Deutscher Bundestag **Drucksache 21/4960**

21. Wahlperiode 24.03.2026

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Robin Jünger, Ruben Rupp, Alexander Arpaschi, weiterer Abgeordneter und der Fraktion der AfD
– Drucksache 21/4630 –

Maßnahmen der Bundesregierung zur Verhinderung eines Datenabflusses über Telekommunikationskomponenten des Herstellers Huawei

Vorbemerkung der Fragesteller

Die Sicherheit und Integrität öffentlicher Telekommunikationsnetze sind eine zentrale Voraussetzung für die Funktionsfähigkeit des Staates, für den Schutz personenbezogener Daten sowie für die Resilienz kritischer Infrastrukturen. Insbesondere Mobilfunknetze der fünften Generation (5G) sind aufgrund ihrer Rolle für Verwaltung, Wirtschaft, Sicherheitsbehörden und zunehmend auch für industrielle Steuerungsprozesse sicherheitspolitisch besonders bedeutsam. Der Gesetzgeber hat hierzu im Telekommunikationsgesetz (TKG) spezielle Vorgaben für Betreiber öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotenzial geschaffen; dazu gehört insbesondere die Pflicht, kritische Komponenten vor dem erstmaligen Einsatz zertifizieren zu lassen und für kritische Komponenten zusätzliche Anforderungen einschließlich Herstellererklärungen zu erfüllen (www.gesetze-im-internet.de/tkg_2021/__165.html).

Ergänzend konkretisieren technische Regelwerke des Bundesamtes für Sicherheit in der Informationstechnik (BSI) die Nachweiserbringung und Zertifizierungswege für kritische Komponenten in öffentlichen Kommunikationsnetzen, etwa die Technische Richtlinie TR-03163 „Sicherheit in TK-Infrastrukturen“ (www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03163/BSI-TR-03163.pdf?__blob=publicationFile&v=14).

Auch die Bundesnetzagentur veröffentlicht hierfür einschlägige Konkretisierungen, darunter eine „Liste der kritischen Funktionen“, die für die Einordnung von Komponenten und Risiken maßgeblich ist (www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/_DL/ListekritischeFunktionen.pdf?__blob=publicationFile&v=1), sowie den Katalog von Sicherheitsanforderungen nach dem TKG (www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/_DL/KatalogSicherheitsanforderungen.pdf?__blob=publicationFile&v=1).

Vor diesem regulatorischen Hintergrund wird seit Jahren öffentlich und parlamentarisch diskutiert, wie Risiken von Abhängigkeiten und möglichen Sicherheitslücken bei Ausrüstern in 5G-Netzen begrenzt werden können. Die Fraktion der AfD hat diese Debatte seit der 19. Wahlperiode mit Initiativen beglei-

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 24. März 2026 übermittelt.

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

tet und dabei auf die Notwendigkeit eines konsequenten Schutzes kritischer 5G-Infrastruktur hingewiesen. Beispielhaft wird auf den Antrag „Schutz der Kritischen 5G-Infrastruktur vor staatsnahen Netzwerkausrüstern“ auf Bundesdrucksache 19/7723 verwiesen sowie auf die Kleine Anfrage „Möglicher Ausschluss von Huawei beim Aufbau des deutschen 5G-Netzwerkes“ auf Bundestagsdrucksache 19/8650.

Zudem wurde in der gegenwärtigen Wahlperiode ein Antrag der Fraktion der Fraktion der AfD zur Zuständigkeitsausgestaltung des neuen Bundesministeriums für Digitales und Staatsmodernisierung (BMDS) auf Bundesdrucksache 21/3316 eingebracht, was in den Augen der Fragesteller die Relevanz einer klaren Verantwortungszuordnung auch für Fragen der Netz- und Datensicherheit unterstreicht.

