

Anna Sauerbrey

Digitales Troja

Am 9. Oktober veröffentlichte der Chaos Computer Club (CCC) seine Analyse des „Staatstrojaners“ – und sorgte damit für enorme mediale Aufmerksamkeit. Mithilfe dieser staatlich genutzten digitalen Spähsoftware lassen sich offenbar nicht nur E-Mails, Chats und Internettelefonate abhören, sondern auch in Echtzeit Bildschirmfotos von angezapften Rechnern erstellen. Das Programm kann weitere Module nachladen, um mit diesen das Mikrofon des Computers anzusteuern oder Tastatureingaben aufzuzeichnen. Der CCC spricht außerdem von einem technisch „katastrophalen Gesamtumfeld“: Der Trojaner weise erhebliche Sicherheitslücken auf und ermögliche damit Dritten den unbefugten Zugriff auf den PC.

Bereits vor der Enthüllung des CCC war bekannt, dass die bayerischen Behörden Trojaner einsetzen. Anfangs schien es zudem, als ob der Staatstrojaner nur in einer geringen Zahl von Fällen eingesetzt wurde – in Bayern ist die Spähsoftware bislang nachgewiesenerweise mindestens 22 Mal zum Einsatz gekommen.

Doch wie sich kurz nach der Enthüllung des CCC herausstellte, setzen Behörden Trojaner ebenfalls in zahlreichen anderen Bundesländern ein. Die Bundesregierung räumte zudem auch ein, dass der Zoll, die Bundespolizei, das Bundeskriminalamt (BKA) und der Verfassungsschutz Spähsoftware verwenden. Gegenwärtig wird noch untersucht, welche Behörden im Bund und in den Ländern zu welcher Zeit mit welcher Trojaner-Variante gearbeitet haben.

Zwar sollte ein Staat in der Tat über virtuelle Instrumente zur Strafverfolgung verfügen. In dem Maße, wie sich

Wirtschaft, Politik und Sozialleben in die Online-Welt verlagern, müssen auch Ermittlungsbehörden mit der technischen Entwicklung Schritt halten, um im Rahmen von verdeckten Ermittlungen Zugang zu Daten zu erhalten, die auf Rechnern von Verdächtigen gespeichert sind. Allerdings darf der Einsatz von Spähsoftware nur unter Einhaltung strenger rechtsstaatlicher Beschränkungen erfolgen.

Fest steht aber bereits, dass die Strafverfolgungsbehörden weit über das Ziel hinausgeschossen sind: Denn der „Staatstrojaner“ kann nach Angaben des CCC mehr, als er nach den Vorgaben des Bundesverfassungsgerichts darf. Die Karlsruher Richter erklärten im Februar 2008 eine Änderung des Verfassungsschutzgesetzes des Landes Nordrhein-Westfalen, die die sogenannte Online-Durchsuchung regeln sollte, als unvereinbar mit den im Grundgesetz festgeschriebenen Persönlichkeitsrechten und daher für nichtig. Unter der Online-Durchsuchung wird das umfassende Ausforschen eines Computers mithilfe einer digitalen Wanze verstanden. Dabei wies das Gericht nachdrücklich auf die Verschiedenartigkeit von Telekommunikation und netzwerkgestützter Onlinekommunikation hin. Während über das Abhören von Telefonaten „nur“ die Gespräche eines Tatverdächtigen belauscht werden, bedeutet der Zugriff auf den Rechner einen erheblich tieferen Eingriff, schließt er doch private Informationen in weit größerem Umfang ein – und gleicht damit eher einer Hausdurchsuchung. Durch eine länger andauernde Überwachung der Nutzung des Rechners könnten zudem flüchtige Daten wie etwa Passwörter und weitere

intime Informationen über das Nutzungsverhalten des Betroffenen erhoben werden.

Vor diesem Hintergrund formulieren die Bundesverfassungsrichter genaue Grenzen für die Online-Durchsuchung und die sogenannte Quellen-Telekommunikationsüberwachung (Quellen-TKÜ). Ihrem Urteil zufolge darf die Online-Durchsuchung nur bei Bedrohung von Leib und Leben, Freiheit der Person oder Gefährdung des Staates eingesetzt werden. Die rechtlichen Grundlagen für den Einsatz finden sich im BKA-Gesetz und den Polizeigesetzen der Länder.

Beim nun aufgetauchten „Staatstrojaner“ handelt es sich allerdings um eine Software zur Quellen-TKÜ. Mit ihr soll die „laufende Kommunikation“ im Internet abgegriffen werden, also E-Mails, Live-Chats oder Skype-Telefonate. Da die Übertragung in der Regel verschlüsselt erfolgt, müssen die Ermittler auf den Rechner des Beschuldigten zugreifen und das Gespräch vor der Verschlüsselung – und somit an der Quelle – abfangen. Auch für diese Form des Ausforschens stellte das Bundesverfassungsgericht klare Leitlinien auf: Jede einzelne Funktion des elektronischen Abhörtvorgangs soll demnach richterlich abgesegnet sein. Auch muss die Beschränkung der Maßnahme auf das reine Abhören der „laufenden Kommunikation“ technisch sichergestellt werden. Schließlich darf die Ermittlung nicht dazu führen, dass das System für Dritte geöffnet wird.

