Deutscher Bundestag **Drucksache 19/17872**

19. Wahlperiode 12.03.2020

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Markus Herbrand, Christian Dürr, Dr. Florian Toncar, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 19/17369 –

Cyberangriffe auf das Bundesministerium der Finanzen

Vorbemerkung der Fragesteller

Seit 2005 stellen das Bundesamt für Verfassungsschutz (BfV), das Bundeskriminalamt (BKA) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) vermehrt zielgerichtete Angriffe gegen Bundesbehörden, Politik und Wirtschaftsunternehmen fest. Diese finden auf hohem technischen Niveau statt und gefährden daher massiv die Informationssicherheit in diesen Bereichen (vgl. https://www.bmi.bund.de/DE/themen/sicherheit/spionageabwehr-wirtschafts-und-geheimschutz/cyberspionage/cyberspionage-artikel.html).

Zu den Zielen, die in besonderem Maße von Cyberangriffen betroffen sind, zählen auch das Bundesministerium der Finanzen (BMF) und die Finanzverwaltung. Die Fragestellenden möchten sich nach dem Ausmaß der Cyberangriffe auf das Finanzressort und die Finanzverwaltung sowie nach den konkreten Gegenmaßnahmen der Bundesregierung erkundigen.

1. Ist das Finanzressort nach Einschätzung der Bundesregierung ein potenzielles Angriffsziel von Cyber-, Hacker- und Trojanerangriffen, und falls ja, aus welchen Gründen?

Ja. Wie der zitierten Internetquelle zu entnehmen ist, gehört u. a. das Bundesministerium der Finanzen zu den von Cyberangriffen betroffenen Behörden.

Regierungsinstitutionen, auch solche im Finanzressort, sind potentielle Ziele von Cyberangriffen staatlicher und nichtstaatlicher Akteure. Die Interessenlage der Angreifer ist dabei je nach Urheber des Cyberangriffs unterschiedlich und richtet sich häufig nach dem tagesaktuellen politischen Geschehen.

Im Falle des Finanzressorts können die aus der spezifischen Aufgabenstellung von Finanzverwaltung erschließbaren Informationen aus der Festsetzung und Erhebung von Steuern, insbesondere der in diesem Zusammenhang erhobenen, hochsensiblen personenbezogenen Daten sowie die auf Ebene der obersten Bundesbehörde liegende Zuständigkeit für die Steuer- und Haushaltspolitik im nationalen sowie internationalen Rahmen (einschließlich der Europäischen Finanzpolitik), für potentielle Angreifer von großem Interesse sein.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums der Finanzen vom 10. März 2020 übermittelt.

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

2. Welche Datenbanken und Informationen aus dem Finanzressort sind aus Sicht der Bundesregierung besonders schutzbedürftig, um die Informationssicherheit zu gewährleisten (bitte namentlich aufführen)?

Nach sorgfältiger Abwägung können weder die im Finanzressort betriebenen Fachverfahren bzw. Datenbanken noch deren Schutzbedarfe explizit benannt werden, da deren Bekanntwerden möglichen Akteuren Informationen liefern würden, die zu gezielteren Angriffen führen könnten. Da dies die Aufgabenerfüllung des BMF gefährden könnte, muss die Weitergabe der Information aus Staatswohlgründen unterbleiben. Wegen der besonderen Sensibilität der Informationen kommt die Bundesregierung nach Abwägung zudem zu der Auffassung, dass auch eine eingestufte Übermittlung nicht in Betracht kommt.

Als elementare Verfahren im BMF, seien jedoch beispielhaft das hiesige Personalverwaltungssystem (PVS) und das Dokumentenmanagementsystem (DMS) genannt.

PVS dient u. a. der Vergütung/Besoldung, Erfassung von Arbeits-, Abwesenheitszeiten, Aus- und Fortbildungen sowie dem Arbeitsschutz. Ein Ausfall bzw. Systemschaden beträfe die Beschäftigten demnach persönlich.

