Deutscher Bundestag **Drucksache 19/2307**

19. Wahlperiode 24.05.2018

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Stephan Thomae, Jimmy Schulz, Manuel Höferlin, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 19/2009 –

Cybersicherheit

Vorbemerkung der Fragesteller

Beim „NotPetya"-Virus handelte es sich um einen Cyber-Angriff, der im Juni 2017 weltweit, darunter auch in Deutschland, für Schäden in Milliardenhöhe sorgte. Der Virus hatte zunächst Rechner in der Ukraine befallen, ehe er sich auf die Geschäftspartner ukrainischer Firmen im europäischen, amerikanischen und asiatischen Ausland ausweitete. Zu den Opfern sollen unter anderem der Pharmakonzern Merck, der Konsumgüterkonzern Beiersdorf, die dänische Reederei A.P. Moller-Maersk und das Logistikunternehmen TNT sowie FedEX gehört haben. Die US-Regierung schätzt den weltweiten Schaden von „NotPetya" auf mehr als 10 Mrd. Dollar. Vor der Bundestagswahl 2017 warnte die Bundesregierung, dass russische Geheimdienste „versuchen könnten, die Bundestagswahl 2017 durch Cyber-Angriffe zu beeinflussen". Die Bundesregierung schreibt Russland die Cyber-Angriffe auf den Deutschen Bundestag im Frühjahr 2015 sowie auf politische Parteien im April, Mai und August 2016 zu.

Vorbemerkung der Bundesregierung

1. Die Beantwortung der Fragen 1, 2, 3 und 15 kann aus Gründen des Staatswohls nicht in offener Form erfolgen. Die unbefugte Kenntnisnahme von Einzelheiten zu Aufklärungserkenntnissen der Nachrichtendienste des Bundes könnte sich nachteilig auf die Interessen der Bundesrepublik Deutschland auswirken. Aus ihrem Bekanntwerden können Rückschlüsse auf die Arbeitsweise und Methode der Nachrichtendienste des Bundes gezogen werden, die nach der Rechtsprechung des Bundesverfassungsgerichts besonders schutzbedürftig sind (BVerfGE 124, 161 (194). Hierdurch würde die Funktionsfähigkeit der Sicherheitsbehörden beeinträchtigt, was wiederum die Sicherheit der Bundesrepublik Deutschland gefährdet. Diese Informationen werden daher als Verschlusssache gemäß der Allgemeinen Verwaltungsvorschrift des Bundesministerium des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA) mit dem VS-Grad „Nur für den Dienstgebrauch" eingestuft und dem Deutschen Bundestag gesondert übermittelt.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 18. Mai 2018 übermittelt.

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

2. Die Beantwortung der Frage 7 kann nicht in offener Form erfolgen. Der Schutz vor allem der technischen Fähigkeiten der Bundesbehörden stellt für die Aufgabenerfüllung der Bundesbehörden einen überragend wichtigen Grundsatz dar. Er dient der Aufrechterhaltung der Effektivität der Informationsbeschaffung und -sicherung durch den Einsatz spezifischer Fähigkeiten und damit dem Staatswohl. Hier sind Erkenntnisse über Analysefähigkeiten von Sicherheitsvorfällen und Maßnahmen zur Sicherung von IT-Systemen betroffen. Eine Veröffentlichung von Einzelheiten betreffend solche Fähigkeiten würde zu einer wesentlichen Schwächung der den Behörden zur Absicherung der IT-Systeme und zur Reaktion auf Angriffe zur Verfügung stehenden Möglichkeiten führen. Dies würde für ihre Auftragserfüllung erhebliche Nachteile zur Folge haben und für die Interessen der Bundesrepublik Deutschland schädlich sein. Die Schutzmaßnahmen dienen der Aufrechterhaltung der Sicherheit und Funktionsfähigkeit des IVBBs und damit dem Staatswohl. Daher ist die Antwort zu Frage 7 als Verschlusssache nach § 4 Absatz 2 des Sicherheitsüberprüfungsgesetzes in Verbindung mit der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA) mit dem Geheimhaltungsgrad „VS – Nur für den Dienstgebrauch“ eingestuft.*

1. Liegen der Bundesregierung Erkenntnisse vor, wer hinter dem Cyber-Angriff „NotPetya“ steckt?

Die Antwort auf diese Frage ist als Verschlusssache mit dem VS-Grad „VS – Nur für den Dienstgebrauch“ eingestuft und wird dem Deutschen Bundestag gesondert übermittelt. Zur Begründung wird auf die Vorbemerkung der Bundesregierung Nummer 1 verwiesen.*

2. Hält die Bundesregierung die Zuschreibung der Länder USA, Großbritannien, Kanada, Neuseeland und Dänemark, Russland sei verantwortlich, für plausibel (vgl. www.reuters.com/article/us-britain-russia-cyber-usa/white-house-blames-russia-for-reckless-notpetya-cyber-attack-idUSKCN1FZ2UJ; www.dw.com/en/uk-us-blame-russia-for-notpetya-cyberattack/a-42598806)?

