DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 890 729 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Anleitung VeraCrypt

Inhalt

USB-Stick / USB-Festplatte mit Veracrypt verschlüsseln

24. März 2021 Andy Software

Einen USB-Stick sicher verschlüsseln mit Vera-Crypt. So gehts!

Mit der kostenlosen Software VeraCrypt lassen sich auch USB-Sticks sicher verschlüsseln, sodass diese erst nach Eingabe eines Passwortes ausgelesen werden können. Damit können Sie ihre Daten unterwegs schützen und auch, wenn Sie den Stick verlieren kommt so niemand an ihre Daten. Der Vorteil von VeraCrypt ist zudem die Kompatibilität mit anderen Betriebssystemen, so kann VeraCrypt auf Linux, Windows und MacOS verwendet werden.

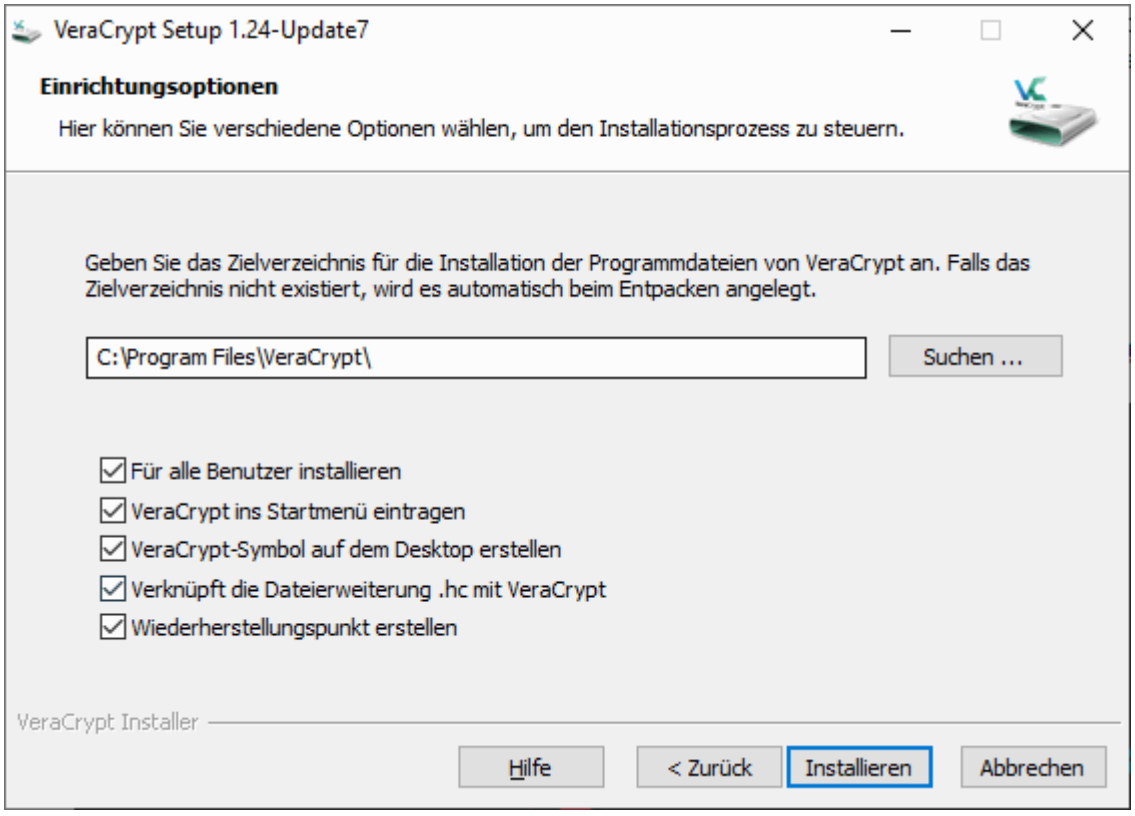
Videoanleitung

Anleitung

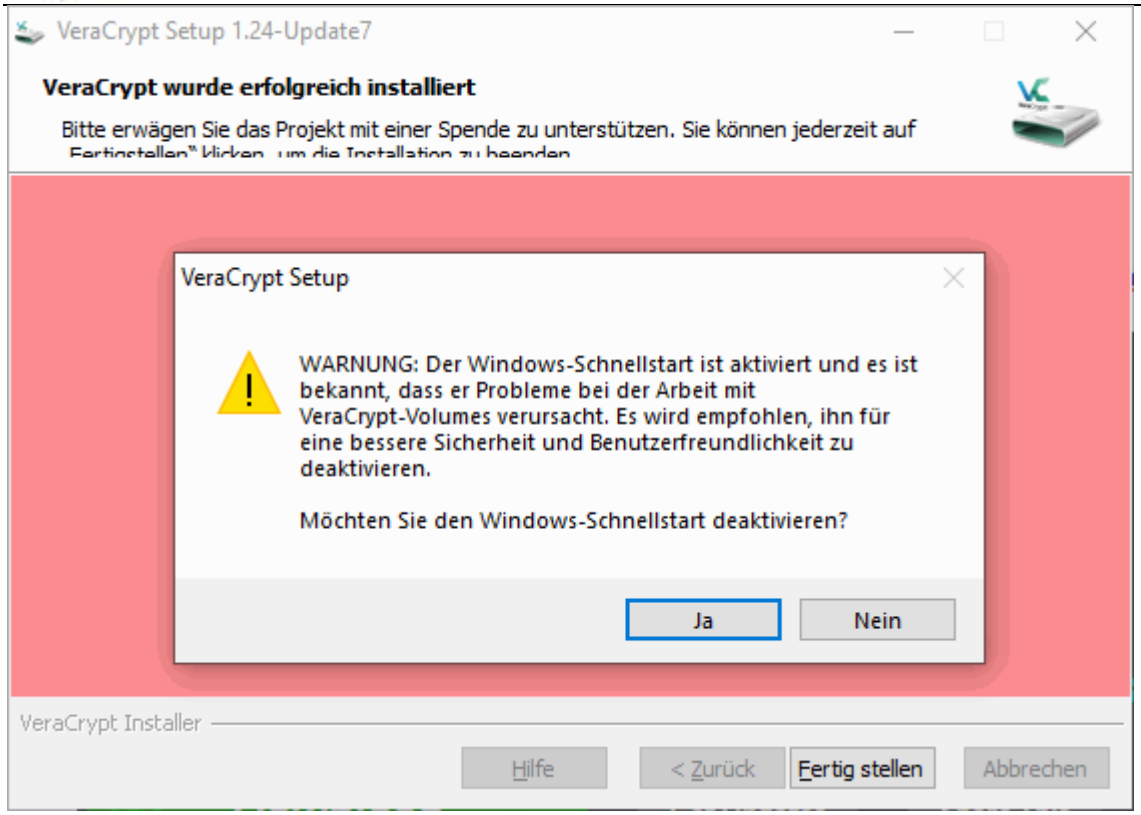
Download von VeraCrypt

Zuerst laden wir VeraCrypt herunter.

Nach dem Download wird die Software installiert.

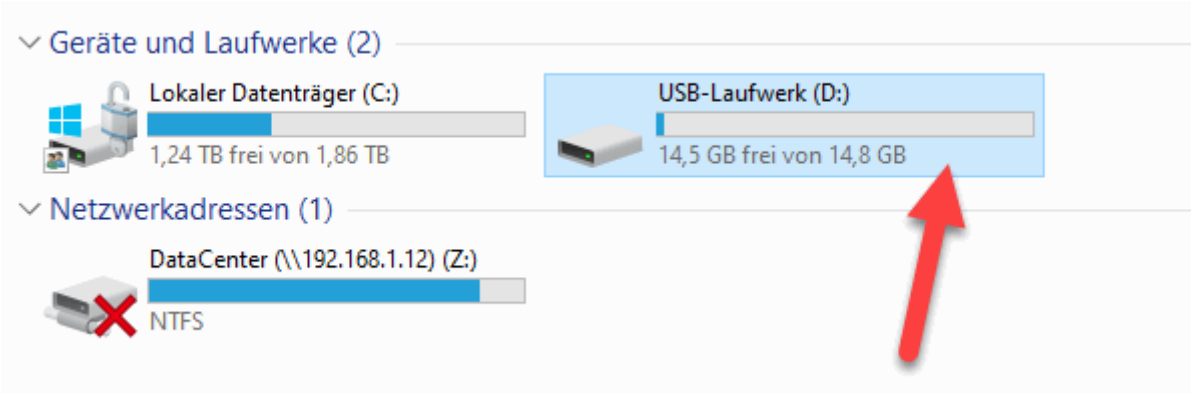


Während der Installation fragt uns VeraCrypt ob wir den Schnellstart deaktivieren wollen. Die Schnellstartfunktion kann bewirken, dass verschlüsselte Datenträger eingebunden bleiben nach dem Herunterfahren und erneuten Hochfahren. Falls das ein Problem ist, dann den Schnellstart deaktivieren.

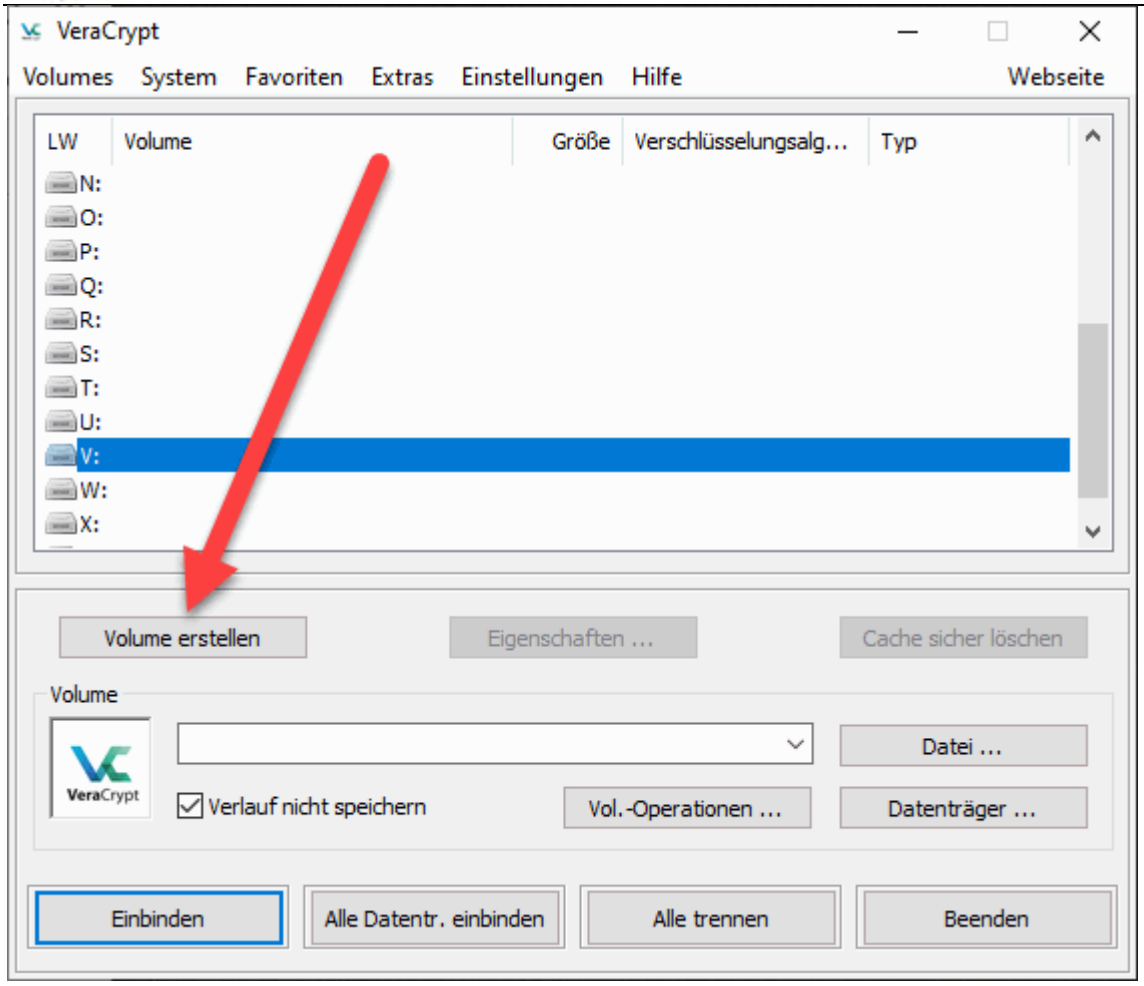


USB-Laufwerk verschlüsseln

Nun wollen wir unser USB-Laufwerk verschlüsseln. In unserem Fall ist es das Laufwerk D:\



Wir starten VeraCrypt und rufen „Volume erstellen“ auf.



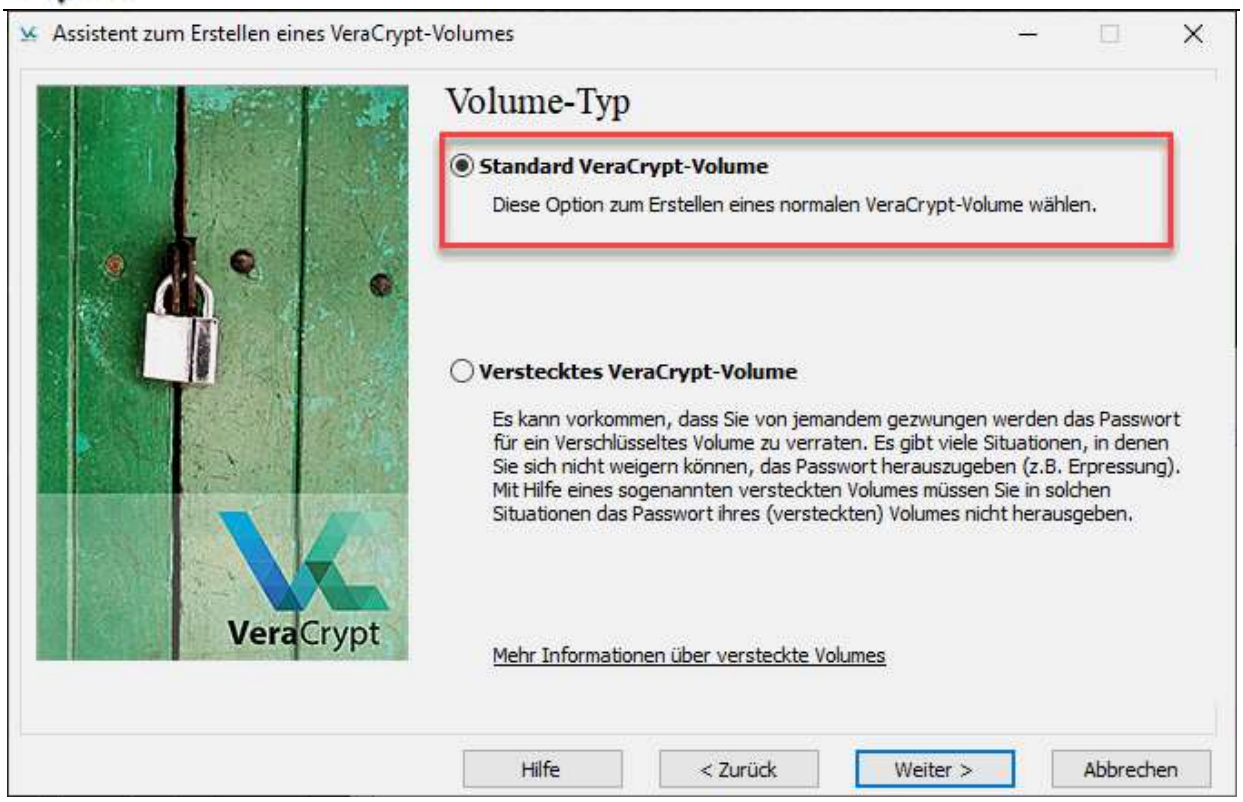
Wir haben nun zwei Möglichkeiten der Verschlüsselung, wir erstellen einen verschlüsselten Container oder wir verschlüsseln das gesamte Laufwerk. Die Verschlüsselung als Container legt auf dem Datenträger eine Containerdatei ein, welche wir als Laufwerk einbinden können. Die Daten innerhalb des Containers werden verschlüsselt. Dies hat den Vorteil, dass neben den verschlüsselten Daten auch unverschlüsselte Daten auf dem Datenträger abgelegt werden können-

Alternativ können wir auch das gesamte Laufwerk verschlüsseln. Wir erklären im folgenden die Vorgehensweise für beide Varianten und auch die Vor- und Nachteile der jeweiligen Methode.