Nach § 12 GGO sind die Ministerien verpflichtet, Akten zu führen und dort den Stand und die Entwicklung der Vorgangsbearbeitung nachvollziehbar darzulegen. Insofern gilt das DMS als Grundlage des Verwaltungshandelns als besonders schützenswert. Weitere Fachverfahren/Datenbanken dienen zur Vereinfachung der Zusammenarbeit oder als Hilfsmittel bei Berechnungen, Prognosen, Auswertungen. Relevante Ergebnisse sind nachvollziehbar in den Akten zu hinterlegen.

3. Wie viele Cyber-, Hacker- und Trojanerangriffe gab es nach Kenntnis der Bundesregierung wann auf das BMF und die jeweiligen ihm unterstellten Behörden seit dem 24. Oktober 2017 bis zum heutigen Stichtag, und von wo aus wurden diese Angriffe wann ausgeführt (bitte alle Behörden tabellarisch darstellen und nach Datum des Cyberangriffs, Anzahl der Cyberangriffe und Ort aufschlüsseln)?

   a) Wann, und wie viele Angriffe auf Passwörter gab es in welcher Behörde?

   b) Wann, und wie viele Infizierungen mit Schadsoftware bzw. Malware gab es in welcher Behörde?

   c) Wann, und wie viele Phishing-Angriffe gab es in welcher Behörde?

   d) Wann, und wie oft wurden Software-Schwachstellen in welchen Behörden ausgenutzt?

   e) Wann, und wie viele DDOS-Attacken gab es in welcher Behörde?

   f) Wann, und wie viele „Man-in-the-middle“-Angriffe oder Mittelsmann-Angriffe gab es in welcher Behörde?

   g) Wann, und wie viele Fälle von Spoofing gab es in welcher Behörde?

Cyber-, Hacker- und Trojanerangriffe bei Bundesbehörden werden nach § 4 BSIG beim Bundesamt für Sicherheit in der Informationstechnik (BSI) erfasst. Auswertungen können den öffentlich zugänglichen, jährlichen Lageberichten (https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html) entnommen werden (siehe auch die Antwort der Bundesregierung auf die Kleinen Anfrage der Fraktion der FDP auf Bundestagsdrucksache 19/7607).

Dem BSI als zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes sind nach § 4 BSIG „Informationen insbesondere zu Sicherheitslü-

cken, Schadprogrammen, erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und der dabei beobachteten Vorgehensweise“ zu übersenden. Dies erfolgt regelmäßig durch die Behörden des Finanzressorts. Jedoch führen weder das BMF noch die ihm unterstellten Behörden derart dezidierte Statistiken, mit denen die konkreten Fragen beantwortet werden können.

4. Gab es nach Kenntnis der Bundesregierung seit der Einführung des automatischen Informationsaustauschs über Finanzkonten (AIA) Cyberangriffe auf die AIA-Daten, und falls ja, wann fanden diese statt, von wo aus wurden diese durchgeführt, und konnten AIA-Daten von den Angreifern erbeutet werden?

Der Bundesregierung liegen keine Hinweise auf Cyberangriffe auf AIA-Daten vor.

5. Wurden nach Kenntnis der Bundesregierung AIA-Datensätze, die Deutschland an andere Länder übermittelt hat, Ziel von Cyberangriffen, und falls ja, welche Länder wurden wann angegriffen, und konnten Daten erbeutet werden?

Der Bundesregierung liegen hierzu keine Erkenntnisse vor.

6. Bei wie vielen Fällen von Cyber-, Hacker- und Trojanerangriffen seit dem 24. Oktober 2017, die der Bundesregierung im Finanzressort bekannt sind, konnten Datensätze und Informationen erbeutet werden?

   In wie vielen Fällen kann die Bundesregierung und in wie vielen Fällen kann sie nicht sicher ausschließen, dass Daten abgeflossen sind?

Der Bundesregierung sind keine Fälle im Finanzressort bekannt, bei denen Datensätze oder Informationen erbeutet werden konnten oder Daten abgeflossen sind.

7. Wie oft waren nach Kenntnis der Bundesregierung die Finanzverwaltungen der Länder von Cyberangriffen und Trojanern seit dem 24. Oktober 2017 bis zum heutigen Stichtag betroffen, und von wo aus wurden diese Angriffe wann ausgeführt?

Der Bundesregierung liegen keine Kenntnisse über Cyberangriffe oder Trojaner vor, die die Finanzverwaltung der Länder betreffen.

