Deutscher Bundestag **Drucksache 19/7607**

19. Wahlperiode 11.02.2019

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Stephan Thomae, Grigorios Aggelidis, Renata Alt, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 19/7321 –

Bedrohung durch Cyberangriffe

Vorbemerkung der Fragesteller

Im Mai 2015 wurde ein Cyberangriff auf das interne Netzwerk des Deutschen Bundestages entdeckt (vgl. www.zeit.de/digital/datenschutz/2015-05/hackerangriff-bundestag-sommerpause), hinter dem russische Hacker der APT28-Gruppe vermutet wurden (vgl. www.zeit.de/2017/20/cyberangriff-bundestag-fancy-bear-angela-merkel-hacker-russland). Noch im selben Jahr soll die gleiche Gruppe Angriffe auf mehrere NATO-Staaten sowie Rüstungsunternehmen insbesondere aus der Luft- und Raumfahrtbranche verübt haben (vgl. https://web.archive.org/web/20170702222852/www.tagesschau.de/inland/hacker-123.html). Am 15. und 24. August 2016 kam es zu sog. Spear-Phishing-Angriffen unter anderem auf Mitglieder des Deutschen Bundestages (vgl. www.spiegel.de/netzwelt/netzpolitik/bundestag-spur-von-hacker-angriff-fuehrt-nach-russland-a-1113264.html).

Ende 2016 wurden auf der Internetseite WikiLeaks Dokumente aus dem NSA-Untersuchungsausschuss veröffentlicht (vgl. www.zeit.de/digital/datenschutz/2016-12/wikileaks-veroeffentlichung-nsa-untersuchungsausschuss-dokumente).

Im Februar 2018 wurde der Hackerangriff auf das Datennetz der Bundesverwaltung, den Informationsverbund Berlin-Bonn (IVBB), öffentlich (vgl. www.zeit.de/digital/datenschutz/2018-02/hacker-dringen-in-deutsches-regierungsnetz-ein).

Im Januar 2019 wurde ein Fall des Doxing bekannt, bei dem Daten von fast 1000 Politikern bzw. Prominenten im Internet veröffentlicht wurden (vgl. www.zeit.de/politik/deutschland/2019-01/hackerangriff-politiker-leak-daten-dokumente-twitter).

Diese nicht abschließende Liste sicherheitsrelevanter Aktivitäten zeigt, dass die Bedrohung durch Cyberangriffe wächst.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 7. Februar 2019 übermittelt.

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

1. Wie definiert die Bundesregierung den Begriff „Cyberangriff“?

2. Welche Aktivitäten fasst die Bundesregierung unter den Begriff Cyberangriff (bitte Aktivitäten auflisten und Definition angeben)?

Die Fragen 1 und 2 werden gemeinsam beantwortet.

Die von der Bundesregierung angenommene „Cyber-Sicherheitsstrategie für Deutschland 2016“ definiert den Begriff „Cyber-Angriff“ wie folgt:

„Ein Cyber-Angriff ist eine Einwirkung auf ein oder mehrere andere informationstechnische Systeme im oder durch den Cyber-Raum, die zum Ziel hat, deren IT-Sicherheit durch informationstechnische Mittel ganz oder teilweise zu beeinträchtigen.“

Aus dieser Definition ergibt sich – mit Hinweis auf das Einwirken – auch die Antwort zu Frage 2.

3. Welche im engen Zusammenhang mit Cyberkriminalität stehenden sicherheitsrelevanten Aktivitäten gibt es nach Kenntnis der Bundesregierung in der Bundesrepublik Deutschland (bitte Aktivitäten auflisten und Definition angeben)?

Das jährlich vom Bundeskriminalamt herausgegebene Bundeslagebild Cybercrime stellt die Erkenntnisse über Cyberkriminalität in Deutschland ausführlich u. a. anhand der Regelungen im Strafgesetzbuch (StGB) und relevanter Fallbeispiele dar (Quelle: www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html).

Die statistische Grundlage für das Bundeslagebild Cybercrime bildet die Polizeiliche Kriminalstatistik (PKS). Die Fallzahlen des Bundes und der Länder können dort recherchiert werden (Quelle: www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/pks_node.html).

4. Wie viele Cyberangriffe oder sonstige sicherheitsrelevante Aktivitäten gab es nach Kenntnis der Bundesregierung seit 2010 auf staatliche Institutionen (bitte nach Jahren, Institutionen, Aktivität und Urheber aufschlüsseln)?

