Mojahedeen Secrets, reloaded

Bruce Schneider hat sich vorgestern mit den *Mujahideen Secrets 2*. beschäftigt. Die Sau wurde schon vor einem Jahr von gulli.com durch's Dorf getrieben: „Geheimnisvolle Software soll Transfers via USB-Stick verschlüsseln". Ich wundere mich, dass die Mainstream-Medien daraus noch keine Schäuble-freundliche Schlagzeile gemacht haben: „Terroristen nutzen immer öfter geheimnisvolle Verschlüsselungssoftware – das gehört doch verboten? Dürfen die das?" [Ulrich Meyer, übernehmen Sie!]

Kai Raven hat sich jetzt – ihm sei Lob und Preis! – die Mühe gemacht, die zweite Version der Software unter die Lupe zu nehmen und diese auszuprobieren [dort auch zahlreiche Screenshots und weitere Links]. „Eine der Grundregeln beim Einsatz von Verschlüsselungsanwendungen bricht das Programm bereits, wenn man das Softwarearchiv öffnet: Bei den Secrets handelt es sich nämlich um ein fertig kompiliertes Windows-Programm mit einer arabischsprachigen Windows-Hilfedatei, die das Programm ausführlich dokumentiert. Für den ambitionierten Cyber-Jihadisten gibt es also keine Möglichkeit, sich einen Quellcode anzuschauen oder selbst zu kompilieren." Fazit: „Aus Sicht eines an Verschlüsselung interessierten Anwenders und Internetnutzers würde ich die Secrets jedenfalls nicht anwenden und schon gar nicht empfehlen."

Bruce Schneier: „No one has explained why a terrorist would use this instead of PGP – perhaps they simply don't trust anything coming from a U.S. company. But honestly, this isn't a big deal at all: strong encryption software has been around for over fifteen years now, either cheap or free. And the NSA probably breaks most of the stuff by guessing the password, anyway. Unless the whole program is an NSA plant, that is."

Yeah. That's it. Und man sollte es natürlich nur von Warez-Websites herunterladen – „with-crack-serial-keygen" und Magic Lanterns.

Security by obscurity im Bundestag

Der Bundestag bietet an, den Abgeordneten verschlüsselte E-Mails senden zu können. Das hört sich gut an, funktioniert aber nicht: Kaum ein Abgeordnetenbüro weiß damit umzugehen. Bei technischen Fragen geht man zudem nach dem Motto vor: Security by obscurity.

Die rot-grüne Bundesregierung hat am 22. Januar 2002 die Telekommunikations-Überwachungsverordnung (TKÜV) erlassen. Seitdem wird die Kommunikation aller Bundesbürger komplett überwacht. Die Technik – eine Echtzeit-Schnittstelle – muss von den Telekommunikationsanbietern eingerichtet und selbst finanziert werden. Nur kleine Provider sind davon ausgenommen. Wer seine elektronische Kommunikation verschlüsselt, kann natürlich nicht belauscht werden. Was liegt also näher, auch bei vertraulichen Nachrichten an einen Abgeordneten des Bundestages kryptografische Verfahren zu verwenden.

Es scheint zunächst einfach zu sein: Unter der Überschrift

„Senden verschlüsselter E-Mails an Mitglieder oder Mitarbeiter des Deutschen Bundestages“ kann sich jeder über die Grundlagen asymmetrischer Kryptografie informieren. Man wird auch hinreichend über die Methode aufgeklärt:

„Für die Verschlüsselung von E-Mails muss der jeweilige Absender den öffentlichen Schlüssel des Empfängers in seinen E-Mail Client einbinden. Der öffentliche Schlüssel für die jeweilige E-Mail Adresse der Abgeordneten und Verwaltungsmitarbeiter ist automatisch in jeder signierten E-Mail des Abgeordneten oder Mitarbeiters enthalten. Gegebenenfalls bitten Sie Ihren Kommunikationspartner im Deutschen Bundestag Ihnen eine signierte E-Mail zu senden, um ihm verschlüsselt antworten zu können.“

Vor das Verschlüsseln hat die Verwaltung des Bundestags eine hohe Hürde gestellt: Die E-Mail-Adressen, die man benötigt, um seinen eigenen öffentlichen Schlüssel an die Abgeordneten zu senden, werden nicht verraten, sondern stattdessen jeweils ein Kontaktformular angeboten. Viele Abgeordnete haben zwar eine Website, die muss man aber in jedem Fall einzeln und mühsam selbst recherchieren. Ob das zu erwartende System vorname.nachname@bundestag.de funktioniert, erfährt man auch nicht.

Selbst bei Jörg Tauss (SPD), der bei Internet-Themen als relativ kompetent gilt, ist von einem öffentlichen Schlüssel nichts zu sehen. (Dafür begegnet man aber auf seiner Website dem „Regenzauber“, gegen Spam das @ verklausuliert (a) zu schreiben, wodurch man gezwungen ist, die E-Mail-Adresse mühsam von Hand einzutippen, statt im Quellcode zum Beispiel schlicht Unicode zu benutzen, um es den Spambots nicht ganz so einfach zu machen)

Man muss also zuerst die real existierende E-Mail-Adresse erfragen, auf eine signierte Antwort hoffen, das Zertifikat des Bundestags in den eigenen E-Mail-Client implementieren, die Signatur der empfangenen E-Mail überprüfen, den darin enthaltenen Schlüssel einbinden, dann mit einem eigenen Zertifikat signieren und mit dem öffentlichen Schlüssel des Abgeordneten verschlüsseln – und hoffen, dass der Empfänger die gleiche Methode anwendet und dann endlich auch verschlüsselt schreiben kann.

