The Big Equalizer

PRISM und Co aus Sicht linksradikalen Datenschutzes

> Schon mit der letzten RHZ kamen ein paar politische Bewertungen der Snowden'schen Enthüllungen zu den großen Überwachungsprogrammen von NSA und anderen Geheimdiensten. Nach drei Monaten fortgesetzter Enthüllungen mögen viele achselzuckend weitergehen und die „Post-Privacy" ausrufen wollen, da „sie" ja doch alles können. Da hätten wir Einspruch anzumelden.

Zunächst allerdings können wir nicht widerstehen, auf einen Nebenaspekt einzugehen, der in der bürgerlichen Kommentierung *sehr* zu kurz kam. Vielleicht spricht er ein wenig die niederen Instinkte des_der durchschnittlichen Linken an, und doch: All das, was jenseits der unmittelbaren Profiteure in Innen- und Kanzleramtsministerien zumindest für Befremden sorgte, entspricht auch deutscher Rechtslage, sofern die Opfer nur Linksradikale und andere Verbrecher sind. Für diese sind Telefonüberwachung, Bewegungsprofile aufgrund von Mobiltelefon-Standortdaten oder Abschnorcheln des Internetverkehrs rechtsstaatlicher Standard. Dank großzügiger Polizeigesetze und der Willkürkonstrukte aus der Familie 129 StGB müssen sie dazu noch nicht mal spürbar revolutionäre Umtriebe entfalten.

In dem Sinn sagen wir hier NSA, GCHQ und all den anderen Zwielichtern ein herzliches Dankeschön, dass wenigstens ihre staatliche Überwachung auch all die Duckmäuser und Zufriedlinge trifft, die von Repression gegen uns nie etwas haben wissen wollen. Da fühlen wir, die wir ja wirklich das eine oder andere zu verbergen haben könnten, uns doch gleich viel mehr angenommen von dieser Gesellschaft. The Big Equalizer: Die modernen Programme überwachen alle. Aber tatsächlich ist das weniger paranoid, als es zunächst scheinen mag. Die Unruhestifter von morgen sind ja heute noch brave Bürger_innen (oder ihr Nachwuchs).

No they can't

Bei aller Genugtuung über die Gleichberechtigung von Zecken und Zahmen: Die Debatte nahm im August eine potenziell destruktive Wende, als plötzlich allenthalben gemunkelt wurde, die NSA könne „fast alle" Verschlüsselung knacken.

Das Wichtigste in Kürze: *Das ist Unfug*. Was an halbwegs aktuellen Verschlüsselungsverfahren draußen ist, ist auch von Läden von der Größe der NSA nach wie vor nicht effektiv angreifbar.

Was allerdings angreifbar ist, ist die „schlechte" Benutzung dieser Kryptographie. Selbst dabei ist jedoch beim Brot- und Butter-Werkzeug, das wir in den letzten zehn Jahren allerorten angedient haben, noch keine akute Warnung angebracht: Uns ist immer noch kein Fall bekannt, in dem die NSA oder sonst ein Geheimdienst versucht hätte, den nachlässigen Umgang mit Schlüsseln in den diversen Szenen auszunutzen.

Höchst angreifbar ist demgegenüber – und das sollte regelmäßige Leser_innen unserer Kolumne nicht überraschen –, SSL, die Technik hinter verschlüsselt übertragenen Webseiten („https-URLs") und auch der Transportverschlüsselung von Mails („pops", „imaps", „smtps"). Um die Problematik dahinter zu verstehen, hilft die Lektüre von „Vertrauen unter GenossInnen" (RHZ 4/09, vgl. auch die URL am Fuß dieses Artikels). Darin wird erläutert, wie jemand, dem ihr im Rahmen von SSL vertraut, euch Schlüssel unterschieben kann.

Das ist fatal, denn während euer Browser glaubt, er verschlüssele für, sagen wir, datenschmutz.de, verschlüsselt er dann in Wirklichkeit für den VS, die NSA, oder beide. Diese können dann an eurer Statt mit dem wirklichen datenschmutz.de sprechen und bekommen die ganze, scheinbar verschlüsselte Kommunikation mit. Diese „man-in-the-middle"-Angriffe gehen immer, wenn der Schlüsselaustausch nicht abgesichert ist, und ihre Abwehr ist letztlich Sinn des Web of Trust, das im zitierten Artikel erklärt wird.

