



POSTANSCHRIFT Bundesministerium des Innern, für Bau und Heimat, 11014 Berlin

Präsident des Deutschen Bundestages  
– Parlamentssekretariat –  
Reichstagsgebäude  
11011 Berlin

HAUSANSCHRIFT Alt-Moabit 140, 10557 Berlin

POSTANSCHRIFT 11014 Berlin

TEL +49 (0)30 18 681-11117

FAX +49 (0)30 18 681-11019

INTERNET [www.bmi.bund.de](http://www.bmi.bund.de)

DATUM 20. April 2018

BETREFF **Kleine Anfrage des Abgeordneten Andrej Hunko u. a. und der Fraktion DIE LINKE.**

**Kompromittierung deutscher Regierungsnetze**

**BT-Drucksache 19/1390**

Auf die Kleine Anfrage übersende ich namens der Bundesregierung die beigefügte Antwort.

**Hinweis: Teile der Antwort sind VS - NUR FÜR DEN DIENSTGEBRAUCH bzw. VS - GEHEIM (liegt der Geheimschutzstelle des Deutschen Bundestages vor) eingestuft.**

Mit freundlichen Grüßen  
in Vertretung



Dr. Günter Krings

Kleine Anfrage des Abgeordneten Andrej Hunko u.a.  
und der Fraktion DIE LINKE.

Kompromittierung deutscher Regierungsnetze

BT-Drucksache 19/1390

---

Vorbemerkung der Fragesteller:

Am 28. Februar 2018 meldete die Deutschen Presse-Agentur (dpa), „ausländische Hacker“ seien in den Informationsverbund des Bundes Berlin-Bonn (IVBB) eingedrungen („Innenministerium: Hacker griffen deutsches Regierungsnetz an“, [morgenpost.de](http://morgenpost.de) vom 28. Februar 2018). Im Auswärtigen Amt habe es „einen entsprechenden Vorfall“ gegeben, auch das Verteidigungsministerium sei betroffen. Den Hinweis auf die Kompromittierung hätten deutsche Geheimdienste nach Informationen des Senders rbb am 19. Dezember von einem „ausländischen Partner“ erhalten („Von der Uni ins Ministerium?“, [tagesschau.de](http://tagesschau.de) vom 2. März 2018). In der Bundespressekonferenz vom 2. März 2018 wurde hierzu gemutmaßt, dieser Dienst käme aus dem Baltikum („Regierungs-pressekonferenz vom 2. März 2018“, [bundesregierung.de](http://bundesregierung.de)). Nun ermitteln Bundesamt für Sicherheit in der Informationstechnik (BSI) und das für Spionageabwehr zuständige Bundesamt für Verfassungsschutz (BfV), auch der Auslandsgeheimdienst Bundesnachrichtendienst (BND) ist eingebunden. Verbindungsdaten des IVBB werden drei Monate aufgehoben. Für rund neun Monate der Angriffe stehen für die Ermittlungen deshalb keine Logfiles zur Verfügung.

Als Urheber des „Vorfalls“ wurde von der dpa das in Russland verortete Netzwerk „APT28“ benannt, das auch für Phishing-Mails an Bundestagsbüros im Jahr 2015 verantwortlich sein soll. Einen Tag später korrigierte sich die Agentur und schrieb den „Vorfall“ unter Berufung auf ungenannte „Kreise“ dem ebenfalls in Russland verorteten Netzwerk „Snake“ zu, das „Verbindungen“ zu russischen Geheimdiensten habe („Kreise: Russische "Snake"-Hacker hinter Angriff“, dpa vom 1. März 2018). „Snake“ ist eigentlich die Bezeichnung für die Schadsoftware „Turla“ bzw. „Uroburos“ (<https://www.kaspersky.de/resource-center/threats/epic-turla-snake-malware-attacks>), wird jedoch synonym zur Bezeichnung mutmaßlicher Angreifer gebraucht. Der Trojaner „Uroburos“ wurde 2008 entdeckt und soll kyrillische Schriftzeichen im Programmcode enthalten, seit 2014 soll eine Linux-Variante kursieren (<https://malwarebattle.blogspot.de/2014/03/g-data-found-russian-cyber-weapon.html>).

Sicherheitsfirmen wiesen in den vergangenen Jahren darauf hin, dass „Uroburos“ Teil einer internationalen „Spionagekampagne“ gewesen sei, die weltweit „Botschaften, Rüstungsfirmen, Lehranstalten und Forschungsinstitute“ betroffen habe (<https://securelist.com/the-epic-turla-operation/65545/>).

Auch im Bundesinnenministerium war dies bekannt. Im Verfassungsschutzbericht für 2016 heißt es, dass „Snake“ seit 2005 mit der „sehr komplexen und qualitativ hochwertigen Schadsoftware“ aktiv sei. „Uroburos“ sei darauf ausgelegt, „in großen Netzwerken von Behörden, Firmen und Forschungseinrichtungen zu agieren“.

Betroffen seien insbesondere die Bereiche Energietechnik, Röntgen- und Nukleartechnologie, Messtechnologie sowie Luft- und Raumfahrt.

Das Rootkit „Uroburos“, das sich selbstständig in infizierten Netzwerken verbreitet, besteht aus zwei Dateien für 32- und 64-Bit-Windows-Systeme mit einem Treiber.

Die Kompromittierung des IVBB sei laut der dpa über Computer einer Fachhochschule des Bundes für öffentliche Verwaltung erfolgt, Aktivitäten seien ab Ende 2016 festgestellt worden („Kreise: Russische "Snake"-Hacker hinter Angriff“, dpa vom 1. März 2018).

Der Angriff wurde möglicherweise durch fehlende Sicherheitsupdates oder eine großzügige Rechtevergabe begünstigt. Gewöhnlich nutzen Angreifer auch nicht veröffentlichte Sicherheitslücken („Zero Day Exploits“). Laut dem

Verfassungsschutzbericht für 2016 erfolgten Infektionen mit „Uroburos“ meist über sogenannte Watering-Hole-Attacken, bei denen Angreifer Webpräsenzen, die für das Opfer potenziell interessant sind, auf infizierte Webserver umleiten. Werden die Seiten aufgerufen, erfolgt die Installation der Schadsoftware bei dem Opfer des Cyberangriffs.

