Deutscher Bundestag **Drucksache 19/31372**

19. Wahlperiode 06.07.2021

Kleine Anfrage

der Abgeordneten Markus Herbrand, Christian Dürr, Dr. Florian Toncar, Frank Schäffler, Katja Hessel, Till Mansmann, Grigorios Aggelidis, Renata Alt, Nicole Bauer, Jens Beeck, Dr. Jens Brandenburg (Rhein-Neckar), Mario Brandenburg (Südpfalz), Dr. Marcus Faber, Dr. Christopher Gohl, Thomas Hacker, Reginald Hanke, Peter Heidt, Katrin Helling-Plahr, Torsten Herbst, Dr. Gero Clemens Hocker, Manuel Höferlin, Reinhard Houben, Ulla Ihnen, Konstantin Kuhle, Ulrich Lechte, Michael Georg Link, Alexander Müller, Dr. Martin Neumann, Matthias Nölke, Christian Sauter, Frank Sitta, Judith Skudelny, Dr. Hermann Otto Solms, Bettina Stark-Watzinger, Dr. Marie-Agnes Strack-Zimmermann, Benjamin Strasser, Katja Suding, Stephan Thomae, Gerald Ullrich, Sandra Weeser, Nicole Westig und der Fraktion der FDP

IT-Sicherheit im deutschen und europäischen Bankwesen

In den vergangenen Jahren sind sowohl das Bankenwesen als auch die Finanzmarktinfrastrukturen zunehmend digitaler geworden. Vor dem Hintergrund dieser Entwicklung stützen sich Banken und Kreditinstitute immer stärker auf IT-Systeme und eine digitale Datenverarbeitung. Hierdurch entstehen signifikante Effizienzvorteile, die eine schnellere Bearbeitung komplexer Vorgänge ermöglichen, bürokratischen Aufwand verringern und den Finanzsektor der Europäischen Union im globalen Wettbewerb stärken. Mit dem Ausbau der Digitalisierung im Finanzsektor geht auch ein erhöhtes Risiko für IT-Störungen und Cyberangriffe einher, weshalb vorhandene Risiken nach Ansicht der Fragesteller genau beobachtet und Gegenmaßnahmen geprüft und ggf. eingeleitet werden müssen. Aus diesem Grund möchten sich die Fragestellenden über die Risiken von IT-Störungen und Cyberangriffen informieren, um sich ein sachgerechtes aktuelles Bild der aktuellen Sicherheitssituation im deutschen und europäischen Bankwesen – auch vor dem Hintergrund des im Zuge der Corona-Pandemie zu beobachtenden Digitalisierungsschubs im Finanzsektor – zu erhalten.

Wir fragen die Bundesregierung:

1. Welche Rolle misst die Bundesregierung aus welchen Gründen dem Risiko von IT-Störungen und Cyber-, Hacker- und Trojanerangriffen auf Banken in Deutschland bei?
2. Welche Maßnahmen werden von der Bundesregierung im Hinblick auf die IT-Sicherheit der Kreditinstitute, die von ihr beaufsichtigt werden, durchgeführt, und welchen Vorgaben und Regelungen kommt sie hiermit nach?

3. Inwiefern, und aus welchen Gründen sind das deutsche Bankenwesen und die deutschen Finanzmarktinfrastrukturen nach Einschätzung der Bundesregierung ein potenzielles Angriffsziel von Cyber-, Hacker- und Trojanerangriffen?
4. Führt nach Kenntnis der Bundesregierung die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) oder eine andere Behörde analog zu den on-site inspections der Bankenaufsicht der EZB eigene Vor-Ort-Überprüfungen deutscher Kreditinstitute durch, um die Funktionsfähigkeit und das Cyber-Risiko-Management einzelner Kreditinstitute zu prüfen und zu bewerten?
   a) Falls ja, welche Stelle führt diese Vor-Ort-Überprüfungen durch, und welche Aspekte stehen im Fokus der Prüfung?
   b) Falls ja, wie lange dauert eine Vor-Ort-Überprüfung, und wie viele Personalstellen werden durchschnittlich eingesetzt?
   c) Falls ja, wie viele Vor-Ort-Überprüfungen fanden (aufgeschlüsselt nach der Anzahl der Überprüfungen, dem Jahr und dem Bundesland, in dem die Prüfungen vorgenommen wurden) seit Beginn der Legislaturperiode bis zum heutigen Stichtag jeweils jährlich statt (bitte tabellarisch darstellen)?
   d) Falls ja, welche Bewertungskriterien werden bei den Vor-Ort-Überprüfungen angelegt, und welche dieser Kriterien waren am häufigsten erfüllt, und welche waren am häufigsten nicht erfüllt?
   e) Falls nein, weshalb sind solche Vor-Ort-Überprüfungen, die beispielsweise die EZB bei der Aufsicht signifikanter Kreditinstitute für erforderlich hält und regelmäßig durchführt, aus Sicht der Bundesregierung für die Finanzaufsicht in Deutschland nicht erforderlich (bitte begründen)?
5. Wie hat sich nach Kenntnis der Bundesregierung die Anzahl von IT-Pannen, die gegenüber der BaFin und/oder einer anderen Bundesbehörde von Finanzinstituten in Deutschland gemeldet wurden, in den letzten fünf Jahren jeweils entwickelt (bitte auch vorläufige Zahlen aus dem Jahr 2021 berücksichtigen)?
6. Wie hat sich die Anzahl von Cyber-, Hacker- und Trojanerangriffen, die gegenüber der BaFin und/oder einer anderen Bundesbehörde gemeldet wurden, in den letzten fünf Jahren jeweils jährlich entwickelt (bitte auch vorläufige Zahlen aus dem Jahr 2021 berücksichtigen)?
   a) Wann, und wie viele Angriffe auf Passwörter gab es bei wie vielen Instituten?
   b) Wann, und wie viele Infizierungen mit Schadsoftware bzw. Malware gab es bei wie vielen Instituten?
   c) Wann, und wie viele Phishing-Angriffe gab es bei wie vielen Instituten?
   d) Wann, und wie oft wurden Software-Schwachstellen bei wie vielen Instituten ausgenutzt?
   e) Wann, und wie viele DDOS-Attacken gab es bei wie vielen Instituten?
   f) Wann, und wie viele Man-in-the-Middle-Angriffe oder Mittelsmann-Angriffe gab es bei wie vielen Instituten?

