Facebook-Verbot für Lehrer: Burks gefällt das

Aus dem Heise-Forum über die Frage, was Lehrer auf Facebook zu suchen haben: „So gut funktioniert die Privatsphären-Einstellung bei Facebook nicht, dass man einfach den Lehrer in seine Kreise nehmen kann, und dann trotzdem die Lästereien über die Schule unter den Schülern privat bleiben („Die Knüppelkuh ist eine total doofe Rektorin!“ Mathilda und 300 anderen gefällt das).“

Oder: „Hoheitliche Aufgaben des Staates, wie den Schulbetrieb, über einen US-amerikanischen Spionagekonzern abwickeln, der Persönlichkeitsprofile anfertigt und verkauft, und dabei fortwährend deutsches und europäisches Recht bricht. Geht gar nicht. Gehört definitiv verboten.“

NSAisten

Berlin (dpo) – Eine neue Sekte, deren Anhänger die allwissende und -mächtige Gottheit NSA verehren, erfährt deutschlandweit regen Zulauf. Die sogenannten NSAisten sind davon überzeugt, dass NSA nicht nur alles weiß, sondern über jeden ihrer Schritte aufmerksam wacht. Kanzleramtsminister Ronald Pofalla (CDU) sowie Innenminister Friedrich (CSU) nehmen in den Augen der Religionsgemeinschaft den Rang von Propheten ein. [mehr…]

Gehen Sie weiter, es gibt nichts zu sehen

Der US-amerikanische VPN-Anbieter Cryptoseal schließt, jedenfalls für Privatleute. Dazu ein schon etwas älteres Zitat Jürgen Schmidts (Heise Security):

Die wichtigste Lehre aus den Vorgängen beim E-Mail-Provider Lavabit ist, dass man der Verschlüsselung amerikanischer Dienst-Anbieter nicht mehr vertrauen kann. Das ist nun keine Vermutung übereifriger Verschwörungstheoretiker mehr, sondern ein von einem Gericht dokumentierter Fakt.

Der Titel bei Heise „Todesurteil für Verschlüsselung in den USA“ ist ein wenig irreführend: Phil Zimmermanns Firma sitzt ja auch in den USA.

Es wird Zeit, langsam Bilanz zu ziehen, was hierzulande als Konsequenz aus den Enthüllungen Snowdens geschehen ist: Nichts. Das Thema ist auch aus den Medien verschwunden.

Komplette Internetkommunikation speichern

Russischer Geheimdienst will komplette Internetkommunikation speichern.

Weitere Nachrichten: [Bitte länderspezifisch selbst ausfüllen] Geheimdienst will komplette Internetkommunikation speichern.

Lass Dich verzaubern

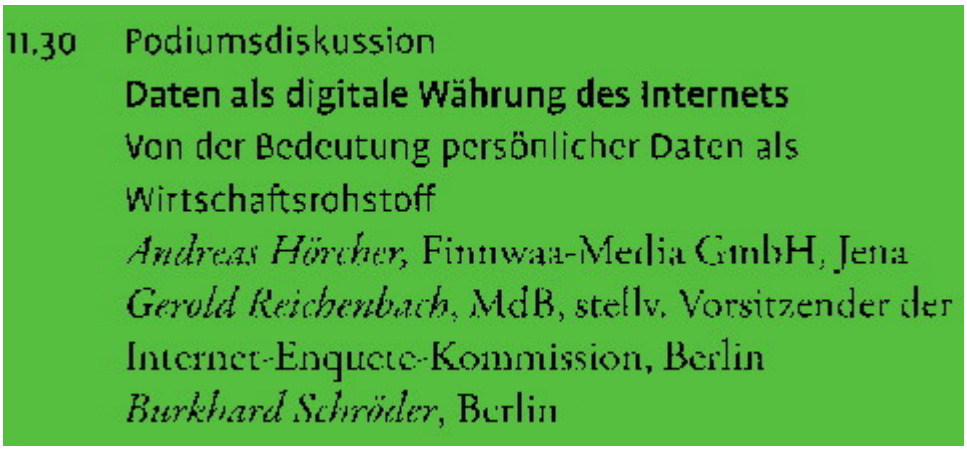
Lass Dich verzaubern zur selbst verschuldeten Unmündigkeit… Gesehen in den Neukölln Arcaden. Ich frage mich, ob die Datenschutzgesetze das eigentlich erlauben?