Die ausgewählten Betroffenen seien auf einer sogenannten White-List gespeichert. In der Süddeutschen Zeitung vom 6. März 2018 heißt es dazu, die Angreifer hätten das Mailprogramm Microsoft Outlook genutzt, um dort codierte Befehle in einem Mail-Anhang zu verstecken. Der betroffene Rechner war demnach bereits mit Schadsoftware infiziert. Über Outlook sollen die Dokumente schließlich auch ausgeleitet worden sein.

Infiziert worden sei zunächst die Liegenschaftsverwaltung des Außenministeriums, danach ein Referat mit Russlandbezug. Im Januar 2017 habe die Malware einen Steuerbefehl erhalten und begonnen, Informationen an einen nicht näher benannten Server auszuleiten. Im März hätten die Angreifer dann Administrator-Rechte auf Windows-Clients im Auswärtigen Amt erlangt.

Erst kurz vorher wurden die dortigen Linux-Systeme zu Windows und Microsoft migriert (Drucksache 18/4473). Einen der Rechner habe ein Mitarbeiter des Bundesverteidigungsministeriums genutzt. Das Verteidigungsministerium soll deshalb entgegen erster Informationen nicht direkt betroffen gewesen sein.



Der IT-Angriff hat nach derzeitigem Stand keinen großen Schaden angerichtet. Im IVBB werden keine vertraulich oder geheim eingestuft Dokumente verteilt („Regierungspressekonferenz vom 2. März 2018“, [bundesregierung.de](http://bundesregierung.de)). Die Rede ist von sechs abgeflossenen Dokumenten, die zum Teil „Bezüge zu Russland, der Ukraine und Weißrussland“ hätten. Ein Mitarbeiter des Innenministeriums erklärte im Ausschuss für Verkehr und digitale Infrastruktur, das Parlament und die Öffentlichkeit sei nicht früher über den Vorfall informiert worden, um die Angreifer weiter beobachten und rückverfolgen zu können. Die an die Presse geleakten Informationen hätten die weitere Aufklärungsarbeit zwangsläufig beendet. Die Bundesanwaltschaft hat deshalb Vorermittlungen auf der Suche nach der undichten Stelle begonnen („Bundesanwaltschaft nimmt Vorermittlungen auf“, [haz.de](http://haz.de) vom 2. März 2018). Nicht auszuschließen sei, dass die Veröffentlichungen dafür sorgten, dass die Angreifer Spuren löschen konnte.

In der Vergangenheit will die Bundesregierung täglich 20 „hoch spezialisierte Cyberangriffe“ festgestellt haben, von denen nach Einschätzung des BSI einer pro Woche „einen nachrichtendienstlichen Hintergrund“ gehabt hätte (Drucksache 18/11106, Frage 18).

Für die Einstufung als „hoch spezialisierter Cyberangriff“ genügt es jedoch, wenn eine Schadsoftware die Virens Scanner des BSI überwinden kann. In keinem der Fälle konnte der vermutete „nachrichtendienstliche Hintergrund“ bestätigt oder gar nachweislich einer Regierung zugeordnet werden.

Trotzdem will die Bundesregierung die rechtlichen und technischen Fähigkeiten zu digitalen Gegenschlägen ausweiten („Hacking back? Technische und politische Implikationen digitaler Gegenschläge“, SWP-Aktuell 59, August 2017). Der Bundessicherheitsrat soll hierzu eine Analyse der benötigten technischen Fähigkeiten vornehmen und der Regierung Vorschläge für notwendige gesetzliche Änderungen vorlegen.

Solche „Hackbacks“ könnten laut dem Chef der neuen Entschlüsselungsbehörde des Bundes (ZITiS) helfen, „entwendete Dateien und Dokumente zumindest auf den Servern der Diebe zu löschen“ („Entschlüsselungsbehörde - Staat muss digital zurückschlagen können“, [de.reuters.com](http://de.reuters.com) vom 22. November 2018). Auch im Koalitionsvertrag von Union und SPD heißt es, man wolle „Angriffe aus dem Cyberraum gegen unsere kritischen Infrastrukturen abwehren und verhindern“.

#### 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 3, 5a, 5c, 5e bis 5g, 10, 10a, 10b, 13, 17 und 16 nicht vollständig in offener Form erfolgen kann.

Die erbetenen Auskünfte zu den Fragen 5a, 5c, 5e bis 5g und 16 sind 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 Details operativer Maßnahmen und erlauben potentiellen Angreifern Rückschlüsse auf die Fähigkeiten und das Vorgehen deutscher Behörden. Hierzu zählen Einzelheiten zu der Erkenntnislage der Behörden über das Vorgehen und die Fähigkeiten des Angreifers. Die Veröffentlichung dieser Erkenntnisse ließe Rückschlüsse auf die Aufklärungsschwerpunkte zu und würde die zukünftige Aufgabenerfüllung der beteiligten Behörden und damit die Gewährleistung der IT-Sicherheit gefährden. Diese würde zukünftige Angriffe erleichtern.

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 - insbesondere nachrichtendienstlicher - Informationsbeschaffung durch den Einsatz spezifischer Fähigkeiten und damit dem Staatswohl. Auch 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 Informationsverbundes Bonn-Berlin (IVBB) und damit dem Staatswohl.

Daher sind die Antworten zu den genannten Fragen als Verschlussache nach § 4 Absatz 2 Sicherheitsüberprüfungsgesetz in Verbindung mit der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlussachen (VS-Anweisung – VSA) mit dem Geheimhaltungsgrad „GEHEIM“ eingestuft und können bei der Geheimschutzstelle des Deutschen Bundestages eingesehen werden.

Die Auskünfte zu den Fragen 3 und 13 sind geheimhaltungsbedürftig, weil die Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland nachteilig sein kann. Eine öffentliche Zuordnung von Angriffskampagnen zu ausländischen Diensten bedarf einer sorgfältigen Abwägung. Daher könnte eine vollständige offene Beantwortung hinsichtlich der konkreten Attribution für die auswärtigen Beziehungen der Bundesrepublik schädlich sein.



Ferner könnte eine öffentliche Auskunft Dritten Erkenntnisse über Analysefähigkeiten von Sicherheitsvorfällen ermöglichen. 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. Daher sind die Antworten zu den genannten Fragen als Verschlussache nach § 4 Absatz 2

Sicherheitsüberprüfungsgesetz in Verbindung mit der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlussachen (VS-Anweisung – VSA) mit dem Geheimhaltungsgrad „VS-NUR FÜR DEN DIENSTGEBRAUCH“ eingestuft.

