Hörspiel/Hintergrund Kultur

Dossier

Redaktion: Karin Beindorff

Sdg. 2. Januar 2015

Crypto wars oder
Die Freiheit im Netz

Von Walter van Rossum

Musik

Autorin:
Im Herbst 2005 beschloss der US-amerikanische Jurist und Verfassungsrechtler Glenn Greenwald im Internet einen politischen Blog zu eröffnen. Ihn beunruhigte zunehmend, …

Zitator:
… das radikale und extremistische Machtdenken der amerikanischen Regierung nach dem 11. September.

Autorin:
Sein Blog wurde ein großer Erfolg, ebenso wie sein kritisches Buch über die Einschränkungen der Bürgerrechte in den USA. Greenwald war bald ein bekannter Bürgerrechtler.

Am 1. Dezember 2012 erhielt Glenn Greenwald eine rätselhafte E-Mail, die mit den Worten begann:

Zitator:
Es liegt mir sehr am Herzen, dass Menschen sicher miteinander kommunizieren können.

Autorin:
Der Verfasser der E-Mail bat Greenwald, ein bestimmtes Verschlüsselungsprogramm zu installieren und erklärte:

Zitator:
Verschlüsselung ist etwas Essentielles, nicht nur für Spione und Schürzenjäger. Es ist eine absolut unerlässliche Maßnahme für jeden, der sich mit Ihnen in Verbindung setzen will.

Autorin:
Erst dann könnte er Greenwald ein paar Informationen zukommen lassen, die ihn zweifelsohne interessieren müssten.

Zitator:
Mit kryptographischen Grüßen

Ansage:
Crypto wars oder
Die Freiheit im Netz
Ein Dossier von Walter van Rossum.

Autorin
Wer da kryptographisch grüßte, war kein anderer als Edward Snowden. Es bedurfte übrigens einer ganzen Weile, bis der Kontakt und der Austausch jener Informationen, die die Welt erschüttern sollten, endlich zustande kamen. Um ein Haar hätte Greenwald den Coup verpasst.

Diese kleine Geschichte enthält zwei hochinteressante kryptographische Aspekte. Zum einen wäre da Glenn Greenwald, der wie kaum ein anderer über die Machenschaften der US-amerikanischen Geheimdienste Bescheid wusste, der darüber publiziert hatte und es dennoch nicht für nötig hielt, auf seinem Computer eine Verschlüsselungssoftware zu installieren. Ja, nicht einmal eine Ahnung hatte, wie das überhaupt gehen könnte. Auf der anderen Seite Edward Snowden, der viele Jahre für die NSA gearbeitet und im Laufe der Jahre verstanden hatte, dass diese Firma den „schlüsselfertigen Apparat für eine Tyrannei“ errichtet hatte: Edward Snowden, der ziemlich genau zu wissen scheint, was die NSA kann, vertraut gängiger Verschlüsselungssoftware, die überall erhältlich ist.

Zitator:
„Wir werden dafür sorgen, dass noch mehr Menschen in Deutschland ihre eigene Kommunikation noch sicherer machen.“

Innenminister Hans-Peter Friedrich, CSU, 2013

O-Ton R. Weis
Kryptographie ist Kommunikation in Anwesenheit von Gegnern.
Autorin
Rüdiger Weis, Professor für Informatik und Kryptograph
O-Ton R. Weis
Wir gehen in der Kryptographie eigentlich immer davon aus, dass ein Angreifer alle Nachrichten abhören kann. (…) Und wir gehen davon aus, dass der Angreifer sehr mächtig ist und sehr viel Geld zur Verfügung hat.

Autorin:
Schon im Jahre 2000 sprach der Mitbegründer des Chaos Computer Clubs Wau Holland in einem Vortrag über das Recht auf Privatheit:

O-Ton: Wau Holland
Es geht darum, bestimmte Reste von informationeller Selbstbestimmung überhaupt noch zu haben. In den Niederlanden gibt es den Professor Barkin, und der hatte ein Buch geschrieben: 2008 Ende der Privatheit. Seine Vorstellung ist, wenn sich die Datenmaschinerie und die Kontrolle der Einzelnen dadurch, dass Dateien über sie angelegt werden, so weiterentwickelt, wie es jetzt absehbar ist, dann war die Vision von Orwell mit 1984 nur vom Datum falsch, aber nicht von der Struktur her. Ungefähr 2008 sind derartige Datenmengen verwaltbar, dass es letztlich keine Privatheit mehr gibt. An der Stelle ist das Recht auf Privatheit zurückzugewinnen, dadurch dass man seine Nachrichten verschlüsselt.

Autorin:
Ausdrücklich verwies Wau Holland, der 2001 starb, damals bereits auf die NSA, von der er vermutete, dass sie einen technischen Vorsprung von sieben bis zehn Jahren auf die allgemeine Entwicklung habe. Leuten wie Wau Holland verdanken wir das Internet in seiner bis heute bekannten Form: eine freie und improvisierte Struktur, die niemandem gehört und die niemand vollkommen beherrscht.

Zitator: /O-Ton

Declaration of the independance

"…We will create a civilization of the Mind in Cyberspace.
May it be more humane and fair than the world your governments
have made before."

Autorin

Holland und seine Mitstreiter hatten allerdings auch früh erkannt, dass die Freiheit des Internets ganz schnell zu einer Falle werden könnte. Denn niemals war es leichter, Massenkommunikation massenhaft zu überwachen.

Zitator:

Artikel 10 Grundgesetz:

(1) Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.

(2) Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. Dient die Beschränkung dem Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes, so kann das Gesetz bestimmen, daß sie dem Betroffenen nicht mitgeteilt wird und daß an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt.

