WIRTSCHAFT

Zürich | vor 11 Std

«Ich verschlüssele immer meine E-Mails»

Die Enthüllungen um die Praktiken der amerikanischen National Security Agency ziehen immer grössere Kreise. Wer seine Daten im Internet schützen will, muss wissen wie. Bernd Fix vom Chaos Computer Club Zürich erklärt Grundlegendes.

Bernd Fix (pd)

Sie senden mir E-Mails mit PGP-Schlüssel. Machen Sie das immer?

Bernd Fix: Gerne hätte ich Ihnen die E-Mails auch verschlüsselt zugeschickt – aber leider haben Sie keine E-Mail-Verschlüsselung. Das erkennt mein
E-Mail-Programm und signiert die E-Mails nur, damit Sie prüfen könnten, ob sie tatsächlich von mir stammen.

Aus welchem Grund?

Verschlüsseln und Signieren sind Standardeinstellungen, die ich in meinem E-Mail-Programm gewählt habe. Ich verschlüssele immer, damit die Tatsache, dass ich verschlüssele, keine Information an sich ist.

Wie verschafft sich eine Organisation wie NSA Zugang zu den Daten?

Das Internet ist nicht so chaotisch aufgebaut, wie sich das die meisten Leute vorstellen, sondern ziemlich hierarchisch. Es gibt Knoten und Verbindungen im Netz, über die sehr viel Netzverkehr läuft – viele davon in den USA: An diesen Knoten hat die NSA sogenannte «Tapping Points», welche die Daten abschnorcheln. Wenn Sie ein E-Mail von Zürich nach Hamburg schicken, kann es durchaus passieren, dass die Daten über die USA geleitet und dort abgehört werden. Alle anderen Daten werden zum Beispiel bei Firmen wie Facebook oder Google abgegriffen – ob mit oder ohne Wissen der jeweiligen Firma, ist dabei egal.

Welches sind die grössten Fehler, die normale Computernutzer begehen?

Naivität und Blauäugigkeit, wenn es um Datenschutz und informationelle Selbstbestimmung geht: Naivität, dass «wer nichts zu verbergen hat, auch nichts zu befürchten hat», und Blauäugigkeit gegenüber Datenschnüfflern, egal ob im Ausland oder in der Schweiz. Beides führt dann schnell zu einer unbedachten Offenlegung von persönlichen Daten auf «Faceboogle».

Was kann man tun, um den Computer zu schützen?

Nicht der Computer muss geschützt werden, sondern der Mensch, der ihn benutzt. Und das bedeutet, das sich

dieser Mensch zuerst einmal bewusst werden muss, welchen Gefahren seine digitalen Bürgerrechte im Netz ausgeliefert sind und dass nur Anonymität und Vertraulichkeit der Kommunikation hier Schutz bieten. Anonymität erreicht man durch Netzwerke wie «Tor» und Vertraulichkeit durch Verschlüsselung mit «GnuPG».

Auch wenn man keinen IT-Hintergrund hat?

Fachwissen ist nicht entscheidend, sondern der Wille, sich mit der Thematik zu beschäftigen und neue Programme und Verhaltensmuster zu lernen – auch wenn das oft der Bequemlichkeit zuwiderläuft. Wie sagte Obama anlässlich der Enthüllungen um die National Security Agency doch so passend: «Es gibt keine hundertprozentige Sicherheit und keine hundertprozentige Privatsphäre ohne Unannehmlichkeit.»

Gibt es Programme oder Betriebssysteme, die man favorisieren sollte?

Grundsätzlich gibt es gute Gründe, Open-Source-Programme und -Betriebssysteme zu bevorzugen, aber im Kontext geheimdienstlicher Schnüffelei ist das eher nebensächlich. Für jedes gängige Betriebssystem wie Windows, MacOS, Linux oder Android gibt es Programme, um Anonymität und Vertraulichkeit im Netz zu unterstützen.

Sollen wir nun Linux nutzen?

Nur wenn Sie den Vorteil quell-offener Programme verstehen und unterstützen wollen. Linux hilft zwar nicht so sehr gegen staatliche Schnüffelei, ist aber bei vielen anderen Bedrohungen aus dem Internet ein echter Vorteil.

Jeder hat einen, die wenigsten verstehen ihn – ist der Computer das ideale Ziel für Datensammler?

Die Datensammler sind an unserer Kommunikation untereinander interessiert, nicht so sehr an dem Medium der Kommunikation. Auch wenn das im Moment etwas in Vergessenheit gerät, werden auch flächendeckend Telefon- und Handykommunikation abgehört und ausgewertet – nicht nur Computerdaten. Also ist nicht der Computer das Ziel, sondern der Mensch, der ihn nutzt. Und weil der Computer als universelles Kommunikationsmedium dem menschlichen Bedürfnis nach sozialem Geschnatter enorm entgegenkommt, passiert viel Kommunikation im Internet – und die wird abgehört.

Wie gefährlich sind Smartphones für die Nutzer oder Onlinebanking, Bezahlen mit Kreditkarte im Internet und vertrauliche Inhalte in E-Mails zu versenden?

Alles das ist gefährlich, vor allem wenn man naiv und blauäugig die Technik einfach nur nutzt, ohne sich der Gefahren bewusst zu sein.

Wer ausser der NSA ist sonst noch da draussen im Web und überwacht uns?

Alle Dienste in jedem Land der Welt – auch die Schweizer – machen das. Bisher sind die meisten einfach nicht erwischt worden. Weil kein mutiger Mensch bereit war, sein Leben aufzugeben, um diese dreckigen Geheimnisse an die Öffentlichkeit zu bringen. Aber wie Ingeborg Bachmann in ihrem Gedicht «Alle Tage» schrieb: «Es werden Zeiten kommen, da werden Orden verteilt: für den Verrat unwürdiger Geheimnisse.»

**Das Interview wurde schriftlich geführt.*

Interview: Daniel Stehula

LESERKOMMENTARE

Aktuell keine Kommentare vorhanden