Akademie
für Lehrerfortbildung
und Personalführung

Truecrypt

IT-Qualifizierung
für Lehrkräfte

Datenverschlüsselung in der Schule

Impressum

Herausgeber:	Akademie für Lehrerfortbildung und Personalführung Kardinal-von-Waldburg-Str. 6-7 89407 Dillingen
Autor:	Georg Schlagbauer
URL:	http://alp.dillingen.de/schulnetz
Mail:	schlagbauer@alp.dillingen.de
Stand:	Juli 2008

Truecrypt

Datenverschlüsselung in der Schule

Inhalt

Einführung

Elektronisch gespeicherte Daten haben eine immer größere Bedeutung und deshalb muss auch die Datensicherheit immer mehr beachtet werden. Diese Datensicherheit besteht jedoch aus verschiedenen Komponenten, die sich gegenseitig sogar widersprechen können. Zum einen geht es um den möglichen Verlust der Daten. Dagegen helfen ausgefeilte Strategien zur Datensicherung. Daten werden auf Wechselmedien oder auf eigenen verteilten Backupservern gespeichert, wodurch das Risiko des möglichen Verlustes reduziert wird. Zum anderen geht es um den Schutz der Daten vor Missbrauch. Mit den Anforderungen einer guten Datensicherung widerspricht sich dies, wenn auf die Datensicherung auch Personen Zugriff haben könnten, die selbst ein Interesse an diesen Daten haben. Daneben gibt es gerade bei mobilen Datenträgern beliebig viele Möglichkeiten, dass diese in fremde Hände gelangen könnten.

Eine Möglichkeit, sensible Daten vor fremdem Zugriff zu schützen, ist, diese Daten nur verschlüsselt aufzubewahren oder nur verschlüsselt zu transportieren.

Das Programm Truecrypt bietet diese Möglichkeit. Es bietet eine hohe Sicherheit und gleichzeitig genügend Komfort im praktischen Einsatz. Es ist ein Open Source-Programm und für die gängigen Betriebssysteme Windows, Linux und MacOS erhältlich. Die Daten werden dabei in einem verschlüsselten Container abgelegt, der mit einem Passwort gesichert ist. Im Dateisystem ist dieser Container eine ganz normale Datei, die zunächst mit Zufallszahlen gefüllt ist. Nach dem Öffnen des Containers wird dieser unter Windows als Laufwerk angeboten, unter Linux lässt er sich an beliebiger Stelle in den Dateibaum einhängen. Wird der Container wieder geschlossen, präsentiert er sich als eine einzige Datei, in der alle Dokumente verschlüsselt abgelegt sind. Es lässt sich nicht erkennen, welche oder wie viele Dokumente darin verborgen sind. Lediglich aus der Größe des Containers im Dateisystem lassen sich Vermutungen über die maximale Menge der darin enthaltenen Daten anstellen.

Der verschlüsselte Datencontainer kann in die normale Sicherungskette aufgenommen werden. Dadurch wird die Gefahr reduziert, dass die Daten verloren gehen. Die Verschlüsselung des Datencontainers schützt vor Missbrauch. Ohne das Passwort ist niemand in der Lage, die Daten zu entschlüsseln.

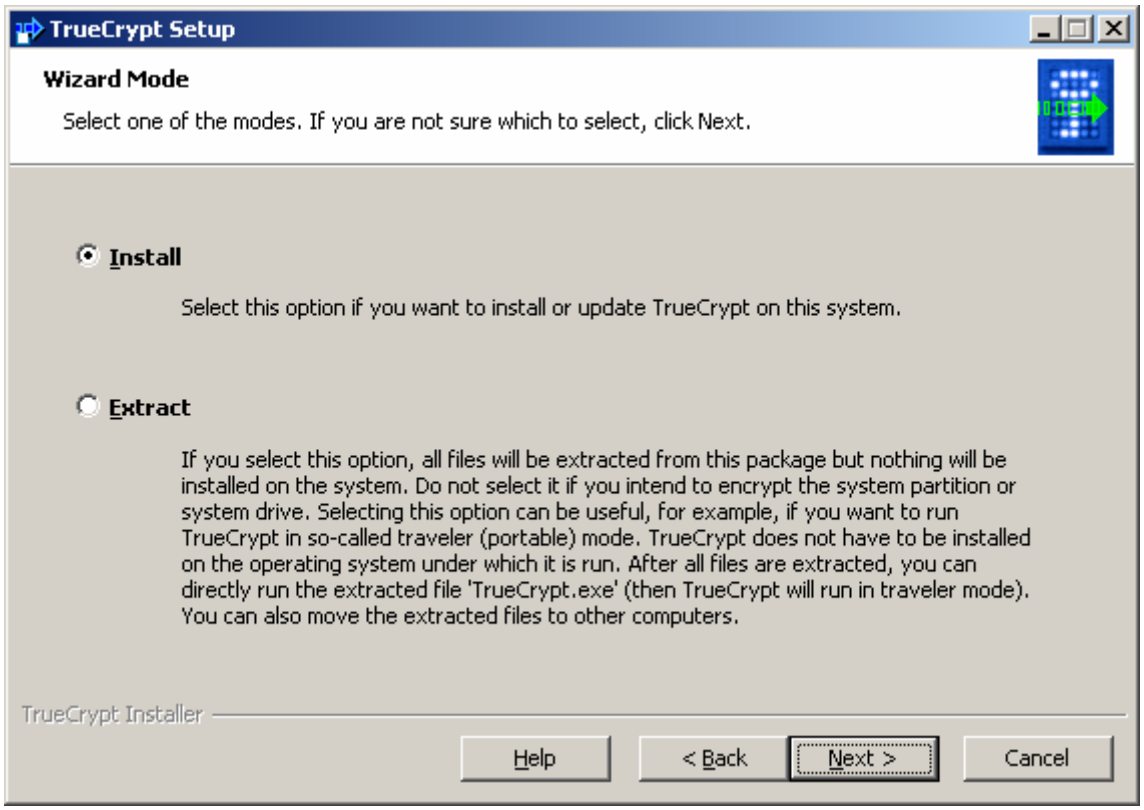
Neben verschlüsselten Datencontainern, die auf Dateiebene erzeugt werden, bietet Truecrypt auch die Möglichkeit, ganze Partitionen einer Festplatte oder einen gesamten USB-Stick zu verschlüsseln. Wenn ein verschlüsselter USB-Stick verloren geht, erhält der „Finder“ nicht einmal einen Hinweis, dass es sich hier um ein verschlüsseltes Medium handelt. Windows bringt z. B. nur die Meldung, dass der Datenträger nicht formatiert ist.

