Truecrypt – verschlüsselte Ablage sensibler Daten

Manuel Selling | Computer- und Medienservice, Systemsoftware und Kommunikation | Manuel.Selling@cms.hu-berlin.de

Heutzutage ist es unumgänglich, schützenswerte Daten zu verschlüsseln, um einen ungewollten Zugriff bei Verlust oder Missbrauch zu verhindern, insbesondere wenn man mit einem Notebook oder USB-Stick unterwegs ist. Sobald man also zu dieser Erkenntnis gekommen ist, stellt sich die Frage, mit welchen Hilfsmitteln man seine Daten verschlüsseln kann und welche Tools sicher und leicht zu bedienen sind. Aus der Vielzahl der Anbieter und Software soll hier die Verschlüsselungssoftware Truecrypt vorgestellt werden, welche sich durch ihre Zuverlässigkeit und ihre Bedienbarkeit hervorhebt. Außerdem ist sie kostenlos erhältlich.

Truecrypt (aktuell in der Version 5.1a) ist ein vielseitiges Open-Source-Verschlüsselungstool, welches es ermöglicht, Daten, Festplatten und Systempartitionen komfortabel, sicher und einfach zu verschlüsseln. Es ist für die gängigsten Betriebssysteme (Windows, Mac, Linux) erhältlich und steht kostenlos zum Download auf der Webseite bereit. Es existiert eine sehr aktive Community, die stark an der Weiterentwicklung und Verbesserung von Truecrypt beteiligt ist (z. B. vier Releases der Software in den ersten 3 Monaten diesen Jahres).

Die Software deckt mit ihrem Funktionsumfang fast sämtliche Szenarien des sicheren Umgangs mit sensiblen Daten ab. Im Folgenden werden kurz die einzelnen Features beschrieben, um die Möglichkeiten der Software und deren Einsatzgebiete zu skizzieren. Die Wahl des Betriebssystems fiel auf Windows Vista Business, da sich unter Windows die Funktionalität von Truecrypt voll entfaltet.

Die Wahl der Installation

Wenn man sich also die aktuelle Version von der offiziellen Homepage heruntergeladen hat, steht man vor der Entscheidung, ob man die Software installieren oder ob man sie ohne Installation betreiben möchte. Truecrypt bietet für die zweite Möglichkeit den sogenannten „Traveler Mode“ an, der es ermöglicht, die Anwendung ohne Installation direkt aus dem Programmverzeichnis zu starten. Hierfür muss man entweder bei der Installation den „Extract-Mode“ wählen oder nach der Installation über das Menü „Tools → Traveler Disk Setup“ ein entsprechendes Verzeichnis erzeugen. Nachteil des Traveler-Modus ist, dass er nur mit administrativen Rechten auf dem entsprechenden Windows-System läuft. Der Traveler-Modus ist zu empfehlen, wenn verschlüsselte USB-Sticks oder externe Festplatten an einem anderen Rechner angeschlossen werden, auf dem Truecrypt nicht installiert ist. Hat man sich für die Installation entschieden, können weitere Nutzer des Rechners – ohne administrative Berechtigung – die Anwendung benutzen.

Die Funktionen

Truecrypt bietet dem Nutzer drei verschiedene Verschlüsselungsalgorithmen (AES → Rijndael, Serpent, Twofish) an, die auch untereinander kombiniert werden können. Serpent gilt als sehr sicher, ist aber im Gegensatz zu den anderen Algorithmen der langsamste. Etwas schneller ist der Twofish-Algorithmus, er gilt ebenfalls als sehr sicher. Ein ausgewogenes Ergebnis hinsichtlich der Sicherheit und Performance bietet der AES (Advanced Encryption Standard)-Algorithmus. Dieser wurde offiziell von der US-Regierung zum Schutz von vertraulichen Dokumenten der höchsten Geheimhaltungsstufe zugelassen.

Nach dem Start von Truecrypt hat der Nutzer mehrere Möglichkeiten, seine Daten zu verschlüsseln, die, je nach Anforderung, gewählt werden sollten.

