

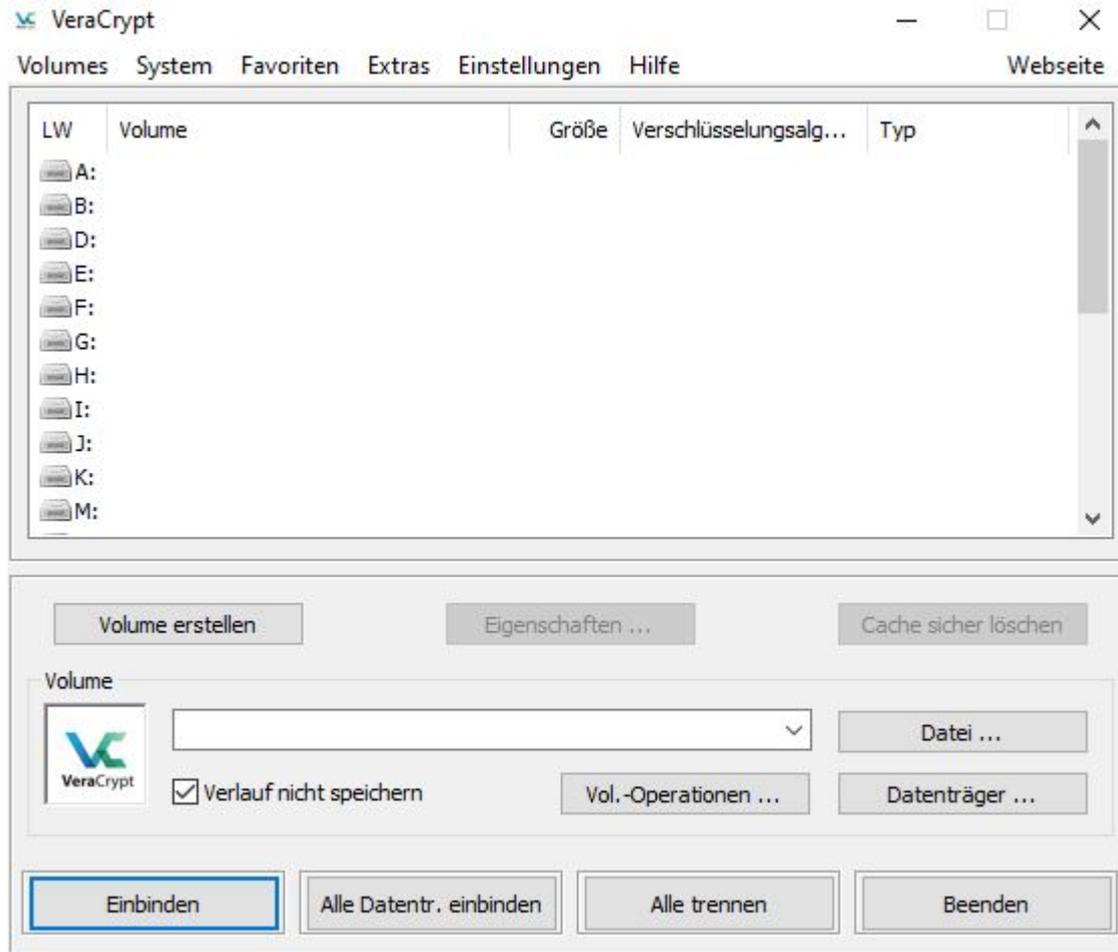
# Konfiguration VeraCrypt (Datenverschlüsselungstool) VHD Datei

Publiziert [it-support@fhnw.ch](mailto:it-support@fhnw.ch) allgemeine Anleitung Benutzerdokumentation

VeraCrypt, Datenverschlüsselungstool, VHD Datei

Folgende Schritte dienen zur Konfiguration einen VHD ( Virtual-Hard-Disk-Format ) Datei in VeraCrypt

