Deutscher Bundestag **Drucksache 19/3398**

19. Wahlperiode 16.07.2018

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Martina Renner, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 19/2774 –

Nationale und internationale Kooperationen des Bundesamtes für die Sicherheit in der Informationstechnik

Vorbemerkung der Fragesteller

In der 18. Wahlperiode hat sich der Deutsche Bundestag aufgrund der Veröffentlichungen von Edward Snowden intensiv mit der Arbeitsweise der Nachrichtendienste befasst. Dabei wurde nach den Würdigungen der Fraktionen DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN in deren gemeinsamen Sondervotum zum Abschlussbericht des 1. Untersuchungsausschusses der 18. Wahlperiode (Bundestagsdrucksache 18/12850, S. 1394 ff.) auch die Mitwirkung des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) an der Einrichtung der Massenüberwachung des Bundesnachrichtendienstes bei der Deutschen Telekom bekannt und auch internationale Kooperationen mit US-amerikanischen und britischen Behörden (vgl. Bundestagsdrucksache 18/12850, S. 1431 ff., 551 ff.). Zudem ist bekannt geworden, dass entgegen früherer Darstellungen das BSI durch das Bundesministerium des Innern angewiesen wurde, das Bundeskriminalamt bei der Entwicklung der Software für die Quellen-TKÜ (TKÜ = Telekommunikationsüberwachung) zu unterstützen (www.heise.de/newsticker/meldung/Geheimpapiere-BSI-entwickelte-Bundestrojaner-mit-2577582.html).

Vorbemerkung der Bundesregierung

Der gesetzliche Auftrag des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) als nationale, zivile IT-Sicherheitsbehörde besteht u. a. in der präventiven Förderung der Informations- und Cybersicherheit. Die nationale und internationale Zusammenarbeit des BSI leitet sich aus der gesetzlichen Aufgabenstellung des BSI ab. Eine Aufgabe des BSI ist beispielsweise die Förderung der Sicherheit in der Informationstechnik, insbesondere die Abwehr von Gefahren für die Sicherheit der Informationstechnik des Bundes. Im Rahmen dieser Aufgabenstellung arbeitet das BSI im nationalen und internationalen Rahmen jeweils mit Behörden und Anbietern von Telekommunikationsdiensten zusammen, um seiner Pflicht von Prävention, Detektion und Abwehr von Angriffen auf die IT-Infrastrukturen der Bundesrepublik Deutschland nachzukommen.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 13. Juli 2018 übermittelt.

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

Dies umfasst aufgrund der Rolle als Nationale Kommunikationssicherheits- und Cybersicherheitsbehörde zum Beispiel für die USA auch die NSA. Diese Zusammenarbeit resultierte direkt aus der Mitgliedschaft der Bundesrepublik Deutschland in der NATO (vgl. Bundestagsdrucksache 17/14797, z. B. Antwort zu den Fragen 10 und 12).

Bezüglich des grundsätzlichen Umgangs des BSI mit Schwachstellen/Exploits ist zu betonen, dass das BSI diese im Rahmen seines gesetzlichen Auftrags des Schutzes der IT nicht unter dem Aspekt der potentiellen Verwertbarkeit für Maßnahmen einer Telekommunikationsüberwachung (z. B. für Quellen-TKÜ, Onlinedurchsuchung etc.) bewertet, sondern nur bezüglich der grundsätzlichen Ausnutzbarkeit für einen Missbrauch durch einen Angreifer mit dem Ziel Warnungen und Informationen bereitstellen zu können.

In den Fragen 1 bis 12 wird nach Kooperationen des BSI gefragt. Unter Kooperation im Sinne dieser Kleinen Anfrage ist aus Sicht der Bundesregierung eine etablierte, strukturierte, wiederkehrende und auf bestimmte Zeit ausgelegte institutionelle Zusammenarbeit zu verstehen. Zur allgemeinen Zusammenarbeit von Mitarbeitern des BSI mit ausländischen Sicherheitsbehörden und Nachrichtendiensten wird auf die Antwort zu den Fragen 19 und 20 verwiesen.

