Warnung vor dem Microsoft Internet Explorer

Ich ärgere mich immer maßlos über den Quatsch, den Spiegel Online und andere Medien zum Thema Computersicherheit von sich geben.“Finger weg vom Internet Explorer – das empfiehlt das Bundesamt für Sicherheit in der Informationstechnik. Eine Sicherheitslücke ermöglicht es, Schadsoftware über den Browser einzuschleusen. Es genügt, infizierte Webseiten aufzurufen. Ein Sicherheitsupdate steht noch aus.“ Und was lesen wir bei Heise? „Da der Exploit dafür JavaScript verwendet, hilft es als temporäre Maßnahme, JavaScript zu deaktivieren.“ Welcher verblödete DAU surft denn mit eingeschaltetem Javascript auf unbekannte Websites? Davor warnt das Bundesamt für Sicherheit in der Informationstechnik schon seit Jahren. Vermutlich weiß man bei Spiegel online aber gar nicht, was Javascript ist oder wird, wie bei vielen Medien-Unternehmen, gewzungen, eine bestimmte kommerzielle Software zu benutzen. Selbst schuld und hört auf zu Jammern!

Ein ehrenvoller 60. Platz

Burks‘ Blog ist bei Twingly – „Top 100 – German Blogs“ auf Platz 60. Na ja.

Schlafwandelnd das Internet benutzen

Telepolis News: „die Neurologen von der University of Toledo in der Fachzeitschrift Sleep Medicine berichten, nämlich die ersten Person, von der es zumindest bekannt wurde, dass sie schlafwandelnd das Internet benutzte.“ Ist das so neu? Ich kenne viele Personen, bei denen dieser Zustand per default zutrifft, darunter auch hochrangige Politiker. SCNR.

Keine VDS für Tor-Nodes

Die German Privacy Foundation e.V. hat von einer international tätigen Wirtschaftskanzlei ein Gutachten zu den Fragen erstellen lassen, wie der Dienst Tor rechtlich einzuordnen ist; inwieweit der Betrieb eines Tor-Servers Speicherverpflichtungen im Sinne der Vorratsdatenspeicherung auslöst, und – falls das zuträfe – welche Daten zu speichern wären.

Als Ergebnis dieser rechtlichen Untersuchung sieht sich die German Privacy Foundation e.V. nicht verpflichtet, im Rahmen der Vorratsdatenspeicherung Daten zu erheben und zu speichern. Dementsprechend wird die German Privacy Foundation auch nach Ablauf der Übergangsfrist zum 01.01.2009 weiterhin im Rahmen des Betriebs unserer Tor-Server keine Daten auf Vorrat speichern.

Die German Privacy Foundation e.V.weist vorsorglich darauf hin, dass die Ausführungen der umfangreichen rechtlichen Stellungnahme nur für den Verein gelten; andere können sich darauf nicht berufen.

Nachtrag: Heise: „German Privacy Foundation speichert nicht auf Vorrat“

Laptop-Benutzung kann in Hauptverhandlung versagt werden

Das Bundesverfassungsgericht ist im Gegensatz zu vielen anderen deutschen Gerichten beim Thema Computer up to date: „Eine erhebliche Beeinträchtigung der Pressefreiheit ist durch den Ausschluss von Laptops nicht zu befürchten, denn dadurch wird die Berichterstattung nicht nachhaltig erschwert- (…) Gleichwohl ist zu berücksichtigen, dass moderne Laptops teils über Kameras und Mikrofone verfügen, deren – § 169 Satz 2 GVG zuwider laufende – Verwendung während der mündlichen Verhandlung sich kaum kontrollieren ließe. [mehr…]

Übrigens empfiehlt das Bundesverfassungsgericht, E-Mails zu verschlüsseln und nutzt selbst Pretty Good Privacy, auch für die Signatur.

Ego-Shooter 2.0 oder: Der letzte Sportsfreund

Natürlich hat die FAZ Recht, wenn sie sich über die 3D-Welt Twinity (ohne einen Link dahin zu setzen) lustig macht. Aber völlig ahnungslos ist der Kollege Klaus Ungerer, wenn es um Second Life geht: „Gerade hatte man sich schulterzuckend von der Medienblase Second Life abgewendet, gerade ein paar letzte Schnappschüsse leerer, irrer Landschaften von dort bewundert…“ Was kann Second Life dafür, wenn Journalisten nicht in der Lage sind zu rechercheren, wo etwas los ist: Wenn man, wie sie FAZ, immer nur langweiliges Bildmaterial von dpa zum Thema nutzt, kann man den Eindruck bekommen. Der ist aber falsch. Und was „man“ tut, hat mich noch nie interessiert und sollte auch sonst keinen Journalisten interessieren.

