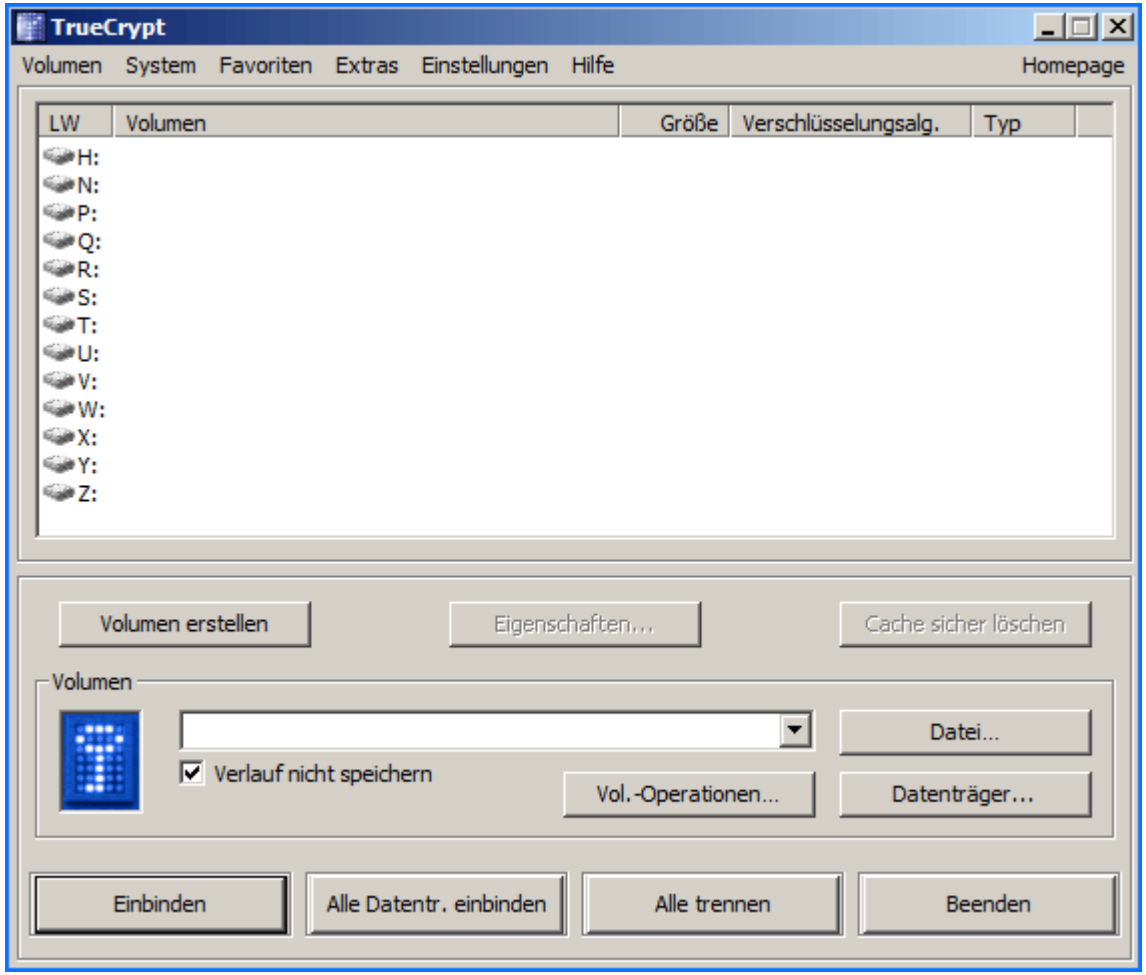
Anleitung

TrueCrypt 7.xx – PC-Verschlüsselung

Gefahr der Datenspionage

Unverschlüsselte Daten können von allen gelesen werden, die Zugriff auf Ihren PC haben. Das Ausspähen von Daten verletzt die Privatsphäre und die ökonomischen Interessen von Privaten und Firmen.



Schutz durch Verschlüsselung

Die Technik der Kryptographie schützt wirksam vor unbefugtem Zugriff auf Ihren PC und Ihre vertraulichen Daten.

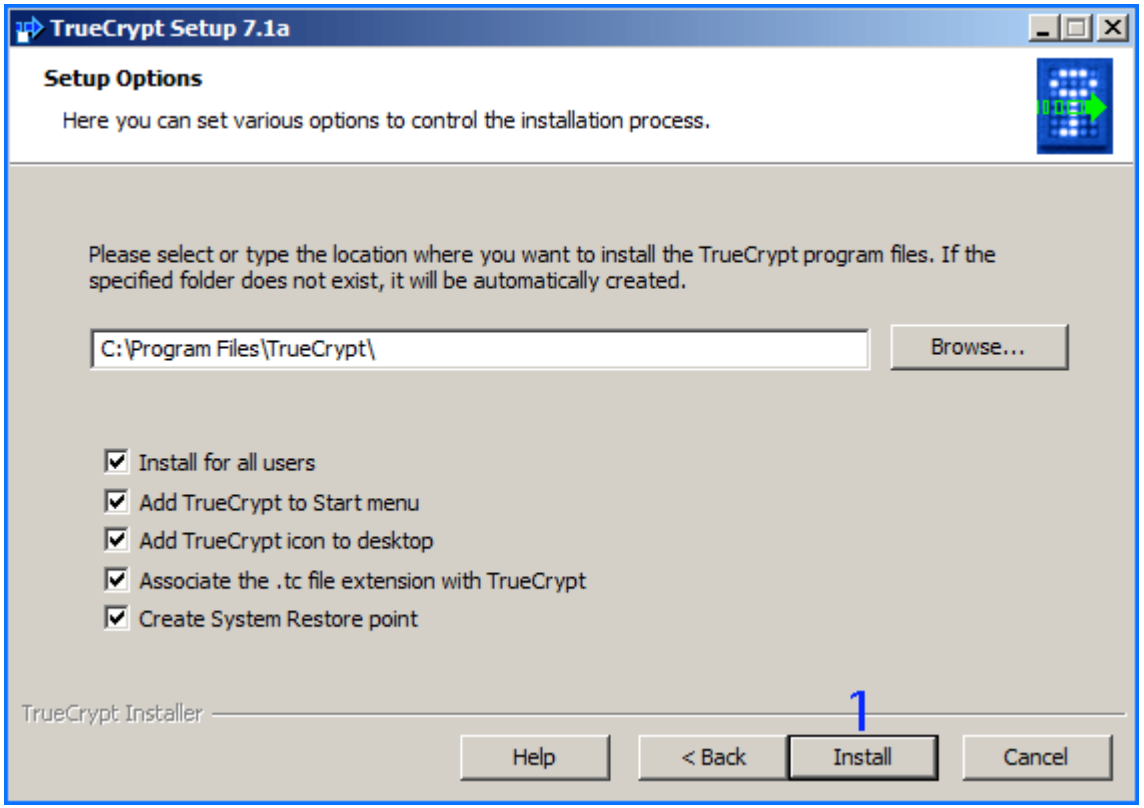
- Unternehmer können mit Hilfe der Verschlüsselung Firmendaten, Kunden- und Kontodaten sowie die marktreife Erfindung vor neugierigen Blicken der Mitbewerber schützen.
- Muss Ihr PC oder Notebook plötzlich repariert werden und Sie können die Daten nicht auf eine externe Festplatte kopieren, schützt der Datentresor vor der Neugierde des IT-Experten.
- In einem unbeobachteten Moment kann Ihr Notebook in einer Bar, auf einer Messe oder im Bahnhof den Besitzer wechseln. Ist die Festplatte verschlüsselt, hat der Dieb zumindest auf Ihre vertraulichen Daten keinen Zugriff.
- Schließlich ist die Verschlüsselung ein technisches Schutzschild des Grundrechts auf „informationelle Selbstbestimmung“. Für investigative Journalisten ist Kryptographie zum effektiven Schutz der Informanten geradezu ein Muss.

