Akademie
für Lehrerfortbildung
und Personalführung

VeraCrypt

IT-Qualifizierung
für Lehrkräfte

Datenverschlüsselung in der Schule

Impressum

Herausgeber:	Akademie für Lehrerfortbildung und Personalführung Kardinal-von-Waldburg-Str. 6-7 89407 Dillingen
Autoren:	Georg Schlagbauer, Akademie Dillingen Wolfgang Plank, Goethe-Gymnasium Regensburg
URL:	http://alp.dillingen.de/schulnetz
Mail:	schlagbauer@alp.dillingen.de
Stand:	Januar 2016

VeraCrypt

Datenverschlüsselung in der Schule

Inhalt

Einführung

Elektronisch gespeicherte Daten haben eine immer größere Bedeutung und deshalb muss auch dem Datenschutz und der Datensicherheit immer mehr Beachtung geschenkt werden. Die Datensicherheit versucht dem möglichen Verlust der Daten vorzubeugen. Dagegen helfen ausgefeilte Strategien zur Datensicherung. Daten werden auf Wechselmedien oder auf eigenen verteilten Backupservern gespeichert, wodurch das Risiko des möglichen Verlustes reduziert wird. Der Datenschutz möchte die Daten vor Missbrauch schützen und besteht deshalb auf eine sparsame Verwendung und sichere Verwahrung der Daten. Das Recht auf Datenschutz ist im Grundgesetz verankert. So ist auch bei einer Datensicherung, die meist eine Vervielfältigung darstellt, darauf zu achten, dass keine Personen darauf zugreifen können, die selbst ein Interesse an diesen Daten haben. Daneben gibt es gerade bei mobilen Datenträgern beliebig viele Möglichkeiten, dass diese in fremde Hände gelangen könnten.

Eine Möglichkeit, sensible Daten vor fremdem Zugriff zu schützen, ist, diese Daten nur verschlüsselt aufzubewahren oder nur verschlüsselt zu transportieren.

Das Programm VeraCrypt bietet diese Möglichkeit. Es stellt eine Weiterentwicklung des bekannten Programms TrueCrypt dar und ist in der aktuellen Version teilweise dazu kompatibel (https://de.wikipedia.org/wiki/VeraCrypt). Es bietet eine hohe Sicherheit und gleichzeitig genügend Komfort im praktischen Einsatz. Es ist ein Open Source-Programm und für die gängigen Betriebssysteme Windows, Linux und MacOS erhältlich. Die Daten werden dabei in einem verschlüsselten Container abgelegt, der mit einem Passwort gesichert ist. Im Dateisystem ist dieser Container eine ganz normale Datei, die zunächst mit Zufallszahlen gefüllt ist. Nach dem Öffnen des Containers wird dieser unter Windows als Laufwerk angeboten, unter Linux lässt er sich an beliebiger Stelle in den Dateibaum einhängen. Wird der Container wieder geschlossen, präsentiert er sich als eine einzige Datei, in der alle Dokumente verschlüsselt abgelegt sind. Es lässt sich nicht erkennen, welche oder wie viele Dokumente darin verborgen sind. Lediglich aus der Größe des Containers im Dateisystem lassen sich Vermutungen über die maximale Menge der darin enthaltenen Daten anstellen.

Der verschlüsselte Datencontainer kann in die normale Sicherungskette aufgenommen werden. Dadurch wird die Gefahr reduziert, dass die Daten verloren gehen. Die Verschlüsselung des Datencontainers schützt vor Missbrauch. Ohne das Passwort ist niemand in der Lage, die Daten zu entschlüsseln.

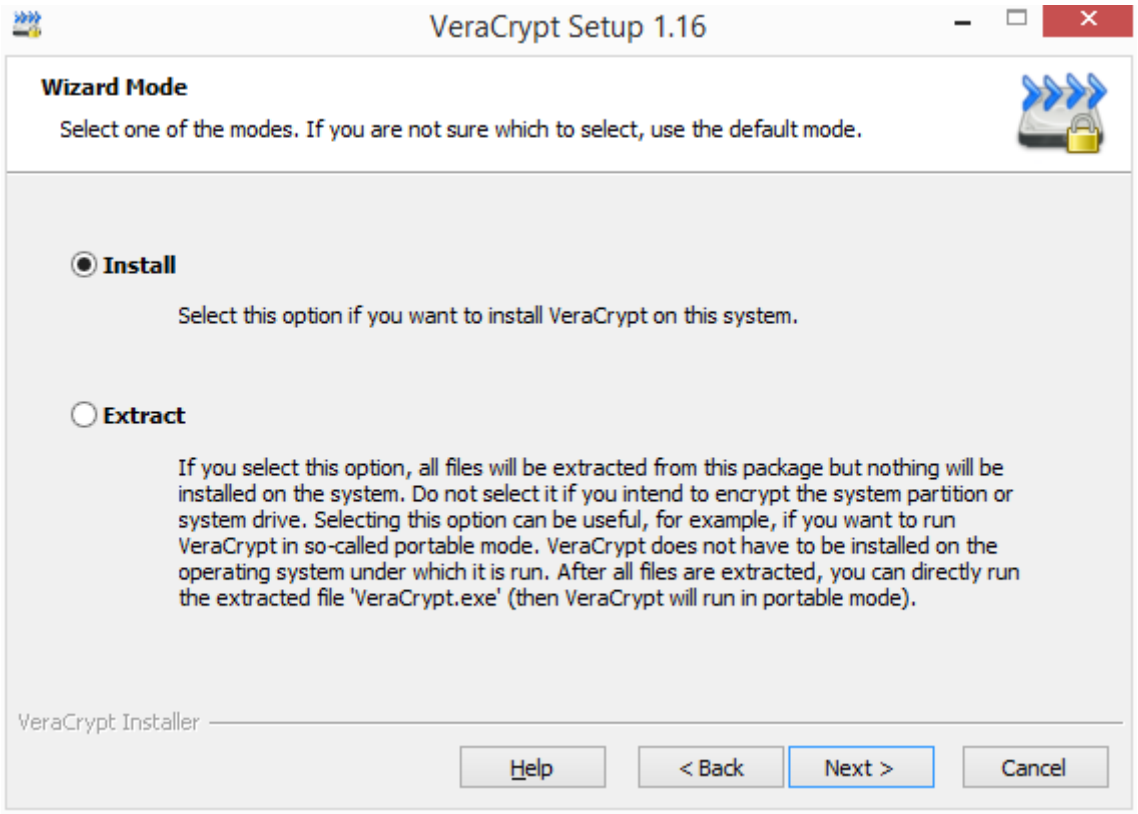
Neben verschlüsselten Datencontainern, die auf Dateiebene erzeugt werden, bietet VeraCrypt auch die Möglichkeit, ganze Partitionen einer Festplatte oder einen gesamten USB-Stick zu verschlüsseln. Wenn ein verschlüsselter USB-Stick verloren geht, erhält der „Finder“ nicht einmal einen Hinweis, dass es sich hier um ein verschlüsseltes Medium handelt. Windows bringt z. B. nur die Meldung, dass der Datenträger nicht formatiert ist.

VeraCrypt speichert die Daten auf der Festplatte immer verschlüsselt. Selbst nach einem plötzlichen Stromausfall oder nach dem Ausschalten des PC liegen die Daten nur verschlüsselt vor. Wird ein Dokument aus einem geöffneten Container von einem Programm geladen, so wird es von VeraCrypt im Hintergrund entschlüsselt und dem Programm angeboten. Umgekehrt werden die Daten bevor sie auf der Festplatte abgelegt werden wieder verschlüsselt.