Für diejenigen wohlwollenden Leserinnen und geneignten Leser, die vielleicht auch wegen meiner ausführlichen Postings zum Thema Second Life irrig meinen, es handele sich um eine Kommunikationsplattform für künsterlisch interessierte ältere Damen und Herren, muss hier klargestellt werden, dass es – neben den unzähligen „Roleplay“-Territorien – natürlich innerhalb von Second Life auch zahlreiche Gegenden gibt, in denen man das erlebt, was man aus den klassischen Ego-Shootern kennt. Der Avatar kann dort „getötet“ werden, muss reloggen oder wird ins virtuelle Nirwana gebeamt. Der Vorteil gegenüber

klassischen Computerspielen ist, dass man nach dem Adrenalin-Schock, den ein Ego-Shooter mit sich bringen soll, gleich wieder etwas ganz anderes machen kann, sich zum Beispiel zu den Frauen gesellen und schnattern. Man muss noch nicht einmal die Kriegsgeräte abgeben.

Einer meiner beiden Avatare ist bis an die Zähne bewaffnet – oben sieht man mich beim „Waffenkauf“. Ab und zu trainiere ich auch das Ballerspiel innerhalb der 3D-Welt. Das ist zum Teil noch komplizierter als bei „richtigen“ Computerspielen. Gestern zum Beispiel geriet ich bei den „Dreharbeiten“ zu meiner neuen Bilderserie auf einer scheinbar verlassenen „Militärbasis“ in Second Life plötzlich und unerwartet unter schweren Beschuss und konnte meinen Avatar gerade noch retten. Das zum Thema „leere Landschaften.“

Ubuntu Privacy Remix

privacy-cd.org/: „Ubuntu Privacy Remix ist eine modifizierte Live-CD die auf Ubuntu Linux aufsetzt. UPR ist nicht für eine dauerhafte Installation auf der Festplatte gedacht. Das Ziel von Ubuntu Privacy Remix ist, eine abgeschottete Arbeitsumgebung bereitzustellen, in der vertrauliche Daten sicher bearbeitet werden können. Das auf dem dafür verwendeten Computer installierte System bleibt dabei völlig unverändert. Die Gefahr des Diebstahls solcher Daten geht heute nicht mehr nur von gewöhnlichen Internet-Kriminellen und ihren Trojanischen Pferden, Rootkits und Keyloggern aus. Vielmehr ergreift in vielen Ländern der Welt auch der Staat Maßnahmen, die Computer der Bürger mit solchen Mitteln zu bespitzeln und zu überwachen. Ubuntu Privacy Remix ist ein Werkzeug, um seine Daten gegen unbefugte Zugriffe zu schützen.“ [mehr und download/]

Gartenzwerge und Trojaner zielgenau platzieren

Dr. Michael Bürsch (SPD) auf abgeordnetenwatch.de:
„Das Aufbringen des sogenannten Trojaners auf den Rechner, ist eine Frage der technischen Umsetzung der Maßnahme. Diese muss den Voraussetzungen der Befugnisnorm und der darauf beruhenden richterlichen Anordnung entsprechen. Es ist demnach selbstverständlich, dass technisch einwandfrei sichergestellt werden muss, dass die Software auf den richtigen Rechner, also dem Rechner, von dem eine dringende Terrorgefahr ausgeht, aufgebracht werden muss. Bestehen Zweifel, dass der richtige Rechner erfasst wird, muss die Online-Durchsuchung unterbleiben. Ich habe mir von Experten versichern lassen, dass es technisch möglich ist einen Rechner einwandfrei zu identifizieren und den Trojaner zielgenau dort zu platzieren. Nach dem Abschluss der Maßnahme wird der Trojaner spurenfrei gelöscht, so dass eine Identifizierung und ein möglicher Missbrauch der Software durch Dritte ausgeschlossen sind.“

Mir fehlen die Worte. Wie soll man diesen Unfug illustrieren? Wahrscheinlich geht das nur mit Gartenzwergen als Symbol für die ahnungslosen Schmalspurdenker, die von Computern so viel verstehen wie Schäuble höchstderoselbst. Man sieht, wie das urbane Märchen sich in den Köpfen verfestigt hat und durch rationale Argumente nicht mehr hinauszukiegen ist. Die

„Experten“ möchte ich gern mal persönlich in die Mangel nehmen. Und wenn die das so gesagt haben, würde ich sie in Gegenwart ihrer Anwälte als Hochstapler bezeichnen.

