Deutscher Bundestag **Drucksache 19/19092**

19. Wahlperiode 12.05.2020

Kleine Anfrage

der Abgeordneten Martina Renner, Dr. André Hahn, Gökay Akbulut, Simone Barrientos, Anke Domscheit-Berg, Ulla Jelpke, Niema Movassat, Norbert Müller (Potsdam), Petra Pau, Dr. Petra Sitte, Kersten Steinke, Friedrich Straetmanns, Dr. Kirsten Tackmann und der Fraktion DIE LINKE.

Einsatz von Schadsoftware und Ausnutzen von Sicherheitslücken durch Bundesbehörden

Seit der Änderung des Bundeskriminalamtgesetzes (BKAG) im Frühjahr 2017 darf das BKA Schadsoftware wie Trojaner bzw. Überwachungssoftware auch präventiv zur sog. Gefahrenabwehr im Bereich des internationalen Terrorismus einsetzen. Darüber hinaus steht diese Möglichkeit den Polizeien auch im Zusammenhang mit der Strafverfolgung als repressives Mittel für die Aufklärung „besonders schwerer Straftaten“ zur Verfügung. Auch der Zoll hat inzwischen eine gesetzliche Regelung für den Einsatz von Überwachungssoftware u. a. für die präventive Telekommunikationsüberwachung erhalten. In mehreren Bundesländern (u. a. Bayern, Hessen, Niedersachsen) wurden ebenfalls vergleichbare Regelungen eingeführt. Zuletzt wurde berichtet, dass künftig auch dem Bundesamt für Verfassungsschutz (BfV) der Angriff auf informationstechnische Systeme erlaubt werden soll (https://www.spiegel.de/politik/deutschland/horst-seehofer-verfassungsschutz-soll-trojaner-einsetzen-koennen-a-1ef96a12-fc06-4f0f-a9ca-235326b0f30b). Der tatsächliche Umfang des Einsatzes, deren Nutzung sowie der insoweit möglicherweise sogar angerichtete Schaden durch diese Überwachungsmaßnahmen ist völlig ungewiss, da Bundesregierung und Behörden an einer transparenten Information der Öffentlichkeit nicht interessiert sind und stattdessen Sicherheitsbedenken und Geheimhaltungsinteressen zitieren.

Wir fragen die Bundesregierung:

1. Wie oft gebrauchte das BKA seit dem 1. Juni 2017 seine Befugnisse gemäß den §§ 20h, 20k, 20l Absatz 2 BKAG a. F. bzw. §§ 46, 49, 51 Absatz 2 BKAG n. F. (bitte nach Norm, Jahr und Zahl der je Betroffenen aufschlüsseln)?
2. 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)?

3. Wie oft kamen diese oder vergleichbare Verfahren bis zum heutigen Tage jeweils zum Einsatz, und auf welcher Rechtsgrundlage konnte dies nach Auffassung der Bundesregierung geschehen?
4. Wie oft sind der Bundesnachrichtendienst (BND), das Bundesamt für den Militärischen Abschirmdienst (BAMAD), das BfV, das BKA, das Zollkriminalamt und die Bundespolizei seit dem 1. Juni 2017 jeweils in Messenger-Dienste-Konten von nach dem Grundgesetz geschützten Personen sowie Angehörigen von Drittstaaten eingedrungen?
5. Wie oft wurde die Quellen-TKÜ-Software (TKÜ = Telekommunikationsüberwachung) des BKA (RCIS) seit dem 1. Juni 2017 eingesetzt, und auf welcher Rechtsgrundlage erfolgte dies jeweils?
6. In wie vielen Fällen war die gezielte Ausnutzung von sog. Zero-Day-Sicherheitslücken Grundlage und Voraussetzung des Einsatzes von RCIS?
7. Wie viele Versionen des RCIS wurden vom BKA oder in seinem Auftrag entwickelt?
8. Wie oft wurde die Quellen-TKÜ-Software des BKA (FinSpy) seit dem 1. Juni 2017 eingesetzt, und auf welcher Rechtsgrundlage erfolgte dies jeweils?
9. In wie vielen Fällen war die gezielte Ausnutzung von sog. Zero-Day-Sicherheitslücken Grundlage und Voraussetzung des Einsatzes von FinSpy?
10. Von welchen anderen Bundesbehörden wurde nach Kenntnis der Bundesregierung die oben genannte oder andere Quellen-TKÜ-Software seit dem 1. Juni 2017 wie häufig eingesetzt (bitte nach Behörde, Jahr und Anzahl der Einsetzungen aufschlüsseln)?
11. In wie vielen Fällen war die gezielte Ausnutzung von sog. Zero-Day-Sicherheitslücken Grundlage und Voraussetzung des Einsatzes von Quellen-TKÜ-Software durch andere Bundesbehörden?
12. Welchen Phänomenbereichen (Organisierte Kriminalität, Politisch motivierte Kriminalität – PMK, Internationaler Terrorismus, Betäubungsmittel(BtM)-Handel, Geldwäsche usw.) waren bzw. sind die in Frage 10 genannten Fälle zuzuordnen?
13. Von welchen Bundesländern wurde die oben genannte oder andere Quellen-TKÜ-Software des BKA nach Kenntnis der Bundesregierung seit dem 1. Juni 2017 jeweils erlangt, und in welchen Ländern wurde sie bereits wie häufig konkret eingesetzt?
14. Welchen Phänomenbereichen (Organisierte Kriminalität, PMK, Internationaler Terrorismus, BtM-Handel, Geldwäsche usw.) waren bzw. sind die in Frage 13 genannten Fälle nach Kenntnis der Bundesregierung zuzuordnen?
15. Welche Behörden des Bundes sind nach Kenntnis der Bundesregierung mit der Suche nach und der Prüfung von sog. Zero-Day-Sicherheitslücken beschäftigt?
16. In welchem Umfang haben sich welche Bundesbehörden sog. Zero-Day-Sicherheitslücken wann beschafft oder waren hieran wann auf europäischer bzw. multilateraler Ebene beteiligt?

17. In welcher Höhe sind nach Kenntnis der Bundesregierung bei der Suche bzw. Beschaffung von Informationen betreffend sog. Zero-Day-Sicherheitslücken seit dem 1. Januar 2018 Kosten entstanden (bitte nach Jahr, Behörde und Höhe sowie Zweck der Aufwendungen aufschlüsseln)?

Berlin, den 7. Mai 2020

Amira Mohamed Ali, Dr. Dietmar Bartsch und Fraktion

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.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