HEISSE FRAGEN
Gewinnen Sie ein Wochenende im Engadin
SEITE 67

HEISSE TIPPS
Wie Sie der Schnüffelei ein Schnippchen schlagen
SEITE 64

Knacknuss NSA

Der amerikanische Geheimdienst untergräbt die Demokratie. An der ETH Lausanne diskutierten Fachleute, wie die Privatsphäre wiederhergestellt werden könnte

VON JOACHIM LAUKENMANN, BARNABY SKINNER (TEXT) UND CORTIS & SONDEREGGER (FOTOS)

Für Bill Binney gibt es stehende Ovationen. Der ehemalige technische Direktor der National Security Agency (NSA) wurde wie Edward Snowden zum Whistleblower und wettert am Kongress über Privatsphäre und Überwachung an der ETH Lausanne über seinen ehemaligen Arbeitgeber. Snowden habe mit seinen Enthüllungen «der ganzen Welt einen Dienst erwiesen», sagt Binney. «Jeder ist betroffen. Die NSA sammelt alle Daten, die sie zu fassen kriegt.» Und weiter: «Ich bin stinksauer. Ich möchte denen direkt ins Gesicht schlagen.» Der Saal mit rund 800 Konferenzteilnehmern tobt.

Binney und andere Redner haben letzten Montag in Lausanne die wahre Problematik hinter der Bespitzelung durch die NSA und andere Geheimdienste aufgezeigt – und nach Lösungen gesucht. Demnach geht es nicht in erster Linie um den unbescholtenen Nutzer von Facebook, der auf dem sozialen Netzwerk persönliche Daten preisgibt. Kern der Debatte ist vielmehr, dass die umfassende Überwachung des Internets und der Telekommunikation unser gesetzlich festgeschriebenes Recht auf Privatsphäre untergräbt und damit letztlich die Demokratie gefährdet. Ohne das Recht auf Privatsphäre gebe es keine wirklich freie Meinungsäusserung und damit keine echte Demokratie, sagte jüngst auch Dilma Rousseff, die von der NSA bespitzelte Präsidentin Brasiliens.

Aus Sicht der NSA hat die Bespitzelung drei Ziele: die Terrorismusbekämpfung, die Sicherheit im Internet und den Kampf gegen die Weiterverbreitung von Massenvernichtungswaffen. Die NSA und andere Geheimdienste haben deshalb das Internet zu einer gigantischen Überwachungsplattform gemacht. «Das Internet mit seinen neuen Möglichkeiten wird gegen uns benutzt», sagt der Kryptologe Arjen Lenstra von der ETH Lausanne, der den Kongress organisiert hat. «Das können wir nicht akzeptieren. Wir brauchen ein neues Internet, das unseren Wünschen gerecht wird: ein Internet, das gratis ist, offen und vertrauenswürdig.»

Hersteller mussten Hintertüren für Spione einbauen

Wie die «New York Times» letzte Woche enthüllte, kann die NSA aus den gesammelten Daten ausgefeilte Karten über das soziale Netzwerk von Zielpersonen erstellen. Darauf ist zu sehen, mit wem die Leute Kontakt haben, wo sie sich wann aufhalten, die Facebook-Profile, Steuerdaten und vieles mehr. So geraten selbst gewöhnliche Bürger in den Dunstkreis von Terroristen.

Um an Informationen über Personen, Unternehmen, Regierungen und Behörden zu gelangen, verfolgt die NSA mehrere Strategien. Ein Ansatz sind geheime Abkommen mit diversen Telekommunikations- und Internetfirmen, die ihre Daten an die NSA liefern müssen. Weiter attackiert die NSA Hardware und Software nahe am Nutzer, etwa Internetrouter und Firewalls. Offenbar wurden Hersteller teilweise dazu gezwungen, Hintertüren in ihre Produkte einzubauen, über die Geheimdienste in Computer eindringen können.

Selbst die Verschlüsselung ist kein garantierter Schutz vor den Blicken der Spione. Zwar rechnen die meisten Kryptografie-Experten nicht damit, dass die NSA oder andere Geheimdienste die trickreichen mathematischen Methoden hinter kryptografischen Standards geknackt haben. «Aber es gibt zahlreiche andere Möglichkeiten, heimlich an verschlüsselte Informationen zu gelangen», sagt Lenstra.

