Einführung in VeraCrypt und Keepass

Peter Willadt

2018-09-17

VeraCrypt dient zur Datenverschlüsselung, KeePass ist ein Passwort-Manager. Beide Programme sind kostenlos, Open Source und plattformübergreifend erhältlich. Veracrypt ist im Schulnetz verfügbar.

1 Veracrypt

1.1 Erste Schritte

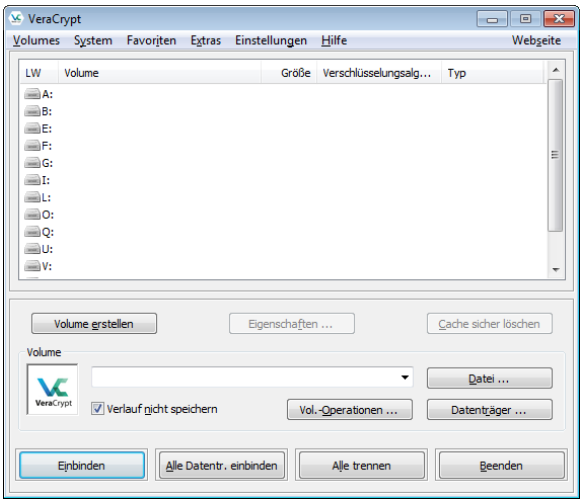
VeraCrypt bietet sichere Verschlüsselung. Das Programm ist Open Source, dadurch lassen sich Hintertüren nicht unbemerkt einbauen. Es wurde von unabhängiger Seite auditiert. In diesem Zusammenhang wurden Fehler beseitigt.

VeraCrypt verschlüsselt keine einzelnen Dateien, es stellt verschlüsselte Laufwerke bereit. Es können physikalische Laufwerke oder sogenannte Container (virtuelle Laufwerke) verwendet werden. Dateien werden beim Speichern in diesen Laufwerken automatisch verschlüsselt und beim Öffnen automatisch entschlüsselt. VeraCrypt ermöglicht auch eine Komplettverschlüsselung eines Gerätes. Das it besonders bei tragbaren Geräten (Notebook) sinnvoll.

VeraCrypt wird wie jedes andere Programm installiert, deswegen gehe ich hier nicht auf die Installation ein. Eine portable Installation ist (eingeschränkt) möglich, aber nicht sinnvoll, da VeraCrypt tief ins System eingreifen muss.

1.2 Das Leben erleichtern

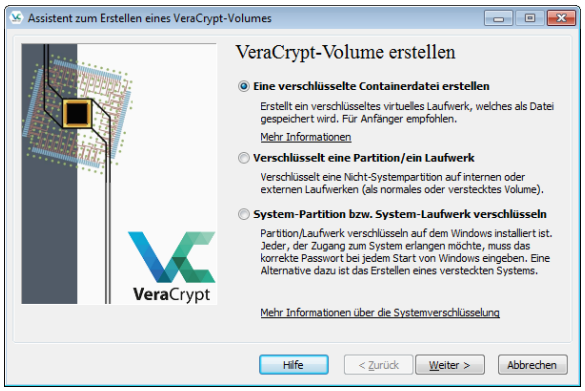
Zuerst *Settings/Select Language* und *Deutsch* aussuchen. Zuhause machen Sie das einmal, im Schulnetz dürfen Sie das jedes Mal machen. Anschließend zeigt sich VeraCrypt wie nebenstehend abgebildet.



Laufwerksbuchstaben, die bereits vergeben sind, werden nicht angezeigt.

1.3 Volumen erstellen

So erstellen Sie eine Containerdatei: Wählen Sie *Volume erstellen* und dann *Eine verschlüsselte Containerdatei erstellen*.

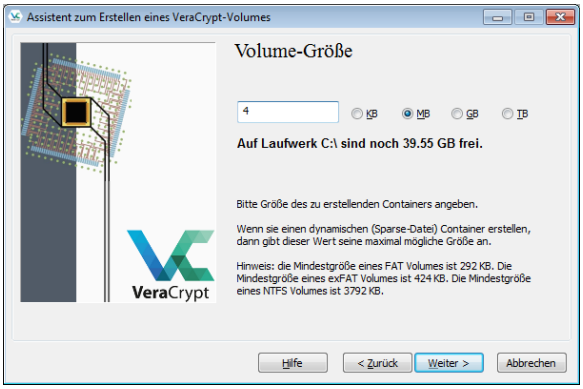


Wählen Sie dann *Standard VeraCrypt-Volume*.

