Deutscher Bundestag **Drucksache 20/7956**

20. Wahlperiode 01.08.2023

Antwort

der Bundesregierung

auf die Kleine Anfrage der Fraktion der CDU/CSU
– Drucksache 20/7698 –

Sicherheit europäischer 5G-Mobilfunknetze

Vorbemerkung der Fragesteller

Am 15. Juni 2023 wurde der Zweite Fortschrittsbericht über die Umsetzung des EU-Instrumentariums für die 5G-Cybersicherheit (EU-Toolbox on 5G Cybersecurity) veröffentlicht. Im Zuge dessen hat die Europäische Kommission eine Mitteilung zur Umsetzung des EU-Instrumentariums für die 5G-Cybersicherheit angenommen (digital-strategy.ec.europa.eu/en/library/communication-commission-implementation-5g-cybersecurity-toolbox).

Darin zeigt sich die EU-Kommission „besorgt über die Risiken, die von bestimmten Mobilfunk-Netzausrüstungsanbietern für die Sicherheit der Union ausgehen“ und nennt dabei insbesondere die Anbieter Huawei und ZTE. Gleichzeitig kündigt die Kommission an, künftig zu vermeiden, dass interne Kommunikation über Mobilfunknetze, in denen Komponenten von Huawei und ZTE verbaut sind, stattfindet. Zudem sollen fortan „keine neuen Netzanbindungsdienste beschafft werden, die auf Ausrüstung dieser Anbieter angewiesen sind“.

Im Fortschrittsbericht wird dargelegt, dass bisher 21 Staaten den legislativen Rahmen geschaffen hätten, um das unterschiedliche Risikoprofil verschiedener Lieferanten zu bewerten und darauf aufbauend Restriktionen, einschließlich notwendiger Ausschlüsse, anzuwenden (digital-strategy.ec.europa.eu/de/library/second-report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity). EU-Kommissar Thierry Breton kritisierte in einer Rede jedoch deutlich, dass bisher nur zehn Mitgliedstaaten tatsächlich Maßnahmen ergriffen hätten, um Hochrisikoanbieter zu beschränken oder auszuschließen. Dies sei deutlich zu langsam, stelle ein erhebliches Sicherheitsrisiko dar und kreiere wesentliche Abhängigkeiten für die EU (ec.europa.eu/commission/presscorner/detail/en/speech_23_3314).

In Deutschland wurden mit dem von der CDU/CSU-geführten Vorgängerregierung auf den Weg gebrachten IT-Sicherheitsgesetz 2.0 Instrumente geschaffen, um den Einbau von Komponenten nichtvertrauenswürdiger Hersteller in kritischen Infrastrukturen zu untersagen (§ 9b des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG). Zum jetzigen Zeitpunkt ist nach Kenntnis der Fragesteller jedoch keine entsprechende Untersagung erfolgt und nur erstmalig eingesetzte Komponenten wurden einer kritischen Prüfung unterzogen. Im März 2023 wurden Unternehmen der Branche in einem Schreiben darauf hingewiesen, dass künftig auch weitere kriti-

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern und für Heimat vom 31. Juli 2023 übermittelt.

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

sche Komponenten überprüft werden sollen (background.tagesspiegel.de/digitalisierung/us-sanktionen-setzen-huawei-schwer-zu). Als Antwort auf die Kleine Anfrage der Fraktion der CDU/CSU auf Bundestagsdrucksache 20/6921 bestätigte die Bundesregierung, dass derzeit eine Prüfung von im Einsatz befindlichen kritischen Komponenten in 5G-Mobilfunknetzen erfolgt. Das Verfahren soll im Sommer abgeschlossen werden (Bundestagsdrucksache 20/6921). „DER SPIEGEL“ berichtete indessen, dass das Bundesministerium des Innern und für Heimat (BMI) eine wichtige Softwarekomponente des Herstellers Huawei untersagen könnte. Dabei handle es sich um ein „Programm, mit dem die Basisstationen des chinesischen Konzerns aus der Ferne konfiguriert und gesteuert werden können“ (www.spiegel.de/panorama/5g-mobilfunknetz-in-deutschland-behoerden-koennten-einsatz-von-huawei-technik-untersagen-a-c5657fae-515d-48fc-aabd-fa3f657adf71). Demnach stehen „dabei Bauteile des 4G-Netzes im Fokus, die per Software-Update 5G-fähig werden und damit kritische Funktionen für den Netzbetrieb übernehmen können. Die Befürchtung ist, dass dadurch Daten für Spionagezwecke gesammelt und im Extremfall das Handynetz manipuliert oder abgeschaltet werden könnte. Die Vorstellung, einen eindeutigen Beweis in Form eines „Kill Switches“ zu finden, halten die Sicherheitsbehörden für abwegig. Das eigentliche Risiko ergebe sich durch die Software-Updates, mit denen sich bestimmte Bauteile umprogrammieren ließen – womöglich unbemerkt von den Netzbetreibern.“ (www.handelsblatt.com/politik/deutschland/huawei-innenministerium-hat-anhaltspunkte-fuer-sicherheitsprobleme/29212436.html).

