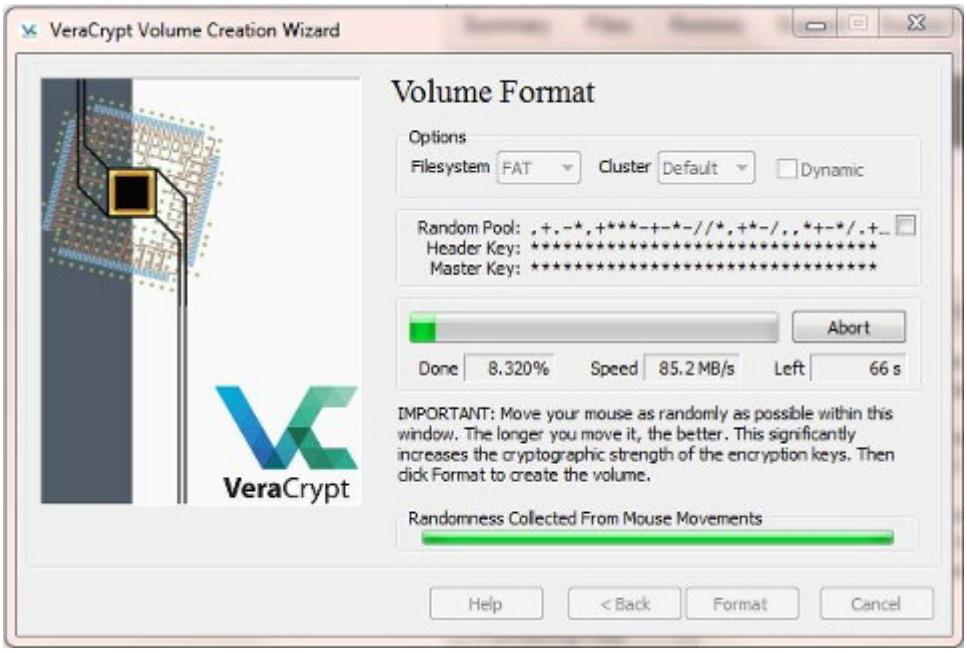
Veracrypt



Ich habe jetzt alle meine Rechner auf Veracrypt (Version 1.19) umgestellt.

Für Windows ist die Installation selbsterklärend und identisch mit der von Truecrpyt. Bei Linux muss man auf die Kommandozeile:

```
$ sudo add-apt-repository ppa:unit193/encryption
$ sudo apt-get update
$ sudo apt-get install veracrypt
```

Der Verein German Privacy Fund bietet zwar immer noch Truecrypt an, aber empfiehlt jetzt auch Veracrypt. (By the way: der GPF hat einen neuen PGP-Schlüssel.)

Burks‘ Patchday oder: Immer ist irgendetwas (update: mit Ventrilo) [Update]

An meinem letzten freien Wochenende habe ich mich entschieden, nur notwenige, aber eigentlich überflüssige Dinge zu tun – anstatt etwas etwas Sinnvolles zu schreiben zum Beispiel. Vier Rechner, das heisst jeweils zwei Linux- und zwei Windows-7-Partitionen updaten und synchronisieren (inklusive der Truecrpyt-Container), dazu das Laptop (Windows 10 mit unüberwindbarem UEFI) und das Netbook mit Ubuntu. (Vom Tablet und dessen Android rede ich jetzt nicht.)

Mit Linux gibt es selten Probleme, aber Windows bringt mich jedesmal zum Wahnsinn. Immer ist irgendetwas. Dass ich fast bei jedem Hochfahren unzählige Programme per Hand updaten soll, ist nicht neu: Openoffice, Libreoffice, Filezilla, Thunderbird (in einem Truecrpyt-Container, deswegen auch per Hand) usw.. Heute kam bei einem Rechner dazu: Das Aufgabenabbild ist beschädigt oder wurde verfälscht.

Nicht genug, dass man sich durch fünf Jahre alte Forumsbeiträge wühlen muss, um das Problem zu lösen – es funktioniert auch nichts wirklich. Immerhin hatte ich nach

einer halben Stunde verschwendeter Lebenzeit kapiert, woran es ungefähr lag. Guckst du C:\Windows\System32\Tasks\Microsoft\Windows\WindowsBackup, löschst du den Ordner und erstellst einen neuen, der leer ist. Voila.

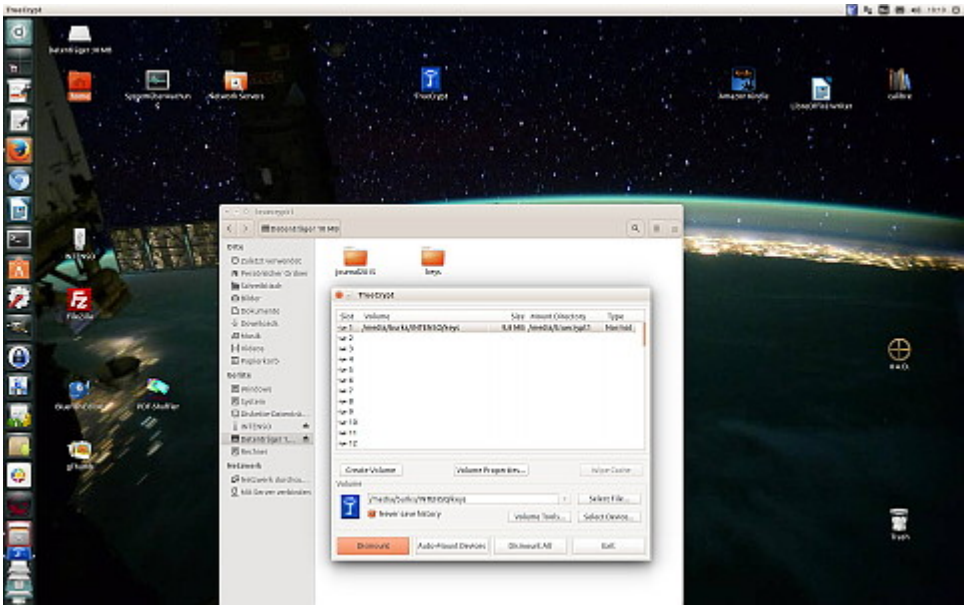
By the way: Die Leuchte über dem Klavier habe ich umfunktioniert, falls das jemanden interessiert, weil ich mehr lese als Klavier spiele. Man muss seine Ressourcen im Alter gut einteilen.

Ach ja. Kennt sich jemand mit der Konfiguration eines Ventrilo-Servers aus? Bringt mich auch zum Verzweifeln (für Secondlife natürlich, zum gemeinsam rumballern). Ich habe für sehr wenig Geld einen Voiceserver (10 Slots) bei einem einschlägigen Anbieter gemietet.

Ein US-Amerikaner schickte mir einen Link zu einer angeblich idiotensicheren Anleitung. Aber mein Ventrilo will einfach nicht mit dem Server connecten, obwohl das Setup korrekt eingestellt ist. Kann es sein, dass mein Router nicht mitspielt und ich bei dem noch ein Türchen öffnen muss?