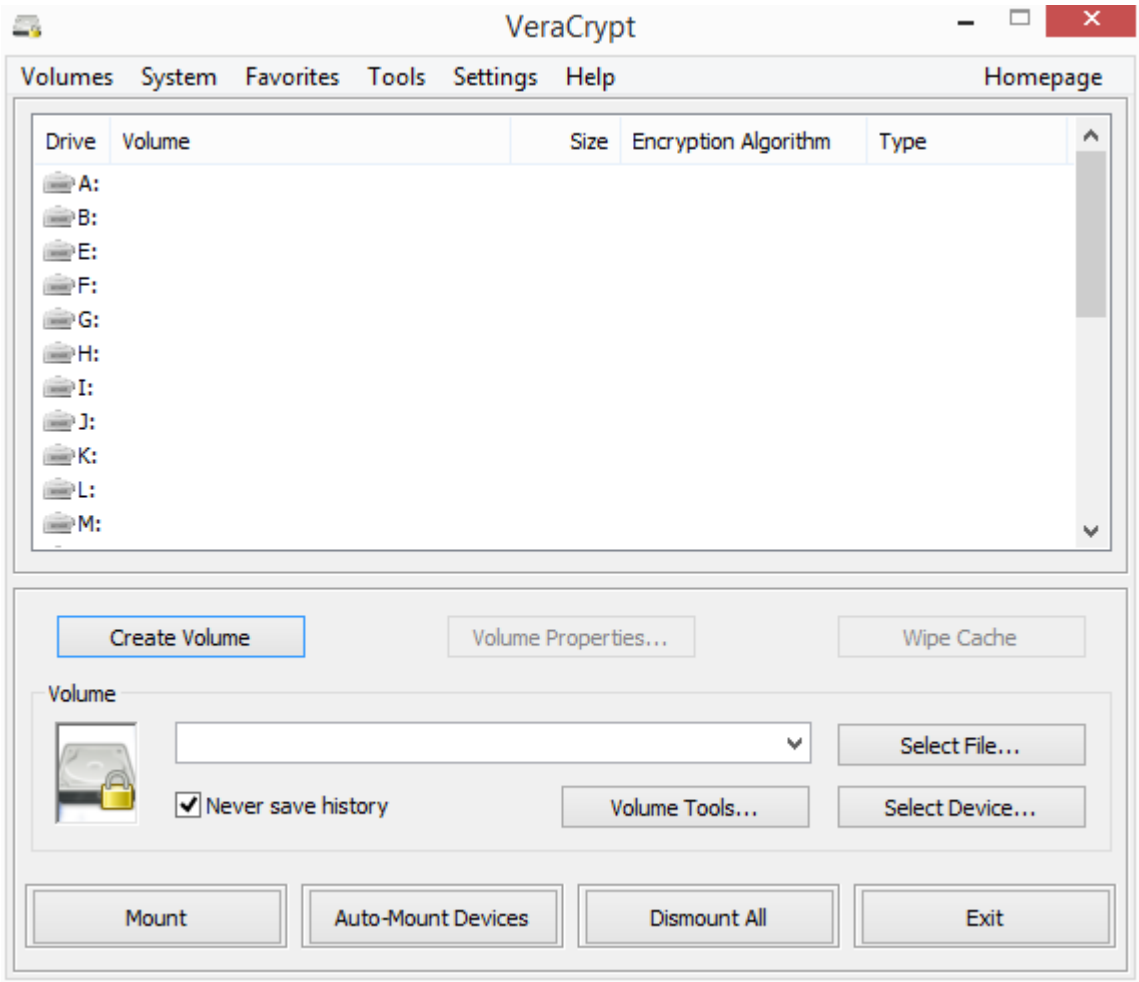
Installation von VeraCrypt unter Windows

VeraCrypt erhält man zum Download unter https://veracrypt.codeplex.com/

Bei der Installation wird angeboten, das Programm zu installieren oder die Dateien nur auszupacken. Der letztere Punkt ist interessant, wenn VeraCrypt als „Portable Application“ auf einem USB-Stick betrieben werden soll. VeraCrypt nennt dies „portable mode“. Beim Installieren sind Administratorrechte nötig. VeraCrypt lässt sich auch in einem „portable mode“ (ohne Installation) auf einem Rechner ausführen. Dabei sind jedoch bei jedem Start von VeraCrypt Administrationsrechte notwendig.



Erzeugen eines verschlüsselten Containers

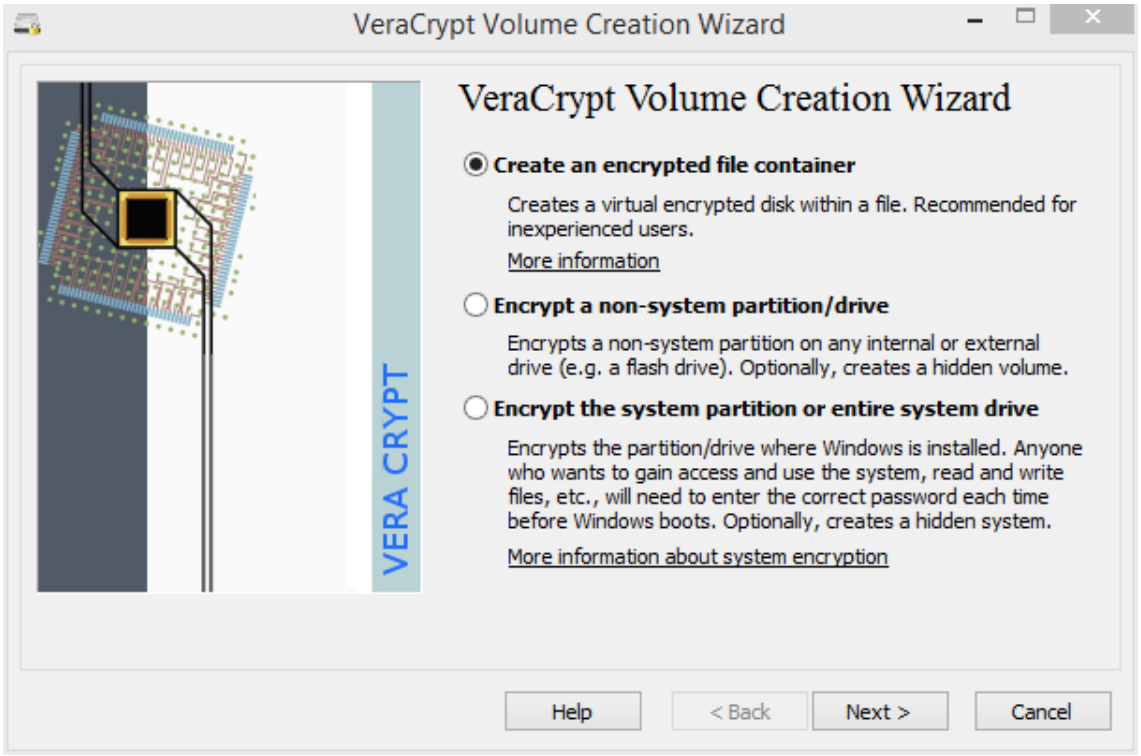


Über den Button „Create Volume“ erzeugt man mit Hilfe eines Assistenten einen verschlüsselten Container. Dieser beinhaltet später die vertraulichen Daten. Beim Einrichten eines Containers bietet VeraCrypt verschiedene Optionen an:

- Neben einem einfachen Datei-Container lässt sich auch eine ganze Datenpartition oder sogar die Systempartition verschlüsseln.
- Innerhalb eines bereits existierenden Containers lässt sich ein „Hidden Volume“ anlegen. Dabei werden nicht nur die darin enthaltenen Daten verschlüsselt, es ist auch nicht erkennbar, dass ein solcher Bereich existiert. Auf die Sicherheit der Verschlüsselung hat ein Hidden Volume keinen Einfluss.
- Bei einem Dateicontainer ist der Name und Speicherort der Datei zu bestimmen. VeraCrypt verzichtet dabei auf eine Dateiendung, so dass es nicht sofort ersichtlich ist, dass es sich um einen verschlüsselten Container handelt. Die Datei kann hinterher auch beliebig umbenannt werden.
- Der Verschlüsselungsalgorithmus kann gewählt werden. Standardmäßig wird AES-512 vorgeschlagen.

