Dateiverschlüsselung

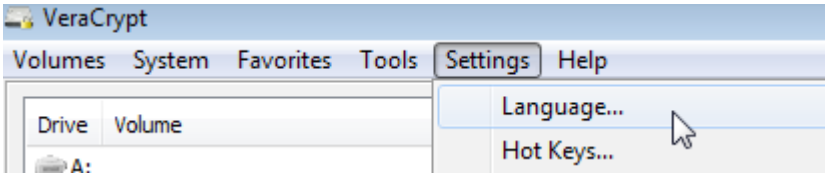
VeraCrypt kann ganze Datenträger, einzelne Partitionen oder Container verschlüsseln. Container kann man sich dabei als passwortgeschützte Ordner vorstellen.

Schritt 1: Software installieren

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

Schritt 2: Sprache ändern

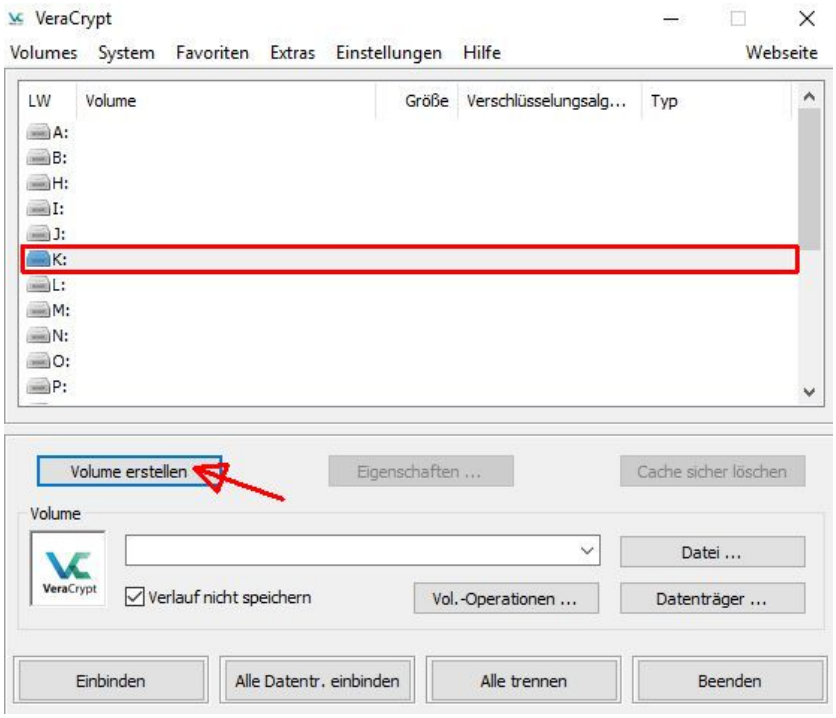
Beim ersten Start ist die Oberfläche von VeraCrypt standardmäßig englischsprachig. Die Sprache kann oben im Menü auf Deutsch geändert werden, wenn man auf **"Settings"** klickt und dann auf **"Language...":**