Truecrypt speichert die Daten auf der Festplatte immer verschlüsselt. Selbst nach einem plötzlichen Stromausfall oder nach dem Ausschalten des PC liegen die Daten nur verschlüsselt vor. Wird ein Dokument aus einem geöffneten Container von einem Programm geladen, so wird es von Truecrypt im Hintergrund entschlüsselt und dem Programm angeboten. Umgekehrt werden die Daten bevor sie auf der Festplatte abgelegt werden wieder verschlüsselt.

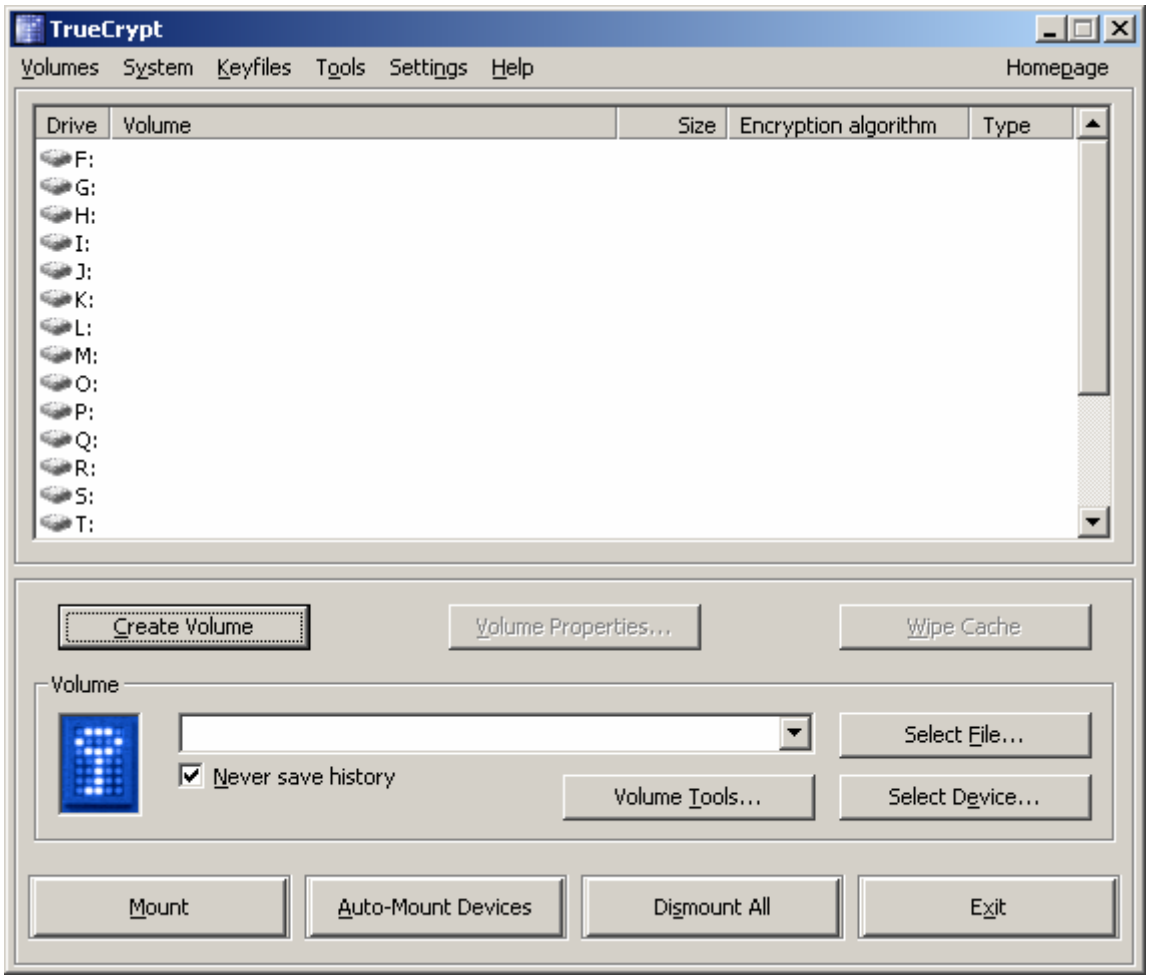
Installation von Truecrypt unter Windows

Truecrypt erhält man zum Download unter http://www.truecrypt.org/

Bei der Installation wird angeboten, das Programm zu installieren oder die Dateien nur auszupacken. Der letztere Punkt ist interessant, wenn Truecrypt als „Portable Application“ auf einem USB-Stick betrieben werden soll. Truecrypt nennt dies „Traveler mode“.



Erzeugen eines verschlüsselten Containers

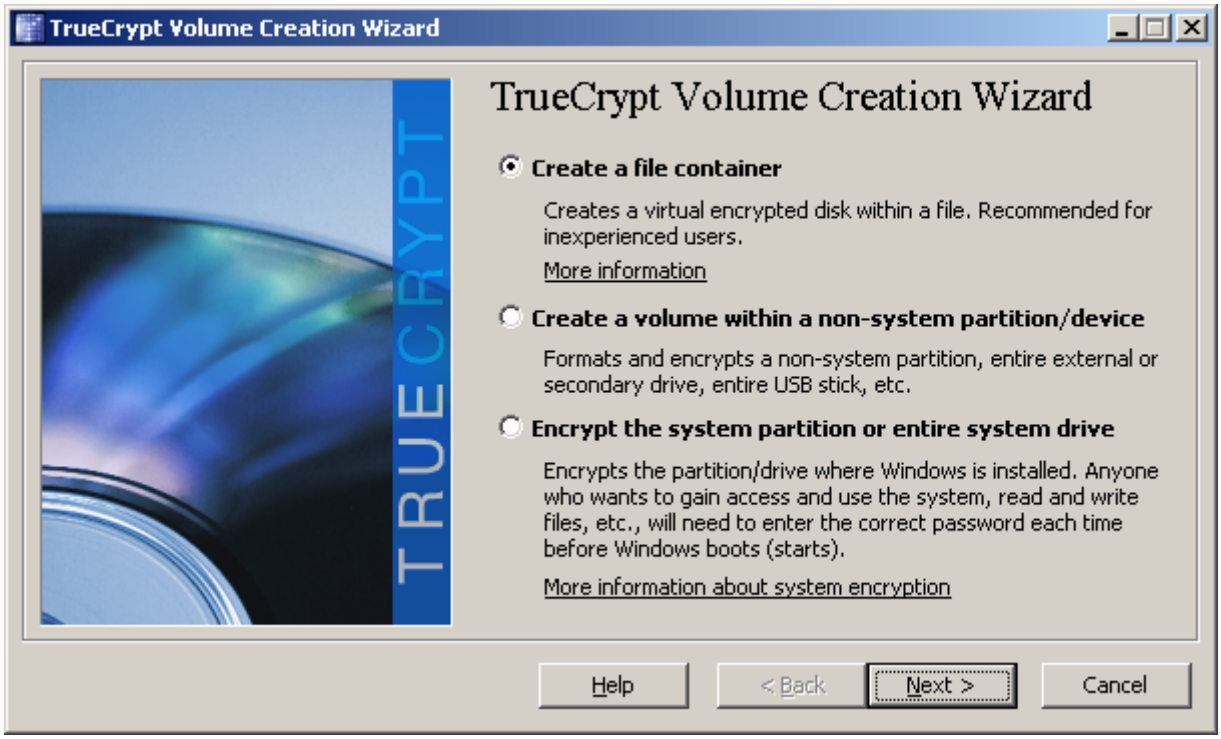


Über den Button „Create Volume“ erzeugt man mit Hilfe eines Assistenten einen verschlüsselten Container. Dieser beinhaltet später die vertraulichen Daten. Beim Einrichten eines Containers bietet Truecrypt verschiedene Optionen an:

- Neben einem einfachen Datei-Container lässt sich auch eine ganze Datenpartition oder sogar die Systempartition verschlüsseln.
- Innerhalb eines bereits existierenden Containers lässt sich ein „Hidden Volume“ anlegen. Dabei werden nicht nur die darin enthaltenen Daten verschlüsselt, es ist auch nicht erkennbar, dass ein solcher Bereich existiert. Auf die Sicherheit der Verschlüsselung hat ein Hidden Volume keine Einfluss.
- Bei einem Dateicontainer ist der Name und Speicherort der Datei zu bestimmen. Truecrypt sieht die Endung tc (Truecrypt Container) vor, dies ist aber nicht zwingend. Wenn man verbergen möchte, dass es sich um einen verschlüsselten Container handelt, ist es besser, keine Endung oder eine andere Endung zu wählen.
- Der Verschlüsselungsalgorithmus kann gewählt werden. Standardmäßig wird AES-256 vorgeschlagen.

- Bei Datei-Containern kann die Größe bestimmt werden. Die Größe sollte sich an der Menge der zu verschlüsselnden Daten orientieren. Wenn ein Datencontainer zu groß ist, wird das Handling unpraktisch.
- Das Dateisystem (FAT/NTFS) muss festgelegt werden. Wenn der Container auch unter Linux geöffnet werden soll oder auf CD gebrannt werden soll, ist FAT vorzuziehen.
- Das Passwort zum Öffnen des Containers muss festgelegt werden. Aus Sicherheitsgründen sollte dieses Passwort lang und komplex genug gewählt werden. Ergänzend zum Passwort könnte ein keyfile gewählt werden. Ein Entschlüsseln wäre dann nur in Verbindung von Passwort und Keyfile möglich.

Am flexibelsten ist man, wenn man einen einfachen Datei-Container erzeugt. Dieser erscheint im Dateisystem als normale Datei, deren Inhalt jedoch nicht erkennbar ist. Die Datei kann beliebig kopiert werden und kann damit in die normale Datensicherungskette mit eingebunden werden.

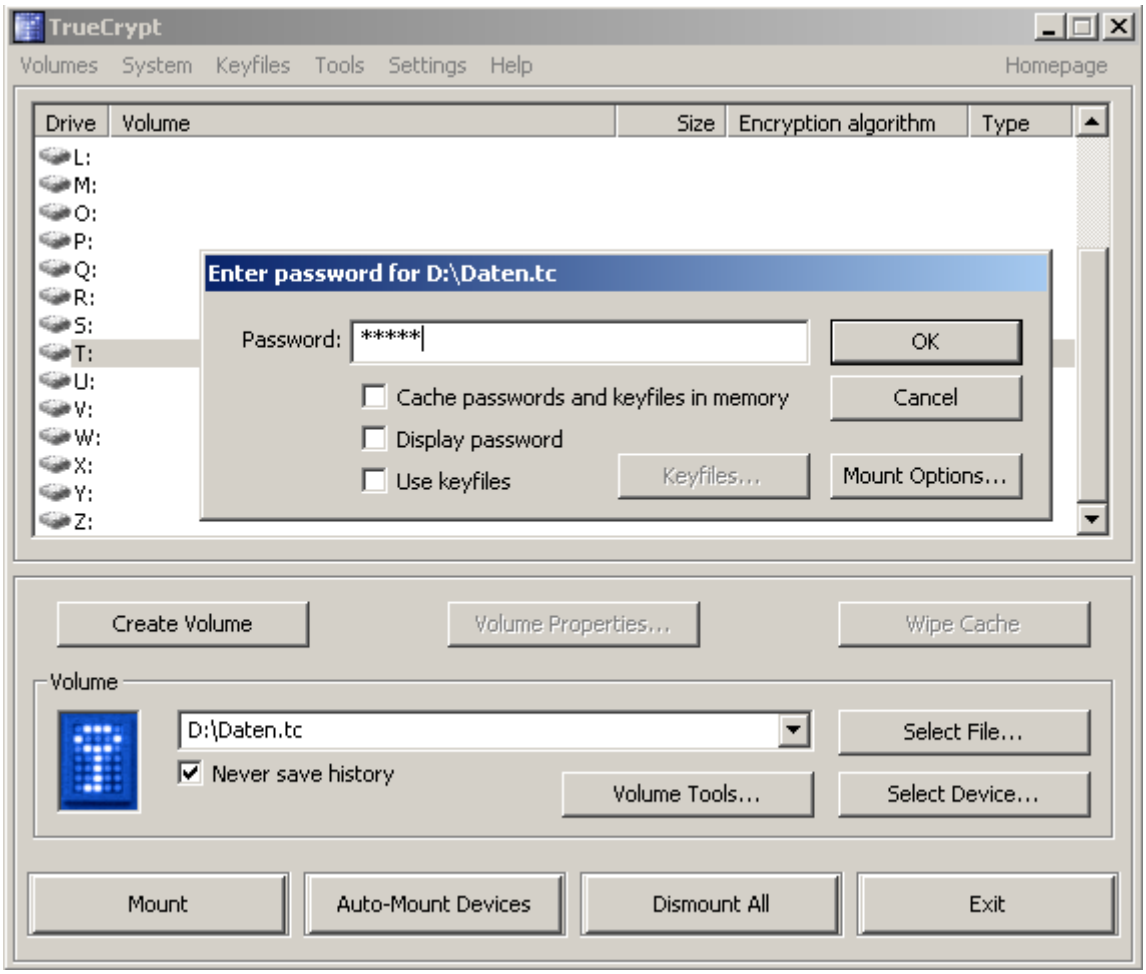


Öffnen eines Containers unter Windows

Zum Öffnen eines Containers sind grundsätzlich folgende Schritte notwendig:

1. Das Programm Truecrypt muss gestartet werden.
2. Der verschlüsselte Container muss ausgewählt werden.
3. Ein Laufwerksbuchstabe muss ausgewählt werden, unter dem der Inhalt des Containers angeboten werden soll.
4. Der Container wird gemountet. Dabei ist die Eingabe des Passwortes erforderlich.