Verschlüsselten Container erstellen

Beginnen wir mit dem verschlüsselten Container.

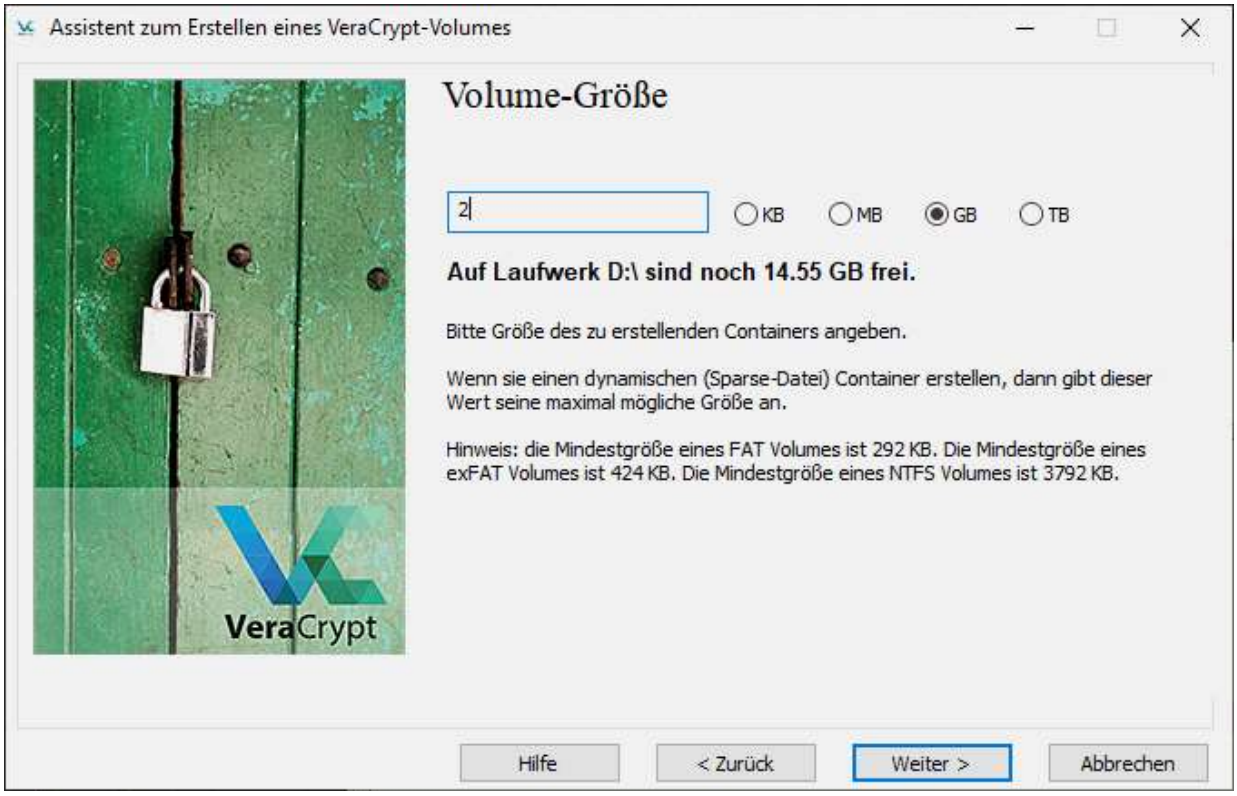
Im ersten Schritt werden wir gefragt, ob wir einen Standard-Container oder ein verstecktes Volume erstellen wollen. Wir wollen hier die Standard-Methode verwenden.



Anschließend legen wir den Speicherort fest. Der Speicherort ist in unserem Fall auf unserem USB-Datenträger, natürlich können Sie den Container auch auf der lokalen Festplatte ablegen. Die Standard-Dateiendung von VeraCrypt ist „.hc“. Damit kann der Container per Doppelklick geöffnet werden. Wenn der Container nicht direkt als solcher zu erkennen sein soll, können Sie auch eine beliebige Anwendung verwenden.

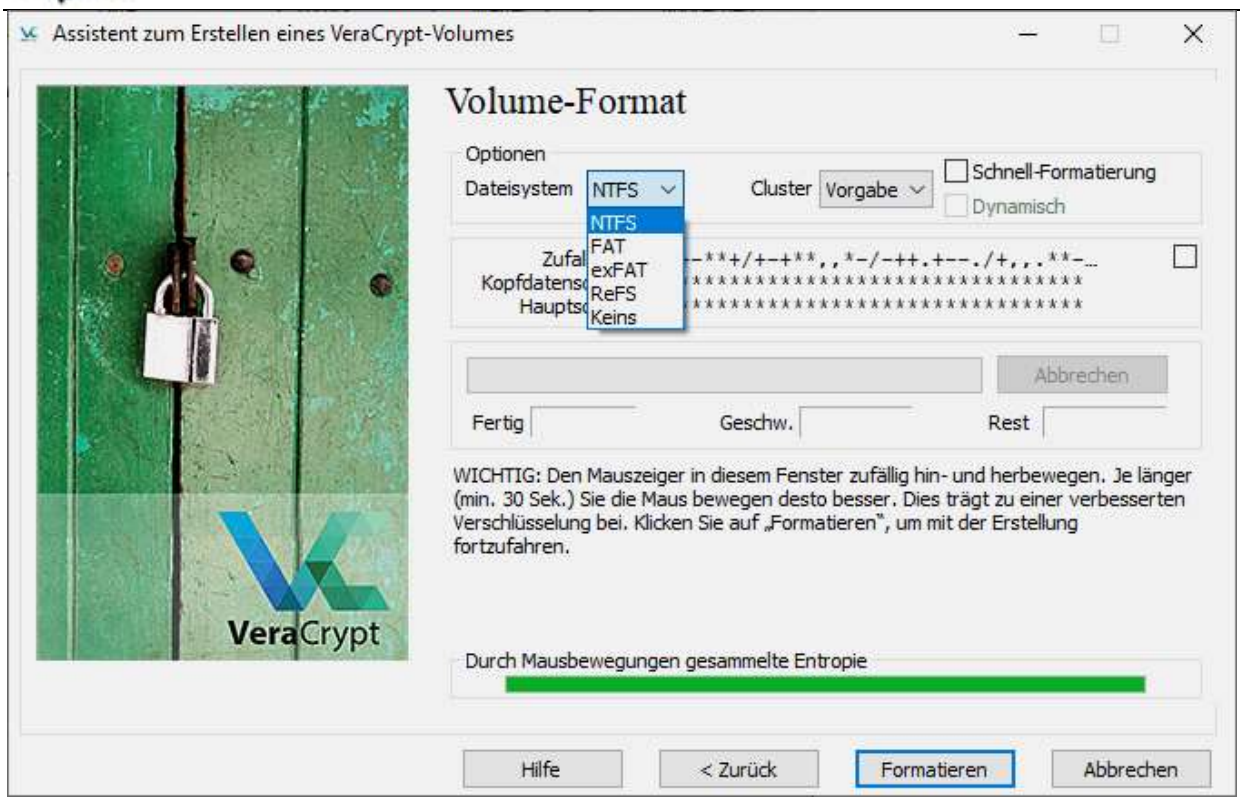
Bei der Verschlüsselung übernehmen wir die Standardeinstellungen, diese sind eine sinnvolle Voreinstellung.

Anschließend können wir die Größe des Containers festlegen. Hier sollten Sie abwägen, was an Daten in den Container soll, jetzt und in der Zukunft.

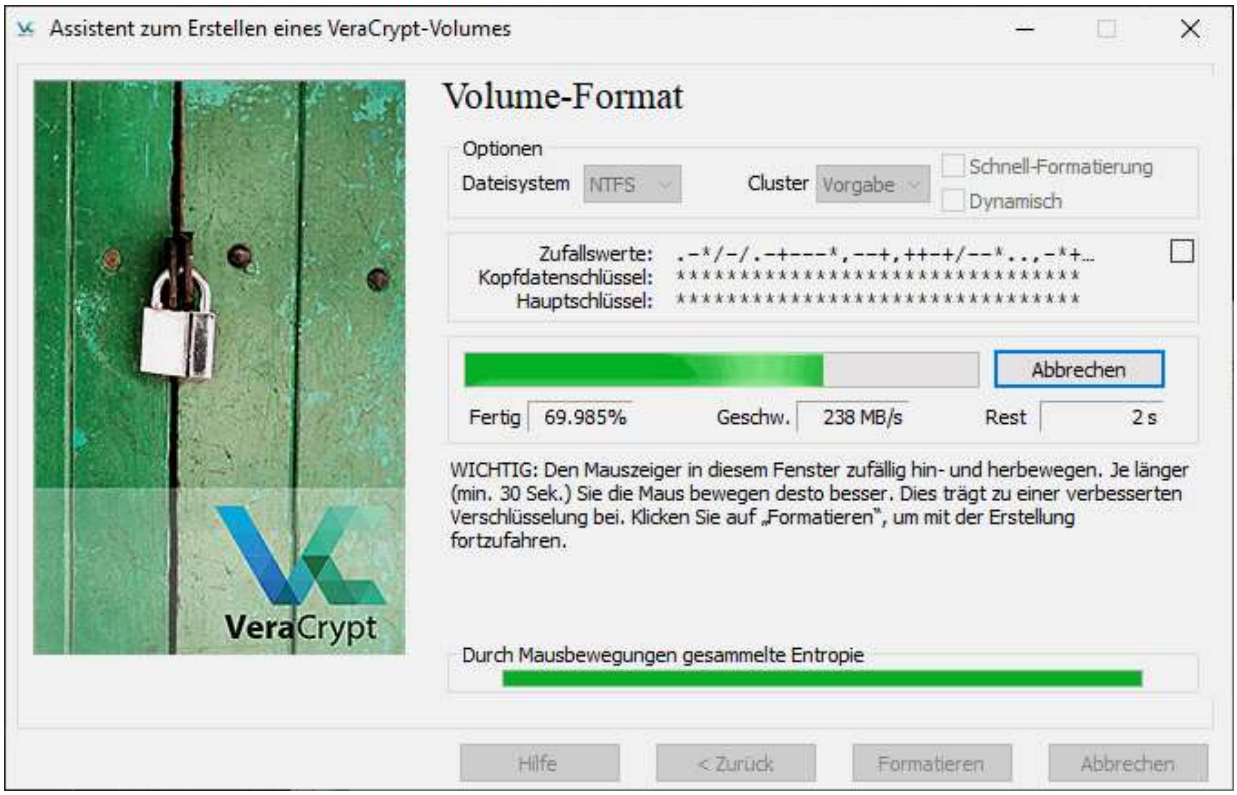


Nun geben wir das Passwort ein. Es gilt, je länger das Passwort, desto sicherer die Verschlüsselung. Ein kurzes Passwort kann im Zweifelsfall durch ausprobieren von speziellen Programmen geknackt werden.

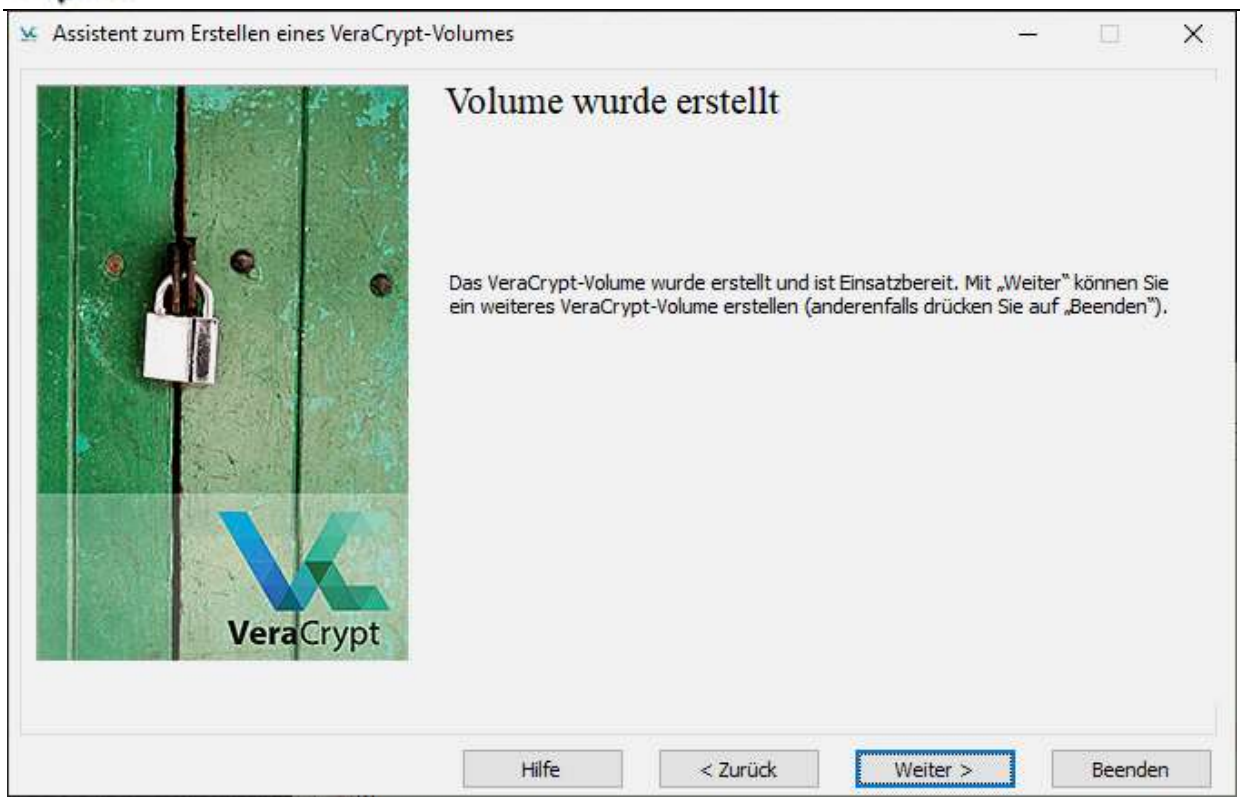
Im nächsten Schritt legen sammelt VeraCrypt Zufallsdaten für die Schlüsselerzeugung, bewegen Sie die Maus innerhalb des Fenster, idealerweise bis der Balken grün wird. Beim Dateisystem können Sie festlegen, wie der Datenträger formatiert werden soll. NTFS ist meist eine gute Wahl. Sofern Sie den Haken „Schnell-Formatierung“ nicht aktivieren, wird der Container langsamer formatiert, dafür bleiben keine Daten in den Datenbereichen zurück.



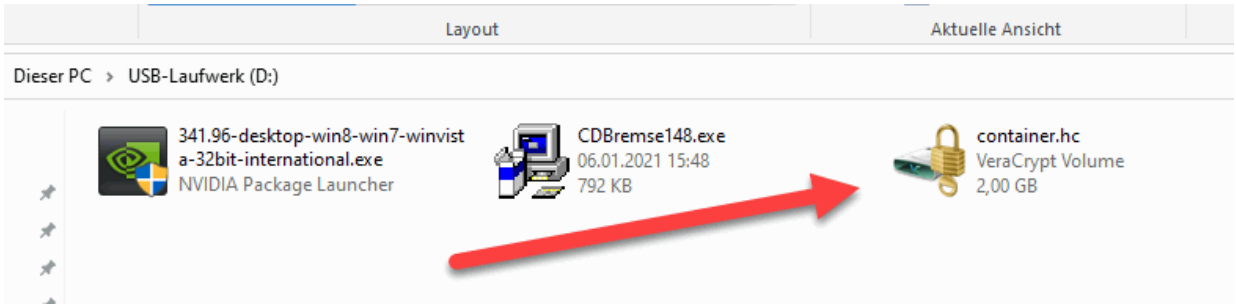
Mit einem Klick auf Formatieren, startet die Formatierung.



