

Ubuntu rulez!

[TippingPoint DV Labs](#): Der [Ubuntu](#)-Laptop bleibt ungehackt... (vgl. auch [Heise](#)).

Meine Firefox-Erweiterungen



Die Google-Falle

Die [Google-Falle](#), vgl. auch [Telepolis](#): „Die Google-Verschwörungstheorie“.

Die ultimative E-Mail-Signatur

Diese E-Mail kann zur Gänze oder in Teilen vertrauliche und/oder persönliche Informationen enthalten und ist ausschließlich für den/die im Text („Body“) oder in der elektronischen Kopfzeile („Header“) genannten primären Empfänger („Recipient:“) bzw. sekundären Empfänger von elektronischen Kopien („Cc:“) bzw. weiteren, im Text oder ggf. in Anhängen („Attachments“) namentlich genannten bzw. durch Kurz-, Spitz- Ordens- oder Künstlernamen eindeutig identifizierbaren Empfänger zur alleinigen, vertraulichen und/oder persönlichen Verwendung bestimmt. Für den Fall, dass der tatsächliche Empfänger dieses E-Mails nicht zu den im Text oder in der elektronischen Kopfzeile genannten primären Empfängern bzw. sekundären Empfängern von elektronischen Kopien bzw. weiteren, im Text oder ggf. in Anhängen namentlich bzw. durch Kurz-, Spitz- Ordens- oder Künstlernamen genannten Empfängern gehört bzw. nicht von einem Mitglied dieses Personenkreises ausdrücklich, z.B. durch Weiterleiten („forwarding“), Kopieren und Einfügen („copy and paste“), bzw. Ausschneiden und Einfügen („cut and paste“), oder durch andere belegbare und nachvollziehbare Art und Weise, wie z.B. dem

Ausdrucken und Versenden als persönliches Übergabeeinschreiben, zum Empfang autorisiert wurde, weisen wir darauf hin, dass das Ansehen, Lesen, Kopieren, die Wiedergabe, Verbreitung, Vervielfältigung, Bekanntmachung, Veränderung, Verteilung und/oder Veröffentlichung, sowohl in elektronischer Form als auch als Ausdruck auf Papier oder anderen bedruckbaren bzw. belichtbaren Materialien wie Folien, Filme oder Microfiche, sowie die alleinige Kenntnis seiner Existenz strengstens untersagt sind und Straf- und/oder Zivil- und/oder Datenschutz- und/oder Sozial- und/oder Arbeits- und/oder sonstige rechtliche Verfolgung sowie eine lebenslange Vendetta der Kalabrischen Mafia nach sich ziehen können. Sollten Sie dieses E-Mail irrtümlich erhalten haben, sind Sie verpflichtet innerhalb einer angemessenen Frist den Absender per E-Mail, Einwurfeinschreiben ohne Rückschein, Telefonanruf im Festnetz oder Mobil, Telex, Telefax, Teletext, Minitel, Postkarte (Motiv freigestellt), persönliches Aufsuchen und/oder Strip-Telegramm zu benachrichtigen. Laut Auskunft unserer Rechtsabteilung beträgt eine angemessene Frist derzeit 7,049 " (Sieben Komma Null Vier Neun Sekunden). Vorsorglich machen wir Sie darauf aufmerksam, dass Sie zum Ausfindigmachen des Absenders das E-Mail nicht lesen dürfen! Unmittelbar im Anschluß an das Benachrichtigen des Absenders ist das E-Mail komplett und rückstandslos und in einer Weise zu löschen, die eine Wiederherstellung mit allgemeinen und/oder speziellen Mitteln der Datenwiederherstellung wie Archivierungssoftware, sogenannte „Disk Utilities“, Festplattenelektronenmikroskopie, Tricoder und/oder naturwissenschaftlich nicht anerkannte Methoden wie unter anderem (aber nicht ausschließlich) das Besprühen der Festplatte mit Weihwasser unter Anstimmen stupider Gesänge unmöglich macht. Der Inhalt dieses E-Mail ist nur rechtsverbindlich, wenn er innerhalb einer angemessenen Frist von unserer Seite ausdrücklich und schriftlich sowohl durch Brief als auch durch Telefax, Einwurfeinschreiben ohne Rückschein, Teletext, Minitel, Postkarte mit floralem Motiv und Strip-Telegramm bestätigt wird, wobei die Übermittlung des Strip-Telegramms unter notarieller Aufsicht erfolgen muss.