How to Bypass Internet Censorship

Das 200-seitige Buch „How to Bypass Internet Censorship“ ist jetzt (als pdf) kostenlos zum Download verfügbar. „Because of concerns about the effect of internet blocking mechanisms, and the implications of censorship, many individuals and groups are working hard to ensure that the Internet, and the information on it, are freely available to everyone who wants it. This book documents simple circumvention techniques such as a cached file or web proxy, and also describes more complex methods using Tor, which stands for The Onion Router, involving a sophisticated network of proxy servers. „

Nun sucht mal schön et al!

Heute fällt mir irgendwie nichts ein zum Bloggen. Und geichzeitig sehr viel. Hier mein aktueller Desktop für diejenigen, die meinen, man könnte bei mir „online durchsuchen“ – eine Übersicht über häufig benutzte Programme. Das Motiv ist ein unveränderter Screenshot aus Second Life (Verzeihung!) – so mag ich mein virtuelles Leben. Real habe ich das auch schon genau gemacht, außer dem Leoparden. Und Jeeps können im Dschungel auch nicht so gut fahren. Bitte die Maya-Ruinen 2.0 im Hintergrund nicht übersehen!

Ich habe mein einfaches Sicherheitskonzept für Daten konsequent umgesetzt. Wer meinen Rechner beschlagnahmte, würde an keine Daten mehr herankommen – er oder sie würde noch nicht einmal in den Rechner hineinkommen.

Warum machen das nicht alle so? Tja. Gestern rief mich eine Kollegin vom Medienmagazin Zapp an. Sie hätte da gehört, mein Rechner sei beschlagnahmt worden. Hatte sie sich vorher informiert, gar meine Website gelesen? Mitnichten. Mir wäre das peinlich, aber vielleicht habe ich auch andere journalistische Maßstäbe. Ich merkte an, dass ich über journalistische Themen oder gar über die Hausdurchsuchung usw. nicht unverschlüsselt, also nicht via elektronischer Postkarte

kommunizieren werde. Die Kollegin sagte, das könne sie nicht. Klar, Zapp ist der Mainstream der „investigativen“ Recherche in Deutschland. Träumt schön weiter. Kritisch und unbequem? Aber nicht für Schäuble und Konsorten.

Ich muss aufpassen, dass ich mir’s nicht mit allen verscherze. Sonst berichtet niemand mehr, wenn das LKA Düsseldorf den Antrag stellt, mich einstweilig erschießen zu lassen, weil sie mich anders nicht kleinkriegen könnten. Mit Zapp habe ich mich schon herumgestritten in meiner damaligen Eigenschaft als Chefredakteur des Medienmagazins Berliner Journalisten. (Wieso kann man da auf einzelne Blogeinträge nicht mehr verlinken? Wikipedia hilf: Permalink!)

Bei *Berliner Journalisten* gelesen: Die Welt bezeichnete Majdanek als *polnisches* Konzentrationslager. So sind sie, die Deutschen. Da helfen keine Pillen.

Nah- und Ferndurchsuchungen

Der Irrsinn geht weiter. Laut Heise plant die EU: „Neben einem standardisierten europäischen Informationssystem und besserer Koordination bei allen Formen von Cybercrime sind darin auch gemeinse Internet-Ermittlungsteams der EU und grenzüberschreitende heimliche Online-Durchsuchungen angedacht.“ (Das Verb „Andenken“ gibt es jedoch nicht im Deutschen, obwohl man bei einigen Menschen nur eine Vor- und Embryonalform des Denkens voraussetzen kann.)