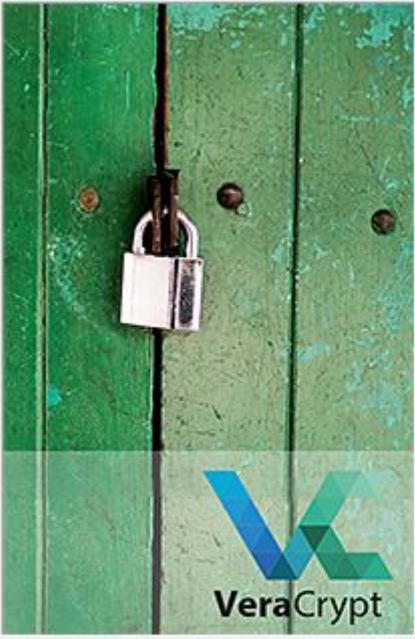
1. Starten von VeraCrypt und mit einem klick auf "Volume erstellen"



2. Es wird nun der Assistent zum Erstellen eines VeraCrypt-Volume gestartet.

**WICHTIG:** Im folgenden Schritt kann Ausgewählt werden, ob nur eine Container Datei oder eine Partition oder das System Laufwerk Verschlüsselt werden soll!

In unserem Fall entscheiden wir uns für eine Verschlüsselte Containerdatei



## VeraCrypt-Volumen erstellen

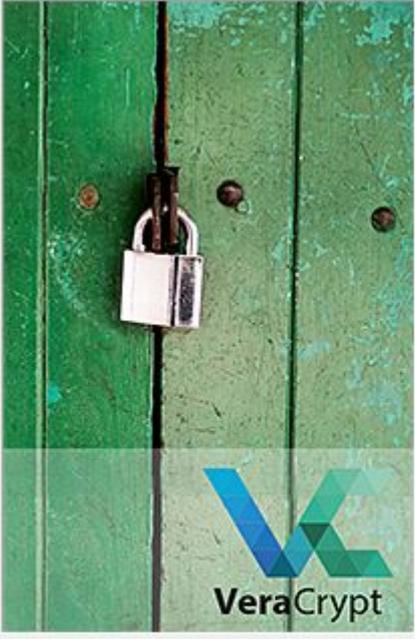
**Eine verschlüsselte Containerdatei erstellen**  
Erstellt ein verschlüsseltes virtuelles Laufwerk, welches als Datei gespeichert wird. Für Anfänger empfohlen.  
[Mehr Informationen](#)

**Eine Partition/ein Laufwerk verschlüsseln**  
Verschlüsselt eine Nicht-Systempartition auf internen oder externen Laufwerken (als normales oder verstecktes Volumen).

**Eine System-Partition bzw. ein System-Laufwerk verschlüsseln**  
Partition/Laufwerk verschlüsseln auf dem Windows installiert ist. Jeder, der Zugang zum System erlangen möchte, muss das korrekte Passwort bei jedem Start von Windows eingeben. Eine Alternative dazu ist das Erstellen eines versteckten Systems.  
[Mehr Informationen über die Systemverschlüsselung](#)