Sollte dieses oder ein bzw. mehrere andere E-Mails von uns an Sie Computerviren, sogenannte „Trojanische Pferde“, bzw. sonstige Software zum Vervielfältigen, Ausspionieren, Manipulieren und/oder Löschen Ihrer Daten und/oder unrechtmäßig kopierte Software, Texte, Bilder, Filme, Tonaufnahmen enthalten, bzw. solche Software, Texte, Bilder, Filme, Tonaufnahmen enthalten, die im Sender- und/oder Empfängerland oder einem sonstigen Land der Erde als illegal oder gegen die guten Sitten verstoßend gelten, so verzichten Sie mit der Annahme dieser Mail automatisch und unwiderruflich auf sämtliche Garantien, Gewährleistungen, Ansprüche und/oder sonstige Verpflichtungen unsererseits, die sich aus diesem E-Mail oder aus anderen E-Mails oder auch aus ganz anderen Gründen mittelbar oder unmittelbar ergeben. Die Versendung von E-Mails an uns hat keine fristwahrende, fristverlängernde, fristverkürzende, aufschiebende, abziehende, rechtlich oder in irgend einer anderen Weise verbindliche bzw. bindende oder sonstige Wirkung und wird generell nicht empfohlen.

Credits: [Florian Hentschel](#)

Lügenmärchen nehmen zu

[Heise.de](#) wiederkaut ein Interview mit BKA-Präsident [Jörg Ziercke](#) in der [Neuen Osnabrücker Zeitung](#). Das ist nur eine dpa-Meldung, und sogar bei Heise ohne Link auf das Original (pfui!). Ich habe mich geärgert und im Forum rustikal fomuleirt, warum Heise die Lügenmärchen Zierckes unkritisch aufberieten müsse.

„Nach Schätzungen sind heute mehr als 750 000 Computer in Deutschland mit Schadprogrammen infiziert, etwa 150 000 Rechner werden von Kriminellen unbemerkt ferngesteuert‘,

erklärte er.“ Ach ja? Und welche werden von Schäubles real gar nicht existierenden Bundestrojanern ferngesteuert? Ich glaube kein Wort davon. Und „dass der gesamte Bereich der Internet-Kriminalität weiter rasant zunehmen wird“, ist geschenkt. Wenn das nicht so wäre, brauchten die Sicherheitsbehörden keine neuen Stellen und Sachmittel fordern. Ziercke hätte auch sagen können: Es wird immer alles schlimmer, und wir brauchen natürlich mehr Geld, um das Böse allüberall bekämpfen zu können.

„Bilder und Filme, auf denen Kinder und sogar Babys brutal missbraucht werden, breiten sich im Internet rasend schnell aus.“ So habe das BKA zum Beispiel in einem Verfahren in Deutschland fast 240.000 Zugriffe auf 4600 kinderpornografische Dateien festgestellt, erklärte Ziercke.“ Ach ja: War das die [Operation Heiße Luft](#)? Auch das halte ich für frei erfunden.

Eine Faustregel im Journalismus lautet: Veröffentliche nie etwas, wenn du nicht mindestens zwei unabhängige Quellen hast. Hier haben wir nur eine abhängige. Die Regel gilt übrigens nicht bei Propaganda-Thesen, die als solche zu erkennen sind wie: „Angela Merkel sagte, unter der weisen Führung der CDU werde die Welt immer schöner.“ Bei Pressemitteilungen des Bundeskriminalamtes, die sich als Interview von pieseligen Lokalzeitungen tarnen, gilt das auch. Zwar steht bei Heise „Laut BKA nehmen Schäden durch Phishing rasant zu“, aber das müsste erst nachgeprüft werden. bevor man es als Tatsache ausgibt.

Die [indirekte Rede](#) verlangt im Deutschen – wie hier in der Überschrift bei Heise – den [Konjunktiv I](#), und dummerweise ist der bei „nehmen“ identisch mit dem Indikativ. Wäre ich Chefredakteur der Neuen OZ, ich hätte Ziercke die [Ersatzform](#) „würde zunehmen“ untergejubelt, um klar und angenehm zu sagen, was Sache ist. Noch schöner wäre „Kriminalität nähme zu“. Das suggerierte den Nachsatz: „wenn sich das Ziercke nicht nur ausgedacht hätte“.

Das BKA war es nicht

Sehr geehrter Herr Schröder,

(...) Bei uns ist lediglich nachweisbar, dass die Süddeutsche Zeitung Anfang Dezember 2006 zum Thema Online-Durchsuchung angefragt hat. Leider ist nicht mehr nachvollziehbar, welche Auskunft Herr Müller im Wortlaut gegeben hat bzw. ob dieses Zitat von ihm autorisiert worden ist.

