Erlaubt oder verboten?

Reuters: „Richter ebnen Weg für Online-Durchsuchungen“.
ORF.at: „Verfassungsgericht kippt Online-Durchsuchung“.

Heuchlerische Mischpoke

tagesschau.de: Nach dem Urteil des Bundesverfassungsgerichts – Online-Durchsuchungen sollen bald umgesetzt werden

> *Der FDP-Parteichef Guido Westerwelle bezeichnete die Karlsruher Entscheidung als einen „Meilenstein der Rechtsgeschichte für Freiheit und Bürgerrechte“. Das Gericht stoppe mit seinem Urteil „die Aushöhlung der Privatsphäre, wie sie unter Rot-Grün mit Otto Schily begann und wie sie jetzt unter Schwarz-Rot mit Wolfgang Schäuble fortgesetzt werden soll“. Auf die Tatsache, dass in NRW ein FDP-Politiker für das gekippte Gesetz zuständig sei, ging Westerwelle nicht ein.*

Hausaufgaben für Wolfgang Schäuble

Ein Artikel von mir in der Netzeitung (27.02.2008): „Hausaufgaben für Wolfgang Schäuble“.

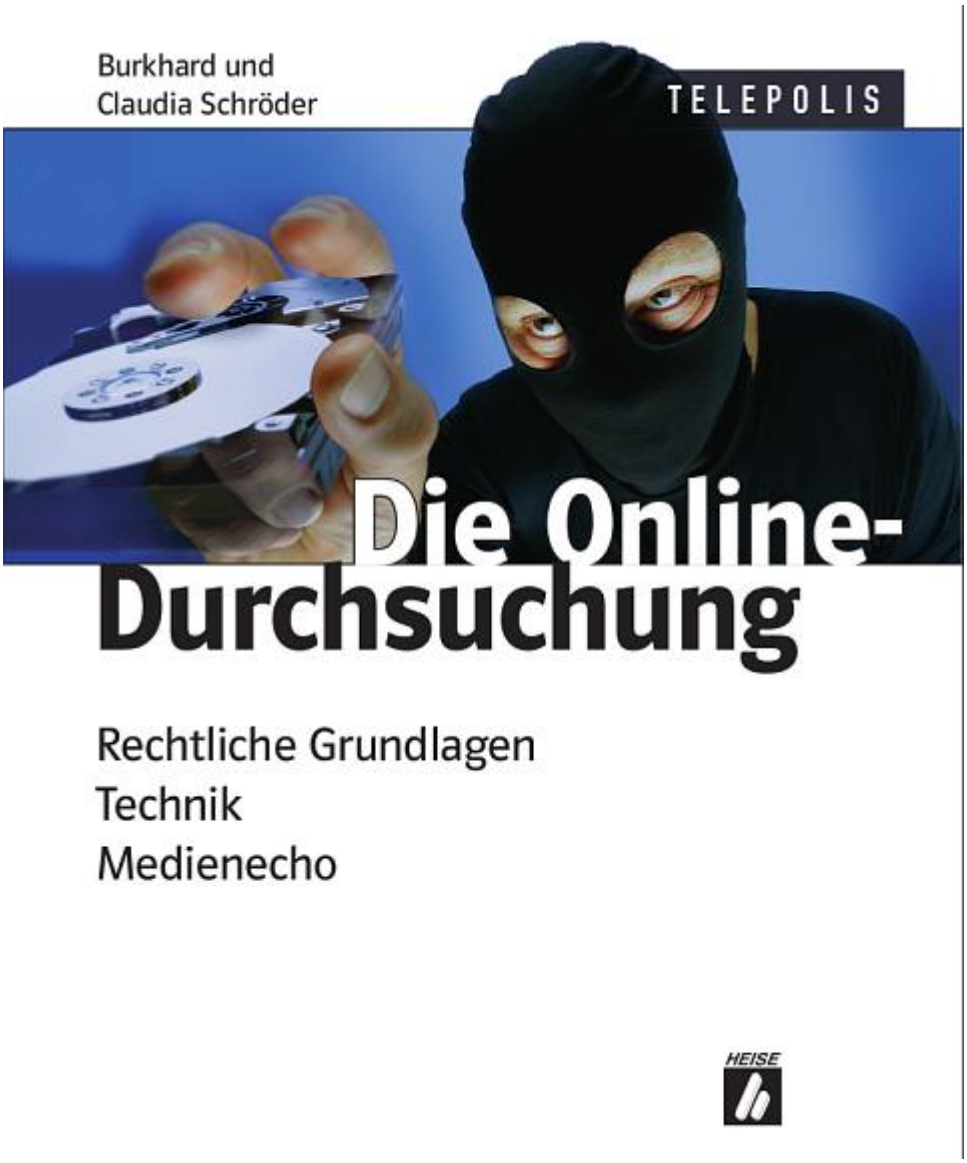
Neues Grundrecht | Papier holt die große Keule raus