- Bei Datei-Containern kann die Größe bestimmt werden. Die Größe sollte sich an der Menge der zu verschlüsselnden Daten orientieren. Wenn ein Datencontainer zu groß ist, wird das Handling unpraktisch.
- Das Dateisystem (FAT/NTFS) muss festgelegt werden. Wenn der Container auch unter Linux geöffnet werden soll oder auf CD gebrannt werden soll, ist FAT vorzuziehen.
- Das Passwort zum Öffnen des Containers muss festgelegt werden. Aus Sicherheitsgründen sollte dieses Passwort lang und komplex genug gewählt werden. Ergänzend zum Passwort könnte ein keyfile gewählt werden. Ein Entschlüsseln wäre dann nur in Verbindung von Passwort und Keyfile möglich.

Am flexibelsten ist man, wenn man einen einfachen Datei-Container erzeugt. Dieser erscheint im Dateisystem als normale Datei, deren Inhalt jedoch nicht erkennbar ist. Die Datei kann beliebig kopiert werden und kann damit in die normale Datensicherungskette mit eingebunden werden.



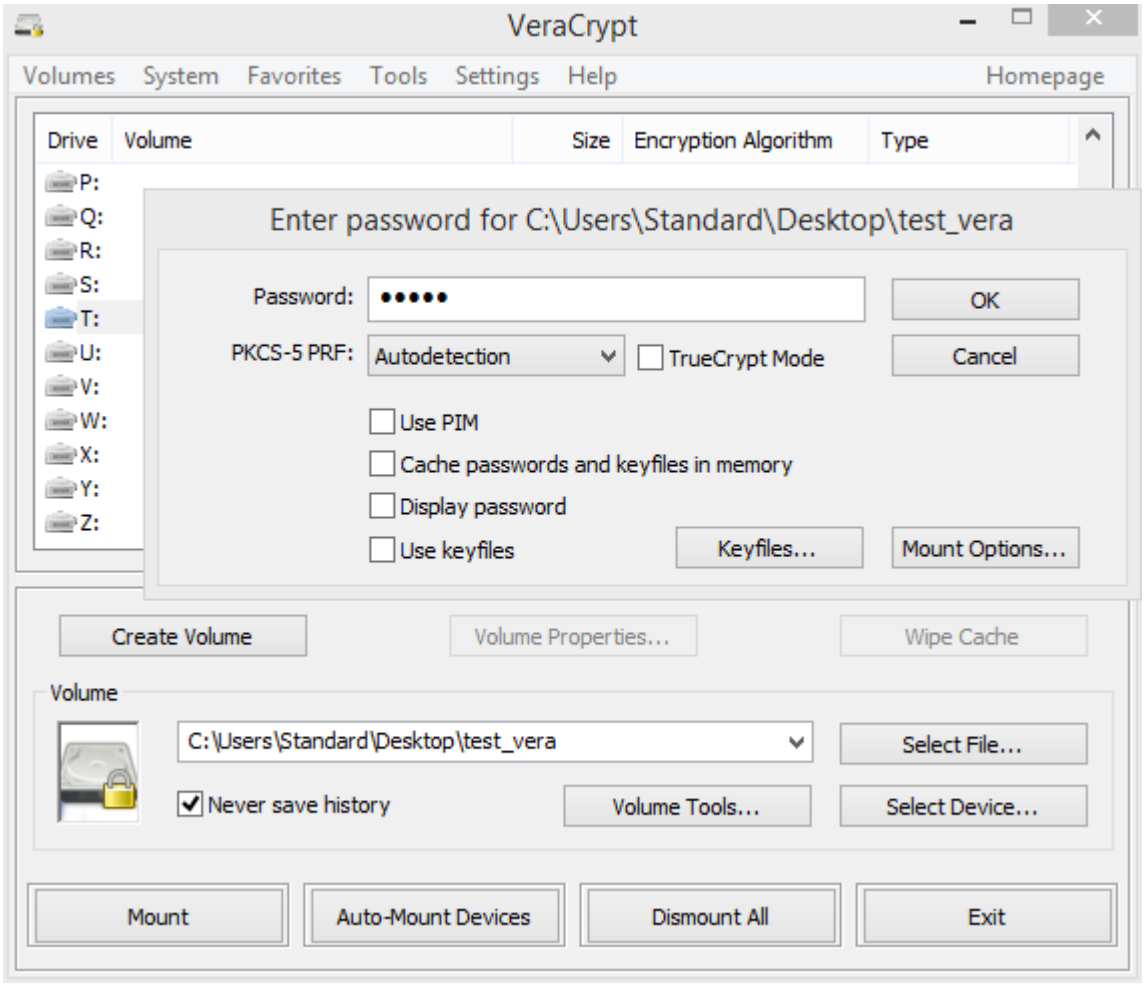
Öffnen eines Containers unter Windows

Zum Öffnen eines Containers sind grundsätzlich folgende Schritte notwendig:

1. Das Programm VeraCrypt muss gestartet werden.
2. Der verschlüsselte Container muss ausgewählt werden.
3. Ein Laufwerksbuchstabe muss ausgewählt werden, unter dem der Inhalt des Containers angeboten werden soll.
4. Der Container wird gemountet. Dabei ist die Eingabe des Passwortes erforderlich.

Wer vorher TrueCrypt, den Vorgänger von Veracrypt, verwendet hat, kann über die Auswahl „TrueCrypt Mode“ auch die mit TrueCrypt erstellten Container einbinden.

Nach der Eingabe des Passwortes ist der Inhalt des Containers über den gewählten Laufwerksbuchstaben zugänglich.



Öffnen eines Containers mit einem Kommandozeilenbefehl:

Wenn VeraCrypt nicht in den Suchpfad eingebunden ist, muss zum Aufruf der komplette Pfad angegeben werden:

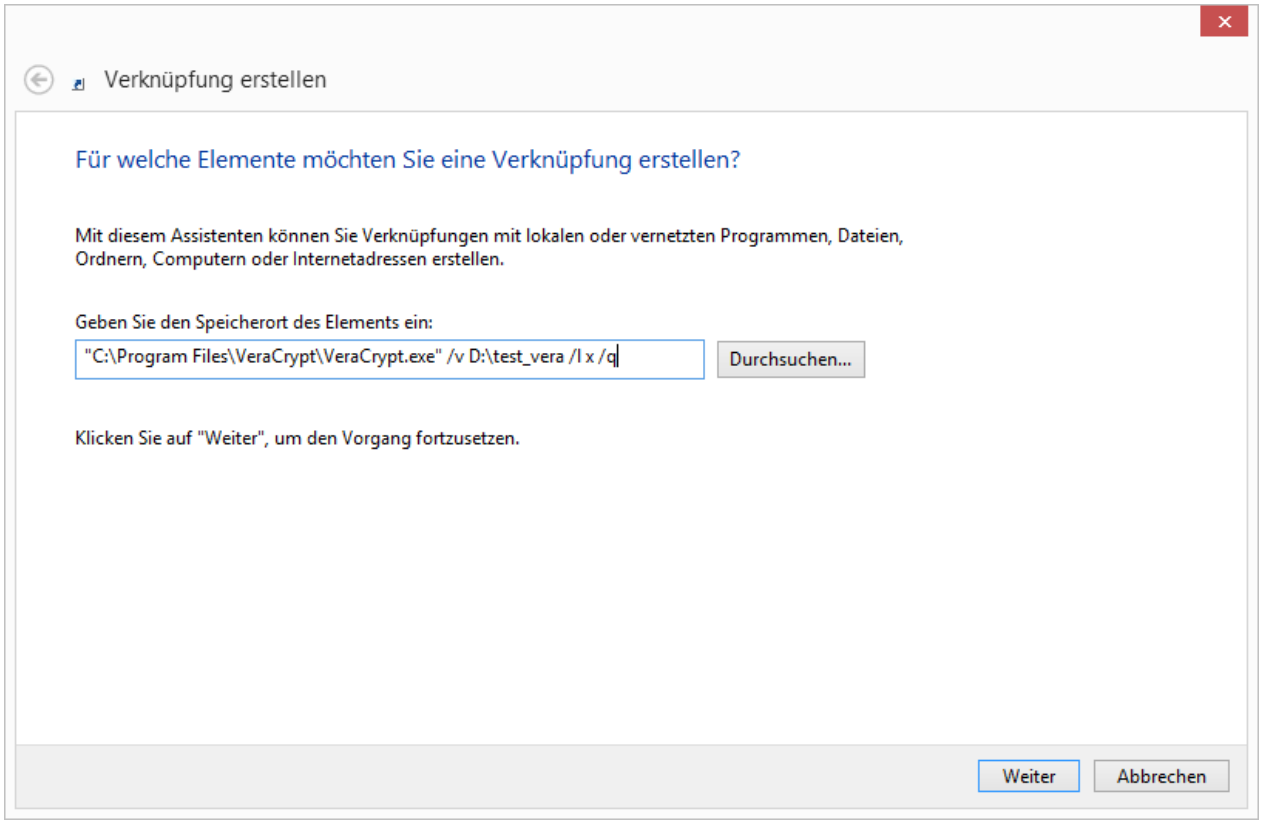
```
"%ProgramFiles%\VeraCrypt\VeraCrypt.exe" /v D:\test_vera /l x /q
```