1. Über welches Mobilfunknetz kommuniziert die Bundesregierung intern?

Für die offene Kommunikation im Mobilfunknetz nutzt die Bundesregierung die am Markt verfügbaren Angebote. Für die verschlüsselte Kommunikation verwendet die Bundesregierung individuelle Sicherheitslösungen.

2. Wie hoch ist der Anteil von Komponenten von Huawei und ZTE in dem Mobilfunknetz, das die Bundesregierung für ihre interne Kommunikation nutzt?

Hierzu liegen der Bundesregierung keine Erkenntnisse vor.

Auf die Antworten zu den Fragen 1 und 31 wird verwiesen.

3. Wie bewertet die Bundesregierung die Ankündigung der EU-Kommission, die Nutzung von Mobilfunknetzen mit Komponenten von Huawei und ZTE für die interne Kommunikation künftig zu vermeiden, und plant die Bundesregierung, der Auffassung der EU-Kommission zu folgen?

Die Bundesregierung hat die Ankündigung der EU-Kommission, Maßnahmen zu ergreifen, um die Verwendung von Mobilfunknetzen, die Komponenten der Hersteller Huawei und ZTE einsetzen, zu vermeiden, zur Kenntnis genommen.

In der Bundesrepublik Deutschland ist insoweit § 9b des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) maßgeblich. Hierbei macht die Bundesregierung von dem ihr zur Verfügung stehenden gesetzlichen Rahmen vollumfassend Gebrauch und hat für den Einsatz von Komponenten der o. g. Hersteller in deutschen 5G-Mobilfunknetzen eine Prüfung nach § 9b Absatz 4 BSIG (sog. ex post-Prüfung) eingeleitet. Wie in der Vorbemerkung der Fragesteller zutreffend dargestellt, befindet sich die Prüfung derzeit im Stadium der Sachverhaltsermittlung, die noch im Sommer 2023 abgeschlossen werden soll. Anschließend erfolgt die Entscheidungsfindung der Bundesregierung. Das Bundesministerium des Innern und für Heimat (BMI) prüft gegenwärtig, welche Auswirkungen die Entscheidung der EU-Kommission für

die sicherheitspolitische Bewertung der Bundesregierung im Rahmen der laufenden Prüfungsverfahren haben könnte.

Auf die Antwort zu Frage 14 wird verwiesen.

4. Plant die Bundesregierung, der EU-Kommission zu folgen, künftig keine neuen Netzanbindungsdienste zu beschaffen, die auf Ausrüstung von Huawei und ZTE angewiesen sind, wenn ja, warum, und wenn nein, warum nicht?

Der Begriff Netzanbindungsdienste ist der Bundesregierung im Zusammenhang mit Telekommunikationstechnik nicht bekannt.

5. In welchen EU-Staaten gibt es nach Kenntnis der Bundesregierung chinesische Mobilfunknetzbetreiber, und stellt dies nach Auffassung der Bundesregierung ein grenzüberschreitendes Sicherheitsrisiko für die EU dar (bitte entsprechende EU-Staaten und jeweilige Mobilfunknetzbetreiber einzeln auflisten)?

Hierzu liegen der Bundesregierung keine über die öffentlich recherchierbaren Informationen hinausgehenden Erkenntnisse vor.

6. Welche Maßnahmen hat die Bundesregierung getroffen, um gemäß den Empfehlungen der EU-Toolbox Hochrisikoanbieter (SM03) einzuschränken?

7. Sieht die Bundesregierung bei sich Versäumnisse in der Umsetzung der EU-Toolbox, insbesondere im Bereich der Anwendung von Maßnahmen zur Einschränkung von Hochrisikoanbietern, wenn ja, warum, und wenn nein, warum nicht?

