Deutscher Bundestag **Drucksache 18/11106**

18. Wahlperiode 08.02.2017

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Wolfgang Gehrcke, Christine Buchholz, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 18/10952 –

Ermittlungen zu angeblich russischen Cyberangriffen

Vorbemerkung der Fragesteller

Das Bundesamt für Verfassungsschutz (BfV) verfügt laut seinem Präsidenten Dr. Hans-Georg Maaßen über „Indizien“, dass die russische Regierung im Dezember 2016 einen „Hackerangriff“ auf Computer der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) verübt habe (ZEIT ONLINE vom 7. Januar 2017, „Russland womöglich für Cyberattacke auf OSZE verantwortlich“). Der Vorfall sei demnach vom BfV selbst aufgedeckt worden. Eine Analyse habe ergeben, dass die „Angriffsinfrastruktur“ die gleiche sei, die das BfV „von anderen Cyberattacken“ kenne. Gemeint ist die mutmaßliche Gruppe „Advanced Persistent Threat“ (APT28), die im Jahr 2015 Phishing-Mails an Abgeordnete des Deutschen Bundestages versendet haben soll. Laut der Bundesregierung gebe es hierfür eine „Vielzahl von Indizien“ (Bundestagsdrucksache 18/10759).

Berichten einiger deutscher Medien zufolge seien solche „Cyberangriffe“ auch im Vorfeld der Bundestagswahl 2017 zu erwarten (beispielhaft: FAZ vom 10. November 2016, „Sicherheitskreise: Moskau kann Bundestagswahl beeinflussen“). Belege oder Quellen für ihre Behauptungen nennen die Zeitungen nicht. Entsprechende Gerüchte für eine russische Einflussnahme hatten im April 2016 bereits Dr. Hans-Georg Maaßen und der damalige Chef des Bundesnachrichtendiensts (BND), Gerhard Schindler, im Magazin „FOCUS“ gestreut (FOCUS vom 16. April 2016, „Nach diesem Interview werden Sie nicht ruhiger schlafen“). Die Geheimdienstchefs warnen darin vor „psychologische[n] Operationen“ des Kreml, darunter „Desinformation, Infiltration, Einflussnahme, Propaganda und Zersetzung“. Auf mehrmalige Nachfrage erklärt die Bundesregierung jedoch, ihr lägen hierzu keine Erkenntnisse vor (Bundestagsdrucksachen 18/8631, 18/10313, 18/10759).

Zu den vermeintlich russischen Aktivitäten im Cyberraum hat der für die Nachrichtendienste des Bundes zuständige Staatssekretär Klaus-Dieter Fritsche einen Bericht beim BND und beim BfV beauftragt, der zwar fertiggestellt, der Öffentlichkeit oder Abgeordneten aber nicht zugänglich ist. Dadurch ist keine unabhängige Prüfung der dort zusammengetragenen Annahmen, Indizien oder Beweise möglich. Die Antworten der Bundesregierung auf die Kleinen Anfragen der Fraktion DIE LINKE. zeigen, dass die bislang vorgetragenen Vorwürfe zu

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 6. Februar 2017 übermittelt.

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

angeblichen Cyberangriffen der russischen Regierung einer Überprüfung nicht standhalten: Weder sind laut der Bundesregierung Planungen zur Störung der Bundestagswahl erkennbar, noch lassen sich Medienberichte über eine angebliche Beeinflussung des Brexit-Votums untermauern. Als einzigen Beleg führt das Bundesministerium des Innern US-Untersuchungen an, die einen „Datendiebstahl“ vom Sommer 2016 auf Server der Demokraten in den USA nachweisen sollen, bei denen E-Mails des Parteivorstands sowie des Stabs von Hillary Clinton kopiert und an die Enthüllungsplattform Wikileaks weitergereicht wurden. Ein damals betroffener Mailaccount war lediglich mit dem Passwort „password“ gesichert (http://gleft.de/1yJ).

