# 2013/03 Lifestyle

https://shop.jungle.world/artikel/2013/03/im-stillen-kreis

**Die neue Verschlüsselungstechnik Silent Circle**

# Im stillen Kreis

Von **Boris Mayer**

**Eine neue Verschlüsselungstechnik soll es jeder Person ermöglichen, sicher zu kommunizieren. Umsonst gibt es das nicht.**

Ob sich der ehemalige Chef der CIA, David Petraeus, noch heute darüber ärgert, keinerlei Vorkehrungen zum Schutz seiner privaten E-Mail-Korrespondenz getroffen zu haben, ist nicht bekannt – aber unwahrscheinlich ist es nicht, zumal der Geheimdienstler ja durchaus hätte wissen müssen, wie einfach unverschlüsselte Nachrichten von Dritten gelesen werden können. In der Diskussion um die Petraeus-Affäre hatten Bürgerrechtler zudem immer wieder verlangt, dass das Verhalten des FBI in der Affäre genauestens überprüft werden müsse. Anthony Romero von der American Civil Liberties Union sagte beispielsweise der New York Times: »Nicht das persönliche Verhalten von General Petraeus und General Allen sollte untersucht werden, sondern welche Überwachungsmethoden vom FBI angewendet wurden, um ihre Privatleben zu durchleuchten.«
Für einen Unternehmer kam diese Diskussion definitiv zur rechten Zeit: Phil Zimmermann, ein Vorreiter in Sachen Kommunikationsverschlüsselung, will unter dem Namen Silent Circle mit seinen Partnern die Kryptographie von morgen für jeden anbieten – gegen einen monatlichen Mitgliedsbeitrag.

Als Zimmermann vor 20 Jahren Pretty Good Privacy (PGP) erschuf, war es sein Ziel, starke Verschlüsselung jeder und jedem, insbesondere aber Bürgerbewegungen, zur Verfügung zu stellen. Deshalb konnten alle das Programm kostenlos herunterladen und es benutzen, um sich vor dem Zugriff von Geheimdiensten oder anderen interessierten Dritten zu schützen. Zimmermann stellte es auf einen öffentlichen FTP-Server, auf den jede Person im damaligen Internet zugreifen konnte. Aber weil PGP bei der ersten Veröffentlichung schon so fortgeschritten war, fiel es unter das Waffenexportgesetz der USA – ein Export als Software war damit ausgeschlossen. Zimmermann, selbst Anti-Atomkraft-Aktivist, war aber sehr viel daran gelegen, dass auch außerhalb der USA Menschen auf elektronischem Weg kommunizieren können, und so kam es zu einer der Kuriositäten der IT-Geschichte: Zimmermann ließ den Quellcode von PGP als Buch drucken, weil er in gedruckter Form

nicht mehr unter die Exportbeschränkung fiel. Das Buch »PGP Source Code and Internals« wurde dann außerhalb der USA wiederum von mehr als 60 Freiwilligen abgetippt und daraus dann eine internationale Version von PGP erstellt. PGP ist heute immer noch der Standard, wenn es um das Signieren von E-Mails oder Websites, also die digitale Unterschrift, oder um Verschlüsselung geht. Es wird weltweit in Unternehmen eingesetzt und von vielen Privatpersonen genutzt, auch wenn es immer noch die eine oder andere Hürde bei der Einrichtung gibt, insbesondere die, den initialen Schlüsseltausch sicher zu gestalten.
In den folgenden Jahren beschäftigte sich Zimmermann mit verschlüsselter Telefonie. Das Programm PGPfone, das zwar den gleichen Namensbestandteil trägt, mit der Technik von PGP aber nichts gemeinsam hat, war seiner Zeit zu weit voraus: 1995 steckte IP-Telefonie noch unstandardisiert in den Kinderschuhen und war wegen der mangelnden Bandbreite der Internetanschlüsse nur für einen kleinen Nutzerkreis überhaupt verfügbar. So konnte es keine große Fangemeinde erschließen. Und auch der Nachfolger Zfone, beruhend auf den Ideen von PGPfone, aber mit moderner IP-Telefonie-Technik, konnte in den Jahren zwischen 2006 bis zur Einstellung der Entwicklung 2009 nicht genügend Interesse wecken. Gemeinsam hatten diese Lösungen allesamt, dass nur die Software zum Download bereitgestellt wurde. Bei Produkten für verschlüsselte Kommunikation ist das ein Problem, weil man nicht nur selbst ein Programm herunterladen, installieren und einrichten, sondern auch den jeweiligen Kommunikationspartner davon überzeugen muss, dies ebenfalls zu tun. Dazu müssen gegebenenfalls noch die Schlüssel sicher ausgetauscht werden und man muss sich immer darum kümmern, die Produkte auch korrekt einzusetzen. Das ist nicht ganz einfach, wie man im Fall des abgedruckten Passworts für eine Datei von Wikileaks in David Leighs Buch gut erkennen konnte, bei dem sich beide Seiten den Vorwurf gefallen lassen müssen, geschlampt zu haben.

