

Anleitungen

- [Diceware](#)
- [Signal](#)
- [Keepassxc](#)
- [Nextcloud](#)
- [Nextcloud-App-Passwords](#)
- [Nextcloud-Webdav](#)
- [Vera-Crypt](#)
- [Backup](#)

Diceware

Diceware ist ein Verfahren um mit Würfeln und einer Wortliste, Passphrases / Passwörter zu generieren. Diese enthalten echten Zufall und sind bei ausreichender Länge als sicher zu betrachten.

In diesem Tutorial wird kurz beschrieben, wie du in wenigen Schritten so ein sicheres Passwort erstellen kannst. Eine Anleitung auf Englisch findest du [hier](#).

Tip

Wir empfehlen dir vorher die Seite zu [Passwörtern](#) durchzulesen. Dort erklären wir auch, wie lang deine Passphrase sein sollte und warum wir die Passphrase zufällig generieren. Es ist in jedem Fall nicht ausreichend, wenn du dir selbst 'zufällig' Wörter ausdenkst bzw. aus der Liste aussuchst. Außerdem empfehlen wir dir einen [Passwortmanager](#) zu benutzen damit du dir nur wenige wirklich sichere Passwörter merken musst.

Konzept

Die Idee ist, dass du für dein Passwort verschiedene Wörter aus einer Liste von ca. 7000 Wörtern auswählst. So bekommst du ein Passwort, das leicht zu merken ist und trotzdem echten Zufall enthält. Dazu brauchst du nur einen Würfel.

Schritt 1

Wähle eine Wortliste in einer Sprache aus, in der du dich wohlfühlst. Wenn deine Sprache nicht in der Liste ist, kannst du eine Wortliste finden, indem du nach "Diceware Wordlist" + "Sprache" suchst. Suche dir dabei eine Liste die für mindestens fünf Würfel ausgelegt ist, also mindestens 7776 Wörter enthält.

- [Dereko Wortliste \(kurze Worte\) DE](#)
- [dys2p/wordlists-de DE](#)
- [EFF's Long Wordlist EN](#)
- [Website mit anderen Sprachen](#)

Für dieses Beispiel verwenden wir die deutsche Dereko Wortliste mit kurzen Wörtern. Ihr könnt aber auch jede andere Liste welche für fünf Würfel ausgelegt ist nehmen.

Schritt 2

Würfle nun fünfmal mit dem Würfel und schreibe das Ergebnis in der Reihenfolge auf, in der du gewürfelt hast. zum Beispiel: `14314`

Nun schlage in der Wortliste nach welches Wort zu dieser Zahl passt. In diesem Fall: `batterie`

Schritt 3

Wiederhole Schritt 2 insgesamt sechs Mal. Du solltest jetzt sechs Wörter haben. Zum Beispiel:

`batterie tackler pferde wehen tresen zettel`

Herzlichen Glückwunsch zu deinem neuen Passwort!

Schritt 4

Wenn keine akute Repressionsgefahr besteht. Schreibe das Passwort auf einen Zettel und gib es ein- bis zweimal täglich ein. Nach ein bis zwei Wochen können sich die meisten Leute ihr neues Passwort gut merken. Dann vernichte den Zettel! Es ist auch ratsam, sich eine Geschichte zu den Wörtern auszudenken, um sie sich besser merken zu können.

Technische Details

Die Empfehlung sechs Wörter zu nehmen stammt aus dem offiziellen [EFF Guide für Diceware](#)

Signal

Credit: Sämtliche Inhalte dieses Artikels wurden 1-zu-1 aus dem Signal Bereich des [LG-Wikis](#) übernommen.

Signal PIN einrichten

Es ist sehr wichtig, dass du in Signal eine PIN einrichtest. Diese schützt vor unberechtigter Neuregistrierung. Dein Netz-Provider muss auf richterlichen Beschluss hin SMS an die Polizei umleiten. Ohne PIN kann die Polizei Signal mitlesen - aber das merkst du, weil du dann selbst aus Signal raus fällst: es kann nur ein Handy bei Signal registriert sein.

So geht's:

- iOS: tippe deinen Avatar an » Einstellungen » Konto
- Android: Einstellungen » Account (Konto) » Registration Lock (Registrierungssperre)

Verschwindende Nachrichten

In einzelnen Chats/Gruppen: Im Chat oben auf den Namen klicken » Disappearing Messages/Verschwindende Nachrichten

Es lässt sich auch ein default Zeitraum einstellen, dass das Feature für neue Chats automatisch aktiviert ist:

- Einstellungen » Privacy/Privatsphäre » Disappearing Messages/Verschwindende Nachrichten » Default Timer/Standardablaufzeit für neue Chats

Mehrere Signal-Accounts auf einem Gerät

Du kannst mehrere Signal-Accounts auf einem Gerät nutzen. Die Möglichkeiten sind für jedes Betriebssystem unterschiedlich, siehe die entsprechende Anleitung für dein Gerät.