5. Wie viele Cyberangriffe oder sonstige sicherheitsrelevante Aktivitäten gab es nach Kenntnis der Bundesregierung seit 2010 auf die Deutsche Bahn AG, die Deutsche Telekom AG sowie auf andere öffentliche Unternehmen (bitte nach Jahren, Datum, Zielunternehmen, Aktivität, Dauer der Aktivität und Urheber der Aktivität aufschlüsseln)?

6. Wie viele Cyberangriffe oder sonstige sicherheitsrelevante Aktivitäten gab es nach Kenntnis der Bundesregierung seit 2010 auf private Unternehmen (bitte nach Jahren, Datum, Zielunternehmen, Aktivität, Dauer der Aktivität und Urheber der Aktivität aufschlüsseln)?

Die Fragen 4 bis 6 werden gemeinsam beantwortet.

Cyberangriffe bzw. Sicherheitsvorfälle bei Bundesbehörden werden in der Meldestelle des Bundes nach § 4 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) beim Bundesamt für Sicherheit in der Informationstechnik (BSI) erfasst.

Meldungen über Cyberangriffe oder sonstige sicherheitsrelevante Aktivitäten auf öffentliche und private Unternehmen werden durch die Meldestelle gemäß § 8b BSIG und der Meldestelle der Allianz für Cyber-Sicherheit statistisch beim BSI erhoben.

Auswertungen können den jährlichen Lageberichten entnommen werden, die unter der folgenden Adresse öffentlich zugänglich sind: www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html.

7. In wie vielen Fällen konnte die Identität der Täter einwandfrei festgestellt werden?

Der Bundesregierung liegen keine Erkenntnisse im Sinn der Fragestellung vor.

8. In wie vielen Fällen kam es zu einer Verurteilung (bitte nach Delikt und Strafe aufschlüsseln)?

Die vom Statistischen Bundesamt herausgegebene Strafverfolgungsstatistik erfasst Verurteilungen nur deliktsbezogen und liefert keine Hinweise auf über die Tatbestandsmerkmale hinausgehende Tatmodalitäten (hier: Cyberangriffe). Der Bundesregierung liegen daher aus dem Bereich der Justiz keine Erkenntnisse zu der Fragestellung vor.

9. Existiert nach Kenntnis der Bundesregierung ein Mechanismus zur Bewertung der Intensität bzw. Kategorisierung eines Cyberangriffs oder sonstiger sicherheitsrelevanter Aktivitäten (z. B. Skala)?

Die Bundesregierung hat keine Kenntnis von einem derartigen Mechanismus. Nach Auffassung der Bundesregierung kann die Intensität (inklusive entsprechender Kategorisierung) aufgrund der Vielzahl an Angriffsmöglichkeiten nicht nach einem global gültigen Mechanismus bewertet werden.

10. Wie beurteilt die Bundesregierung die Intensität der in den Antworten zu den Fragen 4 bis 6 genannten Aktivitäten jeweils?

11. Wann und durch wen erfuhr die Bundesregierung von den jeweiligen Angriffen oder sonstigen sicherheitsrelevanten Aktivitäten (bitte nach Datum und Angriff aufschlüsseln)?

Die Fragen 10 und 11 werden gemeinsam beantwortet.

Auf die Antwort zu den Fragen 4, 5 und 6 wird verwiesen.

12. Wie lange dauerten die Angriffe oder sonstigen sicherheitsrelevanten Aktivitäten nach Kenntnis der Bundesregierung jeweils an (bitte nach Datum, Aktivität und Dauer aufschlüsseln)?

Die Dauer von Cyber-Angriffen und -Vorfällen wird nicht systematisch erhoben.

13. Welche Kenntnisse liegen der Bundesregierung über aktuell noch laufende Angriffe oder sonstige sicherheitsrelevante Aktivitäten vor (bitte nach Datum der erstmaligen Kenntniserlangung, Aktivität, Ziel der Aktivität und Urheber aufschlüsseln)?

Cyber-Angriffe auf die Regierungsnetze finden täglich statt. Die Vielzahl der Angriffe und Angriffsarten geht aus den Berichten über die Lage der IT-Sicherheit in Deutschland des BSI hervor (vgl. die Antwort zu den Fragen 4, 5 und 6).