Optionen

`/v D:\test_vera`	Auswahl des Containers
`/l x`	Auswahl des Laufwerksbuchstabens x
`/q`	Quit; Das Programmfenster wird nicht angezeigt. Es wird nur das Passwortfenster geöffnet.
`/q background`	Das Programmfenster wird nicht angezeigt. Es wird jedoch ein Icon in der Taskleiste erzeugt.
`/s`	Silent-Modus; Jede Interaktion wird unterdrückt.
`/e`	Es wird ein Explorerfenster mit dem Inhalt des Containers geöffnet.
/d	Ein gemountetes Volumen ausbinden (Bsp: /d F)

Öffnen eines Containers über eine Verknüpfung auf dem Desktop:

Wird der obige Kommandozeilenbefehl als Verknüpfung auf dem Desktop abgelegt, lässt sich der Container mit einem Doppelklick öffnen. Die Übergabe des Passwortes auf Kommandozeile wäre ebenfalls möglich. Dies dürfte jedoch in den meisten Fällen nicht sinnvoll sein.

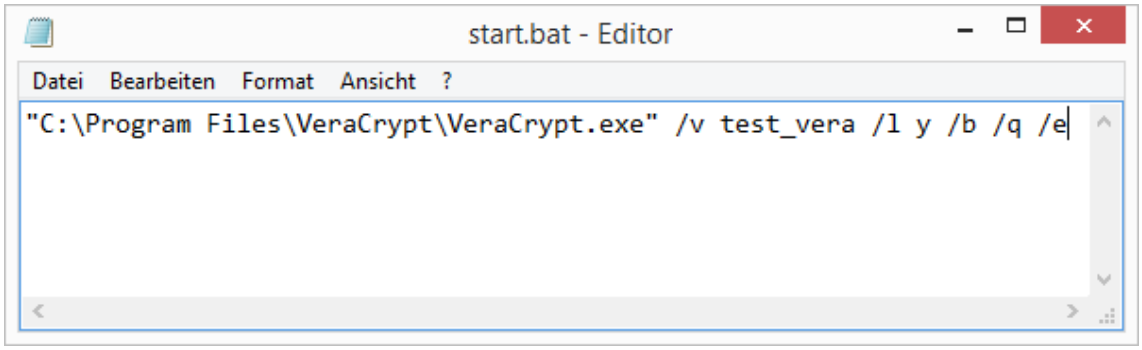


Zugang zum verschlüsselten Container über eine Verknüpfung auf dem Desktop.

Öffnen eines Containers über ein Startscript

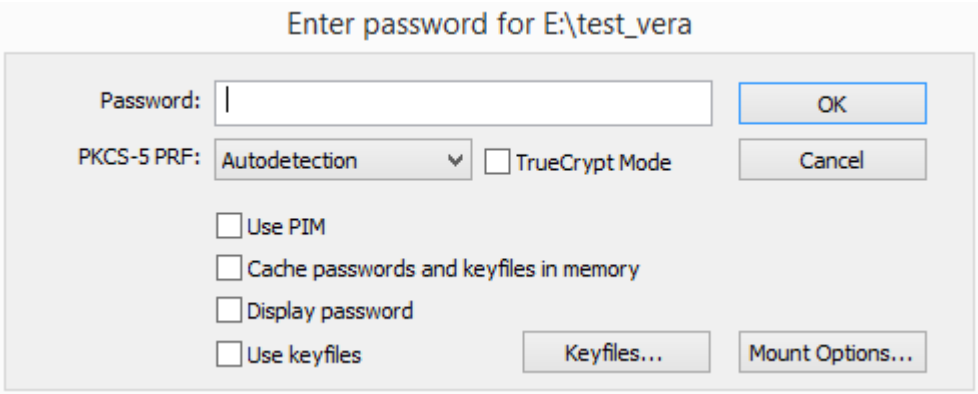
Ein Startscript kann in einigen Fällen sinnvoll sein. Zum einen erhält der Benutzer eine genauere Fehlerausgabe, wenn etwas nicht funktioniert, zum anderen lassen sich relative Pfade zum Programm und zum Container benutzen.

Dazu öffnet man einen einfachen Editor, schreibt den Kommandozeilenbefehl in die Datei und speichert diese unter beliebigerName.bat ab. Dadurch wird die Datei für Windows ausführbar.



Das obige Beispiel kann einen Container mit Namen test_vera, der sich im gleichen Verzeichnis wie das Script befindet, auf den Laufwerksbuchstaben Y einbinden.

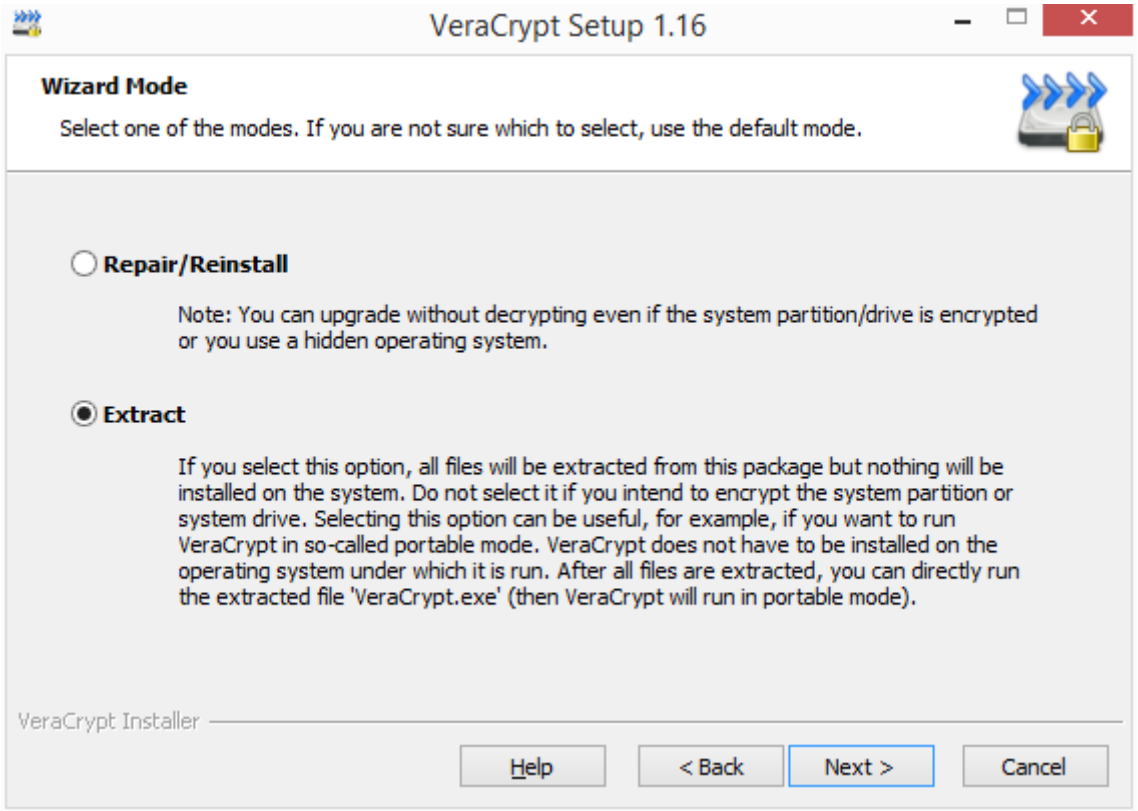
Folgendes Fenster zur Eingabe des Passworts für die Entschlüsselung erscheint:



Wenn das Passwort korrekt eingegeben wurde, öffnet sich ein Explorer-Fenster mit dem Inhalt des Datenordners.