Multiple Signal Accounts auf PC

Am einfachsten ist es, wenn du dir das Tool `signal-account-switcher` herunter lädst. Damit kannst du vier zusätzliche Signal-Accounts gleichzeitig nutzen. Dazu

1. auf diesen Link klicken: <https://github.com/kmille/signal-account-switcher/releases/tag/v0.1.0>
2. das Tool für dein entsprechendes Betriebssystem herunterladen (unten auf der Seite, `signal-account-switcher.exe` für Windows, `signal-account-switcher` für Linux, `signal-account-switcher-mac-{amd,arm}` für Mac).
3. das Tool starten (es kann sein, dass Windows erst mal meckert, weil das ja "unsicher" sei, einfach eine Datei aus dem Internet auszuführen) und einfach auf "Start Signal Account #1" klicken. Dann öffnet sich eine neue signal-desktop Instanz.

Wenn du keine Lust hast, ein extra Tool dafür zu installieren, kannst du das auch mit etwas manueller Konfiguration selbst machen:

- Anleitung für Windows: <https://www.youtube.com/watch?v=TejhH80jktE>
- Anleitung für Mac (dazu erst die Kommandozeile/Terminal öffnen):

```
mkdir $HOME/Library/Application/Signal-Account-1  
/Applications/Signal.app/Contents/MacOS/Signal --user-data-dir="$HOME/Library/Application/Signal-Account-1"
```

Multiple Signal Accounts auf Android

Molly

Es gibt den Signal Fork **Molly**, der neben der normalen Signal App installiert und mit einem anderen Account eingerichtet werden kann.

1. Falls noch nicht geschehen, installiere **F-Droid**
 - Lade den alternativen App-Store F-Droid herunter.
 - Installiere f-droid, indem du die .apk-Datei öffnest, die du heruntergeladen hast.
 - Lasse "Installation von Apps aus unbekannten Quellen" zu, wenn du danach gefragt wirst.
 - Erlaube ggf. "Apps aus dieser Quelle installieren".
2. Füge Molly's **Paketquelle** zu deinem F-Droid hinzu (**Anleitung**)
 - Gehe auf <https://molly.im/download/fdroid/> und wähle Molly (wenn du gerade am Handy liest), oder scanne den QR-Code, wenn du den Artikel am PC liest. **Wähle Molly, nicht Molly-FOSS, außer du weißt, was du tust** (zB keine Google-Play Dienste).

- Öffne F-Droid und refresh einmal (wische vom oberen Rand nach unten; damit lädst du Infos über alle verfügbaren Apps, dies kann bis zu 2 Minuten dauern.)
3. Installiere Molly über F-Droid
- Suche in F-Droid nach Molly und installiere es. Lass dafür ggf. wieder “installieren aus dieser Quelle” für F-Droid zu.

Jetzt ist Molly bereit und du kannst die App ganz normal wie Signal einrichten.

Am Anfang wirst du jedoch gefragt, ob du eine zusätzliche *Passwortverschlüsselung* nutzen möchtest, deine Wahl kann später nicht mehr geändert werden. Für sensible Accounts (z.B. PP) ist das sinnvoll, ansonsten ist es wie bei der normalen Signal-App.

Erstelle eine Signal-PIN, die du dir wirklich sicher merken kannst, oder speichere sie in deinen sicheren Passwortmanager, aber schreib sie nicht auf einen Zettel! Dieser kann nach einer Hausdurchsuchung von der Polizei genutzt werden, um Nachrichten an dich abzufangen.

App Klone

Einige Hersteller bieten eine Dual-App-Funktion, um mehrere Accounts auf einem Handy zu betreiben. Suche im Netz, ob dein Gerät über diese Funktion verfügt. Ab Android 14 könnte diese Option standardmäßig auf vielen Geräten vorhanden sein.

Du kannst diese Funktion auch nutzen, um Signal und Molly zu klonen, so dass du dann 4 Accounts hast. Du könntest damit auch auf die Nutzung von Molly verzichten und 2x Signal nutzen, Molly ist aber sinnvoller, da Molly über eine leicht bessere Verschlüsselung und Sicherheitsmechanismen verfügt, die im Falle einer Hausdurchsuchung einen Vorteil bieten.

Du kannst die Funktion einfach in den Android-Einstellungen aktivieren:

Samsung: Einstellungen > Erweiterte Funktionen > Dual Messenger

Huawei: Einstellungen > Apps > App Twin

LG: Einstellungen > Allgemein > Dual App

Daraufhin sollte ein Menü mit allen klonbaren Apps angezeigt werden, dort kannst du Signal (und ggf. weitere zu klonende Apps) einfach auswählen und verdoppeln.

Weitere Android Profile

Android bietet die Möglichkeit, wie Linux MacOS und Windows auch, mehrere Benutzerprofile anzulegen.

KeePassXC

Getting Started

Die offizielle *englischsprachige* KeePassXC [Dokumentation](#) bietet einen sehr guten und umfangreichen "[Getting Started](#)" Artikel. Es empfiehlt sich diesen einmal durchzulesen um einen Überblick über die verfügbaren Funktionen zu bekommen!