Abhilfe mit TrueCrypt

TrueCrypt ist ein Open-Source-Programm, mit dem Sie Datencontainer, komplette Festplatten sowie ganze Betriebssysteme verschlüsseln und verstecken können. Die Existenz des zweiten, versteckten Betriebssystems ist nicht nachweisbar.

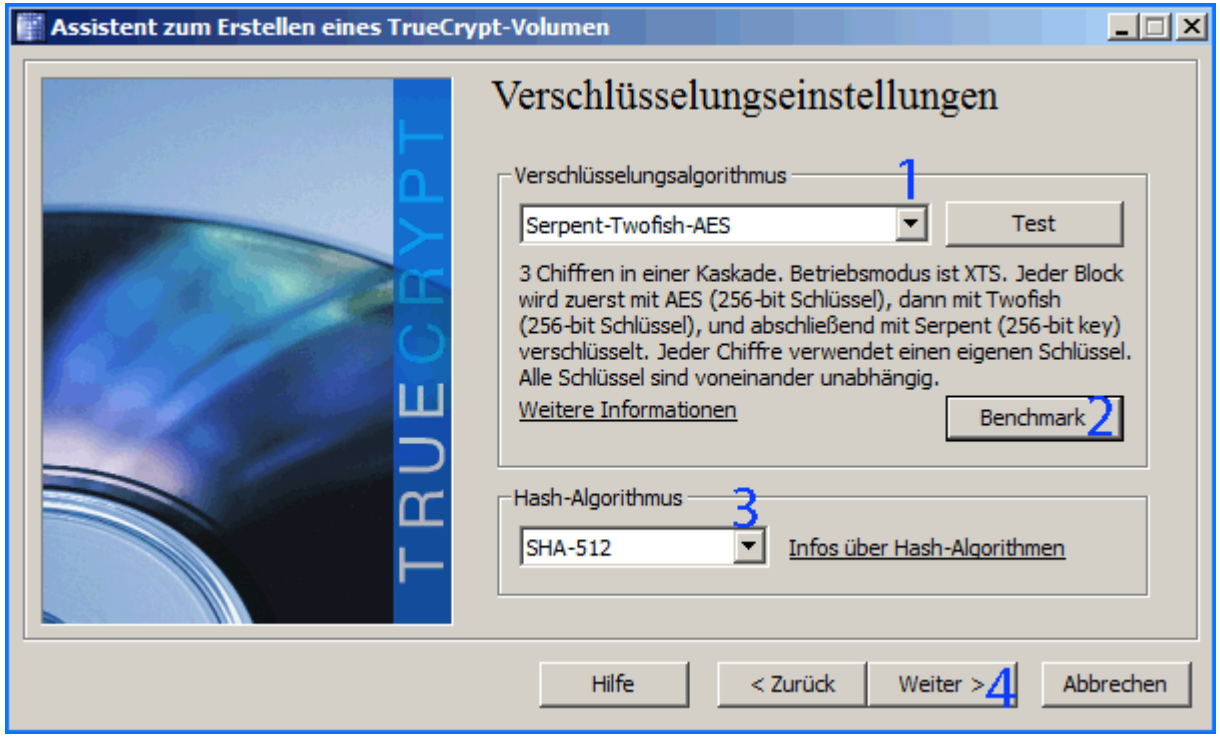
TrueCrypt downloaden

- Rufen Sie die Homepage von Truecrypt auf www.truecrypt.org auf. Unter dem Menüpunkt **Downloads** laden Sie die **Latest Stable Version** für Windows/Mac oder Linux herunter. Speichern Sie die Datei in Ihr Downloadverzeichnis.
- Laden Sie auch das deutsche Sprachpaket herunter. Dieses finden Sie über die Links **Source code, language packs, past versions, public key** und **Language packs.**



TrueCrypt installieren

- Öffnen Sie Ihr Downloadverzeichnis und starten Sie das Setup mit einem Doppelklick auf die exe-Datei **TrueCrypt Setup 7.xx.** Zunächst öffnet sich das Lizenzfenster. Setzen Sie ein Häkchen vor **I accept the license therms** und bestätigen mit **Next >.** Belassen Sie im nächsten Fenster die Auswahl **Install** und drücken Sie auf **Next >.** Belassen Sie die Vorgaben in der nächsten Dialogbox und klicken Sie auf **Install (1).** Kurz darauf erscheint ein Info-Fenster über die erfolgreiche Installation; klicken Sie auf **Ok.** Schließen Sie das Setup-Fenster mit einem Klick auf **Finish.** Starten Sie zum Abschluss Ihren PC neu.
- Installieren Sie noch das deutsche Sprachpaket. Kopieren Sie den Inhalt des entpackten ZIP-Archivs in den TrueCrypt-Programmordner (Windows 7: C:\Programme\TrueCrypt). Starten Sie nun TrueCrypt und ändern Sie die Programmsprache über **Settings/Language…**



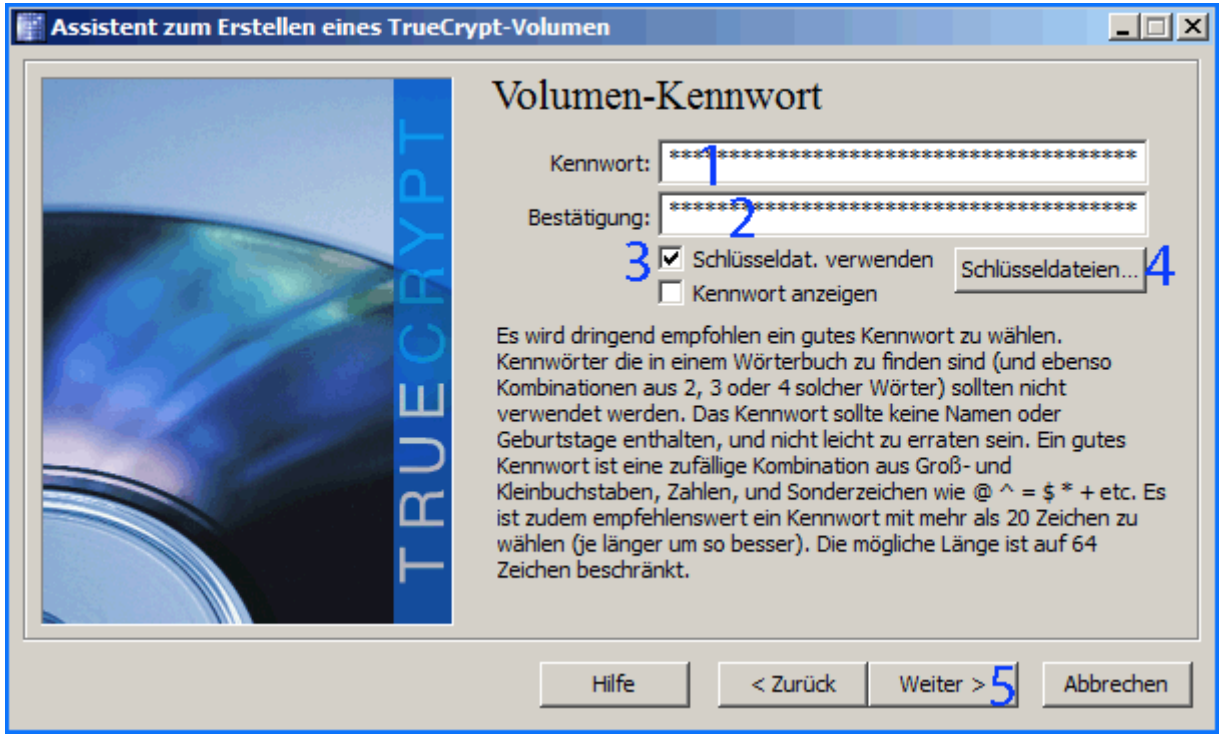
Verschlüsselten Container erstellen

Mit TrueCrypt können Sie verschlüsselte Laufwerke in Containerdateien erstellen, die gegen Passwort-Eingabe in den Windows-Verzeichnisbaum eingebunden werden.

