ASAN · Berlin

Autonomes • Solidarisches • Antifaschistisches • Netzwerk • Berlin

Basics zur sicheren Kommunikation

Daten Verschlüsselung mit VeraCrypt

Version 1.0.1 – Stand 22.03.2020

Einleitung

Willkommen bei dieser kleinen Anleitung, Deine Aktivitäten sicherer, den Bonzen, Bullen und dem VS das Leben erheblich schwerer zu machen.

Denke immer daran:

Nur was Du in Deinem Kopf hast und behältst ist wirklich sicher!

Sobald Du anfängst Deine Gedanken in Wort, Bild und Ton über digitale Medien mit anderen zu teilen, bist Du nicht mehr allein. Du kannst Dir niemals zu 100% sicher sein, dass Deine Informationen nur die Menschen erreichen, für die sie bestimmt sind.

Wirklich wichtige Informationen teile darum immer nur persönlich OHNE ein fremdes Transportmedium wie Telefon und Internet mit!

„Ich habe doch nichts zu verbergen“ – Richtig! Ich auch nicht!

Allerdings möchte ich selbst bestimmen können, mit wem ich kommuniziere und welche Gedanken ich mit wem teile. Kurz gesagt: was Du in Deinem täglichen Leben tust geht niemensch etwas an!

Du kannst mit einigen wenigen Schritten und Deinem Verhalten im Umgang mit digitalen Medien Deine Kommunikation erheblich sicherer gestalten, Deine Privatsphäre besser abschirmen, Dich selbst und Dein soziales Umfeld vor staatlichen Repressionen schützen.

Viele wollen ihren Computer, Tablett oder Smart Phone einfach nur nutzen und sich nicht zum „Nerd“ entwickeln. Bonzen und Bullen wollen den gläsernen Bürger und haben null Interesse daran, für Deine Sicherheit und den Schutz Deiner Privatsphäre zu sorgen.

Schlimmer noch, das PAG kommt oder ist in einigen Bundesländern bereits aktiv, neben der Aufhebung der ohnehin schon weitgehend aufgeweichten elementaren Grundrechte folgt nun der Generalverdacht der Bevölkerung und die damit einhergehende Überwachung der Netze ohne konkreten Grund.

Die Handhabung mag zu Anfang vielleicht etwas komplizierter oder umständlich erscheinen. Sich daran zu gewöhnen ist jedenfalls einfacher, als an eine 8 qm große Zelle, zu der Du den Schlüssel weggeworfen hast, mit dem sie Dich eingesperrt haben.

Komplizierte Programme und unfreundliche Handhabung schrecken ab, diese Anleitung soll Dir einen möglichst leichten Einstieg in die Thematik geben und den Umgang damit erleichtern.

Diese Anleitung beansprucht nicht vollständig oder 100%ig sicher zu sein. Auch besteht nicht der Anspruch, die hier verwendete Programm als einzig und allein „sicher“ oder herausragend „gut“ zu bewerten.

Die Screenshots wurden auf einem Windows PC erstellt und können bei anderen Betriebssystemen abweichend sein.

VeraCrypt verfügt über „Hilfe“ eine sehr detaillierte Beschreibung des Programms, sowie eine Kurzanleitung in englischer Sprache.

Für Fragen, Korrekturen und Verbesserungen gerne an: x-berg@systemli.org

Inhalt

VeraCrypt 1.24 Update 6 4

Anwendung 5

Traveler-Disk-Installation 6

Ein verschlüsseltes Laufwerk, USB Stick oder Containerdatei einbinden 8

Ein verschlüsselte Containerdatei erstellen 9

Eine Partition/Laufwerk verschlüsseln 14

Ein Systempartition/Laufwerk verschlüsseln 19

Volume Passwort ändern 20

Die Option PIM und wozu wird sie benötigt 24

Die VeraCrypt Einstellungen 25

VeraCrypt 1.24 Update 6

VeraCrypt ist die aktuelle Weiterentwicklung von TrueCrypt, ein open source Programm und dient zur Verschlüsselung ganzer Laufwerke (Volumes) + USB Sticks oder Partitionen, auch dem Startlaufwerk (Systemlaufwerk), sowie der Erstellung von sogenannten „Containerdateien“.

Containerdateien sind große verschlüsselte Dateien ab 1 MB bis XX, die wie ein Laufwerk eingebunden und auf denen beliebige Dateien gespeichert werden können.

VeraCrypt steht für folgende Betriebssysteme zur Verfügung:

- Windows
- Mac OS X
- Linux
- FreeBSD 11

Download: https://www.veracrypt.fr/en/Downloads.html

Die Installation ist selbsterklärend, das Programm steht nach Installation in vielen Sprachen (auch Deutsch) zur Verfügung.

Der Assistent führt Dich auch in der Sprache Deiner Wahl durch alle Schritte und erläutert Dir die wichtigsten Informationen zu den einzelnen Schritten oder Optionen.

Wichtig!

Präge Dir Dein Passwort gut ein, es gibt **keine** Möglichkeit, ein vergessenes Passwort wiederherzustellen oder Verschlüsselungen ohne gültiges Passwort zu entschlüsseln!

Bevor Du nun alles verschlüsselst und ggf. noch Dein Bootlaufwerk verschlüsseln möchtest (was sehr empfohlen wird), denke daran, dass der Bootvorgang dadurch länger dauert und auch das Entschlüsseln die Leistung Deines Rechners belasten kann.

Die einmalige Verschlüsselung kann bei großen Laufwerken oder Partitionen – vor allem in-place (ohne Formatierung), wenn die bereits gespeicherten Daten erhalten bleiben sollen – viele Stunden, manchmal auch Tage in Anspruch nehmen.

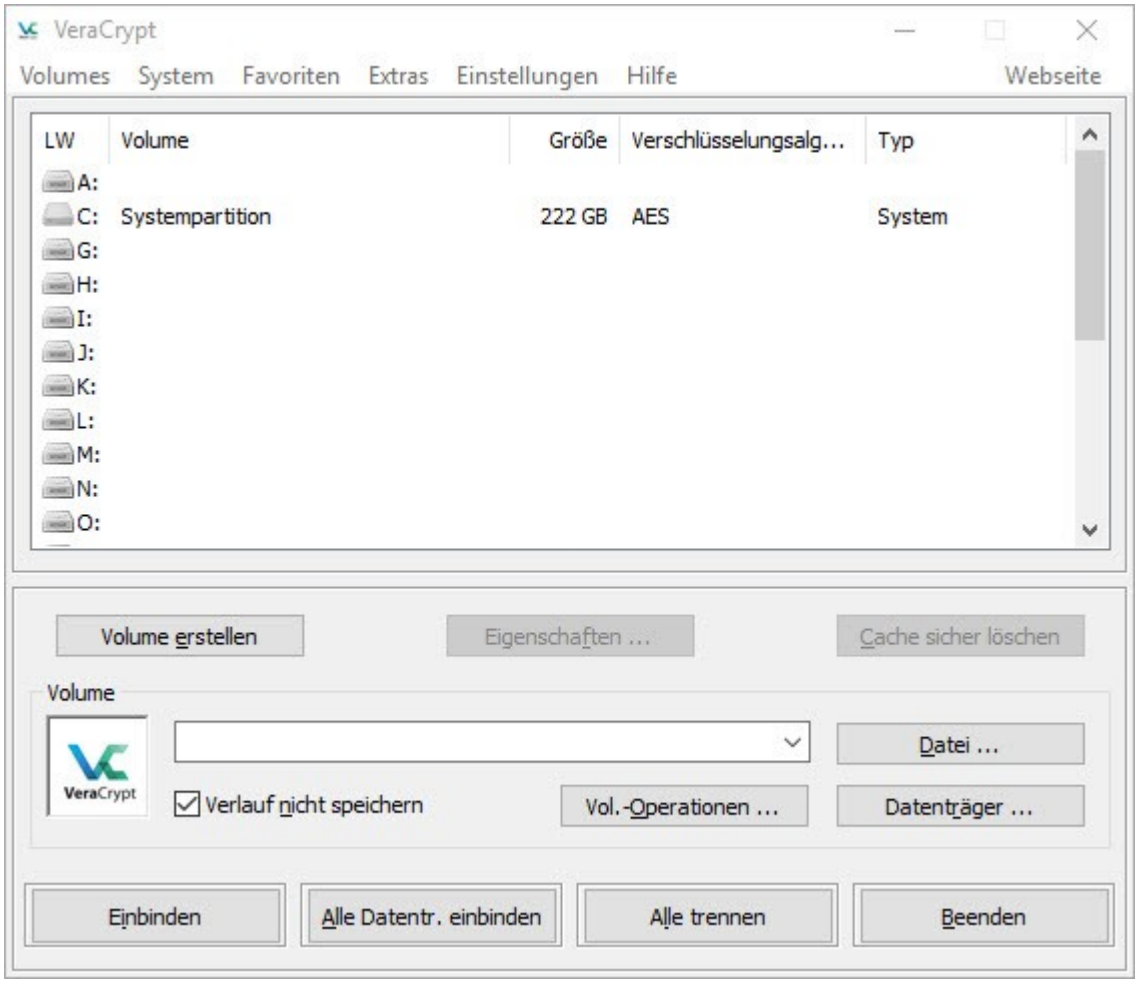
Und noch etwas:

Wenn Du ein Laufwerk, Container oder Partition neu erstellt und den Datenträger damit formatiert hast, kannst Du damit anfangen, sensible Daten an Deinen sicheren Ort zu kopieren.

Wenn Du die Daten danach auf dem ursprünglichen Speicherort löschst, achte immer darauf, eine sichere Löschmethode zu verwenden! Die Dateien könnten sonst einfach rekonstruiert werden.

Auch dafür gibt es kleine kostenlose Tools wie zum Beispiel den CCleaner die das für Dich erledigen, bei großen Datenmengen dauert auch dieser Vorgang erheblich länger als der Klick „Papierkorb leeren“.

Anwendung



Im Arbeitsbereich sind zunächst alle wichtigen Informationen für den Gebrauch enthalten. Eine ausführliche Dokumentation ist in Englisch unter „Hilfe“ verfügbar.

Volume erstellen: erzeugen von verschlüsselten Laufwerken oder Container Dateien

Eigenschaften: zeigt die Eigenschaften eines verschlüsselten Laufwerkes an

Cache sicher löschen: löscht alle Passwörter (die auch verarbeitete Schlüsseldateien enthalten können), die im Treiberspeicher zwischengespeichert werden. Wenn sich im Cache keine Kennwörter befinden, ist diese Schaltfläche deaktiviert.