1. Container

Sollen nur einzelne Dateien oder Verzeichnisse verschlüsselt werden, können sogenannte Container angelegt werden, die die Dateien aufnehmen können. Die Definition der Container fragt die wichtigsten Eckdaten ab, wie z. B. welche Größe der Container haben soll (hierbei sollte man großzügig sein, da die Größe im Nachhinein nicht geändert werden kann), mit welchem Algorithmus verschlüsselt, welches Dateisystem genutzt und mit welchem Passwort und/oder Keyfile verschlüsselt werden soll. Nutzer, die über keine administrativen Berechtigungen verfügen, können als Dateisystem nur FAT auswählen, welches die maximale Größe von Dateien auf 4 GB beschränkt.

Mit der Angabe von Keyfiles (beliebige Dateien oder Verzeichnisse) kann man die Verschlüsselung wieder ein Stück sicherer machen, denn nur mit den entsprechenden Keyfiles und dem vergebenen Passwort ist ein Zugriff auf die verschlüsselten Daten möglich. Die Keyfiles sollten daher immer gesichert werden, da bei Verlust kein Zugriff mehr möglich ist. Zum Verschlüsseln benutzt Truecrypt nicht direkt das Passwort/Keyfile, sondern erzeugt lange und zufällige Schlüssel, die mit Hilfe von Mausbewegungen gebildet werden.

2. Partitionen

Als zweite Option besteht die Möglichkeit, ganze Partitionen zu verschlüsseln. Diese werden neu formatiert und mit den gleichen Methoden verschlüsselt wie die Container. Hat man vor, große Dateien (über 4 GB) zu speichern, sollte bei der Formatierung NTFS gewählt werden. Bei den beiden bisher genannten Optionen der Verschlüsselung hat man außerdem die Möglichkeit, sogenannte „Hidden Volumes“, also versteckte Container, anzulegen, die im freien Speicherbereich von schon erzeugten und verschlüsselten Containern eingefügt werden. Wird man z. B. zur Herausgabe des Passworts für den verschlüsselten Container gezwungen, so kann man nur den äußeren Container entschlüsseln, der z. B. unwichtige Daten enthält. Der Angreifer ahnt indes nicht, dass sich im entschlüsselten Container noch ein versteckter Container befindet.

3. Systempartition (Windows)

Als dritte und letzte Option kann man mit der neuen Version von Truecrypt (5.1a) unter Windows die Systempartition verschlüsseln. Es ist somit also nicht mehr möglich, Windows ohne die Eingabe des richtigen Passworts zu booten (Pre-Boot-Authentisierung). Ein Zugriff über ein gebootetes Live-System ist somit auch nicht mehr möglich, da die Partition verschlüsselt ist. Als Auswahl steht hier die Verschlüsselung der Windows-Partition oder des gesamten Laufwerkes zur Verfügung. Logische Laufwerke in erweiterten Partitionen werden von der aktuellen Version (noch) nicht unterstützt.

Hat man die Verschlüsselung der gesamten Festplatte gewählt, werden noch Informationen zu der Anzahl der installierten Betriebsysteme (Single-boot oder Multi-boot) und zum Verschlüsselungsalgorithmus eingeholt. Danach erfolgt die Eingabe des Passworts. Eine Angabe von Keyfiles ist zu diesem Zeitpunkt nicht möglich. Vor der Verschlüsselung wird noch eine Rescue Disc angelegt, ein bootfähiges CD-ISO-Image, was den Bootloader sowie den Volume-Header (beinhaltet die verwendeten Schlüssel) enthält. Dieses Image muss man zuerst auf eine CD brennen, erst dann startet der Assistent die Verschlüsselung der Festplatte. Die Rescue Disc sollte gut gesichert werden da ohne sie, bei einem beschädigten System kein Zugriff auf die verschlüsselten Daten möglich ist.

Handhabung

Die zuvor erzeugten verschlüsselten Container/Partitionen (außer der verschlüsselten Systempartition) können zu jeder Zeit und nach Bedarf in das laufende System eingehängt (Mount) bzw. ausgehängt werden (Dismount).

