gpfTOR4 online

German Privcy Foundation proudly presents: Der 4. Tor-Server ist online (gpfTOR4). Voraussichtlich ab Montag wird er schon unter den Top 10 weltweit sein.

Wovon Schäuble noch träumt

Parodie eines Telekom-Werbespotes von NDR – Extra3: “Wovon Schäuble noch träumt, ist bei uns schon Wirklichkeit!“

Kurze Einführung in Anon-Dienste für Schäuble

Karsten hat eine „Kurze Einführung in Anon-Dienste für Ermittlungsbehörden“ verfasst.

Jahresstatistik TK-Überwachung

Bundesnetzagentur: „Die Bundesnetzagentur hat heute in ihrem Amtsblatt die Jahresstatistik 2007 der strafprozessualen Überwachungsmaßnahmen der Telekommunikation gemäß § 110 Abs. 8 Telekommunikationsgesetz (TKG) veröffentlicht. Danach wurden von den Gerichten im letzten Jahr 38.386 Anordnungen zur Überwachung der Telekommunikation sowie 7.603 Verlängerungsanordnungen erlassen. Die Anordnungen betrafen 39.200 Rufnummern von Mobiltelefonanschlüssen und 5.078 Rufnummern von Festnetzanschlüssen (analog und ISDN).(…) Im Mobilfunkbereich ist ein anhaltender Anstieg der Überwachungsmaßnahmen zu verzeichnen, der generell auf Teilnehmerzuwächse zurückzuführen ist. Besonders im Jahr 2007 zog eine Zunahme der Mobiltelefonteilnehmer von über 13 Prozent einen entsprechend steileren Anstieg der Überwachungsmaßnahmen im Vergleich zu den Vorjahren nach sich. Im Festnetzbereich wurde ein leichter Rückgang der Überwachungsmaßnahmen analog zum Jahr 2006 beobachtet.“

Spionageangriff auf Bundescomputer

Tagesanzeiger (09.05.2008): „An dem E-Mail [sic] war nichts Verdächtiges. 500 Mitarbeitende der Bundesverwaltung wurden Ende 2007 persönlich angeschrieben und von einem Bundesamt aufgefordert, an einem Fotowettbewerb teilzunehmen. Wer mitmachte, wurde über einen Link im Mail auf die Website des Bundesamts geführt und konnte in der Rubrik Fotowettbewerb seine Stimme für ein Bild abgeben. Dieses wurde dann automatisch als Bildschirmschoner auf den eigenen Computer heruntergeladen. (…) Das E-Mail war genau so gefälscht, wie der Absender und die Website mit den Fotos. Letztere war als perfekte Kopie des Originals auf einem Server in einem afrikanischen Staat aufgeschaltet worden. Von dort aus infiltrierten so genannte Trojanische Pferde via Bildschirmschoner die Bundesverwaltung. (…) ‚Der Angriff war so gut gemacht, dass man den Opfern nicht einmal einen Vorwurf machen kann', sagt der Experte. Die arglosen Angestellten wurden mit Vor- und Nachnamen angeschrieben."

Keine Chance? Das ist doch Unfug. Erstens funktioniert die oben geschilderte Methode so nur bei Windows-Rechnern. Und zweitens würde ich allen Angestellten verbieten, Postkarten zu öffnen und zu lesen. Und als EDV-Verantwortlicher hätte ich drittens „automatische Downloads" und die Installation von Bildschirmschonern sowieso untersagt. Viertens handelt es sich um Spam, wie im Artikel auch steht. Was nach Afrika geschickt wurde, wird leider nicht verraten; man weiß noch nicht einmal, ob es nicht nur ein Spammer-Test war.