Ferner sind die erbetenen Auskünfte zu den Fragen 10, 10a, 10b und 17 geheimhaltungsbedürftig, weil die Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland nachteilig sein kann. Details zu den IT-Systemen der Bundesregierung sind schützenswerte Informationen, deren Bekanntwerden die Cybersicherheit dieser Systeme in ihrer Wirkung schwächen würde. Daher sind die Antworten zu den genannten Fragen als Verschlussache nach § 4 Absatz 2

Sicherheitsüberprüfungsgesetz in Verbindung mit der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlussachen (VS-Anweisung – VSA) mit dem Geheimhaltungsgrad „VS-NUR FÜR DEN DIENSTGEBRAUCH“ eingestuft.

Frage 1:

*Wie viele „hoch spezialisierte Cyberangriffe“ stellt das BSI in 2016 und 2017 im Durchschnitt täglich im IVBB und im Bundestagsnetz fest, bei denen es als Einstufung genügt, dass die Virens Scanner die Schadsoftware übersehen (Drucksache 18/11106, Frage 18)?*

Frage 2:

*In wie vielen der Fälle wurde dabei ein „nachrichtendienstliche Hintergrund“ angenommen und in wie vielen Fällen wurde dieser bestätigt oder gar nachweislich einer Regierung zugeordnet?*

Antwort zu Frage 1 und 2:

Für die Beantwortung der Fragen wird auf die Berichte des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur IT-Sicherheit in Deutschland von 2016 und 2017 verwiesen.

Diese sind unter den Adressen

[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2016.pdf?\\_\\_blob=publicationFile&v=5](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2016.pdf?__blob=publicationFile&v=5) und

[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf?\\_\\_blob=publicationFile&v=4\\_abrufbar](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf?__blob=publicationFile&v=4_abrufbar).

Gemäß Bericht des BSI zur Lage der IT-Sicherheit in Deutschland 2016 wurden im Berichtszeitraum Juli 2015 bis Juni 2016 täglich über 400 Cyberangriffe detektiert, die mit kommerziellen Sicherheitsprodukten nicht erkannt worden wären. Gerechnet auf Kalenderjahre, lag die durchschnittliche Anzahl täglicher Angriffe in 2016 darüber, während sie in 2017 etwas geringer ausfiel.

Der Rückgang der Zahlen resultiert u.a. aus einer stärkeren Vorfilterung durch vorgelagerte Systeme, die nicht in diese Statistik eingeht. Eine exakte Differenzierung und Attribution von hoch spezialisierten Cyberangriffen findet nicht in jedem Fall statt und ist auch nicht zielführend, da dies zur Abwehr des Angriffes nicht immer erforderlich ist und gegen den jeweils entstehenden Aufwand abgewogen werden muss.

Im Übrigen wird auf die Antwort der Bundesregierung zu Frage 17 der Kleinen Anfrage der Fraktion DIE LINKE. auf BT-Drs. 18/11106 vom 8. Februar 2017 verwiesen. Die dort getätigten Ausführungen gelten auch für das Jahr 2017 fort.

Frage 3:

*Welchem russischen Geheimdienst ordnet die Bundesregierung die „Cyberangriffskampagne APT 28“ zu (Drucksache 18/13667, Frage 12 des MdB Andrej Hunko)?*

- a) *Welche „Hinweise“ auf eine Spear-Phishing-Angriffswelle auf mehrere politische Parteien auf Bundes- und Landesebene wurden im August 2016 bekannt?*
- b) *Aus welchen Erwägungen oder nach welchen „Indizien“ wurden zurückliegende „Angriffsversuche“ dem Netzwerk „APT 28“ zugerechnet und welche „nachrichtendienstlichen Erkenntnisse“ lagen hierzu vor (18/11106, Frage 18; bitte die „Indizien“ ausführen)?*
- c) *Welche „Angriffsvorbereitungen“ konnten im Februar 2017 „erfolgreich verhindert werden“?*

- d) *Welche „Cyberangriffe“ erfolgten anschließend auf Netzwerke politischer Stiftungen und inwiefern handelte es sich dabei lediglich um den Versand von Spear- Phishing-Mails?*
- e) *Aus welchen Erwägungen oder nach welchen Indizien wurden diese Vorfälle von den deutschen Sicherheitsbehörden „als mögliche Vorbereitungshandlungen für Versuche einer Einflussnahme auf die Bundestagswahl angesehen“, die nach Kenntnis der Fragestellerinnen und Fragesteller schließlich nie erfolgte oder nachgewiesen werden konnte?*

Antwort zu Frage 3:

APT 28 wird verbreitet einem staatlichen russischen Akteur zugeordnet. Auf den „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß Vorbemerkung der Bundesregierung wird verwiesen.

Antwort zu Frage 3a:

Im August 2016 erhielt die Bundesregierung Hinweise auf Spear-Phishing-Angriffe gegen mehrere politische Parteien. Nach Kenntnis der Bundesregierung waren diese nicht erfolgreich.

Antwort zu Frage 3b:

Indizien beziehen sich insbesondere auf die bei zurückliegenden Angriffen genutzten technischen Infrastrukturen, die bereits von anderen Angriffen der APT 28-Kampagne bekannt sind.

Antwort zu Frage 3c:

Die Vorbereitung von Phishing-Angriffen auf eine deutsche Partei konnten verhindert werden. In diesem Zusammenhang erhielt das Bundesamt für Verfassungsschutz (BfV) den Hinweis auf eine kurz zuvor registrierte Domain, die eine legitime Seite einer deutschen Partei imitierte. Die betroffene Partei wurde unverzüglich über den Sachverhalt informiert.

Antwort zu Frage 3d:

Anfang März 2017 erlangte das BfV Kenntnis von einem Spear-Phishing-Angriff auf das Netzwerk der Konrad-Adenauer-Stiftung.

Zudem identifizierte das BfV Anfang April 2017 eine kurz zuvor registrierte Domain, bei der davon auszugehen war, dass sie für Credential-Phishing-Angriffe gegen die Friedrich-Ebert-Stiftung angelegt wurde. Hierzu hatten Mitarbeiter der Stiftung Spear-



Phishing-Mails von dieser Domain als nachgeahmte Login-Seite erhalten, mit dem Ziel, auf diese Weise die Zugangsdaten dieser Mitarbeiter abzugreifen.

