Deutscher Bundestag **Drucksache 20/3308**

20. Wahlperiode 06.09.2022

Kleine Anfrage

der Fraktion der CDU/CSU

Aktueller Stand Umsetzung der Cybersicherheitsagenda

Die Bundesministerin des Innern und für Heimat Nancy Faeser hat am 12. Juli 2022 die Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat (BMI) öffentlich vorgestellt (https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2022/07/cybersicherheitsagenda.html). Das Bundeskabinett hat über diese vom BMI vorgelegte Cybersicherheitsagenda bisher noch keinen Beschluss gefasst.

Am 23. April 2021 verabschiedete der Deutsche Bundestag den vom damaligen Bundesminister des Innern, für Bau und Heimat Horst Seehofer eingebrachten Gesetzentwurf eines „Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme – IT-Sicherheitsgesetz 2.0“ (https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2021/04/it-sicherheitsgesetz.html), am 8. September 2021 beschloss die damalige Bundesregierung die „Cybersicherheitsstrategie für Deutschland 2021“ (https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2021/09/cybersicherheitsstrategie-2021.html).

Zahlreiche Landesregierungen, wie zum Beispiel die baden-württembergische (https://www.baden-wuerttemberg.de/de/service/presse/pressemitteilung/pid/land-beschliesst-umfassende-cybersicherheitsstrategie/) und die nordrhein-westfälische (https://www.land.nrw/pressemitteilung/cybersicherheit-landesregierung-legt-strategie-bis-2024-fest#:~:text=Jahr%202020%20vorgelegt.-,Das%20Kabinett%20hat%20in%20dieser%20Woche%20die%20Cybersicherheitsstrategie%20des%20Landes,und%20gilt%20zun%C3%A4chst%20bis%202024), haben ebenfalls eigene Cybersicherheitsstrategien beschlossen, die sich in der Umsetzung befinden.

Im Interesse der Stärkung einer föderal geprägten Cybersicherheitsarchitektur erarbeiteten zuvor alle Länder eine „Leitlinie zur Entwicklung föderaler Cybersicherheitsstrategien“, die auf der Innenministerkonferenz (IMK) vom 16. bis 18. Juni 2021 in Rust unter TOP 40 und 41 behandelt wurde (https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/20210616-18/beschluesse.pdf?__blob=publicationFile&v=2).

Wir fragen die Bundesregierung:

1. Wurde die am 12. Juli 2022 vorgestellte Cybersicherheitsagenda des BMI zuvor mit den Ressorts der Koalitionspartner BÜNDNIS 90/DIE GRÜNEN und FDP inhaltlich abgestimmt?
2. Wann (Datum) plant die Bundesregierung, die Cybersicherheitsagenda des BMI zu beschließen?

3. Gibt es nach Ansicht der Bundesregierung inhaltliche Übereinstimmungen zwischen der am 12. Juli 2022 vorgestellten Cybersicherheitsagenda des BMI im Vergleich zu der am 8. September 2021 von der damaligen Bundesregierung beschlossenen Cybersicherheitsstrategie für Deutschland 2021?
4. Falls ja, welche inhaltlichen Übereinstimmungen sind das?
5. Welche Gesetzentwürfe zur Umsetzung der Cybersicherheitsagenda befinden sich in Vorbereitung?
6. Welche Gesetzentwürfe zur Umsetzung der Cybersicherheitsagenda plant das BMI in den Deutschen Bundestag einzubringen?
7. Wird an einem „IT-Sicherheitsgesetz 3.0“ gegenwärtig gearbeitet?
8. Welche Haushaltsmittel haben welche Ressorts nach dem Regierungsentwurf zum Bundeshaushalt 2023, der vom Bundesminister der Finanzen Christian Lindner am 1. Juli 2022 öffentlich vorgestellt wurde, zur Umsetzung der Cybersicherheitsagenda zur Verfügung?
9. Wie viele Cyberangriffe gab es seit Beginn des russischen Angriffskrieges gegen die Ukraine auf KRITIS-Unternehmen (kritischer Infrastrukturen), an denen der Bund beteiligt ist?
10. Wie viele Cyberangriffe gab es seit Beginn des russischen Angriffskrieges gegen die Ukraine auf KRITIS-Unternehmen (KRITIS = kritische Infrastrukturen), an denen keine Bundesbeteiligung vorliegt?
11. In welcher Höhe beläuft sich der Gesamtschaden dieser Cyberangriffe auf KRITIS-Unternehmen, an denen der Bund beteiligt ist?
12. Welche konkreten Maßnahmen hat die Bundesregierung veranlasst, um Unternehmen in Deutschland vor Cyberangriffen zu schützen?
13. Welche konkreten Befugnisse sollen nach der am 12. Juli 2022 vorgelegten Cybersicherheitsagenda des BMI das Bundeskriminalamt (BKA), das Bundesamt für Verfassungsschutz (BfV), die Bundespolizei und das Bundesamt für Sicherheit in der Informationstechnik (BSI) zur Abwehr und Verfolgung von Cyberkriminalität zukünftig erhalten?
14. Was konkret versteht die Bundesregierung unter einer „Zentralstelle“ im Bund-Länder-Verhältnis, zu der das BSI laut Cybersicherheitsagenda ausgebaut werden soll?
15. Welche Aufgaben und Kompetenzen, die bisher den Ländern obliegen, sollen auf den Bund aufgrund der angestrebten Änderung des Grundgesetzes, nach der das BSI eine Zentralstellenfunktion im Verhältnis Bund-Länder erhalten soll, übertragen werden?
16. Soll das BSI durch die angestrebte Grundgesetzänderung eine institutionell unabhängig agierende Behörde werden?
17. Wann und wie wird die Bundesregierung die Ankündigung aus dem Koalitionsvertrag zwischen SPD, BÜNDNIS 90/DIE GRÜNEN und FDP, „Wir (…) stellen das Bundesamt für Sicherheit in der Informationstechnik (BSI) unabhängiger auf (…)“ (Koalitionsvertrag, S. 16) umsetzen?
18. Welche Haushaltsmittel sind für das BSI für die Jahre 2023 bis 2025 geplant (bitte nach HH-Jahren aufschlüsseln)?
19. Mit welchen Maßnahmen will der Bund nach der angestrebten Grundgesetzänderung die Zusammenarbeit von Bund und Ländern im Bereich der Cybersicherheitspolitik ausbauen?

