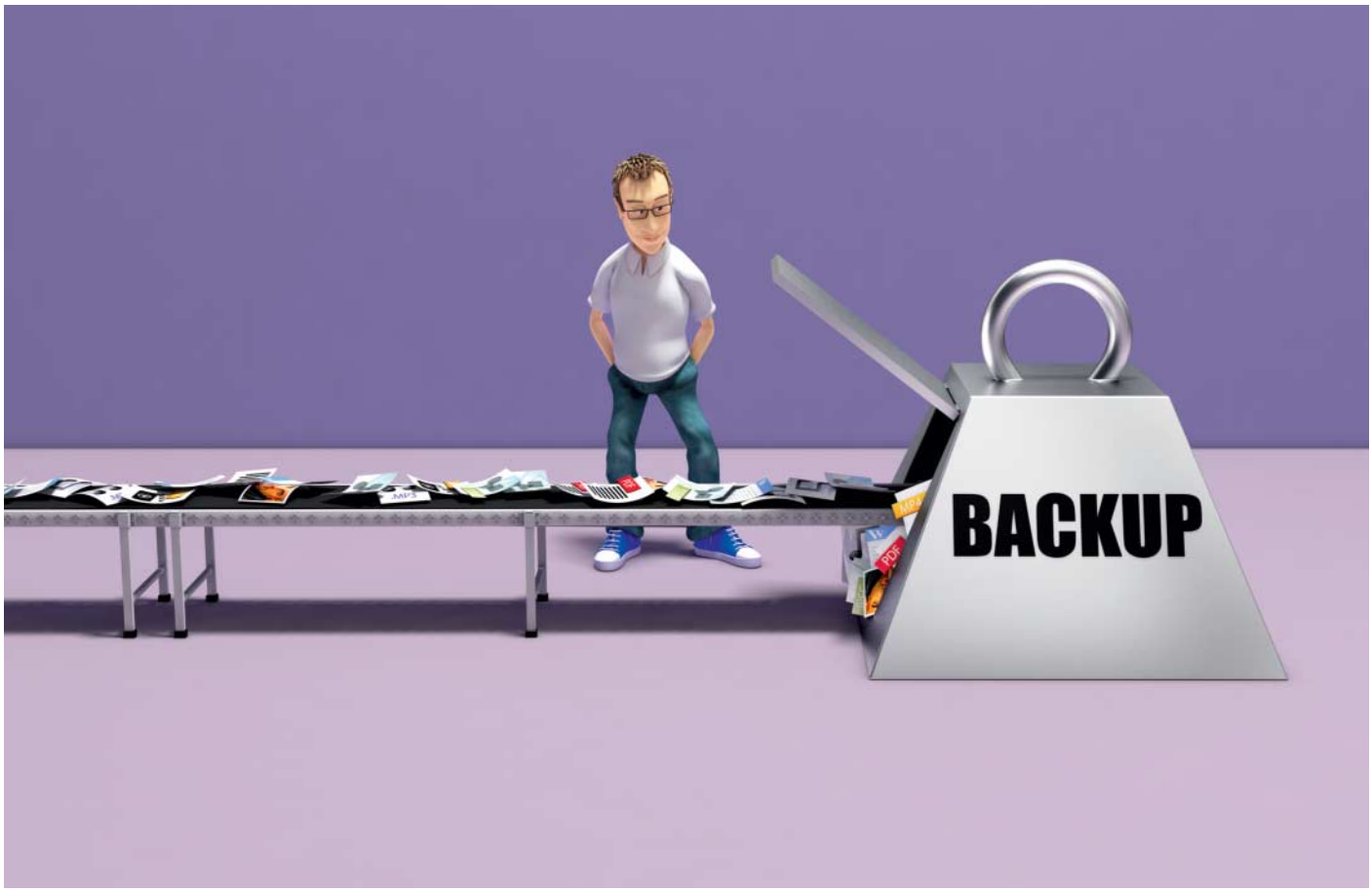


Backups vom Fließband

Mit Duplicati in fünf Minuten zum Trojaner-sicheren Backup

Wenige Klicks genügen, um Unersetzliches mit dem kostenlosen Backup-Tool Duplicati außer Reichweite von Krypto-Trojanern zu sichern. Als Backup-Speicher können USB-Sticks, externe Platten, NAS oder auch die Fritzbox dienen. Dank der Anbindung an Online-Dienste sind auch verschlüsselte Sicherungen außer Haus schnell eingerichtet.

