Deutscher Bundestag **Drucksache 19/2297**

19. Wahlperiode 24.05.2018

Kleine Anfrage

der Abgeordneten Andrej Hunko, Christine Buchholz, Heike Hänsel, Zaklin Nastic, Dr. Alexander S. Neu, Alexander Ulrich und der Fraktion DIE LINKE.

Unklare Faktenlage zum sogenannten „Bundeshack“

Es ist weiterhin unklar, wer für den sogenannten „Bundeshack“ auf den Informationsverbund Berlin-Bonn (IVBB) verantwortlich ist (Quelle hier und im Folgenden: Bundestagsdrucksache 19/1867). Zwar ermitteln hierzu das Bundesamt für Sicherheit in der Informationstechnik (BSI) und das für Spionageabwehr zuständige Bundesamt für Verfassungsschutz (BfV), auch der Auslandsgeheimdienst Bundesnachrichtendienst (BND) ist eingebunden. Jedoch habe das Bundesministerium des Inneren, für Bau und Heimat (BMI) nur „Indizien“, dass die in Russland verorteten Netzwerke „APT28“ oder „Snake“ etwas mit dem Sicherheitsvorfall zu tun haben könnten. Laut dem Bundesinnenministerium sprächen die bei früheren Angriffen genutzten Infrastrukturen, ein nicht näher bezeichneter „Modus Operandi“, technische Merkmale sowie die Ziele „mit hoher Wahrscheinlichkeit“ für einen Angriff von „APT 28“ oder „Snake“. Als „Hinweis“ für die Urheberschaft gilt demnach auch ein Datendiebstahl bei den US-amerikanischen Präsidentschaftswahlen.

Nach Medienberichten deutet etwa eine genutzte kyrillische Tastatur oder ein Zeitstempel als Indiz, dass die russische Regierung involviert sei („Hacker mit Stil“, www.faz.de vom 2. Mai 2018). Diese Spuren könnten aber leicht manipuliert worden sein. Das gelte auch für IP-Adressen der Server, von denen aus Schadsoftware eingeschleust wird. Schließlich ist bisher noch kein zusammenhängender Code der Schadsoftware aus dem Angriff bekannt, obwohl danach „intensiv gesucht“ wird. Die deutschen Ermittlungsbehörden hätten sich deshalb Hilfe beim US-Geheimdienst National Security Agency (NSA) gesucht, der eine Datenbank mit „Stilproben von Programmierern“ führt.

Der beim „Bundeshack“ genutzte Trojaner „Turla“ bzw. „Uroburos“ ist dem BSI seit Jahren bekannt. Das könnte aus Sicht der Fragestellerinnen und Fragesteller bedeuten, dass das Regierungsnetz also entsprechend gesichert war und der Angriff in Ruhe beobachtet werden konnte. Das wirft die Frage auf, warum das Parlamentarische Kontrollgremium erst nach dem öffentlichen Bekanntwerden des Angriffs unterrichtet wurde. Laut dem BMI hat es hierzu Meinungsverschiedenheiten in der „interne[n] Willensbildung der Bundesregierung zum Umgang mit dem laufenden Angriff“ gegeben, die dazu geführt haben, dass das Parlamentarische Kontrollgremium erst durch Medienberichte von dem Angriff erfuhr.

Die in der Antwort benannten Meinungsverschiedenheiten innerhalb der Bundesregierung dürfen aus Sicht der Fragestellerinnen und Fragesteller nicht dazu führen, die parlamentarische Kontrolle auszuhöhlen. Die Bundesregierung muss wie in den Jahren 2016 und 2017 auch im Jahr 2018 ressortübergreifende Cybersicherheitskonsultationen mit Russland durchführen. Noch besser wäre es, mit russischen Behörden im Bereich der Cybersicherheit oder der Abwehr von IT-Angriffen in technischen, operativen und strategischen Fragen zusammenzuarbeiten.

Wir fragen die Bundesregierung:

1. Welche „diverse[n] Werkzeuge“ wurden bei dem „Bundeshack“ genutzt, „die größtenteils speziell für diesen Angriff angefertigt worden sein dürften“ (Antwort zu Frage 5b auf Bundestagsdrucksache 19/1867)?
2. Inwiefern kann sich die Bundesregierung mittlerweile auf eine Urheberschaft eines der in Russland verorteten Netzwerke „APT28“ oder „Snake“ festlegen (Antwort zu Frage 12 auf Bundestagsdrucksache 19/1867)?
3. Worin bestanden der „Modus Operandi“ und die „technische[n] Merkmale“, die „mit hoher Wahrscheinlichkeit“ für Urheberschaft vom „APT28“ bzw. „Snake“ sprechen?
4. Mit welcher Schadsoftware wurden das deutsche Regierungsnetz, deutsche Auslandsvertretungen in westlichen Staaten, mehrere Schulen und Hochschulen sowie Forschungsinstitute angegriffen, und wann trugen sich diese Angriffe zu (Antwort zu Frage 14a auf Bundestagsdrucksache 19/1867)?
5. Inwiefern trifft es zu, dass bei dem Angriff Schadsoftware genutzt wurde, die auf Computern mit kyrillischem Zeichensatz programmiert wurde („Hacker mit Stil“, www.faz.de vom 2. Mai 2018)?
   a) Welche Programmierwerkzeuge wurden dabei vermutlich genutzt?
   b) Welche Spuren der bei dem Angriff genutzten Schadsoftware konnten die Ermittlungsbehörden mittlerweile sichern, und in welcher Programmiersprache wurde diese geschrieben?
6. Was ist der Bundesregierung über eine Datenbank des US-Militärgeheimdienstes National Security Agency (NSA) bekannt, in der Programmiercode gesammelt wird, um die Urheber von Schadsoftware ermitteln zu können?
   a) Welche deutschen Behörden und Geheimdienste arbeiten hierzu mit der NSA zusammen?
   b) Inwiefern wurde die NSA-Datenbank auch in den Ermittlungen zum „Bundeshack“ genutzt?
7. Was ist der Bundesregierung darüber bekannt, inwiefern im sogenannten Darknet Belohnungen ausgesetzt wurden, um Informationen über den „Bundeshack“ zu erlangen?
   a) In welchem Ausmaß machen welche Bundesbehörden von solchen Informationsaufkäufen Gebrauch?
   b) Mit welchen externen Beratern und Sicherheitsunternehmen arbeiten die Bundesministerien bzw. das Bundeskanzleramt hierzu zusammen?