Nach Angaben der Bundesregierung hat das Bundesministerium des Innern (BMI) Betreiber öffentlicher 5G-Mobilfunknetze bereits 2023 aufgefordert, alle in den jeweiligen Netzen im Einsatz befindlichen kritischen Komponenten der Hersteller Huawei und ZTE mitzuteilen und nach einer vorgegebenen Systematik aufzulisten (www.bundestag.de/presse/hib/kurzmeldungen-951412?utm_source=chatgpt.com). Im Jahr 2024 teilte das BMI ferner mit, dass in 5G-Kernnetzen bis spätestens Ende 2026 keine Komponenten von Huawei und ZTE mehr eingesetzt werden dürfen und weitere Schritte auch Zugangs- und Managementbereiche betreffen sollen (www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2024/07/5g.html).

Aus Sicht der Fragesteller ist dabei entscheidend, welche technischen, organisatorischen und rechtlichen Maßnahmen die Bundesregierung konkret ergriffen hat und ergreift, um einen Datenabfluss oder unautorisierte Zugriffe über Komponenten bestimmter Hersteller in öffentlichen Kommunikationsnetzen auszuschließen bzw. bestmöglich zu verhindern, wie die Umsetzung überwacht wird und welche Rolle hierbei das BMDS spielt.

1. Auf welche konkreten Rechtsgrundlagen stützt die Bundesregierung die im Juli 2024 vom BMI kommunizierten Maßnahmen, wonach in 5G-Kernnetzen bis spätestens Ende 2026 keine Komponenten von Huawei und ZTE mehr eingesetzt werden dürfen, und in welcher Rechtsform wurden diese Maßnahmen gegenüber den Netzbetreibern verbindlich gemacht?

Die Bundesregierung hat für die Bundesrepublik Deutschland öffentlich-rechtliche Verträge jeweils mit den deutschen Mobilfunkanbietern Telekom, Vodafone und Telefónica geschlossen. Mit den Verträgen wurden die auf Basis von § 9b Absatz 4 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik in seiner alten Fassung (BSIG a. F.) gegenüber den vorbezeichneten Unternehmen jeweils geführten Verwaltungsverfahren abgeschlossen.

2. Welche Rolle und Zuständigkeit kommen dem Bundesministerium für Digitales und Staatsmodernisierung (BMDS) bei der strategischen Steuerung, Koordinierung und Kontrolle dieser Maßnahmen zu, und welche weiteren Bundesministerien sind in welcher Form beteiligt?

Nach § 9b Absatz 4 S. 1 BSIG a. F. konnte das Bundesministerium des Innern (BMI) den weiteren Einsatz einer kritischen Komponente gegenüber dem Betreiber der Kritischen Infrastruktur im Einvernehmen mit dem Bundesministerium für Digitales und Verkehr (BMDV) sowie dem Auswärtigen Amt untersagen oder Anordnungen erlassen, wenn der weitere Einsatz die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland voraussichtlich beeinträchtigt, insbesondere wenn der Hersteller der kritischen Komponente nicht vertrauenswürdig ist.

Gem. § 41 Absatz 1 BSIG kann das BMI gegenüber dem Betreiber kritischer Anlagen den Einsatz von kritischen Komponenten eines Herstellers im Benehmen mit dem Bundesministerium für Wirtschaft und Energie im Sektor Energie, dem Bundesministerium für Wirtschaft und Energie sowie dem Bundesministerium für Forschung, Technologie und Raumfahrt im Sektor Weltraum, dem Bundesministerium für Digitales und Staatsmodernisierung in den Sektoren Informationstechnik und Telekommunikation, dem Bundesministerium für Verkehr in den Sektoren Transport und Verkehr, dem Bundesministerium für Gesundheit im Sektor Gesundheit, dem Bundesministerium für Ernährung und Landwirtschaft im Sektor Ernährung, dem Bundesministerium der Finanzen im Sektor Finanzwesen, dem Bundesministerium für Arbeit und Soziales in den Sektoren Sozialversicherungsträger sowie Grundsicherung für Arbeitsuchende und dem Bundesministerium für Umwelt, Klimaschutz, Naturschutz und nukleare Sicherheit in den Sektoren Wasser sowie Siedlungsabfallentsorgung sowie dem Auswärtigen Amt untersagen oder Anordnungen dazu erlassen, wenn der Einsatz die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland voraussichtlich beeinträchtigt.

