Deutscher Bundestag **Drucksache 19/29669**

19. Wahlperiode 14.05.2021

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Bernd Reuther, Frank Sitta, Torsten Herbst, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 19/28718 –

Cyberangriffe auf das Bundesministerium für Verkehr und digitale Infrastruktur

Vorbemerkung der Fragesteller

Seit 2005 stellen das Bundesamt für Verfassungsschutz (BfV), das Bundeskriminalamt (BKA) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) vermehrt zielgerichtet Angriffe gegen Bundesbehörden, Politik und Wirtschaftsunternehmen fest. Diese finden auf hohem technischem 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 für Verkehr und digitale Infrastruktur (BMVI) und dessen nachgeordnete Behörden. Diese besitzen zahlreiche Informationen zu Fahrzeughaltern und deren personenbezogenen Daten (Schifffahrt, Straßen- und Luftverkehr). Die Fragestellenden möchten sich nach dem Ausmaß der Cyberangriffe auf das Verkehrsressort und die Verwaltung der Verkehrs- und digitalen Infrastruktur sowie nach den konkreten Gegenmaßnahmen der Bundesregierung erkundigen.

1. Sind das BMVI und dessen nachgeordnete Behörden nach Einschätzung der Bundesregierung potenzielle Angriffsziele von Cyber-, Hacker- und Trojanerangriffen, und falls ja, aus welchen Gründen?

Nach Auffassung der Bundesregierung sind das Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) und dessen nachgeordnete Behörden nicht in größerem Maße potentielle Angriffsziele von staatlichen und nichtstaatlichen Cyberakteuren und Cyberkriminellen wie andere Organisationen, die sich im Internet bewegen oder mit diesem verbunden sind.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums für Verkehr und digitale Infrastruktur vom 14. Mai 2021 übermittelt.
Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

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

Im nachgeordneten Geschäftsbereich des BMVI werden in mehreren Behörden Informationen mit sehr hohem Schutzbedarf verarbeitet. Ein „sehr hoher“ Schutzbedarf im Sinne der Anlage 2.12 Informationssicherheitsmanagement wird nach Schutzbedarfskategorien der Gemeinsamen Geschäftsbedingungen mit dem Informationstechnikzentrum Bund in der Version 2.3.4 definiert.

Das BMVI ist nach sorgfältiger Abwägung der Auffassung, dass im Übrigen eine Beantwortung der Frage aus Gründen des Staatswohls nicht erfolgen kann.

Die erbetenen Informationen sind als Informationen mit sehr hohem Schutzbedarf auch in Ansehung des parlamentarischen Fragerechts geheimhaltungsbedürftig, weil sie sicherheitsrelevante Angaben enthalten, deren Bekanntwerden für die Sicherheit der Bundesrepublik Deutschland nachteilig sein und eine Gefahr für Leib und Leben bedeuten könnte, oder ihre Sicherheit gefährden bzw. ihr schweren Schaden zufügen könnte. Die Datenbanken und dazugehörigen Informationen bestehen um beispielsweise kritische Infrastrukturen im Sektor Transport und Verkehr im Sinne der Verordnung zur Bestimmung kritischer Infrastrukturen nach dem BSI-Gesetz vor internen sowie externen staatlichen und nichtstaatlichen Cyberangriffen (Cyber-Terrorismus) zu schützen oder Individuen vor Verfolgung und Denunzierung zu bewahren.

Detaillierte Angaben zu besonders schutzwürdigen Datenbanken oder Informationen könnten gezielte elektronische Angriffe ermöglichen oder erleichtern, so dass ein Risiko des Bekanntwerdens im Falle einer eingestuften Beantwortung der Frage – auch unter Berücksichtigung des hohen Stellenwerts des parlamentarischen Fragerechts – unter keinen Umständen hingenommen werden kann.

3. Wie viele Cyber-, Hacker- und Trojanerangriffe gab es nach Kenntnis der Bundesregierung wann auf das BMVI 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 Softwareschwachstellen in welchen Behörden ausgenutzt?

   e) Wann, und wie viele DDoS-Attacken (DDoS = Distributed Denial of Service) gab es in welcher Behörde?

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

   g) Wie viele Fälle von Spoofing gab es wann in welcher Behörde?

6. Bei wie vielen Fällen von Cyber-, Hacker- und Trojanerangriffen seit dem 24. Oktober 2017, die der Bundesregierung im BMVI oder dessen nachgeordneten Behörden 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?

Die Fragen 3 und 6 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Das Schadprogramm-Erkennungssystem (SES) dient insbesondere der Detektion höherwertigerer, ggf. auch nachrichtendienstlicher Angriffe gegen die Regierungsnetze. Konkrete Zahlenwerte könnten Angreifern wertvolle Informationen über die Leistungsfähigkeit dieser Schutzmaßnahme und ggf. die Detektion eigens durchgeführter Angriffskampagnen liefern. Aus diesem Grund werden diese Kennzahlen kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres im Bericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) an den Innenausschuss des Bundestags, auf den hier Bezug genommen wird, nur eingestuft herausgegeben.

