Wissenschaftler der TU Dresden entwickeln Software gegen NSA-Schnüffler

Was früher als machbar, aber paranoid galt, hat sich durch die "Prism"-Enthüllungen von Edward Snowden bewahrheitet, sagt Stefan Köpsell, wissenschaftlicher Mitarbeiter der Informatikfakultät an der TU Dresden. Er und seine Kollegen klopfen derzeit ihr Anonymisierungs-Programm "ANON", das Datenwege im Internet verschleiert, nach bisher unbekannten Einfalltoren für den US-Geheimdienst NSA ab. Und sie entwickelt derzeit eine ähnliche Anonymisierungs-Software für Android-Computertelefone (Smartphones), die in wenigen Monaten auch mobiles Surfen sicherer machen soll. DNN-Redakteur Heiko Weckbrodt hat ihn ausgefragt.

Foto: Heiko Weckbrodt
Stefan Köpsell

Haben die Enthüllungen von Edward Snowden über das Schnüffel-Programm "Prism" Sie und Ihre Kollegen überrascht?

Ja und Nein. Das Internet wirkt auf den Laien riesig. Aber wenn sich ein Geheimdienst auf die richtigen Knoten in Frankfurt, London und Amsterdam konzentriert, kann er nahezu den gesamten Verkehr überwachen. Dass dieses enorme Maß an Überwachung technisch möglich ist, war uns hier seit Jahren bekannt. Dass die Amerikaner dies tatsächlich tun, war aber schon neu. Ich kann mich noch an meine Vorlesungen hier bei Professor Andreas Pfitzmann erinnern, der uns immer gesagt hat: Die Frage ist nicht, ob E-Mails von einem "großen Überwacher des Internets" gelesen werden, sondern wieviel. Als Student hat man sich damals gedacht: Na ja, klingt ein bisschen nach Verschwörungstheorie. Aber genau das hat sich nun bestätigt.

Wie sehen Sie die Rolle der deutschen Regierung dabei?

Mich hat überrascht, dass die Bundesregierung diese NSA-Praktiken anscheinend zumindest wissentlich mitgetragen hat. Nachdem seinerzeit das Echelon-Programm der NSA bekannt geworden war, hatte ein Untersuchungsausschuss der EU ja davor gewarnt, dass die Amerikaner diese Überwachung nicht nur für militärische Zwecke und Terrorabwehr verwenden, sondern auch für Wirtschaftsspionage. Wenn die Regierung "Prism" unterstützt, heißt das nichts anders, als dass sie Innovationsvorsprünge der deutschen Industrie den USA auf dem Tablett liefert

Gibt es eine Möglichkeit für den Bürger, sich gegen diese Schnüffeleien zu schützen?

Einen gewissen Schutz bietet der Einsatz von Verschlüsselungstechniken im privaten E-Mail-Verkehr. Das ist den meisten Nutzern aber offensichtlich zu umständlich. Gerade die Einführung des elektronischen Personalausweises und der sogenannten DE-Mail wäre eine sehr gute Chance gewesen, dies zum Standard zu machen: indem jeder Bürger mit dem Ausweis einen Schlüssel bekommen hätte und auch die DE-Mail durchgängig chiffriert worden wäre, um die Hürden für den Normalverbraucher zu senken, diese Schutzmaßnahmen auch einzusetzen. Aber das war wohl nicht gewollt.

Wie meinen Sie das: "nicht gewollt"?

Weil man Polizei und Geheimdiensten - auch ausländischen - die Möglichkeit offen halten wollte, da hineinzu-gucken.

Internet-Dienstleister wie die Telekom haben nach der Prism-Affäre angekündigt, den E-Mail-Verkehr ihrer Kunden künftig zu verschlüsseln. Hilft das?

Das bringt mehr Sicherheit, aber reinhören kann ein Überwacher dennoch. Denn die E-Mails werden nur zwischen den Kunden und dem Server zum Beispiel der Telekom verschlüsselt. Auf den Servern aber ist ein Zugriff möglich.

Die TU-Professur für Datenschutz hatte im Jahr 2000 mit ihrem Anonymisierungsdienst "ANON" bundesweit für Schlagzeilen gesorgt. Kann der nicht gegen NSA-Angriffe dienen?

Zunächst: ANON verschleiert nur beim Internetsurfen den Absender, nicht aber bei E-Mails. Wir durchforsten ihn seit der Prism-Geschichte verstärkt nach Schwachstellen und entwickeln gerade eine Variante für Android-Smartphones, der in etwa sechs Monaten fertig sein soll.

Aber ehrlich gesagt macht sich bei uns im Hause derzeit auch etwas Resignation breit. Wir haben immer gedacht, dass die Hardware und die Betriebssysteme sichere Anker wären, von denen wir ausgehen könnten. Nun fragen wir uns mehr und mehr: Welche Hintertüren für Geheimdienste hat Google in sein Android-Betriebssystem eingebaut? Sind unsere Server so sicher, wie wir immer dachten?

Es wird manchmal gesagt, die jüngeren Internet-Nutzer, die mit der "Teilen"-Mentalität von Facebook & Co. groß geworden sind, jucke es gar nicht, wenn ihre Mails vom "Großen Bruder" mitgelesen werden-

Ich glaube, da ist ein Umdenkprozess im Gange: Da merken immer mehr, welche negativen Folgen es haben kann, wenn jede Äußerung öffentlich wird. Das Problem mit dem Datenschutz ist nur, dass Ursache und Folge im Netz nicht so offensichtlich sind. Im Alltag ist natürlich jedem klar, dass es ein Fehler war, die Wohnung unverschlossen zu lassen, wenn sie nachher ausgeräumt wurde. Dagegen kann man nie ganz sicher sein, ob es wirklich an diesem oder jenem Facebook-Eintrag lag, dass man den Job bei der neuen Firma nicht bekommen hat.

Aus den Dresdner Neuesten Nachrichten vom 29.08.2013.