Ich mache mir meine Vorratsdatenspeicherung selbst

.schtieF's live, Android, cooking, IT: „Auf der Seite schtief.org sieht man eine Karte auf der mit Rot mein Bewegungsprofil der letzten 36 Stunden dargestellt wird. Dieses Bewegungsprofil erstelle ich anhand der Ortungsdaten die mein Handy aussendet. Diese Positionsangabe sendet mein Handy auch ohne angeschaltetes GPS…"

SSLSTRIP und Etherpad

Ich empfehle Etherpad: „EtherPad is the only web-based word processor that allows people to work together in really real-time. When multiple people edit the same document simultaneously, any changes are instantly reflected on everyone's screen. The result is a new and productive way to collaborate on text documents, useful for meeting notes, drafting sessions, education, team programming, and more."

Und jetzt zu etwas ganz Anderem: Sehr interessant ist SSLSTRIP. Ein oberflächlicher, „aktueller" und gewohnt linkfreier Artikel der taz vom 19.11. brachte mich auf die Idee, selbst zu recherchieren. Das Event, auf dem dieser mögliche Angriff auf HTTPS vorgestellt wurde, fand schon im Februar statt.

„This tool provides a demonstration of the HTTPS stripping attacks that I presented at Black Hat DC 2009. It will transparently hijack HTTP traffic on a network, watch for

HTTPS links and redirects, then map those links into either look-alike HTTP links or homograph-similar HTTPS links.“

Clickjacking

Gestern stieß ich auf das Bild einer attraktiven Frau auf pressetext.de und bekam die obige Fehlermeldung.

Man lernt doch nie aus – es handelte sich um Clickjacking: „Dabei lassen Angreifer die ahnungslosen Anwender – scheinbar – auf die überlagerten Objekte klicken. Tatsächlich jedoch wird der ursprüngliche Inhalt (Button/Link) der Internetseite ausgelöst. So geschieht es, dass der User – anstatt lediglich auf die ihm vorgegaukelten Links an einer Stelle zu klicken – eine vom Hacker definierte, beliebige Aktion auslöst.“

Von pressetext.de bzw. pte.at hätte ich so etwas nicht erwartet. Zum Glück benutze ich NoScript.

German Privacy Foundation bloggt

Die German Privacy Foundation hat jetzt nicht nur ein Forum, sondern auch ein Blog.

Nicht ohne eure IP-Adressen

Das ist doch eine hübsche Meldung: „Der Berliner Datenschutzbeauftragter [sic] hat dem Bildblogger Stefan Niggemeier bezüglich dessen Seite www.stefan-niggemeier.de untersagt, IP-Adressen von Nutzern ohne deren Einwilligung zu speichern und somit heimlich Nutzungsprofile zu erstellen. Außerdem hat der Datenschutzbeauftragte unter Bußgeldandrohung eine fehlende Unterrichtung über die Erhebung, Verwendung und Verarbeitung von Nutzerdaten auf Niggemeiers Webseite gerügt. Ferner sei es unzulässig, in Foren E-Mail-Adressen als Pflichtfeld abzufragen. Dies geht aus mehreren Schreiben der

Behörde, zuletzt vom 26.10.2009 hervor (Az. 521.4501).“ [mehr…]

Übrigens: Mein Provider minuscel screen partner speichert *nicht*. Jetzt muss ich mal schnell bei Kai Diekmann vorbeischauen, ob der speichert….

Tor-Betreiber freigesprochen

Pressemitteilung: Jena, den 29.10.2009
„Am heutigen Tage fand in Saal 1 des Amtsgerichts Jena eine Strafverhandlung gegen den Domaininhaber von wikileaks.de, Theodor Reppe, statt. Der Tatvorwurf lautete: Computerbetrug – Reppe soll unter Verwendung von falschen Angaben einen Internetzugang gebucht und hierdurch einen Schaden in Höhe von 38,55 EUR verursacht haben. Einziges Beweismittel: Eine IP-Adresse, die zu den Kundendaten von Reppe führt. Nach einer gleich zu Beginn vom Verteidiger Norman Lenz verlesenen Stellungnahme und weiteren Erklärungen Reppes mussten Gericht und Staatsanwaltschaft jedoch einsehen, dass Reppe nicht der Täter ist. Es stellte sich heraus, dass ein von Reppe betriebener Tor-Server von Unbekannten missbraucht wurde.