Die Fragen 6 und 7 werden gemeinsam beantwortet.

Die Umsetzung der EU-Toolbox in Deutschland ist im Wesentlichen durch die Einführung des § 9b BSIG im IT-Sicherheitsgesetz 2.0 erfolgt, das im Mai 2021 in Kraft getreten ist. Dabei hatte sich der Gesetzgeber für eine technologie- und herstellerneutrale Einzelfallprüfung des Komponenteneinsatzes entschieden. Die Einstufung einzelner Hersteller als Hochrisikoanbieter ist im deutschen Recht damit nicht angelegt. Eine gesetzliche Grundlage für Beschränkungen des Einsatzes kritischer Komponenten in 5G-Mobilfunknetzen besteht nur in Form des § 9b BSIG, von dem die Bundesregierung vollständig Gebrauch macht – wie in der Antwort zu Frage 3 erläutert.

8. Sind der Bundesregierung Planungen der EU-Kommission bekannt, verbindliche Vorgaben zum Ausschluss von Hochrisikoanbietern beim Ausbau von 5G-Mobilfunknetzen einführen zu wollen (www.spiegel.de/netzwelt/netzpolitik/5g-eu-erwaegt-wohl-doch-verbindliche-vorgaben-zum-huawei-ausschluss-a-5d82424a-3689-4102-a90f-8fbd268c389f), und ist die Bundesregierung in diese Planungen einbezogen?

9. Ist nach Auffassung der Bundesregierung ein EU-weites Verbot von Komponenten von Hochrisikoanbietern in 5G-Mobilfunknetzen rechtlich möglich?

Die Fragen 8 und 9 werden gemeinsam beantwortet.

Über die Berichterstattung hinausgehende Erkenntnisse liegen der Bundesregierung hierzu nicht vor. Vorhaben, über deren Ausgestaltung nichts bekannt ist, können nicht rechtlich bewertet werden.

10. Ist es zutreffend, dass sich das Bundesamt für Sicherheit in der Informationstechnik (BSI) bei der derzeit laufenden Überprüfung von Bestandskomponenten auf eine Softwarekomponente des chinesischen Herstellers Huawei konzentriert (www.spiegel.de/panorama/5g-mobilfunknetz-in-deutschland-behoerden-koennten-einsatz-von-huawei-technik-untersagen-a-c5657fae-515d-48fc-aabd-fa3f657adf71)?

Die Prüfverfahren nach § 9b BSIG führt das BMI durch, nicht das Bundesamt für Sicherheit in der Informationstechnik (BSI). Zu den Inhalten laufender Prüfverfahren äußert sich die Bundesregierung nicht. Die Kontrollkompetenz des Parlaments erstreckt sich grundsätzlich nur auf bereits abgeschlossene Vorgänge und umfasst nicht die Befugnis, in laufende Entscheidungsvorbereitungen einzugreifen.

11. Ist es nach Kenntnis der Bundesregierung technisch zutreffend, dass in Basisstationen deutscher Mobilfunknetze Softwarekomponenten verbaut sind, die aus China konfiguriert und gesteuert werden können (www.spiegel.de/panorama/5g-mobilfunknetz-in-deutschland-behoerden-koennten-einsatz-von-huawei-technik-untersagen-a-c5657fae-515d-48fc-aabd-fa3f657adf71)?

Grundsätzlich sind nahezu alle Softwarekomponenten per Fernwartung konfigurierbar.

Auf die Antwort zu Frage 14 wird verwiesen.

12. Was genau könnte nach Kenntnis der Bundesregierung mit den in Rede stehenden Softwarekomponenten aus China heraus konfiguriert und gesteuert werden?

Die Antwort zu Frage 11 gilt grundsätzlich für alle Funktionen vernetzter Komponenten. Zu den einzelnen Inhalten laufender Prüfverfahren kann sich die Bundesregierung nicht äußern, vgl. Antwort zu Frage 10.

13. Ist es nach Kenntnis der Bundesregierung zutreffend, dass im Extremfall das Mobilfunknetz aus China heraus abgeschaltet werden könnte (www.handelsblatt.com/politik/deutschland/huawei-innenministerium-hat-anhaltspunkte-fuer-sicherheitsprobleme/29212436.html)?

Auf die Antworten zu den Fragen 11 und 12 wird verwiesen.