Auch der faktenfreie Textbaustein „Spam, Identitätsdiebstahl und Kinderpornografie breiten sich immer mehr aus“ fehlt nicht. „Und es sollen ‚remote searches‘ (wörtlich „entfernte Durchsuchungen“ oder „Ferndurchsuchungen“, womit offensichtlich die in der deutschen Debatte ‚heimliche Online-

Durchsuchung‘ genannte umstrittene Maßnahme der Strafverfolger gemeint ist), erleichtert werden, wenn sie nach nationalen Gesetzen möglich sind. Dies soll ‚Investigationsteams ermöglichen, mit der Zustimmung des Gastlandes schnell auf Informationen zuzugreifen'“.

BBC hat das Thema auch aufgegriffen: „Forces will also take part in „remote searches“ and patrol online to track down criminals.“ Das bedeutet: Falls es jemandem gelänge, eine Überwachungssoftware auf dem Recher eines deutschen Verdächtigen zu implementieren (Windows und abgrundtiefe Dämlichkeit beim „Opfer“ vorausgesetzt), sollen gleich alle Polizisten Europas die Ergebnisse bekommen.

Da hat Leitner schon Recht: „Europol will also Spam bekämpfen, indem es neben die Spammer-Malware auf euren Computern noch Europol-Malware auf eure Computer tut. Das ist wie mit beidseitig benutztem Klopapier: der Vorteil liegt auf der Hand!“

Nazis nutzen immer öfter das Internet

Unkritisch wiedergekäuter Propagandaquark der Jugendschutzwarte und der üblichen Verdächtigen bei Heise: „Zahl rechtsextremer Seiten im Internet auf Höchststand“.

Hatte ich das nicht schon mal kommentiert? Ach ja: Im Mai diesen Jahres schrieb ich in der *Jungle World* etwas darüber.

Und was schrieben andere? Die PC Welt: „Rechtsextreme nutzen immer mehr das Internet“ (vor acht Jahren, im Dezember 2000). Chip Online: „Verfassungsschutz: Rechtsextreme nutzen das Web

intensiv“ (2000). Berliner Zeitung: „Kampf gegen Neonazis im Internet. Die Organisation jugendschutz.net beobachtet rechtsextreme Seiten und lässt sie sperren.“ (22.11.2007)

Vermutlich haben sie heute die fast zehn Jahre alten Textbausteine und die aus dem letzten Jahr nur recycelt. Auffallen würde das niemandem.

Nachtrag. Immer wieder schön zu lesen: Alvar Freudes Kaderakten über die Firma (!) jugendschutz.net.

Cyberterroristen und Propaganda im Internet

Man ist sehr erstaunt. Heise reiht sich unkritisch in die Reihe der Schäubleschen Propagandisten ein, die mit den sattsam bekannten alarmistischen Textbausteinen um sich werfen. Und das gleich doppelt: „Schlag gegen virtuelle Glaubenskrieger und Propaganda im Internet“ und „Bundesanwaltschaft: Schlag gegen islamistische Internetpropaganda„.

Die Leser sind zu recht empört und reagieren satirisch: „Bei

einer Razzia hob die Bundesanwaltschaft am Dienstag eine Reihe mutmaßlicher Cyber-Terroristen aus, die mit Counterstrike-Spielen den Boden für Radikalisierungen in der Spieleszene bereiten. (…) Der 23-Jährige aus dem nordrhein-westfälischen Schlangen soll ebenfalls bereits einschlägig aufgefallen sein – mit einer Teilnahme an den Worldcybergames. Bewiesen werden konnte der Vorwurf bisher nicht, da die Überwachungsdaten der Telekom aus Versehen gelöscht wurden."

Und hier: „Bitte Heise, diese Gossenformulierungen sind eurer echt nicht würdig. Da war ja mal wieder alles drin: „Cyber-Terroristen", „Internetpropaganda", „virtuelle Glaubenskrieger, die den Dschihad mit Maus und Tastatur führen", „Enthauptungsvideos", „al-Qaida", „Hassbotschaften", „Drohvideo", „Konvertiten", „Sessel-Dschihadisten", „islamistische Websites", „Horrorvideos", „Bombenbauanleitungen", „Computerspiele", „virtuelles Trainingscamp".