4. Gab es nach Kenntnis der Bundesregierung seit der Einführung des verpflichteten Einbau einer OBFCM-Einrichtung (OBFCM = On Board Fuel Consumption Monitoring) Cyberangriffe auf die Daten, und falls ja, wann fanden diese statt, von wo aus wurden diese durchgeführt, und konnten AIA-Daten (AIA = Automatischer Informationsaustausch) von den Angreifern erbeutet werden?

5. Wurden nach Kenntnis der Bundesregierung OBFCM-Einrichtungsdatensätze, die an die Europäische Kommission übermittelt wurden, Ziel von Cyberangriffen, und falls ja, welche Daten konnten erbeutet werden?

7. Wie oft waren nach Kenntnis der Bundesregierung die Verkehrsverwaltung 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?

Die Fragen 4, 5 und 7 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Der Bundesregierung liegen hierzu keine eigenen Informationen vor.

8. 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?

Meldepflichten für Unternehmen sind für die Betreiber Kritischer Infrastrukturen gesetzlich geregelt, um die Sicherstellung der Versorgung der Bevölkerung mit den jeweiligen Leistungen dieser Infrastrukturen zu gewährleisten (vgl. § 8b BSIG).

Die Etablierung von Meldewegen zwischen den jeweiligen Ansprechpartnern für IT-Sicherheitsthemen im Vorfeld eines konkreten Vorfalls hat sich bewährt, um die Reaktionsfähigkeit im Ernstfall sicherzustellen. Da nicht nur Cyberangriffe, sondern auch Sicherheitsvorfälle mit Bezug zu IT-Systemen gemeldet werden müssen, wird das BSI darüber hinaus in die Lage versetzt, mit den Meldenden systemische Probleme und Schwachstellen in den IT-Systemen zu identifizieren.

Die im Entwurf des zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme verankerte Ausweitung von Meldepflichten auf Unter-

nehmen, die von besonderem öffentlichen Interesse sind, soll zur weiteren Verbesserung der Krisenreaktionsfähigkeit in diesen Bereichen beitragen.

Gleichzeitig werden die staatlichen Stellen durch die Meldungen befähigt, Lagebilder zu erstellen, zu verteilen sowie Warnungen, Hinweise und Hilfestellungen in Ansehung der aktuellen Lage an Akteure in Staat, Wirtschaft und Gesellschaft zu geben.

Es entspricht der allgemeinen Sorgfaltspflicht der Unternehmen, dass sie die Sicherheit ihrer IT-Systeme überwachen. Zusätzliche Nachteile für die einer Meldepflicht unterliegenden Unternehmen entstehen nach Auffassung der Bundesregierung – abgesehen von den Kosten für die Durchführung der Meldungen – nicht.

9. 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, die der Bundesregierung übermittelt wurden und vorliegen, aufführen)?

Die Bundesregierung erhebt keine systematischen Informationen über den volkswirtschaftlichen Schaden durch Cyber-Angriffe in Deutschland.

Darüber hinaus wird auf die Antwort der Bundesregierung zu der Frage 2 auf Bundestagsdrucksache 19/21675 verwiesen.

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

a) betroffen,

b) vermutlich betroffen?

Der Bundesregierung liegen keine abschließenden Informationen über die Anzahl der betroffenen Unternehmen vor.

Die Anzahl der im Rahmen des § 8b BSIG von Betreibern Kritischer Infrastrukturen gemeldeten Störungen beträgt:

Jahr	**Gemeldete Störungen**
2019	254
2020	345

Nicht alle Störungen sind auf Angriffe bzw. Datendiebstahl, Industriespionage oder Sabotage zurückzuführen. Teilweise handelt es sich um technisches Versagen von Hard- oder Software sowie menschliches Fehlverhalten.

Die Bundesregierung geht von einer weitaus größeren Dunkelziffer an tatsächlichen Cyber-Angriffen aus, da die vorliegenden verpflichteten Meldezahlen und freiwilligen Meldungen nur einen Ausschnitt der Wirtschaft abdecken.

Laut einer repräsentativen Studie des Bundesministeriums für Wirtschaft und Energie, welche im letzten Jahr veröffentlicht wurde, sind 2018/2019 zwei Fünftel (41,1 Prozent; N=4 981) der befragten 5 000 Unternehmen Opfer eines Cyberangriffes geworden. Zu einer weiteren Unterteilung nach Straftatbeständen können keine weiterführenden Angaben gemacht werden, aktuellere Zahlen für die Jahre 2020 und 2021 liegen nicht vor.

11. Welche Maßnahmen setzt die Bundesregierung bereits um, um gegen Cyber-, Hacker- und Trojanerangriffe auf das BMVI und dessen nachgeordnete Behörden vorzugehen?

Das BSI bietet im Rahmen seines gesetzlichen Auftrages eine Vielzahl von Maßnahmen an, um gegen Cyber-, Hacker- und Trojanerangriffe vorzugehen. Diese reichen beispielhaft von der Beratung über Lageinformationen und Warnungen bis hin zur Unterstützung bei IT-Sicherheitsvorfällen.

