Deutscher Bundestag **Drucksache 19/20245**

19. Wahlperiode 22.06.2020

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Martina Renner, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 19/19092 –

Einsatz von Schadsoftware und Ausnutzen von Sicherheitslücken durch Bundesbehörden

Vorbemerkung der Fragesteller

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.

Vorbemerkung der Bundesregierung

Zwar ist der parlamentarische Informationsanspruch grundsätzlich auf die Beantwortung gestellter Fragen in der Öffentlichkeit angelegt, soweit parlamentarische Anfragen jedoch Umstände betreffen, die aus Gründen des Staatswohls geheimhaltungsbedürftig sind, hat die Bundesregierung zu prüfen, ob und auf welche Weise die Geheimhaltungsbedürftigkeit mit dem parlamentarischen Informationsanspruch in Einklang gebracht werden kann.

Die Bundesregierung ist nach sorgfältiger Prüfung zu der Auffassung gelangt, dass aufgrund der Schutzbedürftigkeit der erfragten Informationen eine Beantwortung sämtlicher Fragen in offener Form nur teilweise erfolgen kann.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 19. Juni 2020 übermittelt.

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

Im Einzelnen:

Die Antworten zu den Fragen 1, 4, 5, 7 und 10 sind in Teilen als „VS – Nur für den Dienstgebrauch“ eingestuft. Die erbetenen Auskünfte sind in Teilen geheimhaltungsbedürftig, weil sie Informationen enthalten, die im Zusammenhang mit der Arbeitsweise und Methodik der von der Kleinen Anfrage betroffenen Behörden des Bundes und insbesondere deren Aufklärungsaktivitäten und Analysemethoden stehen. Die Fragen betreffen zum Teil detaillierte Einzelheiten zu ihren technischen Fähigkeiten und ermittlungstaktischen Verfahrensweisen. Aus dem Bekanntwerden der Antworten könnten Rückschlüsse auf Vorgehensweise, Fähigkeiten und Methoden der Sicherheitsbehörden gezogen werden, was wiederum nachteilig für die Aufgabenerfüllung der durchführenden Stellen und damit für die Interessen der Bundesrepublik Deutschland sein kann.

Deshalb sind die Antworten zu den genannten Fragen gemäß § 2 Absatz 2 Nummer 4 der Allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung – VSA) in Teilen als „VS – Nur für den Dienstgebrauch“ eingestuft und werden als nicht zur Veröffentlichung in einer Bundestagsdrucksache bestimmte Anlage übermittelt.*

Die Antwort zu Frage 4 wurde als „VS – Geheim“ eingestuft, da die erbetenen Auskünfte Informationen enthalten, die im Zusammenhang mit der Arbeitsweise und Methodik der Nachrichtendienste des Bundes und insbesondere deren Aufklärungsaktivitäten und Analysemethoden stehen. Der Schutz vor allem der technischen Aufklärungsfähigkeiten der Nachrichtendienste des Bundes stellt für deren Aufgabenerfüllung einen überragend wichtigen Grundsatz dar. Er dient der Aufrechterhaltung der Effektivität nachrichtendienstlicher Informationsbeschaffung durch den Einsatz spezifischer Fähigkeiten und damit dem Staatswohl. Eine Veröffentlichung von Einzelheiten betreffend solche Fähigkeiten würde in zunehmendem Maße zur Ineffektivität der eingesetzten Mittel führen, da Personen im Zielspektrum der Maßnahmen sich auf die Vorgehensweisen und Fähigkeiten der Sicherheitsbehörden einstellen und entsprechend auf andere Kommunikationswege ausweichen könnten. Dies hätte – mit Blick auf das derzeitige Kommunikationsverhalten der im Fokus stehenden Akteure – eine wesentliche Schwächung der den Nachrichtendiensten des Bundes zur Verfügung stehenden Möglichkeiten zur Informationsgewinnung zur Folge.

Dies würde für die Auftragserfüllung der Nachrichtendienste des Bundes erhebliche Nachteile zur Folge haben. Insofern könnte die Offenlegung entsprechender Informationen die Sicherheit der Bundesrepublik Deutschland gefährden oder ihren Interessen schweren Schaden zufügen. Deshalb sind die entsprechenden Informationen als Verschlusssache gemäß § 2 Absatz 2 Nummer 2 VSA „VS – Geheim“ eingestuft und werden zur Einsichtnahme in der Geheimschutzstelle des Deutschen Bundestages hinterlegt.**

Die Beantwortung der Fragen 2, 3, 10, 16 und 17 berühren in besonders hohem Maße das Staatswohl. Nach Abwägung ist die Bundesregierung zu dem Schluss gekommen, dass auch das geringfügige Risiko ihrer Offenlegung nicht getragen werden kann und deshalb die Fragen hinsichtlich der Nachrichtendienste des Bundes auch nicht in eingestufter Form beantwortet werden können.