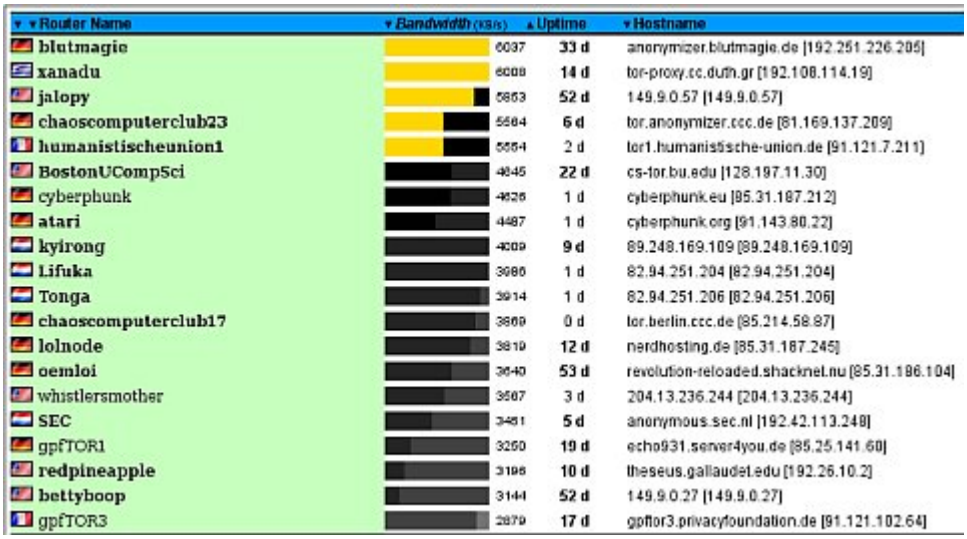
Im Heise-Forum gibt es ein paar hübsche Statements dazu, etwa: „Es gibt für den mac ein programm namens „little snitch„, welches sofort bei " connect „zu einem Server Alarm schlägt, gibts sowas für PCs nicht?" (vergleichbar mit ZoneAlarm: „so wirksam wie eine Schale mit Weihwasser neben dem Bildschirm").

Oder: „>braucht man zu installieren von malware nicht root rechte? Kommt drauf an. Unter Windows nein, da kannst du per Doppelklick alles starten das nicht bei 3 auf dem Baum ist. Was man starten kann, kann sich auch irgendwo einnisten. Unter z.B. Linux ist das schon komplexer…“ Oder: „Leider kann auch Gast einen Screensaver installieren. Der Nutzer DAU, welcher rechtemäßig weit unter Gast steht, ist in Windows nicht enthalten. Mit Linux wäre das nicht passiert.“

Die Online-Durchsuchung, revisited

Ankündigung des dpunkt-Verlages: „‚Die Online-Durchsuchung‘ ist das erste Sachbuch, das sich dem umstrittenen Thema widmet. Die Autoren zeichnen kritisch die widersprüchliche Berichterstattung in den Medien nach, beschreiben die Technik und deren Grenzen, heimlich in fremde Rechner einzudringen und fassen die weit verstreute, schwer zugängliche und oft einem Laien nicht verständliche juristische Fachliteratur zur „Online-Durchsuchung“ zusammen. Die aktuelle Rechtssprechung des Bundesverfassungsgerichts wird berücksichtigt. Das Buch richtet sich nicht nur an Juristen, IT-Fachleute und Journalisten. Es ist so geschrieben, dass es für ein breites Publikum eine interessante Lektüre bietet. Die Autoren beantworten auch ausführlich eine Frage, die viele interessiert: Kann man sich vor einer Online-Durchsuchung schützen?“
Erscheint voraussichtlich Juli 2008, ca. 180 Seiten, Broschur, ISBN-13 978-3-936931-53-2, ca. 16 Euro (D) / 16,5 Euro (A) / 28 sFr

GPF proudly presents



Router Name	Bandwidth (KB/s)	Uptime	Hostname
blutmagie	6037	33 d	anonymizer.blutmagie.de [192.251.226.206]
xanadu	6009	14 d	tor-proxy.cc.duth.gr [192.108.114.19]
jalopy	5863	52 d	149.9.0.57 [149.9.0.57]
chaoscomputerclub23	5584	6 d	tor.anonymizer.ccc.de [81.169.137.209]
humanistischeunion1	5564	2 d	tor1.humanistische-union.de [91.121.7.211]
BostonUCompSci	4645	22 d	cs-tor.bu.edu [128.197.11.30]
cyberphunk	4626	1 d	cyberphunk.eu [85.31.187.212]
atari	4487	1 d	cyberphunk.org [91.143.80.22]
kyirong	4089	9 d	89.248.169.109 [89.248.169.109]
Lifuka	3986	1 d	82.94.251.204 [82.94.251.204]
Tonga	3914	1 d	82.94.251.206 [82.94.251.206]
chaoscomputerclub17	3869	0 d	tor.berlin.ccc.de [85.214.58.87]
lolnode	3819	12 d	nerdhosting.de [85.31.187.245]
oemloi	3640	53 d	revolution-reloaded.shacknet.nu [85.31.186.104]
whistlersmother	3567	3 d	204.13.236.244 [204.13.236.244]
SEC	3481	5 d	anonymous.sec.nl [192.42.113.248]
gpfTOR1	3260	19 d	echo931.server4you.de [85.25.141.60]
redpineapple	3196	10 d	theseus.gallaudet.edu [192.26.10.2]
bettyboop	3144	52 d	149.9.0.27 [149.9.0.27]
gpfTOR3	2879	17 d	gpftor3.privacyfoundation.de [91.121.102.64]