Da das Bundeskriminalamt (BKA) faktisch niemals eine Online-Durchsuchung durchgeführt hat, kann ich Ihnen das u.g. Zitat leider nicht bestätigen. Korrekt müsste es vielmehr lauten: „Es gab bereits zwei Fälle in Strafverfahren des BKA, bei denen solche Durchsuchungen von der StA beantragt wurden, in einem Fall richterlich angeordnet, in einem weiteren abgelehnt wurden und in keinem Fall stattgefunden haben.“

Mit freundlichen Grüßen

Christian Brockert, Bundeskriminalamt

—Ursprüngliche Nachricht—

Gesendet: Donnerstag, 14. Februar 2008 16:55

An: info@bka.de

Betreff: An BKA Pressestelle

(...) ich beziehe mich auf einen Bericht auf sueddeutsche.de vom 07.12.2006: Zitat: „Es gab bereits Einzelfälle in Strafverfahren, bei denen richterlich angeordnet solche Durchsuchungen stattgefunden haben“, sagt Dietmar Müller, Pressesprecher des BKA in Wiesbaden.“ (...)

Mit freundlichen Grüßen

Burkhard Schröder

Bericht zur Lage der Nation im Internet

[Lagebericht IT-Sicherheit 2007](#) des Bundesamtes für Sicherheit in der Informationstechnik ([pdf](#)): „Im Jahre 2004 gaben noch 46 Prozent der Befragten an, sich sehr gut oder zumindest gut mit IT-Sicherheit auszukennen. 2006 sind dies nach Erkenntnissen des BSI nur noch knapp 17 Prozent.“ Ähm. Was sagt uns das jetzt? Selbsterkenntnis ist der erste Weg zur Besserung? Mitnichten: „Das Bewusstsein für IT-Sicherheit ist vorhanden. Andererseits besteht auch eine Tendenz, die Lösung der Probleme vor allem an Internetanbieter und die Hersteller von IT-Sicherheitslösungen delegieren zu wollen.“

Provider liefert falsche Daten ans BKA

[Law blog](#): „Provider liefert falsche Daten ans BKA“

Logfiles

Top 50 von 9193 URLs					
#	Anfragen		kb		URL
1	47685	10.54%	453899	5.45%	/forum/phpBB2/viewtopic.php
2	8110	1.79%	32287	0.39%	/forum/phpBB2/login.php
3	6367	1.41%	158010	1.90%	/recherchegruppe/blog/
4	5203	1.15%	26418	0.32%	/favicon.ico
5	4362	0.96%	309334	3.71%	/burksblog/
6	3101	0.69%	41532	0.50%	/burksblog/feed/
7	2967	0.66%	34230	0.41%	/forum/phpBB2/profile.php
8	2789	0.62%	14431	0.17%	/forum/phpBB2/favicon.ico
9	2565	0.57%	1232	0.01%	/
10	2529	0.56%	8251	0.10%	/forum/phpBB2/spiggel.php
11	2014	0.45%	231	0.00%	/robots.txt
12	1835	0.41%	62740	0.75%	/forum/phpBB2/viewforum.php
13	1832	0.40%	44107	0.53%	/forum/phpBB2/
14	1325	0.29%	18834	0.23%	/burksblog/feed/atom/
15	812	0.18%	68042	0.82%	/nazis.html
16	597	0.13%	28084	0.34%	/kawumm.html
17	515	0.11%	20933	0.25%	/krypto.html
18	461	0.10%	1039	0.01%	/burksblog/wp-login.php
19	413	0.09%	37857	0.45%	/medien.html

Joseph Weizenbaum | Albtraum Computer

Zum Tode [Joseph Weizenbaums](#): „Albtraum Computer“ – ein [Artikel](#) von ihm in der *Zeit*, erschienen im Januar 1972 (!). Zum Gedenken an Joseph Weizenbaum ist eine Trauerfeier am 18. März um 14 Uhr im jüdischen [Gemeindezentrum](#) Berlin angesetzt.

