



PHILIPPE LOPEZ / AFP

„Als Zielobjekt markiert“

Der Enthüller Edward Snowden über die geheime Macht der NSA

Kurz bevor Edward Snowden zum weltweit bekannten Whistleblower wurde, beantwortete er einen umfangreichen Katalog von Fragen. Sie stammten unter anderem von Jacob Appelbaum, 30, einem Entwickler von Verschlüsselungs- und Sicherheitssoftware. Appelbaum unterweist internationale Menschenrechtsgruppen und Journalisten im sicheren und anonymen Umgang mit dem Internet.

Einer breiteren Öffentlichkeit wurde er 2010 bekannt, als er den WikiLeaks-Gründer Julian Assange als Redner bei einer Hacker-Konferenz in New York vertrat. Zusammen mit Assange und weiteren Co-Autoren veröffentlichte er unlängst den Gesprächsband „Cypherpunks: Unsere Freiheit und die Zukunft des Internets“.

Im Zuge der Ermittlungen rund um die WikiLeaks-Enthüllungen ist Appelbaum ins Visier amerikanischer Behörden geraten, die Unternehmen wie Twitter und Google aufgefordert haben, seine Konten preiszugeben. Er selbst bezeichnet seine Haltung zu WikiLeaks als „ambivalent“ – und beschreibt im Folgenden, wie er dazu kam, Fragen an Snowden stellen zu können:

Mitte Mai hat mich die Dokumentarfilmerin Laura Poitras kontaktiert. Sie sagte mir zu diesem Zeitpunkt, sie sei in Kontakt mit einer anonymen NSA-Quelle, die eingewilligt habe, von ihr interviewt zu werden.

Sie stellte dafür gerade Fragen zusammen und bot mir an, selbst Fragen beizusteuern. Es ging unter anderem darum

festzustellen, ob es sich wirklich um einen NSA-Whistleblower handelt. Wir schickten unsere Fragen über verschlüsselte E-Mails. Ich wusste nicht, dass der Gesprächspartner Edward Snowden war – bis er sich in Hongkong der Öffentlichkeit offenbarte. Er wusste auch nicht, wer ich war. Ich hatte damit gerechnet, dass es sich um jemanden in den Sechzigern handeln würde.

Das Folgende ist ein Auszug aus einem umfangreicheren Interview, das noch weitere Punkte behandelte, viele davon sind technischer Natur. Einige der Fragen erscheinen jetzt in anderer Reihenfolge, damit sie im Zusammenhang verständlich sind.

Bei dem Gespräch ging es fast ausschließlich um die Aktivitäten der National

Security Agency und um ihre Fähigkeiten. Es ist wichtig zu wissen, dass diese Fragen nicht im Zusammenhang mit den Ereignissen der vergangenen Woche oder des vergangenen Monats gestellt wurden. Sie wurden in einer Zeit totaler Ruhe gestellt, als Snowden noch auf Hawaii war.

Ich hatte zu einem späteren Zeitpunkt noch einmal direkten Kontakt mit Snowden, an dem ich auch meine eigene Identität offenbarte. Er hat mir damals die Einwilligung gegeben, seine Aussagen zu veröffentlichen.

Frage: Was ist die Aufgabe der National Security Agency (NSA) – und wie ist deren Job mit den Gesetzen in Übereinstimmung zu bringen?

Snowden: Aufgabe der NSA ist es, von allem Wichtigem zu wissen, das außerhalb der Vereinigten Staaten passiert. Das ist eine beträchtliche Aufgabe, und den Leuten dort wird vermittelt, dass es eine existentielle Krise bedeuten kann, nicht alles über jeden zu wissen. Und dann glaubt man irgendwann, dass es schon in Ordnung ist, sich die Regeln etwas hinzubiegen. Und wenn die Menschen einen dann dafür hassen, dass man die Regeln verbiegt, wird es auf einmal überlebenswichtig, sie sogar zu brechen.

Frage: Sind deutsche Behörden oder deutsche Politiker in das Überwachungssystem verwickelt?

Snowden: Ja natürlich. Die (NSA-Leute –Red.) stecken unter einer Decke mit den Deutschen, genauso wie mit den meisten anderen westlichen Staaten. Wir (im US-Geheimdienstapparat –Red.) warnen die anderen, wenn jemand, den wir packen wollen, einen ihrer Flughäfen benutzt – und die liefern ihn uns dann aus. Die Informationen dafür können wir zum Beispiel aus dem überwachten Handy der Freundin eines verdächtigen Hackers gezogen haben, die es in einem ganz anderen Land benutzt hat, das mit der Sache nichts zu tun hat. Die anderen Behörden fragen uns nicht, woher wir die Hinweise haben, und wir fragen sie nach nichts. So können sie ihr politisches Führungspersonal vor dem Backlash (deutsch etwa: Rückschlag –Red.) schützen, falls herauskommen sollte, wie massiv weltweit die Privatsphäre von Menschen missachtet wird.

Frage: Aber wenn jetzt Details dieses Systems enthüllt werden, wer wird dafür vor Gericht gestellt werden?