Zwischen Gericht und Verteidigung entbrannte die Frage, ob Reppe deswegen schuldig sei, weil er die Datenübertragung für die Betrugstat ermöglicht habe. Das Gericht offenbarte konservativ-populäre Ansichten, wonach Projekte wie Tor gesellschaftlich mehr schadeten als nutzten. Es fielen Sätze wie: ‚Wer nichts zu verbergen habe, müsse sich nicht fürchten!‘ und ‚Mit ihrem Server ist auch die anonyme Verbreitung von Kinderpornographie möglich!‘. Die Verteidigung konterte: ‚Mit solchen Parolen könne auch das Post- oder Briefgeheimnis aufgehoben werden.‘. Am Ende siegte die

Unschuldsvermutung: Weil der Tor-Server Reppes nur der Anonymisierung und Verschlüsselung dient, nicht jedoch selbst Quelle von rechtswidrigen Aktivitäten war, musste das Gericht ihn freisprechen.

Fragen können gern an die eMail-Adresse tor@morphium.info gesendet werden und werden zeitnah beantwortet.“

Anonymisierungsdienste sollen verboten werden

…in der Slowakei. Aber wenn unsere Internet-Ausdrucker das jetzt lesen, weiß ich schon, was dann kommt. Aus der Tor-Mailingliste:

„In September, the Slovak Ministry of Transport, Post and Telecommunication prepared an amendment of the Electronic Communication Act. The Ministry of Internal Affairs integrated their suggestions, which include prohibition of anonymizing services.

An anonymizer is defined there as „A service that restrains or makes impossible tracking of Internet users“, which is a very vague term. It’s not obvious, exactly what technologies (HTTP proxy, VPN, Tor, SSH tunnelling?) will be treated as „anonymizers“.

Providing or even allowing such a service (within this could probably fall running a Tor relay) will be prosecuted. The fee can rise up to 33,000 Euros.

The reason for this is (no surprise here), that anonymizers are mostly used for spreading child pornography, for

extremists‘ communication and for financial frauds.

If this amendment gets approved in this or similar form, it will pose a serious threat to Tor and online anonymity in general.

I was unable to find any related text in english, so here is google translation of an article analyzing this amendment in slovak: translate.google.cz.“

Die Bücher der Anderen

Netzpolitik.org deckt Datenleck bei libri.de auf: „500.000 Rechnungen von Libri.de standen mehr oder weniger frei im Netz. “

Mir hat der Satz besonders gut gefallen: „Danach kontaktierten wir Libri.de, was erstmal nicht so einfach war. Auf der Webseite gibt es nur kostenpflichtige Kunden-Hotlines und eine externe PR-Agentur als Presseansprechpartner. Irgendwann klappte es über die Zentrale und der Hinweis, dass wir Zugriff auf ca. 500.000 Rechnungen haben, brachte uns schnell die Pressesprecherin ans Telefon.“

Ich würde denen noch die Kosten in Rechnung stellen, die beim Anruf der Hotline angefallen sind. Hotlines treiben mich in den Wahnsinn.

Dumm gelaufen: Kinderpornografie auf Manchesters Flughafen

Child porn fears scupper airport 'nude X-ray' scans

By JASON LEWIS
Last updated at 1:22 PM on 18th October 2009

Comments (325) | Add to My Stories

Airport security chiefs have been banned from subjecting children to a controversial new X-ray scanner that produces 'naked' pictures of passengers because of legal warnings the images may break child pornography laws.

Die britische Zeitung Daily Mail berichtet: Kinder dürfen von den neuen Nacktscannern auf Manchesters Flughafen nicht mehr erfasst werden:

„But now – with the system due to begin operating at full capacity at Manchester's Terminal 2 next week – security chiefs have been told no one under 18 can be subjected to the new checks. Child protection experts have warned that the image produced by the Rapiscan machines may break the law which prevents the creation of an indecent image or pseudo-image of a child."

