Deutscher Bundestag **Drucksache 19/31673**

19. Wahlperiode 21.07.2021

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Markus Herbrand, Christian Dürr, Dr. Florian Toncar, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 19/31372 –

IT-Sicherheit im deutschen und europäischen Bankwesen

Vorbemerkung der Fragesteller

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.

1. Welche Rolle misst die Bundesregierung aus welchen Gründen dem Risiko von IT-Störungen und Cyber-, Hacker- und Trojanerangriffen auf Banken in Deutschland bei?

Die Bundesregierung misst dem Risiko von IT-Störungen und Cyber-, Hacker- und Trojanerangriffen auf Banken eine hohe Bedeutung bei. Durch Cybervorfälle ausgelöste Ausfälle oder Beeinträchtigungen bei Banken können Versorgungsengpässe auslösen und bei besonders schweren grenzüberschreitenden Vorfällen auch die Finanzstabilität beeinträchtigen.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums der Finanzen vom 20. Juli 2021 übermittelt.
Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

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?

Die Bundesregierung misst der IT-Sicherheit im Finanzsektor seit Jahren eine große Bedeutung bei. Aus den §§ 25a Absatz 1, 25b und 25c Absatz 1 des Kreditwesengesetzes (KWG) ergeben sich für Kreditinstitute Anforderungen an die IT-Sicherheit. Diese Normen werden durch die beiden BaFin-Rundschreiben „Mindestanforderungen an das Risikomanagement (MaRisk)“ und „Bankaufsichtliche Anforderungen an die IT (BAIT)“ konkretisiert. Für Kreditinstitute, die zugleich Kritische Infrastrukturen gemäß der Verordnung zur Bestimmung Kritischer Infrastrukturen (BSI-KritisV) sind, gelten zusätzlich noch die Anforderungen nach §§ 8a und 8b des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz). Zahlungsdienstleister müssen zudem die Anforderungen nach §§ 53 und 54 des Zahlungsdiensteaufsichtsgesetzes (ZAG) erfüllen, in Umsetzung der Zweiten Zahlungsdiensterichtlinie.

In Zukunft wird für den Finanzsektor der derzeit im Rat verhandelte europäische Digital Operational Resilience Act (DORA) als übergreifendes Regelwerk gelten.

Die Einhaltung dieser Anforderungen wird durch von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) angeordnete IT-Prüfungen bei den Instituten und/oder bei deren IT-Dienstleistern regelmäßig überprüft. Zudem begleitet die BaFin auch die Mängelbeseitigung aktiv. Außerdem wertet die BaFin die IT-bezogenen Teile der einzelnen Jahresabschlussprüfungsberichte aus. Anforderungen nach dem BSI-Gesetz werden durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) begleitet.

Bei Bekanntwerden von (großflächigen) IT-Vorfällen, bei denen eine Betroffenheit des Finanzsektors nicht ausgeschlossen werden kann, führt die BaFin regelmäßig standardisierte Schnellumfragen bei vorab festgelegten Instituten und/oder deren IT-Dienstleistern sowie ggf. den Verbänden der Kreditwirtschaft durch.

Zahlungsdienstleister und sonstige Betreiber Kritischer Infrastrukturen müssen IT-Sicherheitsvorfälle an die BaFin sowie das BSI melden. Betreiber Kritischer Infrastrukturen müssen nach § 8a Absatz 3 Satz 1 BSI-Gesetz zudem alle zwei Jahre einen Nachweis erbringen, dass sie die Anforderungen nach § 8a Absatz 1 und 1a BSI-Gesetz erfüllen. Die entsprechenden Nachweise werden vom BSI überprüft.

BaFin und BSI tauschen sich auch über den UP KRITIS mit Bankenverbänden und Vertretern der Institute aus und erarbeiten gemeinsam Lösungsansätze für IT-Sicherheitsfragestellungen. UP KRITIS ist eine öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen (KRITIS), deren Verbänden und den zuständigen staatlichen Stellen.

Die BaFin ist darüber hinaus assoziierte Stelle im Cyber-Abwehrzentrum. In diesem Kontext erhaltene Erkenntnisse in Bezug auf IT-Sicherheit werden sanitarisiert grundsätzlich auch der Kreditwirtschaft und ihren Verbänden zur Verfügung gestellt.

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?

Der Finanzsektor ist weltweit potentielles Angriffsziel von Cyberkriminellen primär zur Befriedigung finanzieller Interessen. Dabei versuchen Angreifer oftmals, auch verwertbare Daten zu erlangen oder Erpressungspotential aufzubauen.

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?

Die Fragen 4 und 4a werden gemeinsam beantwortet.