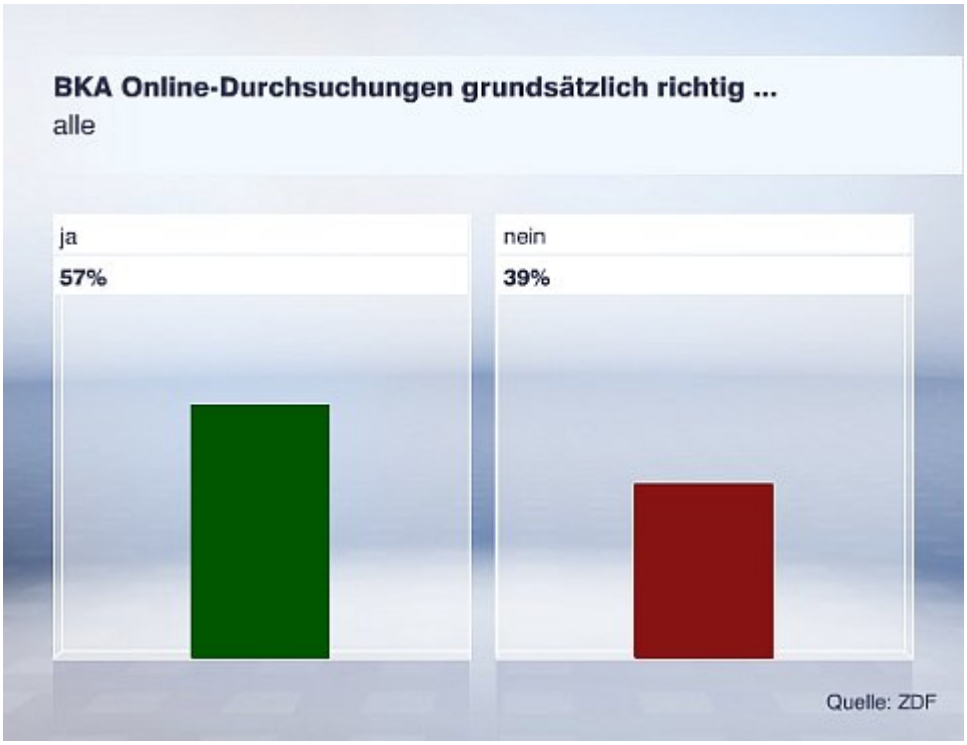
Schauen wir uns die Fakten an. Das erste medientheoretische Märchen: Die „Cyber-Terroristen", „die mit Internetpropaganda den Boden für Radikalisierungen in der Islamistenszene bereiten." Ach wirklich? Dazu müsste man beweisen können, *wie* Propaganda „im Internet" wirkt. So einfach ist das aber nicht. Die These im Artikel: Die Propagandisten „dürften" „kaum weniger wichtig sein als ein Attentäter" sein. Aha. Propaganda ist genau so schlimm wie eine Mordtat. Das ist in der Tat eine kühne These, die so aus einem Wahrheitsministerium stammen dürfte. Es gibt bisher nur „Verdächtige", aber die Ermittler seien den Glaubenskriegern angeblich „entscheidend" „auf den Leib gerückt."

Was lesen wir über den ersten Verdächtigen? „Nach Informationen von dpa ist er dort aber keine zentrale Figur, kein Rädelsführer gewesen, wenn auch seit etwa drei Jahren unter Beobachtung der Sicherheitsbehörden." Was schreibt das Lokalradio aus Paderborn wohltuend sachlich und weitaus journalistischer als der unsägliche Heise-Artikel: „Der

Haftbefehl gegen einen mutmaßlichen Terror-Helfer aus Schlangen ist außer Vollzug gesetzt worden. Der 23jährige legte vor dem Ermittlungsrichter ein umfassendes Geständnis ab. Demnach hat er zusammen mit einem anderen Verdächtigen Texte für eine islamistische Internetseite verfasst. Nach Ansicht der Bundesanwaltschaft unterstützte der Schlänger damit die Terrorgruppen Al-Kaida und Ansar el Islam. Allerdings gibt es auch Hinweise darauf, dass der 23jährige psychisch krank ist.“ Was für ein „entscheidender“ Schlag!