Datei: hier kann die Containerdatei ausgewählt werden, die eingebunden werden soll

Vol. Operationen: Änderung für Einstellungen eines ausgewählten Laufwerks

Datenträger: Auswahl von Festplatten, Partitionen oder USB Sticks die eingebunden werden sollen

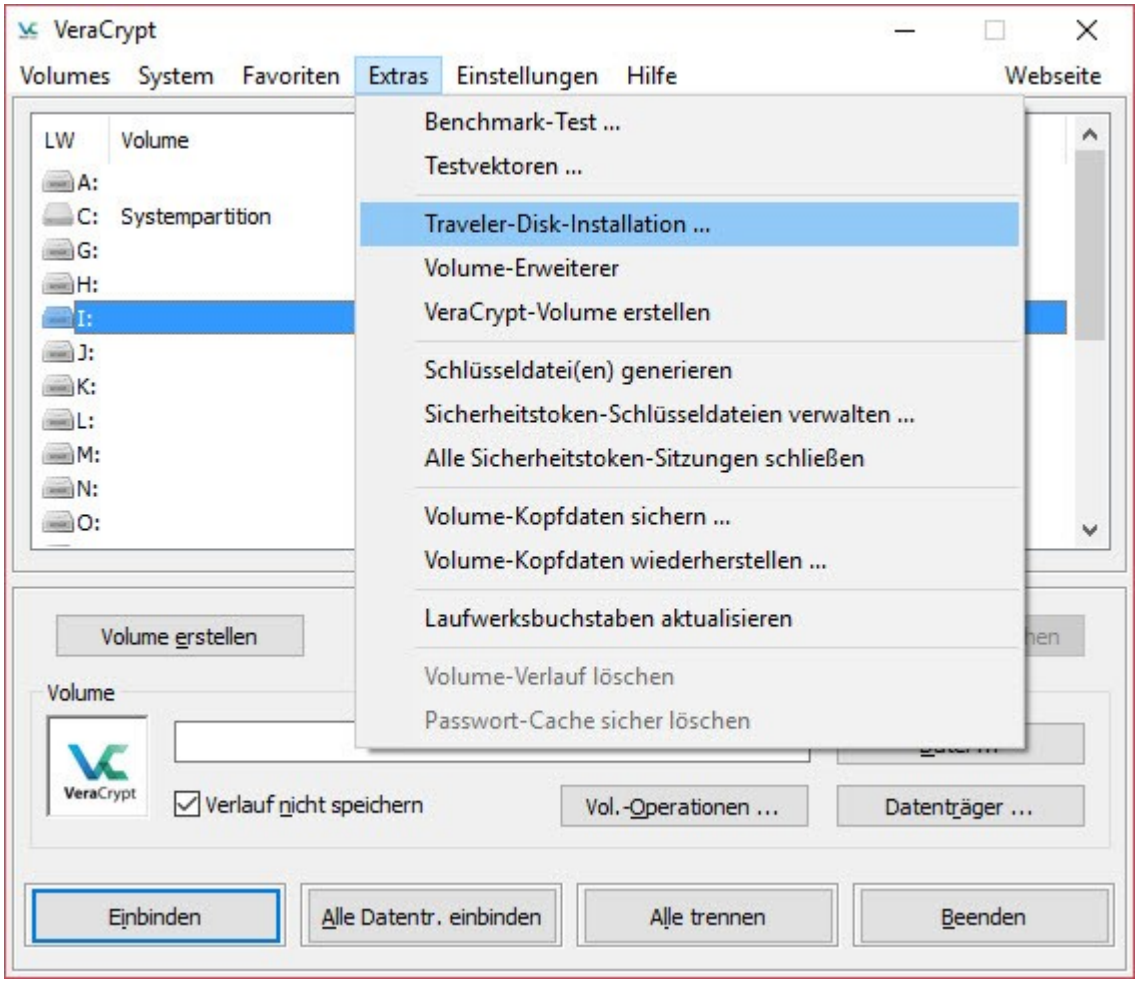
Einbinden: eines Containers, einer Partition, Laufwerks oder USB Sticks

Alle Datentr. Einbinden: bindet mehrere angeschlossene Laufwerke, USB Sticks, Container ein

Alle trennen: trennt alle eingebundenen Laufwerke und verschlüsselt sie wieder

Beenden: das Programm schließen

Traveler-Disk-Installation



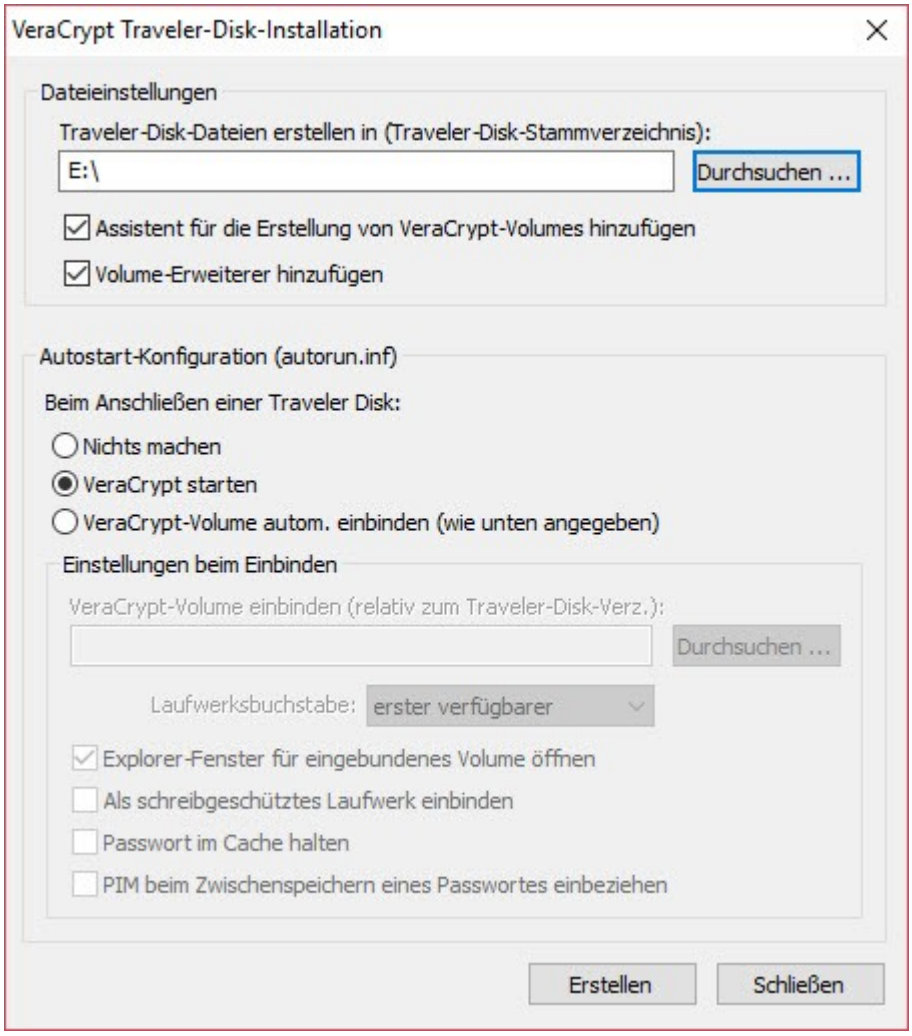
Damit Du Deine Wechselfestplatte oder Deinen USB Stick auch bei Menschen nutzen kannst, die VeraCrypt nicht installiert haben, kannst Du mit wenigen einfachen Schritten eine sog. Traveler-Disk-Installation auf einem USB Stick erstellen.

Damit kannst Du VeraCrypt auch auf einem Rechner nutzen und auf Deine verschlüsselten Daten zugreifen, ohne auf einem Fremden Rechner das Programm installieren zu müssen. Voraussetzung dafür ist allerdings, dass Du Administratorberechtigung hast, um Programme von einem USB Stick zu starten.

Den Assistenten findest Du unter „Extras“ → Traveler-Disk-Installation.

Wichtig:

Auch wenn das Programm nicht installiert und vom USB Stick mobil gestartet wurde, sind auf dem Windows PC Registry Einträge vorhanden, anhand dessen nachgewiesen werden kann, dass das Programm VeraCrypt auf diesem Rechner gestartet wurde.



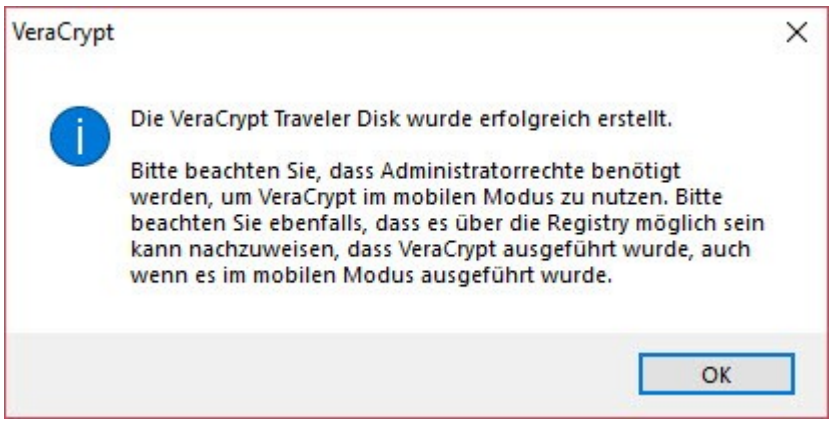
Mit „Durchsuchen“ kannst Du das Laufwerk oder den USB Stick auswählen, auf dem die Traveler-Disk-Installation erfolgen soll und welche Programmmodule installiert werden sollen.

Darüber hinaus was geschehen soll, wenn Du Deine Traveler-Disk an den PC steckst.

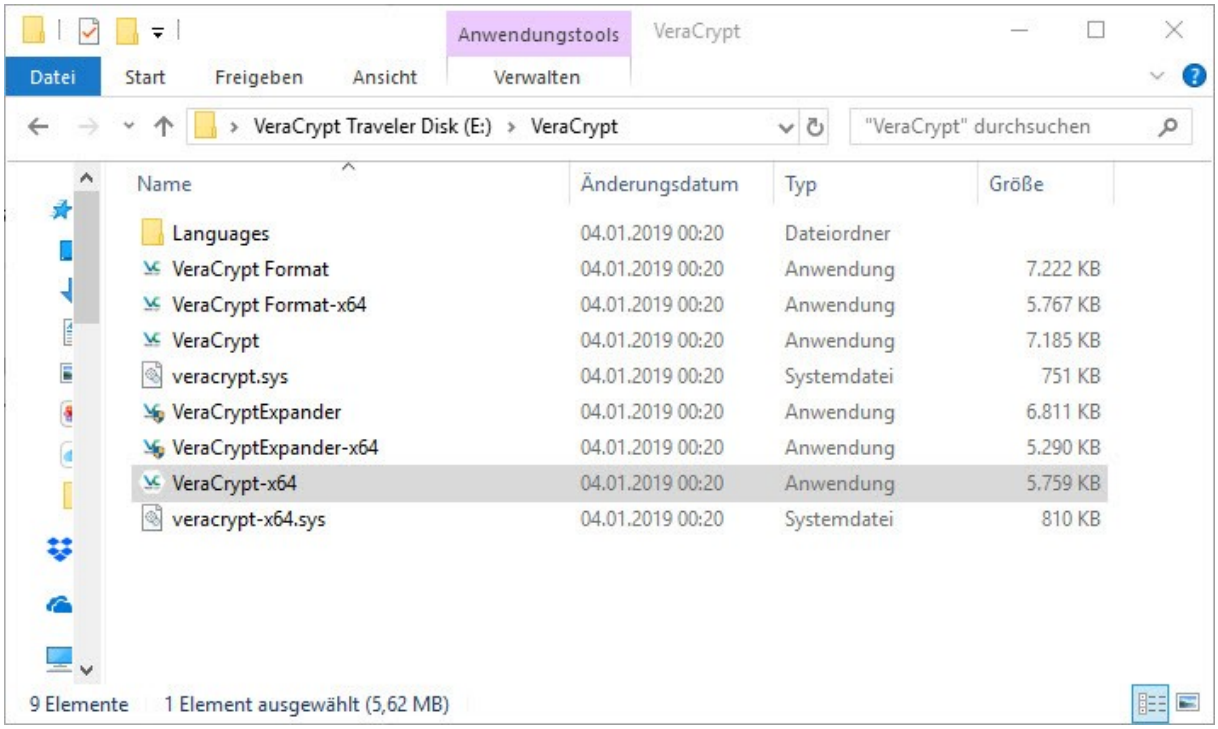
Hinweis:

Abhängig von der Systemkonfiguration kann die Autostartfunktion von Wechseldatenträgern nicht funktionieren. Dann kannst Du im Verzeichnis „VeraCrypt“ das Programm manuell starten.