Online-Durchsuchung | Auf Entenjagd

Bundesverfassungsgericht

– 1. Senat –

Postfach 1771

76006 Karlsruhe

bverfg@bundesverfassungsgericht.de

Sehr geehrte Damen und Herren,

Ich beziehe mich auf das Urteil des 1. Senats (1 BvR 370/07 vom 27.2.2008, Absatz-Nr. I, 1c) über das Verfassungsschutzgesetz Nordrhein-Westfalen. Dort heißt es über den heimlichen „Zugriff auf informationstechnische Systeme mittels technischer Infiltration“: „Vereinzelt wurden derartige Maßnahmen durch Bundesbehörden bereits ohne besondere gesetzliche Ermächtigung durchgeführt.“

Sind dem Bundesverfassungsgericht dazu andere Quellen bekannt als die Berichterstattung in den Medien?

BKA-Chef Jörg Ziercke hat in einem Interview mit „Spiegel Online“ vom 01.03. gesagt: „Zum Zeitpunkt des Inkrafttretens einer gesetzlichen Regelung werden wir über eine einsatzfähige Software verfügen.“ Daraus lässt sich schließen, dass es eine derartige Software noch nicht gibt. Der Verfassungsschutz hat mehrfach auf Anfrage behauptet, er habe auch noch keine „Online-Durchsuchungen“ gemacht.

Ich vermute, dass die nur in einigen Medien verbreitete These, es habe schon erfolgreiche „Online-Durchsuchungen“ gegeben, schlicht eine Ente und frei erfunden ist. Ulf Buermeyer bestätigt das indirekt in seinem – auch im Urteil zitierten – Aufsatz: Die „Online-Durchsuchung“. Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme“.

Hintergrund meiner Anfrage: Im Mai wird ein Buch über die Online-Durchsuchung von mir im Heise-Verlag erscheinen.

Mit freundlichen Grüßen

Burkhard Schröder

Sehr geehrter Herr Schröder,
vielen Dank für Ihre Mail vom 3. März 2008. Dem Bundesverfassungsgericht sind keine anderen Quellen bekannt (vgl. Rn 7 des auf unserer Homepage veröffentlichten Urteils vom 27. Februar 2008).
Mit freundlichen Grüßen
Dietlind Weinland

Nächste Runde im Streit um die Online-Durchsuchung

Ein Artikel von mir auf [Telepolis](#): „Nächste Runde im Streit um die Online-Durchsuchung“.

Die taz blamiert sich wieder:

Sorry, hatte ich gar nicht mibekommen: [Kommentar](#) vom „Rechtsexperten“ der taz, Christian Rath (28.02.2008): „Für eine wirksame Terrorabwehr würde es genügen, dass sie E-Mail-Verkehr und Telefonate auch überwachen kann, wenn diese verschlüsselt im Internet geführt werden.“ Man fasst es nicht. Verschlüsselte E-Mails überwachen? Das möchte ich sehen. Das kann jeder bei mir gern tun – aber wie sieht es mit dem Lesen aus?

Wir sind alle Deutsche

[Rob Gonggrijp](#): „Today, we are all Germans“ (vgl. auch [Heise](#) zum Thema):

So the people of Germany seem to be successfully defending themselves against their government. What's wrong with the rest of the world?

Javascript



Schlagzeilen | TV-Programm | RSS | News

SPIEGEL ONLINE VIDEO

NACHRICHTEN VIDEO ENGLISH EINESTAGES FORUM SPIEGEL WISSEN ABO & SHOP

Video | Fotostrecken | Interaktive Grafiken | SPIEGEL TV

Der benötigte Flash Player 8 wurde nicht gefunden.

Mögliche Ursachen:

JavaScript ist deaktiviert.

Der Player ist nicht vorhanden.
[Jetzt herunterladen und installieren](#)

Hinweis: Sie werden zum Installieren des Flash Players auf die Website von Macromedia Deutschland weitergeleitet. Wenn Sie den Internet Explorer nutzen, wird "Yahoo! Toolbar" automatisch mitinstalliert. Wenn Sie das nicht möchten, müssen Sie dies explizit kenntlich machen und den Haken vor dem Angebot entfernen.

Meine

Lieblingsmeldung bei Spiegel Online, seitdem mich die kleinen Filmchen dort mit Werbung zuspammen wollen.

BKA-Chef fordert Redeverbot über Online-Durchsuchungen

Ziercke in Hochform – jetzt [fordert](#) er Redeverbot: „Vor allem sei in der Öffentlichkeit nicht weiter über die mögliche Technik des so genannten Bundestrojaners zu spekulieren, erklärte der Oberpolizist gegenüber [Spiegel Online](#). Zugleich zeigte er sich zuversichtlich, dass das BKA zum Zeitpunkt des Inkrafttretens einer gesetzlichen Regelung über eine einsatzfähige Software verfügen werde.“

Ich bin es jetzt leid, mir ständig diese urbanen Märchen anzuhören – und unkritische Interviews. Gestern habe ich eine E-Mail geschrieben:

Lieber Kollege Gebauer,

ich schreibe ein [Buch](#) über das Thema Online-Durchsuchung.