Hilfe < Zurück Weiter > Abbrechen

3. Auswahl eines Standard VeraCrypt-Volumes



## Volumen-Typ

**Standard VeraCrypt-Volumen**  
Diese Option zum Erstellen eines normalen VeraCrypt-Volumens wählen.

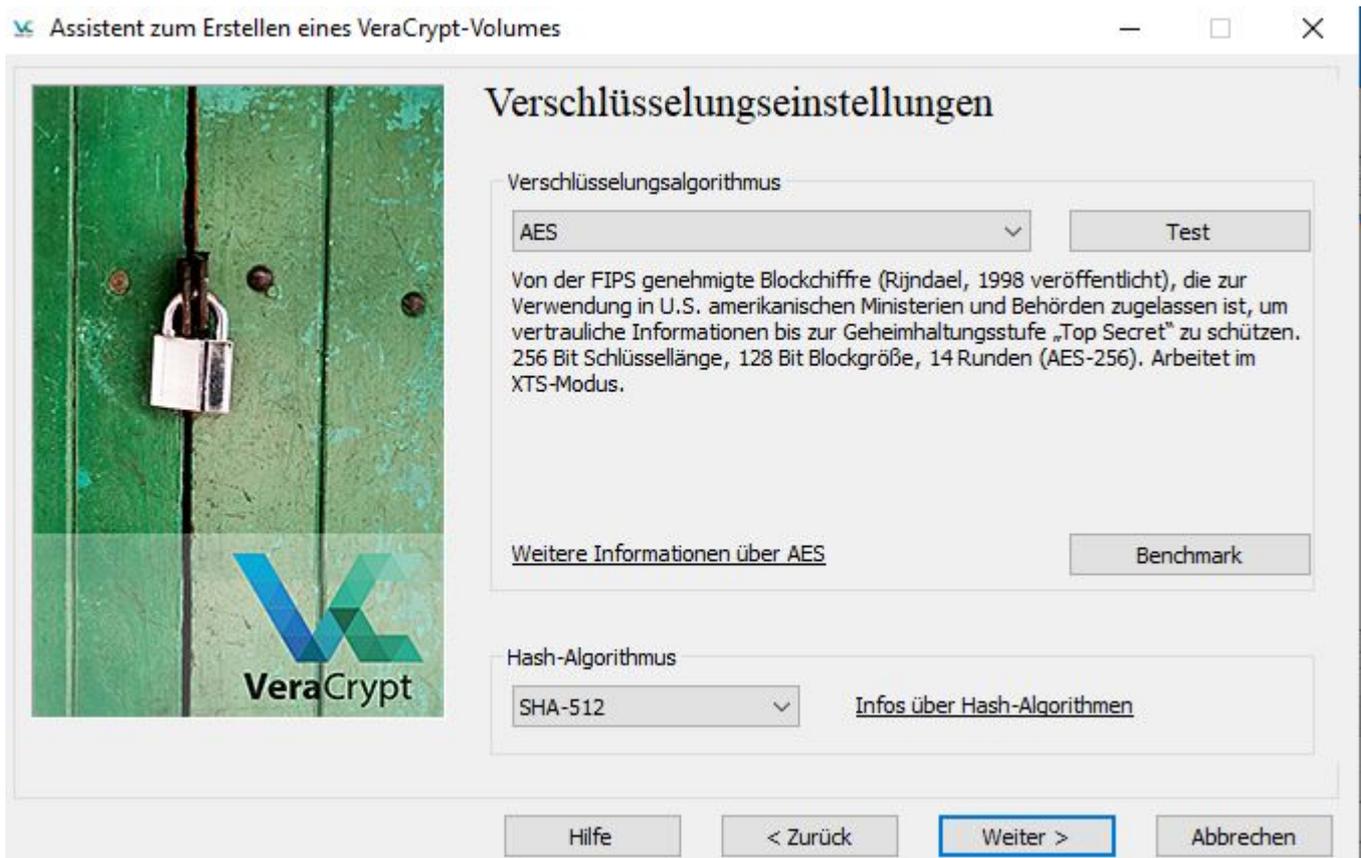
**Verstecktes VeraCrypt-Volumen**  
Es kann vorkommen, dass Sie von jemandem gezwungen werden, das Passwort für ein verschlüsseltes Volumen zu verraten. Es gibt viele Situationen, in denen Sie sich nicht weigern können, das Passwort herauszugeben (z.B. Erpressung). Mit Hilfe eines sogenannten versteckten Volumens müssen Sie in solchen Situationen das Passwort ihres (versteckten) Volumens nicht herausgeben.  
[Mehr Informationen über versteckte Volumens](#)

