Deutscher Bundestag **Drucksache 19/21476**

19. Wahlperiode 04.08.2020

Kleine Anfrage

der Abgeordneten Reinhard Houben, Michael Theurer, Dr. Marcel Klinge, Prof. Dr. Martin Neumann, Manfred Todtenhausen, Gerald Ullrich, 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, Dr. h. c. Thomas Sattelberger, Frank Schäffler, Frank Sitta, Dr. Marie-Agnes Strack-Zimmermann, Benjamin Strasser, Linda Teuteberg und der Fraktion der FDP

Cybersicherheit im deutschen Mittelstand

Deutsche Unternehmen, auch KMUs (kleine und mittlere Unternehmen), sehen sich zunehmend mit Cyberangriffen und Datendiebstahl konfrontiert. Laut einer Studie („Wirtschaftsschutz in der digitalen Welt“) des Digitalverbands Bitkom wurden 2019 drei von vier Unternehmen Opfer von Sabotage, Datendiebstahl oder Spionage. Durch die Angriffe (analog und digital) entsteht der deutschen Wirtschaft jährlich ein Schaden von 102,9 Mrd. Euro. Damit hat sich der Schaden seit 2016 nahezu verdoppelt (2016/2017: 55 Mrd. Euro p. a.). So haben digitale Angriffe in den vergangenen beiden Jahren bei 70 Prozent der Unternehmen einen Schaden verursacht, im Jahr 2017 waren es erst 43 Prozent.

So gaben 21 Prozent der Unternehmen an, dass sensible digitale Daten abgeflossen sind, bei 17 Prozent wurden Informationssysteme und Produktionssysteme oder Betriebsabläufe digital sabotiert, und bei 13 Prozent wurde die digitale Kommunikation ausgespäht. Dennoch spielen analoge Angriffe nach wie vor eine große Rolle. Bei 32 Prozent wurden IT-Geräte oder Telekommunikationsgeräte gestohlen, sensible Dokumente, Maschinen oder Bauteile wurden bei jedem sechsten entwendet. Ein wachsendes Problem ist demnach „Social Engineering“. Hierbei werden Mitarbeiter dazu gebracht, sensible Informationen preiszugeben, mit denen man beispielsweise Schadsoftware auf Firmenrechner installieren konnte. 22 Prozent der befragten Unternehmen waren davon analog betroffen, 15 Prozent digital.

Lediglich bei 13 Prozent der Unternehmen gab es Hinweise auf Delikte durch externe Strafverfolgungsbehörden oder Aufsichtsbehörden. Eine dramatische Mehrheit der Unternehmen (96 Prozent) fordern deswegen eine engere Zusammenarbeit mit Staat und Behörden. Außerdem fordern sie mehr Unterstützung durch die Behörden bei Fragen der IT-Sicherheit. 91 Prozent der Unternehmen sehen die Notwendigkeit von Verbesserung beim Informationsaustausch zwischen staatlichen Stellen. Die breite Mehrheit der Unternehmen (82 Prozent) sieht in Zukunft eine Verschärfung der Sicherheitslage und gehen von einer Zu-

nahme der Cyberangriffen auf die Unternehmen aus (https://www.bitkom.org/sites/default/files/2019-11/bitkom_wirtschaftsschutz_2019_0.pdf).

Im Jahr 2015 wurde das „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ verabschiedet. An einem Nachfolger, dem IT-Sicherheitsgesetz 2.0, wird seit zwei Jahren gearbeitet. Bereits 2018 verkündete der Bundesminister des Innern, für Bau und Heimat, Horst Seehofer, die Einführung des Gesetzes. Der Cybersicherheitsrat wurde mit der Cybersicherheitsstrategie 2011 errichtet und mit der Cybersicherheitsstrategie 2016 reformiert, bleibt aber bis heute, laut Medienberichten, eine „leere Hülle“. Das Nationale Cyber-Abwehrzentrum sollte ursprünglich alle operativen Akteure der Cybersicherheit in Deutschland (Bundesamt für Sicherheit in der Informationstechnik (BSI), Bundeskriminalamt und Bundeswehr) zusammenbringen. „Bis heute wurde versäumt, die Plattform auf eine vernünftige rechtliche Grundlage zu stellen. Diese sollte unter anderem regeln, welche Informationen ausgetauscht werden können, dürfen und müssen. Seit Jahren werden Reformen angestrebt, die getrost als gescheitert angesehen werden können“, schreibt netzpolitik.org (https://netzpolitik.org/2020/eine-vertane-chance-fuer-die-it-sicherheit-in-deutschland/#spendenleiste). Auf diese Defizite machte die Fraktion der FDP bereits im Februar 2019 aufmerksam (vgl. Bundestagsdrucksache 19/7698).

