

Vertrauen ist gut, dagegen stimmen besser

15. April 2016

von Volker Birk, NZZ

NZZ-Redaktor Jan Flückiger fordert eine zeitgemässe Strafverfolgung ein. Diese Forderung teilen die Büp-Gegner. Das mag überraschen, wenn man die Allianz gegen das Büp nicht kennt.

Ständerat und Nationalrat haben sich am Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs nicht gestossen. Sie sollten es aber tun. Das gemeinsame Ziel aller Demokraten ist hier die Förderung des Rechtsstaates. Ein Grossteil der Projektträger des Büp-Referendums sind immerhin Bürgerrechtler. Und Bürgerrechte bestehen in der Praxis ohne den Rechtsstaat nicht. Über die Art und Weise, wie die genannte Rechtsstaatsförderung jedoch genau ausschauen soll, kann und muss diskutiert werden. Denn die Gesetzesvorlage fährt weiter auf einem Weg, der bisher keinen Erfolg vorweisen kann, dafür aber wesentliche Elemente der freien Gesellschaft in Frage stellt.

Ein Blick auf den Originaltext des Büp-Entwurfes zeigt die Stossrichtung: noch mehr Vorratsdatenspeicherung, IMSI-Catcher, Staatstrojaner. Dabei sind alle drei Mittel höchst fragwürdig in einer Strafuntersuchung. Zur Vorratsdatenspeicherung ist vor den Verfassungsgerichten Europas bis hin zum Europäischen Gerichtshof viel gesagt worden. Die Urteile aller Verfassungsgerichte und auch des EuGH sind im Tenor praktisch gleichlautend: die Massnahme ist unverhältnismässig. Nun besitzt die Schweiz kein Verfassungsgericht. Es kann entsprechend für den Stimmbürger lohnend sein, die europäischen Urteile zur Kenntnis zu nehmen - und vor allem auch, wie es dazu kam.

Erfolgsbeispiele gesucht

Denn bei jedem solchen Prozess, sei es in Deutschland, in Tschechien oder in Luxemburg, ist von den Gegnern der Vorratsdatenspeicherung an ihre Befürworter dieselbe Frage gestellt worden: man möge bitte die Fälle aufzeigen, bei denen diese Massnahme eine positive Wirkung zur Aufklärung schwerer Verbrechen gezeigt hat. Und vor keinem einzigen Gericht, in keinem der Prozesse konnte auch nur ein einziger solcher nachvollziehbarer Fall vorgebracht werden. Eine bemerkenswerte Argumentationsnot, in die man die Befürworter mit einer derart einfachen Frage bringen kann - jedoch für Insider nicht überraschend.

Sehr gut auf den Punkt gebracht hat das Versagen der Vorratsdatenspeicherung der Technikchef von Europol, Michel Quillé, in einer Podiumsdiskussion zum Thema Cybercrime in Genf, an der der Autor dieser Zeilen ebenfalls teilnahm. Quillé erklärte in seiner Eigenschaft als Executive President of the Forum International des Technologies de Sécurité: «You have to be swift!» Daten, die Wochen oder gar Monate alt sind, helfen bei einer Strafermittlung gegen das organisierte Verbrechen wenig. Statt der Vorratsdatenspeicherung wünscht sich der Experte «Quick Freeze», also den sofortigen Zugriff auf Daten, die aktuell beim Provider anfallen. Keiner der Büp-Gegner hätte damit ein Problem. Leider ist die Stossrichtung des Büp genau entgegengesetzt.

Hoher Preis

Bei den IMSI-Catchern kann wenigstens festgestellt werden, dass sie überhaupt funktionieren. Jedoch zu welchem Preis! Bei einem IMSI-Catcher geht es um ein Gerät, was eine Funkzelle simuliert, so dass sich damit alle Mobiltelefone in der Nähe überwachen lassen. Und genau das passiert auch: Man überwacht wirklich alle Funktelefone gleichzeitig quasi per Streusschuss. Wer jetzt die Stirn runzelt, liegt richtig: Es leuchtet wohl jedem ein, dass die Strafverfolgungsbehörden Telefone beispielsweise von Verbrechern der Mafia abhören können müssen, wenn sie einen konkreten Verdacht vorliegen haben, dass mal wieder etwas im Busch ist. Weshalb jedoch soll man die Telefone von Tausenden von unbescholtenen Bürgern überwachen, nur um dann nachträglich herauszufinden, dass gar nichts Relevantes dabei war?

Leider passiert mit IMSI-Catchern meistens letzteres. Die Meldungen aus dem nahen Ausland, in dem IMSI-Catcher schon länger eingesetzt werden, sind entsprechend alle gleichlautend: «Funkzellenabfrage in München: Polizei rasterte an einem Tag eine halbe Million Handy-Daten von 70.000 Menschen», berichtete beispielsweise das Portal Netzpolitik.org bereits 2014. Das Ergebnis auch bei dieser Massnahme: kein Treffer. Der Tenor solcher Meldungen ändert sich nicht, alleine die Zahlen werden immer grösser und absurder. Es fragt sich, ob sich die Schweiz wirklich solchen Massnahmen anschliessen sollte. Nicht nur gefährden sie die Meinungsfreiheit, wenn man nie mehr weiss, wer gerade mithört. Schwerverbrecher fängt man auch nicht dadurch, dass man ein Schleppnetz durch den Gartenteich zieht.