Im Folgenden werden die unserer Meinung nach wichtigsten Punkte aus der oben verlinkten Dokumentation von KeePassXC zusammengefasst. Dabei wird immer wieder auf die einzelnen Stellen in der Dokumentation von KeePassXC verwiesen. Falls es Dir schwer fällt, so viel Text zu folgen, gibt es z.B. [dieses Video](#) (*auf YouTube*), das die Kernfeatures von KeePassXC ganz gut erklärt. Daran anknüpfend gibt es auch eine [Fortsetzung](#) für fortgeschrittene Anwendungsfälle.

Datenbank anlegen

Die Datenbank ist im Grunde einfach nur eine Datei, in der die Passwörter verschlüsselt gespeichert werden. Sie endet immer mit `.kdbx`.

KeePassXC ist das Program, um diese Datei dann entschlüsseln und benutzen zu können.

Wenn du noch keine Datenbank hast, musst du zu erst eine neue Datenbank anzulegen. Bevor du startest, könntest du dir aber noch die [Empfehlungen zu Schlüsseldatei](#) (Schlüsseldateien) anschauen. Falls dir das zusagt findest du im Folgenden eine Anleitung dazu.

Zum Anlegen einer neuen Datenbank ohne Schlüsseldatei kannst du dem Schritt in dieser Anleitung folgen: [Neue Datenbank anlegen](#)

Schlüsseldatei

Beim Anlegen der Datenbank gibt es an der Stelle, wo das Passwort für die Datenbank festgelegt wird, einen Button `Zusätzlichen Schutz hinzufügen`.

Danach unter dem Feld `Schlüsseldatei` auf den Button `Schlüsseldatei hinzufügen`.

Hier kann jetzt entweder:

- eine neue Schlüsseldatei angelegt werden.
 - **Erzeugen**: einen Namen und Ort zum Speichern festlegen
- eine existierende Schlüsseldatei angegeben werden, die zum Verschlüsseln dieser Datenbank benutzt werden soll:
 - **Durchsuchen**: Datei auswählen

Datenbank mit Schlüsseldatei und Passwort entschlüsseln

Hast du deine Datenbank mit einem Passwort und zusätzlichem Schlüsseldatei geschützt, brauchst du auch beides, um sie wieder zu entsperren:

- Datenbank mit KeePassXC öffnen
- **Ich habe eine Schlüsseldatei**
 - Im Dateimanager die Schlüsseldatei auswählen
- Passwort eingeben
- bestätigen

Schlüsseldatei nachträglich hinzufügen

Falls du schon eine Passwortdatenbank hast, kannst du auch nachträglich noch ein Schlüsseldatei hinzufügen.

Wir empfehlen dringen vorher ein Backup deiner Datenbank zu machen. Damit verhindern wir den Verlust sämtlicher Passwörter, falls dabei etwas schief gehen sollte. *(Dafür einfach eine Kopie der Datenbank mit einem neuen Namen machen. Heißt die Datenbank z.B. "Passwords.kbdx" erstelle eine Kopie namens "Passwords-keyfile.kbdx" oder so.)*

- Öffne die (neue) Datenbank in KeePassXC
 - Jetzt kann es sein, dass du beide Datenbanken gleichzeitig geöffnet hast:
multiple db tabs
 - Das ist nicht weiter schlimm, pass aber auf, dass du nicht durcheinander kommst und die falsche Datenbank bearbeitest. Schließe z.B die originale Datenbank, damit nichts schief geht.
- in der oberen Leiste auf **Datenbank**
- **Datenbanksicherheit...**
- von hier an folge der Anleitung des Abschnitts [hier drüber](#)
- Achtung: hast du nun ein Schlüsseldatei erzeugt und gespeichert, geht KeePassXC davon aus, dass du nun **nur** diese Schlüsseldatei zum Entsperren der Datenbank benutzen willst. Solltest du schon auf **OK** geklickt haben, hast du auch eine solche Warnung gesehen.

- Daher muss mit `Passwort ändern` das Passwort nochmal gesetzt und bestätigt werden.
- `OK`

Passworteinträge

Hier ist erklärt, wie du einen Eintrag anlegen kannst: [Passworteintrag anlegen](#).

Du kannst existierende Einträge auch [nachträglich bearbeiten](#) (Doppelklick auf Eintrag).

Browserintegration

Es gibt eine [offizielle Anleitung](#), um das Browser-Plugin zu installieren (außer für Safari).

TOTP

[Offizielle KeePassXC Anleitung](#) mit guten Screenshots.

TOTP ist eine Form der 2-Faktor-Authentifizierung, die viele Webdienste wie z.B. E-Mail oder Cloud Zugänge nutzen. Um für einen Dienst die 2FA einzurichten, braucht es zwei Dinge:

1. Die entsprechende Einstellung im Webdienst, also z.B. in den E-Mail Einstellungen.
2. Die Konfiguration des entsprechenden KeePassXC Eintrages für diesen Webdienst.

Die Einstellung der Webdienste sehen natürlich alle etwas unterschiedlich aus, aber in den meisten Fällen gibt es in den Konto Einstellungen:

- eine Sektion mit `Sicherheit` oder `Privatsphäre`.
- Hier sollten sich die `2FA` bzw. `TOTP` Einstellungen finden.
- `TOTP aktivieren` oder ähnliches

Jetzt sollte ein QR-Code und im besten Fall eine zufällige Zeichenkette erschienen (Siehe KeePassXC Anleitung). Der QR-Code ist praktisch, wenn du TOTP auf dem Handy einrichtest, da du mit den Handy-Apps einfach per Kamera das `Secret` auslesen kannst. Am PC brauchen wir dafür die Zeichenkette.

