Dateiverschlüsselung

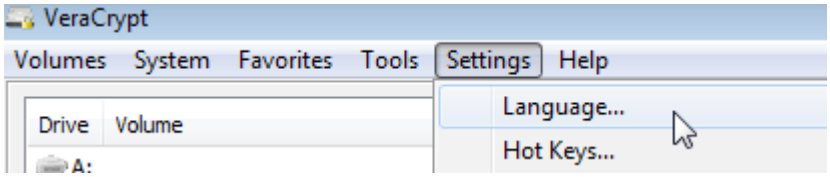
VeraCrypt kann ganze Datenträger, einzelne Partitionen oder Container verschlüsseln. Container kann man sich als passwortgeschützte Ordner vorstellen.

Schritt 1: Software installieren

VeraCrypt kann unter https://www.veracrypt.fr/en/Downloads.html für GNU/Linux, Windows und macOS heruntergeladen werden.

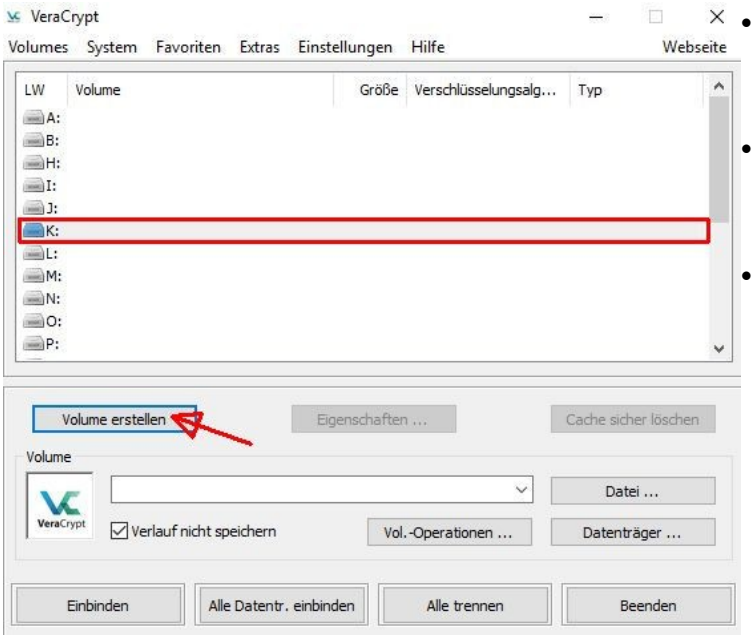
Schritt 2: Sprache ändern

Beim ersten Start ist die Oberfläche von VeraCrypt standardmäßig englischsprachig. Die Sprache kann über das Menü geändert werden: ***Settings*** (Einstellungen)→ ***Language*** (Sprache)



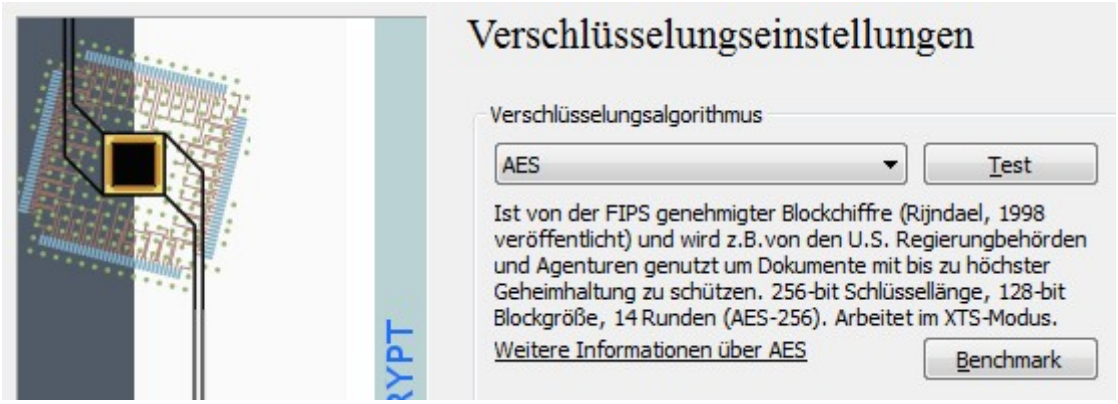
Schritt 3: Container erstellen

- Zuerst musst du (unter Windows) einen freien Laufwerksbuchstaben auswählen („LW“). Welche Buchstaben verfügbar sind, ist von deiner individuellen Situation abhängig. Später benötigst du diesen Buchstaben, um den Container einzubinden (dazu Schritt 4). Der Container muss nicht jedes Mal mit dem gleichen Laufwerksbuchstaben eingebunden werden, aber es kann hilfreich sein, den Buchstaben nicht zu wechseln. Unter Linux und macOS gibt es keine Laufwerksbuchstaben, VeraCrypt zeigt stattdessen *slots*, die keine weitere Bedeutung haben.



