Deutscher Bundestag **Drucksache 19/8051**

19. Wahlperiode 27.02.2019

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Frank Schäffler, Christian Dürr, Dr. Florian Toncar, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 19/7603 –

Aufsichtlich kontrollierte Hackerangriffe auf Banken-IT

Vorbemerkung der Fragesteller

Das am 2. Mai 2018 veröffentlichte European Framework for Threat Intelligencebased Ethical Red Teaming (Tiber-EU) der Europäischen Zentralbank (EZB) ist ein Rahmenwerk, um mittels kontrollierter Cyber-Hackingangriffe die Widerstandsfähigkeit von Akteuren im Finanzsektor zu testen und um so eine Vergleichbarkeit auf europäischer Ebene herzustellen (vgl. Pressemitteilung der EZB vom 2. Mai 2018). Dieses Rahmenwerk enthält Anleitungen und Standards zur europäischen Harmonisierung von kontrollierten Cyberattacken externer Dienstleister gegen wichtige Banken, aber auch gegen Zahlungsdienstleister, Börsen, Clearinghäuser oder Versicherer. Dänemark, Belgien und die Niederlande hätten bereits die rechtlichen Bedingungen dafür geschaffen, indem sie Tiber-EU implementierten:

– Veröffentlichung des Tiber-NL-Ratgebers im November 2018 (www.dnb.nl/binaries/TIBER-NL%20Guide%20Second%20Test%20Round%20final_tcm46-365448.pdf);

– Veröffentlichung des Tiber-BE-Ratgebers im November 2018 (www.nbb.be/doc/be/be6/tiber_be_framework.pdf);

– Veröffentichung des Tiber-Dk-Ratgebers im Dezember 2018 (www.nationalbanken.dk/da/finansielstabilitet/fsor/Documents/TIBER%20Implementeringsguide.pdf).

Die „Börsen-Zeitung“ berichtete am 16. Januar 2019, in Deutschland solle eine Entscheidung über die Implementierung eines solchen Rahmenwerks für Cyber-Stresstests hingegen noch ausstehen. Sie werde jedoch in der ersten Jahreshälfte erfolgen, hätten mit den Plänen vertraute Personen verlauten lassen.

Nicht nur aktuelle Fälle der rechtswidrigen Datenbeschaffung haben den Fokus auf die Cyber- bzw. Datensicherheit noch einmal erhöht. Auch etwa der Spotlight Report 2018 mit dem Titel „Could an Equifax-sized data breach happen again?“ zeigte einen Anstieg der Sicherheitsverletzungen in allen Branchen, einschließlich der Finanzdienstleistungen, auf. Weltweit würden Finanzdienstleis-

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums der Finanzen vom 25. Februar 2019 übermittelt.

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

ter immer mehr Cyberangriffen ausgesetzt. Hacker nutzten bisweilen sogenannte versteckte Tunnel, um sich in Unternehmensnetzwerken einzunisten und wertvolle Daten aus der Ferne abzuschöpfen.

1. Kann die Bundesregierung bestätigen, dass in Deutschland das Rahmenwerk von Tiber-EU noch nicht implementiert wurde bzw. ein entsprechender Ratgeber (Guide bzw. Guidance) noch nicht veröffentlicht wurde?

2. Wenn ja, welche Gründe haben es bislang verhindert, einen solchen Ratgeber zu erarbeiten?

Die Fragen 1 und 2 werden zusammen beantwortet.

In Deutschland wird die Implementierung des TIBER-DE Rahmenwerk derzeit vorbereitet. Dabei werden auch die im Oktober 2018 von den G7-Finanzministern und Notenbankgouverneuren verabschiedeten unverbindlichen „G7 Fundamental Elements for Threat-Led Penetration Testing“ (www.bundesfinanzministerium.de/Content/DE/Downloads/2018-10-30-g7-penetration-testing.pdf?__blob=publicationFile&v=3) berücksichtigt.