Dafür startet man Truecrypt, wählt einen geeigneten Laufwerksbuchstaben und den entsprechenden Container/Partition aus und hängt diesen mit Betätigung des „Mount“-Schalters und nach Eingabe des Passwortes/Keyfile in das laufende System ein (Abb. 1). Danach erscheint ein neues Laufwerk im Windows-Explorer, das die im Container

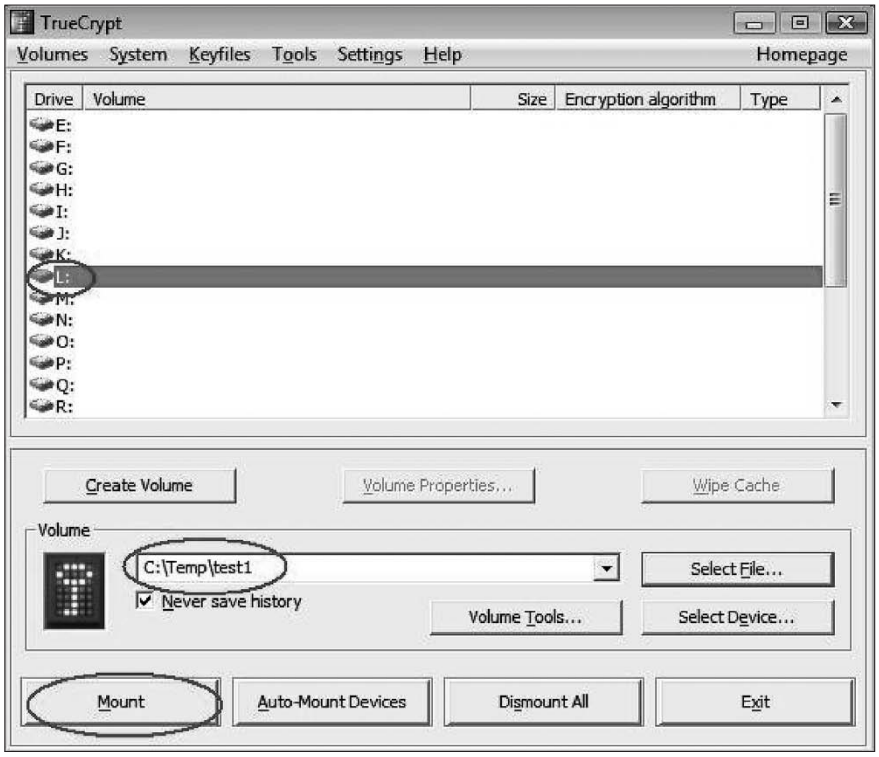

Abb. 1: Auswahl Container, Laufwerksbuchstabe und „Mount“-Befehl

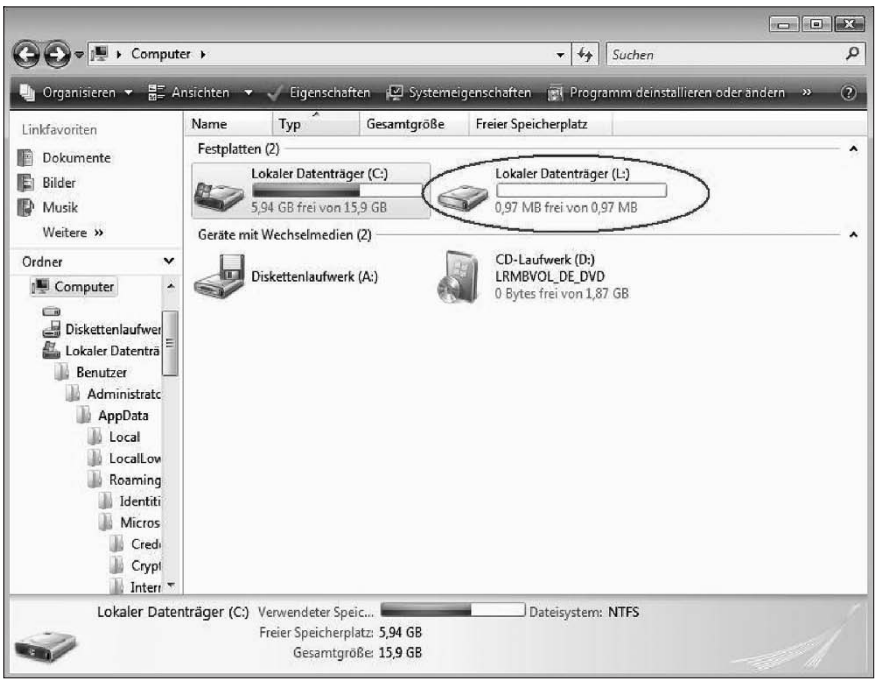

Abb. 2: Eingebundener Container als Laufwerk L:

verschlüsselten Daten zur Bearbeitung bereitstellt (Abb. 2). Nach der Arbeit mit dem eingebundenen Laufwerk lässt sich dieses einfach durch Betätigung des „Dismount"-Schalters aus dem laufenden System aushängen.

