VERSCHLÜSSELUNG IST BÜRGERPFLICHT

Das Internet ist ein Kriegsschauplatz. Wer sich nicht schützt, riskiert auch als Unbeteiligter, etwas abzukriegen. Verschlüsselung ist deshalb das Gebot der Stunde.

Dass Datenkrieg herrscht, dürfte nach der PRISM-Affäre jedermann klar sein. Man hätte es schon anfangs der 90er Jahren wissen können, als Verschlüsselungssoftwares von den USA noch als «Waffen» behandelt und mit einem Exportverbot belegt wurden. Das Verbot fiel, als der Programmierer Phil Zimmermann den Code seiner «Pretty Good Privacy»-Software als Buch druckte und – geschützt durch die Meinungsfreiheit – exportierte.

Die Logik ist einfach: Wenn Verschlüsselung eine Waffe sein soll, dann muss die Gegenseite auch Waffen haben. Und nachdem sie diese offensichtlich einsetzt, herrscht Krieg.

Plug, play, security: *Mit der Enigma-Box kann man spurenlos surfen, verschlüsselt telefonieren und bis Ende Jahr verschlüsselt e-Mails verschicken.*

Die Gefahr liegt zwar vor allem in den USA, wo die IP-Adressen, mit der jeder Computer identifiziert werden kann, durch die ICANN zugeteilt werden. Diese «Internet Corporation for Assigned Names and Numbers» ist zwar eine non-profit-Organisation, wurde aber 1998 auf Initiative der US-Regierung gegründet, um die Steuerung des ursprünglich militärischen Internet zu übernehmen. Ein weiterer Risikofaktor für Computer-Anwender auf der ganzen Welt ist die Tatsache, dass ein grosser Teil des Internetverkehrs über die USA läuft, wo die Daten von den Geheimdiensten abgesogen werden können. Die wichtigsten Internetkonzerne wurden zur Zusammenarbeit mit den Geheimdiensten verpflichtet. Dank der riesigen Datenbank «XKeyscore» haben Mitarbeiter der NSA ohne Autorisierung aufgrund der IP- oder e-Mail-Adresse Zugang zu e-Mails, Freundeslisten, Passwörtern und dergleichen.

«Nur gegen Zielpersonen» richte sich die Überwachung, beteuerte die National Security Agency im Nachgang zu den Enthüllungen von Edward Snowden. Aber das ist mit Sicherheit gelogen. Potenzielle Terroristen werden gewiss kein Facebook-Profil unterhalten.
Bereits 2007 wurden gemäss veröffentlichten Dokumenten 850 Milliarden Telefon- und 150 Milliarden Internet-Verbindungen überwacht. Mittlerweile dürfte die Zahl ein Mehrfaches betragen. Selbst bei einer unwahrscheinlich hohen Zahl von einer Million Terrorismusverdächtigen, müssten diese täglich 2328 Telefongespräche führen. Wir stehen also alle im Visier, aus welchen Gründen auch immer. Schutz wird zur Bürgerpflicht.

Das sieht auch der Verein Enigma so, der nach zweijähriger Entwicklungsarbeit vor kurzem eine Verschlüsselungsbox mit Telefon auf den Markt gebracht hat. Die Box erlaubt spurenloses Surfen im Internet durch Verwendung des cjdns-Protokolls, indem jeder Nutzer seine eigene IPv6-Adresse generiert. Die von der amerikanischen ICANN verwaltete Vergabe der IP-Adresse, die jeden Computer identifizierbar macht, wird umgangen. Die Enigma-Box erlaubt ferner abhörsicheres Telefonieren – allerdings nur mit anderen Besitzern einer Enigma-Box. Für jede Verbindung wird ein neuer Verschlüsselungscode erstellt, der dann wieder verworfen wird. Ohne Box an der Zieladresse funktioniert das Telefon wie ein normales Internet-Telefon. Allein wenn es als solches verwendet wird, amortisieren sich die Kosten von Fr. 350.– pro Set relativ schnell. Bis Ende Jahr soll dann noch die e-Mail-Verschlüsselung dazu kommen. Ziel der Entwickler war ein in der Schweiz hergestelltes Gerät, das ohne Software-Installation auf der Basis von plug'n'play funktioniert und absolut sicher ist. Wir haben es in der Redaktion installiert – und es funktioniert. *CP*

Weitere Informationen und Bestellung:
enigmabox.net

EIN GESTIEGENES INTERESSE AN VERSCHLÜSSELUNG

stellt auch der Chaos Computer Club Zürich fest. An sogenannten Kryptoparties, die seit Ende Juli regelmässig stattfinden, zeigen Hacker, wie man sich gegen elektronische Überwachung schützt und helfen bei der Installation von Programmen. Termine, Orte und weitere Informationen:
www.ccczh.ch