VeraCrypt auf Homedirectory nutzen

Dieses Dokument beschreibt, wie die Software VeraCrypt zur eigenen Verschlüsselung von Daten und Verzeichnissen verwendet werden kann. Mit Hilfe dieses Dokuments können Nutzer:innen Dateien oder Verzeichnisse mit einem selbst gewählten Schlüssel so verschlüsseln, dass sie für andere nicht mehr zugänglich sind. Für die hier beschriebene Verschlüsselung wird keine Unterstützung durch weiteres technisches Personal benötigt.

Es ergänzt Schulungsunterlagen zum Thema „Daten selbst verschlüsseln“.

VeraCrypt

VeraCrypt verschlüsselt Dateien oder Verzeichnisstrukturen auf Speichersystemen, die durch gängige Betriebssysteme wie Windows, MacOS (Apple) und Linux verwaltet werden. Die Dateien oder Verzeichnisse werden in einem Container gespeichert, der nur mit VeraCrypt wieder lesbar gemacht werden kann. In VeraCrypt werden Container als **Volume** bezeichnet, auch in der deutschen Version. Zur Entschlüsselung dienen Passphrasen und/oder Schlüsseldateien. Eine Passphrase wird als Wissen angesehen, eine Schlüsseldatei als Besitz. Zur Verschlüsselung können beide Faktoren auch kombiniert verwendet werden.

VeraCrypt ist als Software von unabhängigen Stellen auditiert worden. Dabei wurden Schwächen gefunden, die aber nicht als kritisch angesehen werden und eher auf die Implementierung zurückgehen, nicht auf grundsätzliche Fehler der Programmlogik. In der Abwägung zum Schutz von eigenen Daten wird der Einsatz von VeraCrypt vom *Bundesamt für Sicherheit in der Informationstechnik* empfohlen, ebenso von Organisationen für Bürgerrechten wie der EFF (Electronic Frountier Foundation, https://www.eff.org) und NGOs, die den Schutz von Menschenrechtsaktivist:innen und Journalist:innen verbessern möchten.

Einsatzfelder

VeraCrypt ist für den individuellen Einsatz. Damit lassen sich Probleme mit der Vertrauenswürdigkeit lösen, die einzelne Personen haben, weil es keine institutionellen Angebote in ihrem Bereich gibt. Es kommt auch zum Einsatz, wenn eine Situation so spezifisch ist, dass es keinen vorgefertigten Weg oder Workflow gibt. Deswegen wird VeraCrypt oft Journalist:innen, Menschenrechtsaktivist:innen oder anderen Reisenden in Mission empfohlen.

Grenzen

Ein Container, von VeraCrypt als Volume eingebunden, wird bei jedem Speichervorgang als Ganzes zurückgespeichert. Das liegt in der Organisation des verschlüsselten Speichers begründet, wo die Vertrauenswordigkeit nur hergestellt werden kann, wenn das Zufallsrauschen, in dem die Daten versteckt sind, immer über alles verschleiert.

Das hat mehrere Konsequenzen. Ein VeraCrypt-Volume sollte nicht über eine Verbindung zwischen verarbeitendem Computern und Speichersystem geschickt werden, die langsam oder unzuverlässig ist. Die Größe von Volumes kann prinzipiell sehr groß werden, aber irgendwann wird es unpraktisch, bei selbst kleinen Änderungen eine sehr große Datei auf den Speicher zu schreiben.

Die Daten in einem Volume sind nur so lange geschützt, wie es von VeraCrypt ungeöffnet auf einem Speicher liegt. Sobald mit VeraCrypt ein Volume eingebunden ist, können die Dateien in ihm auf herkömmlichem Weg ausgelesen werden. Sobald der Verdacht aufkommt, dass ein Computer kompromittiert ist und die Daten geschützt bleiben sollen, darf ein Volume nicht geöffnet werden.

Installation

Die Erläuterungen in diesem Kapitel sind nicht für die Benutzung durch Anwender:innen, sondern Hinweise, die gegebenenfalls an IT-Beauftragte wie Systemadministratoren weiterzugeben sind. Je nach Zugriff auf den Computer kann VeraCrypt selbst installiert werden.

Die Installation wird auf der Webseite des Anbieters beschrieben.

Auf Arbeitssystemen, wo die Rechte der Nutzer:innen eingeschränkt ist, muss VeraCrypt durch eine befugte Person installiert werden. Je nach Berechtigungsmanagement werden beim Anlegen von verschlüsselten Containern kurzzeitig erweiterte Benutzerrechte benötigt. In solchen Fällen sollte der oder die zuständige Administrator:in kontaktiert werden.

VeraCrypt ist ein Programm mit relativ wenig Speicherbedarf. Es kann auch von einem USB-Stick oder eine mobilen Festplatte gestartet werden, sofern dies vom Betriebssystem erlaubt ist. Die Software lässt sich also auf einem mobilen Datenträger mitführen und auf anderen Computern mit einem Container auf dem gleichen Träger starten.

Volumes

Im Internet finden sich einige Anleitungen, wie verschlüsselte Container angelegt werden können (siehe Referenzen). Die Beschreibung in diesem Dokument zeigt den Vorgang mit einem Homedirectory, wie es vom Rechenzentrum der Universität Freiburg für jedes Mitglied mit einem Uniaccount bereitgehalten wird.

Die Benutzeroberflächen der VeraCrypt-Versionen für MacOS und Linux unterscheiden sich in Details, der grundlegende Aufbau lässt sich aus der hier vorliegenden Beschreibung nachvollziehen.

