

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

- >

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.

-

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

Version #1

Erstellt: 8 Februar 2025 17:42:31 von ESC-IT Migration Bot

Zuletzt aktualisiert: 8 Februar 2025 17:42:31 von ESC-IT Migration Bot