DIE LINKE.

Beschluss der Bundesarbeitsgemeinschaft Netzpolitik vom 11.11.2017

Staatstrojaner zerstören Privatssphäre, Demokratie und IT-Sicherheit

Am 22. Juni 2017 hat der Deutsche Bundestag die gesetzliche Grundlage zum breiten Einsatz von Staatstrojanern beschlossen und damit rechtlich den Weg freigemacht für einen massiven Verlust informationeller Selbstbestimmung, Demokratie und IT-Sicherheit. Schon Jahre zuvor wurden Staatstrojaner entwickelt, von Behörden gekauft und eingesetzt. Eklatante Fehlfunktionen der Schadsoftware wurden durch Enthüllungen des Chaos Computer Club (CCC) schon im Jahr 2011 nachgewiesen und sind als prinzipbedingt einzuschätzen. Auch das Landeskriminalamt (LKA) Berlin beschaffte im Jahr 2013 kommerzielle Trojanersoftware und strebte Eigenentwicklungen von Staatstrojanern an. Durch geleakte Geheimdokumente ist im Juli 2017 bekannt geworden, dass bereits im Feburar 2016 ein eigenentwickelter Trojaner des Bundeskriminalamts (BKA) „RCIS 1.0“ anhand einer standardisierten Leistungsbeschreibung (SLB) zertifiziert wurde.[1] Ein Urteil des Bundesverfassungsgerichts (BVerfG) von 2016 erklärte die im BKA-Gesetz festgehaltene Regelung zum Einsatz von Staatstrojanern zur Terrorabwehr für teilweise verfassungswidrig. Anstatt die Problematik des Trojanereinsatzes zu begreifen, wurde an einer neuen rechtlichen Grundlage gearbeitet, um über vertrackte Formulierungen den Weg für dessen Einsatz selbst gegen Alltagskriminalität freizumachen - am 22. Juni dieses Jahres war es schließlich soweit, das neue Gesetz wurde beschlossen. [2] Der CCC lehnte den Gesetzesentwurf in seiner Gänze ab [3].

Die BAG Netzpolitik der LINKEN lehnt Staatstrojaner grundsätzlich ab, aus folgenden Gründen:

1. Schon 2008 hat das BVerfG festgehalten, dass das allgemeine Persönlichkeitsrecht auch ein Grundrecht auf Integrität informationstechnischer Systeme beinhaltet. [4] Die Infektion eines Gerätes durch einen Staatstrojaner ist jedoch in jedem Fall ein manipulativer Eingriff in das System. Neben der massiven Verletzung der Privatssphäre besteht das Problem, dass bei den spionierten Daten aufgrund des Eingriffs und der Störung der Sicherheitssysteme, nicht zwischen Fake und authentischem Material unterschieden werden kann.
2. Staatstrojaner gefährden die IT-Sicherheit. Sicherheitslücken müssen geschlossen werden, anstatt sie verdeckt zu sammeln. Tatsache ist, dass der Staat den

Schwachstellenschwarzmarkt durch Beteiligung fördert oder eigene Forschung nach Schwachstellen betreibt, und diese verdeckt hält. Der Staat macht sich mit dieser Arbeitsweise selbst zum kriminellen Subjekt und zur globalen Gefahr für IT-Sicherheit. Der im Mai 2017 erfolgte Cyberangriff mittels WannaCry veranschaulicht deutlich, wie schwerwiegend die Auswirkungen sind, wenn Schwachstellen – in diesem Fall seitens der NSA – zu Spionagezwecken verdeckt gehalten und somit nicht rechtzeitig geschlossen werden können. Auch der Code des Trojaners selbst kann Schwachstellen beinhalten, die wiederum Tür und Tor für Kriminelle öffnen, die Geräte anzugreifen.

