Deutscher Bundestag **Drucksache 19/1900**

19. Wahlperiode 26.04.2018

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Brigitte Freihold, Dr. André Hahn, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 19/1419 –

Reaktion der EU auf Cyberangriffe

Vorbemerkung der Fragesteller

In einem „Cybersicherheitspaket“ will die Europäische Union ihre „Reaktionsfähigkeit auf Cyberangriffe“ verbessern (Quelle hier und im Folgenden: Pressemitteilung sowie Factsheet der Europäischen Kommission vom 19. September 2017). Als neues „Instrument zur Verbesserung des Schutzes gegen Cyberangriffe“ plant die EU-Kommission unter anderem die Einrichtung einer „EU-Agentur für Cybersicherheit“, um die bislang existierende Abwehrfähigkeit und Reaktion der EU bei Cyberattacken zu verbessern, indem die bereits existierende Agentur für Netz- und Informationssicherheit (ENISA) „gestärkt“ wird und Mitgliedstaaten beim Umgang mit Cyberangriffen unterstützt werden. Hierzu soll die ENISA mit einem ständigen Mandat ausgestattet werden. Zusätzlich zu den regelmäßig abgehaltenen „EU-Cyberübungen“ soll auch die neue Agentur jährliche europaweite „Cybersicherheitsübungen“ durchführen. Wie in der Richtlinie über die Sicherheit von Netz- und Informationssystemen vorgesehen, soll die runderneuerte ENISA dafür sorgen, dass in jedem Mitgliedstaat „schwerwiegende Cybersicherheitsvorfälle“ einer nationalen Behörde gemeldet werden müssen.

Ebenfalls geplant ist die Einrichtung eines europäischen „Forschungs- und Kompetenzzentrums für Cybersicherheit“, ein entsprechendes „Pilotzentrum“, soll noch 2018 starten, um die Mitgliedstaaten bei der Entwicklung und Nutzung von „Instrumenten und Technik“ gegen die „immer neuen Bedrohungen“ zu unterstützen. Das Zentrum könnte außerdem „um eine Cyberabwehr-Abteilung ergänzt werden“. Dessen ungeachtet stellt die Kommission ein „Kompetenzdefizit im Bereich der Cyberabwehr“ fest, dem noch 2018 mit einer „Plattform für die Ausbildung und Aufklärung im Bereich der Cyberabwehr“ begegnet werden soll. Von Cyberangriffen betroffene Mitgliedstaaten könnten ähnlich wie beim EU-Katastrophenschutzmechanismus aus einem „Cybersicherheits-Notfallfonds“ unterstützt werden, allerdings müssten diese zuvor alle nach EU-Recht vorgeschrieben Cybersicherheitsmaßnahmen „ordnungsgemäß umgesetzt haben“. Weitere neue Kapazitäten sollen für die „Enttarnung, Rückverfolgbarkeit und Verfolgung von Cyberkriminellen“ sorgen. Genannt werden jedoch keine Maßnahmen zur Bekämpfung von Cyberangriffen, sondern lediglich „Betrug und Fälschung im Zusammenhang mit bargeldlosen Zahlungsmitteln“. Ebenfalls als „Ermittlungsarbeit bei Cyberdelikten“ wird die Erleichterung des

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 25. April 2018 übermittelt.

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

grenzüberschreitenden Zugangs zu elektronischen Beweismitteln genannt, die eigentlich zur Beschlagnahme von Cloud-Daten im EU-Ausland dienen soll und die „Überlegungen zur Rolle der Verschlüsselung bei kriminaltechnischen Ermittlungen".

Schließlich arbeitet die EU-Kommission an einem „Konzept, wie Europa und die Mitgliedstaaten in der Praxis gemeinsam rasch reagieren können, wenn es zu einem groß angelegten Cyberangriff kommt". In einer bereits vorgelegten Empfehlung werden die Mitgliedstaaten und die EU-Organe aufgefordert, für die praktische Umsetzung einen EU-Rahmen für die Reaktion auf Cybersicherheitskrisen zu schaffen. Zur Verbesserung der Cyberabwehr sollen auch militärische Strukturen („Cyberabwehrprojekte") eingebunden werden, die EU-Kommission nennt hierzu die ständige strukturierte Zusammenarbeit (PESCO) und den Europäischen Verteidigungsfonds. Insbesondere mit der NATO soll die Europäische Union die „Forschungs- und Innovationszusammenarbeit" intensivieren. Wie in den Jahren 2017 und 2018 ist die Beteiligung an „parallelen und koordinierten Übungen" geplant (Antwort der Bundesregierung auf die Kleine Anfrage auf Bundestagsdrucksache 19/1212). Zur Verbesserung der internationalen Zusammenarbeit plant die EU-Kommission die Umsetzung eines „Rahmens für eine gemeinsame diplomatische Reaktion auf böswillige Cyberaktivitäten". Auch Drittländer sollen bei der „Bewältigung von Cyberbedrohungen" unterstützt werden.

