

Kaltstartangriffe und Hidden Volumes, minderlegal reloaded



Multiple nested encrypted containers, inspired by VeraCrypt, layered vaults inside each other, glowing secure cores, digital locks and keyholes, symbol of strong cryptography, dark background, blue and cyan light, ultra detailed, cinematic lighting, 3d render, octane style --ar 3:2 --s 750 (Midjourney)

Ich habe mich kurz umgesehen, was es an verständlichen Anleitungen gibt, ein *hidden volume* mit Veracrypt anzurichten. Es gibt einige und [recht gute](#) (auf Englisch), sogar [für Lehrer](#).

Wenn man weiß, [wie Veracrypt funktioniert](#), ist es fast selbsterklärend.

Merke: *Bevor Sie ein komplettes Laufwerk inklusive Daten verschlüsseln, sollten Sie die Dateien zuvor unbedingt sichern. Zwar arbeitet Veracrypt seit Jahren sehr zuverlässig, doch Fehler können trotzdem passieren.*

Das habe ich noch nie gemacht. So viele Daten, die privat bleiben sollten, habe ich gar nicht. Ich begnüge mich mit Containern und verschlüsselten USB-Sticks (vor allem auf Reisen). Umgekehrt: Wenn man das ganze Laufwerk des Rechners

verschlüsselt, braucht man *keine* Container.

Aber: Wozu sollte man *hidden volumes* überhaupt haben? Für [misstrauische Ehepartner](#)?

Ich habe mir ein Szenario überlegt, das vielleicht für Geschäftsleute realistisch ist, die davon ausgehen müssen, dass sie in dem Land, in dem sie gerade sind, [gezwungen werden](#), den Inhalt ihrer Rechner den neugierigen Augen der dortigen Sicherheitsbehörden preiszugeben, etwa China und Hongkong, USA, Großbritannien, Kanada. (Fährt hier jemand oft nach Russland? Weiterlesen!)



Ich muss ein bisschen ausholen. Vor Jahren habe ich ein Vortrag in einem großen Rüstungskonzern über Sicherheit und Recherche gehalten und einer der Teilnehmer fragt, ob von ihrer Firma etwas im Darknet zu finden sei. Nichts leichter als das.

Man muss natürlich die Realität berücksichtigen; In welcher Firma ist es erlaubt, den Tor-Browser zu installieren und in dunkelsten Ecken des Netzes herumzusurfen? Ich habe schon in internationalen Konzernen gearbeitet, die sich IT-mäßig als Hochsicherheitstrakt – ohne jedwede Fremdgeräte – gaben, aber natürlich lagen alle Daten bei Microsoft in der Cloud.

Ich fand damals irgendwelche internen Preislisten der Firma im Darknet und löste eine gewissen Panik aus nach dem Motto:

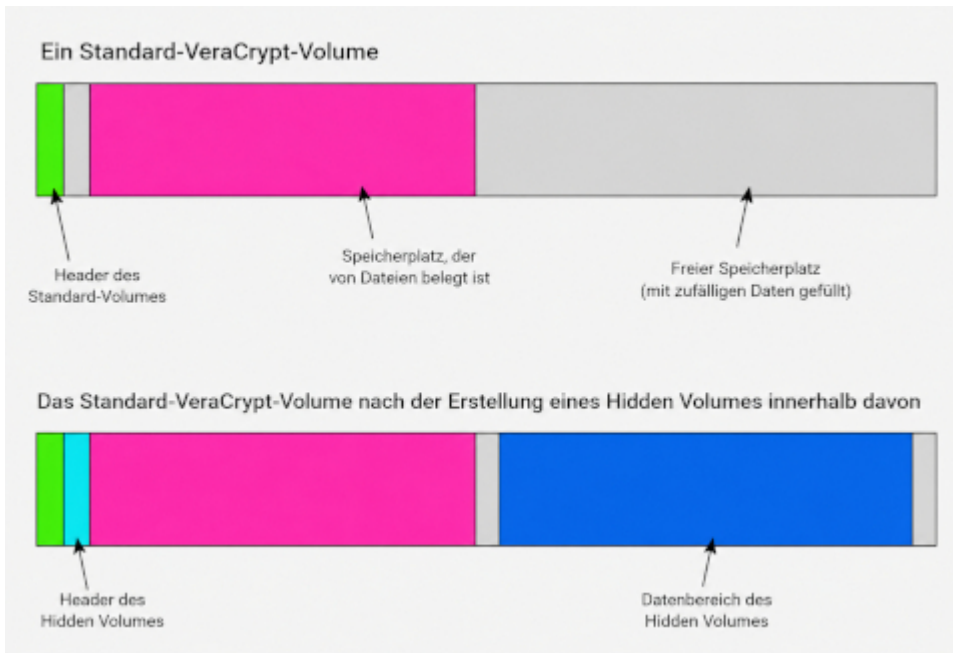
Kriegt man das wieder da weg?

