»Seit Snowden hat sich eine Menge getan«

Vor drei Jahren hat der Whistleblower Edward Snowden die Praktiken der NSA aufgedeckt. Wir haben uns mit der Netzpolitik.org-Redakteurin Constanze Kurz unterhalten, wie man seine Daten schützen kann und was sich seit den Enthüllungen gesellschaftlich verändert hat.

FOTO: KENO BUDDE

Ein Interview von
[johann] & [keno]

Kann man denn überhaupt etwas gegen Überwachung tun und seine Daten effektiv schützen?
Das sind zwei verschiedene Dinge: Das kann ja sich selbst schützen oder sich juristisch und politisch wehren. Das ist ja nicht dasselbe wie sich erstmal um die eigenen Daten Gedanken zu machen. Technisch kann man sich schützen. Und wenn man sehr viel Aufwand betreibt, kann man das auch sicher zu tun.
Aber sollte es für den Normalbürger so anstrengend sein, wie es momentan ist?
Ich glaube ja, ein bisschen. Man muss einen Sinn darin sehen, sich für oder gegen bestimmte Apps zu entscheiden, oder für oder gegen Verschlüsselung. Die Kryptologie dahinter muss man nicht verstehen, aber man muss sich ein wenig informieren. Das ist nicht im Vorbeigehen zu schaffen.
Findest du das richtig, wie es momentan ist oder sollte es Aufgabe des Staates sein zu verhindern, dass es überhaupt solche Datenkraken gibt?
Ich glaube beides. Ich finde die Situation nicht richtig, weil es viele Leute gibt, die zu viel Überwachung ausgesetzt sind. Sei es geheimdienstliche, sei es kommerzielle. Andererseits glaube ich schon, dass auch der einzelne sich entscheiden muss. Das ist ein bisschen wie beim Mülltrennen: Der Staat macht viele Gesetze, um Recycling zu unterstützen, aber natürlich müssen die Bürger auch mitmachen, sonst wird es nicht funktionieren.
Wie siehst du denn dieses fehlende Bewusstsein in der Gesellschaft für Datensicherheit?
Also ich finde, es hat sich seit Snowden eine Menge getan. Ich glaube schon, dass viele Leute anders darüber denken. Die Leute wissen über die Überwachung, sie wissen, dass es das sowohl im geheimdienstlichen als auch im kommerziellen Bereich gibt. Das heißt aber noch nicht, dass alle danach handeln. Die andere Frage ist jetzt, ob genug Leute ihr Verhalten ändern und damit die Politik beeindrucken.

ZUR PERSON

Constanze Kurz, Jahrgang 1974, hat Informatik studiert und lange Zeit im universitären Bereich gearbeitet. Seit letztem Jahr ist sie als Redakteurin bei Netzpolitik.org tätig. Desweiteren ist sie eine Sprecherin des Chaos Computer Clubs und auch als Buchautorin und Bloggerin aktiv.

Auf der anderen Seite ist der Trend in den letzten Jahren, auch nach Snowden, immer stärker gewachsen, dass Firmen Nutzer belohnen, wenn Daten preisgegeben werden. Was hältst du davon?
Ich glaube, diese Intensivierung über diese Fitnesstracker und Versicherungen wird zunehmen. Das wird auch deswegen zunehmen, weil viele Leute Spaß daran haben, sich zu vermessen.

Wenn ich mir selber einen Fitnesstracker kaufe, dann bin ich mir dessen sehr wohl bewusst und kann mich nicht rausreden. Was anderes ist es, wenn jemand hinter meinem Rücken Daten abgreift. Zum Beispiel Mobiltelefone haben eine hohe Sensorik und können Bewegungen messen. Es geht darum, ob es mit deinem Einverständnis stattfindet oder eben nicht.
Es gibt einen weiteren Trend, der aus amerikanischen Polizeistellen nach Deutschland herüberschwappt. Die Gefahrenerkennung von Verbrechen, die überhaupt noch nicht begangen wurden. Wie findest du es, nach solchen Systemen einzelne Personen zu bewerten?
In den USA fand ich das insofern interessant, dass dieser Modellversuch auch Social-Media einbezieht. So werden beispielsweise in Echtzeit Daten über jemanden herangezogen, der in einer Notrufzentrale anruft. Nicht nur den Beruf, sondern auch der Sprache oder Geschlecht. Da gab es einen interessanten Fall: Eine weibliche Person hat ein Computerspiel gespielt, das heißt *Rage* und darüber hat sie auch getwittert und auf Facebook Sachen geteilt. Das änderte ihren Score-Wert, weil das Wort *Rage*, was so viel wie Wut bedeutet, sehr oft auftauchte, weswegen man automatisiert eine andere Einstufung dieser Person vornahm. Das sind ethische Fragen. Und das kann passieren, weil natürlich die Auswertung nicht semantisch ist.