Von Ronald Eikenberg

Es gibt keinen Grund mehr, kein Backup zu haben: Mit Duplicati sichert man das digitale Hab und Gut mit wenigen Minuten Konfigurationsaufwand. Es ist leicht einzurichten und äußerst flexibel. Richten Sie individuelle Backup-Pläne für die unterschiedlichen Typen von Daten an. Während etwa die große Foto-Sammlung nur auf Zuruf auf die USB-Platte gesichert wird, könnten die häufig bearbeiteten Dokumente regelmäßig und automatisch in der Speicher-Cloud landen. Duplicati beherrscht einige Übertragungprotokolle, die derzeit als Trojaner-sicher gelten: etwa FTP, SSH (SCP) oder auch das Speichern in Amazons S3-Cloud. Das eröffnet viele Möglichkeiten: Neben externen Platten und USB-Stick kann auch das NAS, Webspace oder ein Raspberry Pi als Speicherziel dienen. Dabei gilt: viel hilft viel! An je mehr Orten die Backups liegen, desto größer ist die Wahrscheinlichkeit, dass man nach einem Trojanerbefall noch Zugriff auf mindestens eine Kopie hat. Um die Sicherheit Ihrer Daten müssen Sie sich keine Sorgen machen: Duplicati verschlüsselt standardmäßig mit AES-256. Wenn Sie ein ausreichend langes Passwort wählen, sind die Backup-Dateien praktisch nicht zu knacken. Duplicati nutzt offene Formate wie Zip, die man auch ohne das Tool entpacken kann.

Mit ein paar Kniffen richtet man das Backup-Tool so ein, dass es mit Hilfe der Aufgabenplanung automatisch eine Sicherung startet, sobald ein bestimmter USB-Speicher mit dem Rechner verbunden ist.

Die folgenden Seiten beziehen sich auf Windows, das Backup-Tool läuft aber auch unter OS X und Linux.

Klick, Klick, Backup

So schnell legen Sie ein Backup an: Installieren Sie die derzeit aktuelle Version 1.3.4 (siehe c't-Link am Ende des Artikels). Diese wurde zwar bereits 2013 veröffentlicht, leistet aber nach wie vor gute Dienste – selbst unter dem aktuellen Windows 10. Beim ersten Start begrüßt Sie der Assistent. Die ersten Schritte sind immer gleich: Klicken Sie auf „Eine neue Sicherung planen“ und geben Sie dem Backup-Job einen sinnvollen Namen, etwa „Dokumente auf USB-Stick“. Im nächsten Schritt wählen Sie, welche Dateien gesichert werden sollen. Vorausgewählt sind bereits die Daten im Dokumenten-Ordner von Windows, die Bilder im Standardverzeichnis sowie alles, was sich auf dem Desktop befindet. Über die Option „Benutzerdefinierte Ordnerliste“ können Sie auch beliebige andere Ordner angeben.

Danach wählen Sie ein Passwort für die AES-Verschlüsselung. Dieses benötigen Sie nur zweimal: jetzt und wenn Sie Dateien aus dem Backup wiederherstellen möchten. Da Sie es nicht häufig eingeben müssen, kann es ruhig lang und kompliziert sein. Der wichtigste Stellhebel in puncto Sicherheit ist dabei die Länge. Schreiben Sie sich das Passwort am besten auf einen Zettel, den Sie fortan an einem sicheren Ort verwahren – etwa im Portemonnaie oder im Tresor. Mit einem Klick auf den Zauberstab generiert das Tool auf Wunsch ein zufälliges Passwort.

Im nächsten Schritt geben Sie an, wohin Duplicati die Sicherungen speichern soll. Dabei haben Sie die Wahl: Das Tool unterstützt fast alle Trojaner-sicheren Speicherziele, die wir auf Seite 102 beschrieben haben.

Backup auf USB-Speicher

Um die Sicherungen auf einer externen Platte oder einem USB-Stick abzulegen, wählen Sie als Speicherort die Option „Datei-basierend“. Im nächsten Schritt geben Sie einen Zielpfad auf dem externen Laufwerk an. Handelt es sich um einen Wechseldatenträger wie einen USB-Stick, können Sie unter „Wechsellaufwerk“ auch einfach den entsprechenden Laufwerksbuchstaben wählen und den Namen des gewünschten Zielordners angeben. Existiert das Verzeichnis nicht, legt es Duplicati an.

Backup auf NAS oder Fritz!Box

Möchten Sie Ihre Backups auf einem Netzwerkspeicher (NAS) oder einer an den Router angeschlossenen Platte speichern, sollten Sie dies bevorzugt über das FTP-Protokoll tun. Die aktuell kursierenden Trojaner können zwar auf SMB-Freigaben zugreifen, nicht aber auf FTP-Server. Wählen Sie als Speicherort „FTP-basierend“ und tragen Sie im nächsten Schritt Server, Pfad und die Zugangsdaten für den FTP-Server ein. Wer einen anderen Port als 21 nutzt, muss die Einstellung entsprechend anpassen. Achten Sie bei der Einrichtung von FTP darauf, den relativen Pfad anzugeben – also ausgehend von dem Ort, von dem aus der FTP-Nutzer nach dem Einloggen startet. Kommt es zu Verbindungsproblemen, kann es helfen, ein Häkchen bei „Passive Verbindung benutzen“ zu setzen.

Backup auf Webspace und Server

Für Backups auf Webspace-Accounts und Server gilt das Gleiche, wie für die Speicherung auf Netzwerkspeichern. Da die Daten in diesem Fall wahrscheinlich über das Internet übertragen werden, sollten Sie den FTP-Server möglichst verschlüsselt kontaktieren. Setzen Sie hierzu das Häkchen „Benutze SSL“. Standardmäßig sind FTP-Verbindungen unverschlüsselt. Wer den Datenverkehr belauscht, kann alles mitlesen. Zwar sind die von Duplicati erzeugten Backups weiterhin verschlüsselt, ein Datenlauscher kann jedoch die FTP-Zugangsdaten mitlesen und damit unter Umständen die Backups löschen. Wenn Sie auf ein Linux-System sichern möchten, etwa auf einen Root-Server oder einen Raspberry Pi, können Sie auch zum SSH-Protokoll (SFTP) greifen, wählen Sie hierzu „SSH-basierend“.