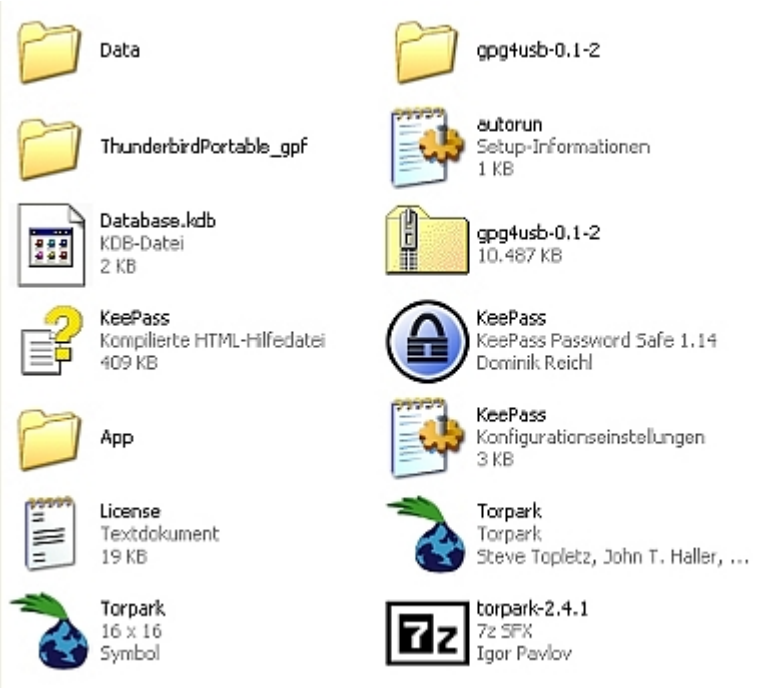
Heise käut kritiklos die Propaganda der Glaubenskrieger gegen den Terror wider: „Wie gefährlich solche ‚Sessel-Dschihadisten‘ sind, lässt sich ermessen, wenn man sich die Bedeutung des Internets für den islamistischen Terrorismus vor Augen hält.“ Über „die Bedeutung des Internet“ für alle möglichen Ismen (bitte selbst ausfüllen: [x] Kinderpornografie [x] Rechtsextremismus [x] Bombenbauanleitungen [x] Drogenhandel [x] gewaltverherrlichende Computerspiele] haben wir schon so viel gehört, dass man diese Textbausteine einfach nicht mehr ernst nehmen kann. Mann muss sich fragen, wer in Wahrheit die eigentlichen „Sessel-Dschihadisten“ sind. Bisher dachte ich, bei Heise säßen die nicht. Offenbar habe ich mich getäuscht.

Die Online-Durchsuchung – das Windei



Worauf es Schäuble wirklich ankommt, zeigt das aktuelle Politbarometer des ZDF. Zu den technischen und rechtlichen Details der heimlichen Online-Durchsuchung und des Bundestrojaners bringt c't in Ausgabe 25/08 (ab Montag, den 24. 11., im Handel) einen Hintergrundartikel: „Windei Bundestrojaner, Online-Durchsuchung vs. Gewährleistung von Vertraulichkeit und Integrität informationstechnischer Systeme", S. 86ff. Da bin ich aber mal gespannt. Die Überschrift klingt schon erfreulich.

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.

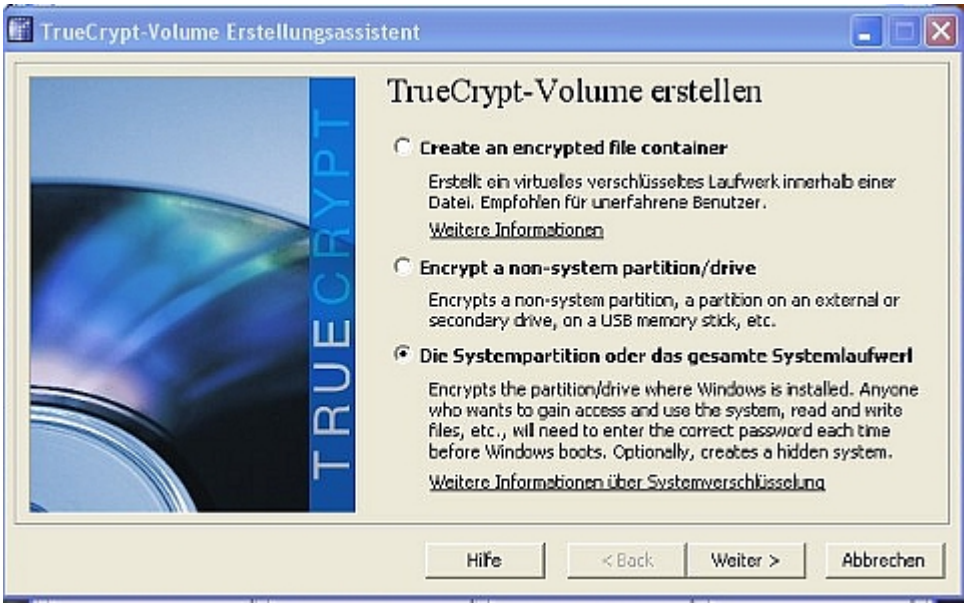
Zweitens: Der alte Windows-Rechner, den ich zur Zeit nur für Second Life und eventuell andere virtuelle Welten nutze, enthält keine sensible Daten. Für die Verschlüsselung der Festplatte nutze ich Truecrypt (Screenshot unten).

