Die Trojaner sind los!

24. Juni 2013

Christian Thommen, «Debatte» Nr. 25

Das Trojanische Pferd war in der griechischen Mythologie ein hölzernes Pferd, in dessen Bauch Soldaten versteckt waren. Mit dieser Kriegslist gewannen die antiken Griechen den Trojanischen Krieg. Heute wird der Begriff Trojaner für eine bestimmte Klasse von Schadsoftware verwendet, welche versteckt und von den Benutzer_innen unbemerkt wirkt.

Zu den Aktivitäten eines Trojaners gehören insbesondere das Ausspionieren von Zugangsdaten wie Benutzernamen und Passwörter sowie anderer personenbezogener Daten. Wird ein Trojaner vom einer amtlichen Stelle einer zu überwachenden Person untergejubelt, spricht man von einem «Staatstrojaner», auch wenn der Bundesrat den verniedlichenden Begriff *«Government Software»* verwendet.

Staatsschutz will Befugnisse der Strafverfolgungsbehörden

Im Juni 2007 legte der Bundesrat einen Entwurf zur Verschärfung des Staatsschutzgesetzes vor (BWIS II), welcher neu auch strafprozessuale Zwangsmassnahmen wie die Überwachung von Post, Telefon, E-Mail und Internet innerhalb der Schweiz sowie das geheime Durchsuchen von privaten Räumen und Computern, Letztere auch mit dem Einsatz von Trojanern, vorsah. Im Gegensatz zur Strafverfolgung setzt der Staatsschutz diese verdeckten Schnüffeleien aber präventiv, das heisst ohne Hinweise auf eine Straftat, ein. Allgemein stiessen die Vorschläge des Bundesrats auf breite Kritik. In der Folge haben der Ständerat am 3. März 2009 und der Nationalrat am 27. März 2009 die Rückweisung von BWIS II an den Bundesrat beschlossen.

Im Jahr 2010 erfolgte eine Vernehmlassung zur Totalrevision des Bundesgesetzes betreffend die (strafprozessuale) Überwachung des Post- und Fernmeldeverkehrs (BÜPF), welche eine zeitliche Verdoppelung der Vorratsdatenspeicherung von 6 auf 12 Monate vorsah. Als Vorratsdatenspeicherung wird die Erfassung der Verbindungs- und Rechnungsdaten, für Mobiltelefone zusätzlich auch Standortdaten und für Internetdienste dynamische IP-Adressen, bezeichnet. Neu soll der Einsatz von Trojanern für die Strafverfolgung möglich werden, ebenso Antennensuchläufe, bei welchen rückwirkend ermittelt wird, welche Nutzer_innen sich in einem bestimmten Zeitintervall in der Nähe einer spezifischen Antennenanlage befanden. Ferner sollen zudem IMSI-Catcher zulässig sein, mit welchen ermittelt werden kann, welche Mobiltelefone, auch im Ausland registrierte, sich im Moment in einem bestimmten Gebiet befinden. Wie BWIS II stiess die Totalrevision des BÜPF auf breite Kritik.

Im Oktober 2011 wurde aufgrund von Enthüllungen in Deutschland bekannt, dass ebenfalls in der Schweiz von diversen Behörden bereits Staatstrojaner eingesetzt wurden, obwohl es keine gesetzliche Grundlage dazu gibt. So wurde etwa Andrea Stauffacher, der Sprengstoff- und Brandanschläge vorgeworfen werden, ohne richterliche Genehmigung gestützt auf Artikel 280 der Strafprozessordnung mit Trojanern ausspioniert und anschliessend auch verurteilt.

Knüppeldick kam es dann im Jahr 2013: Im Februar erfolgte die Botschaft zur Totalrevision des

BÜPF, welche trotz aller Kritik die erweiterte Vorratsdatenspeicherung und Trojaner enthält, und im März gelangte das neue Nachrichtendienstgesetz (N DG), welches BWIS ablösen soll, in die Vernehmlassung. Auch hier wurden sämtliche fragwürdigen Neuerungen inklusive Trojaner aus BWIS II übernommen. Zusätzlich kam noch die Kabelaufklärung dazu, bei welcher der gesamte Internet- und Email-Verkehr aller Benutzer_innen eines Kupfer- oder Glasfaserkabels nach vorgegebenen Schlüsselwörtern durchsucht wird. Obendrein enthält das NDG eine Bestimmung, welche den Nachrichtendienst verpflichtet, strafrechtlich relevante Erkenntnisse aus der präventiven verdeckten Überwachungen der Privatsphäre von unverdächtigen Personen an die Strafverfolgungsbehörden weiterzugeben.