Hilfe < Zurück Weiter > Abbrechen

4. Auswahl des Speicherortes, wo die Containerdatei abgespeichert werden soll

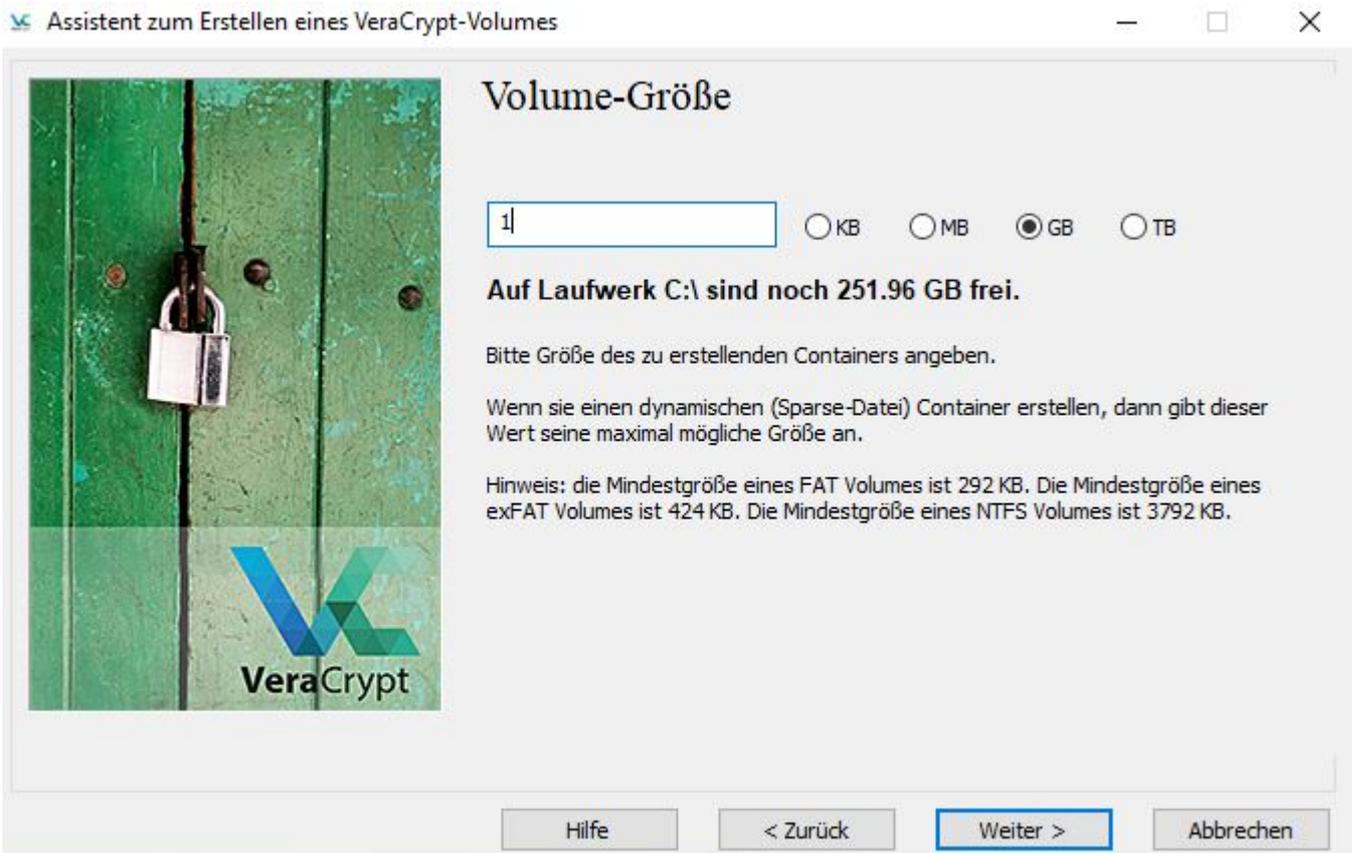


5. Standardwerte so belassen



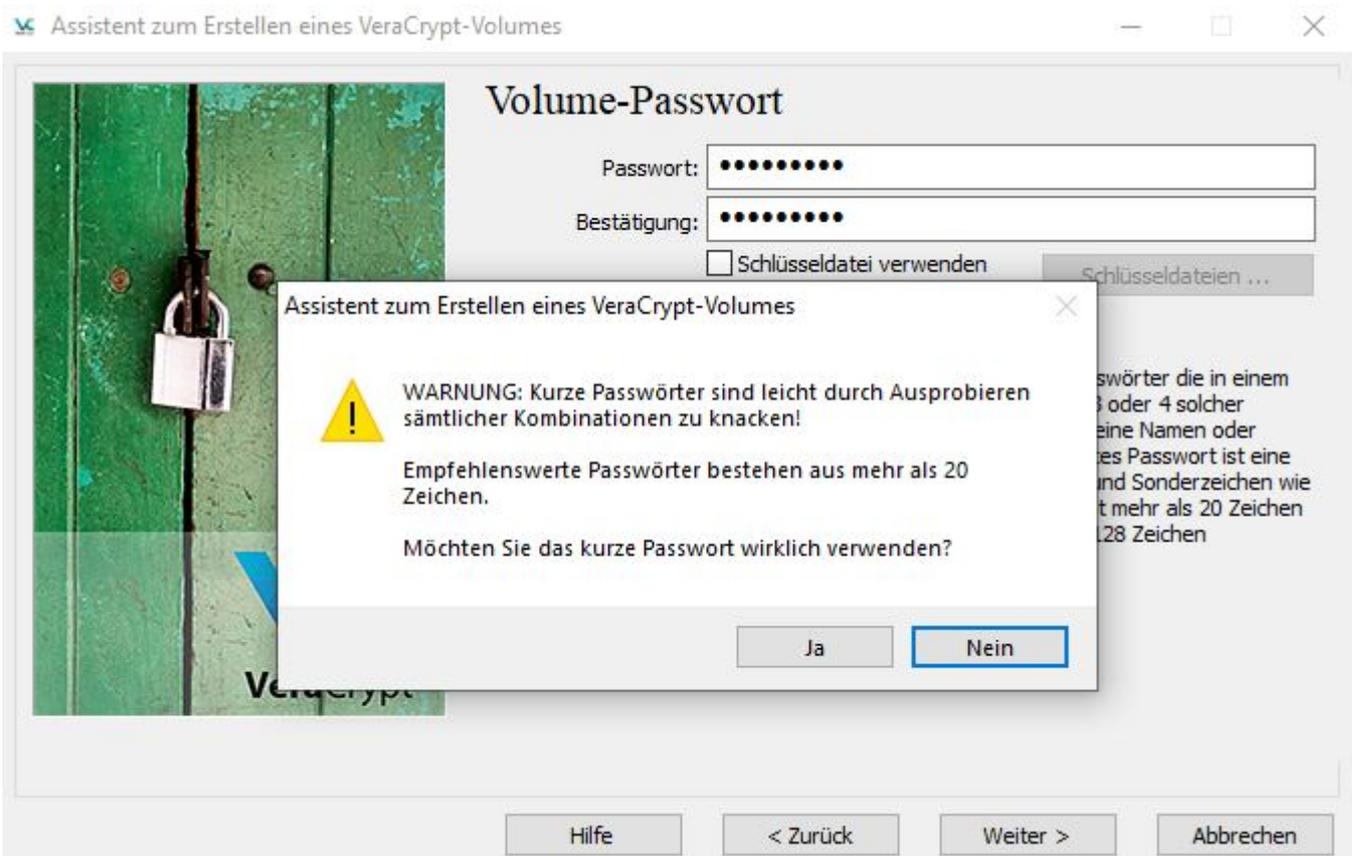
6. Auswahl der Volume Größe

**WICHTIG:** Die Maximalgröße kann NICHT Größer sein, als der Freie Bereich auf Laufwerk C



#### 7. Vergabe eines Passwortes

WICHTIG: Bei Verlust des Passwortes, kann auf die Daten innerhalb des Verschlüsselnden Laufwerks nicht mehr zugegriffen werden! Deshalb sollte das Passwort nicht Verloren gehen!