Dann werden Familien mit Kindern vermutlich in Zukunft besonders verdächtig, weil die lieben Kleinen der Terroristen den Sprengstoff tragen werden. Die spinnen, die Überwachungs-Paranoiker…

By the way. Sehr schön die Kommentar-Funktion der Daily Mail. Lichtjahre von den Websites deutscher Holzmedien entfernt.

Davon können die noch viel lernen.

Google Censorship | Chilling Effects Clearinghouse

Gerade eine interessante Site gefunden, um die Zensur bei Google transparenter zu machen: Chilling Effects Clearinghouse – „A joint project of the Electronic Frontier Foundation and Harvard, Stanford, Berkeley, University of San Francisco, University of Maine, George Washington School of Law, and Santa Clara University School of Law clinics.“ Man gibt einen Suchbegriff ein und erhält jeweils die Ausgabe der deutschen und der englischen Google-Version. Probiert es mit „stormfront„.

Tja, auf so etwas kommen deutsche Universitäten natürlich nicht. Forschungsgelder beantragen, um die Internet-Zensur in Deutschland zu erforschen. Doch halt – es gibt Ausnahmen! Heise (und selbstredend kein anderes Medium) berichtet: „Überwachung im Visier von Wissenschaftlern“.

Jemand im (öffentlichen Teil des) Forum(s) der German Privacy Foundation möchte wissen, wo man die Listen indizierter Websites (zum Beispiel in Nordrhein-Westfalen) abrufen könne? Eine Recherche-Aufgabe für die geneigten Leserinnen und wohlwollenden Leser…

Wahlbetrüger

[via F!XMBR]

Romania rulez!

Heise: „Rumänisches Verfassungsgericht untersagt Vorratsdatenspeicherung“. „Das rumänische Verfassungsgericht hat damit einer Klage von Bürgern gegen den Telekommunikationsanbieter Orange entsprochen, es unter Berufung auf Artikel 28 der Verfassung zu unterlassen, Verbindungsdaten, E-Mails und SMS-Inhalte bereitzuhalten.“

Hurra! Ganz Europa soll ein Überwachungsstaat werden. Nur ein, nein zwei kleine osteuropäische Ländern leisten Widerstand. Hätten Sie’s gewusst? Man muss sich für deutsche Politiker wie Schäuble, Bosbach und Zensursula und andere mit Überwachungswahnvorstellungen schon im Ausland schämen…

Da kein deutsches Mainstream-Holzmedium in der Lage sein wird, auf die Original-Quelle zu verlinken: es ist die rumänische Nachrichtenagentur Mediafax (in englischer Sprache!).

BKA darf Sperr-Verträge nicht

umsetzen

Die bremer Firma Ready2host meldet auf ihrem Blog: „Am 10.07.2009 wurde vom Justiziar des BKAs zwar in einer eidesstaatliche Versicherung erklärt, dass bisher keine Sperrlisten herausgegeben wurden, doch stellt das Gericht hier fest: Es sei fraglich, wie weit ein Prozessreferat überhaupt "für das Handeln von Fachabteilungen verbindliche Erklärungen […] abgeben kann". Das Gericht stellt weiterhin fest, dass eine gesetzliche Grundlage für die Sperrverträge fehlt und verlangt vom BKA, die geschlossenen Verträge nicht durchzusetzen:" [mehr…]

Hintergrund ist ein zivilrechtolich gescheitertes Eilverfahren gegen Arcor wegen des BKA-Vertrags. Spiegel Online setzt übrigens sogar Links, erwähnt aber den Namen des Betreibers nicht. „Ein Blog-Betreiber" ist keine journalistische Quellenangabe. Vermutlich denken die: Wenn wir schon Links setzen müssen, damm verschweigen wir wenigstens den Namen des Blogs.

Zum Thema meldet Heise: „Brüssel signalisiert grünes Licht für Sperrgesetz".