Mit „Erstellen“ wird die Traveler-Disk-Installation dann ausgeführt.



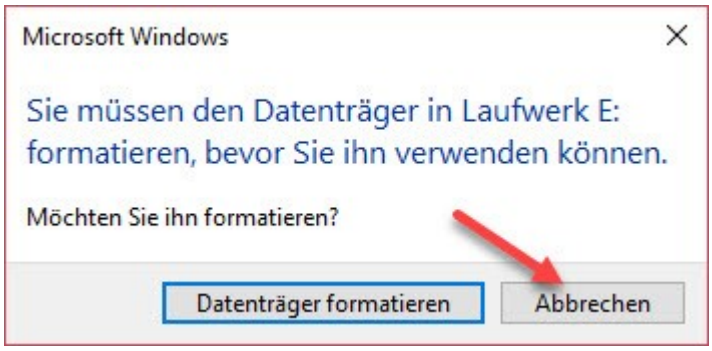
Fertig, Deine Traveler-Disk-Installation wurde abgeschlossen.



Hier findest Du auf Deiner Traveler-Disk im Verzeichnis „VeraCrypt“ die gleichnamige Anwendung x32 oder x64.

Ein verschlüsseltes Laufwerk, USB Stick oder Containerdatei einbinden

Wenn Du ein verschlüsseltes Laufwerk oder USB Stick anschließt, erhältst Du unter Windows immer folgende Fehlermeldung:



Diese Fehlermeldung ist leider „normal“, da ein verschlüsseltes Laufwerk oder USB Stick von Windows nicht gelesen werden kann und als nicht formatiert erkannt wird.

Klicke unbedingt auf „Abbrechen“! – mit „Datenträger formatieren“ zerstörst Du Dein verschlüsseltes Laufwerk und alle gespeicherten Daten sind verloren.

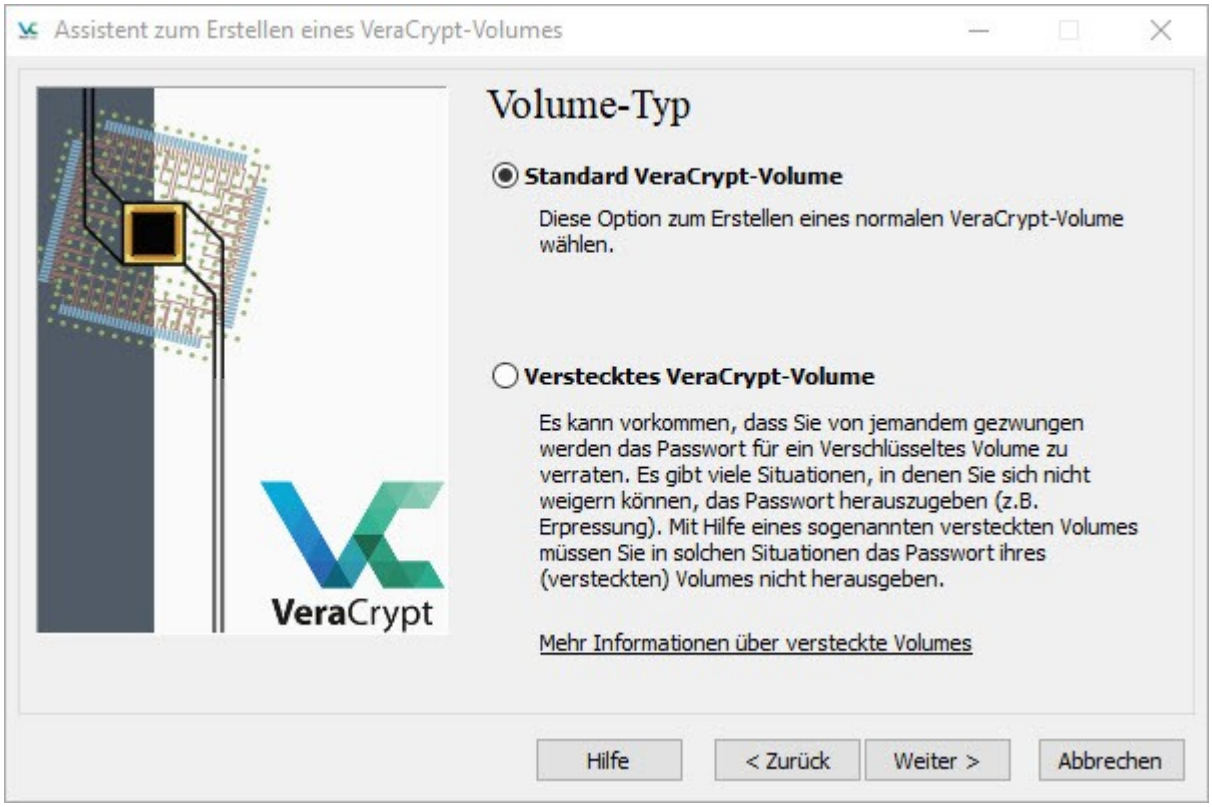
1. Wähle im VeraCrypt Anwendungsfenster einen freien Laufwerksbuchstaben
2. Klicke auf „Datei“ oder „Datenträger“ um Deine Containerdatei oder Laufwerk zu bestimmen
3. Klicke auf „Einbinden“, gebe Dein Passwort ein und bestätige mit „OK“

Dein Laufwerk oder USB Stick steht Dir nun wie gewohnt zur Verfügung.

Mit Laufwerk trennen wird Dein Laufwerk oder USB Stick wieder sicher verschlüsselt.

Ein verschlüsselte Containerdatei erstellen

Zuerst klickst Du auf Volume erstellen, wählst „Eine verschlüsselte Containerdatei erstellen“ und klickst auf „Weiter“



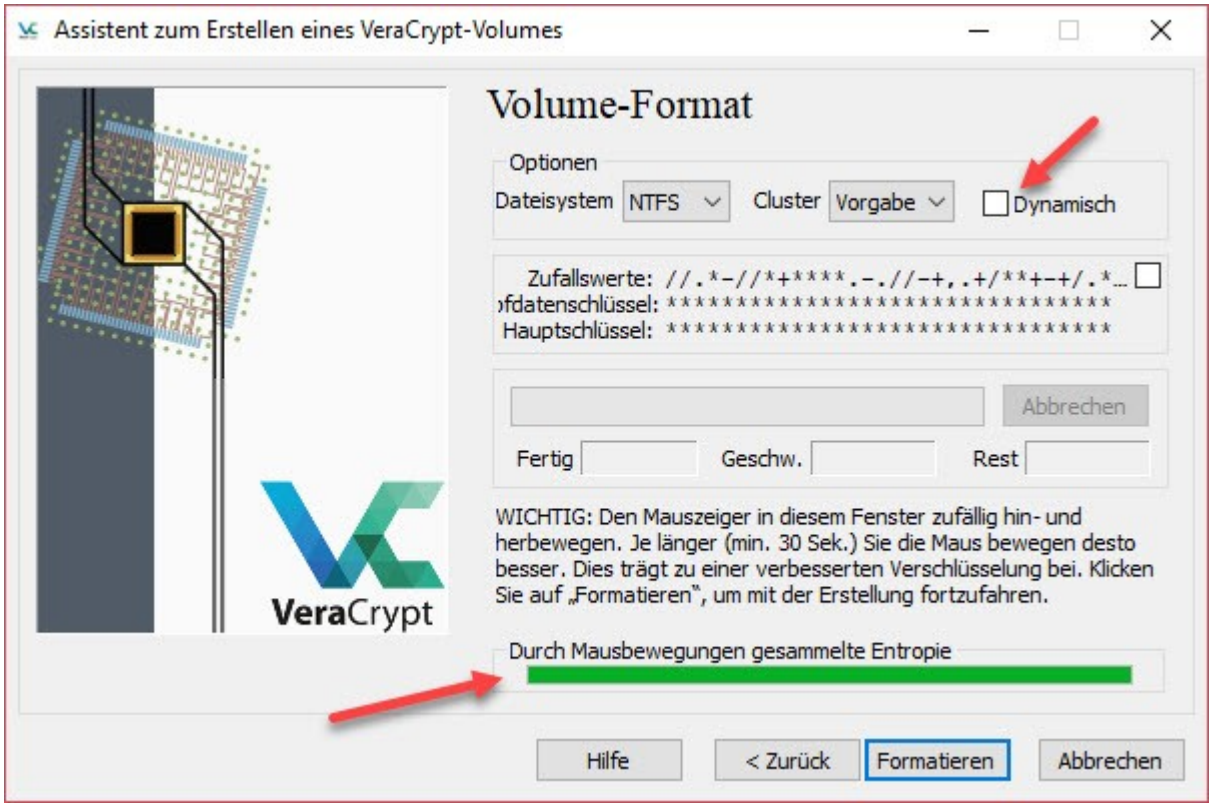
Hier kannst Du wählen, ob Du ein Standard VeraCrypt Volume oder ein verstecktes VeraCrypt Volume erstellen möchtest. Anschließend auf „Weiter“ klicken.

Klicke auf „Datei…", lege Dateinamen und Speicherort fest und klicke anschließend auf „Weiter"

Hier kannst Du den Verschlüsselungsalgorithmus und den Hash-Algorithmus anpassen. Anschließend auf „Weiter" klicken.

Hier kannst Du festlegen, wie groß Deine Containerdatei sein soll. Eine dynamische Größe kannst Du an späterer Stelle noch auswählen → „Weiter“

An dieser Stelle musst Du das Passwort festlegen, bitte beachte die Hinweise zu einem sicheren Passwort. Unter 20 Zeichen bekommst Du nach „Weiter“ eine Hinweismeldung, Du kannst entweder Dein Passwort anpassen oder die Hinweismeldung ignorieren.