Sollte hier nur der QR-Code, ohne Zeichenkette auftauchen, müssen wir das `Secret` aus dem QR-Code heraus lesen.

Secret aus QR-Code herauslesen

Das funktioniert mit allen gängigen Handy Kameras, die QR-Codes lesen können.

Hier taucht sehr wahrscheinlich mehr auf, als das reine `Secret`, sondern eine URL, die eigentlich für mobile Apps gedacht ist, z.B.:

```
otpauth://totp/example.org:username?secret=PABRSLZNHFLAIENT&issuer=Example
```

Das `Secret` versteckt sich hier zwischen dem `secret=` und dem nächsten Sonderzeichen, hier `&issuer...`.

Unser `Secret` lautet somit: `PABRSLZNHFLAIENT`.

- `Secret kopieren`

Nun gehen wir in die KeePassXC Datenbank:

- Rechtsklick auf den entsprechenden Passworteintrag
- `TOTP`
- `TOTP einrichten`
- `Secret` einfügen
- `OK`

Jetzt sollte neben dem Passworteintrag eine kleine Uhr zu sehen sein. *Die symbolisiert den temporären Charakter der TOTP Codes.* totp clock symbol

Wir müssen abschließend die TOTP-Einrichtung synchronisieren. Dafür muss der aktuelle TOTP-Token wieder in den Einstellungen des Webdienstes eingegeben werden. Der TOTP-Token kann auf zwei Arten kopiert werden:

- `Steuerung` + `T`, oder
- `Rechtsklick` > `TOTP` > `TOTP kopieren`

Wir gehen wieder in die Einstellungen des Webdienstes:

- TOTP-Token einfügen
- Bestätigen

Jetzt solltest du angezeigt bekommen, dass die Einrichtung erfolgreich war.

Backup

KeePassXC bietet eine automatische Backup-Funktion. Damit ist sichergestellt, dass Du immer eine up-to-date Version deiner Passwortdatenbank an einem anderen "Ort" hast, als die, die du hauptsächlich benutzt.

Unter [Einstellungen \(Zahnrad\) > Allgemein > Dateiverwaltung](#) findet sich die Option [Vor dem Speichern Backup der Datenbank erstellen](#). Dort kannst du einen Pfad festlegen, wo die Ersatz-Datei gespeichert werden soll.

Hier kann es sich anbieten, einen Cloud-Speicher anzugeben, wenn du die Datenbank nicht schon darüber synchronisierst: [Empfehlungen](#)

Achtung

Obwohl die Datenbank immer verschlüsselt ist, auch in der Cloud, gibt es Szenarien die dabei mitbedacht werden müssen. Lies dich hier schnell ins [Beispiel Szenario](#) einer potentiellen Bedrohung ein!

Synchronisation/Backup in Nextcloud

Bei aktivismus.org findest Du Links zu Anleitungen für sämtliche Plattformen, wie du Dateien über eine Nextcloud synchronisieren kannst.

Das Prinzip funktioniert genauso mit iCloud, OneDrive, Dropbox, etc ...

Nextcloud

Nextcloud ist eine Open-Source Software, die frei von jedem selbst auf einem eigenen Server installiert (gehostet) werden kann. Solidarische Technik Kollektive betreiben teilweise ihre eigenen "Instanzen". "Instanzen" nennt man die jeweils einzelnen Nextcloud Installationen, also z.B. der verschiedenen Gruppen/Vereine/Firmen, usw. Je nach Einstellungen der jeweiligen Instanz, ist die einzelne Nextcloud also vollkommen "autark", sprich sie hat mit anderen Instanzen nichts zu tun.

Auch für politische Gruppen kann die Nextcloud ein attraktives Werkzeug sein, die eigene Arbeit mit geteilten Passwörtern, Kalendern, Dokumentationen, Pads, usw. zu organisieren.

Account-Verwaltung (Konzept)

Quelle: <https://wiki.systemli.org/howto/nextcloud/gruppen>

Wenn ihr die Cloud als Gruppe nutzen wollt, stellt sich das Problem, welchem User die gemeinsam genutzten Daten (Dokumente, Kalender, Deck-Boards, ...) gehören. Deshalb empfehlen wir für Gruppen die Nutzung von Teams

Teams

- Jedes Mitglied eurer Gruppe bekommt einen **persönlichen Account**.
- Zusätzlich erstellt ihr einen **Gruppen-Account** als Admin, der von mehreren Personen verwaltet wird.
- Erstellt mit dem Gruppen-Account in der **Collectives-App** (*wenn verfügbar*) ein Kollektiv für die Gruppe.
 - unter **Mitglieder verwalten** fügt ihr alle persönlichen Accounts hinzu.
 - Gebt wenn nötig einzelnen oder gar allen Accounts Admin-Rechte.
 - neben **Teams** auf das **+** und Beschreibung folgen

Technisches Detail: Warum nicht in Kontakte?