Bekannt wurde kürzlich der Fall von RSA, einer Tochter des amerikanischen IT-Konzerns EMC. Die Geschichte war so gut, dass sich weltweit 25 000 Medien darauf stürzten. Die Schlagzeile lautete ungefähr so: Die US-Sicherheitsfirma rät von eigenen Produkten ab. RSA hat offenbar seit Jahren einen Algorithmus in ihren Produkten eingesetzt, der, so die Vermutung, zuvor von der NSA manipuliert worden war. Der sogenannte Dual_EC_DRBG-Algorithmus dient dazu, Inhalte mithilfe zufällig erzeugter Zahlenreihen zu verschlüsseln.

Gesamte US-IT-Branche steht unter Generalverdacht

Durch die Manipulation, so vermuten Netzexperten, waren die Spitzel in der Lage, in aller Ruhe vermeintlich verschlüsselte Mails zu lesen oder auf geschlossene Netzwerke zuzugreifen. Der in der Szene angesehene Kryptograf Matthew Green geht sogar davon aus, dass die NSA die Sicherheitsfirma RSA im Jahre 2006 dazu zwang, Dual_EC in ihrem Kryptografiesystem einzusetzen.

Am Hauptsitz der RSA in Bedford bei Boston schütteln die Techniker über die Schlagzeilen und besonders über Green den Kopf. Sam Curry, Chief Technologist, sagt: «Erstens haben wir unseren Kunden nicht empfohlen, auf unsere Produkte zu verzichten, sondern ihnen nahegelegt, in Kombination mit unserer Software auf andere Zufallsgeneratoren zu setzen.» Und zweitens gebe es keine Fakten zu diesem Fall. «Ob die NSA Dual_EC tatsächlich manipuliert hat, bleibt Theorie.» Die Frage, ob es denn zwischen der Sicherheitsfirma RSA und den Spionen der NSA jemals zu einem Kontakt gekommen sei, verneint Curry. Für weitere Fragen verweist er an seine Rechtsabteilung *(siehe auch Interview Seite 64)*.

Was soll er auch anderes tun? Unter den Snowden-Enthüllungen haben – neben den Datenfetischisten Google oder Facebook – am meisten die US-Sicherheitsfirmen zu leiden. Im Grunde steht die gesamte US-IT-Branche unter Generalverdacht, der NSA bei der Spionage zu hel-

FORTSETZUNG AUF SEITE 64

FORTSETZUNG VON SEITE 63

Knacknuss NSA

fen. Die Folge: der totale Vertrauensverlust. «Den Firmen, die unsere Internet-Infrastruktur aufbauen und unterhalten, den Firmen, die uns ihre Hard- und Software verkaufen, den Firmen, die unsere Daten verwalten: Wir können ihnen nicht mehr länger vertrauen», schreibt Kryptografie-Experte Bruce Schneier auf seinem Blog. Doch «Vertrauen ist essenziell für unsere Demokratie.»

Wie Schneier auf der Konferenz in Lausanne vorträgt, geht es beim Thema Privatsphäre weniger um den Schutz persönlicher Geheimnisse als vielmehr um Kontrolle: Wer über uns Bescheid weiss, der hat uns in der Hand. Und das sei wegen des Machtgefälles zwischen Staat und Individuum sehr gefährlich. «Erzwungene Offenheit reduziert unsere Freiheit», sagt Schneier. «Die Privatsphäre indes erhöht unsere Macht.»

Wie gross das Misstrauen gegenüber IT-Firmen und Geheimdiensten ist, veranschaulicht der Internetaktivist Jacob Applebaum, der an der Auswertung der Snowden-Dokumente beteiligt ist. «Ich habe sogar das Mikrofon aus meinem Notebook entfernt», sagt er in seinem Vortrag und fordert zu technischem und politischem Widerstand gegen die Maschinerie des Überwachungsstaats auf, welche die NSA aufgebaut habe.

Weit schlimmer ist die Manipulation der Infrastruktur

Wie die Privatsphäre wiederhergestellt werden kann, ist jedoch alles andere als offensichtlich. Ein guter Start ist laut Lenstra, wenn sich die Menschen der Situation bewusst werden: Jede Information, die in eine Tastatur eingegeben wird, lässt sich praktisch nie mehr löschen und kann mitgelesen werden – sofern sich jemand dafür interessiert.

Einige Fachleute auf der Konferenz plädierten für ein neues Internetgesetz, das die Geheimdienste in ihre Schranken weist. Das EU-Parlament plant derzeit ein neues Gesetz zur elektronischen Kommunikation. Aber der Rechtsexperte Nikolaus Forgó hat wenig Hoffnung, dass dieses einen grossen Unterschied machen wird. «Es ist ein Chaos», sagte er in Lausanne.

