So geht's leichter...

In die Cloud: Aber sicher!

- Cloud-Lösungen nutzen
- Schnell Daten austauschen
- Daten in der Cloud wirksam schützen
- Cloud-Konten absichern
- Meine eigene Cloud-Lösung

Jörg Schieb

Autoren:
Jörg Schieb
Andreas Erle

Impressum:
Redaktion schieb.de
Humboldtstr. 10
40667 Meerbusch
Kontakt: fragen@schieb.de
www.schieb.de

So geht's leichter | In die Cloud – aber sicher!

Inhalt

So geht's leichter | In die Cloud – aber sicher!

So geht’s leichter | In die Cloud – aber sicher!

In die Cloud: Aber sicher!

Die Cloud: Lange schon Bestandteil unseres Lebens, mit der Zeit aber immer wichtiger geworden. Nicht nur, weil Windows mit OneDrive und Microsoft 365 immer mehr Daten und Dienste in die Cloud auslagert und ihr dem bei Windows 10 und 11 kaum noch entgehen könnt. Auch unser Arbeitsverhalten hat sich mehr und mehr geändert. Ein lokaler Arbeitsplatz ist Geschichte, wir arbeiten von überall und mit verschiedenen Geräten.

Die Cloud ist mächtig und hilft uns, aber sie ist auch gefühlt unbeherrschbar. Während wie unsere eigene Festplatte im Gerät auf dem Schreibtisch im Notfall sogar anfassen können, die Daten in der Cloud nicht greifbar. Irgendwo im Cyberspace, unter der Kontrolle eines Dienstleisters, dem wir vertrauen müssen, ob wir wollen oder nicht.

Seid ihr unruhig? Wollt Ihr die Cloud nutzen, aber mehr Sicherheit haben, dass Eure Daten vor Fremdzugriffen geschützt sind? Wir zeigen euch, wie ihr auch bei Fremdanbietern wie Microsoft oder Dropbox

So geht's leichter | In die Cloud – aber sicher!

sicherstellen könnt, dass eure Daten sicher sind. Durch gesicherte Zugänge, Verschlüsselung und gute Passwörter. Das reicht Euch nicht? Dann ist vielleicht das Aufsetzen einer eigenen Cloud-Lösung auf einer Netzwerkfestplatte oder mittels eines Anbieters wie Nextcloud eine Alternative!

Nutzen einer externen Cloud-Lösung

Für Eure Dokumente verwendet ihr die Cloud, weil sie einen großen Vorteil hat: eure Daten sind dann immer verfügbar, auf jedem Gerät. Entweder online oder als offline-Kopie, wenn ihr die Synchronisation einmal eingerichtet habt. Dazu braucht ihr nicht einmal teure Technik oder Zusatzsoftware, eurer PC/Notebook und Windows reichen da vollkommen aus.

Nutzen der Cloud

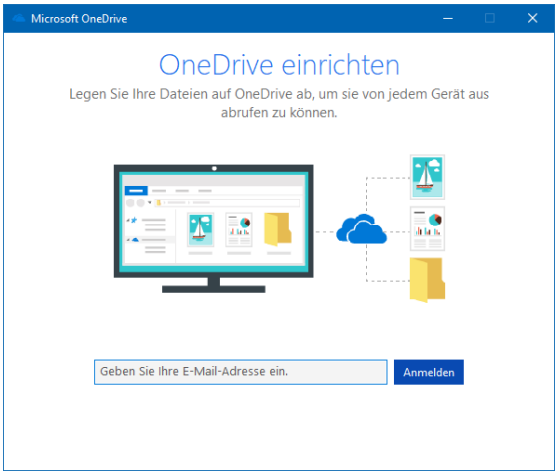
Dabei ist es am Ende egal, welchen externen Cloudspeicher ihr verwendet, das Prinzip ist dasselbe: Ihr ladet Dateien zum Dienst hoch, synchronisiert diese und gebt diese gegebenenfalls frei.

Einrichten der Synchronisation

Die Synchronisation funktioniert bei allen Cloud-Diensten gleich: Ladet die zugehörige App herunter, dann richtet einmalig die Synchronisation ein. Egal, ob es OneDrive, Dropbox, Google Drive oder die Amazon-Cloud ist:

So geht's leichter | In die Cloud – aber sicher!

- Meldet euch mit dem Konto an, zu dem das Cloud-Konto gehört: Das Microsoft-Konto für OneDrive, das Microsoft 365-Konto für Onedrive for Business, der Google- oder Dropbox-Account etc.



- Nach der Einrichtung der Synchronisation zeigt euch Windows im Explorer das Cloud-Konto als eigenen Speicherort an.

- Jeden der Ordner auf dem Cloud-Konto könnt ihr natürlich als Teil Ihrer Bibliotheken festlegen und beispielsweise den Ordner **Bilder** als Standardordner für die Bilder festlegen.

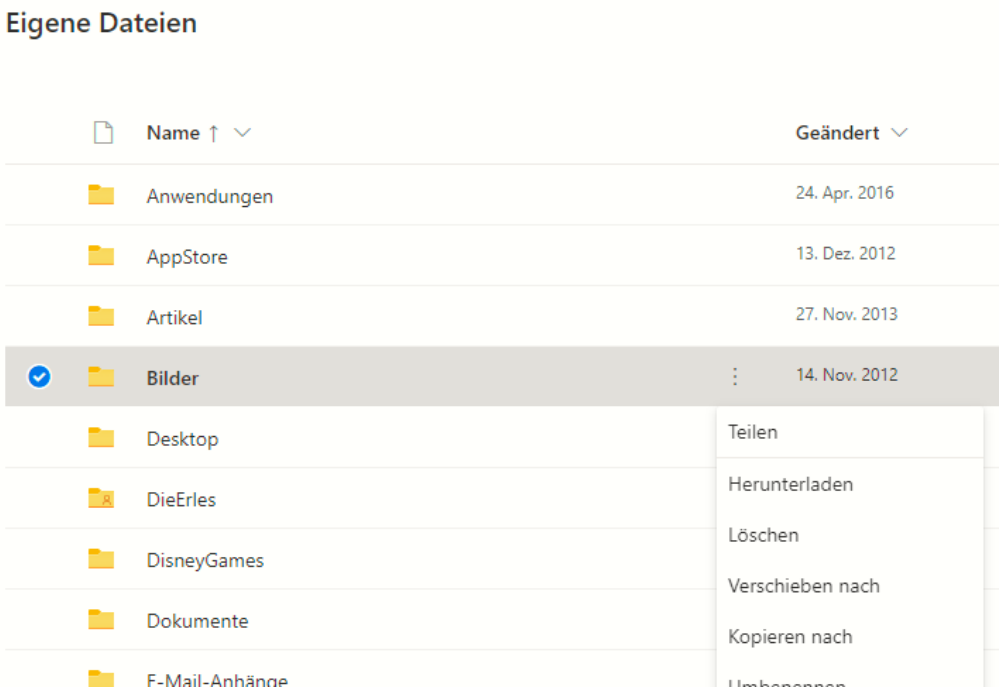
Teilen von Dateien über das Cloud-Konto

Wenn ihr eure Dateien schon im Cloud-Konto abgelegt habt, dann könnt ihr dieses auch gleich zum Teilen der Dateien nutzen. Dabei solltet ihr aber sehr genau unterscheiden, um was für Dateien es sich handelt. Während es Sinn macht, die Familie an den Urlaubserlebnissen teilhaben zu lassen, solltet ihr eure Musiksammlung oder eure Videos

So geht's leichter | In die Cloud – aber sicher!

besser nicht teilen, denn die sind in den meisten Fällen urheberrechtlich geschützt. Dasselbe gilt für vertrauliche Informationen, bei denen ihr sehr genau kontrollieren solltet, mit wem ihr sie mit welchen Rechten teilt.

- Ruft die Webseite eures Clouddienstes auf meldet euch mit euren Kontoinformationen an.
- Markiert den Ordner oder die Datei, den ihr teilen wollt, indem ihr links neben deren Namen klickt und einen Haken setzt.



- Klickt dann auf die drei Punkte rechts vom Namen und dann auf **Teilen**. Hier habt ihr noch einmal Zugriff auf den Link zur Freigabe und könnt Veränderungen an der Art der Freigabe vornehmen.

So geht's leichter | In die Cloud – aber sicher!

- Bei den eigenen Bildern beispielsweise solltet Ihr den Haken neben **Bearbeitung zulassen** entfernen, ein reiner Lesezugriff reicht vollkommen aus. Nach Eingabe der E-Mail-Adresse der Berechtigten schickt der Cloud-Dienst automatisch eine E-Mail mit dem Link an die Empfänger heraus.
- Die können dann auf eure Dateien zugreifen. Was aber, wenn ihr die Freigabe beenden wollt?
- In der Ordneransicht von Eurer Cloud-Dateien seht ihr neben jedem freigegebenen Ordner in der Spalte **Teilen** den Status **Geteilt**. Das ist ein Link, den ihr anklicken könnt.
- Der Cloud-Dienst zeigt euch jetzt an, welche Benutzer Zugriff auf diesen Ordner haben und welche Berechtigungen sie für den Ordner haben.

- Um diese zu ändern beziehungsweise den Zugriff zu entfernen, klickt auf den Pfeil nach unten bei einer Person und dann auf **Nicht mehr teilen**. Der Zugriff wird entfernt und der damals versendete Link ist nicht mehr aktiv.

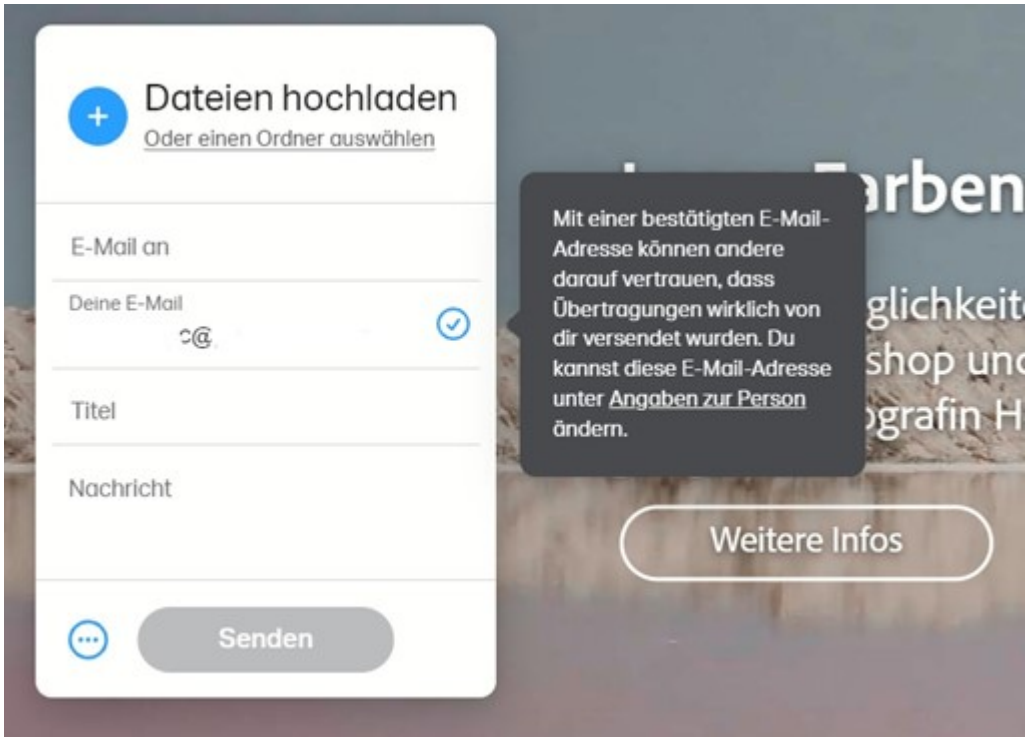
Schnell Daten austauschen: WeTransfer

OneDrive und DropBox leben davon, dass ihr möglichst alle Daten in der Cloud liegen habt. Das muss aber nicht sein: Oft wollt ihr nur eine größere Datei oder ein Verzeichnis teilen und das nach dem Abruf durch

So geht’s leichter | In die Cloud – aber sicher!

den Empfänger wieder loswerden. Das geht ohne OneDrive, Dropbox oder einen anderen permanenten Cloudspeicher! Der große Vorteil: Dateien, die nicht mehr in der Cloud sind, können auch nicht abgegriffen werden.

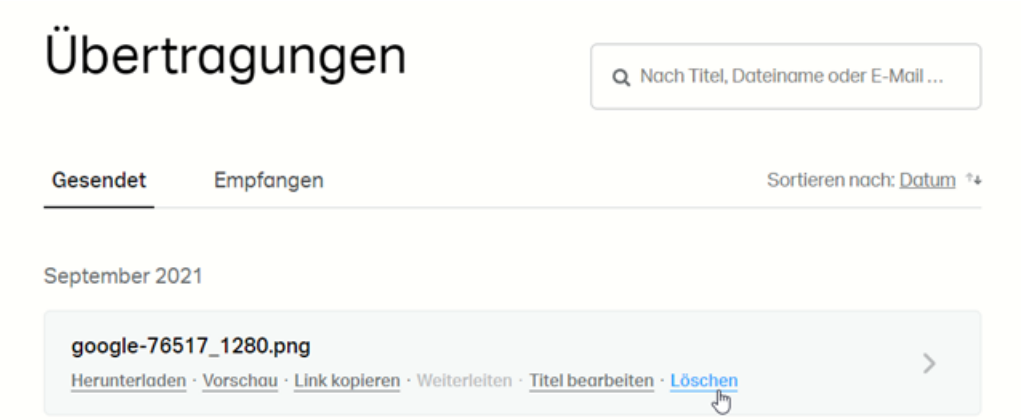
Dazu bietet sich WeTransfer an. Diesen Dienst könnt ihr kostenlos nutzen bis zu einer Transfergröße von 2GB, für die meisten Anwender vollkommen ausreichend. Mit der kostenpflichtigen Version (ab EUR 10,- pro Monat) kommen dann noch einige Funktionen und mehr Speicher hinzu.



Nach der Anmeldung könnt ihr Dateien oder einen Ordner zum Transfer anwählen, gebt dann die Empfänger und den Text der Nachricht ein. Mit dem Link können die Empfänger dann auf die Datei(en) zugreifen, solange sie da sind.

