Deutscher Bundestag **Drucksache 19/2774**

19. Wahlperiode 15.06.2018

Kleine Anfrage

der Abgeordneten Martina Renner, Dr. André Hahn, Gökay Akbulut, Christine Buchholz, Anke Domscheit-Berg, Heike Hänsel, Andrej Hunko, Ulla Jelpke, Amira Mohamed Ali, Niema Movassat, Thomas Nord, Dr. Petra Sitte, Helin Evrim Sommer, Kersten Steinke, Friedrich Straetmanns, Dr. Kirsten Tackmann und der Fraktion DIE LINKE.

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

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).

Wir fragen die Bundesregierung:

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?
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)?
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?
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)?
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?
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?

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?

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?

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?

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?

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?

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)?

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)?

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)?

Berlin, den 11. Juni 2018

Dr. Sahra Wagenknecht, Dr. Dietmar Bartsch 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