

Entfesselter Staatstrojaner: Große Koalition verhöhnt IT-Sicherheit und Demokratie

Gestern haben CDU/CSU und SPD im Bundestag das staatliche Hacking zum Alltagsinstrument für Behörden erklärt. Es geht dabei nicht einmal um die Verhinderung des sonst so gern herangezogenen internationalen Terrorismus, sondern um die Aufklärung bereits erfolgter Taten wie etwa Steuerhinterziehung, Betäubungsmitteldelikte oder missbräuchlicher Asylantragstellung.[0]

Unter den gleichen rechtlichen Voraussetzungen, mit denen zuvor Telefonleitungen abgehört werden konnten, können nun ganze Computersysteme jeglicher Art mit staatlicher Schadsoftware angegriffen, infiltriert, kontrolliert und ausgespäht werden. „Einmal ins System gelangt, hat der Staatstrojaner dann technisch freie Hand, egal ob in Handys, Autos, Kühlschränken, Laptops oder Herzschrittmachern.“ erklärt Rainer Rehak aus dem Vorstand des FIfF. An der rechtlich fantasievollen, aber technisch nicht haltbaren Unterscheidung von „grundrechtsschonender“ Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) einerseits und vollaktiver heimlicher Online-Durchsuchung andererseits wurde ebenfalls naiverweise festgehalten.

Der Einsatz von Quellen-TKÜ oder Online-Durchsuchung ist nur dann überhaupt nur ansatzweise nachvollziehbar, wenn BVerfG-MehrDemokratiePolizeien im absoluten Notfall auf die Nachrichten von Ende-zu-Ende-verschlüsselten Messengern wie WhatsApp (Facebook) oder Signal (Open Whisper Systems) zugreifen oder unbemerkt (verschlüsselte) Festplatten auslesen wollen um etwa Leben zu retten. Doch in den vorliegenden Anlässen geht es gerade nicht um Notfälle, sondern schon verübte Straftaten. Es werden also Maßnahmen, die das Bundesverfassungsgericht im Jahre 2008 gerade noch bei tatsächlichen Anhaltspunkten einer konkreten Gefahr für Leib, Leben oder den Bestand des Staates[1] für verfassungsmäßig erachtet hat nun für die Verfolgung gewöhnlicher Delikte vorgesehen.

Doch zu den direkten, hoch problematischen Komplikationen einer heimlichen Infiltration fremder Systeme, der prinzipiellen Undokumentierbarkeit und Unbelegbarkeit von Trojaneraktivitäten oder der technisch nach wie vor ungelösten Frage, wie laufende Kommunikation klar von anderen Datenverarbeitungsprozessen unterschieden werden kann, kommen noch unzählige weitere folgenschwere Eigenschaften hinzu. Einerseits sind die so erlangten Informationen technisch bedingt in der Regel nicht forensisch – also gerichtsfest – und damit für die Strafverfolgung größtenteils wertlos; und andererseits sind für die Infiltration von Systemen in der Regel unveröffentlichte, ausnutzbare IT-Sicherheitslücken vonnöten.

Diese benötigten IT-Sicherheitslücken sind auf internationalen Schwarzmärkten teuer zu erwerben und ein Ankauf solcher Lücken stützt, ja legitimiert derartige Märkte sogar noch. Je mehr finanziell potente, staatliche Akteure derartiges nachfragen, umso unsicherer wird die gesamte IT-Infrastruktur, weil Lücken nicht mehr an Hersteller gemeldet, sondern lieber an Behörden versteigert und von diesen gehortet werden. Das jüngste Beispiel war der Erpresserwurm „Wannacry“, der beispielsweise ganze Krankenhäuser lahmlegte und aus dem Sicherheitslückenfundus des US-Geheimdienstes NSA stammte. Anstatt also mit Softwarehaftung und allgemeinen Sicherheitslücken-Meldepflichten[2] unsere IT-abhängige

Gesellschaft wirklich sicherer zu machen, wird hier ein kurzfristiges Sicherheitsversprechen mit langfristiger brandgefährlicher IT-Unsicherheit[3] erkaufte.