»Die Frage ist jetzt, ob genug Leute ihr Verhalten ändern und damit die Politik beeindrucken.«

Die Frage ist ja: Dürfen wir Daten gegen Anschläge abwägen? Dürfen wir Daten sammeln, um einen Anschlag zu verhindern, wo beispielsweise 20 Menschen sterben würden.
Ich denke, da muss man etwas unterscheiden: Sammele ich diese Daten, weil ich konkrete Verdachtsmomente habe oder sammele ich einfach alle? Eine Vorratsdatenspeicherung, wo erstmal alles erfasst wird, was möglich ist, halte ich für falsch. Aus Verhältnismäßigkeitsgründen, aber auch, weil ich der Meinung bin, dass Grundrechte wie Privatsphäre ein hohes Gut sind. Wenn es aber um konkrete Verdachtsfälle geht, dass jemand Gewalt ausüben will, dann halte ich das für richtig. Dass sie das in vielen Terrorfällen nicht hinbekommen haben, obwohl die Täter längst auf allen Listen waren, steht auf einem anderen Blatt. Das ist eine Frage der Effizienz der Polizeiarbeit.
Es können auch die Falschen verdächtigt werden. Das heißt, man kann auch durch eine falsche Äußerung in dieses Raster geraten, dass man überwacht wird.
Es kann manchmal auch Menschen treffen, die dem Staat nicht passen. In der Geschichte der Demokratie ist das relativ häufig vorgekommen. Als Beispiel kann man Martin Luther King nehmen, der damals von den US-amerikanischen Behörden verfolgt, bedroht, genötigt wurde.
Könnte das durch transparentere Behörden gedeckt werden?
Gerade im Bereich der Strafverfolgung gibt es eine ganze Menge nachgelagerter Prüfungen, weil der Verdacht auf eine Straftat irgendwann zu einem Gerichtsverfahren führt,

Tipps, um seine Identität im Internet zu schützen

CYBER GHOST
Anbieter von sogenannten VPN-Servern wie beispielsweise CyberGhost ermöglichen einen verschlüsselten Datenverkehr. Dabei baut der Anwender eine verschlüsselte Direktverbindung zu einem VPN-Server auf, der den Nutzer mit einer neuen IP-Adresse versorgt. Über diesen VPN-Server laufen alle geöffneten Webseiten oder Datenverbindungen, sodass der eigentliche Benutzer nur mit erhöhtem Aufwand zu ermitteln ist.

TOR
Noch etwas sicherer ist die Nutzung des Tor-Projektes. Auch bei dieser Funktionsweise wird der Nutzer mit einer neuen IP-Adresse versorgt, allerdings nicht von einem festen Server, sondern werden die Daten durch drei Knoten geleitet, die alle zehn Minuten wechseln.

KEEPASS 2
Besser als die Speicherung von Passwörtern direkt im Browser ist die Nutzung von Passwortmanagern. Angenehm ist die Verwendung des quelloffenen Programms KeePass 2, das auch als App zur Verfügung steht. Eine verschlüsselte Schlüsseldatei kann nur mit dem sogenannten Master Key geöffnet werden und mit der Auto-Type-Funktion können Passwörter mit einem Tastenkürzel automatisch eingefügt werden.