Schritt 3: Container erstellen

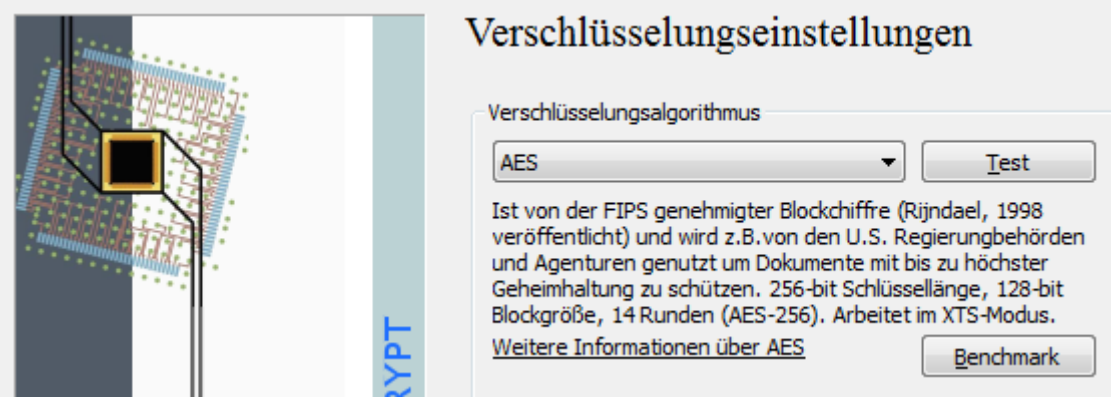
- Zuerst musst du einen freien Buchstaben auswählen (Hinweis: Die noch verfügbaren Buchstaben können auf jedem Computer anders aussehen. Das richtet sich danach, ob bereits in deiner Dateiverwaltung einige Buchstaben belegt sind). Später benötigst du diesen Buchstaben, um den Container einzubinden (dazu Schritt 4). (Hinweis: Es ist auch möglich, den Container später unter einem anderen Laufwerksbuchstaben einzubinden)

- Danach klickst du auf **"Volume erstellen"**, Volume ist englisch für „Datenträger“:



- Im sich neu aufgebauten Fenster klickst du unten zweimal auf "**Weiter**".
- Unter "**Datei...**" legst du fest, wie der Container benannt wird und wo er gespeichert werden soll.

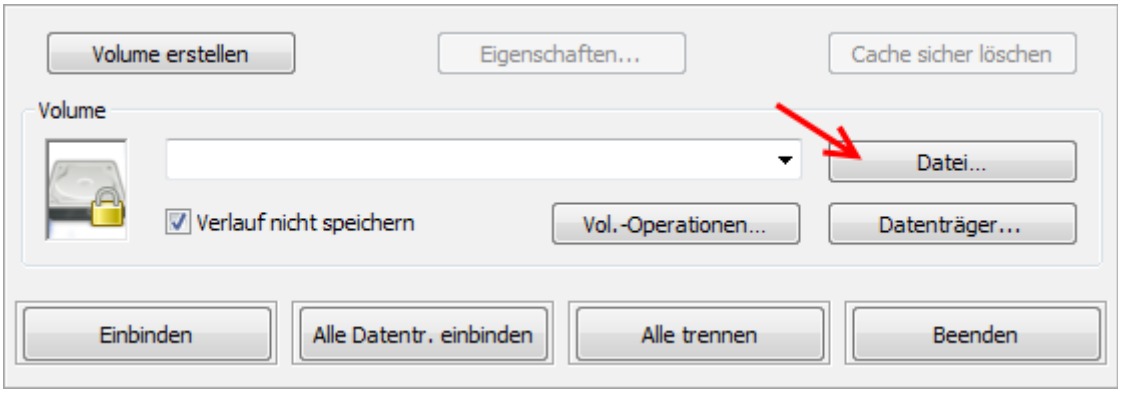
- Hier kann man auch die Verschlüsselungsart einstellen. Standardmäßig musst du aber nichts ändern:



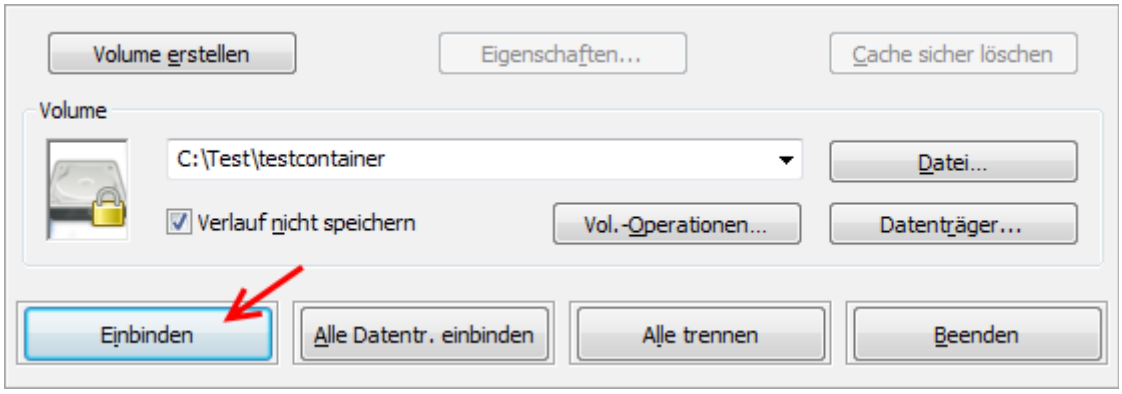
- Dann legst du die Größe des Containers fest.
- Als Nächstes musst du ein Passwort eingeben, mit dem der Container ver/-entschlüsselt wird.
- Dann kannst du das Dateisystem einstellen. Bewege den Mauszeiger für mind. 30 Sekunden zufällig über das VeraCrypt-Fenster. Anschließend auf "**Formatieren**" klicken. Der verschlüsselte Container wird nun erstellt.

Schritt 4: Container öffnen

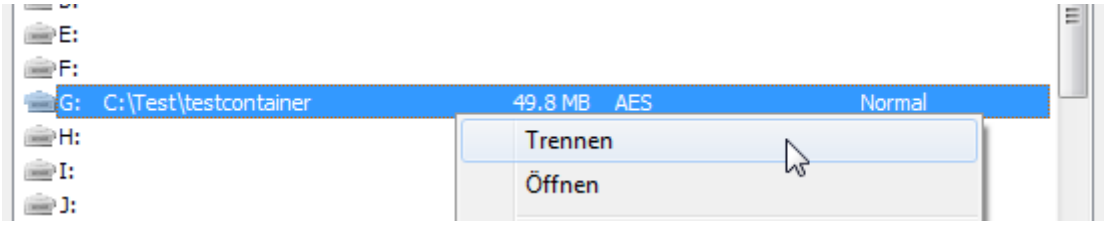
- Über "**Datei**" wählst du den Container aus:



- 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-Volume und einem verstecktem VeraCrypt-Volume?

- Ein Standardvolume ist die Containerdatei an sich, mit deren Hilfe ihr eure Dateien verschlüsseln könnt.
- Ein verstecktes Volume ist ein Container im Container. Man sieht nur den äußeren Container, aber nicht den inneren. Ihr benötigt zwei Passwörter für die jeweiligen Container. Im sichtbaren Container befinden sich – idealerweise – Dateien, die ihr notfalls auch preisgeben könnt. Im versteckten Container befinden sich die Daten, die ihr nicht preisgeben möchtet. (Hinweis: Bitte beachtet, dass es Länder gibt, in denen ihr zur Herausgabe des Passworts gegenüber Behörden verpflichtet seid; in Deutschland ist dieses z. Zt. 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 euch nichts, wenn euer Passwort schlecht ist. Deshalb wählt unbedingt ein gutes Passwort.

Administratorrechte

- Um mit VeraCrypt zu arbeiten, brauchst du an einem Windows-PC Administratorrechte. Falls das nicht geht, lade dir einfach die „portable version“ von VeraCrypt herunter. Diese kannst du z.B. von einem USB-Stick starten und so deine Container ver-/entschlüsseln. Die „portable version“ findest du auch auf der Homepage von VeraCrypt: https://www.veracrypt.fr/en/Downloads.html

Verschlüsselung eines/r USB-Sticks/Festplatte oder Systemlaufwerks

- Um deinen USB-Stick oder deine externe Festplatte sowie dein Systemlaufwerk (auf dem dein Betriebssystem ist) zu verschlüsseln, wiederhole Schritt 3 – Container öffnen. Anstelle der Erstellung eines verschlüsselten Containers, wählst du eine andere Art der Verschlüsselung 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/

- Linux-Nutzer, welche lieber mittels 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/