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 15c und 15d nicht vollständig in offener Form erfolgen kann.

Die Einstufung der Antwort auf die Fragen 15c und 15d als Verschlusssache (VS) mit dem Geheimhaltungsgrad „VS – Nur für den Dienstgebrauch" 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 der Allgemeinen Verwaltungsvorschrift zum materiellen und organisatorischen Schutz von Verschlusssachen (Verschlusssachenanweisung, 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 und dem Deutschen Bundestag gesondert übermittelt.

1. Inwiefern teilt die Bundesregierung die Einschätzung der EU-Kommission, die ein „Kompetenzdefizit im Bereich der Cyberabwehr" feststellt, und worin liegt dies begründet?

In der „Gemeinsamen Mitteilung an das Europäische Parlament und den Rat – Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der Europäischen

Union (EU) wirksam erhöhen" vom 13. September 2017 (im Folgenden „Gemeinsame Mitteilung") stellen die Europäische Kommission und die Hohe Vertreterin der Union für Außen- und Sicherheitspolitik fest, dass die Mitgliedstaaten der EU über Kompetenzen im Bereich der Cyberabwehr verfügen, die in unterschiedlichem Maß fortschrittlich sind. Die Cyberabwehrkompetenzen seien auszubauen, um insgesamt eine Erhöhung der Cybersicherheit herbeizuführen

Die Bundesregierung teilt die in der oben genannten Gemeinsamen Mitteilung geäußerte Einschätzung, dass die Ausbildung und Weiterentwicklung von Kompetenzen im Bereich der Cyberabwehr eine kontinuierlich zu bearbeitende Aufgabe in der EU darstellt. Hierfür bedarf es eines umfassenden gemeinsamen Ansatzes.

Zu diesem Zweck setzt sich die Bundesregierung auch auf europäischer Ebene für eine kohärente Cyber-Sicherheitspolitik ein. Der Ausbau von Kompetenzen im Bereich der Cyberabwehr ist hierbei ein essentieller Bestandteil. Mit der EU-Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen (im Folgenden „NIS-Richtlinie“) soll die Abwehrbereitschaft der Mitgliedstaaten, die unterschiedlich stark ausgeprägt ist, auf ein gemeinsames hohes Niveau gehoben werden.

Zuletzt bestätigte am 20. November 2017 der Rat der Europäischen Union in seinen Schlussfolgerungen zu der o. g. Gemeinsamen Mitteilung, dass die Gewährleistung von Cybersicherheit in der EU eine Stärkung der Abwehrfähigkeit der Mitgliedstaaten und der hierfür notwendigen Kompetenzen voraussetzt.

2. Ab welcher Schwelle einer „Cybersicherheitskrise“ sollten „Europa und die Mitgliedstaaten in der Praxis“ aus Sicht der Bundesregierung „gemeinsam rasch reagieren können, wenn es zu einem groß angelegten Cyberangriff kommt“?

Generell sind die Maßnahmen bei Cyberkrisen Sache des einzelnen Mitgliedstaats. Derzeit wird über Maßnahmen bei einem Cyber-Sicherheitsvorfall im Rahmen der Verhandlungen über den Cybersecurity-Act verhandelt. Die Verhandlungen darüber, ob und welche Maßnahmen zu ergreifen sind und ob hierfür Schwellenwerte festgelegt werden sind nicht abgeschlossen. Die Meinungsbildung der Bundesregierung hierzu ist noch nicht abgeschlossen.

Auf nationaler Ebene wurden in Deutschland unter anderem mit dem IT-Sicherheits-gesetz, der BSI-Kritis-Verordnung, der Cyber-Sicherheitsstrategie für Deutschland der Bundesregierung vom November 2016 und der Umsetzung NIS-Richtlinie bereits zentrale Vorhaben umgesetzt. Der strategische, rechtliche und institutionelle Rahmen wird desgleichen weiterentwickelt, um die mit der hohen Dynamik der Digitalisierung einhergehenden Herausforderungen zu bestehen.

3. Welche wesentlichen Akteure der Mitgliedstaaten und der Europäischen Union sind aus Sicht der Bundesregierung im Bereich des operativen und strategischen Krisenmanagements im Cyberraum unterrepräsentiert und müssten stärker beteiligt werden (etwa Reaktionsteams für Computersicherheitsverletzungen, Europol, der Europäische Auswärtige Dienst, die East StratCom Task Force, die Website „EUvsdisinformation“)?

