

Merkblatt «Daten verschlüsseln»

Zusammenfassung

Oft besteht die Notwendigkeit, vertrauliche Daten gegen fremden Zugriff zu schützen. Die gängige Annahme, dass man mit einem guten Windows-Kennwort seine Daten schützen kann, ist falsch. Wenn jemand mit den richtigen Kenntnissen Zugang zu einem PC hat, gewinnt er innerhalb von ein paar Minuten Zugang zu allen Dateien, ohne Spuren zu hinterlassen.

Hier eine Liste der meistgebrauchten Verschlüsselungsmethoden:

- **Windows Encrypting File System (EFS)**. Mit diesem System können einzelne Dateien oder ganze Ordner auf einfache Weise verschlüsselt werden. Leider ist Entschlüsselung auf einem anderen PC komplex.
- **Windows BitLocker**. Mit diesem System können ganze Laufwerke verschlüsselt werden. BitLocker gibt es bloss auf den teuren Varianten von Windows 7.
- **TrueCrypt**. Dieses System ist in der öffentlichen Domäne angesiedelt. Mit ihm können Dateien oder Ordner verschlüsselt werden. Verschlüsselte Dateien können leicht auf anderen PCs gelesen werden, sofern man das Passwort kennt.

Keines dieser Systeme kann geknackt werden. Dieses Merkblatt erläutert das Verschlüsselungsprogramm *TrueCrypt*.

Bitte beachten: TrueCrypt benützt ein eigenes Kennwort, das vom Windows-Kennwort unabhängig ist. **Wenn dieses Kennwort verloren geht, dann sind die verschlüsselten Daten ebenfalls verloren**. Sie können nicht geknackt werden.

Prinzip

Nach der Installation erstellt man mit TrueCrypt einen „Dateienkorb“. Diesen Korb kann man irgendwo speichern: Auf dem Desktop, im Ordner „Eigene Dokumente“ oder auf einem externen Speicher. Gleichzeitig wählt man für diesen Korb ein gutes Kennwort. Der Korb ist nun verschlossen und kann nur mit dem Kennwort geöffnet werden.

Wenn der Korb geöffnet wird, dann erstellt TrueCrypt ein künstliches Laufwerk, z.B. Laufwerk Z:. Auf diesem Laufwerk sind sämtliche Dateien sichtbar, welche sich im Korb befinden. Sie können wie jede andere Datei geöffnet, bearbeitet und gespeichert werden.

Wenn man mit der Bearbeitung fertig ist, dann schliesst man den Korb. Das Laufwerk Z: verschwindet, und die Dateien im Korb sind nicht mehr zugänglich.

Installation

Die Installation ist einach:

1. TrueCrypt von hier herunterladen: <http://www.truecrypt.org/downloads>
2. Das heruntergeladene Programm installieren.
3. Sich überlegen, ob man die Arbeit der Programmierer mit einer Spende anerkennen will.

Herstellung eines „Korbes“

Bei der Herstellung des Korbes überlegt man zwei Dinge:

- Wo soll der Korb aufbewahrt werden. Die Wahl ist völlig frei.
- Wie gross soll der Korb sein? Seine Grösse muss ausreichen, um die zu erwartenden Dateien aufzunehmen. Erwartet man 10 MBytes, dann ist eine Grösse von 20 MBytes empfohlen, um genügend Ellbogenfreiheit zu haben.

Und so geht man bei der Herstellung des Korbes vor:

1. TrueCrypt starten.
2. Die Taste *Create Volume* klicken.
3. Den Knopf *Create an encrypted file container* wählen, dann *Next* klicken.
4. Im weissen Fenster Ort und Namen des Korbes tippen, z.B. *D:\Eigene Dokumente\Vertraulich.tc*, dann zwei Mal *Next* klicken. Die Dateierweiterung „tc“ ist nicht obligatorisch, aber empfohlen.
5. Die Grösse des Korbes festlegen, also etwa 20, dann den „MB“-Knopf klicken. Anschliessend *Next* klicken.
6. Das gewünschte Kennwort tippen. Bitte beachten: **Wenn dieses Kennwort verloren geht, dann sind die verschlüsselten Daten ebenfalls verloren.**
7. Die Taste „Format“ klicken. TrueCrypt wird sich melden, wenn der Korb formatiert ist.
8. Die Tasten *Next* und *Exit* klicken.

Der Korb ist jetzt bereit zum Gebrauch.

Eine Bemerkung zum Thema Passwort: Passwörter wie *er5(aX9!* sind zwar schwer zu knacken, aber für Menschen noch viel schwieriger zu merken. Andererseits ist ein Pass-Satz wie *?WarumKochstDuDeinFahrradAmSamstag* leicht zu merken, aber noch viel schwieriger zu knacken. Der Grund ist einfach: Es gibt bloss etwa 80 unterschiedliche Buchstaben und Zeichen, aber mehrere Tausend Wörter. Zu vermeiden sind allerdings Passsätze wie *MeinNameIstEugen*.

„Korb“ öffnen

Um die verschlüsselten Dateien zu öffnen, muss man erst den Korb öffnen.

1. Den Namen der Korbdatei doppelt klicken.
2. Das gewünschte Laufwerk klicken, z.B. Laufwerk Z:.
3. Die Taste *Mount* klicken.
4. Das Kennwort eintippen, dann *OK* klicken.
5. Die Dateien im Korb sind jetzt auf Laufwerk Z: sichtbar.

„Korb“ schliessen

Um den Zugang zu den verschlüsselten Dateien zu sperren, geht man so vor:

1. Alle Dateien, die sich im Korb befinden, schliessen.
2. TrueCrypt starten.
3. Auf die Taste *Dismount* klicken.

Der Korb ist jetzt geschlossen und kann nur noch mit dem richtigen Kennwort geöffnet werden. Der Korb wird übrigens automatisch geschlossen, wenn man sich von Windows abmeldet.

Daten austauschen

Körbe können ohne weiteres mit anderen Leuten ausgetauscht werden, z.B. per EMail. Die Grösse des Korbes beachten! Es ist natürlich zwingend notwendig, dass der Empfänger das Kennwort kennt.