[Update] Offenbar muss man das, es funzt aber trotzdem nicht. Ich habe nach dieser Anleitung die richtigen Ports auf meinem Router freigegeben, Ventrilo verbinde sich immer noch nicht mit dem Server.

Truecrypt mit Linux, reloaded



Mir geht es so wie den meisten Leute: Erst wenn ich etwas wirklich brauche, beschäftige ich mich damit, zumal wenn ich das Thema schon genügend zu kennen glaube.

Morgen fahre ich in den Ruhrpott – inne Heimat, wie man dort zu sagen pflegt. Da ich eine Woche Pause von Secondlife machen will, brauche ich nur mein Netbook mitnehmen, auf dem Ubuntu läuft. (In Unna ist erst recht Neuland-Entwicklungsland, was die Geschwindigkeit angeht.)

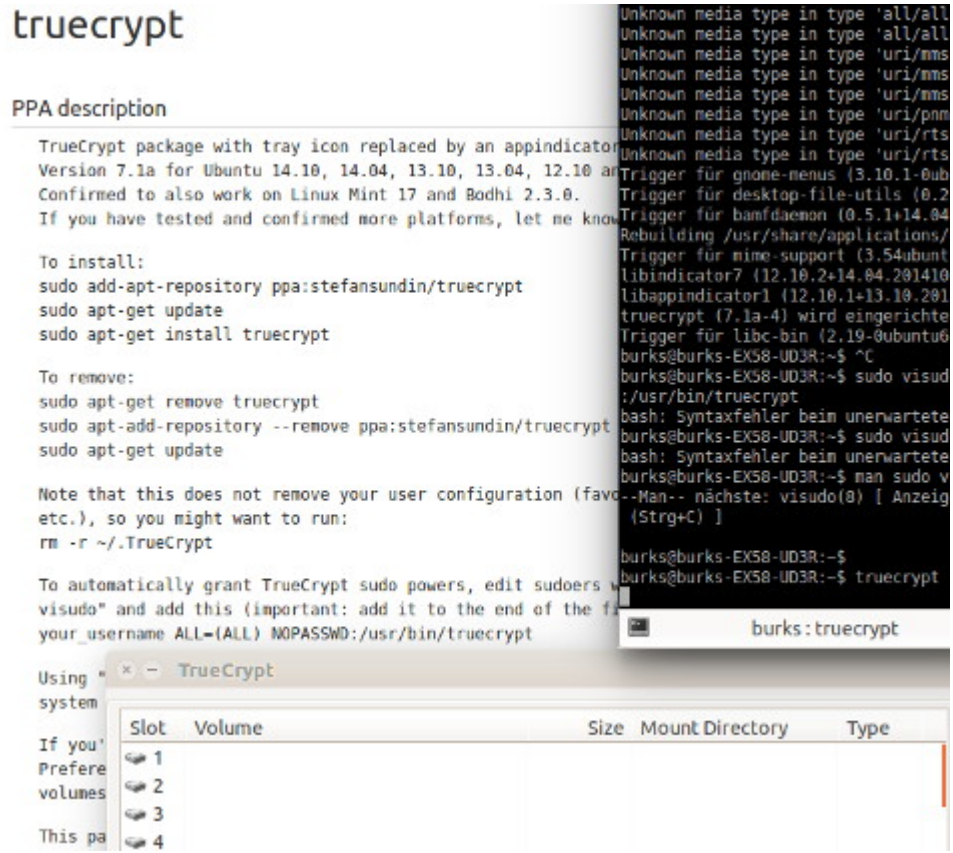
Aber habe ich dort auch wirklich alle Schlüssel, um verschlüsselte E-Mails lesen zu können? Ich erwarte wichtige Post für eine aufwändige Recherche.

Also schnell einen Container auf einem USB-Stick erzeugen. Ähhhh… aber auf dem Netbook hatte ich kein Truecrypt. Ich muss doch dort den Container wieder öffnen können! (Keys import etc.) Wie ging das noch mal gleich?

Das entsprechende Wiki erklärt, wie man einen Leopard-Panzer, den man als Bausatz gekauft hat, selbst zusammenbaut. Ich hasse es. Wieder in Ruhrpöttisch: Die kommen imma von Hölzken auf Stöcksken. Besser gleich das hier lesen und anwenden.

Voilá! (Ja, ihr könnt da gern draufgucken, es gibt nichts zu sehen, was ihr nicht sehen dürftet!)

Truecrypt mit Ubuntu



Nein, es ist *nicht* einfach. Wie kann man einen Truecrypt-Container, den man mit Windows erzeugt und in sein (Linux-)“home“-Verzeichnis kopiert hat, öffnen („mounten“)?

Der Problem bei den hilfsbereiten Linux-Nutzer in den einschlägigen Foren ist immer, dass sie auf ein einschlägiges Wiki (eine Anleitung) verweisen können. Das Problem bei einschlägigen Wikis ist, dass in nullkommanix 85 Fenster geöffnet sind, weil fast jeder Wort auch ein Link ist, und man komplett die Übersicht verliert. Von Pädagogik keine Spur.

Ich nutze die Linux-Version „Trusty Tahr“ (nein, kein Link dahin), was bei meinem Problem aber irrelevant war. Normalerweise installiert man neue Programme über das Ubuntu-Software-Center, das bei der Installation schon eingerichtet

wird. (Ich bevorzuge übrigens Synaptik, weil ich das von früher kenne.) Mausklick und Admin-Passwort genügen. Hier geht das aber nicht so einfach, weil die Quelle für die Software – Truecrypt – in der Liste, die das Ubuntu-Software-Center abfragt, nicht vorhanden ist. Man muss also das Software-Center dazu zwingen, auch andere Quellen zu installieren.

Die Installation der Version 7.1a muss daher entweder über ein „Personal Package Archiv“ (PPA) oder manuell (an der Paketverwaltung vorbei) erfolgen.

Super. Das versteht man doch auf Anhieb, oder? Also ein neues Fenster öffnen zu PPA:

Um Programme aus einem PPA zu installieren, muss es wie andere Paketquellen auch, in der Paketverwaltung freigeschaltet werden. Bei einem PPA ist dies jedoch recht komfortabel.

Ich will so etwas eigentlich gar nie mehr in einem Forum lesen. Ich fühle mich dabei nicht recht komfortabel, weil ich weiß, dass auf jeden Fall die Kommandozeile auf mich zukommt (die ist bei Linux jedoch recht komfortabel SCNR).

Danach habe ich nicht weitergelesen, weil ich heute noch etwas anderes tun wollte als Wikis zu studieren.