Eine russische Urheberschaft für den Phishing-Angriff ist auch in den USA umstritten. So ist es beispielsweise kein Indiz für einen Cyberangriff aus Russland, wenn beim Programmieren eine kyrillische Tastatur verwendet wurde. Ehemalige US-Geheimdienstler bestätigen diese Auffassung (http://gleft.de/1yH). Trotzdem behaupten die US-Geheimdienste NSA, FBI und CIA weiterhin, der Phishing-Angriff auf die Demokratische Partei sei Teil einer Kampagne, die der russische Präsident Wladimir Putin persönlich angeordnet habe. Ein Anfang Januar 2017 veröffentlichter Bericht enthält in seiner deklassifizierten Version (http://gleft.de/1yL) jedoch ebenfalls keine Beweise für eine „Kampagne“ aus Russland, zu der verdeckte Geheimdienstoperationen, offene Bemühungen russischer Regierungsstellen und Staatsmedien, Eingriffe von Außenstehenden sowie bezahlte Teilnehmer sozialer Netzwerke gehören sollen.

Der Geheimdienstbericht wurde dem amtierenden (Barack Obama) sowie dem designierten (Donald Trump) Präsidenten durch den nationalen Geheimdienstdirektor James R. Clapper präsentiert, der bereits zu den Edward-Snowden-Enthüllungen der Lüge überführt wurde (http://gleft.de/1yK). Als Motivation für die angebliche russische Cyber-Kampagne nennt Clapper die Ablehnung der damaligen Präsidentschaftskandidatin Hillary Clinton. So habe der Kreml eine „deutliche Präferenz“ für den Republikaner Donald Trump entwickelt. Putin erwarte sich demnach ähnlich gute Erfahrungen von Trump, wie er sie mit dem deutschen Ex-Bundeskanzler Gerhard Schröder (SPD) gemacht habe.

Vorbemerkung der Bundesregierung

1. Die Beantwortung der Fragen 15 und 16 kann aus Gründen des Staatswohls nicht in offener Form erfolgen. Die unbefugte Kenntnisnahme von Einzelheiten zu Aufklärungserkenntnissen des BfV 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 „VS – Nur für den Dienstgebrauch“ eingestuft und dem Deutschen Bundestag gesondert übermittelt.

2. Die Bundesregierung ist nach sorgfältiger Abwägung ferner zu der Auffassung gelangt, dass eine Beantwortung der Fragen 1c, 1d, 2, 4, 7b, 7d sowie 20a und 20b aus Gründen des Staatswohls nicht offen erfolgen kann. Arbeitsmethoden und Vorgehensweisen der Nachrichtendienste des Bundes sind im Hinblick auf die künftige Erfüllung ihres gesetzlichen Auftrags besonders schutzwürdig. Ebenso schutzbedürftig sind Einzelheiten zur nachrichtendienstlichen Erkenntnislage.

Eine Veröffentlichung von Einzelheiten solche Erkenntnisse betreffend würde zu einer wesentlichen Schwächung der zur Verfügung stehenden Möglichkeiten zur Informationsgewinnung führen. Dies würde für die Auftragserfüllung erhebliche Nachteile zur Folge haben. Sie kann für die Interessen der Bundesrepublik Deutschland schädlich sein. Deshalb sind die entsprechenden Informationen als Verschlusssache gemäß der VSA mit dem VS-Grad „VS – Vertraulich“ eingestuft und werden in der Geheimschutzstelle des Deutschen Bundestages hinterlegt.

3. Frage 14 berührt in Teilen solche Informationen, die in besonders hohem Maße das Staatswohl berühren und daher selbst in eingestufter Form nicht beantwortet werden können. Das verfassungsrechtlich verbürgte Frage- und das Informationsrecht des Deutschen Bundestages gegenüber der Bundesregierung wird durch gleichfalls Verfassungsrecht genießende schutzwürdige Interessen wie das Staatswohl begrenzt. Eine Offenlegung der angefragten Informationen birgt die Gefahr, dass Einzelheiten bekannt würden, die unter dem Aspekt des Schutzes der nachrichtendienstlichen Zusammenarbeit mit ausländischen Partnern besonders schutzbedürftig sind. Eine öffentliche Bekanntgabe von Informationen zum Kenntnisstand, zur Leistungsfähigkeit, zur Ausrichtung und zu technischen Fähigkeiten von ausländischen Partnerdiensten und damit einhergehend die Kenntnisnahme durch Unbefugte würde erhebliche nachteilige Auswirkungen auf die vertrauensvolle Zusammenarbeit haben. Würden in der Konsequenz eines Vertrauensverlustes Informationen von ausländischen Stellen entfallen oder wesentlich zurückgehen, entstünden signifikante Informationslücken mit negativen Folgewirkungen für die Genauigkeit der Abbildung der Sicherheitslage in der Bundesrepublik Deutschland sowie im Hinblick auf den Schutz deutscher Interessen im Ausland.

