Festplatten verschlüsseln mit TrueCrypt

16. Januar 2013

Verschlüsseln bedeutet, dass man Informationen bzw. Daten nicht als Klartext sondern codiert, verschlüsselt also so speichert, dass ein Fremder Sie nicht ohne weiteres lesen kann. Jeder und jede, der schon einmal einen USB-Stick verloren hat oder dem sein Laptop abhanden gekommen ist kennt die Sorge, wer sich wohl nun über die dort befindlichen Daten hermacht.

Um so etwas zu verhindern, kann man die Festplatte seines Computers, USB-Sticks, SD-Speicherkarten usw. ganz oder teilweise verschlüsseln. Nur mit Wissen des Passworts kommt man an die Daten heran. Je länger ein Passwort ist, umso sicherer ist es. Passwörter, die nicht nur aus einem Wort bestehen nennt man auch *Passphrase*. Zur guten Wahl eines Passworts oder einer Passphrase gibt es ein eigenes Kapitel. Folgende drei wichtige Hinweise noch:

1. Keine Verschlüsselung kann 100%ige Sicherheit bieten, erst recht nicht mit dem Voranschreiten der IT-Entwicklung. Was vor fünf oder zehn Jahren noch als sicher verschlüsselt galt, kann heute zum Teil mit mehr oder weniger Aufwand geknackt werden. Das sollte man stets im Hinterkopf behalten, sich aber davon auch nicht abhalten lassen, seine Daten zu schützen.
2. Jede Verschlüsselung ist nur so sicher wie das verwendete System. Sofern man die Wahl hat sollte man immer dann hochwertige Verschlüsselungsverfahren einsetzen, solange die damit verbundene höhere Rechenzeit kein wesentlicher Gesichtspunkt ist.
3. Ist das Passwort (Passphrase) weg, sind die Daten weg. Also gut merken. :)

Was ist TrueCrypt?

TrueCrypt ist ein (relativ) freies und kostenlos verfügbares Computerprogramm, das die Verschlüsselung von ganzen oder teilweisen Speichermedien ermöglicht. Es gibt neben TrueCrypt weitere Programme, die dieses ebenfalls leisten. Auf Vor- und Nachteile gehen wir hier nicht ein und besprechen nur das Arbeiten mit TrueCrypt.

TrueCrypt erlaubt es sowohl ganze System-Festplatten von Computern im Nachhinein zu verschlüsseln, ermöglicht aber auch das Verschlüsseln externer Speichermedien (Festplatten, USB-Sticks, Speicherkarten etc.) und unterstützt das Anlegen von so genannten *Containern*. Das sind Teile von Speichermedien, die verschlüsselt sind. So kann man also z.B. auf einem USB-Stick einen Container anlegen, der sich nach außen als einfache und nicht-lesbare Datei darstellt, der aber tatsächlich eine oder mehrere verschlüsselte Dateien enthalten kann.

Als besonderen Trick erlaubt TrueCrypt zudem noch die Einrichtung unsichtbarer Container. Das bedeutet, dass dieser verschlüsselte

Bereich beim Aufrufen des Inhaltsverzeichnisses gar nicht auftaucht. Nur wenn man weiss, dass sich ein solcher Container auf dem Speichermedium befindet und zudem das Password kennt, kommt an diese Daten heran.

Installation von TrueCrypt

Zur Installation die Homepage von TrueCrypt aufrufen und die je nach System (Windows, Mac OS X, Linux) herunterladen und installieren. TrueCrypt ist ein eigenes Programm, das man starten muss, um damit zu arbeiten.

`www.truecrypt.org`

Computer-Festplatte vollständig verschlüsseln

(Siehe auch GPF-Privacy-Handbuch Kapitel 11.2.6)

Man kann (bei normalen, einfachen Rechnersystemen!) die Festplatte seines Computers vollständig verschlüsseln. Startet man danach den Rechner neu, wird man zur Eingabe der vorher angegebenen Passphrase aufgefordert. Ohne die korrekte Eingabe startet der Rechner nicht hoch.

WICHTIG: Sobald und solange der Rechner eingeschaltet ist und ein Benutzerkonto geöffnet wurde, ist jedem an der Tastatur sitzenden alles wie sonst gewohnt und üblich. Das bedeutet: Trojaner oder andere Spähsoftware oder auch fremde Bediener können die Daten dann einsehen und abrufen. Die Verschlüsselung schützt nur dann gegen unberechtigten Zugriff, wenn der Computer heruntergefahren ist und in diesem ausgeschalteten Zustand in falsche Hände gerät!

Vorgehensweise:

- Systempartition im Auswahlfenster anwählen (bei Windows meistens **C:**) und **Create Volume** anklicken.
- **Encrypt the system partition or entire system drive** anwählen und weiter.
- **Single Boot** anwählen, sofern man keine komplexer partitionierte Festplatte besitzt und weiter.
- Verschlüsselungsalgorithmus auswählen und weiter.
- Bestätigen der Verschlüsselung des gesamten Volumens mit **Next**.
- Passphrase eingeben und weiter.
- Eine Weile lange den Mauszeiger irregulär bewegen, damit ein möglichst zufälliger Schlüssel generiert wird und mit **Format** bestätigen.

- Weitere Sicherheitsabfragen bestätigen, die Formatierung beginnt.
- Die Datei für eine Rettungs-CD erzeugen lassen (ISO-Image der Rescue Disk) und später als CD brennen. Diese CD kann hilfreich und rettend wirken, falls das initiierende Startprogramm der Festplatte (Boot Loader) einmal kaputt gehen sollte.
- Fertig

WICHTIGER HINWEIS: Das Verschlüsseln kann je nach Größe von Festplatte mehrere Stunden lang dauern. Das ist nicht ungewöhnlich. Von daher bietet sich das Durchführen des Verschlüsselungsprozess für einen Zeitpunkt an, an dem man den Rechner für diese längere Zeit nicht nötig hat.