14. Hält die Bundesregierung es für möglich, dass Software-Updates bei Mobilfunk-Komponenten mit Fernwartungsfunktionen vollständig überprüft und ihre Sicherheit garantiert werden können (www.handelsblatt.com/politik/deutschland/huawei-innenministerium-hat-anhaltspunkte-fuer-sicherheitsprobleme/29212436.html)?

Im Regelprozess sind Softwareupdates nicht vollständig überprüfbar. Auch intensive Testungen können keine vollständige Sicherheit garantieren. Bei den Prüfungen nach § 9b BSIG ist im Schwerpunkt eine sicherheitspolitische Prognoseentscheidung zu treffen, in die neben der Vertrauenswürdigkeit des Her-

stellers nach § 9b Absatz 5 BSIG die in § 9b Absatz 2 BSIG genannten, nichttechnischen sicherheitspolitischen Aspekte, z. B. die sicherheitspolitischen Ziele der Bundesrepublik Deutschland, der Europäischen Union oder des Nordatlantikvertrages, staatliche Kontrolle des Herstellers oder Beteiligung des Herstellers an Aktivitäten, die nachteilige Auswirkungen auf die öffentliche Ordnung oder Sicherheit haben oder hatten, berücksichtigt werden können.

15. Teilt die Bundesregierung, die Auffassung des Bundesministers für Wirtschaft und Klimaschutz Dr. Robert Habeck, derzufolge „Deutschland […] künftig keine Huawei-Produkte mehr in modernen 5G-Mobilfunknetzen verbauen [will].“ (www.spiegel.de/netzwelt/netzpolitik/5g-eu-erwaegt-wohl-doch-verbindliche-vorgaben-zum-huawei-ausschluss-a-5d82424a-3689-4102-a90f-8fbd268c389f)?

Die Prüfungen des BMI nach § 9b BSIG befinden sich derzeit noch im Stadium der Sachverhaltsaufklärung, diese soll in diesem Sommer abgeschlossen werden. Auf die Antwort zu Frage 3 wird verwiesen. Anschließend wird die Bundesregierung eine Entscheidung treffen. Bis dahin ist die Willensbildung innerhalb der Bundesregierung nicht abgeschlossen.

16. Wie viel Prozent der in Deutschland ansässigen Unternehmen sind von Mobilfunknetzen mit verbauten Komponenten chinesischer Hersteller abhängig?

Hierzu liegen der Bundesregierung keine Erkenntnisse vor.

17. Welche weiteren Bundesbehörden sind neben dem BSI an der derzeit laufenden Prüfung der kritischen Komponenten im Mobilfunknetz beteiligt (bitte auflisten)?

18. Welche weiteren Bundesministerien wurden von Beginn an vom BMI mit in den in Frage 17 genannten Prüfungsprozess einbezogen?

19. Werden seitens der Bundesregierung auch Sicherheitsbehörden der Länder an der Prüfung beteiligt?

20. Wird seitens der Bundesregierung auch die Bundeswehr (Kommando Cyber- und Informationsraum, Kommando CIR) an der Prüfung beteiligt?

Die Fragen 17 bis 20 werden gemeinsam beantwortet.

Die Prüfverfahren nach § 9b BSIG führt das BMI durch, nicht das BSI.

Das BMI beteiligt an den Prüfverfahren zunächst das Bundesministerium für Digitales und Verkehr (BMDV), das Auswärtige Amt (AA), das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) und das Bundeskanzleramt. Diese beteiligen wiederum Geschäftsbereichsbehörden: das BMI, das Bundesamt für Verfassungsschutz (BfV) und das BSI, das BMDV die Bundesnetzagentur, das Bundeskanzleramt den Bundesnachrichtendienst. Als Zentralstelle für den Verfassungsschutz beteiligt das BfV im Einzelfall auch Landesbehörden für Verfassungsschutz. Eine Beteiligung der Bundeswehr ist bisher nicht erfolgt.

21. Würde das Kommando CIR im Spannungsfall (Artikel 80a des Grundgesetzes – GG) federführend die Aufgabe des Cyberschutzes der kritischen Infrastrukturen übertragen bekommen, wenn ja, für welche kritischen Infrastrukturen wäre das Kommando CIR im Spannungsfall federführend zuständig (bitte auflisten), und wenn nein, bleiben auch im Spannungsfall die Betreiber für den Cyberschutz der kritischen Infrastrukturen zuständig?

    Welche Rolle nimmt das BSI im Spannungsfall beim Cyberschutz kritischer Infrastrukturen ein?