Humor für Geeks

Bruce Schneier Facts:
„Bruce Schneier doesn’t need to talk about security theater, he defines it.
Bruce Schneier accurately predicts the random.
Bruce Schneier doesn’t need to hide data with steganography – data hides from Bruce Schneier.
Bruce Schneier knows who the Anonymous Coward is.

Bruce Schneier can recite pi. Backwards.
Bruce Schneier can securely wipe any hard drive by shaking it like an etch-a-sketch.
When Bruce Schneier observes a quantum particle, it remains in the same state until he has finished observing it.
Bruce Schneier can write a recursive program that proves the Riemann Hypothesis. In Malbolge.
Bruce Schneier can read captchas.
Hashes collide because they’re swerving to avoid Bruce Schneier.
Bruce Schneier is the root of all certificates.
Bruce Schneier intercepts all your internal monologues by a man-in-the-middle attack.
For a woman to be impregnated by Bruce Schneier, she must decrypt his sperm with a 128-bit blowjob.
I once shook Bruce Schneier’s hand at a conference, and now my palm activates RFID card readers.“

Das Ende der Privatsphäre?



„Die digitale Revolution hat unsere Vorstellung von Privatheit und Öffentlichkeit grundlegend verändert. Dreißig Jahre nach Einführung des Grundrechts auf informationelle

Selbstbestimmung fragt die Tagung nach dem Umgang mit persönlichen Daten heute. Wo verlaufen heute die Grenzen zwischen Privatheit und Öffentlichkeit?“ (Freitag, 27.09.2013)

Newsletter German Privacy Fund Nr. 15

Der Newsletter German Privacy Fund (GPF) Ausgabe Nr. 15 vom 15.09.2013 ist jetzt online.

DJV Berlin verschlüsselt

Recherchegruppe: „Der DJV Berlin kann jetzt auch verschlüsselte Nachrichten empfangen – der öffentliche Schlüssel wurde gestern auf die Website gestellt. Der Berliner Journalistenverband zieht damit als erster bundesweit die Konsequenzen aus den Enthüllungen des US-amerikanischen Whistleblowers Edward Snowden.“ [mehr…]

Waffen, Drogen, Dissidenten

Motherboard: „Waffen, Drogen, Dissidenten – Eine Dokumentation über das Darknet“ (Video, leider mit nerviger Werbung vorab):

VICE Chefredakteur Tom Littlewood sucht nach diesen Überschneidungen und merkt, wie einfach und zuverlässig dieses System funktioniert, als er mit einem deutschen Waffenhändler über seinen Vertrieb im Darknet spricht. Außerdem diskutiert er mit mit dem Kryptospezialisten Karsten Nohl, mit Moritz Bartl, dem Gründer von Torservers.net und mit Ehsan Norouzi, einem iranischen Journalisten der Aktivisten dabei unterstützt sicher zu kommunizieren, über die positiven und negativen Aspekte eines Ortes, der durch seine Anonymität rechtsfrei geworden ist.

Open Letter From UK Security Researchers

Bristol Cryptography Blog: „Open Letter From UK Security Researchers“

However, the documents released show that NSA and GCHQ worked to weaken international cryptographic standards, and to place „backdoors“ into security products; such backdoors could of course be potentially exploited by others than the original creators. One of the prime missions of the security services is to protect citizens and corporations from Cyber Attack. By weakening cryptographic standards, in as yet undisclosed ways, and by inserting weaknesses into products which we all rely on to secure critical infrastructure, we believe that the agencies have been acting against the interests of the public that they are meant to serve. (…) We call on the relevant parties to reveal what systems have been weakened so that they can be repaired, and to create a proper system of oversight with well-defined public rules that clearly forbid weakening the security of civilian systems and infrastructures.“

Apples Erde ist eine Scheibe

Kai Biermann (Zeit online) und Udo Vetter (law blog) schreiben über Fingerabdruckscanner:
Apple verspricht, dass die Fingerabdrücke des Touch ID genannten Sensors das Telefon nicht verlassen. Sie würden nur lokal und nur verschlüsselt gespeichert und nie an Server von Apple übertragen oder in der Clouddatenbank hinterlegt.