Autorin:

Gegen die massenhafte Bespitzelung hilft vor allem die Verschlüsselung der elektronischen Kommunikation. Eine Idee, die einigen Behörden gar nicht in den Kram passte. Das führte bereits in den 90er-Jahren zu einem sog. Crypto war – einem ersten Krieg um die Verschlüsselung im Netz. Die Befürworter einer Regulierung wollen verhindern, dass im Internet ein unkontrollierbarer Austausch stattfindet, die Gegner verlangen, dass das grundsätzlich geschützte Recht auf Privatheit und die Wahrung des Brief- und Fernmeldegeheimnisses garantiert bleiben.
Wer waren die Kombattanten?

O-Ton Klaus Schmeh
In Deutschland waren die Befürworter einer Krypto-Regulierung, es waren gar nicht so viele. Das waren Leute im Innenministerium und von der Polizei, die haben gesagt, es kann nicht sein, dass jeder Kriminelle seine E-Mails verschlüsselt und wir können sie nicht mehr mitlesen.

Autorin:
Klaus Schmeh ist Informatiker, Sachbuchautor und Kryptograph.
Und auf der anderen Seite?

O-Ton Schmeh
Es gab sehr viele Gegner einer Kryptoregulierung, das war eine ziemlich bunte Mischung vom Chaos Computer Club bis zur Verschlüsselungs- und Computerindustrie, die alle haben gesagt, das kann nicht sein, dass wir unsere Sachen nicht verschlüsseln dürfen.

Autorin:
Die Crypto wars der 90er-Jahre fanden noch auf nationalen Schlachtfeldern statt. In Frankreich z. B. galt Kryptographie als Waffe und ihre Anwendung wurde nur unter bestimmten Umständen erlaubt. In den Vereinigten Staaten durfte man zwar verschlüsseln, aber der Export von Chiffrierprogrammen mit einer Schlüssellänge von mehr als 56 Bits war verboten. In diesem Zusammenhang wurde der Informatiker Phil Zimmermann zu einer Art Volksheld des digitalen Freiheitskampfes. Er entwickelte nämlich das Programm PGP – pretty good privacy, zu Deutsch etwa: ziemlich guter Datenschutz. Bereits 1991 stellte Zimmermann PGP zum kostenlosen Download ins Netz. Und ihm widerfuhr, was seitdem jeder erlebte, der solche Dinge tat:

Zitator.:
In den USA bekommen alle Firmen, die Verschlüsselungsprogramme herstellen, Besuch von der NSA. In einem vertraulichen Gespräch legt man ihnen nahe, den Schutz dieser Programme abzuschwächen.

Autorin:
Doch Phil Zimmermann wollte nicht 'abschwächen', und so wurde er viele Jahre lang mit Gerichtsverfahren überzogen, weil er angeblich gegen die US-Exportbestimmungen verstoßen hat.

Musik

Autorin:
Auch in Deutschland wurde schon in den 1990ern heftig für und gegen Verschlüsselung gestritten. Am Ende schienen die Freunde der Verschlüsselung gewonnen zu haben, und die Geheimdienste schienen sich dem Stand der Dinge zu ergeben.
In Wahrheit hatten sich die Geheimdienste, wenigstens in den USA, keineswegs geschlagen gegeben, sondern sich vielmehr auf ihr ureigenes Terrain besonnen: sie spionierten im Geheimen, ohne rechtsstaatliche Kontrolle. Und diese Überwachung nahm nach dem 11. September 2001 Ausmaße an, die alle Befürchtungen in den Schatten stellten. Federführend bei der Entwicklung der globalen Schnüffelei war die NSA – die National Security Agency. Der 1952 gegründete Geheimdienst ist für die weltweite Überwachung der gesamten elektronischen Kommunikation zuständig – angeblich zum Schutz der US-amerikanischen Sicherheit. Offiziell verfügt die Agency über ein Budget von über zehn Milliarden Dollar. Inoffiziell dürften es etliche Milliarden mehr sein, die Geheimdienste sind nicht verpflichtet ihre Etats zu veröffentlichen. Die NSA beschäftigt über 40.000 Mitarbeiter und gilt weltweit als der größte Arbeitgeber für hochqualifizierte Mathematiker. Zurzeit rühmt sich der Dienst auf seiner Webseite damit, täglich 29 Petabyte an Daten zu sammeln und zu speichern. Ein Petabyte ist eine eins mit 15 Nullen oder 1000 Billiarden Bytes.
NSA-Direktor General Keith Alexander auf der offiziellen Webseite zur Reichweite seines Dienstes:

Zitator
Öfter als wir zählen können, haben wir Geschichte gemacht, ohne dass die Geschichte überhaupt wusste, dass wir da waren.

Autorin:
Dieses Bekenntnis lässt Rückschlüsse auf ein nicht eben lupenreines Demokratieverständnis zu. In einem internen Strategiepapier erklärte General Alexander 2010, dass die „digitale Revolution“ der NSA „eine einzigartige Position“ verschafft habe. Sie strebe die „global cryptologic dominance“ an, die weltweite kryptografische Dominanz – mit anderen Worten die totale Überwachung der globalen Kommunikation. Wie diese ‚einzigartige Position‘ der NSA sich im Alltag jedes Einzelnen auswirkt, hat Edward Shnowden beschrieben:

Zitator (Shnowden):
Jedes Mal, wenn Sie telefonieren, eine E-Mail schreiben, etwas überweisen, mit dem Mobiltelefon Bus fahren und irgendwo eine Karte durch ein Lesegerät ziehen, hinterlassen Sie eine Spur. Und die Regierung hat beschlossen, dass es eine gute Idee ist, das alles mit diesen Programmen zu sammeln. Alles, selbst wenn Sie noch nie eines Verbrechens verdächtigt wurden.