8. Kann die Bundesregierung bestätigen, dass die Finanzverwaltung in Niedersachsen aufgrund eines Trojanerangriffs mit „Emotet“ im Januar 2020 nur eingeschränkt erreichbar ist?

   Hat die Bundesregierung mit den niedersächsischen Behörden Kontakt aufgenommen, um sich nach der Situation zu erkundigen und ggf. Hilfe anzubieten?

Der Vollzug der Steuergesetze obliegt nach der Kompetenzordnung des Grundgesetzes den Ländern. Die Länder sind damit für die Umsetzung des Besteuerungsverfahrens – insbesondere auch für die automationstechnische Unterstützung – zuständig und bearbeiten derartige Vorfälle grundsätzlich in eigener Zuständigkeit.

Das Land Niedersachsen hat sich zu der Thematik nicht an die Bundesregierung gewandt.

9. Welche Vor- und Nachteile erkennt die Bundesregierung hinsichtlich einer generellen Pflicht für Unternehmen, Cyberangriffe an eine staatliche Stelle zu melden, und setzt sich die Bundesregierung für diese Meldepflicht ein?

Voraussetzung für die nationale Handlungsfähigkeit bei Cyberangriffen und Grundlage für bundesweit abgestimmte Reaktionen sind zunächst Meldungen über solche Angriffe an eine Behörde, damit dort ein valides Lagebild erstellt werden kann. Eine bundesweite Meldepflicht ist daher aus Sicht der Bundesregierung wünschenswert.

Eine staatliche Meldepflicht muss dabei jedoch so ausgestaltet sein, dass der damit beim Meldenden entstehende Aufwand in einem angemessenen Verhältnis zu dem gesamtstaatlichen Schadenspotential eines Cyberangriffs steht.

Mit dem Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vom 17. Juli 2015 (IT-Sicherheitsgesetz) wurden daher zunächst nur die Betreiber kritischer Infrastrukturen in Deutschland verpflichtet, erhebliche Störungen, die die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse betreffen, (dem BSI) zu melden.

Diese Meldepflicht hat sich aus Sicht der Bundesregierung bewährt. Gleichwohl beobachtet die Bundesregierung aufmerksam die zunehmende Abhängigkeit weiterer Wirtschaftsbereiche von informationstechnischen Systemen im Zusammenhang mit ihrer gesamtstaatlichen Bedeutung.

Eine generelle Pflicht für Unternehmen, Cyberangriffe an eine staatliche Stelle zu melden, verursacht voraussichtlich einen hohen Aufwand an Bürokratie bei den Unternehmen und beim Staat. Ein Mehrwert gegenüber den bereits vorhandenen Verfahren, die die Bundesregierung unterstützt, ist nicht erkennbar.

Im Rahmen der Allianz für Cyber-Sicherheit können Unternehmen bzw. Institutionen aktuelle Warnmeldungen, Unterstützung bei Cyberangriffen und Hintergrundinformationen im Bereich der Cyberbedrohung erhalten und ihre Cyberangriffe freiwillig melden.

10. Wie hoch ist nach Kenntnis der Bundesregierung der finanzielle Schaden für die deutsche Wirtschaft, der aus Spionage und Cyber-, Hacker- und Trojanerangriffen hervorgeht, und wie hat sich dieser in den vergangenen Jahren entwickelt (bitte Angaben aus Schätzungen aufführen, die der Bundesregierung übermittelt wurden und vorliegen)?

Die Bundesregierung verfügt zum Ausmaß der finanziellen Schäden für die deutsche Wirtschaft über keine eigenen Erhebungen oder Schätzungen, die über die öffentlich zugänglichen Informationen hinausgehen. Sie verweist auf die Aussagen des Branchen-verbandes BITKOM vom 6. November 2019. Danach haben digitale Angriffe bei der Mehrzahl der Unternehmen einen Schaden verursacht. Insgesamt beziffert BITKOM auf der Basis der Selbsteinschätzung der Unternehmen einen Schaden von 205,7 Mrd. Euro in den letzten zwei Jahren (vgl. https://www.bitkom.org/sites/default/files/2019-11/bitkom_wirtschaftsschutz_2019.pdf).

