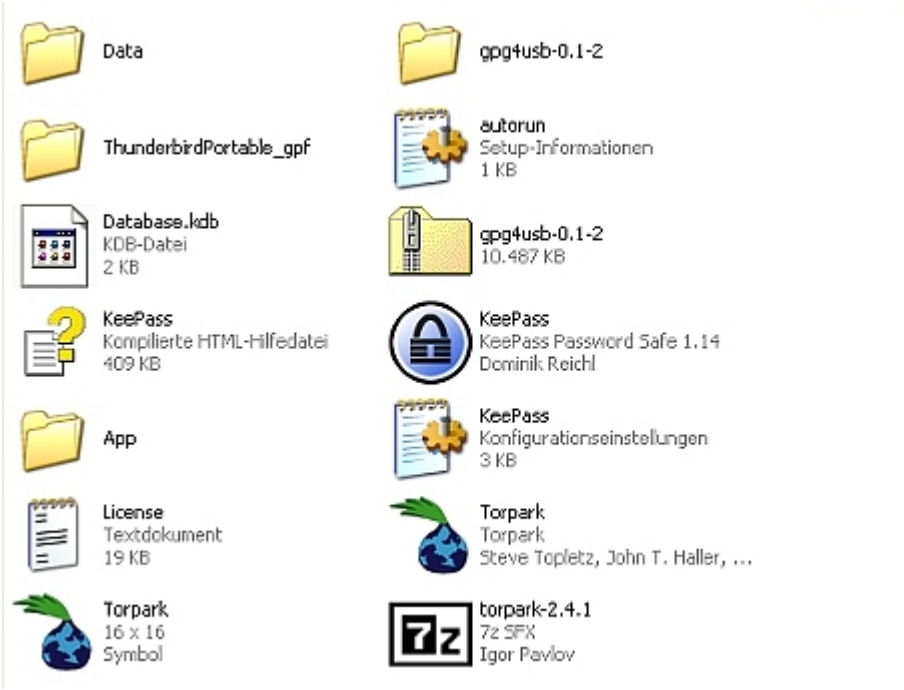
Ein einfaches Sicherheitskonzept für Daten



In den letzten Tagen habe ich mir Gedanken darüber gemacht, wie man sich davor schützt,. dass die eigenen Daten bei einer Beschlagnahme der Rechner in „falsche Hände“ geraten. Der Anlass ist den wohlwollenden Leserinnen und geneigten Lesern bekannt. Man muss davon ausgehen, dass Richter und Staatsanwälte das Thema „Computer“ wie der sprichwörtliche dümmste anzunehmende User behandeln. Sie glauben im Ernst, man könne Daten auf Rechnern finden, wenn man danach sucht. Eine erpresserische Methode ist, die gesamte Hardware zu beschlagnahmen und diese nach zwei Jahren zurückzugeben, wenn die Gerichte die Maßnahme für illegal erklärt haben.

Ein Sicherheitskonzept muss einfach sein, sowohl für Windows als für Linux (mit Apple kenne ich mich nicht so gut aus) funktionieren und garantieren, dass die Daten, die man benötigt, sowohl sicher als auch jederzeit verfügbar sind. Ich meine, dass ich ein Konzept gefunden habe. Es kostet so viel wie ein USB-Stick – ich habe heute einen für elf Euro gekauft (acht Gigabyte).

Erstens: Mein Linux-Rechner ist komplett mit dem alternate Desktop verschlüsselt. Man kommt also gar nicht mehr an die Daten heran. Das Passwort ist lang genug und nirgendwo aufgeschrieben. Falls dieser Rechner beschlagnahmt würde, bekäme ich ihn nie wieder – aber die Ermittler könnten auch nichts mit ihm anfangen.

Zweitens: Der alte Windows-Rechner, den ich zur Zeit nur für Second Life und eventuell andere virtuelle Welten nutze, enthält keine sensible Daten. Für die Verschlüsselung der Festplatte nutze ich Truecrypt (Screenshot unten).

Drittens: Auf dem USB-Stick habe ich zwei Ordner, einen für Linux und einen für Windows (vgl. Screenshot oben). Der Windows-Ordner enthält das E-Mail-Programm ThunderbirdPortable und eine Kopie meiner Schlüsselbünde. Ich kann also den Stick in jeden beliebigen Rechner stecken, auch in einem Internet-Cafe, und habe immer meine E-Mails (Voreinstellung natürlich IMAP). Dazu habe ich den Torpark vom PrivacyDongle auf dem Stick installiert. Ich führe also immer einen eigenen Hochsicherheitsbrowser bei mir – mit den empfehlenswerten Erweiterungen NoScript, CookieSafe und No-Referer – alle drei sowohl für Windows als auch für Linux. Ich hinterlasse beim Surfen also keine Datenspuren.

Auf dem Stick habe ich auch noch andere Daten gesichert, zuzüglich die verschlüsselten Passwort-Daten für Revelation (Passwort-Manager für Gnome/Linux) als auch KeePass Password Safe (Passwort-Manager für Windows). Dazu sowohl für Linux als auch für Windows das auf Burks‘ Blog schon empfohlene GPG4USB. Alle genannten Programme sind einfach zu installieren und zu nutzen, auch für Computer-Laien. Den USB-Stick kann man vor einer Hausdurchsuchung verstecken – eine Leibesvisitation ist nicht immer inklusive.

Wenn alle meine Rechner beschlagnahmt würden, hätte ich in wenigen Stunden alle meine Daten wieder zur Verfügung und könnte einfach weiterarbeiten. Eine Beschlagnahme kostet also

nur“ die Hardware, und das „Ergebnis“ wäre für die Ermittler gleich null. Nicht zu vergessen: Adressen und Termien verwalte ich auf meinem Server mit eGroupware – also über ein WWW-Interface. Wer Fragen und Tipps dazu hat, sollte hier gleich kommentieren.