Ausreichend Sachverstand

Fragenkatalog der SPD-Bundestagsfraktion / AG Kultur und Medien / AG Neue Medien an den Bundesinnenminister, 22. August 2007:

> *Frage:Wer berät sachverständig die Sicherheitsbehörden und das BMI bei der Konfiguration von Online-Durchsuchungen?*
> *Antwort:Die Sicherheitsbehörden und das Bundesministerium des Innern verfügen grundsätzlich über genügenden Sachverstand.*

Das hatte ich noch nicht gelesen…. Dann kann ja nichts mehr schiefgehen.

Duo faciunt collegium terroristicum?

Lauschen wir den Worten August Hannings, seines Zeichens Staatssekretär im Bundesinnenministerium und Ex-Chef des Bundesnachrichtendienstes (BND): „Wir sollten etwa darüber nachdenken, ob es noch zeitgemäß ist, dass drei Täter zusammenkommen müssen, um den Straftatbestand der Bildung einer terroristischen Vereinigung zu erfüllen“.

Drei? Sind das nicht schon viel zu viele? Nein, viel zu inkonsequent, Herr Hanning. Auf ein Wort: *Eine* Person sollte schon ausreichen, um eine terroristische Vereinigung zu bilden, vor allem dann, wenn sie manchmal Selbstgespräche führt. Und die kann man bestimmt nachweisen, wenn man sie nach Damaskus zu den befreundeten Behörden schickt und sie dort foltern lässt. Dann würde die verdächtige Person sicher alles

zugeben, auch ohne die von Ihnen so geliebte Online-Durchsuchung.

BVerfG 2008

Schöne Übersicht über die Verfahren, in denen das Bundesverfassungsgericht anstrebt, im Jahre 2008 unter anderem zu entscheiden (Auszug):
– 1 BvR 1299/05 – Verfassungsbeschwerde gegen Vorschriften des Telekommunikationsgesetzes betreffend die Bereithaltung und den Abruf von Telekommunikations-Bestandsdaten zu Zwecken der öffentlichen Sicherheit.
– 1 BvR 370/01 | 1 BvR 595/07 – Verfassungsbeschwerden gegen Vorschriften des nordrhein-westfälischen Verfassungsschutzgesetzes, unter anderem betreffend so genannte **Online-Durchsuchungen**.
– 1 BvR 2074/05 | 1 BvR 1254/07 – Verfassungsbeschwerden gegen polizeirechtliche Vorschriften über die automatisierte Erfassung von Kfz-Kennzeichen zum Zweck des Abgleichs mit dem Fahndungsbestand.
– 1 BvR 1602/07 | 1 BvR 1606/07 | 1 BvR 1626/07 – Verfassungsbeschwerden gegen Grundsatzurteile des Bundesgerichtshofs zum Verhältnis von Pressefreiheit und Bildnisschutz Prominenter (Caroline von Hannover).
– 1 BvR 462/06 – Verfassungsbeschwerde eines Professors einer theologischen Fakultät, der bisher das Fach „Neues Testament“ in Forschung, Lehre und Weiterbildung vertrat, betreffend eine Verfügung der Universität, mit der er unter Abänderung der bisherigen Einweisungsverfügung künftig das Fach „Geschichte und Literatur des frühen Christentums“ vertreten soll.
– 1 BvR 1886/06 – Verfassungsbeschwerde zur Frage, ob ein Rechtsanwalt Beratungsleistungen in einem Internetauktionshaus versteigern darf.

– 1 BvR 1620/04 – Verfassungsbeschwerde zur Frage, ob es (insbesondere) mit Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG vereinbar ist, einen Vater zum Umgang mit seinem Kind mittels der Androhung eines Zwangsgeldes zu zwingen.

Anti-Terror-Kampf im Internet


Anti-Terror-Kampf im Internet

„Der Verfassungsschutz muss die Möglichkeit erhalten, auf Internet-Festplatten zuzugreifen, um inländische Terrorzellen aufzuspüren und zu beobachten", sagte Innenminister Ingo Wolf (FDP) zur WAZ.