- Starten Sie TrueCrypt, klicken Sie auf **Volume erstellen** und es öffnet sich der Assistent zum Erstellen eines TrueCrypt-Volumes.
- Belassen Sie die Option **Eine verschlüsselte Containerdatei erstellen** und klicken Sie zwei Mal auf **Weiter >.**
- Legen Sie als Nächstes den Dateinamen und den Speicherort für den Datencontainer fest. Klicken Sie hierzu auf **Datei…,** navigieren Sie dann zur Partition, wo der Container erstellt werden soll und geben Sie einen Dateinamen in das Feld Dateiname ein. Bestätigen Sie mit **Speichern** und klicken Sie auf **Weiter >.**
- Die Voreinstellungen zu den Verschlüsselungseinstellungen können unverändert bleiben. Mit **Weiter >** **(4)** geht's zur nächsten Dialogbox.

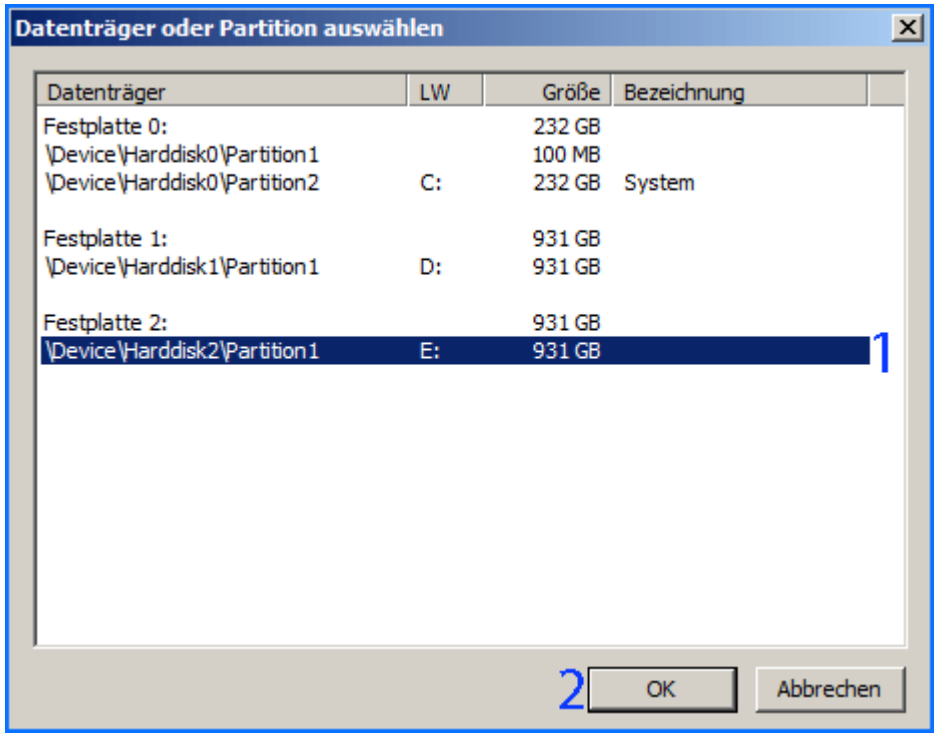
Hinweis

Klicken Sie auf den **Drop-Down-Pfeil** **(1)**, öffnet sich ein Auswahlfenster mit den drei Verschlüsselungsalgorithmen AES, Serpent und Twofish sowie Kombinationen daraus. Jeder Verschlüsselungsalgorithmus gilt als sicher. Bei einer kaskadierten Verschlüsselung bleiben die Daten auch dann vor unbefugten Zugirfen sicher, wenn einer der Algoritmen gebrochen werden sollte. Über die Schaltfläche **Benchmark** **(2)** können Sie einen Benchmark-Test für die einzelnen Verschlüsselungsalgorithmen durchführen. Weiters stehen die drei Hash-Algorithmen RIPEMD-160, SHA-512 und Whirlpool zur Auswahl **(3).** Wählen Sie Whirlpool oder SHA-512, weil diese einen 512 Bit langen Hash erzeugen und RIPEMD-160 „nur" einen 160 Bit langen.



- Jetzt ist die gewünschte Größe des Containers an der Reihe. Berücksichtigen Sie, dass eine Volume-Größe von 700 MB noch auf eine CD sowie 4.300 MB noch auf eine DVD passen. Sie können auch 1.000.000 MB eintippen, sofern Sie diese Größe benötigen. Mit **Weiter >** geht's zum nächsten Arbeitsschritt.
- Geben Sie Ihrem Datencontainer ein sicheres Passwort (Workshop: KeePass_Passwortmanager) **(1, 2).** Sie können auch eine Schlüsseldatei oder eine Kombination aus Passwort und Schlüsseldatei als Volume-Kennwort **(3)** wählen. Klicken Sie auf **Schlüsseldateien… (4),** dann öffnet sich das Schlüsseldateien-Fenster. Als Schlüsseldatei können Sie irgendeine Ihrer Dateien auswählen, eine eigene Schlüsseldatei erstellen oder einen Security Token bzw. eine Smart Card verwenden. Bestätigen Sie mit **Weiter > (5).**

- Als Nächstes legen Sie das Dateisystem des Containers fest und formatieren den Container. Für die Formatierung verwendet TrueCrypt einen zufälligen Schlüssel, der sich aus den Bewegungen der Maus ergibt. Bewegen Sie den Mauszeiger für ca. 30 Sekunden und klicken Sie dann auf **Formatieren.**
- Ist die Formatierung abgeschlossen, erscheint ein Bestätigungsfenster. Schließen Sie dieses mit **OK** und beenden Sie den Assistenten mit einem Klick auf **Beenden.** Ihr erster Datencontainer ist nun einsatzbereit.



