# Ein anderes Internet ist möglich!

14. Februar 2014 | Erstellt von Michael Kappes

**„Das Internet gab uns das große Versprechen der Befreiung und der Demokratisierung“ schrieb Glenn Greenwald in der ZEIT vom 30.10.2013 um dann, im Lichte der Enthüllungen von Edward Snowden darauf hinzuweisen, dass inzwischen der Überwachungsstaat die Macht im Netz ergreife. „Er will dieses Werkzeug der Freiheit in sein Gegenteil verkehren, in ein Werkzeug der Überwachung und Kontrolle. Wir stehen an einem Scheideweg.“**

**Der Beitrag geht der Frage nach, wie real die Gefahren tatsächlich sind und welche Möglichkeiten es gibt, sich individuell und kollektiv gegen sie zu schützen.**

## Die NSA-Affäre

Die sogenannte NSA-Affäre begann im Sommer 2013 mit ersten Hinweisen in der englisch sprachigen Zeitung Guardian. Im Juni wurden Dokumente veröffentlicht, die das PRISM Programm offenlegten. Noch im gleichen Monat „outete“ sich Edward Snowden als Übermittler (Whistleblower) dieser geheimen Daten. Einzelheiten wie das massenweise und weltweite Abgreifen von Kreditkarten-Daten und die Zusammenarbeit der NSA mit den Britischen Geheimdiensten (GCHQ) wurden bekannt. Die Bundesregierung zeigte sich empört und Obama wiegte ab. Guardian und die inzwischen auch dazu Stellung nehmende Washington Post legen noch einen oben auf und berichteten, dass Google und Facebook von der NSA ganz massiv angezapft werden. Die beiden Firmen-Chefs beschwichtigen, und relativieren. Der mediale Schlagabtausch brauste auf, ab Juli 2013 gibt es ständig Neues zu berichten. "Sie (die Dienste, Anmerk. MK) können buchstäblich sehen, wie Ihre Ideen entstehen, wenn Sie tippen", zitiert die Zeitung ihren Informant in der Washington Post über die Echtzeitüberwachung des Internet. Zugleich stieß die New York Times in das gleiche mediale Horn und berichtete von dem Auslandsspionage-Gesetz FISA (Foreign Intelligence Surveillance Act) von einem eigens dafür zuständigen geheimen Gericht, und obwohl die Administration in den USA davon wisse, seien Gesetz und Gericht so geheim, dass nicht einmal ihre Existenz bestätigt werden dürfe, schrieb die Zeitung. Die in FISA-Anfragen eingeforderten Daten zu übergeben sei Pflicht, so weiter im Beitrag. Es gibt also de facto keinerlei demokratische Kontrolle, wer da was (mit)liest. Die US Regierung beschwichtigte nochmals und bemühte sich um Schadensbegrenzung. Kurz darauf beschäftigte sich das britische Parlament mit dem Thema. Die politischen und medialen Kreise, die der Skandal zog, wurden immer größer. Es gibt weltweit kein medien-technisch entwickeltes Land, das nicht involviert war. Aber alle europäischen Regierungen, die sich damit beschäftigen sind seither nur um Schadensbegrenzung bemüht oder geben windelweiche Versprechen ab. Das veranlasste Glen Greenwald, US-amerikanischer Journalist, Blogger, Schriftsteller und Rechtsanwalt, in die Öffentlichkeit zu gehen und selbst Stellung zu beziehen. In der Zwischenzeit kamen immer weitere Details wie FoxAccid, ein Tool mit dem sich die NSA Zugang zu fremden Rechnern verschaffen kann und XkeyStore, eine weitere

Spionagesoftware an die Öffentlichkeit.

## Hintertüren für die Überwachung

Egal ob Facebook, Google oder Microsoft und Apple, alle arbeiten, nein sind per Gesetz dazu verpflichtet, Hintertüren für Überwachungstools in ihre Software einzubauen oder den staatlichen Überwachungsbehörden jederzeit und ohne Grund Auskunft zu geben. Mittlerweile gibt es auch in Europa Gesetze, die Internet Service Provider oder Anbieter von Massen-eMails dazu verdonnern, Technik und Infrastruktur anzubieten, die einen automatischen Zugriff der Sicherheitsbehörden zulassen. Die sogenannte „Lawfull Interception“ - also die gesetzeskonforme Überwachung stellt ein grundsätzliches als auch technisches Problem dar. Für Endanwender ist es zwar nicht möglich, diese Abhör-Schnittstellen, die per Gesetz vorgeschrieben sind, zu nutzen, ohne sich strafbar zu machen. Online-Kriminelle hält dies aber nicht davon ab, die Schwachstellen zu gebrauchen.