Das Anlegen des Teams ginge zwar auch unter **Kontakte**, allerdings **gehört** euch dann das Team und das wollen wir wie weiter unten beschrieben, vermeiden. Falls die Collectives-App nicht verfügbar ist, legt unter **Kontakte** ein Team an, denkt aber an die Probleme damit

Jetzt habt ihr (*mit dem Gruppen Account*) ein Kollektiv*(Team)* erstellt. Ab sofort könnt ihr so ziemlich alles, was ihr in der Nextcloud macht, mit diesem Team teilen: Dateien, Kalender, Kanban-Boards (Deck-App), Umfragen, usw.

Dabei ist allerdings eine Sache zu beachten: Die **Ownership** (dt: *Eigentum*, aber der englische Begriff sagt hier mehr aus). Und zwar gehören sämtliche Dateien (*also auch Kalender, Kanban-Board, etc*) immer dem Account, der sie angelegt hat! Auch wenn diese **Ressourcen** (Fachbegriff) dann mit dem ganzen Team geteilt werden, **gehören** sie immer noch dem Ersteller-Account.

Achtung

Sollte nun der Ersteller-Account einer Ressource plötzlich gelöscht werden, werden auch alle Dateien gelöscht, die diesem Account gehört haben!

Tip

Deshalb ist es sehr ratsam, möglichst alle geteilten Ressourcen mit dem **Gruppen-Account** zu erstellen und sie von dort mit dem Team zu teilen.

ownership & sharing concept

Die obere Grafik zeigt, dass der Gruppen-Account eine Passwortdatenbank in seine Dateien hochlädt und diese eine Datei dann mit dem Team teilt. Diese wiederum können dann auf diese Datei zugreifen.

So könnt ihr später ganz einfach Personen zu eurem Team/Kollektiv hinzufügen/entfernen. Ihr müsst nicht bei jeder neuen Person sämtliche Ressourcen neu teilen. Außerdem könnt ihr die Verwaltung des Admin-Accounts einfach weiterreichen und es ist kein Problem, wenn die ursprünglichen Admins inaktiv werden.

Oder anders herum können mit einem Klick einzelne Accounts aus dem Team entfernt werden, sodass diese keinen Zugriff mehr auf Gruppen-Ressourcen haben.

Oder anders herum können mit einem Klick einzelne Accounts aus dem Team entfernt werden, sodass diese keinen Zugriff mehr auf Gruppen-Ressourcen haben.

Oder anders herum können mit einem Klick einzelne Accounts aus dem Team entfernt werden, sodass diese keinen Zugriff mehr auf Gruppen-Ressourcen haben.

Ownership Übertragen

Falls ihr mal keinen Zugriff auf den Gruppen-Account haben solltet, gibt es auch die Möglichkeit die „Ownership“ einer von eurem persönlichen Account angelegten Datei zum Gruppen-Account zu

übertragen. Nextcloud bietet dafür eine eigene Anleitung

- Der Transfer muss allerdings immer erst vom Gruppen-Account (*der die Ownership übertragen bekommt*) bestätigt werden, bevor er in Kraft tritt.
- Erfahrungsgemäß kann das auch ein paar Minuten dauern, bis der Gruppen-Account die entsprechende Benachrichtigung zum Bestätigen bekommt. Es kann also sein, dass ihr etwas abwarten müsst.

Nextcloud-App-Passwords

Bei Nextcloud ist es möglich sich App Passwörter anzulegen. Damit kann jedem Gerät oder App, die man mit dem eigenen Account verbindet, ein anderes Passwort gegeben werden. Der Vorteil davon ist, dass so einfach aus den Account-Einstellungen einzelnen Geräten oder Apps der Zugriff auf das Konto wieder entzogen werden kann.

- In der Cloud einloggen und oben rechts auf den Avatar klicken

Nextcloud avatar

- `Settings` > `Security` auswählen

Nextcloud security settings

Hier kann ein neues App Passwort erstellt werden:

1. Zuerst geben wir dem neuen Passwort einen Namen, um später zu wissen, wofür wir dieses Passwort benutzt haben (um nicht das falsche wieder zu löschen). Hier nennen wir es "Sync Client".
2. Klicke `Create new app password`

name new app password

Jetzt wird das Passwort zum ersten und letzten Mal angezeigt! Der Nutzernamen und das App spezifische Passwort. Klicken wir dieses Fenster zu, kann das Passwort nicht mehr angezeigt werden. Das ist prinzipiell nicht schlimm, da wir dieses Passwort auch einfach wieder löschen und ein neues anlegen könnten.

Der Button `Show QR code for mobile apps` erlaubt es Nextcloud-Apps für Mobilgeräte sich einmalig einzuloggen.

onetime view app password

Hier sehen wir nun die verschiedenen "Sessions", die auf unseren Account zugreifen können.

different sessions

Alte Sessions löschen

Hier wird auffallen, dass jedes Mal, wenn wir uns im Browser anmelden und später nicht mit dem `Logout-Button` abmelden, diese "Session" gültig bleibt. Das ist etwas nervig, da wir dann schnell den

Überblick verlieren, ob es unsere eigenen "Sessions" sind, oder ob sich zwischenzeitlich zum Beispiel auch ein Angreifer eingeloggt hat.

delete old sessions

Hier sieht man zum Beispiel, dass wir uns vor 10 Stunden nicht ordentlich abgemeldet haben, sondern einfach nur das Browser-Fenster zu gemacht haben. Die Session ist theoretisch noch gültig, aber für uns nicht mehr nützlich. Also löschen wir die alte Session.