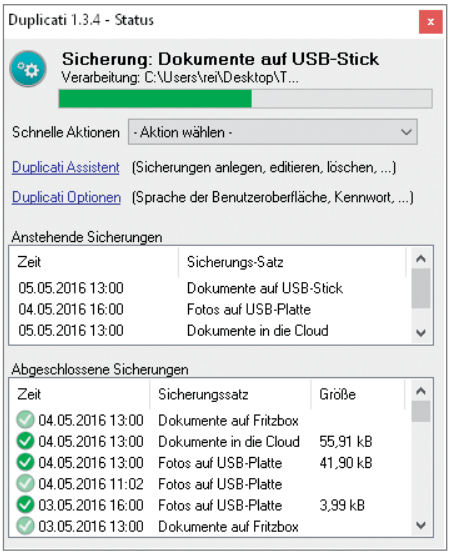
Backup in die Cloud

Das Speichern in die Datenwolken von Google, Dropbox und Co. beherrscht die aktuelle Duplicati-Version in Verbindung mit den jeweiligen Synchronisations-Clients. Um Backups in die Cloud zu sichern, wählen Sie als Speicherort „Datei-basierend“ und anschließend einen lokalen Ordner, den der Client des Speicher-Anbieters synchronisiert. Diese Lösung ist allerdings nur bedingt Trojaner-sicher: Verschlüsselt ein Trojaner die Backup-Dateien im lokalen Ordner, ersetzt der Sync-Client anschließend auch die Backups in der Cloud durch die fremdverschlüsselten Versionen. Zwar kann man bei den meisten Speicher-Anbietern über mehrere Tage hinweg ältere Versionen von Dateien wiederherstellen, darauf sollten Sie sich jedoch nicht verlassen. Ein solcher Backup-Job eignet sich also nur als Ergänzung für weitere Sicherungen an Trojaner-sichere Orte.

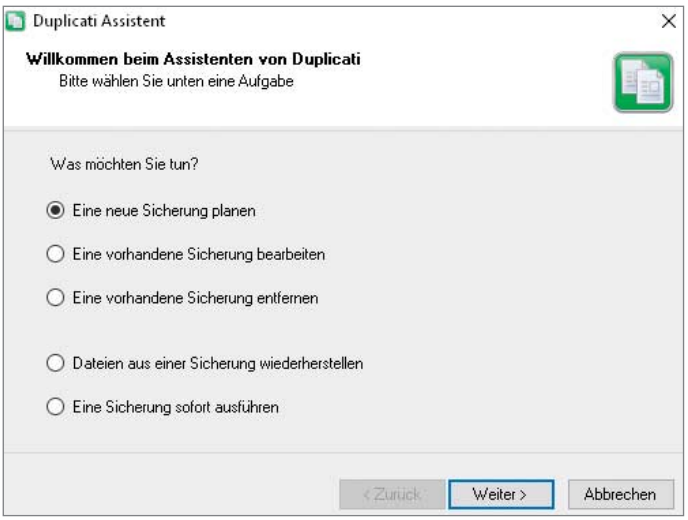
Duplicati beherrscht auch das WebDAV-Protokoll, über das Sie zum Beispiel Online-Speicher wie den 1&1 Online Speicher oder Stratos HiDrive ansteuern können. Zudem unterstützt das Backup-Tool Amazons S3-Speichercloud. Die Funktionen zur Speicherung bei Google Docs und „SkyDrive“ (inzwischen OneDrive) sind nicht mehr intakt. Abhilfe naht mit Duplicati 2.0 (siehe Kasten „Ausblick auf Duplicati 2“).

Und los!

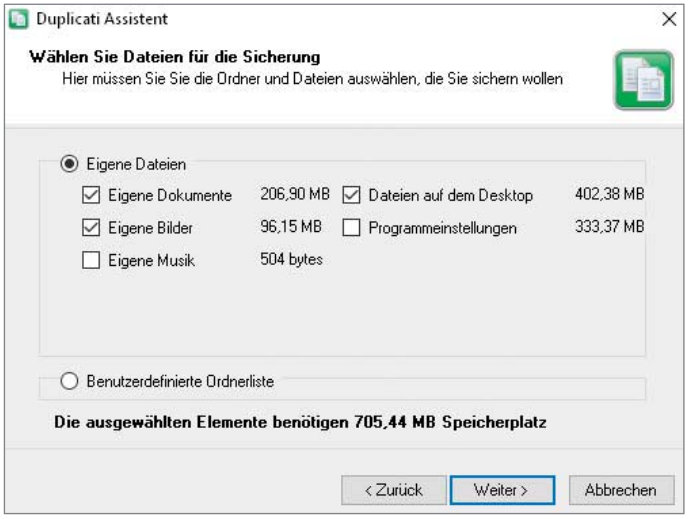
Nachdem Sie das Speicherziel eingerichtet haben, bietet Ihnen Duplicati erweiterte Einstellungen an, die Sie erst mal getrost



Das Open-Source-Tool Duplicati sichert Ihre unersetzlichen Dateien an Orten, die Krypto-Trojaner nicht ohne Weiteres erreichen.



