Entfesselter Staatstrojaner: Große Koalition verhöhnt IT-Sicherheit und Demokratie

23. Juni 2017 – 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, Betäubungsmitteldelikten oder missbräuchlicher Asylantragstellung.[1]

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 vollaktivierter heimlicher Online-Durchsuchung andererseits wurde ebenfalls naiverweise festgehalten.

Der Einsatz von Quellen-TKÜ oder Online-Durchsuchung ist nur dann überhaupt ansatzweise nachvollziehbar, wenn Polizeien 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[2] 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[3] unsere IT-abhängige Gesellschaft wirklich sicherer zu machen, wird hier ein kurzfristiges Sicherheitsversprechen mit langfristiger brandgefährlicher IT-Unsicherheit[4] erkauft.

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.[5] Drittens „vergaß“ das Bundesjustizministerium, die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Andrea Voßhoff, von dieser auswirkungsreichen „Formulierungshilfe“ in Kenntnis zu setzen,[6] sodass sie „erst am 17. Mai 2017 durch Medienberichte“ davon erfuhr. Dieser herrschaftliche und ignorante Gesetzgebungsstil scheint insgesamt langsam politischer Usus zu werden.[7]

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 Fluggastdatenweitergabe, 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.

Keines 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 auswerten, um vorhandene Ermittlungsansätze 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.

Weitere Stimmen

Peter Schaar: „Arroganter Umgang mit der Macht zulasten der Demokratie und des Rechtsstaats“,
http://www.berliner-zeitung.de/politik/interview-ehemaliger-datenschutzbeauftrager-schaar-sieht-staatstrojaner-kritisch-27843956

Heribert Prantl: „Man soll nicht bei jeder Gelegenheit von einem Skandal reden. Aber das, was heute am späten Nachmittag im Bundestag geschehen soll, ist eine derartige Dreistigkeit, dass einem die Spucke wegbleibt.“,
http://www.sueddeutsche.de/digital/ueberwachung-der-staatstrojaner-ist-ein-einbruch-ins-grundgesetz-1.3555917

Patrick Beuth, Kai Biermann: „Wir analysieren es Satz für Satz und erklären, warum es wohl verfassungswidrig ist.“,
http://www.zeit.de/digital/datenschutz/2017-06/staatstrojaner-gesetz-bundestag-beschluss

Markus Reuter: „Dauerfeuer gegen das Grundgesetz – so treibt die Große Koalition das Land in den Überwachungsstaat“,
https://netzpolitik.org/2017/dauerfeuer-gegen-das-grundgesetz-so-treibt-die-grosse-koalition-das-land-in-den-ueberwachungsstaat/

Anmerkungen

1. *https://www.gesetze-im-internet.de/stpo/__100a.html*
2. *https://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html*
3. *https://cyberpeace.fiff.de/Kampagne/Forderung10*
4. *https://vimeo.com/216584485*
5. *http://dip21.bundestag.de/dip21/btd/18/112/1811272.pdf*
6. *https://netzpolitik.org/2017/bundesdatenschutzbeauftragte-ruegt-vorhaben-den-staatstrojaner-einsatz-drastisch-zu-erweitern/*
7. *http://www.faz.net/aktuell/feuilleton/aus-dem-maschinenraum/netzwerkdurchsetzungsgesetz-nicht-einmal-mehr-die-simulation-von-partizipation-15015559.html*

FIfF e. V. – Pressemitteilung

Verfälschte Studie zur Tauglichkeit grundrechtswidriger Techniken

FIfF lehnt automatisierte Identifizierung und Verhaltenskontrolle am Berliner Bahnhof Südkreuz ab

1. August 2017 – Am Berliner Bahnhof Südkreuz testen die Deutsche Bahn, das Bundesministerium des Innern und die Bundespolizei in Kooperation mit dem Bundeskriminalamt ab heute, ob es möglich ist, mit biometrischer Gesichtserkennung im öffentlichen Raum nach Menschen zu fahnden. In einer späteren Phase des Projektes sollen zusätzlich Verhaltenserkennung und Verhaltensbewertung zum Einsatz kommen.

Beim aktuellen Test könne man die als beobachtet markierten Bereiche noch umgehen, kündigte die Bundespolizei an. Tatsächlich sind die Bereiche jedoch so gewählt, dass zum Beispiel diejenigen, die auf eine Rolltreppe angewiesen sind, dem Blick der Kameras nicht ausweichen können. Wenn es zu einem späteren Echt-Einsatz solcher System überwachten Ausweichbereich oh die am öffentlichen Leben teilneh gehen, dass sie in ihrer täglichen kehrsmittel von Computern in Echtzeit vermessen, analysiert, bewertet und in allen möglichen privaten Momenten identifiziert werden können. Gleichzeitig können diejenigen, nach denen gefahndet wird, sich mit einfachsten Maßnahmen wie Sonnenbrillen, Mützen, Bärten, Make-up oder dem einfachen Blick nach unten aufs Smartphone der Identifizierung entziehen.

Aussagekraft des Versuchs

Die Tests am Südkreuz sind nicht die ersten. Schon vor zehn Jahren testete das Bundeskriminalamt mit dem Projekt „Foto-Fahndung“ biometrische Gesichtserkennung am Mainzer Hauptbahnhof.[1]

Einer der Hauptgründe, warum dieser und vergleichbare Tests scheiterten, war, dass die überwachten Menschen einfach nicht ten. Auch ohne tieferes techni lich, dass ein Mensch, der vom ng erkannt werden soll, koope st grob in die Richtung der Kamera schaut. Nur so können individuelle Merkmale wie Augen, Wangenknochen und Nasenrücken vom Blick der Kamera und der Analysesoftware erfasst und zur Identifizierung herangezogen werden.

Ganz offensichtlich will die Bundespolizei dem Problem der mangelnden Kooperation aus dem Weg gehen, um den Test am Südkreuz möglichst erfolgreich dastehen zu lassen – den Testpersonen wurden nämlich ausgerechnet dann „Attraktive Preise“ in Aussicht gestellt,[2] wenn sie besonders häufig vom System erfasst werden. Bei solchen Anreizen ist von den Testpersonen, vielleicht sogar unbewusst und mit den besten Absichten den