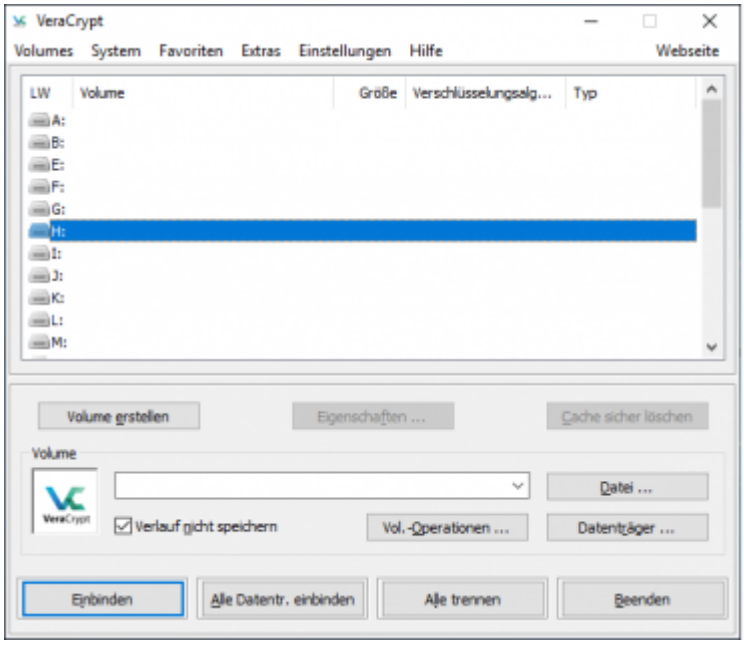
Vorüberlegungen

Bevor ein Container angelegt wird, sollte ein Passwort mit ausreichender Qualität vorbereitet sein, falls eine Verschlüsselung nach dem Prinzip Wissen beabsichtigt ist. Von diesem Passwort hängt die Sicherheit der Daten im Container ab. Deswegen sollte es ausreichend lang sein und nicht an anderer Stelle bereits verwendet werden.

Soll der Container über eine Datei nach dem Prinzip Besitz geschützt werden, muss eine solche vorher ausgewählt werden. VeraCrypt erlaubt beliebige Dateien, zum Beispiel eine Bilddatei. Falls dieses Verfahren gewünscht ist, muss sichergestellt sichergestellt sein, dass diese Datei im Zugriff des Computers liegt, auf dem der Container geöffnet wird.

Volume erzeugen

Nach dem Start von VeraCrypt zeigt sich folgender Eingangsbildschirm:

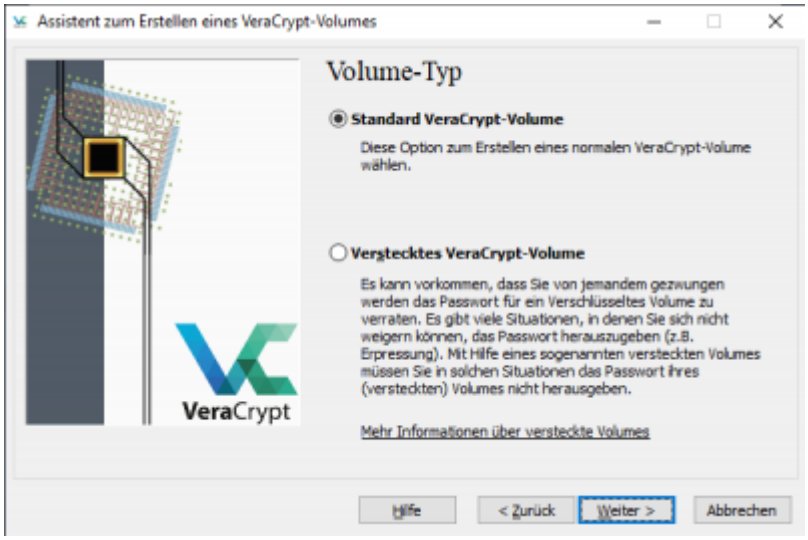


Mit Klick auf `Volumes→Neues Volume erstellen…` beginnt die Prozedur, um einen neuen Container einzurichten:

Im folgenden wird ein Container erzeugt, der wie Datei abgespeichert ist und als solche von einem physischem Laufwerk auf ein anderes verschoben werden kann, zum Beispiel von einer Festplatte auf einen USB-Stick.

Mit den anderen Optionen lassen sich auch ganze Festplatten oder Betriebssystem-Partitionen verschlüsseln, was aber administrative Rechte und die Kenntnis der Hardware voraussetzt. Für

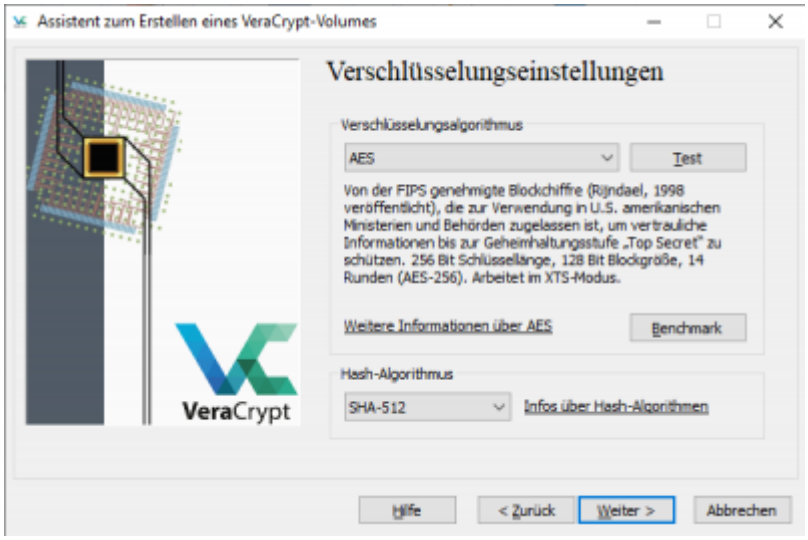
individuelle Einsatzszenarios genügen *Standard-Volumes*.