In Bezug auf die Verantwortlichkeiten zum Schutz von Infrastrukturen wird auf die Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der CDU/CSU „Verteidigung im Cyberraum – EU-Kooperation und aktive Cyberverteidigung“ auf Bundestagsdrucksache 20/5597, im Einzelnen die Vorbemerkung sowie Fragen 12 und 40 verwiesen. Grundsätzlich, und so auch im Spannungsfall, sind die Betreiber von Kritischen Infrastrukturen für Schutzmaßnahmen (z. B. Gewährleistung IT-Sicherheit) in ihren Objekten verantwortlich. Das gilt auch für Gefahren im und aus dem Cyberraum. Wie in der Cybersicherheitsstrategie für Deutschland 2021 ausgeführt, zielt die Bundesregierung auf eine enge Zusammenarbeit und einen intensiven Informationsaustausch zwischen Wirtschaft und den zuständigen staatlichen Stellen ab. In Bezug auf die staatliche Aufgabe der Abwehr von Gefahren und Angriffen bewirkt die Feststellung des Spannungsfalles keine Neuaufteilung von Aufgaben und Befugnissen staatlicher Institutionen im Sinne einer Übertragung der Federführung für den Schutz von Objekten in Deutschland. Das BSI nimmt auch im Spannungsfall seine gesetzlichen Aufgaben, insbesondere durch seine Rolle als zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen, wahr. Jedoch haben die Streitkräfte gemäß Artikel 87a Absatz 3 Satz 1 des Grundgesetzes (GG) im Verteidigungs- und Spannungsfall unter anderem zusätzlich die Befugnis, zivile Objekte auch gegen zivile Störer zu schützen, jedoch nur, soweit dies für die Erfüllung des Verteidigungsauftrages erforderlich ist.

22. Würde das Kommando CIR im Verteidigungsfall (Artikel 115a GG) federführend die Aufgabe des Cyberschutzes der kritischen Infrastrukturen übertragen bekommen, wenn ja, für welche kritischen Infrastrukturen wäre das Kommando CIR im Verteidigungsfall federführend zuständig (bitte auflisten), und wenn nein, bleiben auch im Verteidigungsfall die Betreiber für den Cyberschutz der kritischen Infrastrukturen zuständig?

    Welche Rolle nimmt das BSI im Verteidigungsfall beim Cyberschutz kritischer Infrastrukturen ein?

Die Ausführungen in der Antwort zu Frage 21 gelten sinngemäß auch im Falle des festgestellten Verteidigungsfalls.

23. Führt die Bundesregierung Übungen durch, in denen das Zusammenspiel von Kommando CIR und weiteren Sicherheitsbehörden zum Cyberschutz kritischer Infrastrukturen im Spannungs- oder Verteidigungsfall geübt wird?

Die in der Antwort zu den Fragen 21 und 22 dargestellten grundsätzlichen Zuständigkeiten gelten sowohl in Friedenszeiten als auch im Spannungs- und Verteidigungsfall. Bereits in Friedenszeiten ist daher eine enge Zusammenarbeit und Abstimmung unter den Behörden mit Aufgaben der Cybersicherheit erforderlich. Die Bundesregierung hat dies in der Nationalen Sicherheitsstrategie aufgezeigt und zielt darauf ab, ausgehend vom gemeinsamen Cyberlagebild im

täglichen Betrieb flexible Abstimmungs- und Entscheidungsprozesse für den Krisenfall einzuüben. Hierzu werden ressortübergreifende Übungen hinsichtlich des Cyberschutzes Kritischer Infrastrukturen unter Beteiligung Kommando Cyber- und Informationsraum (CIR) und weiterer Sicherheitsbehörden durchgeführt. Die Bundesregierung geht davon aus, dass dies auch im Spannungs- und Verteidigungsfall eine ausreichende Koordinierung sicherstellt.

24. Verbaut die Deutsche Bahn nach Kenntnis der Bundesregierung weiterhin Komponenten von Huawei „zum Aufbau eines betriebsinternen IT-Netzwerks“ (www.handelsblatt.com/politik/deutschland/kritische-infrastruktur-ampel-politiker-fordern-ausschluss-von-huawei-bei-der-deutschen-bahn/29081420.html), und wie bewertet die Bundesregierung diesen Sachverhalt?

