Deutscher Bundestag **Drucksache 18/13413**

18. Wahlperiode 21.08.2017

Kleine Anfrage

der Abgeordneten Dr. Konstantin von Notz, Hans-Christian Ströbele, Volker Beck (Köln), Katja Keul, Renate Künast, Monika Lazar und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Einsatz von Schadsoftware (sog. Bundestrojaner) und Zurückhaltung und Ausnutzung von Sicherheitslücken durch Bundesbehörden

Seit der Änderung des Bundeskriminalamtgesetzes (BKAG) im April 2017 hat das BKA in § 49 BKAG die Ermächtigung zum präventiv-polizeilichen Einsatz von sog. Staatstrojanern erhalten. Dabei wurde in § 49 BKAG u. a. verfahrensrechtlich nicht sichergestellt, „dass die vom BKA einzusetzende Überwachungs-Software Mindestanforderungen an die Datensicherheit erfüllen“ (Buermeyer, Stellungnahme für die Öffentliche Anhörung zum Gesetzentwurf zur Neustrukturierung des BKAG, Ausschussdrucksache 18(4)806 E). Die Rechtsgrundlage für den Einsatz der Staatstrojaner führt zu einem Interesse der Sicherheitsbehörden, Sicherheitslücken offen zu halten, um Systeme von Zielpersonen infiltrieren zu können und nicht im Sinne der Cybersicherheit und des Schutzes aller Bürgerinnen und Bürger an die zuständigen Behörden und die Betroffenen zu melden, damit diese geschlossen werden. Das Gesetz tritt am 25. Mai 2018 in Kraft. Bezüglich der Frage, ob die vom BKA entwickelten Trojaner sowie die zusätzlich erworbenen, kommerziellen Trojanerprodukte verfassungskonform eingesetzt werden können, bestehen aus Sicht der Fragesteller weiterhin erhebliche Zweifel. Die Rechtmäßigkeit des Einsatzes und die Verfassungskonformität des Programms wären u. a. nur über die vollständige Offenlegung des Quellcodes nachzuweisen. Dass die Schadsoftware wie im Falle der sog. Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) ausschließlich auf Kommunikationsvorgänge beschränkt werden kann, halten Experten jedoch für kaum möglich (vgl. https://netzpolitik.org/2017/staatstrojaner-bundestag-beschliesst-diese-woche-das-krasseste-ueberwachungsgesetz-der-legislaturperiode/). Durch die Schaffung neuer Rechtsgrundlagen in der Strafprozessordnung (StPO) zum Einsatz von Trojanern in der Strafverfolgung verschärft sich die Problematik der vom BKA entwickelten Software. Es besteht die Möglichkeit, dass die Software massenhaft in der Strafverfolgung eingesetzt werden wird und sich die Risiken sowohl für die Rechte der Bürgerinnen und Bürger als auch für die IT-Sicherheit dadurch potenzieren. Zudem wurden jüngst Berichte darüber öffentlich, dass das BKA jedoch nicht einmal die passende Überwachungssoftware besitze, um die als geringfügigerer Eingriff geltende, sog. Quellen-TKÜ durchführen zu können. So funktioniere der neue Bundestrojaner nach Informationen der „taz“ nur auf Computern mit den Betriebssystemen Windows 7 und Windows 8. An einer Version für Windows 10 werde gearbeitet. Noch gar keine Lösung gibt es angeblich für die gängigen Betriebssysteme von Smartphones – wo eigentlich der Hauptbedarf bestehe (taz vom 20. Januar 2017, www.taz.de/!5373564/).

Wir fragen die Bundesregierung:

1. Wie oft gebrauchte das BKA seit 2008 seine Befugnisse gemäß den §§ 20g bis 20n BKAG (bitte nach Norm, Jahr und Zahl der je Betroffenen aufschlüsseln)?
2. In wie vielen Fällen davon war die gezielte Ausnutzung von sog. Zero-Day-Sicherheitslücken Grundlage und Voraussetzung des Einsatzes?
3. Wie viele allgemein technisch unterscheidbare Verfahren der gezielten Ausnutzung von IT-Sicherheitslücken einzelner Kommunikationsanbieter unterhalb der Schwelle des Trojanereinsatzes (vgl. dazu etwa https://motherboard.vice.com/de/article/exklusiv-wie-das-bka-telegram-accounts-von-terrorverdächtigen) werden von Seiten der Bundesregierung bislang unterschieden (bitte im Einzelnen erläutern)?
4. Wie oft kamen diese Verfahren bis zum heutigen Tage jeweils zum Einsatz, und auf welcher Rechtsgrundlage konnte dies nach Auffassung der Bundesregierung geschehen?
5. Welche Konsequenzen zieht die Bundesregierung aus dem landgerichtlichen Verfahren zu den Ermittlungen gegen Tatverdächtige der Old-School-Society-Gruppe und die im Verfahren sowie in der öffentlichen Diskussion dazu aufgeworfenen rechtlichen Fragen (Quelle siehe Frage 3)?
6. Wie oft sind der Bundesnachrichtendienst, der Militärische Abschirmdienst, das Bundesamt für Verfassungsschutz, das BKA, das Zollkriminalamt und die Bundespolizei seit 2008 jeweils in Messenger-Dienste-Konten von nach dem Grundgesetz geschützten Personen sowie Angehörigen von Drittstaaten eingedrungen?
7. Auf welcher Rechtsgrundlage erfolgten jeweils diese Zugriffe?
8. In wie vielen Fällen davon waren sog. Zero-Day-Sicherheitslücken Grundlage und Voraussetzung der jeweiligen Maßnahme?
9. Wie oft wurde die Quellen-TKÜ-Software des BKA (RCIS) bereits seit Freigabe im Februar 2016 eingesetzt?
10. Auf welcher Rechtsgrundlage erfolgte nach Auffassung der Bundesregierung der jeweilige Einsatz?
11. Wie oft wurde die Quellen-TKÜ-Software des BKA (FinSpy) seit 2015 eingesetzt?
12. Auf welcher Rechtsgrundlage erfolgte der jeweilige Einsatz?
13. Von welchen Bundesländern wurde die Quellen-TKÜ-Software des BKA nach Kenntnis der Bundesregierung jeweils erlangt, und in welchen Ländern wurde sie bereits wie häufig konkret eingesetzt?
14. Von welchen Behörden wurde die Quellen-TKÜ-Software nach Kenntnis der Bundesregierung wie häufig eingesetzt (Nennung der Behörde und die Anzahl der Einsetzung)?
15. Um welche Verfahren handelt es sich dabei (Nennung der Deliktsbereiche)?
16. Wie hoch waren die Entwicklungskosten im BKA in Bezug auf die Quellen-TKÜ-Software?
17. Wie ist der Stand der Entwicklung der Version RCIS 2.0 für Mobilgeräte?
18. Welche Überprüfungen der Sicherheit der Quellen-TKÜ-Software RCIS haben vor ihrer Freigabe im Februar 2016 stattgefunden?
19. Durch wen erfolgte die Überprüfung?
20. Wie hoch waren die Kosten?

21. Hat die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit vollumfänglichen Zugriff auf alle zur Prüfung nach dem BDSG erforderlichen Informationen und Daten (einschließlich der Quellcodes der unterschiedlichen Trojanerprodukte) erhalten?
22. Wenn nein, warum nicht?
23. Auf welche Weise ist das Bundesamt für Sicherheit in der Informationstechnik (BSI) nach wie vor in den Prozess der Erstellung der Trojaner eingebunden?
24. Stellt die Bundesregierung den sog. Trojanerleitfaden (Titel: „Bedrohung der Informationssicherheit durch den gezielten Einsatz von Schadprogrammen“) der Öffentlichkeit zur Verfügung, damit nachvollzogen werden kann, welche Empfehlungen diese dafür zuständige Behörde ursprünglich gegeben hat, und wenn nein, warum nicht (vgl. https://netzpolitik.org/2015/geheime-kommunikation-bsi-programmierte-und-arbeitete-aktiv-am-staatstrojaner-streitet-aber-zusammenarbeit-ab/)?
25. Welche Ergebnisse der Quellcodeprüfung der BKA-eigenen Quellen-TKÜ-Software RCIS lieferte der Bericht des BSI-zertifizierten Softwareprüflabors TÜV Informationstechnik GmbH?
26. Kommt die Quellen-TKÜ-Software ebenfalls unter Ausnutzung von verdeckten Software-Schwachstellen (sog. Zero Day Exploits) zum Einsatz?
27. Wer ist konkret mit der Beschaffung der sog. Zero Day Exploits beauftragt?
28. Auf welche Weise werden diese Sicherheitslücken derzeit erworben?
29. Wer kontrolliert und überprüft den Ankauf der Sicherheitslücken?
30. Verfügen die zuständigen Stellen über einen eigenen Etat für den Erwerb der entsprechenden Lücken?
31. Wenn ja, wie hoch ist dieser Etat, und bestehen Vorgaben und Richtlinien für den Ankauf dieser sog. Zero Day Exploits?
32. Wird das BKA die von ihm entwickelte oder erworbene Software zur Quellen-TKÜ und Onlinedurchsuchung den Polizei- und Strafverfolgungsbehörden des Bundes und der Länder zur Verfügung stellen, wenn die neu geschaffenen Rechtsgrundlagen zur Telekommunikationsüberwachung und Onlinedurchsuchung in der StPO in Kraft treten?
33. Teilt die Bundesregierung die Auffassung, dass die Zurückhaltung bzw. fehlende staatliche Meldung jeglicher Formen von Sicherheitslücken an Hersteller wie Bürgerinnen und Bürger im konkreten Fall nicht nur Gefahren für Einzelpersonen, sondern für die kritischen Infrastrukturen der Bundesrepublik Deutschland insgesamt nach sich ziehen können, und wie verantwortet und rechtfertigt sie diese gravierende Gefährdungslage?

Berlin, den 18. August 2017

Katrin Göring-Eckardt, Dr. Anton Hofreiter und Fraktion

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