Nach der Eingabe des Passwortes ist der Inhalt des Containers über den gewählten Laufwerksbuchstaben zugänglich.



Öffnen eines Containers mit einem Kommandozeilenbefehl:

Wenn Truecrypt nicht in den Suchpfad eingebunden ist, muss zum Aufruf der komplette Pfad angegeben werden:

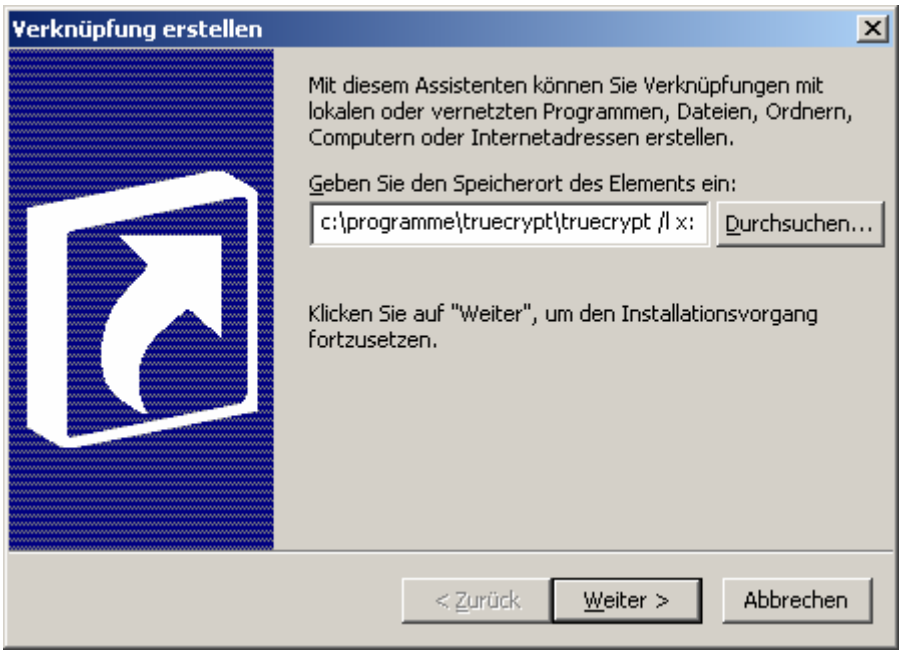
```
C:\Programme\TrueCrypt\TrueCrypt.exe /lx /v d:\daten.tc /q /e
```

Optionen

`/l x:` oder `/lx`	Auswahl des Laufwerksbuchstabens x
`/v d:\daten.tc`	Auswahl des Containers
`/q`	Quit; Das Programmfenster wird nicht angezeigt. Es wird nur das Passwortfenster geöffnet.
`/q background`	Das Programmfenster wird nicht angezeigt. Es wird jedoch ein Icon in der Taskleiste erzeugt.
`/s`	Silent-Modus; Jede Interaktion wird unterdrückt.
`/e`	Es wird ein Explorerfenster mit dem Inhalt des Containers geöffnet.

Öffnen eines Containers über eine Verknüpfung auf dem Desktop:

Wird der obige Kommandozeilenbefehl als Verknüpfung auf dem Desktop abgelegt, lässt sich der Container mit einem Doppelklick öffnen. Die Übergabe des Passwortes auf Kommandozeile wäre ebenfalls möglich. Dies dürfte jedoch in den meisten Fällen nicht sinnvoll sein.

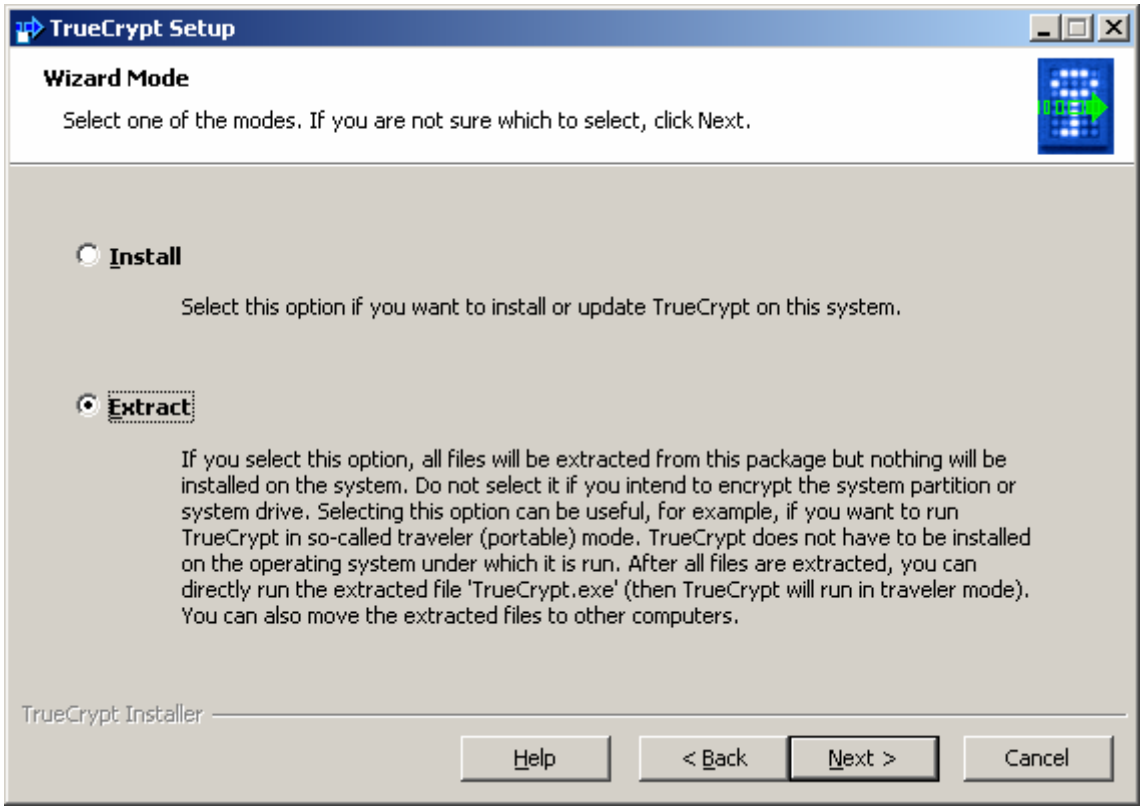


Zugang zum verschlüsselten Container über eine Verknüpfung auf dem Desktop. (Im Bild ist nicht der gesamte Kommandozeilenbefehl sichtbar.)

Verschlüsselte Daten auf einem USB-Stick

Der Traveler-Modus von Truecrypt

Bei der Installation von Truecrypt wird angeboten, das Programm nur zu entpacken. Dies ist interessant, wenn Truecrypt als „Portable Application“ auf einem USB-Stick betrieben werden soll. Truecrypt nennt dies „traveler mode“.