Im [Interview](#) mit BKA-chef Ziercke behaupten Sie: „Die beiden bekannten Fälle von Online-Durchsuchungen wurden gegen den Berliner Islamisten Reda S., der gute internationale Kontakte in die Dschihad-Szene unterhält, und einen Iraner geführt, der der [Proliferation](#) verdächtigt wurde.“

Ich gehe davon aus, dass Sie das nicht beweisen können bzw. dass die einzige Quelle die [Focus-Falschmeldung](#) vom 05.01.2008 ist.

Da noch gar keine Software zur Verfügung steht, um eine Online-Durchsuchung technisch zu bewerkstelligen, wäre ich daran interessiert, ob Sie für die These, es habe schon zwei gegeben, andere Quellen besitzen.

Vgl. [tagesschau.de](#): „Seit 2005 haben deutsche Geheimdienste nach Angaben des Bundesinnenministeriums knapp ein Dutzend Privatcomputer heimlich via Internet durchsucht“ sowie [tagesschau.de](#): „Wir gehen auch davon aus, dass das noch nie

richtig geklappt hat. Es gab technische Schwierigkeiten. Das Einschleusen hat nicht geklappt und gerade die gefährliche Szene wird Wege finden, sich vor Bundestrojanern zu schützen.“
Wie viele verifizierte (!) Online-Durchsuchungen gab es Ihrer Meinung nach von 1995 bis heute?

Mit freundlichen Grüßen

Burkhard Schröder

Schlechte Karten für „Bundestrojaner“

Das [Urteil](#) des Bundesverfassungsgerichts, das Verfassungsschutzgesetz in Nordrhein-Westfalen für nichtig zu erklären, ist salomonisch und listig: Es gestattet allen Beteiligten, das Gesicht zu wahren. Erst im Kleingedruckten – in der ausführlichen Begründung – wird deutlich, dass die juristischen Hürden für die vom Bundesinnenministerium gewünschten „Online-Durchsuchungen“ fast unüberwindbar hoch sind.



Das neu eingeführte Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme als Teil des allgemeinen Persönlichkeitsrechts schließt einige juristische Lücken, die sich laut Gericht aus „neuartigen Gefährdungen“ im Zuge des „wissenschaftlich-technischen Fortschritts“ ergeben. Die durch das [Grundgesetz](#) garantierte „freie Entfaltung der Persönlichkeit“ musste exakter gefasst werden, weil Computer dafür eine immer größere Bedeutung erlangt haben, insbesondere in vernetzten Systemen. Das ist an sich nichts Neues. Interessant ist jedoch, dass das Bundesverfassungsgericht es für fragwürdig hält, prophylaktisch Informationen über Personen zu sammeln:

„Dabei handelt es sich nicht nur um Daten, die der Nutzer des Rechners bewusst anlegt oder speichert. Im Rahmen des Datenverarbeitungsprozesses erzeugen informationstechnische Systeme zudem selbsttätig zahlreiche weitere Daten, die ebenso wie die vom Nutzer gespeicherten Daten im Hinblick auf sein Verhalten und seine Eigenschaften ausgewertet werden können. In der Folge können sich im Arbeitsspeicher und auf den Speichermedien solcher Systeme eine Vielzahl von Daten mit Bezug zu den persönlichen Verhältnissen, den sozialen Kontakten und den ausgeübten Tätigkeiten des Nutzers finden. Werden diese Daten von Dritten erhoben und ausgewertet, so kann dies weitreichende Rückschlüsse auf die Persönlichkeit des Nutzers bis hin zu einer Profilbildung ermöglichen“.

Daraus ergebe sich ein „erhebliches Schutzbedürfnis“, dem im Urteil Rechnung getragen wird. Der Einzelne sei darauf angewiesen, wenn er sich im Sinne des Grundgesetzes frei entfalten wolle, dass auch der Staat die Integrität und Vertraulichkeit informationstechnischer Systeme achte.