So geht's leichter | In die Cloud – aber sicher!

Mit der Pro-Version könnt ihr zusätzlich noch eine Gültigkeit festlegen. Damit könnt ihr die Freigabe automatisch beispielsweise nach einer Woche löschen lassen und müssen sich nicht selbst darum kümmern.



All eure Freigaben könnt ihr in der Übersicht eures WeTransfer-Kontos unter **Übertragungen** sehen.

Bewegt die Maus auf einen Eintrag, dann klickt auf **Löschen**, um die Freigabe – und damit auch die Dateien – zu entfernen und nicht mehr zugänglich zu machen.

Deutschland oder USA?

TeamDrive: Cloudspeicher aus Deutschland

Die Cloud ist nicht mehr wegzudenken, doch sie bereitet einigen Menschen Bauchschmerzen: Entweder haben die Dienste eine Verbindung außerhalb Europas oder sie sind nur von wenigen Geräten und Betriebssystemen nutzbar. Wenn Ihr zu diesem Nutzerkreis gehört, dann ist vielleicht TeamDrive eine Alternative.

Die gängigen Cloud-Dienste wie OneDrive, AWS, Google Drive haben alle US-amerikanischen Hintergrund. Auch wenn die Rechenzentren in Deutschland oder in der EU liegen, dürfen US-amerikanische Behörden

So geht’s leichter | In die Cloud – aber sicher!

unter bestimmten Bedingungen darauf zugreifen. Der Hintergrund ist der Cloud Act, der "Claryfying Lawful Overseas Use of Data Act". Der verpflichtet amerikanische Unternehmen, US-Behörden auf Anforderung Zugriff auf Datenbestände zu ermöglichen, auch wenn diese nicht in den USA liegen. Auch wenn sich das Mitte 2023 durch EU-Entscheidungen ein wenig entspannt hat: Wohl ist vielen Anwendern nicht dabei.

TeamDrive löst dies, indem die Datenhaltung komplett in Deutschland stattfindet und damit im Geltungsbereich der Datenschutzgrundverordnung (DSGVO) und die Daten so verschlüsselt sind, dass selbst der Anbieter diese nicht mehr lesen kann. Mit Clients für alle gängigen Betriebssysteme (Windows, macOS, Linux, Android, iOS, ...) könnt ihr eure Daten aller Geräte und über alle Verbindungen nutzen.

So geht's leichter | In die Cloud – aber sicher!

Das hat allerdings auch seinen Preis: Während zumindest die Basisversion der Pläne der gängigen Cloudanbieter kostenfrei ist, fallen bei TeamDrive nicht unerhebliche jährliche Kosten an. Los geht es bei EUR 59,50 für einen Client und 10GB Speicher, je mehr Clients zugreifen können sollen und je größer der Speicher sein soll, desto teurer wird es dann.

Mehr Schutz von Dateien in der Cloud

Nun habt ihr eure Daten in der Cloud gespeichert und verlasst euch darauf, dass die da schon sicher sein werden. Oder? Wie so oft ist die Antwort nicht so einfach: Die Anbieter setzen schon einiges daran, eure Daten vor unberechtigten Zugriffen zu schützen. Trotzdem ist jede Schutzmaßnahme potenziell umgehbar, und oft ist es ein kleiner Fehler, eine Unaufmerksamkeit von euch als Benutzer, der zu einem Datenabfluss führt. Wir zeigen euch einfache und anwendbare Maßnahmen, die dagegen helfen.

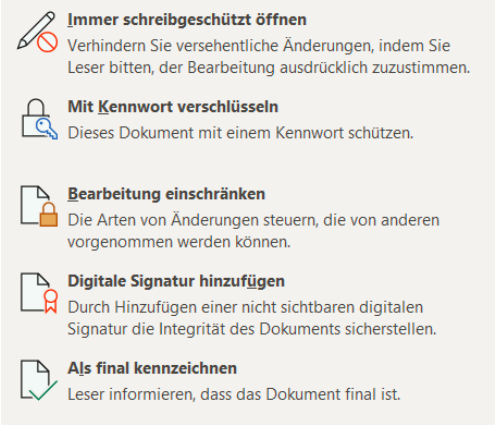
Schützen/Verschlüsseln von Dateien

Eure Dateien sind das A und O eurer Arbeit am Rechner. Ihr wollt meist nicht, dass ein Unbefugter auf diese zugreifen kann und sehen kann, womit ihr euch beschäftigt habt. Darum schützt ihr Festplatte, Cloud-Konto und Dateien durch Verschlüsselung oder Passwörter. Je höher die Hürde ist, die ein Angreifer überwinden muss, desto sicherer und geschützter sind die Informationen!

So geht's leichter | In die Cloud – aber sicher!

Passwortschutz bei Office-Dokumenten

Wie schnell eine Datei in falsche Hände gelangen kann: Dazu bedarf es nicht unbedingt eines Datenlecks, oft ist die eigene Unachtsamkeit der Grund: Ein verlorener USB-Stick, eine versehentliche an eine E-Mail angehängte Datei, und schon ist eine Datei in den falschen Händen. Dasselbe trifft natürlich auch Cloud-Dateien, die Fremden in die Hände fallen. Das macht aber noch nichts, wenn der Empfänger die Datei nicht verwenden kann, weil sie durch ein Passwort geschützt ist. Das kennt der Unberechtigte im Regelfall ja nicht.



- Office bietet die Möglichkeit des Passwortschutzes ein wenig versteckt in den Office-Apps. Klickt auf **Datei** > **Informationen** > **Dokument schützen**.
- Klickt dann auf **Mit Kennwort verschlüsseln**. Office fragt nun nach dem Kennwort für das Dokument und fordert nach der Eingabe eine zweite Eingabe zur Absicherung an.
- Nachdem ihr das Kennwort festgelegt und die Datei gespeichert habt, kann die Datei nur noch durch Eingabe dieses Kennwortes geöffnet werden. Vergesst ihr dies, dann habt ihr euch selbst aus eurem eigenen Dokument ausgeschlossen.
- Wichtig: Wenn ihr die Datei über einen Cloud-Dienst teilt, dann solltet ihr das Kennwort auf einem anderen Weg als den Freigabelink, beispielsweise per Anruf, SMS oder WhatsApp/Signal weitergeben. Damit vermeidet ihr, dass der

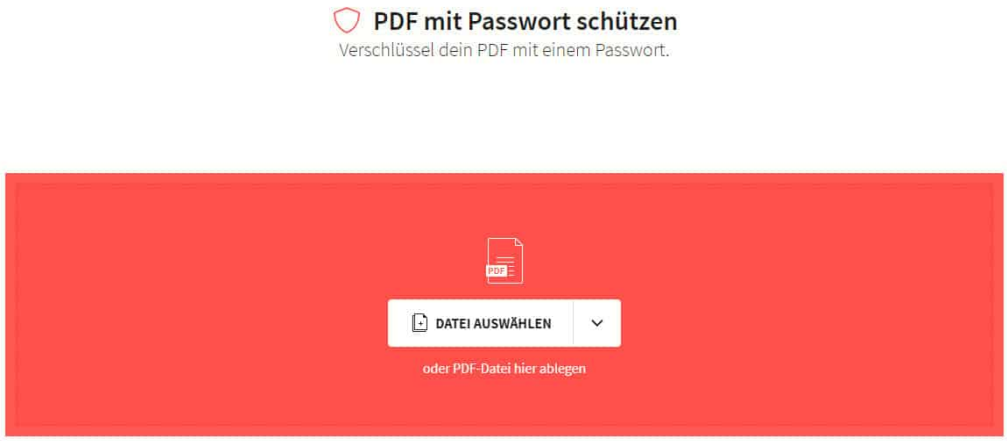
So geht’s leichter | In die Cloud – aber sicher!

Passwortschutz wirkungslos ist, weil jemand die E-Mail (und damit Datei und Kennwort) abfängt!

PDFs mit Passwort schützen

Manchmal hat auch eine PDF-Datei eine gewisse Vertraulichkeit, und ihr möchten sicherstellen, dass sie nur von einer berechtigten Person geöffnet werden kann. Die einfachste Möglichkeit ist auch hier die Vergabe eines Kennwortes, das ihr den Berechtigten zukommen lasst.

Die kostenlose Version des Acrobat Readers unterstützt die Vergabe von Kennwörtern nicht, hier müsst ihr einmal mehr ein Abonnement der kostenpflichtigen Version erwerben. Wenn es sich aber nur um einzelne Dateien handelt, dann ist der Webdienst SmallPDF eine gute Alternative. Auf den könnt ihr am Tag zwei PDF-Dateien hochladen, ein Passwort hinterlegen und dann die passwortgeschützte PDF-Datei wieder herunterladen. Der Empfänger kann diese ohne Eingabe des Kennworts nicht öffnen.

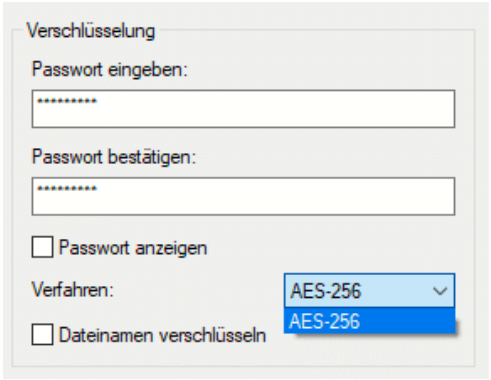


So geht's leichter | In die Cloud – aber sicher!

Verschlüsseln von Dateien in einem ZIP-Archiv

Wenn die Dateien sich nicht separat verschlüsseln lassen, dann legt sie doch einfach in eine. Passwortgeschützten Archiv in der Cloud ab. 7-Zip (https://www.7-zip.de/) ist ein gebräuchliches Archivierungsprogramm, das zudem auch noch kostenlos ist.

- Nachdem ihr es installiert habt, startet den Explorer und sucht euch die Datei(en) heraus, die ihr verschlüsseln wollt. Markiert sie, dann klickt mit der rechten Maustaste hinein. Im Kontextmenü klickt dann auf **7-Zip** > **Zu einem Archiv hinzufügen**.

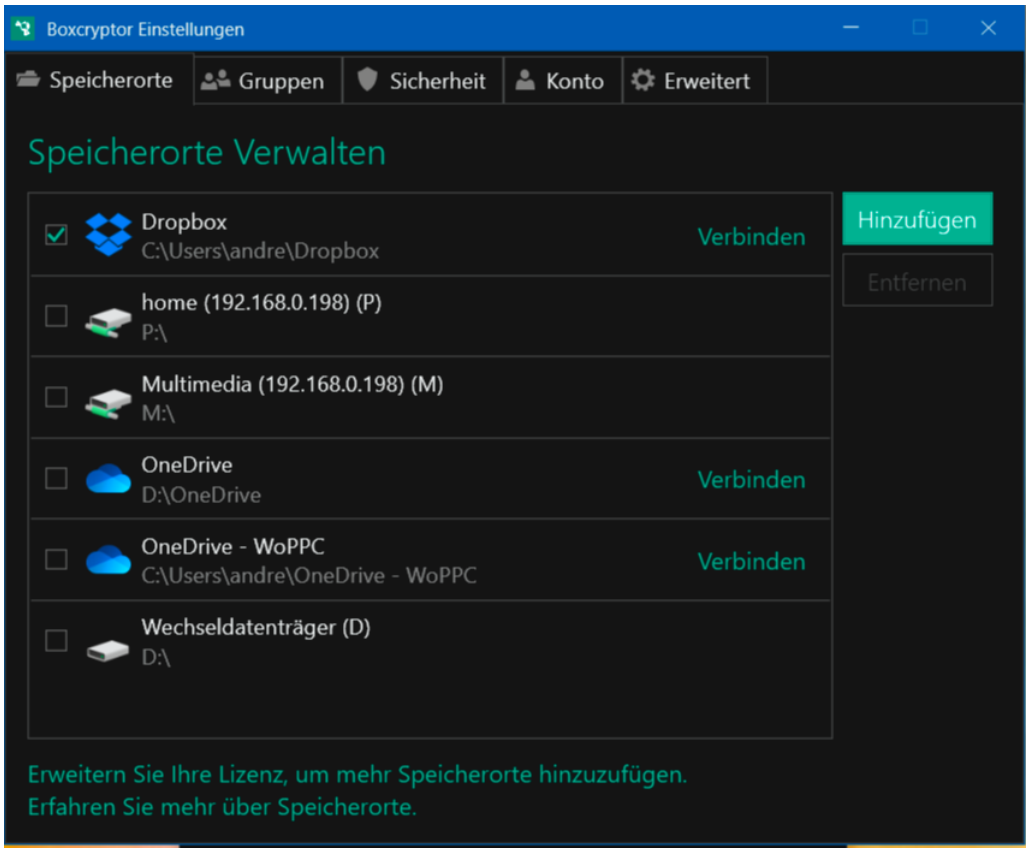


- Stellt nun den Archivtyp auf **.ZIP** ein, damit können so gut wie alle gebräuchlichen Archiv- und Kompressionsprogramme die Datei öffnen. Also auch das Windows 10/11-interne, WinZIP und WinRAR.
- Unter Verschlüsselung könnt ihr jetzt ein Passwort eingeben. Das wird dazu verwendet, um das Archiv, das dann die Dateien enthält, zu verschlüsseln. Ohne das Passwort – oder signifikante Rechenleistung, um es zu knacken – kommt niemand mehr an die Dateien heran.
- Das so verschlüsselte Archiv könnt ihr dann auf Euren Cloud-Dienst hochladen. Selbst wenn jemand an Euer Cloud-Konto kommt, ist da eine weitere Hürde vor dem Zugriff auf die Daten_ en. Der Empfänger wird beim Versuch, es zu öffnen, nach dem Passwort gefragt. Kennt er es nicht, wird das Archiv nicht geöffnet und die Dateien bleiben sicher verschlossen darin.

So geht's leichter | In die Cloud – aber sicher!

Verschlüsselung direkt in der Cloud

Natürlich sind die meisten Cloud-Anbieter alleine schon aus Eigeninteresse so weit, dass die Daten der Kunden verschlüsselt abgelegt sind. Damit habt ihr als Kunde und Nutzer nichts zu tun, und das ist genau der Punkt: Eine Eingangstür, zu der nicht nur ihr, sondern auch der Vermieter einen Schlüssel hat, ist eben doch nicht ganz sicher. So ungefähr könnt ihr die Verschlüsselung bei einem Cloud-Anbieter beschreiben: Der hat den Schlüssel und kann so theoretisch eure Daten lesen.

