Verschlüsselung externer Speicher und Ordner

Hier erfährst du:

- Wie du USB-Sticks, Festplatten und Partitionen verschlüsseln kannst
- Wie verschlüsselte Ordner (Container) erstellen kannst, die du dann verschicken oder auf eine Cloud stellen kannst

---

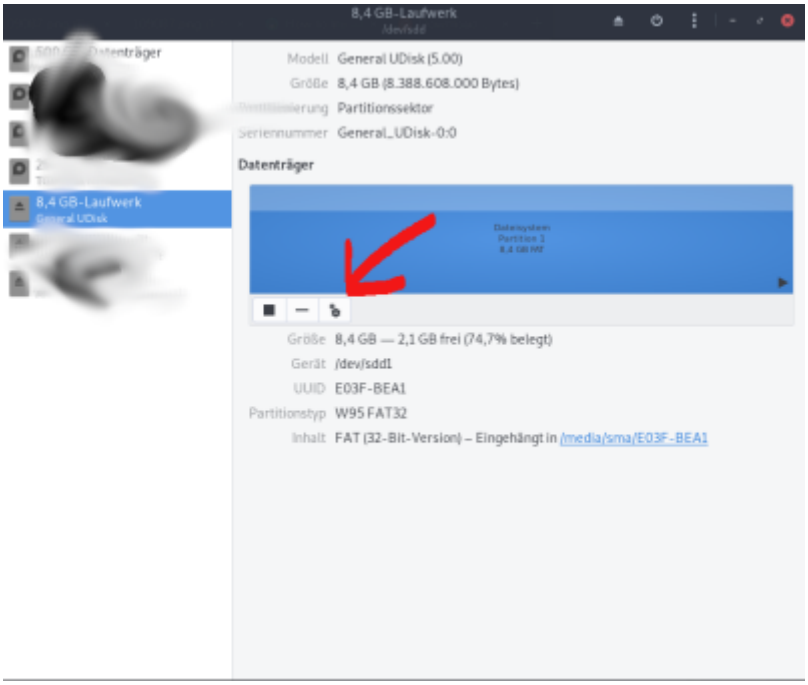
Wenn du einen externen Datenträger (zB eine Festplatte oder einen USB-Stick) verschlüsseln willst gibt es unterschiedliche Lösungen. Durch die Verschlüsselung gehen aber (meist) alle Daten auf dem Datenträger verloren, die sollten also davor gesichert werden.

Mehr ist mehr! Verschlüssel so viel wie möglich:
Beim Anschließen und Entschlüsseln externer Speichermedien können Spuren der verschlüsselten Dateien auf deinem Computer hinterlassen werden. Das könnten Einträge unter zuletzt geöffnete Dateien oder Vorschaubilder sein. Am besten verschlüsselst du sowohl externe Speichermedien als auch deinen Computer.

Linux: Datenträger verschlüsseln

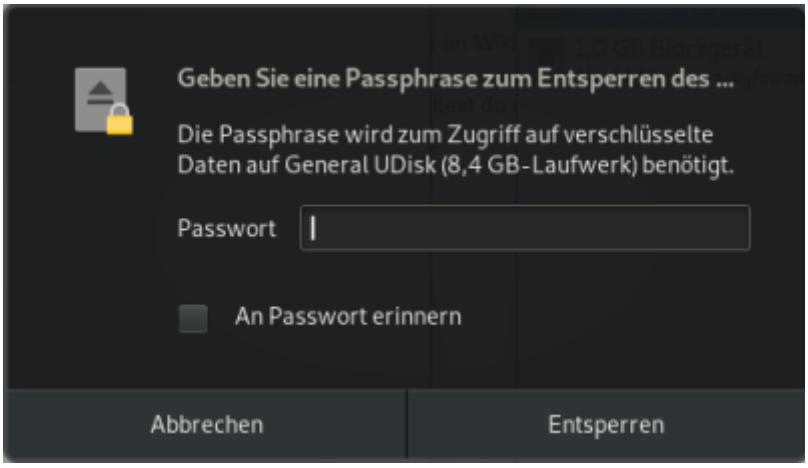
In einer Linux-Distribution (z.B. Debian oder Ubuntu) lassen sich leicht externe Datenträger verschlüsseln, sie sind dann jedoch leider nur unter Linux zu öffenen (um sie unter anderen Betriebssystemen öffnen zu können, können Zusatzprogramme installiert werden, die die Laufwerke dann entschlüsseln können).

⇒ Starte die Laufwerksverwaltung, - zB „gnome disk utility“. (Meist heißt sie einfach „disks“ oder „Laufwerke“)
⇒ Wähle den zu verschlüsselnden Datenträger aus. Achte darauf, dass alle Daten zuvor gesichert wurden.



⇒ Wähle *Einstellungen* (das kleine Symbol mit den Zahnrädern) → *Partition formatieren*
⇒ Gib die gewünschte Größe an. Für den gesamten Datenträger wähle das Maximum.
⇒ Gib einen Namen ein: Mit diesem Namen wird das Laufwerk dann angezeigt
⇒ Wähle nun „for use with Linux systems only“ und mache das Häckchen bei „password protect volume (LUKS)„
⇒ Wähle ein sicheres Passwort! Tipps zu sicheren Passwörtern findest du hier im Wiki.

