Deutscher Bundestag **Drucksache 19/2337**

19. Wahlperiode 25.05.2018

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Jimmy Schulz, Manuel Höferlin, Mario Brandenburg, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 19/2064 –

Hessentrojaner und Online-Durchsuchung: Zum Gesetzentwurf der hessischen Landesregierung zur Neuausrichtung des Verfassungsschutzes

Vorbemerkung der Fragesteller

Mit dem Gesetzentwurf zur Neuausrichtung des Verfassungsschutzes in Hessen (Hessischer Landtag, Drucksache 19/5412) plant die hessische Landesregierung eine Ausweitung der Befugnisse des Landesamtes für Verfassungsschutz (LfV). Insbesondere soll das LfV Hessen danach die Befugnis und Mittel erhalten, zur Informationsgewinnung Computersysteme zu hacken. Gerade der geplante Einsatz zur sog. Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) und zur „Online-Durchsuchung“ informationstechnischer Systeme wurde von verschiedenen Gruppierungen (Sachverständigenauskunft des Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. – FifF www.fiff.de/presse/pressemitteilungen/FIfF_Stellungnahme_HVSG_Hessentrojaner.pdf sowie die Stellungnahme des Chaos Computer Club e. V. CCC https://ccc.de/system/uploads/252/original/CCC-staatstrojaner-hessen.pdf) sowohl aus technischer als auch verfassungsrechtlicher Sicht kritisiert.

So weist bspw. der CCC in seiner Stellungnahme zum vorliegenden Gesetzentwurf darauf hin, dass ebenjener nicht die 2008 vom Bundesverfassungsgericht in einem Urteil festgelegten Bedingungen für den Einsatz von Staatstrojanern erfüllt: „Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen“ (vgl. BVerfG, Urt. vom 27. Februar 2008 – 1 BvR 370/07, 1 BvR 595/07, 2. Leitsatz). Der CCC konstatiert, dass im vorliegenden Gesetzentwurf diese Einschränkung in Bezug auf die Online-Durchsuchung nicht erfolgen würde. Außerdem erfolge noch nicht einmal eine Einschränkung auf Straftaten nach § 3 Absatz 1 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G10-Gesetz).

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 23. Mai 2018 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

Gerade aufgrund der polarisierenden öffentlichen Debatte, der Schwere eines solchen Eingriffs und den damit einhergehenden technischen Risiken, ist es nach Ansicht der Fragesteller notwendig, dass sich auch der Deutsche Bundestag und die Bundesregierung mit dieser Problematik beschäftigen.

1. Hat die Bundesregierung Kenntnis von dem oben genannten Gesetzentwurf?

   Wenn ja, hat die Bundesregierung sich hierzu eine Meinung gebildet, insbesondere dazu, ob die §§ 6 ff. des Gesetzentwurfs

   a) die Vorgaben des BVerfG, insbesondere die im oben genannten Urteil des BVerfG sowie der Entscheidung zum BKA-Gesetz (Urteil vom 20. April 2016, 1 BvR 966/09 und 1 BvR 1140/09) aufgestellten Bedingungen für die Infiltration informationstechnischer Systeme – sowohl zum Zwecke der Online-Durchsuchung als auch der Quellen-Telekommunikationsüberwachung – erfüllen;

   b) einen ausreichenden Schutz des Kernbereichs privater Lebensgestaltung enthalten;

   c) das zu kompromittierende informationstechnische System ausreichend klar definieren, damit insbesondere sichergestellt ist, dass ein Zugriff auf ein System zumindest dessen Nutzung voraussetzt und nicht lediglich der Verdacht ausreicht, auf einem System könnten sich relevante Daten befinden;

   d) einen Eingriff auch auf Systeme, die nach der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) Teil der kritischen Infrastruktur sind (etwa Stromnetze, Internetknotenpunkte), oder auch Behördennetze, Fahrzeugelektronik sowie medizinisch genutzte Computersysteme (Herzschrittmacher, lebenserhaltende Maschinen) ausschließen und, wenn nicht, auf welche Systeme ein solcher Zugriff möglich wäre;

   e) mit der Kompromittierung informationstechnischer Systeme Dritter, sofern diese Systeme durch die von der Maßnahme betroffene Person genutzt werden, dem LfV die Möglichkeit eröffnet, ganze Serversysteme wie bspw. E-Mailserver zu hacken;

   f) die Gefahr erhöhen, dass damit die Funktionsfähigkeit der betroffenen Systeme gefährdet und die Erfassung der Daten vieler Unbeteiligter nicht ausgeschlossen werden kann?

Die Fragen 1a bis 1f werden gemeinsam beantwortet. Die Bundesregierung hat Kenntnis von dem Gesetzentwurf, der als Landtagsdrucksache – wie oben angegeben – veröffentlicht ist. Die Bundesregierung hat sich zu dem Gesetzentwurf keine Meinung gebildet. In der föderalen Ordnung des Grundgesetzes, die Bund und Ländern je eigene Gesetzgebungszuständigkeiten zuweist, besteht dazu kein Anlass.

2. Welche Konsequenzen hat die Bundesregierung nach den Attacken mit dem sogenannten WannaCry-Trojaner, der eine von der NSA für mindestens fünf Jahre geheim gehaltene Sicherheitslücke ausnutzte und 230 000 Computer in über 150 Ländern infizierte, im Hinblick auf die Geheimhaltung von Sicherheitslücken zum Zwecke nachrichtendienstlicher Ermittlungen gezogen?