Nehmen wir an, wie schicken dem potenziellen Geschäftskunden keine verschlüsselte E-Mails, sondern möchte bestimmt Dokumente, die viel wert sind, persönlich diskutieren. Und die Konkurrenz sollte davon auch nichts erfahren.

Es fängt schon bei den *basics* an und mit der – bei Microsoft-Hassern – [legendären Schlagzeile](#) „Microsoft Word bytes Tony Blair in the butt“. Oder jemand erstellte ein PDF für uns mit eingebettetem Javascript, das beim Aufrufen [dieses](#) und [jenes](#) aus dem Internet lädt. „Wenn es mehrere Möglichkeiten gibt, eine Aufgabe zu erledigen, und eine davon in einer Katastrophe endet oder sonst wie unerwünschte Konsequenzen nach sich zieht, dann wird es jemand [genau so machen](#).“

Wir haben uns bemüht das zu vermeiden, und wollen zwei Dutzend Dokumente absolut sicher verbergen, auch wenn die Briten, Russen und US-Amerikaner unseren Laptop bei der Einreise auseinandernehmen, die Daumenschrauben rausholen und verkünden: Wenn du uns nicht alle Passwörter verrätst, musst du wieder heim!

Wir machen es richtig schwer. Die Chinesen sagen sogar: Öffnen Sie den Veracllypt-Containel! Und wenn der leer ist, werden sie erst recht misstrauisch.



Wenn wir nicht freiwillig verraten, dass da noch in den Tiefen ein *hidden volume* schlummert, sind wir auf der sicheren Seite – mit kleineren Einschränkungen, die zu beachten wären.

Segment	Bedeutung	Erklärung
Header des Standard-Volumes	Startbereich des normalen VeraCrypt-Volumes	Enthält die verschlüsselten Informationen, mit denen VeraCrypt das äußere Volume öffnen kann.
Speicherplatz, der von Dateien belegt ist	Sichtbare Dateien im äußeren Volume	Hier liegen die normalen, harmlosen Dateien, die beim Öffnen mit dem äußeren Passwort sichtbar werden.

Segment	Bedeutung	Erklärung
Freier Speicherplatz	Scheinbar leerer Bereich	Dieser Bereich ist mit Zufallsdaten gefüllt. Dadurch ist nicht erkennbar, ob er wirklich leer ist oder ein Hidden Volume enthält.
Header des Hidden Volumes	Startbereich des versteckten Volumes	Wird nur mit dem Passwort des Hidden Volumes erkannt. Für Außenstehende sieht er wie Zufallsdaten aus.
Datenbereich des Hidden Volumes	Geheimer Speicherbereich	Hier liegen die eigentlichen geheimen Dateien. Ohne das richtige Passwort ist dieser Bereich nicht vom übrigen Zufallsdatenbereich zu unterscheiden.

Wer das noch nie gemacht hat und des Lesens von kurzen Texten mächtig ist: Bei VeraCrypt wird ein Hidden Container (bei mir unter Linux) über die grafische Oberfläche genauso geöffnet wie ein normaler Container.

Zunächst startet man VeraCrypt über das Anwendungsmenü und klickt anschließend auf *select file (Veracrypt gibt es auch auf Deutsch)*, um die Container-Datei auszuwählen. Danach markiert man einen freien Slot (oder „Laufwerk“) und klickt auf *mount*.

Entscheidend ist allein das eingegebene Passwort: Wird das

Passwort des **äußeren Containers** (oder *volume*) eingegeben, öffnet VeraCrypt das normale äußere Volume; wird dagegen das Passwort des **Hidden Volumes** eingegeben, wird automatisch das versteckte Volume geöffnet.