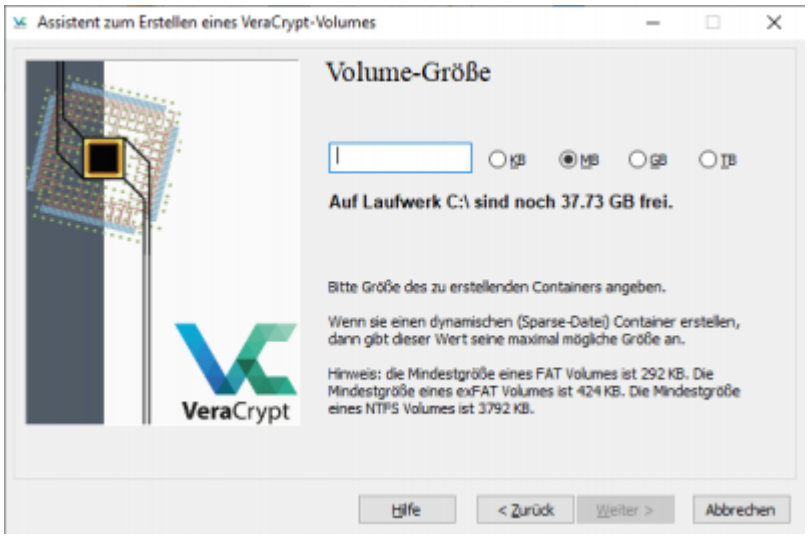
Auch wenn der Container später unter Windows mit einem Laufwerksbuchstaben angezeigt wird, muss er als Datei auf einem Speichersystem angelegt werden. Der Assistent fragt nach dem Speicherort.

Per Klick auf `Datei…` wird der bekannte Auswahlbildschirm gezeigt, über den im Verzeichnissystem navigiert werden kann.

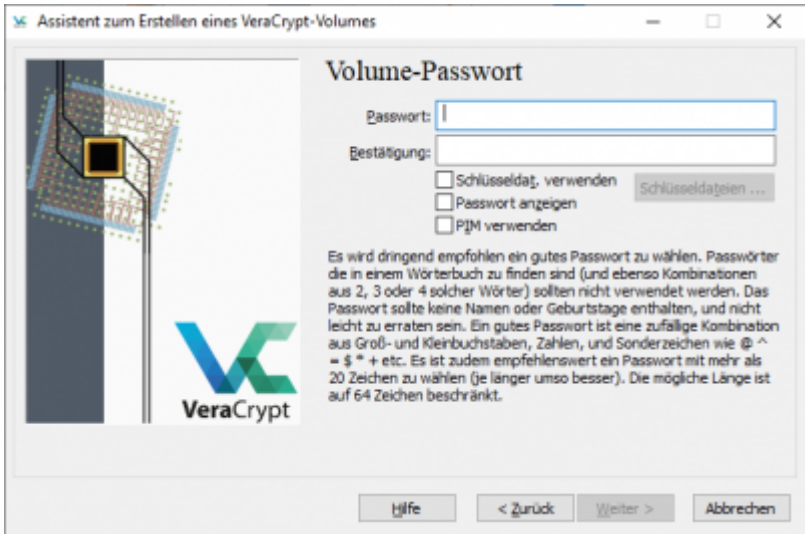
Nach Auswahl des Speicherorts und des Dateinamens für den Container sind die Einstellungen festzulegen, insbesondere die Algorithmen für die Verschlüsselung und das Hashing. Die Voreinstellungen *AES* für die Verschlüsselung und *SHA-512* für das Hashing können übernommen werden.



Nun ist die Größe des Volumes zu bestimmen. Die Entscheidung sollte den Einsatzzweck und die technische Umgebung berücksichtigen. Es gibt verschiedene Überlegungen, wie groß ein Volume sein sollte. Die erste ist, wieviel Platz auf dem Speichermedium für den Container verfügbar ist. Wenn ein USB-Stick, auf dem der Container gespeichert werden soll, 16 Gigabyte hat, begrenzt dies auch das Volume auf maximal diesen Wert. Außerdem ist zu bedenken, dass beim Speichern von Daten in einem VeraCrypt-Laufwerk immer das ganze Volume geschrieben wird. Aus diesem Grund sind große Container auf Dropbox oder anderen Speicherformen, die mit begrenzter Leitung angebunden sind, nicht wirklich sinnvoll. Es muss immer der ganze Container beim Speichern neu geschrieben werden, selbst wenn nur in einer Datei innerhalb des Volumes einige Buchstaben geändert werden.