Bezüglich Frage 20 ist die Bundesregierung nach sorgfältiger Abwägung zu der Auffassung gelangt, dass eine Beantwortung nicht vollständig in offener Form erfolgen kann. Zwar ist der parlamentarische Informationsanspruch grundsätzlich auf die Beantwortung gestellter Fragen in der Öffentlichkeit angelegt. Eine Offenlegung der angefragten Informationen birgt jedoch die Gefahr erheblicher nachteiliger Auswirkungen auf die zukünftige vertrauensvolle Zusammenarbeit mit ausländischen Partnern, da eine Offenlegung von IT-Sicherheitsvorfälle in anderen Ländern durch die Bundesregierung als Vertrauensbruch angesehen werden dürfte. Die Veröffentlichung kann daher für die Interessen der Bundesrepublik Deutschland schädlich sein. Deshalb sind die entsprechenden Informationen als Verschlusssache gemäß der VSA § 3 Nummer 3 als „VS – Vertraulich“ eingestuft.

1. Wie viele Kooperationen hat das BSI seit 2015 mit ausländischen Sicherheitsbehörden oder Nachrichtendiensten im Zusammenhang mit bereits erfolgten oder begonnenen Angriffen auf in Deutschland befindliche bzw. genutzte IT-Systeme durchgeführt oder begonnen?

Das BSI hat speziell im Zusammenhang mit bereits erfolgten oder begonnenen Angriffen auf in Deutschland befindliche bzw. genutzte IT-Systeme seit dem Jahr 2015 keine Kooperationen mit ausländischen Sicherheitsbehörden oder Nachrichtendiensten durchgeführt oder begonnen. Wegen der Zusammenarbeit im Allgemeinen wird auf die Vorbemerkung sowie auf die Antwort zu den Fragen 19 und 20 verwiesen.

2. Welche deutschen und ausländischen Behörden waren an den in Frage 1 erfragten Kooperationen beteiligt (bitte nach Jahr, Anzahl, Namen und Herkunftsland der beteiligten Stellen einzeln auflisten)?

3. Auf welchen gesetzlichen, vertraglichen oder vertragsähnlichen Grundlagen basierten die in Frage 1 erfragten Kooperationen unter Beteiligung des BSI im Einzelnen jeweils?

4. Wurden bei den in Frage 1 erfragten Kooperationen zwischen den beteiligten Stellen Daten aus oder von in Deutschland befindlichen bzw. genutzten IT-Systemen ausgetauscht, und wenn ja, zwischen welchen Stellen welche Daten in welcher Größenordnung?

5. Wurden bei den in Frage 1 erfragten Kooperationen Betreiber und/oder Nutzer der betroffenen in Deutschland befindlichen bzw. genutzten IT-Systeme informiert (bitte einzeln auflisten Art, Umfang und der Adressat Informationen)?

6. Welche die Aufsicht führenden bzw. für die Kontrolle zuständigen Bundesministerien, Gremien oder Behörden wurden wann und wie über die in Frage 1 erfragten Kooperationen informiert (bitte einzeln auflisten, ob Informationen vor oder nach Beginn oder nach Abschluss der Kooperation erfolgten)?

Die Fragen 2 bis 6 werden gemeinsam beantwortet.

Auf die Antwort zu Frage 1 wird verwiesen.

7. Wie viele Kooperationen hat das BSI seit 2015 mit ausländischen Sicherheitsbehörden oder Nachrichtendiensten anlässlich bevorstehender oder erwarteter Angriffe auf in Deutschland befindliche IT-Systeme durchgeführt oder begonnen?

Das BSI hat speziell anlässlich bevorstehender oder erwarteter Angriffe auf in Deutschland befindliche IT-Systeme seit dem Jahr 2015 keine Kooperationen mit ausländischen Sicherheitsbehörden oder Nachrichtendiensten durchgeführt oder begonnen. Wegen der Zusammenarbeit im Allgemeinen wird auf die Vorbemerkung sowie auf die Antwort zu den Fragen 19 und 20 verwiesen.

8. Welche deutschen und ausländischen Behörden waren an den in Frage 7 erfragten Kooperationen beteiligt?

9. Auf welchen gesetzlichen, vertraglichen oder vertragsähnlichen Grundlagen basierten die in Frage 7 erfragten Kooperationen unter Beteiligung des BSI im Einzelnen jeweils?

10. Wurden bei den in Frage 7 erfragten Kooperationen zwischen den beteiligten Stellen Daten aus oder von in Deutschland befindlichen IT-Systemen ausgetauscht, und wenn ja, zwischen welchen Stellen welche Daten in welcher Größenordnung?

11. Wurden bei den in Frage 7 erfragten Kooperationen Betreiber und/oder Nutzer der betroffenen in Deutschland befindlichen bzw. genutzten IT-Systeme informiert (bitte Art, Umfang und der Adressat Informationen einzeln auflisten)?