Der Assistent von Duplicati führt Sie in wenigen Schritten zum individuellen Backup.



Die wichtigsten Ordner für persönliche Daten sind bereits vorausgewählt.

ignorieren können. Mit den Standardeinstellungen startet die Sicherung täglich um 13 Uhr. Danach zeigt das Programm eine Zusammenfassung an und fragt, ob die Sicherung sofort gestartet werden soll. Dieses Angebot sollten Sie annehmen.

Duplicati sichert jetzt die gewählten Ordner vollständig in verschlüsselte Datenhäppchen à 10 MByte. Am Ziel finden Sie neben diesen Schnipseln auch sogenannte Manifest-Dateien, die Metadaten des Backups enthalten. Über diese kann das Tool unter anderem die Integrität der Backup-Dateien überprüfen. Zudem legt es Signature-Dateien an, mit denen es dokumentiert, wie eine Datei zu einem bestimmten Zeitpunkt aussah. Diese spielen bei der zweiten Ausführung des Backup-Jobs eine zentrale Rolle: Es handelt sich nämlich um inkrementelle Sicherungen. Duplicati sichert die Dateien also nicht jedes Mal komplett neu, sondern nur jene Teile, die sich geändert haben. Insbesondere bei großen Dateien wie Festplatten-Images virtueller Maschinen spart das effektiv Speicher und Übertragungszeit.

Wenn Sie den Artikel bis hierhin nachvollzogen haben, besitzen Sie nun eine Sicherung Ihrer Dateien, mit der Sie Ihr digitales Hab und Gut im Fall der Fälle wiederherstellen können. Wiederholen Sie die oben beschriebenen Schritte, um weitere Speicherziele einzurichten.

Notfallübung

Sie sollten nach dem ersten Sichern unbedingt überprüfen, ob Sie sich auf Ihr Backup im Ernstfall verlassen können, also ob die Wiederherstellung der gesicherten Daten funktioniert. Starten Sie den Duplicati-Assistenten und wählen Sie „Dateien aus einer Sicherung wiederherstellen“. Im nächsten Schritt selektieren Sie einen Backup-Job und anschließend den Stand der Datei. Da Duplicati mit jeder Ausführung Zwischenstände geänderter Dateien speichert, können Sie nicht nur den Stand bei der letzten Sicherung wiederherstellen, sondern auch weiter in die Vergangenheit reisen. Das ist nützlich, wenn Sie zum Beispiel Änderungen an einem bereits gespeicherten Dokument vorgenommen haben, die Sie rückgängig machen möchten. Danach wählen Sie einen Ordner, in dem die geretteten Dateien gespeichert werden sollen. Mit der Option „Nur die unten ausgewählten Elemente wiederherstellen“ können Sie gezielt einzelne Dateien rekonstruieren. Abschließend zeigt Duplicati eine Zusammenfassung an und beginnt mit der Wiederherstellung.

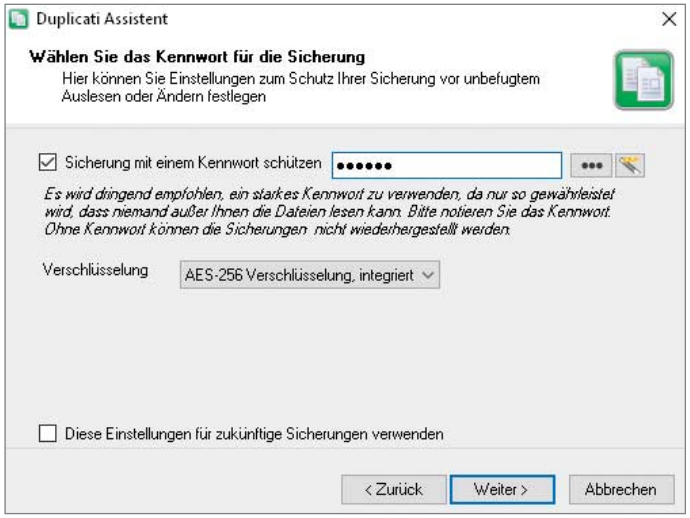
Offene Formate

Duplicati zeigt sich offen: Das Programm ist Open Source und die Backups werden in dokumentierten Formaten gespeichert, die man auch ohne das Tool öffnen kann. Es handelt sich um Zip-Archive, die im Format des Krypto-Tools AES Crypt verschlüsselt werden. Man kommt daher auch ohne Duplicati an die gesicherten Dateien. Zunächst entschlüsselt man die Dateien mit AES Crypt, anschließend entpackt man sie mit einem beliebigen Entpack-Programm oder der Standardfunktion von Windows. Die Dateien liegen in den Backup-Schnipseln, die mit duplicati-full-content beginnen und auf .zip.aes enden. Nach dem Entpacken findet man die gesicherten Dateien im Ordner snapshot. Standardmäßig sind die Zip-Archive 10 MByte groß. Dateien, die größer sind, zerteilt Duplicati auf mehrere Archive. In solchen Fällen kann man die Dateien rekonstruieren, indem man sie nach dem Entpacken aneinander kopiert; etwa, indem man sie in datei.endung.001, datei.endung.002, ... umbenennt und mit dem Tool HJ-Split zusammenfügt.