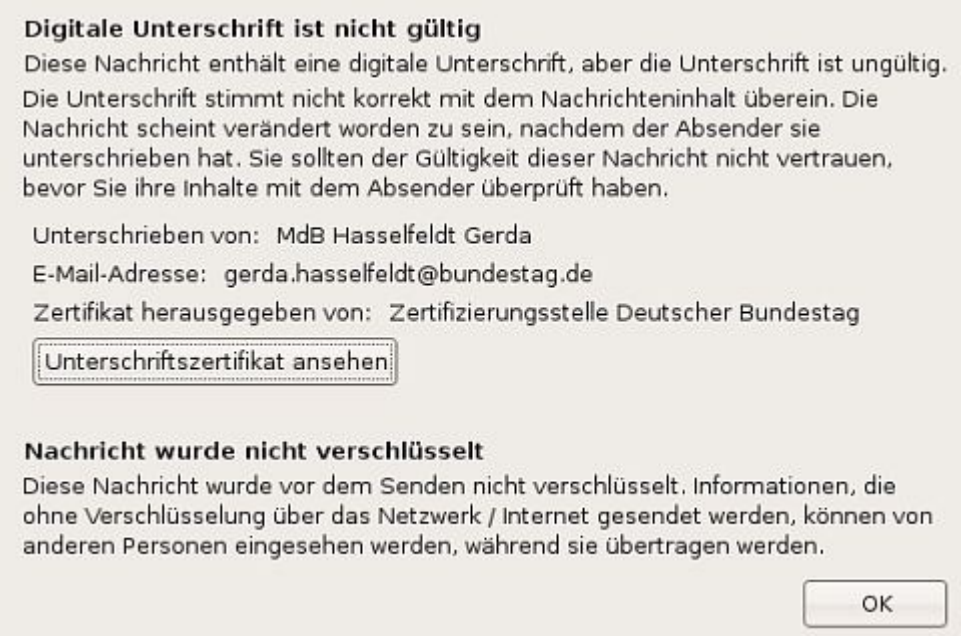
Der Bundestag verwendet nicht die Open-Source-Methode GNU Privacy Guard (GnuPG) oder gar die kommerzielle Version Pretty Good Privacy (PGp) wie etwa das Bundesverfassungsgericht,

sondern verschlüsselt über Secure/Multipurpose Internet Mail Extensions (S/MIME).

Diese Methode hat ihre Tücken: Benutzerfreundlich ist sie nicht, denn kaum ein Computer-Laie wird wissen, wie er oder sie an ein S/Mime-Zertifikat kommen kann und wie das anzustellen sei. Außerdem vertragen sich bei den meisten gängigen E-Mail-Programmen die beiden Verschlüsselungs-Methoden nicht. Thunderbird zum Beispiel arbeitet zuerst die S/Mime-Routinen ab, dann GnuPG. Wenn man eine E-Mail mit S/Mime signiert, kann man GnuPG nicht parallel verwenden, da eine anschließende Verschlüsselung die Mail verändern würde und die Signatur ungültig wäre. Es gibt auch keine Möglichkeit, für bestimmte Empfänger festzulegen, welche S/MIME-Funktion angewendet werden soll. Es ist also immer mühsame Handarbeit angesagt. Das weiß offenbar auch die Pressestelle des Bundestags, die auf Anfrage dazu etwas vage antwortet: „Der Deutsche Bundestag hat sich nur für eine der beiden Alternativen entschieden, da die parallele Verwendung zu technischen und organisatorischen Problemen führen könnte." Der Bundestag hat das zusätzliche Problem, dass er nur eine deutsche Zertifizierungsinstanz benutzen kann. Er ist zwar Certification Authority, kann aber das – auch aus Kostengründen – nicht in gängige Browser und Mail-User-Agenten implementieren lassen.

Am 19. Januar wurden 46 (von 613) nach dem Zufallsprinzip ausgewählte Abgeordnete angeschrieben mit der Bitte: „Bitte schicken Sie mir eine signierte E-Mail zu." Nach einer Woche (!) hatten nur sieben geantwortet, von dem angeschriebenen Abgeordneten der Partei „Die Linke" reagierte sogar niemand. Das Büro von Michael Glos (CSU) war mit am schnellsten: Man wusste offenbar sofort, worum es ging, jedoch fehlte die Signatur. Dafür erfährt man immerhin bei jeder Antwort die eigene IP-Adresse, die man beim Abschicken der E-Mail verwendet hatte – warum auch immer: „Diese Nachricht wurde im Internet des Deutschen Bundestages erfasst – Sa Jan 19

18:03:31 2008 – Externe IP-Adresse: 217.83.70.227.“ Auf Nachfrage reagierte Glos‘ Büro dann nicht mehr.



Eine Mitarbeiterin Volkmar Vogels (CDU) rief sogar an, um sich erklären zu lassen, um welchen unverständlichen Sachverhalt es sich in der fraglichen E-Mail gehandelt habe. Danach scheint das Interesse am Thema aber erloschen zu sein – eine elektronische Antwort kam nicht. Auch das Büro des Bundesinnenministers Wolfgang Schäuble (CDU) schwieg eisern. Zugunsten Schäubles muss erwähnt werden, dass die Standard-Signatur des Autors vermutlich sehr abschreckend wirkt: „Please note that according to the German law on data retention, information on every electronic information exchange with me is retained for a period of six months.“

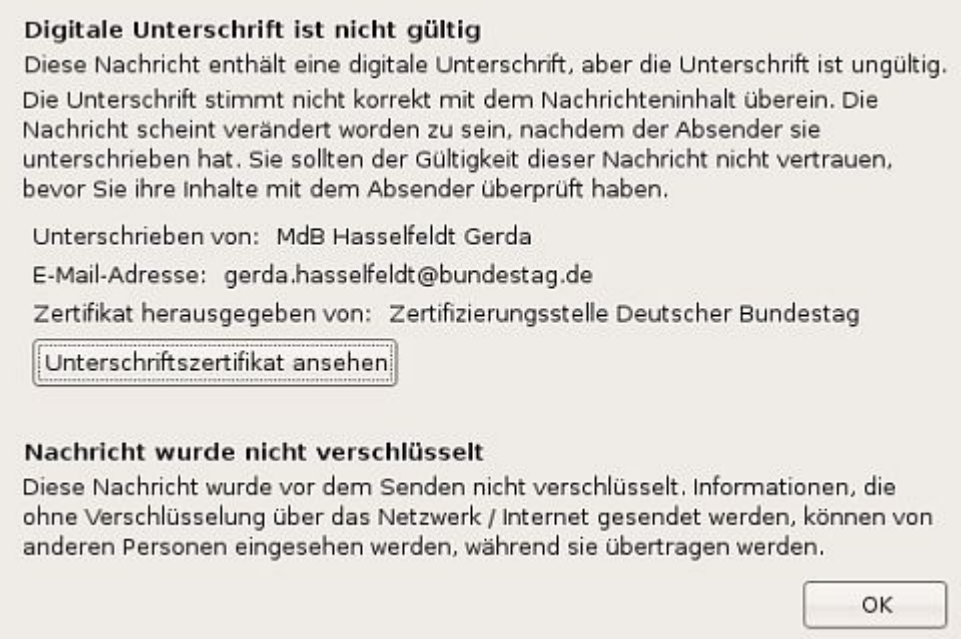
Gerda Hasselfeldt, CDU/CSU, Petra Bierwirth (SPD), Lydia Westrich (SPD) und Miriam Gruß (FDP) antworteten kurzfristig und korrekt signiert, jedoch nur zwei Männer: Markus Löning (FDP) und Hans-Christian Ströbele (Die Grünen). Das Büro Ströbeles, das offenbar zusätzlich die EDV im Bundestag bemühte, kommentierte: „Leider mussten die Techniker einräumen, dass das System noch nicht wirklich gut funktioniert.“ Nur sieben von 47 Mitgliedern des Bundestages reagieren also auf eine E-Mail, die um das bittet, was der Bundestag selbst empfiehlt – eine traurige Bilanz.

