LE MONDE diplomatique

WOZ Nr. 25/2013 vom 20.06.2013

INTERNETÜBERWACHUNG

«Macht ihnen das Leben schwer!»

Der US-Geheimdienst kontrolliert den digitalen Datenverkehr. Das ist weder skandalös noch überraschend, sondern logisch. Am Ursprung des Problems stehen die NutzerInnen selbst. Um sich gegen die Überwachung zu wehren, muss man dort ansetzen.

Von Jan Jirát (Text) und Luca Schenardi (Illustration)

Als der Whistleblower Edward Snowden am vorletzten Sonntag in Hongkong die Überwachungspraktiken des US-amerikanischen Geheimdiensts National Security Agency (NSA) enttarnte, löste das weltweit einen Sturm der Entrüstung aus. Gemäss dem 29-jährigen IT-Spezialisten, der von 2007 bis 2009 für die CIA in Genf stationiert war, verfügt die NSA über direkten Zugang zu den Servern von neun grossen US-amerikanischen Internetfirmen.

«Skandal!», riefen Medien und PolitikerInnen im Chor, die Netz-Community taufte die USA kurzerhand in «United Stasi of America» um, und George Orwells über sechzig Jahre alter Überwachungsstaatsroman «1984» stürmte die Bestsellerlisten. Doch die Empörung und das mediale Rauschen führen auf die falsche Fährte. Das Prinzip Gut gegen Böse klärt in dieser Geschichte nur wenig auf. Im Gegenteil. Es lenkt davon ab, dass die InternetuserInnen selbst am Ursprung dieser Geschichte stehen.

Wie die Wirtschaft, so das Militär

Wir verwenden das Internet auf vielfältigste Weise. Die Kommunikation und der Konsum vollziehen sich heute vorwiegend online. Dafür nutzen wir Infrastruktur – Facebook als soziale Plattform, Amazon als digitale Buchhandlung, iTunes als Musikbörse. Wir hinterlassen dabei bereitwillig diverse persönliche Daten.

Wir tun dies im Wissen, dass es sich bei den Anbietern der Infrastrukturen in der Regel um private, gewinnorientierte Firmen handelt. Sie folgen einer kapitalistischen Logik, und dementsprechend nutzen sie unsere Daten: Sie sammeln sie, werten sie aus und erstellen Profile. Ihr Motiv ist es, unser zukünftiges Konsumverhalten möglichst präzise vorhersagen zu können, um so das ideale Angebot oder die passende Werbung platzieren zu können. Auf diese Weise sind in den vergangenen zwanzig Jahren riesige Datensammlungen entstanden.

An diesem Punkt kommen die Geheimdienste ins Spiel. Diese folgen einer militärischen Logik. Ihr Motiv ist es, das zukünftige Verhalten von möglichen Staatsfeinden – seien das Terroristen, Hackerinnen oder andere Staaten – so gut wie möglich vorhersagen zu können. Dafür sammeln sie Daten, werten sie aus und erstellen Profile. Die Daten holen sie sich logischerweise vor allem über die immensen Datensammlungen der US-amerikanischen Internetriesen.

«Die Verschmelzung der militärischen und der ökonomischen Sphären hat eine neue gesellschaftliche DNA geschaffen, in der private Wirtschaftsunternehmen mit militärischer Rationalität und Präzision Daten produzieren können und militärische und geheimdienstliche Bürokratien sie nach privatwirtschaftlichen Effizienz- und Risikokriterien verwerten dürfen», fasst der deutsche Publizist Frank Schirrmacher diese Symbiose in einem lesenswerten Aufsatz in der «Frankfurter Allgemeinen Sonntagszeitung» zusammen.

«Kaum taugliche Rechtsmittel»

Die Überwachungspraktiken der NSA können unter diesen Umständen kein Skandal sein. Sie sind «nicht einmal rechtswidrig», sagt Bruno Baeriswyl, der Datenschutzbeauftragte des Kantons Zürich. «Die NSA stützt sich auf das sogenannte Fisa-Gesetz, das die Auslandsspionage der USA regelt und den Zugriff auf sensible Daten rechtsstaatlich legitimiert.» Auf rechtlicher Ebene könne folglich kaum etwas gegen die Praktiken der NSA getan werden, schon gar nicht über das Schweizer Datenschutzgesetz, das einzig für den Schweizer Nachrichtendienst Gültigkeit besitzt. Auch Hanspeter Thür, oberster Datenschützer der Schweiz, bestätigt, dass «gegen Cyberauslandsspionage kaum ein Rechtsmittel tauglich ist».

Eine weitere falsche Fährte legt die Fixierung auf die NSA und die neun Internetfirmen. Das Ausmass der Überwachung ist nämlich weit umfassender. «Wenn ein Akteur wie die National Security Agency an deine Daten heranwill, dann schafft er das auch. Da hast du keine Chance», sagte Boris Kartheuser, einer der renommiertesten investigativen Journalisten Deutschlands, am vergangenen Wochenende an einem Recherchekongress in Hamburg.

