Grossangriff auf Verschlüsselung

Well, when the president does it, that means it is not illegal. (Richard Nixon)

Heise: „Laut Guardian verlangten Vertreter der Geheimdienste von der britischen Zeitung und ihren Partnern New York Times und ProPublica, die Enthüllungs-Artikel über die Angriffe von NSA und GCHQ auf Verschlüsslung im Internet zu unterlassen. Begründung: Zielpersonen im Ausland könnten durch die Veröffentlichung veranlasst werden, zu neuen Formen der Verschlüsselung oder der Kommunikation im Allgemeinen zu wechseln, die schwerer zu sammeln und zu entschlüsseln wären. Guardian, New York Times und ProPublica lehnten das Ansinnen zwar ab. Sie entschieden sich aber, bestimmte detaillierte Informationen aus den Artikeln zu entfernen."

Was für Weicheier! Ich bin mal gespannt, ob deutsche Medien, die eventuell mit dem *Guardian* in der causa Snowden kooperiert haben, sich ähnlich feige verhalten. Aber vermutlich werden sie auf Grund ihrer obrigkeitshörigen Attitude (Interviews werden autorisiert, E-Mail-Verschlüsselung ist weitgehend unbekannt) erst gar nicht berücksichtigt.

Man muss bei dem Begriff „Verschlüsselung" auch genauer hinschauen. Ist SSL gemeint? [Wikipedia über SSL] Oder geht es um public-key-Verfahren, also zum Beispiel um OpenPGP? Letzteres hat Snowden selbst benutzt und empfohlen, man kann also eine Hintertür ausschließen (nicht aber im Betriebssystem, mit dem man das nutzt).

Der Guardian schreibt:
A 10-year NSA program against encryption technologies made a breakthrough in 2010 which made „vast amounts" of data collected through internet cable taps newly „exploitable".

Leider werden wir im Unklaren darüber gelassen, was genau damit gemeint ist. Die New York Times ist ähnlich vage:
Beginning in 2000, as encryption tools were gradually blanketing the Web, the N.S.A. invested billions of dollars in a clandestine campaign to preserve its ability to eavesdrop. Having lost a public battle in the 1990s to insert its own „back door" in all encryption, it set out to accomplish the same goal by stealth.

Immerhin. Wenn man den Artikel in der *New York Times* aufmerksam liest, erkennt man auch viel Wünschen und Wollen wie das Agitprop hiesiger interessierter „Kreise": „The N.S.A. hacked into target computers to snare messages before they were encrypted." Da haben wir fast wortwörtlich, was auch hier zum Thema „Online-Durchsuchung" herausposaunt wurde. Ich würde schon gern mehr und Genaueres wissen, wie sie das angestellt haben wollen. Die Wired hat darüber vor sieben Jahren geschrieben: „FBI Spyware: How Does the CIPAV Work?" Man sollte auch noch einen zehn Jahre alten Artikel über den so genannten „Clipper Chip" erwähnen.

Some of the agency's most intensive efforts have focused on the encryption in universal use in the United States, including Secure Sockets Layer, or SSL; virtual private networks, or VPNs; and the protection used on fourth-generation, or 4G, smartphones.

Damit kommen wir der Sache schon näher.

For at least three years, one document says, GCHQ, almost certainly in collaboration with the N.S.A., has been looking for ways into protected traffic of popular Internet companies: Google, Yahoo, Facebook and Microsoft's Hotmail.

Ich denke, dass die Metadaten, die Google et al erheben, viel mehr aussagen als wenn man die angeblichen „Sicherheits"-Features dieser Firmen knackt. Wer seine E-Mails verschlüsselt, kann auch weiter über Google-Mail vertrauliche

kommunzieren, aber nur was die Inhalte angeht. Wer mit wem kommuniziert, wird and die Geheimdienste weitergereicht.

Bevor alle in Panik ausbrechen, bringt die *New York Times* noch ein Original-Zitat Snowdens:
„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".

Quod erat demonstrandum. Sichere Verschlüsselung auf einem unsicheren System bedeutet, das Schloss vor die Tür zu nageln.
At Microsoft, as The Guardian has reported, the N.S.A. worked with company officials to get pre-encryption access to Microsoft's most popular services, including Outlook e-mail, Skype Internet phone calls and chats, and SkyDrive, the company's cloud storage service.

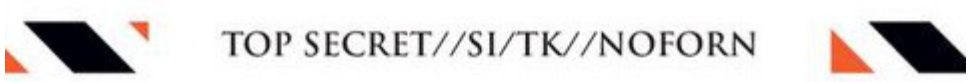
Man sieht aber auch, dass es neben der Totalüberwachung der Bevölkerung um Industriespionage geht:
By this year, the Sigint Enabling Project had found ways inside some of the encryption chips that scramble information for businesses and governments…

Bruce Schneier gibt folgenden Rat:
– Be suspicious of commercial encryption software, especially from large vendors.
– Try to use public-domain encryption that has to be compatible with other implementations.

Surveillance Industry Documents

Wikileaks: „Today, Wednesday 4 September 2013 at 1600 UTC, WikiLeaks released ‚Spy Files #3' – 249 documents from 92 global intelligence contractors. These documents reveal how, as the intelligence world has privatised, US, EU and developing world intelligence agencies have rushed into spending millions on next-generation mass surveillance technology to target communities, groups and whole populations."

Special Intelligence and Talent-Keyhole Information



Washington Post: „Inside the 2013 U.S. intelligence ‚black budget'" (das hatten wir hier schon im Zusammenhang mit Comical Hans-Peter).

Verrat unter Freunden

Ein wohlwollender Leser wies mich darauf hin, dass die ZEIT einen Artikel (1999, Nr. 40) aus ihrem Online-Archiv und von ihrer Website entfernt hat. Er heißt „Verrat unter Freunden – Wie die NSA, Amerikas größter und verschwiegenster Geheimdienst, deutsche Firmen ausspioniert und dabei einen Milliardenschaden anrichtet“.

Der Artikel ist noch im Usenet (cl.nordamerika.allgemein) einsehbar.

Ein Schelm, wer Böses dabei denkt.

Früher auch schon

Hintertür für Spione

Die US-Geheimdienste wollen sich Zugang zu verschlüsselten Daten verschaffen - weltweit VON CHRISTIANE SCHULZKI-HADDOUTI

31. Dezember 1899 01:00 Uhr

Wir verschlüsseln alle Daten

Wie soll ich einen Artikel über ein Thema schreiben, wenn die andere Seite nicht versteht, was ich meine? Ich hatte die Pressestelle der „Grünen“ gefragt: „Warum gibt es keinen öffentlichen OpenPGP-Schlüssel zur Kontaktaufnahme?“

Die Anwort kam: „Wir verschlüsseln alle Daten mit SSL.“

Deutsche Daten und Server in Deutschland sind sicher…

„Gemäß § 110 TKG hat der Betreiber einer Telekommunikationsanlage, mit der Telekommunikationsdienste für die Öffentlichkeit erbracht werden, unter anderem ab dem Zeitpunkt der Betriebsaufnahme auf eigene Kosten technische Einrichtungen zur Umsetzung gesetzlich vorgesehener Maßnahmen zur Überwachung der Telekommunikation vorzuhalten und organisatorische Vorkehrungen für die unverzügliche Umsetzung zu treffen.“

Pofalla beendet nicht

„Unsere Regierungen haben kein interesse daran, ihre Bürger zu informieren, wenn es um Überwachung geht. Die Regierungen der Vereinigten Staaten, Großbritanniens, Deutschlands und anderer Länder wollen vielmehr, dass diese Debatte zu Ende geht. Aber

das tut sie nicht.“ (Laura Poitras)

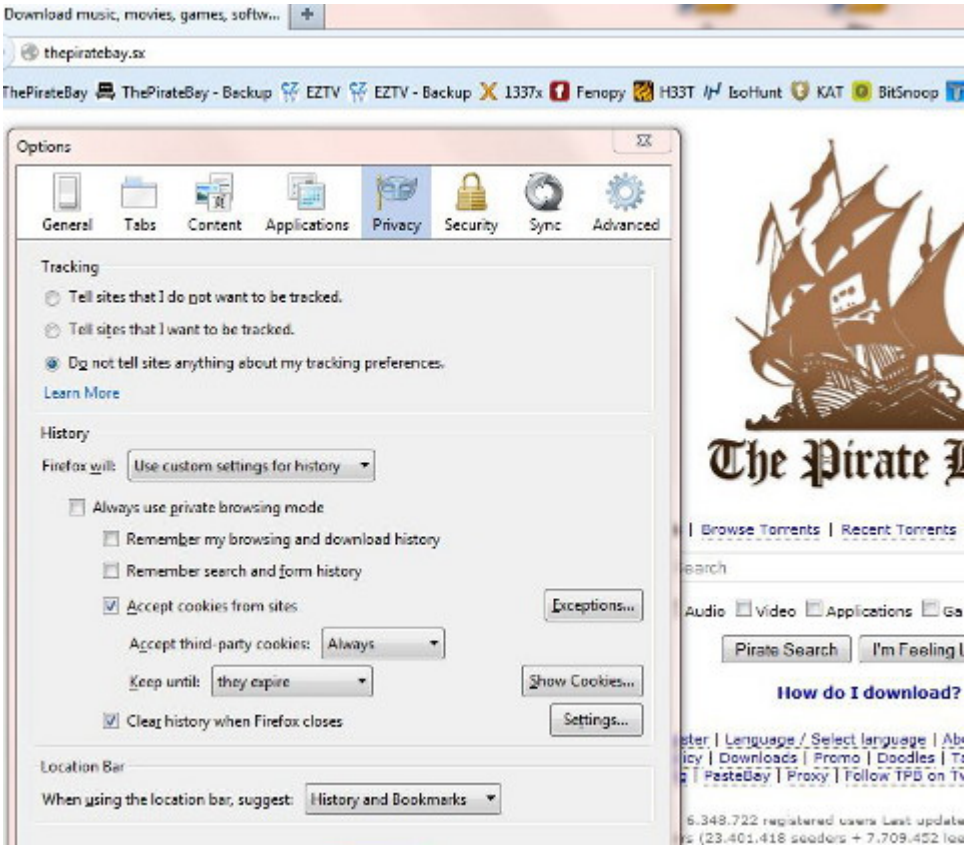
Die Kronjuwelen der NSA

The Guardian: „NSA paid millions to cover Prism compliance costs for tech companies“.

The technology companies, which the NSA says includes Google, Yahoo, Microsoft and Facebook, incurred the costs to meet new certification demands in the wake of the ruling from the Foreign Intelligence Surveillance (Fisa) court.

Noch ein Grund, wieder auf Linux umzusteigen. Eigentlich müsste das Bundesverfassungsgericht der deutschen Regierung verbieten, Microsoft-Produkte anzuschaffen und zu benutzen.

Pirate Bay launches own PirateBrowser



Man kann auch das Rad neu erfinden und sich deswegen feiern lassen. In einigen Medien wie der [taz] und dem [Guardian] erfahren wir etwas aus der Public-Relations-Abteilung von *Pirate Bay* „to evade ISP filesharing blocks“.

Zu meiner Überraschung hat die *taz* richtig kritisch gefragt und auch eine ander Meinungen dokumentiert, die diesen Browser als einen schlecht gemachten Werbegag ansieht – was sich bei einem Blick auf die Voreinstellungen bestätigt. „Cookies per default“ erlaubt – damit fängt es schon an.

PirateBrowser is a bundle package of the Tor client (Vidalia), FireFox Portable browser (with foxyproxy addon) and some custom configs that allows you to circumvent censorship that certain countries such as Iran, North Korea, United Kingdom, The Netherlands, Belgium, Finland, Denmark, Italy and Ireland impose onto their citizens.

Das gibt es doch schon alles. Warum muss Pirate Bay jetzt noch einmal einen eigenen Browser „erfinden“?

Der *Guardian* schreibt:
Users are warned that despite its use of Tor, the browser does not guarantee their ability to surf the web anonymously, with the recommendation that they continue to use a virtual private network (VPN) service „if you are looking for something more secure.

Wer mit Tor surft, ist nicht anonym? Das ist doch wieder ein Schmarrn. Und Tor zusammen mit VPN ist nur dann kein weißer Schimmmel, wenn alle Tor-Server vom jeweiligen Provider geblockt würden. Man kann natürlich auch mit dem Tor Browser Bundle alle aktiven Inhalte erlauben und so das Schloss vor die Tür nageln.

Der PirateBrowser ist meines Erachtens ein alter Hut.

Verzicht auf Privatsphäre

Heise: „Wer ein E-Mail an einen Gmail-Nutzer schickt, verzichtet auf Privatsphäre. Diesen Standpunkt vertritt Gmail-Betreiber Google offiziell in einer Eingabe bei Gericht. Anlass für das Verfahren ist, dass Google E-Mails scannt und ihre Inhalte auswertet.“

Richtig wäre: Wer eine unverschlüsselte E-Mail verschickt, nicht nur an Gmail-Nutzer, verzichtet auf Privatsphäre.

PRISM und Co.: Was bisher geschah

Heise fasst die bisherigen Berichte zusammen: „NSA-Überwachungsskandal: Von PRISM, Tempora, XKeyScore und dem Supergrundrecht – was bisher geschah“.

Unverzeihlicher Leichtsinn und die Furcht, nicht patriotisch genug zu sein

Edward Snowden in einem Interview mit der New York Times (via Fefe) auf die Frage, warum er denn mit seinem Material nicht zu ihnen gekommen sei:

After 9/11, many of the most important news outlets in America abdicated their role as a check to power – the journalistic responsibility to challenge the excesses of government – for fear of being seen as unpatriotic and punished in the market during a period of heightened nationalism. From a business perspective, this was the obvious strategy, but what benefited the institutions ended up costing the public dearly. The major outlets are still only beginning to recover from this cold period.

Schön ist auch das hier:
I was surprised to realize that there were people in news organizations who didn’t recognize any unencrypted message sent over the Internet is being delivered to every intelligence service in the world. In the wake of this year’s

disclosures, it should be clear that unencrypted journalist-source communication is unforgivably reckless.

Spionageziel Deutschland

„…dabei werde die Weitergabe der Daten an die Bedingung geknüpft, dass auf ihrer Grundlage nicht gefoltert werde oder eine Verurteilung zum Tode erfolge.“ (Quelle)

Seminare

Seminarreihe: „Sicher im Internet – Kommunikation, Recherche und Verschlüsselung“ beim DJV Berlin
Termine:
03. September 2013 – 19.00 Uhr
10. September 2013 – 19.00 Uhr
17. September 2013 – 19.00 Uhr
24. September 2013 – 19.00 Uhr
01. Oktober 2013 – 19.00 Uhr
08. Oktober 2013 – 19.00 Uhr
15. Oktober 2013 – 19.00 Uhr
22. Oktober 2013 – 19.00 Uhr

Investigative Recherche im Internet an der Berliner Journalisten-Schule
Termine:
16. / 17. August 2013, jeweils 9.00 bis 17.00 Uhr
09. / 10. Dezember 2013, jeweils 9.00 bis 17.00 Uhr

Sicherheit im Internet – Crashkurs“
Termine:
02. September 2013, 9.00 bis 17.00 Uhr
20. Dezember 2013, 9.00 bis 17.00 Uhr

Alle Seminare sind auch für Nicht-Journalisten offen.

SSL ist nicht OpenPGP

Netzpolitik.org: „E-Mail made in Germany: Deutsche Telekom, WEB.DE und GMX machen SSL an und verkaufen das als ’sicher'“.

Die Initiative kann als reine Marketing-Aktion abgetan werden, wirkliche Sicherheit wird nicht gewährleistet.

So ist es.