Antwort zu Frage 3e:

Bereits im Vorfeld der US-amerikanischen Präsidentschaftswahlen im Sommer 2016 war APT 28 entsprechend aktiv gewesen. Zudem sprachen zunehmende Cyberangriffe auf den Deutschen Bundestag, Parteien und politische Stiftungen seit Mitte 2016 für eine solche Einschätzung.

Frage 4:

*Handelt es sich bei dem jüngsten Angriff auf das deutsche Regierungsnetz nach Auffassung der Bundesregierung um einen Vorgang von besonderer Bedeutung gemäß § 4 Abs. 1 PKGr und bitte begründen Sie diese Auffassung? Falls ja, wurde das PKGr umgehend unterrichtet oder wer entschied, vorerst von einer Unterrichtung abzusehen?*

Antwort Frage 4:

Gemäß § 6 Absatz 2 des Gesetzes über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (PKGrG) kann die Bundesregierung von einer Unterrichtung nach § 4 Absatz 1 PKGrG absehen, wenn der Kernbereich der exekutiven Eigenverantwortung betroffen ist. Dies war bei der operativen Bewältigung des Angriffes auf Teile des Kommunikationsnetzes der Bundesregierung der Fall. In dem Zeitraum zwischen der ersten Kenntnisnahme und dem öffentlichen Bekanntwerden des Vorfalls stellte das Tätigwerden der Sicherheitsbehörden ein laufendes Verfahren dar, indem es einerseits darum ging, genug Erkenntnisse über die Angriffsvektoren und Informationen für den Schutz im IVBB zu sammeln und ein Konzept für die sichere und nachhaltige Bereinigung der IT-Systeme auszuarbeiten. Darüber hinaus war die interne Willensbildung der Bundesregierung zum Umgang mit dem laufenden Angriff auch wegen des andauernden Erkenntnisgewinns noch nicht vollständig abgeschlossen. Von einer Unterrichtung gemäß § 4 Absatz 1 PKGrG bis zum öffentlichen Bekanntwerden wurde aus diesen Gründen abgesehen. Auf das Vorliegen eines Vorganges besonderer Bedeutung gemäß § 4 Absatz 1 PKGrG kommt es daher nicht an. Das Parlamentarische Kontrollgremium (PKGr) wurde nach dem öffentlichen Bekanntwerden unverzüglich unterrichtet.

Frage 5:

*Welche IT-Systeme und welche Ministerien bzw. nachgelagerte Bundesbehörden waren von dem am 28. Februar 2018 bekannt gewordenen IT-Angriff nach derzeitigem Stand betroffen?*

- a) Welche der dabei genutzten Angriffsinfrastruktur (insbesondere die Nutzung von Outlook und bekannter Server zum Ausleiten der Dokumente) ist bereits bei anderen Angriffen gegen Einrichtungen des Bundes festgestellt worden (Drucksache 18/11106, Frage 1)?*
- b) Welche Schadsoftware wurde nach derzeitigem Stand bei dem Angriff genutzt?*
- c) Wann und wo genau ist die Kompromittierung des IVBB erfolgt und welchen Weg nahm die Schadsoftware?*
- d) Inwiefern wurden bei dem Angriff nach derzeitigem Stand der Ermittlungen Webpräsenzen, die für das Opfer potenziell interessant sind, auf infizierte Webserver umgeleitet?*
- e) Wann erhielten die Angreifer Administrator-Rechte auf den Web-Clients im Auswärtigen Amt?*
- f) Wann erhielt die Schadsoftware einen Steuerbefehl und begann, Informationen auszuleiten und welche Server wurden hierfür genutzt?*
- g) Wann wurde der Angriff endgültig unter Kontrolle gebracht und die Schadsoftware aus dem IVBB entfernt? Ist die Bundesregierung sich sicher, dass die Schadsoftware vollständig entfernt wurde und kann ausschließen, dass sich Teile davon noch im IVBB Netz befinden?*
- h) Für welchen Zeitraum werden im IVBB Vorratsdaten gespeichert und welche Logfiles des in Rede stehenden Angriffs stehen ab welchem Datum für Analysen und Ermittlungen zur Verfügung?*

Antwort zu Frage 5:

Betroffen waren IT-Systeme beim Auswärtigen Amt (AA) und bei der Hochschule des Bundes (HS Bund).

Zu den Fragen 5a, 5c und 5e bis 5g wird auf die VS-„GEHEIM“ eingestufteten Antworten gemäß der Vorbemerkung der Bundesregierung verwiesen.

Antwort zu Frage 5b:

Es wurden diverse Werkzeuge bei diesem Angriff genutzt, die größtenteils speziell für diesen Angriff angefertigt worden sein dürften.



Antwort zu Frage 5d:

Nach dem derzeitigen Stand der Analysen wurden keine Webpräsenzen auf infizierte Webserver umgeleitet.

Antwort zu Frage 5h:

Nach § 5 Absatz 2 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) dürfen Protokolldaten für die automatisierte Auswertung längsten für drei Monate gespeichert werden. Eine darüber hinausgehende Verwendung personenbezogener Daten ist nach § 5 Absatz 3 BSIG vom Einzelfall abhängig. Nach § 2 Absatz 8 BSIG sind Protokolldaten im Sinne dieses Gesetzes Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung, die unabhängig vom Inhalt eines Kommunikationsvorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden und zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind. Protokolldaten können Verkehrsdaten gemäß § 3 Nummer 30 des Telekommunikationsgesetzes und Nutzungsdaten nach § 15 Absatz 1 des Telemediengesetzes enthalten.

Im Übrigen sind personenbezogene Daten, welche das BSI im Rahmen seiner Befugnisse erhebt, nach § 6 BSIG unverzüglich zu löschen, sobald sie für die Erfüllung der Aufgaben, für die sie erhoben worden sind, oder für eine etwaige gerichtliche Überprüfung nicht mehr benötigt werden. Für die technischen Analysen des vorliegenden Falles standen dem BSI Protokolldaten nach § 5 Absatz 2 BSIG beginnend ab September 2017 zur Verfügung.