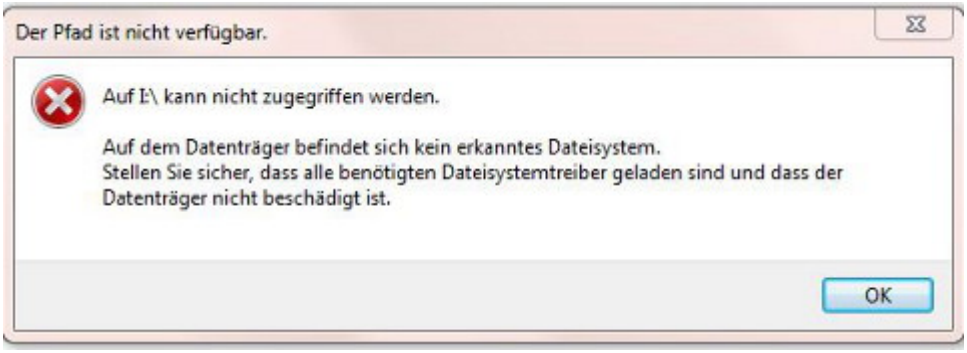
Wie es funktioniert, kann man bei Stefan Sundin nachlesen:

To install:
sudo add-apt-repository ppa:stefansundin/truecrypt
sudo apt-get update
sudo apt-get install truecrypt

Vier Zeilen mit der Bash reichen. Geht doch, oder? Die zu lesen und auszuführen, kostete mich eine Minute. Ich bin auch ganz gut darin, unerwartete und unverständliche Fehlermeldungen der Bash zu ignorieren.

Und siehe, mein Linux-Truecrpyt kann alle Windows-Truecrypt-Container öffnen und anzeigen.

Wetter-Apps und Kryptoprogramme



„Bei einer Wohnungsdurchsuchung stießen die Ermittler auf einen Computer, dessen Sofware-Konfiguration so aussieht, als ob sie ein Geheimdienst präpariert habe. Auf dem Rechner ist eine Wetter-App installiert, fragt der Nutzer das Wetter in New York ab, öffnet sich automatisch ein Kryptoprogramm.“ (Aus dem aktuellen Spiegel über den enttarnten BND-Agenten)

Super. Jetzt weiß ich endlich, wie ich meine Rechner konfigurieren muss. Ich würde aber das Wetter in Tel Aviv oder auf der Krim abfragen. Die Links auf die Truecrpyt-Container auf dem Desktip Windows-Rechner sind öffenbar nicht intelligence-kompatibel, obwohl sich beim Klicken darauf ein „Kryptoprogramm“ öffnet. Da das ehemalige Nachrichtenmagazin uns nicht verrät, um welches „Kryptoprogramm“ es sich handelt, obwohl uns das am meisten interessiert, kann man nur vermuten, dass ~~der Volontär~~ die fünf Redakteure, ~~der~~ die von der Agitprop-Abteilung des Verfassungsschutzes gebrieft wurde, diesen Artikel zu ~~lancieren~~ schreiben, nicht interessiert waren genau zu wissen, was in Wahrheit geschehen ist.

Welt online formuliert vorsichtig: „Noch größer ist die Verwunderung darüber, dass der Verdächtige sich am 28. Mai dieses Jahres unter Beifügung vertraulicher Dokumente von

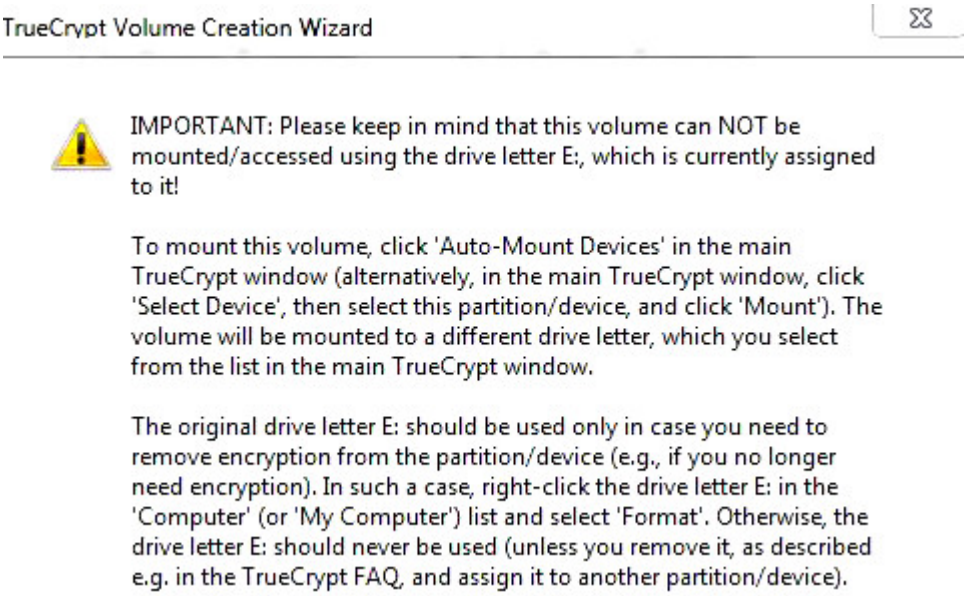
einem Google-Mail-Account aus an das russische Generalkonsulat in München gewandt hatte.“ Sicher, und auch noch unverschlüsselt.

Faszinierend, wie kompetent die BND-Mitarbeiter im Dienste der USA sind, die den NSU-Untersuchungsausschuss ausschnüffeln sollten. „Tatsächlich las der Verfassungsschutz die Mail an das russische Konsulat mit.“ Ach?! Der Verfassungsschutz hat jetzt vielleicht auch V-Leute beim BND. Har har.

„Stefan Wels vom NDR sagte in der Tagesschau, die Ermittler hätten das Haus der Verdächtigen durchsucht und dabei einen USB-Stick sichergestellt. Dieser werde ausgewertet“, meldet die Tagesschau. Und ganz bestimmt hat die BND-Pappnase auf seinem USB-Stick kein *hidden volume*. Das wäre nicht kompatibel mit Wetter-Apps und auch zu kompliziert, dass Verfassungsschützer und Journalisten das verstehen würden.

Wisst ihr was? Ich glaube dieser Sau, die gerade ~~durch die Netzgemeinde~~ durchs Dorf getrieben wird, kein Wort. Ein Geheimdienst, der „Kryptoprogramme“ hinter Wetter-Apps versteckt, ist eine Lachnummer. Für mich sieht das wie eine – gewohnt dilettantisch gemachte – Nebelkerze des Verfassungsschutzes aus, der genau weiß, dass diejenigen Journalisten, die zu solchen Briefings eingeladen werden, nicht nachhaken, sondern alles brav mitschreiben und genau so publizieren. Just my 20 Cents.

Hidden Volume – Expertinnen gefragt



Eine Frage an die Truecrypt-ExpertInnen – das Setting ist wie folgt: Ein Hidden Container auf einem USB-Stick, darin Thunderbird Portable samt Enigmail und GPG für Thunderbird Portable. So weit, so gut.

Das Problem ist: Wenn ich an einem fremden Rechner säße, auf dem Truecrpyt *nicht* installiert ist, kann ich das Hidden Volume gar nicht öffnen. Deswegen frage ich mich, wie ich Truecrypt Portable auf den Stick kriege, also sozusagen am Hidden Volume „vorbei“. Es sehe keine Möglichkeit.

