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'“.

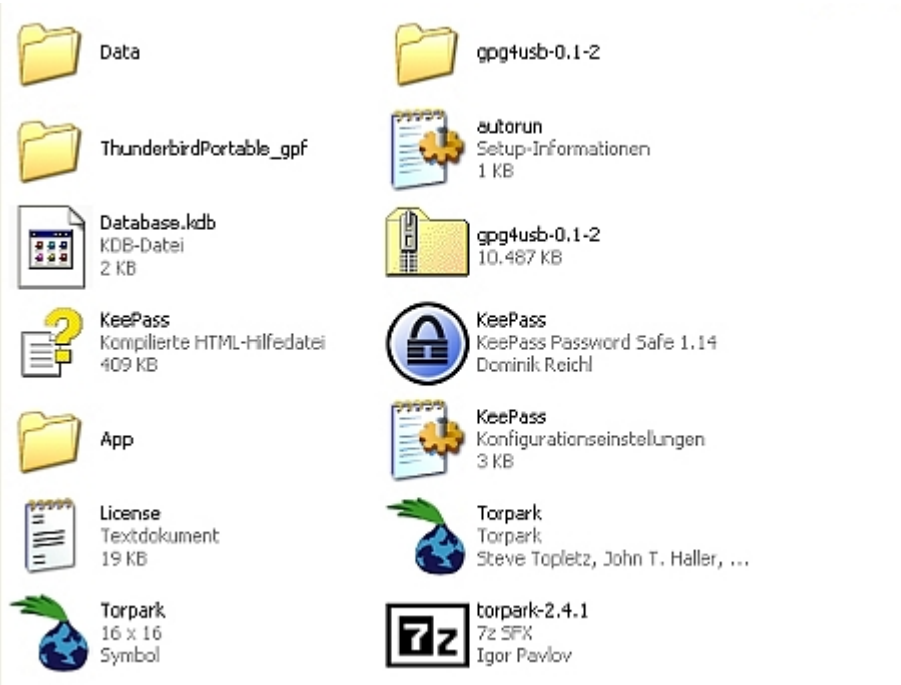
BBC hat das Thema auch aufgegriffen: „Forces will also take part in „remote searches“ and patrol online to track down criminals.“ Das bedeutet: Falls es jemandem gelänge, eine Überwachungssoftware auf dem Recher eines deutschen Verdächtigen zu implementieren (Windows und abgrundtiefe Dämlichkeit beim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

BKA-Gesetz gescheitert

Welt.de: „Das BKA-Gesetz ist vom Bundesrat abgelehnt worden. Die Länderkammer entschied sich zudem gegen die Anrufung des Vermittlungsausschusses. Jetzt will die Bundesregierung das Gremium anrufen. Innenminister Schäuble hatte für die Verabschiedung des Gesetzes ein Ultimatum bis Weihnachten gesetzt.“

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.

Keine Paranoia

Das schrieb mir gerade ein Kollege (Auszug): „Ich saß am selben Abend im Freien Neukölln, vorne am großen Fenster zur Pannierstraße. hin, zusammen mit Kollegen. So etwa um 20 Uhr. Wir wunderten uns, warum die ganze Zeit vor dem Fenster ein Staßenkehrer stand – er hatte einen Knopf im Ohr, rauchte eine Zigarette nach der anderen. Er war in voller Montor, mit mobiler Tonne und Besen ausgestattet, aber seltsame Uhrzeit für einen Kehrer und warum hing der die ganze Zeit da rum? Wir witzelten schon, ob der wegen uns hier sein. Irgendwann hielt dann kurz auch eine Limousine neben ihm und er verschwand alsbald – ca. 20.30 Uhr. Kurz vor neun, meinte dann noch mein Kollege, he, ist das nicht Burks, der da gerade die Kneipe verlassen hat? Wie dem auch sei, könnte also sein, dass du an diesem Tag einen Schatten hattest.“

Merke: Wenn du *keine Paranoia* hast, ist das noch keine Garantie, dass sie *nicht* hinter dir her sind…

Das BKA als Hüter der Pressefreiheit?

Claudia hat noch einen Artikel in Telepolis geschrieben: „Das BKA als Hüter der Pressefreiheit? – Das Bundesverfassungsgericht beschrieb 1966 in der so genannten Spiegel-Entscheidung die Bedeutung der Presse in der Demokratie so: ‚Eine freie, nicht von der öffentlichen Gewalt gelenkte, keiner Zensur unterworfene Presse ist ein