11. Wie viele Unternehmen waren nach Kenntnis der Bundesregierung in den letzten zwei Jahren von Datendiebstahl, Industriespionage oder Sabotage

    a) betroffen,

    b) vermutlich betroffen?

Es wird auf die Antwort zu Frage 10 verwiesen.

12. Welche Maßnahmen plant die Bundesregierung, um gegen Cyber-, Hacker- und Trojanerangriffe auf das Finanzressort und die Finanzverwaltung aus dem Ausland vorzugehen?

Die Gewährleistung der Sicherheit von Informations- und Kommunikationssystemen ist für Deutschland von hoher Bedeutung für Staat, Wirtschaft und Gesellschaft. Daher wurde bereits im Jahr 2015 das IT-Sicherheitsgesetz geschaffen. Das Gesetz sieht u. a. Maßnahmen zum Schutz der Bundesverwaltung vor. Für die Bundesregierung sind präventive Maßnahmen ein zentraler, essentieller und wirksamer Baustein eines ganzheitlichen Cyber-Sicherheits-Ansatzes. Dies beinhaltet Schutzsysteme wie Schadsoftwareerkennungs- und -präventionssysteme sowie die Weiterentwicklung von Detektionssystemen zur Angriffserkennung.

Da sich die Rahmenbedingungen stetig ändern, müssen die strategischen Ansätze und Ziele sowie die daraus resultierenden Maßnahmen kontinuierlich ergänzt bzw. weiterentwickelt werden. Deshalb soll das IT-Sicherheitsgesetz um weitere Maßnahmen der Prävention und Detektion für den Schutz der Bundesverwaltung ergänzt werden.

13. Welche Maßnahmen plant die Bundesregierung, um den Informationsaustausch zu IT-Sicherheitsthemen zwischen Staat und Wirtschaft zu verbessern?

Es wurden bereits in jüngster Vergangenheit verschiedene Maßnahmen und Initiativen umgesetzt.

Mit der Allianz für Cybersicherheit (ACS) existiert seit 2012 eine Kooperationsplattform zwischen Staat und Wirtschaft zum Austausch zu Themen der IT-Sicherheit. Als einer der Initiatoren übernimmt das BSI hier eine koordinierende Rolle. Die über 4100 Teilnehmer der ACS bestehen aus Institutionen von Experten bis hin zu Anwendern. Zu den vielfältigen Angeboten der ACS zählen neben den Cyber-Sicherheits-Tagen als Informations-veranstaltungen auch Weiterbildungsmöglichkeiten, die von den Partnern bereitgestellt werden. Getreu dem Motto „Netzwerke schützen Netzwerke“ verfolgt die ACS damit das Ziel, die Widerstandsfähigkeit des Standortes Deutschland gegenüber Cyber-Angriffen zu stärken.

Zudem wurde im September 2018 das sogenannte „Cyberbündnis mit der Wirtschaft“ zwischen dem Bundesministerium des Innern, für Bau und Heimat (BMI) und dem Bundesverband der Deutschen Industrie e. V. (BDI) etabliert. BDI und BMI haben in enger Kooperation als erstes Arbeitsergebnis eine kompakte Übersicht zu bestehenden Cybersicherheitsinitiativen erstellt. So können bestehende Kooperationen von Unternehmen zukünftig besser identifiziert, genutzt und die Verzahnung zwischen den Initiativen gestärkt werden. Langfristig ist zudem eine engere Kooperation zwischen den Initiativen sinnvoll. Um diesen Gedanken weiter voranzutreiben, werden BMI und BDI in Zukunft in einem geeigneten Dialogformat – wie etwa im Rahmen der Allianz für

Cybersicherheit – zur Optimierung der Kooperation und zu einer besseren Vernetzung von Staat und Wirtschaft einladen.