Dies würde folgenschwere Einschränkungen der Informationsgewinnung bedeuten, womit letztlich der gesetzliche Auftrag des Bundesnachrichtendienstes – die Sammlung und Auswertung von Informationen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind (§ 1 Absatz 2 des Gesetzes über den Bundesnachrichtendienst) – nicht mehr sachgerecht erfüllt werden könnte. Die Gewinnung von auslandsbezogenen Informationen ist für die Sicherheit der Bundesrepublik Deutschland und für die Aufgabenerfüllung des Bundesnachrichtendienstes jedoch unerlässlich.

Eine VS-Einstufung und Hinterlegung der angefragten Informationen in der Geheimschutzstelle des Deutschen Bundestages würde ihrer erheblichen Brisanz im Hinblick auf die Bedeutung für die Aufgabenerfüllung des Bundesnachrichtendienstes nicht ausreichend Rechnung tragen. Die angefragten Inhalte beschreiben die Fähigkeiten und Arbeitsweisen des Bundesnachrichtendienstes so detailliert, dass eine Bekanntgabe auch gegenüber einem begrenzten Kreis von Empfängern ihrem Schutzbedürfnis nicht Rechnung tragen kann. Bei einem Bekanntwerden der schutzbedürftigen Information wäre kein Ersatz durch andere Instrumente der Informationsgewinnung möglich.

Aus dem Vorgesagten ergibt sich, dass die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht wesentlich überwiegt. Insofern muss ausnahmsweise das Fragerecht der Abgeordneten gegenüber dem Geheimhaltungsinteresse der Bundesregierung zurückstehen.

1. Worin bestehen die „Indizien“, die das BfV zur Annahme verleiten, dass die russische Regierung im Dezember 2016 einen „Hackerangriff“ auf Computer der OSZE verübt haben soll (ZEIT ONLINE vom 7. Januar 2017, „Russland womöglich für Cyberattacke auf OSZE verantwortlich“)?

Die Indizien für eine russische Urheberschaft beziehen sich vorrangig auf die beim Angriff genutzte technische Infrastruktur.

a) Wann und auf welche Weise hat das BfV den Vorfall wie berichtet selbst aufgedeckt?

Die Infektion des OSZE-Netzwerkes wurde im vergangenen Jahr im Rahmen der operativen Bearbeitung festgestellt.

b) Wie gingen die Urheber des „Hackerangriffs“ vor, und welche Werkzeuge benutzten sie dabei?

Die Infektion erfolgte nach derzeitigem Kenntnisstand über sogenannte Spear-Phishing-E-Mails.

c) Welche Schäden oder Datenabflüsse sind entstanden (bitte auch die abgeflossene Datenmenge benennen)?

d) Von wem wurde der „Hackerangriff“ untersucht (bitte auch etwaige externe Experten benennen)?

Die Fragen 1c und 1d werden gemeinsam beantwortet.

Die Antwort zu diesen Fragen ist als Verschlusssache mit dem VS-Grad „VS – Vertraulich“ eingestuft und in der Geheimschutzstelle des Deutschen Bundestages hinterlegt.[1]

e) Im Rahmen welcher Untersuchungen bzw. Vorfälle im Cyberraum haben das Bundesamt für Sicherheit in der Informationstechnik (BSI) oder das BfV die bei der OSZE gefundene „Angriffsinfrastruktur“ bereits in der Vergangenheit beobachtet?

Die Angriffsinfrastruktur ist bereits bei zahlreichen anderen Angriffen gegen Einrichtungen des Bundes festgestellt worden.

[1] Die Antwort kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

2. Inwiefern liegen den Geheimdiensten des Bundes seit Beantwortung der Kleinen Anfragen der Fraktion DIE LINKE. auf Bundestagsdrucksachen 18/8631, 18/10759 weiterhin „keine Erkenntnisse“ zu tatsächlich geplanten oder durchgeführten „psychologische[n] Operationen“ des Kreml vor, die laut den Präsidenten von BND und BfV „Desinformation, Infiltration, Einflussnahme, Propaganda und Zersetzung“ beinhalten könnten?