Der zweite Schritt gab auch den wenigen Abgeordneten, deren Mitarbeiter verstanden hatten, was eine elektronische Signatur ist, große Rätsel auf:
„Um nachzuprüfen, ob nicht nur die elektronische Signatur, sondern auch die Verschlüsselung funktioniert, bitte ich Sie um eine weitere kurze Mail, die Sie bitte an mich verschlüsseln. Mein öffentlicher Schlüssel (S/Mime) ist in meiner Signatur enthalten."

Nur zwei Abgeordnete – Lydia Westrich und Markus Löning – meisterten diese Hürde und antworteten per verschlüsselter E-Mail. Das Büro von Miriam Gruß gab sich Mühe und kündigte an, man werde sich im Haus sachkundig machen – was aber seitdem offenbar noch nicht von Erfolg gekrönt war. Ein Verantwortlicher für die Technik im Bundestag verriet per verschlüsselter E-Mail, dass es für Probleme dieser Art sogar eine telefonische Hotline gebe und jederzeit Hilfe, falls ein Abgeordneter darum bäte.

Welche technischen Probleme Mitglieder des Bundestag daran hindern könnten, ihre Kommunikation zu verschlüsseln, war nicht zu erfahren. Einige Signaturen wiesen darauf hin, dass die Unterschrift ungültig sei. Das wird vermutlich daran liegen, dass verschlüsselte E-Mails an Bundestagsabgeordnete von einem zentralen Server entschlüsselt werden – ein Prinzip, dass der Idee widerspräche, dass nur der Empfänger einer kodierten Nachricht diese auch lesen sollte. Wie die Sicherheit der Kommunikation zwischen dem Server des Bundestags und Empfänger gewährleistet sei, darüber wollte man keine Details preisgeben. Anna Rubinowicz-Gründler, Pressereferentin im Bundestag, antwortete: „Zu IT-sicherheitsrelevanten Fragen können wir keine Auskünfte erteilen." Auf die Frage, warum ein Kontaktformular, das Signieren und den Austausch von Schlüsseln per S/MIME nicht erlaubt, angeboten wird statt einer funktionierenden E-Mail-Adresse, verwies man darauf, dass „die in das Formular eingetragenen Daten (..) verschlüsselt über ‚HTTPS'

übertragen“ werden. Das bedeutet in diesem Fall nichts, da offenbar niemand genau weiß, wer im Bundestag die Mails welcher Abgeordneten lesen kann. Die mangelnde Fähigkeit oder Bereitschaft der Abgeordneten, ihre E-Mails vor dem Zugriff anderer zu schützen zu wollen, mochte man ebenfalls nicht kommentieren: „Die Pressestelle des Deutschen Bundestages informiert über Sachverhalte, transportiert aber keine Meinungen.“



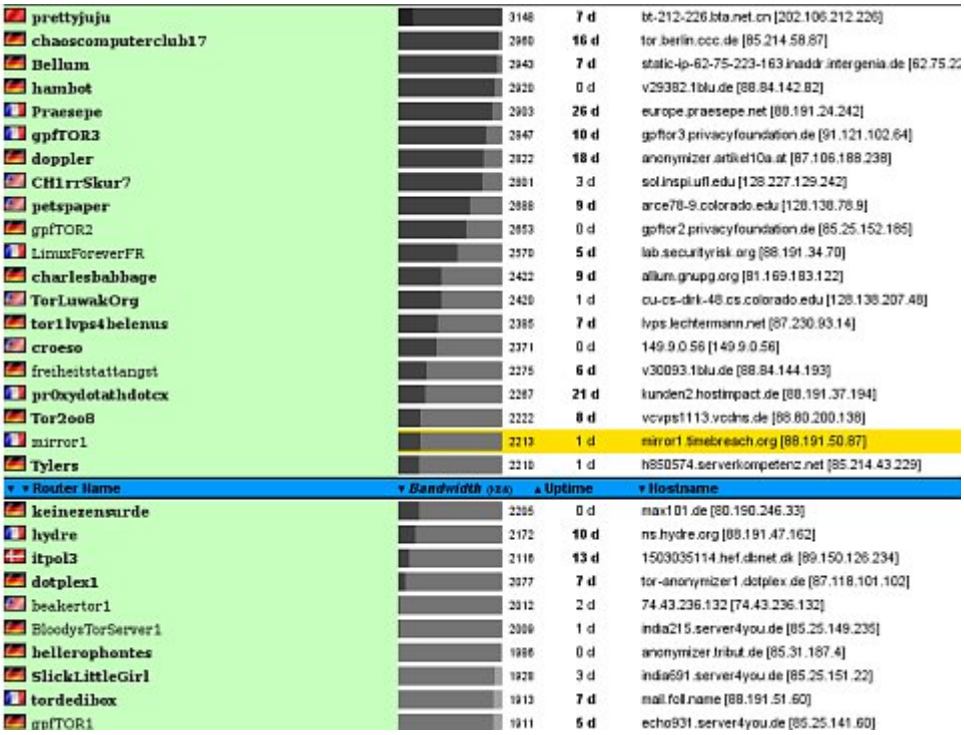
Über diesen Sachverhalt kann man geteilter Meinung sein. Dass ein Abgeordneter des Bundestages keinen technischen Sachverstand besitzt, ist verzeihlich. Dass sie oder er auf auf den Sachverstand verzichtet, der ihm innerhalb des Hauses gratis angeboten wird, ist einfach nur ignorant.

Dieser Artikel erscheint leicht verändert am 04.02.2008 auf Telepolis.

Second Life plus Anonymität ist gleich Terrorismus

Gulli.com beruft sich auf einen Bericht der Washington Post: „Laut einem Bericht der Washington Post finden Vertreter der Geheimdienste Missfallen an diesen dreidimensionalen Spielewelten. Deren weltweite Erreichbarkeit, die Möglichkeiten zur Wahrung der eigenen Anonymität und die Tatsache, dass darüber auch finanzielle Transfers möglich sind, sollen Spiele wie Second Life zu potenziellen Gefahrenquellen machen.“ Im Original: „U.S. intelligence officials are cautioning that popular Internet services that enable computer users to adopt cartoon-like personas in three-dimensional online spaces also are creating security vulnerabilities by opening novel ways for terrorists and criminals to move money, organize and conduct corporate espionage.“ Ich wundere mich, dass Schäuble noch nicht auf die Idee gekommen ist, den Verfassungsschutz in Second Life agieren zu lassen…
Der Screenshot zeigt einen Avatar (mich) beim Terror-Training (Fallschirmspringen) in Second Life.