Autorin
Und die NSA hat eine Reihe von sehr wirkungsvollen Techniken entwickelt, mit denen sie die aberwitzigen Datenmengen globaler Überwachung in präzise Instrumente individueller Verfolgung verwandelt. Wichtiger Bestandteil dieser grenzenlosen Bespitzelung ist das Programm Xkeyscore. Edward Snowden:

Zitator (Snowden):
Es ist eine Technik, mit der man alle Daten durchsuchen kann, die weltweit täglich von der NSA gespeichert werden. (…) Man könnte jede E-Mail auf der ganzen Welt lesen, von jedem, von dem man die E-Mail-Adresse besitzt. Man kann den Verkehr auf jeder Webseite beobachten, auf jedem Computer. Jeden Laptop, den man ausfindig macht, kann man von Ort zu Ort über die ganze Welt verfolgen. Es ist eine einzige Anlaufstelle, über die man an alle Informationen der NSA gelangt. Darüber hinaus kann man Xkeyscore benutzen, um einzelne Personen zu verfolgen. Sagen wir, ich habe Sie irgendwo gesehen und finde interessant, was Sie machen. Oder Sie haben Zugang zu etwas, das mich interessiert. Sagen wir, Sie arbeiten für ein großes

deutsches Unternehmen, und ich möchte Zugang zu diesem Netzwerk haben. Ich kann Ihren Benutzernamen auf einem Formular irgendwie herausfinden, ich kann Ihren echten Namen herausfinden, ich kann Beziehungen zu Ihren Freunden verfolgen und ich kann etwas bilden, was man als Fingerabdruck bezeichnet. Das heißt eine Netzwerkaktivität, die einzigartig für Sie ist. D. h., egal, wohin Sie auf der Welt gehen, egal, wo Sie versuchen, ihre online-Präsenz, ihre Identität zu verbergen, kann die NSA Sie finden. Und jeder, der berechtigt ist, dieses Instrument zu benutzen, kann dasselbe tun. Deutschland ist eines der Länder, die Zugang zu Xkeyscore haben.

Autorin

Xkeyscore ist allerdings nur eine von vielen Waffen der National Security Agency.

Musik

Zitator:

„Wer seine Daten sichern will, wird sie wohl verschlüsseln müssen und kann nicht mehr auf seinen Nationalstaat hoffen“.

Hans Peter Uhl, Innenpol. Sprecher der Unionsfraktion im Juli 2013

Autorin

Angeblich dient der Versuch der lückenlosen Überwachung von allem und jedem dem Schutz der Vereinigten Staaten vor terroristischen Anschlägen. Angeblich hat die NSA auch eine Reihe von Attentaten verhindert. Doch Glenn Greenwalds Recherchen sagen etwas anderes:

Zitator:

Eine Studie der in der politischen Mitte angesiedelten New America Foundation zur Glaubwürdigkeit der offiziellen Rechtfertigungen für die Massendatensammlung kam zu dem Schluss, dass das Programm „keinen erkennbaren Beitrag zur Verhinderung von Terroranschlägen geleistet hat“. Wie die *Washington Post* berichtete, wurden dieser Studie zufolge Terrorpläne vor allem dadurch zunichte gemacht, dass „traditionelle Gesetzesvollstreckung und Ermittlungsmethoden zu einem Verdacht oder Anhaltspunkt führten, die Anlass zur Eröffnung eines Falls gaben“.

Autorin
Sicher ist jedenfalls: Ein großer Teil der NSA-Aktivitäten hat überhaupt nichts mit Terrorismus zu tun, wie z.B. das Abhören befreundeter Regierungen, internationaler Organisationen oder die Ausspähung ganzer Wirtschaftskonzerne.

Musik

Autorin:
Das Logo der NSA zeigt einen Adler bewehrt mit US-Flagge als Schild. Mit seinen Krallen sitzt er auf einem großen goldenen Schlüssel. Der Schlüssel ist natürlich ein Zentralmotiv der Kryptographie.
Die Kunst der Verschlüsselung ist uralt, sagt Klaus Schmeh:

O-Ton Schmeh
Früher gab es recht einfache Verfahren, die Buchstaben ersetzt haben: dann wurde halt das A durch das E und das B durch das F oder so ersetzt.

Autorin:
Und der Schlüssel besagte dabei, um wie viele Stellen die Buchstaben des Alphabets sich verschoben. Die Erfindung dieses System wird dem römischen Herrscher Gaius Julius Caesar zugeschrieben. Und bald gab es auch einen Apparat mit zwei Scheiben, der die Chiffrierung und Dechiffrierung erleichterte. Diese Verschlüsselung ist leicht zu durchschauen und enthält einen weiteren Nachteil: Sender und Empfänger müssen den Schlüssel austauschen - und zwar im Klartext, also unverschlüsselt.

Musik

Autorin
Heute geht es bei der Kryptographie nicht mehr darum, einzelne Botschaften von Kaisern, Militärs oder Agenten zu chiffrieren bzw. dechiffrieren, sondern darum die Massenkommunikation vor ihrer massenhaften Erfassung zu schützen. Spätestens

mit dem Aufkommen der Telegraphie im 19. Jahrhundert verlief ein erheblicher Teil der privaten Kommunikation über öffentliche Leitungen, die leicht abzuhören waren. Unter den modernen Umständen massenhafter Kommunikation auf offenen Kanälen entstand damals ein verblüffendes kryptographisches Prinzip.

O-Ton Wau Holland
Ein Verschlüsselungsverfahren taugt nur dann etwas, wenn man es komplett dokumentieren kann.
Autorin:
der Hacker Wau Holland.
O-Ton Wau Holland
Man muss nachvollziehen können, wie es funktioniert. Und damit kann man die meisten Verschlüsselungsverfahren einfach knicken.