   Wenn ja, welche Gründe sprechen aus Sicht der Bundesregierung dafür?

   Wenn nicht, welche Gründe sprechen aus Sicht der Bundesregierung dagegen?

Die Antwort auf diese Frage ist als Verschlusssache mit dem VS-Grad „VS – Nur für den Dienstgebrauch“ eingestuft und wird dem Deutschen Bundestag gesondert übermittelt. Zur Begründung wird auf die Vorbemerkung der Bundesregierung Nummer 1 verwiesen.

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

3. Haben die genannten Staaten ihre Erkenntnisse mit deutschen Nachrichtendiensten geteilt?

   Wenn ja, waren diese überzeugend?

   Welche Gründe gab es, sich der öffentlichen Verurteilung Russlands nicht anzuschließen?

Die Antwort auf diese Frage ist als Verschlusssache mit dem VS-Grad „VS – Nur für den Dienstgebrauch“ eingestuft und wird dem Deutschen Bundestag gesondert übermittelt. Zur Begründung wird auf die Vorbemerkung der Bundesregierung Nummer 1 verwiesen.

4. Weshalb hat die Bundesregierung im Fall des Cyber-Angriffs auf das Auswärtige Amt, der Anfang März 2018 bekannt wurde, nicht gezögert, Russland verantwortlich zu machen – und unter anderem auch die Ausweisung russischer Diplomaten damit begründet (vgl. www.bundesregierung.de/Content/DE/Interview/2018/04/2018-04-16-maas-spiegel.html)?

   Welche Erkenntnisse ließen den Schluss zu, Russland sei verantwortlich?

Nach bisherigen Erkenntnissen lässt sich die Cyberoperation gegen das geschützte IT-System der Bundesregierung mit hoher Wahrscheinlichkeit russischen Quellen zurechnen (vgl. auch Pressemitteilung des Auswärtigen Amts vom 26. März 2018).

Zur zweiten Teilfrage wird auf die Antwort der Bundesregierung zu Frage 12 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 19/1867 sowie die Antwort der Bundesregierung auf die Schriftliche Frage 24 des Abgeordneten Andrej Hunko auf Bundestagsdrucksache 19/1979 verwiesen.

5. Liegen der Bundesregierung Zahlen vor, die den durch „NotPetya“ entstandenen Schaden in Deutschland beziffern?

Der Bundesregierung liegen hierzu keine Erkenntnisse vor.

6. Konnten die deutschen Sicherheitsbehörden vor der Bundestagswahl 2017 Versuche russischer Geheimdienste, die Bundestagswahl durch Cyber-Angriffe zu beeinflussen, feststellen (vor der Bundestagswahl 2017 warnte die Bundesregierung, dass russische Geheimdienste „versuchen könnten, die Bundestagswahl 2017 durch Cyber-Angriffe zu beeinflussen“)?

Eine Beeinflussung der Bundestagswahl 2017 wurde nicht festgestellt.

7. Welche Maßnahmen wurden im Anschluss an den erfolgreichen Hacker-Angriff auf das Netz der Bundesregierung ergriffen, der Anfang März 2018 bekannt wurde, um das Netz der Bundesregierung wirksamer vor Cyber-Angriffen zu schützen und einen weiteren erfolgreichen Angriff zu verhindern?

Die Antwort auf diese Frage ist als Verschlusssache mit dem VS-Grad „VS – Nur für den Dienstgebrauch“ eingestuft und wird dem Deutschen Bundestag gesondert übermittelt. Zur Begründung wird auf die Vorbemerkung der Bundesregierung Nummer 2 verwiesen.

8. In welchen Abständen erhalten Mitarbeiter der Bundesministerien, der zugehörigen Behörden und Einrichtungen, Schulungen in IT-Sicherheit?

   Was ist der Inhalt dieser Schulungen, und wie hoch ist der Anteil der Mitarbeiter, die Schulungen in IT-Sicherheit bekommen?