Die Server gpfTOR1 und gpfTOR3 sind unter den ersten 20 weltweit, gpfTOR2 hoppelt ein wenig hinterher….

Quick Scan

Auf security-check.ch kann man Browser und System auf Sicherheitslücken online testen lassen. Empfehlenswert!

Auch schön: [Wie Personal Firewalls ausgetrickst werden können](), [c't-Browsercheck](), [CERT Tech tips]() und vor allem die [Hardcore-Version]() von Lutz.

John the Ripper

Passwortknacker: „John the Ripper is a fast password cracker, currently available for many flavors of Unix (11 are officially supported, not counting different architectures), Windows, DOS, BeOS, and OpenVMS. Its primary purpose is to detect weak Unix passwords.“

Mehr mächtige Spionage-Werkzeuge, bitte!

Vorgestern hatte ich mich schon über die faktenarmen Textbausteine echauffiert, die jetzt wieder zum Thema „Bundestrojaner“ im Umlauf sind. „Der Angriff mittels eines sogenannten [sic] Trojaners“, schreibt SPIEGEL Print. Nein. Erstens heißt das Ding „Trojanisches Pferd“. Die Trojaner waren das Opfer, nicht die Täter. Und zweitens ist es nicht legitim, jedwede Art von Spionagesoftware jetzt als „Trojaner“ zu bezeichnen. Es hat sich bisher auch niemand erkühnt zu behaupten, die Implementierung der Überwachungs-Software sei *online* geschehen.

„Sie schleusen heimlich einen Trojaner in das Computernetzwerk des Ministeriums für Handel und Industrie, eine Spähsoftware, die sich auf den fremden Rechnern einnistet und in aller Stille hilft, den Inhalt der Festplatten nach Deutschland zu schicken. Heimlich schleusen – geht es etwas genauer? Ist das afghanische Netz so unzureichend gesichert, haben es die Deutschen vielleicht selbst aufgebaut, Datenlecks per default inbegriffen? Ich gehe davon aus, dass die Schlapphüte Keylogger und das übliche Zeugs direkt und „händisch“

installiert haben – oder denen gleich die ab Werk verwanzten Rechner direkt vor die Nase gestellt haben. Windows, I presume.

Auch im Kongo haben die Geheimdienstler im letzten Jahr Rechner verwanzt, berichtet SPIEGEL Print (28.04.2008, S. 24). „Der Einsatz flog auf, weil einer der BND-Männer das mächtige Spionage-Werkzeug zweckentfremdete, um romantische Postg seiner Partnerin an einen Bundeswehrangehörigen abzufangen." Bruhahaha.

Die Leitung am Hindukusch muss übrigens recht dick sein, wenn man ganze Festplatten (ab 40 Gigabyte aufwärts) verschicken kann, ohne dass die Kisten abrauchen oder alles nur noch in Zeitlupe geschieht. Die „Unterlagen zu diesem Fall wurden offenbar weitgehend vernichtet". Sehr schön. Also bleibt viel Platz für wildes Herumspekulieren.