Der Schutz der „Persönlichkeit“ wird durch das Urteil erweitert auf die Technik, die die Person benutzt, um ihr Leben zu gestalten. Dazu passt, dass die Wohn-, Betriebs- und Geschäftsräume, die durch das [Urteil zum Großen Lauschangriff](#) vor dem Zugriff des Staates grundsätzlich geschützt wurden,

jetzt auch die genutzten Rechnersysteme umfassen. Setzt sich jemand mit seinem Laptop in ein Cafe, gehört dieser automatisch zum „Kernbereich der privaten Lebensgestaltung“, in dem der Staat nicht einfach so herumschnüffeln darf. Der Bundesverfassungsgericht geht sogar ins Detail, Keylogger zu erwähnen und die elektromagnetische Abstrahlung des Computers, die man [abfangen und auslesen](#) könnte.

Selbst das bisherige Recht auf informationelle Selbstbestimmung ging dem Bundesverfassungsgericht nicht weit genug, weil heute jeder darauf angewiesen sei, Computer zu benutzen.

„Ein Dritter, der auf ein solches System zugreift, kann sich einen potentiell äußerst großen und aussagekräftigen Datenbestand verschaffen, ohne noch auf weitere Datenerhebungs- und Datenverarbeitungsmaßnahmen angewiesen zu sein. Ein solcher Zugriff geht in seinem Gewicht für die Persönlichkeit des Betroffenen über einzelne Datenerhebungen, vor denen das Recht auf informationelle Selbstbestimmung schützt, weit hinaus.“

Das höchste deutsche Gericht beweist in seinem Urteil mehr technischen Sachverstand und hat investigativer zum Thema recherchiert als die meisten deutschen Medien. Es räumt auch gleich mit einigen urbanen Legenden auf. Hat es schon eine „Online-Durchsuchung“ privater Rechner gegeben? Es sei nichts über die Technik der bisherigen „Online-Durchsuchungen“ und über deren Erfolge bekannt. Die Präsidenten des BKA und des Verfassungsschutzes hatten keine Aussagegenehmigung. Das Bundesinnenministerium hatte auch in den Medien immer ausweichend reagiert und auf die [Fragen des Bundesjustizministeriums](#) geantwortet, die dazu nötigen Programmen würden erst noch entwickelt.

Im [Verfassungsschutzgesetz](#) Nordrhein-Westfalen findet sich die wolkige Formulierung, man wolle heimlich auf „informationstechnische System“ zugreifen. Noch schwammiger

ist der „Zugriff auf [Internet-Festplatten](#)“. Von einer „Online-Durchsuchung“ war ursprünglich nicht die Rede. Letztlich lässt sich nicht mehr klären, ob der Gesetzgeber von Anfang an beabsichtigte, auch private Rechner durchsuchen zu lassen. Das Bundesverfassungsgericht hat die Diskussion kurz und bündig beendet. Nicht ganz humorlos wird erklärt, sowohl ein einzelner Rechner als auch das Internet als solches sei jeweils ein „informationstechnisches System“.



„Unter einem heimlichen Zugriff auf ein informationstechnisches System ist demgegenüber eine technische Infiltration zu verstehen, die etwa Sicherheitslücken des Zielsystems ausnutzt oder über die Installation eines Spähprogramms erfolgt. Die Infiltration des Zielsystems ermöglicht es, dessen Nutzung zu überwachen oder die Speichermedien durchzusehen oder gar das Zielsystem fernzusteuern. Die nordrhein-westfälische Landesregierung spricht bei solchen Maßnahmen von einer clientorientierten Aufklärung des Internet. Allerdings enthält die angegriffene Vorschrift keinen Hinweis darauf, dass sie ausschließlich Maßnahmen im Rahmen einer am Server-Client-Modell orientierten Netzwerkstruktur ermöglichen soll.“

Da der heimliche Zugriff auch auf private Rechner definitiv nicht ausgeschlossen sei, müsse man auch über die „Online-

Durchsuchung“, wie sie allgemein diskutiert werde, urteilen.

Spannend ist das Urteil vor allem in den Passagen am Schluss, die die Ausnahmen regeln. Der Schutz des „Kernbereichsschutz“ wird aufgeweicht. Bisher mussten Lauscher die Mikrofone ausschalten, wenn die Verdächtigen anfangen zu beten oder über Sex redeten. Praktisch war eine Überwachung kaum noch möglich. Das Bundesverfassungsgericht hat festgestellt, dass das im Prinzip auch für Computer gilt. Die aus technischer Sicht sehr [kühnen Thesen](#) des Bundesinnenministeriums, man könne einfach durch das Design der Software die Privatsphäre ausreichend schützen, ein Spionage-Programm werde keine anderen Programme des betroffenen Rechters beeinträchtigen und diesen nicht verändern, glaubt das Bundesverfassungsgericht nicht. Es sei „praktisch unvermeidbar“ bei einem heimlichen Zugriff, wenn er bei einem technisch unbedarften Verdächtigen funktioniere, auch an Daten zugelangt, die die Ermittler weder zur Kenntnis nehmen noch verwerten dürfen. Einen „rein lesenden Zugriff infolge der Infiltration“ gebe es nicht.