Die Bundesregierung teilt die Auffassung, dass wesentliche Akteure unterrepräsentiert seien, nicht, und trifft keine Aussagen über die Akteure anderer Mitgliedstaaten oder der der EU.

4. Welche Rolle sollte eine „EU-Agentur für Cybersicherheit“ aus Sicht der Bundesregierung hinsichtlich der Abwehrfähigkeit und Reaktion der EU auf Cyberangriffe übernehmen, und welche Maßnahmen hält sie dazu für geeignet?

Die Bundesregierung begrüßt und unterstützt ausdrücklich ein stärkeres gemeinsames Vorgehen der EU bei der Abwehr von Cyber-Angriffen. Dabei kommt dem Rat und den Mitgliedstaaten, bei denen wesentliche Kapazitäten und Kompetenzen im Bereich Cyber-Sicherheit liegen, eine zentrale Rolle zu. Ein permanentes Mandat für ENISA wird ausdrücklich begrüßt. Regelungen für die Ausgestaltung der Aufgaben der ENISA werden derzeit mit dem Cybersecurity-Act verhandelt.

5. Inwiefern sollte die neue Agentur aus Sicht der Bundesregierung zusätzlich zu den regelmäßig abgehaltenen „EU-Cyberübungen“ weitere „Cybersicherheitsübungen“ durchführen, und welche Defizite sollten damit überbrückt werden?

Aus Sicht der Bundesregierung sind die heute durchgeführten Übungen der Gefahrenlage und der bestehenden Organisation angepasst. Neue, durch die EU-Agentur für Cybersicherheit durchgeführte, Übungsformate müssen sich in den Kontext bestehender EU, NATO und nationaler Übungen einfügen.

6. Wo soll nach Kenntnis der Bundesregierung das europäische „Forschungs- und Kompetenzzentrums für Cybersicherheit“ bzw. ein entsprechendes „Pilotzentrum“ eingerichtet werden, um die Mitgliedstaaten bei der Entwicklung und Nutzung von „Instrumenten und Technik“ gegen die „immer neuen Bedrohungen“ zu unterstützen?

Nach derzeitiger Kenntnis wurden noch keine konkreten Festlegungen zu einem solchen Zentrum getroffen. Vielmehr wurden seitens der EU-Kommission mögliche Pilotprojekte ausgeschrieben, die im Ergebnis als Ausgangspunkt für ein solches Zentrum (oder mehrerer solchen Zentren) dienen können (vgl. http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/su-ict-03-2018.html).

Laut der Ausschreibungsunterlage sind bis zu drei Pilotprojekte vorgesehen, die vor allem die Forschungskoordination zum Ziel haben. Aus diesen könnten in der Folge (drei) koordinierende Zentren – verteilt über Europa – hervorgehen. Der Umfang der Ausschreibung beläuft sich auf ca. 50 Mio. Euro. Es ist vorgesehen, dass die aufzustellenden Konsortien aus mindestens 20 Teilnehmern aus mindestens neun Mitgliedstaaten bestehen. Die Ausschreibungsfrist endet im Mai. Mit der Vergabeentscheidung ist Ende 2018 zu rechnen.

Darüber hinaus hat die EU-Kommission mit der Veröffentlichung eines Inception Impact Assessment (IIA) (vgl. https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2018-1598442_de) angekündigt, neben der zuvor dargestellten Option die Einrichtung eines Europäischen Cybersecurity Forschungs- und Kompetenzzentrums in Form einer Generalunternehmung gem. Artikel 187 des Vertrags über die Arbeitsweise der europäischen Union zu prüfen. Damit würde eine eigenständige EU Einrichtung geschaffen werden. Auf Aufwand und Kosten wird im IIA nicht detailliert eingegangen. Als dritte Option führt das IIA die Einrichtung eines Zentrums basierend auf Artikel 173 des Vertrags über die Arbeitsweise der europäischen Union auf. Dieses soll ebenfalls als zentrale Einheit eingerichtet werden und in Zusammenarbeit mit den möglicherweise aus der zuvor

genannten Ausschreibung entstehenden Koordinierungszentren entsprechend Synergien erzielen. Details sind ebenfalls nicht ausgeführt. Daher sind diesbezüglich ebenfalls keine konkreten Aussagen zu treffen.

a) Welche Mitgliedstaaten oder sonstigen Einrichtungen nehmen an dem Zentrum teil, und welche Kapazitäten stellt die Bundesregierung hierfür zur Verfügung?