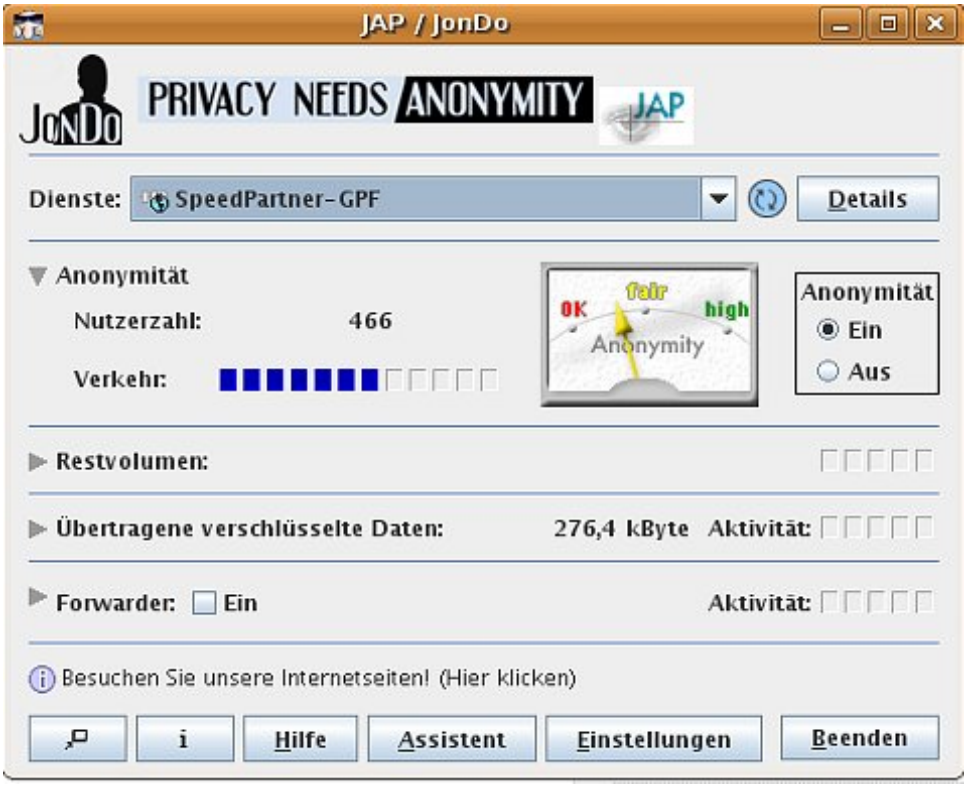
Wesenselement des freiheitlichen Staates; insbesondere ist eine freie, regelmäßig erscheinende politische Presse für die moderne Demokratie unentbehrlich.‘. Der Bundestag hat jetzt das umstrittene Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt (BKAG) durchgewunken und damit ein eindeutiges Zeichen gegen die Pressefreiheit gesetzt: Deren Schutz würde in das Ermessen des BKA gestellt worden.“

Kleine USB-Sticks

Wer etwas über Geheimverstecke und USB-Sticks wissen will: true-random.com/homepage/projects/usbsticks/small.html!

Intrepid Ibex und Unterstützung aus der Nachbarschaft

„Unterstützung aus der Nachbarschaft“ hieß die E-Mail, die ich vor ein paar Tagen zum Thema „Hausdurchsuchung“ bekam. Tobias Hensel vom Technische Kundendienst der SRZ Berlin | Firmengruppe besscom hat mir einen Rechner geschenkt, der – abgesehen von der Grafikkarte und der Lautstärke (Rasenmäher) – genau so gut ist wie der, der jetzt beim Landeskriminalamt steht. Noch einmal Dank an K., der mir schon einen Tag nach der Beschlagnahme ein älteres Modell vorbeibrachte und an die Kleinspender, an die ich mich noch einmal persönlich wenden werden, sobald ich alle Zugangsdaten und Accounts geändert habe.



Hal Faber ist auch noch einmal auf die Ereignisse der letzten Tage eingegangen. Ich habe meine Lehren gezogen – ab sofort werde ich nie wieder ein regelmäßiges Backup vergessen, mein Rechner (jetzt mit Ubuntu 8.04 Intrepid Ibex) ist komplett verschlüsselt, dazu benutze ich wie bisher noch zusätzliche Container mit Truecrypt. Es geht alles wieder, auch andere Programme wie Revelation und den Jondos-Client (vgl. Screenshot) habe ich sofort zum Laufen bekommen. Alle neueren Screenshots aus Second Life sind leider weg. Auch muss ich Danger from the Deep neu installieren. Das alles hat mich zwei Tage Arbeit gekostet, und das war das Ärgerliche. Die Solidarität vieler Net-Citizens, Bürgerrechtler und Zensurfeinde hat das aber aufgewogen.

EU-Recht und Vorratsdatenspeicherung

Cöaudia hat einen Artikel in Telepolis geschrieben: „EU-Recht und Vorratsdatenspeicherung – Wenn der Europäische Gerichtshof über die Klage Irlands entscheidet, geht es nicht nur um Formalia“.

Auf den Busch und den Fefe

klopfen

Vorgestern war ich bei busch@n-tv und habe einige Worte zum Thema „Die Online-Durchsuchung“ gesagt. Hansjörg Geiger, Ex-Verfassungsschutz-Chef, Ex-BND-Chef, hat sich offenbar vom Saulus zum Paulus gewandelt und nur Vernünftiges von sich gegeben und am BKA-Gesetz kein gutes Haar gelassen.

