Dropbox-Alternativen

Dateisynchronisation in der Cloud, auf dem eigenen Server und Peer-to-Peer

Dateien teilen kann harte Arbeit sein: Der datenschutzbewusste Freund will keine Cloud-Anbieter nutzen, der Linux-affine Kollege klagt über den abgekündigten Dropbox-Support und die Großeltern haben das OneDrive-Passwort vergessen. Wir zeigen, warum es sich lohnt, andere Cloud-Speicherdienste als Dropbox in Betracht zu ziehen oder sogar auf ganz andere Konzepte zum Dateiabgleich zu setzen.

Von Merlin Schumacher

Früher hatte man einen Computer, auf dem alles lag, was man regelmäßig benötigte. Heute jongliert man seine Dateien auf Smartphones, Tablets, Laptops und PCs zugleich – alle brauchen also aktuelle Kopien der Dateien. Diesen Gerätepark per Hand abzugleichen ist eine unlösbare Aufgabe. Wie von Zauberhand erledigen das Cloud-Speicheranbieter wie etwa Dropbox, Google Drive oder Microsofts OneDrive. Dafür muss man denen aber die eigenen Daten anvertrauen. Ähnlich komfortabel, aber auf dem privaten Server laufen Lösungen wie Nextcloud oder Seafile. Ganz ohne zentrale Instanz hingegen arbeiten Peer-to-Peer-Synchronisationsdienste. Hier gleichen alle beteiligten Geräte (Peers) ihre Dateien untereinander ab.

Bei der Wahl des Dienstes gibt es vielerlei zu beachten. Man sollte sich klarmachen, welches Problem man zu lösen versucht und welches Produkt dazu passt. Dabei darf man aber auch Datenschutz und die eventuell notwendige administrative Arbeit nicht vergessen. Vielleicht sollte man auch bestehende Lösungen wie etwa die Netzwerkfreigabe des heimischen WLAN-Routers durch etwas Leistungsfähigeres und vor allem Sichereres ersetzen.

Das Gute an den Cloud-Diensten ist, dass man sich nicht um die Wartung und Pflege zu kümmern braucht. Man kann sich guten Gewissens darauf ausruhen, dass es in der Verantwortung der Anbieter liegt, den Dienst stabil und sicher zu betreiben – oft besser, als man das selber könnte. Die Lösungen für den eigenen Server muss man selber warten und updaten. Gibt es Probleme, muss man selbst ran!

Dieser Gedanke funktioniert aber auch anders herum: Man ist auf Gedeih und Verderb dem Anbieter ausgeliefert. Ist der Dienst gestört, kann man nichts tun als warten, bis das Unternehmen die Probleme beseitigt hat. Beim eigenen Server legt man Hand an und beseitigt das Problem bestenfalls in Minuten. Dabei hat man die freie Wahl, auf welche Technik man setzt: Wer ohnehin regelmäßig mit der Versionskontrollsoftware Git arbeitet, findet ebenso eine Lösung wie jemand, der von Linux-Kommandozeilenbefehlen keine Ahnung hat, aber dennoch einen eigenen Server aufsetzen will (Seite 84).

Freigaben vs. Synchronisation

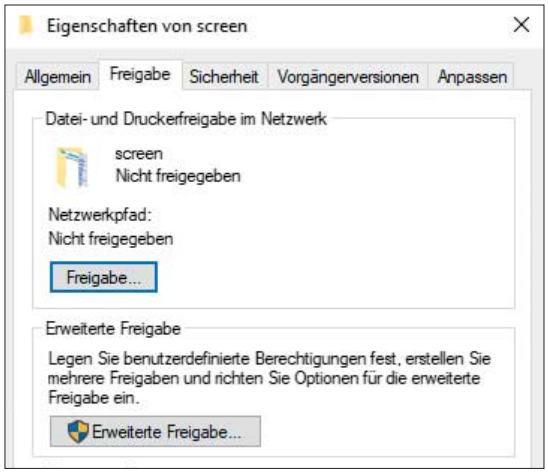
Der Klassiker zum Austausch von Dateien über das Netz sind Windows-Netzwerkfreigaben oder korrekter: SMB-Freigaben. Diese unterstützen praktisch alle Betriebssysteme, NAS und Router seit Jahrzehnten. Im Gegensatz zu den hier vorgestellten Lösungen gleichen Netzwerkfreigaben jedoch nichts ab. Die Daten lagern lediglich auf einem zentralen Server. Clients können die Daten einsehen und bearbeiten. Zudem sind die SMB-Freigaben nicht über das Internet erreichbar, sondern nur im LAN oder per VPN. Auf Smartphones macht das Gehampel mit den Netzwerkfreigaben gar keinen Spaß – wenn es überhaupt klappt.