Das nordrhein-westfälische Verfassungsschutzgesetz ist nichtig. Online-Durchsuchungen bleiben verboten. Noch mehr: Papier beginnt seine Begründung mit dem Satz, das Bundesverfassungsgericht konstituiere ein neues **Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme**. Schlimmer hätte es für Schäuble nicht kommen können.

Update (10.30 Uhr) Papier erteilt indirekt auch der Vorratsdatenspeicherung eine Absage. Der große Rundumschlag – ein Sieg der Bürgerrechte auf ganzer Linie.

Update: Das Urteil ist online.

Die Online-Durchsuchung



Burks proudly presents, hier exklusiv. Erscheint Anfang September 2008.

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.

Datenkrake Google, die 456ste

Golem.de (25.02.2007): „Google: IP-Adressen sind keine personenbezogenen Daten“. Noch einmal zum Mitschreiben: Google sagt, das *sei* so. Das stimmt aber nicht. „Fleischer machte deutlich, dass Googles Geschäftsmodell auf der Nutzung von personenbezogenen IP-Adressen basiert: „Wir müssen wissen, wer wonach fragt – andernfalls könnte unser Unternehmen nicht funktionieren“. Fleischer wurde sekundiert von Microsoft-Vertreter Thomas Nyrup, der darauf hinwies, dass „das Internet nicht wäre, was es ist, gäbe es die Werbung nicht“. Google bestätigte in der Anhörung, die Inhalte von über Google-Mail versandten E-Mails zu Werbezwecken zu analysieren.“

Sehr schön gesagt: Das Internet wäre nicht das, was es ist, gäbe es Microsoft nicht. Das Erde wäre nicht das, was sie wäre, gäbe es die Sonne nicht. Burks‘ Blog wäre nicht das, was es ist, gäbe es Burks nicht. By the way: Welcher Vollidiot verschickt unverschlüsselte E-Mails via Google-Mail? Auch lesen: Heise Newsticker: „Datenschützer stoppt das Speichern von IP-Adressen“.

Cold Boot Attacks on Encryption Keys

Es geht doch nichts über den physischen Zugriff auf einen Rechner, wenn man an die Daten herankommen will. Das Center for Information Technology Policy der Universität von Princeton hat jetzt bewiesen, dass die meisten Verschlüsselungssysteme, unter anderem auch Truecrypt, unter bestimmten Bedingungen unsicher sind: „Contrary to popular assumption, DRAMs used in most modern computers retain their contents for seconds to minutes after power is lost, even at operating temperatures and even if removed from a motherboard. Although DRAMs become less reliable when they are not refreshed, they are not immediately erased, and their contents persist sufficiently for malicious (or forensic) acquisition of usable full-system memory images.“

Die *Technology Review* hat ein ausführliches Interview dazu mit Edward W. Felten im Angebot – Felten ist Professor für Informatik an der Princeton University und hat die ausführliche Studie verfasst.