Unter dem Titel „Mehr Sicherheit für die digitale Transformation“ veröffentlichte der „Weisenrat für Cybersicherheit“ am 6. Juni 2020 seinen ersten Jahresbericht. Im Bericht spricht der Weisenrat acht Handlungsempfehlungen für Politik und Wirtschaft aus, die als Entscheidungshilfe zur Gestaltung gesetzlicher Rahmenbedingungen verstanden werden können. Das Cyber Security Cluster Bonn hat den unabhängigen Weisenrat für Cybersicherheit 2019 ins Leben gerufen, um einen weiteren Beitrag zur Immunisierung der Gesellschaft gegen Cyberattacken zu leisten (https://cyber-security-cluster.eu/_Resources/Persistent/a/1/d/9/a1d95dca3a8642822f22eb1372cd2b66e271d4fe/Mehr%20Sicherheit%20f%C3%BCr%20die%20digitale%20Transformation%20-%20Jahresbericht%20des%20Weiserats%20f%C3%BCr%20Cyber-Sicherheit.pdf).

Wir fragen die Bundesregierung:

1. Welcher besonderen Gefahr sieht die Bundesregierung mittelständische Unternehmen durch Cyberangriffe ausgesetzt?
2. Welche Erkenntnisse liegen der Bundesregierung über den volkswirtschaftlichen Schaden durch Hackerangriffe in Deutschland vor?
3. Inwiefern sind deutsche KMU im Vergleich zu großen Unternehmen in Deutschland nach Kenntnis der Bundesregierung gegen Cyberangriffe gewappnet?

   Welchen Handlungsbedarf sieht die Bundesregierung hier vonseiten des Staates?
4. Welche Möglichkeiten hat die Bundesregierung, mittelständische Unternehmen bei dem Schutz vor Cyberangriffen zu unterstützen?

   Welche Verbesserungsmöglichkeiten sieht die Bundesregierung?
5. Welche politischen Maßnahmen plant die Bundesregierung in naher Zukunft zur Eindämmung von Cyberangriffen auf deutsche Unternehmen, insbesondere KMU?
6. Welche Schlussfolgerungen zieht die Bundesregierung aus der Arbeit des „Weisenrats für Cybersicherheit“?

   Inwiefern gibt es Pläne für ein öffentliches Mandat des Weisenrats oder eines ähnlichen Sachverständigenrats für Cybersicherheit?

7. Welche Schlussfolgerungen zieht die Bundesregierung aus den acht Handlungsempfehlungen des „Weisenrats für Cybersicherheit“?
8. Welche Schlussfolgerungen zog die Bundesregierung aus der Studie „Wirtschaftsschutz in der digitalen Welt“ des Digitalverbands Bitkom?

   Welche Maßnahmen wurden aufgrund der Studie in Angriff genommen?
9. Welche eigenen Nachforschungen unternimmt die Bundesregierung, um das Ausmaß von Cyberangriffen auf deutsche Unternehmen zu bestimmen?

   Welche Schlussfolgerungen wurden daraus gezogen?
10. Welche Schlussfolgerungen zieht die Bundesregierung aus der Arbeit der von Bundesministerium für Wirtschaft und Energie geförderten Transferstelle IT-Sicherheit im Mittelstand (TISiM)?

    Welche Verbesserungsmöglichkeiten sieht die Bundesregierung?
11. Wie bewertet die Bundesregierung die Arbeit des Nationalen Cyber-Abwehrzentrums?
12. Welche Bedeutung hat das Nationale Cyber-Abwehrzentrum beim Schutz der deutschen Wirtschaft, insbesondere von mittelständischen Unternehmen?
13. Welche Schlussfolgerungen zieht die Bundesregierung aus der negativen Einschätzung des Nationalen Cyber-Abwehrzentrums durch netzpolitik.org?
14. Welche Pläne gibt es vonseiten der Bundesregierung, das Nationale Cyber-Abwehrzentrum zu reformieren?
15. Wie sieht die Bundesregierung staatliche Stellen in der Abwehr von Cyberangriffen auf mittelständische Unternehmen aufgestellt?
16. Inwiefern sind staatliche Behörden nach Auffassung der Bundesregierung ausreichend vorbereitet und ausgestattet, um Unternehmen bei Fragen der IT-Sicherheit zu unterstützen?

    Welche Verbesserungsmöglichkeiten sieht die Bundesregierung?
17. Welche Förderungen der Mitarbeiterschulungen durch Bundesmittel im Bereich der Cybersicherheit existieren für kleine und mittlere Unternehmen?
18. Wann plant die Bundesregierung, einen Entwurf für das IT-Sicherheitsgesetz 2.0 vorzulegen?

    Welche zentralen Maßnahmen sind im Rahmen des Gesetzes aus Sicht der Bundesregierung von zentraler Bedeutung?
19. Inwiefern könnte das geplante IT-Sicherheitsgesetz 2.0 zur Sicherheit von mittelständischen Unternehmen beitragen?

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