„Der Trojaner meldet nach Pullach, dass Farhang eine E-Mail-Adresse des amerikanischen Internet-Anbieters Yahoo nutzt, und das Passwort liefert er gleich mit." Übersetzt heißt das: Ein afghanischer Minister nutzt keine eigenen Server, sondern ein Postfach bei Yahoo. Kann man so blöd sein? Ja, kann man. By the way: „Die Menschenrechtsorganisation Amnesty International hat den US-Unternehmen Microsoft, Google und Yahoo vorgeworfen, bei der Zensur des Internets durch China mitzuwirken." Farhangund seine ganze Behörde haben offenbar vom Internet so viel Ahnung wie Michael Konken vom Bloggen. Und alle schreiben Postkarten. Das ist mittlerweile irgendwie ein Running Gag. Traurig, aber wahr.

Ich gönne ihnen die „Trojaner". Mehr davon, bitte! Gegen die schier unfassbare Naivität, Belehrungsresistenz und Ignoranz der meisten Menschen, die Sicherheit der Daten und der elektronischen Kommunikation betreffend, kann man offenbar erst dann verändern, wenn man ihnen demonstriert, welche Folgen das hat. Ich wette, dass Farhang noch immer Postkarten schreibt, und die betroffene Journalistin auch.

Nachtrag. Die FAZ schreibt: „So sei nicht das persönliche E-Mail-Konto des Ministers, sondern seine Dienst-Mail-Adresse betroffen gewesen, sagte ein BND-Sprecher. Im ‚Spiegel'-Bericht sei von einer persönlichen Yahoo-Mail-Adresse des Ministers die Rede. Nach Angaben des BND wird jedoch der gesamt E-Mail-Verkehr des Ministeriums über den amerikanischen Provider Yahoo abgewickelt." Das ist ja noch schlimmer…

Bundestrojaner beim Afghanen?

Stefan Krempl scheibt bei Heise: „Der Bundesnachrichtendienst (BND) hat Berichten zufolge eine heimliche Online-Durchsuchung beim afghanischen Handels- und Industrieminister Amin Farhang durchgeführt, bei der auch die Kommunikation mit einer Spiegel-Reporterin erfasst worden sein soll." Ich glaube vorsichtshalber erst einmal gar nichts. Weiter heißt es: „Nach Informationen der Nachrichtenagentur ddp war es dem BND gelungen, mit Hilfe eines Trojaners auf der Festplatte von Farhang ein Spähprogramm zu installieren." Was sagen die Quellen?

Krempl zitiert sich in typischer Manier selbst: „Die

monatelange Observation der Journalistin zwischen Juni und November 2006, die das Nachrichtenmagazin am Wochenende bekannt machte, war demnach offenbar ein ‚Nebenprodukt' der Bespitzelung des Spitzenpolitikers". Das – der zweite Satz des Artikels – suggeriert, als sei die Observation eine „Online-Durchsuchung" gewesen. Das war aber mitnichten so. Hinter dem verlinkten „bekannt geworden verbirgt sich ein Artikel von Spiegel Online, in dem es lediglich heißt: „Der Bundesnachrichtendienst (BND) hat monatelang die E-Mail-Korrespondenz der 42-jährigen SPIEGEL-Reporterin mit dem afghanischen Politiker überwacht und mitgeschnitten." Das Abhören des Kommunikation hat mit einer Online-Durchsuchung nichts zu tun und ist ein Kinderspiel, wenn die Beteiligten ihre Korrespondenz nicht verschlüsseln. Typisch für das Niveau deutscher Recherche ist auch, dass das „Opfer" Susanne Koelbl meinte, an einen afghanischen Politiker Postkarten schreiben zu müssen und „nicht ahnte", dass auch andere Leute die lesen wollten – und das natürlich getan haben. Die Kollegin antwortet übrigens nicht auf meine E-Mails zum Thema.

Die Welt online berichtet: „…wurde zum Abschöpfen des E-Mail-Verkehrs zwischen der „Spiegel"-Journalistin Susanne Koelbl und dem Politiker aus Kabul zwischen Juni und November 2006 ein ‚Trojaner' eingesetzt. Das Spionageprogramm, für dessen Einsatz das Bundesverfassungsgericht unlängst hohe Hürden gesetzt hat, sei auf der Festplatte des Computers des Afghanen installiert worden, hieß es. Dabei seien auch ‚intime Bereiche' der persönlichen Lebensführung der Journalistin ausgespäht worden."