Neben dezentralen Schutzmaßnahmen der einzelnen Behörden kommen in den Regierungsnetzen zentrale Schutzmaßnahmen wie das Schadprogramm-Erkennungs-System (SES) des BSI zum Einsatz. Diese Maßnahmen tragen erheblich zur Reduktion des Risikos erfolgreicher Cyber-Angriffe gegen die Behörden in den Regierungsnetzen bei.

12. Welche Maßnahmen setzt die Bundesregierung bereits um, um den Informationsaustausch zu IT-Sicherheitsthemen zwischen Staat und Wirtschaft zu verbessern?

14. Welche Maßnahmen setzt die Bundesregierung bereits um, um die Wirtschaft bei Fragen zur IT-Sicherheit besser zu unterstützen?

Die Fragen 12 und 14 aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Mit dem UP KRITIS und der Allianz für Cybersicherheit bestehen zwei etablierte Public Private Partnerships, in denen ein enger Austausch zwischen Unternehmen und Bundes- und Landesbehörden gepflegt wird. Gleichzeitig werden in diesen Netzwerken gegenseitige Unterstützungen in Form von Informationsaustausch, Fort- und Weiterbildungen als auch Beratung geteilt.

Zudem steht das BSI als zentrale Cybersicherheitsbehörde des Bundes den Unternehmen beratend zur Seite. Von den besonders im Fokus stehenden Betreibern Kritischer Infrastrukturen über die Verbände bis zum kleinen und mittelständischen Unternehmen.

Zusätzlich zu Informationsangeboten, dem Teilen von Warnungen, Lageinformationen sowie Hilfestellungen stellt das BSI zielgruppenspezifische Angebote bereit, um die Informationssicherheit in Unternehmen zu verbessern. Dies umfasst auch die Bereitstellung von konkreten IT-Grundschutzprofilen für einzelne Wirtschaftsbereiche (siehe z. B. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Profile/Profile/itgrundschutzProfile_Profile_node.html) ebenso wie die themenspezifische Aufbereitung der IT-Sicherheit für aktuelle Digitalisierungsthemen (siehe z. B. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Digitalisierung_made-in-GER.html).

Das Bundesamt für Verfassungsschutz (BfV) steht in enger Zusammenarbeit mit anderen zuständigen Behörden im kontinuierlichen Dialog mit verschiedensten Unternehmen und identifiziert frühzeitig mögliche sicherheitsrelevante Schwachstellen anhand einer eigenen und zielgruppenspezifisch aufgearbeiteten Lagebewertung. Mit Hilfe von Sensibilisierungsprogrammen und anlassbezogenen Gesprächen steht das BfV der Wirtschaft als Ansprechpartner zur Verfügung und adressiert ebenfalls aktiv bestehende Bedrohungslagen. Darüber hinaus engagiert sich das BfV in der „Initiative Wirtschaftsschutz“ des Bundesministeriums des Innern, für Bau und Heimat (BMI), die die Zielsetzung verfolgt, Sicherheitsthemen gerade kleinen und mittelständischen Unternehmen zielgruppengerecht zur Verfügung zu stellen.

In der Zusammenarbeit mit der Wirtschaft und mit von staatlichen Cyberangriffen betroffenen Unternehmen sensibilisiert das BfV regelmäßig durch Veranstaltungen und Gespräche sowie die Übermittlung von Warnmeldungen und technischen Indikatoren zur Überprüfung der IT-Systeme.

13. Welche Maßnahmen setzt die Bundesregierung bereits um, um den Informationsaustausch zu IT-Sicherheitsthemen zwischen der Verkehrsverwaltung des Bundes und Bürgerinnen und Bürgern zu verbessern?

Ein unmittelbarer Austausch zwischen der Verkehrsverwaltung des Bundes und Bürgerinnen und Bürgern besteht nicht. Das BSI stellt auf seiner Webseite (www.bsi.de) wichtige Sicherheitsempfehlungen, Informationen zu aktuellen Sicherheitsrisiken bzw. Angriffsmethoden sowie Kontakt- und Beteiligungsmöglichkeiten zur Verfügung.

15. Welche Maßnahmen plant die Bundesregierung, um den Informationsaustausch innerhalb der Verkehrsverwaltung des Bundes zu verbessern?

In Bezug auf IT- Sicherheit in der Verkehrsverwaltung finden regelmäßig Austausche der IT- und Informationssicherheitsbeauftragten der Ressortbehörden untereinander und darüber hinaus auch ein Austausch und Abstimmungen der IT-Sicherheitsbeauftragten der Ressortbehörden mit dem Ressort-IT-Sicherheitsbeauftragten statt; anlassbezogen werden das BSI oder Unternehmen der IT-Sicherheit einbezogen. Der Informationsaustausch innerhalb der Verkehrsverwaltung findet zudem auf weiteren Ebenen statt (Besprechungen der Behördenleitungen, der IT-Leiter-Besprechungen und zum Beispiel im IT-Rat Ressort).

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