Ich habe mir jetzt den Original-Artikel aus der WAZ besorgt, der den Medien-Hoax um die „Online-Durchsuchung" maßgeblich beeinflusst hat. In meinem Telepolis-Artikel vom 06.02.2007 hieß es:

> *Wolf hat überhaupt nichts von „Online-Durchsuchungen" gesagt. Im August 2006 heißt es im Heise-Newsticker korrekt nur, es solle jetzt das Internet überwacht werden. Die dort erwähnte Formulierung „Zugriff auf Internet-Festplatten" stammt aus der Welt. Die wiederum bezieht sich auf ein Interview der WAZ vom 28.08.2006 mit Ingo Wolf: ‚Der Verfassungsschutz muss die Möglichkeit erhalten, auf Internet-Festplatten zuzugreifen, um inländische Terrorzellen aufzuspüren und zu beobachten.' Das ist allgemein formuliert und bedeutet gar nichts Konkretes. Was mit „Internet-Festplatten" gemeint ist, kann man nur vermuten: Festplatten in den Rechnern der Provider, im Gegensatz zu privaten Festplatten, die manchmal offline*

sind?

Aus den „Internet-Festplatten“ haben dann die Medien private Computer gemacht – und die urbane Legende des Behörden-Hackers war geboren. Demnächst mehr in einem größeren Werk…

Tarnkappe und Lichtschwert

Interessante Diskussion zur „Online-Durchsuchung“ auf beck-blog…

Wählt Dreier!

Die taz schreibt: „‚Herr Dreier vertritt in der Frage der Menschenwürde und des Lebensschutzes fundamental andere Positionen als die CSU‘, sagte etwa am Wochenende Bayerns Ministerpräsident Günter Beckstein. Auf Unverständnis stieß außerdem, dass Dreier den christlichen Kirchen vorhält, sie hätten erst spät ein positives Verhältnis zu den Menschenrechten entwickelt. Diese hätten „vielfach gegen den Widerstand“ der Kirchen erkämpft werden müssen. Laut FAZ gingen Unionsvertreter in den Ländern deshalb davon aus, Dreier sei ein „kämpferischer Atheist“. Tatsächlich ist Dreier aber sogar Mitglied des Hochschulbeirats der Evangelischen Kirche.“ Frage: Warum muss man irgendein höheres Wesen verehren, um Verfassungsrichter zu sein? Primitiver Aberglauben hat beim Bundesverfassungsgericht bekanntlich nichts zu suchen. Anderenfalls könnte das BVerfG auch gleich

die Online-Durchsuchung durchwinken….

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.

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.

Bundesverfassungsgericht entscheidet

Am 27.02.2008 will das Bundesverfassungsgericht über die Klage gegen das nordrhein-westfälische Verfassungsschutzgesetz entscheiden („Online-Durchsuchung").
Nachtrag, 03.02.2008: [Heise] „Entscheidung zur Onlinedurchsuchung rückt näher"

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!

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…]

Eingemauerte Speichermedien

HRSS 1/2008: „‚Online-Durchsuchung light‘ – Die Änderung des § 110 StPO durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung“

> *3. Der Begriff der räumlich getrennten Speichermedien*
> *a) Nach Absatz 3 darf von einem Speichermedium auf ein anderes, räumlich getrenntes elektronisches Speichermedium zugegriffen werden. Der vom Gesetzgeber gewählte Begriff des „Speichermediums“ ist unglücklich. Regelmäßig haben Speichermedien wie DVDs, USB-Speichersticks oder Festplatten keine eigene Programmlogik, die es ermöglicht, von ihnen auf*

> *andere Geräte zuzugreifen. Der Begriff kann nach Sinn und Zweck daher nur so verstanden werden, dass als „Speichermedium von dem zugegriffen wird“ ebenso wie das Speichermedium auf das zugegriffen wird, ein Computersystem zu verstehen ist. Bei einem solchen handelt es sich um ein programmierbares System mit Eingabe-, Ausgabe- und Speichermöglichkeiten“…*

Harhar. Ich schlage folgende Methode vor: Eine externe Festplatte wird samt Stromanschluss in die Wand eingemauert und kommunziert mit dem Hauptrechner via Bluetooth. Dann laufen die Hausdurchsucher demnächst mit Wünschelruten und Metalldetektoren durch die Wohnung.

„Bayerntrojaner“ zum Abhören von Internet-Telefonie?