Gründe gegen Trojaner et al.

Begründet wird die Ausweitung der verdeckten Ermittlungen sowohl bei der Revision des BÜPF als auch beim neuen NDG damit, dass Terroristen und Verbrecher die neuesten Techniken benutzen würden und daher der Staat nachziehen müsse. Dem ist entgegenzuhalten, dass schon lange vor der Internetzeit geheime Besprechungen in privaten Räumen durchgeführt wurden, aber eine rückwirkende Erfassung nie möglich war. Erst mit der Einführung digitaler Telefonzentralen in den 1980er-Jahren und später bei Internetdiensten war eine systematische Speicherung von Verbindungsdaten möglich. Nur dadurch konnte und kann die Frage «wer hat wann mit wem für wie lange kommuniziert» für die gesamte Bevölkerung in die Vergangenheit schauend beantwortet werden. Seit diese Daten vorhanden sind, wurden sie in der Schweiz zur Strafverfolgung genutzt, zuerst auf kantonaler gesetzlicher Basis, dann ab 2002 gestützt auf das BÜPF, ohne dass Terroristen und Verbrecher durch die digitalen Telefonzentralen einen entscheidenden Vorteil gehabt hätten. Es war also der Staat, der die neue Technik ausnutzte, und nicht umgekehrt, wie vom Bundesrat in den Unterlagen zu den neuen Gesetzen behauptet wird.

Noch einen Schritt weiter geht die Überwachung für Personen, welche ständig ein Mobiltelefon auf sich tragen. Der Standort des Telefons wird regelmässig erfasst, und so lassen sich von jede_r beliebigen Abonnent_in eines mobilen Telefons alle Bewegungen innerhalb der Schweiz für ein halbes Jahr und mehr in die Vergangenheit zurückverfolgen. Mit Antennensuchläufen und IMSI-Catchern können die Aufenthaltsorte von beliebigen Personen ermittelt werden, was zur Zeit der guten alten Telefonkabinen ebenfalls nicht möglich war.

Die Rechtmässigkeit der Vorratsdatenspeicherung ist stark umstritten. Insbesondere wird präventiv in das Telefongeheimnis und in die Bewegungsfreiheit, welche auch das Recht, nicht ständig beobachtet zu werden, beinhaltet, praktisch aller Bürger eingegriffen. Die Vorratsdatenspeicherung wurde bisher von allen Verfassungsgerichten europäischer Staaten, welche sie beurteilt haben, als verfassungswidrig beurteilt.

Schon am 8. Oktober 2009 hat der Verfassungsgerichtshof Rumäniens das rumänische Gesetz zur sechsmonatigen Vorratsspeicherung aller Verbindungs-, Standort- und Internetzugangsdaten als verfassungswidrig verworfen. In dem Urteil heisst es, die Erfassung aller Verbindungsdaten könne nicht als vereinbar mit den Bestimmungen der Europäischen Menschenrechtskonvention erachtet werden. Auch in Irland und Bulgarien wurden dem schweizerischen BÜPF entsprechende Gesetze für verfassungswidrig erklärt und aufgehoben. Am 2. März 2010 hob das deutsche Bundesverfassungsgericht das Gesetz zur Vorratsdatenspeicherung auf und ordnete die sofortige Löschung aller Daten an. Vor dem Europäischen Gerichtshof für Menschenrechte in Strassburg sind diverse Verfahren in dieser Angelegenheit hängig, darunter eines aus Irland und eines aus Deutschland.