Da haben wir's. Jede Wette, dass der BND den physischen Zugriff auf den Rechner hatte und entweder einen Keylogger oder so etwas sie EnCase® Field Intelligence Model eingesetzt hat. [Vgl. c't: Der weisse Spion]. Die Stattzeitung für Südbaden erwähnt ein weiteres interessantes Detail: Der heutige afghanische Wirtschaftsminister, ein ehemaliges Mitglied der deutschen Grünen uind „langjährig in Nord-Rhein-

Westfalen ansässig,… (…) Die Ausspähung geschah ab 2006 per Trojaner. Also existiert schon ein funktionsfähiges Modell. Dabei wurde offiziell immer wieder geächzt, wie teuer so was sei und wie schwer zu installieren.“ Und genau das ist die Pointe: Der berüchtigte „Bundestrojaner“ wird im öffentlichen Diskurs als heimlciher Zugriff über das Internet verstanden. Darum geht es hier aber gar nicht, sondern um ein Spionageprogramm, dass auf der Festplatte installiert worden war. Und so etwas ist gar nicht teuer und auch nicht kompliziert und existiert natürlich schon in verschiedenen Varianten.

Farhang hat das selbst bestätigt, wie die FTD meldet: „Er habe erfahren, dass der BND *seinen Computer im Büro* manipuliert habe. Er gehe davon aus, dass nicht nur einer seiner Computer für wenige Monate überwacht worden sei, wie der BND behaupte. „Ich habe das Vertrauen verloren und nehme an, dass deutsche Agenten alle meine Telefonate und E-Mails noch immer überwachen.“ Quod erat deminstrandum.

Falsch im Heise-Bericht ist definitiv: „Im Januar war bekannt geworden, dass der Geheimdienst bereits rund 60 Mal heimlich Zielrechner Verdächtiger im Ausland über das Internet ausgeschnüffelt haben soll“. Soll. Nicht hat. Dass das gar nicht stimmt und auch im damaligen Focus-Artikel falsch war, hat man mir mir telefonisch bestätigt. Es soll damals – durch den BND – nur *eine* „Online-Durchsuchung“ gegeben haben, und dafür auch nur eine Quelle. Es ist also gar nichts verifizierbar.

Stasi 2.0, reloaded

Heise.de unter dem Titel: „Schäuble und die Online-Durchsuchung: „heimliches Betreten der Wohnung“ grundgesetzkonform?“: „Unionspolitiker sind dagegen der Ansicht, das „heimliches Betreten“ genannte Vorgehen zur Installation des Bundestrojaners vor Ort sei keine Wohnungsdurchsuchung und daher grundgesetzkonform.“

Die lesen Gesetze und Urteile gar nicht mehr – nach dem Prinzip „legal, illegal, scheißegal“. Aus dem Urteil des BVerfG vom 27.02.2008, Randnummer 193: „Darüber hinaus kann eine staatliche Maßnahme, die mit dem heimlichen technischen Zugriff auf ein informationstechnisches System im Zusammenhang steht, an Art. 13 Abs. 1 GG zu messen sein, so beispielsweise, wenn und soweit Mitarbeiter der Ermittlungsbehörde in eine als Wohnung geschützte Räumlichkeit eindringen, um ein dort befindliches informationstechnisches System physisch zu manipulieren. Ein weiterer Anwendungsfall des Art. 13 Abs. 1 GG ist die Infiltration eines informationstechnischen Systems, das sich in einer Wohnung befindet, um mit Hilfe dessen bestimmte Vorgänge innerhalb der Wohnung zu überwachen, etwa indem die an das System angeschlossenen Peripheriegeräte wie ein Mikrofon oder eine Kamera dazu genutzt werden.“

Nur zur Erinnerung die Passage im Grundgesetz, Artikel 13, Absatz 1 und 2: „Die Wohnung ist unverletzlich. Durchsuchungen dürfen nur durch den Richter, bei Gefahr im Verzuge auch durch die in den Gesetzen vorgesehenen anderen Organe angeordnet und nur in der dort vorgeschriebenen Form durchgeführt werden.“

Freiheitskampf im Netz

Freiheitskampf im Netz – ganz wunderbarer Kommentar von Kai Biermann in ZEIT online: „Es geht bei der Onlinedurchsuchung nicht darum, ein wirksames Instrument für Strafermittler zu schaffen. Das ist nach der Einigung von Innenminister Wolfgang Schäuble und Justizministerin Brigitte Zypries nun offensichtlich. Es geht um Abschreckung. Und es geht auf der anderen Seite darum, dass die demokratische Gesellschaft sich ihre Freiheiten und Rechte im Zeitalter des Internets neu erkämpfen muss."