8. Worin bestanden die Meinungsverschiedenheiten in der „interne[n] Willensbildung der Bundesregierung zum Umgang mit dem laufenden Angriff“, die dazu geführt haben, dass das Parlamentarische Kontrollgremium erst durch Medienberichte von dem Angriff erfuhr (Antwort zu Frage 4 auf Bundestagsdrucksache 19/1867)?
9. Was ist der Bundesregierung darüber bekannt, inwiefern sich auch deutsche Träger für die Einrichtung eines der drei geplanten „Forschungs- und Kompetenzzentren für Cybersicherheit“ bzw. ein entsprechendes „Pilotzentrum“ bewerben wollen (Antwort zu Frage 6 auf Bundestagsdrucksache 19/1900)?
10. Welche Haltung vertritt die Bundesregierung zur von der Europäischen Kommission geprüften Einrichtung eines Europäischen „Cybersecurity Forschungs- und Kompetenzzentrums“ in Form einer Generalunternehmung gemäß Artikel 187 oder Artikel 173 des Vertrags über die Arbeitsweise der Europäischen Union?
11. In welchen Cyberübungen, an denen sich die Bundeswehr im Jahr 2018 beteiligt, wird mit den Anwendungen „Cobalt Strike“, „Metasploit“ oder „Burp Proxy“ geübt (Antwort zu Frage 15d auf Bundestagsdrucksache 19/1900)?
12. Wann und wo finden die diesjährigen ressortübergreifenden „Cybersicherheitskonsultationen“ mit Russland statt, die der Vertrauensbildung und der strategischen Zusammenarbeit dienen sollen (Antwort zu Frage 22 auf Bundestagsdrucksache 19/1900)?
13. Sofern diese „Cybersicherheitskonsultationen“ derzeit nicht stattfinden, welche Gründe sind dafür maßgeblich?
14. Über welche „Hinweise“ verfügt der Präsident des Bundesamtes für Verfassungsschutz (BfV), die er von Dritten gehört haben will und die illustrieren sollen, dass „Russland“ (an anderer Stelle ist von „russischen Trollen“ die Rede) die katalanische Unabhängigkeitsbewegung „mit Propaganda unterstützt“ („Geheimdienste werfen Russland Unterstützung von Separatisten vor“, spiegel.de vom 14. Mai 2018)?
    a) Von welchen Dritten hat der BfV-Präsident diese „Hinweise“ auf eine „Unterstützung im Bereich von Desinformation und Propaganda“ gehört?
    b) Inwiefern können diese „Hinweise“ belegen, dass es sich bei der behaupteten Einflussnahme um eine staatliche Maßnahme handelt?
15. Welcher „gleiche Angreifer mit der gleichen Schadware“ hat versucht, welche „deutsche Infrastruktur anzugreifen“, nachdem dieser zuvor einen Cyberangriff „auf ein ukrainisches Kraftwerk im Dezember 2015“ verübt haben soll („Maaßen warnt vor Cyberangriffen auf kritische Infrastruktur in Deutschland“, afp.com vom 14. Mai 2018)?
    a) Welche „deutsche Infrastruktur“ wurde dabei angegriffen?
    b) Wie wurde festgestellt, dass es sich um den „gleiche[n] Angreifer handelt?
    c) Mit welchen ukrainischen Behörden haben welche deutschen Behörden hierzu ermittelt?

16. Inwiefern sind die „Prüfungen zu Maßnahmen einer (zivilen) aktiven Cyber-Abwehr“ nach der Antwort zu Frage 24 auf Bundestagsdrucksache 19/1867 inzwischen fortgesetzt worden, und was kann die Bundesregierung dazu mitteilen?

    a) Für welche Szenarien, in welcher Form und auf wessen Entscheidung sind „zivile Maßnahmen der aktiven Cyber-Abwehr“ aus Sicht der Bundesregierung derzeit denkbar („Deutschland im Visier“, tagesschau.de vom 14. Mail 2018)?

    b) Welche (auch militärischen) Attributionsmöglichkeiten sollen vor einer „aktiven Cyber-Abwehr“ ausgeschöpft werden?

    c) Sofern die Ergebnisse dieser Prüfungen weiterhin nicht vorliegen, wann ist damit zu rechnen?

17. In welchen Fällen haben welche deutschen Behörden bereits einen „Gegenangriff bei Hackerangriffen“ durchgeführt, und inwiefern wurde dabei ein „Server eines Gegners“ zerstört, kopierte Daten „im Verlauf gelöscht“, Daten gelöscht, nachdem sie „bereits auf einem Server in einem Drittstaat“ lagen oder Schadsoftware eines Angreifers manipuliert, um „im Gegenzug ausländische Rechner zu infiltrieren“ („Maaßen warnt vor Cyberangriffen auf kritische Infrastruktur in Deutschland“, afp.com vom 14. Mai 2018)?

Berlin, den 16. Mai 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