3. Eine Zertifizierung von Trojanersoftware durch eine standardisierte Leistungsbeschreibung (SLB) - wie im Feburar 2016 für RCIS 1.0 praktiziert – ist unseriös. Sie schließt zwangsläufig die Beschreibung einer gewollten/erwünschten Sicherheitslücke von Systemen ein, die sich zur Infektion mit Schadsoftware eignet, was schon aus o.g. IT-Sicherheitsproblemen heraus nicht akzeptabel ist. Egal, ob die Schadsoftware manuell vor Ort installiert oder über das Netz eingeschleust wird. Es existiert zudem keine plausible Vorstellung davon, wie der Einsatz des Staatstrojaners im Rahmen der gesetzlich festgehaltenen Anforderungen überhaupt möglich sein soll.
4. Die fehlende objektive Überprüfbarkeit des Einsatzes wie auch des Trojanercodes selbst, ermöglicht das spurenlose Nachladen illegaler Tools und allgemein den Missbrauch von Trojanersoftware durch den Staat oder Dritte. Der Quellcode liegt nicht offen, es wird mit privaten Anbietern von Trojanersoftware wie DigiTask und FinFisher zusammengearbeitet.
5. Die gesetzliche Trennung von Qell-Telekommunikationsüberwachung (QTKÜ) und Online-Durchsuchung ist künstlich und hält keiner Praxis stand. Kommunikation bereits abzugreifen, noch bevor eine Nachricht überhaupt verschickt wurde, ist letztlich nicht das Abhören der Kommunikation (TKÜ), sondern ein Ausspionieren der gespeicherten Daten, was einer Online-Durchsuchung gleichkommt. Technisch ist es beispielsweise nicht möglich, in einem Web-Browser zu unterscheiden, ob gerade an einer Email oder einem Tagebuch geschrieben wird.
6. Eine gezielte Verstrickung des Staates in schädigende, kriminelle Tätigkeiten mit dem Ziel der Infiltration, entwickelt ein bizarres und kontraproduktives Eigenleben. Wie derartiges passiert, kann man beispielhaft an den Ergebnissen der Infiltration der rechtsextremen Szene durch V-Männer sehen.
7. Wenn der Staatstrojaner schon ganz grundsätzlich als keine geeignete Überwachungsmaßnahme einzuschätzen ist, so ist es umso erstaunlicher, dass dessen Einsatz mit dem jüngst beschlossenen Gesetz auf Alltagskriminalität ausgeweitet werden soll. Dies ist angesichts der genannten Probleme vollkommen unverhältnismäßig und wird vom Transparenz- und Vertrauensdefizit abgesehen auch ein hohes Maß der Gefährung von IT-Systemen mit sich bringen und somit die Sicherheit insgesamt verringern.
8. Internationaler Terror und andere ernste Risiken bedürfen neben der alles entscheidenden Ursachenbekämpfung freilich auch der unmittelbaren Gefahrenabwehr. Als LINKE sehen wir in verdeckter Überwachung und Geheimdiensten jedoch kein Mittel, Sicherheit herzustellen, weil die Geheimdienste selbst ein Sicherheitsrisiko sind und die Funktionsfähigkeit einer jeden Demokratie unterminieren. Der Staatstrojaner wäre ein weiteres Beispiel dafür.

9. Nie gab es so viele, schnell abrufbare Daten wie heute - eine kompetente Auswertung öffentlich zugänglicher Quellen würde zur Gefahrenabwehr beitragen, ohne dass durch die Ermittlungsarbeit selbst neue Gefahren heraufbeschwört würden. Verschlüsselte Kommunikation führt keineswegs zu einem "Going Dark" [5]. Auch sie hinterlässt Metadaten, die im Rahmen von TKÜ, Funkzellenabfragen usw. gesammelt werden. Statistiken weisen aus, dass die Attentäter der seit 2014 in Europa erfolgten Terroranschläge allesamt bereits vor der Tat mindestens durch Gewaltaffinität behördenbekannt, oftmals sogar bereits überwacht waren [6]. Nicht zuletzt wird ein Sprengsatz, eine Waffe oder ein Bündel Drogen auch in der heutigen digitalisierten Welt wohl kaum über Telefonleitungen produziert, verschickt oder eingesetzt werden können! Staatstrojaner sind keineswegs alternativlos, wohl aber das übelste und vermeidbarste Mittel der Gefahrenabwehr.
10. Die Entwicklung von Staatstrojanern und der Export der Produkte auch durch mitteleuropäische Unternehmen wie die FinFisher GmbH mit Firmensitz in München nützt schon heute manchem autokratischen Regime zur rigorosen Überwachung und Unterdrückung der Bevölkerung. Es ist gerade auch deshalb antidemokratisch, derartige Produkte zu exportieren und deren Entwicklung zu tolerieren.

Einzelnachweise

[1]
Bericht zur Nr. 10 des Beschlusses des Haushaltsausschusses des Deutschen Bundestages zu TOP 20 der 74. Sitzung am 10. November 2011
https://netzpolitik.org/2017/geheimes-dokument-das-bka-will-schon-dieses-jahr-messenger-apps-wie-whatsapp-hacken/

[2]
Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze. Drucksache 18/11272
http://dip21.bundestag.de/dip21/btd/18/112/1811272.pdf

[3]
Risiken für die innere Sicherheit beim Einsatz von Schadsoftware in der Strafverfolgung.
Linus Neumann, Constanze Kurz, Frank Rieger, Mai 2017
https://www.bundestag.de/blob/509192/77ee7be3c9401ef4619fa0411758b045/neumann-data.pdf

[4] BVerfG, Urteil des Ersten Senats vom 27. Februar 2008 - 1 BvR 370/07 - Rn. (1-333),
http://www.bverfg.de/e/rs20080227_1bvr037007.html

[5] James B. Comey, Director Federal Bureau of Investigation (2014):
Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?,
https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course

[6]
https://upload.wikimedia.org/wikipedia/commons/c/cb/20170531_Attent
%C3%A4ter_islamistischer_Mordanschl%C3%A4ge_in_der_EU_2014-2017.jpg?uselang=de

[7] Koalitionsvereinbarung 2016-2021 Berlin
http://www.die-linke-berlin.de/fileadmin/download/2016/161116_Koalitionsvertrag_finale_Fassung.pdf