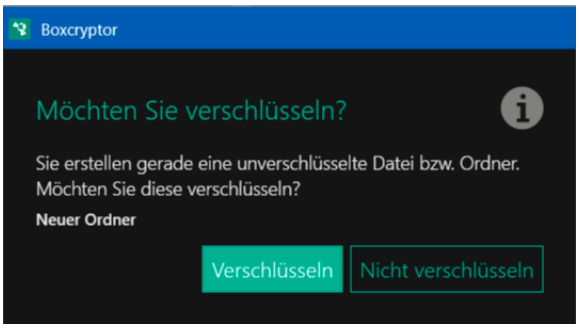


- Ein weiteres Schloss anzubringen, ist im Standard nicht möglich, da wehren sich die Anbieter vehement gegen. Aus

So geht's leichter | In die Cloud – aber sicher!

Wartungsgründen, aber auch, weil sie sich das Recht herausnehmen, das selbst zu bestimmen.

- Dafür gibt es Dienste wie BoxCryptor. Dieser ist im Standard kostenlos für einen Cloud-Anbieter und zwei Endgeräte, kostenpflichtige und leistungsfähigere Abos gibt es dann ab EUR 36,- im Jahr.
- BoxCryptor hängt sich in den Windows Explorer und lässt sich mit den gängigen Cloud-Diensten, unter anderem OneDrive und Dropbox, aber auch mit lokalen Dateisystemen verbinden.



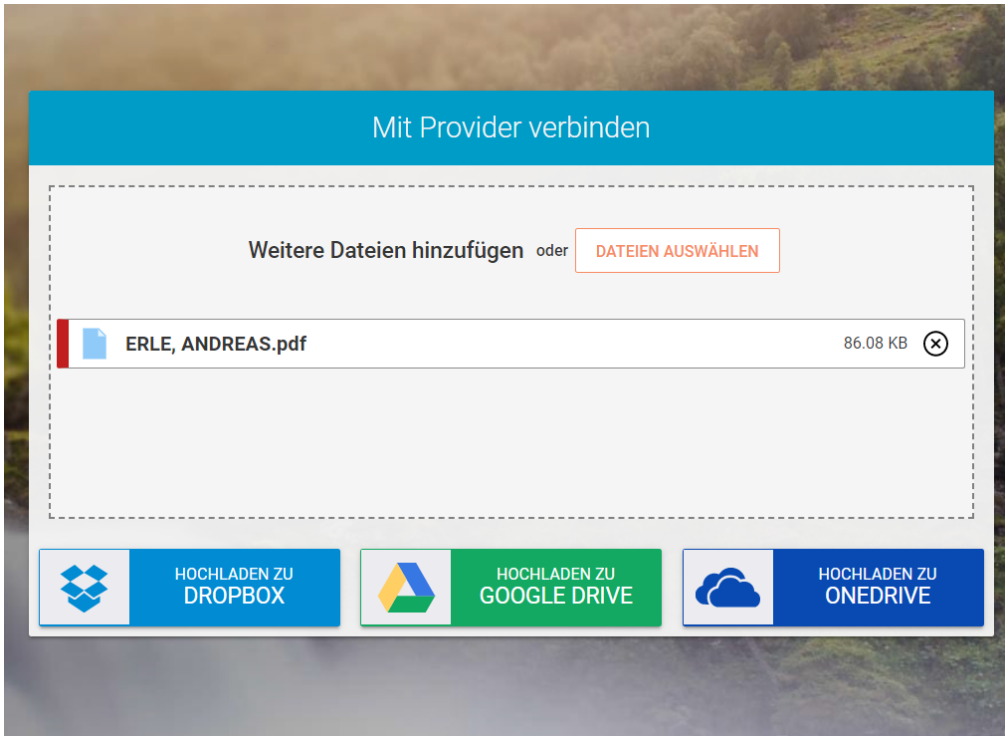
- Sobald ihr einen neuen Ordner anlegt, fragt die App, ob ihr diesen verschlüsseln wollt. Stimmt ihr dem zu, dann werden alle Dateien und Verzeichnisse, die ihr in diesem Ordner ablegt, ebenfalls verschlüsselt. Die so für Unberechtigte unleserlichen Dateien werden dann auf den Cloud-Server hochgeladen. Der Anbieter kann damit überhaupt nichts anfangen, auch ein Hacker findet nur eine zufällige Ansammlung von Bits und Bytes, nicht aber lesbare Daten und Informationen.
- Wenn ihr eine Datei öffnet, dann wird diese automatisch entschlüsselt, einen Unterschied zu einer unverschlüsselten Datei spürt ihr im Normalfall nicht.

So geht's leichter | In die Cloud – aber sicher!

Teilen von verschlüsselten Dateien

Was nutzt euch die schönste verschlüsselte Datei, wenn ihr sie weitergeben müsst und der Empfänger eure Verschlüsselungssoftware nicht einsetzt? Damit ihr euch diese Frage gar nicht stellen müsst, gibt es Whisply, mit der ihr verschlüsselte Dateien ebenfalls verschlüsselt übertragen und den Link teilen könnt.

Für die Nutzung von Whisply benötigt ihr kein Konto beim Dienst selbst, wohl aber eines bei DropBox, OneDrive oder Google Drive, denn dort wird die verschlüsselte Datei abgelegt. Zieht die Datei(en) in das Whisply-Fenster, dann klickt auf **Hochladen zu...** und wählt den Cloudservice eurer Wahl aus.

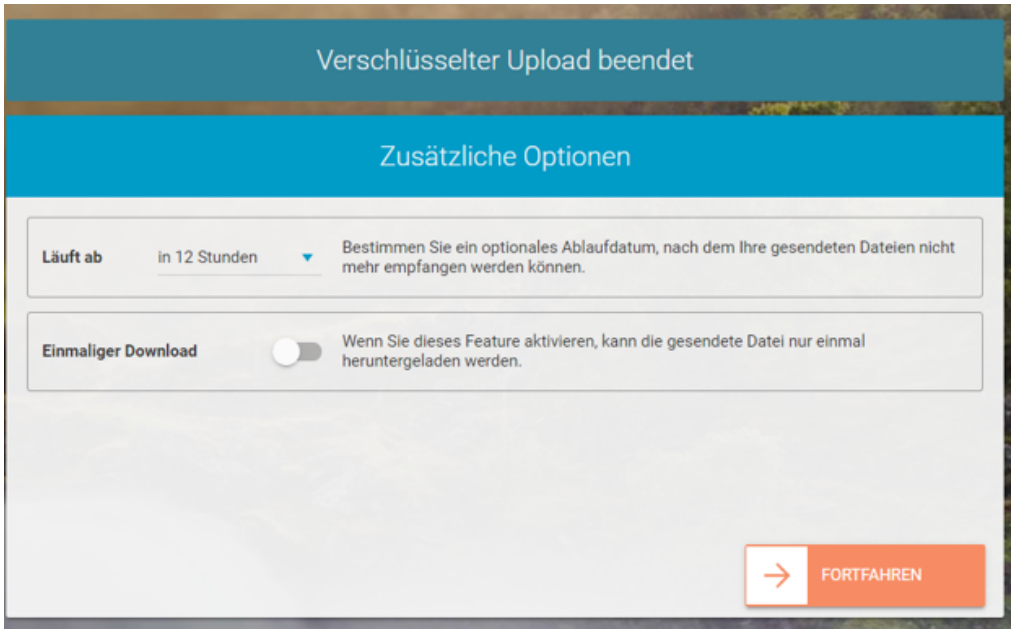


- Beim ersten Mal müsst ihr Whisply und den Cloud-Dienst miteinander verknüpfen. Folgt dazu den Anweisungen auf dem

So geht's leichter | In die Cloud – aber sicher!

Bildschirm. Whisply lädt die Datei verschlüsselt zum Cloud-Dienst hoch und erlaubt es euch, den Link einzuschränken.

- Ihr könnt beispielsweise festlegen, dass der Download nur einmal erfolgen kann und der Link dann deaktiviert wird. Zusätzlich erlaubt Whisply, die Gültigkeit zeitlich einzuschränken. Der Link läuft dann nach dem eingestellten Zeitraum automatisch ab und kann nicht mehr genutzt werden.



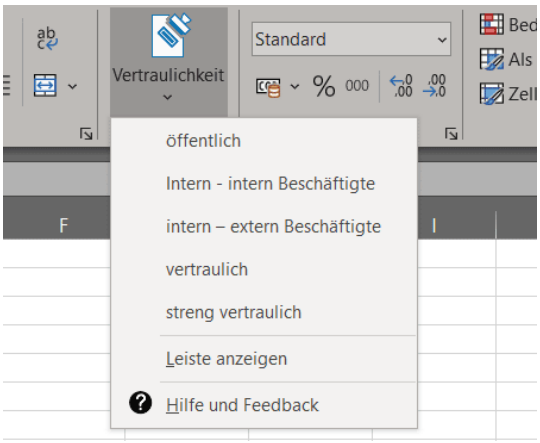
- Auf Wunsch könnt ihr den Link zusätzlich noch durch eine PIN oder ein Passwort schützen und dann an den Empfänger versenden. Auf dem gesamten Weg ist die Datei verschlüsselt.

Azure Information Protection

Wem dürft ihr ein Dokument zeigen? Oft steht das irgendwo im Dokument mit Vermerken wie "Vertraulich" oder "Öffentlich". Microsoft gibt mit der Azure Information Protection (AIP) eine Möglichkeit, das direkt im Dokument als Attribut zu verankern.

So geht's leichter | In die Cloud – aber sicher!

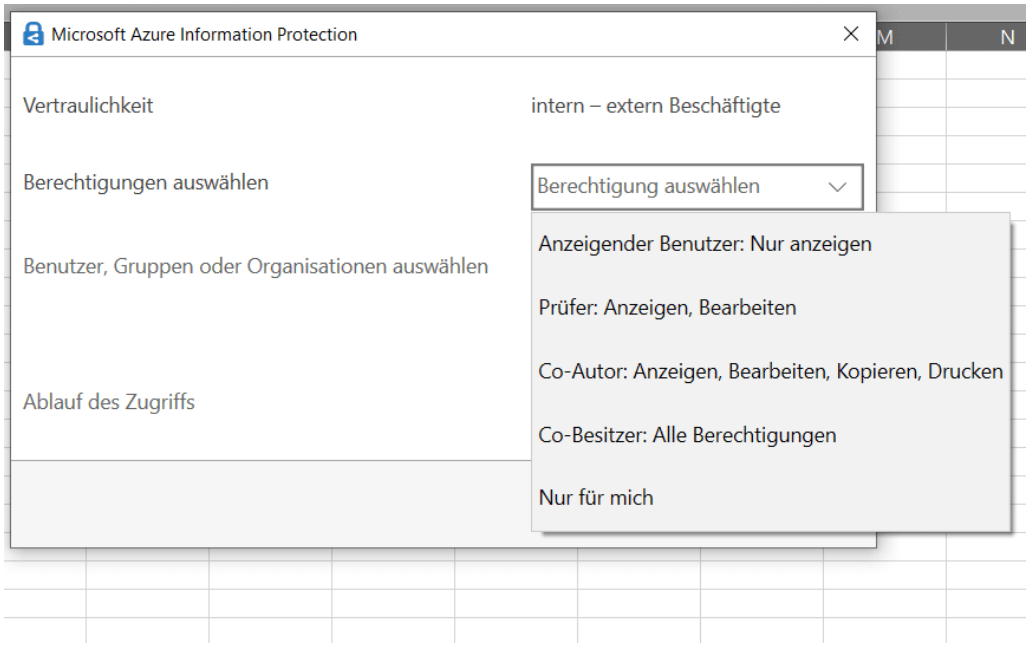
Im privaten Umfeld werdet Ihr das Problem selten vorfinden, wenn aber nur der Hauch von Vertraulichkeit in Euren Dokumenten vorhanden ist, dann ist das Euer täglich Brot: Im Verein, in der Firma, mit dem Steuerberater oder Anwalt. Da gibt es dann verschiedene Vertraulichkeitsstufen:



öffentlich: Jeder darf das Dokument lesen
intern: Nur interne Benutzer (intern im Sinne einer Firma, Kanzlei etc.)
vertraulich: Nur bestimmte, festlegbare Personen dürfen das Dokument lesen.
streng vertraulich: Nur bestimmte, vorher festgelegte Personen dürfen das Dokument lesen.

In der Azure Information Protection (die unter Microsoft 365/Azure vom Administrator installiert und aktiviert werden muss) könnt Ihr diese Klassifizierung direkt über das Symbol **Vertraulichkeit** in der Symbolleiste der E-Mail vornehmen.

So geht's leichter | In die Cloud – aber sicher!



Hier ist der **intern-Status** noch einmal unterteilt in intern und extern Beschäftigte. Das berücksichtigt, dass beispielsweise in einem Projekt sowohl der Firma zugehörige als auch von externen Firmen eingekaufte Benutzer als intern gelten können.

Wenn ihr die Funktion häufiger nutzt, dann klickt einmal im Menü auf **Leiste anzeigen**, dann wird aus dem Symbol in der Symbolleiste eine immer dargestellte Leiste mit den Informationsklassifizierungen.

Die Klassifizierung wirkt auch auf die Dateien, die ihr im OneDrive oder SharePoint in der Cloud ablegt.

Sicherheit in der Cloud

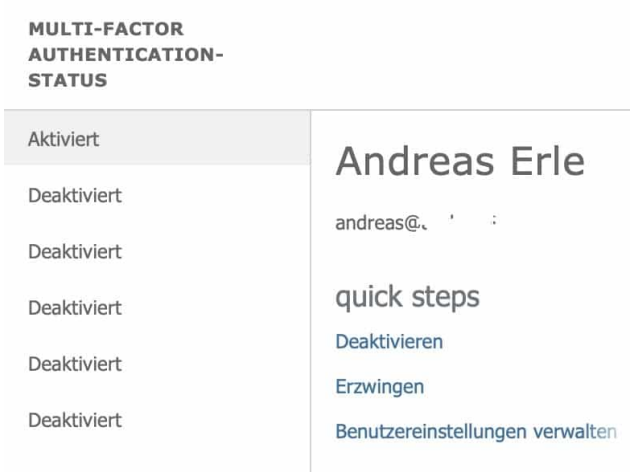
Sicherheit hat immer zwei Aspekte: Die Technik (die im Fall der Cloud größtenteils vom Anbieter übernommen wird und für die Dateien von euch sichergestellt werden kann) und dir Organisation. Wo immer der Mensch beteiligt ist, besteht ein Risiko. Ihr verliert ein Passwort, jemand

So geht's leichter | In die Cloud – aber sicher!

errät es, liest es bei der Eingabe mit, es gibt diverse Möglichkeiten. Es empfiehlt sich also, auch hierfür Vorkehrungen zu treffen.