---

* Das Bundesministerium des Innern, für Bau und Heimat hat Teile der Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

** Das Bundesministerium des Innern, für Bau und Heimat hat die Antwort als „VS – Geheim“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

Das verfassungsmäßig verbürgte Frage- und Informationsrecht des Deutschen Bundestages gegenüber der Bundesregierung wird durch schutzwürdige Interessen von Verfassungsrang begrenzt, wozu auch und insbesondere Staatswohlerwägungen zählen.

Durch eine Offenlegung der erfragten Informationen würden Einzelheiten zur konkreten Methodik der Nachrichtendienste benannt, die die weitere Arbeitsfähigkeit und Aufgabenerfüllung auf dem spezifischen Gebiet der technischen Aufklärung gefährden würde.

Eine Bekanntgabe von Einzelheiten über angewandte Verfahren im Zusammenhang mit Sicherheitslücken in IT-Systemen und deren Beschaffung würde weitgehende Rückschlüsse auf die Arbeitsweise sowie technischen Fähigkeiten und damit mittelbar auch auf die technische Ausstattung und das Aufklärungspotential der Nachrichtendienste zulassen.

Dadurch könnte die Fähigkeit, nachrichtendienstliche Erkenntnisse zu gewinnen, in erheblicher Weise negativ beeinflusst werden. Die Gewinnung von Informationen durch technische Aufklärungsmaßnahmen ist für die Sicherheit der Bundesrepublik Deutschland und für die Aufgabenerfüllung der Nachrichtendienste jedoch unerlässlich.

Sofern solche Informationen entfallen oder wesentlich zurückgehen sollten, würden empfindliche Informationslücken auch im Hinblick auf die Sicherheitslage der Bundesrepublik Deutschland drohen. Dies betrifft insbesondere die Möglichkeiten zur Aufklärung nationaler und internationaler terroristischer Bestrebungen, bei denen derartige Kommunikationsmittel in besonderem Maße von den beobachteten Personen genutzt werden.

Insofern birgt eine Offenlegung der erfragten Informationen die Gefahr, dass Einzelheiten zur konkreten Methodik und zu aus den vorgenannten Gründen im hohen Maße schutzwürdigen spezifischen Fähigkeiten der Nachrichtendienste des Bundes bekannt würden. Infolgedessen könnten sowohl staatliche als auch nichtstaatliche Akteure Rückschlüsse auf spezifische Vorgehensweisen und Fähigkeiten der Nachrichtendienste des Bundes gewinnen. Dies würde folgenschwere Einschränkungen der Informationsgewinnung bedeuten, womit letztlich der gesetzliche Auftrag der Nachrichtendienste des Bundes (§ 1 Absatz 2 des Gesetzes über den Bundesnachrichtendienst [BNDG], § 3 Absatz 1 des Bundesverfassungsschutzgesetzes [BVerfSchG], § 1 Absatz 1 und § 14 Absatz 1 des Gesetzes über den militärischen Abschirmdienst [MADG]) nicht mehr sachgerecht erfüllt werden könnte.

Soweit die Sicherheitsbehörden des Bundes mit polizeilichen Aufgaben Bundeskriminalamt (BKA), Bundespolizei (BPOL) und Zollkriminalamt/Financial Intelligence Unit (ZKA/FIU) von den Fragestellungen betroffen sind, kann die Beantwortung der Fragen 2, 4, 5, 6, 8, 9, 13, 16 und 17 ebenfalls nicht bzw. nicht vollumfänglich erfolgen.

Eine Bekanntgabe von Einzelheiten der bei diesen Behörden zur Bekämpfung von Kriminalität und Terrorismus im Rahmen ihrer jeweiligen Zuständigkeit eingesetzten Softwareprodukte für die Bearbeitung und Auswertung von Ermittlungsverfahren würde weitgehende Rückschlüsse auf die technischen Fähigkeiten sowie die taktischen Einzelheiten bzw. Arbeitsabläufe und damit mittelbar auch sowohl auf die derzeitige als auch die geplante technische Ausstattung sowie das Strafverfolgungs- und Gefahrenabwehrpotenzial dieser Behörden zulassen. Diese taktischen Einzelheiten umfassen insbesondere die hier von den Fragestellungen umfassten Methoden zur forensischen Sicherung und Analyse, Umgehung oder Entsperrung von Verschlüsselungen sowie das Einbringen von Software, darüber hinaus auch die Informationen über den konkreten operativen Einsatz entsprechender Software inklusive der Frage über etwa-

