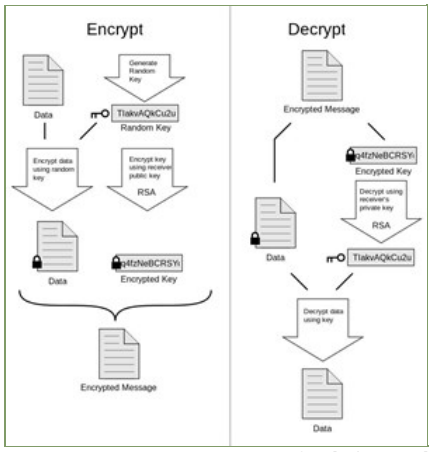


foto: [cc;by-sa; 3.0]
Wie PGP funktioniert: Zum Vergrößern klicken, Grafik: Wikimedia/xaedes & jfreax & Acdx

foto: [cc; by-sa; 4.0]
GnuPG-Erfinder Werner Koch...

foto: picture alliance/schönherr
... und PGP-Erfinder Phil Zimmermann waren sich oft uneins, kämpften aber für dasselbe

## PGP, Gnu PG: Wie ein ungleiches Duo das Postgeheimnis beschützt

FABIAN SCHMID
27. Juni 2015, 09:00

**Phil Zimmermann und Werner Koch haben die zwei wichtigsten Verschlüsselungstools entwickelt – und früher heftig miteinander gestritten.**

Jene Männer, die in den vergangenen Jahrzehnten wohl am meisten zum Schutz der Privatsphäre beigetragen haben, könnten ungleicher nicht sein.

Da wäre einerseits Phil Zimmermann: ein 61-jähriger Friedensaktivist, Informatiker und Geschäftsmann, der nie um einen Scherz verlegen ist. "Seid vorsichtig, was ihr jetzt sagt", witzelte der US-Amerikaner unlängst in Wien, als bei einer Podiumsdiskussion die Teilnehmer verkabelt wurden. Die Universität Wien hatte aus Anlass von 25 Jahren Internet in Österreich zu einer Debatte über Privatsphäre geladen, die Zimmermann mit seiner Präsenz dominierte – und dabei kräftig gegen Geheimdienste und datensammelnde Konzerne austeilte.

**Im Kampf gegen die NSA**

Der andere Teil des ungleichen Duos lebt zurückgezogen in Düsseldorf und sieht laut taz aus "wie ein deutscher Familienvater: kleiner Bauchansatz, Jeans, Hemd, kein bisschen modisch". Doch Werner Koch gilt als jener Entwickler, der mit dem Verschlüsselungsstandard GnuPG sogar die mächtige NSA vor große Probleme stellt. Das hatten Filmemacherin Laura Poitras und Aktivist Jacob Appelbaum Anfang 2015 anhand von Snowden-Dokumenten enthüllt. Bei einer Rede beim Hackerkongress 31C3 in Hamburg bedankten sie sich öffentlich bei Koch, der im Publikum anwesend war. Die restlichen Zuhörer – über tausend an der Zahl – erhoben sich, um Koch mit Standing Ovations ihren Respekt zu zeigen.

**Vom Kalten zum Krypto-Krieg**

Den Anfang machte jedoch Zimmermann. 1991 schuf er die Verschlüsselungssoftware "Pretty Good Privacy", die unter der Abkürzung PGP berühmt wurde. Zimmermann war somit der erste Informatiker, der ein kryptografisches Verfahren für Normalverbraucher zugänglich machte. Zuvor hatte sich Zimmermann als Friedensaktivist einen Namen gemacht. In den 1980ern war er in der Anti-Atom-Bewegung aktiv, demonstrierte gegen die nuklearen Drohgebärden der Supermächte USA und Sowjetunion. Nach dem Ende des Kalten Krieges überlegte Zimmermann, welche Entwicklungen nun die Bürgerrechte bedrohen könnten.

**Behörden werden mitlesen**

Fündig wurde er beim Thema Überwachung. Die Infrastruktur des Internets wurde gerade ausgebaut, erstmals hatten auch Privatpersonen Zugang zum WWW. Zimmermann war klar, dass Behörden jederzeit E-Mails abfangen und lesen konnten. Deshalb mussten diese verschlüsselt werden. Das Wundermittel dafür war eben PGP, das relativ einfach funktioniert: Jeder Nutzer hat einen öffentlichen Schlüssel, der ihn eindeutig identifiziert. Der Absender verschlüsselt die Nachricht nun für den öffentlichen Schlüssel. Um die E-Mail dann zu lesen, muss der Empfänger den dazu passenden privaten Schlüssel einsetzen, der passwortgeschützt ist.

Fangen Behörden die Nachricht ab, sehen sie nur eine wirre Kette an Ziffern und Buchstaben. Sie müssen nun den Verschlüsselungsalgorithmus knacken oder sich den privaten Schlüssel des Empfängers besorgen. Im militärischen Bereich

waren solche Vorsichtsmaßnahmen schon lange Usus – was übrigens zur Entwicklung des Computers geführt hatte: Denn Alan Turing hatte in den 1940ern vom britischen Geheimdienst die Aufgabe erhalten, den Enigma-Code der Nazis zu knacken. Das war nur mittels neuer Rechenmaschinen möglich.

**Exportverbot für Software**

Aufgrund dieser militärischen Logik nahmen dann auch US-Behörden die Fährte von Zimmermann auf: Er durfte den Programmcode von PGP nicht exportieren, da es sich um ein Rüstungsgut handle, beschied ihm das FBI. Zimmermann trickste die Behörden aus, indem er den Code einfach in gedruckter Form zur Verfügung stellte.

1997 wurde PGP dann vom Antiviren-Hersteller McAfee gekauft. Ein Schritt, der Zimmermann heftige Kritik einbrachte – und Koch indirekt dazu brachte, GnuPG zu entwickeln. Inspiriert von der Bewegung für Freie Software und deren Ikone Richard Stallmann, machte sich Koch daran, eine offene Alternative zum jetzt in der Konzernwelt beheimateten PGP zu schaffen.

**Spenden für Privatsphäre**

Eine Aufgabe, die ihn nicht mehr losließ: Seit 1997 widmet Koch den Großteil seiner Zeit GnuPG. Mehr als 16 Jahre war er auf Spenden angewiesen: "Anfang 2013 hatte ich fest geplant, die Sache aufzugeben, nach den Snowden-Enthüllungen im Juni konnte ich das aber nicht mehr machen."

Durch das große Lob von Poitras, Snowden und Co konnte Koch nun genug Geld auf die Beine stellen, um GnuPG sorgenfrei weiterentwickeln zu können. Zimmermann hat indes eine neue Firma namens Silent Circle, mit der er abhörsichere Telefonate ermöglichen will. Die Pioniere der Verschlüsselung: Sie kämpfen weiter für unsere Privatsphäre. (Fabian Schmid, 27.6.2015)

**Links:**
GNU PG

PGP

Silent Circle

**Nachlese:**
Gnu-PG-Erfinder Werner Koch: "War kurz vorm Aufgeben"

**Weiterlesen:**

Schwerpunkt "Die überwachten Bürger"



. . . . .