Alternative Anleitung

Systemli hat auch eine Anleitung zu App Passwörtern, falls hier etwas unklar sein sollte.

Nextcloud-Webdav

Nextcloud Sync Client

Der Nextcloud Sync Client ist Nextcloud's eigene Software, um Inhalte in der Cloud mit den eigenen Endgeräten (*PC, Handy, Tablet*) zu synchronisieren. Die Installation und Einrichtung ist in den allermeisten Fällen sehr einfach.

Das bedeutet, es erstellt einen Ordner auf dem Gerät, in dem dann alle Dateien aus der Cloud liegen. Wird eine Datei in diesem Ordner geändert, ändert sie sich direkt in der Cloud und somit auch für alle anderen Geräte, die damit verknüpft sind.

Ein praktikables Beispiel dafür ist unser Modul KeePassXC als Gruppe nutzen

Installieren

- Software downloaden: <https://nextcloud.com/install/#desktop-files>

sync client download page

- Sync Client installieren

Einrichten

- Login
- die URL deiner Cloud-Instanz eintragen (*auf der du einen Account hast*)
- dann sollte sich ein Browserfenster mit dem Login der Cloud öffnen

sync client login process

Hier gibt es zwei Optionen:

1. Mit den normalen Zugangsdaten einloggen
2. Oder besser auf Alternative log in using app password mit einem extra App Passwort einloggen!

login with app password

Haben wir uns eingeloggt, erscheint ein solches Konfigurationsfenster, in dem wir festlegen können, welche Ordner aus unserer Cloud auf unseren/mit unserem Rechner synchronisiert werden sollen. Entweder wählen wir hier nur spezifische Ordner () aus, oder einfach alle. Außerdem können wir unter festlegen, wo auf unserem Rechner der synchronisierte Nextcloud Ordner liegen soll.

sync options

Je nachdem wie viele Daten wir in der Cloud haben kann der Synchronisationsprozess ein bisschen dauern. Dann sollten wir unsere Persönlichen Cloud Dateien alle auf dem Rechner in dem festgelegten Ordner direkt zugänglich haben.

Vera-Crypt

Für alle hier genannten Methoden ist die Software VeraCrypt notwendig. Das heißt sowohl zu verschlüsseln, also auch zum entschlüsseln (verschlüsselte Sticks/Ordner wieder öffnen) muss dieses Programm auf dem PC installiert sein. Ohne geht es leider nicht.

Komplette Festplatten/USB-Sticks oder Ordner mit VeraCrypt verschlüsseln

Um einen gesamten USB-Stick oder Festplatte (Speichermedium) zu verschlüsseln gibt es zwei Möglichkeiten:

1. Einen Ordner so groß, wie das gesamten Speichermedium erstellen und verschlüsseln
2. Das Dateisystem der Festplatte selbst verschlüsseln

Weil bei Option 2 so einiges schief gehen kann, empfehlen wir generell die 1. Option. Dadurch sollte es keinerlei Nachteile geben. Das bedeutet auch, dass bei der 1. Option der Vorgang für einzelne Ordner zu verschlüsseln, oder gleich den gesamten Stick/Festplatte, identisch sind.

Wenn das zu verschlüsselnde Gerät aber FAT32 formatiert und größer als 4GB ist funktioniert das leider nicht, was leider häufiger der Fall ist.

Details zu FAT32 und co.

Neue USB-Sticks werden oft mit FAT32 Formatierung ausgeliefert. Das ist in sofern ein Problem, als das auf FAT32 u.ä. keine Dateien größer 4GB abgespeichert werden können.

Da der Stick wahrscheinlich größer als 4GB ist, muss für Option 1 auch eine Datei (dh. der Ordner; siehe weiter unten) größer als 4GB darauf erstellt werden, was in diesem Falle fehlschlagen wird.

Das merkst du spätestens am Ende, wenn sich der Prozess (wie in dem Screenshot unten) bei 4GB aufhängt: \$32GB \cdot 13% \approx 4GB\$

Sollte das besagte Speichermedium eben solch eine Formatierung haben, muss es für entweder für Option 1 umformatiert werden (benötigt andere Software), oder Option 2 gewählt werden.

Wir beschreiben von nun an beide Optionen parallel. Sofern es bei einzelnen Punkten Abweichungen gibt, werden die beiden Optionen durch die Überschriften "Option 1" bzw "Option 2" gekennzeichnet. Der Rest gilt für beide Optionen.

VeraCrypt öffnen

- Klicke auf

Screenshot von neu geöffnetem VeraCrypt

Option 1: Datei für Container erstellen

Der verschlüsselte "Ordner" ist für den PC eigentlich nur eine Datei, die bei VeraCrypt Container heißt. Wir können sie nur später mittels VeraCrypt als normalen Ordner benutzen.