Der Vorgang dauert je nach Geschwindigkeit des USB-Datenträgers und Größe des Containers etwas. Anschließend wird eine Erfolgsmeldung ausgegeben.

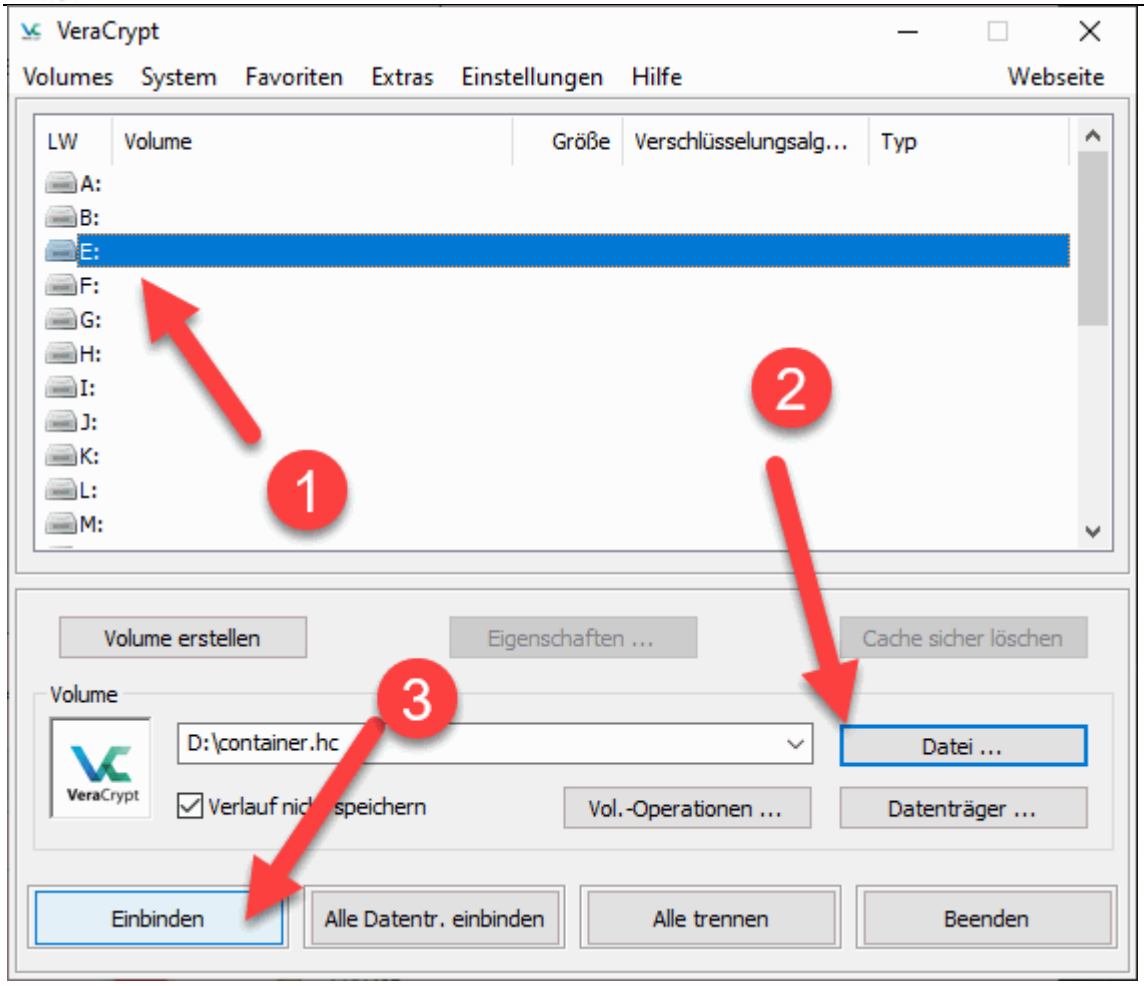


Nun klicken wir auf Beenden. Die Containerdatei liegt nun auf unserem USB-Stick.

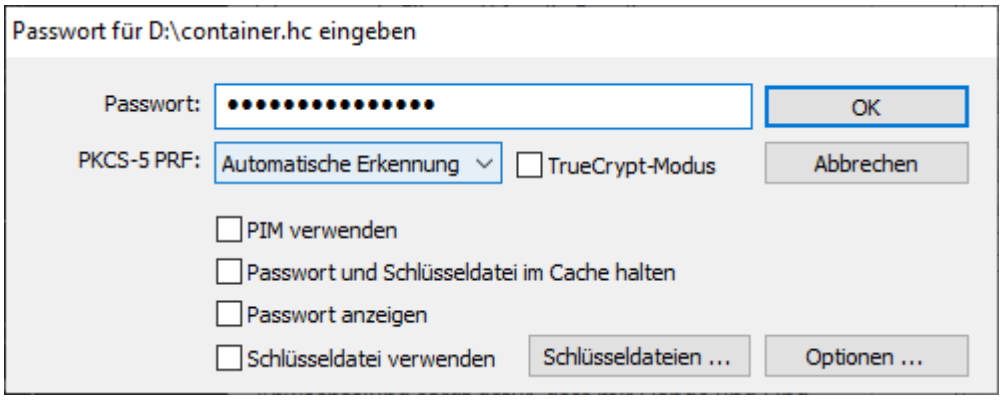


Öffnen des Container

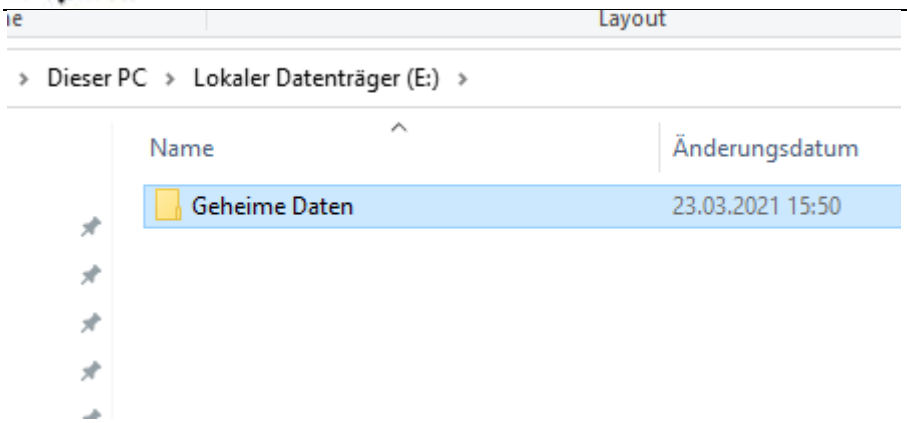
Den Container können wir nun mit Doppelklick öffnen, sofern er die passende Dateiendung hat. Ansonsten können wir den Container auch über VeraCrypt selbst mounten, bzw. einbinden. Zuerst wählen wir einen freien Laufwerksbuchstaben aus, anschließend die Container-Datei und zuletzt klicken wir auf „Einbinden".



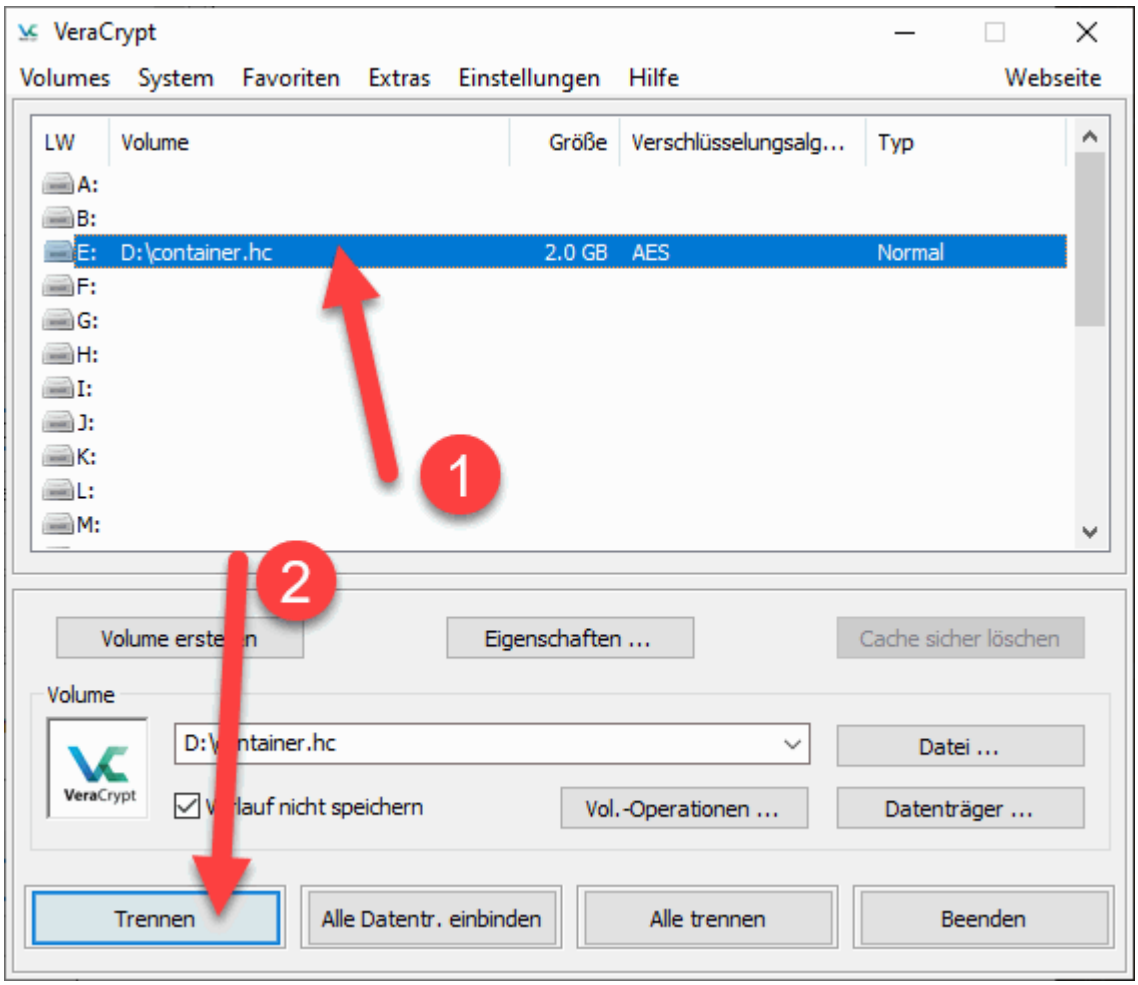
Nun geben wir das Passwort ein. Bei korrekter Eingabe wird der Container geöffnet und als Laufwerk eingebunden.



Im Explorer können wir nun auf das Laufwerk zugreifen und ganz normal verwenden.



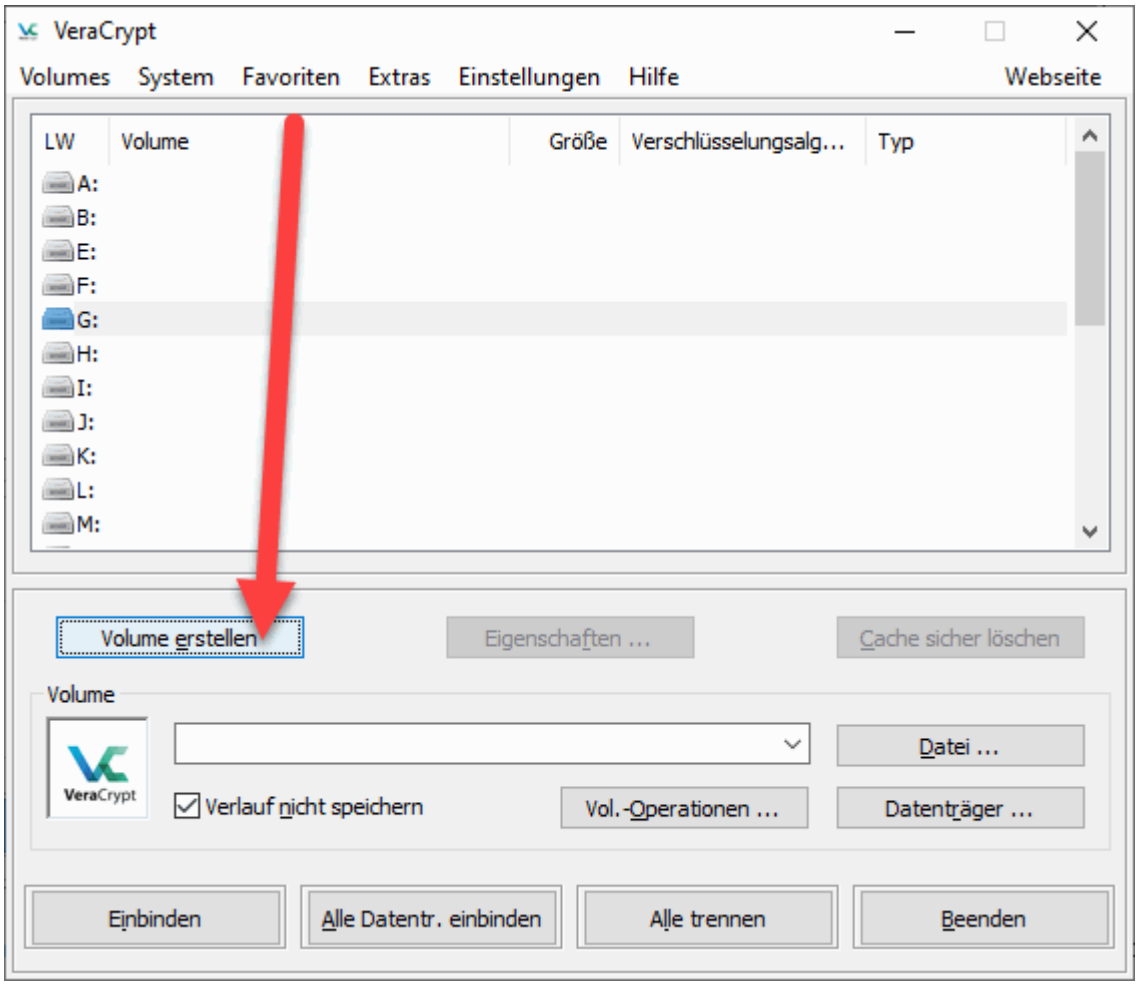
Vor dem Abziehen des Datenträgers empfiehlt sich das Laufwerk über VeraCrypt zu trennen, damit keine Daten beschädigt werden.



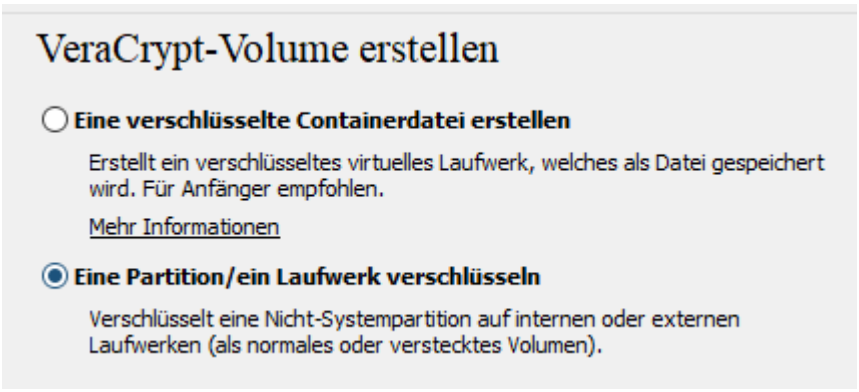
Ein weiterer Vorteil der Containerlösung, den Container können wir einfach sichern oder auf einen anderen USB-Stick kopieren.

Laufwerk komplett verschlüsseln

Die Verschlüsselung des kompletten Laufwerks ist in vielen Schritten sehr ähnlich, daher überspringen wir Schritte die gleich sind. Bei der Methode wird der gesamte Datenträger verschlüsselt. Jemand der den Stick einsteckt bekommt einen unformatierten USB-Stick angezeigt. Wie bereits bei der Containermethode erstellen wir hier ein Volume.