Und die Erde ist eine Scheibe.

Vetter: Fingerabdruckdaten sind keine Kommunikationsdaten. „Auch so wird die Polizei das Fingerabdruck-Ident toll finden. (…) Es ist auf jeden Fall viel leichter, jemanden einen Fingerabdruck abzunötigen, als ihn zur Preisgabe seines Handypassworts oder des Entsperrmusters zu bewegen.“

Wer Wert auf Privatsphäre legt, nutzt kein soziales Netzwerk!

Noch Fragen?

Videoüberwachte Wahlkabinen

Tomás Marcelo Santillán (die Linke, Bergisch-Gladbach):
Da die Stadtverwaltung Bergisch Gladbach trotz einiger Beschwerden aus der Bevölkerung die Überwachungskameras in den Wahlräumen für die Briefwahl in Bensberg und in Stadtmitte nicht entfernen oder mindestens verhängen will, werde ich eine Wahlprüfungsbeschwerde erheben und eine Klage erwägen.

Ach ja? Jetzt werden schon Überwachungskameras in Wahlräumen installiert? Ein Schelm, wer Böses dabei denkt! Ich denke, dass man schon mit einer einstweiligen Verfügung die Dinger wegbekäme… Santillán schreibt:
Um die Integrität des Wahlvorgangs nicht zu stören reicht es nicht aus, zu erklären, dass die Kameras ausgeschaltet sind oder nichts aufzeichnen. Dieses ist für die Bürgerinnen und Bürger nicht transparent und nachvollzierbar, denn man kann nicht erkennen, was sich hinter der schwarzen Halbkugeln der Kameras tut. Die Wahlprüfungsbeschwerde wird sich nicht nur auf die Kameras direkt in den Wahlräumen beziehen, sondern auch auf die zahlreichen Kameras, die auf die Wählerinnen und Wähler an den Eingängen der Banken auf dem Weg zum Wahlraum lückenlos beobachten und dieses auch ständig Aufzeichnen und speichern.

Verschlüsselung ist sicher, kommt aber drauf an, welche

Technlogy-Review und Heise:
Kryptographie-Experten geben nun nach einer gründlichen Analyse der Dokumente Teilentwarnung: Die NSA habe wohl nicht

die mathematischen Verfahren ausgehebelt, auf denen der sichere Datenverkehr bei Online-Banking oder –Handel aufbaut. Vielmehr scheinen sich die Angriffe der NSA gegen die Implementierung von Kryptoverfahren in den gängigen Programmen sowie gegen deren Nutzer zu richten.

Quod erat demonstrandum.

Nie wieder in die USA

Wired: „The agents confiscated his laptop computer, a thumb drive and a digital camera. ICE held onto the equipment for 49 days – longer than the 30 days allowed in regulations – finally returning it only when the ACLU of Massachusetts intervened on his behalf with a letter.

Under the ‚border search exception, of United States criminal law, international travelers can be searched without a warrant as they enter the U.S..“

Ich frage mich, wie das die deutschen Korrespondenten machen, die in die USA reisen? Wiseo hört man nichts davon? Und wieso

haben die deutschen Medien über das Thema nicht berichtet? Werden die alle durchgelassen, weil deutsche Medien Interviews autorisieren lassen und deshalb pe default harmlos sind? Oder zeigen die alle bereitwillig Ihre Rechner vor mit den Worten „jawoll, geliebte Obrigkeit“ auf den Lippen?

Die *American Civil Liberties Union (ACLU)* von Massachusetts, von der *Wired* die Story wohl hat, berichtet über diese Fälle noch detaillierter:
The government searched House's electronics for 183 keywords, turning up more than 26,000 potentially responsive „files/objects.“ But even the government's own invasive analysis of House's information concluded that „no data was found that constituted evidence of a crime (and would justify ICE's seizure of the materials).“

Das Ministerium für Innere Sicherheit der Vereinigten Staaten (United States Department of Homeland Security) arbeitet also mit dem Justizministerium zusammen, beschlagnahmt Rechner politischer Aktivisten und sucht darauf. Nein, sie löschen sogar die Daten: „the government has agreed to destroy all data it obtained from his laptop and other electronics when he entered the U.S. after a vacation“.