Der Portable-Modus von VeraCrypt

Bei der Installation von VeraCrypt wird angeboten, das Programm nur zu entpacken. Dies ist interessant, wenn VeraCrypt als „Portable Application“ beispielsweise auf einem USB-Stick betrieben werden soll. VeraCrypt nennt dies „portable mode“.

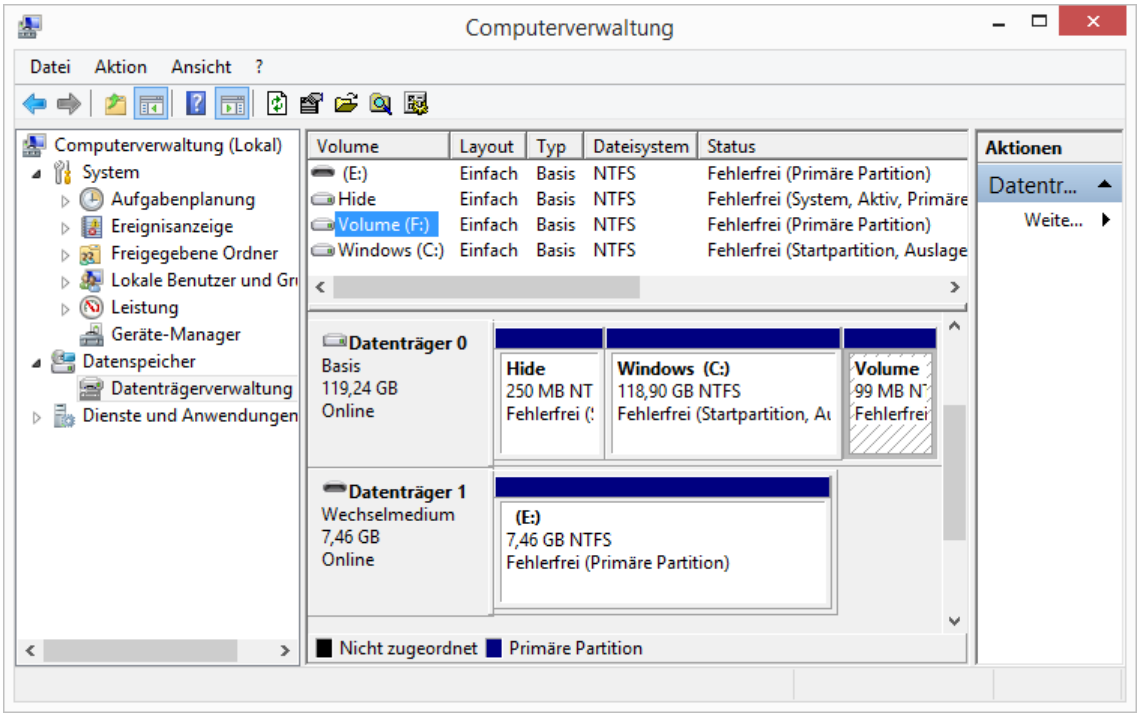


Bringt man den verschlüsselten Container zusammen mit den VeraCrypt-Programmdateien auf einem USB-Stick unter, lässt sich der Container auf jedem Windows-Rechner ohne Installation von VeraCrypt öffnen. Auf einem Windows-Rechner sind dazu jedoch administrative Rechte notwendig. Ein Benutzer ohne Administratorrechte kann VeraCrypt nur verwenden, wenn es auf dem Computer installiert wurde.

Verschlüsseln von Datenpartitionen

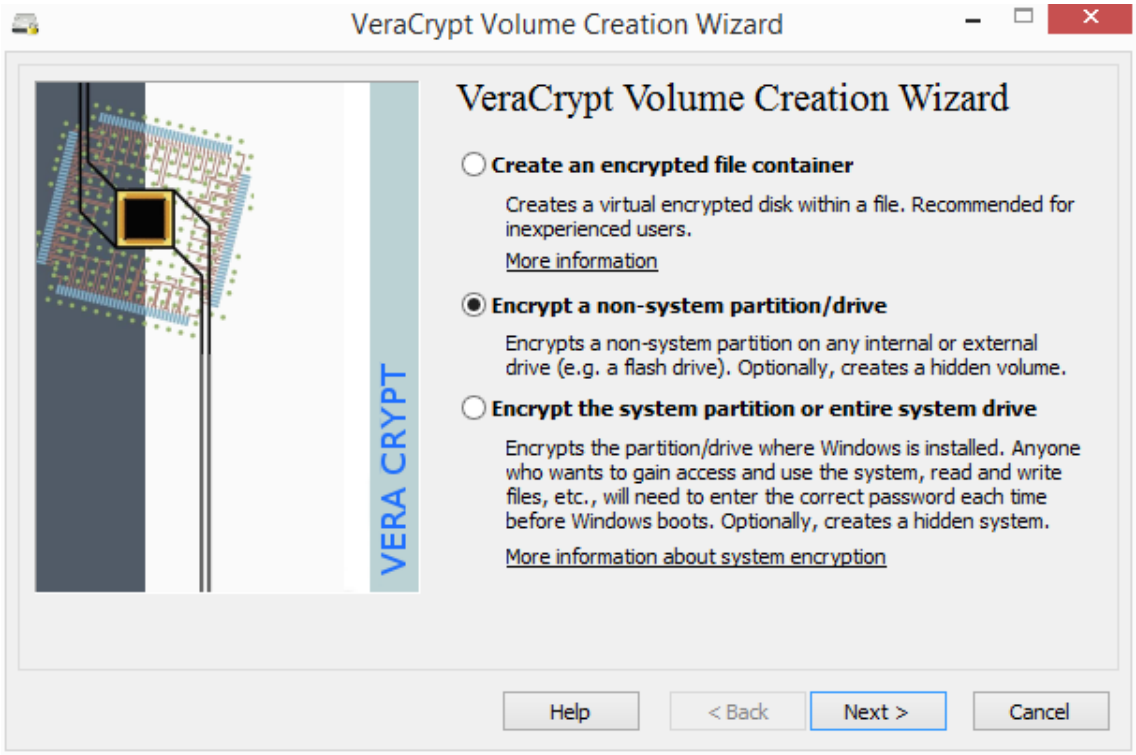
Auf Notebooks oder persönlichen Computern, bei denen nicht ausgeschlossen werden kann, dass fremde Personen Zugriff haben könnten, bietet es sich an, eine gesamte Datenpartition zu verschlüsseln. Dazu wird unter Windows eine neue Partition angelegt. Diese wird nicht formatiert und erhält auch keinen Laufwerksbuchstaben. So erscheint diese Partition später nicht im Dateisystem bevor sie von VeraCrypt gemountet wurde.