Auf die Antwort zu Frage 6 wird verwiesen.

b) Welche Haltung vertritt die Bundesregierung zur Frage, inwiefern das Zentrum um eine „Cyberabwehr-Abteilung“ ergänzt werden sollte, und über welche Kompetenzen dieses verfügen sollte?

Die Etablierung einer „Cyberabwehr-Abteilung“ innerhalb eines Forschungszentrums bzw. einer Forschungskoordinierungsstelle ist nicht vorgesehen und aus Sicht der Bundesregierung nicht zielführend.

7. Wo soll die von der EU-Kommission angekündigte „Plattform für die Ausbildung und Aufklärung im Bereich der Cyberabwehr“ nach Kenntnis der Bundesregierung eingerichtet werden?

Auf die Antwort zu Frage 9 wird verwiesen. Bei der in der Frage benannten Plattform handelt es sich um die ETEE („education, training, evaluation and exercise“) Plattform als Teil des ESDC.

8. Auf welche Weise arbeiten Bundesbehörden mit dem „Incident and Threat Information Sharing EU Centre“ (ITIS-EUC) zusammen, über das „Informationen über Cyberbedrohungen und -vorfälle im Energiesektor analysiert und ausgetauscht werden“ (Ratsdokument 11539/17)?

Bei dem Incident and Threat Information Sharing EU Centre (ITIS-EUC) handelt es sich um eine webbasierte Plattform, die von der Europäischen Kommission eingerichtet worden ist. Die Nutzung dieser Plattform steht nur bestimmten Nutzern – nämlich Übertragungsnetzbetreibern (ÜNB) und Verteilnetzbetreibern (VNB) und Betreibern aus dem Gas-, Strom- und Ölbereich – offen. Vor Nutzung der Plattform ist eine Registrierung erforderlich.

ITIS-EUC sammelt Informationen über Vorfälle und Bedrohungen im Energiebereich und nutzt dabei Open-Source-Informationen. ITIS-EUC kann auch Informationen von einzelnen registrierten Betreibern aus dem Energiebereich erhalten und an seine übrigen registrierten Nutzer weitergeben. Eine Zusammenarbeit von mitgliedstaatlichen Einrichtungen und Behörden mit dem ITIS-EUC ist nicht vorgesehen.

Die von ITIS-EUC zur Verfügung gestellten Informationen und Analysen sollen das Bewusstsein für mögliche Cyberbedrohungen im Energiesektor und in den in diesem Bereich tätigen Unternehmen erhöhen.

9. Was ist der Bundesregierung über die Einrichtung einer „Cyber platform for education, training, exercise and evaluation“ (ETEE) bekannt (http://gleft.de/29D), wo wird diese installiert, und wer nimmt daran teil?

Die Europäische Verteidigungsagentur (EDA) hat basierend auf einer Beauftragung durch den EU Capability Development Plan (CDP) die Machbarkeit einer solchen Plattform bzw. eines Zentrums untersucht. Ein erster Studienbericht zu der Frage, der drei verschiedene Modelle vorschlug, wurde dem European Union Military Committee (EUMC) und der Politisch-Militärischen Gruppe (PMG) des PSK im Sommer 2016 zur Bewertung vorgelegt. Basierend auf diesem Bericht wurde die Präferenz der Mitgliedsstaaten für das Modell, welches eine Plattform innerhalb des European Security and Defence College (ESDC) beschrieb, zum Ausdruck gebracht. Eine Implementierungsstudie wurde durch EDA im Herbst 2017 vorgelegt. Basierend auf den Machbarkeitsanalysen der EDA und einer Empfehlung des EUMC vom Oktober 2017 sowie einer einstimmigen Entscheidung des zuständigen Steuerungskomitees des ESDC vom Februar 2018 wird die Cyber ETEE Plattform als Teil des ESDC in Brüssel eingerichtet. Damit unterliegt die Plattform der Steuerungsstruktur des ESDC und ist allen EU Mitgliedstaaten zugänglich.

a) Welche Ziele werden mit der ETEE verfolgt, und wie werden Doppelungen mit bestehenden Einrichtungen vermieden?