8. Im folgenden Fenster ist es Wichtig, den Mauszeiger im Fenster hin und her zu bewegen für ca. 30sec. Anschliessend mit einem Klick auf "Formatieren" bestätigen

## Volume-Format

Optionen

Dateisystem **FAT** Cluster **Vorgabe**  Schnell-Formatierung  
 Dynamisch

Zufallswerte: /\*,,+,+.,+./\*+...--/\*,.. /---.++/\*,-...   
 Kopfdatenschlüssel: \*\*\*\*\*  
 Hauptschlüssel: \*\*\*\*\*

Fertig  Geschw.  Rest

WICHTIG: Den Mauszeiger in diesem Fenster zufällig hin- und herbewegen. Je länger (min. 30 Sek.) Sie die Maus bewegen desto besser. Dies trägt zu einer verbesserten Verschlüsselung bei. Klicken Sie auf „Formatieren“, um mit der Erstellung fortzufahren.

Durch Mausbewegungen gesammelte Entropie

9. In den folgenden Fenster muss nur noch bestätigt werden und das VeraCrypt Volume ist erstellt

## Volume-Format

Optionen

Dateisystem **FAT** Cluster **Vorgabe**  Schnell-Formatierung  
 Dynamisch

Zufallswerte: \*.,/,+,+,-,\*/-/+\*\*\*,+\*-.,++\*-, -, , , ...   
 Kopfdatenschlüssel: \*\*\*\*\*  
 Hauptschlüssel: \*\*\*\*\*

Fertig  Rest

- und herbewegen. Je länger trägt zu einer verbesserten mit der Erstellung

Durch Mausbewegungen gesammelte Entropie

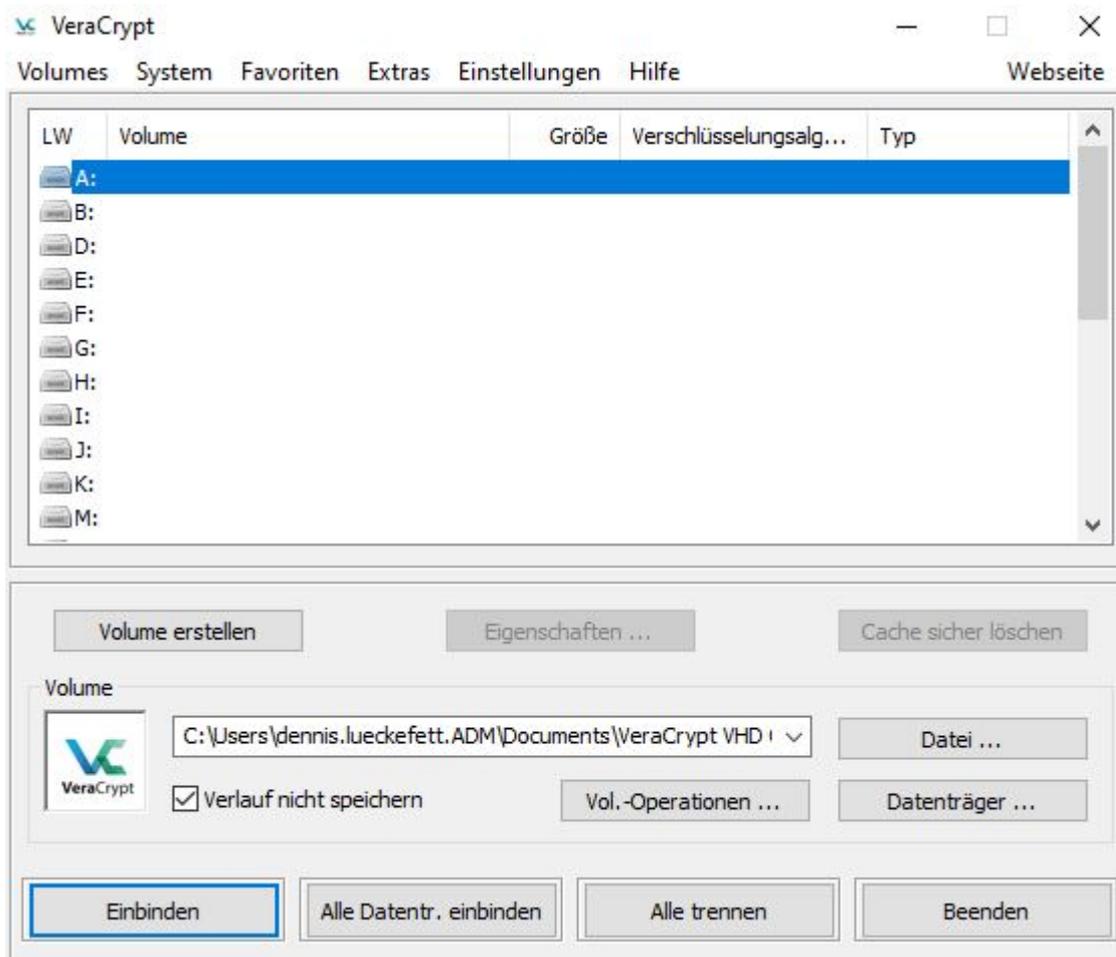
Assistent zum Erstellen eines VeraCrypt-Volumes

