Deutscher Bundestag **Drucksache 20/14372**

20. Wahlperiode 23.12.2024

Kleine Anfrage

der Abgeordneten Manuel Höferlin, Maximilian Funke-Kaiser, Konstantin Kuhle, Renata Alt, Christine Aschenberg-Dugnus, Nicole Bauer, Jens Beeck, Dr. Jens Brandenburg (Rhein-Neckar), Dr. Marcus Faber, Daniel Föst, Martin Gassner-Herz, Julian Grünke, Thomas Hacker, Philipp Hartewig, Peter Heidt, Katrin Helling-Plahr, Reinhard Houben, Olaf in der Beek, Pascal Kober, Ulrich Lechte, Michael Georg Link (Heilbronn), Kristine Lütke, Alexander Müller, Ria Schröder, Anja Schulz, Dr. Stephan Seiter, Jens Teutrine, Manfred Todtenhausen, Katharina Willkomm und der Fraktion der FDP

Auswirkungen von Cyberangriffen auf die Sicherheit und die Wirtschaft von Deutschland

Die Cybersicherheit ist die Achillesferse des digitalen Zeitalters und ein entscheidender Faktor für die Sicherheit Deutschlands. Die wachsende Bedrohungslage im Cybersicherheitsbereich wird nicht nur durch technische Entwicklungen, sondern auch durch geopolitische Spannungen, wie den russischen Angriffskrieg gegen die Ukraine, geprägt (Bundesamt für Sicherheit in der Informationstechnik (BSI), Die Lage der IT-Sicherheit in Deutschland 2024, S. 22).

Cybersicherheit ist daher nicht nur ein technologisches, sondern auch ein sicherheitspolitisches und gesellschaftliches Kernanliegen. Cyberangriffe stellen auch eine der größten Herausforderungen für die deutsche Wirtschaft dar. Laut einer aktuellen Studie im Auftrag des Bitkom beläuft sich der durch Cyberkriminalität verursachte Schaden auf rund 267 Mrd. Euro – ein alarmierender Wert (www.behoerden-spiegel.de/2024/08/28/267-milliarden-euro-schaden-durch-cyber-angriffe/#:~:text=Eine%20neue%20Studie%20im%20Auftrag,noch%20206%20Milliarden%20Euro%20gewesen). Ein umfassender Schutz unserer informationstechnischen Systeme ist unabdingbar, um die Sicherheit von Bürgern, Unternehmen und kritischen Infrastrukturen zu gewährleisten und die demokratische Integrität zu schützen (BSI, Die Lage der IT-Sicherheit in Deutschland 2024, S. 91).

Die bisherige Verteilung der Aufgaben und Zuständigkeiten der Cybersicherheit auf Bundesebene steht bereits seit einiger Zeit in der Kritik. Im Kern geht es dabei um den Interessenkonflikt zwischen der Offenlegung von Sicherheitslücken durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) und der Zurückhaltung und Nutzung von Sicherheitslücken, beispielsweise durch das Bundesamt für Verfassungsschutz oder das Bundeskriminalamt. All diese Institutionen sind nachgeordnete Behörden unter dem Dach des Bundesministeriums des Innern und für Heimat (BMI) – mit unterschiedlichen Interessen. Aus diesem Grund wird von Expertinnen und Experten bereits seit Jahren gefordert, dass das BSI unabhängiger vom BMI aufgestellt wird, damit es in seiner Rolle als glaubwürdiger und vertrauenswürdiger Ansprechpartner für IT-

Sicherheitsbelange auftreten kann (zum Beispiel Kipker; Mayr, Zur Unabhängigkeit des BSI, Datenschutz und Datensicherheit, 2023, S. 790 ff.). Dies hat zuletzt auch die Präsidentin des BSI in ihrer Stellungnahme zur Anhörung zum Gesetzentwurf zur Umsetzung der NIS (Netzwerk- und Informationssicherheit)-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung betont (www.bundestag.de/resource/blob/1027138/0e7d977acf676897233c034b842807be/20-4-523-C.pdf#page3).

Um die Informationssicherheit auf nationaler Ebene zu koordinieren, existiert in vielen Ländern bereits ein Chief Information Security Officer (CISO) (www.cio.gov/handbook/key-stakeholders/ciso/, https://cyber.gouv.fr/en/what-we-do , www.canada.ca/en/treasury-board-secretariat/corporate/mandate/chief-information-officer.html).

Für die Bundesverwaltung gibt es nach wie vor keinen Koordinator, der ressortübergreifend für die Etablierung entsprechender Risikoanalysen, Schutzzielen und einem Managementsystem zuständig ist. Expertinnen und Experten fordern, dass ein solcher CISO-Bund mit entsprechenden Durchsetzungsbefugnissen ausgestattet (Kipker, Stellungnahme zur Anhörung zum Gesetzentwurf zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung) und beim BSI angesiedelt wird, weil dort die Expertise zur Informationssicherheit liegt. Im aktuellen Gesetzentwurf zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung ist zwar ein Koordinator für die Informationssicherheit vorgesehen (§ 48 des BSI-Gesetzes (Neufassung (BSIG-E)), allerdings ist seine Stellung innerhalb der Bundesverwaltung und seine konkreten Kompetenzen noch nicht geregelt.