Auf die Antwort der Bundesregierung auf die Schriftliche Frage 16 der Abgeordneten Dr. Anna Christmann auf Bundestagsdrucksache 19/1241 und auf die Schriftliche Frage 10 auf Bundestagsdrucksache 19/1470 wird verwiesen.

9. Wie ist die Position der Bundesregierung zu den Vorschlägen, das Bundesamt für Sicherheit in der Informationstechnik (BSI) aus dem BMI herauszulösen (vgl. www.handelsblatt.com/my/politik/deutschland/it-sicherheit-warum-der-bundestag-ein-leichtes-ziel-fuer-hacker-ist/21139900.html?ticket=ST-1750805-xH0rEmd9hz7E1fFdeSXn-ap3)?

Die Bundesregierung verfolgt keine Pläne, das Bundesamt für Sicherheit in der Informationstechnik (BSI) aus dem Geschäftsbereich des Bundesministeriums des Innern herauszulösen. Die Beibehaltung der bisherigen organisatorischen Struktur des BSI ist im Interesse einer effizienten Steuerung und Koordination der Zusammenarbeit mit anderen Sicherheitsbehörden zur Gewährleistung von Cyber-Sicherheit geboten. Darüber hinaus ist insbesondere eine organisatorische Stärkung des BSI zur Verbesserung der Cyber-Sicherheit der öffentlichen Verwaltung wie auch der Wirtschaft und Bürger geboten.

10. Ist die Attribution des jüngsten erfolgreichen Hackerangriffes auf das Netz der Bundesregierung, der Anfang März 2018 bekannt wurde, abgeschlossen?

    Wenn ja, wie ist das Ergebnis?

Die Untersuchungen zur Cyberoperation gegen das Auswärtige Amt (AA) sind noch nicht abgeschlossen. Im Übrigen wird auf die Antwort zu Frage 4 verwiesen.

11. Welche Hackerangriffe, neben den bekannten aus den Jahren 2015 auf den Deutschen Bundestag und 2016 auf politische Parteien, auf deutsche Ziele – etwa Behörden, Unternehmen, Infrastruktur, Forschungseinrichtungen – weisen auf Täter im Dienst des russischen Staats hin?

Neben den genannten Zielen waren seitdem auch weiterhin politische Strukturen wie Parteien und Stiftungen von Cyberoperationen mutmaßlich staatlicher russischer Stellen betroffen. Darüber hinaus gehören Regierungseinrichtungen und Behörden, Nichtregierungsorganisationen (NGOs), Think Tanks und Wirtschaftsunternehmen zu den Angriffszielen.

12. Wie viele Cyber-Angriffe aus den Jahren 2014 bis 2018 konnten attribuiert werden (bitte nach Jahren – 2014, 2015, 2016, 2017, 2018 – und Herkunftsländern aufschlüsseln)?

Die Attribution von Cyberoperationen, insbesondere zu staatlichen Akteuren mit entsprechenden professionellen und profunden IT-Fähigkeiten, ist grundsätzlich mit einer Unschärfe verbunden. Dabei erfolgt die Attribution von Cyberoperationen zu staatlichen Akteuren mit unterschiedlich hoher Wahrscheinlichkeit. Eine zweifelsfreie Zuordnung insbesondere zu Herkunftsländern des Akteurs kann daher in der Regel nicht getroffen werden.

13. Für welche der in Frage 12 genannten Cyber-Angriffe sind nach Einschätzung der Bundesregierung ausländische Nachrichtendienste verantwortlich?

14. Für welche der in Frage 12 genannten Cyber-Angriffe sind nach Einschätzung der Bundesregierung Extremisten bzw. Terrorgruppen oder weitere kriminelle Netzwerke verantwortlich?

Die Fragen 13 und 14 werden gemeinsam beantwortet.

Auf die Antwort zu Frage 12 wird verwiesen.

15. Wie schätzt die Bundesregierung die russische Cyber-Strategie ein?

Welche Ziele verfolgen russische Nachrichtendienste mit ihren Hacker- und Desinformationskampagnen?

Die Antwort auf diese Frage ist als Verschlusssache mit dem VS-Grad „VS – Nur für den Dienstgebrauch“ eingestuft und wird dem Deutschen Bundestag gesondert übermittelt. Zur Begründung wird auf die Vorbemerkung verwiesen.

16. Stimmt die Bundesregierung der Einschätzung der USA zu, dass Cyber-Angriffe gegenwärtig das drängendste Sicherheitsproblem seien (vgl. www.defense.gov/News/Article/Article/1440838/cyber-tops-list-of-threats-to-us-director-of-national-intelligence-says/)?