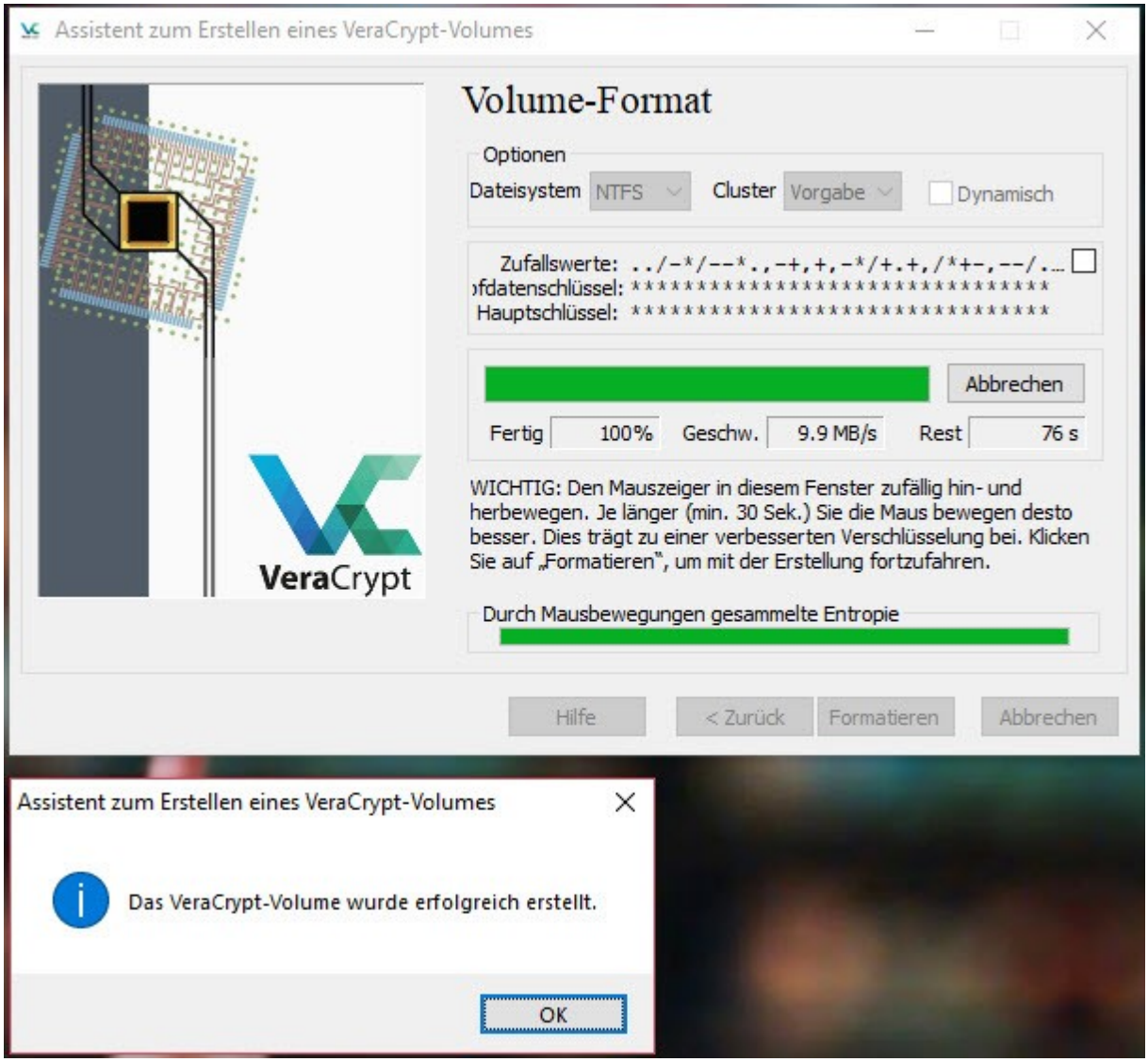


Hier kannst Du das Dateisystem festlegen. Wenn Du „Dynamisch" anklickst (Pfeil oben), erweitert sich die Größe Deines Containers bis zum dem Maximalwert, den Du bei „Volume Größe" angegeben hast.

Wichtig!

In diesem Fenster die Maus einfach zufällig hin und her bewegen, bis sich die Anzeige (Pfeil unten) in den grünen Bereich bewegt, möglichst bis zum Ende der Anzeige.

Anschließend auf „Formatieren" klicken, Deine Containerdatei wird jetzt erstellt.



Abhängig von der Größe der Containerdatei und der Prozessorleistung kann dieser Vorgang längere Zeit in Anspruch nehmen.

Der Assistent zeigt Dir eine Hinweismeldung, wenn der Vorgang vollständig abgeschlossen wurde.

Deine Containerdatei findest Du an dem Speicherort, den Du bei „Volume-Speicherort“ eingestellt hast.

Über das Button „Datei…“ kannst Du Deinen neu erstellten Container auswählen, klicke einen freien Laufwerksbuchstaben an und mit „Einbinden“ nach Eingabe Deines Passwortes als Laufwerk laden.

Jetzt kannst Du wie auf einer Festplatte oder einem USB Stick auf Deine Dateien zugreifen und neue Dateien sicher ablegen.

Hinweis:

Wenn Du länger Deinen Rechner verlässt, trenne alle verbundenen TrueCrypt Laufwerke und sperre Deinen Desktop! Im Idealfall fährst Du Deinen Rechner einfach runter.

Eine Partition/Laufwerk verschlüsseln

Diese Funktion erlaubt Dir, ganze Festplatten, Partitionen auf Deiner Festplatte und USB Sticks zu verschlüsseln. Das macht Sinn, wenn Du Daten auf externe Festplatten auslagern/archivieren möchtest, oder sensible Daten auf einem USB Stick in der Tasche hast, die bei Verlust nicht von Dritten eingesehen werden sollen.

Wichtig!

Wenn Du Laufwerke mit vorhandenen Daten verschlüsseln willst, kann das mit der Gutmann Löschmethode je nach Größe des Laufwerks nicht nur viele Stunden und Tage, sondern auch Wochen dauern!

Egal! Es ist Deine persönliche Sicherheit und die Deines sozialen Umfelds, nimm es einmalig in Kauf.

Warum der Aufwand?

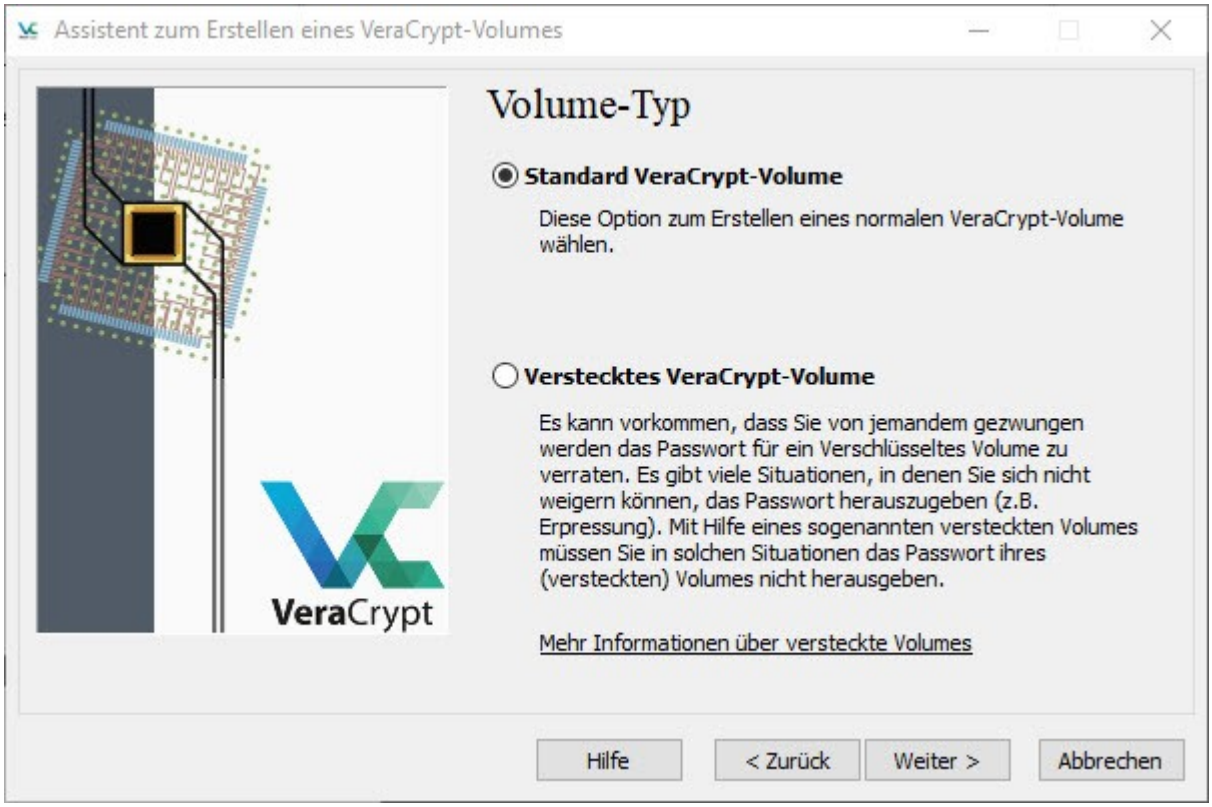
Alles was Dritte über Dich wissen, ist ein Indiz, gibt Aufschluss über Dich, Dein Verhalten, Deine Vorlieben, Deine Abneigungen, Deine Gewohnheiten, Dein soziales Umfeld.

Wenn zum Beispiel gegen jede Vernunft auf einer Demo Fotos und Videos gemacht werden und es geschafft wurde, sie sicher Heim zu bringen, dann ist es wenig zielführend, wenn die Bullen diese heiß begehrten „Beweise“ auf Deinem Rechner oder Deinen Festplatten frei Haus serviert bekommen.

Je weniger die Bullen über Dich erfahren, um so weniger bist Du angreifbar!

Je weniger die Bullen über Dein soziales Umfeld erfahren, um so sicherer sind alle Menschen die Dir nahestehen oder solidarisch mit Dir Seite an Seite kämpfen.

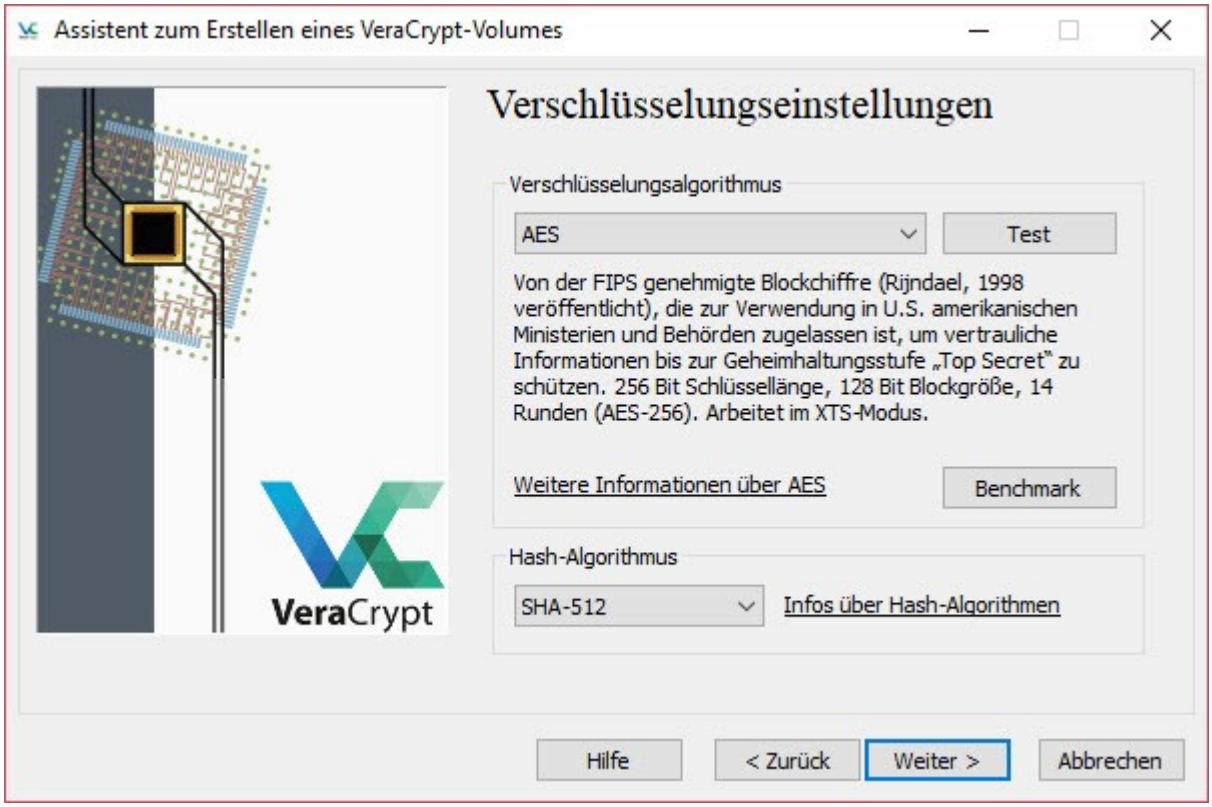
Hier triffst Du die Auswahl was Du verschlüsseln möchtest.