Wenn man die Kommentare de Kolleginnen und Kollegen anhört, gibt es nur ein Fazit: Schäuble hat sein Ziel erreicht. Alle, mit wenigen Ausnahmen, gehen davon aus, dass die Behörden in privaten Rechnern herumschnüffeln. Ob und wie das gehen soll, fragt niemand mehr. Es interessiert auch keinen. „Die Hacker“ machen das auch ständig. Das haben wir selbst in Hollywodd-Filmen gesehen. Der „Bundestrojaner“ ist zum urbanen Märchen geworden wie das Einhorn im Mittelalter.

Auch Fefe bläst genau in dieses Horn und lässt sich von denjenigen instrumentalisieren, die der Bevölkerung ein Gefühl der Ohnmacht gegenüber der Obrigkeit implementieren wollen. „Es spielt keine Rolle, ob der Staat im Moment in der Lage ist, einen effektiven Bundestrojaner zu bauen oder nicht. Dass gezielte Trojaner effektiv sein können, ist unbestritten“

schreibt Leitner. Das ist doch lachhaft. Es spielt genau eine Rolle. Leitner ist naiv, wenn er den Medienberichten einfach so traut. Und die sind die einzige Quelle für das Märchen, es habe schon Online-Durchsuchungen gegeben. Das war die Ausgangsfrage des Buches. Und siehe da: während der Recherche stellt sich heraus, dass alles frei erfunden oder von anderen abgeschrieben worden war oder von den Presseerklärungen der einschlägigen Ministerien unkritisch übernommen. Das ist der *aktuelle* Stand und nicht nur der in Buermeyers Artikel: „Die „Online-Durchsuchung". Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme".

Wer Buermeyers Aufsatz liest – das hat Fefe offenbar gar nicht getan – und die dortigen Fakten mit den Medienberichten vergleicht, merkt sehr schnell, dass dort die beiden Fälle diskutiert werden – die „Durchsuchung" einer Mailbox (BBS) in den 90-er Jahren und der gescheiterte Versuch, einem Verdächtigen eine CD zuzuspielen -, die in den Medien zunächst als einzige (!) Quelle auftauchten, es habe schon erfolgreiche (!) Online-Durchsuchungen gegeben und die per „Stille Post" so oft umgeschrieben wurden, dass sich ihr irriges Fazit als Hoax im Diskurs verselbständigte.

Und das soll keine Rolle spielen? Ich würde schon gern wissen, wer von der Journaille auf der Honorarliste des BND oder BKA steht, unbewusst oder bewusst. Ein Köngreich für eine aktuelle Liste der „Pressesonderverbindungen"!

Ja, „gezielte Trojaner" wirken bei Klein Windows-Fritzchen und offenbar auch bei Klein Felix. Aber bei sonst niemandem, dessen Intelligenzquotienten die Zimmertemparatur übersteigt. Und damit wären wir immer noch nicht bei einer „erfolgreich durchgeführten" Onliine-Durchsuchung. Wie Fefes Gesinnungsgenosse Andreas Bogk in seinem Gutachten für das Bundesverfassungsgericht schreibt: „Des weiteren ist die Umgebung des Trojaners meistens so komplex, daß er sich in ihrer Interaktion nicht modellieren läßt. Die Fehlerfreiheit eines Trojaners ist also nicht zu erwarten." Quod erat

demonstrandum. Demnach lässt sich auch keine Online-Überwachung mit gerichtsverwertbaren Daten mittels eines „Trojaners“ erwarten.

„Aufgabe der Presse ist es, den Blödsinn, den Ziercke so von sich gibt, zu publizieren“, schreibt Fefe. Richtig, sehr wahr. Aber da muss Leitner sich nun wirklich nicht auch noch einreihen und seinerseits Nebelkerzen werfen.

Sorry, schon wieder neuer Schlüssel:

Ich habe mich leider beim Generieren des neuen Schlüssels insoweit vertan, als dass ich das Ablaufdatum falsch gesetzt habe. Hier also der funktionierende *neue* öffentliche Schlüssel: burks_0EF407565E3013AB.asc – | Fingerprint: 67F1 C108 3BB1 8B12 D24F 9B4F 0EF4 0756 5E30 13AB

Polizei beschlagnahmt Computer eines Telepolis-Autors

Heise Newsticker: „Am Dienstag wurden auf Anordnung eines Berliner Amtsrichters die Wohn- und Arbeitsräume des Journalisten und Telepolis-Autors Burkhard Schröder von der Polizei durchsucht und sein Arbeitscomputer beschlagnahmt. Der

Durchsuchungsbeschluss stützte sich auf den Verdacht eines Vergehens nach den Paragraphen 40 und 52 des im April 2008 novellierten Waffengesetzes. Paragraph 40 verbietet unter anderem, ‚zur Herstellung' von Waffen ‚anzuleiten'." [mehr…]

Berliner Justiz lässt Bombe platzen

Telepolis: „Berliner Justiz lässt Bombe platzen – ‚Herstellung von Explosivstoffen': Wohnungsdurchsuchung bei Telepolis-Autor Burkhard Schröder. Computer beschlagnahmt.

Wohnungsdurchsuchung reloaded 2