Erzeugen Sie im nächsten Schritt eine neue Datei. Wichtig: Wenn Sie eine bestehende Datei auswählen, wird diese zerstört! Seien Sie besonders sorgfältig, wenn Sie ganze Datenträger verschlüsseln, um nicht versehentlich Ihre Festplatte unbenutzbar zu machen.

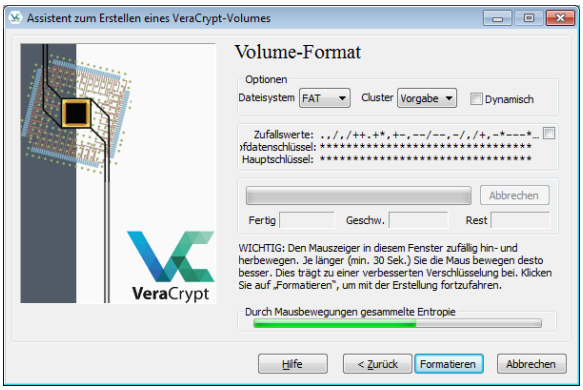
Die Verschlüsselungseinstellungen können Sie wie vorgegeben übernehmen.

Wählen Sie eine sinnvolle Größe für die Containerdatei. Falls Sie schon vorab wissen, was Sie hineinpacken, ergibt sich daraus die Mindestgröße. Die Höchstgröße orientiert sich daran, was Sie damit vorhaben. Für Emails sollten Sie nicht über 4 Megabyte gehen. Container werden beim Zippen nicht kleiner.



Wählen Sie ein ausreichend langes Passwort, das in keinem Wörterbuch vorkommt und auch nicht aus Ihren persönlichen Daten abgeleitet werden kann. Statt eines Passwortes können Sie auch einen ganzen Satz verwenden, zum Beispiel die erste Strophe Ihres Lieblingsgedichtes. Wichtig: Das Passwort dürfen Sie nicht verlieren oder vergessen, die Daten sind sonst unwiederbringlich verloren! Die Daten zusätzlich unverschlüsselt aufzubewahren, widerspricht dem Sinn der Verschlüsselung, Sie können dies jedoch durch gesicherte Aufbewahrung (USB-Stick im Tresor) teilweise ausgleichen.

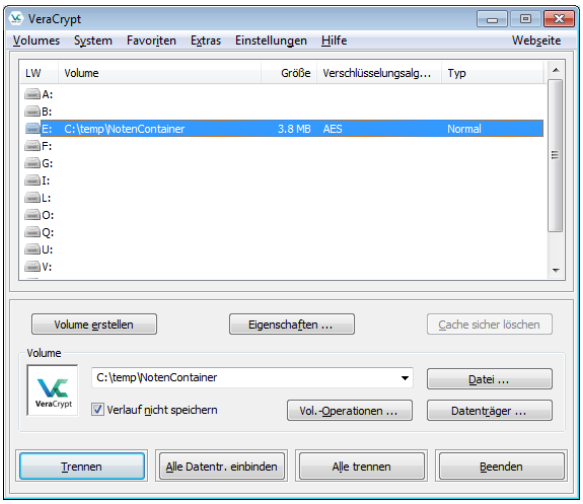
Im nächsten Schritt müssen Sie zur Erzeugung von Zufälligkeit mit dem Mauszeiger herumzappeln, bis der anfangs rote Balken grün wird. Im Normalfall ist das Dateisystem FAT in Ordnung. Dann klicken Sie auf Formatieren und wenn die Meldung *Volume wurde erstellt* erscheint, klicken Sie auf Beenden. Sie sind jetzt wieder im VeraCrypt-Fenster.



Die Formatierung benötigt beträchtliche Zeit, bei einem USB-Stick mit 8 GB kann durchaus eine halbe Stunde vergehen.

Für das Format des Containers wählen Sie FAT, es sei denn, Sie haben Dateien mit mehr als 4 GB Größe zu verschlüsseln, dann muss es NTFS sein.

1.4 Volumen benutzen



Als nächstes suchen Sie sich einen Laufwerksbuchstaben aus, gehen auf *Datei* und wählen Ihren neu erstellten Container. Dann klicken Sie auf Einbinden. Geben Sie Ihr Passwort ein und der Container ist bereit.

