06. Januar 2019, von Michael Schöfer
Die digitale Schizophrenie

Es ist anders, wenn man selbst betroffen ist, nicht wahr? Solange nur wir Bürger unter der Bespitzelung leiden, sieht man keinen dringenden Handlungsbedarf. Im Gegenteil: "Der Bundesnachrichtendienst (BND) darf weiterhin in großem Umfang Daten beim Internet-Knoten De-CIX aus Frankfurt am Main abzapfen", urteilte das Bundesverwaltungsgericht im Mai vergangenen Jahres. [1] Doch wenn massenhaft Daten von Politikern im Netz auftauchen, die zuvor von irgendwelchen Hackern erbeutet wurden, wertet man das Ganze gleich als "schwerwiegenden Angriff auf das Recht auf Privatsphäre und damit einen Grundpfeiler unserer Demokratie" (Bundesjustizministerin Katarina Barley). Nicht, dass diese Bewertung grundsätzlich falsch wäre, doch spiegelt die Reaktion von Barley bloß die vorherrschende digitale Schizophrenie wider.

Wie Ende 2017 aus den Sondierungsgesprächen von Union, FDP und Grünen verlautete, sollten Behörden ihnen bekannte IT-Sicherheitslücken nicht mehr horten, sondern unverzüglich dem Bundesamt für Sicherheit in der Informationstechnik (BSI) melden. [2] Doch dazu kam es nie, denn Jamaika ist bekanntlich an der FDP gescheitert. Im Koalitionsvertrag von CDU, CSU und SPD steht zur Cybersicherheit: "Die Hersteller und Anbieter digitaler Produkte und Dienstleistungen müssen Sicherheitslücken bekanntmachen und schnellstmöglich beheben." [3] Wohlgemerkt, die Hersteller und Anbieter, nicht die Behörden. Besser wäre eine gesetzliche Verpflichtung, dass die Behörden ihrerseits die Hersteller unverzüglich über entdeckte Sicherheitslücken informieren müssen.

Ein Teil der Regierung setzt sich durchaus für mehr Sicherheit im Cyberraum ein, der andere Teil befürchtet jedoch daraus resultierende Nachteile für die Sicherheitsbehörden. So hat sich beispielsweise das Auswärtige Amt 2017 dafür eingesetzt, "sogenannte Zero-Day-Exploits - Schadsoftware, die bislang unbekannte Sicherheitslücken ausnutzt - international zu ächten". Der Bundesnachrichtendienst hingegen will solche Sicherheitslücken nutzen, um in fremde Computersysteme einzudringen. [4] Auf dem letztjährigen Digital-Gipfel der Bundesregierung setzte sich Thomas Kremer, Vorstandsmitglied der Deutschen Telekom, für den Verzicht auf das Horten von Schwachstellen ein. Bundesinnenminister Horst Seehofer wollte allerdings auf "die aktive Abwehr von Attacken zumindest als Option nicht verzichten". [5] Eine Option, für die er naturgemäß auf die Existenz von nicht beseitigten Schwachstellen angewiesen ist. Ein unauflöslicher Zielkonflikt also.

Mit weitreichenden Folgen: So hat etwa die Cyberattacke, die im Jahr 2017 mithilfe der WannaCry-Ransomware weltweit zahlreiche Computersysteme lahmlegte, "eine von der National Security Agency (NSA) gefundene bzw. entwickelte Lücke verwendet". [6] Der US-Nachrichtengeheimdienst nutzte sie zuvor über mehr als fünf Jahre, ohne Microsoft darüber zu informieren. Und sie tat das obendrein erst, als Hacker der NSA das Wissen um die Sicherheitslücke entwendeten. Wie man daran sehe, könne aus dem Horten von Sicherheitslücken durch Regierungen der Zivilbevölkerung großer Schaden entstehen, sagte der Chefjurist des Software-Herstellers Microsoft.

Die deutschen Behörden machen bei dem Cyberangriff auf die Politiker keine gute Figur, sie hinterlassen vielmehr einen chaotischen Eindruck. Ob sie bei einem organisierten Angriff auf die digitale Infrastruktur unseres Landes abwehrbereit wären, ist angesichts dessen stark zu bezweifeln. Angeblich haben die deutschen Sicherheitsbehörden die NSA bei der Aufklärung des Falles um Hilfe gebeten. Ausgerechnet die NSA! Mit der eigenen Expertise scheint es also nicht so weit her zu sein. Wie dem auch sei, jedenfalls muss sich die Politik endlich entscheiden: Entweder will sie Sicherheitslücken weiterhin gezielt aus-

nutzen oder das Netz sicherer machen - beides zugleich geht nicht. Man kann nicht bei Bedarf in alles reinkommen wollen (Stichwort: Staatstrojaner) und gleichzeitig vor den Angriffen anderer geschützt sein. So gesehen wirkt die aktuelle Aufregung um die Veröffentlichung sensibler Daten von Politikern, nun ja, ein bisschen gekünstelt. Der Gesetzgeber hätte es selbst in der Hand, für mehr Sicherheit zu sorgen. Da er - siehe oben - bislang bewusst darauf verzichtet hat, wäre betretenes Schweigen der Politiker wesentlich angemessener. Zumindest von denen, die den Regierungsparteien angehören.

[1] heise.de vom 31.05.2018
[2] heise.de vom 15.11.2017
[3] CDU, Koalitionsvertrag 2018, Seite 45, PDF-Datei mit 8,3 MB
[4] Die Zeit-Online vom 09.10.2017
[5] heise.de vom 04.12.2018
[6] WinFuture vom 15.05.2017
