19.04.2019 08:15 Uhr

Seehofers Geheimdienstgesetz: Die Abrissbirne für die Grundrechte

Der Plan von Innenminister Seehofer, die Geheimdienste etwa mit Staatstrojanern aufzurüsten, atmet Orwellschen Geist, analysiert Stefan Krempl.

Von **Stefan Krempl**

462

(Bild: dpa, Uli Deck)

EINE ANALYSE VON STEFAN KREMPL

Stefan Krempl schreibt seit fast 20 Jahren als freier Autor in Berlin über politische, rechtliche und kulturelle Themen rund um Internet. Schwerpunkte seiner Berichterstattung bei heise online sind die Bereiche Netzpolitik, Überwachung, Datenschutz, Urheberrecht und Regulierung.

Der Referentenentwurf für ein "Gesetz zur Harmonisierung des Verfassungsschutzrechts" aus dem von Horst Seehofer geführten Bundesinnenministerium hätte das Licht der Welt nie erblicken dürfen. Es handelt sich um ein monströses Vorhaben unter dem Deckmantel, doch "nur" überbordende

Überwachungspraktiken des Bundesnachrichtendiensts (BND) zu legalisieren. Und wenn die auf fragwürdige Weise gewonnenen Daten schon mal da sind, kann man sie nach Logik der Verfasser auch gleich mit schier allen austauschen, die angeblich irgendwie etwas mit "Sicherheit" zu tun haben.

Dabei stapelt die Mannschaft des CSU-Politikers unverhohlen einen Angriff aufs Grundgesetz auf den anderen und rüttelt so an den Fundamenten der liberalen Demokratie und des Rechtsstaats. In einem Haus, zu dessen Aufgabenbereich nicht nur die öffentliche Sicherheit, sondern auch der Schutz der Verfassung gehört, hätte dies eigentlich dem ein oder anderen Juristen auffallen müssen.

Die vergiftete Maximalwunschliste

Doch keiner der zahlreichen Rechtsexperten des Ministeriums hat die Notbremse gezogen und verhindert, dass das gefährliche Papier an die anderen Ressorts geht, um einen Beschluss durch die Bundesregierung vorzubereiten. Dahinter kann Nachlässigkeit stecken oder das Kalkül, eine bislang im Verborgenen gehegte, vergiftete Maximalwunschliste aus der Schublade zu ziehen und es einfach mal zu probieren. Irgendwas wird bei der SPD schon mit den üblichen Bauchschmerzen durchgehen, selbst wenn der Koalitionspartner einen Großteil der ins Spiel gebrachten Vorschriften erst mal ablehnt.

Insgesamt atmet der Entwurf einen unguten Geist, der nicht nur an Orwell erinnert. Eigentlich ist das Dossier der Kritik kaum wert, so grobschlächtig ist es gestrickt. Einige der geworfenen Hämmer rufen aber doch nach einer Einzelkritik.

Da hilft nur noch Trojaner-Einsatz

Da ist etwa der Vorstoß, dass der BND künftig unter anderem deutsche Staatsbürger und juristische Personen auch im Inland trojanisieren dürfen soll. Und zwar nicht "nur" für die Quellen-Telekommunikationsüberwachung, um WhatsApp, Skype & Co. abzuhören. Sondern auch zur noch weiter gehenden heimlichen Online-Durchsuchung etwa von Smartphones oder größeren Computern, auf denen längst das digitale Abbild ihrer Nutzer fein säuberlich verzeichnet ist.

Der Einsatz von Bundes- oder Staatstrojanern stellt generell einen sehr tiefen Eingriff in die Grundrechte und insbesondere in Artikel 10 Grundgesetz und das darin verbriefte

Fernmeldegeheimnis dar. Das Bundesverfassungsgericht hat eine solche Maßnahme im Kampf gegen den "internationalen Terrorismus" nur unter hohen Hürden und bei einer konkreten Gefahr von sehr schweren Straftaten beim Bundeskriminalamt (BKA) zugelassen und zugleich ein Recht auf die Vertraulichkeit und die Integrität von IT-Systemen aufgestellt.

Der Staat als Hacker

Eigentlich müsste der Staat – und am besten federführend das Innenministerium – nach vielen Jahren endlich den damit verknüpften Auftrag annehmen und mit Leben erfüllen, die IT-Sicherheit der Bürger umfassend zu gewährleisten. Stattdessen hat die große Koalition bereits während der vergangenen Legislaturperiode der Polizei allgemein die Lizenz erteilt, zur Strafverfolgung und zur Gefahrenabwehr etwa Handys oder Laptops zu hacken. Die Länder sind eifrig dabei, entsprechende Befugnisse zusätzlich in ihren eigenen Polizeigesetzen zu verankern.

Dagegen laufen mehrere Verfassungsbeschwerden. Unterstützer der Eingaben an Karlsruhe halten die breiten Kompetenzen für Quellen-TKÜ und Online-Durchsuchungen für den "schwersten Eingriff in der Privatsphäre", der "dramatischer" sei "als der große Lauschangriff" zur Wohnraumüberwachung. Da die Behörden dafür Schwachstellen "horten" müssten, sei letztlich die IT-Sicherheit von Millionen Nutzern weltweit bedroht.

Daten "zum Abschuss freigegeben"

Statt die Entscheidung der Verfassungshüter respektvoll abzuwarten, will Seehofer massiv draufsatteln. Der Auslandsgeheimdienst soll offiziell auch Deutsche hacken dürfen für recht vielfältige Zwecke und ohne schlagkräftige Kontrolle, Ausländer natürlich sowieso und vogelfrei, denn deren Daten sind schon jetzt "zum Abschuss freigegeben".

Nun empfiehlt sich eine Lekture von Paragraf 1 BND-Gesetz: Demnach sammelt die Behörde Informationen "zur Gewinnung von Erkenntnissen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind". Auswerten darf sie das Gefundene auch noch, nur vom Inland steht da nichts.

"Transit-Kabelstrecken" aus dem "virtuellen Ausland"

Um trotzdem erstmals an einen internationalen Internetknoten in Frankfurt am Main herangehen, im großen Stil Daten ausleiten und diese teils an die NSA weitergeben zu können, bemühte der BND anfangs noch die krude Theorie vom "virtuellen Ausland". Dahinter verbarg sich die Idee, dass die Daten von "Transit-Kabelstrecken" erfasst werden, die zwischen zwei Punkten im Ausland verlaufen und Deutschland sowie die Mainmetropole nur durchqueren.

Schwarz-Rot hat zwar inzwischen das Überwachen ganzer Netzknoten auch im Inland durch den Geheimdienst mit einem überarbeiteten Paragraf 6 BND-Gesetz legalisiert und damit nach eigenen Angaben Folgen aus den Snowden-Enthüllungen und dem NSA-Untersuchungsausschuss gezogen. Laut Hans-Jürgen Papier, Ex-Präsident des Bundesverfassungsgerichts, werden dabei aber die Grundrechte nicht angemessen geschützt. So habe der Bundestag etwa einkalkuliert, dass derzeit "begrenzte personelle und sachliche Kapazitäten" die BND-Spionage praktisch einschränkten. Dem muss aber nicht immer so sein, was hierzulande bekannt sein sollte. Natürlich läuft auch gegen diese Netz-Überwachung im NSA-Stil eine Verfassungsbeschwerde, was das Innenressort wiederum nicht stört.

Der Datenstaubsauger wird aufgedreht

Bleibt noch das G10-Gesetz, das selbst schon seit Langem zu einem Trojaner für das Grundgesetz geworden ist. Es schränkt Artikel 10 ein und erlaubt den Geheimdiensten zum einen Überwachungsmaßnahmen gegen einzelne Personen beim begründeten Verdacht auf schwere Straftaten wie Hoch- oder Landesverrat, Gefährdung des demokratischen Rechtsstaats oder der äußeren Sicherheit, Terrorismus oder Sabotage von IT-Infrastrukturen. In etwa in diesem Rahmen soll der BND nun auch den Bundestrojaner von der Leine lassen dürfen.

Wichtig für den Auslandsgeheimdienst ist zudem die viel breiter gestreute und damit sensiblere zweite vom G10-Gesetz vorgesehene Überwachungsvariante. Sie hört auf den Titel "strategische Fernmeldeaufklärung". Der sperrige Begriff beschreibt eine Art Datenstaubsauger, mit dem der BND internationale Telekommunikation anlasslos, also ohne Verdacht auffangen, sieben und durchsuchen darf. Wen sollte es wundern: auch dagegen läuft eine Verfassungsbeschwerde.

Einbruch beim Spähopfer

Zurück zum Staatstrojaner: Von einer Online-Durchsuchung soll hier laut dem Entwurf nur noch bedingt die Rede sein, da die Schlapphüte zumindest für "Vorbereitungshandlungen" auch heimlich die Wohnung eines künftigen Spähopfers "betreten" dürften. "Einbrechen" wäre der klarere Ausdruck gewesen, denn den Zugang könnten sich Agenten "auch ohne Zustimmung des Wohnungsinhabers" verschaffen.

Das erinnert an die Bestimmungen für den großen Lauschangriff mit einer nochmals erhöhten Eingriffsintensität. Polizeirechtler gehen davon aus, dass die psychologischen Folgen für die Betroffenen – so sie jemals tatsächlich im Nachgang über das Vorgehen informiert werden sollten – wohl ähnlich stark wie bei einem Wohnungseinbruchsdiebstahl ausfallen dürfen.

Dass die gleichen Rechte auch für das Bundesamt für Verfassungsschutz (BfV) gelten und die Staatsschützer ferner fortan Daten von Kindern erheben und speichern können sollen, sorgte schon für den ein oder anderen Aufreger in der Presse. Angesichts des gesamten Ansatzes des Entwurfs sind das aber fast schon die "geringeren Übel". Dazu kommt etwa, dass der BND für den Trojanereinsatz auch Amtshilfe bei anderen Sicherheitsbehörden leisten soll, obwohl es dafür doch schon die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (Zitis) gibt, vor der prinzipiell auch vernetzte Autos nicht sicher sind.

Das BSI als Geheimdienst

Dann der vorgesehene umfassende "nachrichtendienstliche Informationsverbund", in dem unter anderem das Bundesamt für Sicherheit in der Informationstechnik (BSI) voll eingebunden werden soll. Aufhänger ist hier die gemeinsame Aufklärung "elektronischer Angriffe fremder Mächte". Die Bonner Behörde sei zwar "kein Nachrichtendienst" – das ist auch dem Innenministerium nicht entgangen. Sie versucht gerade auch eigentlich, ihre Wurzeln just in diesem Umfeld hinter sich zu lassen.

Seehofers Juristen finden aber, dass das BSI "keine vollzugspolizeilichen Zwangsbefugnisse" hat und "die informationelle Zusammenarbeit danach ebenso wie im Falle des BND nicht spezifischen Einschränkungen einer grundsätzlichen informationellen Trennung unterworfen ist". Parallel soll aber auch noch das Trennungsgebot zwischen Geheimdiensten und Polizei weiter aufgeweicht werden. So dürfte der BND an Ermittler auf Basis der Initiative im Rahmen einer möglichst

"ressourcenschonenden Zusammenarbeit" auch "unselektierte, unbearbeitete Informationen einschließlich personenbezogener Daten" übermitteln.

Nebulöse Gesetzgebungsprosa

Die Begründung für die skizzierte virtuelle Zusammenschaltung liest sich ähnlich blumig wie so manche wolkige BND-Theorie: "Der automatisierte Abruf aus der Verbunddatenbank bleibt im Übrigen aufgabengeprägt restriktiv geregelt, wird dabei aber mit den Regelungen zu gemeinsamen Dateien synchronisiert", heißt es da rabulistisch. "Dies dient der technikneutralen Klarstellung, dass solche Dateien durch ihre speziellen Verarbeitungsregelungen eine logische Struktur bilden, die jedoch nicht notwendig auf physisch gesonderter Basis realisiert werden muss."

Noch nicht genug von der nebulösen Gesetzgebungsprosa? Hier noch eine nicht leicht verdauliche Kostprobe, um den Charakter des Entwurfs zu verstehen (nicht die angeführten Details): "Bedrohungen für die herausragenden Schutzgüter des § 1 Absatz 1 mit der spezifischen Potenzialität der Gefährdungslagen nach § 3 Absatz 1 (zweckgerichtete Personenzusammenschlüsse und Wirkungsmacht fremder Staaten) bedingen effektive Frühaufklärung bereits mit niedriger Risikoschwelle. 'Vorfeld'-Charakteristik nachrichtendienstlicher Aufklärung ist ein bereits risikobasierter Aufgabenansatz, der grundsätzlich nicht erst bei konkreten bzw. konkretisierten Gefahren einsetzt, sondern deren Entstehen frühzeitig erkennt".

Wer schützt uns vor Staatsterrorismus?

Es ist zwar prinzipiell ein ehrenhaftes Unterfangen, die Bürger oder den Staat vor Terror schützen und geheimdienstliche Aktivitäten aus der tiefdunklen Grauzone herausholen zu wollen. Der alleinige Anspruch dabei kann aber nicht sein, "viele Detailregelungen, die bisher in BND-internen Dienstvorschriften festgelegt waren, nunmehr unmittelbar im Gesetz" einfach zu kodifizieren. Um die Freiheit und die Menschen vor Staatsterrorismus zu schützen, sollte eine ernsthafte und erstzunehmende Politik auch den Mut haben, wild gewachsene Befugnisse ganz zu kappen oder zumindest zurechtzuschneiden.

Mit alldem nicht genug: Gleichzeitig holt Seehofer mit seinem Referentenentwurf für ein IT-Sicherheitsgesetz 2.0 zu einem weiteren Rundumschlag aus. Das BSI soll damit massiv mit Millionen und fast 900 neuen Stellen zu einer riesigen

Netzüberwachungsmaschine im Namen der IT-Security aufgerüstet werden. Dazu gepackt hat das Innenministerium umfangreiche strafrechtliche Verschärfungen, um gegen Darknet-Betreiber, "digitalen Hausfriedensbruch" und Doxxing vorzugehen und die Hackerparagrafen insgesamt aufzublähen.

Beugehaft für die Passwortrausgabe

Hier kommt das "Computergrundrecht" auf Vertraulichkeit von IT-Systemen plötzlich zur Sprache, weil viele Politiker Anfang des Jahres selbst erlebten, was es heißt, wenn ihre persönlichen Informationen plötzlich im Netz gestreut werden. Gemünzt wird es folglich auch genau auf damit verknüpfte Online-Straftaten.

Es droht sogar bis zu sechs Monate Beugehaft, wenn Nutzer sich weigern, ihre Passwörter herauszugeben. Erleichtern will das Ministerium damit, dass Staatsanwaltschaft und Polizei sich der "virtuellen Identität" Verdächtiger bemächtigen und mit Dritten in Kontakt treten können. Dieser Zwang soll bei Ermittlungen rund um schwere Delikte genauso gelten wie bei "mittels Telekommunikation" begangener. Insgesamt werden so auch hier sinnvolle Vorhaben etwa für ein IT-Gütesiegel oder die Zertifizierung von Kernbausteinen für kritische Infrastrukturen von überzogenen Grundrechtseingriffen nebst neuer Vorratsdatenspeicherung völlig überlagert. (axk)

Kommentare lesen (462)

Zur Startseite

MEHR ZUM THEMA

BND DATENSCHUTZ GEHEIMDIENSTE TERRORBEKÄMPFUNG TROJANER ÜBERWACHUNG

Forum zum Thema: Politik

TEILE DIESEN BEITRAG

Kurzlink: https://heise.de/-4401986

Top-News der Redaktion von heise online »

Erweiterungen irrtümlich abgeschaltet

Zertifikat abgelaufen: Firefox deaktiviert Add-ons

Der Firefox-Browser schaltet derzeit die meisten Add-ons ab – wegen eines abgelaufenen Zertifikats. Die Entwickler arbeiten ber...

941

Deutsche Nobelmarke: Loewe meldet vorläufige Insolvenz an

477 c't Magazin

Ladestrom für E-Autos teurer als Dieselkraftstoff

Radikalisierung im Netz – Wie gefährlich ist das Internet?

202

nach oben

Alle Angebote

Datenschutzhinweis

Impressum

Kontakt

2663876