Sie können jetzt mit beliebigen Programmen Daten in den Container bringen, zum Beispiel mit dem Explorer oder aus Ihrem Textprogramm heraus mit *Speichern unter*. Sie finden den Container als eigenes Laufwerk mit dem von Ihnen gewählten Laufwerksbuchstaben.

Der Container bleibt geöffnet, auch wenn Sie VeraCrypt beenden. Um ihn zu schließen, müssen Sie in VeraCrypt auf *Trennen* klicken. Dazu können Sie VeraCrypt erneut starten oder das Icon in der Taskleiste benutzen.

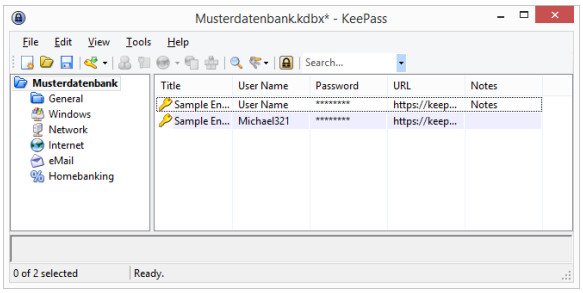
Falls Sie einen Stick komplett verschlüsselt haben, taucht er nach der Einbindung mit zwei Laufwerksbuchstaben in Ihrem Windows-Explorer auf. Eines der beiden Laufwerke ist dabei vollständig gefüllt und zu nichts zu gebrauchen, das andere ist der Container.

1.5 Volumen weitergeben

Wenn der Container in VeraCrypt getrennt wurde, können Sie die Containerdatei wie jede andere Datei kopieren, verschieben und so weiter. Bitte beachten Sie, dass Sie das Passwort über einen anderen Kanal als die Datei selbst weitergeben. Dieser andere Kanal sollte möglichst sicher sein.

2 KeePass

Passwort-Manager speichern Zugangsdaten zu Webseiten, aber auch Passwörter für lokale Software. Die beliebten Passwortspeicher von Browsern sind leider unsicher, Webdienste wie LastPass haben sich auch nicht mit Ruhm bekleckert.



KeePass ist eine systemübergreifende kostenlose Open-Source Passwort-Verwaltung. Alle Anmeldedaten werden in einer lokalen verschlüsselten Datenbank gespeichert. Falls Sie KeePass auf mehreren Geräten nutzen möchten, müssen Sie die Datenbank also am jeweiligen Gerät zugänglich machen. KeePass muss nicht installiert werden, eventuell wird aber das Dotnet-Framework benötigt.

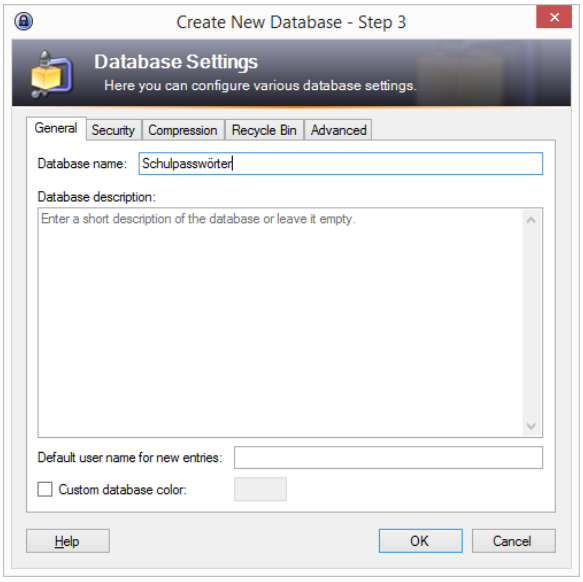
Für Android-Smartphones gibt es KeePass-kompatible Lösungen. Empfehlenswert ist KeePass2Android. Eine Beschreibung steht in c't Heft 8/2018, Seite 144 f.

2.1 KeePass benutzen

Beim ersten Programmstart suchen Sie eine Passwort-Datenbank aus oder legen eine an. In Zukunft versucht KeePass immer, die letzte Passwort-Datei zu öffnen, Sie werden dann direkt nach dem Passwort gefragt.