- Danach klickst du auf ***Volume erstellen*** (volume: englisch für „Datenträger“)
- Im sich neu aufgebauten Fenster klickst du unten zweimal auf ***Weiter***
- Unter ***Datei…*** legst du den Namen und den Speicherort für die Containerdatei fest

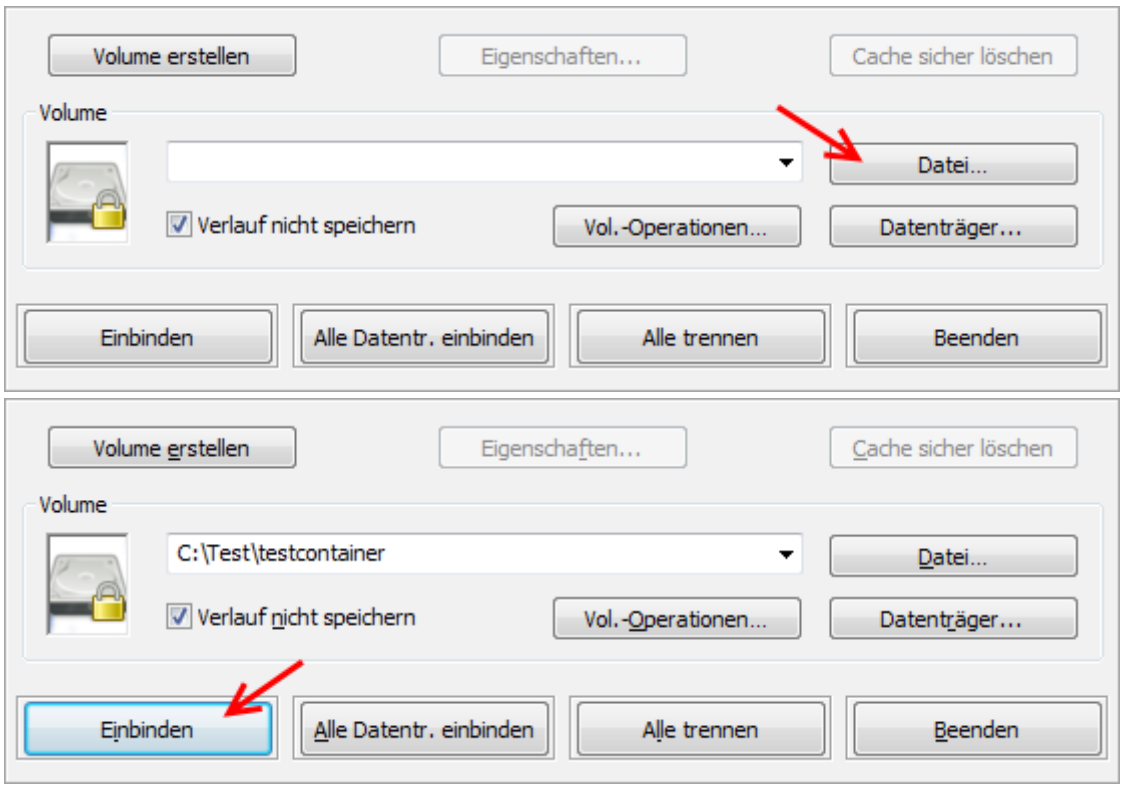
- Im folgenden Dialog kannst du auch die Verschlüsselungsart einstellen. Standardmäßig muss aber nichts geändert werden:



- Als Nächstes legst du die Größe des Containers fest, also wieviel Speicherplatz für Dateien der Container bieten soll.
- Dann gibst du ein Passwort an, mit dem der Container ver/-entschlüsselt wird. Merke dir dieses Passwort gut: Wenn du es vergisst, ist der Inhalt des Containers verloren.
- Dann wird der Container formatiert. Die Verschlüsselung benötigt Zufallszahlen, dafür bewegst du den Mauszeiger mindestens 30 Sekunden lang über das VeraCrypt-Fenster. Anschließend auf ***Formatieren*** klicken. Der verschlüsselte Container wird nun erstellt.