Im Übrigen beteiligt das BMI etwaig betroffene Ressorts grundsätzlich nach der Gemeinsamen Geschäftsordnung der Bundesministerien (GGO).

3. Welche Arbeitsdefinition von „Komponenten“ und „kritischen Komponenten“ legt die Bundesregierung in diesem Zusammenhang zugrunde, und wie grenzt sie diese Definitionen gegenüber den Begrifflichkeiten des TKG, insbesondere § 165 TKG, ab?

Der Tatbestand des § 9b BSIG a. F. war ausschließlich auf kritische Komponenten i. S. d. § 2 Absatz 13 BSIG a. F. anwendbar. Für die Bestimmung einer Komponente als kritisch war nach § 2 Absatz 13 Nr. 3b BSIG i. V. m. § 167 Absatz 1 Nr. 2 Telekommunikationsgesetz (TKG) die im Amtsblatt Nr. 16/2021 der Bundesnetzagentur (BNetzA) veröffentlichte Liste kritischer Funktionen (LkrF) nach § 109 Absatz 6 Satz 1 Nr. 2 TKG (mittlerweile a. F.) für öffentliche Telekommunikationsnetze und -dienste mit erhöhtem Gefährdungspotenzial maßgeblich. Auch § 41 BSIG ist ausschließlich auf kritische Komponenten anwendbar. Gemäß § 2 Nr. 23 BSIG sind kritische Komponenten, IKT-Produkte, die in einer Rechtsverordnung aufgrund von § 56 Absatz 7 und 8 als kritische Komponenten bestimmt werden. Eine derartige Rechtsverordnung existiert bisher nicht. Gem. § 167 Absatz 2 S. 2 TKG ist eine von der BNetzA auf der Grundlage von § 167 Absatz 1 Satz 1 Nr. 2 TKG erlassene Allgemeinverfügung mit dem Inkrafttreten einer Rechtsverordnung nach § 56 Absatz 7 des BSIG für den Sektor Informationstechnik und Telekommunikation aufzuheben.

4. Welche konkreten Netzbereiche sind von den bis 2026 bzw. den weitergehenden Maßnahmen bis 2029 erfasst, und welche Netzbereiche sind nach aktuellem Stand ausdrücklich nicht erfasst (bitte getrennt nach 5G-Kernnetz, 5G-Zugangsnetz bzw. Radio Access Network, Transport- bzw. Backhaul, Netzmanagement- bzw. Orchestrierungs- und Betriebsunterstützungssystemen angeben)?

Die Verträge verpflichten die vorbezeichneten Mobilfunkanbieter jeweils, bis spätestens Ende 2026 keine kritischen Komponenten der Hersteller Huawei und ZTE mehr in ihren 5G-Kernnetzen einzusetzen. Außerdem sind die Mobilfunkbetreiber verpflichtet, bis Ende 2029 die kritischen Funktionen der 5G-Netzwerkmanagementsysteme der Hersteller Huawei und ZTE in ihren Zugangs- und Transportnetzen des 5G-Mobilfunknetzes durch technische Lösungen anderer Hersteller zu ersetzen. Hinsichtlich der Definition der Netzbereiche haben

sich das BMI und die Mobilfunknetzbetreiber an den für 5G-Mobilfunknetze relevanten Standards der 3rd Generation Partnership Project (3GPP) orientiert.

5. Welche Betreiber öffentlicher 5G-Mobilfunknetze wurden nach Kenntnis der Bundesregierung aufgrund der Aufforderung vom 6. März 2023 zur Meldung kritischer Komponenten zur Übermittlung welcher Daten verpflichtet, und haben alle Betreiber vollständig und fristgerecht geantwortet (bitte Betreiber nennen, soweit zulässig, andernfalls nachvollziehbar anonymisiert darstellen)?

