SCHAFFT DIE E-MAIL AB!

Internet Jacob Appelbaum ist Computersicherheitsexperte, Hacker und einer der wichtigsten Mitglieder des Tor-Projekts. Als einer der Ersten bekam er die brisanten Informationen von Edward Snowden zu sehen. Appelbaum wurde mehrfach von den US-Behörden kontrolliert und verhört. Er lebt in Berlin, weil er sich in den USA nicht mehr sicher fühlt.

Foto: Jens Gyarmaty/Visum

Derzeit haben Firmen und die US-Regierung zu großen Einfluss auf vitale Teile des Internets. Das müssen wir ändern. Dafür brauchen wir nicht das alte System vollständig aufzugeben, aber wir müssen es erweitern, um es widerstandsfähiger zu machen und jene Privatheit, Diskretion und Integrität zu ermöglichen, die wir offensichtlich nicht hatten.

Wir müssen das Internet dezentralisieren, beispielsweise mit Peer-to-Peer-Netzwerken. Dort verteilen wir die Verantwortung darüber, wer Inhalte veröffentlichen kann. Es gibt Bestrebungen in diese Richtung. Zum Beispiel das New.net oder das alternative Namensverzeichnis GNS des GNUnets. Auch das Tor-Netzwerk ist ein Versuch, das Netz zu dezentralisieren.

Und wir müssen die E-Mail abschaffen! Zurzeit ist es für die NSA einfach, sie abzufangen. Jede E-Mail, selbst wenn sie innerhalb eines Landes verschickt wird, läuft über einige wenige Knotenpunkte. Diese Technologie ist nicht gut genug. Nachrichten, die auf Servern eines Providers warten, von mir abgerufen zu werden – das ist Privatsphäre auf dem Niveau des 19. Jahrhunderts.

Das Verschlüsselungsverfahren PGP ist leider keine Alternative, weil es nicht hundertprozentig sicher und zudem ein Albtraum in Sachen Benutzerfreundlichkeit ist. Besser sind Initiativen, um die E-Mail ganz abzuschaffen: das Projekt „Pond" des Google-Sicherheitsexperten Adam Langley beispielsweise. Es gibt auch schon sichere Messenger. Ich selbst arbeite mit am Off-the-Record-Messaging *(ein Verschlüsselungsprotokoll für Instant Messenger; d. Red)*. Man kann auch via Voice over IP bereits jetzt nutzerfreundlich und verschlüsselt telefonieren.

Verschlüsselung schützt unsere Privatheit. Ich glaube nicht, dass es der NSA gelingen wird, unsere besten Verschlüsselungssysteme zu knacken. Die Mathematik ist zu gut. Doch es gibt noch ungelöste Probleme: End-to-End-Verschlüsselung muss Folgenlosigkeit bieten. Es dürfen also nicht alle vorhergehenden oder nachfolgenden Schlüssel automatisch wertlos werden, wenn ein einziger geknackt wurde. Und es muss uns gelingen, unsere Metadaten zu schützen *(die anzeigen, wer wann mit wem kommuniziert hat; d. Red.)*.

Zugegeben, das ist alles technisch sehr anspruchsvoll. Wer wird uns künftig die sicheren Kommunikationstools programmieren? Die Hacker? Auf irgendjemanden muss man seine Hoffnungen setzen – warum nicht auf die Hacker-Gemeinschaft? Sie sind motiviert, sichere und nutzerfreundliche Kommunikationsmethoden zu entwerfen. Bei Apple arbeiten viele Menschen, die großartige Designer und zugleich aktive Mitglieder der Computer-Security- und Hacker-Gemeinschaft sind. Leider ist Apple ein Komplize des NSA-Systems. Aber es müsste nicht so sein. Apple könnte auch ein Partner der Menschheit sein.

Was passieren muss: Leute, die gut darin sind, eine Benutzerschnittstelle zu designen, müssen sich mit Leuten zusammentun, die gut darin sind, Verschlüsselung zu programmieren. Ich bin zuversichtlich, dass dies künftig geschehen wird, sodass wir am Ende den Nutzern nur noch eines beibringen müssen: Wie sie sich gegenseitig zuverlässig authentifizieren, bevor sie miteinander sicher kommunizieren können. Der Rest sollte automatisch im Smartphone passieren. Sichere Verschlüsselung muss Standard sein – und zwar in jedem Smartphone. William Gibson sagte einmal: „Die Zukunft ist bereits da, sie ist nur nicht gleichmäßig verteilt." Dass ich ein verschlüsseltes Smartphone habe und viele andere nicht, ist der Beweis.

PROTOKOLL: JENS LUBBADEH