Deutscher Bundestag **Drucksache 19/21478**

19. Wahlperiode 04.08.2020

Kleine Anfrage

der Abgeordneten Gerald Ullrich, Michael Theurer, Reinhard Houben, Dr. Marcel Klinge, Prof. Dr. Martin Neumann, Manfred Todtenhausen, Sandra Weeser, Jens Beeck, Dr. Jens Brandenburg (Rhein-Neckar), Mario Brandenburg (Südpfalz), Britta Katharina Dassler, Dr. Marcus Faber, Otto Fricke, Markus Herbrand, Torsten Herbst, Manuel Höferlin, Ulla Ihnen, Dr. Christian Jung, Karsten Klein, Pascal Kober, Alexander Müller, Frank Müller-Rosentritt, Bernd Reuther, Dr. h. c. Thomas Sattelberger, Frank Sitta, Dr. Marie-Agnes Strack-Zimmermann, Benjamin Strasser und der Fraktion der FDP

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

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 bun-

desweit bereitgestellt. Aus Sicht der Fragesteller besteht allerdings die Gefahr, dass die schnelle Umstellung auf digitale Prozesse, welche meist ohne weitere Hilfe stattfinden musste, die Gefahr für Cyberangriffe erhöht hat.

Wir fragen die Bundesregierung:

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

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?

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

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

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

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?

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?

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

    Sieht sie im Bereich der Cyberversicherungen Regulierungsbedarf?

Berlin, den 29. Juli 2020

Christian Lindner und Fraktion

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