ige Alternativen. Durch ein Bekanntwerden der genannten Methoden könnten die Fähigkeiten der Sicherheitsbehörden mit polizeilichen Aufgaben, Erkenntnisse im Wege der technischen Strafaufklärung zu gewinnen, in erheblicher Weise negativ beeinflusst werden, insbesondere, wenn keine ausreichenden Alternativen zu den für die Strafverfolgung und Gefahrenabwehr genutzten Produkten zur Verfügung stehen. Denn Beschuldigte könnten sich somit gezielt eben jener Strafverfolgung und Gefahrenabwehr entziehen, etwa durch Maßnahmen zur Hinderung des Einsatzes der entsprechenden Software.

Dies ist jedoch nicht hinnehmbar, da die Gewinnung von Informationen durch eine IT- bzw. softwaregestützte Strafverfolgung und Gefahrenabwehr notwendig ist aber für die Aufgabenerfüllung dieser Behörden und damit für die Sicherheit der Bundesrepublik Deutschland und bei der Bekämpfung vor allem des Terrorismus, der politisch motivierten sowie der organisierten Kriminalität unerlässlich ist. Sofern solche Informationen entfallen oder wesentlich zurückgehen sollten, würden empfindliche Informationslücken auch im Hinblick auf die Sicherheitslage der Bundesrepublik Deutschland drohen. Dies würde folgenschwere Einschränkungen der Strafverfolgung und Gefahrenabwehr bedeuten, womit letztlich die gesetzlichen Aufträge von BKA, verankert im Grundgesetz (Artikel 73 Nummer 10 des Grundgesetzes [GG], Artikel 87 GG) und im Bundeskriminalamtgesetz [BKAG], BPOL (Artikel 87 GG sowie Bundespolizeigesetz [BPolG]) und ZKA/FIU (Artikel 87 GG, Zollfahndungsdienstgesetz (ZFdG), Geldwäschegesetz (GwG), Unionszollkodex (UZK)) nicht mehr sachgerecht erfüllt werden könnten.

Eine VS-Einstufung und Hinterlegung der erfragten Informationen in der Geheimschutzstelle des Deutschen Bundestages würde ihrer erheblichen Brisanz im Hinblick auf die Bedeutung der Informationen sowohl für die Aufgabenerfüllung der Nachrichtendienste des Bundes als auch der Sicherheitsbehörden des Bundes mit polizeilichen Aufgaben nicht ausreichend Rechnung tragen, weil insoweit auch ein geringfügiges Risiko des Bekanntwerdens unter keinen Umständen hingenommen werden kann (vgl. BVerfGE 124, 78 [139]). Schon die Angabe, mittels welcher technischen Produkte die Sicherheitsbehörden z. B. von der Telekommunikationsüberwachung Gebrauch machen, könnte zu einer Änderung des Kommunikationsverhaltens der betreffenden beobachteten Personen führen, die eine weitere Aufklärung der von diesen verfolgten Bestrebungen und Planungen unmöglich machen würde. In diesem Fall wäre ein Ersatz durch andere Instrumente nicht möglich.

Aus dem Vorgesagten ergibt sich, dass die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht überwiegt. Insofern muss ausnahmsweise das Fragerecht der Abgeordneten gegenüber den Geheimhaltungsinteressen der Sicherheitsbehörden des Bundes zurückstehen.

Bezüglich der Vorbemerkung der Fragesteller weist die Bundesregierung darauf hin, dass weder durch das BKA noch durch eine andere Sicherheitsbehörde des Bundes „Schadsoftware“ zur Durchführung von Ermittlungs- und Präventions- bzw. Aufklärungs-Maßnahmen im Kontext von Fragestellungen der hier vorliegenden Kleinen Anfrage eingesetzt wird.

Die ggf. in Bezug genommenen Softwarelösungen zur Durchführung von Maßnahmen der Informationstechnischen Überwachung durch die Sicherheitsbehörden des Bundes entsprechen den geltenden rechtlichen Rahmenbedingungen. Daher ist der Begriff „Schadsoftware“ hierfür unpassend bzw. irreführend.

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)?

Es wird auf den als „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.

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)?