Die letzten beiden Bedingungen erfüllt der bayerische Trojaner eindeutig nicht. Das Programm ist nicht technisch beschränkt, sondern ermöglicht im Gegenteil eine Online-Durchsuchung. Auch dass der Trojaner Screenshots versenden kann, etwa von Emails, die noch nicht verschickt wurden und somit nicht Teil der „laufenden Kommunikation“ sind, ist eindeutig verfassungswidrig.

Genau so hatte auch das Landgericht Landshut in einem Fall von 2009 ent-

schieden. (Der Anwalt des abgehörten Verdächtigen gab damals eine der Festplatten an den CCC weiter, auf der sich auch der Trojaner befand.) Das Landgericht kam damals allerdings zu dem Schluss, dass es für die Durchführung der Quellen-TKÜ grundsätzlich keiner eigenen, neuen Rechtsgrundlage bedürfe. Die Installation der Software sei vielmehr durch Paragraph 100 der Strafprozessordnung gesichert. Dieser Paragraph wurde für die Telefonüberwachung geschaffen.

Analog = digital?

Zugespitzt formuliert könnte man sagen, dass die Quellen-TKÜ bislang aufgrund der Annahme angewandt wurde, ein Computer sei dasselbe wie ein Telefon. Damit wird ein zentrales Dilemma berührt, mit dem sich der Gesetzgeber in Zeiten der Digitalisierung konfrontiert sieht. Das Recht soll möglichst allgemein gehalten sein, damit nicht für jede technische Erfindung neue Gesetze verabschiedet werden müssen. Gleichzeitig stellt sich damit die Frage: Funktioniert die Analogie zur analogen Welt? Funktioniert ein Computer wirklich wie ein Telefon?

Wohl kaum. Anders als das Telefon, das lediglich Töne übermittelt, ist die Festplatte ein Kondensat der Persönlichkeit. Auf ihr ist jener „Kernbereich persönlicher Lebensführung“, den das Grundgesetz besonders schützt, in komprimierter Form gespeichert. Durch die Quellen-TKÜ ist das Risiko, unrechtmäßig an intime Informationen zu gelangen, somit ungleich höher als beim Abhören des Telefons. Zudem bietet die Quellen-TKÜ geradezu eine Einladung für das weitergehende Schnüffeln der Ermittlungsbehörden.

In der Ermittlungs- und Spionagewelt der 70er Jahre benötigte man noch einen Nachschlüssel zur Wohnung eines Verdächtigen, wenn man dessen persönliche Unterlagen unbemerkt einsehen wollte. Und den Telefon-

anschluss zapften die Ermittler bei der Post an. Heute hingegen ist der Zugriff auf persönliche Daten wie auch auf Kommunikationskanäle zentralisiert möglich: Steuerakten, Fotoalben, Liebeschwüre, geschäftliche Korrespondenz – all das ist inzwischen nur noch einen Mausklick voneinander entfernt, sobald man Zugriff auf den Rechner eines Menschen erhält.

Diese grundlegenden Veränderungen hat das Bundesverfassungsgericht in seinem Urteil zur Online-Durchsuchung anerkannt. Das Gericht merkt an, dass die Informationstechnik neue Chancen eröffne, zugleich aber auch „neuartige Gefährdungen der Persönlichkeit“ begründe. Da die Eingriffe oft unbemerkt blieben und das Sichern des Computers „zumindest den durchschnittlichen Nutzer“ überfordere, sehen die Richter bei persönlichen Rechnern „ein grundrechtlich erhebliches Schutzbedürfnis“.

Gebot der Zurückhaltung

Die rechtliche Analogie zwischen Telefon und Computer führt somit in die Irre, und die Quellen-TKÜ bedarf eines eigenen Gesetzes. Der Skandal um den Bundesrojaner ist daher vor allem ein Weckruf: Bürger und Politiker müssen sich entscheiden, welchen Staat sie sich wünschen – einen Rechtsstaat oder einen Präventivstaat.¹

Es kommt entscheidend darauf an, die überfällige rechtliche Regelung endlich in Angriff zu nehmen. Dabei muss die Devise gelten: Je heikler der Eingriff und je näher er einem Grundrechtsverstoß kommt, desto klarer sollte er geregelt sein. Die Dringlichkeit gesetzlicher Regelungen wird umso deutlicher, wenn man zudem noch jene technische Entwicklungen einbezieht, die derzeit an Bedeutung gewinnen: Wie etwa ist der Zugriff auf Daten in der

Datenwolke, der sogenannten Cloud, zu bewerten, wenn nämlich die Daten gar nicht auf der Festplatte eines Verdächtigen, sondern auf einem externen Server liegen – möglicherweise gar im Ausland?