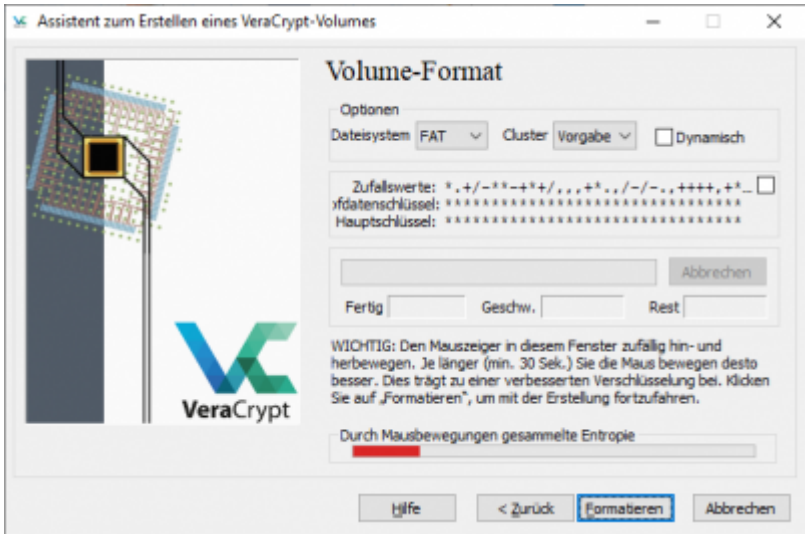


Nach der Größenbestimmung wird der Schutz des Volume festgelegt. Es ist möglich, ein Passwort oder eine Schlüsseldatei auszuwählen. Der folgende Bildschirmdialog gibt eine kurze Richtlinie, wie ein gutes Passwort aussehen sollte. Insbesondere sollte es einzigartig sein und nicht bereits an anderer Stelle verwendet werden.

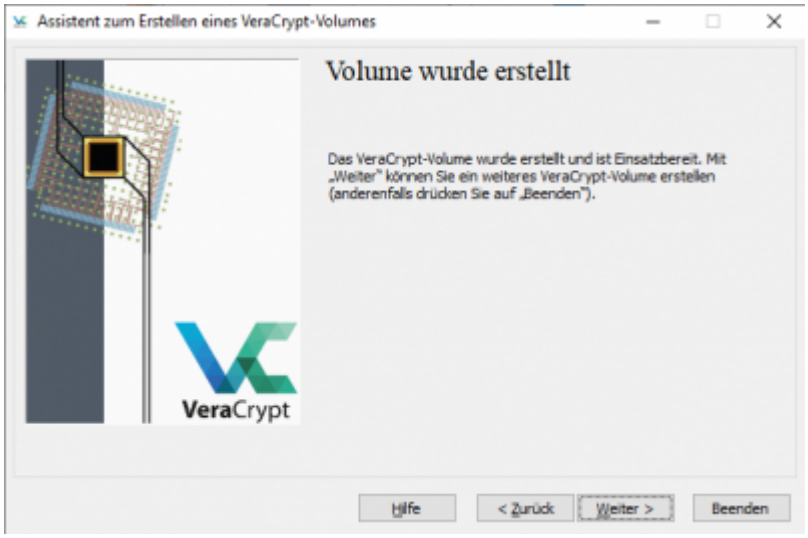


Für das Schulungsmodul, dem diese Dokumentation zugrundeliegt, ist bereits ein Beispiel mit dem Namen *Training* angelegt, das über das hier angezeigte Passwort geöffnet werden kann. Dieses Passwort sollte auf keinen Fall woanders recycelt werden.

Mit diesen Angaben wird von VeraCrypt nun ein Volume in einem Dateicontainer erzeugt. Um im Container die zufällig generierte Informationsdichte, die sogenannte Entropie, zu erhöhen, wird beim Formatieren der Weg des Mauszeigers ausgewertet. Der gesamte Container wird mit Zufallszeichen vollgeschrieben, in denen die eigentliche Botschaft, ob äußeres oder verstecktes Volume, verschleiert wird. Eine hohe Entropie ist deswegen besser, weil damit der Aufwand erhöht wird, aus dem Zeichensalat die eigentliche Information zu extrahieren. Je mehr die Maus bewegt wird, desto schneller wechselt die Farbe des Fortschrittsbalkens von rot auf grün.



Nach einer Weile ist der Container fertiggestellt. Mit Klick auf den Button Beenden wird der Assistent geschlossen.