Ziel der Plattform ist es, auf europäischer Ebene den Cyberausbildungs- und Übungsbedarf, der sich aus der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP) ergibt, zu koordinieren, zu harmonisieren und zu standardisieren, sowie die Erfüllung dieses Bedarfes entlang der Grundprinzipien des ESDC durch nationale Ausbildungs- und Übungseinrichtungen der EU Mitgliedsstaaten oder anderen EU Ausbildungseinrichtungen (z. B. CEPOL) sicherzustellen. Damit hat die Cyber ETEE Plattform eine rein koordinierende Funktion. Das ESDC ist die einzige EU-Einrichtung, die sich innerhalb der GSVP Strukturen mit GSVP-spezifischem Ausbildungsthemen befasst. Um das Risiko der Doppelung im EU und multinationalen Kontext zu minimieren, ist es geplant, dass die Cyber ETEE Plattform einen ständigen und strukturierten Dialog mit anderen Einrichtungen (z. B. ENISA; NATO CCD COE) im Themenfeld einrichtet und aufrechterhält.

b) Welche Kosten (auch Machbarkeitsstudien) entstehen für die ETEE, und wie werden diese übernommen?

Hierzu liegen der Bundesregierung keine Informationen vor.

c) Wann soll die ETEE starten bzw. ihre volle Einsatzbefähigung erreichen?

Die Initial Operational Capability (IOC) ist für September 2018 und die Full Operational Capability (FOC) für April 2019 geplant.

10. Welchen neuen EU-(Rechts-)Rahmen für die Reaktion auf „Cybersicherheitskrisen“ hält die Bundesregierung für notwendig, und wie müsste dieser ausgestaltet werden?

Der von der Europäischen Kommission vorgeschlagene Rechtsrahmen wird durch das Cybersecurity Package, insbesondere dem Cybersecurity-Act, widergespiegelt. Generell begrüßt die Bundesregierung die von der Kommission vorgeschlagenen Maßnahmen zur Stärkung der Cybersicherheit. Die Ausgestaltung des Rechtsrahmens wird derzeit verhandelt.

11. Welche Haltung vertritt die Bundesregierung zur Frage, wie ein „Cybersicherheits-Notfallfonds“ ausgestaltet werden könnte, und ob Mittel hierfür aus vorhandenen Strukturen verteilt werden könnten?

Über die Einrichtung eines „Cybersicherheits-Notfallfonds“ auf EU-Ebene ist der Bundesregierung derzeit nichts bekannt.

12. Welche neuen Kapazitäten sollte die Europäische Union aus Sicht der Bundesregierung zur „Enttarnung, Rückverfolgbarkeit und Verfolgung von Cyberkriminellen“ entwickeln?

Aus Sicht der Bundesregierung müssen die Strafverfolgungsbehörden stets in der Lage sein, mit der technischen Entwicklung im Bereich der Cyberkriminalität Schritt zu halten. Deshalb begrüßt die Bundesregierung grundsätzlich den Aufbau neuer Kapazitäten zur Enttarnung, Rückverfolgbarkeit und Verfolgung von Cyberkriminellen in der Europäischen Union und bei den Mitgliedsstaaten.

13. Welche Haltung vertritt die Bundesregierung zur Frage, welche militärischen EU-Strukturen („Cyberabwehrprojekte“) in die zivile Cyberabwehr eingebunden werden sollten?

Militärische Cyberabwehrprojekte sollen nur innerhalb des Militärs und seiner eigenen Netzwerke Geltung haben. Für die Cybersicherheit von Behörden, Unternehmen und Bürgern sind zivile Einrichtungen zuständig. Die Bundesregierung erachtet einen Informationsaustausch zu Cyber-Bedrohungen zwischen militärischen und zivilen EU-Strukturen bzw. EU-Einrichtungen zum Zweck der Prävention im Rahmen des geltenden Rechts grundsätzlich als sinnvoll.

a) Was ist der Bundesregierung über Planungen bekannt, die ständige strukturierte Zusammenarbeit (PESCO) und den Europäischen Verteidigungsfonds stärker in die eigentlich zivile Cyberabwehr zu integrieren (bitte etwaige Projekte oder Initiativen aufführen)?

Der Bundesregierung sind keine Planungen bekannt.

b) Was ist der Bundesregierung darüber bekannt, auf welche Weise die Europäische Union und die NATO den Informationsaustausch zwischen ihren jeweiligen Cybersicherheitsgremien (laut EU-Kommission dem IT-Notfallteam für die Organe, Einrichtungen und sonstigen Stellen der EU (CERT-EU) und der Computer Incident Response Capability (NCIRC) der NATO), intensivieren, wozu die beiden Partner in den Jahren 2017 und 2018 erstmals parallele und koordinierte Übungen zur Reaktion auf ein hybrides Angriffsszenario abgehalten haben?