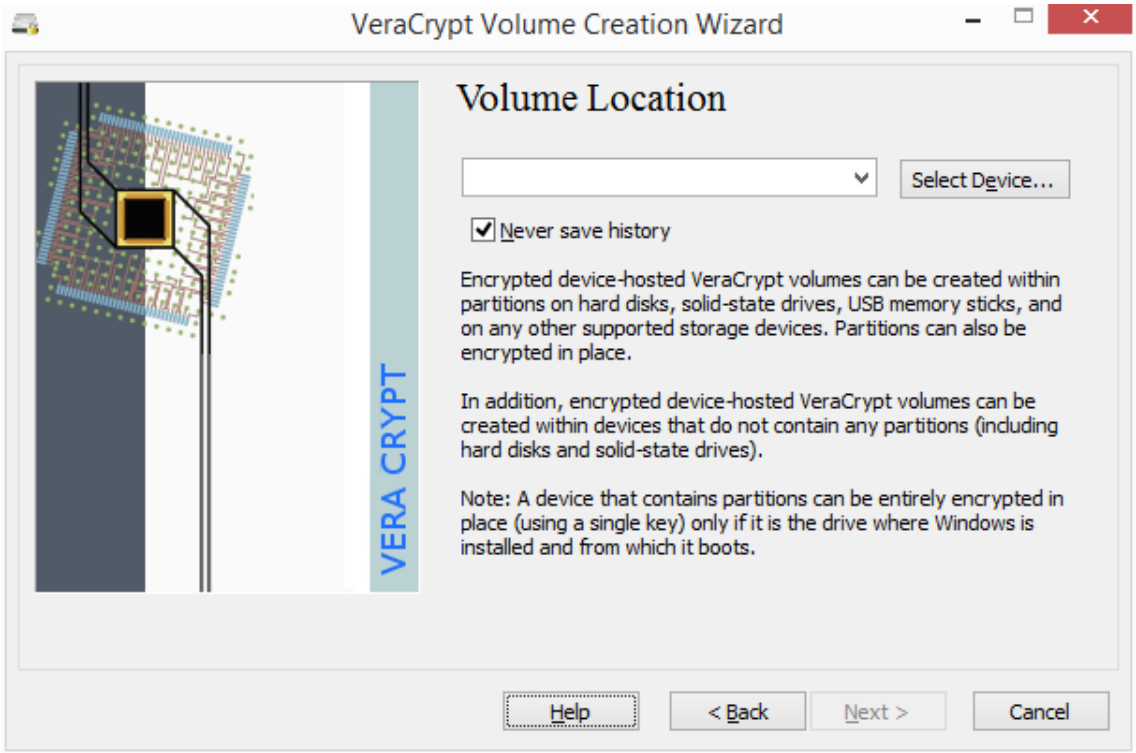
Wenn eine bereits vorhandene Partition verwendet werden soll, darf diese keine Daten enthalten. (Beim Einrichten wird von VeraCrypt alles gelöscht.) Auch der Laufwerksbuchstabe sollte entfernt werden.



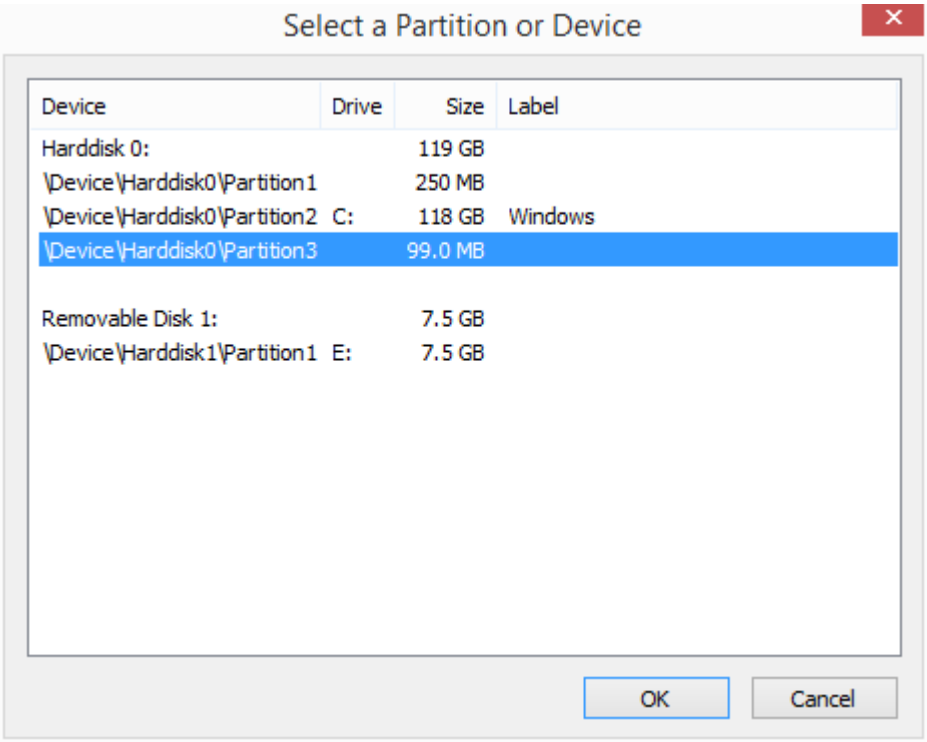
Mit der Datenträgerverwaltung von Windows lassen sich Partitionen neu anlegen oder auch löschen.

Unter VeraCrypt wird über den Button „Create Volume“ ein neuer verschlüsselter Bereich eingerichtet. Dabei wird diesmal jedoch kein Dateicontainer sondern eine Partition ausgewählt.





Über den Button „Select Device“ kann eine verschlüsselte Partition anschließend ausgewählt und gemountet werden.



Öffnen einer verschlüsselten Partition auf Kommandozeile

```
"%ProgramFiles%\VeraCrypt\VeraCrypt.exe" /v
                \Device\Harddisk0\Partition3 /l x /q
```

Der Kommandozeilenbefehl kann über eine Verknüpfung auf dem Desktop aufgerufen werden, so dass der verschlüsselte Container mit einem Doppelklick (und der Eingabe des Passwortes) geöffnet werden kann.

Verschlüsselte Datenpartitionen können nicht nur auf Festplatten sondern auf allen beschreibbaren mobilen Datenträgern angelegt werden. Geht ein solcher Datenträger verloren, ist für den „Finder“ nicht erkennbar, dass darauf Daten enthalten sind. Es gibt keinen sichtbaren Header oder andere Hinweise, die zwingend auf verschlüsselte Daten schließen lassen (plausible deniable). Ein Betriebssystem erkennt nur zufällige Daten, die bei einem nicht formatierten Datenträger durchaus üblich sind.

Installation von VeraCrypt unter Linux

Auf der Internetseite von VeraCrypt (https://veracrypt.codeplex.com/) wird unter „Downloads“ auch ein Paket zur Installation unter Linux angeboten.

Installation unter Debian/Ubuntu

Die Linux-Installationspakete befinden sich nach dem Download in einem gepackten Archiv. Auf der grafischen Oberfläche lässt es sich mit einem Mausklick entpacken (Kontextmenü: Hier entpacken).

Auf der Kommandozeile entspricht dies diesem Befehl:

```
tar -xzf veracrypt-1.16-setup.tar.bz2
```

Es werden die Setup-Scripte für 32 Bit und 64 Bit Installationen jeweils für die grafische und die konsolenbasierte Version entpackt. Die GUI-Versionen enthalten auch die Kommandozeilen-Tools. Darum wird im Folgenden nur die grafische Variante installiert.

Nun kann die entsprechende Datei angeklickt werden und die Option „Im Terminal ausführen“ gewählt werden. Im Terminal erscheint bei der Konsolenvariante sowie bei der grafischen Variante die Frage, ob das Programm installiert werden soll oder nur entpackt. Hier wählt man das Installieren. Auf der Konsole sind das folgende Befehle:

Zunächst navigiert man in das Verzeichnis mit den Installationspaketen:

```
ls veracrypt
```

Danach ruft man die ausführbaren Dateien für ein 64Bit Betriebssystem so auf:

```
./veracrypt-1.16-setup-gui-x64
```

Für ein 32Bit Betriebssystem müssen analog die anderen Dateien aufgerufen werden:

```
./veracrypt-1.16-setup-gui-x86
```

VeraCrypt wird installiert und kann darauf über die grafische Oberfläche oder über die Konsole aufgerufen werden.

Start von VeraCrypt unter Linux

Auf Kommandozeile lässt sich VeraCrypt mit dem Befehl veracrypt starten. Alternativ kann es auch in das Menü (unter KDE oder Gnome) eingebunden werden oder ist bei der Installation bereits eingebunden worden.