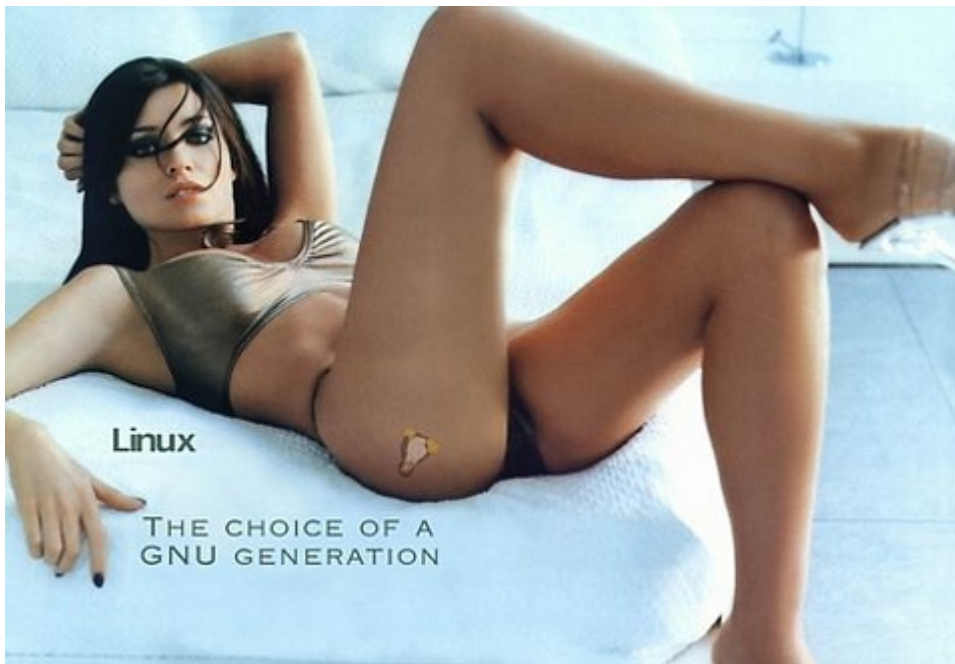
„Im Rahmen des heimlichen Zugriffs auf ein informationstechnisches System wird die Datenerhebung schon aus technischen Gründen zumindest überwiegend automatisiert erfolgen. Die Automatisierung erschwert es jedoch im Vergleich zu einer durch Personen durchgeführten Erhebung, schon bei der Erhebung Daten mit und ohne Bezug zum Kernbereich zu unterscheiden. Technische Such- oder Ausschlussmechanismen zur Bestimmung der Kernbereichsrelevanz persönlicher Daten arbeiten nach einhelliger Auffassung der vom Senat angehörten sachkundigen Auskunftspersonen nicht so zuverlässig, dass mit ihrer Hilfe ein wirkungsvoller Kernbereichsschutz erreicht werden könnte.“

Das Bundesverfassungsgericht hat zur Kenntnis genommen, dass sich jeder vor einer „Online-Durchsuchung“ schützen kann – es verweist ausdrücklich auf die einschlägige [Literatur](#). Dennoch könnte man allein deswegen diese Methode nicht ausschließen. Die Schranken für eine Überwachung eines privaten Rechners

sind aber sehr hoch: Es muss eine konkrete Gefahr vorliegen, die ein „überragend wichtiges Rechtsgut“ bedroht. Klar ist auch, dass eine heimliche „Online-Durchsuchung“ immer einen schweren Grundrechtseingriff bedeutet, für ein ein Richtervorbehalt jetzt gesetzt ist. Das bedeutet: Nur bei unmittelbarer Gefahr für Leib und Leben einer Person oder bei konkreter Bedrohung für „den Bestand des Staates oder die Grundlagen der Existenz der Menschen“ dürfen die Ermittler über eine „Online-Durchsuchung“ anfangen nachzudenken.