14. Welche konkreten Maßnahmen wurden wann von wem ergriffen, um Angriffe oder sonstige sicherheitsrelevante Aktivitäten seit 2010 zu beenden (bitte nach Aktivität, Maßnahme und ausführende Behörde aufschlüsseln)?

Das BSI empfiehlt eine Vielzahl unterschiedlichster Maßnahmen in den Bereichen Prävention, Detektion und Reaktion, die von seinen Zielgruppen eigenverantwortlich umgesetzt werden. Darüber hinaus ergreift das BSI in seinem gesetzlichen Zuständigkeitsbereich eigene Maßnahmen in den genannten Bereichen. Beispielhaft zu nennen sind:

Empfehlungen zur Prävention werden zielgruppengerecht veröffentlicht z. B. auf den Webseiten des BSI (inkl. BSI-für-Bürger, Bürger-CERT, Warn – und Informationsdienst des CERT-Bund). Besonders relevante Aspekte werden als Informationen oder Warnungen an die IT-Sicherheitsbeauftragten der Bundesbehörden, den Verwaltungs-CERT-Verbund mit den Ländern, an die registrierten Betreiber Kritischer Infrastrukturen (KRITIS) sowie den UP KRITIS und an Unternehmen über die Allianz für Cyber-Sicherheit versendet bzw. bereitgestellt.

Bei konkreten Vorfällen wird das BSI tätig. Täglich unterrichtet das BSI Betroffene von Infektionen und Fehlkonfigurationen (www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/CERT-Bund/CERTReports/reports_node.html). Bei der Bewältigung von Netzwerkkompromittierungen werden ggf. Incident-Handler von CERT-Bund, Forensiker sowie das MIRT (Mobile Incident Response Team) eingesetzt, um den Vorfall zu untersuchen und die Systeme und das Netzwerk zu bereinigen. Über das Cyber-Abwehrzentrum werden im Rahmen des geltenden Rechts Informationen zwischen den dort vertretenen Sicherheitsbehörden ausgetauscht, sodass diese ggf. Maßnahmen in eigener Zuständigkeit ergreifen können.

Das Bundesamt für Verfassungsschutz (BfV) kann bei Vorliegen von Erkenntnissen die Betroffenen informieren und dabei unterstützen, die entsprechenden Vorkehrungen zur Beendigung eines Vorfalls zu treffen oder bei Vorliegen entsprechender Verdachtsmomente den Fall den Strafverfolgungs- bzw. Polizeibehörden melden.

Das Bundesministerium für Wirtschaft und Energie unterstützt über seine Initiative „IT-Sicherheit in der Wirtschaft“ Unternehmen darin, ihre IT-Sicherheit zu verbessern. Insbesondere kleine und mittlere Unternehmen (KMU) werden für das Thema sensibilisiert. Gemeinsam mit IT-Sicherheitsexperten aus Wirtschaft, Wissenschaft und Verwaltung werden konkrete, praxisnahe und verständliche Handlungsanleitungen und Maßnahmen zur Verfügung gestellt, die KMU aktiv zum Thema IT-Sicherheit aufklären und Unterstützungsleistungen zum sicheren Einsatz digitalisierter Prozesse und Geschäftsmodelle erarbeiten. Zusätzlich wird eine Transferstelle „IT-Sicherheit in der Wirtschaft“ eingerichtet, die für die Unternehmen die Unterstützungsangebote bündelt, Informationen und Handlungsempfehlungen verständlich und praxisnah aufbereitet, das Auffinden der passenden Angebote erleichtert und über Best-Practice-Beispiele aus den mittelständischen Unternehmen konkrete Handlungsmöglichkeiten der breiten mittelständischen Wirtschaft bekannt macht.

15. Welcher Schaden für öffentliche Institutionen oder öffentliche Unternehmen ging von Angriffen oder sonstigen sicherheitsrelevanten Aktivitäten seit 2010 nach Kenntnis der Bundesregierung aus (bitte nach Aktivität, betroffener Institution bzw. betroffenen Unternehmen, Art und Höhe der Schäden auflisten)?

Für die Abschätzung der Schäden durch Angriffe oder sonstige sicherheitsrelevante Aktivitäten für öffentliche Institutionen oder öffentliche Unternehmen existieren keine allgemein anerkannten Systematiken. Zudem werden die Schäden nicht systematisch erhoben.