SSL hat kein Web of Trust. Euer Browser wird stattdessen ausgeliefert mit einer breiten Auswahl von Stellen, denen er einfach so vertraut, ohne dass er euch da fragen würde. Tut euch den Gefallen und seht euch die Liste mal an, im Firefox etwa in der Gegend von Edit → Preferences → Advanced → Encryption → View Certificates. Von TÜRKTRUST über die Japanische Regierung und den Deutschen Sparkassen Verlag bis hin zu Verisign und – indirekt – der FH Furtwangen reicht die Liste von Gesellschaften, die euch Schlüssel für alles unterschieben können, was sie wollen: Google, riseup.net, datenschmutz.de, egal. Und es ist völlig klar, dass die NSA ebenso wie selbstverständlich auch ausnahmslos alle deutschen „Bedarfsträger“ irgendeinen Schlüssel haben, dem euer Browser vertraut.

Das Schlüsselmanagement von SSL ist also kaputt, wie wir schon 2008 anklingen ließen, und die Jahre seitdem haben das immer wieder bestätigt. Dabei ist die eigentliche Verschlüsselung in Ordnung, nur funktioniert des Schlüsselaustausch so, als würdet ihr bei PGP nie die Schlüssel selbst speichern, sondern einfach nehmen, was an einer Mail dranhängt, sofern die Polizei verspricht, der Schlüssel sei ok.

Eine gewisse Hilfe, auch bei SSL Basissicherungen einzuziehen, sind Browsererweiterungen wie Certificate Patrol; diese merken sich, womit sich Webseiten ausgewiesen haben, und warnen euch, wenn sich das ändert. Das hilft (vielleicht) nichts, wenn euch der BND schon falsche Zertifikate in Massen unterschiebt, ihr merkt aber immerhin, wenn sie plötzlich damit anfangen. Wenn ihr euch etwas sicherer fühlt, könnt ihr auch einfach all die Autoritäten löschen, die in eurem Browser stehen und dann die Schlüssel („Zertifikate“) einzeln bestätigen (was im Firefox allerdings etwas beängstigend aussieht).

Ansonsten: Verlasst euch nicht auf SSL. Was PGP angeht, sind die zugrundeligenden Verfahren ebensowenig gebrochen wie das Prinzip des Web of Trust. Auch Truecrypt (und einige weitere Software ähnlicher Art) dürfte, den überentschlossenen Versuchen, an die Passwörter ranzukommen nach zu urteilen, nicht gebrochen sein. Ähnliches gilt für OTR, das zur Verschlüsselung vor allem von Chats eingesetzt wird. Gerade angesichts des verbreiteten Abgreifens von Verbindungsdaten bleibt auch Tor ein gutes Mittel, unbenommen der Tatsache, dass ein Teil der US-Regierung die Entwicklung von Tor finanziert.

Dennoch wäre jetzt wohl allmählich der in RHZ 4/09 prognostizierte Moment, in dem die RH mit ordentlichem Schlüsselmanagement (also vernünftigen Signaturen darauf) Extrapunkte verdienen könnte.

Unser dringendes Fazit also: Die Snowden-Enthüllungen haben nicht gezeigt, dass Verschlüsselung sinnlos ist. Sie haben im Gegenteil gezeigt, dass Geheimdienste tatsächlich einen ganzen Haufen von dem tun, was vorgestern noch Verschwörungstheorie schien.

Und schließich: Schlechte Verschlüsselung hat vielleicht nicht furchtbar viel Sinn, bleibt aber besser als gar nichts, solange mensch nicht anfängt, wirklich furchtbar Kitzliges zu verschicken. Gute Verschlüsselung mit dem (oder einem) Web of Trust hingegen sind mehr denn je angesagt. Wenn ihr eine Einführung wollt: Schreibt uns, wir kommen gerne bei euch vorbei.

Datenschutzgruppe der Roten Hilfe Heidelberg

Kontakt und Artikel-Archiv: https://datenschmutz.de

PGP Fingerprint: a3d8 4454 2e04 6860 0a38 a35e d1ea ecce f2bd 132a