Bruno Baeriswyl formuliert es etwas anders: «Sobald die Daten einmal im Internet sind, werden sie auch abgerufen und verwendet. Es gibt

online keine hundertprozentige Sicherheit.» Und Hernani Marques, Vorstandsmitglied des Chaos-Computer-Clubs der Schweiz, ist überzeugt, dass potente und global tätige Geheimdienste, über die auch Britannien, Frankreich, Deutschland oder China verfügen, Zugriff auf viele unserer Daten im Netz haben. Der Schweizer Nachrichtendienst spiele hingegen nicht in derselben Liga, so Marques. «Nach der Fichenaffäre Ende der achtziger Jahre war man nicht bereit, dem Geheimdienst weitgehende rechtliche Kompetenzen zuzugestehen. Das soll sich nun aber ändern. Unser Nachrichtendienstgesetz wird aktuell revidiert, die Überwachungsmöglichkeiten des Geheimdiensts sollen massiv ausgebaut werden.» (Vgl. «**Zwei gewalttätige SeniorInnen**[1]»)

Radikal, bequem oder anstrengend

US-Präsident Barack Obama hat nach den Enthüllungen von Edward Snowden die NSA-Praktiken verteidigt: «Man kann nicht hundert Prozent Sicherheit und hundert Prozent Privatsphäre und null Unannehmlichkeiten haben.» In diesem Spannungsfeld bewegen sich die Möglichkeiten angesichts der skizzierten Ausgangslage im Netz.

Der radikalste Weg ist die Verweigerung, doch der soziale Preis eines Lebens ohne Internet und Mobiltelefonie (auch die wird überwacht) dürfte für viele zu hoch sein. Der bequeme Weg ist, sich nicht darum zu scheren, was mit seinen Daten passiert und wer Zugriff darauf hat. Diese Haltung mag für Privatpersonen legitim sein, für Unternehmen, Zeitungsverlage, Nichtregierungsorganisationen oder Parteien ist sie fahrlässig. Nicht umsonst warnt Datenschützer Hanspeter Thür eindringlich vor «Outsourcing- und Cloudlösungen mit Servern in den USA». Trotzdem nutzen Firmen wie ABB und Nestlé, das Medienunternehmen Ringier oder die Umweltorganisation Greenpeace Kommunikationsdienste von Google oder Microsoft.

Wer seine Daten vor Übergriffen – so gut wie möglich – schützen wolle, müsse «etwas Aufwand und Unbequemlichkeit in Kauf nehmen», sagt Bernd Fix, Vorstandsmitglied der Wau-Holland-Stiftung, die sich in Deutschland um die Finanzierung von Wikileaks kümmert. «Ich verschlüssle beispielsweise meinen E-Mail-Verkehr. Das heisst, sobald ich die Mail verschicke, ist sie im Netz nur als unbrauchbarer Zahlensalat erkennbar. Erst der Empfänger kann die Mail mit seinem Passwort wieder entschlüsseln. Das sollte längst Standard sein.»

Fix rät zudem dazu, freie Software zu verwenden, bei der die exakten Codes der Programme öffentlich und somit von den NutzerInnen überprüfbar sind. Bei Facebook oder Skype ist das nicht der Fall. Der Netzaktivist empfiehlt einen Blick auf die Website **www.prism-break.org**[2], die einen guten Überblick bietet.

«Die absolute Sicherheit ist durch diese Massnahmen nicht gewährleistet, aber man kann den Geheimdiensten das Leben so schwer und teuer wie möglich machen», sagt Bernd Fix.

Private SpionInnen

Edward Snowden war kein Mitarbeiter der NSA. Der IT-Spezialist, der die Praktiken des US-Geheimdiensts enttarnt hat, war vor seiner Flucht nach Hongkong bei der Technologieberatungsfirma Booz Allen Hamilton angestellt. Gemäss «Spiegel» existieren fast 2000 Privatfirmen, die im Auftrag der US-Regierung und ihrer Geheimdienste sensible Daten beschaffen und verarbeiten. Das Geschäftsfeld ist offenbar derart attraktiv, dass etwa Booz Allen Hamilton zu 98 Prozent von Regierungsaufträgen lebt.

Rund dreissig Prozent aller SpionInnen in den USA stammen heute von Privatfirmen. Die im Haupttext auf dieser Seite angesprochene Verschmelzung von ökonomischer und militärischer Sphäre zeigt sich hier besonders ausgeprägt.

Die WOZ wollte vom Nachrichtendienst des Bundes wissen, ob auch er private Firmen engagiert habe. Antwort: «Der NDB kommuniziert über seine Geschäftsbeziehungen nicht gegenüber Medien und Öffentlichkeit.» Die Tätigkeit unterliege jedoch der regelmässigen Prüfung durch die Kontrollorgane von Parlament und Verwaltung.

Links

1. http://www.woz.ch/1325/staatsschutz/zwei-gewalttaetige-seniorinnen
2. http://www.prism-break.org