Seit 2016 hängt der SMB-Haussegen endgültig schief: Version 1 des SMB-Protokolls ist unsicher und Microsoft hat den Support – aus gutem Grund – abgekündigt. Das ist leider noch nicht bei allen NAS- und Router-Herstellern angekommen. Besonders dürfte das Fritzbox-Besitzer ärgern, denn die kann nur SMB1 und damit taugt der interne NAS-Dienst MyFritz nicht guten Gewissens als Netzwerkfreigabe. Wer ein älteres NAS verwendet, guckt auch in die Röhre, sofern der Hersteller kein Update für SMB2 oder 3 liefert. Eine kleine Liebhabergemeinde haben sich auch Microsofts Heimnetzgruppen[2] erarbeitet. Die hat Microsoft aber mit Windows 10 1803 ersatzlos gestrichen – die Menge der Fans war dann doch zu klein.

Besitzer moderner NAS haben oft die Möglichkeit, einen oder mehrere der vorgestellten Server- oder Peer-to-Peer-Dienste auszuführen. Die Hersteller bieten dafür installierbare Pakete an. Alternativ kann man bei besseren Modellen auf Docker-Images[3] zurückgreifen. Gewiefte Admins können die eigenen Datenbestände dadurch auf unterschiedlichen Wegen bereitstellen: per Netzwerkfreigabe für Streaming-Clients, per flexiblem Peer-to-Peer-Dienst für die PCs und als Cloud für Smartphones und Tablets.

Wo sind all die Daten hin?

Nicht erst seit der Einführung der DSGVO[4] ist die Frage nach dem physischen Serverstandort wichtig. Liegen die



Für den einmaligen Austausch von Daten im Netz okay, aber für Synchronisation nicht geeignet: die Windows-Netzwerkfreigabe

Dateien im (außereuropäischen) Ausland, gilt das dortige – oft schlechtere – Datenschutzrecht. So strenge Datenschutzgesetze wie in Deutschland findet man fast nirgendwo. Gerade wenn man mit personenbezogenen und privatesten Daten oder Geschäftsgeheimnissen hantiert, sollte einem bewusst sein, welche Verantwortung man trägt. Ist man der Familien-Admin und sichert die Dokumente und Backups der Verwandtschaft, muss man sich bei einem Datenverlust oder Hack im besten Fall nur mit seinem schlechten Gewissen quälen. Für Unternehmen kann schlampiger Umgang mit eigenen Daten oder Daten von Kunden rechtliche und finanzielle Konsequenzen nach sich ziehen.

Wer Daten in der Cloud oder auch auf dem eigenen Mietserver lagert, sollte nachfragen, wo der steht. Gerade bei Cloud-Anbietern ist diese Frage manchmal nicht genau zu beantworten. Einige der Anbieter erlauben (gegen Bezahlung) die Wahl eines innereuropäischen Standorts. Manche werben sogar mit hoher Datensicherheit, dank Servern in der EU oder in Deutschland. Aber auch hier muss man dem Anbieter vertrauen, dass die Daten wirklich da sind, wo er behauptet.

Bei dem eigenen Server oder NAS zu Hause oder im Büro beantwortet sich die Frage nach dem Standort von selbst. Man ist dann aber auch für die (physische) Datensicherheit verantwortlich. Im Büro sollte nicht jeder physischen Zugriff auf die Datenhalde haben, von den Zugriffsrechten mal ganz abgesehen. Ein Einbrecher wittert vielleicht fette Beute beim Anblick des Servers und nimmt die Klientendaten gleich mit. Im Familien-Umfeld sollte man sicherstellen, dass die Daten aller Personen sauber getrennt bleiben und auf die Zugriffsrechte achten, denn das gehört auch zur Wahrung von Privatsphäre und informationeller Selbstbestimmung.