Frage 6:

*Inwiefern war das beim Bundesverwaltungsamt geführte und vom Bundeskriminalamt genutzte Passagierdatensystem in der Vergangenheit von IT-Sicherheitsvorfällen betroffen (bitte jeweils ausführen)?*

- a) *Aus welchen Gründen wurde das System wie berichtet abgeschaltet („Hacker sollen Dokumente zu Brexit und Ukraine entwendet haben“, zeit.de vom 10. März 2018, bitte mitteilen ob vorab nicht nur „Belastungstests“, sondern auch Penetrationstests durchgeführt wurden)?*
- b) *Welche Ergebnisse ergaben diese Tests jeweils mit Blick auf ihre Sicherheit?*

Antwort zu Frage 6, 6a und 6b:

Die Fragen 6, 6a) und 6b) werden gemeinsam beantwortet. Das System zur Fluggastdatenspeicherung wird zurzeit im Bundesverwaltungsamt (BVA) getestet. Der Wirkbetrieb wird vorbereitet. Vor Aufnahme des Wirkbetriebs werden entsprechende Penetrationstests durch das BSI durchgeführt. Die Ergebnisse dieser Tests des BSI werden derzeit von BVA und Informationstechnikzentrum Bund (ITZBund) ausgewertet. Ein Cyber-Angriff, wie teilweise in der Presse berichtet wurde, hat nicht stattgefunden.

Frage 7:

*In welchen Fällen war die Lernplattform „Ilias“, die an der Hochschule des Bundes zu Weiterbildungszwecken genutzt wird, in der Vergangenheit von IT-Sicherheitsvorfällen betroffen („Hack auf Bundesregierung erfolgte über Lernplattform Ilias“, golem.de vom 8. März 2018)?*

- a) *Kann die Bundesregierung bestätigen, dass der Standardaccount mit Administratorrechten mit dem Passwort „homer“ angelegt wurde?*
- b) *Wenn nein, welches war das Passwort bei der Erstanlage? Inwiefern kann die Bundesregierung sicherstellen, dass jedes dieser Initialpasswörter nach Installation sofort auf ein anderes Passwort geändert wurde?*
- c) *Inwiefern trifft es zu, dass „Ilias“ seit März 2017 in der Version 5.1.16 betrieben wurde, obwohl es danach mehrere Sicherheitsupdates gegeben hat?*
- d) *Welche Sicherheitslücken wurden durch die verzögerte Installation von Sicherheitsupdates ermöglicht (etwa Cross-Site-Scripting oder die Behandlung von Mediendateien)?*
- e) *Was ist der Bundesregierung darüber bekannt, wann genau die Version 5.1.16 eingespielt wurde und inwiefern der aktuelle IT-Sicherheitsvorfall davon profitierte, dass eine erst damit geschlossene Sicherheitslücke das Kopieren von Dateien an beliebige Stellen im Dateisystem ermöglichte?*

Antwort zu Frage 7:

Der Bundesregierung ist nicht bekannt, dass die Lernplattform ILIAS, die an der HS Bund genutzt wird, in der Vergangenheit von anderen als dem in Rede stehenden Sicherheitsvorfall betroffen war.



Antwort zu Frage 7a:

Nein, die Bundesregierung kann nicht bestätigen, dass der Standardaccount mit Admin-Rechten mit dem Passwort „homer“ angelegt war.

Antwort zu Frage 7b:

Es wurde ein Initialpasswort gemäß den Passwortrichtlinien des BSI verwendet. Die Änderungen des Initialpassworts nach Installation ist ein Standardverfahren bei der HS Bund entsprechend der Dienstanweisung für die Benutzung von Informationstechnik.

Antwort zu Frage 7c:

Die Lernplattform ILIAS wurde in der Version 5.1.16 ab Dezember 2016 bei der HS Bund eingesetzt. Alle notwendigen Sicherheitspatches wurden unverzüglich installiert.

Antwort zu Frage 7d:

Auf die Antwort zu Frage 7c wird verwiesen.

Antwort zu Frage 7e:

Am 20. Dezember 2016 wurde die Version 5.1.16 installiert. Im Übrigen sind die technischen Analysen des Vorfalles noch nicht abgeschlossen.

Frage 8:

*Welche deutschen Geheimdienste oder Ministerien wurden wann von welchem „ausländischen Partner“, der möglicherweise aus dem Baltikum kommt, über den Angriff informiert?*

Antwort zu Frage 8:

Die Bundesregierung wurde am 18. Dezember 2017 durch einen Partnerdienst unterrichtet. Im Übrigen ist die Auskunft zu der Frage geheimhaltungsbedürftig, weil die Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland nachteilig sein kann. Eine öffentliche Mitteilung, welche deutschen Nachrichtendienste oder Ministerien wann von einem „ausländischen Partner“ informiert wurden, ließe Rückschlüsse auf deren Aufklärungsschwerpunkte und Informationsgewinnung zu.

Dies könnte zu einer wesentlichen Schwächung der Informationsgewinnung und Aufklärungsmöglichkeiten führen und daher die Sicherheit der Bundesrepublik Deutschland nachhaltig gefährden.

Daher ist die Antwort insoweit als Verschlussache nach § 4 Absatz 2 Sicherheitsüberprüfungsgesetz in Verbindung mit der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlussachen (VS-Anweisung – VSA) mit dem Geheimhaltungsgrad „VS-NUR FÜR DEN DIENSTGEBRAUCH“ eingestuft.

Frage 9:

*Von welchen Ministerien, nachgelagerten Bundesbehörden oder Abteilungen wurde die Information über den laufenden Angriff nach derzeitigem Stand der Ermittlungen an die dpa weitergegeben und inwiefern konnte die Bundesregierung analysieren, ob die Veröffentlichungen dafür sorgten, dass die Angreifer Spuren löschen konnten?*

Antwort zu Frage 9:

Der Bundesregierung liegen keine Erkenntnisse vor, wie die Informationen an die dpa gelangt sind. Im Übrigen ist die technische Analyse des Vorfalles noch nicht abgeschlossen.