Oder hätte ich erst den ganzen Stick in einen Truecrypt-Container verwandeln müssen, um dann *darin* noch einen Hidden Volume anzulegen? Die Option habe ich gar nicht gesehen…

Thunderbird-Usability-Problem für fortgeschrittene

Paranoiker

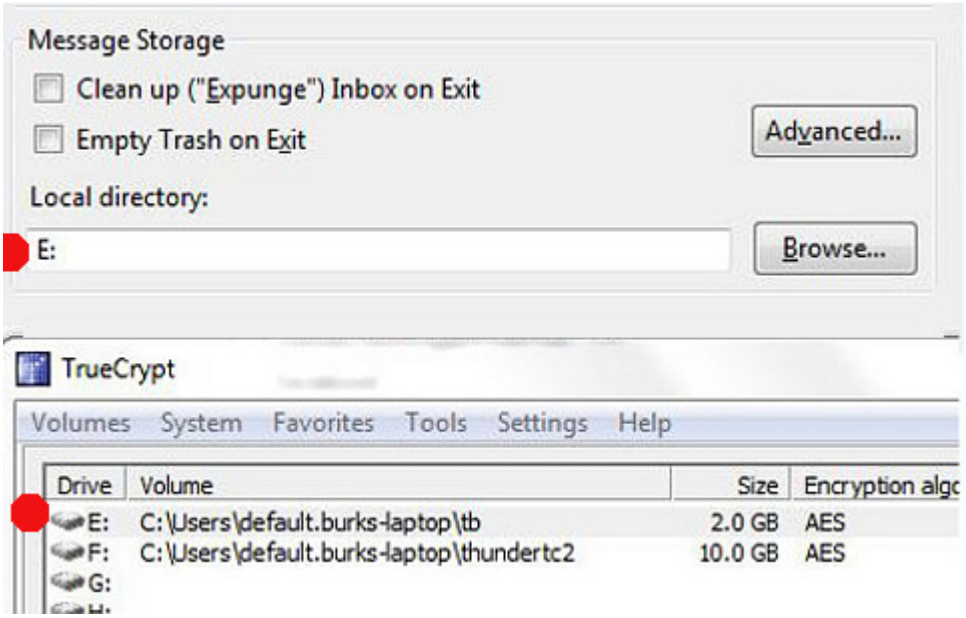
Ich kann gut nachvollziehen, warum viele Leute sich weigern oder schnell entnervt aufgeben, wenn man sie auffordert, ihr Verhalten am Rechner zu ändern. Es begegnen einem so viele Probleme der unerwarteten Art, vor denen die Macher der Software nie warnen. Wenn man aber alle möglichen Tücken der jeweiligen Software gleich in die Anleitung schreiben würde, wäre die unlesbar. Mit Computerprogrammen ist es wie mit komplizierten Haushaltsgeräten: Ich habe keine Lust ein Handbuch zu lesen, das 50 Seiten umfasst, wenn ich mir einen neuen Staubsauger oder einen Nassrasierer gekauft habe. Das Ding soll das tun, wofür ich es angeschafft habe und nicht rumzicken.

Ich habe gegenüber den meisten Menschen, denen ich etwas über Verschlüsseln und dergleichen erzähle, einen Erfahrungsvorsprung von mindestens 15 Jahren, was gleichzeitig bedeutet, dass ich schon alle Fehler gemacht habe, die sie gar nicht mehr machen können. Ich kann mich noch gut daran erinnern, dass ich in den frühen 90-er Jahren mit Windows for Workgroups 3.11 noch unter MSDOS den berühmten Norton Commander zum Absturz gebracht habe, obwohl das eigentlich gar

nicht möglich ist. Ich denke einfach anders als Programmierer: Denen ist Usabilty völlig egal.

Das gilt insbesondere für die kostenlose Software, mit der man E-Mails verschlüsselt. Eigentlich ist das kinderleicht, aber nur eigentlich. Man muss sich nur mal die Website von Gpg4win anschauen:
Gpg4win 2.1.1 contains: GnuPG 2.0.20, Kleopatra 2.1.1 (2013-05-28), GPA 0.9.4, GpgOL 1.1.3, GpgEX 0.9.7, Claws Mail 3.9.1, Kompendium (de) 3.0.0, Compendium (en), 3.0.0-beta1.

Geht's noch? Habt ihr noch alle Tassen im Schrank? Die Hälfte von dem Quatsch braucht kein Mensch. Von Usability (Benutzerfreundlichkeit) keine Spur. Stellt euch doch mal Leute vor, die den Unterschied zwischen Webmail und einem E-Mail-Programm gar nicht kennen, die verlegen zögern, wenn man sie fragt, welches Betriebssystem sie nutzen und die verständnislos mit dem Kopf schütteln, wenn sie nach einem „Texteditor, der *nicht* Word heisst" gefragt werden. Das ist leider die übergroße Mehrheit und *das* ist das Niveau, vom dem man die Leute abholen muss. Ich bin froh, dass ich mit solchen ~~DAUs~~ Menschen oft zu tun habe, die mich auf den Boden der Realität zurückholen.



Heute aber nichts für die, sondern für fortgeschrittene

Paranoiker. Wie schon erwähnt, läuft bei mir das E-Mail-Programm *Thunderbird* in einem Truecrypt-Container. Das bedeutet: Wenn jemand in meinen Rechner schaute, würde diese Person vermuten, ich besäße gar kein E-Mail-Programm oder könnte nicht beweisen, dass ich eins hätte. Ich muss diesen Container, bevor ich nach meinen Mails schaue, immer erst mit zwei Mausklicks und der Eingabe eines langen Passworts öffnen. (Wie unbequem! Das dauert ja zwei Sekunden länger als ich es gewohnt bin! Igitt! Das tu ich mir nicht an!) Ich habe also das E-Mail-Programm auf meinen Windows-Rechnern nicht dort installiert, wo es von ~~dem höheren Wesen Kleinweich~~ Bill Gates vorgesehen ist, sondern die „fortgeschritten"-Option („advanced") gewählt, um das selbst entscheiden zu können – in diesem Fall eben in einen durch Truecrpyt vorher angelegten Container (der, wenn er geöffnet worden ist, vom Dateimanager von Windows mit einem ganz normalen Laufwerksbuchstaben angezeigt wird. Unter Linux ist das viel praktischer, aber das ist heute nicht dran).

Seit einigen Tagen weigerte sich Thunderbird auf meinem Laptop, einen meiner E-Mail-Accounts zu öffnen, ausgerechnet den von burks@burks.de. Auf allen anderen Rechnern, sogar auf meinem Smartphone, rauschten meine E-Mails nur so herein, aber dem Laptop bliebt alles wüst und leer. Nun bin ich kein Laie, sondern versuche immer selbst herauszufinden, was falsch läuft.