Die Bundesregierung trifft keine Bewertung sicherheitspolitischer Lageeinschätzungen anderer Staaten.

Die Cyberbedrohungslage wird sehr ernst genommen. Die Bundesregierung hat deshalb bereits umfassende Maßnahmen zum Ausbau von Cybersicherheitsmaßnahmen und zur Stärkung der IT-Sicherheit in Deutschland umgesetzt.

17. Wie weit sind die Überlegungen der Bundesregierung vorangeschritten, die deutsche Spionageabwehr, wie vom Verfassungsschutzpräsidenten gefordert, mit „Gegenangriffen auf Cyber-Attacken“ reagieren zu lassen?

Sind die schon im vergangenen Jahr laufenden technischen Prüfungen inzwischen abgeschlossen?

Die Bundesregierung prüft derzeit noch die rechtlichen und technischen Möglichkeiten einer aktiven Cyberabwehr.

18. Setzt sich die Bundesregierung für die Ächtung bestimmter, wahllos wirkender Cyber-Waffen ein?

Wäre dafür ein internationales Abkommen sinnvoll oder erforderlich?

Ist das Chemiewaffenabkommen von 1997 ein Vorbild?

Wenn ja, wie kommen die Gespräche mit anderen Staaten voran?

In welchem Rahmen werden sie geführt?

Die Bundesregierung verwendet den Begriff „Cyber-Waffen“, für den keine anerkannte Definition existiert, nicht. Wir verstehen die Fragesteller so, dass sie sich auf Cyber-Wirkmittel beziehen, die im Rahmen eines bewaffneten Konflikts als militärisches Mittel zum Einsatz kämen und deren Anwendung unter das humanitäre Völkerrecht fiele. Das humanitäre Völkerrecht verbietet den Einsatz unterschiedslos wirkender militärischer Mittel, bei denen nicht zwischen zivilen Objekten und militärischen Zielen unterschieden werden kann; dies gilt auch für

Wirkmittel im Cyberraum. Eine völkerrechtliche Ächtung unterschiedslos wirkender Cyber-Wirkmittel ist daher bereits international anerkannt und geltendes Recht.

19. Wie hat sich die von der Bundesregierung am 9. November 2016 vorgelegte Cyber-Sicherheitsstrategie für Deutschland seither fortentwickelt, gerade auch mit Blick auf Fake-News-Kampagnen in Onlinenetzwerken, die den amerikanischen Wahlkampf stark geprägt haben?

„Fake-News“ sind kein Thema der Cybersicherheit. Informationstechnik wird lediglich als Mittel zur Verbreitung eingesetzt. Die Bundesregierung prüft derzeit – auch im Rahmen der europäischen Zusammenarbeit – geeignete Maßnahmen, um auf bewusst herbeigeführte „Fake-News“-Kampagnen zu reagieren.

20. Behält sich die Bundesregierung vor, auf Cyber-Angriffe auch militärisch (konventionell und/oder digital) zu reagieren?

Welche militärischen Gegenmaßnahmen (konventionell und/oder digital) stehen zur Disposition?

Wie glaubwürdig ist diese Form der asymmetrischen Abschreckung aus Sicht der Bundesregierung?

Im Falle eines bewaffneten Angriffs steht dem angegriffenen Staat das Recht auf Selbstverteidigung zu. Auch eine Cyberoperation kann unter bestimmten Bedingungen einen „bewaffneten Angriff“ im Sinne von Artikel 51 VN-Charta darstellen. Hierauf könnte die Bundesrepublik Deutschland mit allen zulässigen militärischen Mitteln reagieren.

Bei Cyberoperationen, die unterhalb der Schwelle des „bewaffneten Angriffs“ verbleiben, aber das Völkerrecht verletzen, erlaubt das Völkerrecht das Ergreifen von Gegenmaßnahmen. Generell sind auf völkerrechtswidrige Aktivitäten gegen die Bundesrepublik Deutschland Reaktionen innerhalb des völker- und verfassungsrechtlich gesteckten Rahmens möglich. Die Wahl der geeigneten Mittel ist vom jeweiligen Einzelfall abhängig. Als eine mögliche Option kann auch der Einsatz der Bundeswehr im Rahmen des verfassungsrechtlichen Auftrages in Betracht gezogen werden. Das Abschreckungspotential liegt in den im Rahmen des verfassungsgemäßen Auftrages der Bundeswehr vorgehaltenen Mitteln.

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