Autorin
Das Zahlenschloss beim Fahrrad öffnet sich nur dann, wenn man genau die vier Ziffern kennt, auf die das Schloss eingestellt ist. Es gibt genau 9999 Möglichkeiten für die richtige Kombination. Das reicht in der Regel für ein Fahrradschloss, denn man bräuchte ein paar Stunden, um alle Möglichkeiten durchzuprobieren. Ein Computer würde eine solche Kombination allerdings in Bruchteilen von Sekunden finden. Da aber das Verfahren bekannt sein muss, damit jeder es anwenden kann, bauen Kryptographen sehr lange Schlüssel mit über 200 Stellen, kombiniert aus Ziffern und Groß- und Kleinbuchstaben. Selbst sehr leistungsfähige Rechner bräuchten Jahrzehnte, um sämtliche Möglichkeiten durchzuspielen.

O-Ton Schmeh
Der Computer macht das mit speziellen modernen mathematischen Verfahren, die genau ausgeklügelt sind. Der AES ist zum Beispiel ein bekanntes Verschlüsselungsverfahren. AES heißt Advanced Encryption Standard, was einfach so viel heißt wie „der fortgeschrittene Verschlüsselungsstandard“ d.h. das Verfahren ist ein Standard, also ist öffentlich bekannt, genormt, da muss man also nichts selber erfinden und

diese Verfahren, die es da heutzutage gibt, sind ziemlich ausgeklügelt, also da steckt oft mehrere Jahre an Arbeit drin.

O-Ton R. Weis
Weil wir damals der Meinung waren, wir haben noch ein bisschen Perfomance übrig, haben wir nochmal Twofish verknüpft, mit ner einfachen xor-Verknüpfung, diese einfache xor-Verknüpfung hat einfach diese nette Eigenschaft, dass ein Angreifer damit beide Verfahren brechen muss.

O-Ton Schmeh R. Weis
Und die gelten dann als sehr sicher. Dieser AES zum Beispiel, den gibt es jetzt seit über 15 Jahren, und da hat noch niemand auch nur annähernd es geschafft, eine Verschlüsselung damit zu knacken.

Autorin:
Die meisten kryptographischen Verfahren sind heute bekannt, aber – und das ist das entscheidende - ohne den Schlüssel nicht zu knacken.

O-Ton Joachim Selzer
Bestimmte Zahlen nennen sich Primzahlen, die haben die interessante Eigenschaft, dass sie sich nicht weiter teilen lassen.
Autorin:
der IT-Experte Joachim Selzer
O-Ton Joachim Selzer
Das sind die Zahlen 2, 3, 5, 7, 11, 13 usw., die lassen sich nicht weiter teilen. Und jetzt gibt es halt ein Gesetz in der Mathematik, dass ich jede Zahl als eindeutiges Produkt von Primzahlen darstellen kann. (…) Es gibt nur eine bestimmte Konstellation von Primzahlen, die eine bestimmte Zahl bestimmte ergeben. So, und jetzt rechnet man in die eine Richtung; man knallt irgendwem ganz viele ganz lange Primzahlen hin und sagt: jetzt multiplizier die mal miteinander. Und das kriegt jeder hin, denn Multiplizieren ist eine einfache Sache. Das klimpert man in seinen Taschenrechner und bekommt dann eine schöne Zahl raus. Wenn ich jetzt allerdings umgekehrt da-

ran gehe und sage: Hier ist eine Zahl mit 200 Stellen, sag mir doch mal die Primfaktoren davon, (…) dann ist man gezwungen, rumzuprobieren. Das heißt, wir haben ein Verfahren, das funktioniert in die eine Richtung ganz toll: Ich nehme Primzahlen, mache daraus eine große Zahl, multiplikativ. Das ist eine Sache von ein paar Sekunden. Ich hab eine riesengroße Zahl und will die in genau diese selben Primfaktoren wieder zerlegen. Ich brauche ewig dazu, um das hinzubekommen. Das ist eben die asymmetrische Verschlüsselung oder ein Prinzip davon.

Autorin:
Der Kryptograph Klaus Schmeh lässt keinen Zweifel an der Sicherheit des Verfahrens.

O-Ton Schmeh
Könnte sein, dass irgendwo auf der Welt ein schlauer Kopf sitzt, der das entschlüsseln kann, ist aber sehr unwahrscheinlich, bisher hat man noch nicht einmal ein Prozent der Verschlüsselung geknackt, von 100 mal ganz zu schweigen.

Autorin:
Der Laie zuhause an seinem Rechner muss aber die Einzelheiten des kryptographischen Verfahrens gar nicht verstehen. Er muss nur bestimmte Programme installieren. Und das lernt er zum Beispiel auf so genannten Kryptopartys.

Atmo Kryptoparty

Autorin:
In den Räumen des Chaos Computer Clubs in Köln treffe ich Joachim Selzer, 45 Jahre alt. Der verdient sein Geld bei einem großen Logistikunternehmen und betätigt sich als Aktivist in Sachen Datenschutz und Netzfreiheit. Und von Zeit zu Zeit veranstaltet er eine Kryptoparty.

O-Ton Selzer
Kryptopartys heißen die, weil das ursprüngliche Konzept aus dem Sommer 2012 lautete: Wir bringen die Leute einfach in einen Raum zusammen, und die organisieren sich irgendwie selbst und bringen sich gegenseitig Krypto bei – also Verschlüsselungstechniken. Das hat dann in Deutschland nicht ganz so gut funktioniert. In Deutschland mag man es gerne etwas seminarlastiger. Dann möchte man, dass da vorne ein Vortrag ist, und an den Vortrag schließt sich dann ein Workshop an.

Autorin:
Kryptopartys gibt es noch nicht so lange. Das Publikum war, sagt Selzer:

O-Ton Selzer
war am Anfang, vor einem Jahr, oder etwas mehr als einem Jahr, als ich damit angefangen hab, noch sehr nerdlastig, d.h. drei Viertel der Leute waren eh schon vom Fach, und denen musste man nichts Neues mehr erzählen. Das hat sich jetzt im Lauf gerade des letzten Sommers, des Snowden-Sommers, sehr geändert. Jetzt ist es eher so, dass ich sag mal die Hälfte bis ¾ der Leute Nicht-Fachpublikum ist, und dass wir denen tatsächlich noch etwas neues erzählen können.