Die Zwei-Faktor-Authentifizierung (2FA)

Der Schutz eines E-Mail-Kontos mit einem Passwort hat ein gewisses Risiko: Bringt ein Angreifer dieses in Erfahrung, dann kann er auf euer Konto zugreifen und es missbrauchen. Besser ist es, einen weiteren Faktor in die Authentifizierung mit aufzunehmen, beispielsweise eine SMS an ein Mobiltelefon.



Der Sinn dieses zweiten Faktors ist die Trennung von Wissen und Besitz. Ein Kennwort wisst ihr, wenn jemand anderes es in Erfahrung bringt, dann weiß der es auch und kann es verwenden. Wenn ihr zusätzlich einen Code per SMS bekommt und diesen als zweiten Teil der Anmeldung nutzen müssen, dann muss der Angreifer zusätzlich noch euer Handy unter Kontrolle bekommen.

2FA bei Microsoft 365/OneDrive/Sharepoint

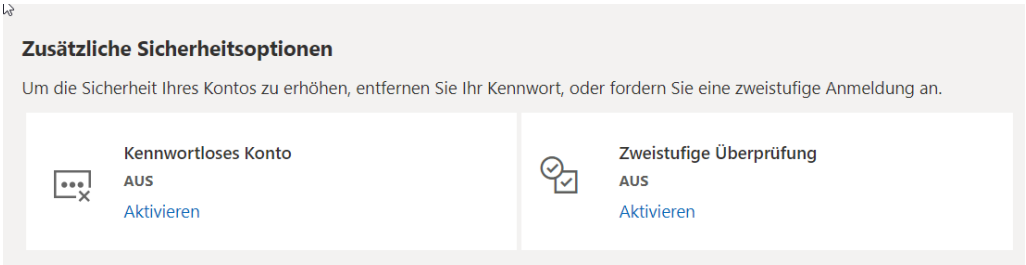
- Wenn ihr einen der Business-Pläne verwendet, dann ruft die Admin-Seite von Microsoft 365 auf, dann klickt auf **Benutzer**, setzt einen Haken bei dem Benutzer, den ihr anpassen wollt und klickt ihn an.

So geht's leichter | In die Cloud – aber sicher!

- Unten rechts klickt dann auf **Mehrstufige Authentifizierung**. Microsoft 365 öffnet den Benutzer und erlaubt unten rechts die **Mehrstufige Authentifizierung** zu aktivieren.

Wenn ihr einen Microsoft 365-Plan für Privatbenutzer verwendet, dann ist das Verfahren leicht anders:

- Geht auf die Kontoverwaltungsseite eures Microsoft-Kontos.
- Klickt in der Registerleiste oben auf der Seite auf **Sicherheit**.
- Klickt unter **Zusätzliche Sicherheitsoptionen** > **Zweistufige Überprüfung** auf **Aktivieren**.



- Folgt den Anweisungen auf dem Bildschirm.

Bei jeder Anmeldung müsst ihr nun neben dem Passwort einen Code eingeben. Diesen bekommet ihr entweder per SMS, per E-Mail oder über die Microsoft Authenticator-App.

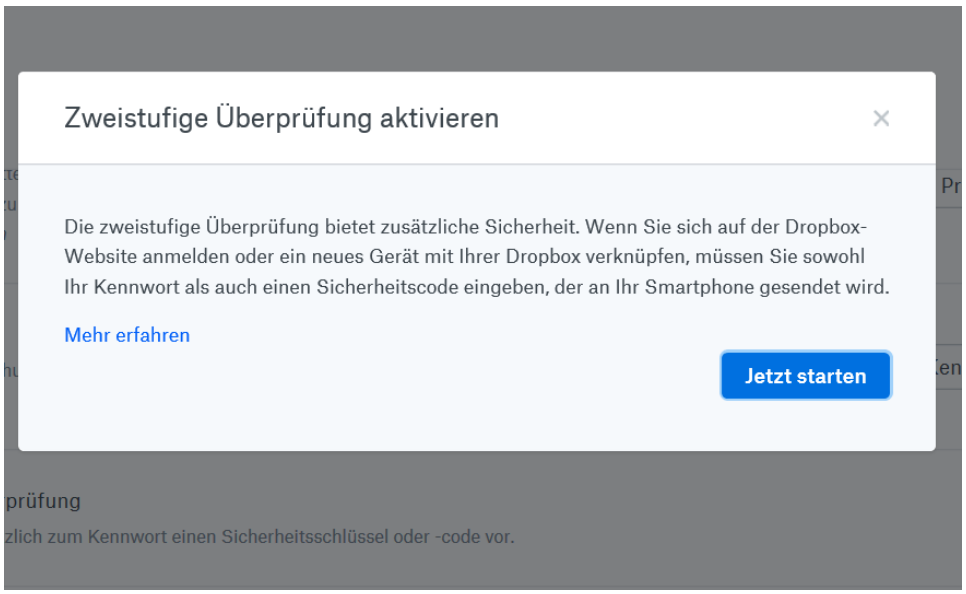
Die Verwendung der Zwei-Faktor-Authentifizierung ist natürlich kein Ersatz für die Wahl eines sinnvollen, nicht leicht zu erratenden Kennworts und dessen regelmäßigen Wechsel!

2FA bei Dropbox

Wechselt in eurem Browser auf die Sicherheits-Seite von Dropbox und meldet euch an.

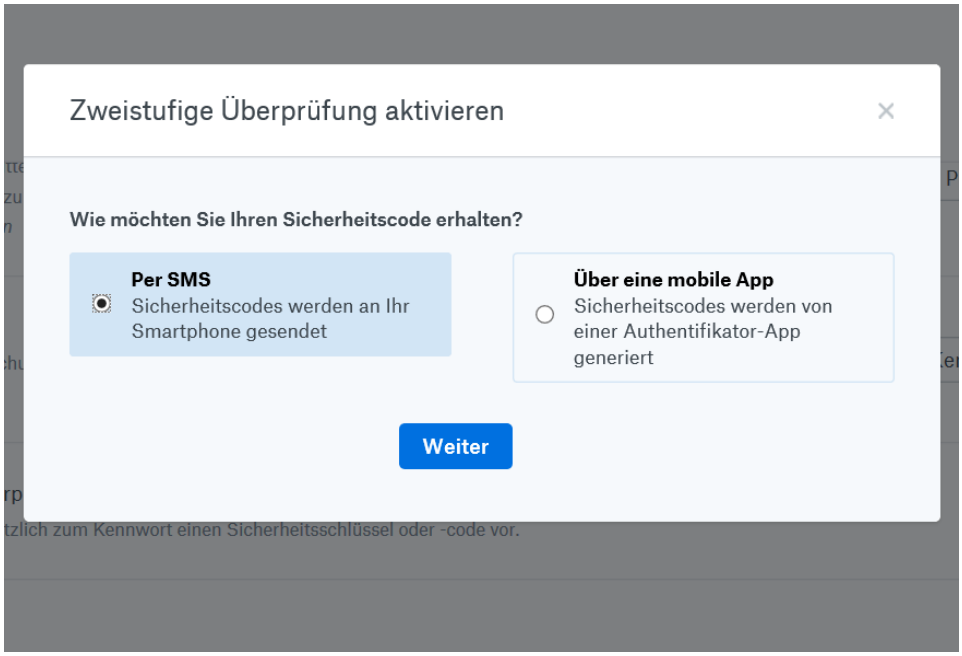
So geht’s leichter | In die Cloud – aber sicher!

- Im Reiter **Sicherheit** findet ihr in der Mitte einen Schalter, mit dem ihr die Zwei-Faktor-Authentifizierung (2FA) aktivieren könnt. Schaltet den ein.
- Dropbox fragt nun auch Sicherheitsgründen nach eurem Konto-Passwort.



- Ihr könnt nun zwischen dem Zusenden des Codes per SMS oder der Ausgabe in einer Authenticator-App wählen.
- Der Bequemlichkeit nach bietet es sich eher an, die SMS-Variante zu wählen. Bei dieser müssten sie nun einmalig die Rufnummer eingeben. Diese bleibt in Ihrem Konto gespeichert.

So geht's leichter | In die Cloud – aber sicher!



- Zur Aktivierung der 2FA schickt euch Dropbox jetzt einen sechsstelligen Code per SMS. Gebt diesen in die Eingabemaske ein.
- Bei jeder weiteren Anmeldung an die Dropbox bekommt ihr an die angegebene Handynummer wieder einen Code. Es nützt einem Angreifer also nichts mehr, wenn er nur das Kennwort hat. Ohne den bei jeder Anmeldung anderen Code ist keine Anmeldung mehr möglich. Eure Dateien sind damit deutlich sicherer.

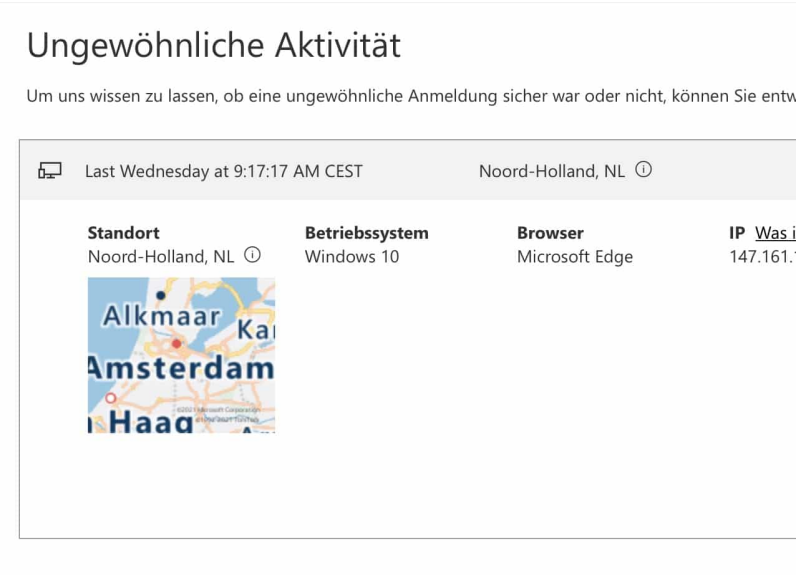
Kontrolle der Anmeldungen am Cloud-Konto

Alle Sicherheitsmaßnahmen können umgangen werden. Ob nun durch einen Zufall, ein Unglück oder durch genügend Rechenpower. Verlasst euch also nicht alleine darauf, sondern kontrolliert auch regelmäßig, was in eurem Cloud-Konto passiert. Zum Beispiel, indem ihr die Anmeldungen kontrolliert:

So geht's leichter | In die Cloud – aber sicher!

Anmeldung an Microsoft 365-Konten kontrollieren

- Meldet euch auf der Webseite https://mysignins.microsoft.com mit eurem Konto an, dann bekommt ihr eine Übersicht aller Anmeldeversuche angezeigt.
- Diese Anmeldeversuche werden automatisch mit einem Hinweis versehen, ob die Anmeldung erfolgreich war oder fehlgeschlagen ist.
- Lasst euch nicht verunsichern: Wenn statt des Wohnortes ein Ort in der Nähe angezeigt wird, dann kann das durchaus sein: Der Internetverkehr geht oft über Proxy-Server, die an zentralen Stellen stehen.



- Wo ihr drauf achten solltet sind die erfolgreichen Anmeldungen aus fremden Ländern, zum Beispiel Russland, China und Korea. Diese deuten darauf hin, dass jemand versucht, in euer Konto zu gelangen. Solange die Versuche als nicht erfolgreich gekennzeichnet sind, bleibt euch nicht viel zu tun, außer diese

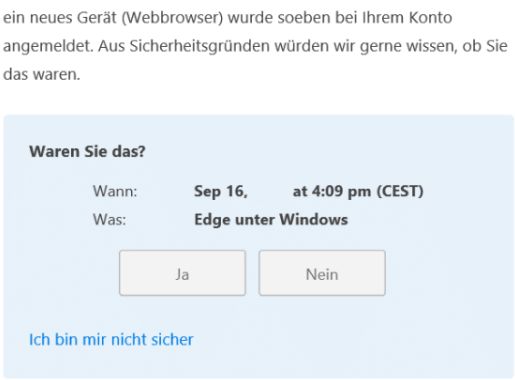
So geht's leichter | In die Cloud – aber sicher!

Kontrolle häufiger durchzuführen und gegebenenfalls die Zwei-Faktor-Authentifizierung einzuschalten.

- Ist eine solche Anmeldung erfolgreich gewesen, dann solltet ihr umgehend das Passwort ändern!