Private Eyes für Blockwart-City

„Schöne neue Welt… bald auch für jeden, der sich privat etwas Geld hinzuverdienen will. So könnte man das Vorhaben der britischen Firma „Internet Eyes" umschreiben. Sie planen einen Online-Service, der die „Sicherheit durch Überwachung" erhöhen soll. Das Prinzip soll dabei folgendermaßen funktionieren:

Ladenbetreiber oder Privatleute mit Videokameras zahlen eine monatliche Gebühr von etwa 20 Pfund pro Monat an „Internet Eyes“. Dafür werden die Videokameras von diesen Leuten an einen Online-Service angeschlossen. Am anderen Ende der Leitung sitzen hunderte Freiwillige, welche die Bilder der Kameras beobachten. Sollten diese „kriminelles oder auffälliges Verhalten“ bemerken, melden sie dieses an die Besitzer der Kameras und erhalten dafür einen Bonus in Form von Punkten und Geld.“ [via gulli.com, Ravenhorst, futurezone.at]

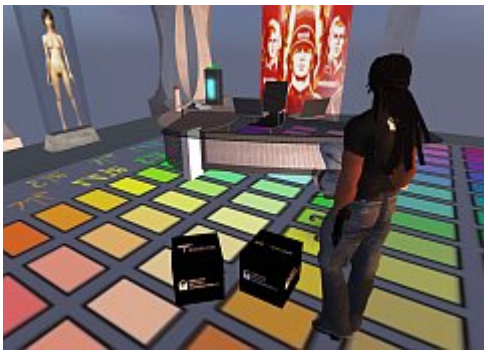
Ich wundere mich, dass das die Deutschen noch nicht erfunden haben. Wäre doch auch was für die Jugendschutzwarte… Überall nur negativ-dekadente Persönlichkeiten…

Eine Zensur findet statt

„Eine kleine Rundreise durch die Welt der Zensur – Wo, Was und Wie?“ auf datenspuren.de. „Die verwendeten Methoden sind vielfältig. Sie reichen von der Filterung unerwünschter Begriffe über die Blockierung bestimmter Webseiten bis hin zur gezielten Manipulation gesicherter Verbindungen („Man in the middle“) oder gar einer Komplettabschaltung des Internets.“

„Einen sehr schönen Überblick über (Netz-)Zensur weltweit hat Jens Kubieziel im Anon-Wiki zusammengestellt„. [via netzpolitik.org]

German Privacy Foundation 2.0



Mein Avatar (Name: Burkhard Schroeder) in Second Life läuft jetzt endlich mit einem T-Shirt der German Privacy Foundation herum. Die virtuelle Textilie gibt es in zwei Versionen: mit der Aufschrift gpg – encrypt und mit einer Überwachungskamera (Terror). Das Logo der GPF ist in Bauchhöhe und auf dem Rücken. Pro Exemplar 500 Lindendollar (Mitglieder der GPF natürlich gratis).

Chinesische Zensoren austricksen

Gulli.com meldet: „TOR-Netz gesperrt. Die chinesische Internet-Zensur ist offenbar weiter auf dem Vormarsch: Offenbar blockt man nun auch verstärkt das Anonymisierungs-Netzwerk TOR.“ Auch Jon Do ist von China aus nicht mehr so einfach zu erreichen.

Ich greife uns selbst mal vor: „Wir sind heute Nacht unsere Server durchgegangen, haben nachgezählt, welche IP-Adressen der GPF-Server bisher nicht im Torstatus erschienen sind, und haben auf diesen IPs Tor-Bridges eingerichtet. Wir haben 3 neue Tor-Bridges eingerichtet und insgesamt betreibt die GPF jetzt 4 Tor-Bridges. (Falls die GPF diese Zahlen für ihre Meinungsäußerung verwenden möchte.)“ Done.

Censorship by Obscurity [Update]

Heise meldet. „Umsetzungsvorgaben für Web-Sperren sollen geheim bleiben“. „Die Bundesnetzagentur hat in ihrem Amtsblatt über einen Entwurf für die technische Richtlinie zur Umsetzung des Gesetzes zur Bekämpfung der Kinderpornographie in Kommunikationsnetzen informiert, der von betroffenen Unternehmen beim Bundeskriminalamt (BKA) zur Kommentierung eingesehen werden kann.] Laut Amtsblatt 16/2009 wird die Richtlinie als nur für den Dienstgebrauch verwendbare

Geheimakte eingestuft“.