Vertrauen ist gut, Verschlüsselung ist besser!

Fast keiner der Cloud-Dienste bietet eine integrierte Verschlüsselung der Daten an. Private Daten liegen also womöglich im Klartext auf fremden Servern. Wer das nicht möchte, kann zum eigenen Server mit verschlüsseltem Speicher greifen oder ein Peer-to-Peer-System verwenden. Soll es auf jeden Fall ein Cloud-Anbieter sein, kann man die Inhalte der Speicher mit Werkzeugen wie Boxcryptor oder Cryptomator verschlüsseln. Selbst wenn jemand die Dateien stehlen sollte und versucht, Einblick zu nehmen, bekommt er nur verschlüsselten und für ihn nicht verwendbaren Datenmüll.

Wer Daten in die Cloud legt, um sie mit anderen zu teilen, sollte sie zumindest als passwortgeschütztes Archiv oder besser noch per PGP verschlüsselt bereitstellen. Sind es Dateien, die ohnehin öffentlich zugänglich sein sollen, ist die Verschlüsselung eher hinderlich als sinnvoll.

Apropos Verschlüsselung: Wer Speicherdienste mit Webinterface auf dem eigenen Server laufen lässt, sollte das nur per SSL-verschlüsselter Verbindung bereitstellen. Dank Let's Encrypt ist das Erzeugen von signierten Zertifikaten kein Aufwand mehr [5]. Das bringt nicht nur für einen selbst Sicherheit, sondern auch für andere, die dann sichergehen können, dass die Verbindung korrekt verschlüsselt ist. Zudem verschwinden hässliche und womöglich irritierende Zertifikatsfehler.

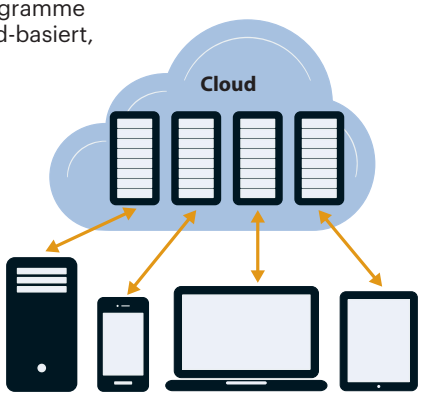
Kein Backup!

Nur weil Daten auf mehreren Geräten lagern, entbindet das nicht von der Pflicht, ein Backup zu machen! Zu schnell sind Dateien aus Versehen aus der Cloud oder vom Gerät gelöscht, die man hinterher doch vermisst. Man hat zwar das Gefühl, dass da Redundanz besteht. Bedenken Sie

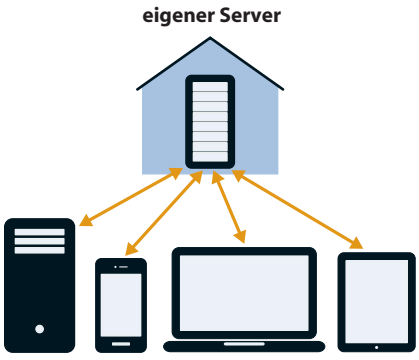
Arten der Dateisynchronisation

Die von uns vorgestellten Dienste und Programme zerfallen in drei Funktionsprinzipien: Cloud-basiert, Server-basiert und Peer-to-Peer.

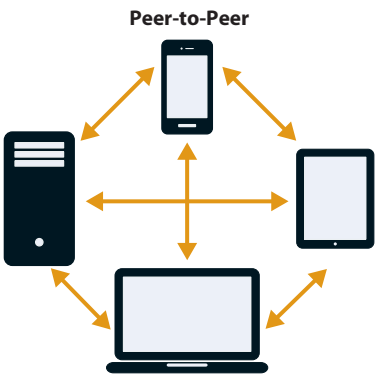
Bei der ersten Variante synchronisieren alle Clients ihre Daten in eine zentrale Cloud, also über das Internet in eine Menge von Servern in einem oder mehreren Rechenzentren. Die Cloud-Dienste sind von überall erreichbar, sodass alle Clients jederzeit darauf zugreifen können.