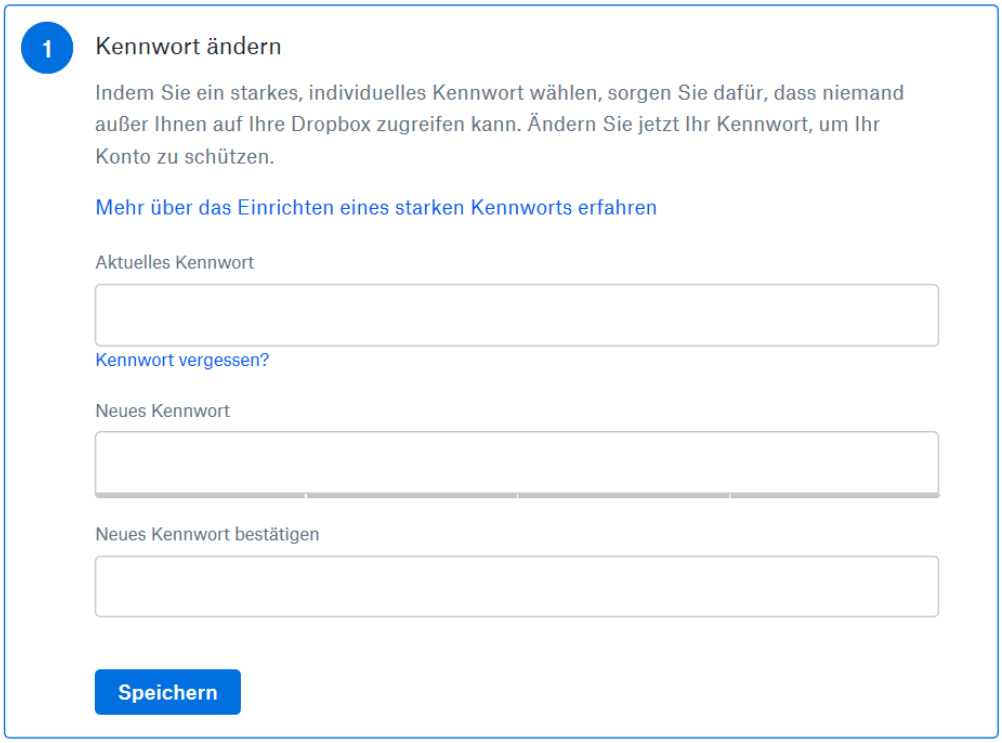
Unbekannte Dropbox-Anmeldungen erkennen

Dropbox verfolgt, welche Geräte sich an eurem Konto anmelden. Der Dienst versucht damit herauszufinden, ob jemand eure Kontoinformationen kennt und sich mit einem anderen, eigenen Gerät anmeldet. Wird ein neues Gerät erkannt, dann bekommen ihr an Ihre hinterlegte E-Mal-Adresse eine Hinweis-E-Mail:



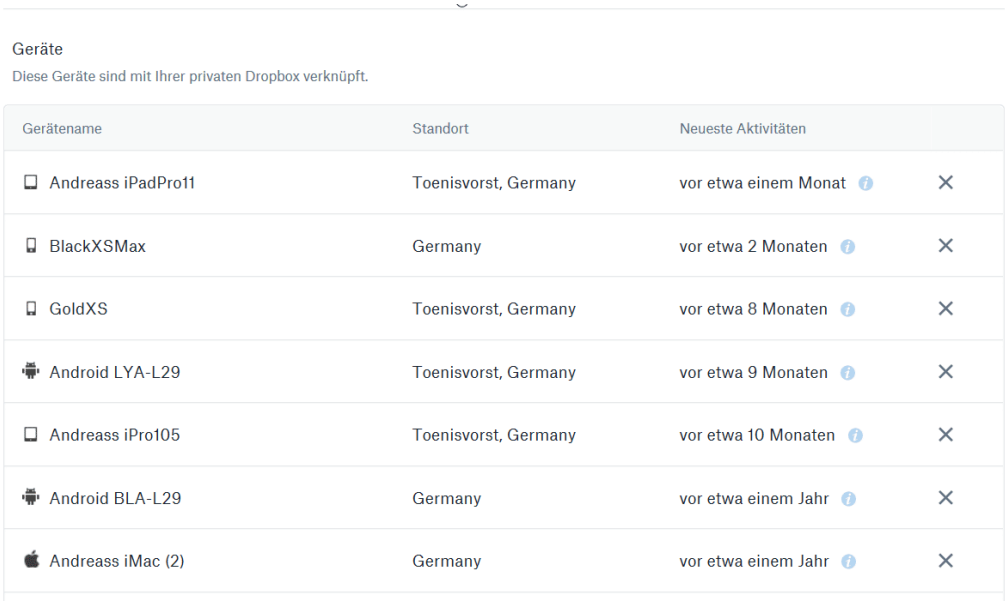
- Keine Sorge: In den allermeisten Fällen habt ihr ein neues Smartphone eingerichtet und Dropbox das erste Mal gestartet. Oder ihr habt einen PC neu aufgesetzt oder mit einem anderen Benutzernamen benutzt. Dann müsst ihr gar nichts machen, denn der Zugriff war ja euer eigener.
- Wenn ihr Dropbox aber nicht benutzt habt, dann solltet ihr schnell handeln. Klickt in der E-Mail auf **Nein**, und ihr werdet direkt auf die Sicherheitsseite von Dropbox geschickt.

So geht’s leichter | In die Cloud – aber sicher!



- Hier könnt (und solltet!) ihr vor allem umgehend euer Kennwort ändern, denn die E-Mail kommt nur bei erfolgreichen Anmeldungen. Und die sind nun mal nur möglich, wenn Benutzername und Kennwort korrekt waren.
- Ebenfalls könnt ihr Browsersitzungen wie auch Geräte, die angemeldet sind, erzwungen abmelden. Damit wird dann der unberechtigte Benutzer direkt von euren Dateien getrennt. Klicken dazu neben einem Eintrag auf das **X**.

So geht's leichter | In die Cloud – aber sicher!



Geräte

Diese Geräte sind mit Ihrer privaten Dropbox verknüpft.

Gerätename	Standort	Neueste Aktivitäten
Andreass iPadPro11	Toenisvorst, Germany	vor etwa einem Monat
BlackXSMax	Germany	vor etwa 2 Monaten
GoldXS	Toenisvorst, Germany	vor etwa 8 Monaten
Android LYA-L29	Toenisvorst, Germany	vor etwa 9 Monaten
Andreass iPro105	Toenisvorst, Germany	vor etwa 10 Monaten
Android BLA-L29	Germany	vor etwa einem Jahr
Andreass iMac (2)	Germany	vor etwa einem Jahr

Kontrolle der Freigabe von Dateien

Ihr teilt die eine Datei, dann noch eine, dann braucht jemand anderes noch eine Freigabe und am Ende habt ihr komplett den Überblick verloren.

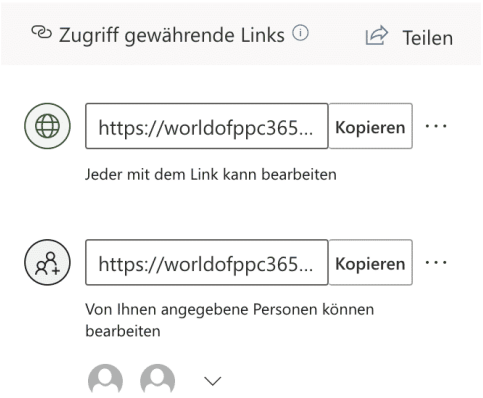
Nun sind Freigaben nicht für die Ewigkeit, und ihr wollt (und solltet!) die Berechtigungen auch wieder entfernen. Das geht aber nur, wenn ihr auch wisst, welche Dateien und Ordner freigegeben sind.

Anzeigen/Ändern von Freigaben in OneDrive

Ein Projekt ist zu Ende, ein Mitarbeitender scheidet aus, ein Bearbeiter der Datei soll ausgetauscht werden. Dann soll auch der Zugriff auf die Dateien möglichst schnell widerrufen oder angepasst werden. Diese Funktion versteckt sich leider ein wenig in den Dialogen.

So geht's leichter | In die Cloud – aber sicher!

- Meldet euch über den Webbrowser an eurem Microsoft- (oder Microsoft 365-) Konto an.
- Klickt auf den Punktwürfel oben links, dann auf **OneDrive**.
- Sucht den freigegebenen Ordner heraus und klickt dann auf die **drei Punkte** rechts von dessen Namen und auf **Details**.



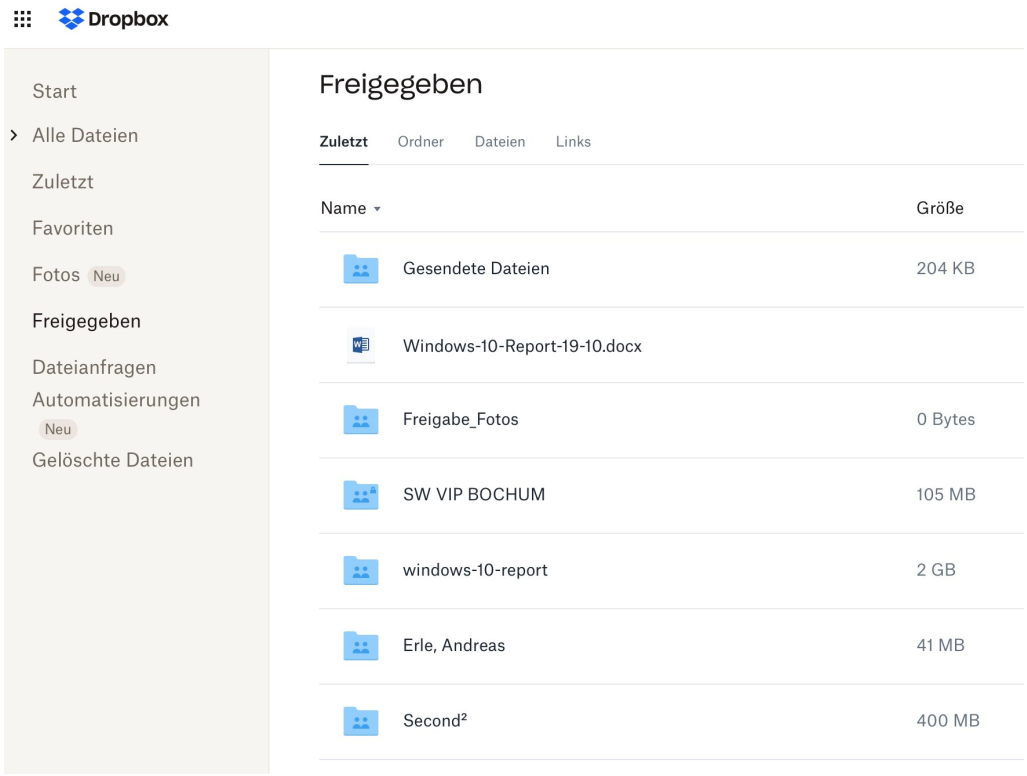
- Rechts im OneDrive-Fenster seht ihr nun die Freigaben. Klickt auf **Zugriff verwalten**. OneDrive zeigt alle Freigaben an.
- Klickt auf die drei Punkte neben einer Freigabe, dann seht ihr alle Benutzer, die diese nutzen können. Ein Klick auf das Kreuz neben einem Benutzer löscht dessen Zugriffsrechte. Ihr könnt an dieser Stelle auch neue Benutzer hinzufügen oder die Berechtigungen zum Ändern von Inhalten anpassen.

Übersicht über DropBox-Freigaben

Auch auf einer Dropbox sammeln sich mit der Zeit unzählige freigegebene Dateien. Da hilft es, dass auch hier eine Möglichkeit des

So geht's leichter | In die Cloud – aber sicher!

Überblicks über Freigaben gibt:



- Meldet euch an eurer DropBox im Webclient an.
- Klickt dann in der Übersicht auf der linken Seite auf **Freigegeben**.
- Im Detailfenster zeigt Dropbox jetzt verschiedene Möglichkeiten an: **Zuletzt** sortiert die vorhandenen Freigaben nach dem Zeitpunkt des Zeitpunkts der Freigabe, die jüngsten sind oben. **Ordner** zeigt nur freigegebene Ordner an, **Dateien** nur einzeln freigegebene Dateien.
- Klickt auf die drei Punkte rechts neben dem Namen des freigegebenen Objekts, dann auf **Teilen**.

So geht's leichter | In die Cloud – aber sicher!

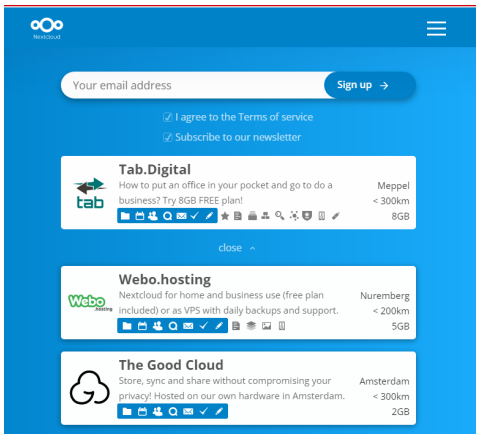
- Oben rechts findet Ihr ein **Zahnrad**-Symbol. Klickt darauf und dann auf **Freigabe beenden**, um die Freigabe zu entfernen und die Datei wieder nur noch lokal verfügbar zu machen.

Einrichten einer eigenen Cloud-Lösung

Ihr vertraut keinen Fremdanbietern, wollt aber trotzdem eure Daten auch von unterwegs verfügbar haben? Dann richtet euch doch einfach eure eigene Cloud ein. Klingt kompliziert? Ist es nicht. Wir zeigen euch, wie Ihr das per Nextcloud über einen Dienstleister oder mittels einer Netzwerkfestplatte ganz allein machen könnt.

Nextcloud – der andere Cloud-Anbieter

Zwei Argumente werden immer wieder gegen eine Cloudlösung ins Feld geführt: Zum einen die Tatsache, dass eure Daten irgendwo auf der Welt liegen. Zum anderen die vollkommene Anhängigkeit von einem Stück Software, das Schwächen, Hintertüren und Fehler haben kann, die aber niemand beurteilen kann. Der Quellcode wird von Anbietern wie Microsoft, Google, DropBox und anderen nicht freigegeben.

