Deutscher Bundestag **Drucksache 18/13566**

18. Wahlperiode 13.09.2017

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Dr. Konstantin von Notz, Hans-Christian Ströbele, Volker Beck (Köln), weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN
– Drucksache 18/13413 –

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

Vorbemerkung der Fragesteller

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 gel-

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 11. September 2017 übermittelt.

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

tende, 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/).

Vorbemerkung der Bundesregierung

Befugnisse zum verdeckten Eingriff in informationstechnische Systeme (§ 49 des Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes – BKAG-neu) und zur Überwachung der Telekommunikation, auch mittels Eingriffs mit technischen Mitteln in vom Betroffenen genutzte informationstechnische Systeme (§ 51 BKAG-neu) durch das Bundeskriminalamt (BKA) werden nicht erst mit dem BKAG-neu mit Wirkung vom 25. Mai 2018 in das BKAG eingeführt, sondern waren bereits mit dem Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt (BKAG) mit Wirkung zum 1. Januar 2009 eingeführt worden (§ 20k und § 20l BKAG). Das Bundesverfassungsgericht hat in seiner Entscheidung vom 20. April 2016 diese Befugnisse im Grundsatz für verfassungsgemäß erachtet (BVerfG Az. 1 BvR 966/09, Rn. 208 ff. – zitiert nach juris – für § 20k BKAG und Rn. 227 ff.). Demgemäß wurden die Befugnisse in der Neuregelung im Kern nicht geändert.

Die Änderungen des § 20k BKAG (§ 49 BKAG-neu) und des § 20l BKAG (§ 51 BKAG-neu) setzen die vom BVerfG aufgestellten Anforderung an

- den Schutz des Kernbereichs privater Lebensgestaltung,
- die ausdrückliche Regelung der Gefahrenlage, die einen Eingriff in informationstechnische Systeme bzw. eine Überwachung der Telekommunikation rechtfertigt sowie
- den Antrag zur Durchführung einer Maßnahme

um.

Als „Trojaner“ werden in der Informationstechnik in der Regel Schadprogramme bezeichnet, die widerrechtlich auf informationstechnischen Systemen ausgeführt werden und zumeist als nützliche Anwendung getarnt sind, im Hintergrund aber ohne Wissen des Anwenders eine andere Funktion erfüllen.

Das BKA setzt deshalb keine „Trojaner“ ein, sondern kann im Rahmen seiner gesetzlichen Befugnisse bei Vorliegen der rechtlichen Voraussetzungen Software zur Quellen-Telekommunikationsüberwachung oder/und Onlinedurchsuchung einsetzen, welche engen rechtsstaatlichen Anforderungen genügt. Bei dieser Software handelt es sich insbesondere um keine „Schadsoftware“.

Die Bundesregierung ist nach sorgfältiger Abwägung zu der Auffassung gelangt, dass eine Beantwortung der Fragen 1, 2, 4, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 23, 25, 26, 27, 28, 29, 30, 31, 32 in offener Form ganz oder teilweise nicht erfolgen kann. Die in den Fragen 1, 2, 4, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 23, 25, 26, 27, 28, 29, 30, 31, 32 erbetenen Auskünfte sind geheimhaltungsbedürftig, weil sie Informationen enthalten, die im Zusammenhang mit der Arbeitsweise und Methodik der von der Kleinen Anfrage betroffenen Dienststellen des Bundes und insbesondere deren Aufklärungsaktivitäten und Analysemethoden stehen. Die Antworten auf die Kleine Anfrage beinhalten zum Teil detaillierte Einzelheiten zu ihren technischen Fähigkeiten und ermittlungstaktischen Verfahrensweisen. Aus ihrem Bekanntwerden könnten Rückschlüsse

auf ihre Vorgehensweise, Fähigkeiten und Methoden gezogen werden. Deshalb sind einzelne Informationen gemäß der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA) als „VS – Nur für den Dienstgebrauch“ eingestuft und werden als nicht zur Veröffentlichung in einer Bundestagsdrucksache bestimmte Anlage übermittelt.

Eine Beantwortung der Fragen 6 und 7 für das Bundesamt für Verfassungsschutz (BfV) kann nicht in offener Form erfolgen. Die erbetenen Auskünfte sind geheimhaltungsbedürftig, weil sie Informationen enthalten, die im Zusammenhang mit der Arbeitsweise und Methodik des BfV und insbesondere dessen Aufklärungsaktivitäten und Analysemethoden stehen. Der Schutz vor allem der technischen Aufklärungsfähigkeiten des BfV im Bereich der Fernmeldeaufklärung 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 zu einer wesentlichen Schwächung der dem BfV zur Verfügung stehenden Möglichkeiten zur Informationsgewinnung führen.