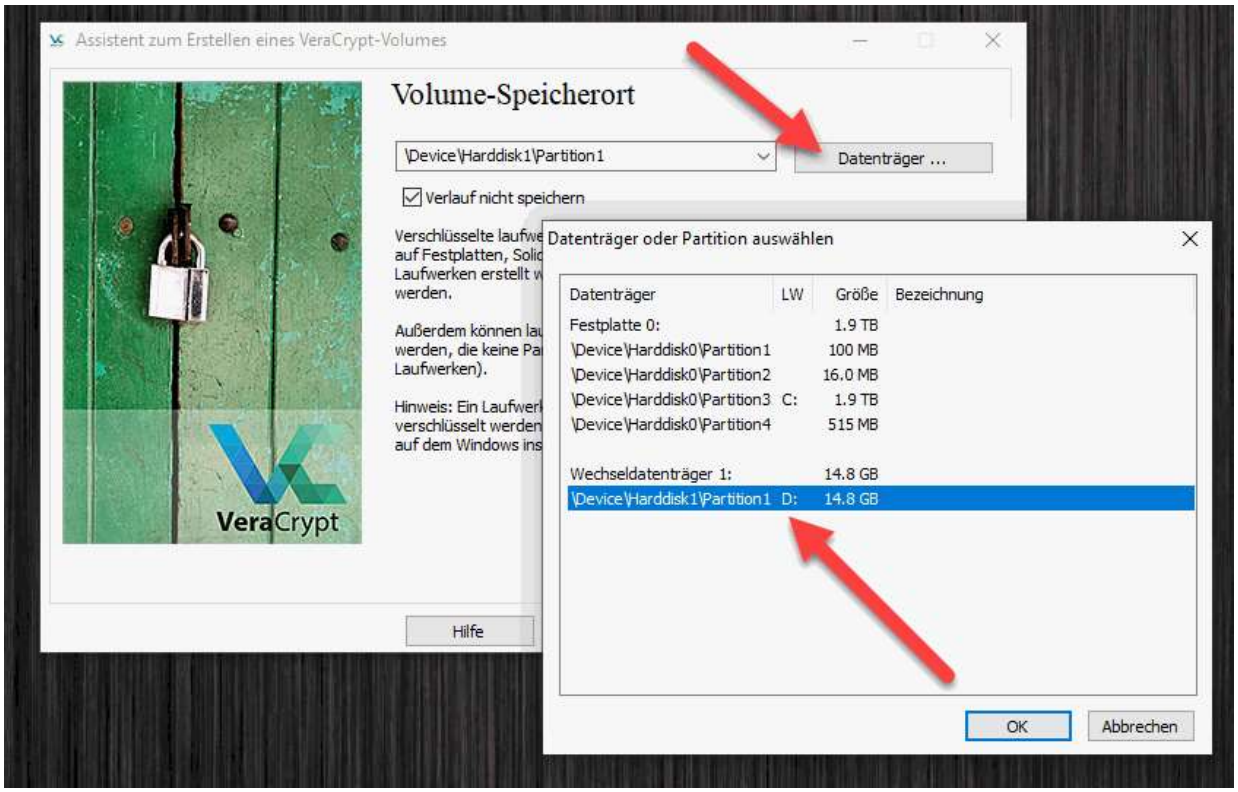


Im nächsten Schritt wählen wir nun die Option zum Verschlüsseln einer Partition oder Laufwerk aus.



Wie bereits beim Container, haben wir die Wahl zwischen der Standard-Verschlüsselung oder einem versteckten Volume. Anschließen müssen wir unser Laufwerk auswählen. Dazu klicken wir auf

Datenträger und wählen die richtige Partition bzw. Datenträger aus.
Hier sollte man auf jeden Fall den richtigen Datenträger bzw. USB-Laufwerk auswählen, damit man nicht aus Versehen die Backup-Platte platt macht oder den falschen USB-Stick.



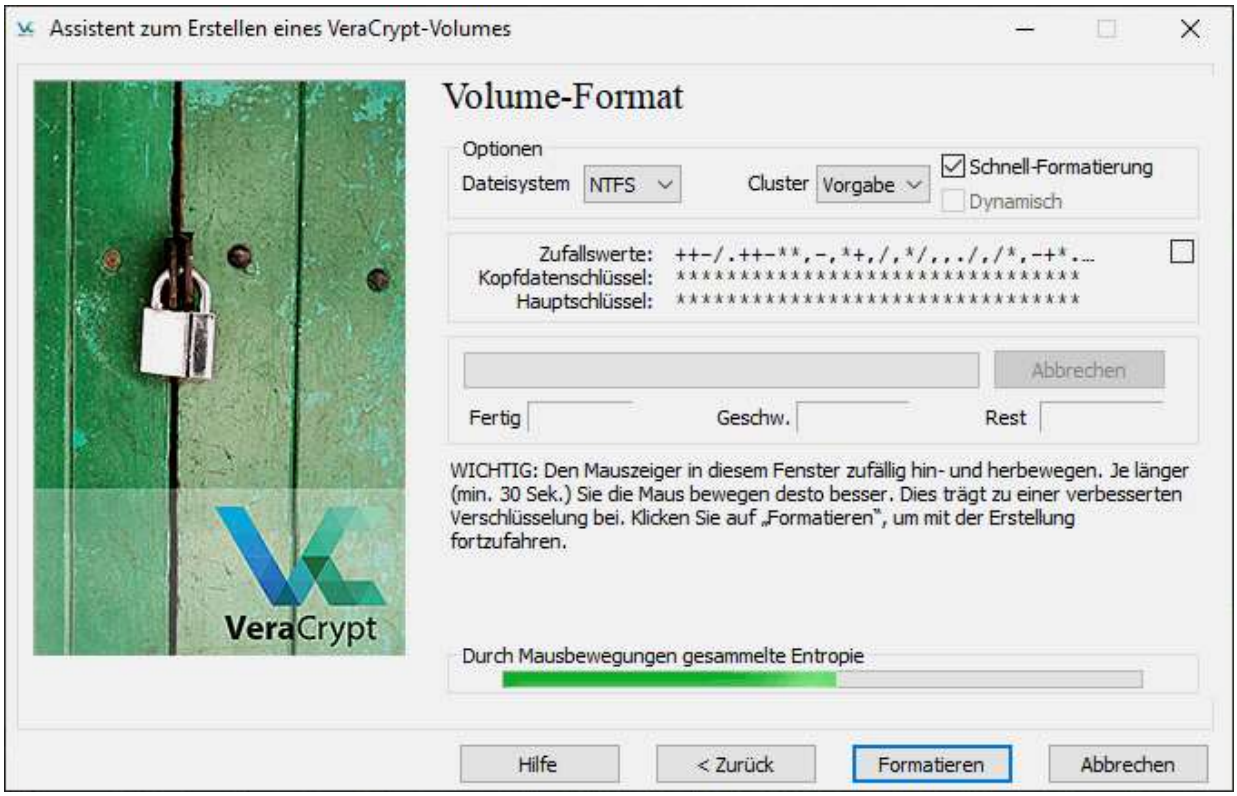
Im nächsten Schritt haben wir zwei Optionen:

Die erste Option: der Datenträger wird formatiert und alle Daten gelöscht. Die zweite Option verschlüsselt die Daten auf dem USB-Stick, die Daten bleiben erhalten. Hier sollten Sie die richtige Option auswählen. Generell gilt, sind die Daten wichtig, auch bei der zweiten Option ein Backup vorher erstellen. Die Option die Daten zu erhalten und zu verschlüsseln steht nur für Datenträger mit NTFS zur Verfügung.

Im nächsten Schritt legen wir die Verschlüsselungsmethode fest, siehe oben. Die Speichergröße können wir in diesem Fall nicht festlegen, der gesamte Datenträger wird verschlüsselt.

Nun folgt die Eingabe des Passwortes. Zuletzt erfolgt die Abfrage, ob größere Dateien abgespeichert werden sollen.

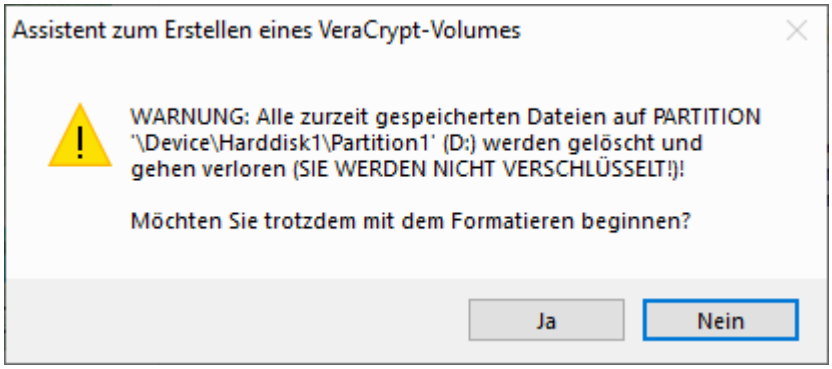
In vielen Fällen ist „Ja“ die richtige Option. Wirklich viele Auswirkungen hat die Option nicht, letztlich wird hier nur das Dateisystem vorausgewählt, welches wir im nächsten Schritt ändern können.



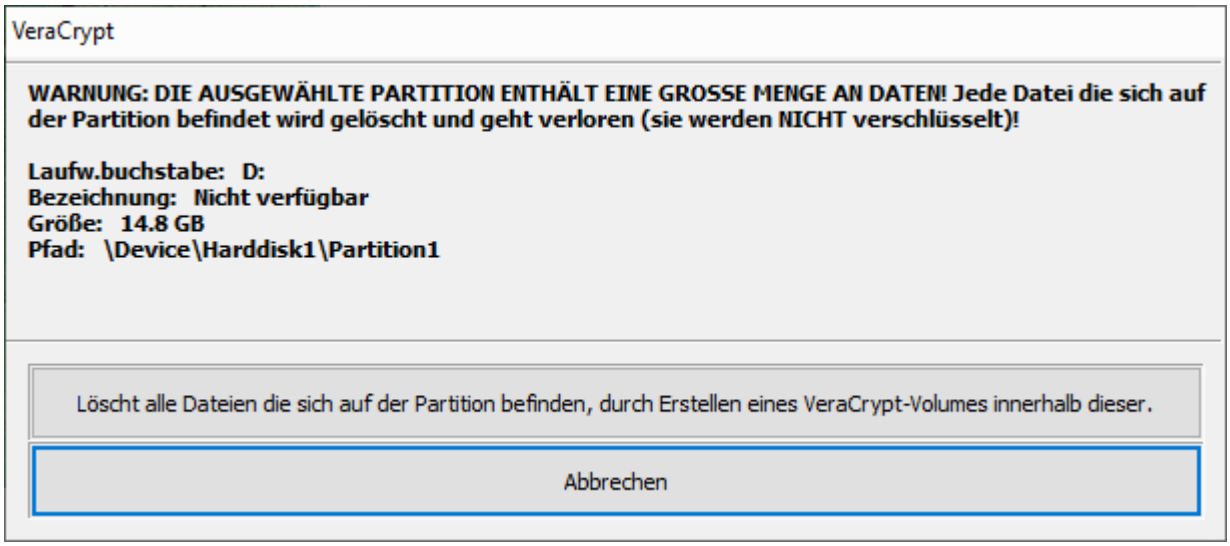
Wie bereits zuvor sollten wir auch hier die Maus einige Zeit im Fenster bewegen. Die Option „Schnellformatierung“ sollten wir nur bei Datenträgern verwenden, welche noch keine sensiblen Daten

enthalten, da hier keine Daten überschrieben werden und Datenrettungsprogramme hier Daten wiederherstellen können.

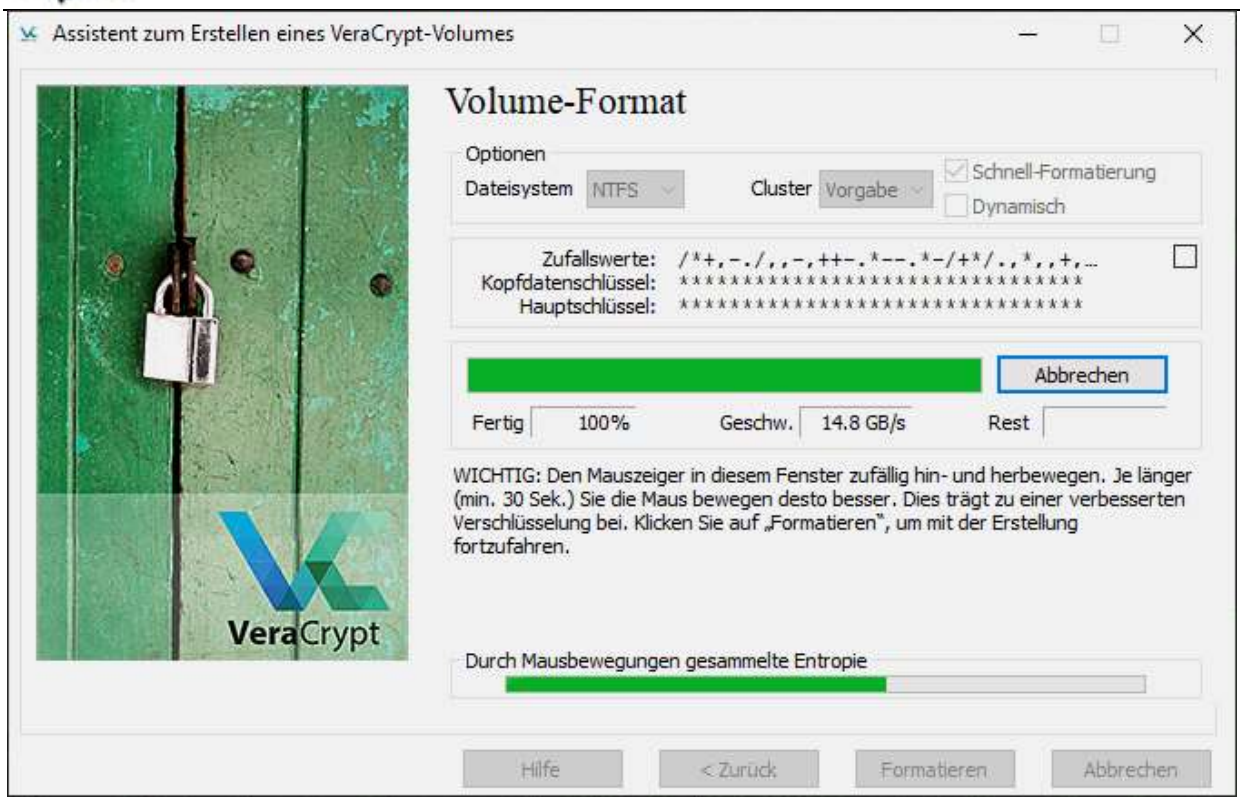
Die Formatierung starten wir mit dem Button „Formatieren“. Es erfolgt eine Warnung, dass alle Daten auf dem Datenträger gelöscht werden.



Sofern bereits Daten auf dem Datenträger sind, erscheint gleich noch eine Warnung!

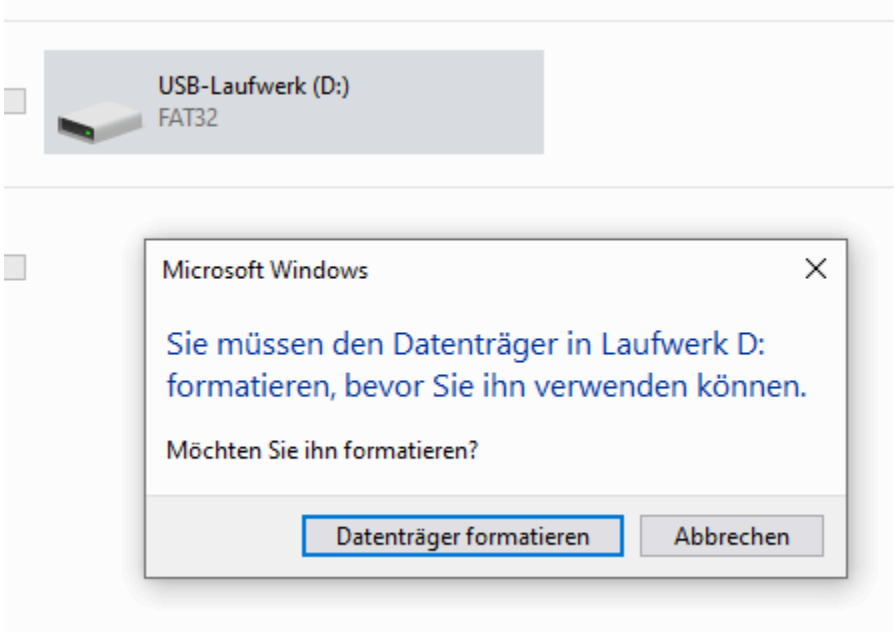


Anschließend wird die Formatierung durchgeführt.



