaufnahme Betrieb	20,2 Watt	18,6 Watt
Lautheit Betrieb	1,8 Sone	1,8 Sone

Besser als der Durchschnitt Schlechter als der Durchschnitt

chenden Reiter nur noch die »Virtual Directories« einrichten. Dorthin speichert der Client später die Dateien. Mit einem Doppelklick auf »Add New Directory« legen Sie einen neuen Sicherungsordner an – vergeben Sie einen passenden Namen wie beispielsweise „MeineFotos“ ohne Leerzeichen. Über den »Browse«-Button gibt man den Pfad zu einem Sicherungsordner eigener Wahl an.

Client mit Server verbinden

Auf dem Arbeitsrechner beziehungsweise Notebook installieren Sie nun ebenfalls DeltaCopy. Im Paket ist auch ein Client enthalten, der später die Daten zu dem alten Windows-PC schickt, auf dem Sie den Server eingerichtet haben. Den Client öffnen Sie im Installationsverzeichnis von DeltaCopy per Doppelklick auf »DeltaC.exe«. Im ersten Schritt legen Sie ein neues Profil an über »Add New Profile«. Vergeben Sie hier einen Namen und unter »Server IP/Host Name« tragen Sie die IP-Adresse des alten Windows-Rechners ein. Die finden Sie am einfachsten über das entsprechende Menü im Netzwerk-Router. Alternativ steht die Information auch in Windows. Sie wird etwa unter Windows 10 in »Einstellungen | Netzwerk und Internet | Ethernet« per Doppelklick auf den Netzwerknamen angezeigt. Danach sollten Sie unter »Test Connection« schon einmal überprüfen, ob der Client die Verbindung zum Server auch wirklich aufnehmen kann. Kommt jetzt eine Fehlermeldung, gibt es typischerweise zwei Bremsklötze in Windows, die man überwinden muss: Im Explorer unter »Netzwerk« sollten Sie die »Netzwerkerkennung und Dateifreigabe aktivieren« und dann die Windows-Firewall ausschalten – die Firewall des Routers gibt im Normalfall genug Sicherheit. Wer das nicht will, muss in der »Systemsteuerung | Windows-Firewall« unter »Erweiterte Einstellungen« eine »Neue Regel« für DeltaCopy erstellen. Im Assistenten gibt man daraufhin den Programmpfad der Server- beziehungsweise Client-EXE von DeltaCopy ein und kann dann die »Verbindung zulassen«.

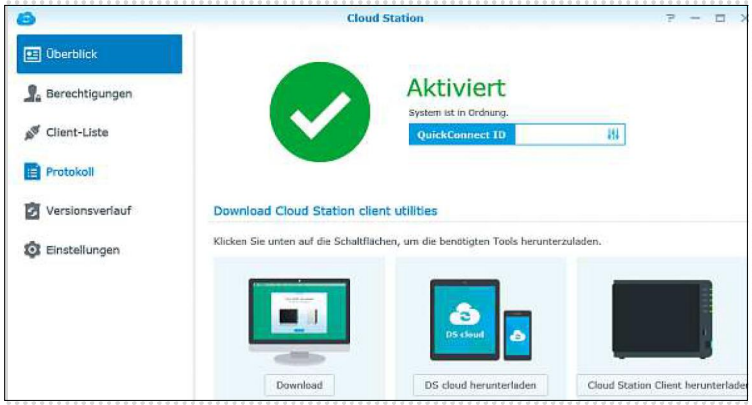
Klappt nun die Erkennung, wählen Sie im DeltaCopy-Client unter »Virtual Directory Name« das zuvor im Server erstellte Zielverzeichnis aus und vergeben einen Profilnamen. Über »Add Profile« schließen Sie die Operation ab. Danach markieren Sie das Profil und konfigurieren es: Unter »File List | Add Folder« geben Sie die zu sichernden Verzeichnisse an. Über »Modify Schedule« öffnet der Windows-Scheduler automatisch einen neuen Job. Im Scheduler-Fenster lässt sich ein »Zeitplan« über »Neu« anlegen – eine tägliche Sicherung ist voreingestellt. Wer eine andere Sicherungsfrequenz will, kann über »Erweitert« genauere Einstellungen vornehmen. Damit der Scheduler den soeben angelegten Job auch ausführt, muss das Windows-Konto mit einem Passwort gesichert sein, das man unter »Kennwort festlegen« angibt. Mit dem Schließen des Schedulers ist der Client eingerichtet und sichert automatisch zum angegebenen Zeitpunkt die Daten.

Stufe 3b: Sicherung auf der NAS

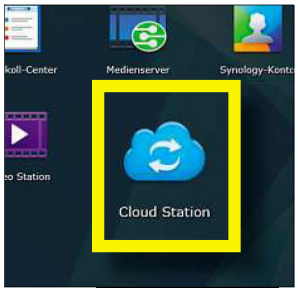
Wer keinen alten Zweit-PC zu Hause hat, für den ist die Sicherung auf einer Netzwerkfestplatte die ideale Lösung. Aktuelle NAS-Systeme lassen sich relativ simpel einrichten und sind mit einer Reihe von Tools zur komfortablen Datensicherung ausgestattet. Hat man sie mit GBit-LAN verbunden, sichern sie Daten ähnlich flott wie eine zweite Festplatte im PC. Für das Backup im Heimnetz sollte man zu einer NAS mit zwei Festplatten greifen. Sie bietet eine gute Kombination aus reellem Preis und Sicherheit, da sich die zweite Platte entweder im RAID-1-Verbund spiegeln lässt oder man alternativ ein internes Backup von der einen auf die andere Platte durchführen kann. Damit sind die gesicherten Daten auch gegen den Ausfall einer Festplatte geschützt. Das fehlt →

Fotos: Hersteller

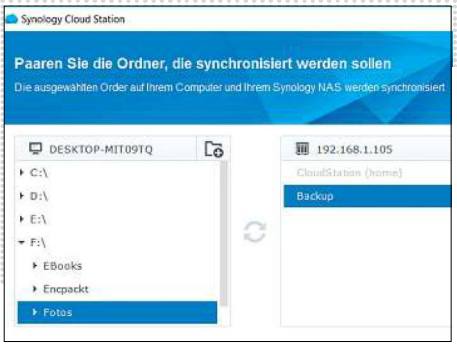
In der Cloud Station auf der NAS lädt man im Hauptfenster über den »Download«-Button den passenden Desktop-Client für Windows herunter



Auf dem NAS-Desktop ist die Verknüpfung zur Cloud Station eingerichtet



In der Systemsteuerung der NAS wird der Ordner eingerichtet und freigegeben, auf dem später die Backup-Daten landen



Im Desktop-Client legt man fest, welche Ordner die Cloud Station auf dem Windows-PC überwachen und synchronisieren soll

bei 1-Bay-NAS, während 4-Bay-NAS teuer sind und keine großen Vorteile bieten. Günstigere 2-Bay-Modelle der etablierten Hersteller Qnap oder Synology haben eine ausgereifte Software, verzichten aber auf ein Mediencenter oder HDMI-Anschluss, die man für das Backup im Heimnetz nicht braucht. Trotzdem lohnt sich vor dem Kauf ein Blick in das Datenblatt, um zu schauen, wo der Hersteller abgespeckt hat. So sollte die maximale Anzahl gleichzeitiger Dateitransfers bei 128 liegen, damit es bei der Sicherung zu keinen größeren Verzögerungen kommt. Anhand der etwas ausgereifteren Synology-Software erklären wir, wie man eine automatische Datensicherung aufsetzt.

Server-Software installieren

Früher war das Einrichten der Synology NAS mit einem auf Linux basierten Betriebssystem ein frickeliger Prozess, heute läuft er weitgehend automatisch ab. Zugriff auf den Einrichtungsassistenten erhalten Sie über die IP-Adresse der NAS im Browser – idealerweise auf dem Rechner, von dem Sie später die Daten sichern wollen. Im Zuge der Systemeinrichtung sollte man den Schritt »empfohlene Pakete« nicht überspringen, denn darüber wird automatisch die Cloud Station zur späteren Datensicherung mit installiert.

Ist alles eingerichtet, gehen Sie links oben auf das »Hauptmenü«-Symbol und dort auf »Cloud Station«. Hier sollte nun ein grünes Häkchen anzeigen, dass die Server-Anwendung schon läuft. Unter »Berechtigungen« aktivieren Sie den Benutzernamen, den Sie bei der Einrichtung angelegt haben und bestätigen dies über »Speichern«. Nun gehen Sie in die »Systemsteuerung | Gemeinsamer Ordner« der NAS und »Erstellen« ein Backup-Verzeichnis. Im nächsten Fenster aktivieren Sie für Ihren Benutzernamen unter »Berechtigungen« die Option »Lesen/Schreiben«. Gehen Sie nun in die »Einstellungen« der Cloud Station zurück, markieren Sie dort den gerade angelegten Ordner und »Aktivieren« Sie die Freigabe.

NAS-Client konfigurieren

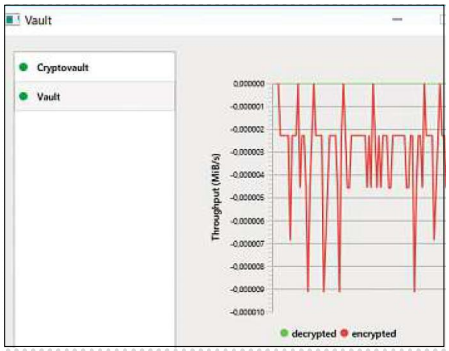
Jetzt geht es darum, den Client auf dem Windows-Rechner einzurichten. Im »Überblick«-Fenster der Cloud Station laden Sie ihn über »Download« auf den Windows-Rechner herunter. Per Doppelklick startet die Installation. Beim ersten Aufruf des Clients führt ein Assistent durch die Konfiguration, in der Sie neben der IP-Adresse der NAS den Benutzernamen und das Passwort Ihres Kontos eingeben. Wählen Sie »Erweitertes Setup«, um einen Synchronisierungsordner auf dem Rechner und das zuvor auf der NAS angelegte Backup-Verzeichnis auszuwählen. Nun überwacht und synchronisiert der Client den Ordner automatisch mit der NAS. Ähnlich wie der Schattenkopiedienst in Windows registriert Cloud Station auch, wenn an einer Datei Veränderungen vorgenommen werden. Die unterschiedlichen Versionen einer gesicherten Datei kann man später im Kontextmenü des Windows-Explorers über »Synology Cloud Station | Frühere Versionen durchsuchen« wiederherstellen.

Stufe 4: Cloud-Sicherung

Neben Heimnetz und zweiter Festplatte bietet sich auch die Cloud im Internet zur zusätzlichen Datensicherung an. Aufgrund der begrenzten Upload-Geschwindigkeit sollte man die Datenmenge auf wichtige Dokumente begrenzen oder sie für Files nutzen, die man mit anderen

Alternative: Cryptomator

Wie BoxCryptor legt der Cryptomator ein Laufwerk an, in dem er Files automatisch verschlüsselt. Das gilt auch für ihre Namen



Zur sporadischen Sicherung persönlicher Daten in der Cloud reicht ein lokaler BoxCryptor-Account aus ❶. Hier muss man darauf achten, dass man die Datei mit dem Passwortschlüssel nicht verliert ❷.

teilt. Da kommt es auf den Schutz der Privatsphäre an – viele Cloudanbieter wie Microsoft und Google analysieren automatisch hochgeladene Dateien. Dem kann eine Verschlüsselung vorbeugen, die noch vor dem Upload lokal durchgeführt wird. Für das Tool BoxCryptor beschreiben wir, wie Sie dabei vorgehen.

BoxCryptor-Account einrichten

Da BoxCryptor sich in Windows als ein eigenes Laufwerk einbindet, spielt die Installationsroutine zu diesem Zweck einen Treiber auf. Als Anwender muss man dieser Operation zustimmen, sonst funktioniert die Software später nicht. Danach erfolgt die Ersteinrichtung: Im Startfenster fordert die Software auf, einen Account beim Online-Service von BoxCryptor anzulegen. Das ist vor allem sinnvoll, wenn Sie kostenpflichtige Features nutzen, wie die Verschlüsselung von Ordner- und Dateinamen – die Dateien an sich verschlüsselt auch die Gratis-Version. Das Gleiche gilt, wenn Sie mehrere Cloud-Anbieter einbinden möchten, auch das kann nur die kostenpflichtige Lösung. Für die einfache, sporadische Sicherung von wichtigen, persönlichen Dokumenten benötigt man diese Features in der Regel nicht. Falls doch, steht als kostenlose Alternative das OpenSource-Tool Cryptomator zur Verfügung (siehe unten links). Das gibt es bislang nur als Beta, funktioniert aber schon reibungslos.

Wer das alles nicht braucht, für den reicht ein lokaler BoxCryptor-Zugang unter Umgehung des Online-Services: Bei der Ersteinrichtung öffnet sich mit einem Klick auf »...« rechts unten ein Fenster mit der Option »Lokaler Account | Account einrichten«. Danach legen Sie eine per Passwort geschützte Schlüsseldatei an und speichern sie lokal auf Ihrem Rechner. Im nächsten Fenster wählen Sie die »Free«-Variante von BoxCryptor, womit der Dienst unter dem Standard-Account local@Boxcryptor.com auf Ihrem PC eingerichtet ist. Dort melden Sie sich mit dem zuvor vergebenen Passwort an, um BoxCryptor zu konfigurieren.

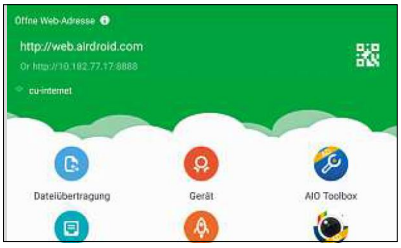
Cloudkonto verknüpfen

Ist schon ein kompatibler Cloudzugang auf dem Rechner eingerichtet, erkennt die Software dies automatisch. BoxCryptor unterstützt von Apples iCloud über Google Drive bis zu Dropbox und Web.de mehr als ein Dutzend bekannter Anbieter. Falls das BoxCryptor-Tool das Cloudverzeichnis nicht erkennt, kann man in den »Einstellungen« den Pfad zum lokalen Cloudordner unter »Speicherorte | Hinzufügen« manuell angeben. Alle Dateien, die später in diesem Ordner landen, verschlüsselt BoxCryptor nach einer Abfrage automatisch und sie werden zur Cloud hochgeladen. Ob das geklappt hat, lässt sich einfach überprüfen, indem man einen Blick auf den Cloudordner im Explorer wirft. Dort haben die verschlüsselten Dateien die Endung „.bc“ und lassen sich nicht öffnen. Sollen die Daten aus der Cloud wieder auf den lokalen PC kommen, geht das im Windows-Explorer einfach per Drag&Drop vom BoxCryptor-Laufwerk in ein gewöhnliches lokales Verzeichnis auf dem PC. BoxCryptor entschlüsselt die Dateien dabei automatisch.

testtechnik@chip.de ■

Smartphone-Backup für Android

> Helium Backup sichert Apps, SMS, WLAN-Passwörter und Nutzerdaten eines Android-Gerätes auf dem PC. Damit das ohne Root-Rechte funktioniert, werden die passenden ADB-Treiber von der Homepage und dem Helium Desktop-Client benötigt, über den man von Windows aus die Verbindung herstellt.



> AirDroid erlaubt den Fernzugriff auf ein Android-Gerät vom PC aus. Der Datentransfer für das Backup wird auch über das Web abgewickelt, sofern man einen AirDroid-Account anlegt. Per AirMirror führt das Tool von Windows aus auch Aktionen auf dem Android-Gerät durch – etwa eine SMS senden.

> Titanium erfordert Root-Rechte, da es sämtliche Daten des Mobilgerätes sichert, so auch System-Apps. Das geht nur, wenn der Super User (SU) freigeschaltet ist, der auf alle Files Zugriff hat. Titanium ist ideal zum Umzug, denn die App kann das Backup auch auf einem anderen Gerät wiederherstellen.