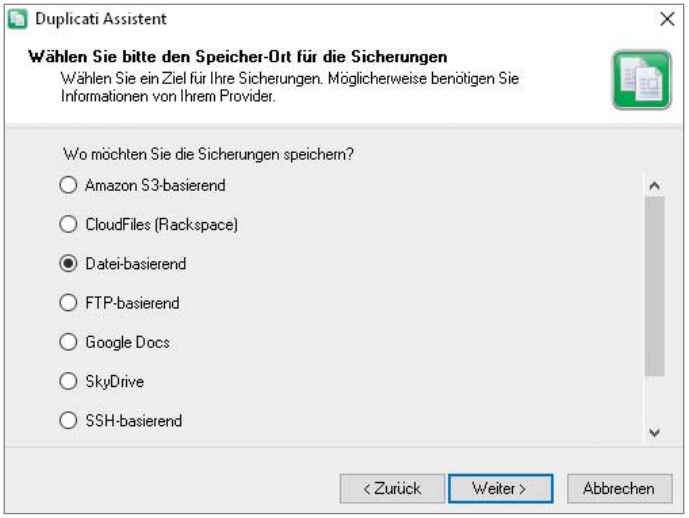
Verfeinern und automatisieren

Wenn die erste Wiederherstellung geklappt hat, geht es bei Bedarf an das Verfeinern und weitergehende Automatisieren Ihrer Backup-Aufträge. Denn das volle Potenzial von Duplicati ist noch längst nicht ausgeschöpft. Los geht es mit den erweiterten Einstellungen, die das Backup-Tool im Verlauf des Assistenten anbietet: Mit „Wählen Sie, wenn die Sicherung ausgeführt werden soll“, legen Sie nicht nur den Zeitpunkt fest, sondern auch, wie oft gesichert werden soll. Die Option „Nie automatisch ausführen“ wählt man, wenn das Speicherziel ein USB-Datenträger ist, der als Schutzmaßnahme vor Krypto-Trojanern nur bei Bedarf mit dem Rechner verbunden wird. In diesem Fall stoßen Sie das Backup über den Assistenten manuell an oder befehlen dem Aufgabenplaner von Windows, den Job auszuführen, sobald ein bestimmter USB-Speicher angeschlossen wird (siehe „Auf Kommando“).

Als Intervall bietet Duplicati im Dropdown-Menü als kleinsten Wert „täglich“ an. Möchten Sie häufiger sichern, wählen Sie „Benutzerdefiniert ...“ und geben etwa 1h an, um den Job stündlich ausführen zu



Duplicati verschlüsselt die Backups standardmäßig mit AES-256.



Das Backup-Tool unterstützt eine ganze Reihe von Speicherzielen.

lassen. Sie können an dieser Stelle auch Jahre (Y), Monate, (M), Wochen (W), Tage (D), Minuten (m) oder Sekunden angeben (s). Die Option „Strategie für vollständige / inkrementelle Sicherungen“ legt fest, wie häufig Duplicati zwischendurch vollständige Kopien der Dateien sichert. Würde das Programm nicht von Zeit solche Kopien anlegen, müsste es sich bei der Wiederherstellung stets durch sämtliche Zwischenstände der inkrementellen Sicherung wühlen, was einige Zeit beanspruchen kann. Mit der erweiterten Einstellung „Wählen Sie, wann alte Sicherungen entfernt werden“, stellen Sie zum Beispiel ein, wie viele vollständige Sicherungen Duplicati aufhebt – und wie lange.

Eine interessante Option versteckt sich hinter „Stellen Sie ein, wie die Rechnerlast begrenzt wird“: Hier können Sie nicht nur die Task-Priorität des Backup-Prozesses einstellen und die Netzwerkauslastung begrenzen, sondern auch die Größe der Datei-Schnipsel bestimmen. Die voreingestellten 10 MByte führen bei größeren Datenmengen schnell zu mehreren tausend Backup-Dateien. Je größer die Schnipsel werden dürfen, desto weniger kommen am Ende dabei raus. Zudem können Sie über die erweiterten Einstellungen Filter definieren, um nur bestimmte Dateitypen in die Sicherung einzuschließen oder unnötigen Ballast auszuschließen.