Verschlüsselte Festplatte anlegen

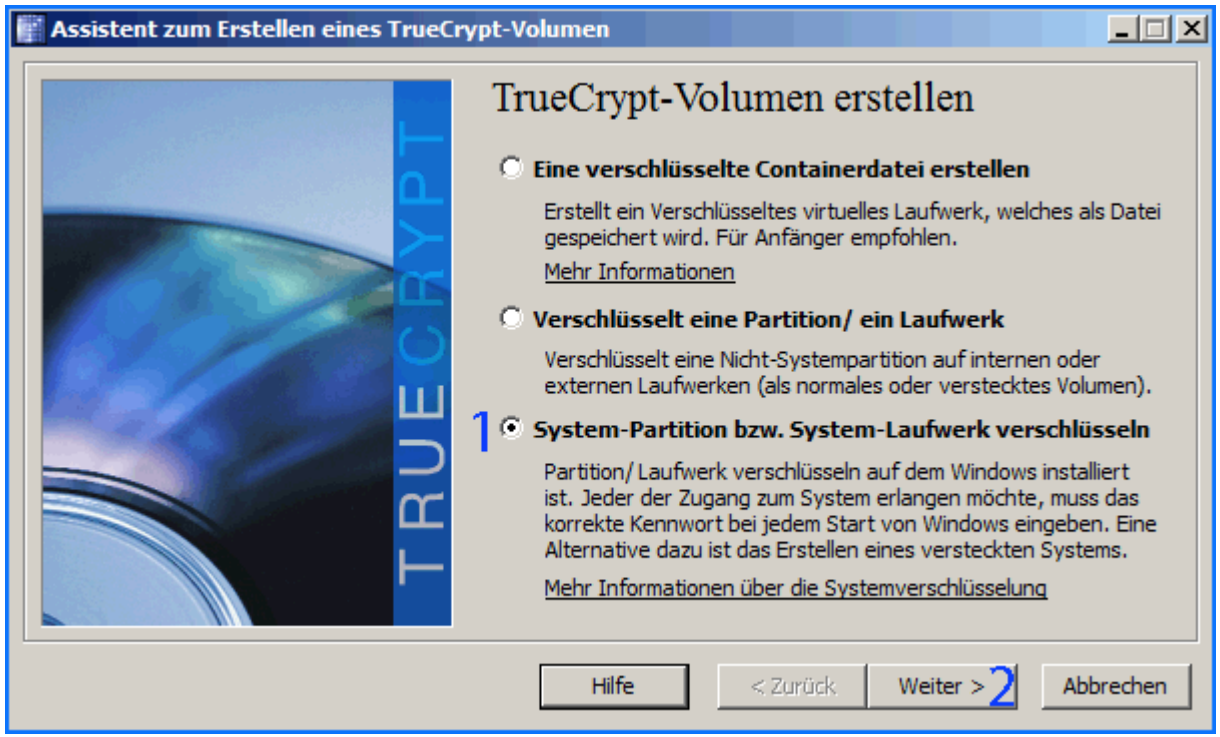
Mit TrueCrypt können Sie auch die gesamte Festplatte bzw. nur eine Partition verschlüsseln. Bevor Sie das Vorhaben angehen, sollten Sie die Festplatte/Partition mit einem Lösch-Tool säubern. So ist es Angreifern (fast) nicht möglich, die unverschlüsselten Daten mit speziellen Verfahren im Nachhinein auszulesen und zu rekonstruieren (vgl. Workshop: Eraser_Daten sicher löschen).

- Starten Sie TrueCrypt, drücken Sie auf **Volume erstellen** und wählen Sie die Option **Verschlüsselt eine Partition / ein Laufwerk.** Klicken Sie zwei Mal auf **Weiter >.**
- Wählen Sie nun den Datenträger aus. Klicken Sie hierzu auf **Datenträger…,** markieren Sie im Auswahlfenster den gewünschten **Datenträger (1),** bestätigen Sie mit **OK (2)** und drücken Sie im nächsten Fenster auf **Weiter >.**
- Soll die Partition verschlüsselt werden, ohne dass dabei die Daten verloren gehen, dann entscheiden Sie sich für die Option **Partition ‚in-place' verschlüsseln.** Belassen Sie die Option **Verschlüsseltes Volume erstellen und es formatieren,** dann gehen alle vorhanden Daten der Partition verloren.

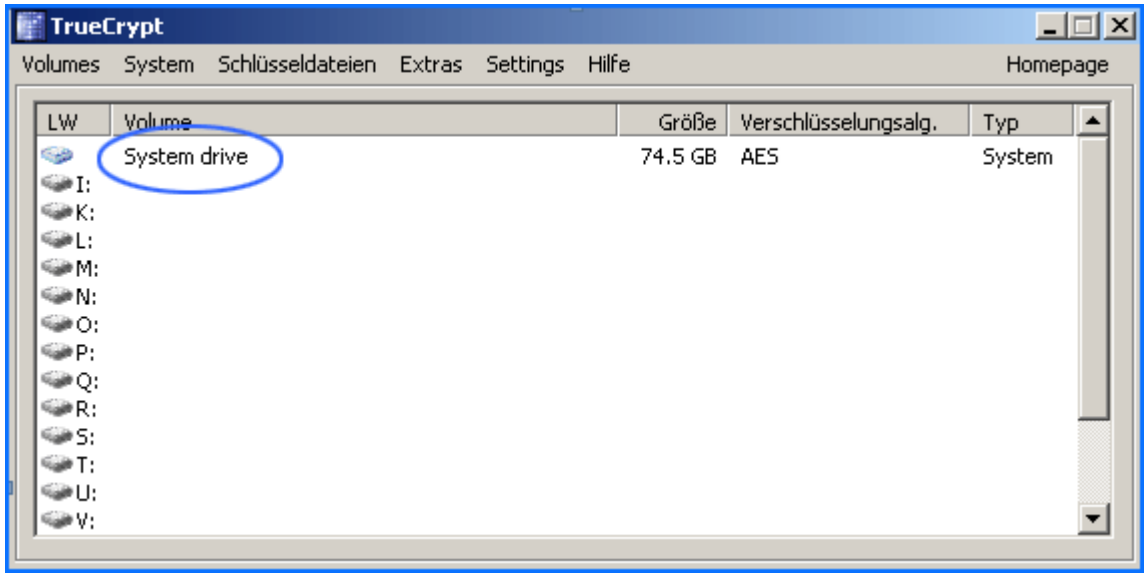
- Mit **Weiter >** gelangen Sie zu den Verschlüsselungseinstellungen, zur Bestätigung der Größe des Datenträgers, zur Kennworteingabe sowie zur Formatierung des Datenträgers. Sind Ihre Daten größer als 4 GB (z. B. Videodateien), dann wählen Sie das NTFS-Format. Starten Sie die Formatierung mit einem Klick auf **Formatieren.** Es erscheint ein Warnhinweis; klicken Sie auf **Ja** und bestätigen Sie zwei Mal mit **OK.** Das erstellte Volume ist nun betriebsbereit. Verlassen Sie den Assistenten mit einem Klick auf **Beenden.**

Betriebssystem verschlüsseln

Die Login-Daten des Windows Accounts können mit einer Live-CD wie Ophcrack einfach ausspioniert werden. TrueCrypt schafft Abhilfe, das Tool verschlüsselt auch die gesamte Windows-Systempartition. Bevor Sie jedoch daran gehen, Ihr Windows zu verschlüsseln, sollten Sie eine komplette Image-Sicherung des Systems vornehmen. Geht etwas schief, können Sie die Image-Sicherung einfach auf die C-Partition zurückspielen.



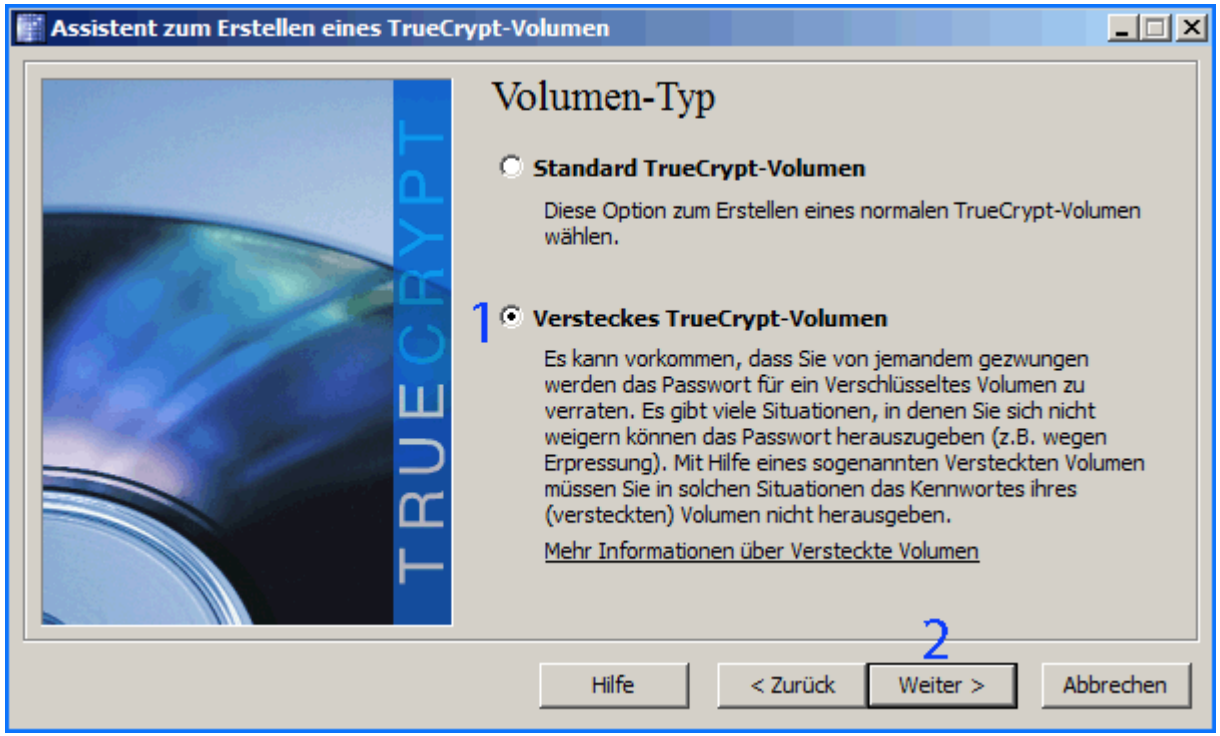
- Klicken Sie im Hauptfenster auf **Volumen erstellen** und es startet ein Assistent, der Ihnen bei der Verschlüsselung der Systempartition zur Seite steht.
- Wählen Sie in der nächsten Dialogbox **System-Partition-Laufwerk verschlüsseln…** (1) und bestätigen Sie mit **Weiter >.** Belassen Sie die Option **Normal** und klicken Sie auf **Weiter >** (2)**.**
- Entscheiden Sie nun, ob das gesamte Laufwerk oder nur die Windows-Partition verschlüsselt werden soll. Klicken Sie auf **Weiter >,** wählen Sie in der nächsten Dialogbox (im Zweifel) die Option **Nein** und gehen zum nächsten Schritt mit **Weiter >.** Haben Sie nur ein Windows installiert, wählen Sie **Ein Betriebssystem,** andernfalls **Mehrere Betriebssysteme.** Klicken Sie erneut auf **Weiter >.**
- Belassen Sie die Voreinstellungen der Verschlüsselungseinstellungen wie sie sind und gehen Sie mit **Weiter >** zur Eingabe des Kennwortes. Wählen Sie ein sicheres Kennwort und bestätigen Sie drei Mal mit **Weiter >** (Workshop: KeePass_Passwortmanager).



- Nun fordert Sie der Assistent auf, eine Rettungs-CD zu erstellen und macht nur weiter, wenn Sie das erledigt haben. Sollte die Systempartition beschädigt sein, können Sie mit der bootfähigen Notfall-CD den TrueCrypt-Bootloader und die Schlüsseldaten neu auf die Festplatte schreiben und im Notfall auch die gesamte Festplatte wieder entschlüsseln. Klicken Sie also auf **Weiter >.** TrueCrypt legt standardmäßig die Datei „TrueCrypt Rescue Disk.iso“ im Verzeichnis „Eigene Dateien“ ab. Brennen Sie die Image-Datei, legen Sie die CD in Ihr CD-/DVD-Laufwerk ein und klicken Sie dann auf **Weiter >.** TrueCrypt überprüft, ob die Image-Datei erfolgreich gebrannt wurde. Ist dies der Fall, erscheint eine Erfolgsmeldung. Bestätigen Sie mit **Weiter >,** entfernen Sie die CD und verwahren Sie diese an einem sicheren Ort. Am besten ist, Sie erstellen noch ein Backup von der Rettungs-CD.

- Im nächsten Arbeitsschritt geben Sie die Methode zur Datenlöschung an. Wählen Sie über den **Drop-Down-Pfeil** zumindest die „3-pass“-Methode, so dass Angreifer die unverschlüsselten Systemdaten nicht so ohne weiteres mit speziellen Verfahren auslesen und rekonstruieren können. Klicken Sie auf **Weiter >,** im Info-Fenster auf **Ja** und noch einmal auf **Weiter>.** Weiter geht es mit Klicks auf **Test, Ja** auf **OK** und zum Schluss noch einmal auf **Ja.** Der PC wird jetzt neu gestartet. Beim Booten werden Sie erstmals zur Passworteingabe aufgefordert. Ist nichts schief gegangen, startet Windows normal.
- Nachdem Windows hochgefahren ist, öffnet sich ein TrueCrypt-Fenster mit der Erfolgsbestätigung. So, jetzt wird’s wirklich ernst. Mit einem Klick auf **Verschlüsselung** und einem weiteren auf **OK** beginnt die tatsächliche Verschlüsselung der Windows-Festplatte. Ist die Verschlüsselung abgeschlossen, erhalten Sie eine Erfolgsmeldung. Bestätigen Sie diese mit **OK** und klicken Sie noch auf **Fertig stellen.**

Das war’s. Im Hauptfenster von TrueCrypt wird von nun an angezeigt, dass die Systempartition verschlüsselt ist – unabhängig davon, ob andere Laufwerke eingebunden sind oder nicht. In Zukunft startet Windows nur nach der korrekten Passworteingabe; man spricht von einer „Pre-Boot-Authentication“.



Warum Container verstecken?

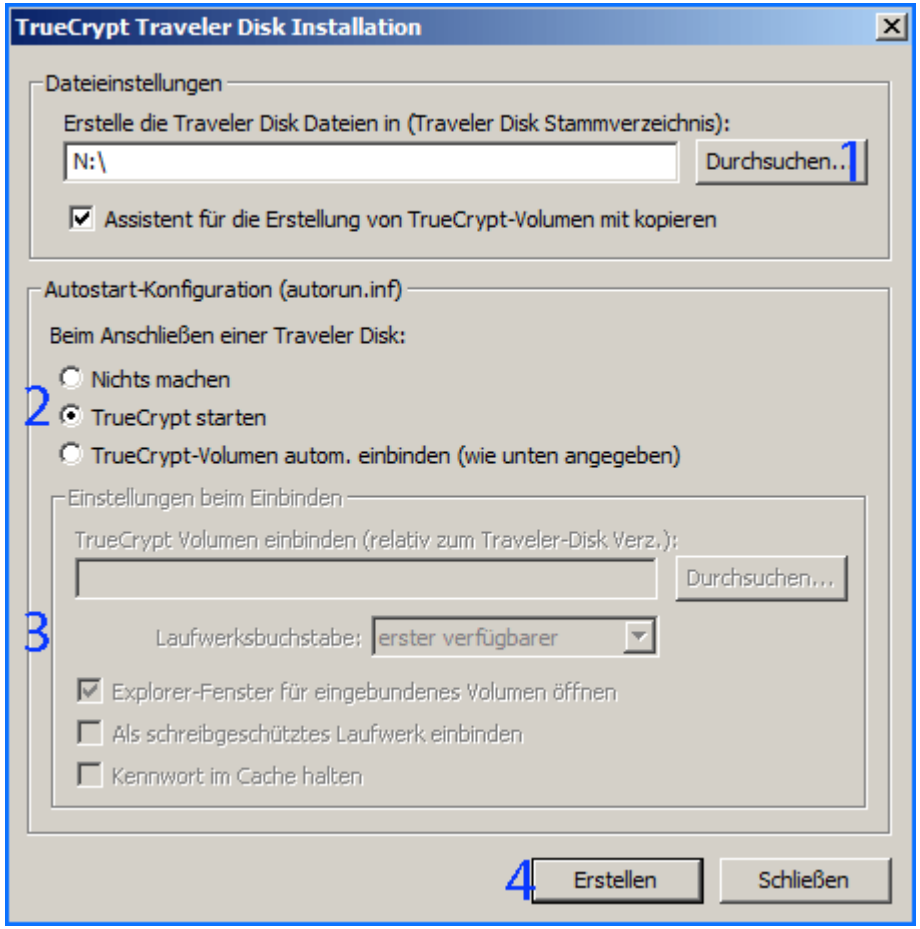
Es kann der Fall eintreten, dass Sie gezwungen werden, das Passwort für Ihren Container herauszugeben. Abhilfe schaffen unsichtbare Container (Hidden Volume).

Sie legen dazu in einem normalen Container einen zweiten, versteckten Container an. Der verborgene Container ist durch ein eigenes Passwort geschützt. Werden Sie nun gezwungen, das Passwort herauszugeben, geben Sie natürlich nur das Passwort für den äußeren Container preis. Der Angreifer kann daher nur auf die „unwichtigen“ Daten zugreifen. Jedenfalls soll die Existenz des geheimen Containers nach Angaben der TrueCrypt-Experten nicht nachweisbar sein.

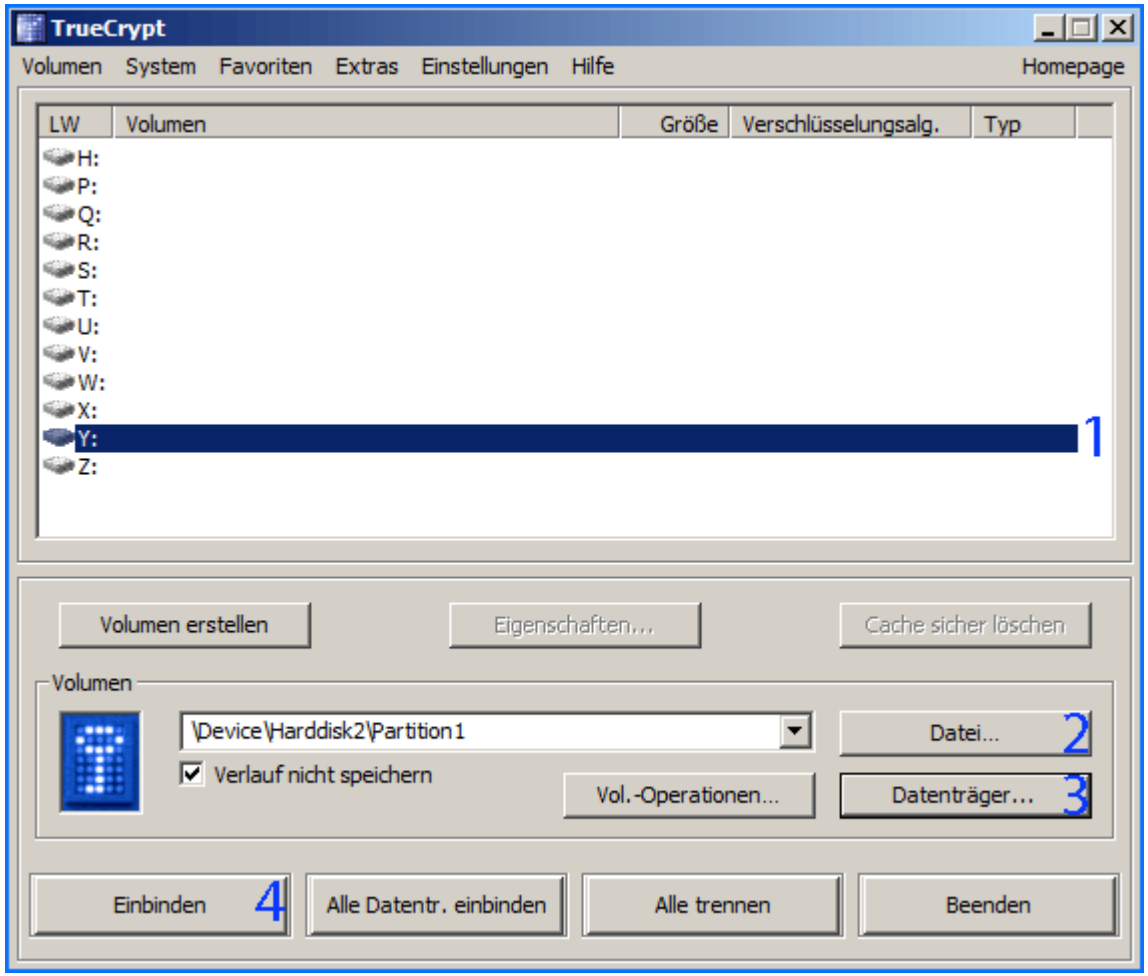
Bevor Sie den versteckten Container anlegen, sollten Sie den bereits erstellten Datencontainer einbinden und ein paar „unwichtige“ Daten in das Laufwerk kopieren – aber nicht völlig belanglose, damit der Angreifer nicht stutzig wird.

- Starten Sie den Assistenten zum Anlegen eines Containers mit einem Klick auf **Volume erstellen**. Belassen Sie die voreingestellte Option und klicken auf **Weiter >.** Wählen Sie im nächsten Dialog-Fenster die Option **Verstecktes TrueCrypt-Volume (1)** und klicken erneut auf **Weiter > (2).**
- Wählen Sie **Direkter Modus** und klicken Sie wiederum auf **Weiter >.** Jetzt wählen Sie den äußeren Container aus und gehen zum nächsten Fenster mit **Weiter >.** Es folgt nun die Eingabe des Kennwortes des äußeren Containers. Mit **Weiter >** und **OK** gelangen Sie zu den Angaben für das versteckte Volumen. Es folgt die Wahl der Verschlüsselungsmethode, Größe und Kennwort.
- Mit **Formatieren, OK** und **Beenden** ist das innere Volumen fertiggestellt.

TrueCrypt hat auch einen „Portable Mode“ an Bord, den es als „Traveler mode“ bezeichnet. Damit muss TrueCrypt nicht mehr installiert werden, sondern kann auch von einem USB-Stick aus direkt auf jedem PC ausgeführt werden. Für den „Traveler mode“ benötigen Sie am fremden PC allerdings Administratorenrechte.