Trügerische Hoffnung

Völlig unverständlich ist für Experten jedoch das Festhalten am sogenannten Staatstrojaner, also dem Verwanzen von Endgeräten durch die Behörden. Aus der Pleite, die die Kapo Zürich mit dem italienischen Anbieter Hacking Team erlebt hat, würde die Politik nun schon die richtigen Schlüsse ziehen, meinten einige. Diese Hoffnung hat sich leider als trügerisch erwiesen. Offenbar ist das Hauptproblem solcher Staatsvirensoftware weiters unverstanden: die Beweiskraft der damit gesammelten Ergebnisse ist praktisch Null. Das liegt jedoch nicht nur an technischen Problemen - jene könnten ja irgendwann behoben werden. Sondern es ist ein prinzipielles und damit unlösbares Problem der Vorgehensweise, dass die Polizei statt offen aufzutreten derart selbst wie ein Einbrecher und Computerkrimineller verfährt.

Es sei an dieser Stelle noch einmal explizit darauf hingewiesen: der Hacking Team-Trojaner hat eine dokumentierte Funktion namens Upload Childporn. Es ist also Teil der offiziellen Funktion dieser Angriffssoftware, dass man Beweise unterjubeln kann, und zwar erklärtermassen solche, gegen die man sich kaum mehr zu verteidigen weiss, wird man einmal Opfer solcher Umtriebe. Wenn jetzt NZZ-Redaktor Flückiger zurecht darauf hinweist, dass man in die Behörden auch Vertrauen haben muss, so geht seine Argumentation damit leider völlig an der Sache vorbei. Denn selbst wenn die Kapo Zürich diesen Staatstrojaner einsetzt - und die Kapo geniesst verdientermassen einen exzellenten Ruf - so ist es eben gerade nicht nur sie, die diese Funktion auslösen kann.

Die Macht ist mit dem Programmierer

Man kann es gar nicht genug betonen: Macht über ein Softwareprogramm hat immer und zuallererst der Hersteller dieses Programmes. Was der Anwender - im Beispiel die Kapo Zürich - wünscht, äussert er durch das Benützen der Bedienoberfläche. Was das Programm jedoch in Wirklichkeit macht, das bestimmt einzig und alleine der Programmierer. Und der arbeitet in einem dubiosen und höchst zweifelhaften Laden wie Hacking-Team, oder einem der anderen Anbieter in diesem per se grauen Markt.

Tatsächlich ist die Lage sogar noch schwieriger. Denn Hersteller wie Hacking Team oder ihre Mitbewerber sind es gar nicht, die den eigentlichen Angriffscodes schreiben. Sie kaufen nämlich die Zero Day Exploit genannten Teilprogramme, die die eigentlichen Angriffe ausführen, selbst zu. Wer jetzt nicht genügend Fantasie entwickelt, wie denn der Markt wohl gestaltet ist, auf dem man solche Informationen und Programme erwerben kann, dem sei hier einmal deutlich gesagt: es ist er ist nicht grau, sondern tiefschwarz.

Zusatzfunktion eingebaut

Nun wird sich der geneigte Leser wohl fragen, wie man die Mafia bekämpfen kann, indem man sie finanziert. Tatsächlich ist es jedoch sogar noch schlimmer: Noch einmal, was ein Programm tatsächlich macht, das bestimmt nur und ausschliesslich der Programmierer. Und der ist jetzt ausgerechnet bei den Programmteilen, die die eigentlichen Angriffe durchführen, für gewöhnlich selbst Teil des organisierten Verbrechens. Muss die Frage, wie zuverlässig eine solche Software ausschliesslich dem Gesetz folgend agiert, wirklich noch gestellt werden? Und glaubt irgendjemand wirklich, dass die Schwarzmarkt-Anbieter von Zero Days nur den Staatstrojaner-Hersteller beliefern, wenn man genausogut Informationen und Programme in Kopie ein zweites Mal an andere interessierte Parteien verhöckern kann, vielleicht noch mit einer kleinen Zusatzfunktion, die Zugriff auf allfällige Staatstrojanereinsätze mit einschliesst?

Jan Flückiger hat tatsächlich recht: man kann den Schweizer Behörden im Grossen und Ganzen vertrauen, und liegt damit in den allermeisten Fällen richtig. Sie, die Behörden, sind es in erster Linie nicht, weswegen man es sich zweimal überlegen sollte, ob ein Staatstrojaner wirklich ein Mittel für die Polizei in einem Rechtsstaat sein kann.

Die Schweiz hat kein Verfassungsgericht. An dessen Stelle tritt bei schwierigen und umstrittenen Entscheidungen der Stimmbürger selbst. Es steht zu hoffen, dass in diesem Falle derselbe die Weisheit haben wird, den BÜPF-Entwurf abzuweisen und der Politik aufzuerlegen, sich die Sache noch einmal gründlich zu überlegen. Es drängt sich nämlich der Eindruck auf, das sei dringend notwendig.

Der Autor ist Mitglied im Chaos Computer Club Schweiz und Stiftungsratsvorsitzender der p?p Stiftung, einer Schweizer Stiftung, die sich für die Menschenrechte auf Meinungsfreiheit, Privatheit und Informationsfreiheit einsetzt. Sowohl Chaos Computer Club als auch die p?p Stiftung sind Träger des Referendums gegen die Neufassung des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF).