Deutscher Bundestag **Drucksache 20/3762**

20. Wahlperiode 29.09.2022

Antwort

der Bundesregierung

auf die Kleine Anfrage der Fraktion der CDU/CSU
– Drucksache 20/3308 –

Aktueller Stand Umsetzung der Cybersicherheitsagenda

Vorbemerkung der Fragesteller

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).

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern und für Heimat vom 28. September 2022 übermittelt.

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

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?

Nein. Die Agenda benennt jene Maßnahmen aus dem Themenfeld Cybersicherheit, die das BMI in der 20. Legislaturperiode umsetzen will. Es handelt sich also um eine BMI-interne Agenda. Die von der Durchführung dieser Maßnahmen inhaltlich betroffenen Ressorts werden selbstverständlich zeitgerecht in die Erarbeitung der Inhalte eingebunden.

2. Wann (Datum) plant die Bundesregierung, die Cybersicherheitsagenda des BMI zu beschließen?

Die Agenda wird nicht von der Bundesregierung beschlossen, da es sich um eine Agenda des BMI handelt.

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?

Die Fragen 3 und 4 werden gemeinsam beantwortet.

Ja.

Die Cybersicherheitsstrategie für Deutschland wird unter Federführung des BMI unter Mitwirkung aller Ressorts erstellt und ist vom Kabinett zu beschließen.

In Abgrenzung dazu handelt es sich bei der Cybersicherheitsagenda um eine Agenda des BMI. Maßnahmen aus der Cybersicherheitsstrategie für Deutschland, die durch das BMI umzusetzen sind, wurden (teilweise) übernommen.

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?

Die Fragen 5 und 6 werden gemeinsam beantwortet.

Es wird kein Gesetz zur Umsetzung der Cybersicherheitsagenda des BMI geben, gleichwohl können Regelungsbedarfe abhängig von Konzeptionierungen in Einzelvorhaben notwendig werden.

7. Wird an einem „IT-Sicherheitsgesetz 3.0“ gegenwärtig gearbeitet?

Das BMI arbeitet gegenwärtig nicht an einem IT-Sicherheitsgesetz 3.0.

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?

Die Cybersicherheitsagenda des BMI zeigt lediglich die Maßnahmen des BMI. Andere Ressorts sind hiervon folglich nicht betroffen.

Im genannten Regierungsentwurf sind keine konkreten Mittel für die Umsetzung der Cybersicherheitsagenda des BMI ausgewiesen.

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?

Die Fragen 9 und 10 werden gemeinsam beantwortet.

Gemäß § 8b des BSI-Gesetzes ist das Bundesamt für die Sicherheit in der Informationstechnik (BSI) die zentrale Meldestelle für Betreiber Kritischer Infrastrukturen in Angelegenheiten der Sicherheit in der Informationstechnik.

Das BSI erhebt keine Beteiligungsformen bei Kritischen Infrastrukturen, daher können Cyber-Angriffe auf KRITIS-Betreiber mit Bundesbeteiligung nicht getrennt von Cyber-Angriffen auf KRITIS-Betreiber ohne Bundesbeteiligung ausgewiesen werden. Ersatzweise werden Zahlen zu gemeldeten IT-Störungen für die Gesamtzahl Kritischer Infrastrukturen übermittelt, die neben Cyber-Angriffen auch Ausfälle von Hard- und Software oder IT-Störungen allgemeiner Art beinhalten.

Für den Zeitraum 24. Februar 2022 bis 9. September 2022 wurden dem BSI 253 IT-Störungen gemeldet.

11. In welcher Höhe beläuft sich der Gesamtschaden dieser Cyberangriffe auf KRITIS-Unternehmen, an denen der Bund beteiligt ist?

Das BSI erhält und erhebt keine systematischen Informationen über den volkswirtschaftlichen Schaden durch Cyber-Angriffe in Deutschland.

12. Welche konkreten Maßnahmen hat die Bundesregierung veranlasst, um Unternehmen in Deutschland vor Cyberangriffen zu schützen?

Mit Blick auf die in Rede stehende Cybersicherheitsagenda des BMI werden die angestrebten Maßnahmen derzeit in ihrer weiteren Umsetzung geprüft und vorbereitet. Dazu zählen insbesondere die Maßnahmen unter Punkt 5 (Cyber-Resilienz Kritischer Infrastrukturen stärken) und 6 (Schutz ziviler Infrastrukturen vor Cyberangriffen).

Darüber hinaus wird auf die Antwort der Bundesregierung zu den Fragen 4 und 5 der Kleinen Anfrage der Fraktion der FDP (zur Cybersicherheit im deutschen Mittelstand) auf Bundestagsdrucksache 19/21675, verwiesen.

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?

Das BMI steht hierzu mit den Sicherheitsbehörden in seinem Geschäftsbereich derzeit im Austausch.

14. Was konkret versteht die Bundesregierung unter einer „Zentralstelle“ im Bund-Länder-Verhältnis, zu der das BSI laut Cybersicherheitsagenda ausgebaut werden soll?

Eine Zentralstelle ermöglicht und koordiniert eine auf Dauer angelegte Form der Kooperation, die die laufende gegenseitige Unterrichtung und Auskunftserteilung, die wechselseitige Beratung sowie gegenseitige Unterstützung und Hilfeleistung in den Grenzen der je eigenen Befugnisse umfasst und funktionelle und organisatorische Verbindungen, gemeinschaftliche Einrichtungen und gemeinsame Informationssysteme erlaubt (vgl. BVerfGE 133, 317 f.).

Ein Konzept wird zurzeit vom BMI erstellt und soll dem Deutschen Bundestag von der Bundesregierung Ende des Jahres vorgelegt werden.

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?

Für den Bund soll eine Gesetzgebungskompetenz über die Zusammenarbeit im Bereich der Informationssicherheit sowie eine Verwaltungskompetenz zur Einrichtung einer Zentralstelle im Bereich der Informationssicherheit im Grundgesetz vorgesehen 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?

Die Fragen 16 und 17 werden gemeinsam beantwortet.

Die Bundesregierung prüft zurzeit Gestaltungsoptionen.

18. Welche Haushaltsmittel sind für das BSI für die Jahre 2023 bis 2025 geplant (bitte nach HH-Jahren aufschlüsseln)?

Bislang wurden keine zusätzlichen Haushaltsmittel mit Bezug zur Cybersicherheitsagenda für die genannten Jahre im Bundeshaushalt für das BSI vorgesehen.

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?

Die Fragen 19 bis 21 werden gemeinsam beantwortet.

Die Bundesregierung will die föderale Zusammenarbeit durch den Ausbau des BSI zu einer Zentralstelle stärken; hierzu ist sie mit allen Ländern im Gespräch.

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?

Die Fragen 22 bis 25 werden gemeinsam beantwortet.

Die Cybersicherheitsagenda des BMI verwendet weder den Begriff einer „aktiven Cyberabwehr“ noch den Begriff eines „Hackbacks“.

Das BMI plant die Cyberfähigkeiten der Sicherheitsbehörden des Bundes zu stärken. Es plant zudem neue Befugnisse zur Gefahrenabwehr für die Sicherheitsbehörden des Bundes zu schaffen. Dabei geht es auch um Maßnahmen, die über eine bloße Aufklärung eines Angriffs hinausgehen. Die konkreten Änderungsbedarfe werden derzeit durch das BMI ermittelt.

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

Projekt	Budget (brutto)	Auftragnehmer
Encrypted Computing	226.100 €	Helmholtz Center for Information Security (CISPA)
Ökosystem vertrauenswürdige IT	476.000 €	FZI Forschungszentrum Informatik Karlsruhe und Hensoldt Cyber GmbH
Startup Landscape	76.500 €	Innospot GmbH
Brain Privacy Framework	152.320 €	NeuroMentum AI GmbH

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

Die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) hat die Aufgabe, die Behörden des Bundes mit Sicherheitsaufgaben im Hinblick auf deren operative Cyberfähigkeiten zu beraten und zu unterstützen.

Hierzu entwickelt, unterstützt und berät die ZITiS bereits heute bedarfsgerecht und anwendungsorientiert die Sicherheitsbehörden als zentraler Dienstleister. Die Bundesregierung strebt einen weiteren Ausbau der ZITiS als zentralen Dienstleister für die Bundesbehörden mit Sicherheitsaufgaben an, was mit finanziellen Mehrbedarfen verbunden wäre.

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

Der Entwurf der Bundesregierung zum Bundeshaushalt 2023 sieht Gesamtausgaben in Höhe von 85 395 000 Euro vor. Gemessen an vorheriger Finanzplanung liegt hierin ein Aufwuchs von 13 000 000 Euro an Personal- und Sachmitteln. Weil der Haushalt 2022 noch in erheblichem Umfang einmalig bereitgestellte Mittel für insbesondere verschiedene Projekte beinhaltete, ergibt sich im reinen Zahlenvergleich 2022 zu 2023 für den Haushaltsentwurf 2023 ein geringerer Haushaltsansatz.

Bislang sind keine zusätzlichen Haushaltsmittel mit Bezug zur Cybersicherheitsagenda für die genannten Jahre im Bundeshaushalt für die ZITiS vorgesehen.

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

Ja. Der Umfang wird aktuell ermittelt.

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)?

Es gibt im BSI bereits sogenannte Mobile Incident Response Teams (MIRT), die KRITIS Betreiber, Bundes- und Landesbehörden auf deren Ersuchen z. B. im Falle von herausgehobenen IT-Störungen unterstützen können.

Zusätzlich ist die Einrichtung eines „Kompetenzzentrums operative Sicherheitsberatung des Bundes“ (KoSi Bund) zur Unterstützung der Bundesbehörden geplant.

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?