Den Heise-Artikel: „Ein „Bayerntrojaner“ zum Abhören von Internet-Telefonie?“ schauen wir uns jetzt unter der Lupe an, die nach Fakten sucht, nicht aber nach Vermutungen und Mutmaßungen. Ein Schreiben des bayerischen Justizministeriums ist der Piratenpartei zugespielt worden, behauptet diese. (Bevor man das nicht im Original gesehen hat, kann es auch ein Wahlkampfgag sein.) Das Schreiben enthalte „Indizien eines erfolgten Einsatzes von Trojanern zum Abhören von Skypetelefonaten und technische Details der eingesetzten Software.“ Merkmale der Software:

> ** Installation durch die Polizei vor Ort oder per E-Mail*
> ** spurenlose Möglichkeit, die Software zu aktualisieren, erweitern und zu entfernen*
> ** Versenden der Daten an und über einen Rechner außerhalb des*

deutschen Hoheitsgebietes
** Zugriff auf interne Merkmale des Skypeclients*
** Zugriff auf SSL-verschlüsselte Websites*

Sicher ist, dass dieses Schreiben Unfug enthält, deshalb nicht ernst genommen werden kann und sich auf dem Niveau der Wahn- und Wunschvorstellungen der „Fragen und Antworten zur Online-Durchsuchung“ des Bundesinnenministeriums bewegt. Es gibt keine Rechtsgrundlage dafür, behördliche Spionageprogramme „vor Ort“ zu installieren. Wie man „per Mail“ etwas implementieren will – das ist reine Verschwörungstheorie. Man könnte das klipp und klar so sagen. Aber Stefan Krempl, der Autor des Heise-Artikels, beliebt es wie gewohnt, geheimnisvoll zu raunen.

Da nützt auch der Verweis auf zwei andere Artikel nichts: „Kommissar Trojaner“ (08.10.2007) behauptet den „Einsatz von Spionagesoftware, mit deren Hilfe sich die Gespräche auf den PCs der Kommunikationspartner abhören lassen sollen.“ Bewiesen ist das nicht. Dem steht entgegen, dass Skype, um das unter anderem geht, nicht so einfach abgehört werden kann. Christiane Schulzki-Haddouti hat – ebenfalls bei Heise – schon am 25.11.2005 geschrieben:

> *„Ob das Abhören aber auch bei Voice-over-IP-Diensten wie Skype möglich sein wird, ist zu bezweifeln. Skype verschlüsselt die Gespräche komplett von Endpunt zu Endpunkt einer Kommunikationsverbindung. Vor einen Monat ventilierte Skype ein Gutachten des IT-Sicherheitsexperten Thomas A. Berson, der Partner der International Association for Cryptologic Research ist. Demnach benutzt Skype kryptographische Methoden, um die Nutzer zu authentifizieren und den Gesprächsinhalt, der über das P2P-Netzwerk übermittelt wird, zu schützen. Berson stellte fest: ‚Das kryptografische System, das für diese Zwecke aufgesetzt wurde, wurde gut entworfen und korrekt implementiert.'“*

Wer hat denn nun Recht?

Der zweite Artikel (20.11.2007) – „Bundesregierung legt Einsatz von Trojanern beim VoIP-Abhören nahe“-, den Krempl selbst verfasst hat und auf den er jetzt verweist, wiederkäut nur die Thesen der Bundesregierung und Schäubles, ein „Bundestrojaner“ sei technisch umsetzbar. „Bei der so genannten Quellen-Telekommunikationsüberwachung (TKÜ) von Voice over IP (VoIP) und der heimlichen Online-Durchsuchung sei die „Technik der Vorgehensweise ähnlich.“ Da noch gar kein „Bundestrojaner“ existiert, ist das frei erfunden. Man kann auch sagen: glatt gelogen. Erst am Ende des aktuellen Artikels wird erwähnt, dass mitnichten ein „Trojaner“ zum Abhören der Internet-Telefonie benutzt wird. „‚Das würde technisch keinen Sinn machen‘, behauptete ein Sprecher der Behörde damals.“ Quod erat demonstrandum. Also sollte man auch nicht von einem „Bayerntrojaner“ faseln.

Ich habe eher den Eindruck, dass hier irgendetwas gezielt lanciert worden ist – mit einer berechenbaren Wirkung.