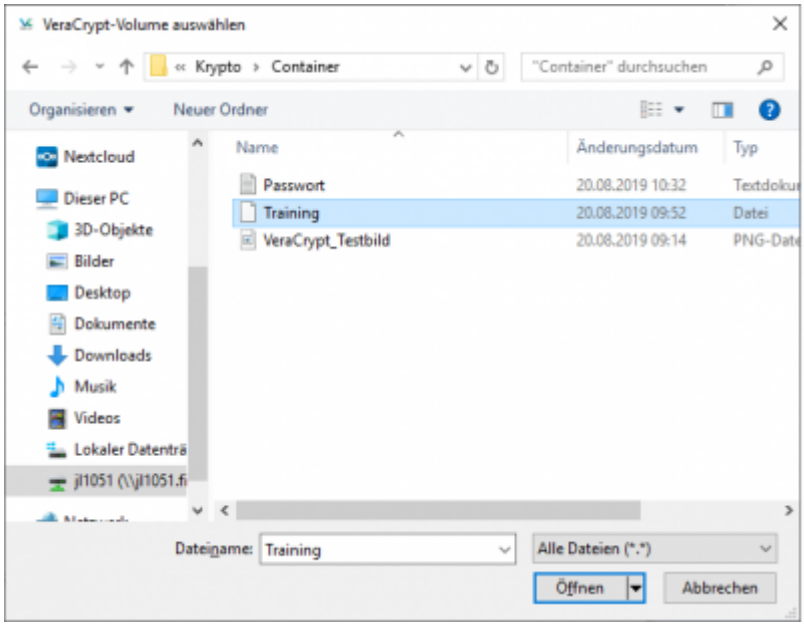


Einbinden eines existierenden Containers

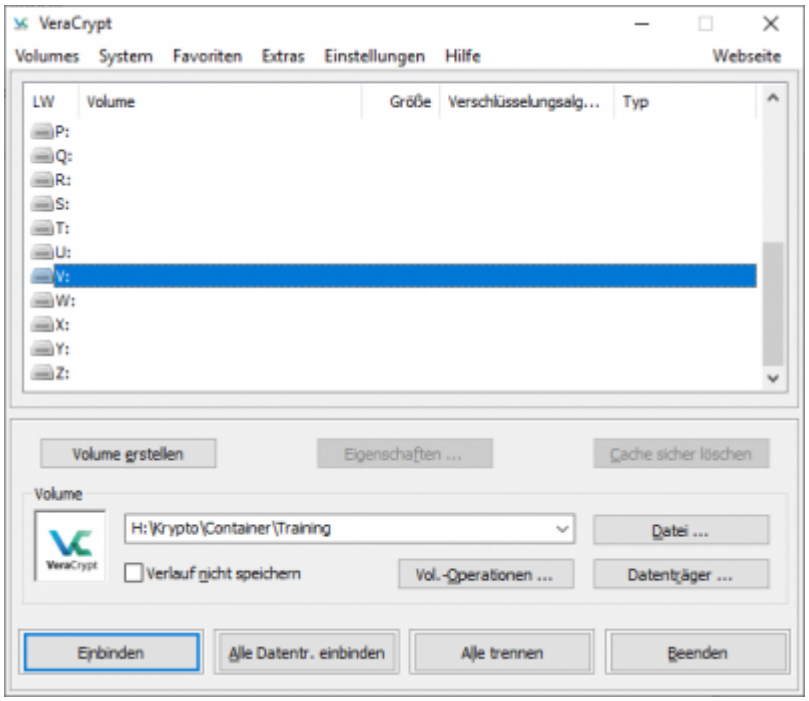
Mounten ist ein Fachausdruck im Zusammenhang mit der Administration von Computern. Damit wird die Einbindung von Speichersystemen bezeichnet, so dass sie von Dateiexplorern angezeigt werden. Unter Windows erhalten gemountete Speicher in der Regel einen Buchstaben, unter dem das Laufwerk angesprochen wird.

Im folgenden wird beschrieben, wie ein Container als Laufwerk eingebunden werden kann. Dafür muss das Betriebssystem Zugriff auf den eigentlichen Speicher haben, der ein USB-Stick, eine mobile Festplatte oder das Homedirectory sein kann.

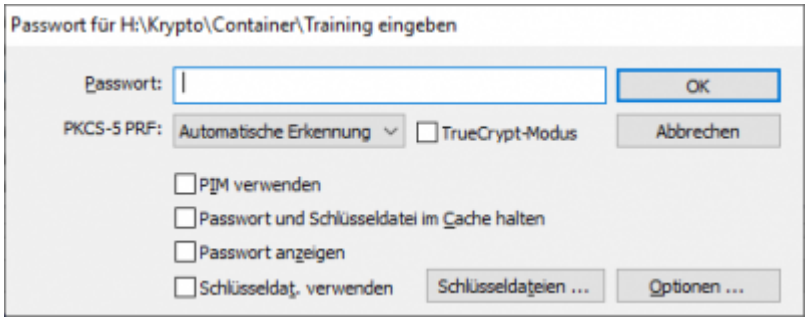
Nach Klick auf den Button `Datei…` öffnet sich ein Dialog zur Auswahl des Containers. Im folgenden Bild wird der Container `Training` auf einem Nextcloud-Verzeichnis ausgewählt.



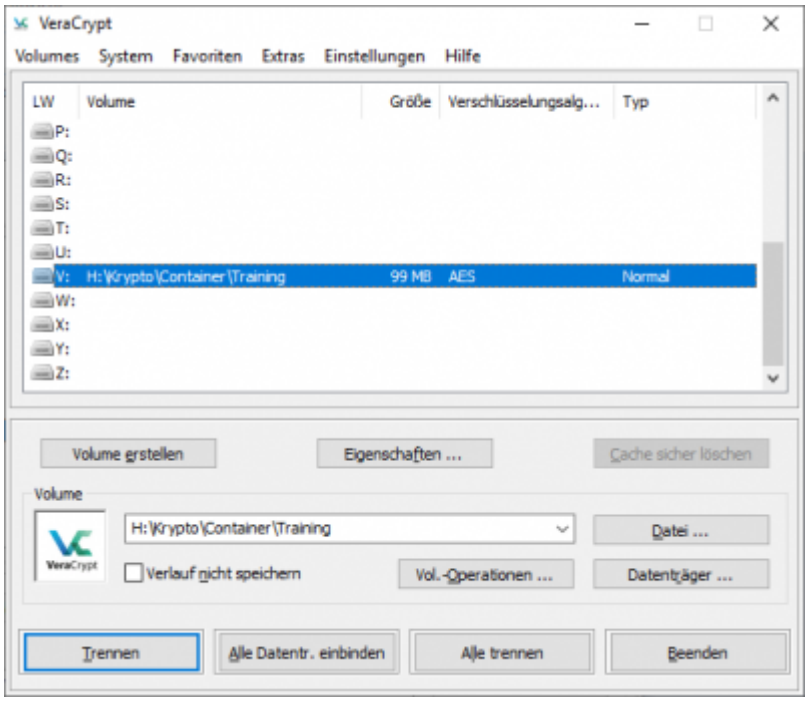
Der Container wird inklusive des Pfades angezeigt. Im oberen Teil des folgenden Dialogs kann der Laufwerksbuchstabe ausgewähl werden. Es werden nur Buchstaben angezeigt, die vom Betriebssystem noch nicht verwendet wurden.