- Stecken Sie einen USB-Stick an den PC, auf dem bereits ein Datencontainer angelegt und noch genügend Speicherplatz für die Installation des portablen Truecrypt-Tools vorhanden ist.
- Klicken Sie im Hauptmenü unter **Extras** auf den Eintrag **Traveler Disk Installation…** und wählen Sie über **Durchsuchen… (1)** das Laufwerk Ihres USB-Sticks aus. Nun legen Sie fest **(2)**, was passieren soll, sobald Sie den USB-Stick am PC anschließen.
- Wählen Sie als Startoption **Nichts machen** oder **TrueCrypt** starten, weil die automatische Einbindung nur auf nicht beschreibbare Medien (CD, DVD) funktioniert. Sollten Sie sich für **TrueCrypt-Volume autom. einbinden** entscheiden, dann wird der Bereich **Einstellungen beim Einbinden (3)** aktiv. In diesem Fall wählen Sie aus, welcher Datencontainer automatisch eingebunden werden soll und welchen Laufwerksbuchstaben der eingebundene Container erhalten soll.
- Mit **Erstellen (5)** werden auf dem USB-Stick das Verzeichnis TrueCrypt angelegt und die portablen Tools ins Verzeichnis kopiert. Zum Abschluss erscheint die Bestätigung, dass TrueCrypt im Traveler mode genutzt werden kann und eine Info über die dazu erforderlichen Administratorenechte. Schließen Sie den Assistenten mit **OK.**



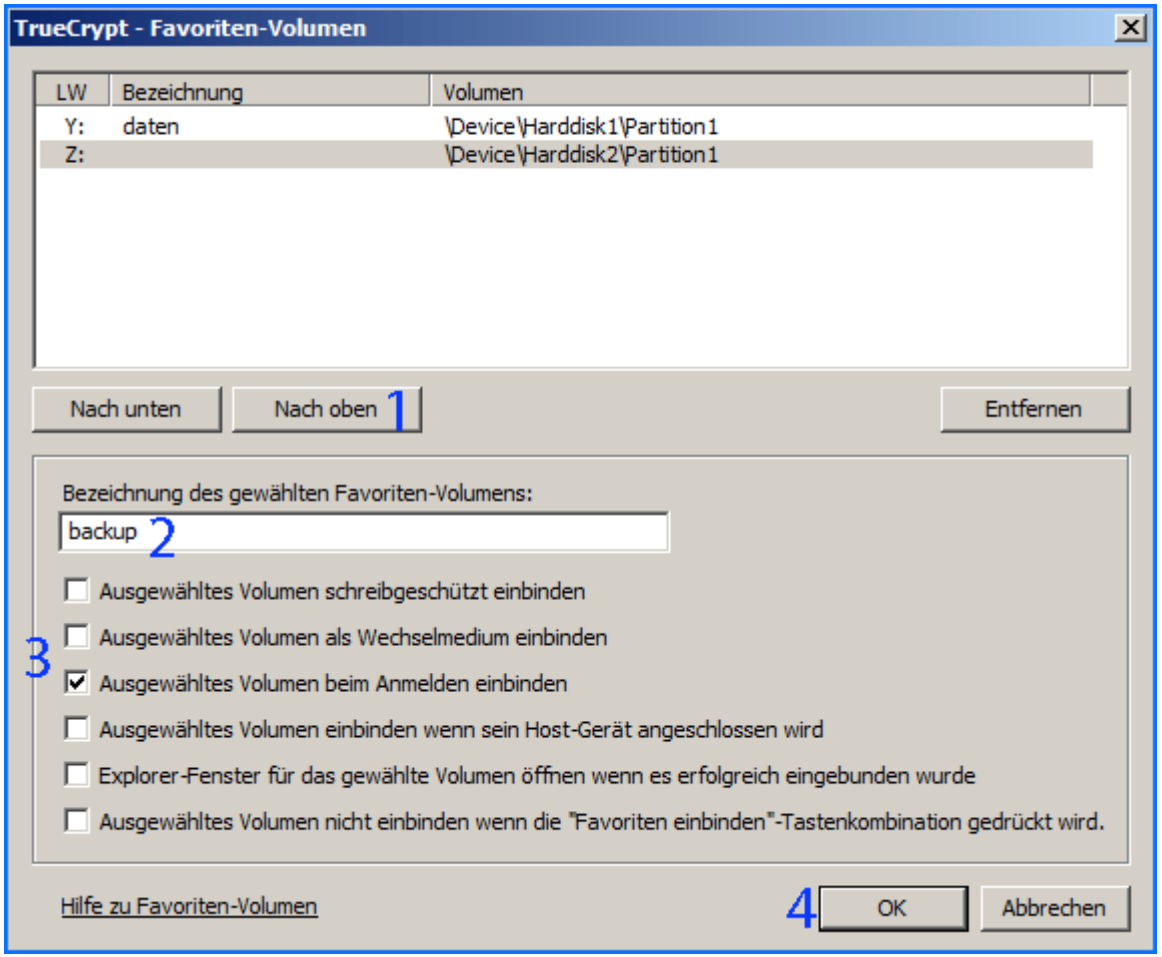
Container/Festplatte einbinden

Damit Sie auf die angelegten Container/Partitionen zugreifen können, müssen Sie diese in Windows einbinden (mounten).

- Markieren Sie zunächst im Hauptfenster einen freien Laufwerksbuchstaben **(1).** Das eingebundene Laufwerk erscheint dann unter diesem Buchstaben im Explorer-Fenster.
- Wollen Sie einen Datencontainer einbinden, dann klicken Sie auf **Datei… (2),** navigieren zum Speicherort und klicken auf **Öffnen.** Nach dem Klick auf **Einbinden (4)** geben Sie das Passwort ein und bestätigen mit **OK.** Soll Ihr Traveler Disk (USB-Stick) in einen fremden PC eingebunden werden, dann öffnen Sie zunächst das TrueCrypt-Verzeichnis auf Ihrem USB-Stick und starten TrueCrypt mit einem Doppelklick auf die Datei truecrypt.exe. Wie es weiter geht, wissen Sie bereits.
- Wollen Sie eine Festplatte/Partition anschließen, dann klicken Sie auf **Datenträger (3)** und wählen die gewünschte Festplatte/Partition aus.
- Wollen Sie Ihren versteckten Container einbinden, dann öffnen Sie zunächst den äußeren Container, geben aber das Passwort für den versteckten Container ein und bestätigen mit **OK.**