Neben der inhaltlichen Kritik verurteilt das Fiff auch den Gesetzgebungsprozess aufs Schärfste. Erstens wurden diese bislang tiefgreifendsten Ermächtigungen für Polizeien in einer digitalen Gesellschaft im Eiltempo durch den Gesetzgebungsprozess gepeitscht, sodass geladene sachverständige Personen und Parlamentarier gleichermaßen nur wenige Tage für die Vorbereitung der mündlichen Anhörung hatten. Zweitens wurden diese Änderungen als „Formulierungshilfe“ in einem ganz anderen Gesetzgebungsprojekt untergebracht, was sich eigentlich mit Schwarzarbeit, Fahrverbot oder Wilderei beschäftigte.[4] Drittens „vergaß“ das Bundesjustizministerium die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Andrea Voßhoff, von dieser auswirkungsreichen „Formulierungshilfe“ in Kenntnis zu setzen,[5] sodass sie „erst am 17. Mai 2017 durch Medienberichte“ davon erfuhr. Dieser herrschaftliche und ignorante Gesetzgebungsstil schein insgesamt langsam politischer Usus zu werden.[6]

Um es ganz deutlich zu sagen: Das Fiff glaubt nicht mehr an eine Häufung von Zufällen oder bedauerlichen Missverständnissen und ist daher geschockt, mit welcher Dreistigkeit die große Koalition aus CDU/CSU und SPD uns allen ins Gesicht lügt, dass sie Partizipation und Demokratie als Grundwerte Deutschlands schätzt. Jede aufrechte Person in der Politik hätte sich – unabhängig vom Inhalt der „Formulierungshilfe“ – weigern müssen, solche undemokratischen Abläufe zu unterstützen, auch nicht „mit Bauchschmerzen“. Gerade in der aktuell so aufgeladenen politischen Situation fördert diese objektiv hintertückische Gesetzgebungsweise verständlicherweise die Politikverdrossenheit und extreme Positionen. Bei einem solchen Parlament brauchen wir nicht einmal fake news oder social bots, um unsere Gesellschaft weiter zu spalten. Wenn schon regelmäßig nach einer Leitkultur gesucht wird, warum nicht ernsthaft einmal eine gute Demokratie in Erwägung ziehen?

Abschließend möchten wir an die Überwachungsgesamtrechnung des Bundesverfassungsgerichtes erinnern. Grundrechtsrelevante Maßnahmen dürfen nicht allein, sondern immer im Kontext aller anderen Maßnahmen bewertet werden, um additive Folgen mitzudenken. Mit den ständigen Ausweitungen und Ausweitungsversuchen von Überwachungsgesetzen, namentlich der neuerlichen Nutzungsfreigabe biometrischer Datenbanken, der Vorratsdatenspeicherung, der Fluggastweitergabe, der Videoüberwachung oder der Bestandsdatenauskunft kommt nun ein weiterer Puzzlestein hinzu, der die Bundesrepublik einen weiteren Schritt weg von der freiheitlichen Grundorientierung hin zu einem repressiven Gesellschaftsmodell führt.

Keine der oben genannten Gesetze bringt bislang einen messbaren Sicherheitsgewinn bei teilweise haarsträubenden Grundrechtsfolgen, während auf der anderen Seite die Polizeien kontinuierlich beklagen, dass überall massiv Personal und Ausrüstung fehlt, um vorliegende Daten auszuwerten, um vorhandene Ermittlungsansätze zu verfolgen oder um einfach genug Beamte auf den Straßen haben zu können. Auch für eine Sicherheitserhöhung durch Prävention sind vielfache Ansätze bekannt, vom Einbezug von Schulstrategien bis hin zu Sozialangeboten. Nichts davon würde Grundrechte einschränken und alles würde tatsächlich Sicherheit bringen. Es würde eben Geld kosten, aber das wäre gut investiert.

Bei Rückfragen wenden Sie sich bitte an:

Rainer Rehak, rainer.rehak@fiff.de, 0D66 63E5 70A3 964A EE60 D927 4427 CFE5 8C19 AE19

Verweise

- [0] https://www.gesetze-im-internet.de/stpo/___100a.html
- [1] https://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html
- [2] <https://cyberpeace.fiff.de/Kampagne/Forderung10>
- [3] <https://vimeo.com/216584485>
- [4] <http://dip21.bundestag.de/dip21/btd/18/112/1811272.pdf>
- [5] <https://netzpolitik.org/2017/bundesdatenschutzbeauftragte-ruegt-vorhaben-den-staatstrojaner-einsatz-drastisch-zu-erweitern/>
- [6] <http://www.faz.net/aktuell/feuilleton/aus-dem-maschinenraum/netzwerkdurchsetzungsgesetz-nicht-einmal-mehr-die-simulation-von-partizipation-15015559.html>

Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FifF) e.V. ist ein Zusammenschluss von Menschen, die sich kritisch mit Auswirkungen des Einsatzes der Informatik und Informationstechnik auf die Gesellschaft auseinandersetzen. Unsere Mitglieder wirken in vielen technischen und nichttechnischen Bereichen der Gesellschaft. Zu unseren Aufgaben zählen Öffentlichkeitsarbeit, Beratung und das Erarbeiten fachlicher Studien. Das FIF gibt vierteljährlich die Zeitschrift FIF-Kommunikation heraus und arbeitet mit anderen Friedens- sowie Bürgerrechtsorganisationen zusammen.