German Privacy Foundation proudly presents



Die German Privacy Foundation hat vor wenigen ,Tagen den dritten Tor-Server in Betrieb genommen. GpfTOR1, gpfTOR2 und gpfTOR3 sind unter den ersten fünfzig Servern weltwelt.

Weitreichende Kommunikationsstörungen

Man mag mich als hyperkritischen Querulanten abtun oder als Nörgler, aber was da gegen die Vorratsdantenspeicherung an „Argumenten“ durch die Medien rauscht, finde ich zum Teil nur

noch lachhaft. Insbesondere die Pressemitteilung des AK Vorratsdatenspeicherung vom 04.02.2008 und die Beispiele aus dem anonymisierten Schriftsatz überzeugen nicht. Das Problem scheint nicht nur die Vorratsdatenspeicherung zu sein, sondern auch die Ignoranz und penetrante Belehrungsresistenz der Betroffenen. Mein Mitleid hält sich daher in Grenzen, wenn ich mir das Gejammer anhöre.

[X] „schaltet sein Mobiltelefon seit Jahresanfang kaum noch ein, um eine Bewegungsdatenspeicherung zu verhindern. Damit ist er auf diesem Wege nicht mehr erreichbar, etwa für Pressekontakte.“ Meinen die mich? Das Handy ist schon immer die unsicherste Art zu kommunizieren, zumal die Gesetzeslage den Einsatz von IMSI-Catchern erlaubt, mit denen auch Unschuldige mal eben so abgehört werden konnen. Mit dem Handy erzeugt man ohnehin ein Bewegunsprofil. Das hat mit der Vorratsdatenspeicherung rein gar nichts zu tun. Wer das vermeiden willl, muss sich Prepaid-Karten aus dem Ausland besorgen.

[X] „berichtet, er unterlasse beim Surfen im Internet jede Aktivität im Bereich seiner Intimsphäre.“ Dann muss man das Gesetzesvorhaben ausdrücklich loben. Endlich kümmern sich die

Surfer um ihre Privatsphäre! Und wenn die Vorratsdatenspeichung für unzulässig erklärt wird, dann ist den Surfern wieder alles egal?

[X] „Da ich mich bekanntermaßen antifaschistisch und politisch betätige muss ich davon ausgehen, dass meine Daten besonders geprüft werden. Darunter fallen natürlich auch private Kommunikationen. Seit in Kraft treten der Speicherung beschränken sich meine Telefongespräche und Internetkorrespondenz nur noch auf das wesentliche“. So ein Unsinn. Welche Daten werden wie „besonders geprüft“? Man sollte sich ohnehin so verhalten, dass so wenig Daten wie möglich anfallen. Private Kommunikation muss daher verschlüsselt werden. Wer das nicht will, darf nicht weinen und klagen. Und was war noch mal „Internetkorrespondenz“? Instant Messaging per Second Life? Internet Relay Chat? SMTP? Oder Postings im Usenet? All das sollte man ohnehin auf das Wesentliche beschränken und nicht das Internet mit sozialen Geräuschen vollmüllen. „Freunde und Bekannte schreiben unabhängig vom jeweiligen Inhalt weniger Emails und führen lieber persönliche statt Telefongespräche.“ Das ist wohl kaum emprisch beweis- und messbar. Wenn die Vorratsdatenspeicherung dazu führte, dass mehr persönlich miteinander gesprochen würde, fände ich das super. Aber natürlich nur in der Sauna oder im Schwimmbad, weil da am Körper angebrachte Wanzen auffallen und Richtmikrophone feucht werden.

[X] „…habe ich mich aus diversen Foren und chats zurück gezogen und somit leider auch keine Möglichkeit mehr mich mit anderen anonymen opfern aus zu tauschen.“ Schlicht Blödsinn. Man kann IRC und Pseudonyme benutzen und seine IP mit Tor schreddern.

„Gesprächspartner wollten etwa nur noch kurze Gespräche führen, oder es wird ein ‚Knacken in der Leitung‘, ein verlangsamter Internetzugang oder eine sonstige technische Störung gemeldet. […] moniert etwa, er habe ‚das eigenartige Gefühl, das eine dritte Person mithört'“. Jetzt gerät es zur

Comedy. Wer eigenartige Gefühle hat, es würde jemand mithören, aber ansonsten keine Fakten beibringen kann, der sollte den Rat beherzigen, den Helmut Schmidt bei Visionen empfiehlt: Zum Arzt gehen! Was hat dieser gequirlte Quark in einem Schreiben an das Bundesverfassungsgericht zu suchen?

Den größten Quatsch verbreiten wieder hier schon behandelten Heiße-Luft-Spezialisten: „Viele Personen berichten, sie oder ihre Gesprächspartner setzten nun Verschlüsselung, Anonymisierungsdienste oder sonstige Umgehungstechniken ein. Bereits in der Beschwerdeschrift ist darauf hingewiesen worden, dass die Vorratsdatenspeicherung die Nutzung von Verschleierungsmöglichkeiten befördert und dadurch selbst im Fall schwerer Straftaten eine gezielte Überwachung vereiteln kann. Die Initiative 'no abuse in internet“ (naiin), eine von der Wirtschaft getragene Einrichtung zur Bekämpfung von Online-Kriminalität, befürchtet nun in der Tat, ‚dass die Aufklärung von per Internet verübten Straftaten durch die massenhafte Speicherung von Verbindungsdaten weiter erschwert wird.'“ Ja, unter diesen Umständen bin ich selbstredend *für* die Vorratsdatenspeicherung! Setzt mehr Verschlüsselung, Anonymisierungsdienste oder sonstige Umgehungstechniken ein!

„Der Journalist […] schreibt, er schränke seine Internetnutzung im Bereich der Recherche über die elektronischen Medien nun stark ein.“ Dann hat er den Beruf verfehlt und/oder keine Ahnung. Man kann sich dagegen schützen, ausspioniert zu werden. Die geplante Vorratsdatenspeicherung erstellt massenhaft Bewegungsprofile von normalen Bürgerinnen und Bürgern; Kriminelle fängt man natürlich nicht damit. Das Gesetz ist ohnehin nur ein Vorwand, um den Überwachungsstaat populistisch zu verkaufen.