Worum geht es? Die DRAM-Speicherchips (für: Dynamic Random Access Memory) erinnern sich an bestimmte Daten, auch wenn der Rechner schon abgeschaltet wurde. Das kann man wieder sichtbar machen – also auch bestimmte Passworte und Schlüssel, die der Chip temporär speichert. Ein Angreifer msus also, soll die vorgeschlagene Methode funktionieren, den Rechner aus- und zeitnah wieder anschalten. Als Pointe haben die Forscher die Chips sogar mit Stickstoff abgekühlt. Dann dauert es noch länger, bis alle Daten nach dem Ausschalten des Computers verschwunden sind.

> *TR: Kann Ihre Methode tatsächlich jedes Festplattenverschlüsselungssystem knacken, das heute auf dem Markt ist?*
> *Felten: Alle, die wir getestet haben, darunter Microsoft BitLocker, Apple FileVault, dm-crypt unter Linux und TrueCrypt. Microsofts System ist in bestimmten Konfigurationen etwas sicherer, aber es sieht wohl so aus, als seien die meisten oder gar alle verfügbaren Festplatten-Verschlüsseler mit großer Wahrscheinlichkeit angreifbar.*

Fazit: Man muss zum Beispiel einen Laptop immer ausschalten,

der „Hibernations“- oder Stand-by-Modus nutzt überhaupt nichts, auch wenn die Festplatte verschlüsselt ist.

> *TR: Der physische Zugriff auf eine Maschine bleibt also immer ein Risiko.*
> *Felten: Ja. Zuvor dachte man aber eben, dass eine Festplattenverschlüsselung die Dateien auf einem Laptop schützt, selbst wenn dieser verloren oder gestohlen wurde. Unsere Ergebnisse zeigen nun, dass das nicht stimmt.*

Vorratsdatenspeicherung | Juristisches

Urteil des Zweiten Senats des Bundesverfassungsgerichts vom 2. März 2006 (2 BvR 2099/04) (ohne Literaturangaben)

> *(…) Das Fernmeldegeheimnis schützt in erster Linie die Vertraulichkeit der ausgetauschten Informationen und damit den Kommunikationsinhalt gegen unbefugte Kenntniserlangung durch Dritte.*
>
> *Als Folge der Digitalisierung hinterlässt vor allem jede Nutzung der Telekommunikation personenbezogene Spuren, die gespeichert und ausgewertet werden können. Auch der Zugriff auf diese Daten fällt in den Schutzbereich des Art. 10 GG; das Grundrecht schützt auch die Vertraulichkeit der näheren Umstände des Kommunikationsvorgangs.*
>
> *Dazu gehört insbesondere, ob, wann und wie oft zwischen welchen Personen oder Endeinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht worden ist. Andernfalls wäre der grundrechtliche Schutz*

unvollständig; denn die Verbindungsdaten haben einen eigenen Aussagegehalt. Sie können im Einzelfall erhebliche Rückschlüsse auf das Kommunikations- und Bewegungsverhalten zulassen. Häufigkeit, Dauer und Zeitpunkt von Kommunikationsverbindungen geben Hinweise auf Art und Intensität von Beziehungen und ermöglichen auf den Inhalt bezogene Schlussfolgerungen. (…)

Die freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist von dem Grundrecht aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG verbürgt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

Das Grundrecht dient dabei auch dem Schutz vor einem Einschüchterungseffekt, der entstehen und zu Beeinträchtigungen bei der Ausübung anderer Grundrechte führen kann, wenn für den Einzelnen nicht mehr erkennbar ist, wer was wann und bei welcher Gelegenheit über ihn weiß. Die Freiheit des Einzelnen, aus eigener Selbstbestimmung zu planen und zu entscheiden, kann dadurch wesentlich gehemmt werden.

Ein von der Grundrechtsausübung abschreckender Effekt fremden Geheimwissens muss nicht nur im Interesse der betroffenen Einzelnen vermieden werden. Auch das Gemeinwohl wird hierdurch beeinträchtigt, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger gegründeten freiheitlichen demokratischen Gemeinwesens ist. (…)

Bei den Verbindungsdaten handelt es sich um personenbezogene Daten, die einen erheblichen Aussagegehalt besitzen können und deshalb des Schutzes durch das Recht auf informationelle

Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) bedürfen.