Die Antwort zu dieser Frage ist als Verschlusssache mit dem VS-Grad „VS – Vertraulich“ eingestuft und ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt.[2]

3. Wer nahm die „Analysen der mutmaßlich russischen Cyberangriffs-Kampagnen mit internationaler Zielauswahl“ vor, aufgrund derer die Bundesregierung die „Annahme“ gründet, dass russische Geheimdienste „versuchen könnten, die Bundestagswahl 2017 durch Cyber-Angriffe zu beeinflussen“ (Bundestagsdrucksache 18/10759)?

Die Analysen beruhen auf einer Sammlung von Informationen der zuständigen Behörden, von privaten IT-Sicherheitsunternehmen und unabhängigen IT-Experten.

4. Inwiefern sind aus Sicht der Bundesregierung mittlerweile konkrete Planungen zur Störung der Bundestagswahl durch die russische Regierung erkennbar?

Die Antwort zu dieser Frage ist als Verschlusssache mit dem VS-Grad „VS – Vertraulich“ eingestuft und ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt.[3]

5. Welche Behörden der Bundesregierung sind an den Ermittlungen zur Veröffentlichung vertraulicher Akten aus dem NSA-Untersuchungsausschuss durch die Enthüllungsplattform Wikileaks beteiligt, wozu die Version kursierte, Russland habe sich die Daten durch einen Cyberangriff beschafft (tagesschau.de vom 18. Dezember 2016, „Bundespolizei vermutet Maulwurf im Bundestag“)?

Bundesbehörden im Sinne der Fragestellung sind an den in Rede stehenden Ermittlungen nicht beteiligt. Das Bundeskriminalamt hat auf Anforderung der Polizei beim Deutschen Bundestag im Rahmen der Amtshilfe bei der Datensicherung der Veröffentlichung bei WikiLeaks unterstützt. Die Amtshilfe wurde am 5. Dezember 2016 beendet.

6. Welche Einrichtungen (Ressorts deutscher Bundesministerien sowie sonstige Teilnehmende) sind an dem im August 2016 gegründeten „Netzwerk zur Abwehr sogenannter hybrider Bedrohungen“ beteiligt, und welche Arbeitsgruppen wurden dort eingerichtet?

Am „Netzwerk gegen hybride Bedrohungen“ sind alle Bundesministerien, das Bundeskanzleramt, die Beauftragte der Bundesregierung für Kultur und Medien sowie das Bundespresseamt beteiligt. Die Einrichtung von Arbeitsgruppen im Rahmen dieses Netzwerks ist derzeit nicht beabsichtigt.

---

[2] Die Antwort kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

[3] Die Antwort kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

7. Welche Ergebnisse zeitigte die Prüfung der Ergebnisse eines Berichts, den die Bundesregierung beim BND und beim BfV zu vermeintlich russischen Aktivitäten im Cyberraum beauftragt hat (Bundestagsdrucksache 18/10759)?

   a) Sofern die Prüfung weiter anhält, für wann rechnet die Bundesregierung mit deren Abschluss?

   c) Wann und wem gegenüber werden die Ergebnisse des Berichts vollständig oder teilweise veröffentlicht?

Die Fragen 7, 7a und 7c werden gemeinsam beantwortet.

Die Bundesregierung hat den Bericht zur Kenntnis genommen. Der Bericht ist nur für den internen Gebrauch bestimmt.

   b) In welchen „Arbeitsbereichen/Abteilungen“ wird der Themenkomplex beim BND bearbeitet?

   d) Inwiefern trifft es zu, dass die Arbeitsgruppe den Namen „PsyOps“ trug (SPIEGEL ONLINE vom 14. Januar 2017, „BND wirft Russland gezielte Stimmungsmache vor“)?

Die Fragen 7b und 7d werden gemeinsam beantwortet.