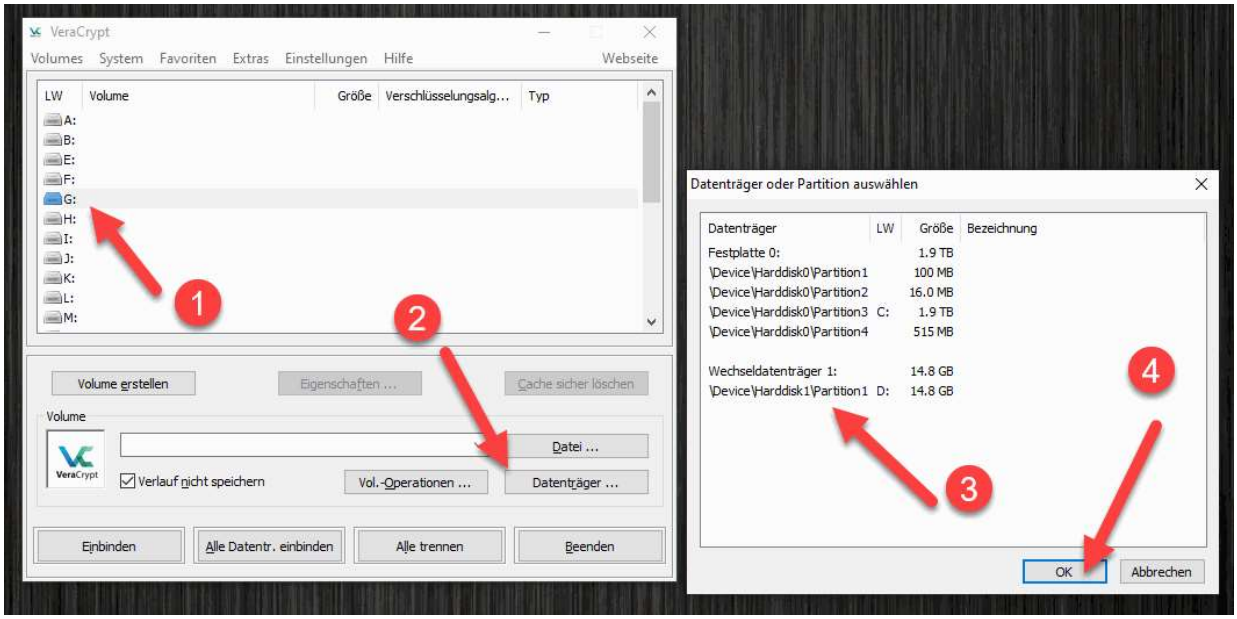
Einbinden des Laufwerks

Nach dem Verschlüsseln sehen wir unser USB-Laufwerk zwar im Explorer, aber es wird kein freier Speicher mehr angezeigt. Klicken wir das Laufwerk erscheint auch der Hinweis, dass der Datenträger erst formatiert werden müsse.

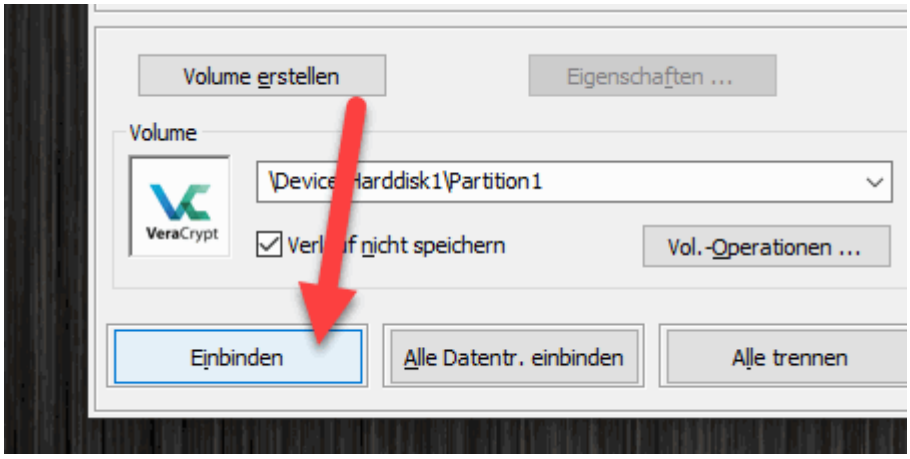


Formatieren Sie den Datenträger auf gar keinen Fall!

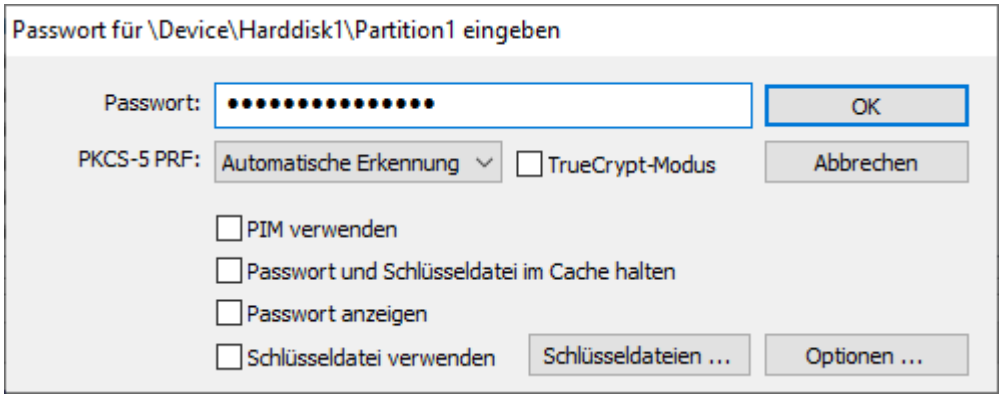
Das Einbinden nehmen wir mit VeraCrypt vor. Hier wählen wir zuerst einen freien Laufwerksbuchstaben aus, klicken auf Datenträger und wählen unseren Datenträger bzw. Partition aus.



Anschließend klicken wir den Button einbinden.



Es erfolgt die Passworteingabe.



Hat alles geklappt wird der verschlüsselte Datenträger nun eingebunden.

Quelle: https://ekiwi-blog.de/8762/usb-stick-usb-festplatte-mit-veracrypt-verschluesseln/

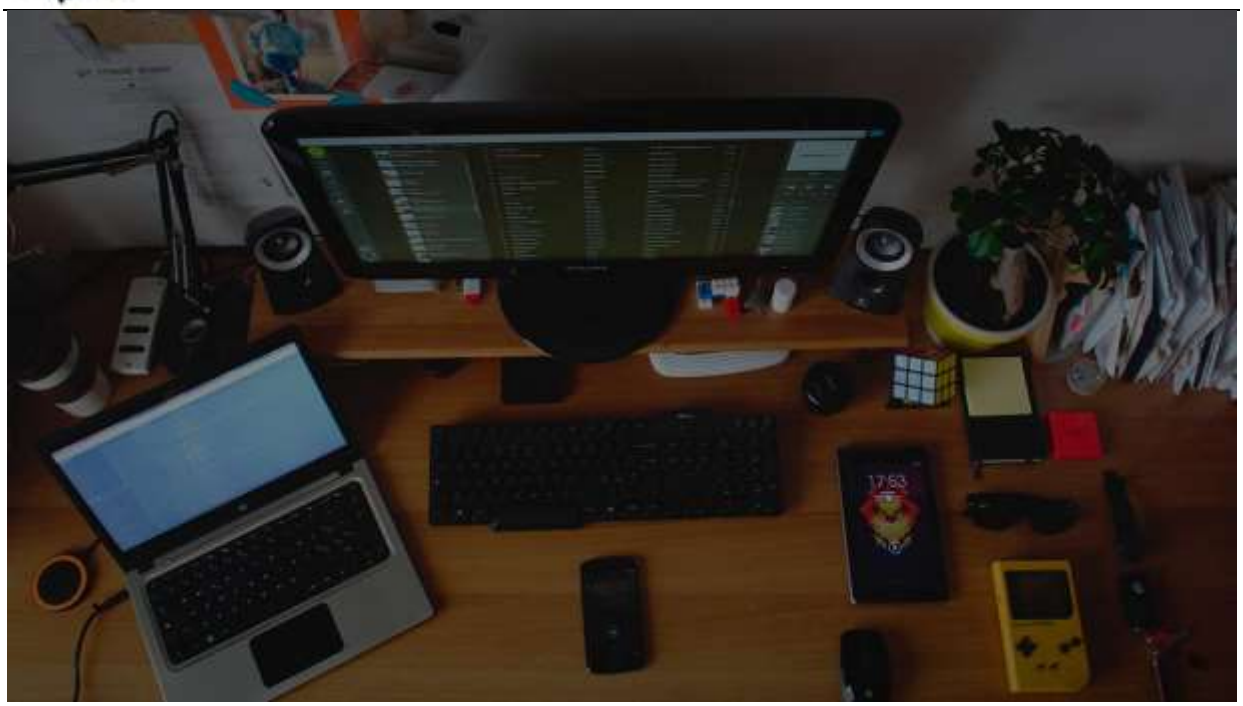
Wie kann ich Dateien von einem verschlüsselten Laufwerk TrueCrypt oder VeraCrypt wiederherstellen?

Lesen Sie, wie Sie gelöschte Dateien aus einem Container TrueCrypt oder VeraCrypt wiederherstellen und ein verschlüsseltes Laufwerk für den Zugriff auf Dateien einbinden und entsperren.

Inhalt

Wenn Sie nach einer einfachen und effektiven Möglichkeit suchen, alle Computerdaten von einem System oder einem normalen logischen Laufwerk auf eine Sicherungsdiskette, ein externes USB-Laufwerk oder eine Speicherkarte zu verschlüsseln, verwenden Sie VeraCrypt. Es ist ein Open Source-Tool, das die höchsten Standards für die Datenverschlüsselung erfüllt.

Zur Ansicht gehen



Verschlüsselung des Systemlaufwerks C mit Bitlocker in Windows 10, Aktivieren von TPM

Was ist TrueCrypt, VeraCrypt und warum werden sie verwendet?

Der beste Weg, um Ihre Dateien vor dem Anzeigen durch Unbefugte zu schützen, besteht darin, sie zu verschlüsseln. Das Verschlüsselungsprogramm verwendet einen geheimen Schlüssel, um den Inhalt von Dateien in einen Strom unlesbaren Delirs zu verwandeln. Solange Sie den Schlüssel nicht zum Entsperren verwenden, können Sie den Inhalt nicht lesen.

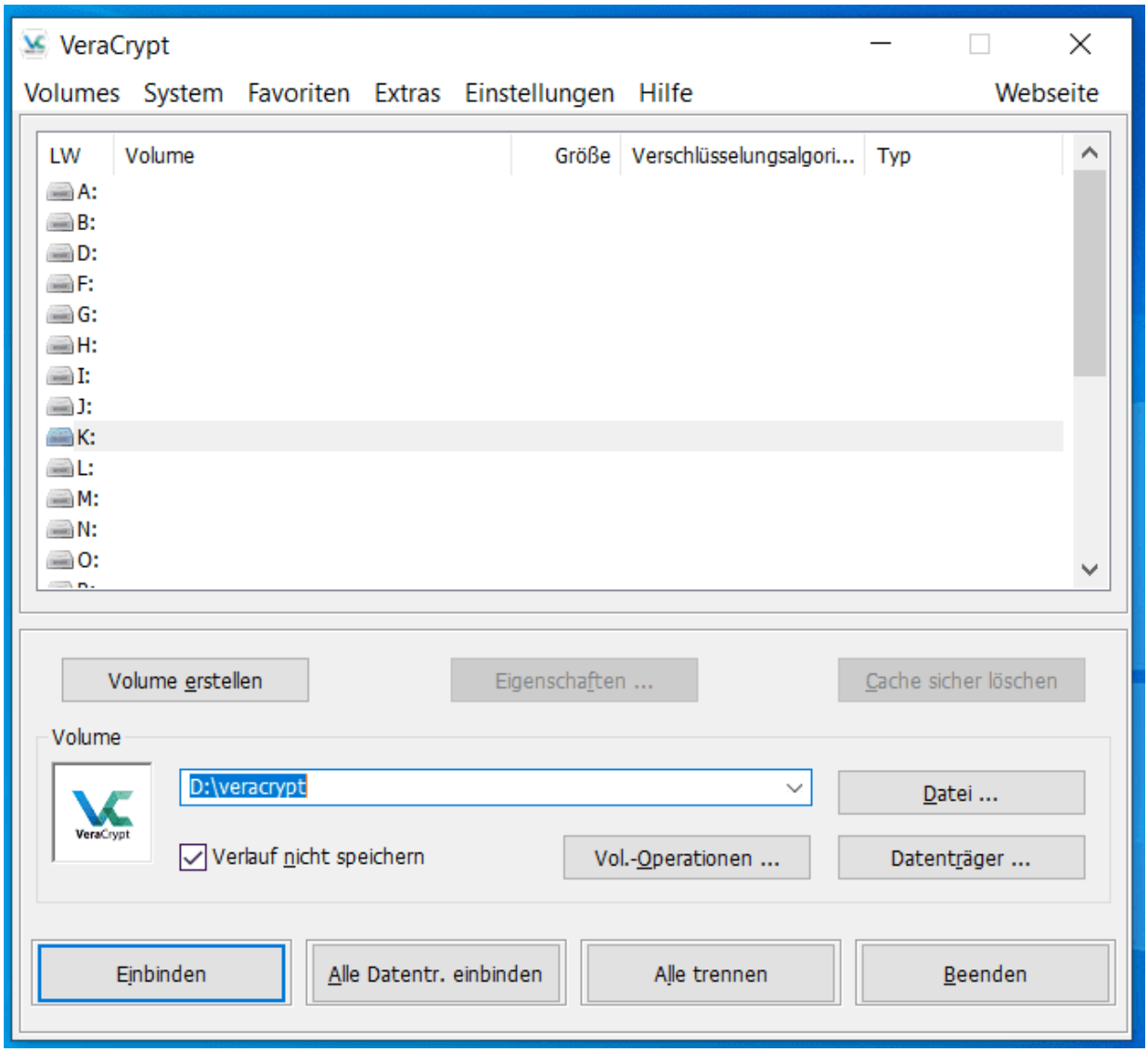
VeraCrypt basiert auf dem sehr beliebten Open Source-Tool TrueCrypt. Nachdem das TrueCrypt-Projekt geschlossen wurde, hat IDRIX das Produkt mit neuen Funktionen und behobenen Sicherheitsproblemen fertiggestellt.

Mit VeraCrypt können Sie einen verschlüsselten Containerdatei erstellen, der wie eine normale Festplatte auf dem System eingebunden wird. Alle Dateien aus diesem Containerdatei werden im laufenden Betrieb verschlüsselt und entschlüsselt. Daher können Sie sie weiterhin so anzeigen und bearbeiten, als wären sie auf Ihrem Flash-Laufwerk. Am Ende der Arbeit mit einem Container blockiert das Programm den Zugriff darauf und löscht die Schlüssel und den Inhalt von Dateien aus dem RAM.