Bei jeder rechtlichen Regelung sollte – angesichts der Schwere des Eingriffs – vor allem das Gebot der Zurückhaltung gegenüber dem Rechtsgut vorherrschen. In den Ermittlungsbehörden wurde diese Kultur der Zurückhaltung von der Politik offenbar nicht ausreichend gefördert und eingefordert – zumindest in Bayern. Insgesamt stehen wir erst am Anfang einer Ermittlungsarbeit, die mit dem Grundgesetz vereinbar wäre: Denn wie der aktuelle Fall zeigt, ist es nahezu unmöglich, einen einmal entfesselten Trojaner politisch zu kontrollieren oder auch nur festzustellen, welche seiner Fähigkeiten im Einsatz waren.

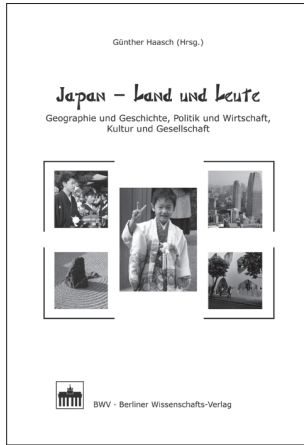
Konstruktive Vorschläge, wie sich in Zukunft die Kontrolle der Software und ihres Einsatzes verbessern ließe, sind allerdings bislang noch rar. Bund und Länder, wie auch FDP und Union, schieben sich bisher vor allem den Schwarzen Peter zu. Weder Bundesinnenminister Hans-Peter Friedrich noch Bundesjustizministerin Sabine Leutheusser-Schnarrenberger wollen offenbar die Verantwortung dafür übernehmen, dass die Politik bislang keine Konsequenzen aus dem Karlsruher Urteil gezogen hat. Dabei hatten Juristen schon nach dem Urteil von 2008 eine eigene gesetzliche Regelung für die Quellen-TKÜ dringend angemahnt.

Diese gesetzliche Regelung ist die Politik bis heute schuldig geblieben. Die Bürger haben allerdings „einen Anspruch darauf“, dass in dem hochsensiblen Bereich ihrer persönlichsten Daten endlich „größtmögliche gesetzliche Klarheit herrscht“.² Mehr noch: Sie haben das Recht, in einem Rechtsstaat zu leben.

1 Vgl. Sabine Leutheusser-Schnarrenberger, Auf dem Weg in den autoritären Staat, in: „Blätter“, 1/2008, S. 61-70.

2 So der Vorsitzende des Deutschen Richterbundes, Christoph Frank, im Gespräch mit dem „Tagesspiegel“, 12.10.2011.

Unter Berücksichtigung der jüngsten Geschehnisse



Günther Haasch (Hrsg.)

Japan – Land und Leute

Geographie und Geschichte, Politik und Wirtschaft, Kultur und Gesellschaft

Dieses Werk informiert nahezu umfassend über fast alle Bereiche des heutigen Japan, das durch schwere Naturkatastrophen jüngst ins Zentrum des öffentlichen Interesses gerückt ist. Es blendet dabei aber nicht die Vergangenheit dieses Inselreiches aus, das in der Geschichte Ostasiens sowohl geologisch als auch geschichtlich ein Spätkommer ist und die viel früher einsetzenden Entwicklungen Chinas und Koreas erst relativ spät übernehmen kann. So kommt es hier zur Ausbildung langer Traditionsketten, die sich fast überall im Brauchtum, im traditionellen Theater und in der Handwerkskunst erhalten haben. Andererseits haben sich die Japaner seit der gewaltsamen Öffnung des Landes im späten 19. Jh. bis heute in einem ganz ungewöhnlichen Maße allem Neuen gegenüber aufgeschlossen gezeigt, sodass sich in der heutigen Gesellschaft die Popkultur, das Avantgarde-Theater und der Experimentalfilm, neue Religionen und der Erfindergeist der Techniker als maßgebliche Instrumente gesellschaftlichen Wandels gezeigt haben, Buddhismus, Shinto und die Ahnenverehrung aber immer wieder dafür gesorgt haben, dass die alten Traditionen bewahrt und weiter gepflegt wurden. Der Leser wird sowohl eingeführt in die japanische Parteienlandschaft als auch in die Grundzüge der japanischen Finanz- und Wirtschaftspolitik und wird entdecken, dass Japan schon in den 70er Jahren das Deutsche Wirtschaftswunder übertroffen hat und in den 90er Jahren stärkste Welthandelsmacht geworden war und zurzeit nur noch von China übertroffen wird. Auch die Veränderungen der japanischen Gesellschaft im 20. und 21. Jahrhundert werden sorgfältig nachgezeichnet, wobei die wesentliche Änderung der Stellung der Frau deutlich wird. Die Beitragsautoren sind zum größten Teil jüngere Experten ihres Faches; der Herausgeber, der 20 Jahre am OAS der FU Berlin unterrichtete, hat davor weit über 10 Jahre in Japan in Lehre und Forschung verbracht.



2011, 373 S., 99 farb., 55 s/w Abb., kart., 32,- €, 978-3-8305-1908-9



BWV • BERLINER WISSENSCHAFTS-VERLAG

Markgrafenstraße 12–14 • 10969 Berlin

Tel. 030 / 841770-0 • Fax 030 / 841770-21

E-Mail: bwv@bwv-verlag.de • Internet: <http://www.bwv-verlag.de>