Die strategische Partnerschaft zwischen der EU und der NATO basiert auf der NATO-EU-Joint Declaration 2016. Ein Teil davon ist die Kooperation im Bereich der Cyber-Sicherheit und der Cyber-Abwehr, unter anderem durch die gegenseitige Teilnahme an Übungen. Um diese politischen Vorgaben umzusetzen, nahmen beispielsweise der EU Military Staff (EUMS) und das Computer Incident Response Team der EU (CERT-EU) an der NATO-Übung CYBER COALITION 2017 als Beobachter teil.

Der Informationsaustausch zwischen dem CERT-EU und der NATO Computer Incident Response Capability (NCIRC) wurde durch ein Technical Arrangement vom Februar 2016 formalisiert.

c) Wie sollen die „Bemühungen um bessere Interoperabilität bei den Cybersicherheitsstandards“ umgesetzt werden?

Der Bundesregierung sind keine Cybersicherheitsstandards bekannt, die in den Kontext der „militärischen EU-Strukturen“ gehören.

14. Was ist der Bundesregierung über Ort und Zeitpunkt einer Cybersicherheitsübung „Cyber Europe 2018“ bekannt (sofern die Übung in einzelne Teile aufgegliedert ist, diese bitte benennen)?

Die zentrale Übungssteuerung erfolgt von der ENISA in Athen aus, so dass alle Übenden von ihren üblichen Arbeitsplätzen aus teilnehmen können. Der Übungstermin wird von der ENISA bekannt gegeben.

a) Wer nimmt an der Übung teil, und inwiefern soll diese im Kontext anderer Übungen, etwa der NATO, abgehalten werden?

Zur Übung sind – wie in den Vorjahren – die nationalen CERTs eingeladen. Diese können nationale Behörden und Unternehmen aus dem Bereich Luftfahrt einladen. Für Deutschland steht noch nicht fest, wer außer dem BSI teilnehmen wird.

b) Welche Szenarien werden dort geübt?

Das Szenario wird mit dem Trailer, der über die Webseite: www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme/cyber-europe-2018 aufgerufen werden kann, illustriert. Detailliertere Informationen sind der Bundesregierung derzeit nicht bekannt und stehen vor der Übung und während des Planungsprozesses nur den Planern zur Verfügung.

c) Sofern auch Szenarien wie die „Verunstaltung von Webseiten“, „Datendiebstahl von Benutzernamen und Passwörtern“, „Ausschalten der Energieversorgung eines Flughafens“, „Kontrolle über die Flugzeugbetankungsanlage“ oder die Reaktion auf das Streuen von Falschinformationen geübt werden sollen, welche Details sind der Bundesregierung hierzu bekannt?

Die genannten Szenarien sind als Übungsszenario grundsätzlich möglich. Im Übrigen wird auf die Antwort zu Frage 14b verwiesen.

15. Welche Szenarien werden nach Kenntnis der Bundesregierung in der militärischen Übung „Locked Shields 2018“ vom 23. bis 27. April 2018 in Tallinn geübt (Antwort der Bundesregierung auf Bundestagsdrucksache 19/1212)?

Locked Shields ist eine Übung zu technischen Einzelaspekten im Cyberraum. Für technische Übungen sind Szenarien eher vernachlässigbar. Weitere Details der Szenarien für „Locked Shields 2018“ sind der Bundesregierung derzeit noch nicht bekannt.

a) Welche Staaten, mit denen Beitrittsverhandlungen zum NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) vor dem Abschluss stehen, werden eingeladen bzw. nehmen teil?

Hierzu liegen der Bundesregierung keine Informationen vor.

b) Inwiefern ist mittlerweile bekannt, welche Cyberübungen, an denen sich die Bundeswehr 2018 beteiligt, an der Schwelle eines bewaffneten Angriffs operieren?

Zum jetzigen Zeitpunkt sind die Szenarien der Cyberübungen, an denen die Bundeswehr in 2018 teilnimmt, noch nicht bekannt.

c) An welchen Cyberübungen der Europäischen Union oder der NATO hat sich die Bundeswehr in der Vergangenheit mit „Red-Teams“ beteiligt (Antwort der Bundesregierung auf Bundestagsdrucksache 19/1212)?

d) In welchen Cyberübungen, an denen sich die Bundeswehr 2017 beteiligt, wurde mit den Anwendungen „Cobalt Strike“, „Metasploit“ oder „Burp Proxy“ geübt?

Die Fragen 15c und 15d werden gemeinsam beantwortet.

Es wird auf den „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß Vorbemerkung der Bundesregierung verwiesen.*

* Das Bundesministerium der Verteidigung hat die Antwort als „VS ‑Nur für den Dienstgebrauch“ eingestuft.
Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

16. Welche weiteren Anstrengungen sollte die Europäische Union aus Sicht der Bundesregierung hinsichtlich von Cyberdiplomatie und internationalen Cybernormen sowie zur Umsetzung der „Cyber Diplomacy Toolbox“ (Ratsdokument 9916/17) unternehmen?