„Die Tatsachen müssen zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann. Dagegen wird dem Gewicht des Grundrechtseingriffs, der in dem heimlichen Zugriff auf ein informationstechnisches System liegt, nicht hinreichend Rechnung getragen, wenn der tatsächliche Eingriffsanlass noch weitergehend in das Vorfeld einer im Einzelnen noch nicht absehbaren konkreten Gefahr für die Schutzgüter der Norm verlegt wird.“

Und wenn dann ein Richter dem zustimmte, bedürfe es noch besonderer Vorkehrungen, um den geschützten Privatbericht nicht zu behelligen. „Gibt es im Einzelfall konkrete Anhaltspunkte dafür, dass eine bestimmte Datenerhebung den Kernbereich privater Lebensgestaltung berühren wird, so hat sie grundsätzlich zu unterbleiben.“



Durch das Urteil rückt das Sicherheitsinteresse der Staates ein wenig näher an die einzelnen Menschen heran. Der so genannte „Kernbereich“ des Privaten ist kleiner geworden, dafür um so sicherer. Ein bloßes Gesetz schützte wenig vor privaten und staatlichen Datenkranken; ein Grundrecht jedoch, das als solches vom Bundesverfassungsgericht definiert ist, kann man kaum außer Acht lassen.

Die Hausaufgabe, die das Gericht dem Bundesinnenminister aufgegeben hat, ist so gut wie unlösbar, zumal eine Online-Überwachung durch die Polizei und das Bundeskriminalamt noch schwieriger ist als durch den Verfassungsschutz, der seine Daten für sich behalten kann. Die Ermittler hätten jedoch vor Gericht das zusätzliche Problem, beweisen zu müssen, dass die gefundenen Beweise auch echt sind. Möglicherweise, so steht es geheimnisvoll im Urteil, sei der „Beweiswert der Erkenntnisse gering“: Eine „technische Echtheitsbestätigung der erhobenen Daten“ setze grundsätzlich „eine exklusive Kontrolle des Zielsystems im fraglichen Zeitpunkt voraus“. Und das muss man erst einmal technisch umsetzen und anschließend einem Richter beweisen – schlechte Karten für jede Art und Version eines „Bundestrojaners“.

Dieser Artikel von mir erschien am 27.02.2008 auf [Telepolis](#).

Online-Durchsuchung zum Aussuchen

- [Tagesschau.de](#) (27.04.2007): „Seit 2005 haben deutsche Geheimdienste nach Angaben des Bundesinnenministeriums **knapp ein Dutzend** Privatcomputer heimlich via Internet durchsucht.“
- [Tagesschau.de](#) (28.04.2007, Wolfgang Wieland im Interview): „Wir gehen auch davon aus, **dass das noch nie richtig geklappt hat**. Es gab technische Schwierigkeiten. Das Einschleusen hat nicht geklappt.“
- [Spiegel Online](#) (09.07.2007, Wolfgang Schäuble im Interview): SPIEGEL: „...wie etwa die heimlichen Online-Durchsuchungen zeigen. Die haben die Sicherheitsbehörden ohne gesetzliche Grundlage **jahrelang angewandt**. Schäuble: Moment. Es gab **einen Anwendungsfall** im Inland.“
- [Focus Online](#) (05.01.2008): „Reda Seyam klickte laut FOCUS die getarnte E-mail der Verfassungsschützer an und aktivierte so **die erste und bislang einzige Online-Durchsuchung** in Deutschland.“
- [Bundesverfassungsgericht](#) (27.02.2008): „**Vereinzelt** wurden derartige Maßnahmen durch Bundesbehörden bereits ohne besondere gesetzliche Ermächtigung durchgeführt. Über die Art der praktischen Durchführung der bisherigen „Online-Durchsuchungen“ und deren Erfolge ist wenig bekannt. Die von dem Senat im Rahmen der mündlichen Verhandlung angehörten Präsidenten des Bundeskriminalamts und des Bundesamts für Verfassungsschutz haben mangels einer entsprechenden Aussagegenehmigung keine Ausführungen dazu gemacht.“
- [Spiegel Online](#) (01.03.2007): „**Die beiden bekannten Fälle** von Online-Durchsuchungen wurden gegen den Berliner Islamisten

Reda S., der gute internationale Kontakte in die Dschiahd-Szene [sic] unterhält, und einen Iraner geführt, der der Proliferation verdächtigt wurde.“

Papier begründet das neue Grundrecht



[Hier](#) ein Mitschnitt von [Phoenix](#) (27.02.): Das Bundesverfassungsgericht begründet das neue Grundrecht. (ca. 420 MB, avi-Format)

Do not even think of



DO NOT EVEN THINK OF
INSTALLING WINDOWS™ ON
THIS COMPUTER