Merke

- Ein VeraCrypt-Container ist für den PC nur eine Datei
- Für uns sieht der Container später wie ein normaler Ordner aus

- Hier wählen wir wie oben beschrieben, einen "Datei-Container" aus:

VeraCrypt view: Encrypt File Container

- Dann wähle und

Unter dem Location Menü, wählen wir jetzt den Ort, an dem VeraCrypt den Ordner(Container) für uns ablegen soll. Das soll natürlich unser Stick/Festplatte sein.

- Klicke also
- Darauf hin öffnet sich der Dateimanager. Navigiere hier auf den Stick/Festplatte, die verschlüsselt werden soll.
- Jetzt erstellen wir diese ominöse Datei, die später zu unserem verschlüsselten Ordner wird. Gib dafür in dem dafür vorgesehenen Feld einen Namen für die Datei ein. Es ist technisch irrelevant wie sie heißt, es wird aber der Name jener Datei sein, die man später sieht, wenn man den Stick einfach einsteckt und öffnet.

VeraCrypt Location Menu

- Bestätige mit

Option 2: Ganzes Dateisystem verschlüsseln

select partition drive

- Standard VeraCrypt Volume > Next>

device location view

Nun müssen wir das Speichermedium auswählen.

Achtung

Die Liste zeigt jetzt alle verfügbaren Speichermedien an, die mit dem Rechner verbunden sind, also auch andere Festplatten, USB-Sticks, SD-Karten usw.

Alle Dateien auf dem Gerät, dass hier ausgewählt wird, werden unwiederbringlich gelöscht, also stelle sicher, dass du das richtige Gerät auswählst!

device selection list on Linux

Meist hilft ein Blick auf die Speichergröße, um den richtigen Stick zu erkennen. Solltest du eine Festplatte verschlüsseln wollen, die evtl genau so groß wie andere angeschlossene Speichermedien ist, musst du dir den Pfad/Mountpoint anschauen.

- Bestätige die Warnung, dass alle Dateien auf dem ausgewählten Gerät zerstört werden.

Encryption Options

Die Standart-Einstellungen sollen uns hier ohne weitere Erklärung genügen, da das sonst den Rahmen sprengt.

- Next>

VeraCrypt encryption options

Option 1: Volume Size

Hier legen wir fest, wie groß der Container(Ordner) später sein soll. Es kann also je nach freiem Speicherplatz eine Größe frei gewählt werden.

Größe wählen

Hier sollte nur beachtet werden, dass wenn später eine z.B. 100 MB große Datei in den Ordner gelegt werden soll, hier etwas mehr Platz gewählt werden sollte, z.B. 110 MB. Das liegt daran, dass die Verschlüsselung auch selber etwas Platz weg nimmt.

VeraCrypt view: select Volume Size

Option 1: Ordner so groß wie gesamter Stick

Wie im oberen Bild zu sehen ist, gibt es ein extra Häkchen, um den gesamten freien Platz für die Erstellung des Containers(Ordners) zu verwenden.

Beispiel

Sollte sich also auf einem 4GB großen Stick schon vorher 1 GB Daten befinden, wird der neue Container mit dieser Option 3GB groß und die vorhandenen Daten bleiben bestehen.

Das ist der Grund, warum wir ganz am Anfang die 1. Option gewählt haben, da bei der zweiten Option alle Daten gelöscht werden, sollte z.B. die falsche Festplatte ausgewählt werden.

Es erscheint eine Warnung, dass Dateien größer als 4GB nicht auf FAT32 gespeichert werden können. Hier könnt ihr einfach klicken.

Password setzen

Hier wird das Passwort gesetzt, mit dem Der Container verschlüsselt werden wird. Dafür sollte ein starkes Passwort gewählt werden, da es sonst einfach erraten werden kann.

Am besten wird hierfür ein Passwort mit einem Passwordmanager generiert und abgespeichert, wie z.B. hier:

Screenshot KeePass with USB Stick Password

VeraCrypt view: set password

Dateisystem Einstellungen

Nun werden wir gefragt, ob wir Dateien größer als 4GB in unserem Ordner speichern wollen (das hatten wir eben schon einmal).

Large Files yes or no

Wenn ihr euch sicher seid, dass ihr das nicht tun werden, klickt auf , ansonsten auf .

Danach muss ein Dateisystem festgelegt werden.

File System selection

- Wähle , wenn du den Speicher auf Windows Computern benutzen willst
- Wähle , wenn du den Speicher sowieso nur auf Linux und MacOS benutzen willst
- Wähle , wenn du den Speicher nur auf Windows benutzen willst.

Die jeweiligen Plattformen können unter Umständen mit allen Formaten umgehen, diese Empfehlungen sollten aber problemlos funktionieren.

Quick Format

Das Häkchen bei ist meist nur für Option 2 verfügbar. Es bedeutet, dass bei der Verschlüsselung der Speichers **nicht** mit zufälligen Bits überschrieben wird. Der Vorteil davon ist, dass, besonders für große Datenträger, sich der Verschlüsselungsprozess extrem verkürzt, bzw. nur noch Sekunden dauert.