Wir fragen die Bundesregierung:

1. Wie viele Cyberangriffe auf deutsche Bundesbehörden wurden in den letzten zwölf Monaten registriert, wie viele hiervon waren erfolgreich, welche Schäden sind aus diesen erfolgreichen Angriffen jeweils entstanden (bitte jeweils nach Behörden aufschlüsseln), und wie werden diese Cyberangriffe und ihre Auswirkungen von der Bundesregierung erfasst?
2. Wie viele Cyberangriffe auf Einrichtungen der kritische Infrastrukturen wurden in den letzten zwölf Monaten registriert, wie viele hiervon waren erfolgreich (bitte nach jeweiligem Industriebereich aufschlüsseln), welche Schäden sind aus diesen erfolgreichen Angriffen jeweils entstanden, und wie werden diese Cyberangriffe und ihre Auswirkungen von der Bundesregierung erfasst?
3. Wie stellt die Bundesregierung sicher, dass Unternehmen, die dem Einfluss autoritärer Regime unterliegen, nicht beim Ausbau von kritischen Infrastrukturen beteiligt werden (zum Beispiel 5G und zukünftig 6G-Ausbau), welche Maßnahmen hat die Bundesregierung bereits ergriffen?
4. Welche Maßnahmen werden allgemein ergriffen, um die IT-Sicherheitsinfrastruktur der Bundesbehörden gegen Angriffe zu schützen, und welche Bundesbehörden lassen nach Kenntnis der Bundesregierung ihre IT-Sicherheitsinfrastruktur im Speziellen mittels Penetrationstests überprüfen (bitte jeweils nach Behörden aufschlüsseln)?
5. Wie viele Cyberangriffe wurden dem BSI seitens Akteuren der Privatwirtschaft innerhalb der letzten zwölf Monate gemeldet (bitte nach Art und Umfang des Angriffs, betroffenen Wirtschaftszweig, Schadenshöhe und getroffenen Gegenmaßnahmen aufschlüsseln)?

6. Ist der Bundesregierung bekannt, ob dem BSI bekannte Schwachstellen nicht an die betroffenen Akteure kommuniziert wurden, und wenn ja, wie viele solcher Fälle sind der Bundesregierung bekannt, um welche Schwachstellen handelt es sich, werden diese auch von Sicherheitsbehörden genutzt, sieht die Bundesregierung insoweit einen Wertungswiderspruch?
7. Welche Förderprogramme und Beratungsangebote vonseiten des Bundes gibt es für Unternehmen und Forschungseinrichtungen, um Innovationen im Bereich Cybersicherheit zu fördern, welche Förderprogramme und Beratungsangebote vonseiten des Bundes gibt es speziell für Einrichtungen der kritischen Infrastruktur, und in welchem Umfang werden die Förderbudgets hier jeweils ausgeschöpft?
8. Welche Maßnahmen des Aktionsplans Wirtschaftsschutz 2024+ wurden bereits umgesetzt oder werden zurzeit umgesetzt, und gibt es bereits Ergebnisse, welche Bedarfe und Maßnahmen bei kleineren und mittleren Unternehmen sind aus Sicht der Bundesregierung erforderlich?
9. Wie plant die Bundesregierung zukünftig die Koordinierung der Zusammenarbeit mit der EU im Bereich Cybersicherheit?
10. Welche Schlussfolgerungen zieht die Bundesregierung aus dem ersten Bericht von ENISA (Europäische Agentur für Netz- und Informationssicherheit) über den Stand der Cybersicherheit in der Union?
11. Welche Rolle spielt Deutschland bei der NATO-Cyberabwehr (NATO Cooperative Cyber Defence Centre of Excellence), und an welchen Übungen mit bzw. für die NATO-Cyberabwehr hat die Bundeswehr konkret teilgenommen?
12. Wie schätzt die Bundesregierung die Rolle künstlicher Intelligenz in Bezug auf die Cybersicherheitsmaßnahmen der Bundesbehörden ein, und ist geplant, diese einzusetzen, und wenn ja, wo soll künstliche Intelligenz eingesetzt werden?
13. Welche nationalen Forschungsprojekte zu Verschlüsselungstechnologien gibt es nach Kenntnis der Bundesregierung, gibt es Planungen und Vorbereitungen, Quantenkryptografie zu verwenden?
14. Welche neuen Bedrohungsszenarien im Cyberraum erwartet die Bundesregierung in den nächsten fünf Jahren?
15. Wie wird die Informationssicherheit auf Bundesebene derzeit koordiniert, in welchen Formaten tauschen sich Bundesbehörden über Cyberangriffe und getroffene Maßnahmen aus, gibt es einen ressortübergreifenden Maßnahmenplan zum Umgang mit Cyberangriffen?

Berlin, den 18. Dezember 2024

Christian Dürr 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.bundesanzeiger-verlag.de
ISSN 0722-8333