Darüber hinaus ist kaum ein Nutzen ersichtlich. Nachdem das Bundesverfassungsgericht in

Deutschland am 2. März 2010 die Vorratsdatenspeicherung verbot, hat die kriminologische Abteilung des Max-Planck-Instituts für ausländisches und internationales Strafrecht im Auftrag des deutschen Bundesamtes für Justiz untersucht, ob Probleme auf dem Gebiet der Strafverfolgung und der Gefahrenabwehr infolge des Wegfalls auswertungsfähiger Verkehrsdaten erkennbar sind. Auf Seite 123 des Berichts ist ein Vergleich der Aufklärungsrate von Verbrechen in der Schweiz und Deutschland:

«Bei aller gebotenen Vorsicht, die unterschiedliche Deliktsdefinitionen, unterschiedliche Zählweisen etc. gebieten, lässt sich doch für die in der Tabelle enthaltenen Deliktsbereiche die Aussage treffen, dass die Aufklärungsquote in Deutschland in keinem Fall unter den für die Schweiz mitgeteilten Aufklärungsquoten liegt. Vielmehr liegen die Aufklärungsquoten teilweise deutlich höher. Dies gilt auch für solche Delikte, für die die besondere Bedeutung des Zugriffs auf Telekommunikationsverkehrsdaten hervorgehoben wird (also Computerbetrug, Verbreitung von Pornografie einschliesslich Kinderpornografie oder Drohung)».

Opposition kommt auch aus den Reihen der Telefon- und Internetanbieter. Einerseits wollen sie nicht zulasten ihrer Kund_innen Hilfspolizei spielen, andererseits bemängeln sie die horrenden Kosten, welche von den anordnenden Behörden nur ungenügend abgegolten werden und somit auf alle Nutzer von Fernmeldediensten, welche ungefragt und ungewollt überwacht werden, überwälzt werden. Im letzten Jahr erhielten alle Fernmeldeanbieter der Schweiz total Fr. 9,756,083 vergütet. Pro Einwohner und Monat stehen also lediglich 10 Rappen zur Verfügung, und das müsste reichen, um alle Daten für 6 Monate zu speichern und auf Abruf zum Teil sehr aufwändig Auskunft zu erteilen.

Widerstand ist aufgegleist

Im August 2010 hat sich grundrechte. ch in einer gemeinsamen Vernehmlassungsantwort mit den Demokratischen Juristen der Schweiz gegen die Verschärfung des BÜPF ausgesprochen. Als der Bundesrat Mitte 2011 mit einer Änderung der zu BÜPF zugehörigen Verordnung bereits einige der vorgeschlagenen Neuerungen ohne gesetzliche Grundlage in Kraft setzen wollte, hat grundrechte.ch gemeinsam mit der Piratenpartei Schweiz, der Swiss Internet User Group (SIUG), der Swiss Privacy Foundation und dem Verein Digitale Allmend in einer Stellungnahme zur geplanten Änderung der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs das vom Bundesrat geplante Vorgehen scharf kritisiert. In der Folge wurden an regelmässigen gemeinsamen «Netzpolitiktreffen» diverse Aktionen, zu Beginn explizit nur gegen die Vorratsdatenspeicherung, momentan aber auch gegen die Totalrevision des BÜPF, und in Zukunft wohl auch gegen das Staatsschutzgesetz, beraten und an die Hand genommen. Die erste Aktion war Mitte 2012 die *«Kampagne VDS»*, mit welcher öffentlich aufgefordert wurde, unter dem Motto *«Meine Vorratsdaten - jetzt!»* beim Telefon- resp. Internetprovider seine eigenen zuhanden der Strafverfolgungsbehörden gespeicherten Daten einzufordern. An die Mitglieder der Kommission für Rechtsfragen des Ständerats, welche die Totalrevision des BÜPF am 2. und 3. Mai 2013 beraten hat, wurden im Vorfeld Briefe verschickt. Die Kommission ist zwar auf die Vorlage eingetreten, hat aber die Detailberatung auf später verschoben, so dass das Geschäft nicht wie geplant in der Sommersession im Juni 2013 behandelt werden kann. Am 30. Juni endet die Vernehmlassung zum neuen NDG. grundrechte.ch wird die gesamte Vorlage zur Rückweisung empfehlen, besonders aber die geheimen Überwachungsmassnahmen, die Verquickung von Staatsschutz und Strafverfolgung sowie die niedere Schwelle für eine Aufnahme in die Staatsschutzdatenbank kritisieren.