Thomas Möhle

Handout zum Fachgespräch vertrauliche Kommunikation im Deutschen Bundestag am 03.09.2013

Session 1
Festplatten- und Dateiverschlüsselung

Um Daten auf Computern vor unbefugtem Zugriff zu schützen, kann man sie verschlüsseln. Nur der Inhaber des Schlüssels (in Form eines Passworts oder einer kleinen Datei) kann dann auf die verschlüsselten Daten zugreifen.

Im täglichen Alltag, gerade bei Laptops, sind eine ganze Reihe von Szenarien denkbar, in denen die Verschlüsselung erwogen werden sollte. Verloren gegangene Laptops oder USB-Speichersticks sind keine Seltenheit und selbst wer noch nicht der Schusseligkeit erlegen ist, ist vor Diebstahl nicht gefeit. Dabei sind auch schnell Dokumente betroffen, die nicht für Dritte bestimmt sind. Es empfiehlt sich also, mindestens diese Dokumente, besser noch die komplette Festplatte zu verschlüsseln.

Auch im laufenden Betrieb des Computers kann für die Daten allerdings eine Gefahr entstehen, wenn Schnüffelprogramme von Kriminellen oder neugierigen Regierungsinstitutionen die Festplatte im eingeschalteten Zustand durchsuchen. Davor schützen dann verschlüsselte Container, die während des konkreten Bedarfs entschlüsselt werden und ansonsten verschlüsselt und verschlossen die darin enthaltenen Daten sicher aufbewahren.

Methode 1 - Festplattenverschlüsselung:

Mit der Verschlüsselung der kompletten Festplatte („Full-Disk-Encryption“) ist es möglich, die Daten eines ausgeschalteten Computers vor fremdem Zugriff zu schützen.

Möglichkeiten zur Festplattenverschlüsselung bietet **FileVault** auf dem Mac, sowie **Bitlocker** unter Windows. Letzterem ist allerdings in vielen Fällen das Open-Source Programm **TrueCrypt** vorzuziehen.

Alle genannten Varianten lassen sich aus dem laufenden Betrieb heraus anstoßen und bedürfen keiner frischen Installation des Betriebssystems.

Methode 2 - Dateiverschlüsselung:

Mit der Verschlüsselung einzelner Dateien auf dem Computer ist es möglich, diese auch im eingeschalteten Zustand des Computers vor fremden Zugriffen und laufender (Schad-)Software zu schützen. Auch USB-Speichersticks, die häufig verloren gehen, sollten wichtige Daten nicht unverschlüsselt aufbewahren. Auch für diesen Zweck ist **TrueCrypt** die Anwendung der Wahl.

Mit TrueCrypt erstellt man dazu zunächst eine verschlüsselte Container-Datei („Volume“), deren Größe man im Vorfeld festlegt. Diese Datei kann dann ins Betriebssystem, wie eine Festplatte, eingebunden werden und mit Daten gefüllt werden. Das ein- und ausklinken des Containers („mounten“ und „unmounten“) aus dem Betriebssystem ermöglicht, dass die Daten immer nur für den jeweiligen Zeitraum unverschlüsselt verfügbar sind.