Die EU sollte aus Sicht der Bundesregierung hinsichtlich Cyberdiplomatie und internationalen Cybernormen den „Rahmen für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten“ („Diplomatischer Reaktionsrahmen“) zur Anwendung bringen. Die EU sollte sich außerdem im Rahmen ihrer Cyberdiplomatie weiterhin dafür einsetzen, dass Staaten sich regelkonform und vertrauensbildend im Cyberraum bewegen.

17. Welche Drittländer außer den USA, Japan, Indien, der Republik Korea und China sollten aus Sicht der Bundesregierung für die Europäische Union zur Etablierung „starker Bündnisse“ oder zu Gesprächen über das Thema Cybersicherheit im Fokus stehen?

Aus Sicht der Bundesregierung sollte sich die EU auch in näherer Zukunft bei Gesprächen und Austauschformaten zum Thema Cybersicherheit auf die genannten Drittländer fokussieren.

18. Welche Haltung vertritt die Bundesregierung zur Frage der Notwendigkeit eines „Rahmens für eine gemeinsame diplomatische Reaktion auf böswillige Cyberaktivitäten“?

Die Bundesregierung betrachtet den „Diplomatischen Reaktionsrahmen“ als notwendig. Sie hat sich an seiner Formulierung beteiligt.

19. Inwiefern bzw. nach welcher Maßgabe sollte die Europäische Union aus Sicht der Bundesregierung zukünftig mit (öffentlichen oder nichtöffentlichen) diplomatischen Verurteilungen, Erklärungen oder Ratsschlussfolgerungen an Regierungen, die als Urheber von Cyberangriffen verdächtigt werden, reagieren (Ratsdokument WK 2641/2018 INIT)?

Der „Diplomatische Reaktionsrahmen“ und dessen Umsetzungsrichtlinien (Ratsdokument 13007/17) stellen die Maßgaben für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten dar. Entsprechende Entscheidungen treffen die Mitgliedstaaten von Fall zu Fall auf der Grundlage von Informationen aus allen relevanten Quellen.

20. Mit welchen Maßnahmen sollte die Europäische Union aus Sicht der Bundesregierung zukünftig gemeinsam auf „böswillige Cyberaktivitäten“ reagieren?

a) Nach welcher Maßgabe fielen „böswillige Cyberaktivitäten“ unter die Regelungen der „Solidaritätsklausel“ nach Artikel 222 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV)?

b) Inwiefern könnten als „Reaktion auf böswillige Cyberaktivitäten“ Instrumente der integrierten EU-Regelung für die politische Reaktion auf Krisen (ICPR) genutzt werden?

c) In welchen zivilen oder militärischen Cyberübungen, an denen sich die Bundesregierung beteiligt hat, wurde der ICPR-Mechanismus bereits berücksichtigt?

d) Inwiefern könnten sich etwaige EU-Reaktionen aus Sicht der Bundesregierung auch auf die United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) berufen, und welche Initiativen sind der Bundesregierung hierzu bekannt?

Die Fragen 20 bis 20d werden gemeinsam beantwortet. Der „Diplomatische Reaktionsrahmen“ und dessen Umsetzungsrichtlinien sehen als außenpolitische

Reaktionsmöglichkeiten auf böswillige Cyberoperationen vorbeugende Maßnahmen, Maßnahmen der Zusammenarbeit, Stabilitätsmaßnahmen, restriktive Maßnahmen und eine Unterstützung völkerrechtskonformer Reaktionen der Mitgliedstaaten durch die EU vor.

Jede Entscheidung über den konkreten Einsatz der genannten außenpolitischen Reaktionen muss im Einzelfall getroffen werden. Eine allgemeine Antwort zu den Fragen 20 a bis 20 d ist daher nicht möglich. Bisher war die Bundesregierung weder an zivilen noch an militärischen Cyberübungen beteiligt, bei denen der ICPR-Mechanismus bereits berücksichtigt wurde.

21. Wie könnte ein „Protokoll für die Notfallreaktion“ auf Cybersicherheitsvorfälle („Emergency Response Protocol”) europäischer Strafverfolgungsbehörden aus Sicht der Bundesregierung ausgestaltet und umgesetzt werden (Ratsdokument 11809/17)?

a) Welches Ausmaß müssten IT-Störungen annehmen, um das Protokoll zu aktivieren, bzw. wie würde die Aktivierung bestimmt?

b) Welche zivilen und militärischen EU-Lagezentren sollten daraufhin aktiviert werden?

c) Welche Einrichtungen sollten mit der Überwachung offener Quellen („Open Source Monitoring” und taktischer Koordination beauftragt werden?