Bringt man den verschlüsselten Container zusammen mit den Truecrypt-Programmdateien auf einem USB-Stick unter, lässt sich der Container auf jedem Windows-Rechner ohne Installation von Truecrypt öffnen. Auf einem Windows-Rechner sind dazu jedoch administrative Rechte notwendig. Ein Benutzer ohne Administratorrechte kann Truecrypt nur verwenden, wenn es auf dem Computer installiert wurde.

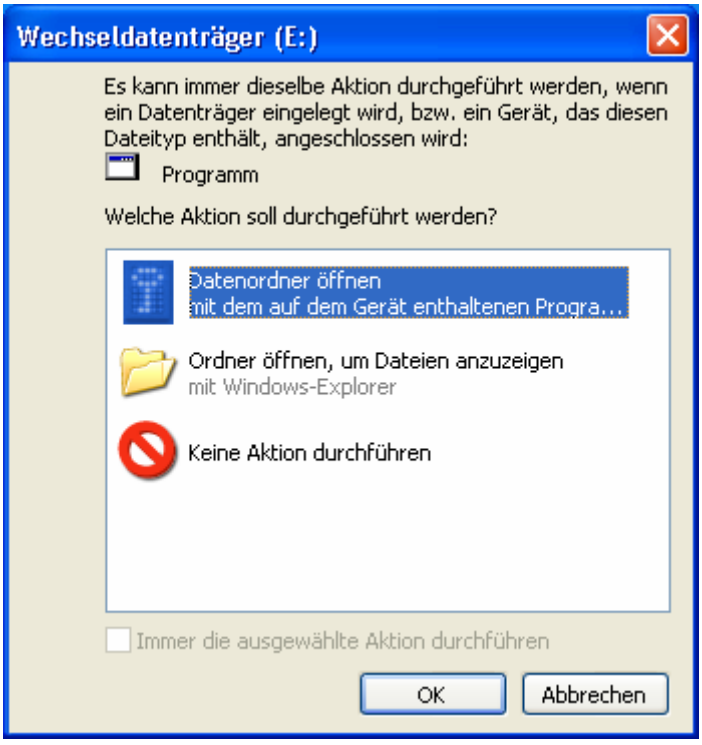
Autostart von Truecrypt auf einem USB-Stick

Auf mobilen Datenträgern gibt es mit einer Datei autorun.inf beim Einbinden des Datenträgers bestimmte Programme zu starten. Die Datei autorun.inf muss sich dabei im Wurzelverzeichnis des USB-Sticks befinden. Im folgenden Beispiel befinden sich die Truecrypt-Programmdateien und der verschlüsselte Datencontainer (Daten.tc) ebenfalls im Wurzelverzeichnis des USB-Sticks.

Inhalt der Datei autorun.inf

```
[AutoRun]
open=truecrypt.exe /lx /v Daten.tc /q background /e
icon=truecrypt.exe
action=Datenordner öffnen
```

Nach dem Einstecken des USB-Sticks bekommt man sofort die Option angeboten, den Datenordner zu öffnen und das Passwort einzugeben:



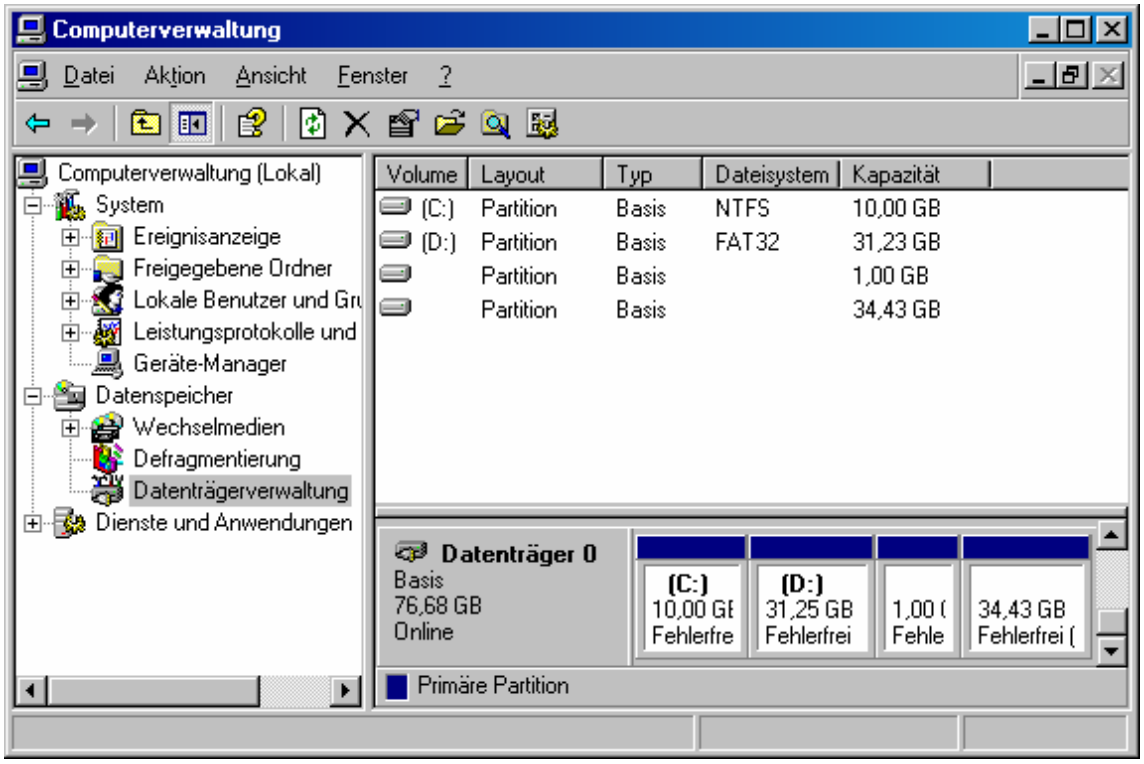
Wenn das Passwort korrekt eingegeben wurde, öffnet sich ein Explorer-Fenster mit dem Inhalt des Datenordners.

Neben der Möglichkeit, einen verschlüsselten Container auf einem USB-Stick anzulegen, gibt es noch die Möglichkeit, den gesamten USB-Stick zu verschlüsseln. Dies ist vor allem dann sinnvoll, wenn nicht erkennbar sein soll, dass der USB-Stick Daten enthält. Ein Betriebssystem erkennt nur, dass der USB-Stick keine gültige Formatierung besitzt und bietet an, den Stick neu zu formatieren.