g) Wann, und wie viele Fälle von Spoofing gab es bei wie vielen Instituten?

h) Von welchen Ländern aus wurden diese Angriffe geführt?

7. Ist der Bundesregierung bekannt, wie viele (vermutete) Cyber-, Hacker- und Trojanerangriffe es auf die Deutsche Bundesbank seit Beginn der 19. Legislaturperiode bis zum heutigen Stichtag jeweils jährlich gab und von wo aus diese Angriffe wann ausgeführt wurden (wenn ja, bitte tabellarisch darstellen und nach Zeitpunkt des Angriffs, Anzahl der Cyberangriffe und Ort aufschlüsseln)?

8. Wie viele (vermutete) Cyber-, Hacker- und Trojanerangriffe gab es nach Kenntnis der Bundesregierung auf die KfW seit Beginn der 19. Legislaturperiode bis zum heutigen Stichtag jeweils jährlich, und von wo aus wurden diese Angriffe wann ausgeführt (bitte tabellarisch darstellen und nach Zeitpunkt des Angriffs, Anzahl der Cyberangriffe und Ort aufschlüsseln)?

9. Welche Kreditinstitute sind nach Kenntnis der Bundesregierung am häufigsten von Cyber-, Hacker- und Trojanerangriffen betroffen, und weshalb sind diese am häufigsten betroffen?

10. Sind nach Kenntnis der Bundesregierung alle Kreditinstitute gleichermaßen von Cyber-, Hacker- und Trojanerangriffen betroffen oder sind Kreditinstitute, die bestimmte Geschäftsmodelle verfolgen, häufiger betroffen?

    Falls Kreditinstitute, die bestimmte Geschäftsmodelle verfolgen, von Cyber-, Hacker- und Trojanerangriffen häufiger betroffen sind, aus welchen Gründen ist dies der Fall?

11. Wie hoch ist nach Kenntnis der Bundesregierung schätzungsweise der finanzielle Schaden, der auf Cyber-, Hacker- und Trojanerangriffe auf in Deutschland ansässige Kreditinstitute zurückzuführen ist?

12. Welche Kenntnisse hat die Bundesregierung auf Grundlage der ihr vorliegenden Informationen und Studien über den finanziellen Schaden für die deutsche Wirtschaft, der auf Cyber-, Hacker- und Trojanerangriffe zurückzuführen ist?

13. In welchem Zustand befindet sich nach Ansicht der Bundesregierung die deutsche Kreditwirtschaft bezüglich Fragen der IT-Sicherheit und der Vorbereitung auf Cyber-, Hacker- und Trojanerangriffe?

14. Worin bestehen nach Ansicht der Bundesregierung die größten Defizite beim Schutz deutscher Kreditinstitute vor Cyber-, Hacker- und Trojanerangriffen?

15. Inwiefern tauscht sich die BaFin zu IT-Sicherheitsthemen mit den Kreditinstituten, die von ihr beaufsichtigt werden, aus?

    Welche Vorschläge und Vorhaben zur Stärkung der IT-Sicherheit werden hierbei thematisiert?

16. Inwiefern wirkt sich nach Kenntnis der BaFin die Corona-Pandemie auf die Digitalisierung des Bankenwesen und der Finanzmarktinfrastrukturen in Deutschland und der Europäischen Union aus?

17. Kann die Bundesregierung die Annahme der Fragestellenden bestätigen, dass es im Zuge der Corona-Pandemie verstärkt im deutschen und europäischen Bankensektor zum Einsatz digitaler Anwendungen gekommen ist und man von einem „Corona-Digitalisierungsschub“ sprechen kann?

    Falls ja, inwiefern wirkt sich dieser Umstand auf die IT-Sicherheit im deutschen und europäischen Bankensektor und die deutschen und europäischen Finanzmarktinfrastrukturen aus?

18. Sind nach Kenntnis der Bundesregierung seit Beginn der Corona-Pandemie in Deutschland und/oder Europa besondere Entwicklungen bezüglich der IT-Sicherheit des Bankenwesens und der Finanzmarktinfrastrukturen zu erkennen?

    Sind seither IT-Bedrohungen für das europäische und das deutsche Bankensystem gestiegen?

    Ist die Anzahl von IT-Störungen und/oder Cyber-, Hacker- und Trojanerangriffen gestiegen?

Berlin, den 23. Juni 2021

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