> *„Möglicherweise sei ein solcher von der bayerischen Landesregierung bereits unter der Hand anberaumt worden, mutmaßt Huwald. Andernfalls sei davon auszugehen, dass die Entwicklungsfirma den Trojaner auch an andere Sicherheitsbehörden veräußere. Dies hätte Huwald zufolge aber ‚katastrophale Folgen für die Sicherheit der Polizei, der Überwachten und der Beweise, die vermeintlich sicher gestellt werden‘.“*

Das ist doch Blödsinn. Die Software will ich erst sehen. Die Anwort auf die Frage des Titel ist also: „Nein“.

Nachtrag: vgl. Kommentar von Felix Leitner

Wer hat uns verraten, revisited

Hoax-Freund Christian Rath hat wieder zugeschlagen. In der taz (18.01.2008) interviewt er den ahnungslosen Dieter Wiefelspütz und verliert kein Wort darüber, wie eine „Online-Durchsuchung“ technisch möglich sei. Das könnte man Verschwörungstheoretiker fragen – und bekäme dann lustige Antworten.

Ein Haufen Irres

Laut Heise will die CDU „heimliche Online-Durchsuchungen“ auch gegen „Kinderpornografie im Internet“ einsetzen. Man merkt, dass sich der Hoax verselbständigt hat: Die Wahnvorstellung, die Regierung könne private Rechner „irgendwie“ fernwarten oder es könne ihr gelingen, ohne Wissen der Nutzer dort herumzuschnüffeln, hat

sich in den Köpfen so festgesetzt, dass rationale Argumente nichts mehr helfen. Der Glaube an den „Regierungshacker“ hat mittlerweile eine religiöse Konsistenz. Beckstein lügt dazu dreist: „Ich kenne keinen Fachmann aus den Landeskriminalämtern oder Landesverfassungsschutzämtern, der nicht die Online-Durchsuchung für notwendig hält.“ Dann sitzen dort nur Idioten. Ich kenne übrigens *keinen* IT-Fachmann (Frauen eingeschlossen), der eine „Online-Durchsuchung“, wie sie sich die CSU offenbar vorstellt, für möglich hielte.

Auch die „groß angelegten Angriffe auf Web-Anwender“ lassen mich kalt: „Zu ihrem Schutz sollten Anwender nur mit einer vollständig gepatchten Version des Internet Explorer arbeiten oder einen alternativen Browser nutzen. Zudem sollten Anwender den RealPlayer deinstallieren.“ Nein, zu ihrem Schutz sollten Anwender auf Windows verzichten, wenn sie damit nicht umgehen können. Ziel der Angriffe sind also nicht Web-Anwender (By the way: „Web“ ist *kein* Synonym für „Internet“!), sondern Windows-Nutzer. „Web-Anwender“ ist da schon ganz richtig, denn die meisten Nutzer halten das WWW für das Internet und haben von den anderen Diensten noch nie etwas gehört.

Hier gibt es ein schönes Interview mit dem Ex-Bundesverfassungsrichter Professor Hans-Joachim Jentsch: „Ob die Klage Erfolg haben wird, ist schwer einzuschätzen. In einer früheren Entscheidung hat das Bundesverfassungsgericht gesagt, dass eine Vorratsdatenspeicherung zu unbestimmten Zwecken nicht zulässig ist“.

Der mit Abstand lustigste Artikel bei Heise, der sich auf eine Meldung der Wirtschaftswoche bezog, ist schon von vorgestern: „Verfassungsschutz soll gezielte Trojanerattacken abwehren.“ Wer gerne lacht, sollte ihn unbedingt lesen. Leider besteht er zur Hälfte aus bloßen Gerüchten, die bisher niemand verifiziert hat: „Sollen häufig professionelle Spione im Staatsauftrag hinter den gezielten Attacken stehen“. Die Chinesen „sollen“ angeblich auch wild in der Gegend herumhacken. Und was die Esten den Russen unterstellen, ist

auch nur ein Gerücht. Was der Verfassungsschutz behauptet, kann man jedoch wie gewohnt als Agitprop bezeichnen, als frei erfunden oder zum Totlachen: „Rund 750.000 Computer hiesiger Unternehmen sollen mit Trojanern infiziert sein und vertrauliche Daten unbemerkt weiterleiten – oft direkt an die Konkurrenz.“ Die Schlapphüte haben genau mitgezählt. Jawoll, was die können, kann der Verfassungsschutztrojaner schon lange. Bruhahaha.