Die BaFin übt die Aufsicht über Institute entsprechend § 6 Absatz 1 KWG aus und ordnet im Rahmen ihrer Aufgaben auch Vor-Ort-Prüfungen bei deutschen Kreditinstituten unter ihrer direkten Aufsicht an. Diese auf Grundlage des § 44 KWG angeordneten Prüfungen werden i. d. R. von der Deutschen Bundesbank oder beauftragten Wirtschaftsprüfungsgesellschaften durchgeführt. Die BaFin kann bei der Durchführung von Vor-Ort-Prüfungen unterstützen und in Einzelfällen auch selbst prüfen.

Gegenstand solcher bankgeschäftlichen Prüfungen ist insbesondere, ob die Institute die organisatorisch-technischen Pflichten gemäß § 25a und § 25b KWG erfüllen. Die Erfüllung der aufsichtlichen Anforderungen ist anhand der einschlägigen BaFin-Rundschreiben (MaRisk und BAIT) zu beurteilen.

   b) Falls ja, wie lange dauert eine Vor-Ort-Überprüfung, und wie viele Personalstellen werden durchschnittlich eingesetzt?

Die Dauer einer Vor-Ort-Überprüfung und der Einsatz der Prüferkapazitäten richten sich maßgeblich nach dem angeordneten Prüfungsschwerpunkt bzw. den Prüfungsinhalten und der Größe des Institutes. In der Regel liegt der Personaleinsatz bei bis zu zwölf Prüfern und die max. Prüfungsdauer bei etwa acht Wochen.

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)?

Anzahl von Vor-Ort-Prüfungen mit einem Schwerpunkt auf IT	2017	2018	2019	2020*	Gesamtergebnis
Baden-Württemberg	5	2	3		10
Bayern	2	3	4		9
Berlin	1	2	1	1	5
Brandenburg		1		1	2
Bremen		1			1
Hamburg	2	2	2	1	7
Hessen	8	10	6	7	31
Niedersachsen	2	5		1	8
Nordrhein-Westfalen	3	3	4	3	13
Rheinland-Pfalz		1	1		2
Saarland		1		1	2
Sachsen	1	2			3
Thüringen		1			1
Gesamtergebnis	**24**	**34**	**21**	**15**	**94**

* Durch die während der SARS-CoV-2-Pandemie bestehenden Einschränkungen konnten nicht alle Vor-Ort-Prüfungen wie geplant durchgeführt werden. Die Zahlen für 2020 sind daher nicht repräsentativ.

Die Zahlen für 2020 können nicht als repräsentativ angesehen werden, da Vor-Ort-Prüfungen aufgrund der COVID-19-Pandemie nur eingeschränkt durchgeführt werden konnten.

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?

Als Bewertungskriterien für die Erfüllung der gesetzlichen Anforderungen im Hinblick auf die Funktionsfähigkeit eines Cyber-Risiko-Managements als Teil einer ordnungsgemäßen Geschäftsführung bei Instituten werden grundsätzlich die einschlägigen BaFin-Rundschreiben MaRisk und BAIT herangezogen. Neben den aufsichtlichen Rundschreiben werden auch Empfehlungen des BSI und andere technische Standards berücksichtigt. Die häufigsten Mängel wurden im Management der Informationsrisiken und im Auslagerungsmanagement festgestellt. In den Bereichen IT-Strategie und IT-Governance wurden vergleichsweise weniger Mängel festgestellt.

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)?

Auf die Antwort zu Frage 4d wird verwiesen.

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)?

Seit Januar 2018 sind Zahlungsdienstleister nach dem ZAG verpflichtet, relevante IT-Vorfälle an die BaFin zu melden. Die BaFin verzeichnet seitdem jährlich einen etwa gleichbleibenden Eingang von Meldungen im niedrigen bis mittleren dreistelligen Bereich.

Seit Januar 2018 sind zudem Betreiber Kritischer Infrastrukturen im Finanzsektor nach dem BSI-Gesetz verpflichtet, relevante IT-Vorfälle an das BSI zu melden. Das BSI verzeichnet seitdem jährlich einen etwa gleichbleibenden Eingang von Meldungen im mittleren zweistelligen Bereich aus den Branchen Banken, Börsen und Finanzdienstleister.

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?

Die Fragen 6 bis 6h werden gemeinsam beantwortet.

Die Anzahl der der BaFin und dem BSI gemeldeten Cybervorfälle ist für die Jahre 2018 und 2019 als vergleichbar anzusehen. Lediglich im Jahr 2020 ist eine leichte Erhöhung erkennbar. Die bisherigen Zahlen für das Jahr 2021 lassen derzeit keine weiteren Erhöhungen erkennen. Unter den Ursachen sind DDoS-Attacken vorherrschend. Nur in einzelnen Fällen sind andere Angriffskategorien zu verzeichnen gewesen. Der Angriffsort ist nicht Teil der in einer Meldung anzugebenden Information.

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)?