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 installlieren 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.



Burkscity

Ich halte MyMiniCity immer noch für eine total sinnfreie, aber lustige Idee, um Traffic zu generieren. Ich habe es in meinen Leserzeichen und gehe einmal pro Woche dahin (vgl. mein Posting vom 04.03.2008).

Seamonkey und Pdfit

Ich habe mir die wunderbare Firefox-Erweiterung pdfit installiert. Pdfit erlaubt, eine Website direkt als Grafik oder als pdf auszudrucken – sehr praktisch. Das konnte ich zuletzt vor Jahren unter Windows mit meinem minderlegalen Acrobat Distiller.

Oft werde ich das Feature aber nicht nutzen. Ich bin jetzt auf den Browser Seamonkey umgestiegen, der Schriften und Grafiken besser anzeigt als Firefox (vielleicht liegt es auch an meiner Grafikkarte). Die Sicherheitseinstellungen sind ähnlich komfortabel: Ich surfe grundsätzlich *ohne* Javascript, und der Seamonkey bietet eine komfortable Verwaltung der Cookies (die ich per default auch verbiete). Auch der JonDo-Client arbeitet einwandfrei.

Operation „Heiße Luft“ abgeschlossen

Schöner Nachtrag zu meinem heutigen Posting „Schließung der Datenautobahn“. Im law blog schreibt Udo Vetter:

„Die Staatsanwaltschaft Berlin meldet stolz den Abschluss der Aktion ‚Himmel‘. Obwohl 12.570 Internetnutzer ins Visier der Fahnder gerieten und es tausende Ermittlungsverfahren mit Durchsuchungen gab, fehlt eine wichtige Information: Wie viele Beschuldigte sind bislang wegen des Besitzes von Material verurteilt worden, das sie von den Berliner Servern

heruntergeladen haben sollen?

Die Berliner Staatsanwaltschaft ist offenbar nicht einmal in der Lage, eine einzige Verurteilung in ihrem Bezirk zu belegen. (…) In gut einem Jahr ist es also nicht gelungen, den Rechner auch nur eines einzigen Beschuldigten auszuwerten und ihn wegen der Sache vor Gericht zu bringen?

Vielleicht gibt es auch andere Erklärungen. Zum Beispiel die wohlweislich verschwiegene Tatsache, dass die weitaus meisten vom Berliner Landeskriminalamt als kinderpornografisch eingestuften Bilder auf den Berliner Servern überhaupt keine waren, sondern nichtpornografische Nacktbilder."

Das sind ja schlechte Aussichten für meinen Rechner, der beim LKA Berlin steht. Bin mal gespannt, ob auch nur ein deutsches Medium in der Lage ist, sich ein kritisches Wort zu der „Operation Heiße Luft" abzuringen. Ich glaube, dass nicht – dazu sind die viel zu feige.

Nachtrag: Ich muss mich korrigieren: In Zeit Online ist ein lesenswerter Artikel zum Thema.

Lively no more – bruhaha

Heise: „Nur wenige Monate nach dem Start der virtuellen 3D-Welt Lively versetzt Google dem vermeintlichen Second-Life-Konkurrenten den Todesstoß. Bis 31. Dezember 2008 bleibt der Dienst noch online; danach ist seine Zeit endgültig vorbei.“ Ja, so hatte ich mir das gedacht: Kein Sex (verboten), und die Zugangssoftware funktioniert nur für Windows. Da kichern ja die Avatare….

Die Razzia ist nur einen Klick entfernt

Law blog: „Ein Klick auf einen Link kann zur Hausdurchsuchung führen?“ [mehr…] Ich frage mich, auf welcher rechtlichen Grundlage das LKA Daten manipulieren und Lockspitzelangebote ins Netz stellen darf?