Autorin:
Was geschieht da?

O-Ton Selzer
Kryptoparty bezeichne ich immer als einen digitalen Erste Hilfe Kurs: man kann in die Veranstaltung rein und muss eigentlich gar nichts wissen. Man muss nur was wissen wollen. Wie beim normalen Erste Hilfe Kurs, man bekommt beigebracht, da liegt irgendwer und jetzt hast Du folgende Möglichkeiten, mit dem was zu machen. Dann läuft ein ganz stures Schema ab, wie man den Menschen beatmet, wie man Verbände angelegt, wie man einen Notruf absetzt, wie man eine stabile Seitenlage herbeiführt. Und bei den Kryptopartys ist es genauso. Wir sagen den Leuten: Ihr habt fünf Stellen, an denen ihr was ändern könnt.

Autorin:
Die 5 Stellen sind: Festplattenverschlüsselung, Mailverschlüsselung, Chat-Verschlüsselung, Passwortverwaltung und Anonymisierung. Und für jedes dieser Felder wird den Partygängern ein ganz bestimmtes Programm gezeigt.

Atmo: Kryptoparty

O-Ton Selzer
Ich habe so als Zielperson immer meinen Vater im Hinterkopf. Der ist jetzt 71 Jahre alt, versteht kaum etwas von Computern und dem möchte ich im Idealfall beibringen: Pass auf, so verschlüsselt Du deine Mails.

Autorin:
Dummerweise ist das Verschlüsseln von E-Mails vergleichsweise kompliziert. Gerade für die Windows-Software benötigt man drei Programme und muss für jede einzelne Mail mehrere Einstellungen vornehmen. Weil die Installation einigermaßen aufwändig ist, sind jetzt einige deutsche Mail-Provider auf die Idee gekommen eine sogenannte SSL-Verschlüsselung anzubieten – und bewerben dies im großen Stile als Mails made in Germany.

O-Ton Selzer
Bullshit made in Germany. (…) Was die jetzt anbieten, ist eine so genannte Transportwegverschlüsselung, im Gegensatz zu der von PGP angebotenen Ende zu Ende Verschlüsselung. Stellen Sie sich vor, ich will Ihnen Geld überweisen, dann überweise ich das ja auf die Bank und die Bank überweist es Ihnen. Und dann habe ich theoretisch zwei Möglichkeiten. Ich baue mir eine Rohrpost zur Bank, und die Bank baut eine Rohrpost zu Ihnen. Und da schicke ich dann im Prinzip ein zusammengeschnürtes Geldbündel durch und das landet dann erstmal bei der Bank. Die schickt es dann durch eine zweite Rohrpost zu Ihnen. Das Geldbündel selbst, ich habe das nur mit so einem Bindfaden gesichert, das liegt bei mir ungesichert auf dem Schreibtisch rum, da kann es jeder klauen, ich schiebe es rüber zur Bank, da liegt das Ding auch bei denen auf dem Schreibtisch ungeschützt rum, kann jeder klauen. Und dann

pusten die das durch die Gegend und dann liegt es bei Ihnen auf dem Schreibtisch, kann auch wieder jeder klauen. Das ist das, was jetzt als E-Mail made in Germany verkauft wird, eine so genannte Transportwegverschlüsselung, weil man das Rohr halt nicht aufsägen kann.

Autorin
Was hingegen das Programm PGP – pretty good privacy -, von dem schon die Rede war, anbietet, funktioniert anders. PGP bietet an, dass ich einen kleinen Tresor baue, und diesen Tresor schicke ich dann auf den Weg. D.h., selbst wenn jemand den Tresor klaut, dann kann er damit nicht allzu viel anfangen, weil er ihn nicht öffnen kann.

O-Ton Selzer
Das ist halt der Unterschied, dass ich nicht den Transportweg sichere und dann diverse Angriffspunkte insbesondere auf dem Server offen lasse, sondern dass ich dafür sorge, dass die Nachricht von mir bis zu Ihnen hin verschlüsselt wird.

Autorin:
Sehr viel einfacher geschieht das Verschlüsseln an anderen Einsatzstellen – zum Beispiel bei der Festplattenverschlüsselung.

O-Ton Selzer
Wir empfehlen seit zwei Jahren, bzw. hier in der Köln-Bonner-Gegend empfehlen wir seit 1 ½ Jahren *True crypt* zur Festplattenverschlüsselung. Vorteil des Programms ist: sehr einfach in der Handhabung, funktioniert auch wunderbar, hat eine schöne, angenehme grafische Oberfläche. Ich habe Leuten, die von Computern und mit Verschlüsselung überhaupt nichts am Hut haben, dieses Programm gezeigt und die waren glücklich.

Autorin:
True Crypt konnte bis vor wenigen Wochen kostenlos aus dem Netz heruntergeladen werden. Jetzt haben die open source Entwickler aber ihre Arbeit eingestellt. Die Experten warnen davor, auf das Verschlüsselungssystem von Windows auszuweichen.

Microsoft steht nach wie vor im Verdacht mit der NSA zusammenzuarbeiten. Eine ebenfalls frei verfügbare Alternative zu True crypt bietet etwa das Programm Keyparc an. Ähnlich einfach wie die Festplattenverschlüsselung funktioniert die Anonymisierung – also die Möglichkeit beim Surfen im Netz nicht identifiziert zu werden, sagt Joachim Selzer:

O-Ton Selzer
Bei Anonymisierung empfehlen wir blind das Programm Tor – mit anderen Worten: ein Programm, das jetzt zwischen meinen Rechner und der Webseite, die ich aufrufe - ich drücke das jetzt mal ganz übertrieben einfach aus, eine Wolke an Rechnern schaltet, die dann stellvertretend die Anfrage absetzen und damit verschleiern, woher ich komme. Das Schöne an dem Programm ist, dass die Installation komplett einfach ist, man lädt sich was runter, klickt auf Auspacken, klickt auf Start und man legt los.