3. Sieht die Bundesregierung in einer aus Sicht der Fragesteller aufgrund des Gesetzentwurfes zu befürchtenden Praxis, sogenannte Zero-Day-Exploits auf dem Schwarzmarkt zu kaufen oder Sicherheitslücken geheim zu halten, um diese zur Infiltration informationsdienstlicher Systeme auszunutzen, eine Gefahr für die IT-Sicherheit des Bundes oder kritischer Infrastruktur?

   Hält die Bundesregierung den hessischen Landesverfassungsschutz – auch im Hinblick auf die Kooperationsverpflichtung in Angelegenheiten des Verfassungsschutzes nach §§ 1 Absatz 2 und § 6 Absatz 1 Satz 1 der Bundesverfassungsschutzgesetzes – gegenüber dem Bund für verpflichtet, diese Gefahr zu vermeiden?

   Wenn ja, was gedenkt die Bundesregierung im Falle eines Verstoßes gegen diese Verpflichtung zu unternehmen?

Die Fragen 2 und 3 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Die Bundesregierung setzt sich inhaltlich mit der Thematik des Umgangs mit Sicherheitslücken und Exploits (auch Zero-Day Exploits) auseinander. Da die Meinungsbildung innerhalb der Bundesregierung nicht abgeschlossen ist, kann weder zur Frage des möglichen Ankaufs noch zum möglichen Umgang mit (erheblichen) Sicherheitslücken in Software- und Hardwareprodukten eine Aussage getroffen werden.

Nach § 2 Absatz 1 Satz 2 des genannten Gesetzentwurfs ist Aufgabe des Landesamts für Verfassungsschutz, es den zuständigen Stellen zu ermöglichen, rechtzeitig die erforderlichen Maßnahmen zur Abwehr von Gefahren für die freiheitliche demokratische Grundordnung, den Bestand und die Sicherheit des Bundes und der Länder zu treffen. Die Bundesregierung sieht in der Wahrnehmung dieser Aufgabe keine Gefahr für die IT-Sicherheit des Bundes oder kritischer Infrastruktur.

4. Entspricht es der Auffassung der Bundesregierung, dass die Quellen-TKÜ technisch mit der Online-Durchsuchung vergleichbar ist?

Es wird auf die Antwort der Bundesregierung zu Frage 14 der Kleinen Anfrage der Fraktion der FDP „Rechtsgrundlagen und Einsatz der Quellen-Telekommunikationsüberwachung“ auf Bundestagsdrucksache 19/1505 verwiesen.

5. Entspricht es der Auffassung der Bundesregierung, dass die Quellen-TKÜ hinsichtlich ihrer rechtlichen Anforderungen, insbesondere im Hinblick auf einen Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Artikel 2 Absatz 1 i. V. m. Artikel 1 Absatz 1 des Grundgesetzes, mit einer Online-Durchsuchung vergleichbar ist?

Es wird auf die Antwort der Bundesregierung zu Frage 15 der Kleinen Anfrage der Fraktion der FDP „Rechtsgrundlagen und Einsatz der Quellen-Telekommunikationsüberwachung“ auf Bundestagsdrucksache 19/1505 verwiesen.

6. Hat sich die Bundesregierung vor dem Hintergrund von Frage 4 und 5 eine Meinung zu den im hessischen Gesetzentwurf geplanten unterschiedlichen Eingriffshürden für die Quellen-TKÜ und die Online-Durchsuchung gebildet?

   Wenn ja, welche?

Auf die Antwort zu Frage 1 wird verwiesen.

7. Wie bewertet die Bundesregierung eine Ausweitung der nachrichtendienstlichen Befugnisse im Hinblick auf die Überwachung informationstechnischer Systeme vor dem Hintergrund, dass Nachrichtendienste nach Ansicht der Fragesteller wesentlich schwieriger demokratisch zu kontrollieren sind als bspw. Polizeibehörden?

Auf die Antwort zu Frage 1 wird verwiesen. Die Nachrichtendienste des Bundes unterliegen einer besonders intensiven Kontrolle, insbesondere durch das Parlamentarische Kontrollgremium nach Artikel 45d des Grundgesetzes (GG).

8. Ist die Bundesregierung – auch im Hinblick auf die Koordinierungsfunktion des Bundesamts für den Verfassungsschutz – der Auffassung, dass auf Grundlage deutscher Bundes- und Landesgesetze auf informationstechnische Systeme wie z. B. E-Mailserver zugegriffen werden darf, die

   a) sich nicht in dem Land befinden, in dem dieses Gesetz gilt, sondern in einem anderen Bundesland;

   b) sich nicht innerhalb der Bundesrepublik Deutschland befinden, sondern in einem anderen europäischen Land?

9. Ist eine deutsche Behörde nach Auffassung der Bundesregierung verpflichtet, den Zugriff auf informationstechnische Systeme zu beenden, wenn sich herausstellt, dass das informationstechnische System sich nicht innerhalb der Bundesrepublik Deutschland befindet?

Die Fragen 8 und 9 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Die Entscheidung über die Durchführung, bzw. die Fortsetzung derartiger Zugriffe ist von den zuständigen Behörden nach Maßgabe des jeweiligen Einzelfalls unter Berücksichtigung der nationalen Befugnisnormen und der anwendbaren völkerrechtlichen Verträge zu entscheiden.

Der Bundesregierung erschließt sich kein Bezug der Koordinierungsfunktion des Bundesamtes für Verfassungsschutz (BfV) zur aufgeworfenen Frage.

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333