12. Welche die Aufsicht führenden bzw. für die Kontrolle zuständigen Bundesministerien, Gremien oder Behörden wurden wann und wie über die in Frage 7 erfragten Kooperationen informiert (bitte einzeln auflisten, ob Informationen vor oder nach Beginn oder nach Abschluss der Kooperation erfolgten)?

Die Fragen 8 bis 12 werden gemeinsam beantwortet.

Auf die Antwort zu Frage 7 wird verwiesen.

13. In wie vielen Fällen hat sich das BSI seit 2015 mit welchen deutschen Stellen hinsichtlich Informationen über potentiell für Maßnahmen der Telekommunikationsüberwachung (bspw. Quellen-TKÜ, Onlinedurchsuchung, Einrichtung von pseudonymen Accounts) nutzbare Schwachstellen und Exploits (Zero-Day-Exploits) ausgetauscht?

Das BSI hat sich seit dem Jahr 2015 in vier Fällen mit deutschen Stellen zu Schwachstellen ausgetauscht. Der Austausch erfolgte mit Sicherheitsforschern, Hochschulen und Unternehmen.

Ein Austausch mit staatlichen Stellen fand nicht statt. Der Austausch fand ausschließlich im Rahmen eines „Coordinated Vulnerability Disclosure“ (CVD) Prozesses statt. Ziel eines solchen Austausches ist es, die Hersteller der von den Schwachstellen betroffenen Produkte geeignet zu informieren, damit diese die Schwachstellen beheben können, bevor sie öffentlich werden.

14. In wie vielen Fällen hat sich das BSI seit 2015 mit welchen europäischen Stellen hinsichtlich Informationen über potentiell für Maßnahmen der Telekommunikationsüberwachung (bspw. Quellen-TKÜ, Onlinedurchsuchung, Einrichtung von pseudonymen Accounts) nutzbare Schwachstellen und Exploits (Zero-Day-Exploits) ausgetauscht?

15. In wie vielen Fällen hat sich das BSI seit 2015 mit welchen außereuropäischen Sicherheitsbehörden oder Nachrichtendiensten hinsichtlich Informationen über potentiell für Maßnahmen der Telekommunikationsüberwachung (bspw. Quellen-TKÜ, Onlinedurchsuchung, Einrichtung von pseudonymen Accounts) nutzbare Schwachstellen und Exploits (Zero-Day-Exploits) ausgetauscht?

Die Fragen 14 und 15 werden gemeinsam beantwortet.

In keinem Fall.

16. In wie vielen Fällen hat sich das BSI seit 2015 mit welchen Betreibern von IT-Netzwerken, Telekommunikationsdiensten, sozialen Netzwerken, Onlineplattformen oder Messengerdiensten hinsichtlich Informationen über potentiell sowohl für Maßnahmen der Telekommunikationsüberwachung (bspw. Quellen-TKÜ, Onlinedurchsuchung, Einrichtung von pseudonymen Accounts) aber auch für sogenannte Hackerangriffe nutzbare Schwachstellen und Exploits (Zero-Day-Exploits) ausgetauscht?

Das BSI hat sich in keinem Fall mit Telekommunikations- und Telemedienanbietern zu Maßnahmen für Telekommunikationsüberwachung (bspw. Quellen-TKÜ, Onlinedurchsuchungen etc.) ausgetauscht.

Das BSI hat sich aber mit verschiedenen relevanten Telekommunikations- und Telemedienanbietern hinsichtlich Informationen über für sogenannte „Hackingangriffe“ nutzbare Schwachstellen ausgetauscht. Schwerpunkte seit dem Jahr 2015 waren hierbei die Bekämpfung von Botnetzen und DDoS-Angriffen (Distributed-Denial-of-Service).

Die Ergebnisse wurden in einer Vielzahl von Veröffentlichungen transparent dargestellt, so z. B. in einer öffentlich verfügbaren Publikation der Allianz für Cybersicherheit (www.allianz-fuer-cybersicherheit.de/.../Partnerbeitrag_ISPs_Gefaehrdungsmatrix_2016.html).

17. In wie vielen Fällen hat sich das BSI seit 2015 mit welchen Betreibern von IT-Netzwerken von Stellen des Bundes und der Länder hinsichtlich Informationen über potentiell sowohl für Maßnahmen der Telekommunikationsüberwachung (bspw. Quellen-TKÜ, Onlinedurchsuchung, Einrichtung von pseudonymen Accounts) aber auch für sogenannte Hackerangriffe nutzbare Schwachstellen und Exploits (Zero-Day-Exploits) ausgetauscht?