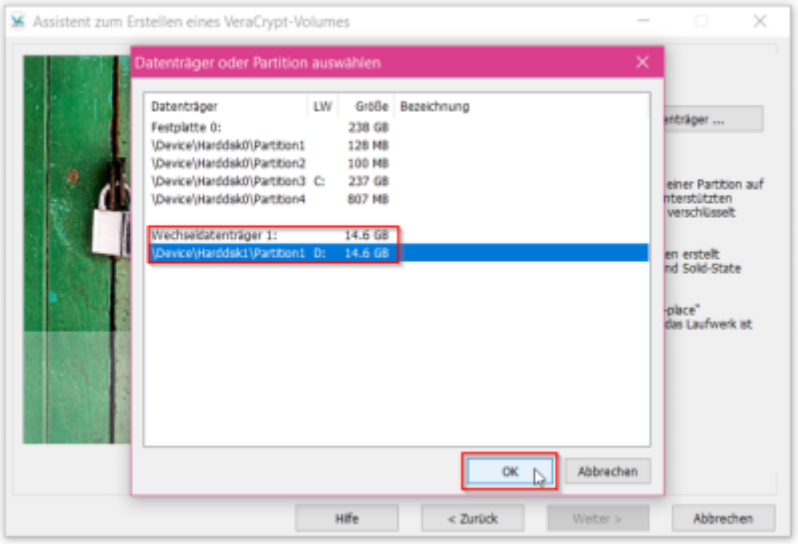
Verschlüsselten Datenträger öffnen Nach dem Anstecken des Datenträgers solltest du direkt nach dem Passwort gefragt werden.



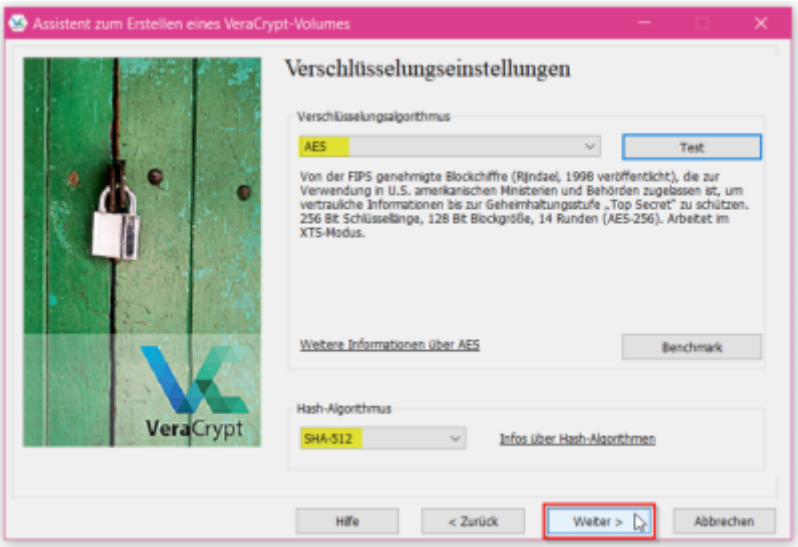
Linux, Windows, Mac: Datenträger verschlüsselung (Veracrypt)

⇒ Veracrypt installieren und starten
⇒ Unter *Volumes* wähle *Create New Volume* aus
⇒ *Create a volume within a partition/drive* auswählen

⇒ *Standard Veracrypt Volume* auswählen
⇒ Den Datenträger auswählen - *Select Device* (Hier werden dir alle Datenträger angezeigt die an den Computer angeschlossen sind - am Besten kannst du dein gewünschtes Device auswählen wenn du die Größe deines USB-Sticks/Datenträgers kennst.)



⇒ Es erscheint ein Dialog mit einer Warnung: Durchlesen und mit *Ja* beantworten.
⇒ Algorithmen auswählen (AES und SHA-256 sind in Ordnung)



⇒ Gib ein sicheres Passwort ein.
Tipps wie du ein sicheres Passwort erstellen kannst findest du hier.

⇒ *Format Option*: Hier können unterschiedliche Formatierungen ausgewählt werden. Wir empfehlen exFat,da es von allen Betriebssystemen gelesen werden kann und große Dateien unterstützt.
⇒ Wähle aus ob du Dateien größer als 4GB speichern können willst: Im Normalfall kannst du hier „Nein" auswählen. Dadurch verändern sich die Formatierungsoptionen))
⇒ Cross-Plattform Support: Das ist eine Überprüfung, ob auch das richtige Format ausgewählt wurde. exFat sollte für alle Betriebsystem funktionieren.
⇒ Formatieren: Nun kannst du auf *formatieren* klicken.