Verschlüsseln von Datenpartitionen

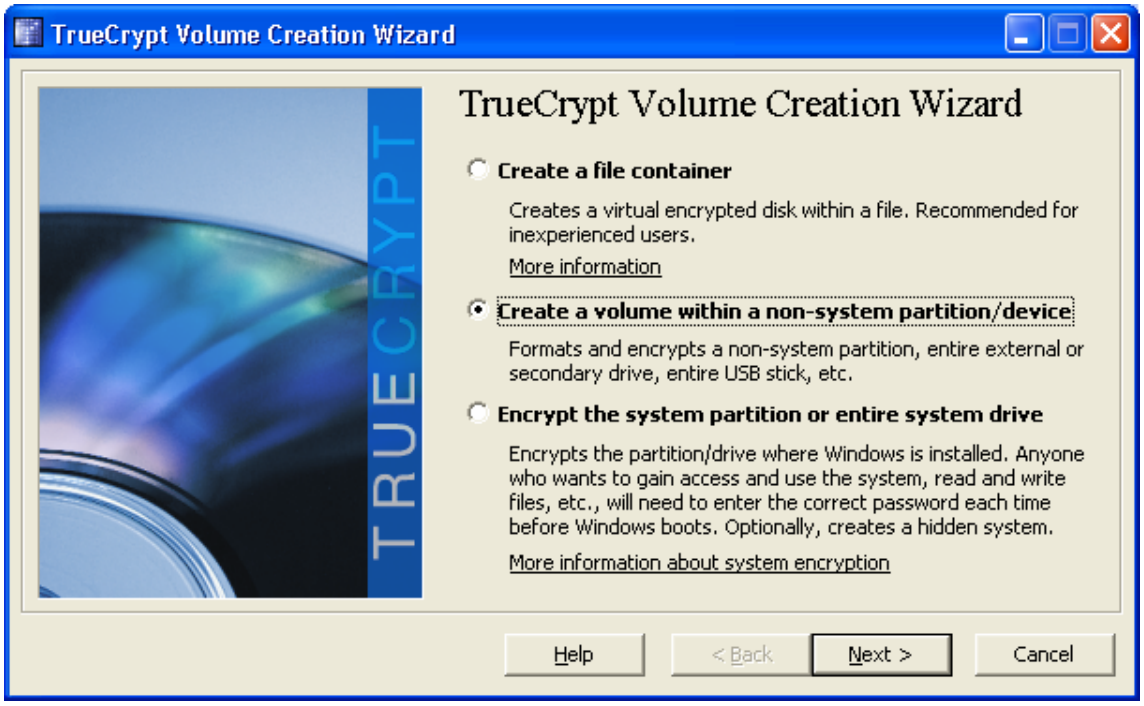
Auf Notebooks oder persönlichen Computern, bei denen nicht ausgeschlossen werden kann, dass fremde Personen Zugriff haben könnten, bietet es sich an, eine gesamte Datenpartition zu verschlüsseln. Dazu wird unter Windows eine neue Partition angelegt. Diese wird nicht formatiert und erhält auch keinen Laufwerksbuchstaben. So erscheint diese Partition später nicht im Dateisystem bevor sie von Truecrypt gemountet wurde.

Wenn eine bereits vorhandene Partition verwendet werden soll, darf diese keine Daten enthalten. (Beim Einrichten wird von Truecrypt alles gelöscht.) Auch der Laufwerksbuchstabe sollte entfernt werden.



Mit der Datenträgerverwaltung von Windows lassen sich Partitionen neu anlegen oder auch löschen.

Unter Truecrypt wird über den Button „Create Volume“ ein neuer verschlüsselter Bereich eingerichtet. Dabei wird diesmal jedoch kein Dateicontainer sondern eine Partition ausgewählt.



Über den Button „Select Device“ kann eine verschlüsselte Partition anschließend ausgewählt und gemountet werden.

Öffnen einer verschlüsselten Partition auf Kommandozeile

```
TrueCrypt.exe /lx /v \Device\Harddisk0\Partition3 /q /e
```

Wenn Truecrypt nicht in den Suchpfad eingebunden ist, muss zum Aufruf von Truecrypt.exe der komplette Pfad (z. B. C:\Programme\Truecrypt\Truecrypt.exe) angegeben werden.

Der Kommandozeilenbefehl kann über eine Verknüpfung auf dem Desktop aufgerufen werden, so dass der verschlüsselte Container mit einem Doppelklick (und der Eingabe des Passwortes) geöffnet werden kann.

Verschlüsselte Datenpartitionen können nicht nur auf Festplatten sondern auf allen beschreibbaren mobilen Datenträgern angelegt werden. Geht ein solcher Datenträger verloren, ist für den „Finder“ nicht erkennbar, dass darauf Daten enthalten sind. Es gibt keinen sichtbaren Header oder andere Hinweise, die zwingend auf verschlüsselte Daten schließen lassen (plausible deniable). Ein Betriebssystem erkennt nur zufällige Daten, die bei einem nicht formatierten Datenträger durchaus üblich sind.

Installation von Truecypt unter Linux

Auf der Internetseite von Truecrypt (http://www.truecrypt.org) werden rpm-Pakete für SuSE und Debian-Pakete für Ubuntu angeboten.

Installation unter Ubuntu

Das Debian-Paket zur Installation wird in einem gepackten Archiv geliefert. Auf der grafischen Oberfläche lässt es sich mit einem Mausklick entpacken (Kontextmenü: Hier entpacken). Ein Doppelklick auf die deb-Datei installiert das Truecrypt-Paket.

Auf der Kommandozeile entspricht dies nachfolgenden Befehlen:

```
tar -xzf truecrypt-5.1a-ubuntu-x86.tar.gz
```

In dem erzeugten truecrypt-Verzeichnis befindet sich das eigentliche Debian-Paket.

```
ls truecrypt-5.1a
License.txt  Readme.txt  truecrypt_5.1a-0_i386.deb
```

Mit dem Debian-Paketmanager wird das Paket installiert:

```
dpkg -i truecrypt_5.1a-0_i386.deb
```

Installation unter Debian

Unter Debian-Etch lässt sich das Debian-Paket von Truecrypt ebenfalls installieren. Beim Ausführen des dpkg-Befehls erhält man jedoch Fehlermeldungen, die auf nicht erfüllte Abhängigkeiten hinweisen. Wenn die entsprechenden Pakete nachinstalliert werden, lässt sich Truecrypt installieren.

Start von Truecrypt unter Linux

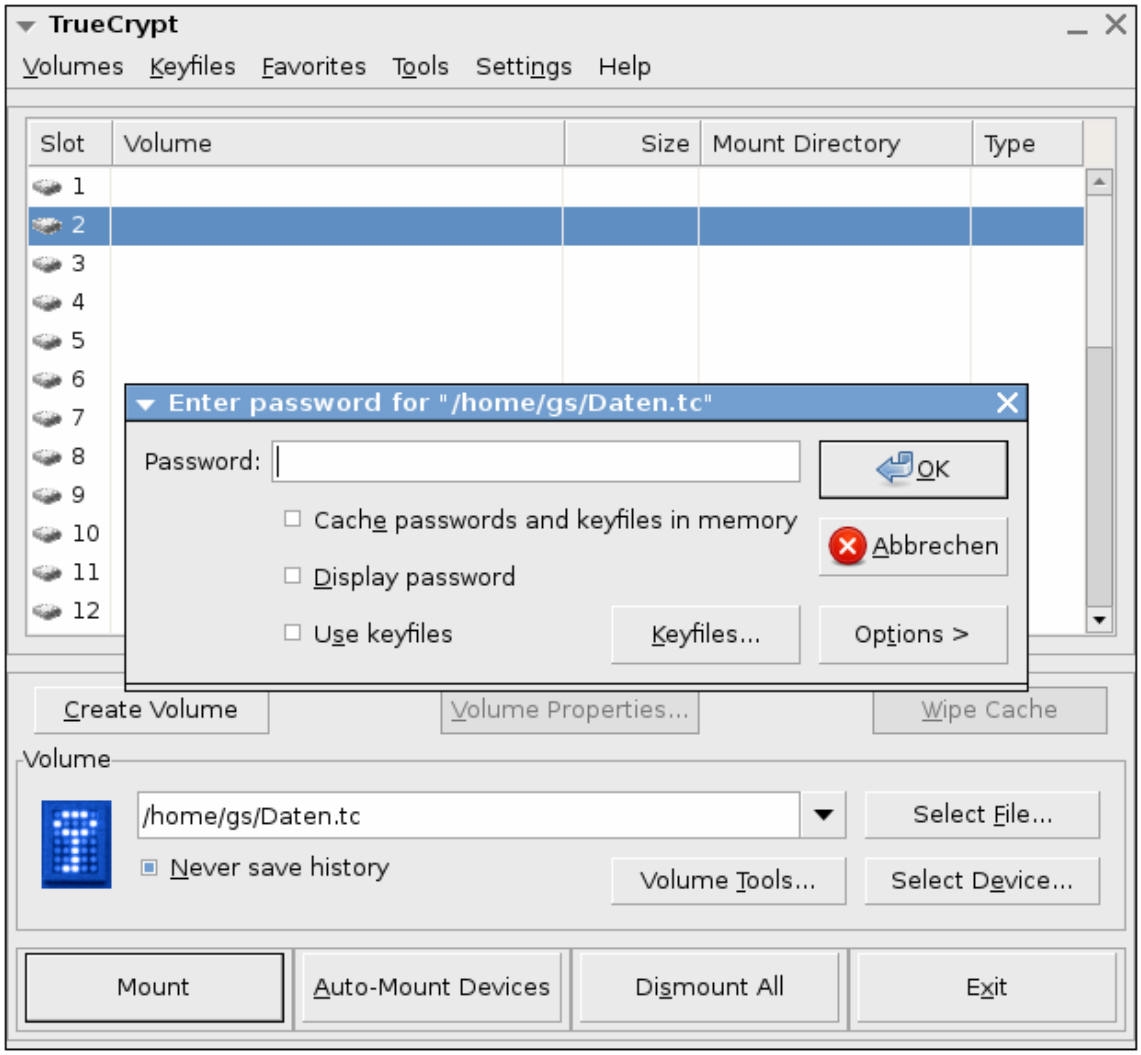
Auf Kommandozeile lässt sich Truecrypt mit dem Befehl truecrypt starten. Alternativ kann es auch in das Menü (unter KDE oder Gnome) eingebunden werden.

Anlegen eines Containers unter Linux

Das Anlegen eines Containers unterscheidet sich nicht vom Vorgehen unter Windows.

Öffnen eines Containers unter Linux

Auch das Öffnen eines Containers unterscheidet sich nur geringfügig vom Öffnen eines Containers unter Windows. Nach dem Start von Truecrypt kann der verschlüsselte Container ausgewählt werden. Danach wird ein beliebiger „Slot“ gewählt. Diese Slots sind ein Überbleibsel der Laufwerksbuchstaben unter Windows und haben ansonst keine Bedeutung. Als Mountpoint wird standardmäßig eines der Verzeichnisse /media/truecrypt1, media/truecrypt2, ... gewählt. Über die Optionen bei der Eingabe des Passwortes lässt sich der Mountpoint jedoch beeinflussen.

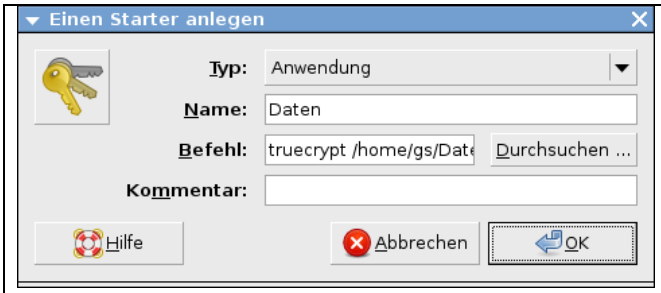


Alternativ lässt sich ein verschlüsselter Container auch über einen Kommandozeilenbefehl einbinden:

```
mkdir Daten
truecrypt Daten.tc Daten
```

oder als vollständiger Kommandozeilenbefehl mit Angabe aller Pfade:

```
mkdir /home/gs/Daten
truecrypt /home/gs/Daten.tc /home/gs/Daten
```



Der vollständige Kommandozeilenbefehl eignet sich auch als Befehlzeile beim Anlegen eines Starters.

Sicherheitsaspekte und Angriffsmöglichkeiten

Das Programm Truecrypt verwendet sichere gängige symmetrische Verschlüsselungsverfahren. Als sicher gilt eine Verschlüsselungsmethode dann, wenn sie nur durch einen "Brute Force"-Angriff geknackt werden kann, also durch Ausprobieren aller möglichen Schlüssel und die Schlüssellänge dabei so groß ist, dass die dafür zur Verfügung stehende Zeit nicht ausreicht. Eine Schlüssellänge von 56 Bit (z. B. DES-Verschlüsselung) kann mit erheblichem Zeit- und Rechenaufwand geknackt werden. Das standardmäßig vorgeschlagene Verschlüsselungsverfahren bei Truecrypt ist AES mit einer Schlüssellänge von 256 Bit. Bei diesem Verfahren ist derzeit kein praktikabler Weg bekannt, um die Verschlüsselung zu knacken.

Neben der prinzipiellen Sicherheit, die durch die Wahl eines geeigneten Verschlüsselungsverfahrens gegeben ist, spielt für die praktische Sicherheit die Art der Implementierung die wichtigere Rolle.