Diagnose: Mein Programm versuchte sich mit dem SMTP-Server meines Providers zu verbinden. So weit, so gut. Aber dann hörte es irgendwann nach ein paar Minuten auf, als sei es frustriert, und nix passierte. („Account Settings" | „Server Settings" | „Server name": IMAP- und SMTP-Server noch richtig? Ja. „Connection Security": SSL/TLS oder STARTTLS? Hab ich vergessen, muss ich nachschauen – Mist, schon wieder eine Minute mehr gebraucht – verdammt, wo steht das noch gleich?) Half aber alles nichts.

Irgendwann habe ich die harte Tour gewählt und einfach das

gesamte Thunderbird-Verzeichnis von meinem Hauptrecher auf meinen Laptop gebeamt, also das offenbar Kaputte mit dem überschrieben, was funktionierte. Dummerweise änderte das gar nichts. Ich konnte meine Mails immer noch nicht aufrufen. („Warum hast du denn alles auf Englisch?“ – „Damit ich besser englische Handbücher lesen kann.“) Dann habe ich mir erst einmal Kaffee gemacht, um von der Palme, auf der ich schon saß, herunterzukommen.

Zum Glück hatte ich irgendwann eine Eingebung: Wenn man Thunderbird zwingt, sich woanders zu installieren als es vorgeschlagen wird, muss man nicht nur per Hand den Ort („Pfad“) eingeben, wo das geschehen soll, sondern auch noch in den Einstellungen bei „Message Storage“ (keine Ahnung, wie das auf Deutsch genau heißt) definieren, wo die Nachrichten gespeichert werden. Das hatte ich bei der Installation auch brav gemacht, aber vergessen, dass Truecrypt einem die Wahl lässt, unter welchem „Laufwerkbuchstaben“ man den Container jeweils öffnet. Und wenn der nicht mit dem übereinstimmt, der bei der Installation eingegeben worden war, dann reagiert Thunderbird wie eine beleidigte Leberwurst, macht gar nichts und spuckt noch nicht einmal eine Fehlermeldung aus – ein Benehmen, dass ich auch von Frauen kenne.

Vorbildlich, taz-Fotograf!

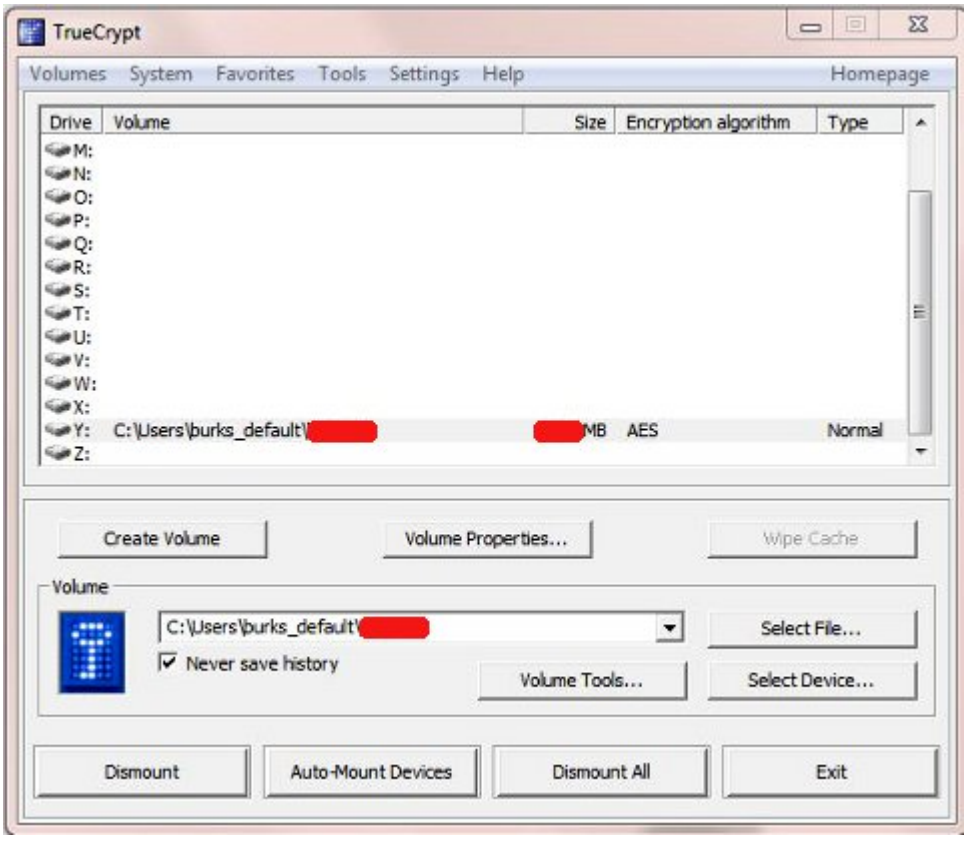
Taz: “ Die Polizei hat am Mittwoch die Wohnungen von neun Fotografen in vier Bundesländern durchsucht. Um sechs Uhr klingelte es auch in Berlin an der Tür von Christian Mang, der als freier Journalist für die taz und andere Auftraggeber arbeitet. (…) Vier Stunden lang durchforsteten sie seine Wohnung und vor allem die Festplatten seines Computers und seines Laptops. Als sie dort eine verschlüsselte Datei fanden,

holten sie auch noch Verstärkung vom Bundeskriminalamt.“

Das BKA kann aber Truecrpyt auch nicht knacken. Das fehlt im Artikel.

By the way: „Die Staatsanwaltschaft Frankfurt begründet die Durchsuchung mit einem Missverständnis.“ Bruhahahaha.

Thunderbird und Truecrypt

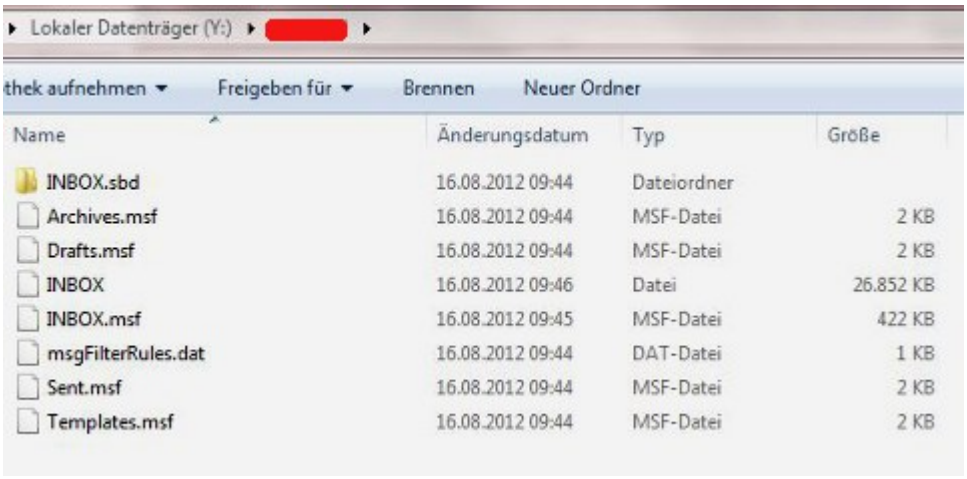


Wie ich gestern schon sagte, habe ich nach der Neuinstallation eines meiner Rechner endlich konsequent auch meine digitale Korrespondenz vor den Augen derjeningen verborgen, die Rechner beschlagnahmen, stehlen oder mit irgendwelchen Methoden durchsuchen wollten – gegen meinen Willen.

