Deutscher Bundestag **Drucksache 19/21711**

19. Wahlperiode 20.08.2020

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Gerald Ullrich, Michael Theurer, Reinhard Houben, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 19/21478 –

Cyberangriffe auf die deutsche Wirtschaft während der COVID-19-Pandemie

Vorbemerkung der Fragesteller

Im Zuge der COVID-19-Pandemie hat die deutsche Wirtschaft einen Digitalisierungsschub zu verzeichnen. Homeoffice und Videokonferenzen haben sich in ihrer Akzeptanz deutlich verbessert. Auch der deutsche Mittelstand hat hierbei hohen Anpassungswillen gezeigt. Doch mit der größeren Verbreitung digitaler Anwendungen im Geschäftsablauf wächst auch die Angriffsfläche für Cyberkriminelle. So musste beispielsweise der Halbleiterhersteller X-Fab in seinem Werk in Erfurt für mehrere Tage die Produktion einstellen, nachdem dieses von einem Angriff getroffen wurde (https://www.mdr.de/thueringen/mitte-west-thueringen/erfurt/x-fab-erfurt-keine-produktion-nach-cyber-angriff-100.html).

Dabei besitzen große Unternehmen zumeist eine eigene IT-Abteilung, welche sich grundlegend mit der Cybersicherheit des Unternehmens beschäftigt. Kleine und mittlere Betriebe hingegen verfügen häufig weder über die Kapazitäten noch die Kompetenzen, um sich allein gegen Cyberangriffe zur Wehr zu setzen. Das Arsenal an Mitteln der Cyberangriffe ist dabei so divers wie die jeweiligen Ziele. Erpressung, Sabotage oder Spionage – der Schaden kann existenzbedrohend sein. Für Aufsehen sorgten auch gefälschte Internetseiten zur Beantragung von Corona-Soforthilfen, welche dazu dienten, Daten abzugreifen. Kleine und mittlere Unternehmen (KMU) sind dabei häufig nur Mittel zum Zweck, um an Daten der jeweiligen Kunden, meist der Großunternehmen, zu gelangen. Gerade in der Stresssituation der COVID-19-Pandemie mussten Unternehmen schnell handeln. Inwieweit sich Cyberkriminelle diesen Druck zunutze gemacht haben, wurde bisher wenig beachtet.

Bereits vor der COVID-19-Pandemie war ein Großteil der Unternehmen von Cyberattacken betroffen (Sichere Digitalisierung im Mittelstand, https://www.it-sicherheit-in-der-wirtschaft.de/ITS/Redaktion/DE/Publikationen/it-sicherheitsstudie-kurzfassung.pdf)?__blob=publicationFile&v=6). Hilfen bei der Cybersicherheit bieten etwa die auf diesen Bereich spezialisierten Mittelstandskompetenzzentren. Auch die Cyberwehr Baden-Württemberg (https://cyberwehr-bw.de/#!/prozess) dient im Notfall als Unterstützung und wurde für Unternehmen im medizintechnischen Bereich während der COVID-19-Pandemie bundesweit bereitgestellt. Aus Sicht der Fragesteller besteht allerdings die Ge-

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 18. August 2020 übermittelt.

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

fahr, dass die schnelle Umstellung auf digitale Prozesse, welche meist ohne weitere Hilfe stattfinden musste, die Gefahr für Cyberangriffe erhöht hat.

1. Haben sich nach Kenntnis der Bundesregierung Cyberangriffe auf deutsche Unternehmen während der COVID-19-Pandemie verstärkt (etwa Anzahl der Fälle), und wenn ja,
   a) welche Methoden und Werkzeuge wurden vornehmlich eingesetzt,
   b) wurden neue Methoden oder Werkzeuge eingeführt, welche spezifisch auf die COVID-19-Pandemie zugeschnitten waren,
   c) inwieweit wurden besonders KMU vermehrt zum Ziel von Cyberangriffen,
   d) welche Auswirkungen auf die politische Arbeit der Bundesregierung würde ein solcher Anstieg auslösen?

Die Fragen 1 bis 1d werden gemeinsam beantwortet.

Die Bundesregierung verzeichnet bislang keinen signifikanten quantitativen Anstieg an Cyber-Angriffen auf deutsche Unternehmen, der auf die COVID-19-Pandemie zurückzuführen ist.

2. Wie hoch liegt nach Kenntnis der Bundesregierung der Schaden durch Cyberangriffe während der COVID-19-Pandemie?

   Inwieweit unterscheidet sich dessen Höhe von nicht-Pandemie-Zeiten?