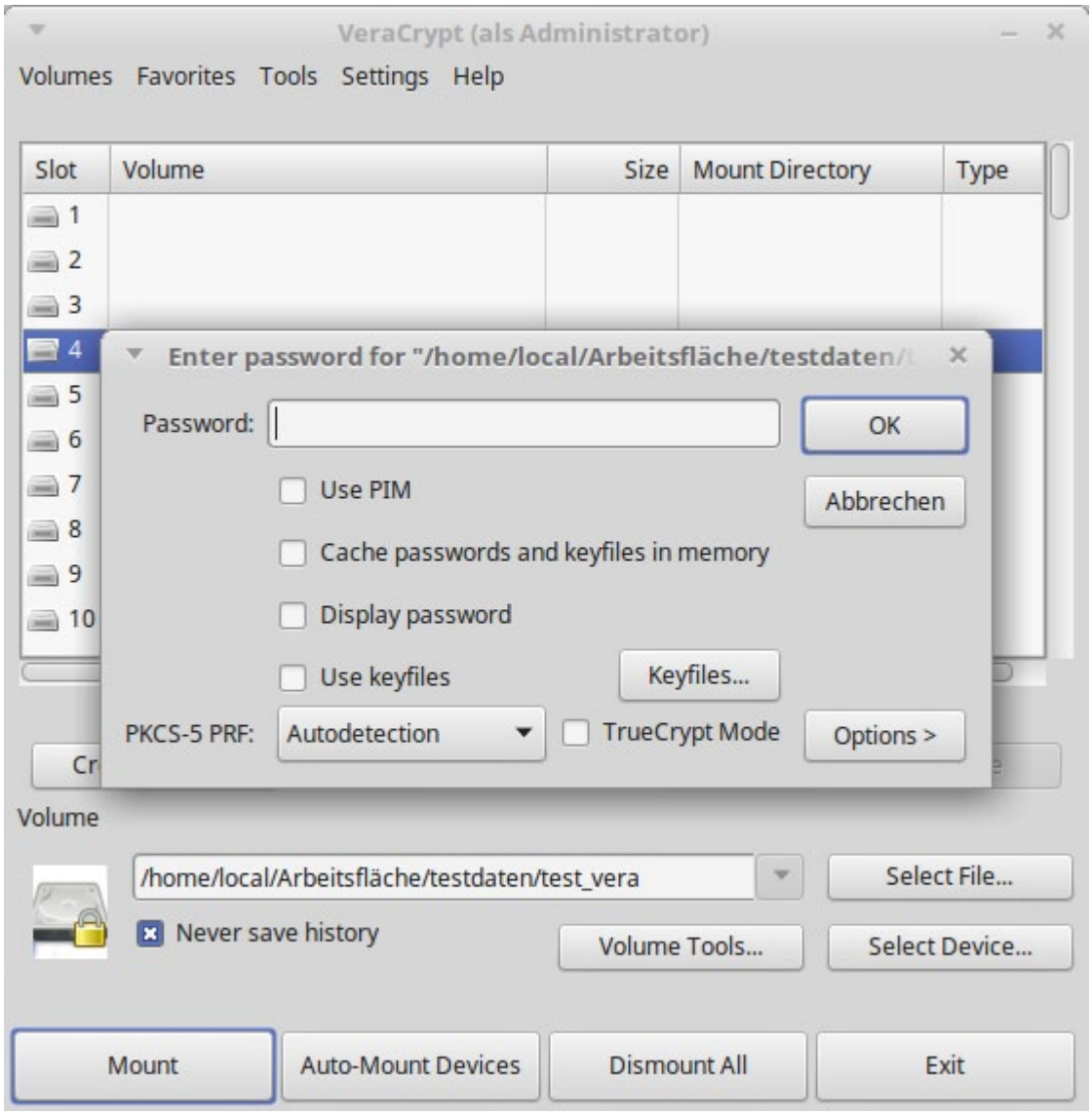
Anlegen eines Containers unter Linux

Das Anlegen eines Containers unterscheidet sich nicht vom Vorgehen unter Windows.

Öffnen eines Containers unter Linux

Auch das Öffnen eines Containers unterscheidet sich nur geringfügig vom Öffnen eines Containers unter Windows. Nach dem Start von VeraCrypt kann der verschlüsselte Container ausgewählt werden. Danach wird ein beliebiger „Slot“ gewählt. Diese Slots

sind ein Überbleibsel der Laufwerksbuchstaben unter Windows und haben ansonst keine Bedeutung. Als Mountpoint wird standardmäßig eines der Verzeichnisse /media/veracrypt1, media/veracrypt2, ... gewählt. Über die Optionen bei der Eingabe des Passwortes lässt sich der Mountpoint jedoch beeinflussen.



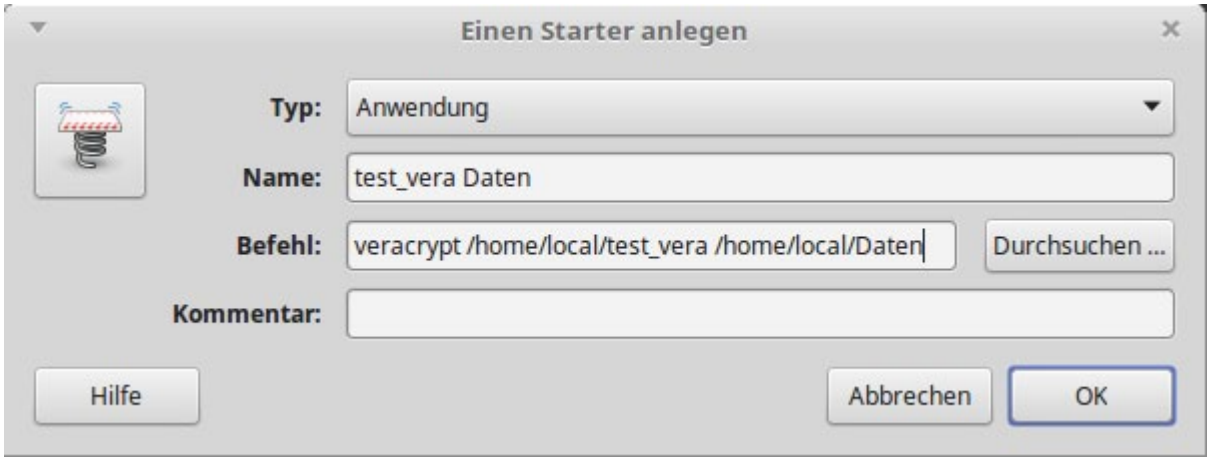
Alternativ lässt sich ein verschlüsselter Container auch über einen Kommandozeilenbefehl einbinden:

```
mkdir Daten
veracrypt test_vera Daten
```

oder als vollständiger Kommandozeilenbefehl mit Angabe aller Pfade:

```
mkdir /home/local/veracrypt/Daten
veracrypt /home/local/test_vera /home/local/Daten
```

Der vollständige Kommandozeilenbefehl eignet sich auch als Befehlzeile beim Anlegen eines Starters.



Ausführen von VeraCrypt-Linux ohne root-Rechte

Auch unter Linux benötigt das Ausführen von VeraCrypt Administrations- bzw. root-Rechte. Um als eingeschränkter Benutzer nicht jedes Mal das root-Passwort eingeben zu müssen, kann das Ausführen von VeracCrypt als root ohne Passwort erlaubt werden.
Dazu trägt man als root an das Ende der Datei /etc/sudoers folgende Zeilen ein:

```
# VeraCrypt ohne root
%users ALL=(root) NOPASSWD:/usr/bin/veracrypt
```

Sicherheitsaspekte und Angriffsmöglichkeiten

Das Programm VeraCrypt verwendet sichere gängige symmetrische Verschlüsselungsverfahren. Als sicher gilt eine Verschlüsselungsmethode dann, wenn sie nur durch einen "Brute Force"-Angriff geknackt werden kann, also durch Ausprobieren aller möglichen Schlüssel und die Schlüssellänge dabei so groß ist, dass die dafür zur Verfügung stehende Zeit nicht ausreicht. Eine Schlüssellänge von 56 Bit (z. B. DES-Verschlüsselung) kann mit erheblichem Zeit- und Rechenaufwand geknackt werden. Das standardmäßig vorgeschlagene Verschlüsselungsverfahren bei VeraCrypt ist AES mit einer Schlüssellänge von 512 Bit. Bei diesem Verfahren ist derzeit kein praktikabler Weg bekannt, um die Verschlüsselung zu knacken.