Focus | Falschmeldung

Focus verbreitet eine Falschmeldung: „Im Frühjahr 2006 hat das Bundesamt für Verfassungsschutz (BfV) eine getarnte E-mail an den Berliner Islamisten Reda Seyam, mit einem ‚Bundestrojaner‘ im Anhang verschickt. Wie das Nachrichtenmagazin FOCUS berichtet, stießen die BfV-Beamten bei der heimlichen Online-Razzia unter anderem auf eine Anleitung zum Bau von Sprengsätzen und Fotos von verstümmelten US-Soldaten. Reda Seyam klickte laut FOCUS die getarnte E-mail der Verfassungsschützer an und aktivierte so die erste und bislang einzige Online-Durchsuchung in Deutschland.“

Für wie dumm hält Focus seine LeserInnen? Was ist eine „getarnte“ E-Mail? Wenn es sich um einen gefälschten Header einer unverschlüsselten (!) Mail handelte: Wir könnte man den wahren Absender nachweisen? Doch nur, wenn der Verfassungsschutz selbst behauptete, der Urheber zu sein?! Bewiesen ist es damit noch nicht. Und wieso „Fotos von verstümmelten US-Soldaten“? Die sind legal und im Internet überall erhältllich. Nur weil sich das so „gruselig“ anhört?

Und noch was: Die „erste und bislang einzige Online-Durchsuchung“? Ach ja? Sonst gab es keine? Quod erat

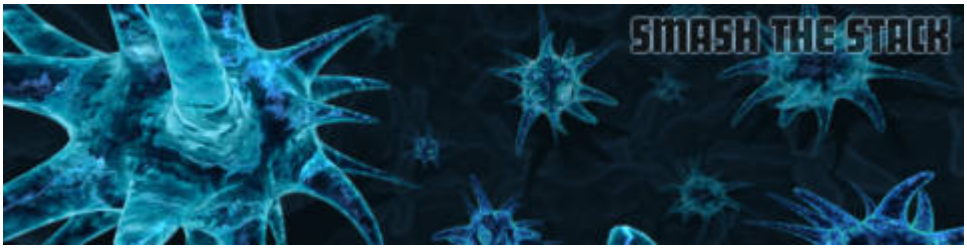
demonstrandum. Ich halte die Geschichte von vorn bis hinten für frei erfunden, also erlogen. Ich verdächtige auch Reda Seyam, sich nur wichtig machen zu wollen. Reda Seyam behauptet, sein „russischer Virenscanner“ (sind russische besonders gut?) habe angeschlagen. „Für seine Chats bevorzuge er seither Internet-Cafes.“ Chats? Was nützten Chats vor „getarnten E-Mails“ mit Viren, die eine Remote Forensic Software enthalten, auf die Windows-Benutzer (alle Islamisten nutzen bekanntlich Windows) klicken, klicken, klicken – und mitnichten an die Folgen denken?

Wenn man sich vergegenwärtigt, welche Quellen Focus hatte, dann muss man zu dem Schluss kommen, dass das Nachrichtenmagazin der Agitprop des Bundesnachrichtendienstes auf den Leim gekrochen ist. Dafür spricht der Satz: „Kollegen des Bundesnachrichtendienstes (BND), Spezialisten auf dem Gebiet der Online-Durchsuchung.“ Wer sonst, wenn nicht der BND selbst, würde sich selbst so loben, obwohl doch das BKA – also die Truppe Schäubles – eine Online-Durchsuchung offenbar noch gar nicht erfolgreich hinbekommen hat?

Selbstredend hat Focus keine zwei unabhängigen Quellen, noch nicht einmal eine. Das wäre Journalismus und viel zu anstrengend. Nichts für Focus also. Lügen, erfinden, nachplappern, und nicht an die Fakten denken…..