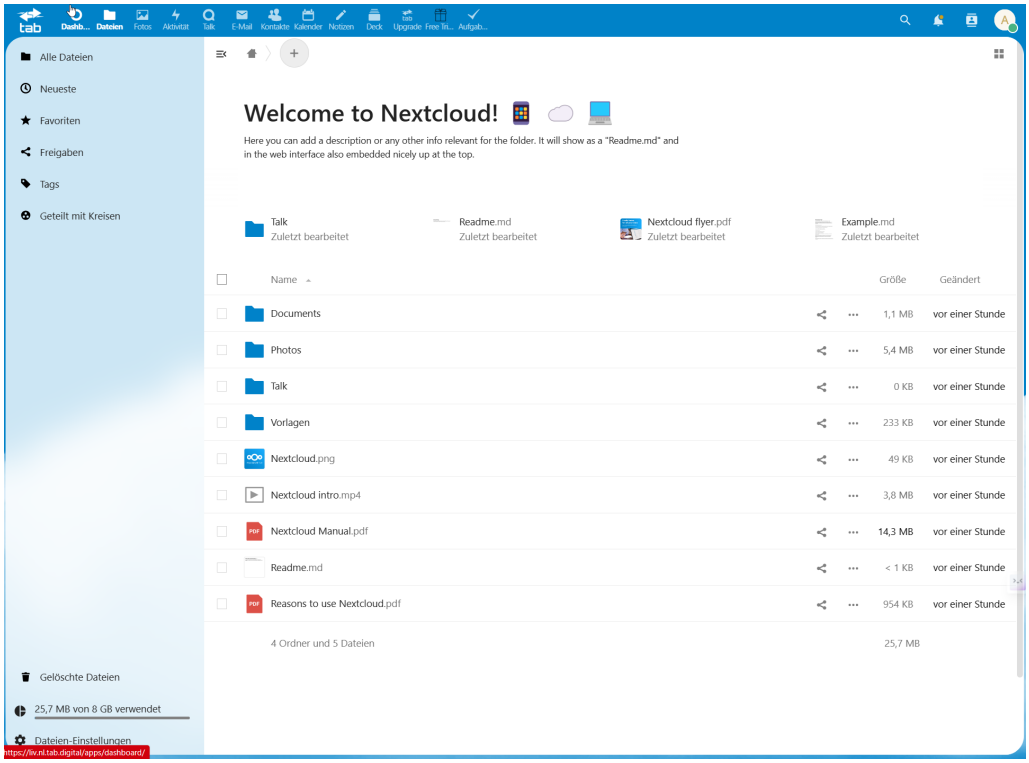


Diese beiden Punkte geht Nextcloud als Anbieter an:

So geht’s leichter | In die Cloud – aber sicher!

Auch als Privatanwender könnt ihr euch kostenlos eine eigene Cloud anlegen. Die liegt dann bei einem vertrauenswürdigen Anbieter liegen (der von Nextcloud entsprechend geprüft wurde).

Weitere Alternativen sind die Installation auf eigener Hardware, die Installation auf einem dedizierten Server bei Nextcloud oder eine gehostete Nextcloud-Lösung bei einem Hoster wie Ionos, Telekom und anderen. Diese Pakete sind kostenpflichtig.



Der Vorteil: Ihr teilt Euch die Cloud nicht mit anderen Anwendern, sondern habt eure eigene, kleine Cloudblase. Natürlich in der kostenlosen Version auf Servern mit ganz vielen anderen Installationen, aber schon privater als auf einem OneDrive, Google Drive oder einer Dropbox. Je höherwertig das Nextcloud-Paket ist, desto besser wird das: In der maximalen Ausbaustufe mit eigener Hardware seid Ihr komplett autark

So geht's leichter | In die Cloud – aber sicher!

Was Nextcloud besonders macht: Der Source-Code ist komplett öffentlich einsehbar.

Der Vorteil: Wer will und kann, der kann ganz genau nachvollziehen, dass sich keine Hintertürchen oder ungewollte Funktionen eingebaut sind. Deutlich mehr Sicherheit als bei einem der großen Anbieter, die sich überhaupt nicht in die Karten schauen lassen.

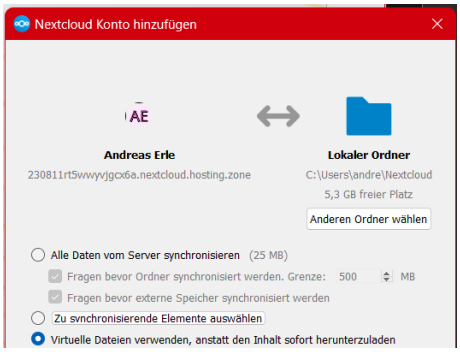
Die Installation von Nextcloud

Die Krux bei der Installation der kostenlosen Nextcloud-Version: Diese wird nicht von Nextcloud selbst angeboten, sondern von externen Anbietern. Damit habt Ihr keinen direkten Nextcloud-Account, sondern einen beim entsprechenden Anbieter. Die Anmeldung an den offiziellen Nextcloud-Apps erfolgt dann über den Umweg des Servernamens. Den allerdings findet ihr bei manchen Anbietern vergeblich. Ein Anbieter, bei dem das auch in der kostenlosen Variante prima funktioniert, ist hosting.de.

- Meldet euch hier für die kostenlose gehostete Nextcloud-Version an.
- Im Zuge des Anmeldeprozesses legt Ihr Euren Benutzernamen und euer Passwort fest. Das gilt dann für alle Nextcloud-Apps auf PC, Mac und Smartphone. Direkt anmelden könnt ihr euch damit aber nicht.
- Meldet euch jetzt am hosting.de-Portal mit den oben vergebenen Benutzerdaten an.
- Die wichtigste Information für das weitere Vorgehen findet ihr, wenn ihr in der Navigationsleiste links auf **Managed Nextcloud** klickt.

So geht’s leichter | In die Cloud – aber sicher!

- Unter **Ihre Serveradresse** findet ihr die Serveradresse eurer Installation, die ihr gleich bei der Installation einer jeder Nextcloud App findet. Kopiert die in die Zwischenablage.
- Passenderweise findet ihr im Dashboard unter **Wie greife ich auf Nextcloud zu** direkt einen Bereich, in dem ihr Links zu allen wichtigen Apps für Desktops, Tablets und Smartphone findet. Ladet die entsprechende Version herunter und installiert sie.
- Nach dem Start der Anwendung klickt auf **Anmelden**. Hier müsst ihr nun als Erstes die oben kopierte Serveradresse eintragen. Die App leitet euch nun im Browser eures Gerätes auf die Anmeldeseite des Hosters um.



- Der fragt gegebenenfalls nochmal seine eigenen Anmeldedaten ab, dann klickt auf **Anmelden**.
- Im nächsten Schritt müsst ihr bei den PC- und Mac-Versionen festlegen, welches Verzeichnis ihr mit der Cloud verbinden wollt. Im Standard ist das ein leeres Verzeichnis, ihr könnt aber natürlich auch ein schon vorhandenes nehmen.
- Wenn Ihr genug Platz auf der Festplatte habt, dann klickt **Alle Daten vom Server synchronisieren** an. Sonst könnt ihr auch

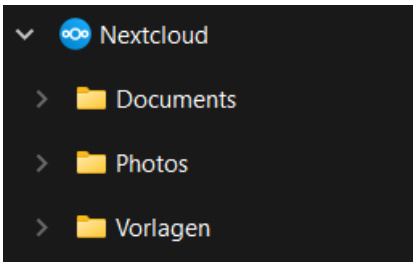
So geht's leichter | In die Cloud – aber sicher!

virtuelle Dateien verwenden, das sind kleine Platzhalter, die wenig Speicher belegen. Erst wenn ihr die Datei öffnet, wird dann aus der Cloud die echte Datei geladen.

- Klickt auf **Verbinden**, um die Verbindung herzustellen.

Nutzung von Nextcloud

Wenn ihr dann Nextcloud nutzen wollt, dann merkt ihr keinen Unterschied mehr zu einem „normalen" Cloud-Dienst.



- Im Windows Explorer findet ihr einen zusätzlichen Speicherort **Nextcloud**.
- Klappt diesen auf, dann seht ihr die Ordner, die in der Cloud vorhanden sind.
- Da der Client eine echte Synchronisation durchführt, wird jede Änderung in der Cloud sofort auf allen euren Rechnern und Smartphones gespiegelt. Genauso natürlich jede neue oder geänderte Datei bzw. Verzeichnis von eurem Gerät in die Cloud.

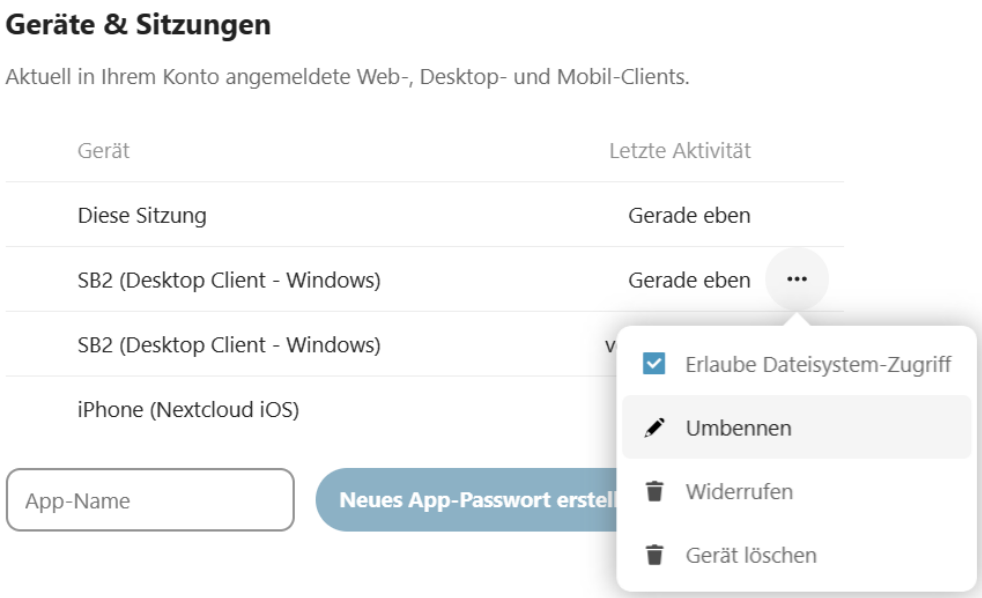
Sicherheit bei Nextcloud

Jede Cloudlösung solltet ihr regelmäßig kontrollieren, ob Zugriffe stattfinden, die nicht zulässig sind. Da könnt Ihr bei Nextcloud über das Webfrontend machen:

- Meldet euch jetzt am hosting.de-Portal mit den oben vergebenen Benutzerdaten an.
- Klickt in der Navigationsleiste links auf **Managed Nextcloud** und schaut dann unter **Geräte & Sitzungen**.

So geht's leichter | In die Cloud – aber sicher!

- Hier findet ihr die Geräte, die den Anmeldeprozess erfolgreich durchlaufen haben unter **Gerät** und die letzte Anmeldung unter **Letzte Aktivität**.
- Wenn ihr dort ein Gerät findet, dass nicht als eures zu identifizieren ist, dann klickt auf die drei Punkte rechts von dessen Eintrag und auf **Widerrufen** (um den Zugang aufzuheben) oder auf **Löschen**, um die Daten remote von diesem Gerät zu löschen.



Ein Netzwerklaufwerk als eigene Cloud

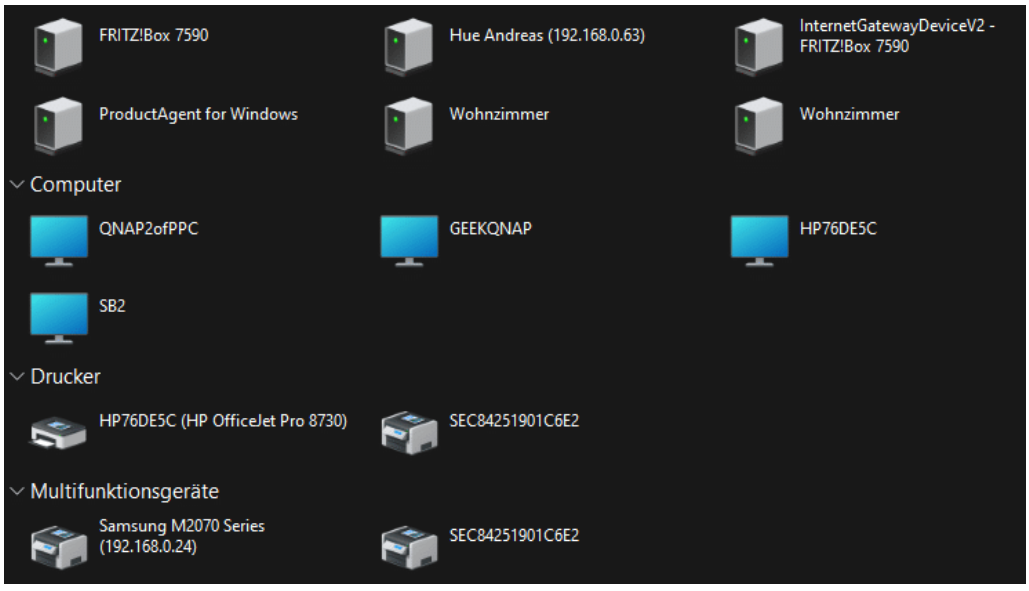
Der erste Schritt eures Wegs in die eigene Cloud ist die Vorbereitung eines Laufwerks, das im Netzwerk immer verfügbar ist: Für alle Geräte, die intern darauf zugreifen wollen, aber eben auch von außen.

So geht's leichter | In die Cloud – aber sicher!

Netzwerkspeicher: Was ist das?

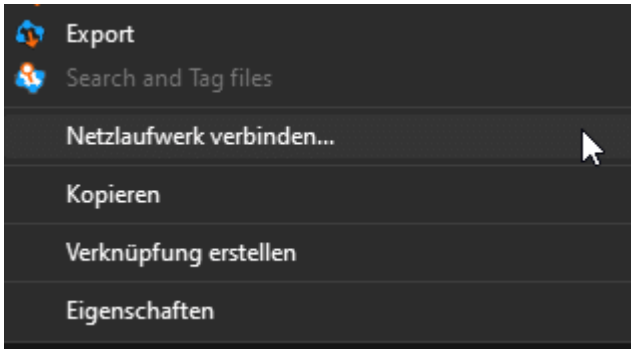
Es ist schon lange nicht mehr so, dass ihr nur auf einem Gerät arbeitet. Desktop und Tablet, diverse Netzwerkgeräte wie ein NAS (Network Attached Storage, also eine Netzwerkfestplatte), euer Router, der einen USB- oder sogar SD-Karten-Slot hat und andere Geräte speichern Daten. Statt nun zwischen diesen Gerten hin- und herzulaufen und Daten zu übertragen, wird die Netzwerkverbindung dazu verwendet. Wenn Ihr der Meinung sei, dass das bei euch ja nicht der Fall ist, dann

- Startet den Windows Explorer.
- Klickt im Verzeichnisbaum auf der linken Seite auf **Netzwerk**.
- In der Liste seht Ihr alle Geräte, die Ihr über das Netzwerk ansprechen könnt.



- Zu den Geräten gehören natürlich auch Drucker, Netzwerklautsprecher und vieles andere, die Kategorie **Computer** aber zeigt euch alle klassischen Geräte mit Speicher.