Wenn das Volume mit einem Passwort verschlüsselt wurde, muss es beim Einbinden eingegeben werden.



Nun meldet VeraCrypt das erfolgreiche Mounten des Volume, hier im Beispiel mit dem Laufwerksbuchstaben `H:`.



Der Dateiexplorer von Windows wird unter dem gleichen Buchstaben ein weiteres Laufwerk anzeigen. Die Größe des Laufwerks wird durch die des Containers bestimmt. Im vorliegenden Beispiel sind es circa 100 Megabyte.

Versteckte Volumes

VeraCrypt bietet ein weiteres Feature an: das Anlegen von *versteckten Volumes* (*hidden volume*). Es ist für den Einsatz im akademischen Umfeld nicht so interessant, aber für die Nutzung auf Reisen, wo Externe Zugriff auf verschlüsselte Container bekommen und die Herausgabe von Daten erzwingen wollen. Es wird deswegen besonders Journalist:innen und Aktivisten empfohlen.

Die Grundidee hinter versteckten Volumes ist, in Zwangssituationen scheinbar nachzugeben, indem ein Passwort genannt wird, das Zugang zu verschlüsselten Dateien gibt. Diese Dateien sind aber nicht diejenigen, die man besonders schützen möchte. Sie sollten ausreichend wichtig scheinen, um glaubhaft zu machen, dass hier wirklich etwas preisgegeben wurde.

Die Dateien, die wirklich geschützt werden sollen, sind mit dem herausgegebenen Passwort nicht sichtbar. Für sie ist ein anderes Passwort notwendig. Mit diesem zweiten Passwort wird ein weiterer Bereich des VeraCrypt-Containers entschlüsselt und eingebunden.

Ohne Wissen des Passworts ist es nicht möglich, auf den versteckten Bereich zuzugreifen oder gar seine Existenz nachzuweisen. Folgende Punkte sollte man sich vorher klar machen:

- Die Qualität des Schutzes hängt von der des Passworts ab. Wenn Externe Zugriff auf das Speichermedium mit dem Container haben, können sie mit *Brute-Force* Passwörter beliebig durchprobieren. Es gibt keine Schutzmechanismen wie Begrenzung von Eingabeversuchen.
- Vor die Alternative gestellt, ein Passwort scheinbar unfreiwillig preisgeben zu müssen, sollte

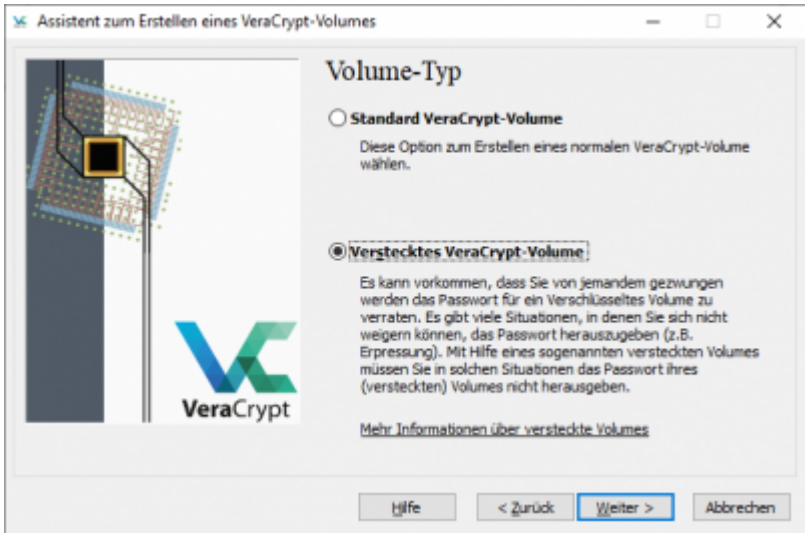
man in der Lage sein, dasjenige herauszurücken, das Zugriff auf den nicht versteckten Bereich im Container gibt. Das muss so überzeugend sein, dass einerseits die Gegenseite glaubt, sie habe ihr Ziel mit Gewalt erreicht, andererseits das Geheimnis gewahrt bleibt.
- **Ohne** das Passwort zum versteckten Volume sind die Daten darin unwiederbringlich verloren.

Anlegen eines versteckten Volumes

Im folgenden werden die Schritte erläutert, die zum Anlegen eines versteckten Bereichs zu machen sind. Es kann der Container benutzt werden, der gemäß der Anleitung aus dem Abschnitt *Volume anlegen* erzeugt wurde. Ein solcher ist notwendig als Hülle für den versteckten Bereich.