Im Rahmen der Einsatz- und Ermittlungsunterstützung werden die bestehenden rechtlichen und technischen Möglichkeiten genutzt, um in Verfahren der Strafverfolgung und Gefahrenabwehr Informationen zu gewinnen. Hierbei unterscheidet die Bundesregierung zwischen der Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) und dem Online-Durchsuchungsverfahren (ODS Verfahren). Darüber hinaus wird auf die Vorbemerkung der Bundesregierung verwiesen.

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?

Es wird auf die Antworten zu den Fragen 1, 4 und 5 verwiesen. Hinsichtlich der Nachrichtendienste des Bundes ist eine Beantwortung aus den in der Vorbemerkung der Bundesregierung genannten Gründen nicht möglich.

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?

Es wird auf die als „VS – Geheim“ und „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteile gemäß der Vorbemerkung der Bundesregierung verwiesen.

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?

Neben der Aufstellung des Bundesamtes für Justiz (BfJ), einsehbar unter www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Telekommunikationsueberwachung.html wird auf den als „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen. Eine weiterführende Beantwortung ist aus den in der Vorbemerkung der Bundesregierung genannten Gründen nicht möglich.

6. In wie vielen Fällen war die gezielte Ausnutzung von sog. Zero-Day-Sicherheitslücken Grundlage und Voraussetzung des Einsatzes von RCIS?

Es wird auf Vorbemerkung der Bundesregierung verwiesen.

7. Wie viele Versionen des RCIS wurden vom BKA oder in seinem Auftrag entwickelt?

Es wird auf den als „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.

8. Wie oft wurde die Quellen-TKÜ-Software des BKA (FinSpy) seit dem 1. Juni 2017 eingesetzt, und auf welcher Rechtsgrundlage erfolgte dies jeweils?

Es wird auf die Ausführungen zu Frage 5 und die Vorbemerkung der Bundesregierung verwiesen.

9. In wie vielen Fällen war die gezielte Ausnutzung von sog. Zero-Day-Sicherheitslücken Grundlage und Voraussetzung des Einsatzes von FinSpy?

Es wird auf Vorbemerkung der Bundesregierung verwiesen.

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)?

Es wird auf den als „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung verwiesen.

Hinsichtlich der Nachrichtendienste des Bundes ist eine Beantwortung aus den in der Vorbemerkung genannten Gründen nicht möglich.

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?

Es wird auf die Antwort zu Frage 10 verwiesen.

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?

Es wird auf die Antwort zu Frage 10 verwiesen.

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?

Auf dem Gebiet der informationstechnischen Überwachung kooperieren die Sicherheitsbehörden des Bundes und der Länder miteinander. Dies kann auch die Weitergabe von Informationstechnischen Überwachungsprodukten (ITÜ-Produkten) umfassen. Darüber hinaus wird auf die Vorbemerkung der Bundesregierung verwiesen.

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?

Es wird auf die Antwort zu Frage 13 verwiesen.

15. Welche Behörden des Bundes sind nach Kenntnis der Bundesregierung mit der Suche nach und der Prüfung von sog. Zero-Day-Sicherheitslücken beschäftigt?

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) wirkt gemäß seines aus § 3 Absatz 1 des BSI-Gesetzes (BSIG) hervorgehenden gesetzlichen Auftrags darauf hin, sämtliche Sicherheitslücken umgehend und im vertrauensvollen Austausch mit den Technologieherstellern zu schließen. Nach Validierung der vorliegenden Informationen werden dem BSI bekannte Sicherheitslücken im Rahmen des Coordinated Vulnerability Disclosure (CVD)- Prinzips mit den für die Absicherung der betroffenen Produkte verantwortlichen Herstellern geteilt. Dies gilt gleichermaßen für gemäß § 7a BSIG durch das BSI entdeckte Sicherheitslücken wie auch für seitens Externer an das BSI gemeldete Sicherheitslücken. Bezüglich der Prüfung von sog. Zero-Day-Sicherheitslücken setzt sich die Bundesregierung derzeit inhaltlich mit dieser Thematik auseinander. Da die Meinungsbildung innerhalb der Bundesregierung hierzu nicht abgeschlossen ist, kann zur Frage des möglichen Umgangs mit Zero-Day-Schwachstellen lediglich im Rahmen aktuell geltender Regelungen eine Aussage getroffen werden.

16. In welchem Umfang haben sich welche Bundesbehörden sog. Zero-Day-Sicherheitslücken wann beschafft oder waren hieran wann auf europäischer bzw. multilateraler Ebene beteiligt?

Es wird auf die Vorbemerkung der Bundesregierung verwiesen.

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)?

Es wird auf die Vorbemerkung der Bundesregierung verwiesen.

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