So geht's leichter | In die Cloud – aber sicher!



Hinzufügen eines Netzwerklaufwerks

Grundsätzlich könnt ihr durch einen Doppelklick auf ein Gerät in dieser Übersicht dessen freigegebenen Laufwerke öffnen und dann darauf zugreifen, einfacher und komfortabler ist es aber, wenn ihr die direkt als eigenes Laufwerk im Explorer zur Verfügung habt. Das ist mit wenig Aufwand machbar:

- Öffnet das Netzlaufwerk aus der Netzwerkumgebung, wie oben beschrieben.
- Klickt mit der rechten Maustaste hinein, dann unten im sich öffnenden Menü auf **Netzlaufwerk verbinden**.
- Im sich öffnenden Fenster müsst ihr nun einige Rahmendaten festlegen.
- Unter **Laufwerk** wählt ihr den Laufwerksbuchstaben, unter dem das Netzlaufwerk in Windows verfügbar sein soll. Windows zeigt euch nur freie Buchstaben an (dazu gehört zum Beispiel nicht C:, der ja schon für die Systemfestplatte belegt ist).
- Der **Ordner** ist die Netzwerkadresse, die Windows erkennt. Die setzt sich immer zusammen aus dem Gerät, in dem die Netzwerkfestplatte eingebaut ist und dem Namen der Freigabe.

So geht's leichter | In die Cloud – aber sicher!

Sie ist in der Form \\<*Server*>\<*Freigabe*>. Hier müsst ihr nichts ändern.

- Wenn die Anmeldung ohne Benutzername und Passwort oder mit euren Windows-Anmeldedaten stattfindet, dann müsst ihr nichts machen. Wenn ihr separate Anmeldedaten habt, dann klickt auf **Verbindung mit anderen Anmeldeinformationen herstellen**. Windows fragt diese Informationen ab, und ihr könnt entscheiden, ob diese gespeichert werden sollen oder nicht.
- Wenn ihr das neue Laufwerk immer verfügbar haben wollt, wenn Windows startet, dann setzt einen Haken bei **Verbindung bei der Anmeldung wiederherstellen**.

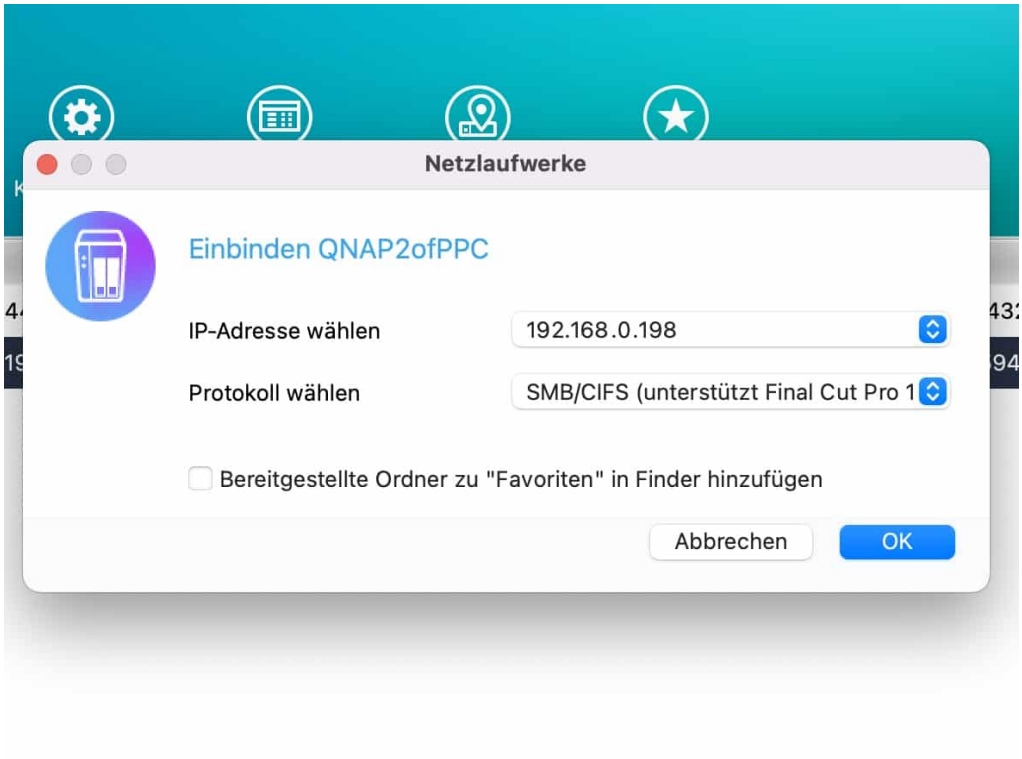
Netzlaufwerke vom NAS einbinden

Network Attached Storage (NAS) übernehmen immer mehr die Rolle einer externen Festplatte für die Speicherung von großen Datenmengen und Datensicherungen. Die Bedienung lässt sich über die eigene Weboberfläche vornehmen, auch über Windows-interne Mechanismen könnt ihr mit ein wenig Aufwand den Zugang regeln. Optimale Voraussetzungen also, damit eure eigene Cloud zu bauen. Die folgende Beschreibung orientiert sich an QNAP-NAS, für Geräte von Synology oder WD funktioniert das Ganze aber ähnlich.

- QNAP bietet mit dem Qfinder ein kostenloses Tool an, mit dem ihr unter Windows wie auch unter macOS mit wenigen Klicks jede Freigabe des NAS auf dem ausführenden Rechner verfügbar machen könnt.
- Nach der Installation startet den Qfinder. Die App durchsucht die Netzwerkumgebung und zeigt euch in einer Liste alle QNAP-NAS an, die im Netzwerk aktiv sind.

So geht's leichter | In die Cloud – aber sicher!

- Klickt das gewünschte NAS einmal mit der Maus an, dann auf **Netzlaufwerk verbinden** und auf **OK**.



- Nun müsst ihr euch mit eurem Benutzerkonto anmelden. Das NAS listet nun alle Freigaben auf, die ihr mit euren Berechtigungen verwenden könnt. Durch einen Doppelklick stellt es die Verbindung zur Freigabe her und ihr könnt diese im Explorer/Finder wie ein normales lokales Laufwerk verwenden.

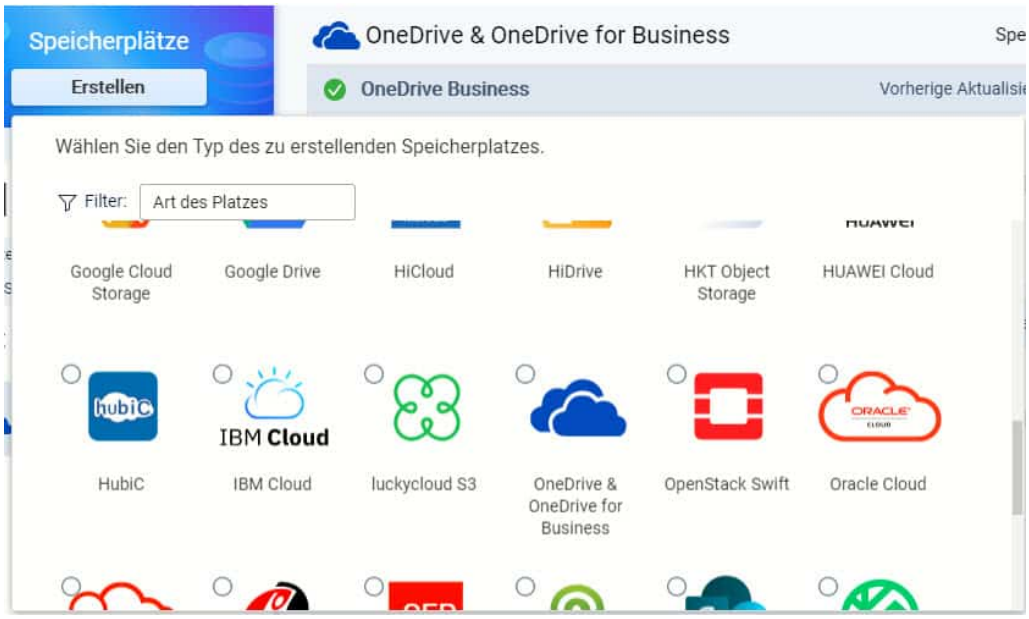
OneDrive/Dropbox mit einem NAS synchronisieren

Ihr müsst jetzt stark sein: Auf den ersten Blick beschreiben wir einen Widerspruch: Das Sichern von Dateien aus dem OneDrive auf eine Netzwerkfestplatte. Tatsächlich aber gibt es viele Anwender, die das OneDrive nicht mit dem PC synchronisieren wollen, aber trotzdem ein

So geht's leichter | In die Cloud – aber sicher!

Backup wünschen. Und wenn Ihr vom OneDrive in eure eigene Cloud wollt, dann ist das der erste Schritt.

- Die für die meisten Betriebssysteme erhältlichen Apps bieten die Synchronisation mit PC und Mac an. Diese ist live und hält beide Seiten auf dem aktuellen Stand. Um eine Sicherheitskopie, die einen gewissen zeitlichen Versatz hat, zu behalten, könnt ihr euer NAS nutzen. Dessen Synchronisations-App unterstützt OneDrive und andere gängige Cloud-Dienste in den meisten Fällen direkt.



- Wenn ihr das noch nicht getan habt, installiert die App **Hybrid Backup Sync** aus dem QNAP Store (oder die entsprechende Sync-App eures NAS-Anbieters) auf dem NAS.
- Klickt jetzt auf **Speicherplätze** > **Erstellen** und wählt in der Liste **OneDrive & OneDrive for Business** (oder den entsprechenden Cloud-Dienst) aus. Die App öffnet dessen Anmeldeseite und lässt euch einmal anmelden.

So geht's leichter | In die Cloud – aber sicher!

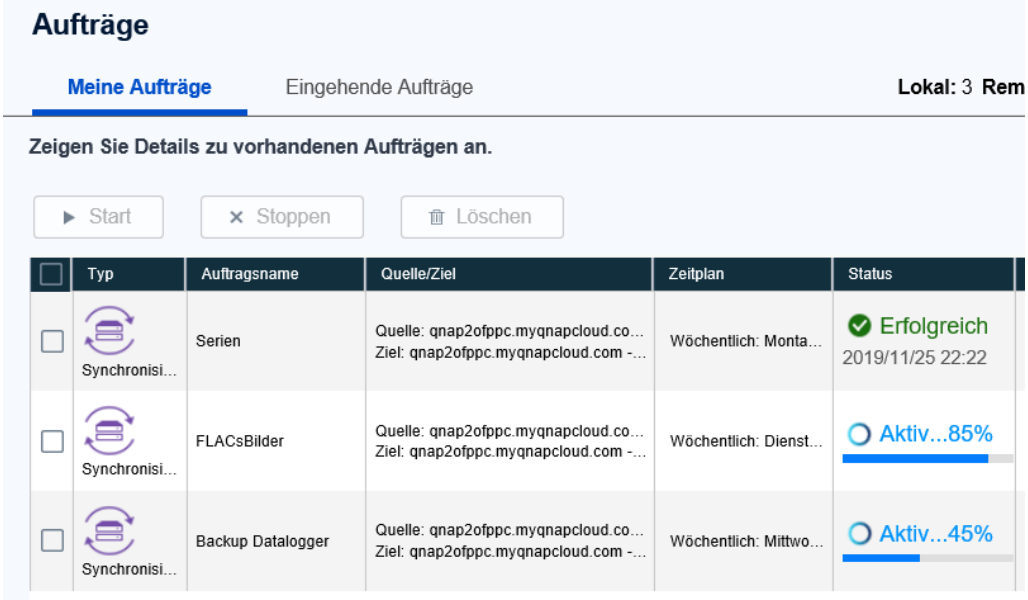
- Nachdem das erfolgt ist, könnt ihr einen neuen Synchronisationsauftrag anlegen, der das OneDrive als Quelllaufwerk hat. Lasst diesen alle zwei Wochen laufen, dann habt ihr eine Sicherung, die live vorgenommene Änderungen für bis zu zwei Wochen rückgängig machen lässt!
- Wenn es nur um das einmalige Übertragen der Daten aus der externen Cloud geht, dann lasst diesen Job nur einmal laufen.

Automatische Synchronisationsjobs auf Netzwerkfestplatten

Im Normalfall wollt ihr nicht die ganze Zeit auf der Netzwerkfestplatte arbeiten, sondern auf dem lokalen Gerät. Dann macht es Sinn, die Daten regelmäßig auf das NAS zu sichern. Das könnt Ihr auf der einen Seite über das Anbinden des Netzwerklaufwerkes des NAS in Windows und eine dort eingesetzte Syncsoftware wie GoodSync machen, oder direkt am NAS. Dazu müsst ihr vorher das lokale Laufwerk im Netzwerk freigeben.

- Auch hier ist wieder die Syncsoftware des NAS der Ausgangspunkt: Klickt auf **Synchronisierung** > **Erstellen**, dann entscheidet euch, ob ihr eine Zwei-Wege-Synchronisierung (Abgleich der Daten zwischen Quelle und Ziel) oder eine Ein-Wege-Synchronisierung (reine Datensicherung von Quelle zu Ziel) wollt.

So geht’s leichter | In die Cloud – aber sicher!



- Als Nächstes müsst ihr das Ziellaufwerk festlegen. Lasst euch nicht verwirren: Die Freigabe erscheint hier nicht als Eintrag. Sie findet sich nur unter dem Eintrag **Lokales NAS**, dort könnt ihr dann das Laufwerk und das gewünschte Verzeichnis auswählen.
- Legen Sie nun den Quell- und den Zielordner fest. Ihr könnt bei der Vergabe des Zielordners auch direkt einen neuen Ordner anlegen, indem ihr auf das Ordnersymbol mit dem Plus klickt.
- Als Letztes legt unter **Zeitplan** fest, ob der Job einmalig, nach einem anderen Job oder regelmäßig ausgeführt werden soll. Den Rest übernimmt das NAS automatisch, ohne einen Benutzereingriff.

