07. September 2013, von Michael Schöfer
Denn sie wissen nicht, was sie tun

Vor ein paar Jahren hat mir mal jemand gesagt, es soll Menschen geben, die vorsichtshalber stets zwei Computer benutzen: Einer, mit dem sie ins Internet gehen. Und ein zweiter, der ständig offline ist und mit dem sie arbeiten. Warum? Aus Angst, sie könnten überwacht werden. Damals klang das in meinen Ohren nach einer kruden Verschwörungstheorie. Etwas abseitig, fast schon als pathologisch zu bezeichnen. Nun muss ich im Lichte der neuen Erkenntnisse Abbitte leisten. Die Wirklichkeit ist noch viel schlimmer. Nicht nur Einzelpersonen werden überwacht, sondern gleich das ganze Internet. Praktisch alles.

Nach Berichten der New York Times und des Guardian können die Nachrichtengeheimdienste NSA und GCHQ gängige Verschlüsselungstechniken für E-Mails, Banküberweisungen oder Telefonate knacken. Bruce Schneier, ein amerikanischer Computerexperte, der an der Entwicklung von Kryptografiealgorithmen mitgearbeitet hat, warnt sogar ausdrücklich vor kommerziellen Anbietern von Verschlüsselungssoftware. "Er schätzt, dass die meisten Produkte großer US-Firmen NSA-Hintertüren haben, viele Produkte aus anderen Ländern ebenso – oder zumindest entsprechende Lücken für den jeweiligen Landesgeheimdienst. Closed-Source sei insgesamt anfälliger für Hintertüren als Open Source." [1] Schneier benutzt deshalb u.a. GPG und TrueCrypt. Wobei selbst das, sofern Betriebssysteme wie Windows oder Mac OX insgeheim Backdoors enthalten, kein unüberwindliches Hindernis darstellt. Wer heimlich Zugang zu einem Computer hat, der kann dort auch leicht Schlüsseldateien entwenden und Passwörter abschöpfen. Nutzer von Tor, einem Netzwerk, das anonymes Surfen erlauben soll, sind offenbar ebenfalls recht schnell identifizierbar. [2] Mit anderen Worten: Es gibt momentan anscheinend überhaupt keinen Schutz mehr. Jedenfalls nicht für Menschen, die keine IT-Koryphäen sind.

Edward Snowden habe der NSA unermesslichen Schaden zugefügt, heißt es. "Auf einer Skala von 1 bis 10 entspricht der Schaden einer 12." [3] Das war jedoch bevor bekannt wurde, wie wenig selbst Verschlüsselungsmethoden vor den Geheimdiensten schützen. Inzwischen dürfte der Schaden auf der Skala einer 15 entsprechen. Tendenz: weiter steigend. Aber Hauptsache, die schwarz-gelbe Bundesregierung ist gelassen: "Danach gefragt, was Kanzlerin Angela Merkel (CDU) zum Schutz der Privatsphäre der Bürger unternehme, sagte Vize-Regierungssprecher Georg Streiter, sie sei hier zunächst einmal nicht gefragt. Das Bundesinnenministerium will seine Haltung zu Verschlüsselungen nicht überdenken. 'Wir haben keine Anhaltspunkte dafür, dass die Behauptungen von Herrn Snowden zutreffend sind; insofern raten wir weiter zur Verschlüsselung', sagte Sprecher Jens Teschke. Es gebe sicher Geheimdienste, die E-Mails ausspähen, allerdings nicht Dienste befreundeter Länder." [4] Soso, "keine Anhaltspunkte" und "nicht Dienste befreundeter Länder". Die zur Schau gestellte Naivität spottet jeder Beschreibung.

Von dieser Bundesregierung ist also keine Hilfe zu erwarten. Verständlich, denn warum sollte sie ein Interesse daran haben, dass sich die Bürger wirksam vor der Bespitzelung der Sicherheitsbehörden schützen können? Sie will uns ja selbst so gut es eben geht überwachen und würde sich dadurch nur ins eigene Fleisch schneiden. Muss man daran erinnern, dass etliche ihrer Gesetzesvorhaben erst vor dem Bundesverfassungsgericht gescheitert sind (Online-Durchsuchung, akustische Wohnraumüberwachung)? Die Aktivitäten von NSA und GCHQ werden natürlich pflichtgemäß verurteilt. Augenzwinkernd, versteht sich. Angela Merkel: "Das Abhören von Freunden mit Wanzen in unseren Botschaften und EU-Vertretungen geht nicht. Wir sind nicht im Kalten Krieg." [5] Wer genau liest, merkt, dass die Kanzlerin von Botschaften und EU-Vertretungen gesprochen hat, nicht von den Bürgerinnen und Bürgern.