Das BMI hatte nach § 9b Absatz 4 BSIG a. F. in drei individuellen Verwaltungsverfahren gegenüber Telekom, Vodafone und Telefónica jeweils geprüft, ob und inwieweit die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland durch den Einsatz bestimmter kritischer Komponenten der chinesischen Hersteller Huawei und ZTE in den öffentlichen 5G-Mobilfunknetzen voraussichtlich beeinträchtigt wird. Die fristgerecht gemachten Angaben der vorbezeichneten Mobilfunkanbieter ermöglichten den Abschluss öffentlich-rechtlicher Verträge.

6. Welche „kritischen Funktionen“ im Sinne der Veröffentlichungen der Bundesnetzagentur waren nach Kenntnis der Bundesregierung zum Zeitpunkt der Datenerhebung bzw. der Entscheidung in deutschen 5G-Netzen durch Komponenten von Huawei abgedeckt (bitte nach Funktionskategorie aufschlüsseln)?

Auf die Beantwortung von Frage 4 wird verwiesen. Im Kernnetz eingesetzte Komponenten gelten insbesondere dann als kritische Komponenten, wenn sie kritische Funktionen der Kategorie a) der LkrF realisieren. Im Kontext Management und Network Orchestration eingesetzte Komponenten gelten insbesondere dann als kritische Komponenten, wenn sie kritische Funktionen der Kategorien b) und c) der LkrF realisieren. Im Zugangs- und Transportnetz eingesetzte Komponenten gelten insbesondere dann als kritisch, wenn sie kritische Funktionen der Kategorien d) bis f) der LkrF realisieren.

7. Welche Zertifizierungs- und Nachweispflichten nach § 165 TKG sowie nach der BSI-TR-03163 wurden nach Kenntnis der Bundesregierung für Huawei-Komponenten in öffentlichen 5G-Netzen bereits erfüllt, und welche noch nicht (bitte jeweils nach Funktionsklasse bzw. Komponentenkategorie aufschlüsseln)?

Gem. § 165 Absatz 4 TKG dürfen kritische Komponenten im Sinne von § 2 Nummer 23 des BSIG von einem Betreiber öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotenzial nur eingesetzt werden, wenn sie vor dem erstmaligen Einsatz von einer anerkannten Zertifizierungsstelle überprüft und zertifiziert wurden. Gem. §§ 165 Absatz 4, 167 Absatz 1 Satz 1 Nr. 1 und Absatz 2 TKG i. V. m. § 35 S. 2 Verwaltungsverfahrensgesetz (VwVfG) hat die BNetzA für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen im Einvernehmen mit dem BSI und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) insoweit in der „Allgemeinverfügung zur Festlegung der Umsetzungsfristen für den Einsatz kritischer Komponenten“ Umsetzungsfristen für Zertifizierungsanforderungen beim Einsatz kritischer Komponenten präzisiert (www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/_DL/Allgemeinverf%C3 ProzentBCgungFestlegungUmsetzungsfristenEinsatzKritischer Komponenten.pdf?__blob=publicationFile&v=1). Die Allgemeinverfügung

sieht als Stichtag für das Entstehen der Zertifizierungspflicht spätestens den letzten Tag des 24. Monats, nachdem die Zertifizierung des Produktes, zu dem die jeweilige kritische Komponente gehört, nach TR-03163 des BSI erstmals möglich ist, frühestens aber den 1. Januar 2026, vor. Die Erfüllung einer insoweit etwaig bestehenden Zertifizierungspflicht nach § 165 Absatz 4 TKG ist Gegenstand der turnusmäßig alle zwei Jahre stattfindenden Überprüfung der Betreiber öffentlicher Telekommunikationsnetze nach § 165 Absatz 9 S. 2 TKG. Bei den Ergebnissen dieser Überprüfung handelt es sich um Betriebs- und Geschäftsgeheimnisse der Netzbetreiber.