Schäuble: Entwurf für Online-Razzien sei verfassungsgemäß

Heise.de: „Schäuble: Entwurf für Online-Razzien ist verfassungsgemäß". Nein, falsches Deutsch: Die indirekte Rede verlangt nach dem Konjunktiv. Es ist mitnichten so, Schäuble behauptet es nur.

Aus dem heise.de-Forum dazu:
„(…) Ein Minister erzaehlt komprimierte Scheisse, die DPA schreibt's ab, SPON kopiert von der DPA sw. usf. Nochmal zum Mitlesen: Der Grosse Lauschangriff ist mit Urteil des BVerfG vom 03.03.2004 gekippt worden. Das Urteil musste bis zum 30. Juni 2005 in einem neuen Gesetz umgesetzt worden sein (ist bisher nicht passiert). Solange der Gesetzgeber nicht gehandelt hat, muss die Polizei das Urteil des Bundesverfassungsgerichts umsetzen.
In diesem Urteil ist *ausdruecklich* von der akustischen – nicht optischen – Wohnraumueberwachung die Rede: Der Einsatz

von Video-Kameras in privaten Wohnraeumen ist somit nicht zulaessig. (…)“
[Link zum Urteil, Aktenzeichen: 1 BvR 2378/98, 1 BvR 1084/99]

Onlinedurchsuchung kommt nicht

Ich muss der Verschwörungstheorie von ZEIT online widersprechen. Die Online-Durchsuchung kommt *nicht*. Aber da ich gerade bei der Endredaktion des Buchmanuskripts zum Thema bin, habe ich keine Zeit, dazu jetzt schon mehr zu sagen.

Das Internet ist die größte Revolution

Süddeutsche Zeitung (11.04.2008): „Der soeben aus dem Amt geschiedene Bundesverfassungsrichter Wolfgang Hoffmann-Riem spricht über die Fernseh- und Medienlandschaft der Zukunft, das Verhältnis von Freiheit und Sicherheit, die Symbolpolitik von Schily und Schäuble sowie die Philosophie der Rechtsprechung des höchsten deutschen Gerichts.“

„…wie die Online-Durchsuchung oder der Große Lauschangriff.
Hoffmann-Riem: Beide wurden als Wunderwaffen angepriesen, ohne die die innere Sicherheit nicht mehr zu gewährleisten sei. Wenn aber nach Nachweisen ihrer Unverzichtbarheit gefragt wird, kommt entweder fast gar nichts oder es folgen

Beschwörungsformeln. Es gab ja beispielsweise schon ein paar Online-Durchsuchungen, deren Auswertung ich bei unserer Entscheidung gern gekannt hätte. Aber in der mündlichen Verhandlung vor unserem Gericht hatten die höchsten Beamten gerade dafür keine Aussagegenehmigung.“

Vgl. Burks‘ Blog (07.03.2008):
„Sind dem Bundesverfassungsgericht dazu andere Quellen bekannt als die Berichterstattung in den Medien?“
„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“

Stasi 2.0 Beta

Heise.de beruft sich auf eine Vorabmeldung von Spiegel Online: „Verfassungsschutz will Internet-Knotenpunkte überwachen. (…) Nicht mehr nur auf Festplatten will er zugreifen dürfen – auch E-Mail-Konten und ganze Internet-Knotenpunkte wollen die Ermittler überwachen.“

Ja, finde ich super. Jeder soll die E-Mails lesen dürfen, die ich bekomme. Hier, bitte:

——BEGIN PGP MESSAGE——
Version: GnuPG v1.4.7 (MingW32) – WinPT 1.2.0
Comment: .

