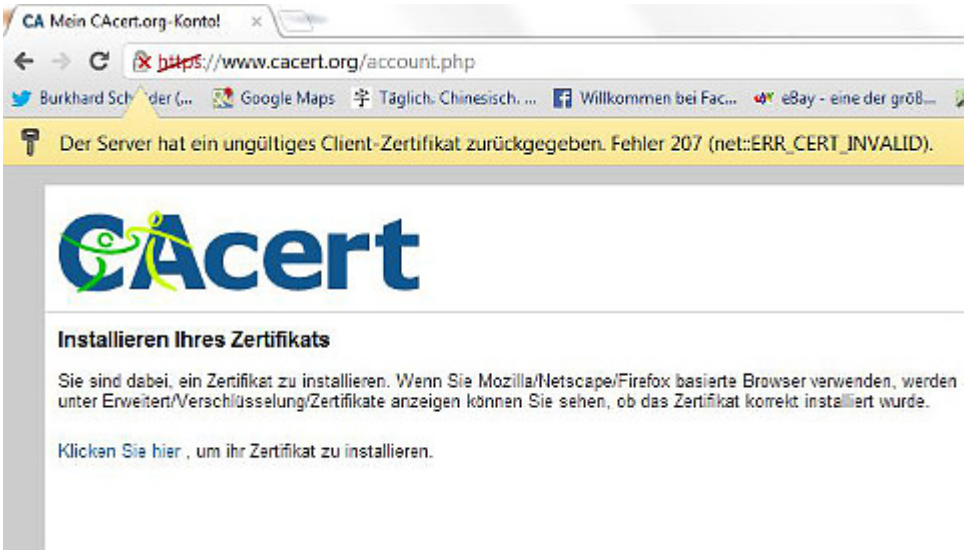
Verschlüsselt!



Heise: „Eine überwältigende Mehrheit von 91 Prozent lebt damit, dass ihre E-Mails nicht vertraulicher als Postkarten sind. (…) Für Verunsicherung gesorgt haben offenbar auch die Meldungen über das Knacken von Verschlüsselungsprotokollen durch Geheimdienste“.

Wenn die Medien so einen gequirlten Unsinn über das Thema schreiben, wundert mich das nicht. Was haben Verschlüsselungsprotokolle mit dem Verschlüsseln von E-Mails zu tun? Nichts, aber es wird gern alles durcheinandergewürfelt. Und das genau liegt auch im Interesse der Geheimdienste. Es war schon bei der so genannten „Online-Durchsuchung“ so: Der gemeine Nutzer sollte sich ohnmächtig fühlen und gar nichts tun.

Oder man bekommt es mit so Superoberexperten wie auf dem Screenshot zu tun. Das schreckt auch ab. Also jammert nicht, sondern schreibt *verständliche* Anleitungen.

GSM phreak und die Schnellmerker

Heise meldet ganz feierlich: „NSA kann auf breiter Front Handys abhören“ und beruft sich auf einen Artikel der Washington Post. Worum geht es?
The vulnerability outlined in the NSA document concerns encryption developed in the 1980s but still used widely by cellphones that rely on technology called second-generation (2G) GSM.

Ach? Da fällt mir doch etwas ein: „Ein Grossteil der weltweiten GSM-Netze kann nach dieser Entdeckung als unsicher gelten. Auch in GSM-Netzen ist es moeglich, auf Kosten fremder Kunden zu telefonieren.“, sagte CCC-Sprecher Frank Rieger.“

Das Zitat stammt aus dem Jahr 1998.

Warum die NSA-Affäre niemanden wirklich stört

Leitmedium.de (Caspar Clemens Mierau) über die Heuchelei deutscher Medien, die über Überwachung schreiben und gleichzeitig die LeserInnen exzessiv tracken und ausspionieren: „Süddeutsche (24 Tracker), Spiegel Online (18 Tracker), ZEIT Online (14 Tracker), Welt (24 Tracker), BILD Online (24 Tracker) – es ist überall die gleiche Situation.“

Vorratsdatenspeicherung verstösst gegen die Grundrechtecharta der EU

Spiegel online: „Die umstrittene Vorratsdatenspeicherung verstößt nach Ansicht eines Gutachters am Europäischen Gerichtshof (EuGH) gegen die Grundrechtecharta der EU. Das geht aus einem am Donnerstag in Luxemburg veröffentlichten Rechtsgutachten von Generalanwalt Pedro Cruz Villalón hervor.“

Skandal, Skandal, Skandal!

„NSA späht Internetnutzer mit Google-Cookies aus“. Weitere Meldungen: „Skandal: Facebook späht Internetnutzer mit Google-Cookies aus.“ – „Skandal: Google späht Internetnutzer mit Google-Cookies aus.“ – Skandal: RenRen späht Internetnutzer mit Facebook-Cookies aus.“ – Skandal: [Bitte selbst ausfüllen] späht Internetnutzer mit [bitte selbst ausfüllen]-Cookies aus.“

Die Wahrung

Ab und zu gibt es auch gute Nachrichten: „Erklärung der Rechtsanwaltskammer Berlin, des Berliner Anwaltsvereins und der Steuerberaterkammer Berlin vom 02.12.2013″:

Als Berliner berufsständige Selbstverwaltungsorganisationen

und Interessenvertretungen der Rechtsanwältinnen und Rechtsanwälte, Steuerberaterinnen und Steuerberater fordern wir von der Bundesregierung sowie von allen politisch tätigen Kräften: (…)
Die Vertraulichkeit der elektronischen Kommunikation im Rechtsverkehr durch eine Ende-zu-Ende-Verschlüsselung zu gewährleisten und unsichere, weil potenziell beobachtbare und sogar veränderbare Kommunikationsverfahren (z.B. De-Mail) zu verhindern.

Geht doch. Die wissen, wovon sie reden.

Die schlechte Nachricht: Ohne Deutsch des Grauens kommen Anwälte nicht aus. „Die Wahrung und der Schutz des Berufsgeheimnisses“. Grusel.

Die Wahrung. Was soll denn das heißen? Ich denke gleich an „die Falschung“. Ist das ein deutsches Wort?

Die Wahrung der Hitze meiner Pizza in der Mikrowelle (die ich gar nicht besitze)? Die Wahrung der Integrität und Sicherheit des skelettösen Systems meines Körpers beim Kampfsport? Die Wahrung der Standhaftigkeit bestimmter männlicher Körperteile bei mechanischen Bewegungen, die der Fortpflanzung der Art dienen oder der Simulation derselben?

Zyniker und Rechtspopulist Gabriel

Gabriel macht klar, warum die SPD für die Vorratsdatenspeicherung ist: Ohne die hätte man Breivik in Norwegen nicht gefasst. „Wir können ja nicht unsere Position

verleugnen.“

Die Wahrheit ist: „Nachdem Polizisten einer Anti-Terror-Einheit auf die Insel gelangt waren, ließ sich Breivik gegen 18:35 Uhr widerstandslos von ihnen festnehmen.“

Bei Wikipedia lesen wir: *Im Zuge der Anschläge in Norwegen 2011 forderten die CSU-Politiker Hans-Peter Uhl und Beate Merk erneut die Einführung der Vorratsdatenspeicherung, um besser gegen derartige Terrorakte gewappnet zu sein. Uhl sprach sich in diesem Kontext überdies für eine anlasslose Vorratsdatenspeicherung aus, die über die ursprünglichen Pläne hinausginge. Diese Forderungen wurde von Seiten der SPD, der Grünen, der FDP sowie der Linkspartei scharf kritisiert. So sei es „geradezu zynisch“ und „populistisch“, die Anschläge für die „innenpolitische Agenda“ der Union zu benutzen, außerdem habe die Vorratsdatenspeicherung in Norwegen die Anschläge nicht verhindern können.“*

Wie moralisch verkommen oder wie dämlich muss man eigentlich sein, um SPD zu wählen oder so ein Lügenmaul als Parteivositzenden zu akzeptieren wie die SPD-„Netzpolitiker“? Aber natürlich wird die Basis trotzdem die Koalition absegnen.

Ich bin dieses Duckmäusertum sowas von leid

Gregor Gysi (Die Linke) im Bundestag am 18.11.2013 über Deutschlands Nicht-Souveränität und den NSA-Skandal. Ansehen!

Als Kontrastprogramm dazu das so genannte Nachrichtenmagazin Focus: „Wie FOCUS aus Berliner Sicherheitskreisen erfuhr, können Staatsfeinde und Schwerverbrecher derzeit nur

unzureichend überwacht werden. Gründe seien Personalmangel und fehlende technische Möglichkeiten.“

Verschlüsselung verboten

„Die IT-Abteilung hat das Verschlüsseln von E-Mails verboten“, schreibt Spon über die „gehackten“ E-Mail-Konten von EU-Abgeordneten. Die französische Quelle, von der die deutsche Medien ihre Informationen abschreiben, formuliert das noch schöner:
„A hacker using elementary computer equipment and what he described as “a few bits of knowledge that everyone is capable of finding on the internet” has succeeded in accessing confidential emails and personal files of Members of the European Parliament, their assistants and even the institution’s IT experts, Mediapart can reveal. The operation was, he said, mounted as a demonstration of the vulnerability of security at both the parliament in Strasbourg and also among many national administrations which use software, notably that of Microsoft, that experts have for years warned is exposed to espionage manipulations through fundamental.

So etwas kann man sich gar nicht ausdenken. Vermutlich werden sie jetzt De-Mail kopieren und die „verschlüsselten“ E-Mails vor dem Absenden auf einem vertrauenswürdigen ~~NSA-~~Server öffnen, um sie „nach Viren“ zu durchsuchen.

Quantum Insert und Burks‘ Law

Nachtrag zu gestern. Heise schreibt: Wie die „Quantum Insert“ getaufte Methode genau funktioniert, beschreibt das Magazin nicht. (Gemeint ist der *Spiegel*). Falsch. Die „beschreiben“ sehr wohl, wie ein Angriff per „gefälschter Website“ angeblich funktioniert.

Der *Spiegel* beruft sich auf einen Artikel Bruce Schneiers im *Guardian*. Schneier:
To trick targets into visiting a FoxAcid server, the NSA relies on its secret partnerships with US telecoms companies. As part of the Turmoil system, the NSA places secret servers, codenamed Quantum, at key places on the Internet backbone. This placement ensures that they can react faster than other websites can. By exploiting that speed difference, these servers can impersonate a visited website to the target before the legitimate website can respond, thereby tricking the target’s browser to visit a Foxacid server. In the academic literature, these are called „man-in-the-middle“ attacks, and have been known to the commercial and academic security communities. More specifically, they are examples of „man-on-the-side“ attacks.

Zum einen geht es um Man-in-the-Middle-Angriffe auf Smartphones via GRX-Router einiger Mobilfunk-Netzbetreiber, was an sich keine große Kunst ist. Jedes Handy ist ein Überwachungwerkzeug. So what?

Zum anderen listet das Magazin (Printausgabe) einen Fall auf, wie ein „Computerfachmann“, der in einer indischen Firma arbeitet, ausgespäht wurde. Die Angreifer „brachten in Erfahrung, mit welcher IP-Adresse er dienstlich im Netz surft und mit weldher privat, einer indischen nämlich.“ Der benutzte auch Skype und sogenannte „soziale“ Netzwerke und natürlich einen Gmail-Account. Das muss ein merkwürdiger „Computerfachmann“ sein. Dem jubelten sie gefakte Linkedin-

Versionen unter. Vermutlich haben sie ihn auch noch aufgefordert, Javascript einzuschalten, was der natürlich brav getan hat (sonst hätten sie ihm nichts unterjubeln können.)

Ich verkneife mir, ein „Burks‘ Law“ zu formulieren: „Wer Skype, Gmail und so genannte ’soziale Netzwerke‘ benutzt, hat auch immer Javascript eingeschaltet und lässt sich auch gern ausspionieren.“

Bitte eure Passwörter!

Die FAZ berichtet (via Fefe): „Eine weitere mit der Angelegenheit vertraute Person sagte, Snowden habe insgesamt 20 bis 25 Kollegen mit der Begründung zur Herausgabe ihrer Passwörter gebracht, er benötige sie für seine Tätigkeit als System-Administrator.“

Muahahahaha. Das erinnerte mich an einen heutigen Tweet von Stefan Graunke: „Ich bin von Twitter als Administrator eingesetzt worden, bräuchte dazu jetzt aber von euch allen mal euer Accountpasswort.“

Ist der Wille erst da

Soeben bekam ich eine verschlüsselte (!) E-Mail:

Sehr geehrte Herren Schröder, Ude, Frau Arslan,
ich habe in den Nachdenkseiten Ihre Anleitung zur Verschlüsselung gefunden und gestern haben wir diesen Weg beschritten und wie Sie heute sehen funktioniert es wunderbar.

Ich bin absoluter Anfänger und benötige Überwindung was das Netz angeht. (…) Ich betreibe eine Praxis für Naturheilkunde und bin Heilpraktikerin. (…)

Löblich! Geht doch!

CDU/CSU/NSA [Update}

Heise: „CDU und CSU wollen Internet im NSA-Stil überwachen“.

Das kommt jetzt nicht wirklich überraschend. Heuchlerische Bande, allesamt.. Und die SPD wird sowieso alles abnicken.

[Update] Angeblich war es ein Missverständnis und ein kleiner Referent ist (natürlich) schuld. Muahahahaha.

„So fühlt man Absicht, und man ist verstimmt.“ (Johann Wolfgang von Goethe: Torquato Tasso)

Nationale imperialistische Interessen

„Gehen Sie davon aus, dass das geschieht. Die Überwachung von internationalen Kommunikationsverbindungen ist gängige Praxis der NSA und eine Doktrin zur Unterstützung nationaler amerikanischer Interessen.“ (Thomas Drake, ehemaliger US-Agent, laut Profil)

Vorratsdatenspeicherung, reloaded

Ich fühle mich wieder „ausreichend“ durch die hart recherchierenden deutschen Medien informiert. Heise: „Union und SPD wollen Vorratsdatenspeicherung wiederbeleben“. Sueddeutsche.de: „SPD und Union uneinig über Vorratsdatenspeicherung“. FAZ: „Union und SPD wollen Vorratsdatenspeicherung“.

Burks‘ Prognose: CDU/CSU und SPD werden die Vorratsdatenspeicherung beschließen.

Wer hat uns verraten? Niemand, denn es war schon vorher klar. dass auch die SPD die Vorratsdatenspeicherung wollte. Wollte sie schon immer.

Truecrypt ist sicher, revisited

Heise Security: „Ein gut dokumentierter Versuch, die vom TrueCrypt-Projekt angebotenen Binärdateien für Windows aus dem öffentlichen Quellcode nachzubauen, zeigt: die Binaries stimmen mit den Quellen überein.“

Das Ministerium für Wahrheit informiert über Tabuwörter

Fefe: „Der Axel-Springer-Verlag geht eine exklusive (vertragliche?) Bindung mit der Bundesregierung ein und wird vom Bundesinnenministerium dafür bezahlt, den E-Perso in Bild, Welt & Co. als ‚Volksausweis' zu propagandieren. Regelmäßig". Das bezieht sich auf „Das Marketing des E-Persos„.

Das Ministerium für Wahrheit, auch bekannt als „Bundesinnenministerium", hatte den elektronischen Ausweis schon einmal umbenannt und dazu eine Sprachregelung erlassen: *in dem dann noch angehängten auszug aus einer präsentation von "servicplan public opintion" werden folgende Tabuwörter aufgeführt: biometrie, chip, daten auslesen, daten auswerten, daten sammeln, datenspeicherung, datenkontrolle, elektronisch, elektronischer ausweis, e-government, gläserner bürger. diese „tabuwörter" sollen niemals ohne „inhaltlichen zusammenhang" verwendet werden.*

Schon klar.

We shall overcome

„Wenn die einfachen Leute auf dieser Welt nicht aufstehen und für ihre Interessen kämpfen, werden die Reichen und Mächtigen gewinnen. Es ist schon immer so gewesen und die Geschichte der Menschheit lehrt uns, dass dies so weitergeht. Der Informationskrieg muss im Informationszeitalter von jedem einzelnen Menschen geführt werden, sonst wird er, sonst wird seine Art zu leben, schnell verschwunden sein. Es ist der Kampf ums Überleben in dieser Welt, einer gegen den anderen. Es ist der ultimative Weltkrieg gegen die Mächtigen und jede Person auf dieser Welt ist als Einzelner an diesem Krieg beteiligt oder in einer Allianz mit allen anderen einfachen Leuten. Wer wird den Frieden gewinnen? Wir werden das. Sie und ich.“ (Fred Cohen, via Hal Faber)

Weniger Sicherheit, bitte!

Chip nicht mehr krypto? [Update]

Spiegel online (18.11.2009): „Neuer Krypto-Chip fürs Kanzler-Handy: Merkel wird abhörsicher.“

Spiegel online (24.10.2013: „Mögliche Überwachung von Kanzler-Handy (…) Nach einer Überprüfung durch den Bundesnachrichtendienst und das Bundesamt für Sicherheit in der Informationstechnik hielt die Regierung den Verdacht offenbar für ausreichend plausibel, um die US-Regierung damit zu konfrontieren.“

Ach? Wie wäre es, die Fakten ein bisschen zu recherchieren, liebe Medien? Was genau und wie wird von wem abgehört? Ist der „Krypto-Chip“ in Merkels Handy nicht mehr „krypto“? Es kann doch nicht sein, dass sich niemand, niemand, niemand für die wesentliche Frage zum Thema interessiert (außer mir)?

Update: Es war nicht das Krypto-Handy, sonder das Partei-Handy, schreibt die FAZ.