Deutscher Bundestag **Drucksache 19/2643**

19. Wahlperiode 11.06.2018

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Christine Buchholz, Heike Hänsel, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 19/2297 –

Unklare Faktenlage zum sogenannten „Bundeshack“

Vorbemerkung der Fragesteller

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

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 7. Juni 2018 übermittelt.

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

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.

Vorbemerkung der Bundesregierung

Zwar ist der parlamentarische Informationsanspruch grundsätzlich auf die Beantwortung gestellter Fragen in der Öffentlichkeit angelegt. Die Bundesregierung ist allerdings nach sorgfältiger Abwägung zu der Auffassung gelangt, dass eine Beantwortung der Fragen 1, 5, 11 und 14 nicht oder nicht vollständig in offener Form erfolgen kann. Zu den Gründen wird im folgenden Stellung genommen.

1. Die erbetene Auskunft zu Frage 1 ist geheimhaltungsbedürftig, weil die Kenntnisnahme der Antworten durch Unbefugte die Sicherheit der Bundesrepublik Deutschland gefährden und ihren Interessen schweren Schaden zufügen kann. Die Antworten enthalten Informationen zu der Erkenntnislage der Behörden über das Vorgehen und die Fähigkeiten des Angreifers sowie zur Wirksamkeit seines Angriffs. Die Veröffentlichung würde die zukünftige Aufgabenerfüllung der beteiligten Behörden und damit die Gewährleistung der IT-Sicherheit gefährden sowie zukünftige Angriffe erleichtern, da Erkenntnisse über Analysefähigkeiten von Sicherheitsvorfällen und Maßnahmen zur Sicherung von IT-Systemen betroffen sind. Der Schutz vor allem der technischen Fähigkeiten der Bundesbehörden stellt für die Aufgabenerfüllung der Bundesbehörden einen überragend wichtigen Grundsatz dar. 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 den Interessen der Bundesrepublik Deutschland schädlich sein. Die Schutzmaßnahmen dienen der Aufrechterhaltung der Sicherheit und Funktionsfähigkeit des IVBBs und hierdurch der Funktionsfähigkeit der Bundesregierung und damit dem Staatswohl.

   Daher ist die Antwort zu Frage 1 als Verschlusssache nach § 4 Absatz 2 Sicherheitsüberprüfungsgesetz in Verbindung mit der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA) mit dem Geheimhaltungsgrad „VS – Geheim“ eingestuft und kann in der Geheimschutzstelle des Deutschen Bundestages eingesehen werden.[1]

2. Eine Beantwortung der Frage 5 muss mit Blick auf die noch fortdauernden Ermittlungen unterbleiben. Trotz der grundsätzlichen verfassungsrechtlichen Pflicht, Informationsansprüche des Deutschen Bundestages zu erfüllen, tritt hier nach sorgfältiger Abwägung der betroffenen Belange im Einzelfall das Informationsinteresse des Parlaments hinter den berechtigten Interessen bei der

[1] Die vom Bundesministerium des Innern, für Bau und Heimat als „VS – Geheim“ eingestufte Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

Durchführung eines strafrechtlichen Ermittlungsverfahrens zurück. Das Interesse der Allgemeinheit an der Gewährleistung einer funktionstüchtigen Strafrechtspflege leitet sich aus dem Rechtsstaatsprinzip ab und hat damit ebenfalls Verfassungsrang.