Mit der Initiative „IT-Sicherheit in der Wirtschaft“ (https://www.it-sicherheit-in-der-wirt-schaft.de/ITS/Navigation/DE/Home/home.html) unterstützt das Bundesministerium für Wirtschaft und Energie (BMWi) Unternehmen darin, ihre IT-Sicherheit zu verbessern. Insbesondere kleine und mittelständische Unternehmen (KMU) werden für das Thema sensibilisiert. Durch konkrete Hilfsangebote bei der Erhöhung ihres IT-Sicherheitsniveaus, werden KMU unterstützt (z. B. durch Webseitenchecks, Handlungsleitfäden, Schulungs- und Lehrmaterialien). Hierzu sind in den vergangenen Jahren eine Reihe von Einzelprojekten gefördert worden, die konkrete Unterstützungs-, Sensibilisierungs- und Qualifikationsangebote für KMU erarbeiten. Im Rahmen der Initiative hat das BMWi Anfang Februar 2020 eine Transferstelle gestartet.

Mit der Pressemitteilung des BMWi vom 2. Februar 2020 wurde der Start der Transferstelle „IT-Sicherheit in der Wirtschaft“ vorgestellt, die vorhandene Unterstützungsangebote für den Mittelstand bündelt und praxisnah und verständlich aufbereitet (vgl. Pressemitteilung vom 2. Januar 2020 https://www.bmwi.de/Redaktion/DE/Pressemitteilungen/2020/20200102-altmaier-wir-machen-mittelstand-fit-gegen-cyberattacken.html).

14. Welche Maßnahmen plant die Bundesregierung, um den Informationsaustausch zu IT-Sicherheitsthemen zwischen Finanzverwaltung und steuerpflichtigen Bürgerinnen und Bürgern zu verbessern?

Für eine sichere Kommunikation zwischen Externen und der Steuerverwaltung wird von der Steuerverwaltung das Verfahren ELSTER zur Verfügung gestellt. Alle mit ELSTER elektronisch übermittelten Daten werden stark verschlüsselt übertragen. Es wird regelmäßig geprüft, ob die hierzu verwendeten Algorithmen den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI, www.bsi.de) entsprechen. Die Kommunikationskanäle über das Internet sind technisch gesichert und für die ELSTER-Webseiten wird ein spezielles Zertifikat genutzt, damit der Anwender sicher sein kann, dass eine hochgradige Verschlüsselung zum Einsatz kommt und er mit einer vertrauenswürdigen ELSTER-Seite verbunden ist. Die Leistungen von ELSTER werden in einer nach ISO 27001 auf Basis der IT-Grundschutz-Kataloge des BSI zertifizierten, eigenen IT-Infrastruktur erbracht. Bezüglich des Datenschutzes steht das Verfahren ELSTER in laufendem Kontakt mit dem Datenschutz Cert (beim BSI akkreditierte Prüfstelle für IT-Sicherheit, www.datenschutz-cert.de) und die Einhaltung von Datenschutz-Standards wird regelmäßig intern überprüft. All diese Maßnahmen dienen dem Schutz der mit der Steuerverwaltung ausgetauschten Informationen gegen unbefugte Kenntniserlangung durch Dritte.

15. Welche Maßnahmen plant die Bundesregierung, um die Wirtschaft bei Fragen zur IT-Sicherheit besser zu unterstützen?

Im Rahmen von allgemeinen Präventionsveranstaltungen informiert die Bundesregierung mit ihren Sicherheitsbehörden zudem über aktuelle und grundsätzliche Gefahren im Bereich der IT-Sicherheit. Diese werden in der Regel im Rahmen von IT-Sicherheitsveranstaltungen oder anderen fachspezifischen Messen oder Konferenzen durchgeführt. Darüber hinaus unterstützt die Bundesregierung mit ihren Sicherheitsbehörden die Wirtschaft bei konkreten staatlich gesteuerten Cyberangriffen durch Sensibilisierungsmaßnahmen, Hinweise zu Handlungsmöglichkeiten sowie „Best-Practice-Beispiele“ und bei Bedarf ggf. Vermittlung von Kontakten zu anderen Sicherheitsbehörden.

Darüber hinaus wird auf die Antwort zu Frage 13 verwiesen, in der verschiedene Maßnahmen und Initiativen beschrieben werden.

16. Welche Maßnahmen plant die Bundesregierung, um den Informationsaustausch innerhalb der Finanzverwaltung zu verbessern?

Es wird auf die Antwort zu Frage 14 verwiesen.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.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