Frage 10:

*Welchen Schaden hat der Angriff nach derzeitigem Stand der Analyse angerichtet und welche Dokumente wurden kopiert?*

- a) *Welches „Referat mit Russlandbezug“ ist von dem Vorfall betroffen?*
- b) *Worin bestehen die „Bezüge zu Russland, der Ukraine und Weißrussland“, die den sechs kopierten Dokumenten zugeschrieben werden, und zu welchen weiteren Ländern hatten diese „Bezüge“?*

Antwort zu Frage 10, 10a und 10b:

Die Fragen 10, 10a) und 10b) werden gemeinsam beantwortet. Auf die „VS - NUR FÜR DEN DIENSTGEBRAUCH“ eingestufte Antwort gemäß Vorbemerkung der Bundesregierung wird verwiesen.



Frage 11:

*Welche Bundesbehörden (auch die Bundesanwaltschaft) ermitteln zu dem Vorfall und damit im Zusammenhang stehenden Fragen, und wie sind die Zuständigkeiten geregelt?*

Antwort zu Frage 11:

Der Generalbundesanwalt hat am 15. März 2018 ein Ermittlungsverfahren wegen des Verdachts der geheimdienstlichen Agententätigkeit gegen Unbekannt eingeleitet und das Bundeskriminalamt mit den polizeilichen Ermittlungen beauftragt. Die Ermittlungen dauern an. Die Zuständigkeiten sind gesetzlich geregelt.

Frage 12:

*Inwiefern kann die Bundesregierung die in den Medien vermutete Urheberschaft der in Russland verorteten Netzwerke „APT28“ oder „Snake“ bestätigen oder nicht bestätigen? Für wie sicher wird die Zuschreibung gehalten?*

Antwort zu Frage 12:

Modus Operandi, technische Merkmale sowie deren Opferflächen sprechen nach bisherigen Erkenntnissen der zuständigen Bundesbehörden mit hoher Wahrscheinlichkeit für die in der Frage vermutete Urheberschaft.

Frage 13:

*Welchem russischen Geheimdienst kann „Snake“ aus Sicht der Bundesregierung zugeordnet werden?*

Antwort zu Frage 13:

Hinweise deuten nach Expertenmeinungen auf den russischen Inlandsdienst FSB. Auf den „VS - NUR FÜR DEN DIENSTGEBRAUCH“ eingestuften Antwortteil gemäß Vorbemerkung der Bundesregierung wird verwiesen.

Frage 14:

*Seit wann ist dem Bundesinnenministerium der Trojaner „Uroburos“ bekannt und welche Vorkehrungen wurden für entsprechende Angriffe getroffen?*

- a) *Welche deutschen Netzwerke „von Behörden, Firmen und Forschungseinrichtungen“ wurden nach Kenntnis der Bundesregierung mit „Uroburos“ infiltriert bzw. welche Versuche sind hierzu bekannt (Verfassungsschutzbericht von 2016; sofern keine Details oder Zahlen der Angriffe mitgeteilt werden können, bitte deren Größenordnung angeben)?*
- b) *Aus welchen Quellen nimmt das BfV die Informationen, dass von „Uroburos“ bzw. „Snake“ insbesondere die Bereiche Energietechnik, Röntgen- und Nukleartechnologie, Messtechnologie sowie Luft- und Raumfahrt ausgeforscht würden?*
- c) *Welche technischen Details sind der Bundesregierung zur Software „Uroburos“ bekannt?*
- d) *Welche Dateisysteme kann „Uroburos“ infiltrieren und wie verbreitet sich die Malware?*

Antwort zu Frage 14:

Der genannte Trojaner ist dem BSI unter anderem Namen mindestens seit Sommer 2012 bekannt. Das BSI pflegt regelmäßig Signaturen zur Erkennung dieser und ähnlicher Angriffe in die Schutzsysteme des IVBB ein und tauscht sich dazu mit Partnern aus. Für die Reaktion auf solche Angriffe wurde u.a. das Mobile Incident Response Team (MIRT) eingerichtet.

Antwort zu Frage 14a:

Zu den deutschen Zielen gehörten das Regierungsnetz, Auslandsvertretungen in westlichen Staaten, mehrere Schulen und Hochschulen sowie Forschungsinstitute. Die bekannten Angriffe bewegen sich im oberen zweistelligen Bereich.

Antwort zu Frage 14b:

Diese Informationen ergeben sich aus dem an der Opferauswahl erkennbaren Aufklärungsinteresse des Angreifers. Zudem sind Opfer aus diesen Bereichen in entsprechenden Berichten von IT-Sicherheitsunternehmen beschrieben.

Antworten zu den Fragen 14c und 14d:

Die Fragen 14c) und 14d) werden gemeinsam beantwortet. Bei der Software „Uroburos“ handelt es sich um eine hochkomplexe Schadsoftware, deren Besonderheit darin liegt, sich unerkannt in Netzwerken über längere Zeit zu bewegen und die in der Lage ist sämtliche Dateisysteme zu befallen.

Frage 15:

*Inwiefern ist die von BfV und BND eingerichtete „temporäre Arbeitseinheit“ zur Prüfung, „ob die russische Regierung mit geheimdienstlichen Mitteln die politische Debatte und die öffentliche Meinung in Deutschland zu beeinflussen versucht“, weiterhin existent (Drucksache 18/10759, Frage 8)?*

- a) *Welche wesentlichen Ergebnisse schildert der Bericht, den die Bundesregierung beim BND und beim BfV zu vermeintlich russischen Aktivitäten im Cyberraum beauftragt hatte, zu denen es heißt die Bundesregierung habe diesen Bericht „zur Kenntnis genommen“ (Bundestagsdrucksache 18/11106, Frage 7)?*
- b) *Hinsichtlich welcher weiterer Regierungen außer den in der Beantwortung der Kleinen Anfragen auf Bundestagsdrucksachen 18/11106, 18/8631 und 18/10759 genannten Regierungen hat das BfV „Anwerbeversuche“ der „Mitarbeiter [deutscher] Parlamentarier oder politischer Stiftungen“ beobachten können?*

Antwort zu Frage 15:

Die Aufgabe der innerhalb des BfV eingerichteten temporären Arbeitseinheit wurde inzwischen in den zuständigen Fachbereich des BfV überführt. Im Bundesnachrichtendienst (BND) wird die Thematik weiterhin in mehreren Arbeitsbereichen/Abteilungen bearbeitet. Eine gemeinsame temporäre Arbeitseinheit von BfV und BND bestand nicht (vgl. BT-Drs. 18/10759; Antworten zu Fragen 7 und 8).