 Das VeraCrypt-Volume wurde erfolgreich erstellt.



Die weiteren Schritte zeigen, wie Sie das Verschlüsselte Volumen Hinzufügen und wieder Entfernen können!

10. Mit Klick auf Datei, muss das zuvor erstellte Volumen (siehe Punkt 4) ausgewählt werden. Anschliessend kann bei Bedarf ein Laufwerksbuchstabe (A, B, C usw.) ausgewählt werden. Und danach einfach mit Klick auf "Einbinden" bestätigen



11. Nun erfolgt die Passwortabfrage. Hier ist das Passwort vonnöten, was im Punkt 7 vergeben wurde

Passwort für C:\Users\dennis.lueckefett.ADM\Documents\VeraCrypt VHD Ordner eingeben

Passwort:

PKCS-5 PRF:   TrueCrypt-Modus

PIM verwenden

Passwort und Schlüsseldatei im Cache halten

Passwort anzeigen

Schlüsseldatei verwenden

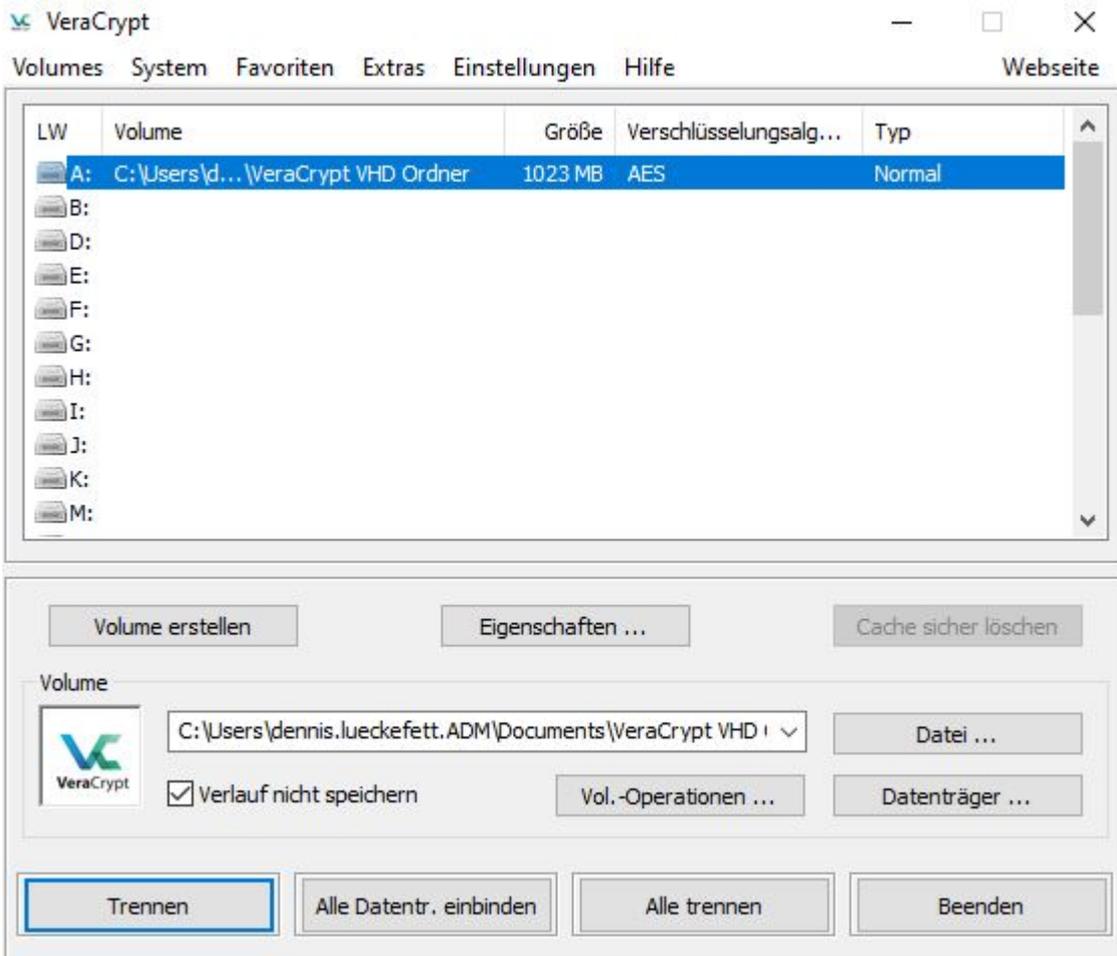
12. Anschließend steht das VeraCrypt Volume im Windows Explorer zur Verfügung. Das Ver- und entschlüsseln der Daten im Volume erfolgt Automaisiert.

The screenshot shows a Windows Explorer window titled "Dieser PC" with a sidebar on the left and a main pane on the right. The sidebar lists various locations like Desktop, Downloads, and