Hier kannst Du die Auswahl treffen, ob Du ein „Standard“ oder verstecktes VeraCrypt-Volume erstellen möchtest.

Klicke auf Datenträger, um das Laufwerk, die Partition oder den USB Stick auszuwählen und anschließend „Weiter“

Option „erstellen und formatieren“ nur bei leeren Laufwerken wählen – „in-place“ verschlüsseln behält Deine bereits vorhandenen Daten, der Vorgang ist jedoch bedeutend langsamer.

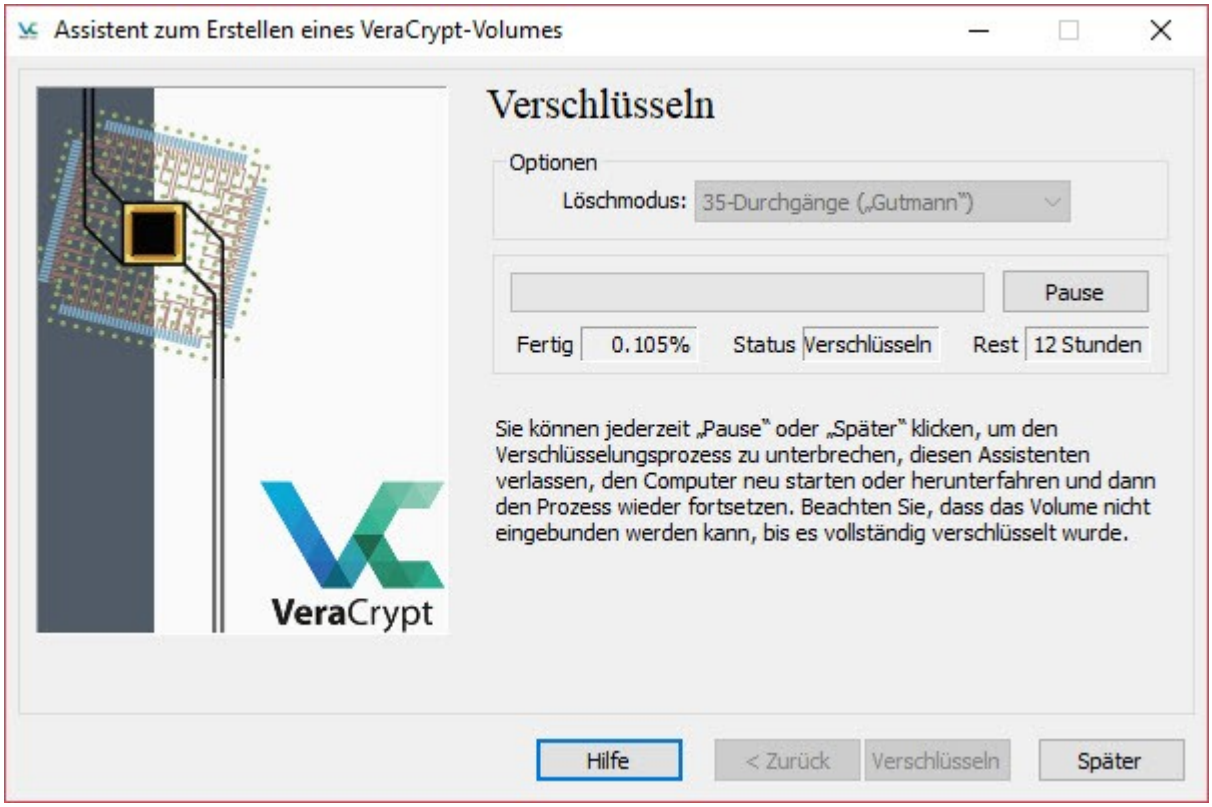


Hier kannst Du den Verschlüsselungsalgorithmus und den Hash-Algorithmus anpassen. Anschließend auf „Weiter“ klicken.

An dieser Stelle musst Du das Passwort festlegen, bitte beachte die Hinweise zu einem sicheren Passwort. Unter 20 Zeichen bekommst Du nach „Weiter“ eine Hinweismeldung, Du kannst entweder Dein Passwort anpassen oder die Hinweismeldung ignorieren.

In diesem Fenster die Maus einfach zufällig hin und her bewegen, bis sich die Anzeige in den grünen Bereich bis zum Ende der Anzeige bewegt. Und „Weiter“.

Ohne Löschen ist zwar schnell, aber unsicher. Optimal jedoch am längsten ist der Löschmodus nach „Gutmann". – und „Weiter".



In diesem Beispiel benötigt ein 3,7 GB USB 2.0 Stick 12 Stunden, um vorhandene Daten sicher zu verschlüsseln und die Daten am ursprünglichen Speicherort zu löschen. Mit USB 3.0 oder SSD Festplatten ist der Vorgang deutlich schneller.

Ein Systempartition/Laufwerk verschlüsseln

Die Programme die Du verwendest hinterlassen eine Menge Spuren und temporären Informationen, die Dir das Leben mit Deinem Rechner einfacher und schneller machen sollen.

Im Umkehrschluss kann allerdings auch jeder, der Zugriff auf Dein Startlaufwerk hat, genaue Rückschlüsse ziehen, wann Du welchem Programm gemacht hast, welche Seiten Du besucht hast, usw.

Mit dieser Funktion kannst Du Dein komplettes Startlaufwerk verschlüsseln, damit ist es nicht mehr möglich Dein Bootlaufwerk auszubauen und auf einem anderen PC auszulesen. Ohne Eingabe des Passwortes kann Dein Rechner auch nicht mehr gestartet werden. Das gilt auch bei einem Neustart Deines Rechners.

Vom Ablauf her funktioniert das ähnlich, wie die Erstellung eines verschlüsselten Laufwerkes oder USB Stick. Wenn möglich mach von Deinem Systemlaufwerk vorher ein komplettes BackUp, idealer Weise auf ein bereits verschlüsseltes Laufwerk.

Auch hier sollten die Speicherplätze der unverschlüsselten Daten nach „Gutmann“ bei der „in-place“ Verschlüsselung gelöscht werden.

Wichtige Hinweise:

Während des Bootvorgangs wirst Du nach einer „PIM“ gefragt. Sofern Du keinen eigenen Wert angegeben hast, bestätige die Abfrage mit „Return“ und Dein System startet.

Während der Erstellung eines verschlüsselten Systemlaufwerks wirst Du nach dem Speichern eines Sicherheitsmediums gefragt, beantworte die Frage mit **Ja**!

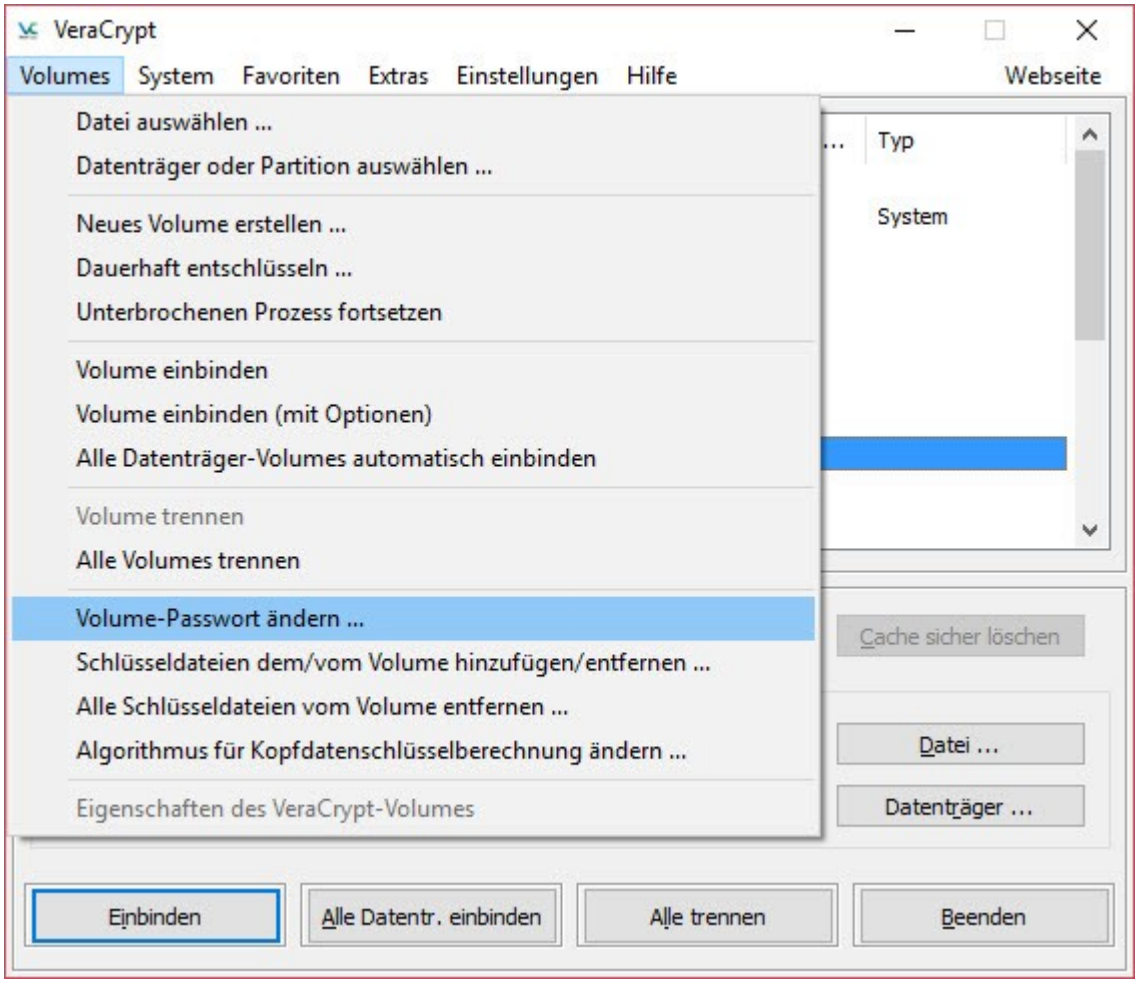
Hierzu benötigst Du einen kleinen USB Stick, der Inhalt ist am Ende keine 3,5 MB groß. Diesen Stick bewahre sicher und gut auf! Kopiere keine weiteren Daten auf diesen Stick!

Dein Rechner muss in der Lage sein, von einem Wechselmedium starten zu können, was in der Regel schon so eingestellt ist. Das kannst Du im BIOS Deines Rechners prüfen und ggf. einstellen, die Festplatte Deines Startlaufwerks darf nicht das primäre Bootlaufwerk sein. Die Tastenkombination für den Zugang zu Deinem BIOS kannst Du am besten über eine Suchmaschine herausfinden.

Sollte Dein Rechner nicht mehr starten können, kannst Du von diesem Stick Deinen Rechner in dem Modus starten, dass Du mit Eingabe Deines gewählten Passwortes Dein Systemlaufwerk wieder entschlüsseln und ggf. reparieren, bzw. Wichtige Daten noch sichern kannst. Dieser Vorgang kann wie beim Verschlüsseln unter Umständen lange Zeit in Anspruch nehmen.

Selbst wenn Dritte Deinen USB Stick und Deinen Rechner haben, können Sie ohne Dein Passwort nicht auf die Daten Deines Systemlaufwerks zugreifen. Der Stick beinhaltet lediglich ein kleines Tool, mit dem Du in der Lage bist, dass Systemlaufwerk wieder vollständig zu entschlüsseln, wenn Du auch das Passwort dafür kennst.