Dies würde für die Auftragserfüllung des BfV erhebliche Nachteile zur Folge haben und kann für die Interessen der Bundesrepublik Deutschland schädlich sein. 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 VSA mit dem VS-Grad „VS – Geheim“ eingestuft und werden zur Einsichtnahme durch die Abgeordneten der Geheimschutzstelle des Deutschen Bundestags übermittelt.

Darüber hinaus ist die Bundesregierung nach sorgfältiger Abwägung zu der Auffassung gelangt, dass eine Beantwortung der Fragen 4 und 6 bis 8 für den Bundesnachrichtendienst (BND) sowie der Fragen 4, 8, 14, 15 und 26 bis 31 für das BfV nicht – auch nicht in eingestufter Form – erfolgen kann. Gegenstand der Fragen sind solche Informationen, die in besonderem Maße das Staatswohl berühren und daher in einer zur Veröffentlichung vorgesehenen Fassung nicht behandelt werden können. Das verfassungsrechtlich verbürgte Frage- und Informationsrecht des Deutschen Bundestages gegenüber der Bundesregierung wird durch gleichfalls Verfassungsrecht genießende schutzwürdige Interessen wie das Staatswohl begrenzt. Eine Bekanntgabe von Einzelheiten zur Ausleitung oder Lesbarmachung der über Messenger-Dienste und andere verschlüsselte Kommunikationsmittel erfolgenden elektronischen Kommunikation würde weitgehende Rückschlüsse auf die technischen Fähigkeiten und damit mittelbar auch auf die technische Ausstattung und das Aufklärungspotential des BND und des BfV zulassen. Dadurch könnten die Fähigkeiten des BND und des BfV, nachrichtendienstliche Erkenntnisse im Wege der technischen Aufklärung zu gewinnen, in erheblicher Weise negativ beeinflusst werden. Die Gewinnung von Informationen durch technische Aufklärung ist für die Sicherheit der Bundesrepublik Deutschland und für die Aufgabenerfüllung des BND und des BfV 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 angefragten Informationen die Gefahr, dass Einzelheiten zur konkreten Methodik und zu aus den vorgenannten Gründen im hohen Maße schutzwürdigen spezifischen Fähigkeiten des BND oder des BfV bekannt würden. Infolgedessen könnten sowohl staatliche als auch nichtstaatliche Akteure Rückschlüsse auf spezifische Vorgehensweisen und Fähigkeiten des BND und des BfV gewinnen.

Dies würde folgenschwere Einschränkungen der Informationsgewinnung bedeuten, womit letztlich der gesetzliche Auftrag des BND – die Sammlung und Auswertung von Informationen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind (§ 1 Absatz 2 des Gesetzes über den Bundesnachrichtendienst – BNDG) – und des BfV – Sammlung und Auswertung von Informationen über Bestrebungen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind (§ 3 Absatz 1 des Gesetzes über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz – BVerfSchG) – nicht mehr sachgerecht erfüllt werden könnte.

Eine VS-Einstufung und Hinterlegung der angefragten Informationen in der Geheimschutzstelle des Deutschen Bundestages würde ihrer erheblichen Brisanz im Hinblick auf die Bedeutung der Methoden für die Aufgabenerfüllung des BND und des BfV 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, ob und in welchem Umfang der BND oder das BfV von derartigen Methoden 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 des BND und des BfV zurückstehen.

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)?

Es wird auf die Vorbemerkung sowie den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.*

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

Es wird auf die Vorbemerkung sowie den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.*

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

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)?

Seitens der Bundesregierung wurde bislang keine allgemeine technische Unterscheidung im Sinne der Fragestellung durchgeführt.

4. Wie oft kamen diese Verfahren bis zum heutigen Tage jeweils zum Einsatz, und auf welcher Rechtsgrundlage konnte dies nach Auffassung der Bundesregierung geschehen?

Verfahren wie das in dem in Frage 3 genannten Onlineartikel beschriebene wurden durch die Bundespolizei (BPOL), das Bundesamt für den militärischen Abschirmdienst (BAMAD) und seitens des Zolls nicht eingesetzt. Im Übrigen wird auf die Vorbemerkung sowie den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.*

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)?