Für Laien und die, die das noch nicht gemacht haben, hier die

Arbeitsschritte für einen Computer mit dem Betriebssystem Windows 7 (64 bit) und Thunderbird 14.0:

1. Truecrypt installieren. (ausführliche Anleitung mit Screenshots)
2. Truecrypt aufrufen und ein verschlüsseltes Laufwerk („container“) erzeugen (meines ist 1 Gigabyte groß – das sollte reichen).
3. Das E-Mail-Programm Thunderbird herunterladen, *aber noch nicht installieren*.
4. Das verschlüsselte Laufwerk öffnen („mounten“, vgl. Screenshot oben) und die ausführbare Datei mit Thunderbird dort hineinschieben. Erst *dann* Thunderbird installieren und bei jeder Frage, *wo* es installiert werden soll, den geöffneten Truecrypt-Container (im Windows-Dateimanager „lokaler Datenträger“ genannt) angeben. Bei mir wäre das das verschlüsselte „Laufwerk“ Y. (vgl. den Screenshot unten)



Jetzt kommt der wichtige Arbeitsschritt, wenn ein E-Mail-Konto eingerichtet wird:
5. Bei den „Account Settings“ (Voreinstellungen des eigenen E-Mail-Accounts, *sorry, ich habe alles in Englisch*) und den dortigen Optionen („Server Settings“) muss der Dateipfad geändert werden („local directory“, vgl. Screenshot unten), so dass die eingehenden Mails innerhalb des verschlüsselten Truecrypt-Containers gespeichert werden.

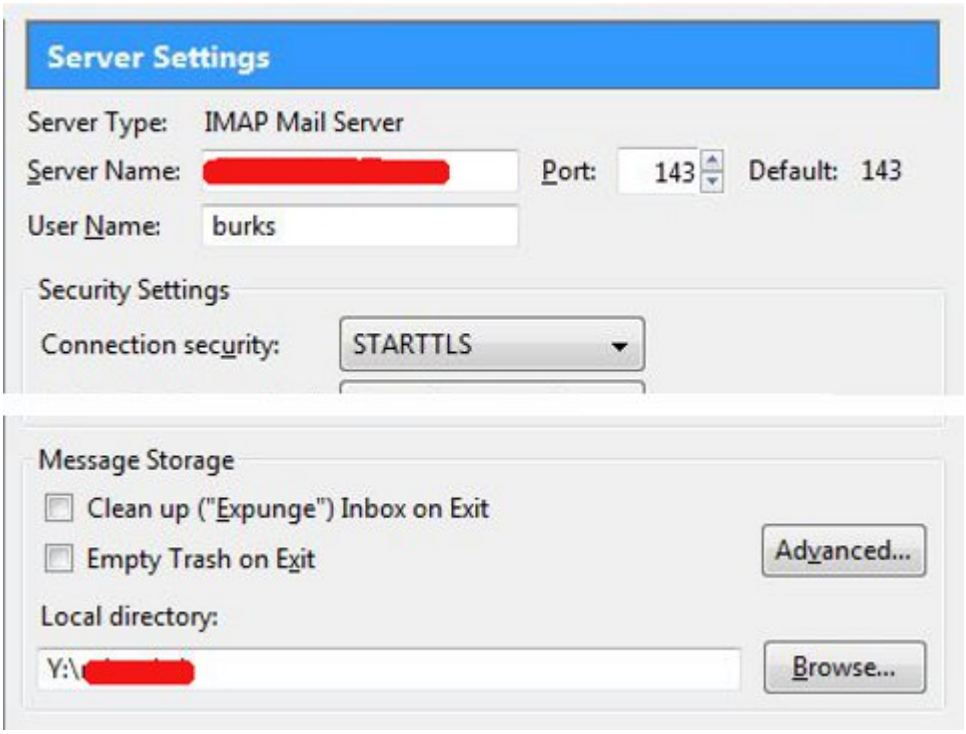
Nicht vergessen: Um mit Thunderbird arbeiten zu können, muss

jetzt natürlich immer erst das verschlüsselte Laufwerk geöffnet („gemounted“) werden.

Ab jetzt ist auf dem so abgesicherten Rechner gar kein E-Mail-Programm mehr zu sehen, auch die unverschlüsselten E-Mails sind verborgen. (Liebe Drehbuch-Autoren von Vorabend-Krimiserien und Tatorten: Da kann auch „die IT-Abteilung“ nichts machen, die bei euch immer zaubern soll, wenn es mit dem Passwort-Raten ausnahmsweise nicht klappt.)

Truecrypt ist nicht „knackbar“. Die Angriffsszenarien, die im Wikipedia-Artikel geschildert werden, beziehen sich alle auf die Situation, dass das Passwort zum Öffnen eines Truecrpyt-Containers dann abgegriffen werden könnte, wenn der Rechner eingeschaltet und das Laufwerk geöffnet ist oder man vergessen hat, es zu schließen („dismount“).

Und jetzt wieder einmal viel Spaß beim Offline- und „Online-Durchsuchen“.



German Internet Angst

Diese Artikel steht – leicht verändert – in der aktuellen Ausgabe des Medienmagazins Nitro.

Kann der Staat private Rechner kontrollieren und durchsuchen? Fachleute des Chaos Computer Club haben Spionage-Software auf Festplatten gefunden, die das beweisen. Aber was ist wirklich geschehen und was machten die Medien daraus?

Dem deutschen Journalismus kann vieles vorgeworfen werden: Die Journaille sei duckmäuserisch und feige, lasse sogar Interviews „autorisieren“, Recherchen fänden im Tagesgeschäft kaum noch statt, und der technische Sachverstand, das Netz aller Netze betreffend, entspräche dem Niveau von Grundschülern. Das ist alles richtig und kann mit dem kulturellen Tradition des Obrigkeitsstaats und der „German Internet Angst“ erklärt werden, ein Begriff, den die US-amerikanische Zeitschrift Wired schon im Juni 1998 prägte.

The reunified nation still shows symptoms of schizophrenia, and nowhere are the symptoms wreaking more havoc than on the Internet. (Wired 1998)

Drei von vier Deutschen haben laut einer repräsentativen Untersuchung Angst vor Computern und dem Internet; die Mehrheit nutzt das Netz nur selten.(Süddeutsche,18.03.2010). Journalisten denken und verhalten sich nicht signifikant anders als der Rest der Bevölkerung. Des Diskurs über staatliche Spionage-Software beweist das immer wieder: Die Berichte und Kommentare in den Medien über die sogenannte „Online-Durchsuchung“ sind seit fünf Jahren fast ausnahmslos eine Mischung aus techischem Voodoo, grobem Unfug und heißer Luft.