Wahl des Passwortes

Zum Ver- und Entschlüsseln benötigt man bei symmetrischen Verfahren jeweils denselben Schlüssel, der natürlich geheim gehalten werden muss. Da man sich einen beliebigen 256-Bit-Schlüssel nicht merken kann und man sich den Schlüssel auch möglichst nicht notieren sollte, verwendet das Programm Truecrypt ein Passwort, aus dem es den zu verwendenden Schlüssel berechnet. (Wenn zusätzlich ein keyfile verwendet wird, wird dieses in die Berechnung des Schlüssels mit einbezogen.) Die theoretische Sicherheit des Verschlüsselungsalgorithmus reduziert sich also in der Praxis auf die Sicherheit des gewählten Passwortes. Wenn es einem Angreifer gelingt, das Passwort herauszufinden, hat er den Container geknackt.

Wörterbuchattacke zum Knacken des Passwortes

Die folgenden kleinen Beispielskripte (unter Windows und Linux) lesen aus der Datei Woerterbuch.txt zeilenweise mögliche Passwörter aus und probieren damit, den Container Daten.tc zu entschlüsseln. Wenn ein Versuch erfolgreich war, bricht das Skript ab und schreibt das Passwort auf den Bildschirm.

Testprogramm zum Entschlüsseln eines Containers unter Windows

```
@echo off
C:\Programme\TrueCrypt\TrueCrypt.exe /d /q /f
for /F %%i in (C:\Woerterbuch.txt) do (
C:\Programme\TrueCrypt\TrueCrypt /lt /q /v C:\Daten.tc /p %%i /s
if not errorlevel 1 (
   echo Passwort: %%i
   pause
   exit
 ) else (
   echo Test: %%i
 )
)
```

Testprogramm zum Entschlüsseln eines Containers unter Linux

```
#!/bin/bash
truecrypt -d

while read inputline
do
  Passwort="$(echo $inputline)"
  truecrypt -t -p $Passwort --non-interactive Daten.tc /mnt
  success=$?
  if [ $success -eq 0 ] ; then
     echo "erfolgreich"
     echo "Passwort: $Passwort"
     exit
  fi
done < Woerterbuch.txt
```

Selbst auf einem langsamen Computer kann man pro Sekunde 1 Passwort ausprobieren. Wenn das Skript mehrere Wochen läuft, lassen sich so problemlos ganze Wörterbücher durchtesten. Passwörter mit einer Länge von weniger als 8 Zeichen oder Passwörter, die als Name in einem Wörterbuch vorhanden sind, bieten damit praktisch keine Sicherheit. Truecrypt empfiehlt Passwörter mit einer Länge von mindestens 20 Zeichen.

Erraten des Passwortes

Ein weiterer Unsicherheitsfaktor ist, dass Benutzer dazu neigen, Passwörter zu notieren oder für verschiedene Authentifizierungen dasselbe Passwort zu verwenden. Wenn man nun weiß, dass manche Anwendungen Passwörter sogar im Klartext speichern, ist dies eine sehr praktikable und einfache Methode, an mögliche Passwörter eines Benutzers zu gelangen.

Angriffsmöglichkeiten während der Bearbeitung eines Containers

Hat ein potentieller Angreifer nur den verschlüsselten Container, sind seine Angriffsmöglichkeiten sehr beschränkt. Sie bestehen im Wesentlichen daraus, auf irgendeine Art an das Passwort zu gelangen.

Mehr Möglichkeiten bieten sich einem Angreifer, dem es gelingt, einen Computer unter seine Kontrolle zu bringen, auf dem ein Anwender einen Container öffnet: In der Auslagerungsdatei könnten sich z. B. Fragmente der vertraulichen Daten befinden. Hat ein Angreifer die Möglichkeit, einen Passwort-Sniffer zu installieren, kann er gezielt die Aktivitäten eines Benutzers mitprotokollieren. Diese Gefahr ist auch gegeben, wenn man durch Unachtsamkeit einen Trojaner oder eine andere Malware auf seinem Computer installiert. Keine Verschlüsselungssoftware kann derartige Angriffe erkennen oder verhindern. Hier kann man nur versuchen, seinen eigenen PC „sauber" zu halten.

Einsatzmöglichkeiten in der Schule

Ein Datencontainer kann auf dem lokalen Computer oder auf einem Netzlaufwerk liegen, es ist jedoch nicht möglich, dass ein Datencontainer mehrfach geöffnet wird oder von verschiedenen Personen gleichzeitig bearbeitet wird.

Die Sicherheit von Truecrypt beruht auf einem Passwort (und eventuell einem zusätzlichen keyfile). Es ist nicht möglich, wie in einer Client/Server-Umgebung unterschiedliche Berechtigungen und Authentifizierungen zu vergeben.

Diese beiden Punkte schließen den Einsatz von Truecrypt dort aus, wo Daten von unterschiedlichen Personen bearbeitet oder eingesehen werden müssen. Dafür eignen sich die klassischen Client/Server-Konzepte, bei denen die Sicherheit darauf beruht, dass niemand unberechtigt physikalischen Zugriff zum Server erhält und die Remote-Zugriffe über Berechtigungen und individuelle Authentifizierungen geregelt sind.

Wenn vertrauliche Daten jedoch nur von einzelnen Personen und zusätzlich in „unsicheren“ Umgebungen verwendet werden sollen, bietet sich der Einsatz einer Datenverschlüsselung mit Truecrypt an.

Dies ist beispielsweise immer dann der Fall, wenn Lehrkräfte vertrauliche Daten auf einem USB-Stick transportieren. Dafür eignet sich der Traveler-Modus oder auch die vollständige Verschlüsselung des mobilen Datenträgers.

Wenn ein Notebook persönliche Daten enthält, bietet es sich an, zumindest die Datenpartition zu verschlüsseln. Daneben wären auch noch weitere Sicherheitsmaßnahmen denkbar. Mit Truecrypt lässt sich auch die Systempartition verschlüsseln. Zudem bieten einige Notebookhersteller eigene Sicherheitskonzepte, bei denen die gesamte Festplatte verschlüsselt ist und auch der Start des Systems nur nach einer Authentifizierung erfolgt. Bei allen Verfahren muss jedoch immer geprüft werden, ob die Daten nach einem möglichen System-Crash noch zugänglich sind.

Für sehr wichtige und sehr vertrauliche Daten, wie z. B. bei Beurteilungen von Schülern oder Lehrern oder bei einer Sammlung persönlicher Zugangsdaten zu anderen Systemen, bietet es sich an, diese grundsätzlich in einem verschlüsselten Container aufzubewahren, der nur bei Bedarf geöffnet wird. Dieser Container kann in die normale Sicherungskette mit einbezogen werden (z. B. Sicherung auf einem Backup-Server, Sicherung auf externen USB-Festplatten, usw.). Solange das Passwort eines solchen Containers nicht bekannt wird, sind die Daten vor Missbrauch sicher.