Die Antworten zu diesen Fragen sind als Verschlusssache mit dem VS-Grad „VS – Vertraulich“ eingestuft und werden in der Geheimschutzstelle des Deutschen Bundestages hinterlegt.[4]

8. Mit welchen Maßnahmen will die Bundesregierung auf die Ergebnisse des Berichts reagieren, etwa um zu verhindern, dass die russische Regierung „mit geheimdienstlichen Mitteln die politische Debatte und die öffentliche Meinung in Deutschland zu beeinflussen sucht“ (tagesschau.de vom 18. Februar 2016, „Russische Desinformation in Deutschland?“)?

Die Bundesregierung beobachtet entsprechende Bestrebungen aufmerksam und wird ggf. geeignete Maßnahmen, dem entgegenzuwirken, prüfen.

9. Wann und von wem wurde die Bundesregierung durch die US-Regierung über Hackerangriffe von Sommer 2016 auf Server der Demokraten in den USA informiert, bei denen E-Mails des Parteivorstands sowie des Stabs von Hillary Clinton kopiert und an die Enthüllungsplattform Wikileaks weitergereicht wurden?

Der Nationale Sicherheitsrat der USA hat im Spätsommer 2016 bei einer Konferenz in den USA einen größeren Personenkreis informiert.

   a) Wann haben den Geheimdiensten der Bundesregierung erstmals Informationen vorgelegen, dass britische Geheimdienste bereits im Frühjahr 2015 durch überwachte Datenflüsse davon gewusst haben wollen, dass „Moskau“ die Server der Demokratischen Partei „gehackt“ habe (theguardian.com vom 7. Januar 2017, „UK intelligence gave US key tipoff about Russian hacking, report says“?

Den Nachrichtendiensten des Bundes liegen derartige Informationen nicht vor.

[4] Die Antwort kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

b) Inwiefern hat die Bundesregierung bei ihrer auf Bundestagsdrucksache 18/10759 skizzierten Einschätzung der Vorfälle auch die Stellungnahme von ehemaligen US-Geheimdienstangehörigen geprüft, die eine russische Urheberschaft anzweifeln (http://gleft.de/1yH)?

Entsprechende Stellungnahmen sind in die Einschätzung eingeflossen.

c) Welche Beweise (nicht Annahmen oder Indizien) sind der Bundesregierung durch eingestufte oder nicht eingestufte Veröffentlichungen der US-Regierung zu den angeblichen russischen Hackerangriffen auf die Partei der Demokraten bekannt geworden?

Der Bundesregierung sind durch die Veröffentlichungen der US-Regierung Beweise im Sinne der Fragestellung nicht bekannt geworden.

10. Was ist der Bundesregierung über eine Spear-Phishing-Kampagne gegen Mitarbeiter von US-Regierung, Thinktanks und Nichtregierungsorganisationen bekannt, die dem US-Geheimdienstbericht zufolge am Wahlabend des 8. November 2016 begonnen hat?

Der Bundesregierung liegen hierzu über Presseberichte hinaus keine Erkenntnisse vor.

11. Was ist der Bundesregierung aus eigenen Erkenntnissen oder der Verfolgung von Veröffentlichungen anderer über eine Instrumentalisierung der Enthüllungsplattform Wikileaks durch die russische Regierung bekannt?

12. Was ist der Bundesregierung darüber bekannt, dass US-amerikanische Geheimdienste die Computer russischer Stromversorger und Telekommunikationsanbieter sowie den Kreml „quasi vorbeugend“ mit „Cyber-Waffen“ infiltriert haben, um diese im Bedarfsfall zum Einsatz zu bringen (faz.net vom 9. Januar 2017, „Amerikas Geheimdienste munkeln“)?

Die Fragen 11 und 12 werden gemeinsam beantwortet.

Der Bundesregierung liegen hierzu keine Erkenntnisse vor.

13. Inwiefern ist auch die Bundesregierung der von US-Geheimdiensten geäußerten Ansicht (http://gleft.de/1yL), der russische Präsident habe eine „deutliche Präferenz“ für den Republikaner Donald Trump entwickelt und erwarte sich von ihm ähnlich gute Erfahrungen, wie er sie mit dem deutschen Ex-Bundeskanzler Gerhard Schröder (SPD) gemacht hat?

Der Bundesregierung sind die veröffentlichten Dokumente der US-Geheimdienste sowie die Presseberichterstattung bekannt. Die Bundesregierung hat keine Erkenntnisse zu den behaupteten Erwartungen von Präsident Putin. An Spekulationen über die Erwartungen von Staatsoberhäuptern beteiligt sich die Bundesregierung nicht.