Antwort zu Frage 15a:

Auf die Antwort der Bundesregierung zu den Fragen 7, 7a und 7 c der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/11106 vom 8. Februar 2017 wird verwiesen. Im Übrigen wurde der Bericht - anders als von den Fragestellern dargestellt - nicht zu vermeintlich russischen Aktivitäten im Cyberraum in Auftrag gegeben, sondern hatte die Prüfung zum Ziel, ob die russische Regierung mit geheimdienstlichen Mitteln die politische Debatte und die öffentliche Meinung in Deutschland zu beeinflussen versucht.

Antwort zu Frage 15b:

Neben Angehörigen der russischen Nachrichtendienste unterhalten auch Angehörige weiterer Nachrichtendienste Kontakt zu politischen Stiftungen. In diesem Zusammenhang hat das BfV Anwerbungsversuche von Mitarbeiterinnen und Mitarbeitern verschiedener Fraktionen des Deutschen Bundestages sowie von politischen Stiftungen durch Angehörige chinesischer Nachrichtendienste beobachten können.



Frage 16:

*Inwiefern könnte der am 28. Februar bekannt gewordene Angriff nach derzeitigem Stand der Analyse durch fehlende Sicherheitsupdates oder eine großzügige Rechtevergabe begünstigt worden sein und wie ist hierzu im Auswärtigen Amt verfahren worden?*

Antwort zu Frage 16:

Der Bundesregierung liegen hierzu noch keine abschließenden Erkenntnisse vor, da die technische Analyse des Vorfalles noch nicht abgeschlossen ist.

Im Übrigen wird auf den „VS-GEHEIM“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.

Frage 17:

*Inwiefern hätte der Angriff nach derzeitigem Stand der Analyse verhindert werden können, wenn das Auswärtige Amt nicht bis 2015 komplett auf Windows XP und Windows 7 umgestiegen wäre (Drucksache 18/4473)?*

Antwort zu Frage 17:

Auf die „VS - NUR FÜR DEN DIENSTGEBRAUCH“ eingestufte Antwort gemäß Vorbemerkung der Bundesregierung wird verwiesen.

Frage 18:

*Wie viele E-Mails, die Schadsoftware enthielten, wurden im IVBB in den Jahren 2016 und 2017 abgefangen?*

Frage 19:

*Wie viele Verbindungen zu Webseiten, die Schadsoftware enthielten, wurden im IVBB in den Jahren 2016 und 2017 unterbunden?*

Antworten zu Frage 18 und Frage 19:

Die Fragen 18 und 19 werden gemeinsam beantwortet. Für die Beantwortung der Fragen wird auf die Berichte des BSI zur IT-Sicherheit in Deutschland von 2016 und 2017 verwiesen.

Diese sind unter den Adressen

[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2016.pdf?\\_\\_blob=publicationFile&v=5](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2016.pdf?__blob=publicationFile&v=5) und

[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf?\\_\\_blob=publicationFile&v=4](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf?__blob=publicationFile&v=4) abrufbar.

Hiernach wurden im Berichtszeitraum 2016 monatlich ca. 44 Tsd. und 2017 monatlich ca. 52 Tsd. mit Schadcode infizierte E-Mails in den Regierungsnetzen abgefangen. Ferner wurden im Berichtszeitraum 2016 täglich ca. 3600 und 2017 täglich ca. 5200 Verbindungsversuche aus den Regierungsnetzen zu Schadcodeservern blockiert.

Frage 20:

*Inwiefern könnten die Angreifer nach derzeitigem Stand der Analyse nicht veröffentlichte Sicherheitslücken („Zero Day Exploits“) genutzt haben und inwiefern ist es dem BSI überhaupt möglich, hierzu am Ende der Analyse und Ermittlungen mit endgültiger Klarheit Aussagen zu treffen?*

Antwort zu Frage 20:

Hierzu liegen der Bundesregierung derzeit keine Erkenntnisse vor. Die Bundesregierung geht davon aus, dass das Ergebnis der technischen Analysen Aufschluss über das Vorgehen des Angreifers geben wird. Sogenannte „Zero Day Exploits“ zeichnen sich jedoch dadurch aus, dass die Schwachstelle i. d. R. nicht bekannt ist und daher erst nach Bekanntwerden durch einen Fix geschlossen werden kann. Es kann daher bei Cyberangriffen nie mit an Sicherheit grenzender Wahrscheinlichkeit ausgeschlossen werden, ob auch sogenannte „Zero Day Exploits“ ausgenutzt wurden.

Frage 21:

*Was kann die Bundesregierung über den Fortgang eines deutschen Prozesses mitteilen, in den Überlegungen zur Nutzung von Schwachstellen (sogenannten Exploits bzw. Zero Day Exploits) durch Strafverfolgungsbehörden oder Geheimdienste münden sollen (Drucksache 18/13696, Frage 25 des MdB Andrej Hunko)?*

- a) *Welche Kriterien müssten aus Sicht der Bundesregierung beispielsweise erfüllt sein, damit entschieden würde, dass eine gefundene Schwachstelle lieber nicht durch die Behörden ausgenutzt wird, sondern die Hersteller und Betreiber der Systeme gewarnt werden, damit sie diese schließen können?*

- b) *Sofern die Meinungsbildung innerhalb der Bundesregierung hierzu immer noch nicht abgeschlossen ist, wann kann sie zur Frage möglicher „Stufen eines Prozesses“ und zu möglichen „Kriterien“ eine Aussage treffen?*

Antwort zu Frage 21:

Auf die Antwort der Bundesregierung zur Schriftlichen Frage des Abgeordneten Hunko auf BT-Drs. 18/13696, Nr. 25 vom 23. Oktober 2017 wird verwiesen. Es ist derzeit auch nicht absehbar, wann die Meinungsbildung innerhalb der Bundesregierung hierzu abgeschlossen sein wird.

Frage 22:

*Mit welchen russischen Behörden arbeiten welche Bundesbehörden im Bereich der Cybersicherheit oder der Abwehr von IT-Angriffen regelmäßig in technischen, operativen und strategischen Fragen zusammen?*

Antwort zu Frage 22:

In den Jahren 2016 und 2017 führte die Bundesregierung ressortübergreifende Cybersicherheitskonsultationen mit Russland, die der Vertrauensbildung und der strategischen Zusammenarbeit dienen sollten. Darüber hinaus besteht keine Zusammenarbeit von Bundesbehörden mit russischen Behörden im Sinne der Fragestellung.