By the way: Wer ist für den Quatsch eigentlich verantwortlich? O je…

GovWare



Gulli: „Was brachte die Woche #1? (mit SkyOut, VXler)“
(…) „Ich find in dem Kontext ja die Online-Durchsuchung/ Bundestrojanergeschichten ja immer noch ne Stufe schlimmer. Burkhard Schröder hält die Geschichte ja vehement für ne Ente, kannst du dir angesichts solcher Patzereien vorstellen, dass das Ding ernsthaft gecoded und eingesetzt werden kann/soll?
(…) „Was ich viel spannender finde ist die Frage, wie solche GovWare gezielt eingesetzt werden soll. Stell Dir eine Zielperson vor, wie soll man diese und nur diese mit einem Trojaner infizieren? Es gab ja schon Gerüchte von Trojanern in Anhängen von Behördenemails. Das hat das E-Government in Deutschland erwartungsgerecht extrem nach hinten zurückgeworfen, was das Vertrauensverhältnis zwischen Bürgern und Regierung angeht. Also eins ist klar: Eine gezielte Unterschiebung eines Trojaners basiert auf gutem Social Engineering oder einer gewissen Unerfahrenheit des „Opfers“ gegenüber dem Thema Internetsicherheit. Ich für meinen Teil kann nur so viel sagen: Meinen PC zu infizieren könnte schwer werden. Nicht nur, dass ich alternative Systeme nutze, auch bin ich allem erstmal skeptisch gegenüber. Beherzigen das auch die anderen Bürger, sehe ich für einen geplanten Bundestrojaner wenig Chancen.“ (…)

Christian Rath |

Vorratsdatenspeicherung

Die taz entwickelt sich beim Thema „Vorratsdatenspeicherung“ aka „Bürgerrechte im digitalen Zeitalter“ immer mehr zur Lachnummer. Jetzt muss es mal deutlich gesagt werden: Schuld ist Christian Rath, der seit Monaten unqualifizierten Quatsch zum Thema von sich gibt.

Rath hat auch den Hoax „Online-Durchsuchung“ in die Welt gesetzt – mit einer Falschbehauptung, die die *taz* nie korrigiert hat. Im Artikel „Festplatten im Visier“ (30.01.2007) behauptet er: „Bei einer Online-Durchsuchung installiert die Polizei über die Internet-Verbindung des Computers eine Hacker-Software auf dem Rechner. Ein solcher Trojaner verschickt dann einmal oder laufend die auf der Festplatte gespeicherten Daten an die Polizei. Das Verfahren stellte ein Mitarbeiter der Bundesanwaltschaft mit einem Aufsatz in der Neuen Zeitschrift für Strafrecht im März 2005 vor.“

Ich schrieb in Telepolis (06.02.2007): „*Das ist nicht wahr*. Der betreffende Autor Manfred Hoffmann, Oberstaatsanwalt beim BGH, beschäftigt sich unter der Überschrift „Die Online-Durchsuchung – staatliches ‚Hacken‘ oder zulässige Ermittlungsmaßnahme?“ ausführlich mit dem Thema, hat aber offenbar wenig technischen Sachverstand. Der Datenspeicher des Computers eines Verdächtigen könne untersucht werden, schreibt er, „indem etwa mittels E-Mail oder auf andere Weise, auf den zu durchsuchenden Computer ‚Trojaner‘ oder ‚Backdoor‘-Programme aufgespielt werden.“ Wie es möglich sein könnte, per Mail etwas auf den Rechner eines Verdächtigen einzuschleusen, wenn der sich weigert, Attachments von unbekannten oder gar anonymen Absendern zu öffnen oder wie man einem Linux-Nutzer eine Spionage-Executable unterjubeln will, verrät Manfred Hoffmann nicht. Der Autor bezieht sich auf einen Fall aus dem Jahr 1997. Damals ging es aber um eine ‚passwortgeschützte Mailbox‘, also das klassische Bulletin Board System, in das

die Strafverfolger eindringen wollten.“

Rath beschwichtigt, „die Verbindungsdaten [würden] *nur* bei den Telefon- und Internetfirmen gespeichert. Obwohl „total“ keinen Superlativ kennt, muss man Rath doch fragen: Überwachung aller Inhalte und aller Kommunikationsdaten – geht es noch totaler?

Die Pointe am Schluss des Artikels toppt alles: „Die Polizei kann – wie bisher! – nur im konkreten Verdachtsfall zugreifen. Davon sollte sich niemand einschüchtern lassen, der auch bisher unbefangen telefoniert und gemailt hat.“ Ein Journalist, der „unbefangen“ telefoniert und – vermutlich unverschlüsselt – mailt wie der taz-Autor, sollte man besten wieder nach Hause gehen und das Maul halten. Er ist eine Schande für die Zunft.