Neben der prinzipiellen Sicherheit, die durch die Wahl eines geeigneten Verschlüsselungsverfahrens gegeben ist, spielt für die praktische Sicherheit die Art der Implementierung die wichtigere Rolle.

Wahl des Passwortes

Zum Ver- und Entschlüsseln benötigt man bei symmetrischen Verfahren jeweils denselben Schlüssel, der natürlich geheim gehalten werden muss. Da man sich einen beliebigen 512-Bit-Schlüssel nicht merken kann und man sich den Schlüssel auch möglichst nicht notieren sollte, verwendet das Programm VeraCrypt ein Passwort, aus dem es den zu verwendenden Schlüssel berechnet. (Wenn zusätzlich ein keyfile verwendet wird, wird dieses in die Berechnung des Schlüssels mit einbezogen.) Die theoretische Sicherheit des Verschlüsselungsalgorithmus reduziert sich also in der Praxis auf die Sicherheit des gewählten Passwortes. Wenn es einem Angreifer gelingt, das Passwort herauszufinden, hat er den Container geknackt.

Wörterbuchattacke zum Knacken des Passwortes

Die folgenden kleinen Beispielskripte (unter Windows und Linux) lesen aus der Datei Woerterbuch.txt zeilenweise mögliche Passwörter aus und probieren damit, den Container „test_vera“ zu entschlüsseln. Wenn ein Versuch erfolgreich war, bricht das Skript ab und schreibt das Passwort auf den Bildschirm.

Testprogramm zum Entschlüsseln eines Containers unter Windows

```
@echo off
"C:\Program Files\VeraCrypt\VeraCrypt.exe" /d /q /f
for /F %%i in (Woerterbuch.txt) do (
"C:\Program Files\VeraCrypt\VeraCrypt.exe" /v test_vera /l t /q
/p %%i /s
if not errorlevel 1 (
   echo Passwort: %%i
   pause
   exit
 ) else (
   echo Test: %%i
 )
)
```

Testprogramm zum Entschlüsseln eines Containers unter Linux

```
#!/bin/bash
veracrypt -d

while read inputline
do
  Passwort="$(echo $inputline)"
  echo "Teste: $Passwort"
  veracrypt -t -p $Passwort --non-interactive test_vera
/media/vera
  success=$?
  if [ $success -eq 0 ] ; then
     echo "erfolgreich"
     echo "Passwort: $Passwort"
     exit
  fi
done < Woerterbuch.txt
```

Hier hat sich VeraCrypt im Gegensatz zu seinem Vorgänger TrueCrypt durch die erhöhung der Iterationen im Entschlüsselungsalgorithmus entscheidend verbessert. Mit einem derzeit aktuellen Rechner dauert der Versuch, ein Passwort auszuprobiere über 20 Sekunden. Dennoch sind Computer in ihrer Arbeit sehr geduldig. Wenn das Skript mehrere Wochen oder Monate läuft, lassen sich problemlos ganze Wörterbücher durchtesten. Passwörter mit einer Länge von weniger als 8 Zeichen oder Passwörter, die als Name in einem Wörterbuch vorhanden sind, bieten damit praktisch keine Sicherheit. VeraCrypt empfiehlt Passwörter mit einer Länge von mindestens 20 Zeichen.

Erraten des Passwortes

Ein weiterer Unsicherheitsfaktor ist, dass Benutzer dazu neigen, Passwörter zu notieren oder für verschiedene Authentifizierungen dasselbe Passwort zu verwenden. Wenn man nun weiß, dass manche Anwendungen Passwörter sogar im Klartext speichern, ist dies eine sehr praktikable und einfache Methode, an mögliche Passwörter eines Benutzers zu gelangen.

Angriffsmöglichkeiten während der Bearbeitung eines Containers

Hat ein potentieller Angreifer nur den verschlüsselten Container, sind seine Angriffsmöglichkeiten sehr beschränkt. Sie bestehen im Wesentlichen daraus, auf irgendeine Art an das Passwort zu gelangen.

Mehr Möglichkeiten bieten sich einem Angreifer, dem es gelingt, einen Computer unter seine Kontrolle zu bringen, auf dem ein Anwender einen Container öffnet: In der Auslagerungsdatei könnten sich z. B. Fragmente der vertraulichen Daten befinden. Hat ein Angreifer die Möglichkeit, einen Passwort-Sniffer zu installieren, kann er gezielt die Aktivitäten eines Benutzers mitprotokollieren. Diese Gefahr ist auch gegeben, wenn man durch Unachtsamkeit einen Trojaner oder eine andere Malware auf seinem Computer installiert. Keine Verschlüsselungssoftware kann derartige Angriffe erkennen oder verhindern. Hier kann man nur versuchen, seinen eigenen PC „sauber" zu halten.

Einsatzmöglichkeiten in der Schule

Ein Datencontainer kann auf dem lokalen Computer oder auf einem Netzlaufwerk liegen, es ist jedoch nicht möglich, dass ein Datencontainer mehrfach geöffnet wird oder von verschiedenen Personen gleichzeitig bearbeitet wird.

Die Sicherheit von VeraCrypt beruht auf einem Passwort (und eventuell einem zusätzlichen keyfile). Es ist nicht möglich, wie in einer Client/Server-Umgebung unterschiedliche Berechtigungen und Authentifizierungen zu vergeben.

Diese beiden Punkte schließen den Einsatz von VeraCrypt dort aus, wo Daten von unterschiedlichen Personen bearbeitet oder eingesehen werden müssen. Dafür eignen sich die klassischen Client/Server-Konzepte, bei denen die Sicherheit darauf beruht, dass niemand unberechtigt physikalischen Zugriff zum Server erhält und die Remote-Zugriffe über Berechtigungen und individuelle Authentifizierungen geregelt sind.

Eine weitere Einschränkung ergibt sich gegebenenfalls, wenn Cloud-Speicher genutzt werden sollen und Daten automatisch synchronisiert werden. Es ist nicht möglich, nur die veränderten Daten zu synchronisieren, es muss immer der gesamte Container synchronisiert werden. Bei dieser vorgesehenen Nutzung sollte die Containergröße möglichst klein gewählt werden.

Wenn vertrauliche Daten jedoch nur von einzelnen Personen und zusätzlich in „unsicheren“ Umgebungen verwendet werden sollen, bietet sich der Einsatz einer Datenverschlüsselung mit VeraCrypt an.

Dies ist beispielsweise immer dann der Fall, wenn Lehrkräfte vertrauliche Daten auf einem USB-Stick transportieren. Dafür eignet sich der Portable-Modus, wenn der Benutzer überall, wo er entschlüsseln muss, Administrationsrechte auf den PCs hat, oder auch die vollständige Verschlüsselung des mobilen Datenträgers, wenn VeraCrypt auf den Arbeitsgeräten fest installiert ist..

Wenn ein Notebook persönliche Daten enthält, bietet es sich an, zumindest die Datenpartition zu verschlüsseln. Daneben wären auch noch weitere Sicherheitsmaßnahmen denkbar. Mit VeraCrypt lässt sich auch die Systempartition verschlüsseln. Zudem bieten einige Notebookhersteller eigene Sicherheitskonzepte, bei denen die gesamte Festplatte verschlüsselt ist und auch der Start des Systems nur nach einer Authentifizierung erfolgt. Bei allen Verfahren muss jedoch immer geprüft werden, ob die Daten nach einem möglichen System-Crash noch zugänglich sind.

Für sehr wichtige und sehr vertrauliche Daten, wie z. B. bei Beurteilungen von Schülern oder Lehrern oder bei einer Sammlung persönlicher Zugangsdaten zu anderen Systemen, bietet es sich an, diese grundsätzlich in einem verschlüsselten Container aufzubewahren, der nur bei Bedarf geöffnet wird. Dieser Container kann in die normale Sicherungskette mit einbezogen werden (z. B. Sicherung auf einem Backup-Server, Sicherung auf externen USB-Festplatten, usw.). Solange das Passwort eines solchen Containers nicht bekannt wird, sind die Daten vor Missbrauch sicher.