Autorin:
Das Problem sind allerdings die verschiedenen Server, denen muss man vertrauen. Kann man aber nicht immer, wie das Beispiel des deutschen Informatikstudenten Sebastian Hahn zeigt. Der betreibt einen Server für das Tor-Netzwerk. Und diesen Server hat die NSA gehackt.

O-Ton:S. Hahn
Das ist ein Rieseneingriff in meine Privatsphäre, dass alle Verbindungen, die ich mit einem Server, den ich selber betreibe in Deutschland, mitgeschnitten werden von einem ausländischen Geheimdienst.

Autorin:
Gegen Sebastian Hahn gibt es nicht den leisesten Verdacht auf einen extremistischen politischen Hintergrund. Doch für die NSA wurde er zum „Extremisten“ - so heißt es wörtlich in den Snowden-Dokumenten -, weil er einen Tor-Knotenpunkt betreibt. Die National Security Agency beobachtet genau etwa die Google-Suchanfragen. Wer da nur „Tor“ eingibt, könnte schon in das Raster der Ermittler geraten.

O-Ton Schmeh
Es gibt heutzutage Verschlüsselungsverfahren, da mache ich mir keine Sorgen, da hat die NSA keine Chance. Man muss es halt anwenden und hoffen, dass keine Fehler passieren.

Autorin
Der Kryptograph Klaus Schmeh:

O-Ton Schmeh
Nehmen wir mal an, ich hab den AES, und ich will eine Nachricht knacken. Jetzt hat er ja eine Schlüssellänge von 128 Bit, jetzt kann ich natürlich einen Schlüssel nach dem anderen durchprobieren und hoffen, dass irgendwann mal der Richtige dabei ist. Das kann ich ja feststellen, wenn dann was Vernünftiges rauskommt … Aber selbst im günstigsten Falle müsste ich da so lange rechnen, da reicht die Zeit vom Urknall bis heute längst nicht aus.

Autorin:
Kryptographen drücken sich gerne vorsichtig aus. Die Dinge entwickeln sich schnell und manchmal in unvorhersehbare Richtung. Alle kennen natürlich die Geschichten über die berühmte deutsche Chiffriermaschine Enigma, die im 2. Weltkrieg eine überragende Rolle spielte.

O-Ton [verschlüsselte Funksprüche]

Autorin
Dem englischen Mathematiker und Informatiker Alan Turing gelang es, mithilfe von 7000 Mitarbeitern den Code der Enigma mehrfach zu knacken. …….
Könnte sein, dass die NSA einige hundert Mathematiker darauf angesetzt hat, die Zeit der Dechiffrierung vom Urknall bis heute zu halbieren. Doch selbst wenn es gelänge, mit Superrechnern schon nach sechs Jahren einen Schlüssel eines geläufigen Codeprogramms zu knacken - dann dürfte das die laufende Massenspionage kaum einen Schritt weiterbringen. So gesehen kann man sehr gut verstehen, wenn Firmen

wie die NSA alle Hebel in Bewegung setzen, Kryptographie gar nicht erst zum Einsatz kommen zu lassen.

O-Ton Schmeh
Ich weiß noch, so in den 90ern, da kam ja gerade in den USA, gerade von der NSA – offiziell oder inoffiziell – da haben die das ja torpediert. Die hatten wahrscheinlich Riesenangst um ihre Existenzberechtigung. Die haben wirklich gedacht, wenn jetzt 95 % des Mailverkehrs, des Verkehrs, im Internet verschlüsselt wird, dann können wir dichtmachen.

Autorin
Doch hatten wir nicht gehört, dass der erste Crypto war Ende des vergangen Jahrhunderts im Großen und Ganzen zugunsten der Kryptographie ausgegangen war? Und hatten die Geheimdienste sich nicht dieser Entwicklung gebeugt?

O-Ton Stefan Krempl
Für Kenner der Materie, die das beobachtet haben, haben sich schon gewundert, wieso geben die sich eigentlich dann doch mit dem Status quo zufrieden.
Autorin:
Stefan Krempl, IT-Publizist
O-Ton Stefan Krempl
Und des Rätsels Lösung war dann natürlich mit den Enthüllungen von Edward Snowden, was vor allem die Geheimdienste selber schon machen, dass sie letzten Endes die Schlüssel gar nicht mehr brauchen in der Tat, dass sie sich selbst geholfen haben und sehr stark versuchen, Standards zu hintergehen, Verschlüsselungsstandards zu schwächen.

Autorin
Nachdem Geheimdienste verstanden hatten, dass man mit Gesetzen wenig gegen Kryptographie ausrichten kann, haben sie die Strategie gewechselt. Sie haben sich scheinbar dem Stand der Dinge ergeben, so dafür gesorgt, dass das Thema wenigs-

tens von der Tagesordnung verschwand, und beförderten damit die Sorglosigkeit der Internetnutzer.

O-Ton Schmeh
Das größte Problem ist einfach, dass ein Großteil von dem, was über das Internet verschickt wird, schlichtweg nicht verschlüsselt wird. Etwa vier Prozent aller E-Mails werden heutzutage verschlüsselt.

Autorin
Dabei wäre es ein Leichtes, Kryptographie etwa im Schulunterricht zu fördern. Ich frage beim Bundesamt für Sicherheit in der Informationstechnologie nach. Zunächst erhielt ich gar keine Antwort und auf weitere Nachfrage:

Zitator
Leider können wir Ihnen derzeit keinen passenden Ansprechpartner des BSI vermitteln. Mit freundlichen Grüßen

Musik

Autorin:
Zweifellos lässt die NSA nach wie vor Kohorten von brillanten Mathematikern an der Lösung kryptographischer Probleme tüfteln. Doch erst nach Edward Snowdens Enthüllungen wurde in vollem Umfang klar, dass die NSA längst mit aller Kraft und Macht andere Wege geht. Stefan Krempl:

O-Ton Krempl
Die Erkenntnis war eben, wie stark die NSA oder ihre Vertreter in einzelnen Gremien, also auch in technischen Gremien, in Standardisierungsgremien, vor allem arbeiten, mitarbeiten und da gezielt die Standard-Entwicklung beeinflussen so dass diese theoretisch sicheren Verschlüsselungsstandards doch praktisch unterlaufen werden können.