Volume Passwort ändern

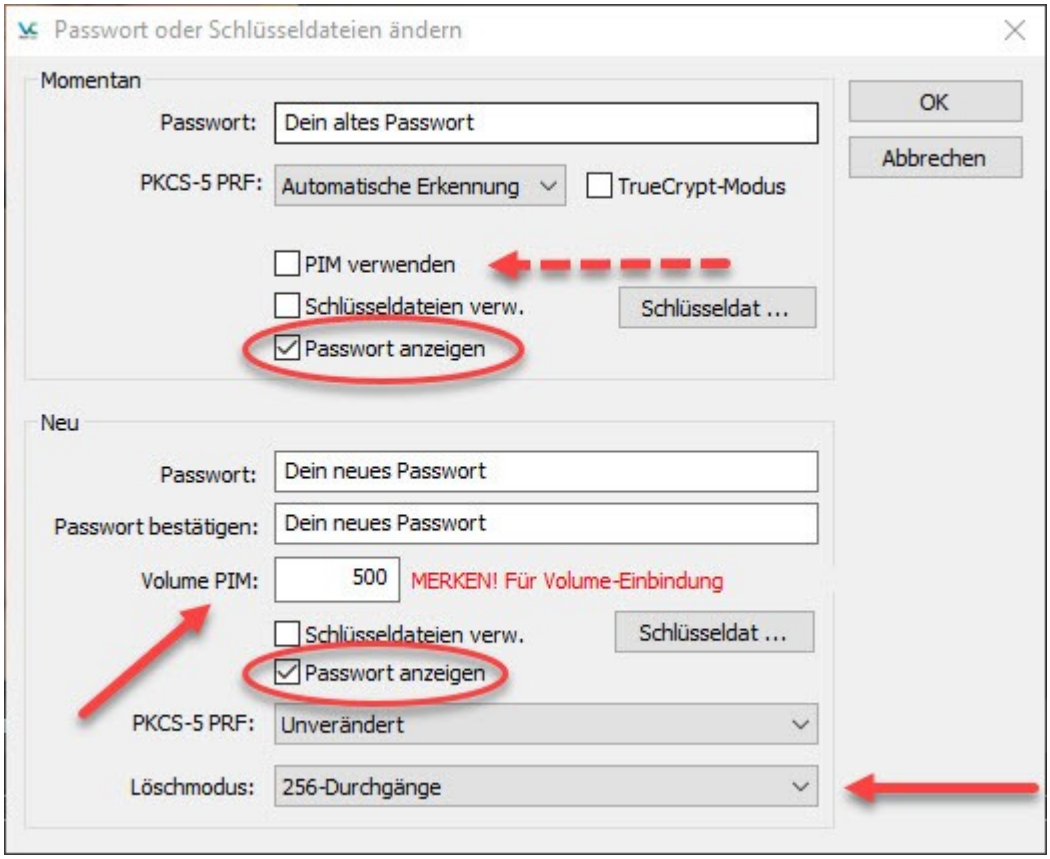


Wenn Du Dein Passwort ändern oder eine 2FA (Zwei Faktor Authentifizierung) mit der PIM (Personal Iterations Multiplier) für das Entschlüsseln Deiner Volumes hinzufügen möchtest, kannst Du das jeder Zeit durchführen.

Weder bei der ersten Verschlüsselung, noch beim Ändern des Volume Passwortes ist die Verwendung der PIM zwingend erforderlich.

Was es mit der PIM auf sich hat, wozu Du das brauchst und wie es funktioniert, dazu später mehr.

Für USB Sticks, Wechselplatten oder verbaute sekundäre Festplatten gehst Du dazu über „ → „Volume-Passwort ändern…“



Hier kannst Du nun Dein Volume Passwort ändern und ggf. auch noch nachträglich die PIM hinzufügen oder ändern.

„Passwort anzeigen“ – ist hier nur für den Screenshot ausgewählt und sollte nicht angehakt werden.

Bei „Momentan“ musst Du das bisher verwendete Passwort eingeben und falls Du beim Verschlüsseln eine PIM angegeben hast, auch den richtigen Wert. Willst Du die PIM erst nachträglich hinzufügen, dann darf das Kästchen dafür nicht angehakt sein.

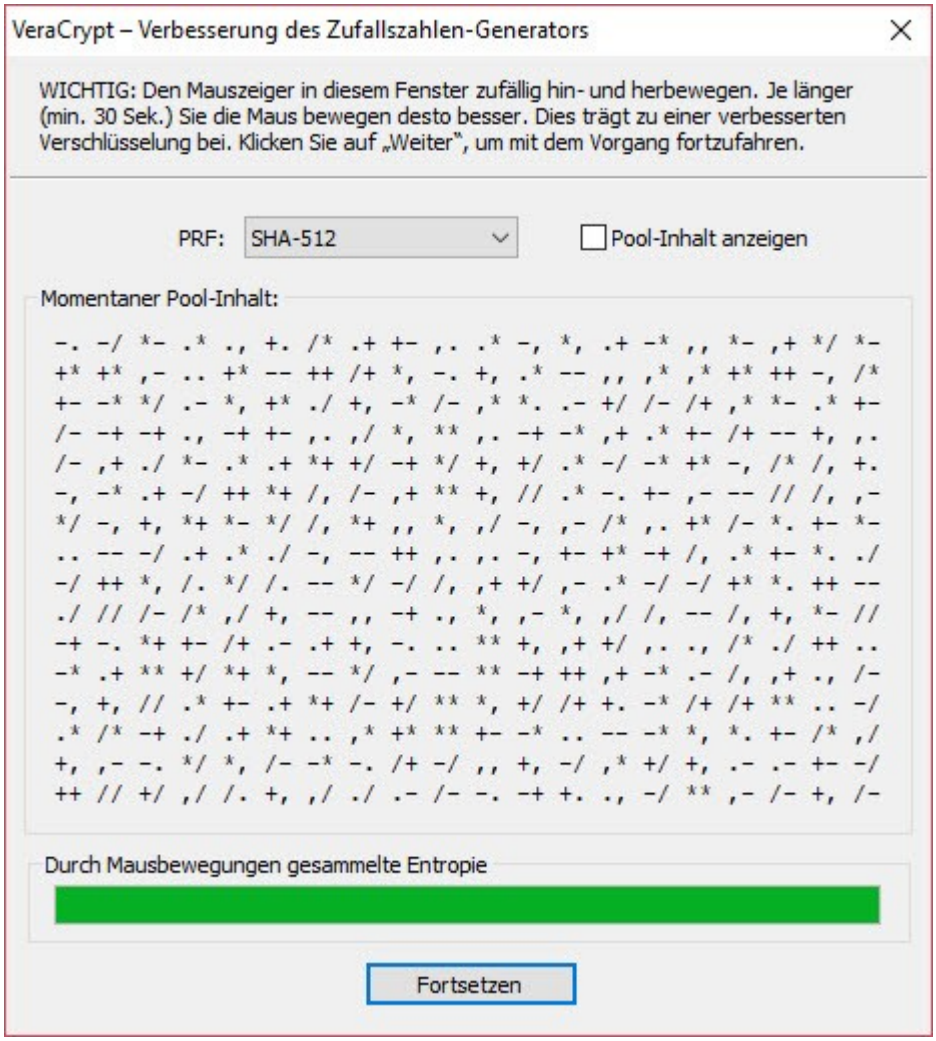
Unter „Neu“ musst Du das neue Passwort (möglichst 20 oder mehr Zeichen) zweimal eingeben, um Tippfehler auszuschließen, verwende daher nicht Copy & Paste.

Fügst Du PIM hinzu, hake das Kästchen an und gib den Wert dazu ein – **Wichtig! Diesen Wert musst Du Dir wie auch Dein neues Passwort zwingend merken!**

Mit „PKCS-5 PRF“ kannst Du die Verschlüsselungsstärke ändern. Wenn Du bereits einen Algorithmus mit hoher Verschlüsselung gewählt hast, lasse den Wert auf „Unverändert“.

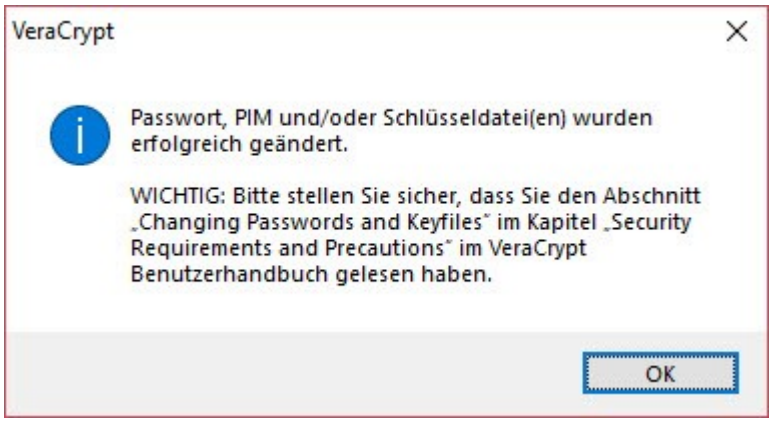
Der „Löschmodus“ vernichtet den alten VeraCrypt Volume Header. Bedenke, dass es Tools gibt, die gelöschte Daten leicht wiederherstellen können. Daher sind 256 Durchgänge empfohlen, auch wenn der Vorgang dadurch länger dauert.

Wenn Du alle Einstellungen vorgenommen und Dir das neue Passwort und PIM gut eingeprägt hast, klicke auf „OK“.



Bewege nun Deine Maus solange in diesem Fenster, bis der Fortschrittsbalken das Ende erreicht hat und klicke dann auf Fortsetzen.

VeraCrypt ändert nun Deinen Volume Header mit den neuen Daten zum Entschlüsseln Deines Volumes.

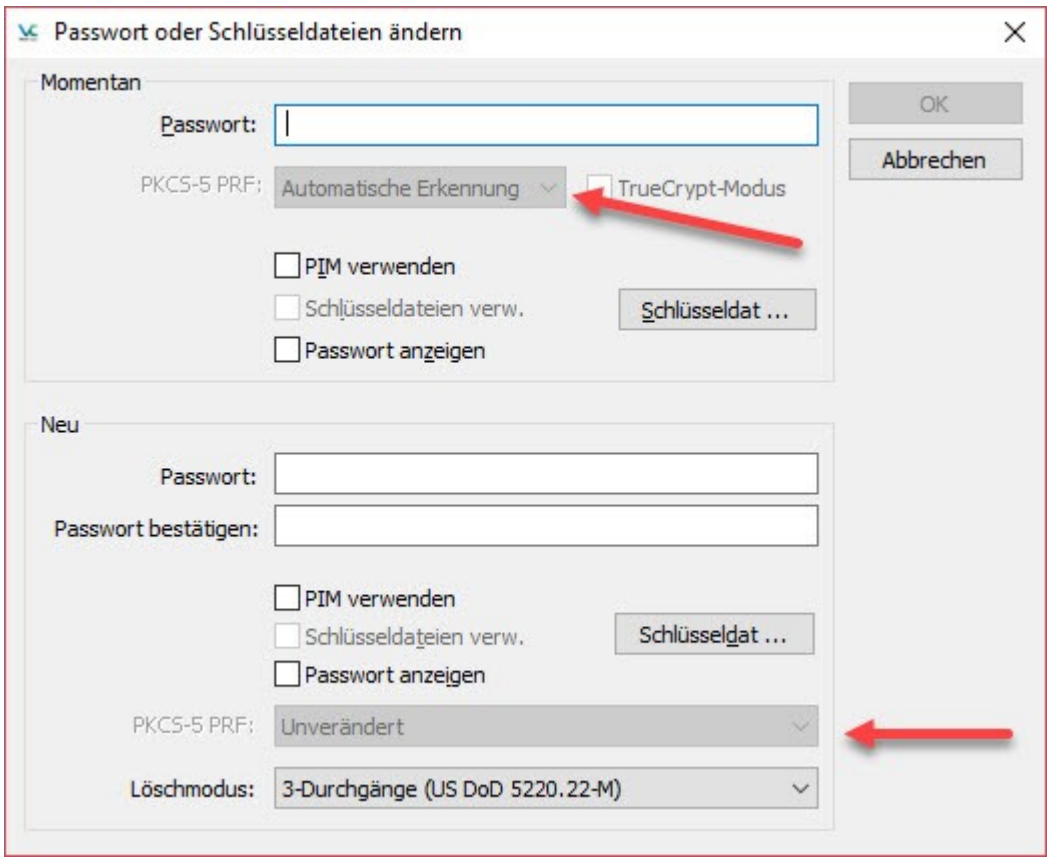


Nach erfolgreichem Abschluss erhältst Du eine Hinweismeldung.