Derzeit werden mehrere tausend unerlaubte Zugriffsversuche auf die Bundesbankinfrastruktur aus dem Internet täglich unterbunden. Zudem werden durch die Schutzmechanismen der Infrastrukturen der Bundesbank täglich mehrere tausend mit Schadcode behaftete Internetaufrufe und E-Mails blockiert. Die Ortszugehörigkeit eines Angriffs wird technisch über die IP-Adresse des Senders ermittelt. Da IP-Adressen jedoch sehr einfach gefälscht werden können, lässt dies nicht auf die Landeszugehörigkeit des Angreifers schließen.

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)?

Für die Zeit seit dem Jahr 2017 liegen der Kreditanstalt für Wiederaufbau (KfW) keine Hinweise auf zielgerichtete Hackerangriffe gegen die KfW vor. Die KfW ist allerdings sehr wohl den allgemeinen, zeitlich diskret verteilten, breit angelegten Malware-Angriffen, die nicht gezielt erfolgen, ausgesetzt. Diese konnten von den Sicherheitsmechanismen der KfW ausnahmslos erkannt und geblockt werden und somit die mit diesen Angriffen verbundene Bedrohung abgewendet werden.

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

Der Bundesregierung liegen hierzu keine belastbaren Daten vor.

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?

Der Bundesregierung liegen hierzu keine belastbaren Daten vor.

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?

Die Fragen 11 und 12 werden zusammen beantwortet.

Das BSI und die BaFin erheben keine systematischen Informationen über den volkswirtschaftlichen Schaden durch Cyber-Angriffe in Deutschland. In dem von Bitkom veröffentlichten Studienbericht 2020 „Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der vernetzten Welt“ wird ein Gesamtschaden für die deutsche Wirtschaft durch analoge und digitale Angriffe zusammen von über 100 Mrd. Euro pro Jahr genannt.

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?

Die deutsche Kreditwirtschaft ist im Vergleich zu anderen Branchen und Sektoren weitaus stärker reguliert, insbesondere auch im Hinblick auf die Anforderungen an den Umgang mit operationellen Risiken, zu denen IT-Risiken gehören. Zudem werden Kreditinstitute regelmäßigen bankgeschäftlichen Prüfungen unterzogen. Die Behebung der dabei festgestellten Mängel wird nachgehalten. Vor diesem Hintergrund kann von einem sich stetig steigernden Reifegrad der IT-Sicherheit ausgegangen werden.

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

Die größte Herausforderung sind sich ständig fortentwickelnde Angriffsvektoren.

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?

Die BaFin tauscht sich intensiv mit den unter ihrer Aufsicht stehenden Kreditinstituten zu IT-Sicherheitsthemen aus. Für diesen Austausch stehen unterschiedlichen Formate zur Verfügung, insbesondere auch das Forum „Fachgremium IT“, in dem sich relevante Vertreter des öffentlichen und privaten Finanzsektors regelmäßig zu vielfältigen Themen der IT-Sicherheit austauschen. In der Vergangenheit wurden z. B. die Umsetzung der starken Kundenauthentifizierung im Zahlungsverkehr, die Weiterentwicklung des IKT- und Sicherheitsrisikomanagements vor dem Hintergrund der entsprechenden EBA-Leitlinien sowie anlassbezogen DDoS- und Ransomware-Angriffe 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?

Im Laufe der Pandemie konnte eine verstärkte Nachfrage der Kunden nach digitalen Vertriebskanälen und Zahlungsmöglichkeiten beobachtet werden. Dabei wurden insbesondere bargeldlose und kontaktlose Bezahlmöglichkeiten vermehrt nachgefragt. Außerdem wurde beobachtet, dass Kreditinstitute vermehrt ihre Digitalisierungsstrategie angepasst haben und dabei eine Ausweitung von Auslagerungstätigkeiten und Kooperationen mit FinTechs erwägen.

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?

Die bereits existierenden digitalen Anwendungen im Bereich des kartengestützten Zahlungsverkehrs wurden vermehrt genutzt. Der Umstand hat sich bislang allerdings nicht in einer Zunahme von Störungsmeldungen nach dem ZAG bei der BaFin manifestiert.

Weltweit konnte eine Zunahme von großen Ransomware-Vorfällen und Angriffen auf IT-Dienstleister unabhängig von der Branchenzugehörigkeit ihrer Kunden beobachtet werden. Ein Anstieg der Zahl der gemäß § 8b BSI-Gesetz gemeldeten IT-Störungen im deutschen Bankensystem ist nicht zu verzeichnen. Ebenso hat sich der Umstand bislang nicht in einer Zunahme von Störungsmeldungen nach dem ZAG bei der BaFin manifestiert.

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?

Weltweit konnte eine Zunahme von großen Ransomware-Vorfällen und Angriffen auf IT-Dienstleister unabhängig von der Branchenzugehörigkeit ihrer Kunden beobachtet werden. Ein Anstieg der Zahl der gemäß § 8b BSI-Gesetz gemeldeten IT-Störungen im deutschen Bankensystem ist nicht zu verzeichnen. Ebenso hat sich der Umstand bislang nicht in einer Zunahme von Störungsmeldungen nach dem ZAG bei der BaFin manifestiert.

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