Applebaum setzt daher auf die Kryptografie: «Der einzige Weg, ein sicheres System aufzubauen, ist die Mathematik. Damit müssen wir verhindern, dass Geheimdienste zum Beispiel die sozialen Netzwerkkarten erstellen können.» Lenstra indes hegt Zweifel, ob bessere Kryptografie das Allheilmittel ist. «Ich sehe zu wenig ökonomische Anreize für die Konstruktion eines neuen, sicheren Internets.»

Zudem ist Lenstra überzeugt, dass Snowdens Enthüllungen über die Fähigkeiten der NSA «nur die Spitze des Eisbergs» sind. Weit schlimmer als das Datenschnüffeln und die Verletzung der Privatsphäre sei die Manipulation von Infrastrukturen wie Kraftwerken oder Pipelines mittels Schadsoftware – ähnlich wie 2010, als der Computerwurm Stuxnet Störungen im iranischen Atomprogramm verursachte.

«Es besteht die Möglichkeit für wirklich desaströse Ereignisse. Gemessen an diesen wirken die Snowden-Enthüllungen geradezu harmlos», sagt Lenstra.

Sicher im Netz – die Rezepte

Open-Source-Software, Verschlüsselungsprogramme, keine US-Cloud-Dienste

VON SIMONE LUCHETTA

1. Der US-Geheimdienst kann verschlüsselte Kommunikation knacken. Welche Verschlüsslungstechnik ist betroffen?
Einige der am meisten verbreiteten Techniken, darunter das Virtual Private Network (VPN) und die SSL-Verschlüsselung von Datenverkehr, wie sie vor allem von Firmen und Behörden benutzt werden. Mit SSL wird etwa die Kommunikation bei Bankgeschäften verschlüsselt.

2. Wie hebelt die NSA die Verschlüsselung aus?
Sie arbeitet vornehmlich mit US-Unternehmen, um Schwachstellen in die Programme einzuschleusen. Sie hat es sogar geschafft, Lücken in internationale Verschlüsselungsstandards einzubauen. Die Wahrscheinlichkeit, dass sie die Verschlüsselungstechnik mit Hochleistungsrechnern knacken kann, ist dagegen gering.

3. Können auch andere diese Lücken nutzen?
Ja. Auch Kriminelle werden die Löcher finden.

4. Ist Verschlüsselung für mich als Privatperson überhaupt relevant?
Wenn Ihnen Ihre Privatsphäre ein wertvolles Gut ist, auf jeden Fall. Ihre E-Mails sind bei jeder Zwischenstation frei les- und analysierbar – von Geheimdiensten genauso wie vom Administrator am Arbeitsplatz. Wenn Sie verschlüsseln, braucht es immerhin etwas Aufwand, um an den Inhalt Ihrer Nachrichten zu kommen.

5. Gibt es noch Systeme, die sicher sind?
Nutzen Sie Open-Source-Software; dort gibt es keine CEOs, mit denen sich Sicherheitslücken aushandeln lassen.

6. Wie kann ich der NSA und anderen Geheimdiensten das Leben schwermachen, wenn sie meine Daten haben wollen?
Verschlüsseln Sie Ihre Nachrichten mit GnuPG (www.gnupg.org), das die Ver- und Entschlüsselung in jedem gebräuchlichen E-Mail-Programm erlaubt, und bringen Sie Ihre Kontakte dazu, es ebenfalls zu tun. Hinterlassen Sie im Web keine Spuren beim Surfen, indem Sie das Tor-Netzwerk zur Anonymisierung von Verbindungsdaten nutzen (www.torproject.org). Setzen Sie möglichst auf Open-Source-Software, auch bei Betriebssystemen: mit GNU/Linux oder BSD sind Sie auf der sichereren Seite. Eine gute Übersicht über freie Alternativen bietet http://prism-break.org

7. Sind iOS, Windows und Android unsicher?
Ja. Apple, Google und Microsoft sind mutmasslich Teil des Überwachsungsprogramms Prism. Ihren Betriebssystemen kann nicht vertraut werden. Inbesondere Smartphones (Blackberry, iPhone, Android) sind für die NSA offene Bücher.

8. Kann ich chatten, ohne das jemand mithört?
Viele Messaging-Programme wie etwa iMessage von Apple oder Threema (Android, iOS) verschlüsseln die Daten bereits; Skype dagegen gilt als nicht vertrauenswürdig. Noch weiter gehen Messaging-Programme (ICQ, AIM, MSN), die das OTR-Protokoll verwenden (off the Record). Es verschlüsselt nicht nur, sondern anonymisiert gegenüber Mithörern die Teilnehmer. Am PC verschlüsseln Sie Instant Messaging mit dem Open-Source-Programm Cryptocat (https://crypto.cat).