[X] „ist Journalist / Chefredakteur für internationale und nationale Medien und berichtet: ‚Seit dem 01.01.08 haben wir größte Probleme mit Informanten die uns bei brisanten Angelegenheiten nur noch sehr begrenzt Telefonate oder elektronische Kommunikation einsetzen.'“ Ich wette, dass

niemand bei diesem Medium verschlüsselt oder zum Beispiel eine anonyme Nachrichtenbox wie die *German Privacy Foundation* nutzt.

Fazit: Wer solche Freunde hat, braucht keine Feinde mehr. Ich weiß nicht, wen die mit dem Blödsinn beeindrucken wollen. Schäuble und Konsorten werden sich ins Fäustchen lachen.

Grosser Online-Lauschangriff, revisited

Meine Gattin Claudia weist mich zu Recht darauf hin, dass ich ihre juristische Argumentation zum Thema „großer Online-Lauschangriff“ übernommen habe. Aber sicher. Sie sagt:

> *Der entscheidende Unterschied zwischen der Argumentation Buermeyers und der meinen: Buermeyer stellt klar, daß mit technischen Maßnahmen und formalgesetzlich sicher zu stellen ist, daß kernbereichsrelevante Daten geschützt bleiben. Eine darüber hinausgehende Schlußfolgerung ist, daß solange diese technischen Maßnahmen nicht vorhanden sind, die Online-Durchsuchung in jedweder Form mit der derzeitigen Rspr. des BverfG zum Kernbereichsschutz nicht in Einklang zu bringen ist.*

Meine Gattin hat natürlich Recht.

Security by obscurity im Bundestag

Ein Artikel von mir auf Telepolis (04.02.2008): „Security by obscurity im Bundestag – Über Ahnungslosigkeit, Versagen und S/Mime. Der Bundestag [extern] bietet an, den Abgeordneten verschlüsselte E-Mails senden zu können. Das hört sich gut an, funktioniert aber nicht: Kaum ein Abgeordnetenbüro weiß damit umzugehen. Bei technischen Fragen geht man zudem nach dem Motto vor: Security by obscurity.“ [mehr…]

Grosser Online-Lauschangriff?

Die aktuellen juristischen Gutachten zur „Online-Durchsuchung“ sind sich in zwei Fragen einig: Technisch ist sie kaum machbar, und gegen sie sprechen schwer wiegende verfassungsrechtliche Bedenken. Das Bundesinnenministerium ficht das nicht an. Dessen Informationspolitik kann auch zu dem Fazit führen, dass die die Öffentlichkeit – wider besseres Wissen der Verantwortlichen – getäuscht werden soll.

Der Dritte Strafsenat des Bundesgerichtshofs hat schon vor einem knappen Jahr die „verdeckte Online-Durchsuchung“ verboten. In Kürze wird entschieden, ob die Verfassungsbeschwerde gegen deren bisher einzige juristische Ermächtigungsgrundlage, das nordrhein-westfälische Verfassungsschutzgesetz, Erfolg haben wird. Das Bundesverfassungsgericht wird über die so genannte „Online-Durchsuchung? jedoch nur indirekt urteilen. Im fraglichen Gesetz heißt es wörtlich, es gehe um „heimliches Beobachten und sonstiges Aufklären des Internets, wie insbesondere die

verdeckte Teilnahme an seinen Kommunikationseinrichtungen bzw. die Suche nach ihnen, sowie der heimliche Zugriff auf informationstechnische Systeme auch mit Einsatz technischer Mittel.“ Der Begriff „Online-Durchsuchung? kommt im Text gar nicht vor. Die Idee, die Strafverfolger und die Behörden würden auf privaten Rechnern heimlich Software installieren können, ist eine Erfindung der Medien, insbesondere der Süddeutschen (07.12.2006) und der taz (30.01.2007). Der polizeiliche „Hackerangriff“ hat sich jedoch im allgemeinen Sprachgebrauch und seit dem Medienhype vor einem Jahr auch als Wunschvorstellung in der Politik eingebürgert.

Ulf Buermeyer, wissenschaftlicher Mitarbeiter beim Bundesverfassungsgericht, hat im August 2007 in einem Aufsatz umrissen, warum schon aus der vergangenen Rechtsprechung abgeleitet werden kann, dass ein heimlicher Zugriff des Staates auf private Rechner, wie von Schäuble befürwortet, schlicht verfassungswidrig ist. Unter „Zugriff? kann man verstehen, mit Hilfe technischer Mittel den Rechner eines Verdächtigen – ohne dessen Wissen – über einen bestimmten Zeitraum zu überwachen, auch ohne dass die dazu notwendige Software „online? implementiert werden müsste. Das ist ohnehin noch nie erfolgreich geschehen, trotz gegenteiliger Meldungen in den Medien, und auch äußerst unwahrscheinlich, da sich jeder dagegen mit einfachen Mitteln schützen könnte.

Buermeyer zweifelt in seinem Text „Die „Online-Durchsuchung“. Verfassungsrechtliche Grenzen des verdeckten hoheitlichen Zugriffs auf Computersysteme? nicht nur daran, dass die Ermittlungsmethode der Online-Durchsuchung „jemals effektiv wird angewendet werden können?, sondern führt zwei gewichtige juristische Argumente an, die das Bundesverfassungsgericht zu erwägen habe – die Unverletzlichkeit der Wohnung nach Artikel 13 Absatz 1 des Grundgesetzes und den so genannten „Kernbereichsschutz“ privater Lebensgestaltung. Interessant ist der Aufsatz Buermeyers vor allem deshalb, weil er beweist, dass das Bundesverfassungsgericht seine bisherige Rechtsprechung über den Haufen werfen müsste, erlaubte es das, was dem Bundesinnenministerium vorschwebt (zum Beispiel in den „Fragen und Antworten zur Online-Durchsuchung“.

Das Bundesverfassungsgericht hat am 3. März 2004 zum „Großen Lauschangriff“ geurteilt, das Grundrecht auf Unverletzlichkeit der Wohnung meine nicht nur den Schutz vor unerwünschter

physischer Anwesenheit eines Vertreters der Staatsgewalt in allen Räumen, die privat und beruflich genutzt werden – inklusive Keller, Balkon und Garten, ja sogar ein zeitweilig genutztes Hotelzimmer. Es ging noch viel weiter:

> *„Die heutigen technischen Gegebenheiten erlauben es, in die räumliche Sphäre auch auf andere Weise einzudringen. Der Schutzzweck der Grundrechtsnorm würde vereitelt, wenn der Schutz vor einer Überwachung der Wohnung durch technische Hilfsmittel, auch wenn sie von außerhalb der Wohnung eingesetzt werden, nicht von der Gewährleistung des Absatzes1 umfasst wäre.“*