   Was sind Gründe für einen möglichen Unterschied?

Der Bundesregierung liegen hierzu keine belastbaren Zahlen vor.

Es kann daher auch kein Verhältnis zu nicht-Pandemie-Zeiten hergestellt werden.

3. Welche Einschätzung besitzt die Bundesregierung über das Dunkelfeld der Cyberkriminalität mit dem Ziel auf deutsche Unternehmen, insbesondere KMU (Anzahl von Straftaten, Schadenshöhe)?

Die Bundesregierung geht von einem hohen Dunkelfeld aus. Über die Anzahl der tatsächlichen Straftaten und die mögliche Gesamtschadenshöhe können keine Angaben gemacht werden.

4. Welche Maßnahmen unternimmt die Bundesregierung vor dem Hintergrund, dass sie in ihrem Bericht „Sichere Digitalisierung im Mittelstand: Aktueller Stand und zukünftige Themen“ (https://www.it-sicherheit-in-der-wirtschaft.de/ITS/Redaktion/DE/Publikationen/it-sicherheitsstudie-kurzfassung.pdf?__blob=publicationFile&v=6) vom Januar 2020 vorwiegend auf Zahlen von Branchenverbänden und Wissenschaft aus den Jahren bis 2018 verweist, um
   a) in einem solch essentiellen Thema stets auf dem aktuellen Stand der Diskussion zu sein,
   b) jährlich oder quartalsweise Informationen zu diesem Thema zu veröffentlichen?

Die Fragen 4 bis 4b werden gemeinsam beantwortet.

Das Thema IT-Sicherheit im Mittelstand ist von großen Dunkelfeldern geprägt, die nur indirekt, z. B. über wissenschaftliche Studien oder Umfragen von Branchenverbänden, erhellt werden können:

Im Rahmen des Nationalen Pakts Cybersicherheit hat das Bundesministerium des Innern, für Bau und Heimat die zahlreichen in Deutschland existierenden Akteure und Beiträge im Bereich der Cybersicherheit strukturiert erhoben. Diese Informationen werden derzeit in einem Online-Kompendium mit einem Gesamtbild der Cybersicherheitsaktivitäten in Deutschland zusammengestellt, das nach seiner Fertigstellung veröffentlicht wird.

Das Bundesministerium für Wirtschaft initiiert zudem wissenschaftliche Forschung, deren Ergebnisse regelmäßig veröffentlicht werden (vgl. zuletzt Cyberangriffe gegen Unternehmen in Deutschland. Ergebnisse einer qualitativen Interviewstudie mit Experten (KFN-Forschungsberichte No. 155). Hannover: KFN, https://kfn.de/wp-content/uploads/Forschungsberichte/FB155.pdf, vom März 2020). Weiterhin wird derzeit eine Studie zum Thema KMU als Nachfrager von IT-Dienstleistungen für mehr IT-Sicherheit bei KMU erarbeitet.

5. Welche Schlüsse zieht die Bundesregierung aus den Fake-Seiten zur Beantragung der Corona-Soforthilfen (https://www1.wdr.de/nachrichten/themen/coronavirus/fake-seite-nrw-wirtschaftsministerium-corona-antraegebetrug-100.html) für zukünftige Projekte, und wie will sie eine Wiederholung verhindern?

   Wie hoch schätzt sie den Schaden für Unternehmen ein, welcher bundesweit durch solche Seiten entstanden ist?

   Kann die Bundesregierung ausschließen, dass Betreiber solcher Seiten an Mittel aus den Hilfsprogrammen gelangt sind?

Die Bundesregierung hat für die Umsetzung der Corona-Überbrückungshilfen des Bundes, die entsprechend der Corona-Soforthilfen von den Ländern durchgeführt wird, im Juli 2020 eine neue Antragsplattform im Rahmen eines Bund-Länder-Projekts zur Umsetzung des Onlinezugangsgesetzes gestartet, die von allen Ländern genutzt wird. Für die Entwicklung und den Betrieb werden hohe Standards für die Datensicherheit, u. a. des Bundesamtes für die Sicherheit in der Informationstechnik (BSI), berücksichtigt. Der Bundesregierung liegen derzeit noch keine validen Informationen zur Schadenshöhe vor, die durch Manipulation der Antragsportale der Länder eingetreten ist.

6. Welches sind nach Kenntnis der Bundesregierung die am häufigsten auftretenden Schwachstellen in der Cybersicherheit bei KMU?