OWNCLOUD
Owncloud ist eine Dropbox-Alternative, die auf einem lokalen Server speichert, somit weiß man wo die Daten liegen und muss sich bei sensiblen Daten keine Gedanken machen, dass Unbeteiligte mitlesen können. Für die Einrichtung des Servers und die Installation der Owncloud ist allerdings auch ein klein wenig Fachwissen nötig.

wo man rechtliche Dinge überprüft. Da hat man einen Anwalt. Anders sieht es im Geheimdienstbereich aus, da ist wenig Kontrolle. Und das hat sich auch in dem NSA-Untersuchungsausschuss gezeigt, dass die parlamentarischen Kontrolleure vielfach gar nichts wussten.

Der Verfassungsschutzpräsident Hans-Georg Maaßen will ja diese Kontrolle am liebsten abschaffen, da er den Abgeordneten nicht traut.

Ein Geheimdienst ist ja auch in gewisser Weise inhärent. Deren Business ist, ihre Strukturen geheim zu halten. Sie haben natürlich Interesse an der Ausweitung ihrer Fähigkeiten. Sie nutzen Freiräume und kontrollfreie Räume aus. Das ist ein Kennzeichen von Geheimdiensten.

Haben denn dann Geheimdienste in einer Demokratie überhaupt noch Daseinsberechtigung?

Bei den Geheimdiensten ist in der Vergangenheit viel schief gegangen: Die amerikanischen Dienste haben etwa nachweislich gefoltert. Der deutsche Auslandsnachrichtendienst hat radioaktives Material geschmuggelt und sich eine Weltraumtheorie ausgedacht. Die Frage ist, was man in Zukunft möchte. Sollen diese Dienste weiterhin geheim operieren oder will man sie auf nachrichtenorientierte Dienste reduzieren, die die Faktenbasis für politische Entscheidungen sammeln? Natürlich wünsche ich mir eine Welt, wo wir Geheimdienste nicht brauchen, denn insgesamt ist die Bilanz dieser Dienste negativ. Sie verursachen mehr Schaden als Nutzen. Ich bezweifele aber, dass das auch die Mehrheit der Bevölkerung so sieht.

Was ist denn jetzt aber für den einzelnen Bürger schlimmer, die Überwachung durch die Geheimdienste oder das Datensammeln von Unternehmen?

Das konvergiert ja. Das ist die Essenz aus den Snowden-Veröffentlichungen, dass die amerikanischen Geheimdienste intensiv Daten von kommerziellen Unternehmen ausnutzen. Der Unterschied ist der, dass ich mich aktiv dafür entscheide. Ich kann eine Gmail-Adresse haben oder auch nicht. Ich kann mich bei Facebook anmelden oder auch nicht. Ich kann freie Alternativen nutzen oder auch nicht. Bei der staatlichen Überwachung habe ich diese Wahl nicht.

Ist das Internet dann dadurch, dass kommerzielle Geschäftsmodelle immer übermäßiger geworden sind, immer noch der freie Platz, der es einmal war?

Ich glaube, das Netz ist schon lange kein utopischer Ort mehr – die Kommerzialisierung ist 15 Jahre her. Das ist ein kommerzielles Netz und viele politische Entscheidungen orientieren sich an ökonomischen Parametern. Wenn man sich aber die Technik ansieht, ist vieles möglich. In seinem Herzen ist das Internet eine offene Struktur.

Also obwohl das Internet so kommerziell ist, hat es die Grundidee, ein freier Raum zu sein, noch nicht aufgegeben?

Ich denke, das emanzipatorische

»Man sollte den Schutz vor Überwachung mit in seine Bedürfnispyramide aufnehmen.«

Potenzial hat es auf jeden Fall. Ich bin frei die Technik zu nutzen: Natürlich braucht man manchmal ein gewisses technisches Know-How. Oder man hat eine Community, die das Know-How zur Verfügung stellt und das für andere Ziele als Profit. Was cool ist.

Was müsste denn getan werden, um den normalem Nutzer zu schützen?

Das Erste ist ein gewisses Bewusstsein dafür, aber das gilt für alle Verbraucherthemen. Man muss sich entscheiden: Welches Betriebssystem hole ich mir? Was für eine Hardware nehme ich? Was für Apps hole ich ich mir? Wo hole ich mir meine Mail-Adresse? Man sollte den Schutz vor Überwachung mit in seine Bedürfnispyramide aufnehmen.

Constanze, wir danken dir für das Interview!