Schritt für Schritt Anleitungen mit Bildern

Wie du einen ganzen Datenträger verschlüsseln kannst, findest du hier auf deutsch bei Heise: Externe Speicher verschlüsseln

Eine Anleitung auf englisch findest du bei freedom.press: Veracrypt Guide in English

Andere gute Anleitung findest du bei der Universität Mannheim:Veracrypt-Anleitung Uni Mannheim

---

Verschlüsselten Datenträger öffnen (Veracrypt)

Um einen mit Veracrypt verschlüsselten Datenträger zu öffnen muss er zuerst wieder über Veracrypt entschlüsselt werden.

⇒ VeraCrypt starten
⇒ Zahl/Buchstaben auswählen
Bei Linux einfach eine Zahl auswählen, Bei windows sind es Buchstaben.
⇒ “Select Device” und den Datenträger auswählen
⇒ „mount”
⇒ Passwort eingeben und “Ok” klicken (Achtung bei manchen Betriebssystemen wirst du auch nach dem Administor:innen-Passwort gefragt: Lies genau welches Passwort du eingeben sollst, sonst kann es leicht dazu kommen, dass du dich wunderst, dass die Meldung kommt dass das Passwort falsch sei.)
⇒ Nun kannst du darauf normal zugreifen

Warnmeldung bei macOS: Beim Anstecken eines veracrypt verschlüsselten Datenträger eine Warnung - die kann ignoriert werden.

MacOS: Datenträger verschlüsseln

Aktiviere FileVault in deinem Betriebssystem. Anleitung von Apple für FileVault

Eine gute Alternative ist das Programm VeraCrypt.

Einzelne Ordner verschlüsseln

Du kannst auch einen Ordner („Container“) erstellen und deine Daten darin ablegen, anstatt die ganze Festplatte zu verschlüsseln. Dieser Container ist einfach nur ein Ordner, der von uns im vorhinein eine Größe zugewiesen bekommt und nur noch mit einem Passwort über Veracrypt geöffnet werden kann. Du kannst die Datei dann über Veracrypt (und mit deinem Passwort) öffnen. Die Datei erscheint dann wie ein angesteckter USB Stick.

Dann musst du natürlich darauf achten keinerlei kritische Daten außerhalb des Containers zu belassen, was nicht immer ganz einfach ist. Wir würden dir also empfehlen das ganze System zu verschlüsseln.

⇒ VeraCrypt installieren und starten
⇒ “Create Volume” klicken
⇒ “Create an encrypted file container” anwählen und “Next” klicken
⇒ “Standard VeraCrypt volume”
⇒ Einen Speicherort und Dateinamen für deinen Container auswählen, den Haken bei “Never save history” belassen
⇒ Algorithmen auswählen (AES und SHA-256 sind in Ordnung)
⇒ Größe des Containers festlegen
⇒ Passwort eingeben (siehe dazu Passwortsicherheit)
⇒ Ein Dateisystem auswählen (FAT ist in Ordnung) und die Maus möglichst zufällig durch das Fenster bewegen bis der grüne Balken voll ist, dann “Format”
⇒ Abwarten bis die Erstellung abgeschlossen ist und mit “Exit” das Programm verlassen

Veracryt auf Microsoft Windows: Eine auführliche Anleitung [English] wie du Veracrypt auf Windows installieren und verwenden kannst findest du bei Veracrypt auf Windows by "Security in a Box"

Container mit VeraCrypt öffnen

Damit ihr jetzt euren Container öffnen könnt, müsst ihr in Veracrypt im Menü “Volumes” eine “Datei auswählen” und dann noch einen Laufwerksbuchstaben (unter windows) festlegen. Das heisst nachdem ihr die Datei ausgewählt habt klickt ihr im Hauptfeld des Programms auf einen Buchstaben eurer Wahl, und klickt dann links unten auf “Einbinden”. Jetzt gebt ihr das Passwort ein und wartet etwas. Der Container taucht jetzt als Festplatte im System auf. Alles was ihr darauf speichert ist verschlüsselt.

⇒ VeraCrypt starten
⇒ Freien Laufwerksbuchstaben oder Zahl auswählen
⇒ “Select File” und die Containerdatei auswählen
⇒ “Mount”
⇒ Passwort eingeben und “Ok” klicken

Verschlüsselung und Cloud (Cryptomator)

Um Dateien verschlüsselt in der Cloud abzuspeichern gibt es verschiedene Möglichkeiten. Die Einfachste ist es wohl einen verschlüsselten Container:Container mit VeraCrypt (Windows und Linux), wie oben beschrieben zu erstellen. Diesem kannst du dann einfach in die Cloud verschieben. Weil der Container auf dem Computer mit dem du zugreifst entschlüsselt/verschlüsselt wird und nicht in der Cloud selber, ist er sicher - wie immer gilt, wenn der Computer mit dem du arbeitest und dein Passwort sicher ist.

Als Alternative empfehlen wir das OpenSource Programm „Cryptomator“. Eine Anleitung wie du Cryptomator am besten verwenden kannst findest du hier auf der Webseite von Heise oder die Anleitung zu Cryptomator von der Universität Mannheim.

Zum Weiterlesen

Ausführliche Anleitungen by "Security in a Box", für Linux und Windows.