In keinem Fall.

18. In wie vielen Fällen hat das BSI seit 2015 welchen Betreibern von IT-Netzwerken von Stellen des Bundes und der Länder über potentiell sowohl für Maßnahmen der Telekommunikationsüberwachung (bspw. Quellen-TKÜ, Onlinedurchsuchung, Einrichtung von pseudonymen Accounts) aber auch für sogenannte Hackerangriffe nutzbare Schwachstellen und Exploits (Zero-Day-Exploits) gewarnt und auf Maßnahmen gegen jene hingewirkt?

Das BSI hat seit dem Jahr 2015 die Betreiber von IT-Netzwerken von Stellen des Bundes und der Länder vor einer Vielzahl von Schwachstellen gewarnt.

Das BSI stellt allen Stellen des Bundes, den Landesverwaltungen, den kritischen Infrastrukturen aber auch allen anderen Unternehmen sowie Bürgerinnen und Bürgern den Warn & Informationsdienst (WID) (www.cert-bund.de/) zur Verfügung. Über den WID werden Informationen zu neuen Schwachstellen und Sicherheitslücken sowie aktuellen Bedrohungen für IT-Systeme publiziert.

Das BSI hat im angefragten Zeitraum die folgende Anzahl an Schwachstellen-Meldungen (Advisories) herausgegeben:

- 2015: 729
- 2016: 861
- 2017: 788
- 2018: 226

(Stand: 19. Juni 2018).

Daneben informiert das BSI auch mit „Cyber-Sicherheitswarnungen“ die Stellen der Bundes- und Landesverwaltungen über besonders relevante Schwachstellen und Gefährdungen. Diese Meldungen gehen an alle durch die Bundes-Ressorts gemeldeten IT-Sicherheitskontakte sowie an die Computer Emergency Response Teams (CERTs) der Landesverwaltungen im VerwaltungsCERT-Verbund (VCV). Das BSI hat im angefragten Zeitraum die folgende Anzahl an Cyber-Sicherheitswarnungen herausgegeben:

- 2015: 44
- 2016: 51
- 2017: 57
- 2018: 25

(Stand: 19. Juni 2018).

19. Haben Mitarbeiter ausländischer Sicherheitsbehörden oder Nachrichtendienste seit 2015 mit dem BSI in Deutschland zusammengearbeitet, und wenn ja,

a) jeweils zu welchem Zeitpunkt oder in welchem Zeitraum,

b) Mitarbeiter von welchen ausländischen Sicherheitsbehörden oder Nachrichtendiensten,

c) jeweils aus welchem Anlass, zu welchem Zweck und in welcher Weise,

d) auf welcher rechtlichen Basis?

Eine entsprechende Zusammenarbeit in Deutschland fand nicht statt.

20. Haben Mitarbeiter des BSI seit 2015 mit ausländischen Sicherheitsbehörden oder Nachrichtendienste außerhalb Deutschlands zusammengearbeitet, und wenn ja,

a) jeweils zu welchem Zeitpunkt oder in welchem Zeitraum,

b) mit welchen ausländischen Sicherheitsbehörden oder Nachrichtendiensten,

c) jeweils aus welchem Anlass, zu welchem Zweck und in welcher Weise,

d) auf welcher rechtlichen Basis?

Gemäß seiner gesetzlichen Aufgaben arbeitet das BSI kontinuierlich im internationalen Rahmen jeweils mit den Behörden zusammen, denen vergleichbare Aufgaben im Bereich der IT- und Cybersicherheit in Partnerländern zugewiesen sind (siehe Vorbemerkung der Bundesregierung).

Im Wesentlichen findet dies im Kontext und an den Standorten von Europäischer Union und NATO statt. Zweck dieser Zusammenarbeit ist vor allem:

- Erarbeitung gemeinsamer Regelwerke zu Aspekten der Cybersicherheit, Schutz der Kommunikationsverbindungen oder Interoperabilität.
- Austausch zu Mindestanforderungen für IT-Sicherheit und Möglichkeiten zur Abwehr von Cyberangriffen.
- Planung, Teilnahme und Nachbereitung von und an Übungen zum Themenkomplex IT-Sicherheit oder IT-Krisenmanagement.

Die rechtliche Grundlage ergibt sich dabei aus § 3 Absatz 1 Satz 2 Nummer 16 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG).