Documents. The main pane shows a tree view of folders and drives. A VeraCrypt dialog box is open in the foreground, displaying a table of volumes. The table has columns for 'LW', 'Volume', 'Größe', 'Verschlüsselungsalg...', and 'Typ'. The first row shows 'A: C:\Users\d... \VeraCrypt VHD Ordner' with a size of 1023 MB and AES encryption. Below the table, the 'H:' drive is selected. At the bottom of the dialog, there are buttons for 'Einbinden', 'Alle Datentr. einbinden', 'Alle trennen', and 'Beenden'. The 'Alle trennen' button is highlighted, indicating the volume is being removed.

LW	Volume	Größe	Verschlüsselungsalg...	Typ
A:	C:\Users\d... \VeraCrypt VHD Ordner	1023 MB	AES	Normal

13. Das Verschlüsselte VeraCrypt Volume wird Entfernt, wenn das Volume markiert und mit einem Klick auf "Alle trennen" bestätigt wird.

WICHTIG: Ein bearbeiten der Daten im Verschlüsselten VeraCrypt Volume ist dann nicht mehr möglich!



## Verwandte Artikel

- [Windows 10 Konfiguration Microsoft BitLocker \(Laufwerksverschlüsselungstool\) VHD Datei](#)

publiziert: 29. April 2020 11:34 Service: S0006 - Fileserver