Die wenigen Juristen, die eine heimliche „Online-Durchsuchung“ für unbedenklich halten, kommen um diese Argumentation des Bundesverfassungsgerichts nicht herum. Die Wohnung ist sakrosankt, und was das Bundesverfassungsgericht einmal entschieden hat, besitzt quasi Gesetzeskraft. Man kann das nur durch verbale Taschenspielertricks umgehen. Einige Juristen konstruieren um den Computer einen „virtuellen Raum?, der mit einem Online-Anschluss entstehe und der daher nicht mehr zur „Wohnung? gehöre (*vgl. Beulke/Meininghaus: „Anmerkung zur Entscheidung des BGH vom 21.2.2006 StV 2007, S. 63*). Noch abwegiger ist zum Beispiel die These, derjenige, der sich des Internet bediene, wüsste, dass sein Computer „hierdurch vielfältigen Angriffen durch Würmer usw.“ ausgesetzt sei. Der Nutzer nehme das somit in Kauf, öffne sein System selbst und begebe sich damit in die „Sozialsphäre?, die keine „Wohnung? mehr sei. Dr. Jürgen P. Graf, damals Oberstaatsanwalt beim Bundesgerichtshof, meinte noch 1999 in der Deutschen Richterzeitung, der Anbieter von Daten erkläre sich mit der Eröffnung des freien Zugangs im Internet „mit dem Zugriff durch beliebige Dritte? automatisch einverstanden. Mit dem technischen Sachverstand der meisten Juristen ist es ohnehin nicht sehr weit her. Die überwiegende Anzahl der Autoren nimmt es unkritisch als Tatsache hin, dass ein – wie auch immer gearteter – „Bundestrojaner“ technisch umsetzbar sei. Man

könnte auf ähnlichem Niveau auch darüber diskutieren, ob der Einsatz einer Tarnkappe – wie im Nibelungenlied – für Polizisten der Verfassung entspräche.

Buermeyer aber war Netzwerk-Administrator der Universität Leipzig und ist daher eine Ausnahme. Die zweite Säule seiner Argumentation, warum eine Online-Durchsuchung verwassungswidrig sei, ist der Schutz des Kernbereichs privater Lebensgestaltung. Der fußt auf der durch den Artikel 1 des Grundgesetzes geschützten unantastbaren Menschenwürde. Noch nicht einmal der Bundestag könnte diesen Artikel mehrheitlich abschaffen oder verändern:

> *„Aus der Menschenwürdegarantie folgt nach der Rechtsprechung des Bundesverfassungsgerichts zwar nicht, dass ein heimliches Vorgehen des Staates schlechthin unzulässig wäre, denn allein darin, dass der Mensch zum Objekt der Beobachtung wird, ist noch nicht zwingend eine Missachtung seines Wertes als Mensch zu erblicken. Gleichwohl ist bei staatlichen Beobachtungen ein unantastbarer Kernbereich privater Lebensgestaltung zu wahren, denn würde der Staat in ihn eindringen, verletzte dies die jedem Menschen unantastbar gewährte Freiheit zur Entfaltung in den ihn betreffenden höchstpersönlichen Angelegenheiten. Selbst überwiegende Interessen der Allgemeinheit können einen Eingriff in diesen absolut geschützten Kernbereich privater Lebensgestaltung nicht rechtfertigen. Insbesondere ist kein Raum für eine Abwägung mit kollidierenden Rechtsgütern wie dem staatlichen Strafverfolgungsinteresse.“*

In diesem „Kernbereich? darf der Staat noch nicht einmal Daten erheben. Das hat das Bundesverfassungsgericht eindeutig formuliert und damit auch allen Ideen eines „Richterbands“ oder „Richtervorbehalts? eine Absage erteilt. Für die Online-Durchsuchung heißt das: Da es keine technischen Möglichkeit gibt, auf einem Rechner vorab „private“ Daten, die unter diesen „Kernbereich“ fallen, von denen zu trennen, für die das

eventuell nicht zutrifft, verbietet sich der Einsatz heimlicher staatlicher Schnüffel-Software sogar bei Keyloggern.

Das Bundesinnenministerium müsste genug sachverständige Experten haben, die sowohl die juristische Argumentation als auch die technischen Implikationen nachvollziehen könnten. In den „Fragen und Antworten zur Online-Durchsuchung“, die mittlerweile auch auf der Website des Bundeskriminalamts verlinkt ist, wird jedoch das Gegenteil suggeriert. Auf das Urteil des Bundesgerichtshofs gegen die Online-Durchsuchung wird mit keinem Wort eingegangen, bloße technische Spekulationen werden für bare Münze ausgegeben:

> *„Bevor eine Online-Durchsuchung durch Beamte des Bundeskriminalamts (BKA) durchgeführt wird, prüft ein unabhängiger Richter grundsätzlich, ob diese Durchsuchung auf einem PC einer Privatperson oder in einer Firma durchgeführt werden darf.“ (…) Die Ermittlungs-Software wird nicht zu einer Beeinträchtigung der auf dem betroffenen Rechner installierten Sicherheitssoftware führen. (…) Sollte die Software dennoch entdeckt werden, wird sie vom Zielsystem entfernt.“*

Diese drei Thesen haben weder eine rechtliche Grundlage noch sind sie als unverbindliche Idee gekennzeichnet. Technisch erscheinen sie ohnehin als unsinnig. Eine derartige Software – inklusive einer Art Selbstzerstörungsmechnismus und der Möglichkeit, gerichtfeste Daten zu bekommen – gibt es noch nicht und wird es wohl auch nicht geben. Das Gutachten Prof. Ulrich Siebers zum Beispiel bekräftigt das differenziert: „Nach den Standards für digitale Forensik ist die Analyse eines im Betrieb befindlichen Systems problematisch, da ständig Daten verändert werden." Falls die Daten einen dümmsten anzunehmenden Kriminellen „online" zu den Strafverfolgern gelangten, hätte die Staatsanwaltschaft größte Probleme, deren Authentizität zu beweisen.

Das Bundesinnenministerium verweigert über den technischen Hintergrund jede Auskunft. Auch auf einfache Fragen erhält man keine Anwort, zum Beispiel:

„Ist Ihnen bekannt, dass sich jeder Computer-Nutzer leicht dagegen schützen kann, dass ihm unbemerkt Fremdsoftware auf den Rechner „gespielt" wird, wenn man sich an die Ratschläge des Bundesamtes für Sicherheit in der Informationstechnik hält? Wie kann verhindert werden, dass Terroristen die Ratschläge des BSI zum Thema Internet-Sicherheit beherzigen? Ist ihnen bekannt, dass bis jetzt in Deutschland noch kein erfolgreicher Versuch seitens des Bundeskriminalamtes und des Verfassungsschutzes (nach dessen eigenen Angaben) stattgefunden hat, einem Verdächtigen ohne dessen Wissen eine Software auf den Rechner zu spielen, um einen so genannten Remote-Access-Zugang zu erhalten? Haben Sie vor der Veröffentlichung „Fragen und Antworten zum Thema Online-Durchsuchungen" den Rat Sachverständiger eingeholt, ob eine Online-Durchsuchung überhaupt technisch umsetzbar sei? Was veranlasst Sie zu der Annahme, das sei zukünftig der Fall?