Checkliste Sicherheit

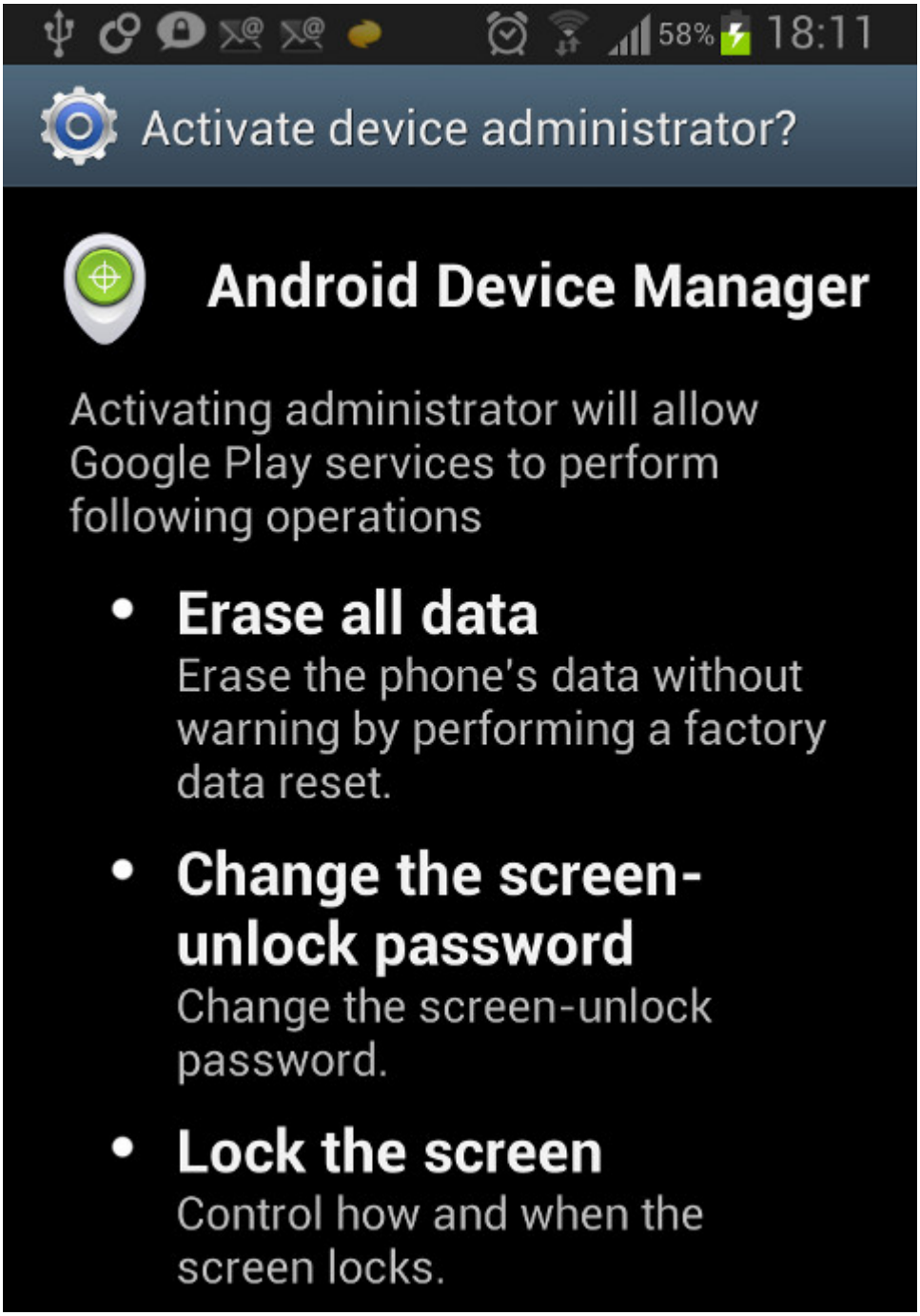
Zur gefälligen Beachtung: Ich arbeite gerade an einer volkstümlichen Checkliste Sicherheit, die durch Links und Tutorials komplettiert werden soll. Wer Vorschläge hat: nur zu!

Companies with physical ties to the United States [Update]

Ladar Levison von Lavabit (via Fefe): „I would _strongly_ recommend against anyone trusting their private data to a company with physical ties to the United States.“

[Update] Jetzt steht es auch bei Spiegel online.

Erase all Data



Da sitze ich ahnungslos mit meinem Laptop und dem Android-Smartphone in einem Café und lese bei Heise etwas über den ~~NSA~~Google-Ortungsdienst: „Will man im Notfall das Gerät aus der Ferne löschen können, setzt man zuvor unter Einstellungen/Sicherheit/Geräteadministratoren das Häkchen beim Gerätemanager.“

Ach?! Das also soll ich aktivieren? Geht’s noch?

Dissent in Numbers: Making Strong Anonymity Scale

David Isaac Wolinsky, Henry Corrigan-Gibbs, and Bryan Ford (Yale University 2012): „Dissent in Numbers: Making Strong Anonymity Scale“ – ein Text über die Zukunft von und die Alternativen zu Tor.

This paper has made the case that by delegating collective trust to a decentralized group of servers, strong anonymity techniques offering traffic analysis resistance may be adapted and scaled to offer anonymity in groups of thousands of nodes, two orders of magnitude larger than previous systems offering strong anonymity. Through its novel client/server DC-nets model, Dissent is able to accommodate anonymity set sizes of up to 5,000 members, while maintaining end-to-end latency low enough to enable wide-area interactive messaging. In local-area settings, Dissent is fast enough to handle interactive Web browsing while still offering users strong local anonymity guarantees. Although Dissent represents a step towards strong anonymous communication at large Internet scales, many challenges remain for future work, such as further scalability and robustness improvements and protection against long-term intersection attacks.