Deutscher Bundestag **Drucksache 19/7603**

19. Wahlperiode 11.02.2019

Kleine Anfrage

der Abgeordneten Frank Schäffler, Christian Dürr, Dr. Florian Toncar, Bettina Stark-Watzinger, Markus Herbrand, Katja Hessel, Grigorios Aggelidis, Renata Alt, Jens Beeck, Nicola Beer, Dr. Jens Brandenburg (Rhein-Neckar), Mario Brandenburg, Dr. Marco Buschmann, Dr. Marcus Faber, Otto Fricke, Thomas Hacker, Katrin Helling-Plahr, Manuel Höferlin, Dr. Christoph Hoffmann, Reinhard Houben, Ulla Ihnen, Olaf in der Beek, Thomas L. Kemmerich, Dr. Marcel Klinge, Pascal Kober, Carina Konrad, Ulrich Lechte, Oliver Luksic, Till Mansmann, Alexander Müller, Frank Müller-Rosentritt, Bernd Reuther, Christian Sauter, Matthias Seestern-Pauly, Frank Sitta, Katja Suding, Michael Theurer, Stephan Thomae, Gerald Ullrich und der Fraktion der FDP

Aufsichtlich kontrollierte Hackerangriffe auf Banken-IT

Das am 2. Mai 2018 European Framework for Threat Intelligencebased Ethical Red Teaming (Tiber-EU) der 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 EVZ 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 Ratgeber 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 Finanzdienstleister immer

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

Wir fragen die Bundesregierung:

1. Kann die Bundesregierung bestätigen, dass in Deutschland das Rahmenwerk von Tiber-EU noch nicht implementiert wurde bzw. ein entsprechender Ratgeber (guide/guidance) noch nicht veröffentlicht wurde?
2. Wenn ja, welche Gründe haben es bislang verhindert, einen solchen Ratgeber zu erarbeiten?
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 Ministerium 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?
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)?
   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 beispielsweisen Ausschlussfaktoren und wenn ja, wie lauten diese?
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 Bundesbank sollen nach Kenntnis der Bundesregierung künftig mit dieser Aufgabe betraut werden?

Berlin, den 30. Januar 2019

Christian Lindner und Fraktion

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