VeraCrypt – Container und Datenträger

Installation (Debian)

VeraCrypt ist nicht in jeder Debian-Paketquelle verfügbar. Ein für das System geeignetes Paket muss aus einer vertrauenswürdigen Quelle bezogen und überprüft werden.

veracrypt.fr
github.com

Download

```
wget https://launchpad.net/veracrypt/trunk.....deb
```

Pfad & Dateiname holen unter https://www.veracrypt.fr/en/Downloads.html und ersetzen.

Installation

```
sudo apt install ./veracrypt-console-.....deb
```

Nach der Installation:

```
veracrypt --version
```

Zweck und Funktionsprinzip

VeraCrypt verschlüsselt Containerdateien, Partitionen und Datenträger. Die Nutzdaten werden symmetrisch verschlüsselt; eine Passphrase und gegebenenfalls Keyfiles dienen dazu, die erforderlichen Schlüssel freizugeben.

Typische Einsatzfälle

- Transportabler verschlüsselter Datei-Container
- Verschlüsselter USB-Datenträger
- Schutz von Daten im ausgeschalteten beziehungsweise ausgehängten Zustand

Container erstellen

Die grafische Oberfläche führt durch Containergröße, Algorithmus, Passwort und Dateisystem. Vor der Einrichtung eines Datenträgers sind vorhandene Daten zu sichern: Eine falsche Geräteauswahl kann Daten zerstören.

Linux-Kommandozeile

VeraCrypt bietet eine CLI. Vorher die verfügbaren Optionen der installierten Version prüfen:

```
veracrypt --help
```

Beispiel für das Einhängen eines **bereits vorhandenen** Containers (Passphrase wird interaktiv abgefragt):

```
veracrypt --text --mount /pfad/container.hc /mnt/veracrypt
```

Dateien im eingebundenen Container anzeigen:

```
ls -la /mnt/veracrypt
```

Aushängen:

```
veracrypt --text --dismount /mnt/veracrypt
```

Die Einhängeoptionen hängen von Version, Rechten und Containerformat ab.

Sicherheit

Ein eingebundener Container ist für berechtigte Prozesse im laufenden System zugänglich. Verschlüsselung schützt nicht gegen Schadsoftware, die während des Betriebs mit Benutzerrechten auf die Daten zugreift. Container vor dem Abziehen von Datenträgern sauber aushängen.

Wenn es wirklich sicher sein muss:
a) VeraCrypt kann ein **verstecktes Laufwerk** (hidden volume) erstellen. Dabei werden zwei verschiedene Passwörter für den selben Container vergeben. Und je nach Passworteingabe wird das sichtbare oder das versteckte Volumen geöffnet. Veracrypt empfiehlt, während der Installation in das sichtbare Laufwerk einige Daten zu legen, die vermeintlich wichtig sind - falls man **ein** Passwort, z.B. bei Entführung, verraten muss. Erst anschließend wird das versteckte Volumen erstellt. Das sichtbare Volumen sollte man dann nicht mehr verändern (keine neuen Daten aufspielen), weil dadurch das versteckte Volumen zerstört werden könnte.

b) Liegt der verschlüsselte Container auf einem entfernten Server, dann sollte dieser nicht auf dem Server „geöffnet“ werden, sondern auf dem lokalen System. Dadurch wird nur der verschlüsselte Container Online übertragen und nicht die darin enthaltenen Dateien bzw. Daten, wodurch die Datenübertragung zusätzlich gesichert ist. Die räumliche Trennung von Containerablage (auf dem Server) und Passworteingabe (auf dem lokalen System) macht zusätzlich Sinn, damit das PW nicht in irgendeinem Zwischenspeicher auf dem Server erhalten bleiben kann.

c) In der Standardeinstellung von Veracrypt bleibt die **Änderungszeit** der Containerdateien erhalten, auch wenn deren Inhalt verändert wurde. Dadurch ist auch der Zeitpunkt der letzten Änderung von außen nicht sichtbar.
Einstellung über die GUI-Anwendung: Einstellungen → Voreinstelllungen → „Änderungszeiten von

Containerdateien erhalten“.
Hinweis: Soll jedoch von einer Containerdatei regelmäßig ein Backup erstellt oder diese synchronisiert werden (Nextcloud, etc.), kann ggf. nicht erkannt werden, ob sich innerhalb des Containers Änderungen ergeben haben und der Vorgang kann scheitern. Lösung: Auf betroffenen Systemen o.a. Änderungszeiten … erhalten → **abschalten**. Die Änderung bezieht sich auf das System und nicht auf den Container!

Wiederherstellung

Passphrase, verwendete Keyfiles und gegebenenfalls ein gesicherter Volume-Header sind kritisch. Ohne diese Daten kann ein Container dauerhaft unzugänglich sein. Backups des verschlüsselten Containers und Wiederherstellungsversuche regelmäßig prüfen.

Zurück zur Übersicht

From:
https://wiki.bluegnu.de/ - **wiki**

Permanent link:
https://wiki.bluegnu.de/doku.php/open:it:secure:veracrypt

Last update: **2026/11/15 20:52**