Die Bundesregierung nimmt zu Einzelheiten eines konkreten landgerichtlichen Verfahrens nicht Stellung.

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?

Durch das BAMAD und die BPOL wurden bislang keine Maßnahmen im Sinne der Fragestellung durchgeführt. Im Übrigen wird auf die Vorbemerkung, den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil sowie auf den als Verschlusssache mit dem Einstufungsgrad „VS – Geheim“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.**

7. Auf welcher Rechtsgrundlage erfolgten jeweils diese Zugriffe?

Es wird auf die Antwort zu Frage 6 und im Übrigen auf die Vorbemerkung, den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil sowie auf den als Verschlusssache mit dem Einstufungsgrad „VS – Geheim“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.**

---

* Das Bundesministerium des Innern hat die 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 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.

8. In wie vielen Fällen davon waren sog. Zero-Day-Sicherheitslücken Grundlage und Voraussetzung der jeweiligen Maßnahme?

Es wird auf die Antwort zu Frage 6 und im Übrigen auf die Vorbemerkung sowie den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.*

9. Wie oft wurde die Quellen-TKÜ-Software des BKA (RCIS) bereits seit Freigabe im Februar 2016 eingesetzt?

Es wird auf die Vorbemerkung sowie den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.*

10. Auf welcher Rechtsgrundlage erfolgte nach Auffassung der Bundesregierung der jeweilige Einsatz?

Es wird auf die Vorbemerkung sowie den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.*

11. Wie oft wurde die Quellen-TKÜ-Software des BKA (FinSpy) seit 2015 eingesetzt?

Es wird auf die Vorbemerkung sowie den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.*

12. Auf welcher Rechtsgrundlage erfolgte der jeweilige Einsatz?

Es wird auf die Vorbemerkung sowie den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.*

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?

Es wird auf die Vorbemerkung sowie den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.*

14. Von welchen Behörden wurde die Quellen-TKÜ-Software nach Kenntnis der Bundesregierung wie häufig eingesetzt (Nennung der Behörde und die Anzahl der Einsetzung)?

Durch das BAMAD und die BPOL wurde die Quellen-TKÜ-Software des BKA bislang nicht eingesetzt. Im Übrigen wird auf die Vorbemerkung sowie den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.*

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

15. Um welche Verfahren handelt es sich dabei (Nennung der Deliktsbereiche)?

Es wird auf die Antwort zu Frage 14 und im Übrigen auf die Vorbemerkung sowie den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.*

16. Wie hoch waren die Entwicklungskosten im BKA in Bezug auf die Quellen-TKÜ-Software?

Es wird auf die Vorbemerkung sowie den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.*

17. Wie ist der Stand der Entwicklung der Version RCIS 2.0 für Mobilgeräte?

Es wird auf die Vorbemerkung sowie den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.*

18. Welche Überprüfungen der Sicherheit der Quellen-TKÜ-Software RCIS haben vor ihrer Freigabe im Februar 2016 stattgefunden?

Es wird auf die Vorbemerkung sowie den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.*

19. Durch wen erfolgte die Überprüfung?

Es wird auf die Vorbemerkung sowie den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.*

20. Wie hoch waren die Kosten?

Es wird auf die Vorbemerkung sowie den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.*

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?

Hinsichtlich des missverständlichen und unpassenden Begriffs „Trojaner“ wird auf die Vorbemerkung der Bundesregierung verwiesen.

Der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wird durch das BKA vollumfänglicher Zugriff auf alle zur Prüfung nach BDSG erforderlichen Daten, einschließlich des Quellcodes der dem BKA zur Verfügung stehenden Softwareprodukte zur Durchführung von Quellen-TKÜ- bzw. Onlinedurchsuchungsmaßnahmen gewährt.

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

22. Wenn nein, warum nicht?

Auf die Antwort zu Frage 21 wird verwiesen.

23. Auf welche Weise ist das Bundesamt für Sicherheit in der Informationstechnik (BSI) nach wie vor in den Prozess der Erstellung der Trojaner eingebunden?

Hinsichtlich des missverständlichen und unpassenden Begriffs „Trojaner“ wird auf die Vorbemerkung der Bundesregierung verwiesen.

Im Übrigen wird auf die Vorbemerkung sowie den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.*

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/)?