Hinweis

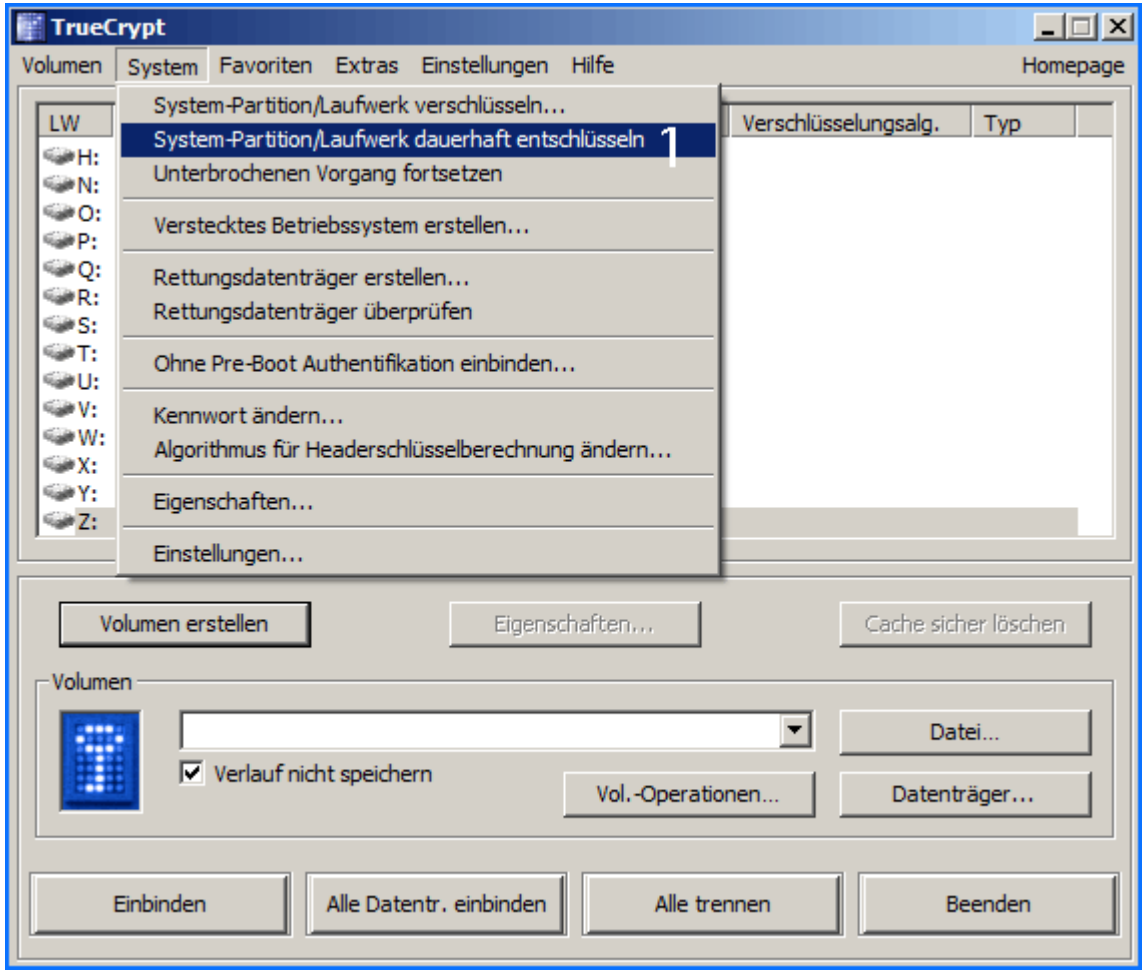
Bevor Sie den USB-Stick vom PC abziehen, trennen Sie erst einmal das eingebundene Laufwerk und werfen dann den USB-Stick über die Windows-Funktion „Hardware sicher entfernen“ aus. Das Symbol dafür finden Sie in der Taskleiste rechts unten. Entfernen Sie den USB-Stick während eines geöffneten Containers oder Schreibprozesses, kann der Datencontainer beschädigt werden und im schlimmsten Fall sind die Daten verloren.



Einbindung automatisieren

Sie können die Einbindung der Laufwerke auch mit Hilfe der „Favoriten“ automatisieren.

- Mounten Sie zunächst eine Festplatte/Partition, klicken Sie dann unter **Favoriten** auf den Eintrag **Eingebundes Volumen zu den Favoriten hinzufügen…** und es öffnet sich der Einstellungsdialog zu den Favoriten. So können Sie hier die Reihenfolge der Favoriten über die Button **Nach unten** und **Nach oben** **(1)** festlegen, dem Favoriten-Laufwerk einen Namen zuweisen **(2)** und festlegen, wie das ausgewählte Volume eingebunden werden soll **(3)**.
- Bestätigen Sie Ihre Einstellungen mit **OK** **(4).** Jetzt werden Sie bereits nach jedem Windowsstart automatisch nach dem Passwort Ihrer verschlüsselten Festplatte/Partition gefragt.



Verschlüsselte Partition entfernen

- Angelegte Container entfernen Sie, indem Sie diese einfach löschen – so wie jede andere Datei oder jedes andere Verzeichnis.
- Ebenso unkompliziert lassen sich verschlüsselte Festplatten wieder entschlüsseln. Klicken Sie auf **Arbeitsplatz,** markieren Sie die verschlüsselte Festplatte und drücken Sie dann im Kontextmenü auf **Formatieren…**

Windows-Verschlüsselung entfernen

Die Verschlüsselung der Systempartition können Sie genauso in wenigen Schritten wieder rückgängig machen.

- Klicken Sie im Hauptfenster auf **System/System-Partition/Laufwerk dauerhaft entschlüsseln (1),** darauf zwei Mal auf **Ja** und die Entschlüsselung wird gestartet.
- Ist die Entschlüsselung abgeschlossen, erhalten Sie eine Erfolgsmeldung. Ihr PC kann wieder ohne Passwort hochgefahren werden und jeder hat ungehinderten Zugriff darauf!

- **Sichere Passwörter verwenden:** Setzen Sie für die Verschlüsselung Ihrer Container, Festplatten oder des Betriebssystems sichere Passwörter ein. KeePass ist ein Open-Source-Programm, das Passwörter in beliebiger Länge, mit Groß- und Kleinschreibung, Zahlen und Sonderzeichen erzeugen und verwalten kann (vgl. Workshop: KeePass_Passwortmanager).
- **Volume-Header sichern:** Eine Beschädigung des „Kopfdatenbereichs“ des Datenträgers bewirkt, dass das Laufwerk nicht mehr eingebunden wird. TrueCrypt hat deshalb eine Funktion zum Sichern und Wiederherstellen des Kopfdatenbereichs an Bord. Öffnen Sie hierzu den Datencontainer bzw. die verschlüsselte Festplatte und starten Sie den Sicherungs-Assistenten mit einem Klick auf „Extras/Volumen-Header sichern…“. Wählen Sie als Speicherort einen externen Datenträger (CD, CF-Karte, USB-Stick usw.).
- **Daten sicher löschen:** Löschen Sie die Daten im Windows-Papierkorb mit wirksamen Lösch-Tools. Shreddern Sie nach jeder PC-Sitzung die Datenspuren, die Windows und Ihre Anwendungen hinterlassen. So können Angreifer keine Rückschlüsse auf Ihre vertraulichen Daten herstellen. Eraser (http://sourceforge.net/projects/eraser) und CCleaner (www.ccleaner.de) sind Tools, mit deren Hilfe Sie Daten und Datenspuren sicher shreddern (vgl. Workshop: Eraser_Daten sicher löschen).
- **Antivirenprogramm einsetzen:** Beachten Sie, dass auch das eingebundene Laufwerk mit Schadcode infiziert werden kann und dass so die zu schützenden Daten ausspioniert werden können. Ist Spyware einmal auf Ihrem PC, macht auch die Verschlüsselung wenig Sinn. Schützen Sie deshalb Anwendungen und Daten durch eine aktuelle Firewall und Antivirensoftware, wie „AntiVir Personal – Free Antivirus“ (www.free-av.de), „AVG Anti-Virus Free“ (http://free.avg.de) oder „avast Free Antivirus“ (www.avast.com). Wollen Sie aber wirklich wichtige Daten schützen, darf Ihr PC nicht ans Netz und es darf auch nur die nötigste Software installiert werden.