Deutscher Bundestag **Drucksache 19/2009**

19. Wahlperiode 04.05.2018

Kleine Anfrage

der Abgeordneten Stephan Thomae, Jimmy Schulz, Manuel Höferlin, Grigorios Aggelidis, Renata Alt, Christine Aschenberg-Dugnus, Jens Beeck, Nicola Beer, Dr. Jens Brandenburg (Rhein-Neckar), Mario Brandenburg, Hartmut Ebbing, Dr. Marcus Faber, Otto Fricke, Thomas Hacker, Katrin Helling-Plahr, Markus Herbrand, Katja Hessel, Reinhard Houben, Ulla Ihnen, Olaf in der Beek, Gyde Jensen, Thomas L. Kemmerich, Katharina Kloke, Daniela Kluckert, Pascal Kober, Dr. Lukas Köhler, Wolfgang Kubicki, Konstantin Kuhle, Alexander Kulitz, Ulrich Lechte, Michael Georg Link, Till Mansmann, Alexander Müller, Roman Müller-Böhm, Dr. Martin Neumann, Christian Sauter, Frank Schäffler, Matthias Seestern-Pauly, Frank Sitta, Judith Skudelny, Bettina Stark-Watzinger, Dr. Marie-Agnes Strack-Zimmermann, Benjamin Strasser, Katja Suding, Linda Teuteberg, Michael Theurer, Manfred Todtenhausen, Dr. Andrew Ullmann, Gerald Ullrich, Johannes Vogel (Olpe) und der Fraktion der FDP

Cybersicherheit

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.

Wir fragen die Bundesregierung:

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

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?

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?

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?

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

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“)?

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?

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?

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)?

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?

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?

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)?

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

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

Berlin, den 24. April 2018

Christian Lindner 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