14. Von welchen weiteren Regierungen der Mitgliedstaaten der Europäischen Union oder der NATO erhielt die Bundesregierung Hinweise über eine vermeintlich russische „Desinformation, Infiltration, Einflussnahme, Propaganda und Zersetzung“, und welche der Regierungen hat dafür auch Beweise mitteilen können?

Russische Desinformations- und Beeinflussungsversuche waren zuletzt wiederholt Thema von multilateralen wie auch bilateralen Gesprächen der Bundesregierung mit EU- und NATO-Partnern und sind Gegenstand eines regelmäßigen nachrichtendienstlichen Austausches.

Dieser Austausch erfolgt auf der Grundlage gegenseitiger Vertraulichkeit. Nähere Angaben können aus Gründen des Staatswohls nicht erfolgen, da dies die Grundlage der Zusammenarbeit gefährden würde. Dies wiederum würde sich nachteilig auf die Interessen der Bundesrepublik Deutschland auswirken.

15. Inwiefern wurden seit Beantwortung der Kleinen Anfragen auf Bundestagsdrucksachen 18/8631 und 18/10759 weiterhin keine Anwerbeversuche der „Mitarbeiter [deutscher] Parlamentarier oder politischer Stiftungen“ durch die russische Regierung festgestellt?

16. Was ist der Bundesregierung darüber bekannt, in wie vielen Fällen Einrichtungen der Europäischen Union im Jahr 2016 von Hackerangriffen betroffen waren und wie viele dieser Fälle einen geheimdienstlichen Ursprung haben?

Die Fragen 15 und 16 werden gemeinsam beantwortet.

Die Antwort zu diesen Fragen ist als Verschlusssache mit dem VS-Grad „VS – Nur für den Dienstgebrauch“ eingestuft und wird dem Deutschen Bundestag gesondert übermittelt.[5]

17. Über wie viele mutmaßlich durch staatliche Stellen erfolgte „elektronische Angriffe gegen digitale Infrastrukturen der Bundesregierung“ wurde das BfV im gesamten Jahr 2016 durch das BSI unterrichtet, und wie viele davon wurden nach Prüfung durch das BfV tatsächlich Regierungen zugeordnet?

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) informierte das BfV im Jahr 2016 durchschnittlich ein Mal pro Woche über einen detektierten Angriff mit mutmaßlich nachrichtendienstlichem Hintergrund.

18. Welche Techniken klassifiziert das Bundesinnenministerium bei solchen Vorfällen als „hochspezialisierte Angriffe, die nur durch manuelle Analysen erkannt werden konnten“ (Bundestagsdrucksache 18/10759)?

Die eingesetzten Techniken müssen die in den Regierungsnetzen vorhandenen Standardsicherheitsmechanismen überwinden, somit von den zentralen Virenscannern und von dem vom BSI betriebenen Virenscanner nicht erkannt werden. In den Bereichen, in denen § 5 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) Anwendung findet, erfolgt durch fortschrittliche Analysetechniken eine automatisierte, dann eine manuelle Analyse.

[5] Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

19. Welche Angriffe auf deutsche Infrastrukturen werden vom BfV und BSI den Personen oder Gruppierungen „Cozy Bear“, „Fancy Bear“, „Guccifer 2.0“, „APT 28“ und „APT 29“ zugerechnet?

Das BSI hat bei der Analyse der Daten an den Schnittstellen der Kommunikationstechnik des Bundes Angriffe detektiert, welche Indizien enthalten, die eine Zuordnung zu den genannten Gruppierungen plausibel machen könnten.

APT 28 (Advanced Persistent Threat) wird für die Cyberangriffe auf den Deutschen Bundestag im Frühjahr 2015 sowie auf politische Parteien im April, Mai und August 2016 verantwortlich gemacht.

APT 29 wurde im Februar 2014 im Zusammenhang mit einem Angriff auf eine Bundestagsabgeordnete beobachtet. Ferner wurde 2016 beobachtet, wie universitäre Infrastruktur kompromittiert und als C&C-Server (Command and Control) zweckentfremdet wurde.

a) Welche Belege konnten die Ämter darüber zusammentragen, wer sich hinter den Kürzeln mutmasslich verbirgt?