Im Jahr 2007 hat das BSI unter dem Titel „Bedrohung der Informationssicherheit durch den gezielten Einsatz von Schadprogrammen“ einen Leitfaden erstellt.

Dieser sogenannte „Trojaner-Leitfaden“ enthält einen Überblick der damals aktuellen Gefährdungen, Empfehlungen zu IT-Sicherheitsmaßnahmen gegen spezialisierte Schadprogramme sowie einen Kurztest zur Einschätzung der eigenen Bedrohungslage. Der Leitfaden ist keine Anleitung zur Entwicklung oder zum Einsatz von Schadsoftware.

Da die Informationstechnologie immer schnelleren Innovationszyklen unterliegt und sich damit auch die Angreiferseite in Bezug auf die Entwicklung neuer Schadprogramme und Angriffsvektoren immer schneller weiterentwickelt, war der „Trojaner-Leitfaden“ im Vergleich zu öffentlich verfügbaren Informationen bereits nach kurzer Zeit in Teilen veraltet und überarbeitungsbedürftig. Eine Veröffentlichung des „Trojaner-Leitfadens“ als Ganzes erschien und erscheint daher nicht sinnvoll. Das BSI hat den „Trojaner-Leitfaden“ als Dokument somit auch nicht weitergeführt.

Die im „Trojaner-Leitfaden“ enthaltenen Einschätzungen und Empfehlungen zur Abwehr von Schadprogrammen sind in der Folge sowohl in den IT-Grundschutz des BSI (zum Beispiel Baustein 1.6 „Schutz vor Schadprogrammen“), in die Empfehlungen des BSI zur Cyber-Sicherheit, die auch im Rahmen der Allianz für Cyber-Sicherheit erarbeitet werden, als auch in die Internetseiten des BSI für Privatanwender (www.bsi-fuer-buerger.de) eingeflossen.

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

25. Welche Ergebnisse der Quellcodeprüfung der BKA-eigenen Quellen-TKÜ-Software RCIS lieferte der Bericht des BSI-zertifizierten Softwareprüflabors TÜV Informationstechnik GmbH?

Es wird auf die Vorbemerkung sowie den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.*

26. Kommt die Quellen-TKÜ-Software ebenfalls unter Ausnutzung von verdeckten Software-Schwachstellen (sog. Zero Day Exploits) zum Einsatz?

Es wird auf die Vorbemerkung sowie den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.*

27. Wer ist konkret mit der Beschaffung der sog. Zero Day Exploits beauftragt?

Es wird auf die Vorbemerkung sowie den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.*

28. Auf welche Weise werden diese Sicherheitslücken derzeit erworben?

Es wird auf die Vorbemerkung sowie den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.*

29. Wer kontrolliert und überprüft den Ankauf der Sicherheitslücken?

Es wird auf die Vorbemerkung sowie den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.*

30. Verfügen die zuständigen Stellen über einen eigenen Etat für den Erwerb der entsprechenden Lücken?

Es wird auf die Vorbemerkung sowie den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.*

31. Wenn ja, wie hoch ist dieser Etat, und bestehen Vorgaben und Richtlinien für den Ankauf dieser sog. Zero Day Exploits?

Es wird auf die Vorbemerkung sowie den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.*

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

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?

Es wird auf die Vorbemerkung sowie den als Verschlusssache mit dem Einstufungsgrad „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.*

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?

Schwachstellen bzw. Sicherheitslücken in informationstechnischen Systemen können, sofern diese Personen oder Stellen bekannt werden, die eine Ausnutzung der Schwachstellen zu rechtswidrigen Zwecken beabsichtigen, Risiken für IT-Infrastrukturen sowie für Bürgerinnen und Bürger darstellen. Daher diskutiert das BSI gemäß seines gesetzlichen Auftrages regelmäßig Erkenntnisse zu Sicherheitslücken, die öffentlich bekannt sind, auf eigenen Analysen beruhen oder im Rahmen der Zusammenarbeit von CERTs gewonnen werden, mit den betroffenen Herstellern, damit diese die Sicherheitslücken kurzfristig schließen können. Falls sich aus Sicherheitslücken eine Gefährdung für Bürger, Unternehmen oder Verwaltungseinrichtungen ergibt, spricht das BSI gemäß seines gesetzlichen Auftrags darüber hinaus zielgruppenspezifische oder öffentliche Warnungen aus.

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

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