hQIOA4Z7um4C7bRaEAgAuLGfQeUWHO9MmVYDQQN58+pPOM8TobWIrTkK/ighfpnW
OC0ShEXtgs6lgaFdj9JcPYIHQmSpnuUuvR4l44sz6krYkj5iwEy5SZxRZfLZBuHD
5uK3FvxIFjiYEGL2SIUbPYbP/NnGctJOh76364jdv6cIsjVcDQ3tCrqaxVc5++

EY
LlaR3i/v21ZwyuZLAGq4xjVrl6DmL8Qeqj54cpLzamxNd65JbBcpDGk5dTTeC4
IW
BSRivch4q4HUZAbGyzqxOhfDrK1+o7vSeMRTPhG1EANrjtOgr2z6YdFTXThbr/
eV
R9RHU4nVk1GaT7fM1KGpGEVO+QlIRtdjjpDUeJASZAf/ZwrdAuo4lpUMVNlS/U
+L
H4RAvs+AgJagJiKEFpctpNUvSizMkIpZgfyXrF9CZCCPfOiOYP/WfgdcEM2loa
3K
7kgaCSsWO1rVNU4TPrRE3jdr1a2r73cwLSxFt9jJ1U9+g46ovrwGkl5FpHj9/h
xd
W6AdtGFAlLZm8EQpj9WsS9iO8NVpiX492+g8bgux/sCKPYsZBl7leQ8Pnn1FsT
Qz
bBcUbhyjY3sE52cEw3lDv5Y64B7TgjxCcOWzHMjcFyYhVVsccuyZEdgABaKeVf
Nk
zl7LVjWAgvy4c7LMXqthgrXrSu8W3PHTQ4oUpvSGS9JvzLbB+terunDNmxhQDv
2a
ZdLAwgEyJpehiV7k5viwT1ung2sMDgsUgLCbwU1z+vaWA0Z/kEupbgJcu44qcR
nL
DsGjmU9K3sWiJapa/SiZfUciw2SPeAWAXxaK6ZwmsS7ZktBnADeCk5yO4GcBrx
Yl
90QRJ/QOPkvSyGBlnaHFiBwnSpax+dco1Ey3UufL3gs++7wRgJf4uLjshpT1FD
SH
82XAQ8wnGv0zTo/2cNIaDrCxQugAYXhx8hPnr0AgdvdGtxlcDbgm9m4JVaPs+u
5W
V9+fvh8tbJpQjzT0aJdIsH3UHmEjyQnXRuGcsYIxHBczOUMqrWfFIwvvQFi0zx
Fb
BRW5j711ZCbovt9yoV89pI/sWtThd8EJLVcCeMHxPlhByI5TIZB2nYZVQxWa7Y
hU
NiCnU8CoXzSzlDSE9Q+6H2jnGC8afuyXBZgRKackWyXCEHeHtEMVGbXOWwnTUQ
Rh
UxDq4cSQHZUAbTnWTDWNZFvET4s3YY+0sypwzE+sFwk8wuAmyPSIibP5SQ71Qx
K9
MkXKUk9g
=d5Yo
——END PGP MESSAGE——

German Privacy Foundation | Mitgliederversammlung

Heute fand die Mitgliederversammlung der German Privacy Foundation im Haus der Demokratie und Menschenrechte statt. Der bisherige stellvetretende Vorsitzende Ricardo Cristof Remmert-Fontes wurde abgewählt. Neuer stellvertretender Vorsitzender ist der Dipl.-Informatiker Jan Suhr.

Kein Speichern unter dieser

Nummer

Ein Artikel (pdf) von mir in der Zeitschrift des Deutschen Fachjournalisten-Verbands (DFJV) über Möglichkeiten, sich gegen die Vorratsdatenspeicherung zu schützen.

Übergriff als Methode

Kai Biermann in Zeit Online: „Übergriff als Methode. (…) Es geht um Missachtung der Grundrechte, um Ignoranz, um die Angst des Staates vor seinen Bürgern. ‚Politische Psychosen', nennt das der frühere Richter Heribert Prantl in der Süddeutschen Zeitung und heißt Karlsruhe ‚die Nervenheilanstalt der Republik'. Ach, wenn es doch nur um ein paar Verrückte ginge. Tatsächlich sind in Berlin offensichtlich an entscheidenden Stellen Anarchisten am Werk, für die Regeln nicht gelten und die nach dem alten Spontispruch handeln: Legal, illegal, scheißegal."