Auch hier sei nochmal daran erinnert, vergisst Du Passwort oder PIM oder beides, sind Deine Daten auf dem verschlüsselten Volume verloren!

Das Systemlaufwerk ist ein besonderer Datenträger, da Du auf ihm Dein Betriebssystem installiert hast von dem Dein Rechner startet.

Die Änderungen kannst Du über das Menü „System“ → „Passwort ändern…“ durchführen und gelangst damit zu diesem Fenster:



Der Vorgang ist vom Grundsatz her gleich, es gibt nurzwei Unterschiede:

Du kannst den „PKCS-5 PRF“ Verschlüsselungsalgorithmus nicht mehr verändern.

Schlüsseldaten verwalten kann ebenfalls nicht ausgewählt werden.

Die Option PIM und wozu wird sie benötigt

PIM ist für die Ver- und Entschlüsselung der VeraCrypt Volume Header zuständig.

Normalerweise brauchst Du nicht zwingend eine PIM verwenden, außer Du willst Dich noch zusätzlich mit einer 2FA absichern, oder bei einem älteren Rechner den Bootvorgang beschleunigen.

Hast Du keinen PIM Wert angegeben, setzt VeraCrypt im Hintergrund beim Systemlaufwerk einen Standardwert von 98. Beim Booten gibst Du daher nur Dein Passwort ein und bestätigst die Abfrage des PIM Wertes mit „Return“.

Veracrypt berechnet mit dem PIM Wert die Wiederholungen mit PIM x 2048, bei dem Standardwert für Systemplatten wäre das 98 x 2048 = 200.000 Durchläufe.

Bei Standard Partitionen ist der PIM Wert sogar auf 485 festgelegt, das entspräche 500.000 Durchläufe.

Wenn Du jetzt einen älteren, langsam Rechner verwendest, kann das Deinen Bootvorgang erheblich ausbremsen. Wie kannst Du also den Bootvorgang verkürzen und das System dennoch sicher halten?

Die Stärke Deiner Verschlüsselung ist in erster Linie von der Stärke Deines gewählten Passwortes abhängig.

Wähle also daher kein kurzes Passwort, verwende GROSS- und Kleinschrift, Ziffern, Satz- und Sonderzeichen, vermeide aufeinanderfolgende Zeichen und Daten, die mit Dir in Zusammenhang stehen (z. B. Geburtsdatum, Handynummer, etc.).

VeraCrypt ermöglicht es, den PIM Wert zu verändern, dafür gilt aber folgende Voraussetzung:

Dein Passwort ist länger als 20 Zeichen

Sonst wird der Standard von 98 (200.000 Durchläufen) oder 485 (500.000 Durchläufen) verwendet.

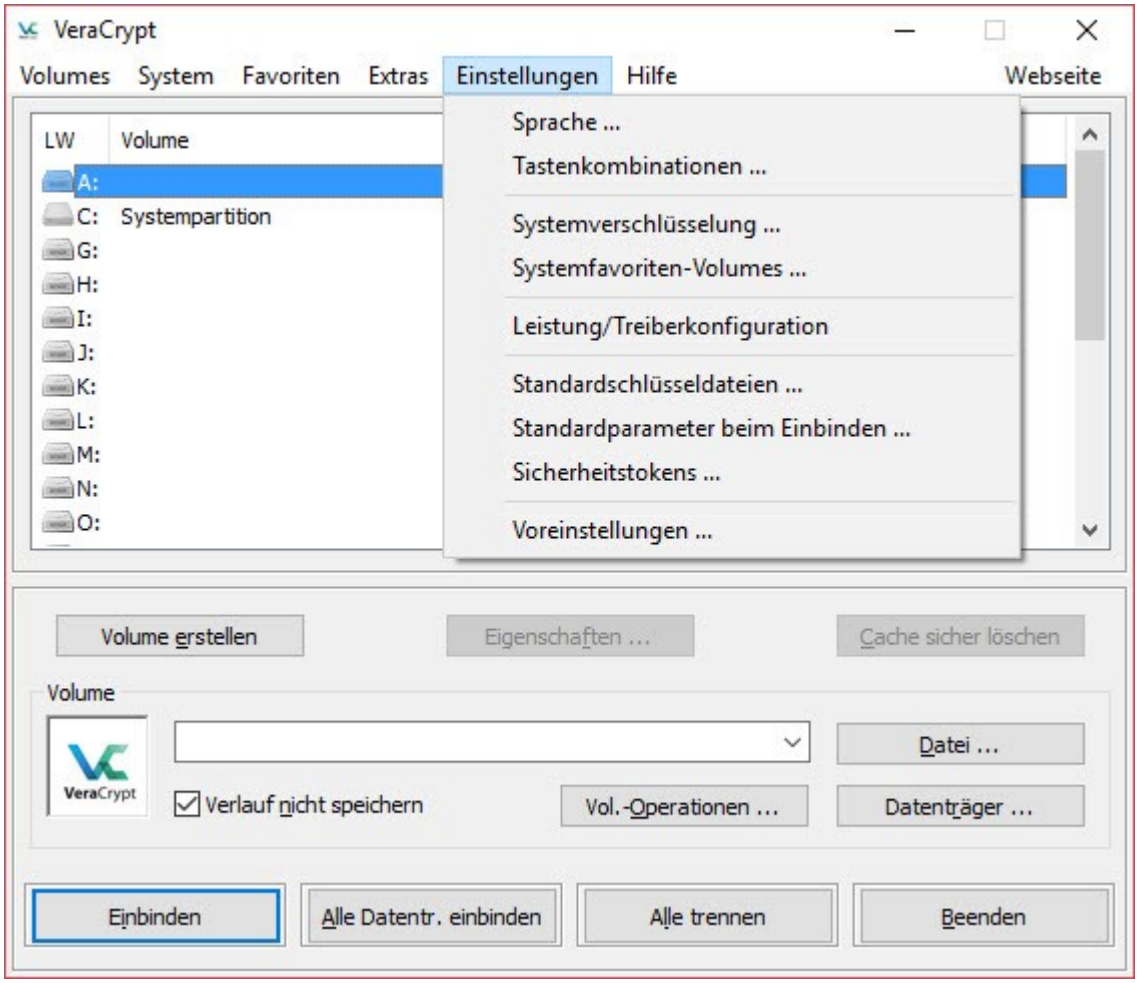
Wenn Du den Bootvorgang unbedingt beschleunigen willst, kannst Du bei einem langen Passwort auch eine PIM von 10, 20 oder 30 verwenden, auch einen Wert von 2, 3 oder 5. Wichtig ist die ausreichende Länge Deines gewählten Passworts und ein PIM Wert über 1.

Wichtig!

Politische Arbeit sollte in einem freien Land eigentlich unbedenklich sein – Du bist hier allerdings in Deutschland, entweder wirst Du schon oder bald mit dem PAG generalverdächtigt, stigmatisiert, kriminalisiert und solltest daher Deinen persönlichen Schutz und den Schutz der Menschen, mit denen Du Dich gerne umgibst, sehr ernst nehmen.

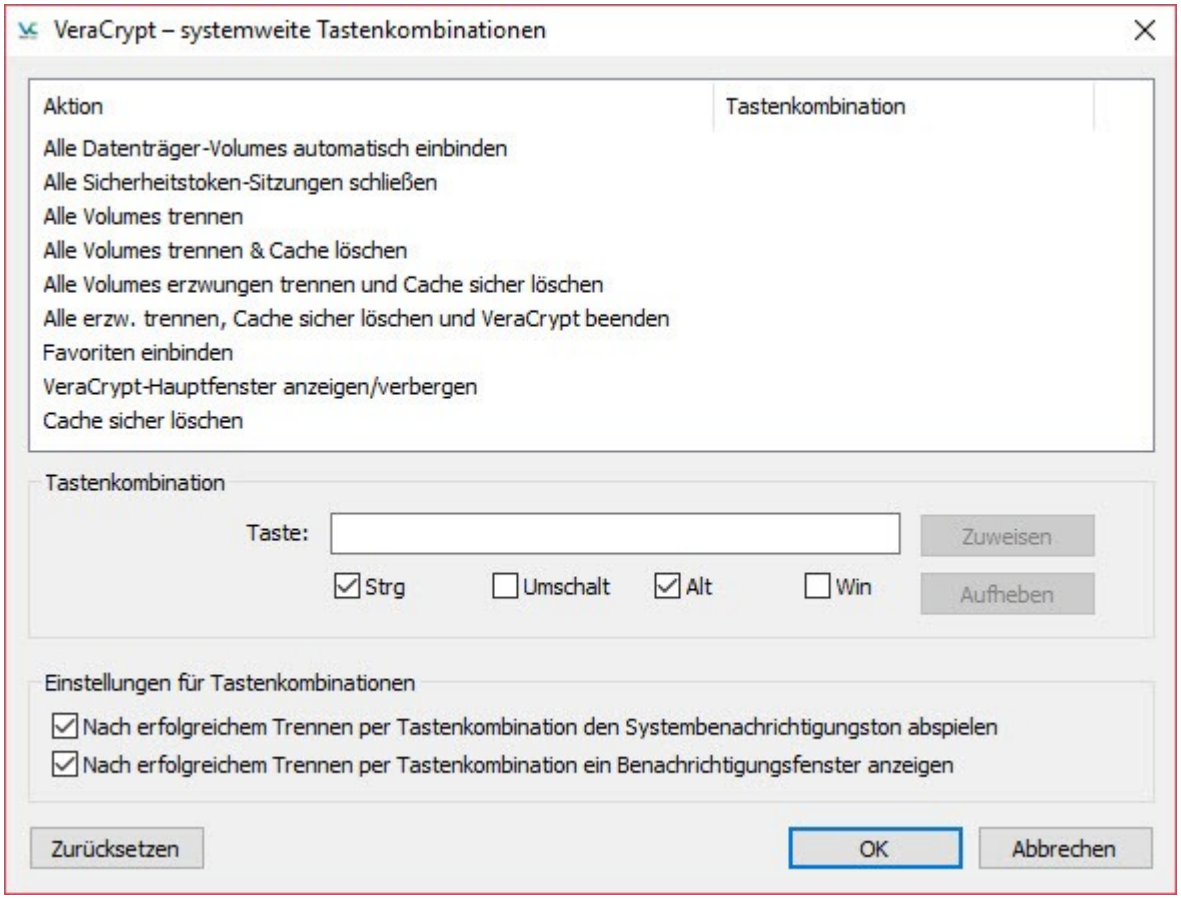
PIM hinzufügen und den Wert verändern ja, aber nicht zu Deinem Nachteil.