Fancy Bear und APT 28 sind Synonyme und bezeichnen dieselbe Cyberangriffsoperation; dasselbe gilt für Cozy Bear und APT 29. Die Verwendung der jeweiligen Bezeichnung unterliegt der Präferenz der jeweiligen Behörde bzw. des IT-Sicherheitsunternehmens. Unter dem Pseudonym Guccifer 2.0 erfolgte im Sommer 2016 die Veröffentlichung gestohlener Dokumente aus dem DNC-Hack. Diese Operation wird ebenfalls der Kampagne APT 28 zugerechnet.

Unter den Kürzeln werden Gemeinsamkeiten einzelner Cyberoperationen, wie beispielsweise dabei verwendete Infrastruktur, Schadsoftware, Exfiltrationswege oder ausgenutzte Sicherheitslücken zu einer Kampagne zusammengefasst.

b) Welche Daten sind bei Angriffen auf deutsche Infrastrukturen, die das BfV oder der BND „Cozy Bear“, „Fancy Bear“, „Guccifer 2.0“, „APT 28“ und „APT 29“ zurechnet, abgeflossen (bitte auch die Datenmenge benennen)?

Bei dem Cyberangriff auf den Deutschen Bundestag im Frühjahr 2015 sind nach Angaben des BSI Daten in der Größenordnung von ca. 16 GB abgeflossen. Über den Inhalt der abgeflossenen Daten ist hier nichts bekannt. Ein Datenabfluss bei von APT 29 attackierten Zielen ist bisher nicht bekannt geworden.

c) Was ist der Bundesregierung darüber bekannt, inwiefern „Cozy Bear“, „Fancy Bear“, „Guccifer 2.0“, „APT 28“ und „APT 29“ in der Vergangenheit auch Ziele auf russischem Hoheitsgebiet angegriffen haben?

IT-Sicherheitsunternehmen wie z. B. TrendMicro berichteten in der Vergangenheit über Cyberangriffe der Kampagne APT 28 gegen russische Dissidenten bzw. Regierungskritiker.

20. Worin besteht die „Vielzahl von Indizien“, wonach die Gruppe APT28 für die im Jahr 2015 versandten Cyber-Angriffe (Phishing-Mails) an Abgeordnete des Deutschen Bundestages versendet haben soll (Bundestagsdrucksache 18/10759)?

Die Vorgehensweise der Angreifer (Angriffs-E-Mail, genutzte Schadprogramme) und die von ihnen genutzte Infrastruktur (Mailserver, C2-Server etc.) sind identisch zu denen von anderen Angriffen der APT28-Kampagne. Dies wurde durch eigene Erkenntnisse sowie durch öffentlich verfügbaren Ergebnisse von Analysen Dritter (z. B. IT-Sicherheitsfirmen) nachgewiesen.

a) Welche Einrichtungen des Bundestages bzw. welche Abgeordnetenbüros waren von den Angriffen betroffen?

b) Welche Einrichtungen des Bundestages bzw. welche Abgeordnetenbüros öffneten die über Phishing-Mails verteilten URL und luden schließlich Schadsoftware aus dem Netz nach (sofern dies für die Bundesregierung nicht feststellbar war, bitte die Gründe mitteilen)?

Die Fragen 20a und 20b werden gemeinsam beantwortet.

Die Antworten zu diesen Fragen sind als Verschlusssache mit dem VS-Grad „VS – Vertraulich“ eingestuft und sind in der Geheimschutzstelle des Deutschen Bundestages hinterlegt.[6]

c) Inwiefern könnten die am 8. Juni 2015 unter dem Absender „Angela Merkel“ versandten Phishing-Mails Informationen aus früheren Datenabflüssen genutzt haben, etwa zur Täuschung durch die angegebene bundestagsinterne URL „eudoxap01.bundestag.btg:8080/eudox/20150608-PDRInformationen.pdf“, hinter der sich im HTML-Code infizierte Server verbargen?

Hierzu liegen der Bundesregierung keine Erkenntnisse vor.

d) Welche Rückschlüsse lassen die Analysen der Bundesregierung auf die Gefährdung bestimmter Einrichtungen oder Büros von Abgeordneten durch zukünftige Angriffe zu?