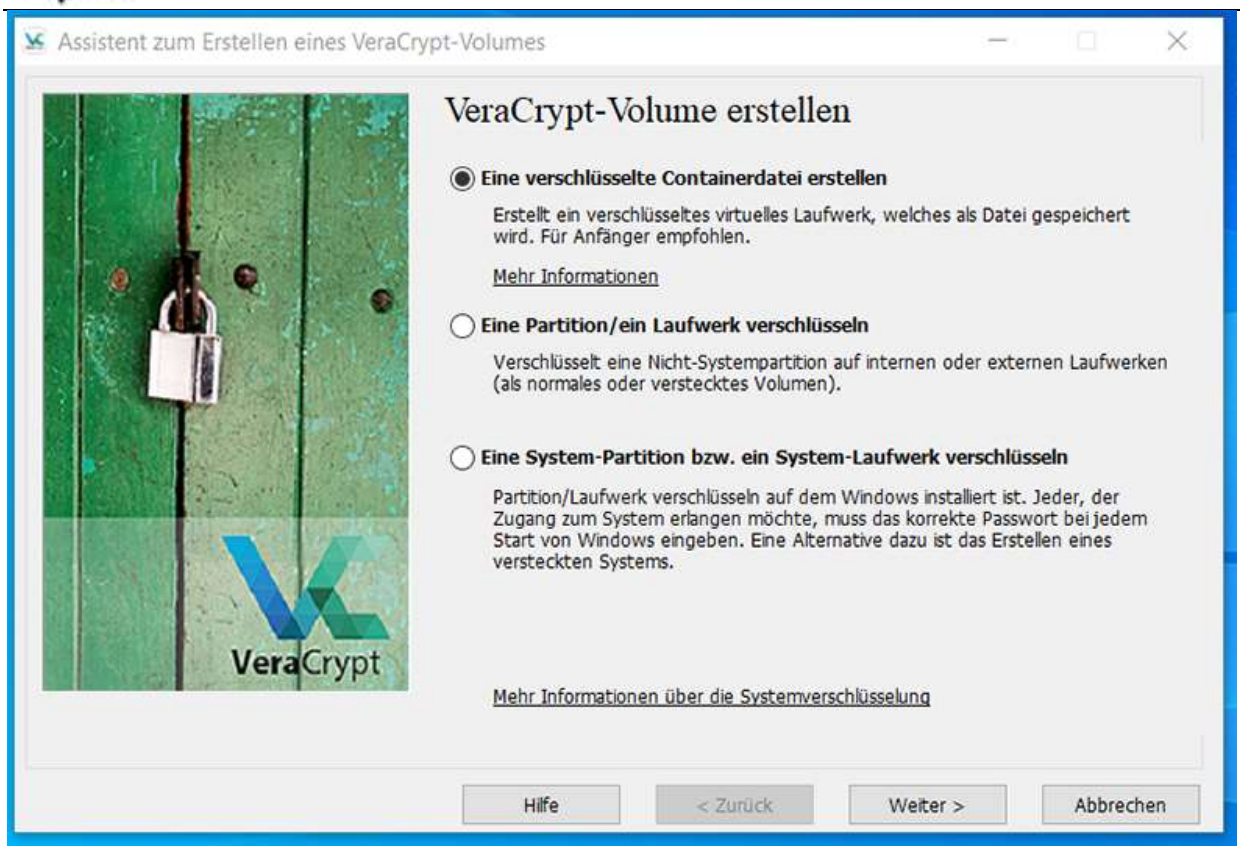
Mit VeraCrypt können Sie das Systemlaufwerk verschlüsseln. Wir empfehlen jedoch die Verwendung des in Windows 10 integrierten Bitlocker-Tools. Eine Funktion von VeraCrypt ist die Möglichkeit, eine versteckte verschlüsselte Partition zu erstellen. Wenn Sie sich in den Händen von Angreifern befinden und diese Sie nach einem Schlüssel fragen, können Sie ihnen einen **„gefälschten“** Schlüssel zur Verfügung stellen, um einen vorbereiteten **„gefälschten“** Abschnitt freizuschalten. Durch die Verwendung des Primärschlüssels wird ein völlig anderer Abschnitt mit realen Daten freigeschaltet.

So erstellen Sie eine verschlüsselte Partition

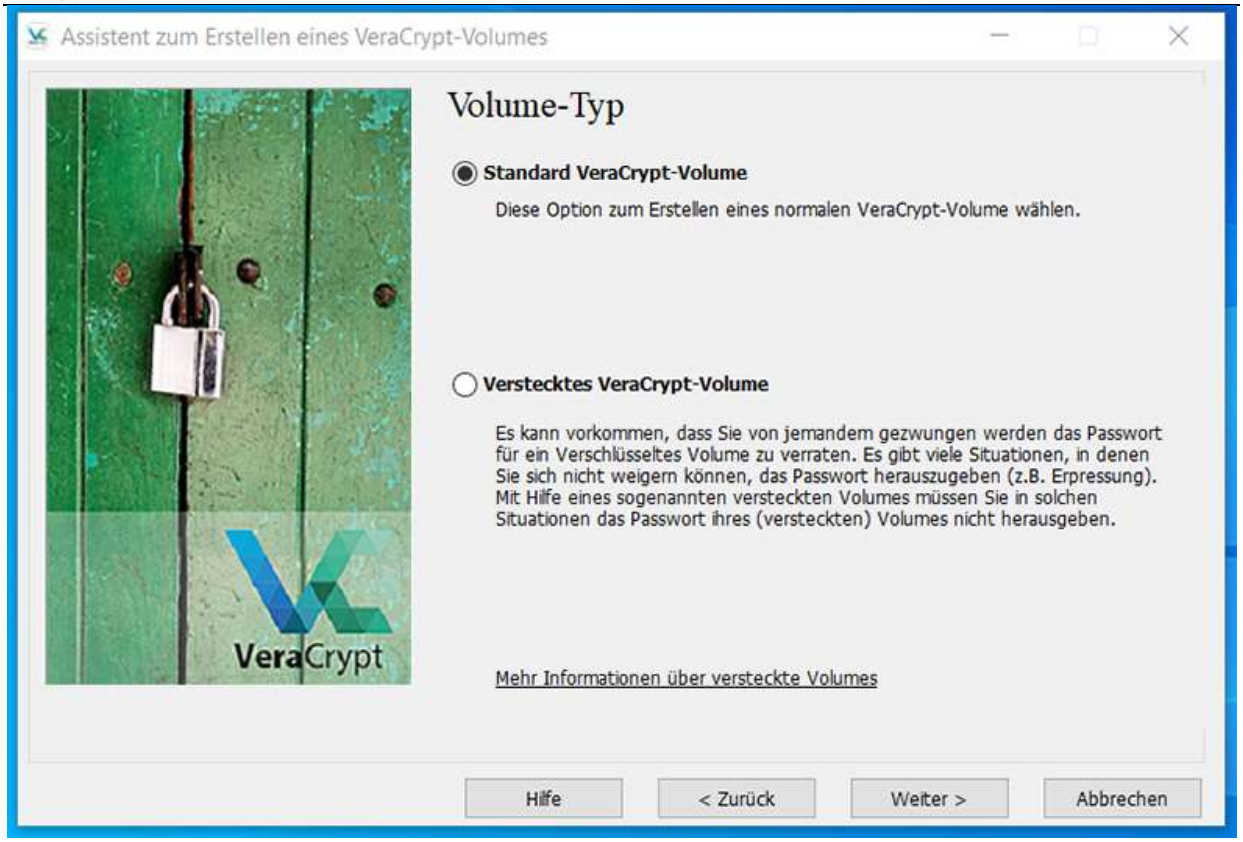
Laden Sie das Programm herunter und installieren Sie es. Gehen Sie dann zum Startmenü und starten Sie VeraCrypt. Sie sehen das Hauptfenster des Programms:



Als erstes sollten Sie auf die Schaltfläche **Volume erstellen** klicken. Diese Aktion startet den Assistenten zum Erstellen verschlüsselter Partitionen, der die folgenden Erstellungsoptionen bietet:



Durch das Erstellen eines verschlüsselten Containerdatei können Sie eine Datei auf jedem Laufwerk erstellen, das an einen Computer angeschlossen ist. Dann kann eine solche Datei als logisches Laufwerk eingebunden werden. In der Datei können Sie Standart VeraCrypt-Volume oder Verstecktes VeraCrypt-Volume erstellen (wir haben den Unterschied oben erläutert).



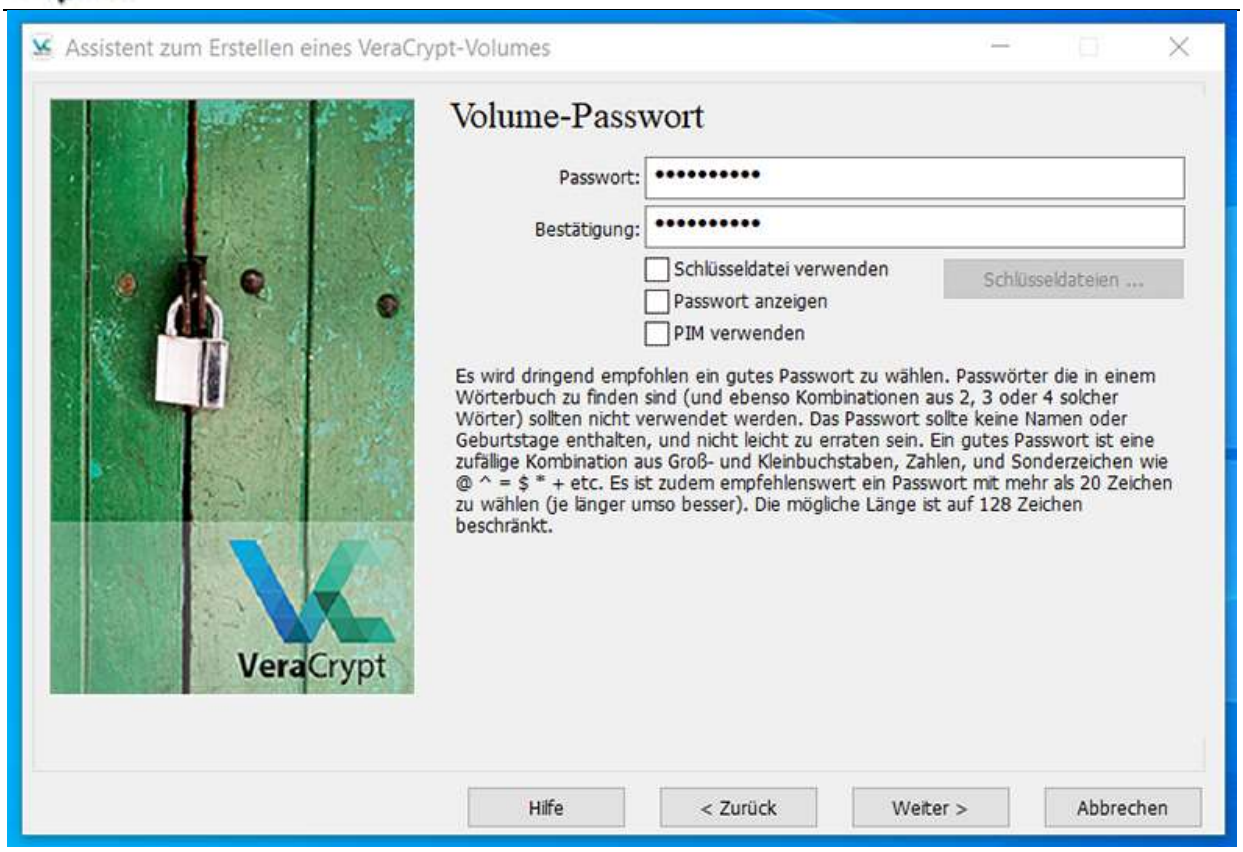
Wir werden Standart VeraCrypt-Volume erstellen. Der nächste Schritt besteht darin, Volume-Speicherort der Containerdatei auszuwählen.

Der nächste Schritt besteht darin, den Verschlüsselungsalgorithmus und Hash-Algorithmus anzugeben. Standardmäßig ist der Verschlüsselungsalgorithmus AES, der Hash-Algorithmus SHA-512. Lassen sie es wie es ist.

Der nächste Schritt besteht darin, die maximale Größe der Containerdatei anzugeben. Geben wir 5 GB an.

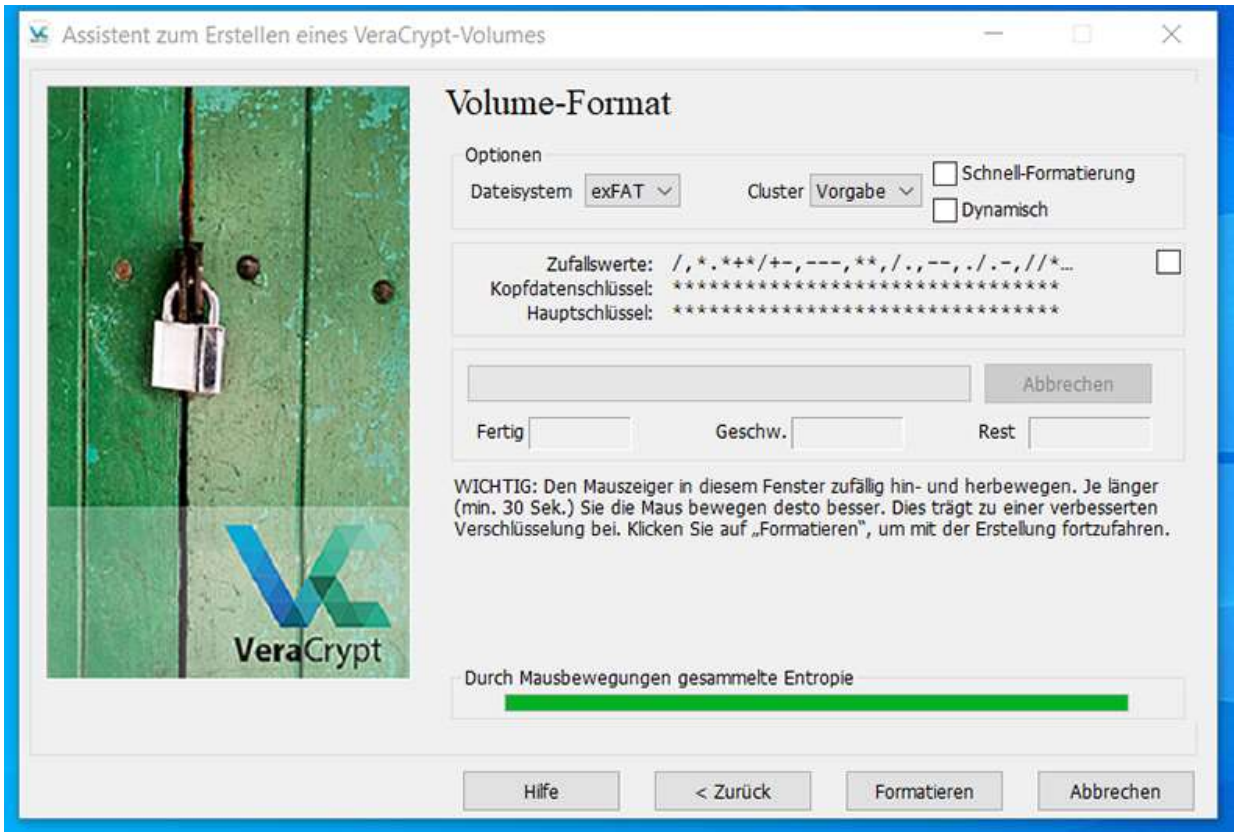
Klicken Sie auf **Weiter** und gehen Sie zum Fenster zur Passworteinstellung. Speichern Sie das Passwort nach der Angabe an einem sicheren Ort oder verwenden Sie ein Passwort, das Sie gut kennen. Das Programm bietet keine Möglichkeit, ein vergessenes oder verlorenes Passwort wiederherzustellen, und das Entschlüsseln von Informationen ohne Passwort schlägt fehl.

Sie können beliebige Dateien verwenden, die als Alternative zu einem Passwort verwendet werden.