Variante Nummer zwei ist der eigene Server. Hier läuft ein Dienst, der sich ähnlich wie bei einem Cloud-Anbieter um die Verwaltung der Dateien und Clients kümmert. Der Server steht dabei entweder gemietet in einem Rechenzentrum oder auch als Eigentum im eigenen Zuhause. Je nach Konfiguration ist er für die Clients jederzeit erreichbar, oder nur wenn diese sich im heimischen Netz befinden.



Die letzte Variante sind die Peer-to-Peer-Dienste. Hier gibt es weder Server noch Clients, sondern nur gleichberechtigte Peers, die Änderungen untereinander austauschen. Damit der Abgleich funktioniert, muss es immer einen Weg von Gerät zu Gerät geben. Wenn im Urlaub das Smartphone Daten mit dem Laptop abgleicht, landen die spätestens bei der Rückkehr auch auf dem Desktop-PC daheim – ob die Änderungen dabei vom Laptop oder vom Smartphone geschickt werden ist unerheblich. Das Spiel geht in jede Richtung.



jedoch, dass auch ein Riese wie Google oder Microsoft nicht unfehlbar ist. Die Daten könnten abhandenkommen. Eine Account-Sperrung kann ein Desaster zur Folge haben. Eine Amok laufende Sync-Software oder ein Verschlüsselungstrojaner kann die gehegten Dokumente mit einem Hieb vernichten. Und manchmal reicht schon ein unbedachter Klick! Ein regelmäßiges Backup ist deshalb trotz Einsatz von Synchronisationsdiensten unentbehrlich.

Testfeld

Gerade aus der Überlegung heraus, dass man eben nicht mehr nur mit einem Gerät arbeitet, haben wir nicht nur die Client-Software für Desktops, sondern auch auf Mobil-Clients und Webinterfaces getestet. Was hilft die beste Synchronisation, wenn man sich mit einer unbedienbaren Smartphone-App rumärgern muss? Dass alle drei großen Betriebssysteme unterstützt werden, ist schön, hilft aber wenig, wenn man kein Web-Interface für den schnellen Upload am fremden PC hat. Außen vor gelassen haben wir Kollaborationslösungen wie Office 365 [1] oder Dropbox Paper. Das sind unabhängige Produktkategorien, die eine gesonderte Betrachtung erfordern.

Eine der größten Herausforderungen für all diese Dienste ist die Effizienz. So sollte ein guter Synchronisationsdienst darauf achten, so wenig Daten wie möglich zu übertragen. Verschobene Dateien sollten genauso wenig zu einem erneuten Upload führen wie das Kopieren einer bereits im (Cloud-)Speicher befindlichen Datei. Wie schlampig mancher Cloud-Anbieter mit der Bandbreite des Anwenders umgeht, hat uns erstaunt. Details lesen Sie auf Seite 90.

Mindestens genauso wichtig ist das Konfliktmanagement. Niemand will Stunden an Arbeit verlieren, weil sich auf dem wenig genutzten Tablet noch eine alte Version eines Word-Dokuments befindet und nun die aktuelle Fassung überschreibt. Selbst wenn der Dienst einen Dateikonflikt nicht erkennt oder falsch löst, sollte ein guter Dienst die Möglichkeit bieten, alte Dateiversionen wiederherzustellen.

