Datensicherheit mit TrueCrypt

Mit verschlüsselten Laufwerken sicher unterwegs

Die verschlüsselte Speicherung aller Worddokumente, Exceltabellen oder sonstigen Datendateien funktioniert erfahrungsgemäß nur, wenn sie automatisch ohne Zutun des Anwenders geschieht. Mit der kostenlosen Software TrueCrypt steht eine komfortable Open-Source-Anwendung zur Verfügung, die es erlaubt, unter Windows und Linux mit verschlüsselten Laufwerken zu arbeiten.

Gerade auf mobilen Datenträgern, die das Unternehmen verlassen, sollten personenbezogene und andere vertrauliche Daten so gespeichert werden, dass ein Verlust des Datenträgers keinen Schaden durch Kompromittierung der Daten verursacht.

Solche Datenträger sind Festplatten in Notebooks, aber auch Disketten, USB-Sticks, USB-Festplatten, CDs oder DVDs. Hier hilft nur eine konsequente Verschlüsselung.

Mit TrueCrypt bequem verschlüsselte Laufwerke erstellen

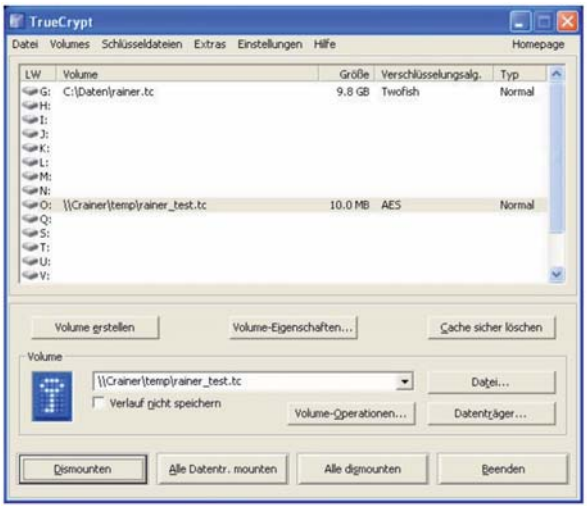
Mit TrueCrypt lässt sich ein Laufwerk über eine Container-Datei oder eine eigene Partition erstellen. Die Partition z.B. eines USB-Sticks kann so komplett verschlüsselt werden. Container-Dateien lassen sich beliebig kopieren und transportieren. Sie dürfen auf Netzwerklaufwerken liegen und können auf CD/DVD gebrannt werden.

Ohne Passwort kein Zugang

Zugang zum Laufwerk verschafft ein Passwort, eine Schlüsseldatei oder eine Kombination aus beiden. Als Schlüsseldatei kann jede Datei fungieren. Sie wird nicht verändert, sondern ihr Bitmuster wird lediglich mit dem Passwort vermischt. Ist die Schlüsseldatei defekt, ist das verschlüsselte Laufwerk nicht mehr zugänglich.

Für Reisende ist die Verschlüsselung ohne Installation sehr praktisch

TrueCrypt unterstützt einen Traveller-Mode, um verschlüsselte Datenträger zu benutzen, ohne die Software zu installieren. Prinzipbedingt benötigt der User hierfür Administratorprivilegien, da er vorübergehend einen Treiber ins System bringen muss.



Das Hauptfenster von TrueCrypt 4.2. Hier werden Laufwerke erstellt, angemeldet und wieder abgemeldet.

Über einen Menüpunkt lässt sich eine Traveller-Disk erstellen. Sie enthält alles, was zum Umgang mit verschlüsselten Laufwerken nötig ist (ca. 1,6 MB). Soweit vom Betriebssystem unterstützt, lässt sich über den Autostart-Mechanismus das Laufwerk sogar automatisch beim Einlegen des Datenträgers starten.

Verbesserungspotenzial bei der Nutzung unter Linux und bei Chipkarten

Das aktuelle TrueCrypt unterstützt Windows 2000, Windows XP, Windows 2003 Server und Linux ab Kernel 2.6.5. Ab Version 4.2 können nun auch endlich unter Linux verschlüsselte Laufwerke erstellt werden. Lediglich ein GUI fehlt noch für Linux.

Während beim Wechsel in den Ruhezustand alle angemeldeten Laufwerke automatisch abgemeldet werden können, müssen bei der Wiederanmeldung aus dem Ruhezustand die Laufwerke explizit wieder angemeldet werden.

Auch gibt es bislang keinen Support für Chipkarten.

Bewertung des Tools

Truecrypt ist ein erstklassiges und kostenloses Werkzeug, um auf Notebooks Daten verschlüsselt zu speichern. Dabei sind eine Programmpartition und eine verschlüsselte Datenpartition sicherlich die beste Lösung. Eine sorgfältige Planung des Einsatzes schützt vor Datenverlust durch vergessene Passwörter.

Sie können dieses Tool unter *www.datenschuetzer.de* herunterladen oder unter *www.truecrypt.org*.

Das Tool ist nicht für den Unternehmenseinsatz geeignet, aber z.B. für den Außendienstler mit Notebook

Die Zielgruppe ist eindeutig der Endanwender. Deshalb fehlen viele der ausgefeilten Unternehmens-Funktionalitäten anderer Produkte, wie z.B. Daten-Recovery-Unterstützung, falls der Mitarbeiter sein Passwort vergisst. Hier hilft nur ein rechtzeitiges Backup.

Prof. Dr. Rainer W. Gerling