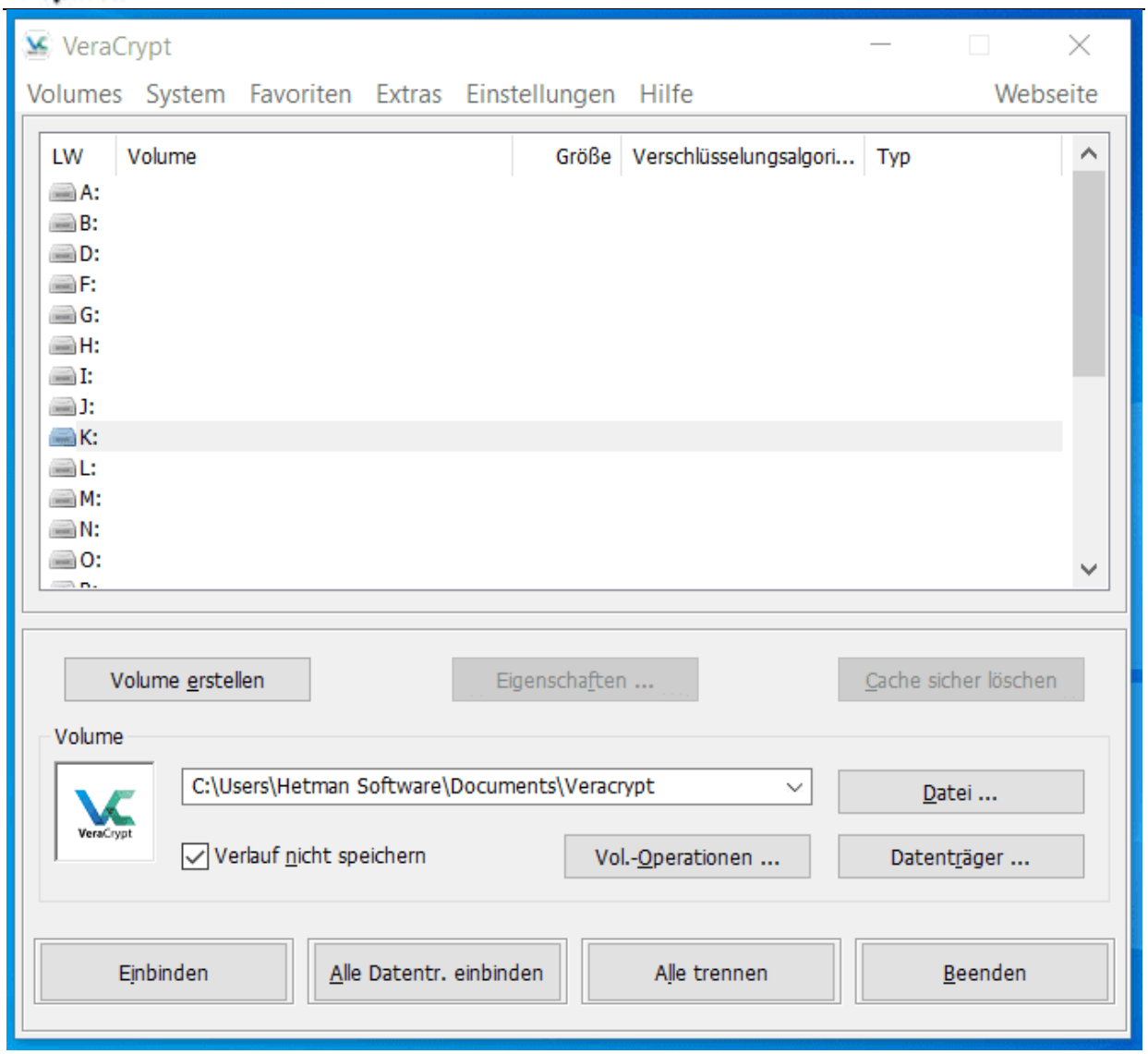
Klicken Sie auf **Weiter** und bestätigen Sie die Verwendung großer Dateien.

Klicken Sie auf **Weiter** und gehen Sie zu den Optionen für die Volume-Format und die Generierung von Verschlüsselungsschlüsseln. Klicken Sie auf Formatieren und warten Sie auf die Erstellung des verschlüsselten Volumes.

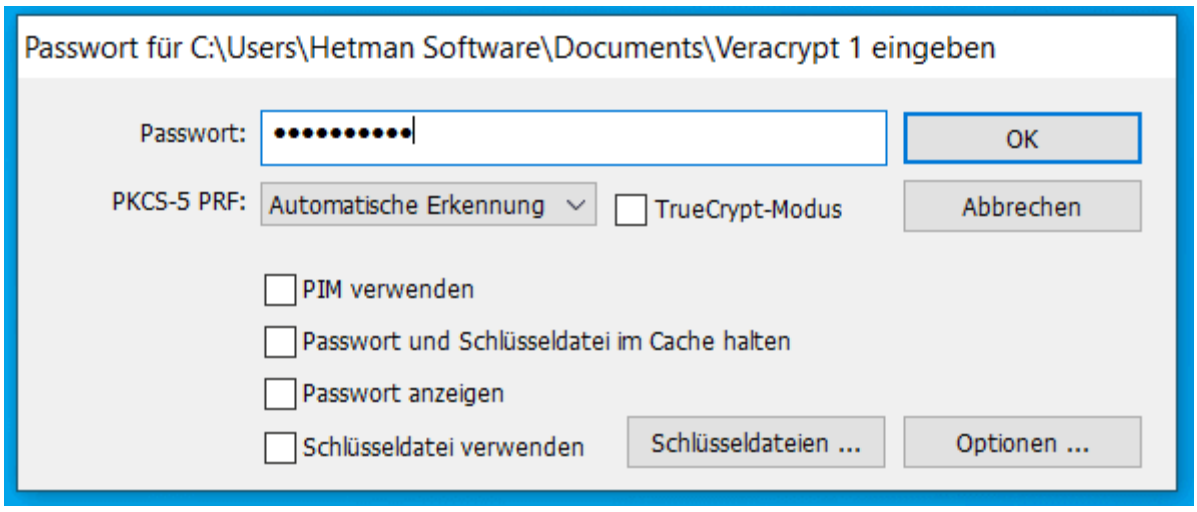


Wie kann ich eine Laufwerk einbinden und entsperren, um auf Dateien zuzugreifen?

Klicken Sie im Hauptprogrammfenster auf die Schaltfläche **„Datei auswählen"** und geben Sie die Datei an, in der Sie den VeraCrypt-Container gespeichert haben. Geben Sie nach Auswahl der Datei im obigen Feld eine der verfügbaren Festplatten an. Wählen Sie beispielsweise Laufwerk K aus und klicken Sie auf **Einbinden**.



Geben Sie als nächstes das Passwort ein.



Danach können Sie zu **Dieser PC** gehen und das Erscheinungsbild des neuen Laufwerk überprüfen.

So wiederherstellen Sie gelöschte Dateien aus dem Container VeraCrypt

Dateien, die versehentlich gelöscht wurden oder Daten, die durch die Formatierung eines verschlüsselten Laufwerk verloren gingen, können mit Hetman Partition Recovery wiederhergestellt werden. Bevor Sie mit dem Scannen eines Laufwerk beginnen, müssen Sie das Laufwerk im Programm einbinden. Da die VeraCrypt- Containerdatei das Prinzip der direkten Verschlüsselung verwendet, ist der Wiederherstellungsprozess der gleiche wie auf einem normalen Laufwerk.

Partition Recovery™ 4.2
Das Tool stellt Daten von allen Geräten wieder her, unabhängig von der Ursache des Datenverlusts.
Herunterladen

Laden Sie das Programm herunter und installieren Sie es. Befolgen Sie dann die Anweisungen im Handbuch zur Dateiwiederherstellung.

Ohne ein Passwort zum Entsperren werden die Daten auf dem Laufwerk verschlüsselt und können nicht wiederhergestellt werden.

Quelle: https://hetmanrecovery.com/de/recovery_news/how-to-recover-files-from-a-truecrypt-or-veracrypt-encrypted-disk.htm

DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 890 729 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

VeraCrypt: Profi-Tricks für das Verschlüsselungs-Tool

06.06.2020 | 08:36 Uhr | Arne Arnold

Das Verschlüsselungsprogramm Veracrypt kann viel mehr, als nur sichere Container für Dateien zu erzeugen. Veracrypt verschlüsselt auch Ihr komplettes System und schützt es so vor neugierigen Blicken. Dieser Beitrag zeigt, wie Sie dabei vorgehen und worauf Sie bei dieser wie auch bei weiteren Profi-Funktionen von Veracrypt achten müssen.

Vergrößern VeraCrypt: Die besten Tipps für Anfänger und Profis.
© © Rob King / Unsplash, Toshiba

Die kostenlose Software Veracrypt zählt zu den beliebtesten Verschlüsselungsprogrammen für Privatanwender. Aus gutem Grund: Hat man sich die Handhabung des Tools einmal angeeignet, lässt es sich einfach nutzen. Das Tool arbeitet sehr schnell und gilt sicherheitstechnisch als besonders zuverlässig. Die meisten Anwender nutzen die Software, um damit einen verschlüsselten Container für Dateien zu erstellen. Veracrypt nennt diese Container auch Volumes. Ein Container ist zunächst mal eine verschlüsselte Datei in einer frei wählbaren Größe. Diese Datei wird nach Eingabe eines Passworts entschlüsselt und automatisch als neues Laufwerk in Windows eingebunden. Der Inhalt des Containers erscheint in diesem Laufwerk, und Sie können die Dateien wie auf einem gewöhnlichen Laufwerk behandeln. Der Unterschied: Sobald Sie das Laufwerk mit Veracrypt per Befehl „Trennen“ wieder entfernen, sind alle Daten darin sicher verschlüsselt und nur für den zugänglich, der das Passwort kennt. Eine ausführliche Anleitung zum Erstellen solcher Container finden Sie in diesem Ratgeber . Tipps für die Profifunktionen von Veracrypt finden Sie hier.

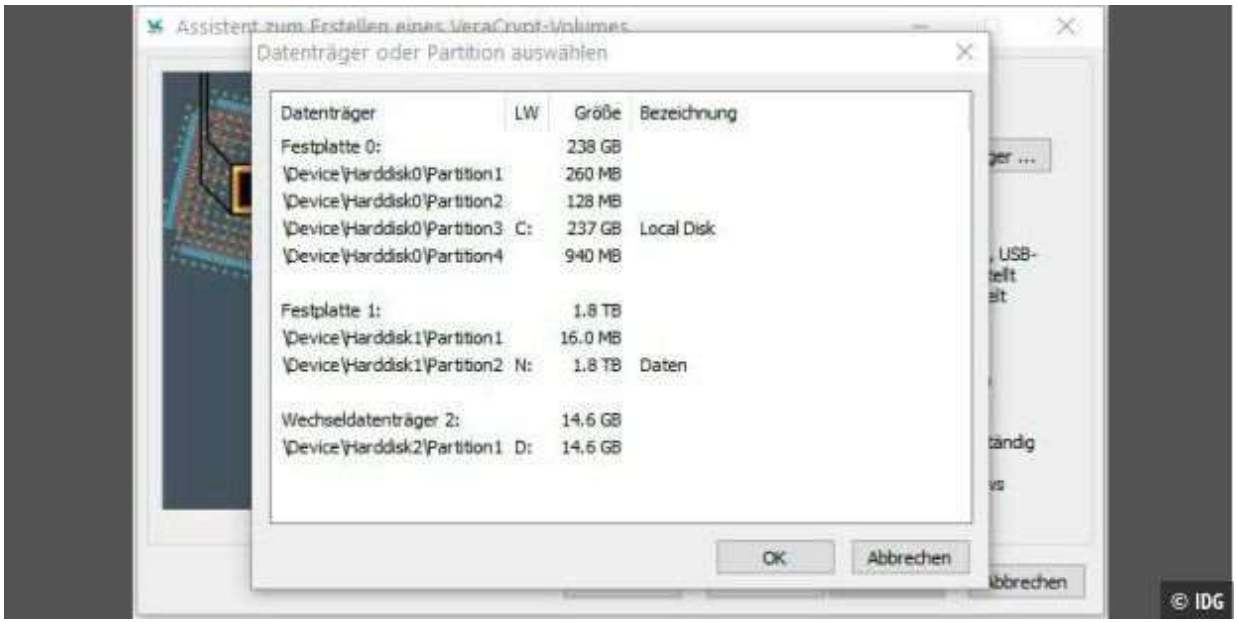
Ein Hinweis noch vorweg: Veracrypt hat die Angewohnheit, einige seiner Assistenten nach Abschluss der Aktion wieder von vorne zu starten. Das passiert etwa nach dem Erstellen eines Containers. Klicken Sie dann einfach auf Abbrechen, um den Assistenten zu beenden.

Tipp: So verschlüsseln Sie E-Mails ganz einfach

Vor der Verschlüsselung kommt unbedingt ein Backup

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 Backup-Gebot gilt für Daten- und für Systemlaufwerke. Empfehlenswert ist etwa das Backup- und Image-Tool Acronis True Image . Darin können Sie übrigens auch angeben, dass das Backup verschlüsselt werden soll. Eine wichtige Funktion, da Sie die Daten ja schützen möchten.

So verschlüsseln Sie komplette Partitionen



Vergrößern Möchten Sie einen Datenträger verschlüsseln, etwa einen USB-Stick, dann wählen Sie ihn in diesem Fenster anhand von Laufwerksbuchstaben, Größe und Bezeichnung zuverlässig aus.

Das Verschlüsseln von ganzen Laufwerken funktioniert mit Veracrypt unkompliziert, wenn Sie ein paar Kleinigkeiten beachten. In diesem Beispiel verschlüsseln wir einen kompletten USB-Stick. Wählen Sie dafür in Veracrypt den Assistenten unter „Volume erstellen –› Verschlüsselt eine Partition / ein Laufwerk –› Standard Veracrypt-Laufwerk“.

Datenträgerauswahl: Im nächsten Fenster steht die Datenträgerauswahl an. Vorsichtig sollten Sie bei der angebotenen Historie neben dem Button „Datenträger“ sein: Diese ist bei externen Datenträgern nicht eindeutig. So kann „\Device\Harddisk1\ Partition1“ einmal Ihren USB-Stick und nach einem Windows-Neustart Ihre externe Festplatte bezeichnen. Beim Klick auf „Datenträger“ dagegen öffnet sich ein neues Fenster, und Ihnen werden zu einem Laufwerk auch der Laufwerksname (falls vorhanden) sowie Laufwerksbuchstabe und -größe angezeigt. Das hilft bei der Zuordnung ungemein. Das Systemlaufwerk können Sie an dieser Stelle nicht auswählen, da das einen anderen Assistenten in Veracrypt voraussetzt. Meiden Sie auch kleine Partitionen mit ein paar MB Größe, die Sie nicht kennen. Dabei handelt es sich meist um systemrelevante Partitionen. In unserem Beispiel ist der USB-Stick leicht an seiner Größe

erkennbar. Wählen Sie die gewünschte Partition sorgfältig aus und klicken Sie auf „Ok“ sowie anschließend auf „Weiter“, um zum Fenster „Volume-Erstellmodus“ zu gelangen.

Vergrößern Veracrypt fordert Sie vor der Erstellung eines verschlüsselten Volumes auf, Ihre Maus längere Zeit zu bewegen. Aus diesen Bewegungen erstellt das Tool Zufallsdaten, die es für die Verschlüsselung benötigt.

Erstellmodus: Im „Volume-Erstellungsmodus“ zeigt Veracrypt als erste Auswahlmöglichkeit „Verschlüsseltes Volume erstellen und formatieren“. Achtung: Diese Option löscht alle Daten auf dem Laufwerk. Die zweite Möglichkeit („Partition ‚in-place‘ verschlüsseln“) behält die Daten und verschlüsselt sie. Voraussetzung für die zweite Möglichkeit ist ein NTFS-Laufwerk. Wählen Sie die Methode je nach Ihren Anforderungen.

Vergrößern Wählen Sie in Veracrypt die Funktion „Volume erstellen –› Eine System-Partition bzw. ein System-Laufwerk verschlüsseln“, um Ihr Laufwerk mit Windows zu verschlüsseln. Sicherheitshalber: Erstellen Sie vorher ein Backup.

Verschlüsselung wählen und abschließen: Der Assistent führt Sie nun weiter durch den Verschlüsselungsprozess. Was dabei zu beachten ist, steht im Kasten unten. Haben Sie beim „Volume-Erstellungsmodus“ die Methode „Partition ‚inplace‘ verschlüsseln“ gewählt, fragt Sie der Assistent noch nach einer Löschmethode. Damit legen Sie fest, wie die unverschlüsselten Originaldateien gelöscht werden sollen, nachdem Veracrypt davon Kopien in den verschlüsselten Container gepackt hat.