Das bringt aber auch Unsicherheiten mit sich und deshalb wählen wir das nur aus, wenn:

- Auf diesem Speichermedium noch **nie** kompromittierende Daten drauf waren. (*Nie heißt hier wirklich nie, siehe Datenhygiene*), oder
- Das Speichermedium jetzt grade auch schon gut verschlüsselt ist, sein Passwort keinem Feind bekannt und es jetzt nur "nochmal neu" verschlüsselt wird (*warum auch immer*).

quick format warning

Tip

Quick Format nur bei nagelneuen Speichermedien!

Gib als nächstes an, ob du das Speichermedium auch auf anderen Betriebssystemen als deinem jetzigen benutzen willst (im Zweifel, nur für den Fall, immer diese Option).

Cross Plattform Support checkbox

Zufallsgenerator

Jetzt öffnet sich der "Zufallsgenerator". Ohne weiter darauf einzugehen sei hier gesagt, dass gute Verschlüsselung von zufällig generierten Daten abhängt, die mit in die Verschlüsselung "rein gemischt" werden.

Da Computer darin nicht perfekt sind, fordert VeraCrypt hier den Menschen dazu auf, mit der Maus zufällige Bewegungen in dem Fenster zu machen. Dabei füllt sich langsam die blaue Leiste unter "Randomness Collected From Mouse Movements".

Randomness Collector

Die Leiste sollte mindestens halb voll werden, mehr ist besser.

-

Verschlüsselungsprozess

Nun beginnt VeraCrypt die Datei in der festgelegten Größe und den gewählten Einstellungen zu verschlüsseln. Dafür schreibt es zuerst (wenn kein gewählt) zufällige Einsen und Nullen auf den gesamten Container. Je nach seiner Größe kann das ein einige Minuten bis zu Stunden dauern.

encryption process with time prediction running

Nachträglich Passwort ändern

Man kann auch nachträglich das Passwort eines VeraCrypt Containers ändern.

- Container mounten

mount file

-

change Volume Password

- Oben das alte und unten zwei mal das neue Passwort eingeben. _(Tipp: Passwörter mit Passwortmanager generieren und abspeichern)

set new password

move mouse for randomness collector

successfully changed

Backup

Im Artikel zu Backups in den Gegenmaßnahmen haben wir versucht zu beschreiben, warum Backups so wichtig sind. Hier wollen wir zeigen, wie Backups überhaupt gemacht werden können.

Backup von was?

Jede/r muss sich natürlich selbst Gedanken darüber machen, was alles zu backupen ist. Hier ist eine Checkliste als Beispiel:

- Passwörter
- Kontaktdaten (Adressen, Telefonnummern, Mail-Adressen, usw.)
- offizielle Dokumente
- selbstgeschriebene Texte (von euch oder anderen)
- Protokolle (wenn nötig)
- Chats (wenn nötig)
- Erinnerungen (Photos, etc)

Wie backupen

Es gibt natürlich etliche Arten, sich Backups zu machen. Vom einfachen Kopieren und Funktionen von Betriebssystemen bis zu mächtigen Programmen wie borg/rsync, Kopia oder anderen.

Wichtig

Nur auf verschlüsselte Datenträger backupen!

Manuell kopieren

Die simpelste Art zu backupen ist natürlich einfach einen USB_Stick in den Rechner zu stecken und einmal das Home-Verzeichnis (Ordner des Benutzers) darauf zu kopieren, bzw am Handy sämtliche Ordner aus dem Dateimanager darauf zu kopieren.

Das kann aber sehr ineffizient sein, da ständig neue Daten anfallen, die gebackupt werden sollen. Dann muss jedes mal aufs neue evaluiert werden, welcher Dateien und Ordner jetzt wieder kopiert

werden müssen.

Vorteile

- copy/paste

Nachteile

- jedes Mal neu evaluieren was zu backupen ist
- nicht automatisiert (man muss von selbst daran denken)
- es müssen jedes mal aufs neue sämtliche Daten rüber kopiert werden (dauert lange)

Systemeigene Backup Funktionen

MacOS

MacOS macht es den Nutzenden sehr einfach, **regelmäßige** Backups zu machen. Das hauseigene Tool heißt `Time Machine`. Die Apple eigene Anleitung ist sehr gut verständlich.

Alles was es braucht ist ein Speichermedium, das groß genug ist. Groß genug bedeutet in dem Fall am besten mindestens doppelt so groß wie die zu backupenden Daten, da `Time Machine`.

Vorteile

- einmal konfigurieren, danach einfach nur noch jedes Mal Speichermedium anschließen
- Dateien, die schon im vorherigen Backup waren und immer noch unverändert sind, werden übersprungen (spart viel Zeit)
- behält (je nach deinen Einstellungen) mehrere Versionen deiner Backups (gestern, letzter Monat und letztes Jahr z.B.) Auch hierbei zählt der Punkt obendrüber, es wird nichts doppelt gespeichert.
- löscht alte Backups automatisch, die im neuen Durchlauf ersetzt werden

Nachteile

- Man muss von selbst daran denken, regelmäßig das Speichermedium anzustecken