O-Ton Schmeh

Bei der NSA hat es immer wieder Geschichten gegeben. Die NSA hat schon vor 40 Jahren, als das erste Verschlüsselungsverfahren standardisiert wurde, da haben die mitgemischt und haben da irgendwelche Sachen reingebracht, von denen keiner verstanden hat, warum, und die haben dafür gesorgt, dass der Schlüssel bekannt bleibt. Und so ging es. Immer wieder hat die NSA undurchsichtige Sachen getrieben, bei denen man halt den Eindruck gewinnen musste, die wollen verhindern, dass richtige Verschlüsselung eingesetzt wird. (…) Die Snowden-Affäre hatte in erster Linie den Effekt, dass mal öffentlich wurde, was aber die Experten schon lange wussten. Ich weiß noch, wenn ich vor zehn Jahren jemand was von der NSA erzählt habe, da wusste keiner, wer das überhaupt ist. Obwohl in der Kryptographieszene wusste es jeder, aber nicht in der Allgemeinheit. Wenn ich jetzt sage, die NSA dies und jenes, dann weiß sofort jeder, wer die NSA ist. (…) Und auch, dass die NSA im großem Stil spioniert, das wusste man früher auch schon, wenn man sich auskannte.

O-Ton Krempl

Man hatte da auch immer schon wieder ein paar Hinweise durchaus immer mal gehabt. Also bei Microsoft hat sich ja eines Tages eine Hintertür gefunden im Betriebssystem, die auch noch mit NSA bezeichnet war. Also da war so eine Art Nachschlüssel direkt im Betriebssystem drin. Da hatte man natürlich immer schon mal gedacht: Für was ist der wohl da? (…) Wie stark die Zusammenarbeit ist, auch mit Technologiefirmen und dass da auch Gelder geflossen sind in Richtung Verschlüsselungsfirmen, das hat man so nicht gewusst.

Autorin:

Erst kürzlich trat wieder ein Fall zu Tage.

O-Ton Weis

Der Elliptic Curve Deterministic Random Bit Generator – echt aufregend – also der kam 2006 oder 2007 raus und das war eine Konstruktion, da habe ich gedacht, ne das musst du dir nicht angucken.

Autorin:
Informatik-Professor Rüdiger Weis hat sich mit den Zufallsgeneratoren befasst, die Schlüssel nach einem Zufallsprinzip erzeugen.

O-Ton Weis
Es war hundert Mal langsamer als alle anderen Generatoren, und es war so ein großes Schild auf der Rückseite: Hier könnte eine Backdoor sein. Man kann sich vorstellen, man will einen Kleinwagen kaufen und kriegt dann einen Kleinwagen, wo eine riesige Stahltür auf der Rückseite ist, die dazu führt, dass der ganze Wagen total langsam fährt, und da ist ein Schlüsselloch drin. Und dann sagt man: Den Schlüssel haben wir nicht. Das Schlüsselloch ist nur so da.

Autorin:
Natürlich war da ein Hintertürchen eingebaut. Der Skandal flog auf, die Verantwortlichen gelobten Besserung, doch dann …

O-Ton Weis
… am 20. Dezember 2013: Bei RSA Security Inc. ist es in diesem Safe-Toolkit und dem Protectionmanager – ist der eingebaut und zwar als default. Nach Snowden wissen wir, dass da zehn Millionen Dollar geflossen sind.

Autorin:
Prinzipiell kann die NSA etwa die US-amerikanischen Provider zur Herausgabe sämtlicher Daten verpflichten. Jeder öffentliche Widerspruch – von Widerstand ganz zu schweigen – wird in nicht-öffentlichen Verfahren strafrechtlich verfolgt. Das bedeutet nichts Geringeres als die Preisgabe elementarer rechtsstaatlicher Prinzipien. Diese Zustände betreffen auch Deutsche, wenn sie mit einem US-amerikanischen Provider oder sozialem Netzwerk wie Google, Microsoft oder Facebook ins Netz gehen.
Doch durch die Methoden der NSA ist die Kryptographie keineswegs überflüssig geworden. Durch Verschlüsselung entzieht man sich zunächst den laufenden Überwa-

chungsroutinen, und man muss erst zum Ziel eines sogenannten maßgeschneiderten Zugriffs gemacht werden – einer aufwändigen tailored access operation.

O-Ton Selzer
Wir müssen davon ausgehen, wenn jemand gezielt was gegen mich vorhat, dann wird er das auf einem Niveau machen, gegen das ich nicht allzu viel ausrichten kann.

O-Ton Schmeh
Also den hundertprozentigen Schutz gibt es nicht vor der NSA, die können halt sehr viel. Und man kann es auch nicht einschätzen, was sie alles können. Aber man kann eben eine Menge tun. D.h. wenn man die richtigen Verschlüsselungsprogramme verwendet, die es so gibt, wenn man Verschlüsselung überhaupt anwendet, dann kann man der NSA das Leben ganz schön schwer machen.