Telekommunikation hat mit der Nutzung digitaler Übertragungsgeräte an Flüchtigkeit verloren und hinterlässt beständige Spuren. Durch die Digitalisierung fallen nicht nur bei den Diensteanbietern, sondern auch in den Endgeräten der Nutzer ohne deren Zutun vielfältige Verbindungsdaten an, die über die beteiligten Kommunikationsanschlüsse, die Zeit und die Dauer der Nachrichtenübertragung sowie teilweise auch über den Standort der Teilnehmer Auskunft geben und regelmäßig über den jeweiligen Kommunikationsvorgang hinaus gespeichert werden. Die Menge und der Aussagegehalt anfallender Verbindungsdaten lassen ein immer klareres Bild von den Kommunikationsteilnehmern entstehen. Auf Grund der Konvergenzen der Übertragungswege, Dienste und Endgeräte kommt es in der Telekommunikation in zunehmendem Maße zu einer Komprimierung des Informationsflusses. Die Endgeräte, vor allem Mobiltelefon und Personalcomputer, dienen nicht nur dem persönlichen Austausch, sondern zunehmend auch der Abwicklung von Alltagsgeschäften, wie dem Einkaufen oder dem Bezahlen von Rechnungen, der Beschaffung und Verbreitung von Informationen und der Inanspruchnahme vielfältiger Dienste. Immer mehr Lebensbereiche werden von modernen Kommunikationsmitteln gestaltet. Damit erhöht sich nicht nur die Menge der anfallenden Verbindungsdaten, sondern auch deren Aussagegehalt. Sie lassen in zunehmendem Maße Rückschlüsse auf Art und Intensität von Beziehungen, auf Interessen, Gewohnheiten und Neigungen und nicht zuletzt auch auf den jeweiligen Kommunikationsinhalt zu und vermitteln – je nach Art und Umfang der angefallenen Daten – Erkenntnisse, die an die Qualität eines Persönlichkeitsprofils heranreichen können.

4. Das Recht auf informationelle Selbstbestimmung schützt vor jeder Form der Erhebung personenbezogener Informationen. Ein Durchsuchungsbeschluss, der – wie hier – zielgerichtet und

> *ausdrücklich die Sicherstellung von Datenträgern bezweckt, auf denen Telekommunikationsverbindungsdaten gespeichert sein sollen, greift in das Grundrecht aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG ein.*
>
> *5. Beschränkungen des Art. 2 Abs. 1 GG bedürfen einer gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht.(…)*

Ich frage mich, ob die Herrschaften, die das Gesetz zur Vorratsdatenspeicherung beschlossen haben, jemals in eines der Urteile des Bundesverfassungsgerichts hineingesehen haben. Die Richter werden ihnen die Vorratsdatenspeicherung in kleine Fetzen zerreißen und auf den traurigen Resten vornehm herumtrampeln, bevor sie in die Tonne fliegen.

Online-Durchsuchung | Chronologie

Ich habe im Rahmen einer größeren Recherche die Medienberichte über die "Online-Durchsuchung" zusammengefasst (Auswahl). Sehr lustig, wenn man den Quatsch vergleicht, der zum Thema geschrieben wurde.

Irrationale Ängste?

Interview mit Albrecht Ude über die Vorratsdatenspeicherung: „Haben Sie irrationale Ängste vor der Vorratsdatenspeicherung, Herr Ude?“

Öffnen Sie den E-Mail-Anhang!