Markus Beyer, Pressereferat des Bundesinnenmministeriums antwortet nur:

> *„Wie Sie wissen handelt es sich bei der geplanten sog. Onlinedurchsuchung, wie auch bei der geplanten Novelle des BKA-Gesetzes insgesamt, um einen laufenden Gesetzgebungsprozess auf Fachebene, der noch nicht abgeschlossen ist. Daher bitten wir um Verständnis, dass wir auf weitere Detailfragen derzeit nicht eingehen können. (…) Insbesondere darf ich darauf hinweisen, dass das Bundesverfassungsgericht allein über eine Regelung des Landes NRW (!) entscheidet. Die geplante Novelle des BKA-G ist nicht Gegenstand der Verhandlung beim Bundesverfassungsgericht.“*

Man tut also so, als ob das möglich sei. Und da das Bundesverfassungsgericht nur über das Verfassungsschutzgesetz eines Bundeslandes befinden will, macht man einfach so weiter, als gebe es die vergangene und aktuelle Rechtsprechung gar nicht. Der Verdacht drängt sich auf, dass man in Schäubles Haus schlicht keine Ahnung hat, wie man das gewünschte polizeiliche „Hacken? bewerkstelligen will. Nur völlig unerfahrene Computer-Nutzer sind durch die wolkigen Formulierungen zu beeindrucken, Terroristen vermutlich nicht.

Auch der bayerische Innenminister Joachim Herrmann forderte in einem
Interview „Online-Durchsuchungen“. Herrmann ist ebenfalls nicht in der Lage, auf nur eine der ihm gestellten Fragen substanziell zu antworten – weder auf die juristischen noch auf die technischen. Zum Beispiel:

„Auf Grund welcher Annahmen geht Herr Joachim Herrmann davon aus, dass es Zukunft eine funktionsfähige Methode zur „Online-Durchsuchung‘ privater Rechner geben wird?“

Oder: „Das Bundesverfassungsgericht hat in einer Entscheidung zum Niedersächsischen Polizeigesetz seine Feststellungen aus dem Jahre 2004 zum Schutz des Kernbereichs privater Lebensgestaltung vor Eingriffen des Staates nochmals verdeutlicht. Das Gericht hebt hervor, ein Erhebungsverbot

bestehe, wenn in einem konkreten Fall Anhaltspunkte vorliegen, dass eine Überwachungsmaßnahme Inhalte erfassen könne, die zu dem definierten Kernbereich gehören. Frage: Wie kann der Schutz des Kernbereichs privater Lebensgestaltung garantiert werden, wenn eine Software auf dem Rechner des Verdächtigen ohne dessen Wissen installiert worden ist?“

Die lapidare Antwort – per Word-Attachment – von Karl Michael Scheufele, dem Pressesprecher des Bayerischen Staatsministeriums des Innern: „Moderne Kommunikationstechnik darf nicht die Folge haben, dass Terroristen rechtsfreie Räume für Verbrechensplanung haben. Wenn solche Organisationen sich dieser Kommunikationsmittel bedienen, dann müssen die Sicherheitsbehörden die Möglichkeiten haben, darauf zu reagieren. Selbstverständlich werden die verfassungsrechtlichen Vorgaben des BverfG eingehalten.“

Man darf getrost annehmen, dass hier der Wunsch der Vater des Gedankens ist. Aber die Leitmedien argumentierten beim Thema auch nicht gehaltvoller als die Politiker. Auf der Website der

Tagesschau wird seit Monaten eine Infografik präsentiert, die suggeriert, eine Online-Durchsuchung würde im Sinne Schäubles schlicht funktionieren, ohne die skeptischen Einwände der IT-Fachleute auch nur ansatzweise zu berücksichtigen. Der Redaktion von tagesschau.de gelang es im Lauf einer Woche nicht, trotz mehrmaliger Anrufe und einiger E-Mails, den zu benennen, der die Infografik erstellt hatte.

„Ist tagesschau.de bekannt, dass es bis jetzt noch keine einzige erfolgreiche Online-Durchsuchung gegeben hat? Was veranlasst tagesschau.de anzunehmen, dass die in der Info-Grafik vorgestellten „Methoden" umsetzbar und praktikabel seien?"

Auch darauf gab es keine Antwort. Was zu beweisen war.

Dieser Artikel erschien leicht gekürzt am 28.01.2008 in Telepolis. Fotomontagen: Burks mit Material des Bundestags und der Tagesschau.

Angriff auf das Briefgeheimnis

Interessanter Artikel in der Zeit Online (22.01.2008) : „Angriff auf das Briefgeheimnis"

(…) „Kaum bekannt ist jedoch, dass die US-Behörden auch bei Paketen, Päckchen und Briefen schon seit mehreren Jahren verlangen, dass ihnen vorab Daten über Absender, Empfänger und – sofern verfügbar – über den Inhalt mitgeteilt werden. (…) Die amerikanische Zoll- und Grenzbehörde CBP (Customs and Border Protection) verlangt bisher bei Express-Paketen die elektronische Bereitstellung der Kundendaten noch vor dem

Eintreffen in den USA. Vier Stunden vor der Landung des Transportflugzeugs müssen die Daten den US-Behörden vorliegen. Ein Handelsabkommen (Trade Act) mit der EU von 2004 sieht vor, dass diese Daten auch an Strafverfolgungsbehörden weitergeben werden und mit kommerziellen Datenbanken abgeglichen werden dürfen. (…) Die Posttochter DHL liefert die Daten bei Express-Sendungen aber bereits, darunter auch die Zollinhaltsangabe, die auf den Paketen gemacht werden muss. DHL, ursprünglich eine amerikanische Firma, hat seinen Sitz in den USA und Deutschland. Auf diesem Wege wurden klammheimlich amerikanische Gesetze auch auf Deutschland ausgedehnt.“ (…) [mehr…]

Track your partner!

www.track-your-partner.com – einfach die gesuchte Handynummer eingeben und auf den Kartenausschnitt warten…

Terroristen und Kinderporno-Zirkel

Die dämlichste Argumentation *gegen* die Vorratsdatenspeicherung liefern laut Heise die Heiße-Luft-Produzenten naiin („no abuse in internet“ – was auch immer das bedeutet):

