Es geht weiter hier dank Phil Zimmermann zu NSA et al

Erfasst am : 28. September 2013 23:19 | Erfasst von : Martin
Verknüpfte Kategorie(n): Internet, Diverses

So, lange ist es her, dass ich meinen letzten Blog-Eintrag machte. Der Grund dafür ist eigentlich ganz einfach: Es ist alles schon millionenfach gesagt. Selbst wenn man bedenkt, dass immer neue Menschen auftauchen, die sich wiederum orientieren (müssen), so haben auch die den Zugriff auf alle essentiellen Informationen, die eben schon lange überall stehen.

Wie ich mal schrieb vor Jahren, wieso ich blogge, so entspreche ich dem wiedereinmal, ich mach's einfach so. Für mich, dass ich raushauen kann, was mich ab und an bewegt - so sehr, dass ich meinen Schreibunwillen überwinde ...

Interessant ist, was ich grad im letzten Blog-Artikel, der schon aus dem letzten Jahr ist, zur Beachtung andiente ... mittlerweile ist alles noch viel offensichtlicher geworden: Was die NSA machte.

Es war mir als intimer Kenner der Computerei immer klar, dass Möglichkeiten Begehrlichkeiten wecken. Dass ein technikgläubiges Land wie die USA diese dann auch realisiert, war mir daher klar. Interessant in diesem Zusammenhang ist das kurze Interview, das der heise-Newsticker mit Phil Zimmermann publizierte: Unter dem Titel PGP-Erfinder zur NSA-Affäre: Sicherheit rechtfertigt keinen Polizeistaat bringt Phil Aspekte ein, die wir schon beachten sollten, wenn es um die Entwicklung der BigData-Geschichten geht.

Phil Zimmermann hat das damals erste wirklich gute Verschlüsselungsprogramm entwickelt, das PGP (Pretty Good Privacy = ganz schön gute Privatsphäre). Es nutzte die mathematischen Probleme, die von den Herren Rivest, Shamir und Adleman erstmals benutzt wurden, um ein Verschlüsselungssystem zu entwickeln, das keinen problematischen Schlüsselaustausch zwischen Sender und Empfänger mehr benötigte. Deshalb heisst es auch asymmetrische Verschlüsselung. Damit war und ist es de facto unmöglich, eine verschlüsselte Meldung zu entschlüsseln. Das kann auch die NSA nicht. Brachiale Rechengewalt kann die Mathematik derzeit nicht beugen, denn die Nutzer können diese Computerpower ja auch nutzen, um die Schlüssel zu vergrössern. So bleibt die Relation zwischen Verschlüsseler und Hacker gewahrt.

Dass in PGP et al damit aus Praxisgründen nur ein Schlüssel eines symmetrischen Verfahrens übertragen wird, mit dem erst die Nutzdaten verschlüsselt werden, sei der Klarheit halber kurz bemerkt - wenn dieses symmetrische Verfahren als ausreichend sicher gilt wie derzeit AES128 oder besser noch AES256, dann ist das gesamte Verfahren nach wie vor sicher.

Vor vielen Jahren also, etwa 1990+, war es noch verboten, starke Verschlüsselungstechniken aus der USA zu exportieren. So wurde das Programm im Quelltext veröffentlicht, so dass eine Community es kompilieren konnte. Die dazugehörige Website www.pgpi.org ist immer noch aktiv und sieht immer noch aus wie vor 10 Jahren.

Also also PZ PGP rausliess, empfand ich es sofort als ein wichtiges Stück Software. So hatte ich schon früh in diesem PGP-Netzwerk mitgemacht, nervte allerdings auch einige meiner Email-Kollegen damit, denn man musste halt schon etwas Aufwand tätigen, um eine sichere Meldung zu transferieren.

Es gab dann auch bald andere Email-Verschlüsselungen, wie S/MIME, die allerdings ein kostenpflichtiges (und damals teures) Zertifikat benötigten.

Auch diese wurden von Durchschnitt der Computeruser nicht angenommen. Ein paar Paranoiker wussten natürlich damals schon, dass der Staat alles abhört. Die nutzten PGP daher - auch in Ländern, wo das damals wie heute verboten ist.

Auch wenn klar gesagt werden muss, dass PGP verschlüsselte Daten immer noch sicher sind, ist PGP alleine auch nicht mehr glückseligmachend. Es ist heute - und das haben die Geschichten um die NSA klargestellt - viel leichter, Computerusern etwas Unerwünschtes unterzujubeln (Trojaner, Rootkits, Sollbruchstellen in Hard- und Software etc.), so dass man Verschlüsseltes ja auch gar nicht knacken muss - irgendwann will ja irgendein Mensch die Daten nutzen - DANN schlagen sie zu.

Wie auch immer, nach diesem Exkurz also nochmals zurück zum Interview mit PZ: Mir erscheint wichtig, die Sicht nach vorn auf die ganzen NSA-Geschichten gebührend zu gewichten, denn wie PZ sagt: *"Wir wissen nicht, wer 2017 im Weißen Haus sein wird und ob sie die politische Einstellung von Thomas Jefferson oder von Wladimir Putin haben werden."*

Denn es darf klar sein, es ist heute schon möglich, Daten in Relation zu setzen, die Fragen beantworten können wie "Wer betritt zu welcher Zeit in welches Hotel? Wer schläft mit wem? Welcher Politiker kann mit diesen Informationen neutralisiert werden?". Wenn man sie denn hat. Der Fall NSA ist nur darum so gravierend, weil die die Daten eben haben - abgesegnet von einem sog. demokratischen Staat wie den USA. Nur das Demos (gr.das Volk) kannte den Umfang gar nicht, den die Staatenlenker ansteuerten mit dem Argument des Schutzes gegen Terrorismus seit 9/11.

Also, das Interview lesen und sich selbst mal Gedanken machen. Ändern kann man zwar (fast) nichts, aber alles Grosse beginnt im Kleinen. Also ist doch jeder kleine Gedanke ein Funke, der andere inspirieren kann. Deshalb schreibe ich doch ab und an wieder einen Blog-Eintrag. Sic.

Ceterum censeo: Think globally, act locally.