20. Welche grundsätzlichen Auswirkungen wird die angestrebte Grundgesetzänderung auf die Cybersicherheitsstrategien der Länder im Lichte der eingangs genannten „Leitlinie zur Entwicklung föderaler Cybersicherheitsstrategien“ haben?

21. Durch welche konkreten Maßnahmen will die Bundesregierung die föderale Zusammenarbeit in der Cybersicherheit stärken?

    Hat die Bundesregierung dazu schon Gespräche mit den Ländern geführt, und wenn ja, mit welchen?

22. Was konkret versteht das BMI laut seiner Cybersicherheitsagenda unter einer „aktiven Cyberabwehr“, und welche konkreten Maßnahmen zur Abwehr eines Cyberangriffs fallen aus Sicht des BMI in den Bereich einer „aktiven Cyberabwehr“ (bitte auflisten)?

23. Subsumiert die Bundesregierung unter einer „aktiven Cyberabwehr“ auch sog. Hackbacks, also intrusive Cyberoperationen?

24. Plant die Bundesregierung neue Rechtsgrundlagen für aktive Cyberabwehrmaßnahmen zu schaffen?

25. Falls nein, worin besteht konkret der Unterschied zwischen einer „aktiven Cyberabwehr“ (laut Cybersicherheitsagenda vom 12. Juli 2022 soll z. B. das BKA Angriffsserver lokalisieren und unschädlich machen können) und einem Hackback?

26. Welche Forschungsaufträge bzw. Forschungsprojekte in welcher Höhe hat die Cyberagentur des Bundes seit ihrem Bestehen an welche Unternehmen vergeben?

27. Sieht es die Bundesregierung als notwendig an, die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) finanziell zu stärken?

28. Falls ja, welchen Aufwuchs an Haushaltsmitteln sieht der Entwurf des Bundeshaushalts 2023 für die ZITiS vor?

29. Sieht die Bundesregierung einen Stellenmehrbedarf im Bereich der Cybersicherheit, und falls ja, in welchem Umfang, und in welcher Behörde?

30. Plant die Bundesregierung die Einführung einer Task-Force bzw. Schnelleingreiftruppe auf Bundesebene zur Unterstützung von Betreibern von KRITIS, Unternehmen, Behörden etc. (Beispiel: Cyberwehr BW/JCU der Europäischen Kommission)?

31. Welche Daten plant die Bundesregierung, in den Hochsicherheitsdatenspeichern (sog. Backup-Server) im Ausland abzuspeichern (https://www.heise.de/news/Staatliche-Daten-Auswaertiges-Amt-setzt-auf-Backup-Speicher-im-Ausland-7188265.html), und mit welchen ausländischen Staaten bzw. Regierungen laufen für deren Umsetzung Gespräche?

    Welches Bundesministerium hat die Federführung bei diesen Backup-Servern?

32. Plant die Bundesregierung, die militärischen und zivilen Cyberfähigkeiten zum Schutz der kritischen Infrastrukturen besser zu verzahnen?

33. Sind seitens der Bundesregierung Maßnahmen und Haushaltsmittel geplant, um das Nationale Cyber-Abwehrzentrum weiter zu stärken?

    Wenn ja, welche konkreten Maßnahmen sind geplant, und welche HH-Mittel sind dafür für die Jahre 2023 bis 2025 vorgesehen (bitte nach HH-Jahren aufschlüsseln)?

34. Wann, und in welcher Form will die Bundesregierung „ein Recht auf Verschlüsselung“ (Koalitionsvertrag, S. 16) einführen?

35. Gibt es seitens der Bundesregierung Überlegungen, die geltenden Regelungen für die Herstellerhaftung bezüglich Schäden, die durch IT-Sicherheitslücken in Produkten verursacht werden, zu verändern?

36. Bis wann und in welchem Umfang plant die Bundesregierung, die Anbindung der Bundeswehr an den Digitalfunk BOS im Sinne der „bundesweiten, sicheren und hochverfügbaren Breitbanddatenkommunikation“ (Cybersicherheitsagenda, S. 14) mit den anderen Behörden und Organisationen mit Sicherheitsaufgaben (BOS) auszubauen?

Berlin, den 5. September 2022

Friedrich Merz, Alexander Dobrindt 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