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.