Alte Journalistenweisheit: einer quatscht immer. Ich will diese Listen haben! Bitte anonym über meine PrivacyBox!

In einer Mailingliste las ich: „Die Provider müssen nach bisherigen Stand namentlich Verantwortliche nennen, die persönlich in Wiesbaden vorstellig werden und dort das Schriftstück über die technische Richtlinie zur Umsetzung in Empfang zu nehmen. Für die Richtlinie besteht derzeit keine Rechtsgrundlage, das Gesetz ist noch nicht in Kraft. Das BKA agiert schon wieder außerhalb des rechtlichen Rahmens. Es besteht zusätzlich die Möglichkeit, dass die Geheimhaltung mit EU-Recht kollidiert. Solche inkompetenten Stümper wären in der freien Wirtschaft längst rausgeflogen…“

Wundert mich nicht. Wer ist noch mal Chef des BKA? Ach ja, Herr Jörg Ziercke. Das ist doch der mit den „vielfältigen Geschichten“ und der Online-Durchsuchung: „Sie können sich die abstrakten Möglichkeiten vorstellen, mit dem man über einen Trojaner, über eine Mail oder über eine Internetseite jemanden aufsucht. Wenn man ihnen erzählt hat, was für eine tolle Website das ist oder eine Seite mit ihren Familienangehörigen, die bei einem Unfall verletzt worden sind, sodass sie dann tatsächlich die Seite anklicken. Die Geschichten sind so vielfältig, dass es kaum jemanden gibt, der nicht auf irgendeine Form dieser Geschichte hereinfällt.“ Obscurity war schon immer Zierckes Spezialgebiet und Hobby.

Update; Heise: „Richtlinie zu Netzsperren keine Verschlusssache mehr“

Unzensierte DNS-Server [Update]

Im Zugangserschwerungsgesetz (Original als pdf) steht, wie die Zensur aussehen wird: „Für die Sperrung dürfen vollqualifizierte Domainnamen, Internetprotokoll-Adressen und Zieladressen von Telemedienangeboten verwendet werden. Die Sperrung erfolgt mindestens auf der Ebene der vollqualifizierten Domainnamen, deren Auflösung in die zugehörigen Internetprotokoll- Adressen unterbleibt.“

Die Germany Privacy Foundation hat eine vollqualifizierte ausführliche Anleitung für alle Betriebssysteme online gestellt, wie man diese Zensur „mindestens auf der Ebene der vollqualifizierten Domainnamen“ leicht umgehen kann. Im Forum steht noch mehr dazu.

Das gewünschte Ergebnis beim Testen des URLs welcome.gpf müsste lauten:
Gratulation
Sie nutzen einen der folgenden unzensierten DNS-Server:
GPF: 87.118.100.175
62.141.58.13
85.25.251.254
DNSBOX: 85.25.149.144
87.106.37.196

Facebook und ungesicherte

Rechner

Via YuccaTreePost: „Ein mutmaßlicher Einbrecher wurde in Martinsburg im US-Bundesstaat West Virginia verhaftet, nachdem er eine Frau um Schmuck im Wert von 3.500 US-Dollar erleichtert haben soll. Auf seine Spur brachte er die Ermittler selbst, weil er während des Einbruchs offenbar nichts Besseres zu tun hatte, als sich auf dem Rechner der Frau in seinen Facebook-Account einzuloggen.“ (Quelle: The Journal)

Kommentar eines Nutzers bei YuccatreePost (das hätte ich sonst geschrieben): „Hat er den Rechner mit Knoppix gebootet oder wieso konnte er den benutzen? Ach nee, dann wäre die Furzbook-Anmeldung nicht mehr nachvollziehbar gewesen. Kein Benutzeraccount mit Passwort? Micky$chrott-Deppen!“