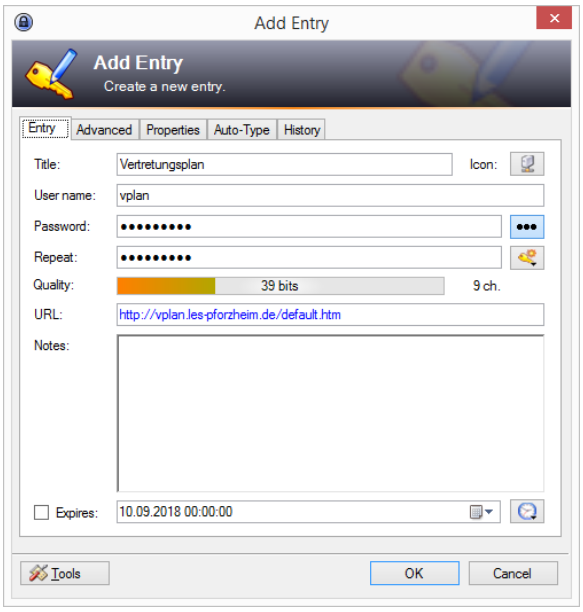
2.1.1 Datenbank anlegen

Klicken Sie auf *New Database*. Verzichten Sie auf *Expert Options* und wählen Sie ein sicheres Passwort, das Sie sich gut merken können. Sie können Ihre Passwort-Datenbank auf Wunsch zusätzlich für erhöhte Sicherheit mit einer Schlüsseldatei absichern. Beispielsweise kann die Passwortdatei auf Ihrem Account im Schulnetz liegen und die Schlüsseldatei auf einem USB-Stick.



Jetzt sind Sie bei den *Database Settings*. Sie brauchen nichts einzustellen, können aber der Datenbank einen Namen geben, falls Sie zum Beispiel eine private Datenbank und eine andere, die Sie mit Dritten teilen, haben. Wenn Sie ein Bankschließfach haben, drucken Sie sich ein *Emergency Sheet* und tragen Sie das Passwort dort ein. Anschließend ist die Datenbank geöffnet. Weisen Sie KeePass beim Schließen unbedingt an, Änderungen zu speichern. Sie können Ihre Einträge in den vorhandenen Ordnern unterbringen, Sie können auch weitere Ordner anlegen. Auch

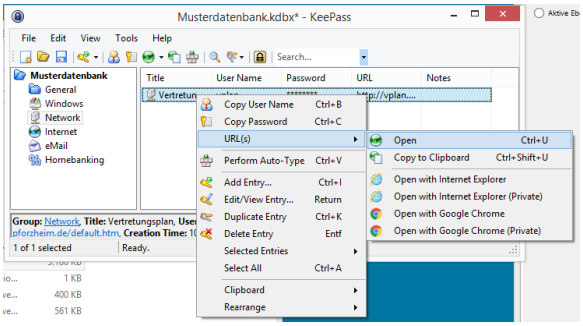
das Umziehen eines Eintrages von einem in einen anderen Ordner ist problemlos möglich.



Neue Einträge legen Sie durch Klick auf den Schraubenschlüssel an. Bei Webseiten hinterlegen Sie URL, Benutzername und Passwort. Für Eingaben, die nicht ins Schema passen (zum Beispiel die Office-Seriennummer) können Sie auch das Notes-Feld missbrauchen.

Auf Wunsch generiert KeePass Passwörter. Das ist sehr empfehlenswert, da diese einerseits vergleichsweise sicher sind und andererseits die Benutzung eines einzigen Passworts für mehrere Webseiten ein großes Sicherheitsrisiko darstellt. Falls Sie eigene Passwörter vergeben möchten: Inzwischen werden lange Passwörter empfohlen, die Maximallänge von Passwörtern ist jedoch leider bei vielen Anbietern begrenzt. Sonderzeichen sind keine Gewähr für gute Passwörter, werden aber von vielen Seiten eingefordert. Die Knackbarkeit eines Passworts können Sie an der Farbe des *Quality*-Balkens erkennen. Wo es darauf ankommt, sollten Sie in den grünen Bereich kommen. Bei `https://haveibeenpwned.com/Passwords` können Sie prüfen, ob Ihr Passwort bereits aus Hacks bekannt ist.

Nach dem Vornehmen von Änderungen gilt auch hier: Weisen Sie KeePass beim Schließen unbedingt an, Änderungen zu speichern.



Wenn Sie eine Webseite aufsuchen möchten, können Sie die URL per Rechtsklick öffnen, ebenfalls per Rechtsklick kopieren Sie die Benutzerdaten, die Sie dann mit STRG-V im Browser einfügen.