Man kann also davon ausgehen, dass man bei der Einreise in die USA alle sichtbaren Truecrypt-Container auf seinen Rechnern löschen muss. Ich habe ja schon 1979 nur ein begrenztes Visum in die USA erhalten im Gegensatz zu allen anderen, die ich kannte, die schon mal dort waren. Die haben mich also schon seit den siebziger Jahre in der Kartei.

Das wird hier auch noch so kommen – die ~~Klassenkämpfe~~ sozialen Spannungen werden hier auch zunehmen. Ich werde das wohl noch erleben. Mein Rechner wurde illegal über zwei jahre lang konfisziert, und es hat auch kaum jemanden interessiert (außer Heise), obwohl das Gericht, das mich endlich freigesprochen hatte, sogar ausdrücklich „rechtsstaatswidrige Weise“ ins Urteil schrieb. Hier gibt es eben keine *ACLU*, auf die man in

einem solchen Fall bauen könnte.

Was sagen unsere Verschwörungstheoretiker von der „Online“-Durchsuchung eigentlich dazu? Warum machen die das in den USA so umständlich?

Annette Ramelsberger (Süddeutsche 2006): „Den meisten Computernutzern ist es nicht klar: Aber wenn sie im Internet surfen, können Verfassungsschützer oder Polizei online bei ihnen zu Hause auf die Festplatte zugreifen und nachschauen, ob sie strafbare Inhalte dort lagern – zum Beispiel Kinderpornographie oder auch Anleitungen zum Bombenbau.“

Warum also Rechner beschlagnahmen, wenn das (angeblich) auch so geht?

Intelligent Intelligence Design

Electronic Frontier Foundation (EFF) (via Fefe): Incredibly, intelligence officials said today that no one at the NSA fully understood how its own surveillance system worked at the time so they could not adequately explain it to the court.“

NSA Can Spy on Smart Phone

Data

Spiegel online (englische Ausgabe): „SPIEGEL has learned from internal NSA documents that the US intelligence agency has the capability of tapping user data from the iPhone, devices using Android as well as BlackBerry, a system previously believed to be highly secure.“

Ich habe gerade den Bericht im Print-Spiegel gelesen. Das war ja auch keine große Überraschung. Fefe schreibt: „Das ist eine hervorragende Nachricht. Denn es bestätigt, dass sie nicht die Kryptographie brechen können, sonst müssten sie nicht die Geräte infiltrieren.“

Aber so wird das wieder in den Medien nicht ankommen. In der Heute-Show vom 06.09. (sehenswert!) wird behauptet, die NSA könne E-Mail-Verschlüsselung und überhaupt alle Verschlüsselungen knacken. Neiiiiiin! Kann sie nicht!

Truecrypt

Fefe schreibt etwas Vernünftiges über Truecrypt.

Verschlüsselte E-Mails auslesen?

Tagesschau: „Die neuen Erkenntnisse zu den Anstrengungen von NSA und GCHQ bedeuten nicht zwangsläufig, dass die

Geheimdienste alle verschlüsselten Mails auslesen. Sie haben nach Ansicht von Experten dadurch in Verdachtsfällen die Möglichkeit jede E-Mail zu knacken – sollten die Angaben Snowdens der Wahrheit entsprechen.“ (Danke, Ruben: „Was berichten die Medien als Nächstes? Das Gerät NSA kann jetzt alles, auch Kaffee kochen?“)

Was ist denn das für ein Unsinn? Und welche „Experten“ wurden da gefragt?

Gestern zitierte ich Edward Snowden. u.a. laut Wired:
Properly implemented strong crypto systems are one of the few things that you can rely on," he said, though cautioning that the N.S.A. often bypasses the encryption altogether by targeting the computers at one end or the other and grabbing text before it is encrypted or after it is decrypted.

Heise übersetzt das so: „Verschlüsselung funktioniert. Sauber implementierte, starke Verschlüsselung ist eines der wenigen Dinge, auf die man sich noch verlassen kann.“ Die Betonung liegt auf „sauber implementiert“.

Wie ich immer in meinem Seminaren sage: Man kann sich das Niveau der Berichterstattung deutscher Medien über Sicherheitsthemen nicht unterirdisch genaug vorstellen.