Philip Zimmermann: Der König der Verschlüsselung über seine Ängste um die Privatsphäre

Der Erfinder von *PGP* hat seine Firma *Silent Circle*, die mobile Verschlüsselungssysteme entwickelt, in die Schweiz verlegt, um frei von der US-amerikanischen Massenüberwachung zu sein. Hier erzählt er warum.

Als Philip Zimmermann in den Achtzigern eine Kampagne für nukleare Abrüstung startete, hielt er einen Fluchtplan in der Hinterhand. Der Erfinder des auf der Welt meist verbreiteten Email-Verschlüsselungssystems *Pretty Good Privacy* (besser bekannt als *PGP*) war bereit, beim kleinsten Anflug einer Gefahr mit seiner Familie von Colorado nach Neuseeland zu ziehen.

Der „Rote Knopf" wurde jedoch nie gedrückt und die Zimmermanns blieben an Ort und Stelle. Bis dieses Jahr: Mit 61 Jahren hat der Neueinzug in die *Internet Hall of Fame* und Gründer des drei Jahre alten Verschlüsselungs-Startup-Unternehmens *Silent Circle* die USA in Richtung Schweiz verlassen. Am Ende war es nicht die nukleare Bedrohung, die ihn davon überzeugte, sein Heimatland zu verlassen, sondern der Überwachungs-Rüstungswettlauf.

„Jede dystopische Gesellschaft hat ein überbordenden Überwachungssystem, aber jetzt sehen wir, dass selbst westliche Demokratien wie die USA und England sich dahin bewegen", warnt er. „Wir müssen das zurückfahren. Über die Leute, die nicht verdächtigt werden, ein Verbrechen zu begehen, sollten keine Informationen gesammelt und in Datenbanken gespeichert werden. Wir wollen nicht wie Nordkorea werden."

Zimmermann legte einen Zwischenstop in London ein, um einen Empfang im Victoria & Albert Museum auszurichten, in dem sein kryptographisches Handset, das *Blackphone*, derzeit ausgestellt wird, zusammen mit den Überresten des Laptops, der auf Regierungsbefehl von Guardian-Redakteuren mit Winkelschleifern zerstört wurde, weil er eine Menge an geheimen Dokumenten enthielt, die durch Edward Snowden enthüllt worden waren.

Zimmermann und Snowden sind vom Alter her 30 Jahre auseinander, aber ihre Aktionen sind fester Bestandteil der Debatte über die Privatsphäre. Zimmermann wechselte 1991 von einer Kampagne gegen Nuklearwaffen zu einer gegen die „Rumschnüffelei" des Staates, als er *PGP* in einem Anflug von politischem Aktionismus kostenlos zur Verfügung stellte. Sein Protest half, eine Gesetzgebung zu verhindern, die Software-Firmen gezwungen hätte, „Hintertürchen" in ihre Produkte einzubauen, um der Regierung zu ermöglichen, verschlüsselte Nachrichten zu lesen.

Die Gebrauchsanweisung für *PGP* wurde von Zimmermann 1991 geschrieben und sieben Jahre später aktualisiert. Sie ist eine erschreckend genaue Vorhersage der Massenüberwachungsmethoden, die letztlich von der NSA nach dem 11. September 2001 übernommen wurden.

Darin steht: „Heute kann eine E-Mail ganz leicht und unbemerkt automatisch nach interessanten Schlüsselbegriffen durchsucht werden. Das ist wie großangelegtes Fischen mit einem Treibnetz."

Es sollte jedoch noch 20 Jahre dauern, bevor Snowdens Enthüllungen diese Bedenken ins Licht einer breiten weltweiten Aufmerksamkeit rückten. Aber als der ehemalige NSA-Mitarbeiter den Kontakt zu Journalisten suchte, die ihm helfen sollten, seine Geheimnisse zu lüften, benutzte er *PGP*.

Keine Kundennummern wurden veröffentlicht, aber das Gemurmel unter gut informierten Risiko-Kapital-Anlegern lässt verlauten, dass *Silent Circle* schnell wächst. Zu Beginn des Jahres stieg sein Wert nach einer zweiten Sponsoren-Welle auf 50 Millionen Dollar. Seine Geldgeber sind u.a. Ross Perot Junior, der Sohn des US-Präsidentschaftskandidaten von 1992.

Das Geheimnis von *PGP*

Philip Zimmermanns eigenes Leben ist ein Beispiel dafür, was mit denen passieren kann, die die Fähigkeiten der USA, Informationen zu sammeln, bekämpfen.