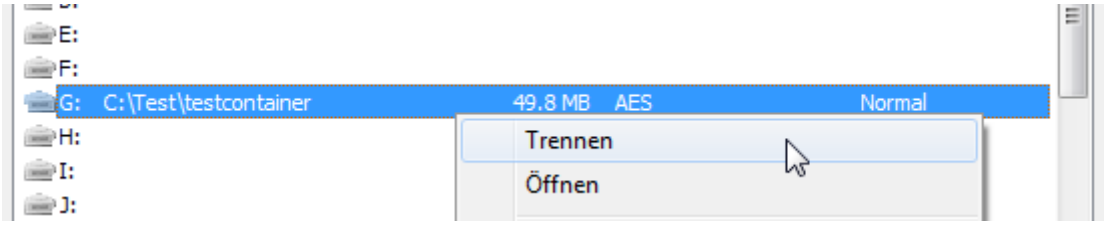
Schritt 4: Container öffnen

- Über ***Datei*** wählst du den Container aus:



- Auf ***Einbinden*** klicken:
  - Passwort eingeben und bestätigen

- **Rechtsklick** auf den neuen Eintrag im VeraCrypt-Fenster:
  – Durch ***Öffnen*** greifst du auf den Container zu
  – Durch ***Trennen*** wird er geschlossen



Weiterführende Hinweise

Was ist der Unterschied zwischen einem Standard- und einem verstecktem VeraCrypt-Volume?

- Ein Standard-Volume ist die Containerdatei an sich, mit deren Hilfe Dateien verschlüsselt werden können.
- Ein verstecktes Volume ist ein Container im Container. Man sieht nur den äußeren Container, aber nicht den inneren. Es werden zwei Passwörter benötigt. Je eines für den jeweiligen Container. Im sichtbaren Container befinden sich – idealerweise – Dateien, die notfalls auch preisgeben werden können. Im versteckten Container befinden sich die Daten, die nicht preisgegeben werden sollen! (Rechtslage: Es gibt Länder, in denen ist man zur Herausgabe des Passworts gegenüber Behörden verpflichtet; in Deutschland ist das zur Zeit nicht der Fall.)
- Je nachdem, welches der beiden Passwörter eingegeben wird, wird der jeweilige Container entsperrt.
- Glaubwürdige Abstreitbarkeit: Für Außenstehende ist nicht erkennbar, ob es sich bei einem Bereich eines Containers um überschriebenen freien Speicherplatz oder einen versteckten Container handelt.

Sichere Passwörter auswählen

- Die beste Verschlüsselung nutzt nichts, wenn das Passwort unsicher ist. Deshalb unbedingt ein gutes Passwort wählen. Näheres im Handout „KeePassXC“.

Administratorrechte

- Um mit VeraCrypt zu arbeiten, benötigt man an einem Windows-PC Administratorrechte. An anderen Windows-Geräten einen Container zu ver-/entschlüsseln, ist nicht ohne Administratorrechte möglich.
- Hier gibt es aber einen einfachen Trick, mit dem man sich helfen kann: Einfach die „portable Version“ von VeraCrypt herunterladen. Diese kann z.B. von einem USB-Stick gestartet werden und so die Container ver-/entschlüsseln.
- Die portable Version findest du direkt unter dem Installer für Windows auf der Website von VeraCrypt: https://www.veracrypt.fr/en/Downloads.html

- ***Windows***: VeraCrypt Setup 1.22.exe (29.6 MB) (PGP Signature)
  - Portable version: VeraCrypt Portable 1.22.exe (29.4 MB) (PGP Signature)
- ***Mac OS X***: VeraCrypt 1.22.dmg (11.1 MB) (PGP Signature)
  - **OSXFUSE** 2.5 or later must be installed.
- ***Linux***: veracrypt-1.22-setup.tar.bz2 (14.6 MB) (PGP Signature)

Verschlüsselung eines/r USB-Sticks/Festplatte oder Systemlaufwerks

- Um einen USB-Stick oder eine externe Festplatte sowie ein Systemlaufwerk (auf dem das Betriebssystem installiert ist) zu verschlüsseln, wird Schritt 3 – Volume erstellen – wiederholt. Anstelle der Erstellung eines verschlüsselten Containers wählst du im Menü die gewünschte Alternative aus.

- **Wichtig: Bevor du ein externes Speichermedium oder dein Betriebssystem verschlüsselst, erstelle unbedingt ein Backup deiner Dateien!**

Weiterführende Links

- Eine weitere Anleitung zu VeraCrypt gibt es von Mike Kuketz unter https://www.kuketz-blog.de/veracrypt-daten-auf-usb-stick-sicher-verschluesseln/ (zuletzt abgerufen am 18.09.2018).
- Linux-Nutzer.innen, die lieber mit dm-crypt/LUKS Daten sicher verschlüsseln möchten, finden ebenfalls eine Anleitung von Mike Kuketz unter: https://www.kuketz-blog.de/dm-crypt-luks-daten-unter-linux-sicher-verschluesseln/ (zuletzt abgerufen am 15.12.2021).