Auf Kommando

Wer einfach nur mit geringem Aufwand das Wichtigste wegsichern möchte, der ist mit dem Assistenten gut bedient. Wer sich mehr Individualität wünscht, der findet im Installationsverzeichnis ein Programm namens Duplicati.CommandLine.exe, mit dessen Hilfe man Duplicati flexibel steuern und automatisieren kann. Die ersten Schritte sind einfach: Nutzen Sie als Grundlage einen mit dem Assistenten erstellten Backup-Job. Im letzten Schritt zeigt der Assistent auf dem Registerreiter „Command Line“ an, mit welchen Parametern man das Kommandozeilen-Äquivalent aufzurufen hat, damit es genau das ausführt, was man über die grafische Bedienoberfläche eingestellt hat. Eine Sicherung des Dokumenten-Ordners auf den USB-Stick I: führt zu folgenden Befehlen:

```
"C:\Program Files\Duplicati\Duplicati.
↳CommandLine.exe" backup --passphrase=
↳********** --aes-encryption-dont-allow-
↳fallback=true --full-if-older-than=1M
↳C:\Users\rei\Documents\ file://I:\

"C:\Program Files\Duplicati\Duplicati.
↳CommandLine.exe" delete-all-but-n 4
↳--aes-encryption-dont-allow-fallback=
↳true --full-if-older-than=1M
↳file://I:\
```

Die Sternchen im Parameter „passphrase“ ersetzen Sie durch das gewünschte Backup-Passwort.

Die erste Zeile führt die Sicherung durch, die zweite mistet alte Backups aus. Um den Job komfortabel per Doppelklick zu starten, kopieren Sie die beiden Zeilen in eine Textdatei, die Sie backup.bat nennen. Dadurch wird das Passwort im Klartext auf dem System gespeichert. Wer allerdings Zugriff auf Ihr System hat, kann ohnehin die Dateien einsehen, die Sie mit dem Passwort schützen. Bei Zugangsdaten, etwa für FTP, sollten Sie sicherheitshalber speziell für diesen Zweck eingerichtete Backup-Nutzer einsetzen (siehe S. 106).

Mit der Batch-Datei können Sie die Sicherung nun bei Bedarf per Doppelklick ohne den Umweg über den Assistenten ausführen – etwa, nachdem Sie Ihren Backup-Stick mit dem Rechner verbunden haben. Mit diesem Konzept übertragen Sie alle Funktionen des Assistenten in Batch-Skripte. Beachten Sie, dass dabei kein Job angelegt wird, der über die Bedienoberfläche sichtbar ist. Eine Liste der möglichen Parameter erhalten Sie, indem Sie das Programm Duplicati.CommandLine.exe über die Kommandozeile ohne Optionen aufrufen. Darunter befinden sich nützliche Funktionen, die man über die Bedienoberfläche nicht erreichen kann, etwa das Logging. Für weitere Details zu den einzelnen Parametern nutzen Sie den Befehl `help`, gefolgt von dem Namen des Parameters, also etwa:

```
Duplicati.CommandLine.exe help logging
```

Komfort durch Aufgaben

Die Kommandozeilenversion von Duplicati ist eine universelle Schnittstelle zur Automatisierung, welche man zum Beispiel über die Aufgabenplanung von Windows ansprechen kann. So bringt man das System etwa dazu, automatisch die Sicherung zu starten, sobald ein bestimmter USB-Speicher mit dem Rechner verbunden wurde. Dazu muss man zunächst den Gerätepfad des Speichers herausfinden. Anschließend erstellt man eine Aufgabe, die auf das Anschließen des Geräts reagiert. Die Einrichtung dauert ein paar

Ausblick auf Duplicati 2

Duplicati 1.3.4 stammt vom Februar 2013 und sieht auch danach aus – das dürfte einige Anwender nervös machen, was die Weiterentwicklung des Programms angeht.

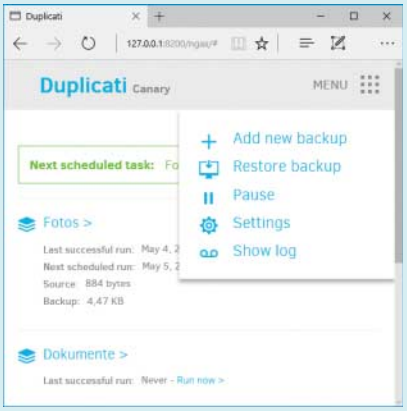
Tatsächlich wird die Nachfolge-Version Duplicati 2 bereits seit 2014 entwickelt. Ein fertiges Release ist aber noch nicht in Sicht – Duplicati ist ein quelloffenes Freizeitprojekt. Eine Vorabversion steht zwar zum Download bereit; zum produktiven Einsatz ist sie aber noch nicht geeignet.

Was bereits zu sehen ist, lässt aber auf eine schnelle Weiterentwicklung hoffen. Duplicati 2 besitzt keine klassische Programmoberfläche mehr; es wird komplett über den Browser konfiguriert und gepflegt. Das Ergebnis wirkt wesentlich aufgeräumter und besser gegliedert als die Assistenten von Duplicati 1.

Die Änderungen unter der Haube beeindrucken ebenfalls: Duplicati 2 versteht neue Kommandozeilenbefehle und arbeitet mit einer neuen Engine zur Verschlüsselung und Kompression; ein integrierter Updater hält die Anwendung auf dem aktuellen Stand. Die kommende Version unterstützt auch neue Cloud-Speicherziele, darunter Amazon Cloud Drive, Google Drive, Microsoft OneDrive, Mega.co.nz und OpenStack.