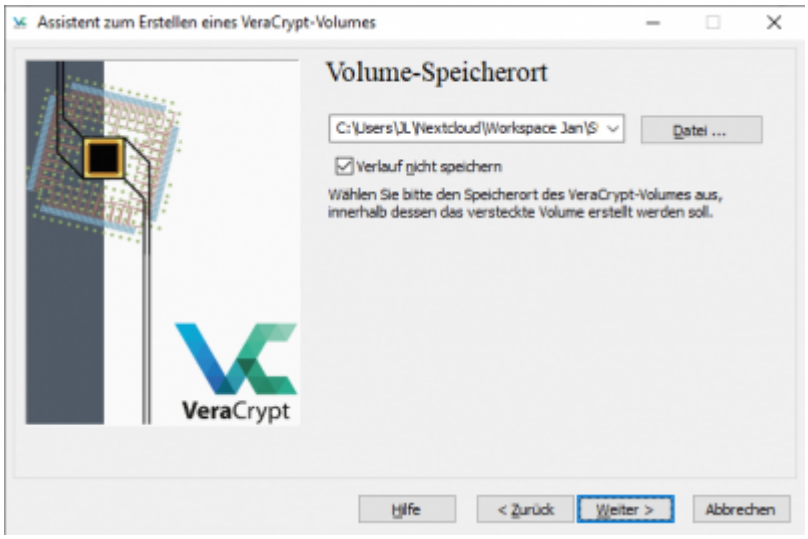
Der erste Schritt zu einem versteckten Volume ist der gleiche wie bei einem Standardcontainer mit Klick auf `Volumes→Neues Volume erstellen…`:

Im nächsten Dialog geht es anders weiter.



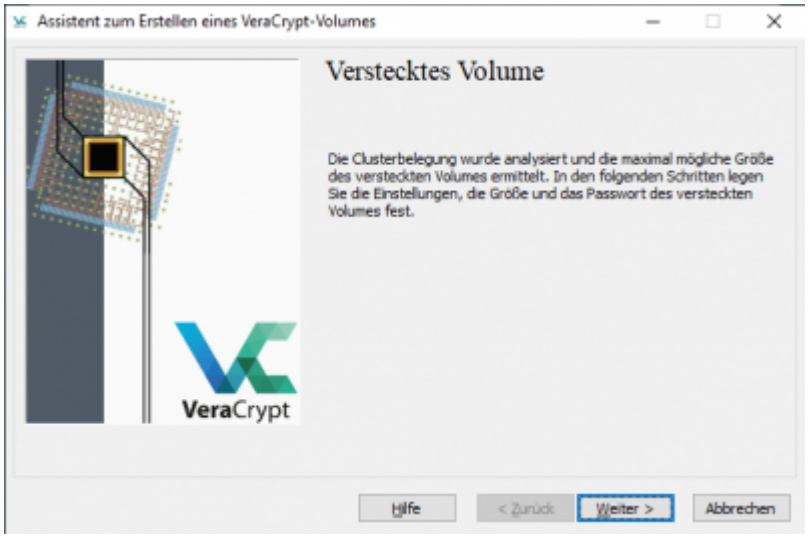
Nun sollte, da bereits ein Volume existiert, die zweite Option ausgewählt werden. Die erste Option würde zunächst ein nur einfach verschlüsseltes Volume anlegen, wie es oben schon beschrieben ist.

Über den Dialog für Dateien sollte der existierende Container ausgewählt werden.



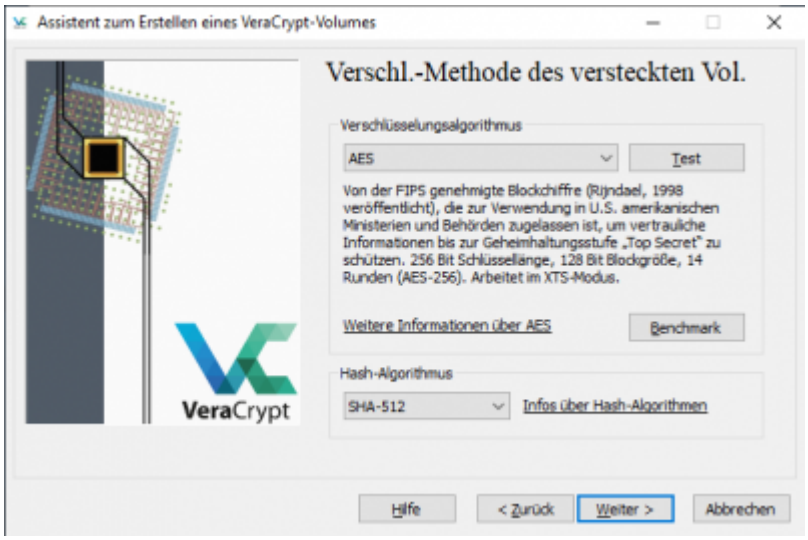
Um auf die existierende Hülle zugreifen zu können, muss zuvor noch ihr Passwort angegeben werden.

Mit dem richtigen Passwort beginnt der Assistent für das Anlegen eines versteckten Volumes.



Als erstes sind die Algorithmen für die Verschlüsselung und das Hashing zu wählen. Die Vorauswahl von *AES* für die Verschlüsselung und *SHA-512* kann übernommen werden.

Für die Erläuterung der Optionen sei auf die Hilfe von VeraCrypt oder die Fachliteratur verwiesen. Ein tieferes Verständnis ist für die Nutzung von VeraCrypt nicht notwendig.