Die Fragen 21 bis 21c werden gemeinsam beantwortet. Die Erarbeitung eines EU-Protokolls für die Notfallreaktion auf schwerwiegende Cybersicherheitsvorfälle ist ein in der Entwicklung befindlicher Prozess unter Sachleitung der derzeitigen bulgarischen EU-Ratspräsidentschaft. Die mögliche Implementierung eines solchen Protokolls wird unter Beteiligung aller EU-Mitgliedstaaten, der EU-Kommission und EUROPOL in Workshops ergebnisoffen diskutiert. Zurzeit steht daher noch nicht fest, ob bzw. wann dieses Protokoll zur Anwendung kommt und wie es im Detail ausgestaltet sein wird.

Wegen der vorgenannten multilateralen Erörterungen und der noch nicht abgeschlossenen Meinungsbildung der Bundesregierung können die Antworten auf die Fragen a bis c noch nicht abschließend beantwortet werden.

22. Welche Defizite sieht die Bundesregierung bei der EU-Reaktion auf die Cyberangriffe mit „Wannacry“ und „NotPetya“ („Herausforderungen, an deren Bewältigung gearbeitet wird“, Ratsdokument 11539/17), und welche Maßnahmen hält sie hierzu für erforderlich?

Die genannten Schadprogramme haben sich vor allem aufgrund von nicht aktualisierten Betriebssystemen und nicht-separierten Netzwerken in Unternehmen ausgebreitet. Gefordert waren daher die Unternehmen, ihre Sicherheitskonzepte auf den Stand der Technik zu bringen. Die EU kann in solchen Fällen nur durch

Informationen und Warnungen agieren. Da diese erfolgt sind, sieht die Bundesregierung insofern bei der Reaktion der EU auf die genannten Vorfälle keine Defizite.

a) Welche Rolle übernimmt das geheimdienstliche Lagezentrum INTCEN schon jetzt bei der Zurechnung („Attribuierung“) von Cyberangriffen, und wie sollten diese Fähigkeiten ausgebaut werden?

Der Bundesregierung ist nicht bekannt, dass das EU-Zentrum für Informationsgewinnung und -analyse (INTCEN) des Europäischen Auswärtigen Dienstes (EAD) eine entsprechende Rolle einnimmt. Die Zurechnung einer bösartigen Cyberaktivität verbleibt eine souveräne politische Entscheidung eines Mitgliedstaats, die von Fall zu Fall auf der Grundlage von Informationen aus allen relevanten Quellen getroffen wird.

b) Auf welche Weise ist das INTCEN bzgl. der Cyberangriffe mit „Wannacry“ und „NotPetya“ tätig geworden?

Der Bundesregierung liegen keine Erkenntnisse dazu vor, ob und wenn ja, auf welche Weise das INTCEN sich mit den genannten Fällen beschäftigt hat oder tätig geworden ist.

c) Welche deutschen Behörden haben hierzu Lageberichte beigesteuert?

Das Bundesamt für Sicherheit in der Informationstechnik hat zu den Vorfällen „Wannacry“ und „NotPetya“ angemessen und ausführlich berichtet.

d) Auf welche Weise sind welche EU-Agenturen oder IT-Netzwerke (etwa die Reaktionsteams für Computersicherheitsverletzungen) bzgl. der Cyberangriffe mit „Wannacry“ und „NotPetya“ tätig geworden bzw. weiterhin damit befasst?

Das CSIRT-Netzwerk hat sich zu NotPetya- und WannaCry-Vorfällen in Europa ausgetauscht und gemeinsame Lageberichte verfasst. Die Behandlung der einzelnen, konkreten Vorfälle oblag jedoch den Betroffenen.

Darüber hinaus hat sich Europol mit dem Cyberangriff „WannaCry“ befasst und war dabei beratend und koordinierend tätig.

23. Was ist der Bundesregierung darüber bekannt, welche EU-Agenturen oder IT-Netzwerke mit Ermittlungen und Analysen zu Angriffen mit der Schadsoftware „Snake“ (bzw. „Turla“, „Uroburos“), „Stuxnet“, „Black Energy“ oder „Mirai“ befasst waren oder sind?

Das CERT-EU analysiert kontinuierlich als relevant angesehene Schadsoftware, darunter auch Snake, Mirai und BlackEnergy. Europol war bei den Ermittlungen zu Mirai Ende 2016 koordinierend eingebunden.

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