Snowden: Vor US-Gerichte? Das meinen Sie doch nicht ernst, oder? Als der letzte große Abhörskandal untersucht wurde – das Abhören ohne richterlichen Beschluss, das Abermillionen von Kommunikationsvorgängen betraf – hätte das eigentlich zu den längsten Haftstrafen der Weltgeschichte führen müssen. Aber

dann haben unsere höchsten Vertreter die Untersuchung einfach gestoppt. Die Frage, wer theoretisch angeklagt werden könnte, ist hinfällig, wenn die Gesetze nicht respektiert werden. Gesetze sind gedacht für Leute wie Sie oder mich – nicht aber für die.

Frage: Kooperiert die NSA mit anderen Staaten wie Israel?

Snowden: Ja, die ganze Zeit. Die NSA hat eine große Abteilung dafür, sie heißt FAD – Foreign Affairs Directorate.

Frage: Hat die NSA geholfen, Stuxnet zu programmieren? (Jenes Schadprogramm, das gegen iranische Atomanlagen eingesetzt wurde –Red.)

Snowden: Die NSA und Israel haben Stuxnet zusammen geschrieben.

Frage: Welche großen Überwachungsprogramme sind heute aktiv, und wie helfen internationale Partner der NSA?

Tage, das mag vielleicht nicht nach viel klingen, aber es geht eben nicht nur um Verbindungsdaten. „Full take“ heißt, dass der Speicher alles aufnimmt. Wenn Sie ein Datenpaket verschicken und wenn das seinen Weg durch Großbritannien nimmt, werden wir es kriegen. Wenn Sie irgendetwas herunterladen, und der Server steht in Großbritannien, dann werden wir es kriegen. Und wenn die Daten Ihrer kranken Tochter in einem Londoner Call Center verarbeitet werden, dann ... Ach, ich glaube, Sie haben verstanden.

Frage: Kann man dem entgehen?

Snowden: Na ja, wenn man die Wahl hat, sollte man niemals Informationen durch britische Leitungen oder über britische Server schicken. Sogar Selfies (meist mit dem Handy fotografierte Selbstporträts –Red.) der Königin für ihre Bademeister würden mitgeschnitten, wenn es sie gäbe.

„Tempora saugt alle Daten auf – egal worum es geht.“

Snowden: Die Partner bei den „Five Eyes“ (dahinter verbergen sich die Geheimdienste der Amerikaner, der Briten, der Australier, der Neuseeländer und der Kanadier –Red.) gehen manchmal weiter als die NSA-Leute selbst. Nehmen wir das Tempora-Programm des britischen Geheimdienstes GCHQ. Tempora ist der erste „Ich speichere alles“-Ansatz („Full take“) in der Geheimdienstwelt. Es saugt alle Daten auf, egal worum es geht und welche Rechte dadurch verletzt werden. Dieser Zwischenspeicher macht nachträgliche Überwachung möglich, ihm entgeht kein einziges Bit. Jetzt im Moment kann er den Datenverkehr von drei Tagen speichern, aber das wird noch optimiert. Drei

Frage: Arbeiten die NSA und ihre Partner mit einer Art Schleppnetz-Methode, um Telefonate, Texte und Daten abzufangen?

Snowden: Ja, aber wie viel sie mitschneiden können, hängt von den Möglichkeiten der jeweiligen Anzapfstellen ab. Es gibt Daten, die für ergiebiger gehalten werden und deshalb häufiger mitgeschnitten werden können. Aber all das ist eher ein Problem bei ausländischen Anzapf-Knotenpunkten, weniger bei US-amerikanischen. Das macht die Überwachung auf eigenem Gebiet so erschreckend. Die Möglichkeiten der NSA sind praktisch grenzenlos – was die Rechenleistung angeht, was den Platz oder die Kühlkapazitäten für die Computer angeht.



Irans Präsident Mahmud Ahmadinedschad in Atomanlage 2008: Schadprogramm von der NSA

Frage: Die NSA baut ein neues Datenzentrum in Utah. Wozu dient es?

Snowden: Das sind die neuen Massendatenspeicher.

Frage: Für wie lange werden die gesammelten Daten aufbewahrt?

Snowden: Jetzt im Moment ist es noch so, dass im Volltext gesammeltes Material sehr schnell altert, innerhalb von ein paar Tagen, vor allem durch seine gewaltige Masse. Es sei denn, ein Analytiker markiert ein Ziel oder eine bestimmte Kommunikation. In dem Fall wird die Kommunikation bis in alle Ewigkeit gespeichert, eine Berechtigung dafür bekommt man immer. Die Metadaten (*also Verbindungsdaten, die verraten, wer wann mit wem kommuniziert hat* –Red.) altern weniger schnell. Die NSA will, dass wenigstens alle Metadaten für immer gespeichert werden können. Meistens sind die Metadaten wertvoller als der Inhalt der Kommunikation. Denn in den meisten Fällen kann man den Inhalt wiederbesorgen, wenn man die Metadaten hat. Und falls nicht, kann man alle künftige Kommunikation, die zu diesen Metadaten passt und einen interessiert, so markieren, dass sie komplett aufgezeichnet wird. Die Metadaten sagen einem, was man vom breiten Datenstrom tatsächlich haben will.