Es gibt dafür keinen besonderen Menüpunkt und auch keine separate Datei für das Hidden Volume, da sich beide Bereiche innerhalb derselben verschlüsselten Containerdatei befinden.

Nach erfolgreichem Einhängen erscheint das Volume wie ein normales Laufwerk im Dateimanager. Wichtig ist außerdem, dass beim Öffnen des äußeren Volumes Schreibzugriffe das versteckte Volume beschädigen können. Deshalb sollte man beim Mounten des äußeren Volumes in den „Mount Options“ [die Funktion](#) „Protect hidden volume against damage caused by writing to outer volume“ aktivieren und zusätzlich das Passwort des Hidden Volumes angeben.

Bei VeraCrypt bleibt ein Hidden Volume auch dann unsichtbar, wenn man beim Öffnen des äußeren Containers die Funktion *mount all devices* beziehungsweise „Alle Datenträger einhängen“ verwendet: **Das versteckte Volume ist technisch kein eigenes Laufwerk und keine eigene Datei.** Äußeres Volume und Hidden Volume befinden sich innerhalb derselben verschlüsselten Containerdatei oder Partition. VeraCrypt erkennt daher nicht zwei getrennte Datenträger, sondern nur einen einzigen verschlüsselten Container. Welcher Bereich tatsächlich geöffnet wird, entscheidet ausschließlich das eingegebene Passwort.

Technisch ist das Hidden Volume zwar nicht von zufälligen verschlüsselten Daten zu unterscheiden. In der Praxis entstehen aber unter Umständen Hinweise durch das Verhalten des Nutzers oder durch „Daten-Beifang“ außerhalb des Containers.



Multiple nested encrypted containers, inspired by VeraCrypt, layered vaults inside each other, glowing secure cores, digital locks and keyholes, symbol of strong cryptography, dark background, blue and cyan light, ultra detailed, cinematic lighting, 3d render, octane style -ar 3:2 -s 750 (Gemini)

Ein Risiko: Das äußere Volume wirkt ungewöhnlich leer. Wenn ein großer Container vorhanden ist, sich darin aber nur wenige harmlose Dateien befinden und gleichzeitig nur wenig freier Speicher angezeigt wird, kann dies Verdacht erregen. Deshalb empfiehlt VeraCrypt, das äußere Volume mit glaubwürdigen Dummy-Dateien zu füllen, damit der belegte Platz plausibel erscheint.

Ich würde als Geschäftsmann daher in den äußeren Container Duplikate aller meiner geheimen Dokumente legen, aber mit falschen Zahlen und Angaben, am besten noch mit „streng geheim“ markiert, und beim erzwungenen Öffnen des (äußeren) Containers händeringend in Tränen ausbrechen.

ChatGPT warnt: Auch Metadaten außerhalb des Containers können problematisch sein. Beispielsweise können Dateimanager, Backup-Programme oder Cloud-Synchronisationsdienste Hinweise liefern, dass bestimmte Dateien häufiger benutzt werden, als es der sichtbare Inhalt des äußeren Volumes vermuten lässt. Ebenso können temporäre Dateien, Vorschaubilder, zuletzt geöffnete Dokumente oder [Einträge in der Shell-History](#)

verraten, dass mit sensiblen Daten gearbeitet wurde.

Ein weiteres Risiko liegt in forensischen Analysen des Systemspeichers. Wenn ein Hidden Volume geöffnet ist, können Schlüsselmaterial oder Dateinamen zeitweise im RAM vorhanden sein. Wird ein laufendes System beschlagnahmt oder ein sogenannter [Cold-Boot-Angriff](#) durchgeführt, könnten Ermittler Hinweise auf ein geöffnetes verstecktes Volume finden. Deshalb schützt VeraCrypt vor allem ruhende Daten ([Data at rest](#)), nicht unbedingt ein bereits laufendes und entsperartes System.

Ich habe natürlich einen unschlagbaren Vorteil – solange niemand mein Blog liest: Bei meinem Alter werden Grenzbeamte sich vermutlich fragen, ob ich den Unterschied zwischen einem Betriebssystem und einem Browser kannte. Und ich werde harmlos lächeln und mich angemessen verbeugen.