

VeraCrypt

Disclaimer: Dieses nette Handout ist nicht vollständig und klammert viele Features von VeraCrypt aus. Es stellt lediglich einen konkreten, aber nach Meinung der Autoren, einfachen, relativ sicheren Weg dar, um einen Crypto-Container anzulegen und zu benutzen.

1 Download und Installation

1.1 Windows und Mac OS X

- Download von der Website: <https://veracrypt.codeplex.com/>
- Download verifizieren, z.B. mit dem PGP Key von VeraCrypt (ebenfalls auf der Website verfügbar).
- Wie üblich, den Installer ausführen

1.2 Ubuntu und Derivate

```
$ sudo add-apt-repository ppa:unit193/encryption
$ sudo apt-get update
$ sudo apt-get install veracrypt
```

2 Anlegen eines Containers

- Im Hauptfenster „Create Volume“ auswählen und wie folgt vorgehen (nach jedem Schritt mit „Next“ zum nächsten Dialog wechseln):
- „Create an encrypted file container“ auswählen
- „Standard VeraCrypt volume“ (erste Option) auswählen
- „Create an encrypted file container“ auswählen
- Speicherort auswählen. Achtung: Cloud-Dienste (z.B. Dropbox können den Container beschädigen, wenn dieser von mehreren Rechnern aus genutzt wird).
- Verschlüsselungs- und Hash-Algorithmus auswählen. Wir empfehlen AES(Twofish) für die Verschlüsselung und SHA-512 als Hash-Algorithmus.
- Die Größe des Containers festlegen. Für einfache Dokumente reichen 5GB. Für Bilder, Videos, etc. sollten mindestens 50GB reserviert werden.
- Vielleicht die schwierigste Einstellung: es muss ein Passwort festgelegt werden. Es sollte hinreichend sicher sein und nicht vergessen werden! Alternativ kann man eine (oder mehrere) Dateien als Schlüssel wählen (diese sollten natürlich auch nicht gelöscht werden).
- Schließlich muss noch ein Dateisystem-Typ ausgewählt werden. Soll von mehreren Betriebssystemen auf den Container zugegriffen werden, empfiehlt sich FAT. Sonst ist NTFS (Windows) bzw. Ext4 (Linux) die bessere Wahl, weil sich größere Dateien anlegen lassen.
- Im letzten Dialog nun auf „Format“ klicken. Eventuell müsst ihr vorher eine Weile warten, bis genug Entropie gesammelt wurde.
- Danach könnt ihr noch einen Container anlegen, oder mit „Exit“ zum Hauptfenster zurückkehren.

3 Einbinden eines Containers

- Einen freien Slot (Linux) oder ein freies Laufwerk (Windows) im Hauptfenster auswählen.
- Mit „Select File...“ den gewünschten Container auswählen.
- Schließlich mit „Mount“ den Container einbinden. Im Passwort-Dialog genügt es das Passwort einzugeben (oder die Schlüsseldateien auszuwählen) und mit „OK“ zu bestätigen.
- Unter Linux steht der Container nun unter dem angezeigten Pfad zur Verfügung; unter Windows findet sich entsprechend ein neues Laufwerk.
- Durch einen Rechtsklick auf einen Slot (bzw. Laufwerk) und die Auswahl von „Dismount“ kann ein Container freigegeben werden.