Duplicati 2 soll sich auch als Systemdienst betreiben lassen – was die Preview aber noch nicht umsetzt. Weiterhin fehlen der Preview ein Installer und eine deutsche Lokalisierung. Auch nach einem „Major Update“ von Ende März 2016 lief die Preview im Test immer noch nicht zuverlässig – so scheiterte jeder FTP-Upload auf ein lokales NAS mit einem Serverfehler.

Selbst wenn dieses Problem beseitigt ist, sollte man tunlichst auf eine von den Entwicklern als „stabil“ deklarierte Version warten: Nicht, dass das Backup-Tool von einem Build auf den nächsten den Dienst verweigert, derweil ein Verschlüsselungs-Trojaner zuschlägt und man plötzlich mit nicht mehr wiederherstellbarem Backup im Regen steht. Datensicherung ist ein Bereich, in dem der Adenauer-Spruch „Keine Experimente“ ausnahmsweise gerechtfertigt ist. *(ghi@ct.de)*



Die kommende Version 2 von Duplicati bietet ein modernes Interface und zahlreiche neue Funktionen.

Minuten länger, langfristig ist das aber äußerst komfortabel.

Starten Sie zunächst die Ereignisanzeige über eine Suche im Startmenü. Anschließend navigieren Sie über die Baumstruktur in der linken Spalte zu folgendem Ereignisprotokoll: Anwendungs- und Dienstprotokolle/Microsoft/Windows/DriverFrameworks-UserMode/Betriebsbereit. Wenn die Ereignisliste im mittleren Bereich leer ist, klicken Sie in der Baumansicht mit rechts auf „Betriebsbereit“ und „Protokoll aktivieren“. Wenn Sie jetzt zum Beispiel einen USB-Stick mit dem Rechner verbinden und F5 drücken, erscheinen im mittleren Bereich des Fensters diverse Ereignisse. Klicken Sie auf eines davon – zum Beispiel das oberste mit dem blauen Symbol (Ebene: Ausführlich). Anschließend wechseln Sie unter der Ereignisliste auf den Registerreiter „Details“. Hier finden Sie einen Parameter namens „instance“, der zum Beispiel den folgenden Pfad enthält:

```
SWD\WPDBUSENUM\_??_USBSTOR#DISK&VEN_↵
↳INNOSTOR&PROD_INNOSTOR&REV_1.00#↵
↳316889782&0#{53F56307-B6BF-11D0-94F2-↵
00A0C91EFB8B}
```

Mit diesen Informationen kann Windows ein bestimmtes USB-Gerät identifizieren. Bevor man daraus eine Aufgabe basteln kann, die auf das Gerät reagiert, muss man die im Text enthaltenen Sonderzeichen maskieren. In unserem Beispiel ist lediglich das &-Symbol durch & zu ersetzen:

```
SWD\WPDBUSENUM\_??_USBSTOR#DISK&amp;↵
↳VEN_INNOSTOR&amp;PROD_INNOSTOR&amp;↵
↳REV_1.00#316889782&amp;0#{53F56307-↵
B6BF-11D0-94F2-00A0C91EFB8B}
```

Sie können für die Maskierung auch einen der zahlreichen Online-Converter oder das schlanke Hilfsprogramm „Sonderzeichen maskieren“ nutzen.

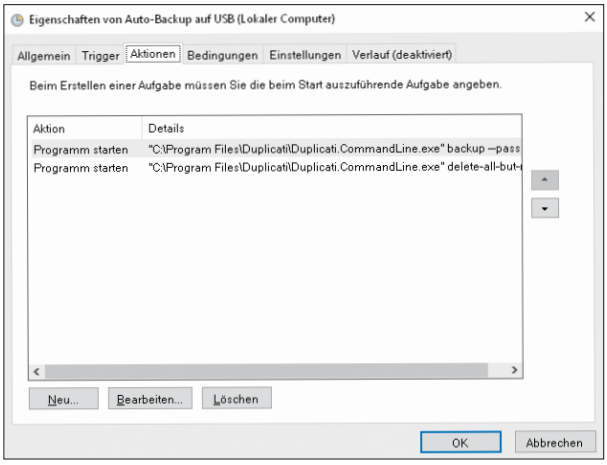
Von Geisterhand

Jetzt müssen Sie nur noch eine Aufgabe anlegen. Um diesen Vorgang abzukürzen, bieten wir über den c’t-Link eine Vorlage an, die Sie leicht anpassen können. Starten Sie die Aufgabenplanung über eine Startmenü-Suche und klicken Sie in der Menüleiste unter „Aktion“ auf „Aufgabe importieren...“. Wählen Sie anschließend unsere Vorlage mit der Endung .xml, woraufhin sich der vorausgefüllte Dialog „Aufgabe erstellen“ öffnet. Auf dem Registerreiter „Trigger“ klicken Sie auf „Bei einem Ereignis“, „Bearbeiten“ und „Ereignisfilter bearbeiten“. Ersetzen Sie den Platzhalter „Hier den Pfad eintragen“ durch den maskierten Pfad Ihres USB-Geräts. Achten Sie darauf, dass er von Anführungszeichen umschlossen wird. Klicken Sie zweimal auf „OK“ und wechseln Sie auf den Registerreiter „Aktionen“. Hier legen Sie fest, welche Aktionen ausgeführt werden sollen.