Aber auch Letztere haben die Bespitzelung durch die Geheimdienste bis dato zurückhaltend aufgenommen. Doch das könnte sich nun ändern. Denn wer bislang bloß ein mulmiges Gefühl hatte, dass ihm NSA und GCHQ beim täglichen Porno-Konsum über die Schulter blicken, könnte in puncto Online-Banking plötzlich hellhörig werden. Immerhin besteht die Möglichkeit, dass ihm jemand die Sparkonten leerräumt und den Überziehungskredit bis zum Anschlag ausreizt. Das werden die Geheimdienste niemals machen, erwidern Sie vielleicht. Nein, natürlich nicht, die halten sich bekanntlich immer streng an die Gesetze. Außerdem könnten die Programme, mit denen die Geheimdienste arbeiten, in die Hände von Kriminellen fallen. Wie Wikileaks gerade enthüllt hat, wird zumindest ein Teil der Überwachungssoftware von Privatunternehmen hergestellt und obendrein an zwielichtige Regime verkauft. [6] Wer aus Profitgier Despoten beliefert, könnte aus den gleichen Motiven heraus auch andere Dunkelmänner in der Kundenkartei führen. Wer will das ausschließen? Niemand! Falls der Überwachungsskandal das Wahlverhalten beeinflusst, wird die Bundesregierung ihre provozierende Gelassenheit vermutlich schnell verlieren.

Es gibt freilich noch ein viel grundlegenderes Problem. In Bezug auf Syrien erleben wir ja gerade, dass Bürger und Parlamentarier gegenüber ihren Regierungen viel misstrauischer geworden sind. Folge der haarsträubenden Lügen von einst. Hier gilt inzwischen: Wer einmal lügt, dem glaubt man nicht... Verlieren Bürger und Unternehmen das Vertrauen in die Sicherheit des Internet, könnte das unter Umständen fatale Auswirkungen auf deren Verhalten haben. Der Wachstumsmotor Digitalisierung gerät eventuell ins Stottern. Firmen, die auf das Vertrauen ihrer Kundschaft angewiesen sind, könnten sogar pleitegehen. Was wird aus Microsoft, wenn viele User auf Ubuntu umsteigen? Nach den heute gültigen Gesetzen darf in den USA ein Software-Unternehmen noch nicht einmal darüber reden, ob es von der Regierung zu irgendetwas gezwungen wurde, wie zum Beispiel den Einbau einer Backdoor. Das Misstrauen wird folglich grenzenlos, weil überhaupt kein Vertrauen mehr vorhanden ist. Doch ohne ein Mindestmaß an Vertrauen kann die Wirtschaft eigentlich nicht funktionieren. Das wirkt sich selbst auf die Rechtsprechung aus. Wie will man jemand aufgrund von Beweisen auf Datenträgern überführen, wenn Dritte potentiell Zugriff darauf haben? Jeder digitale Beweis könnte im Lichte der aktuellen Enthüllungen gefälscht bzw. untergeschoben sein. Welches Gericht will das jetzt noch ausschließen?

Vollkommen abwegig, meinen Sie? Dann lesen sie mal das: "Die HSH Nordbank hat sich beim früheren Leiter ihrer New Yorker Filiale dafür entschuldigt, dass im Rahmen seiner Kündigung der Verdacht aufgekommen war, er habe mit Kinderpornografie zu tun. Nach monatelangen Verhandlungen gab die Bank damit eine Ehrenerklärung für Roland K. ab. K. war im September 2009 fristlos entlassen worden; am selben Tag hatte ein 13-köpfiges Team der Bank, dem auch der kürzlich gekündigte Chefjustitiar Wolfgang Gößmann angehörte, K.s Bürocomputer in New York durchsucht. Sie fanden E-Mails, die zu Kinderporno-Fotos geführt hatten." [7] Das belastende Material sei K. untergeschoben worden, um ihn leichter loszuwerden. [8] Die HSH Nordbank ging aus der Fusion der Hamburgischen Landesbank mit der Landesbank Schleswig-Holstein hervor und befindet sich mehrheitlich in Staatsbesitz. Kaum ein Unternehmen, denkt man, könnte seriöser sein. Die Bank bestreitet nach wie vor, K. die Kinderpornos untergeschoben zu haben. Aber es bleibt offen, wer sonst daran ein Interesse gehabt haben könnte. Und jetzt übertragen Sie den Fall gedanklich einmal in die Sphäre der Geheimdienste und bringen einen missliebigen Oppositionspolitiker oder unbequemen Enthüllungsjournalist wie Glenn Greenwald ins Spiel.

Die Geheimdienste wissen gar nicht, was sie tun. Okay, sie überwachen, das wissen sie schon. Aber sind sie sich auch über die weitreichenden Konsequenzen ihres Verhaltens im Klaren? Ich fürchte, nicht. Und die Politiker, die wenigstens nominell die Aufsicht über die Geheimdienste ausüben, ebenso wenig. Snodens Enthüllungen sind noch viel zu jung, um

schon jetzt alle Folgen aufzuzeigen. Die Aufarbeitung hat ja eben erst begonnen. Und wo uns das Ganze am Ende hinführen wird, ist genauso unbekannt. Die Geschichte des Internet wird sicherlich dereinst eingeteilt werden in eine Zeit vor, und in eine Zeit nach Snowden.

[1] Heise-Online vom 06.09.2013
[2] Heise-Online vom 04.09.2013
[3] Heise-Online vom 30.08.2013
[4] Heise-Online vom 06.09.2013
[5] Focus-Online vom 03.07.2013
[6] Bayerischer Rundfunk vom 04.09.2013
[7] Spiegel-Online vom 19.03.2011
[8] Spiegel-Online vom 28.08.2010