Deutsche Stellen, darunter auch Büros von Abgeordneten, werden nach Einschätzung der Bundesregierung auch zukünftig im Fokus nachrichtendienstlicher Angreifer stehen.

e) Auf welche Weise hat die Bundesregierung die besonders gefährdeten Einrichtungen oder Büros von Abgeordneten über diese Risikoanalyse informiert?

Die Sicherheitsbehörden des Bundes weisen regelmäßig durch Sensibilisierungen und Veröffentlichungen auf die bestehenden Cyberbedrohungen hin.

[6] Die Antwort kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

21. Auf welche Weise werden die Überlegungen der Bundesregierung zum Umgang mit „Fake News“ weiterverfolgt (deutschlandfunk.de vom 9. Januar 2017, „In absehbarer Zeit werden Fake News die Wahl nicht entscheiden“?

Derzeit wird geprüft, ob der Umgang mit sogenannten Fake News gesetzgeberischen Handlungsbedarf auslöst. Die hierzu erforderliche Meinungsbildung zwischen den Ressorts hat noch nicht stattgefunden.

Die Bundesregierung passt ihr Medienmonitoring an die veränderte Kommunikationslandschaft an und trägt dabei der gewachsenen Rolle des Social Web für die öffentliche Kommunikation und Meinungsbildung Rechnung.

22. Auf welche Weise werden die Überlegungen der Bundesregierung weiterverfolgt, die deutsche Spionageabwehr, wie vom Verfassungsschutzpräsidenten gefordert, mit „Gegenangriffen auf Cyberattacken“ reagieren zu lassen (tagesschau.de vom 10. Januar 2017, „Maaßen bläst zur Gegenattacke“)?

a) Welche Behörden sollten aus Sicht der Bundesregierung eine solche Möglichkeit erhalten?

b) Nach welcher Maßgabe müsste ein Urheber von Cyberangriffen als Adressat eines staatlichen Cyberangriffs zuvor zweifelsfrei festgestellt werden?

Die Fragen 22 bis 22b werden gemeinsam beantwortet.

Die Bundesregierung hat in ihrer Cyber-Sicherheitsstrategie für Deutschland vom 9. November 2016 ausgeführt, dass schwerwiegende Cyber-Angriffe vorstellbar sind, gegen die mit den klassischen präventiven Maßnahmen in der notwendigen Zeit nicht nachhaltig vorgegangen werden kann.

Die Bundesregierung hat sich daher im Rahmen der Cyber-Sicherheitsstrategie vorgenommen, zu prüfen, unter welchen rechtlichen Rahmenbedingungen und mit welchen technischen Möglichkeiten in diesen Fällen durch staatliche Stellen Netzwerkoperationen durchgeführt werden könnten.

Die Fragen, welche Behörden insoweit in Betracht kommen und welche Methoden und welcher Nachweisgrad bei der Zurechnung von Cyber-Angriffen zur Anwendung kommen sollen, sind Teil dieser Prüfungen. Diese sind allerdings noch nicht abgeschlossen.

23. Wann soll die konkrete Einrichtung der „EU Hybrid Fusion Cell“ im geheimdienstlichen EU-Lagezentrum „EU Intelligence Analysis Centre“ des Europäischen Auswärtigen Dienstes erfolgen?

a) Welche Details zur personellen Aufstellung sind der Bundesregierung mittlerweile bekannt?

c) Inwiefern ist die Abstimmung der „Hybrid Fusion Cell“ mit einer NATO-Abteilung gegen „hybride Bedrohungen“ zu gemeinsamen Übungen „auf politischer und technischer Ebene“ mittlerweile fortgeschritten, und welche Planungen sind der Bundesregierung dazu bekannt?

Die Fragen 23, 23a und 23c werden gemeinsam beantwortet.

Auf die Antwort der Bundesregierung zu den Fragen 19, 19b und 23 der Kleinen Anfrage der Fraktion DIE LINKE. vom 28. November 2016 auf Bundestagsdrucksache 18/10759 wird verwiesen. Neue Erkenntnisse hierzu sind in der Zwischenzeit nicht angefallen.

b) Wo soll die deutsche nationale Kontaktstelle für die „Hybrid Fusion Cell“ angesiedelt werden?

Die deutsche Kontaktstelle wurde im Auswärtigen Amt eingerichtet.

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