3. Die Einstufung der Antwort zu Frage 11 wird im Hinblick auf das Staatswohl als erforderlich erachtet, da sie Details zu Cyberoperationen enthalten und die offene Bekanntgabe von Informationen die Durchführung zukünftiger Operationen gefährden könnte. Nach § 3 Nummer 4 VSA sind Informationen, deren Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein können, entsprechend einzustufen. Im vorliegenden Fall werden diese Informationen daher als „VS – Nur für den Dienstgebrauch“ eingestuft.[2]

4. Auch die Beantwortung der Frage 14 und der Teilfrage 14b kann aus Gründen des Staatswohls nicht offen erfolgen. Eine Offenlegung der angefragten Informationen birgt die Gefahr erheblicher nachteiliger Auswirkungen auf die zukünftige vertrauensvolle Zusammenarbeit mit ausländischen Partnern. Eine Veröffentlichung würde zu einer wesentlichen Schwächung der dem BfV zur Verfügung stehenden Möglichkeiten zur Informationsgewinnung führen. Dies würde für die jeweilige Auftragserfüllung erhebliche Nachteile zur Folge haben. Die Veröffentlichung kann daher für die Interessen der Bundesrepublik schädlich sein. Deshalb sind die entsprechenden Informationen als Verschlusssache gemäß der VSA § 3 Nummer 3 als „VS – Vertraulich“ eingestuft.[3]

   Die erbetene Auskunft zu Teilfrage 14a kann aus Gründen des Staatswohls in Gänze nicht erteilt werden.

   Sie betrifft Belange, die der sogenannten „Third-Party-Rule“, zum Austausch mit internationalen Partnern unterfallen. Selbst die Bekanntgabe unter Wahrung des Geheimschutzes durch die Übermittlung an die Geheimschutzstelle des Deutschen Bundestages birgt das Risiko des Bekanntwerdens, das unter keinen Umständen hingenommen werden kann. Die so bekannt gewordenen Informationen, die nach den Regeln der „Third-Party-Rule“ erlangt wurden, würden als Störung der wechselseitigen Vertrauensgrundlage gewertet werden und hätten eine schwere Beeinträchtigung der Teilhabe an dem internationalen Erkenntnisaustausch zur Folge. Die notwendige Abwägung zwischen dem Staatswohl, das hier ein Geheimhaltungsinteresse beinhaltet, einerseits und dem grundsätzlich umfassenden parlamentarischen Fragerecht andererseits ergibt daher, dass auch eine eingestufte Übermittlung der Information an die Geheimschutzstelle des Deutschen Bundestages vorliegend nicht in Betracht kommt.

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)?

Nach der Bewertung der Bundesregierung lag dem Cyberangriff auf das Auswärtige Amt eine maßgeschneiderte und aufwändige Vorgehensweise zu Grunde. Die in diesem Fall verwendeten Schadprogramme sind nach derzeitigem Kenntnisstand nicht öffentlich verfügbar und haben keine spezielle Herstellerbezeichnung

[2] Die vom Bundesministerium des Innern, für Bau und Heimat als „VS – Nur für den Dienstgebrauch“ eingestufte Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

[3] Die vom Bundesministerium des Innern, für Bau und Heimat als „VS – Vertraulich“ eingestufte Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

(vgl. auch Antwort der Bundesregierung auf die Schriftliche Frage 24 des Abgeordneten Andrej Hunko auf Bundestagsdrucksache 19/1979. Weiterhin wurden einige wenige öffentlich verfügbare, für sich genommen legitime Administrationswerkzeuge genutzt.

Wegen der weiteren Inhalte der Antwort auf diese Frage wird auf die gemäß der Vorbemerkung der Bundesregierung Nummer 1 als „VS – Geheim“ eingestuften Teile verwiesen.

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)?

Auf die Antwort zu Frage 12 der Kleinen Anfrage auf Bundestagsdrucksache 19/1867 sowie die Antwort der Bundesregierung auf die Schriftliche Frage 24 des Abgeordneten Andrej Hunko auf Bundestagsdrucksache 19/1979 wird verwiesen.

3. Worin bestanden der „Modus Operandi“ und die „technische[n] Merkmale“, die „mit hoher Wahrscheinlichkeit“ für Urheberschaft vom „APT28“ bzw. „Snake“ sprechen?

Hierbei geht es insbesondere um die Art und Weise der Verbreitung der Schadsoftware und ihre Steuerung. Die Verbreitung und Steuerung der Schadsoftware ist für einige Varianten der Schadsoftware „Snake“ bekannt.