   Plant die Bundesregierung Maßnahmen, um KMU zu helfen, diese Sicherheitslücken zu schließen, und wenn ja, welche?

Das IT-Sicherheitsniveau in deutschen KMU variiert sehr stark. Dies liegt unter anderem am Grad der Digitalisierung in den Unternehmen bzw. Branchen oder auch am dort vorzufindenden Cyber-Sicherheits-Know-how. Eine pauschale Aussage über am häufigsten vorzufindenden Schwachstellen ist daher nicht möglich.

Um jedoch das Know-how in KMU und anderen Organisationen nachhaltig zu erhöhen, hat das BSI mit der Allianz für Cyber-Sicherheit eine Plattform geschaffen, auf der deutschen Institutionen kostenlos praxistaugliche Hinweise zur Verbesserung der Cyber-Sicherheit angeboten werden. Die Informationen werden wahlweise über die Webseite der Initiative oder auf regelmäßigen Ver-

anstaltungen vermittelt. Um tagesaktuell auf Bedrohungen reagieren zu können, stehen außerdem Warnmeldungen von CERT-Bund zur Verfügung.

Die Allianz für Cyber-Sicherheit wurde 2012 gegründet. Seitdem haben sich mehr als 4.000 deutsche Organisationen zur Teilnahme angemeldet, wobei das Gros der Inhalte auch ohne Registrierung genutzt werden kann.

Zudem hilft die neue Transferstelle IT-Sicherheit im Mittelstand KMU, passgenaue Lösungen für mehr IT-Sicherheit zu finden. Mit einem von der Transferstelle derzeit entwickelten auf Künstlicher Intelligenz basierten Werkzeug („SecOmat“) können sich KMU passgenaue IT-Sicherheitslösungen vorschlagen lassen.

Unter dem Dach der Initiative IT-Sicherheit in der Wirtschaft haben neben der Transferstelle auch die Einzelprojekte zum Ziel, das IT-Sicherheitsniveau von KMU zu erhöhen. Derzeit laufen die Projekte „KMU einfach sicher“ und „Grundschutz-plus-Aktivator“. Weitere Projekte sind geplant bzw. in Vorbereitung. Auch die Förderprogramme „Digital Jetzt“ und „go-digital“ verfolgen – neben anderen Aspekten – das Ziel, das IT-Sicherheitsniveau von KMU zu erhöhen.

7. Wie viele Unternehmen ließen nach Kenntnis der Bundesregierung ihre Webseite durch das SIWECOS-Projekt (https://siwecos.de/scanned-by-siwecos/?data-siwecos=www.siwecos.de) überprüfen und zertifizieren?

   Wie bewertet sie hierbei die Wirksamkeit des Projektes?

Mindestens 14.419 Domains wurden durch das Projekt geprüft. 5.262 dieser Domains haben das SIVECOS-Siegel erhalten. Da anzunehmen ist, dass Unternehmen mehrere Domains prüfen, können keine Angaben zur Zahl der teilnehmenden Unternehmen getroffen werden.

Im Zeitraum 2018 bis 2019 sank die Zahl der durch das Projekt festgestellten eklatanten Sicherheitsmängel sowie der Anteil der Websites mit auslesbarem CMS leicht, der Anteil von Websites mit maschinell auslesbaren E-Mail-Adressen oder Telefonnummern deutlich. Dies deutet auf eine positive Wirksamkeit des Projekts hin.

8. Mit welchen Maßnahmen will die Bundesregierung die Sensibilisierung von KMU zum Thema Cybersicherheit verbessern?

Die Bundesregierung und Sicherheitsbehörden haben unter Berücksichtigung ihrer unterschiedlichen Aufgaben und Berührungspunkte zu den KMU, sei es im Rahmen der Wirtschaftsförderung, der Beratung in IT-Sicherheitsfragen oder der Kriminalprävention, vielfältige Initiativen entwickelt, um das Bewusstsein für Cybersicherheit in KMU auf allen Ebenen möglichst umfassend zu verbessern:

Dabei hat insbesondere die Transferstelle IT-Sicherheit im Mittelstand (www.tisim.de) sowie das Projekt „KMU Aware“ (www.awareness-im-mittelstand.de) Sensibilisierung von KMU zum Thema Cyber-Sicherheit zum Ziel.

Auch das BSI unternimmt zahlreiche Aktivitäten, um die Sensibilisierung für Cyber-Sicherheit in KMU voranzutreiben. Diese Projekte werden unter dem Dach der Allianz für Cyber-Sicherheit gebündelt.