Die Federführung für die Errichtung eines Digitalen Ausweichsitzes liegt im Auswärtigen Amt. Der Prozess zur Ermittlung des konkreten Bedarfs an zu speichernden Daten wird derzeit entworfen. Eine Auskunft hinsichtlich der Verhandlungen mit in Frage kommenden Drittstaaten kann nicht erteilt werden, da eine solche Auskunft den Entscheidungsspielraum der Bundesregierung im noch laufenden Prozess verengen würde.

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

Änderungen bezüglich der Zuständigkeiten zwischen dem Bundesministerium der Verteidigung und dem BMI im Bereich der militärischen und zivilen Cyberfähigkeiten zum Schutz Kritischer Infrastrukturen sind nicht geplant.

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)?

Die Fortentwicklung des nationalen Cyber-Abwehrzentrums (Cyber-AZ) wird sich auf die Verbesserung des Informationsaustauschs und ein stets aktuelles ganzheitliches Lagebild zu Cyber-Vorfällen konzentrieren. Das Cyber-AZ verfügt weder über eigenes Personal noch über eigene Haushaltsmittel. Das Personal wird von den teilnehmenden Behörden gestellt und liegt jeweils in der dortigen Haushaltsverantwortung. Benötigte Sachmittel werden aus dem Haushalt des BSI bereitgestellt.

Zum jetzigen Zeitpunkt wird zwischen den Ressorts und Behörden erörtert, wie der Informationsaustausch und das Lagebild zu Cyber-Vorfällen weiter verbessert werden können.

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

Verpflichtungen für Dienstanbieter und Dienstleister zur Verschlüsselung der Daten bzw. der Kommunikation von Bürgerinnen und Bürgern bestehen bereits in einigen Bereichen (z. B. Mobilfunk/TKG; Gesundheits- und Sozialdaten/SGB). Ob darüber hinaus ein Erfordernis besteht, den Anspruch auf Verschlüsselung auf andere Bereiche auszuweiten und auch dort Dienstanbieter und Dienstleister in die Pflicht zu nehmen, prüft die Bundesregierung derzeit.

Im Übrigen ist die Nutzung von Verschlüsselungsprodukten durch die Bürgerinnen und Bürger in keiner Weise rechtlich oder faktisch eingeschränkt. Jeder kann derartige Produkte zum Schutz seiner persönlichen Daten uneingeschränkt einsetzen. Insoweit besteht bereits ein generelles Recht auf Verschlüsselung.

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?

Nach Auffassung der Bundesregierung sollten Hersteller für Schwächen in der Cybersicherheit ihrer Produkte auch haftungsrechtlich einstehen müssen und kann eine mangelnde Cybersicherheit schon heute eine Herstellerhaftung begründen. Die außervertragliche Haftung des Herstellers richtet sich im deutschen Recht vornehmlich nach dem Produkthaftungsgesetz (ProdHaftG) und den §§ 823 ff. des Bürgerlichen Gesetzbuches (BGB). Das ProdHaftG setzt die vollharmonisierende Richtlinie 85/374/EWG des Rates vom 25. Juli 1985 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte (Produkthaftungsrichtlinie) um. Grundsätzlich haftet ein Hersteller für Schäden an Personen oder anderen Sachen als dem Produkt selbst nach diesen Vorschriften unter den weiteren dort genannten Voraussetzungen, wenn ein Produkt nicht die Sicherheit bietet, die unter Berücksichtigung aller Umstände berechtigterweise von ihm erwartet werden kann. Die EU-Kommission hat einen Vorschlag zur Revision der Produkthaftungsrichtlinie für den 28. September 2022 angekündigt. Die Bundesregierung wird sich weiterhin dafür aussprechen, dass Hersteller für Schäden haften, die fahrlässig durch IT-Sicherheitslücken in ihren Produkten verursacht werden.

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?

Mit Inkrafttreten des Dritten Gesetzes zur Änderung des BDBOS-Gesetzes am 3. Dezember 2019 wurde die Bundeswehr Nutzer des Digitalfunks BOS neben den Behörden und Organisationen mit Sicherheitsaufgaben.

Eine Differenzierung der Nutzer erfolgt nicht und soll auch zukünftig nicht erfolgen.

Für den schrittweisen Aufbau eines bundesweiten, sicheren und hochverfügbaren breitbandigen Netzes für Sprach- und Datenkommunikation für die Behörden und Organisationen mit Sicherheitsaufgaben (BOS) und der Bundeswehr wurde vom Verwaltungsrat der Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS) sowie der Innenministerkonferenz ein 4-Phasenmodell beschlossen. Demnach wird der gesamte Kommunikationsbedarf inklusive der einsatzkritischen Sprach- und Datenanwendungen der BOS sowie geeignete Anteile des Kommunikationsbedarfs der Bundeswehr in ein gemeinsames Breitbandnetz überführt. Wesentlich für eine Zeitplanung ist die Bereitstellung von Ressourcen und Frequenzen. Notwendige UHF-Frequenzen könnten ab 2031 zur Verfügung stehen.

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