Geboren ist er in New Jersey und aufgewachsen in Florida. Sein Vater war ein Zementlastwagenfahrer. Niemand erwartete, dass er auf eine Universität gehen würde. Aber der Junge wollte Astronom werden. „Meine Familie war arm. Manchmal hatten wir nicht einmal ein Zuhause, also ging ich auf viele verschiedene Schulen. Als ich dann aufs College ging, wurde ich endlich sesshaft."

Die *Florida Atlantic University* besaß keinen Zentralcomputer. Ihre Terminals, manche mit Lochkarten anstelle von Bildschirmen, waren über Telefonleitungen mit Miami verbunden. Zimmermann schrieb sein erstes Programm, welches dem Computer beibrachte, seinen Namen zu lernen. „Etwas war ziemlich cool an dem Geist in der Maschine. Der Computer war eine Maschine, die auf Menschen reagieren konnte."

In den Achtzigern war er dann nach Boulder in Colorado gezogen und arbeitete als IT-Berater, verbrachte aber auch 40 Stunden pro Woche als Friedensaktivist. 1984 traf er den bekannten Astronom Carl Sagan, den Schauspieler Martin Scheen und den „Pentagon-Whistleblower" Daniel Ellsberg in einem Gefängnis. Sie wurden verhaftet, nachdem sie in ein Atomwaffen-Testgelände eingebrochen waren.

Im April 1991, nach dem Golfkrieg, wurde die *coding community* auf einen Satz im Anti-Terror-Senatsbeschluss 266 aufmerksam. Dieser erlaubte der Regierung, „Abschriften" von Stimmen, Dateien und anderen Konversationen zu erstellen, „wenn dies durch das Gesetz legitimiert worden ist".

Zimmermann hatte danach *PGP* in seiner Freizeit entwickelt und stimmte der Veröffentlichung seines Quellkodes im Juni des Jahres zu. Es gab die Hoffnung, dass das neue Gesetz unnütz werden würde, wenn genug Amerikaner begännen, ihre E-Mails so zu schützen, wie Briefe durch Briefumschläge geschützt werden.

PGP stellt jedem Benutzer ein Paar Kodes zur Verfügung, einen öffentlichen und einen privaten. Die Benutzer teilen ihre öffentlichen Kodes, aber jede Nachricht, die an die geht, die sie benutzen, kann nur mit dem privaten Kode entschlüsselt werden. Es gibt keine zentrale Datenbank an privaten Kodes, die so Spionage erleichtern würde.

Der Ingenieur Kelly Goen begann, Kopien von *PGP* an Hauptcomputer zu verteilen. Da er aber eine gerichtliche Anordnung befürchten musste, setzte er dies mit äußerster Vorsicht um. Anstatt von zu Hause aus zu arbeiten, fuhr er mit einem Laptop, einem akustischen Koppler und einem Handy entlang der Küste San Franciscos hin und her. Er stoppte dann an einer Telefonzelle, lud seine Daten für einige Minuten hoch und fuhr zum nächsten Telefon, nachdem er sich ausgeklinkt hatte.

Goens Uploads wurden durch die Behörden gestoppt, aber *PGP* begann, sich immer weiter auszubreiten. Der umstrittene Satz wurde letztlich aus Beschluss 266 gestrichen, jedoch bekam Zimmermann im Februar 1993 Besuch von zwei Zollbeamten. Die Regierung verfolgte ihn anscheinend aufgrund von Export von „Waffen". Nach damaligem US-Recht galten komplexe Verschlüsselungssysteme als Waffen und gegen Zimmermann wurde drei Jahre lang ermittelt, bis die Vorwürfe fallen gelassen wurden.

Heute sind seine größten Sorgen nicht die „Hintertürchen" in Programmen, sondern die Petabytes (eine Million Gigabytes) an Informationen, die von solchen wie *Google* und *Facebook* gehortet werden. „Wenn man alle diese Daten sammelt, wird daraus eine verlockende Falle. Es ist die Art Sirene, die dich anlockt, um sie zu gewinnen. Die Regierungen denken sich also: Wenn die Industrie das kann, warum sollten es unsere Geheimdienste dann nicht auch können?"

Am Ende des Interviews beantwortet Zimmermann die Frage in einem kurzen Video: „Ein gewisses Maß an Aufwand muss bei der Polizeiarbeit bestehen bleiben. Wenn es zu reibungslos zugeht, endet man viel zu leicht in einem Polizeistaat. Ich denke, wir sollten ein bisschen von dieser Reibung bewahren."

Bevor er diese Botschaft aufnahm, hatte er sein Firmenlabel am Revers entfernt. Zimmermann hofft, Geld zu machen, aber hätte es den Vater der E-Mail-Verschlüsselung nicht gegeben, würde die Politik noch immer die Privatunternehmen übertrumpfen.