Meldungen beachten: Bei Problemen meldet sich Veracrypt automatisch. Möchten Sie etwa einen USB-Stick verschlüsseln und haben das Laufwerk des Sticks statt der darauf enthalten Partition ausgewählt, warnt Veracrypt vor Gefahren. Wählen Sie dann wie vorgeschlagen die Partition des Sticks, geht es ohne Beschwerde weiter.

Vergrößern Wenn Sie einen Dateicontainer erstellen, dann können Sie in Veracrypt die Größe wählen. Diese lässt sich nachträglich noch verändern. Das geht in Veracrypt über „Extras –› Volume erweitern“.

So wählen Sie den passenden Schlüssel in Veracrypt

Wenn Sie mit Veracrypt einen neuen Container oder eine Partition verschlüsseln, bietet das Programm mehrere Optionen an. Sie können zwischen „Passwort“ und „Schlüsseldatei“ wählen sowie einen Wert für die Iterationen („PIM“) angeben und den Verschlüsselungsalgorithmus wählen.

Darauf sollten Sie bei der Verschlüsselung achten:

Passwort: Je länger das Passwort, desto besser. Veracrypt erachtet ein Passwort ab 20 Zeichen als sicher. Nach der Eingabe des Passworts müssen Sie in einem weiteren Fenster den Mauszeiger bewegen. Auf diese Weise erzeugen Sie Zufallszahlen, die den Schlüssel sicherer machen.

Tipp: Lassen Sie sich das eingegebene Passwort durch einen Klick auf „Passwort anzeigen“ einblenden. Es besteht die Gefahr, dass Sie sich vertippt haben oder dass in dem Moment der Eingabe ein anderes Tastaturlayout eingestellt ist. Wenn Sie die Eingabe nicht kontrollieren,

aber ein anderes Passwort vergeben haben als gedacht, dann können Sie Ihre Daten nicht mehr entschlüsseln. Sie sind und bleiben unzugänglich.

Personal Iterations Multiplier (PIM): Sie können einen Wert im Feld „PIM“ angeben. Damit bestimmen Sie, mit wie vielen Wiederholungen Ihr Passwort durch die Hashfunktion läuft, bevor es zum Verschlüsseln der Daten verwendet wird. Das erhöht den Aufwand für Passwortknacker.

Grundsätzlich gilt hierfür: Ein kurzes Passwort lässt sich mit einem hohen PIM-Wert sicherer machen. Ein langes Passwort schützt auch mit einem niedrigen PIM-Wert.

Unsere Empfehlung für die meisten Container lautet: Vergeben Sie ein langes Passwort mit mindestens 20 Zeichen und lassen Sie das PIM-Feld leer. Dann nutzt Veracrypt den Standardwert von 500.000 Durchgängen. Der niedrigste PIM-Wert 1 setzt die Iterationen auf 16.000 bei verschlüsselten Partitionen und 2.048 bei Systempartitionen. Je höher der PIM-Wert, desto länger dauert das Entschlüsseln eines Volumes. Auf die Arbeitsgeschwindigkeit nach dem Entschlüsseln hat der Wert aber keinen Einfluss. Diese hängt am verwendeten Algorithmus und der PC-Hardware.

Verschlüsselungsalgorithmus: Die Wahl des Algorithmus für die Verschlüsselung hat entscheidenden Einfluss auf die Sicherheit und Lese-/Schreibgeschwindigkeit der Daten. Einen Überblick über gängige Verschlüsselungsalgorithmen finden Sie hier . Wir empfehlen den bewährten AES-Algorithmus. Dieser ist zusammen mit dem Hash-Algorithmus SHA-512 in Veracrypt voreingestellt.

Vergrößern Wenn Sie einen PC starten, dessen Systempartition mit Veracrypt verschlüsselt ist, sieht der Startbildschirm so aus. Geben Sie hier Ihr Passwort ein und drücken Sie die Enter-Taste. Haben Sie keine Angabe bei „PIM“ gemacht, lassen Sie das Feld beim Neusta

Schlüsseldatei: Statt eines Passworts oder auch zusätzlich lässt sich ein Volume mit einer Datei als Schlüssel schützen. Weitere Infos dazu finden Sie im nächsten Kasten.

So erstellen Sie einen gut versteckten Container

Mit Veracrypt lassen sich auch versteckte Container erstellen. Bei dieser Methode wird innerhalb eines sichtbaren Containers (Volumes) ein weiterer, unsichtbarer Container mit einem eigenen Passwort erstellt. Der Vorteil: Wenn jemand anderes den ersten Container entdeckt und Sie zwingt, das Passwort dafür zu verraten, dann bleibt der zweite Container trotzdem unentdeckt. Er fällt weder durch seine Dateigröße noch durch andere Details auf.

Am einfachsten erstellen sie einen versteckten Container, wenn Sie sich für „Kompletter Modus“ entscheiden. So erstellt Veracrypt den sichtbaren und den unsichtbaren Container in einem Rutsch. Wichtig: Wenn Sie einen versteckten Container auf einem Laufwerk, etwa einem USB-Stick, erstellen wollen, dürfen darauf zunächst keine Daten gespeichert sein, da Veracrypt den Datenträger formatiert.

So geht’s: Wählen Sie in Veracrypt „Volume erstellen –› Verschlüsselt eine Partition / ein Laufwerk –› Verstecktes Veracrypt- Laufwerk“. Im nächsten Fenster wählen Sie „Kompletter Modus“, um sowohl den sichtbaren Container (Volume) als auch den darin befindlichen unsichtbaren Container zu erstellen. Ein Klick auf „Datenträger“ bringt Sie zum Auswahlfenster mit allen verfügbaren Partitionen und Laufwerken.

Nach der Wahl von Passwort und Verschlüsselungsalgorithmus erstellt Veracrypt den ersten Container. Über „Äußeres Volume öffnen“ greifen Sie darauf zu und kopieren einige unwichtige Dateien hinein, die einen Spion ablenken sollen. Machen Sie das gleich, später kann das Schreiben in den äußeren Container zu Datenverlust im inneren Container führen.

Danach erstellen Sie über „Weiter“ im Veracrypt-Assistenten den inneren Container, in den Sie dann die wirklich wichtigen und vertraulichen Daten speichern können. Dieser Container muss ein anderes Passwort erhalten als der äußere.

Siehe auch: Ist mein PC gehackt? So erkennen Sie Angriffe

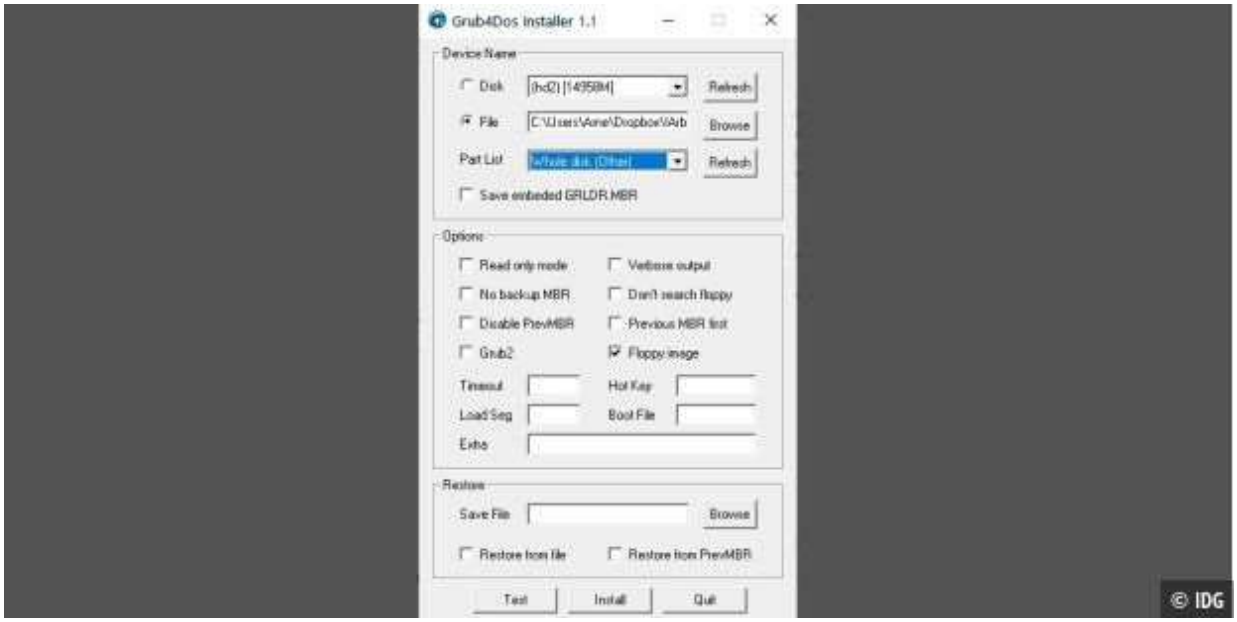
So binden Sie das verschlüsselte Laufwerk in Windows ein

Wenn Sie auf das verschlüsselte Laufwerk zugreifen möchten, dann müssen Sie es zuerst mit Veracrypt entschlüsseln und einem Laufwerksbuchstaben zuweisen. Ist Ihr Container eine Datei, wählen Sie in Veracrypt „Datei“. Möchten Sie einen verschlüsselten Datenträger einbinden, wählen Sie in Veracrypt den Button „Datenträger“. Wählen Sie zudem einen Laufwerksbuchstaben aus der Liste in Veracrypt und klicken Sie auf „Einbinden“.

Versteckte Container einbinden: Um einen versteckten Container als Laufwerk einzubinden, wählen Sie wie gewohnt die Datei oder den Datenträger des äußeren Containers aus. Doch als Passwort geben Sie das Passwort des inneren Containers ein. Veracrypt bindet dann diesen als Laufwerk ein und ignoriert den äußeren.

Wichtig: Wenn Sie einen kompletten Datenträger, etwa einen USB-Stick, verschlüsselt haben, dann greifen Sie nicht vor der Entschlüsselung mit dem Windows-Explorer darauf zu. Denn der Explorer würde Ihnen melden, dass Sie den USB-Stick vor der Nutzung formatieren müssen. Kommen Sie dem nach, vernichten Sie alle Daten auf dem Laufwerk.

Systemverschlüsselung



Vergrößern Vor der Verschlüsselung Ihres Systems speichert Veracrypt die Datei Veracrypt Rescue Disk.iso, die Sie mit dem Tool Veracrypt USB Rescue Disk (Screenshot) bootfähig auf einen USB-Stick bekommen.

Sie können mit Veracrypt auch das Systemlaufwerk verschlüsseln. Das empfiehlt sich etwa für Notebooks, die auch mit nach draußen genommen werden. Als Verschlüsselungsalgorithmus empfiehlt sich hier AES, da dieser flott arbeitet und es so nur zu sehr geringen Verzögerungen beim Festplattenzugriff kommt.

So geht's: Wählen Sie in Veracrypt „Volume erstellen –› Eine System-Partition bzw. ein System-Laufwerk verschlüsseln". Klicken Sie auf „Normal", um die vorhandene Systempartition zu verschlüsseln. An dieser Stelle gibt es auch die Möglichkeit, eine versteckte Systempartition zu erstellen. Nach einem Klick auf „Weiter" wählen Sie „Die Windows-System-Partition verschlüsseln". Nutzen Sie auf Ihrem Rechner nur ein Windows, wählen Sie anschließend „Ein Betriebssystem", nutzen Sie aber mehrere Systeme im Multibootverfahren, wählen Sie die andere Option. Es folgt die Auswahl von Passwort und Verschlüsselung. Folgen Sie den weiteren Anweisungen des Assistenten, der unter anderem ein bootfähiges Rettungs-ISO auf Ihrer Festplatte speichert. Am besten brennen Sie diese ISO-Datei gleich auf CD oder erstellen mithilfe des Tools Veracrypt USB Rescue Disk einen USB-Stick. Der Veracrypt-Assistent bietet an, diese CD umgehend zu prüfen. Wenn Sie dem zustimmen, geht es erst weiter, wenn die Überprüfung erfolgreich war. Sollten Sie das ISO nicht gleich brennen wollen, können Sie es mit der rechten Maustaste anklicken und „Bereitstellen" wählen. Windows bindet das ISO als virtuelle CD ein. So kann Veracrypt die CD prüfen und den Assistenten fortsetzen.

Folgen Sie dem Veracrypt-Assistenten weiter, der zunächst einen Verschlüsselungstest inklusive Neustart durchführt. Ist dieser Test erfolgreich, geht es ans tatsächliche Verschlüsseln.

Vergrößern Die Notfall-CD von Veracrypt hilft immer dann, wenn ein verschlüsseltes Laufwerk nicht booten will. Drücken Sie die Taste F8, um sich die Reparaturoptionen anzeigen zu lassen.

Achtung: An dieser Stelle zeigt Veracrypt eine Anleitung für die Nutzung der Notfall-CD an. Drucken Sie sich diese am besten aus, um im Notfall darauf zugreifen zu können. Speichern Sie sie nicht auf die zu verschlüsselnde Partition.

Nach Abschluss der Systemverschlüsselung müssen Sie bei einem Neustart zunächst das Passwort eingeben und Enter drücken. Haben Sie keine Angabe bei „PIM“ gemacht, lassen Sie das Feld beim Neustart leer und drücken ebenfalls Enter (siehe Abbildung im Kasten unten).

Vergrößern Die Software Veracrypt ist übrigens Donationware. Sie können und dürfen das Tool kostenlos nutzen. Die Entwickler freuen sich aber auch über eine Spende in beliebiger Höhe.

So nutzen Sie die Notfall-CD von Veracrypt

Sollte eine verschlüsselte Systempartition trotz richtigem Passwort nicht starten wollen, nutzen Sie die bootfähige Notfall-CD von Veracrypt. Sie kann Probleme mit dem Bootloader beheben. Sie hilft allerdings nicht, wenn Sie das Passwort vergessen haben. Wie Sie die CD nutzen, steht in der Anleitung, die Sie sich kurz vor der Verschlüsselung der Systempartition ausgedruckt haben. Kurz gesagt können Sie im Menü der Rettungs-CD „Repair Options“ mittels F8-Taste wählen und dann „Restore Veracrypt Bootloader“ mit „Y“ bestätigen, um die Aktion auszuführen. Die CD hält ein paar weitere Rettungswerkzeuge bereit, die in der Anleitung beschrieben sind.

Tipps zu den Veracrypt-Containern

1. Veracrypt-Laufwerk schnell trennen: Klicken Sie mit der rechten Maustaste auf das Veracrypt-Laufwerk im Windows-Explorer, um aus dem Kontextmenü den Trennen-Befehl auszuwählen.

2. Kennwort ändern: Sie können das Passwort eines Containers ändern, wenn er gerade nicht geöffnet ist. Wählen Sie den Container in Veracrypt über „Datei“ aus und klicken Sie dann auf „Volumes –› Volume-Passwort ändern“.

Vergrößern Wenn Sie einen eingebundenen Container per Klick mit der rechten Maustaste zu den Favoriten hinzufügen, kann Veracrypt diesen künftig automatisch entschlüsseln.

3. Schlüsseldatei verwenden: Wenn Sie einen Container erstellen, können Sie zusätzlich zum Passwort oder auch ersatzweise eine Schlüsseldatei wählen. Das kann jede beliebige Datei auf Ihrem PC sein, etwa eine MP3-Datei oder ein Foto. Zum Entschlüsseln des Containers wählen Sie dann diese Datei aus.

Wichtig: Sie dürfen diese Datei nicht verändern oder löschen. Sie ist Ihr Schlüssel zum Volume.

4. Container automatisch laden: Soll mit jedem Windows-Start auch ein Container entschlüsselt werden, müssen zwei Bedingungen erfüllt sein: Veracrypt muss zusammen mit Windows starten, und Sie müssen ein entschlüsseltes Volume zu den Favoriten in Veracrypt hinzufügen. Wie das genau geht, verrät dieser Beitrag . Feedback an PC-WELT

Quelle: https://www.pcwelt.de/ratgeber/VeraCrypt-TrueCrypt-Nachfolger-fuer-Vollverschluesselung-erklaert-Grundlagen-und-Praxis-9643083.html