Mit Silent Circle sollen solche Probleme nicht mehr bestehen. Der Dienst stellt für die Vermittlung von IP-Telefonaten, Textnachrichten, Videoübertragungen und E-Mails die Infrastruktur für das Aufnehmen der Verbindung zur Verfügung. Wer sich dort registriert und bezahlt, bekommt eine Silent-Circle-Nummer zugeordnet, unter der man dann erreichbar ist. Silent Circle zufolge ist dafür ein sehr stark gesicherter Serverpark notwendig und so etwas kostet deutlich mehr Geld, als eine Datei zum Download anzubieten. Zimmermann und seine Partner hoffen, dass die Hürde eines Mitgliedbeitrags von 20 US-Dollar im Monat niedriger ist als die, sich auf eigene Faust mit Verschlüsselungstechnik und dem richtigen Umgang mit privaten Schlüsseln und dem Austauschen von öffentlichen Schlüsseln zu beschäftigen. Deswegen sollen dann auch mehr Menschen verschlüsselte Kommunikation nutzen und nicht länger den Betreibern von Facebook, Yahoo oder einfach nur der Netzinfrastruktur wie den Internetanbietern – oder gar den Geheimdiensten – ermöglichen, jede noch so private Kommunikation mitzuhören oder mitzulesen.
»Ich werde mich nicht dafür entschuldigen, dass der Dienst Geld kostet. Das ist nicht Facebook. Unsere Kunden sind Kunden und nicht Produkte. (…) Sichere Kommunikation ist in einer freien Gesellschaft jedermanns Recht«, verteidigte Zimmermann sein Geschäftsmodell. »Man sollte in der Lage sein, einem Freund etwas ins Ohr zu flüstern, auch wenn sein Ohr tausend Meilen weit entfernt ist.« Zur Zeit gibt es Silent Circle aber nur für iOS, ein iPhone oder iPad sind also Voraussetzung, eine Version für Android soll es

erst in einigen Monaten geben. Die Versionen von Windows und Mac sollen dann später folgen, denn Silent Circle wird für Computer erst angeboten, wenn die Beta-Phase abgeschlossen ist. Aber wenn beide Gesprächspartner mit Apple mobil unterwegs sind, steht der sicheren Kommunikation schon jetzt nichts im Weg – bis auf eben jene 20 US-Dollar für alle, die am stillen Kreis teilnehmen wollen. Und wenn dann jemand trotzdem nicht will, kann man dem Verweigerer einen Schnuppermonat schenken, eine Geschenkkarte gibt es nämlich auch.

Das passt zum Geschäftsimage, das sich das Unternehmen geben möchte. Denn Zimmermann ist zwar das bekannte Aushängeschild von Silent Circle, aber nicht der Einzige mit einschlägiger Erfahrung. »Das Team von Silent Circle besteht aus ehemaligen Experten der U.S. Navy Seals, der Britischen Special Forces und Internetverschlüsselungsexperten, die zusammengekommen sind, um ein einmaliges Produkt und Angebot in Sachen privater Kommunikation von Menschen überall auf der Welt absolut sicher und ohne Hintertüren zu schaffen«, sagte CEO Mike Janke. Mit dabei ist als Technischer Leiter Jon Callas, der schon an der Entwicklung vieler Sicherheitsprodukte beteiligt war, wie zum Beispiel der Festplattenverschlüsselung von Apples OS X oder des PGP Universal Server. Dazu kommen noch der eine oder andere White Hat Hacker und Benutzerschnittstellenexperten. »Wir wollen nichts zu geeky machen«, so Janke, der damit die intuitive Benutzbarkeit ohne Fachwissen als ein wichtiges Ziel von Silent Circle hervorhebt. »Sicherheitsvorkehrungen werden oftmals dadurch unterwandert, dass sie nicht verstanden und damit nicht beachtet oder als Produktivitätsbremsen absichtlich umgangen werden, wie viele frustrierte IT-Manager sicher bestätigen können.« Deshalb sollen sich die Silent-Circle-Apps auf den verschiedenen Plattformen nahtlos in deren Nutzungskonzept einfügen. Nutzer sollen sie genau so bedienen, »wie sie es eben gewohnt sind«, sagte Janke und gibt damit die Erklärung dafür, warum es dauert, die App auf die unterschiedlichen Geräte zu portieren.