Frage 23:

*Sofern der am 28. Februar bekanntgewordene Angriff einem Staat zugerechnet werden kann, nach welcher Maßgabe hätte die Bundesregierung aus ihrer Sicht das Recht, diesen für sein Fehlverhalten zu sanktionieren?*

Antwort zu Frage 23:

In Fällen, in denen eine Cyber-Operation einem fremden Staat zugerechnet werden kann, richtet sich die Zulässigkeit von Gegenmaßnahmen nach dem innerstaatlichen Recht (zum Beispiel dem Gefahrenabwehrrecht) und dem Völkerrecht. Im Übrigen wird auf die Antwort zu Frage 12 verwiesen.

Frage 24:

*Aus welchen Erwägungen hält es die Bundesregierung für notwendig, die rechtlichen und technischen Fähigkeiten zu digitalen Gegenschlägen auszuweiten und welche Pläne wird sie hierzu verfolgen („Hacking back“? Technische und politische Implikationen digitaler Gegenschläge“, SWP-Aktuell 59, August 2017)?*



- a) *Welche Ergebnisse kann die Bundesregierung zu Analysen der hierzu benötigten technischen Fähigkeiten mitteilen und welche Vorschläge für notwendige gesetzliche Änderungen wurden hierzu ermittelt?*
- b) *Inwiefern sollten vor einem digitalen Gegenschlag zunächst internationale Rechtshilfeersuchen gestellt werden, um Angreifer zu ermitteln und die Behörden des zuständigen Landes zur Mitarbeit bei der Abwehr aufzufordern?*
- c) *Welche Behörden sollten aus Sicht der Bundesregierung mit Möglichkeiten digitaler Angriffe oder Gegenschläge ausgestattet werden?*
- d) *Über wie viele Mitarbeiterinnen und Mitarbeiter verfügt das vor einem Jahr bei der Bundeswehr gegründete Kommando „Cyber- und Informationsraum“ und welcher Personalbestand ist geplant?*
- e) *Auf welche Weise soll die Zusammenarbeit von Bund und Ländern bei der Cyberabwehr ausgebaut, verbessert und strukturell neu geordnet werden?*
- f) *Mit welchen Kompetenzen wird die Rolle des BSI diesbezüglich gestärkt und ist geplant, die Behörde unabhängig zu gestalten und die Nachordnung zum Bundesministerium des Innern aufzulösen, um Interessenskonflikte auszuschließen?*

Antwort zu den Fragen 24, 24a bis 24c:

Die Fragen 24 und 24a bis 24c werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Die Bundesregierung hat in der Cyber-Sicherheitsstrategie für Deutschland im Jahr 2016 die Feststellung getroffen (CSS 2016, Seite 29, abrufbar unter:

<https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/cyber-sicherheitsstrategie/cyber-sicherheitsstrategie-node.html>), 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 deswegen Prüfungen eingeleitet, unter welchen rechtlichen Rahmenbedingungen und mit welchen technischen Möglichkeiten in solchen Fällen durch staatliche Stellen Netzwerkoperationen durchgeführt werden können.

Der neue Koalitionsvertrag enthält zudem Aussagen, die auf einen Bedarf der Sicherheitsbehörden in Bezug auf gleichwertige Befugnisse im Umgang mit dem Internet wie außerhalb des Internets gerichtet sind.

Unter diesen Rahmenbedingungen werden die Prüfungen zu Maßnahmen einer (zivilen) aktiven Cyber-Abwehr fortgesetzt.

In die Prüfungen wird mit einbezogen, für welche Szenarien, in welcher Form und auf wessen Entscheidung zivile Maßnahmen der aktiven Cyber-Abwehr durchgeführt werden können.

Zudem fließen in die Prüfungen auch Fragen der Attributionsmöglichkeiten und der Verhältnismäßigkeit solcher Maßnahmen mit ein, ebenso wie das Bewusstsein, dass staatliche Stellen im Rahmen des geltenden Verfassungs- und Völkerrechts agieren müssen und unnötige Eskalationen zu vermeiden sind.

Jegliche Maßnahmen der aktiven Cyber-Abwehr sind einer sehr sorgfältigen rechtlichen und außenpolitischen Bewertung zu unterziehen.

Die Ergebnisse dieser Prüfungen sowie eine Entscheidung der Bundesregierung über den Rechtsetzungsbedarf liegen abschließend noch nicht vor.

Antwort zu Frage 24d:

Das Kommando Cyber- und Informationsraum (KdoCIR) wurde mit einem Startumfang von 258 Dienstposten (DP) am 1. April 2017 aufgestellt. Es wird nach derzeitigem Planungsstand mit Einnahme der Zielstruktur in 2021 ca. 700 DP umfassen. Mit Stichtag zum 3. April 2018 sind 326 DP besetzt.

Der Gesamtumfang des Organisationsbereichs Cyber- und Informationsraum soll im Jahr 2021 die Zielgröße erreichen und dann ca. 12.570 militärische und 1.880 zivile DP umfassen.

Antwort zu Frage 24e:

Cybergefahren und -angriffe sind i. d. R. nicht an Landesgrenzen gebunden. Eine enge Zusammenarbeit von Bund und Ländern ist daher zwingend erforderlich. Bund und Länder sind daher im kontinuierlichen Dialog, wie die Zusammenarbeit gestaltet und verbessert werden kann. So wurde u. a. auf der Herbst-IMK 2016 eine Steuerungs- und Bündelungsfunktion des Bundes beschlossen. Für die Sicherheit der IT der öffentlichen Verwaltung des Bundes und der Länder hat der IT-Planungsrat die IT-Sicherheitsleitlinie verabschiedet und schreibt diese regelmäßig fort.

Um eine noch engere Zusammenarbeit zwischen Bund und Ländern bei der Gefahrenbewertung und -bewältigung zu schaffen, beabsichtigt die Bundesregierung die Länder noch stärker in das weiterzuentwickelnde Cyberabwehrzentrum einzubinden.

Antwort zu Frage 24f:

Wie sich das Verhältnis von Bund und Ländern bei der Zusammenarbeit mit dem BSI konkret gestaltet, ist Gegenstand laufender Prüfung. Die Bundesregierung beabsichtigt nicht, das BSI als unabhängige Stelle einzurichten.