16. Welche gesetzgeberischen und sonstigen Initiativen hat die Bundesregierung im Zusammenhang mit Angriffen oder sonstigen sicherheitsrelevanten Aktivitäten ergriffen (bitte nach Aktivität und jeweiliger Initiative auflisten)?

Die Gewährleistung der Sicherheit von Informations- und Kommunikationssystemen ist für Deutschland von hoher Bedeutung für Gesellschaft und Wirtschaft.

Daher wurde bereits im Jahr 2015 das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) geschaffen. Mit diesem Gesetz wurden die Grundlagen für Sicherungsmaßnahmen und Meldepflichten bei Betreibern Kritischer Infrastrukturen (im Sinne von Betreibern wesentlicher Dienste) insbesondere im BSIG gelegt. Dieses Gesetz bildet den ersten notwendigen Baustein für die Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-RL).

Auf Basis dieses Gesetzes wurde in zwei Schritten die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSIG (BSI-Kritisverordnung – BSI-KritisV) erlassen.

Mit dem Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-RL-UG) vom 30. Juni 2017 hat Deutschland die vom IT-Sicherheitsgesetz noch nicht abgedeckten Bestandteile der NIS-RL in nationales Recht überführt.

Für die Zwecke der praktischen Umsetzung o. g. Rechtsvorschriften wurde das BSI personell und haushälterisch deutlich verstärkt.

Die Gewährleistung von Cybersicherheit in Deutschland verteilt sich themenspezifisch auf Bund und Länder und dort auf die jeweils zuständigen Behörden. Zur Gewährleistung des Informationsaustauschs und der Zusammenarbeit zwischen den beteiligten Stellen wurde das Cyber-Abwehrzentrum (Cyber-AZ) eingerichtet.

Dort sind die für Cyber-Sicherheitsfragen zuständigen Bundesbehörden vertreten. An einer verstärkten Einbindung der Länder wird gearbeitet.

Weitere Maßnahmen stärken die Fähigkeiten deutscher Behörden zur Analyse von und Reaktion auf Sicherheitsvorfälle vor Ort. Dies beinhaltet u. a. die Einrichtung von „Mobile Incident Response Teams“ (MIRTs) im BSI, einer „Quick Reaction Force“ (QRF) beim Bundeskriminalamt und von „Mobile Cyber-Teams“ beim BfV.

Mit dem sog. Cyber-Brief informiert das BfV anlassbezogen zu aktuellen Cyberangriffen und veröffentlicht Indikatoren, mittels derer eine eigene Betroffenheit festgestellt werden kann. Mit diesem Instrument konnten in mehreren Fällen

frühzeitig deutsche Betroffenheiten von Cyberangriffen festgestellt und entsprechende Sicherungsmaßnahmen eingeleitet bzw. mit Hilfe der vom BfV zur Verfügung gestellten technischen Indikatoren Angriffe von vornherein verhindert werden.

Aufbauend auf der Cyber-Sicherheitsstrategie aus dem Jahr 2011 hat Deutschland dieselbe im Hinblick auf Veränderungen der Bedrohungslage und Technik fortentwickelt. 2016 wurde die neue „Cyber-Sicherheitsstrategie für Deutschland“ von der Bundesregierung beschlossen. Sie ist der strategische Überbau für alle laufenden und künftigen Maßnahmen der Bundesregierung im Bereich Cyber-Sicherheit.

17. Wie schätzt die Bundesregierung den Erfolg der ergriffenen Maßnahmen ein?

Lässt sich der Erfolg durch einen zahlenmäßigen Rückgang von Aktivitäten oder ein Rückgang der Höhe der Schäden messen?

Wenn ja, welcher Rückgang ist jeweils zu verzeichnen?

Wie in der „Cyber-Sicherheitsstrategie für Deutschland 2016“ ausgeführt, bedeuten die bislang ergriffenen Maßnahmen eine Weichenstellung für eine zukunftsgerichtete Cyber-Sicherheitspolitik. Cyber-Sicherheit ist inzwischen zu einem wesentlichen Baustein einer Vielzahl strategischer Konzepte und ressortübergreifender Vorhaben der Bundesregierung geworden. Da sich die Rahmenbedingungen stetig ändern, müssen die strategischen Ansätze und Ziele sowie die daraus resultierenden Maßnahmen kontinuierlich ergänzt bzw. weiterentwickelt werden.

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