Die schlimmste Berufskrankheit des deutschen Journalismus ist aber die rational nicht zu erklärende Unart, suggestive Begriffe unkritisch zu übernehmen und wiederzukäuen, die von Behörden und Firmen erfunden wurden, um bestimmte Sachverhalte

zu verschleiern und euphemistisch umzudeuten. In der guten alten Zeit nannte man das unter Journalisten Propaganda oder „Agitprop“. Das gilt insbesondere für die vom bürokratischen Neusprech vergifteten Worthülsen „Staats-Trojaner“, „Online-Durchsuchung“ und „Quellen-Telekommunikationsüberwachung“. Ein Schelm, wer an „Rettungsschirme“ und „friedenserzwingende Maßnahmen“ oder gar an das Wahrheitsministerium von George Orwell denkt.

Eine Mischung aus techischem Voodoo, grobem Unfug und heißer Luft.

Kein Wunder, dass auch viele Journalisten glauben, „die Hacker“ könnten zaubern und mit magischen Methoden in Rechner eindringen und die manipulieren, entweder in staatlichem Auftrag oder aus quasi-kriminellen Motiven. Eine gute Nachricht also vorweg: Die Idee, man könne ohne vorherigen physischen Zugriff (und das auch nur unter ganz bestimmten Voraussetzungen) gezielt auf einen privaten Rechner zugreifen und ohne Zustimmung des Verdächtigen eine Spionage-Software „aus dem Internet” implementieren, ist eine Verschwörungstheorie und technisch gesehen Blödsinn.

Nun rufen alle im Chor: „Ja, aber?“ Richtig: Es ist den Behörden gelungen, auf einigen Rechnern Programme zu installieren, die nicht nur die Kommunikation belauschten, sondern Screenshots anfertigten und unbemerkt versandten, also digitale Fotos dessen, was jeweils auf dem Monitor zu sehen war. Noch mehr: Die Spionage-Software konnte sogar zusätzliche Programme und Features nachladen. Letztlich kann das natürlich dazu führen, dass die befallenen Rechner hätten von fern gewartet, also übernommen („remote access“) werden können. Das streitet niemand ab.

Was macht DPA (10.10.2011) daraus? „Eigentlich Trojanisches Pferd genannt, schleust sich eine solche Schadsoftware unbemerkt in fremde Rechner ein…“ Nein, ganz falsch. Eine Software kann sich nicht selbst einschleusen. Das ist – auch

auf die Gefahr hin, etwas zu wiederholen – eine Verschwörungstheorie.

Auch die Tagesschau machte mit: „Dabei sollen Computer einmal (Online-Durchsicht) oder während eines gewissen Zeitraums (Online-Überwachung) überprüft bzw. überwacht werden, ohne dass der Nutzer das bemerkt. Das Innenministerium sprach 2008 nicht von Bundestrojanern, sondern von „Remote Forensic Software".“ Sollen? Was jemand will, sollte von der jeweiligen Pressestelle verbreitet werden. Journalisten sollten herausfinden, was war und ist, nicht mehr und nicht weniger.

Die Frankfurter allgemeine Zeitung (03.11.2011) schrieb etwas von einer „ferngesteuerten Informationstechnik“. Das ist einfach nur Quatsch. Man braucht sich gar nicht zu streiten, ob es einen Unterschied gebe zwischen einer „Durchsicht“ und einer „Überwachung“. Wer seinen Rechner schützt, etwa nach den im Internet abrufbaren Maßgaben des Bundesamtes für Sicherheit in der Informationstechnik, der braucht sich keine Sorgen zu machen, „online durchsucht“ zu werden. Es hat sich auch noch niemand, noch nicht einmal der Chaos Computer Club, erkühnt, einen Weg zu beschreiben, wie das „von fern“, online und gezielt möglich sei. Wieso ist das eigentlich so schwer zu verstehen?

Im aktuellen Fall geht es um die Überwachung von Internet-Telefonie.

Im aktuellen Fall geht es um die Überwachung von Internet-Telefonie, deren „Nebeneffekt" jedoch war und ist, dass der Rechner komplett überwacht werden kann. Man muss also Programme installiert haben, etwa Skype, die Telefongespräche via Internet ermöglichen.

Apropos Internet-Telefonie: In vielen Unternehmen ist Skype verboten, weil das Sicherheitsrisiko zu groß erscheint. Die Software verhält sich zu Firewalls und Routern wie ein Nashorn, wenn es in Wut gerät: Sie bohrt Löcher hinein, damit

auch der dümmste anzunehmende Nutzer bequem plaudern kann und nicht erst in den digitalen Eingeweiden fummeln muss. Die Innereien von Skype – der Quellcode – sind ohnehin ein Betriebsgeheimnis. „Security by obscurity“ nennt man das System im Hacker-Milieu. Im Internet kursieren detaillierte Analysen wie „Silver Needle in the Skype„, die die Schwachstellen der Software aufzeigen.

Das ist alles seit Jahren bekannt; Software, die Telefonieren per Internet belauscht, wird sogar kommerziell angeboten. Um die aber installieren zu könnten, braucht man den physischen Zugriff auf einen Rechner. Und wenn dessen Besitzer davon nichts merken soll, muss dieser seinen Computer völlig ungesichert herumstehen lassen oder herausgegeben haben.

Die Tageszeitung (11.10.2011) schildert, wie man das so macht: „Bayerns LKA bricht auch mal heimlich in ein Firmenbüro ein, um Schnüffelsoftware zu installieren.” Das erinnert an die zentrale Losung der Hausbesetzer-Bewegung in den 80-er Jahren: legal. illegal, scheißegal.

Kann man sich vorstellen, dass von den zahlreichen deutschen Medien und mehreren tausend Journalisten niemand fragte, wie man denn eine Software zum Spionieren und „Online-Durchsuchen“ gezielt auf einen bestimmten Rechner bekäme? Nein, niemand fragte. Man faselte nur vage herum. Da gab es doch einen Geschäftsmann, der auf einem Flughafen in Bayern seinen Laptop abgeben musste und dem irgendwelche Beamten irgendetwas implementierten? So mag es gewesen sein. Nichts Genaues weiß man nicht, und es interessiert auch niemanden.

Wie dumm muss man aber sein, seinen Computer so einzustellen, dass ein Fremder Software installieren darf? Keine Passworte? Booten von Fremdmedien, etwa USB-Sticks, erlaubt? Keine verschlüsselte Partitionen der Festplatte vorhanden, zum Beispiel mit Truecrpyt? Wie jetzt? E-Mails – also digitale Postkarten – im Klarterxt und unverschlüsselt – so etwas gibt es noch im 21. Jahrhundert? Ja, es handelt sich um Deutschland

einig Entwicklungsland, das Internet betreffend.

Bei staatlicher Datenspionage greifen mittlerweile mediale Beißreflexe, die dem Diskurs über Drogen gleichen.