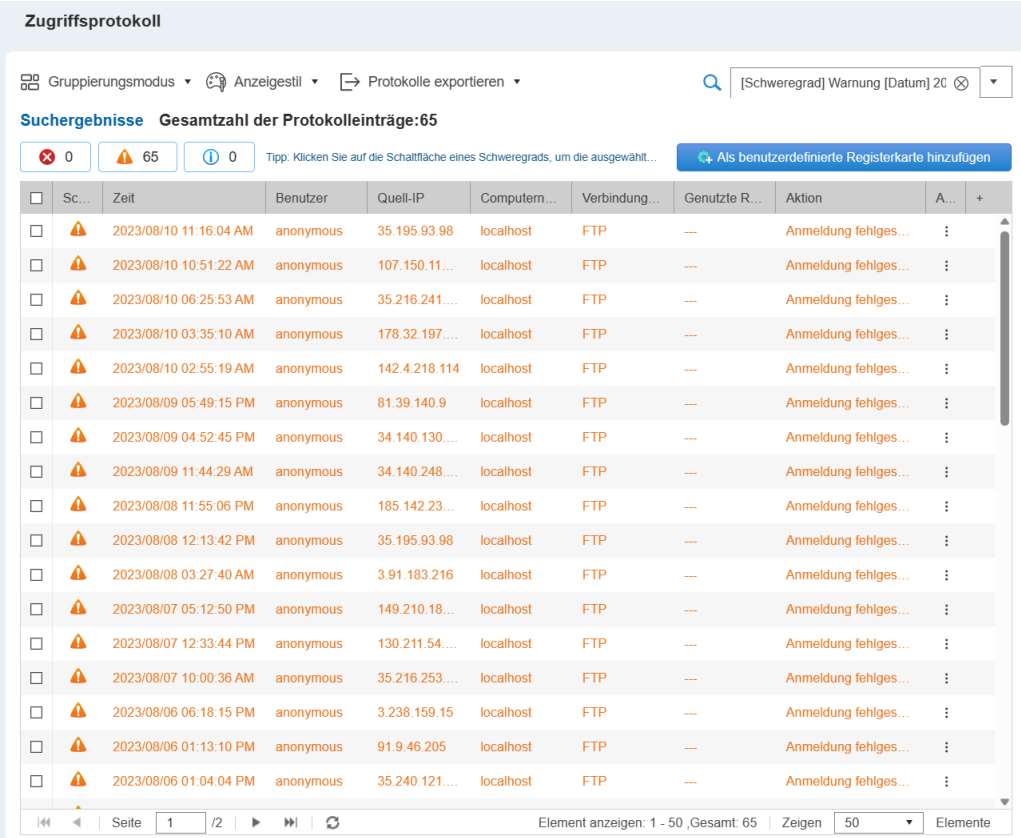
Sicherheitschecks durchführen

Geräte, die im Internet sind, sind immer einem gewissen Risiko ausgesetzt. Ganze Netze von mit Schadsoftware befallenen PCs werden dafür eingesetzt, einfach mal Benutzerkonten auszuspähen. Haben diese ein Gerät gefunden, dann versuchen sie, Standard-Benutzernamen zur

So geht’s leichter | In die Cloud – aber sicher!

Anmeldung zu verwenden. Über Wörterbücher werden dann alle möglichen Passwörter ausprobiert. Schutz gegen die Angriffe gibt es kaum. Wohl aber Verteidigung! Bei einer eigenen Cloud-Lösung habt Ihr nicht die Unterstützung eines Dienstleisters, der für euch die Sicherheitsmaßnahmen ergreift.

- Zuallererst solltet ihr natürlich sicherstellen, dass eure Passwörter so komplex sind, dass ein Angriff mit Begriffen aus einem Wörterbuch (Dictionary Attack) nicht erfolgreich sein kann. Am Ende könnt ihr nur die fehlgeschlagenen Anmeldeversuche im Log des Gerätes erkennen:

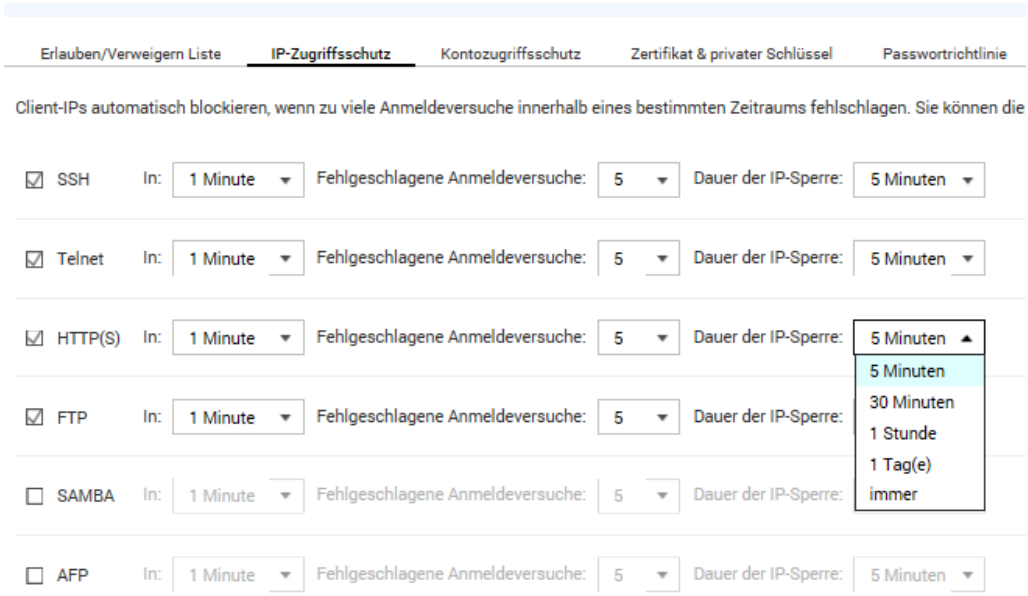


- Bei NAS-Systemen könnt ihr sowohl nach Protokoll (wie HTTP, FTP, ...) und Benutzernamen festlegen, dass das Konto bzw. die

So geht's leichter | In die Cloud – aber sicher!

IP-Adresse nach einer gewissen Zahl an Fehlanmeldungen gesperrt werden soll. Dazu klicken Sie auf **System** > **Sicherheit**.

- Unter **IP-Zugriffsschutz** könnt ihr festlegen, wie eine solche Sperre aussehen soll: Dazu könnt ihr die Zahl der fehlgeschlagenen Anmeldeversuche in einer festzulegenden Zeit angeben. Nach dieser sperrt das System eine IP-Adresse für eine bestimmte Zeit oder gar für immer.



- Unter **Kontozugriffsschutz** aktiviert ihr, dass Konten, die sich in einem bestimmten Zeitraum mehrfach erfolglos anzumelden versuchen, gesperrt werden sollen. Hier solltet ihr allerdings vorsichtig sein: Diese Einstellung wirkt nur dann, wenn tatsächlich ein Konto mit dem entsprechenden Namen existiert. Sonst kann es nicht gesperrt werden.

So geht's leichter | In die Cloud – aber sicher!

Fernzugriff einrichten

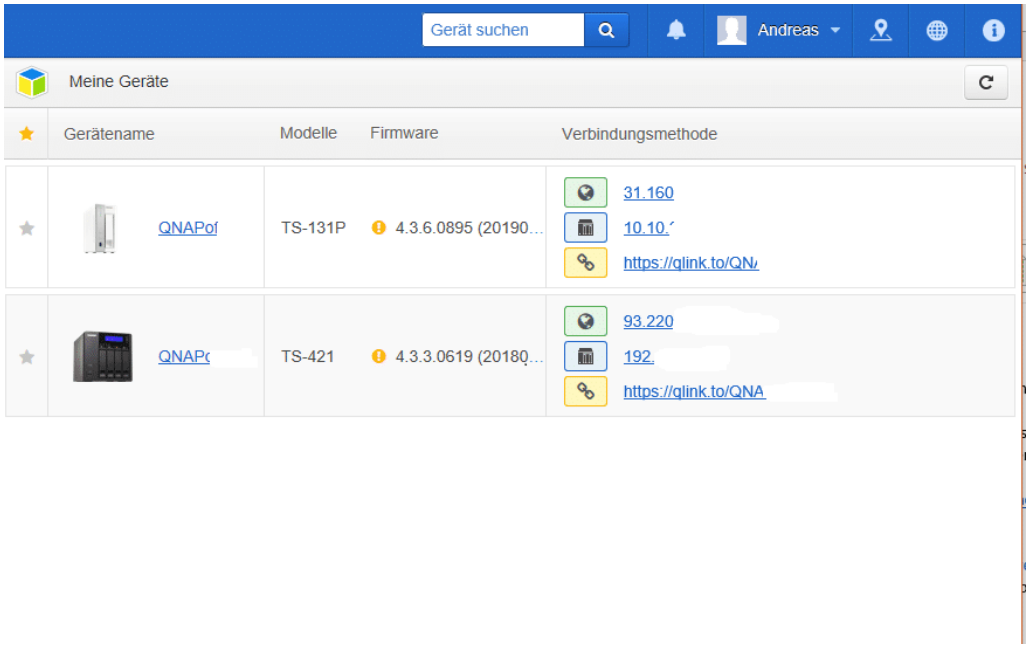
Um das NAS jetzt als vom Internet her zugreifbaren Cloud-Speicher verwenden zu können, müsst ihr einen Fernzugriff einrichten. Im Standard lässt eure Internetverbindung/Euer Router keinen Zugriff von außen zu. Dazu gibt es zwei unterschiedliche Wege: www.b.de

Fernzugriff über einen NAS-Dienst

Die NAS-Hersteller haben diese Aufgabe durch eigene Web-Dienste gelöst. MyQNAPCloud heißt der beispielsweise bei QNAP und er kann kostenlos genutzt werden.

- Dazu müsst ihr euch auf der Webseite einmalig registrieren und euch Benutzername und Kennwort merken. Auf dem NAS müsst ihr dann die myQNAPCloud-App installieren, die ihr im App Center findet. Startet die App, dann meldet euch mit den myQNAPCloud-Kontodaten an.
- Euer NAS meldet sich jetzt automatisch beim QNAP-Dienst an und ist über das Internet über myQNAPCloud.com erreichbar.

So geht's leichter | In die Cloud – aber sicher!



- Der komplette Datentransfer läuft über die Server von QNAP und ist verschlüsselt. Die Dateien liegen aber trotzdem lokal auf eurem NAS.
- Der große Vorteil im Gegensatz zu einer direkten Verbindung zum NAS: Manche Firewalls blockieren diese aufgrund der dyn.com-URL. Das passiert bei myQNAPCloud nicht, zumindest nicht in den Standardeinstellungen der Firewalls. Damit könnt ihr mit jedem Webbrowser auf euer NAS zugreifen und könnt es ganz normal konfigurieren und kontrollieren.

Nach Hause telefonieren: Dynamisches DNS

Wenn ihr den Zugriff auf eure Daten noch weiter einschränken wollt, dann könnt ihr auch einen direkten Weg zu eurem NAS einrichten. Das ist im Standard nicht vorgesehen, denn ihr habt ja keinen Zugriff auf eine Adresse, die euer Zuhause über das Internet erreichbar macht. LAN (Local Area Network, Ihr Heimnetzwerk) und WAN (Wide Area Network, das Internet) sind eigentlich nicht direkt miteinander verbunden.

So geht's leichter | In die Cloud – aber sicher!

„Eigentlich" ist hier das Zauberwort: Natürlich müssen die Datenpakete, die ihr beim Aufruf einer Internetseite anfordert, aus dem Internet zu eurem Rechner kommen. Und so bezieht der Router bei jeder Verbindung eine neue IP-Adresse von eurem Internet-Anbieter. Datenpakete, die er dort bekommt, gehen dann direkt an das anfordernde Gerät in Ihrem lokalen Netzwerk weiter.

Firmen haben zu diesem Zweck eine feste WAN-IP, die sich auch beim Neuaufbau der Verbindung zum Internet nicht ändert. Dies ist aber teuer und für den Privatanwender kaum finanzierbar.

- Dafür gibt es diverse Anbieter sogenannter „dynamischer DNS-Dienste". Internetanbieter wie IONOS und Strato bieten sie an, der bekannteste Dienst ist sicherlich Dyn.
- Die Funktionsweise ist recht einfach: Ihr bekommt vom Anbieter eine Internetadresse zugewiesen, deren ersten Teil ihr frei bestimmen könnt, beispielsweise *meinzuhause.dyndns.org.* Dafür zahlt ihr einen jährlichen Obolus.
- Dieser liegt in der Regel im niedrigen zweistelligen Eurobereich für ein Jahr und damit deutlich günstiger als eine feste IP-Adresse.

So geht's leichter | In die Cloud – aber sicher!

- Bei jedem Neuaufbau der Internetverbindung meldet eine kleine App auf dem PC, im Idealfall sogar direkt der Router, die neue WAN-IP-Adresse an den Dienst.
- Dieser hinterlegt dann diese Adresse, unter der der Router – und damit auch Euer NAS - erreichbar ist, an den Dienst, und der hinterlegt sie eurer externen Adresse.
- Ruft im Beispiel dann von unterwegs *http://meinzuhause.dyndns.org* auf, dann geht die Anfrage auf den Dienstanbieter, der sie auf die richtige Adresse des Routers weiterleitet.
- Um hier dann Daten an ein bestimmtes Gerät in eurem Netzwerk freizugeben, müsst ihr eine so genannte Port-Freigabe einrichten. Das findet in eurem Router statt und ist dort eine Standardfunktionalität. Vereinfacht gesagt hat der Router verschiedene Kommunikations- Anschlüsse, durch die er Daten leiten kann. Jeder Anschluss hat einen bestimmten Zweck. Port

So geht's leichter | In die Cloud – aber sicher!

80 ist für Internetanfragen, Port 21 für FTP, eine Liste der Standardports für verschiedene Anwendungen findet ihr unter https://de.wikipedia.org/wiki/Liste_der_standardisierten_Ports).

- Nehmen wir folgendes Beispiel: Eure Netzwerkfestplatte mit der internen IP-Adresse *192.168.0.45* soll als Cloud-Server via FTP fungieren. Dann muss im Router der Port 21 für Anfragen von außen umgeleitet werden auf diese IP-Adresse.
- Von unterwegs könnt ihr dann in einem FTP-Programm als Server ftp://meinzuhause.dyndns.org eingeben und landet direkt auf der Netzwerkfestplatte. Und das, ohne euch um die wechselnden WAN-IP-Adressen kümmern zu müssen!