Die VeraCrypt Einstellungen



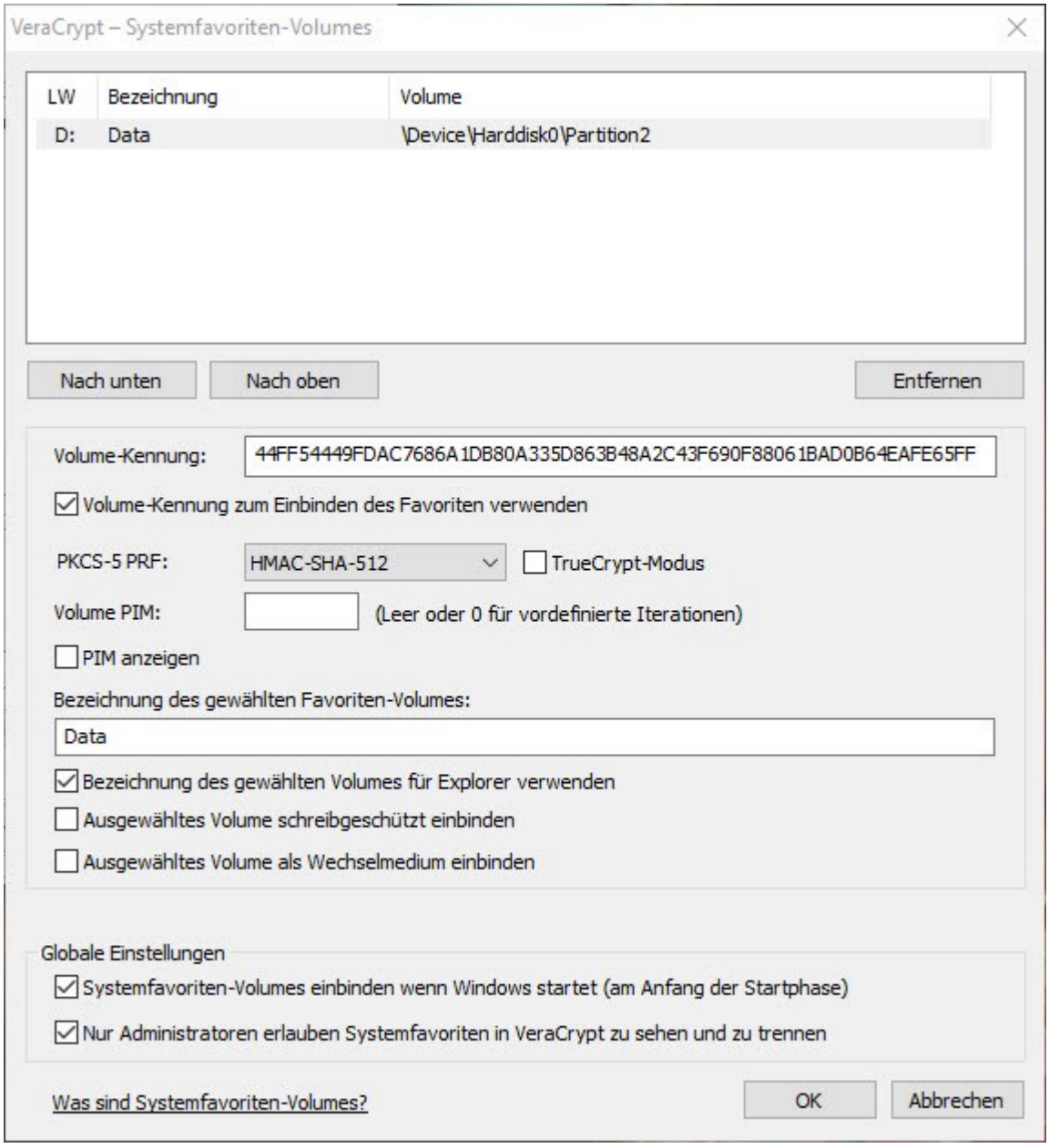
Es gibt einige sinnvolle Einstellungen des Programms, die das Arbeiten erleichtern und sicherer machen. In der Regel reichen die Standardeinstellungen aus, trotzdem sollen einige Punkte kurz angerissen werden.

Sprache – hier kannst Du die Programmsprache einstellen.



Tastenkombinationen – hier können für bestimmte Funktionen Tastenkombinationen festgelegt werden, um zum Beispiel bei überraschendem Besuch von den Cops alle eingebundenen Laufwerke sofort zu trennen.

Systemverschlüsselung – enthält einige Experteneinstellungen, die ohne genaue Kenntnisse nicht verändert werden sollten.



Systemfavoriten-Volumes – hier können Einstellungen für Festplatten vorgenommen werden, die bei einem verschlüsselten Systemlaufwerk automatisch eingebunden werden sollen.

Beispiel:

- Du hast ein 256 GB SSD Systemlaufwerk
- Du hast dazu eine 2 TB Festplatte für Deine Daten

Hier macht es bei Windows zum Beispiel Sinn, wenn Du die Benutzerdaten vom Laufwerk C: auf D: verschiebt, um das Systemlaufwerk nicht unnötig zu belasten bzw. die Speicherkapazität unnötig auszuschöpfen.

Windows speichert viel in einem Verzeichnis des Nutzers auf dem Systemlaufwerk, damit wird die Kapazität der SSD Festplatte schnell erreicht.

Zuerst musst Du das mit dem gewünschten Laufwerksbuchstaben eingebundene Festplattenlaufwerk unter „Favoriten“ zu den Systemfavoriten hinzufügen Die Einstellungen sind die gleichen wie in dem obenstehenden Fenster.

Hier kannst Du eine Laufwerksbezeichnung eingeben und festlegen, ob die Bezeichnung so auch im Explorer angezeigt werden soll.

Alle anderen Einstellungen solltest Du nur verändern, wenn Du das vollständige Englische Handbuch gelesen hast.

Wichtig:

VeraCrypt kann beim Einbinden eines verschlüsselten Volumes nicht den physisch unter Windows zugeordneten Laufwerksbuchstaben verwenden. Wenn Du für Deine Daten das Laufwerk D: haben möchtest, musst Du in der Windows Datenträgerverwaltung den physikalischen Laufwerksbuchstaben zum Beispiel auf B: ändern.

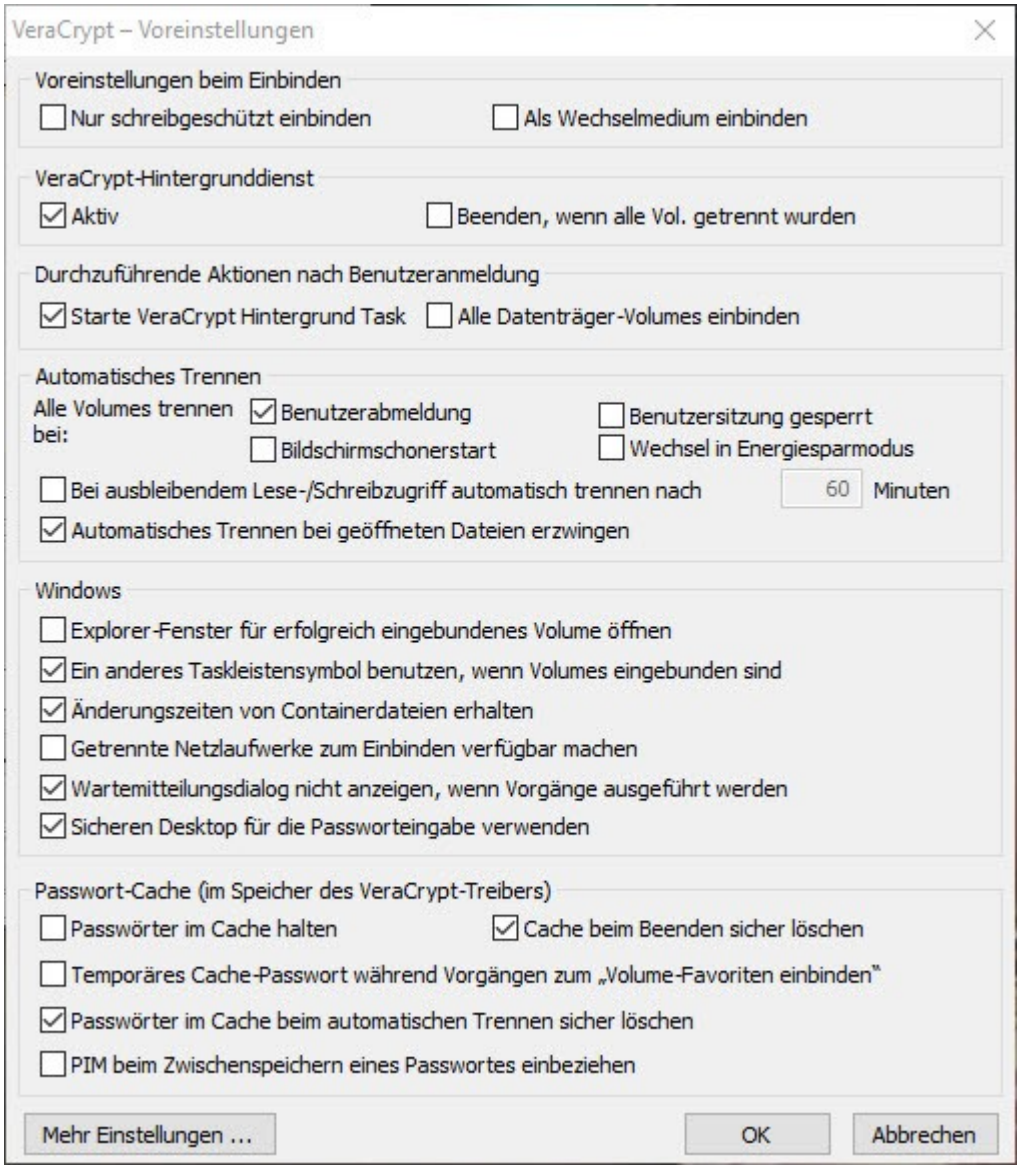
Die Verzeichnisse in Deinem Nutzerordner kannst Du dann anschließend mit Rechtsklick auf das jeweilige Verzeichnis unter“ Eigenschaften“ → „Pfad“ ändern und auf das verschlüsselte Ziellaufwerk verschieben.

Leistung/Treiberkonfiguration – solltest Du nicht verändern.

Standardschlüsseldateien – hier können Schlüsseldateien verwaltet werden, sofern sie in erweiterter Konfiguration verwendet wurden.

Standard Parameter beim einbinden – hier kannst Du einzelne Parameter einstellen, die beim Einbinden als Voreinstellung gewählt sein sollen. Die Einstellung sollte nicht verändert werden, eine Anpassung kann auch direkt beim Einbinden ggf. erfolgen.

Sicherheitstokens – dient zur Unterstützung von Hardwarelösungen wie Dongle, KeyCard oder ähnliches, um eine höhere Sicherheitsstufe beim Entschlüsseln zu erreichen. Dazu wird eine gesonderte Hardware und die dazugehörige Software benötigt, die Einstellungen können in der Standardnutzung ignoriert werden.



Voreinstellungen – hier können Grundlegende Parameter des Programms eingestellt werden.

Der VeraCrypt Hintergrunddienst sollte wie auch das Starten des VeraCrypt Hintergrund Task aktiv sein.

Die Optionen zu „Automatisches Trennen“ und „Windows“ bestimmen das Arbeitsverhalten des Programms, hier kannst Du das Verhalten nach Deinen persönlichen Bedürfnissen anpassen.

Passwort-Cache steuert die Zwischenspeicherung Deiner Passwörter im Speicher des VeraCrypt Treibers.

Es ist empfehlenswert keine Passwörter im Cache zu speichern oder über längere Zeit zu halten. Ebenso solltest Du dafür Sorge tragen, dass die Passphrasen auch wieder sicher gelöscht werden.