Zur Veranschaulichung haben wir zwei Standard-Jobs von Duplicati hinterlegt. Bearbeiten Sie die Einträge und geben Sie unter „Programm/Skript“ den korrekten Pfad zur Duplicati.CommandLine.exe an. In das Feld „Argumente hinzufügen“ kopieren Sie zum Beispiel die

Kommandozeilen-Parameter, die der Duplicati-Assistent generiert hat. Abschließend klicken Sie noch zweimal auf „OK“ – Ihre neue Aufgabe ist nun aktiv. Verbinden Sie das USB-Gerät mit dem Rechner. Jetzt sollte jeweils ein Kommandozeilen-Fenster für das Backup und das Aufräumen erscheinen und nach getaner Arbeit wieder verschwinden. Sie können mit der Aufgabe freilich auch beliebige weitere Programme starten, beispielsweise um den USB-Stick nach dem Backup automatisch auszuwerfen. Hierzu können Sie das auf Seite 104 beschriebene Batch-Skript oder das Tool RemoveDrive nutzen.

Mit Duplicati und der Aufgabenplanung sind Sie äußerst flexibel: Starten Sie Ihre Backups dann, wenn es Ihnen am besten passt. Wenn Sie Ihren Rechner etwa regelmäßig sperren, können Sie das Backup „Bei Arbeitsstation sperren“ ausführen lassen – so wird jedes Mal ein Zwischenstand gesichert, wenn Sie den Rechner verlassen. Ein weiterer Trigger wird ausgeführt, wenn das System im Leerlauf ist und ohnehin nichts Besseres zu tun hat.



Die Aufgabenplanung von Windows startet auf Wunsch automatisch ein Backup, wenn ein bestimmter USB-Stick mit dem Rechner verbunden wird.

Und falls Sie jetzt immer noch kein Backup Ihrer wichtigsten Dateien haben, legen Sie los! *(rei@ct.de)* c't

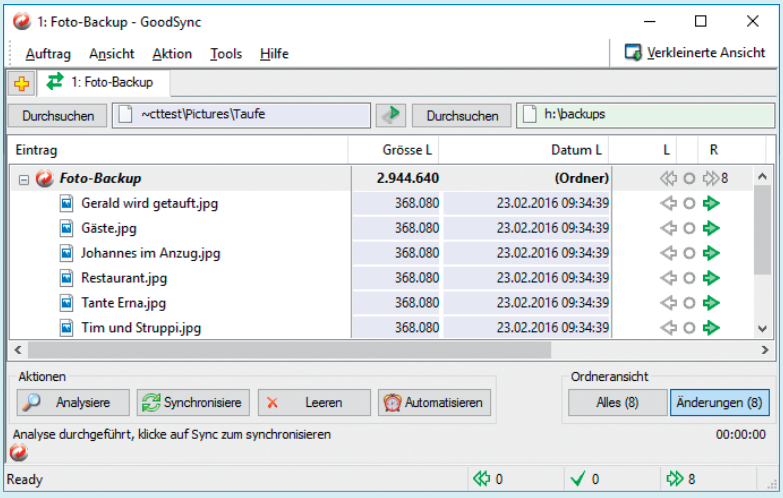
***Duplicati & Co.:* ct.de/ywtg**

Für ein paar Dollar mehr: GoodSync

Das Backup-Programm GoodSync ist ein bisschen komfortabler als Duplicati und zusätzlich für Android und iOS verfügbar. Eine Einzellizenz der Windows- und Mac-Version kostet 30 Euro; zusätzliche Lizenzen schlagen mit je 10 Euro zu Buche. Die Mobil-Apps sind kostenlos.

Das Tool kann sowohl Datenbestände abgleichen als auch sichern. Hierfür definiert man eine linke und eine rechte „Seite“, also Quelle und Ziel, und passt dann an, welchen Bezug die beiden Pfade zueinander haben sollen. Neben Ordnern, Laufwerken und Windows-Freigaben unterstützt GoodSync auch FTP/SFTP und WebDAV sowie die Cloud-Speicher Amazon S3, Azure, Dropbox, Google Drive, Office 365 und OneDrive.

In den Optionen lassen sich viele Details anpassen: ob und wo GoodSync ersetzte Dateiversionen zwischenspeichern soll, ob Dateiinhalte und/oder deren Namen AES-verschlüsselt werden sollen sowie Feinheiten wie die Behandlung von Sicherheitsattributen und der Rückgriff auf Schattenkopien. Sync-Aufträge können bei jeder Dateiänderung oder beim Anschluss eines Wechselmediums starten oder zu festen Terminen. Vor und nach der Synchronisation lassen sich Skripte oder Programme starten und Mails mit Statusnachrichten versenden. GoodSync ist sehr gut englischsprachig dokumentiert und wird etwa im Monatsrhythmus aktualisiert. Die aktuelle Version 9.9 soll in Bälde von GoodSync 10 abgelöst werden, das eine neue Oberfläche, Auftragsgruppen und erweiterte Optionen mitbringt. *(ghi@ct.de)*



Die kommerzielle Duplicati-Alternative GoodSync bietet mehr Komfort, hat aber auch ihren Preis.