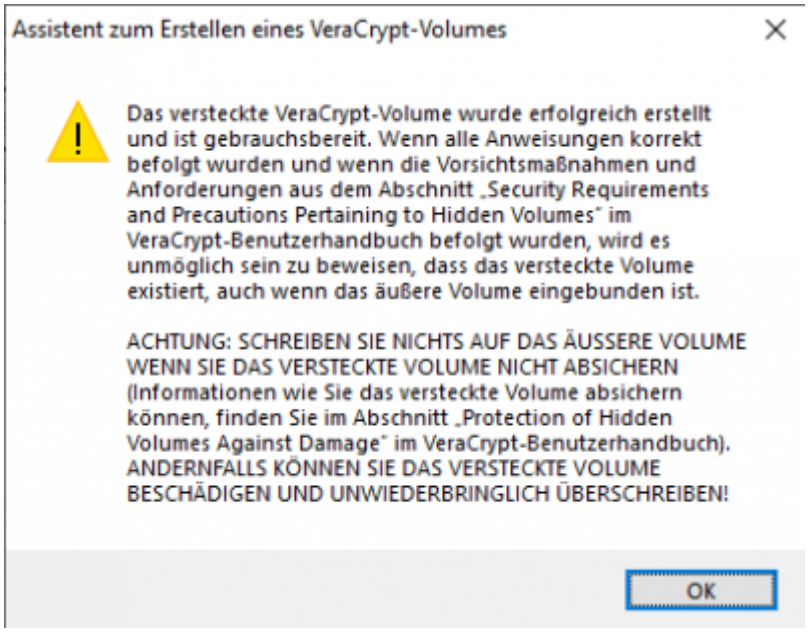
Im nächsten Schritt ist zu bestimmen, wie groß das versteckte Volume sein soll. Die maximale Größe ist theoretisch durch diejenige des äußeren Volumes festgelegt, jedoch sollte das versteckte deutlich kleiner als das äußere Volume sein, um Platz für die Dateien dort zu lassen. Am Ende müssen, falls dieses Feature wirklich eingesetzt werden soll, die Dateien im äußeren Container glaubhaft machen, hier sei etwas wertvolles offenbart worden.

Nun muss noch das Geheimnis für den versteckten Bereich ausgewählt werden. In den meisten Fällen wird es ein Passwort sein. Prinzipiell braucht ein solches nirgends aufgeschrieben sein, doch setzt das ein zuverlässiges und präzises Gedächtnis voraus. Das hier gezeigte Passwort ist verbrannt und sollte nicht benutzt werden. Es wird nur als Beispiel verwendet.

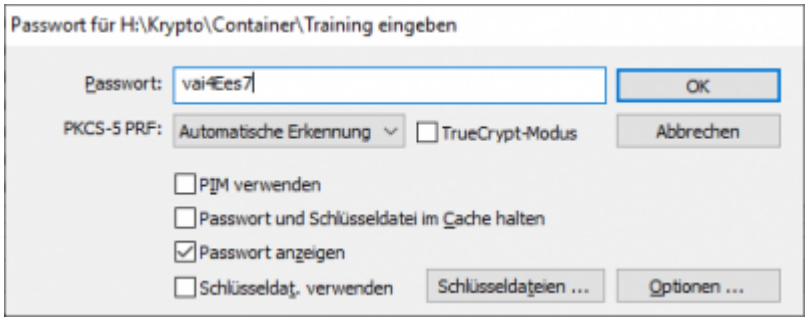
Wiederum wird über die Auswertung der Mausbewegungen die Entropie ermittelt.

Sofern alle Schritte richtig gemacht wurden, gibt es zum Schluss eine Meldung, dass das Volume

korrekt angelegt ist.

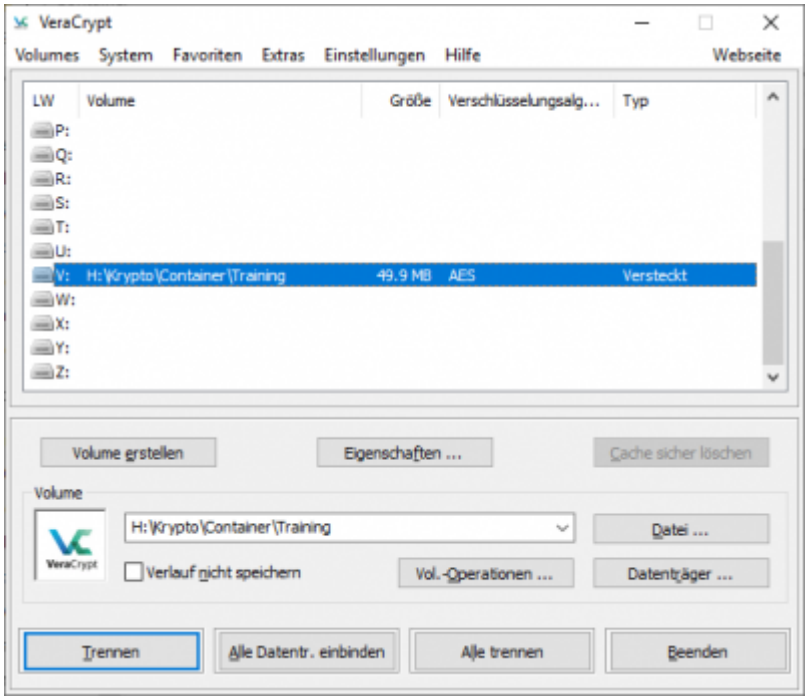


Einbinden eines versteckten Volumes



Der Ablauf beim Einbinden eines versteckten Volumes ist bekannt, er entspricht dem des Einbindens eines normalen Volumes. Sobald es gemountet ist, wird es in VeraCrypt angezeigt, allerdings mit dem Typ „Versteckt".

Im Windows-Explorer, mit dem Dateien und Ordner organisiert werden, ist kein Unterschied zu sehen zwischen den beiden Varianten.



Referenzen

https://securityinabox.org/en/guide/veracrypt/windows/

https://www.veracrypt.fr/en/Beginner%27s%20Tutorial.html

https://www.rz.uni-freiburg.de/services/serverdienste/fileserver