Die Fragen 24 und 26 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Die Vergabe von Aufträgen für Dienstleistungen und Produkte, auch in der kritischen Infrastruktur, ist über formale Ausschreibungsprozesse geregelt, die nach den jeweils gültigen nationalen und europäischen Rechtsgrundlagen und Standards erfolgen. Der Ausschreibungsprozess sieht dabei eine Prüfung der Glaubwürdigkeit der eingereichten Ausschreibungsunterlagen vor. Unter Berücksichtigung der definierten Bewertungskriterien und Anforderungen findet die Zuschlagserteilung statt. Aktuell gibt es keine Rechtsgrundlagen oder Standards, die einen Ausschluss von Huawei-Komponenten rechtfertigen würden.

Nach Angaben der Deutschen Bahn AG hat diese im Rahmen eines europaweiten Vergabeverfahrens einen Auftrag zum Aufbau eines betriebsinternen IT-Netzwerks an die Telekom (Telekom Business-Solutions GmbH) vergeben. Dabei obliegt es dem Lieferanten, die konkreten technischen Komponenten entsprechend den vorgegebenen Spezifikationen festzulegen.

Darüber hinaus kommen im bahnbetrieblichen Mobilfunknetz GSM-R (Global System for Mobile Communication - Rail) der DB Netz AG seit dem Jahr 2015 in einem laufenden Reinvestitionsprojekt Komponenten des chinesischen Herstellers Huawei zum Einsatz. Auch diese Leistungen wurden nach geltendem Recht ausgeschrieben und in diesem Fall an Nokia und Huawei vergeben. Nach intensiver Erprobung, umfassenden Zulassungsverfahren und Freigabe unter Aufsicht des Eisenbahn-Bundesamts (EBA), wurden die Komponenten im Netz der Deutschen Bahn AG verbaut. Dies bezieht sich lediglich auf die Zugangsnetzebene (Funk-Basisstationen), nicht auf die Zentralsysteme der Vermittlungsnetzebene und Datenbanken.

25. Teilt die Bundesregierung die Auffassung der Deutschen Bahn AG, der zufolge für „Netzwerk-Infrastruktur keine Meldepflicht bestehe, weil das Funknetz der DB Netz nicht öffentlich sei. Das Bundesamt für Sicherheit in der Informationstechnik betonte, dass die IT-Systeme der Bahn bislang nicht als kritisch eingestuft würden“ (www.handelsblatt.com/politik/deutschland/kritische-infrastruktur-ampel-politiker-fordern-ausschluss-von-huawei-bei-der-deutschen-bahn/29081420.html), und wenn ja, bitte begründen?

Soweit mit der Meldepflicht die Anzeigepflicht nach § 9b Absatz 1 BSIG gemeint ist, so unterfallen dieser nur kritische Komponenten im Sinne des § 2 Absatz 13 BSIG. Solche wurden bisher nur für öffentliche 5G-Telekommunikationsnetze definiert. Soweit mit der Meldepflicht eine Pflicht zur Meldung von Störungen nach § 8b Absatz 4 BSIG gemeint ist, ist darauf hinzuweisen, dass es sich bei den betreffenden Telekommunikationsanlagen der Deutschen Bahn

AG nicht um Kritische Infrastrukturen im Sinne der BSI-Kritisverordnung handelt.

26. In welchen weiteren internen IT-Systemen und Mobilfunknetzen verbaut die Deutsche Bahn AG derzeit nach Kenntnis der Bundesregierung Komponenten chinesischer Hersteller?

Auf die Antwort zu Frage 24 wird verwiesen.

27. Bezugnehmend auf die Antwort zu Frage 17 auf Bundestagsdrucksache 20/6271 – hat die Bundesregierung inzwischen überprüft, ob die Bundeswehr Komponenten chinesischer Hersteller gekauft oder in Anwendung hat?

28. Bezugnehmend auf die Antwort zu Frage 17 auf Bundestagsdrucksache 20/6271 – in Bezug auf welche Bereiche der Bundeswehr und in Bezug auf welche Produkte hat die Bundesregierung den Verdacht, dass die Bundeswehr Komponenten chinesischer Hersteller gekauft oder in Anwendung hat?

Die Fragen 27 und 28 werden zusammen beantwortet. Die Bundeswehr hat keine solche Prüfung eingeleitet. In nahezu jedem digitalen Gerät sind chinesische Komponenten enthalten. Auch in Produkten europäischer und US-amerikanischer Hersteller sind aus China stammende Einzelteile verbaut, die durch das Personal der Bundeswehr nicht als chinesisch identifiziert werden können. Durch die Schutzmaßnahmen in der Bundeswehr wird sichergestellt, dass diese Geräte nicht unbemerkt kommunizieren können.