Das TIBER-EU ist ein freiwilliges Rahmenwerk, das von der Europäischen Zentralbank (EZB) im Mai 2018 veröffentlicht wurde. Das Rahmenwerk wird allen zuständigen Behörden zur Verfügung gestellt, wobei allerdings die nationale Implementierung nicht verpflichtend ist. Es ist insbesondere zu berücksichtigen, dass der deutsche Finanzsektor im Hinblick auf Größe und Art der Finanzinstitute sehr heterogen ist. Die Ausgangslage ist daher in Deutschland eine andere als in den Ländern, wie z. B. Niederlande, Belgien oder Dänemark.

3. Hat die Bundesregierung einen bereits konkreten Auftrag erteilt, einen Tiber-DE-Ratgeber zu erarbeiten?

   a) Wann wurde dieser Auftrag durch die Bundesregierung bzw. ein Bundesministerium gefasst?

   b) Welche Behörde bzw. Institution ist seitens der Bundesregierung mit der Erarbeitung eines Tiber-DE-Ratgebers betraut worden?

   c) Welche Behörde bzw. welche Institution soll nach Ansicht der Bundesregierung für die Beaufsichtigung der Hackerangriffe zuständig sein?

Die Fragen 3 bis 3c werden zusammen beantwortet.

Die Bundesregierung hat die BaFin beauftragt, in Kooperation mit der Deutschen Bundesbank Rahmenbedingungen für eine nationale Implementierung zu erarbeiten. Die hierfür eingerichtete Arbeitsgruppe hat ihre Arbeit im Oktober 2018 aufgenommen und setzt sich aus Vertretern der Bundesbank und BaFin zusammen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) nimmt beratend an den Sitzungen der Arbeitsgruppe teil. Die Arbeitsgruppe befasst sich auch mit der Frage, welche Behörde/Institution am besten für eine Begleitung von Threat-Led-Penetrationtests geeignet ist.

4. Wurden nach Kenntnis der Bundesregierung bereits Unternehmen und/oder Personen angesprochen, diese Hackerangriffe auszuführen?

   a) Und wenn ja, mit welchen Unternehmen bzw. Personen wurde gesprochen (bitte mit Angabe des jeweiligen Datums und der Namen der teilnehmenden Personen beantworten)?

   b) Nach welchen Kriterien hat die Bundesregierung diese ausgesucht?

   c) Inwieweit prüft die Bundesregierung die Zuverlässigkeit (im untechnischen Sinne) von Hackern, die möglicherweise mit einem Angriff auf die Banken-IT betraut werden sollen?

      Gibt es beispielsweise Ausschlussfaktoren, und wenn ja, wie lauten diese?

Die Fragen 4 bis 4c werden gemeinsam beantwortet.

Es wurden bislang keine Unternehmen und/oder Personen angesprochen, in diesem Rahmen Hackerangriffe auszuführen.

5. Unterstellt die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) solle künftig für die Kontrolle der Hackerangriffe auf die Banken-IT zu Prüfzwecken zuständig sein, wie viele Personen in der BaFin sollen nach Ansicht der Bundesregierung künftig mit dieser Aufgabe betraut werden?

6. Unterstellt die Deutsche Bundesbank solle künftig für die Kontrolle der Hackerangriffe auf die Banken-IT zu Prüfzwecken zuständig sein, wie viele Personen in der Deutschen Bundesbank sollen nach Kenntnis der Bundesregierung künftig mit dieser Aufgabe betraut werden?

Die Fragen 5 und 6 werden zusammen beantwortet.

Die personellen Anforderungen sind nicht davon abhängig, welche Behörde für die die Begleitung der Threat-Led-Penetrationtests zuständig ist. Das TIBER-Rahmenwerk sieht die Etablierung eines sog. Tiber Cyber Teams (TCT) vor. Das TCT kann aus Mitgliedern verschiedener Behörden zusammengesetzt sein. Die Größe des TCT hängt dabei maßgeblich davon ab, wie viele Tests pro Jahr begleitet werden sollen bzw. wie umfassend das TCT in die Tests involviert wird. Diese Fragen werden derzeit im Rahmen der Erarbeitung der Rahmenbedingungen für eine nationale Implementierung geklärt.

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.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