Weiterhin hat das BSI bei der Bewältigung eines IT-Sicherheitsvorfalls im Ausland unterstützt. Zu den weiteren Inhalten dieser Antwort wird gemäß Vorbemerkung der Bundesregierung auf den „VS – Vertraulich“ eingestuften Antwortteil verwiesen.*

* Das Bundesministerium des Innern, für Bau und Heimat hat einen Teil der Antwort zu Frage 20 als „VS – Vertraulich“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

21. In welcher Art und Weise hat das BSI die Zertifizierungsverfahren für die zur Quellen-TKÜ und Onlinedurchsuchung beschafften bzw. programmierten Programme begleitet (bitte einzeln für die jeweiligen Programme auflisten)?

Eine Zertifizierung von Software zur Durchführung von Maßnahmen der Quellen-TKÜ oder der Onlinedurchsuchung ist gesetzlich nicht vorgesehen und wurde nicht durchgeführt.

Das BSI hat vom Bundeskriminalamt (BKA) die Ergebnisse der Überprüfungen einer vom BKA entwickelten Quellen-TKÜ-Software und einer kommerziellen Quellen-TKÜ-Software mitgeteilt bekommen.

22. In welcher Weise war das BSI ggf. daran beteiligt, für von Bundesbehörden beschaffte oder erstellte Programme Vorkehrungen und technische Vorgaben zu entwickeln bzw. zu implementieren bzw. ihre Umsetzung zu prüfen, welche sicherstellen sollen, dass

    a) ausschließlich die laufende Telekommunikation überwacht und aufgezeichnet werden kann (§ 100a Absatz 5 Satz 1 Nummer 1a der Strafprozessordnung – StPO) oder dass ausschließlich gespeicherte Inhalte und Umstände der Kommunikation, die ab der TKÜ-Anordnung während des laufenden Übertragungsvorgangs hätten überwacht und aufgezeichnet werden dürfen, überwacht und aufgezeichnet werden können (§ 100a Absatz 5 Satz 1 Nummer 1b StPO) und die Quellen-TKÜ nicht zu einem Vollzugriff auf Inhalte und Ressourcen des Zielsystems führt und damit faktisch eine rechtswidrige Onlinedurchsuchung bedeutet;

    b) am Zielsystem nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind (§ 100a Absatz 5 Satz 1 Nummer 2 StPO) und die vorgenommenen Veränderungen am Zielsystem, soweit technisch möglich, automatisch rückgängig gemacht werden (§ 100a Absatz 5 Satz 1 Nummer 3 StPO)

    (bitte für die einzelnen Programme jeweils auflisten)?

23. In welcher Weise war das BSI ggf. daran beteiligt, für von Bundesbehörden beschaffte oder erstellte Programme Vorkehrungen und technische Vorgaben zu entwickeln bzw. zu implementieren bzw. ihre Umsetzung zu prüfen, welche sicherstellen sollen, dass

    a) – soweit möglich – technisch sichergestellt ist, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden (§ 100d Absatz 3 Satz 1 StPO),

    b) technisch sichergestellt ist, dass am Zielsystem nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind (§ 100b Absatz 4 i. V. m § 100a Absatz 5 Satz 1 Nummer 2 StPO),

    c) die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisch rückgängig gemacht werden (§ 100b Absatz 4 i. V. m. § 100a Absatz 5 Satz 1 Nummer 3 StPO), und

    d) die Spähsoftware („das eingesetzte Mittel“ in der Terminologie der StPO) nach dem Stand der Technik gegen unbefugte Nutzung geschützt ist (§ 100b i. V. m. § 100a Absatz 5 Satz 2 StPO)?

Die Fragen 22 und 23 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Im Jahr 2012 war das BSI bei der Erstellung der „Standardisierenden Leistungsbeschreibung“ (SLB) für Software zur Durchführung von Maßnahmen der Quellen-TKÜ hinsichtlich kryptographischer Aspekte und IT-Sicherheitsaspekten beteiligt.

24. Welche Kosten sind anlässlich der Entwicklung von Programmen oder Tools für Quellen-TKÜ und Onlinedurchsuchung jeweils für die Einzelpositionen Lizenzkosten, Wartung und Betreuung sowie Entwicklung entstanden (bitte jeweils für die einzelnen entwickelten oder beschafften Programme und Tools sowie nach Jahren auflisten)?

Das BSI hat selbst keine Software im Sinne der Fragestellung entwickelt, daher sind diesbezüglich keine Kosten entstanden.

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