29. Bezugnehmend auf die Antwort zu Frage 25 auf Bundestagsdrucksache 20/6271, der zufolge „die Bundesregierung Kenntnis über verwendete kritische Komponenten im Sinne des § 2 Absatz 13 BSIG aufgrund der beim BMI nach § 9b Absatz 1 BSIG eingehenden Anzeigen“ erlangt – wie hoch ist der Anteil an kritischen Komponenten chinesischer Hersteller in den deutschen Mobilfunknetzen?

Der Anzeigepflicht nach § 9b Absatz 1 BSIG unterfallen nur erstmalig eingesetzte Komponenten. Um auch einen Überblick über den Bestand zu erhalten, hat das BMI im März 2023 eine sog. ex post-Prüfung nach § 9b Absatz 4 BSIG eingeleitet. Diese Prüfung bezieht sich nur auf die Hersteller Huawei und ZTE, nicht auf andere Hersteller. Soweit ein prozentualer Anteil für die Sicherheitsbewertung relevant ist, ermittelt das BMI diesen im Rahmen der laufenden Sachverhaltsaufklärung. Zu den einzelnen Inhalten der laufenden Verwaltungsverfahren kann keine Auskunft erteilt werden.

Auf die Antwort zu Frage 10 wird verwiesen.

30. Bezugnehmend auf die Antwort zu Frage 2 auf Bundestagsdrucksache 20/6921), der zufolge das BMI die „Betreiber von öffentlichen 5G-Mobilfunknetzen am 6. März 2023 aufgefordert [hat], alle in den jeweiligen Netzen im Einsatz befindlichen kritischen Komponenten der Hersteller Huawei und ZTE mitzuteilen und nach einer vorgegebenen Systematik aufzulisten.“ – haben inzwischen alle Betreiber von öffentlichen 5G-Mobilfunknetzen dem BMI geantwortet und ihre kritischen Komponenten der Hersteller Huawei und ZTE mitgeteilt und diese nach der vorgegebenen Systematik aufgelistet, und wenn nein, welche Betreiber von öffentlichen 5G-Mobilfunknetzen haben nicht oder nicht vollständig geantwortet?

Zu den einzelnen Inhalten der laufenden Prüfverfahren kann keine Auskunft erteilt werden. Die Frage berührt zudem Betriebs- und Geschäftsgeheimnisse der beteiligten Betreiber.

31. Kann die Bundesregierung den im Presseartikel genannten Anteil an chinesischen Komponenten im deutschen Mobilfunknetz bestätigen „Andere Länder in Europa haben längst gehandelt und chinesische Komponenten komplett aus ihren Netzen verbannt. Darunter: Estland, Lettland, Litauen, Norwegen, Schweden, Dänemark, Tschechien, die Slowakei und Luxemburg. Frankreich hat den Anteil von 26 auf 17 Prozent gesenkt. In Deutschland aber ist der Anteil chinesischer Technik in den Mobilfunknetzen gestiegen: Von 57 auf 59 Prozent.“ (www.zdf.de/nachrichten/politik/mobilfunknetz-ausbau-technik-china-sicherheitsrisiko-100.html)?

Der Bundesregierung liegen keine über die Presseberichterstattung hinausgehenden Erkenntnisse vor.

32. Wenn der Bundesregierung gemäß Antwort zu Frage 2d auf Bundestagsdrucksache 20/6921 „Anhaltspunkte für eine mögliche voraussichtliche Beeinträchtigung der öffentlichen Ordnung oder Sicherheit der Bundesrepublik Deutschland durch Komponenten der Hersteller Huawei und ZTE, die als kritische Komponenten in öffentlichen 5G-Mobilfunknetzen eingesetzt werden, vor[liegen]“ – wann beabsichtigt die Bundesregierung, darauf zu reagieren?

Als Reaktion auf die vorliegenden Anhaltspunkte hat das BMI im März 2023 eine Prüfung der Bestandskomponenten der beiden Hersteller nach § 9b Absatz 4 BSIG eingeleitet. Zum weiteren zeitlichen Ablauf wird auf die Antwort zu Frage 15 verwiesen.