Quelle: vorwärts, Ausgabe 10/2007, Seite 47

Online-Durchsuchung 1993

Focus (38/1993): „Nationales Netz. Unter Verwendung zentraler Mailboxen bauen Neonazis ein landesweites Computernetz auf“. – „Die System Operators und ihre Überwacher experimentieren mit immer neuen Programmen. Hetzer alias Tetzlaff: ‚Eine Entschlüsselung ist für Unbefugte praktisch nicht mehr möglich.‘ Doch die Verfassungsschutztechniker dringen in die Mailboxen ein. Zunehmend knacken sie auch Paßwörter, die den Zugriff Unbefugter stoppen sollen. Die Beute: Veranstaltungstips, Hinweise auf neue Bücher und Szeneschriften…(…) Bayerns Verfassungsschutz- Vizepräsident Volker Haag: ‚Dann kann die Planungszeit für extremistische Aktionen eventuell so verkürzt werden, daß uns kaum noch eine Möglichkeit zum Eingreifen bleibt.'“

Wie sich die Worte gleichen….

Eilentscheid über Vorratsdatenspeicherung noch

im März

Reuters (14.02.2008): „Das Bundesverfassungsgericht will seine mit Spannung erwartete Eilentscheidung über die umstrittene Vorratsdatenspeicherung rasch verkünden. ‚Wir beabsichtigen, noch im März zu entscheiden', sagte Gerichtspräsident Hans-Jürgen Papier am späten Mittwochabend in Karlsruhe." [mehr…]

Soft Tempest

Informationsdienst Wissenschaft (13.02.2008): „Über Reflexionen in Teekannen, Kaffeetassen, Brillengläsern oder sogar in den Augen eines PC-Benutzers kann man die Daten eines beliebigen Bildschirms ausspionieren. Das haben Informatiker unter Leitung von Prof. Dr. Michael Backes (Lehrstuhl für Informationssicherheit und Kryptographie der Universität des Saarlandes) untersucht. Mit einer speziell angepassten Teleskop-Ausstattung im Wert von rund tausend Euro konnten die Saarbrücker Wissenschaftler noch in einer Entfernung von über zehn Metern Informationen rekonstruieren, die in verschiedenen Gegenständen gespiegelt wurden. Das Forscherteam geht davon aus, dass man mit professionelleren Geräten mühelos aus größerer Entfernung, etwa vom Fenster eines Nachbargebäudes aus, geheime Daten auf diese Weise ablesen könnte." [mehr…]

By the way: So neu ist das Thema nicht. Steht noch viel komplizierter in Markus Kuhns Arbeit (zusammen mit Ross Anderson): „Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations". (Vorsicht – nur für Geeks!). Einfacher hatte Kuhn ein ähnliches Procedere vor zehn Jahren in der c't beschrieben: „In die Röhre geguckt – Unerwünschte Abstrahlung erlaubt Lauschangriff".

Aber so etwas liest man bei Schäubles natürlich nicht….

Nachtrag: Vgl. Van-Eck-Phreaking (Wikipedia).

Online-Durchsuchung, die 234ste

Video: „Heimliche Online-Durchsuchung – wie geht's, wie schütze ich mich?" Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: Offene Informationsgesellschaft und Terrorbekämpfung – ein Widerspruch? Sommerakademie 2007 am 27. August 2007. Sehenswert!

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…

Vorratsspeicherung von Kommunikationsspuren verboten

Urteil: Vorratsspeicherung von Kommunikationsspuren verboten.

> *Ein Berliner Gericht hat dem Bundesjustizministerium in einem Grundsatzurteil untersagt, das Verhalten der Besucher des Internetportals des Ministeriums aufzuzeichnen. Ein Urteil mit Folgen für Internetbranche und Politik.*

Vgl. die Musterklage.

Tarnkappe und Lichtschwert

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

Online-Datenerhebung

Ein Hoax wird zum Gesetzentwurf – sehr lustig. Das bayerische Kabinett radebrecht, dass es nur so kracht: „Unter engen Voraussetzungen brauchen wir deshalb künftig eine Online-Datenerhebung durch das Landesamt für Verfassungsschutz. Die Verfassungsschutzbehörden dürfen von der technischen Entwicklung nicht abgehängt werden.“ Halleluja. Nun programmiert mal schon. Das erinnert mich an einen legendären Satz Heinrich Lübkes, als er eine Wirtschaftsdelegation aus Afrika verabschiedete: „Nun entwickelt euch mal schön da unten.“