Fazit

Truecrypt in der aktuellen Version ist eine sehr gute Wahl, um sensible Daten zu verschlüsseln und somit zu schützen. Es bietet viele Funktionen und ist durch den Einsatz zahlreicher Assistenten leicht und intuitiv zu bedienen. Eine Schnittstelle zur Kommandozeile ist ebenfalls vorhanden, was eine skriptgesteuerte, automatisierte Verwendung von Truecrypt zulässt.

Ein Nachteil ist, dass nur die Verschlüsselung der Systemfestplatte momentan den größtmöglichen Schutz der Daten bietet. Bei einer Verschlüsselung von einzelnen Daten muss man davon ausgehen, dass Windows Teile davon im Klartext in irgendwelche temporären Dateien, Auslagerungsdateien oder Speicherabbilder (im Ruhezustand) schreibt. Ich gehe aber davon aus, dass diese Schwachstelle in einer der nächsten Versionen behoben wird. Nach einem vom Fraunhofer-Institut und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegebenen Leitfaden zur Bitlocker Festplattenverschlüsselung (nur in bestimmten Versionen von Windows Vista) stellt Truecrypt eine „ernstzunehmende Alternative" dar, die sich nur noch in der "fehlenden TPM-Unterstützung" unterscheidet. Leider ist zurzeit noch keine Smartcard-Unterstützung implementiert (siehe Artikel „Verwendung von Zertifikaten zur Erhöhung der Sicherheit von PCs" in diesem Heft).

Die Tatsache, dass der Quellcode für alle einsehbar ist und somit Schwachstellen schneller identifiziert werden können, ist für mich ein entscheidender Vorteil gegenüber anderen kommerziellen Verschlüsselungslösungen (z. B. Safe Guard Private Disk, Bitlocker von Microsoft), die den Quellcode nicht veröffentlichen. Auch die Plattformunabhängigkeit von Truecrypt ist ein wesentlicher Vorteil, was die Möglichkeit bietet, unabhängig vom Betriebssystem mit verschlüsselten Daten zu arbeiten.

Literatur

[1] *Offizielle Homepage.* http://www.truecrypt.org/

[2] *Tutorial: Mit TrueCrypt ganze Partitionen verschlüsseln.* http://www.netzwelt.de/news/77155-tutorial-mit-truecrypt-ganze-partitionen.html

[3] *TrueCrypt Windows-Bedienungsanleitung.* http://www.fz-juelich.de/jsc/sicherheit/download/freeware.1/truecrypt/pc/zam-doc/truecrypt-zam.htm#KAP7

[4] *Wikipedia: Truecrypt.* http://de.wikipedia.org/wiki/TrueCrypt

[5] *Advanced Encryption Standard.* http://de.wikipedia.org/wiki/Rijndael

[6] *Twofish.* http://de.wikipedia.org/wiki/Twofish

[7] *Serpent.* http://de.wikipedia.org/wiki/Serpent_%28Verschl%C3%BCsselung%29

[8] *Sicher aufbewahrt – Datenverschlüsselung unter Windows 2000 und XP Home nachgerüstet.* http://www.heise.de/mobil/Datenverschluesselung-unter-Windows-2000-und-XP-Home-nachgeruestet--/artikel/58723/0

[9] *TrueCrypt-Anleitung.* http://www.fixmbr.de/truecrypt-anleitung/

[10] *BitLocker Drive Encryption im mobilen und stationären Unternehmenseinsatz (Leitfaden Fraunhofer-Institut Sichere Informationstechnologie).* http://testlab.sit.fraunhofer.de/content/output/project_results/bitlocker/