33. Aus welchen Gründen ist nach Kenntnis der Bundesregierung in der Kategorie „Radio Access Network“ (RAN) der „Liste der kritischen Funktionen“ nach § 109 Absatz 6 Satz 1 Nummer 2 TKG [Telekommunikationsgesetz] für öffentliche Telekommunikationsnetze und -dienste mit erhöhtem Gefährdungspotenzial“ (www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/ListekritischeFunktionen.pdf?__blob=publicationFile&v=3) lediglich das 5G-RAN-Management als kritische Funktionalität gemäß § 109 Absatz 6 Satz 1 Nummer 2 TKG eingestuft?

34. Welche weiteren Funktionalitäten werden nach Kenntnis der Bundesregierung durch das RAN erfüllt, und warum werden diese nicht als kritische Funktionen eingestuft?

35. Warum wird nach Kenntnis der Bundesregierung insbesondere das eNodeB-Netzelement nicht als kritische Funktion gemäß § 109 Absatz 6 Satz 1 Nummer 2 TKG in der Kategorie „Radio Access Network“ der „Liste der kritischen Funktionen nach § 109 Absatz 6 Satz 1 Nummer 2 TKG für öffentliche Telekommunikationsnetze und -dienste mit erhöhtem Gefährdungspotenzial“ (www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/ListekritischeFunktionen.html) eingestuft?

Die Fragen 33 bis 35 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Eine Bewertung und Einordnung von Funktionen als kritisch erfolgt gemäß § 167 Absatz 1 Satz 1 Nummer 2 des Telekommunikationsgesetzes (TKG) durch die Bundesnetzagentur im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit auf der Grundlage einer gemeinsamen Gefährdungsanalyse und des jeweils aktuellen Stands der Technik. Die Bewertung und Einordung können u. a. unter Rückgriff auf bereits vorliegende geeignete Untersuchungen erfolgen. Geeignete Untersuchungen in diesem Sinne sind nach Auffassung der Bundesnetzagentur, dem Bundesamt für Sicherheit in der Informationstechnik und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit die EU-Risikoanalyse (CG Publication 02/2019 – „Risk assessment of 5G networks“ vom 9. Oktober 2019) sowie die Implementierungsempfehlungen der EU-Toolbox (CG Publication 01/2020 – „Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures“ vom 29. Januar 2020).

Die Liste der kritischen Funktionen listet kritische Funktionen für öffentliche Mobilfunknetze der 5. Generation im Sinne der EU-Empfehlung 2019/534 vom 26. März 2019 auf. Nur bei diesen handelt es sich um öffentliche Telekommunikationsnetze mit erhöhtem Gefährdungspotenzial. Vor diesem Hintergrund wurde im Bereich des 5G Radio Access Network (RAN) das 5G RAN Management als kritische Funktion festgelegt.

Im Wesentlichen umfassen die Funktionen des 5G Radio Access Network das Access- und Mobilitäts-Management sowie die Bereitstellung des Nutzerdatentransfers und der Signalisierung für die Kommunikation mit dem 5G-Endgerät.

Die Liste der kritischen Funktionen wird aktuell im Rahmen der Überarbeitung des Katalogs von Sicherheitsanforderungen nach § 167 TKG überprüft.

Das eNodeB kommt in LTE-Netzen und nicht in 5G-Mobilfunknetzen zum Einsatz.

36. Wie oft haben Betreiber kritischer Infrastrukturen seit Inkrafttreten des IT-Sicherheitsgesetzes 2.0 im Mai 2021 den geplanten erstmaligen Einsatz einer kritischen Komponente gemäß § 2 Absatz 13 BSI-Gesetz dem Bundesministerium des Innern und für Heimat angezeigt (bitte für 2021, 2022 und das erste Halbjahr 2023 separat auflisten)?

    Wie oft wurde der Einsatz der kritischen Komponenten gemäß § 9b BSI-Gesetz untersagt, und wie oft waren Komponenten chinesischer Hersteller betroffen (bitte für 2021, 2022 und das erste Halbjahr 2023 separat auflisten)?

2021: Keine Anzeigen.

2022: Sechs Anzeigen, darunter zwei mit Komponenten chinesischer Hersteller.

2023: Bisher fünf Anzeigen, darunter eine mit Komponenten chinesischer Hersteller.

Zum Teil wurde im Rahmen einer Anzeige der geplante Einsatz mehrerer Komponenten angezeigt.

Untersagungen nach § 9b BSIG wurden bisher nicht ausgesprochen.

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