Unter anderem tagt mit dem Erfahrungsaustauschkreis „Praxisorientierte Awareness“ regelmäßig eine Arbeitsgruppe, die sich mit Herausforderungen und Maßnahmen zur Sensibilisierung in Organisationen befasst. Außerdem organi-

siert die Initiative den Dialog der Cyber-Sicherheitsinitiativen. Hier wurden Arbeitsgruppen gebildet, die verschiedene Projekte für mehr Cyber-Sicherheit realisieren. Das Thema „Awareness“ gehört ebenfalls zu den avisierten Themen. Bereits im vergangenen Jahr wurden zum Beispiel Grafiken zur Sensibilisierung für mehr Cyber-Sicherheit am Arbeitsplatz entwickelt. Auch im aktuellen Kalenderjahr sollen weitere Inhalte entwickelt werden.

Geplant ist eine Veröffentlichung im Rahmen des European Cyber Security Month (ECSM) im Oktober. Hier werden unter Federführung der ENISA Aktivitäten gebündelt, die das Cyber-Sicherheitsniveau in Wirtschaft und Gesellschaft auch auf europäischer Ebene verbessern. Nicht zuletzt nehmen Mitarbeiter des BSI regelmäßig an Fachtagungen, Messen und sonstigen Veranstaltungen in ganz Deutschland oder Videokonferenzen teil, um im Rahmen von Vorträgen auf die Bedeutung von Cyber-Sicherheit hinzuweisen.

Das Bundeskriminalamt (BKA) führt mit Veröffentlichungen auf der BKA-Homepage, über Social-Media-Kanäle (Twitter, Facebook), über das Netzwerk Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) sowie durch eigene Vortragstätigkeiten fortlaufend konkrete Sensibilisierungsmaßnahmen für Bürger und Wirtschaft durch.

Nicht zuletzt stehen KMU als Zielgruppe generell im Fokus der Präventionsarbeit der Verfassungsschutzbehörden des Bundes und der Länder. Im Rahmen des präventiven Wirtschaftsschutzes informieren das Bundesamt für Verfassungsschutz und die Landesämter für Verfassungsschutz Unternehmen und Forschungseinrichtungen über eigene Erkenntnisse und Analysen, die dazu beitragen, dass diese sich eigenverantwortlich und effektiv gegen Ausforschung (insbesondere Wirtschaftsspionage), Sabotage und Bedrohungen durch Extremismus, Terrorismus und Cyberangriffe schützen können.

Darüber hinaus stehen die Geschäftsbereichsbehörden der verschiedenen Ressorts zur Stärkung der IT-Sicherheit in relevanten Einrichtungen in einem engen Austausch untereinander.

9. Wie viele Hilfestellungen für Unternehmen leisteten nach Kenntnis der Bundesregierung die auf Cybersicherheit spezialisierten Mittelstandskompetenzzentren 4.0 seit 2016 (bitte jährlich aufschlüsseln)?

Aktuell nehmen 15 der 26 Mittelstand-4.0-Kompetenzzentren das Thema Cyber-Sicherheit als Querschnittsaufgabe wahr (2016: 6; 2017: 9; 2018: 15; 2019: 15; 2020: 15). Aufgrund der vorliegenden Daten ist eine Aufschlüsselung nach dem Thema Cyber-Sicherheit nur teilweise möglich:

Diese 15 Kompetenzzentren haben im Jahr 2018 1.974 Termine, im Jahr 2019 4.261 Termine wahrgenommen. Für die Jahre 2016 und 2017 liegen keine, für das laufende Jahr 2020 noch keine Daten vor. Aufgrund einer IT-Umstellung kann folgende Aussage getroffen werden: Seit August 2018 haben diese 15 Kompetenzzentren mindestens 467 Präsenz- oder Online-Veranstaltungen zum Thema IT-Sicherheit durchgeführt.

Sie haben im Jahr 2016 mindestens 4.338, im Jahr 2017 mindestens 12.696, im Jahr 2018 mindestens 34.934 sowie im Jahr 2019 mindestens 61.235 KMU erreicht, wobei aufgrund der Datenlage keine Aussage darüber getroffen werden kann, inwieweit bei diesen Kontakten das Thema Cyber-Sicherheit Gegenstand war.