> *Bei der Wirtschaftsinitiative „no abuse in internet“ (naiin) sind derweil Zweifel am Nutzen der Vorratsdatenspeicherung laut geworden. Die Einrichtung zur Bekämpfung von Online-Kriminalität sorgt sich sogar, dass die Aufklärung von per Internet verübten Straftaten durch die massenhafte Speicherung von Verbindungsdaten weiter erschwert werde. „Es ist davon auszugehen, dass sich Täter in dem Wissen, ständig überwacht zu werden, stärker abschirmen werden als bisher“, gibt naiin-Präsident Arthur Wetzel zu bedenken. Der Grad der Abschottung, der etwa bei Terroristen und Kinderporno-Zirkeln ohnehin schon sehr hoch sei, dürfte so weiter zunehmen. Selbst Kleinkriminelle würden fortan wohl vorsichtiger agieren und somit angesichts der technischen Möglichkeiten zur Umgehung der pauschalen Überwachungsmaßnahme schwerer zu fassen sein.*

Woher wollen die eigentlich wissen, wie „Terroristen und Kinderporno-Zirkel“ sich „abschotten“? Die „Logik“ ist also: Wenn es keine Vorratsdatenspeicherung gebe, seien Kriminelle unvorsichtiger. Das ist doch grober Unfug.

Bei *naiin* heisst es: „Immerhin ist naiin die bis dato einzigste [sic] durch die Bundesregierung ausgezeichnete Initiative, die sich der aktiven Bekämpfung von Internet-Kriminalität verschrieben hat.“ Soso. Wie diese Bekämpfung aussieht, kann man in der unkritischen und falschen

Berichterstattung über die Operation Himmel sehen. *Naiin* ist für Zensur und gründete sich ursprünglich als eine PR-Aktion deutscher Provider. Ceterum censeo: *Naiin* ist so überflüssig wie der Verfassungsschutz.

Heilige Festplatten

„Heimliche Online-Durchsuchung unverzichtbar“, lesen wir bei Heise. Es redete der hessische Staatssekretär Harald Lemke:

> *Lemke ermahnte die Zuhörer, nicht technisch veralteten Vorstellungen nachzuhängen. Es sei längst so, dass Terroristen und die organisierte Kriminalität sich über das Internet koordinieren, ohne dabei E-Mail zu nutzen. Längst würden sie eine End-to-End-Veschlüsselung einsetzen, die nur dadurch zu überwinden sei, dass man vor der Verschlüsselung auf das System zugreift. „Die Vorstellung, dass die Festplatte heilig ist, ist eine veraltete Vorstellung.“*

Nun, mit Religion hat die Festplatte wenig zu tun. Es handelt sich eher um eine Frage der so genannten freiheitlich-demokratischen Gundordnung. Die besagt unter anderem, dass die Entscheidungen des Bundesverfassungsgerichts auch für Politiker bindend sind. Ich zitiere aus meinem Artikel „Großer Online-Lauschangriff?“ bei Telepolis aus dem Urteil des BVerfG zum „Großen Lauschangriff“:

> *Aus der Menschenwürdegarantie folgt nach der Rechtsprechung des Bundesverfassungsgerichts zwar nicht, dass ein heimliches Vorgehen des Staates schlechthin unzulässig wäre, denn allein darin, dass der Mensch zum Objekt der Beobachtung wird, ist noch nicht zwingend eine Missachtung seines Wertes als Mensch zu erblicken. Gleichwohl ist bei staatlichen Beobachtungen*

> *ein unantastbarer Kernbereich privater Lebensgestaltung zu wahren, denn würde der Staat in ihn eindringen, verletzte dies die jedem Menschen unantastbar gewährte Freiheit zur Entfaltung in den ihn betreffenden höchstpersönlichen Angelegenheiten. Selbst überwiegende Interessen der Allgemeinheit können einen Eingriff in diesen absolut geschützten Kernbereich privater Lebensgestaltung nicht rechtfertigen. Insbesondere ist kein Raum für eine Abwägung mit kollidierenden Rechtsgütern wie dem staatlichen Strafverfolgungsinteresse.*

Also: Finger weg von meinen Festplatten!

E-Mail-Attachment für 3000 Euro

Lustige Meldung auf golem.de (28.01.2008): „Wer soll den Bayern-Trojaner bezahlen?“

> *„Das Konzept der Firma DigiTask sieht es vor, auf dem PC des Überwachten eine so genannte Skype-Capture-Unit zu installieren. Diese Capture-Unit ermöglicht das Mitschneiden der Skype-Kommunikation, wie zum Beispiel Voice und Chat, sowie die Ausleitung an einen anonymen Recording-Proxy. […] Für die Installation der Skype-Capture-Unit wird eine ausführbare Datei mitgeliefert die zum Beispiel als Anhang an eine E-Mail versendet werden kann oder aber direkt auf dem Zielsystem installiert werden kann.“*

Bruhahaha. Sehr interessant ist vor allem das Original-Dokument: Der Verdächtige nutzt etwas ganz gefährlich Modernes

– das Internet undsoweiter.

> *Nach Installation greift der Trojaner der Firma DigiTask die gewünschten Informationen vor der Verschlüsselung durch Skype ab, verschlüsselt sie mit AES und leitet sie an einen „anonymen Recording-Proxy“ weiter. Von dort werden die Daten „an den eigentlichen Recording-Server“ übertragen, wo der Zugriff „mittels mobiler Auswertestationen“ erfolgen kann.*

Aha. Und wie wollen Sie die Software auf den Rechner bekommen? Ich sag’s ja: Mindestens drei Mal heimlich einbrechen. Erstens herausfinden, welches Betriebssystem der Verdächtige hat. Dann den Bayern-Trojaner bauen. Dann zweitens wieder einbrechen und ihn implementieren. Dann drittens noch mal einbrechen und ihn wieder abholen. Und in der Zwischenzeit hat er sich dann ein Laptop von Apple gekauft und telefoniert darüber – und alles war für die Katz‘.

Ein Haufen Irrer. Mehr kann ich dazu nicht sagen.

Großer Online-Lauschangriff

Ein Artikel von mir auf Telepolis: „Großer Online-Lauschangriff? – Die aktuellen juristischen Gutachten zur „Online-Durchsuchung“ sind sich in zwei Fragen einig: Technisch ist sie kaum machbar, und gegen sie sprechen schwer wiegende verfassungsrechtliche Bedenken“. [mehr…]

Fragen und Antworten zum Thema Online-Durchsuchungen, revisited

Hier, wie angekündigt, die Antworten des Bundesinnenministeriums auf meinen