Autorin:
Die Einfallstore, die Geheimdienste sich offen halten, dienen keineswegs nur der Staatsicherheit, durch sie können auch Hacker, Kriminelle und Terroristen in Systeme eindringen und unvorstellbaren Schaden anrichten. Wer in so komplexe Systeme wie die Flugsicherung, Kernkraftwerke oder Verkehrsleitsysteme eindringt, kann unter Umständen ganze Städte, wenn nicht das ganze Land lahm legen, sagt der IT-Experte deutscher Geheimdienste, Michael George:

O-Ton Michael George
Es wird nicht mehr funktionieren, dass wir uns schützen, indem wir uns vor einzelnen Angreifern versuchen zu schützen, sondern wir müssen dahin kommen, dass wir die Systeme oder die Daten, die uns wichtig sind vor den Angriffen immunisieren. Es ist völlig egal, wer versucht, mein Handy anzugreifen, ob es ein anderes Land ist, ob das ein Konkurrent oder ein Privatmann. Wir müssen das Gerät oder die Information immunisieren durch Verschlüsselung, durch bessere Technik. So rum muss man das Thema angehen und nicht versuchen, sich gegen einzelne Personen oder Organisationen zu schützen.

Autorin:
Und offenbar verhallt der Apell von Michael George auch in den eigenen Reihen. Anfang November 2014 berichtete *der Spiegel* über ein geheimes Projekt des Bundesnachrichtendienstes mit dem Codenamen „Nitidezza“. Nitidezza ist italienisch und bedeutet „Bildschärfe“. Es geht darum, Wissen über Schwachstellen in Computerprogrammen aufzukaufen, nicht etwa um die Sicherheitslücken zu schließen, sondern um sie für eigene Zwecke zu benutzen. Ausdrücklich ins Visier scheint der BND dabei die Verschlüsselung der Banken zu nehmen, mit denen Banken und ihre Kunden Geschäfte online abwickeln.

Bleibt die Frage: Haben die Enthüllungen Edward Snowdens den Frontverlauf des gerade laufenden cryptowar 2.0 verschoben? Rüdiger Weis überbringt die gute Nachricht:

O-Ton Weis
Die wissenschaftlich starke Kryptographie hält. Die scheint auch durch die NSA nicht brechbar zu sein. Für die Menge an Mitteln und Mathematikern, die die NSA auf die Krypto draufschmeißt, sind die Ergebnisse – bis auf zwei oder drei Stellen – nicht besonders beeindruckend. Bruce Schneier hat es irgendwie schöner und wahrscheinlich treffender zusammengefasst: „Vertrau der Mathematik. Verschlüsselung ist dein Freund.“ Als Hacker möchten wir anmerken: aber möglicherweise einer der wenigen übrig gebliebenen Freunde, die wir haben.

O-Ton Schmeh
Die Verfahren, die man braucht, waren schon vorher bekannt (…) Ich wusste jetzt nicht, dass die NSA das Handy von Angela Merkel abgehört hat, aber wundern tut es mich nicht, weil technisch ist es möglich und warum sollte die NSA das nicht tun, wenn sie es kann? Und Skrupel haben die keine in der Hinsicht. Das war uns schon bekannt. (….)Die Sicherheitsverantwortlichen im Unternehmen, die wussten das auch schon vorher. Es ist nicht so, dass die jetzt hier anrufen und sagen: Hilfe, wir sind völlig überrascht! Kommen Sie! Sondern es ist eher so, dass die hier anrufen und sagen, endlich mal hat mein Chef eingesehen, dass wir da etwas tun müssen.

O-Ton Selzer
Ich glaube gar nicht mal, dass wir mit Gesetzen großartig was bewirken können. Ich glaube z. B. nicht, dass wenn wir jetzt ein Antiüberwachungsgesetz auf den Weg brächten, dass wir damit eine Chance hätten, damit das Rad der Geschichte zurückzudrehen. Ich glaube, wir müssen eine gesellschaftliche Veränderung erreichen. Das hört sich jetzt unfassbar naiv an. Ist es auch. (…) Aber ich glaube z. B. nicht, dass wenn wir jetzt die Y-Partei wählen, und die macht sich total stark für Datenschutz, dass, wir dann morgen in einem freien und gerechten Land aufwachen. Sondern ich glaube, was wir brauchen - da muss man eben noch sehr, sehr lang dran arbeiten - wir brauchen den gesellschaftlichen Umschwung, dass Überwachung einfach als Mittel geächtet wird, dass es sich nicht gehört, anderen Leuten zuzugucken sie Sachen machen, die andere Leute nichts angehen.

Autorin
Und eine Gesellschaft, die das Grundrecht auf Schutz der Privatsphäre kampflos preisgibt, verrät alles über ihre innere Verfassung – so sieht es der Schriftsteller Ilja Trojanow:

O-Ton Trojanow
Ich glaube, dass wir einem grundsätzlichen Irrtum aufgesessen sind. Wir bilden uns ein, dass es irgendwelche Strukturen und Mechanismen und Sicherheiten gibt, die eine Gesellschaft per se demokratisch machen. D. h. der demokratische Bürger kann sich irgendwie zurücklehnen und ein gewisses Maß an Freiheit ist gesichert. Das ist völlig falsch. Ein jeder von uns muss tagtäglich sich immer wieder seine Freiheiten neu erkämpfen oder verteidigen. Und wer das nicht tut – und das ist eine der schockierendsten aber auch wichtigsten Erkenntnisse aus den Reaktionen der letzten sechszehn Monate –, der offenbart, dass er eigentlich tief in seinem Herzen Freiheit nicht wirklich wertschätzt und in seiner Verfasstheit eher einem Untertan ähnelt. Das merke ich ja auch immer wieder in Diskussionen, dass Menschen offensichtlich nichts dabei finden, dass es überhaupt keine menschliche Würde geben kann ohne Privatsphäre.

Absage

Crypto wars oder

Die Freiheit im Netz

Ein Dossier von Walter van Rossum.

Sie hörten eine Produktion des Deutschlandfunks 2014.

Es sprachen: Marietta Bürger und Jochen Langner

Ton und Technik: Wolfgang Rixius und Beate Braun

Regie und Redaktion: Karin Beindorff