Frage: Helfen Privatunternehmen der NSA?

Snowden: Ja. Aber es ist schwer, das nachzuweisen. Die Namen der kooperierenden Telekom-Firmen sind die Kronjuwelen der NSA ... Generell kann man sagen, dass man multinationalen Konzernen mit Sitz in den USA nicht trauen sollte, bis sie das Gegenteil bewiesen haben. Das ist bedauerlich, denn diese Unternehmen hätten die Fähigkeiten, den weltweit besten und zuverlässigsten Service zu liefern – wenn sie es denn wollten. Um das zu erleichtern, sollten Bürgerrechtsbewegungen diese Enthüllungen jetzt nutzen, um sie anzutreiben. Die Unternehmen sollten einklagbare Klauseln in ihre Nutzungsbedingungen schreiben, die ihren Kunden garantieren, dass sie nicht ausspioniert werden. Und sie müssen technische Sicherungen einbauen. Wenn man auch nur eine einzige Firma zu so etwas bewegen könnte, würde das die Sicherheit der weltweiten Kommunikation verbessern. Und wenn das nicht zu schaffen ist, sollte man sich überlegen, selbst eine solche Firma zu gründen.

Frage: Gibt es Unternehmen, die sich weigern, mit der NSA zu kooperieren?

Snowden: Ja, aber ich weiß nichts von einer entsprechenden Liste. Es würde je-

doch sicher mehr Firmen dieser Art geben, wenn die kollaborierenden Konzerne von den Kunden abgestraft würden. Das sollte höchste Priorität aller Computernutzer sein, die an die Freiheit der Gedanken glauben.

Frage: Vor welchen Websites sollte man sich hüten, wenn man nicht ins Visier der NSA geraten will?

Snowden: Normalerweise wird man aufgrund etwa des Facebook-Profiles oder der eigenen E-Mails als Zielobjekt markiert. Der einzige Ort, von dem ich persönlich weiß, dass man ohne diese spezifische Markierung zum Ziel werden kann, sind die Foren von Dschihadisten.

Frage: Was passiert, wenn die NSA einen Nutzer im Visier hat?

Snowden: Die Zielperson wird komplett überwacht. Ein Analytiker wird täglich einen Report über das bekommen, was sich im Computersystem der Zielperson geändert hat. Es wird auch ... Pakete jener Daten geben, die die automatischen Analysesysteme nicht verstanden haben, und so weiter. Der Analytiker kann entscheiden, was er tun will – der Computer der Zielperson gehört nicht mehr ihr, er gehört dann quasi der US-Regierung.

JACOB APPELBAUM,
LAURA POITRAS

„Wir sind alle verwundbar“

Der US-Aktivist und „Cypherpunk“ Jacob Appelbaum über die Enthüllungen von Edward Snowden – und was sie bedeuten

Vor den Veröffentlichungen von Glenn Greenwald, Laura Poitras und Barton Gellman, in denen sie Edward Snowdens Enthüllungen über die Verstöße gegen Menschenrechte detailliert darlegten, wusste die Öffentlichkeit nur sehr wenig über die dunkle Realität der weltweiten Überwachung.

Einen Vorläufer dessen, was wir gerade erleben, gab es in den USA mit dem Senator Frank Church in den siebziger Jahre des vorigen Jahrhunderts. Er stieß damals eine intensive Debatte um schweren Machtmissbrauch bei Geheimdiensten und bei der Bundespolizei an. Der Church-Ausschuss untersuchte die Aktivitäten der Central Intelligence Agency (CIA), der National Security Agency (NSA) und des Federal Bureau of Investigation (FBI).

Senator Church warnte damals das amerikanische Volk und die Welt vor der Macht der NSA. Er sagte, diese Be-

hörde würde es einem Diktator ermöglichen, ein System totaler Tyrannei zu errichten, gegen das niemand ankämpfen könnte. Damals war es allerdings noch unvorstellbar, dass einige wenige Staaten mit der Hilfe privater Firmen irgendwann in der Lage sein könnten, gegen



Chiffrier-Experte Appelbaum
„Bestätigung von ganz oben“

alle demokratischen Spielregeln ein Netz annähernd globaler Überwachung aufzubauen. Und das ist eben keine Verschwörungstheorie, sondern ein Geschäftsmodell.

Diejenigen, die das wussten oder die es zumindest ahnten, aber auch diejenigen, die dafür sorgen wollten, dass dieses Thema offen diskutiert wird, wurden in den vergangenen Jahren weitgehend ignoriert oder als Paranoiker bezeichnet.

Aber es gab sie, und es gab sogar zu viele, als dass man sie alle nennen könnte. Gruppen wie die Electronic Frontier Foundation oder die American Civil Liberties Union sind längst nicht allen bekannt. Auch Einzelkämpfer wie Mark Klein, der eine Abhöranlage in einer Einrichtung des Telefonriesen AT&T entdeckt hatte, kennen nur wenige. Die Informationen, die Klein enthüllte, wurden heruntergespielt, dabei waren sie ein wichtiges Beispiel für das umfassende