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)?

Auf die in Frage 14 auf Bundestagsdrucksache 19/1390 von den Fragestellern selbst genannte Schadsoftware wird verwiesen. Die Angriffe bzw. Angriffsversuche erfolgten seit 2014.

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?

Auf die Vorbemerkung der Bundesregierung zu Nummer 2 wird verwiesen.

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?

Die NSA-Datenbank ist der Bundesregierung aus Wikileaks Veröffentlichungen bekannt. Darüber hinaus liegen der Bundesregierung keine Erkenntnisse vor.

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?

Der Bundesregierung ist nicht bekannt, dass Belohnungen für Erkenntnisse zum Cyber-Angriff auf das Auswärtige Amt ausgesetzt wurden und Bundesbehörden haben derartige Belohnungen auch nicht selbst ausgesetzt oder im Rahmen einer Zusammenarbeit mit externen Beratern oder Sicherheitsunternehmen angeboten.

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)?

In der Antwort zu Frage 4 auf Bundestagsdrucksache 19/1867 wurde ausgeführt, dass die „interne Willensbildung der Bundesregierung zum Umgang mit dem laufenden Angriff auch wegen des andauernden Erkenntnisgewinns noch nicht vollständig abgeschlossen“ sei. Meinungsverschiedenheiten wurden damit nicht angedeutet und bestanden auch nicht.

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)?

Gegenüber BMI und BSI haben einzelne deutsche Vertreter, im Rahmen des „Call for Proposals“ zum geplanten „Forschungs- und Kompetenzzentren für Cybersicherheit“, die Absicht geäußert sich an Konsortien zu beteiligen.

Über das endgültige Bewerberfeld in dieser Ausschreibung der EU-Kommission und zur Zusammensetzung der sich bewerbenden Konsortien hat die Bundesregierung keine Erkenntnisse.

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?

Eine abschließende Position bezüglich der Optionen zur Einrichtung einer Generalunternehmung gem. Artikel 187 oder Artikel 173 AEUV kann derzeit nicht bezogen werden, da zunächst das Pilotprojekt gestartet werden soll, das im Ergebnis als Ausgangspunkt für ein solches Zentrum dient. Dazu wird auf die Antwort zu Frage 6 der Kleinen Anfrage auf Bundestagsdrucksache 19/1900 verwiesen.

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)?

Auf die Vorbemerkung der Bundesregierung zu Nummer 3 wird verwiesen.

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)?

Die ursprünglich für Mitte März 2018 terminierten Cybersicherheitskonsultationen mit Russland wurden nach Bekanntwerden der Cyberoperation gegen das Auswärtige Amt verschoben. Ein neuer Termin wurde noch nicht vereinbart.

13. Sofern diese „Cybersicherheitskonsultationen“ derzeit nicht stattfinden, welche Gründe sind dafür maßgeblich?

Auf die Antwort zu Frage 12 wird verwiesen.

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?

Auf die Vorbemerkung der Bundesregierung zu Nummer 4 wird verwiesen.

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?

Bei dem Angreifer handelte es sich um die APT-Gruppierung SANDWORM, die auch unter den Bezeichnungen BlackEnergy und Quedagh bekannt ist.

a) Eine deutsche Bildungseinrichtung wurde angegriffen.

b) Anhand technischer Parameter wurde die Feststellung getroffen.

c) Mit ukrainischen Behörden bestand zu diesem Sachverhalt keine Zusammenarbeit.

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?

Derzeit prüft die Bundesregierung möglichen Rechtssetzungsbedarf in Bezug auf Maßnahmen der zivilen aktiven Cyberabwehr, dazu gehören völker-, verfassungs- und einfachrechtliche Fragestellungen. Die Bundesregierung geht von einem Abschluss der Prüfungen in der 19. Legislaturperiode aus.

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)?

In keinem Fall.

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