Die Gesamtheit aller 26 Mittelstand-4.0-Kompetenzzentren hat in den Jahren 2018 und 2019 insgesamt 23 Leitfäden/Handlungsanweisungen/Checklisten sowie zehn Publikationen zu Praxisbeispielen zum Thema IT-Sicherheit veröf-

fentlicht. Im Jahr 2019 hat die Begleitforschung „Mittelstand Digital“ eine Publikation zum Thema IT-Sicherheit erstellt.

10. Welche Förderungen der Mitarbeiterschulungen durch Bundesmittel im Bereich der Cybersicherheit existieren für kleine und mittlere Unternehmen?

Mitarbeiterschulungen werden insbesondere durch das Projekt KMU Aware (www.awareness-im-mittelstand.de) sowie die Förderprogramme „go-digital“ und „Digital Jetzt“ angeboten bzw. gefördert. Zudem werden auch von dem Mittelstandskompetenzzentren 4.0 Mitarbeiterschulungen im Bereich Cyber-Sicherheit angeboten.

11. Welche Fördermöglichkeiten haben Unternehmen, insbesondere KMU, um ihre Cybersicherheit zu erhöhen?

Wie bewertet die Bundesregierung die Möglichkeit, Maßnahmen zur Erhöhung der Cybersicherheit für Unternehmen steuerlich absetzbar zu gestalten?

Auf die Antwort zu Frage 6 wird verwiesen.

Aufwendungen für Maßnahmen zur Erhöhung der Cyber-Sicherheit des Steuerpflichtigen sind bei betrieblicher Veranlassung bereits heute nach den allgemeinen Grundsätzen zur Gewinnermittlung grundsätzlich als Betriebsausgaben abziehbar (§ 4 Absatz 4 des Einkommensteuergesetzes).

12. Welche Schlussfolgerungen zieht die Bundesregierung aus der Arbeit der Cyberwehr Baden-Württemberg (https://cyberwehr-bw.de/#!/prozess)

a) insgesamt und als Vorbild für das eigene politische Handeln,

b) besonders im Zuge der bundesweiten Freistellung der Corona-Pandemie?

c) Hält die Bundesregierung ein solches Projekt bundesweit oder jeweils in allen Bundesländern für sinnvoll, und gibt es Pläne, dies umzusetzen?

Die Fragen 12 bis 12c werden gemeinsam beantwortet.

Die Bundesregierung sieht gegenwärtig keine Veranlassung – auch vor dem Hintergrund der vorstehend dargestellten umfangreichen Maßnahmen und Initiativen der Bundesregierung – aus dem genannten Projekt Schlussfolgerungen im Sinne der Fragestellungen zu ziehen.

13. Wie bewertet die Bundesregierung den Nutzen von Cyberversicherungen für kleine und mittelständische Unternehmen?

Sieht sie im Bereich der Cyberversicherungen Regulierungsbedarf?

Cyber-Versicherungen sollen die finanziellen Folgen eines Cyberangriffs im Rahmen des gewählten Versicherungsumfangs auffangen, welche traditionelle Policen in der Regel nicht abdecken. Dies kann v. a. Eigenschäden, Drittschäden sowie Assistance-Leistungen umfassen. Insofern erscheinen Cyber-Versicherungen als eine sinnvolle Ergänzung von bereits vorhandenem Versicherungsschutz.

Ein positiver Begleiteffekt mit der Befassung von Cyber-Versicherungen für KMU ergibt sich zudem, dass die Unternehmen sich mit dem Thema Cybersicherheit näher auseinandersetzen und im Zuge dessen sich eine stärkere Sensibilisierung für die IT-Sicherheit entwickelt. Bei der Antragsstellung müssen Versicherungsnehmer exakte Angaben zu bestehenden Schutzmaßnahmen (z. B. Firewall, Virenschutz, Datensicherung, IT- und Datenschutzbeauftragte, ISO-Zertifizierungen) machen.

Die Beantwortung der Fragen offenbart dem Unternehmer gleichzeitig bestehende Schwachstellen und es besteht dadurch ein Anreiz, die vorhandene IT-Struktur in Bezug auf die IT-Sicherheit zu überprüfen und ggf. zu optimieren. Gleichzeitig ist die Versicherung kein Freibrief, denn i. d. R. hat der Versicherte einen Selbstbeteiligungsbetrag für den Schadensfall zu tragen. Damit kann der Versicherte einerseits eine Absicherung für den Schadensfall erzielen, andererseits erhöht dies seine Wachsamkeit.

Auch für die Cyber-Versicherung gilt das Versicherungsvertragsgesetz (VVG). Derzeit wird in dieser Hinsicht kein Regulierungsbedarf gesehen.

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