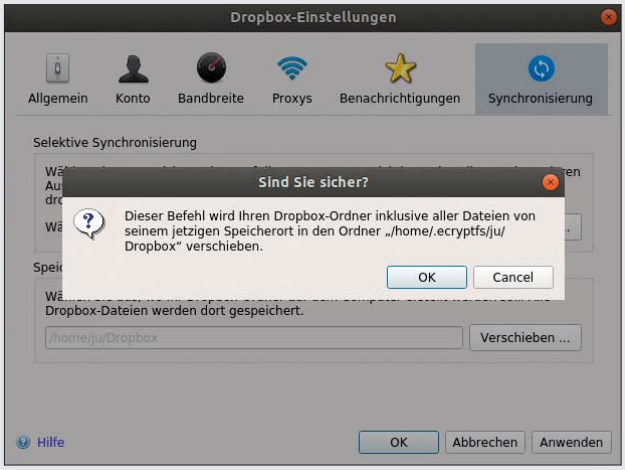
Für welchen Typ von Dateiabgleich Sie sich entscheiden, kommt ganz auf Ihre Anforderungen an: Eine riesige Foto-Sammlung via Peer-to-Peer mit allen Geräten abzugleichen mag für den Profi-Fotografen essenziell sein. Die privaten Familienfotos der letzten 15 Jahre müssen aber nicht auf jedem Laptop schlummern. Um Dokumente mit (entfernten) Kollegen oder Freunden gemeinsam zu bearbeiten, dient sich ein kommerzieller Cloud-Dienst mit integrierter Office-Suite an. Die Smartphone-Fotos der Kinder und die Steuererklärung will man gut verwahrt wissen und sichert sie lieber auf dem eigenen Server als in der Cloud. Manchmal ist man auch mit zwei Lösungen am besten bedient: eine private Nextcloud für die eigenen Daten und ein Cloud-Anbieter für das Teilen von Daten mit anderen. Jenseits von Dropbox gibt es viele unterschiedliche Lösungen, um seine Daten jederzeit griffbereit zu haben. *(mls@ct.de)* c't

Dropbox und Linux

Ab Anfang November 2018 will Dropbox den Support für Linux einschränken. Seit der Ankündigung im August sendet der Dienst unermüdlich Hinweis-E-Mails und der Client zeigt regelmäßig Pop-ups mit der bevorstehenden Support-Abkündigung. Davon betroffen sind alle Linux-Systeme, die andere Dateisysteme als Ext4 verwenden und solche, die die dateisystemeigene Verschlüsselung von Ext4 einsetzen. Das zur Verschlüsselung des Home-Verzeichnisses populäre eCryptfs will Dropbox ebenfalls nicht mehr unterstützen. Anwender, die Ext4 auf einer LUKS-verschlüsselten Partition nutzen, müssen sich keine Gedanken machen.

Trotz massiver Kritik der Dropbox-Kunden hat sich das Unternehmen nicht umstimmen lassen. Dropbox begründet die Einschränkung mit für den Client notwendigen, erweiterten Dateisystemattributen (Extended Attributes). Das scheint aber nur vorgeschoben zu sein, denn die meisten unter Linux gebräuchlichen Dateisysteme unterstützen die geforderten erweiterten Dateisystemattribute. Auch gab es vorher keine bekannten Probleme mit anderen Dateisystemen und dem Client.

Es ist also möglicherweise an der Zeit, sich nach Alternativen umzusehen. Wer das nicht will oder kann, muss sich einen Workaround überlegen. Der einfachste ist, Dropbox nur noch im Web zu nutzen, was der nahtlosen Synchronisation entgegenläuft. Alternativ muss man den Dropbox-Ordner auf eine (per LUKS verschlüsselte) Ext4-Partition verschieben. Die LUKS-Verschlüsselung verschlüsselt dabei nur die lokalen Dateien, aber nicht die in der Dropbox-Cloud. Dort liegen sie noch immer im Klartext. Dafür enthält der Client eine eigene Option (siehe Screenshot). Kommt das nicht infrage, kann man versuchen, Werkzeuge wie Rclone zur Synchronisation einzusetzen oder die Daten mittels des Fuse-Dateisystems Dbxfs zu erreichen.



Den Umzug des Dropbox-Ordners auf ein kompatibles Dateisystem erleichtert der offizielle Client mit der „Umziehen“-Funktion.

Literatur

[1] Jörg Wirtgen, Heim-Office, Office 365 Deutschland für Privatanwender, c't 9/2017, S. 78
[2] Jan Schüßler, Gruppentherapie, Heimnetzgruppen in Windows 10 ersetzen, c't 16/2018, S. 118
[3] Ernst Ahlers, Container-Spielplätze, x86-Netzwerkspeicher mit Docker-Option, c't 7/2018, S. 110
[4] Joerg Heidrich, Aufgewertet, Die DSGVO bringt den Bürgern neue Rechte, c't 5/2018, S. 112
[5] Uli Ries, Let's Encrypt!, SSL/TLS-Zertifikate gratis für alle, c't 4/2018, S. 80