Die Geheimdienste der USA, Großbritanniens, Australiens, Kanadas und Neuseeland, die „5eyes“, tauschen schon lange ihre Daten, die sie aus dem Netz fischen aus und der deutsche BND darf „am Katzentisch“ sitzen, wäre aber gerne auf Augenhöhe dabei. Da wundert es kaum noch, dass wir weiterhin erfahren: Skype und USCloud Dienste (MUSCULAR) haben die „NSA Backdoor per Default“ eingebaut. Lavabit, ein Dienstleister und Anbieter von sicheren eMail-Konten bricht unter dem Druck der US Regierung zusammen, als diese Einblick in Kundendaten verlangt. Das Unternehmen schließt seine Pforten. Ob es Zufall war, dass auch Edi Snowden dort einen eMail Account hatte?!.

## Unbegrenzte Überwachung?

Zügig gingen die Veröffentlichungen weiter. Verwanzte EU-Sitzungen und „Mutti's Mobiltelefon“ werden abgehört, nun steigt die politische Party ins Groteske und Herr Pofalla versucht die „NSA-Affäre“ mit einer Pressekonferenz zu beenden. Mehr Details zur NSA Affäre sprengen hier den Rahmen eines Blogbeitrages. Interessierten Leser_innen ist die als „Timeline“ umgesetzte Webseite des Heise Verlags zu empfehlen. Eine gute Visualisierung zum Thema. Und wie bei einem technischen Fachverlag nicht anders gewohnt, ist man nach ein bis drei Mausklicks auch auf der Unterseite, die erklärt, was die jeweilige Anwendung mit solchen kryptischen Namen wie PRISM, XKeyStore und die anderen so machen. FoxAcid beispielsweise kann automatische und personifizierte Angriffe gegen jeden PC starten. FoxAcid weiß sogar ob es sich um den PC eines Software Entwicklers oder einer politisch interessierten Alleinerziehenden handelt. Gruselig? Nein, so etwas lässt sich alles aus unserem Surfverhalten heraus rechnen.

## Sicher im Netz bewegen

Wer will, kann seine eMails mit den richtigen Tools schnell und einfach verschlüsseln und für das Surfen im Internet TOR-Server nutzen, die ihn anonymisieren. Verschlüsselung ist „gut

und schön“ aber was die NSA nicht knacken kann, kann sie für ewige Zeiten speichern und später auswerten. Zum Teil brechen sie auch in Systeme ein, um die noch oder schon wieder unverschlüsselten Daten abzugreifen, denn das ist vergleichsweise einfach. Dafür ist unter anderem die Abteilung TAO (Tailored Access Operation) zuständig, die neben Servern und Endbenutzer-Systemen auch Router und Switches auf der (Einbruchs-)Liste hat. Und selbst bei RSA, einem Verschlüsselungs-Prinzip, versucht die NSA direkt in der technischen Spezifikation Veränderungen vorzunehmen. Aber die wichtigste Essenz: Verschlüsselung oder Kryptografie funktioniert. Sie wird aber komplett mitgeschnitten und nicht nur dazu gibt es eine regelrechte Überwachungsindustrie.) TOR Anonymisierung funktioniert grundsätzlich auch. Aber weil es zu wenige Internet-User nutzen, können einzelne TOR-Benutzer identifiziert werden. Die technischen Möglichkeiten, Überwachung zu erschweren oder zu verhindern ist nur eine Seite der digitalen Zukunftsgesellschaft. Genauso wie bei der sogenannten Finanzkrise, brauchen wir eine soziale und politische (Bürger)-Bewegung, die sich der digitalen Krise im politischen Sinne annimmt.

## Vorratsdatenspeicherung

Unsere Gesellschaft hat sich fast schon ein bisschen an die täglichen Horrormeldungen von Snowden gewöhnt. Und Bruce Schneier macht sich einen Spaß daraus, die TAO-Applikation des Tages vorzustellen. Einerseits hält das das Thema auf der politischen Tagesordnung und auf der anderen Seite ist es auch so etwas wie eine Lebensversicherung des Herrn Snowden. Die Politik in Europa macht aber ungerührt weiter, aktuellstes Beispiel hierfür ist die Debatte über die Vorratsdatenspeicherung. Internetminister Maas möchte in Deutschland die VDS solange aussetzen, bis das EU Gericht über eine gesetzeskonforme Umsetzung entschieden hat. Im Umkehrschluss heißt das, dass die VDS kommen wird. Dann eben mit „EU Segen“. Der Widerstand gegen die VDS läuft schon lange. 2007 fand die erste ‚Freiheit statt Angst‘-Demo gegen sie statt. Und im Jahr 2014 wird das Thema sicherlich wieder mehr als „up to date“ sein. Also ziehen wir uns warm an, für die digitale Eiszeit. Damit wir aber nicht erfrieren, sollten wir uns auch politisch und sozial auf den Weg machen, das Netz, unsere Kommunikation und unsere persönlichen Daten wieder zurück zu erobern. Es wird ein langer und kalter Weg. Aber auch hier gilt: Ein anderes Internet ist möglich. Packen wir's an.