9. Wie kann ich verhindern, dass meine Daten in der Cloud landen?
Indem Sie keine US-basierten Onlinedienste nutzen: kein Evernote, kein Facebook, kein iCloud, kein Flickr oder Instagram, da die Server in den USA stehen. Statt Skydrive, Google Drive, Dropbox wählen Sie alternative Onlinespeicher mit Webservern in der Schweiz, weil die Datenschutzgesetze hier deutlich strenger sind: Mydrive, SecureSafe, Speicherbox, Filesync. Oder bauen Sie Ihre eigene Cloud mit einem Netzwerkspeicher (NAS, Network Attached Storage) von Seagate, Synology oder Netgear.

10. Spioniert uns der Nachrichtendienst des Bundes (NDB) genauso aus wie die NSA?
Noch nicht. Das revidierte Überwachungsgesetz (Büpf) und das neue Nachrichtendienstgesetz (NDG), die in der Wintersession behandelt werden, zielen aber in die gleiche Richtung. In der «Rundschau» vom 2. Oktober sagte NDB-Vizechef Jürg Bühler, eine Abhörung im Ausmass des NSA «sei völlig unmöglich, sowohl vom finanziellen als auch vom personellen Aufwand her». Moralische Bedenken äusserte er nicht.

FOTOS: CORTIS & SONDEREGGER

«Meine Umgebung soll erkennen, dass ich ich bin»

Sam Curry, Chief Technologist der IT-Sicherheitsfirma RSA, über eine Welt ohne Passwörter

Sam Curry, Sie träumen von einer Welt ohne Passwörter.
Ich glaube, damit bin ich nicht alleine. Ich habe kürzlich gezählt, wie viele Passwörter ich habe. Es sind 78. Das kann ich mir niemals merken. Deshalb muss ich auf professionelle Verwalter zurückgreifen, die wiederum durch Passwörter gesichert sind.

Wie soll eine Welt ohne Passwörter aussehen?
Grundsätzlich müssen wir davon wegkommen, dass wir, um uns digital auszuweisen, nur einen einzigen Parameter brauchen. Authentifizierung im Internet ist heute binär. Entweder stimmt das Passwort, oder es stimmt nicht. Ich glaube, Authentifizierung wird künftig fliessend sein. Sie wird aus vielen Parametern bestehen: Gewicht, Haarfarbe, Fingerabdruck, Augenfarbe und so weiter. Je nachdem, wie viel man von sich verrät, desto mehr Vertrauen wird man beim jeweiligen Dienst geniessen.

Ist das iPhone für Sie ein Schritt in diese Richtung?
Absolut. Der Fingerabdruck allein ist nicht sicher. Aber in Kombination mit meinem Gewicht und Alter wird die Authentifizierung stärker und vertrauenswürdiger. Ich möchte in Zukunft mein Haus verlassen können und ins Auto steigen, ohne einen einzigen Schlüssel oder Knopf bedient zu haben. Meine Umgebung soll erkennen, dass ich ich bin.

Wenn Ihre Umgebung weiss, wer Sie sind, dann kann das auch missbraucht werden.
Sie sprechen den Datenschutz an. Das ist eine Herausforderung. Grundsätzlich muss es uns gelingen, jedem Menschen die vollkommene Kontrolle darüber zu geben, was er teilt, was nicht und vor allem mit wem er etwas teilt. Natürlich sind wir noch lange nicht so weit. Vor allem muss die Kryptografie, also die sichere Verschlüsselungstechnik, besser werden.

Was ist gute Kryptografie?
Das System muss vollkommen offen sein. Denn wenn es einen Weg gibt, ein System zu brechen, dann wird er gefunden. Gute Kryptografie heisst also etwas, was man auf einer Konferenz zeigen kann, damit die Hacker dann versuchen können, das System zu knacken.

Geben Sie uns zwei Beispiele eines guten Systems?
Der Advanced Encryption Standard AES funktioniert ziemlich gut. Er wird mittlerweile von Regierungen auf der ganzen Welt eingesetzt. Dieses System gibt es seit den 1970er-Jahren, und ohne viel Aufwand ist es noch niemandem gelungen, das System zu knacken. Ein neueres Beispiel ist HMAC. Dieses System verspricht nicht nur, Inhalte zu entschlüsseln, sondern den Empfänger zu warnen, wenn der Inhalt nicht das enthält, was er erwartet. Aber HMAC ist eine noch junge Technik. Womöglich wird es schon bald von jemandem geknackt.

INTERVIEW: BARNABY SKINNER