Bei staatlicher Datenspionage greifen mittlerweile mediale Beißreflexe, die dem Diskurs über Drogen gleichen: Seit vier Jahrzehnten sind bei diesem alle Textbausteine und Argumente bekannt, sie werden in konjunkturellen Schüben aus moraltheologischen Gründen ständig wiederholt. So auch hier: Die Überwachungslobby möchte ihrem feuchten Traum, in der digitale Unterwäsche aller Untertanen ständig herumschnüffeln zu dürfen, nicht abschwören, weil es ums Prinzip geht. Die Datenschützer und ihre Verbündeten müssen den Popanz, das sei einfach so möglich, beschwörend vor sich her tragen, um die Gefahr des totalitären Staates 2.0 allen permanent vor Augen führen zu können.

Der Berliner Richter und Verfassungsrechtler Ulf Buermeyer hat in einem Interview mit netzpolitik.org (10.10.2011) lapidar kommentiert: „…solche Software darf es niemals geben, und zwar weil sie auch das Einspielen von Daten auf dem Zielsystem erlaubt. Das ist unter Geltung des Grundgesetzes stets unzulässig“.

Damit ist das Thema eigentlich erledigt. Buermeyer, der während seines Studiums auch als IT-Techniker gearbeitet hat und im Gegensatz zu vieler seiner heutigen Kollegen weiß, wovon er redet, wenn es um Computer geht, kennt jedoch die Mentalität der Behörden: „Richtig ist aber auch, dass sich Teile der Justiz die fehlende Rechtsgrundlage einfach selbst schaffen, indem sie die Regeln für „normale” Telefonüberwachungen für anwendbar erklären.“

Die Überwachungslobby möchte ihrem feuchten Traum, in der digitale Unterwäsche aller Untertanen ständig herumschnüffeln zu dürfen, nicht abschwören.

Im Urteil des Bundesverfassungsgerichts vom 27. Februar 2008

(1 BvR 370/07, 1 BvR 595/07) heißt es: „Das allgemeine Persönlichkeitsrecht umfasst das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen."

Die Zeitschrift „Das Parlament" titelte am 31.10.2011 über eine Abstimmung zum Thema im Bundestag: „Mehrheit für Online-Durchsuchung". Die SPD-Parlamentarierin Gabriele Fograscher meinte, neue Kommunikationstechniken ermöglichten es Straftätern, „sich im Netz zusammen zu finden, zu radikalisieren, zusammen zu arbeiten". Daher müsste die „Online-Durchsuchung" den „Sicherheitsbehörden" erlaubt sein. Also nichts dazu gelernt. Quod erat demonstrandum.

Gesetze? Urteile des höchsten deutschen Gerichts? Hermann Höcherl (NSDAP, später CSU) prägte schon 1963 den bezeichnenden Satz: „Verfassungsschützer können nicht ständig das Grundgesetz unter dem Arm tragen". In einem Bundesland, in dem man mit dem Auto Menschen totfahren kann und trotzdem später Verkehrsminister werden darf, sollte einen also gar nichts mehr wundern. Die Demokratie ist oft nur ein dünner Firnis, unter dem Dinge zum Vorschein kommen, wenn man nur ein wenig kratzt, die man am liebsten gar nicht anschauen möchte.

Festplatten verschlüsseln mit

TrueCrypt

Die wohlwollenden Leserinnen und geneigten Leser haben eine verständliche Anleitung für Truecrypt empfohlen, die ich hier gern weiterleite (für Windows). (Guckst du bei burks.de auch hier)

Jetzt schnattert sie wieder…

Nein, Spiegel Offline, auch wenn ihr euch Mühe gebt, die Ente wiederzubeleben: Es gibt *keine* Online-Durchsuchung, auch wenn ihr die „landläufig“ so nennt. Das bayerische Landeskriminalamt hat nach der Methode „legal, illegal, scheissegal“ einem Bürger den Laptop weggenommen und dann eine Spionage-Software installiert.

„Denn der Kaufmann aus Bayern trug nach jener Kontrolle ein wenig mehr im Gepäck als vorher. Auf seinem Rechner hatte das bayerische Landeskriminalamt (LKA) eine Spionage-Software versteckt. Das heimlich am Flughafen installierte Programm sicherte der Polizei weitreichenden Zugriff auf den Laptop. Sobald sich das Gerät ins Internet einwählte, übermittelte es alle 30 Sekunden ein Foto des Bildschirms zu den Ermittlern – gut 60.000 in drei Monaten.“

Ein Keylogger also. Wie das? War der Rechner passwortgesichert? War er nicht mit Truecrpyt verschlüsselt? Konnte man mit admin-Rechten von externen Laufwerken einfach so booten? Wie haben die das also gemacht? *Das will ich wissen und das zu beschreiben wäre Journalismus, Kollege Steffen Winter und nicht so eine gequirlte Gerüchte-Scheiße wie in dem linkfreien Artikel!*

„Im 30-Sekunden-Takt schickte es Fotos der Skype-Oberfläche und des Internet-Browsers an die Ermittler.“ Ach – es geht also nur um Skype? „Wenn das Programm der eigenen Leistungsbeschreibung gefolgt ist, hat es sich dort inzwischen selbst zerstört.“ Und wie heisst das Programm? So eins will ich auch – eine Software, die sich selbst vernichtet! Wieso ist Bill Gates da noch nicht drauf gekommen, so etwas zu erfinden?

Truecrypt – technische Frage [gelöst]

Ich muss die Leserschaft etwas fragen. Ich benutze Truecrypt unter Windows7 (64bit) und unter Ubuntu 10.04. Wenn ich ein Truecrpyt-Laufwerk unter Windows mounte und dann versuche, über mein eigenes Netz per Ubuntu darauf zuzugreifen, werden die gemounteten Truecrypt-Laufwerke des Windows-Rechners nicht angezeigt (alle anderen Dateien kann ich sehen). Was mache ich falsch oder wo ist der Denkfehler?

Truecrypt und der kurze Weg zum Superkriminellen

Jetzt schlägt es doch dem Fass den Boden in’s Gesicht. Via lawblog: “ Was waren die Gründe für den Staatsanwalt, von erhöhter krimineller Energie und konspirativem Vorgehen zu sprechen? Nun, es war festgestellt worden, dass mein Mandant

auf seinem Rechner TOR nutzen kann. Außerdem hatte er Truecrypt installiert.“

Wer seine Haustär verschließt, ist kriminell, weil er es den hausdurchsuchenden Beamten schwer macht. Ich habe sogar ein Stangenschloss vor der Tür – ich bin superkriminell. Ich nutze auch Tor und Truecrpyt. Und ich verschlüssele wichtige E-Mails.

Ein hübscher Kommentar dort: „Nicht auszudenken, welches Strafmaß die Staatsanwaltschaft fordern würde, wenn er dann auch noch Linux / BSD / Hurd anstatt Windows/OSX verwendet hätte. Wahrscheinlich wäre laut der Anklage selbst ein Mac genug, um als subversiv zu gelten.“

Nur gut, dass dieses Urteil diesem DAU-Gericht in den höheren Instanzen um die Ohren gehauen werden wird.