8. Welche Prüf- und Kontrollmechanismen (z. B. Vor-Ort-Prüfungen, Dokumentenprüfungen, Penetrationstests, Code-Review-Ansätze, Zertifizierungsnachweise, Auditpflichten) setzt die Bundesregierung über das BMI, das BSI und/oder weitere Bundesbehörden ein, um einen Abfluss von Daten oder unautorisierte Zugriffe über Netzkomponenten auszuschließen bzw. bestmöglich zu verhindern (bitte Zuständigkeiten und Prüffrequenzen benennen)?

Für die Cybersicherheit des jeweiligen Mobilfunknetzes ist der Betreiber des Netzes verantwortlich. Für das Erbringen von Telekommunikationsdienstleistungen hat ein Netzbetreiber dabei technische und organisatorische Schutzmaßnahmen zu treffen, vgl. insbesondere § 166 TKG. Gem. § 165 Absatz 9 TKG kann die BNetzA anordnen, dass sich die Betreiber öffentlicher Telekommunikationsnetze oder die Anbieter öffentlich zugänglicher Telekommunikationsdienste einer Überprüfung durch eine qualifizierte unabhängige Stelle oder eine zuständige nationale Behörde unterziehen, in der festgestellt wird, ob die Anforderungen nach § 165 Absatz 1-7 TKG erfüllt sind. Unbeschadet von Satz 1 haben sich Betreiber öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotenzial alle zwei Jahre einer Überprüfung durch eine qualifizierte unabhängige Stelle oder eine zuständige nationale Behörde zu unterziehen, in der festgestellt wird, ob die Anforderungen nach den § 165 Absatz 1-7 TKG erfüllt sind. Die BNetzA legt den Zeitpunkt der erstmaligen Überprüfung fest. Der nach § 165 Absatz 9 S. 1 und 2 TKG Verpflichtete hat eine Kopie des Überprüfungsberichts unverzüglich an die BNetzA und an das BSI, sofern dieses die Überprüfung nicht vorgenommen hat, zu übermitteln. Die Bewertung der Überprüfung sowie eine diesbezügliche Feststellung von Sicherheitsmängeln im Sicherheitskonzept nach § 166 TKG erfolgt durch die BNetzA im Einvernehmen mit dem BSI. Die Prüfung des BSI besteht u. a. aus einer Dokumentenprüfung, Interviews, einem Attack-Surface-Check und einer Vor-Ort-Überprüfung.

9. Welche Erkenntnisse liegen der Bundesregierung zu sicherheitsrelevanten Vorfällen, Schwachstellenmeldungen oder sonstigen Ereignissen mit Bezug zu Huawei-Komponenten in deutschen öffentlichen Mobilfunknetzen vor, die eine potenzielle Vertraulichkeitsverletzung (Datenabfluss) oder Integritätsverletzung nahelegen (bitte Anzahl, Zeitraum, Klassifizierung und zuständige Meldestellen angeben, soweit möglich)?

Die Frage zu sicherheitsrelevanten Vorfällen, Schwachstellenmeldungen oder sonstigen Ereignissen mit Bezug zu Huawei-Komponenten in deutschen öffentlichen Mobilfunknetzen berührt hinsichtlich der Aufklärungsfähigkeiten der Nachrichtendienste des Bundes (NdB) solche Informationen, die in besonders hohem Maße das Staatswohl berühren und daher selbst in eingestufter Form nicht beantwortet werden können. Das verfassungsrechtlich verbürgte Frage- und Informationsrecht des Deutschen Bundestages gegenüber der Bundesregierung wird durch gleichfalls Verfassungsrecht genießende schutzwürdige Inte-

ressen wie das Staatswohl begrenzt. Eine Offenlegung der angefragten Informationen birgt die Gefahr, dass Einzelheiten bekannt würden, die in Zusammenhang mit der Arbeitsweise, Kenntnisstand und Methodik der NdBs stehen.

Hierzu zählen auch Informationen über den Umfang sicherheitsrelevanter Vorfälle sowie Schwachstellenmeldungen mit dem Bezug zu Huawei-Komponenten in deutschen öffentlichen Mobilfunknetzen. So könnten fremde Nachrichtendienste durch die Kenntnis von Schwachstellen Rückschlüsse auf Quantität und Qualität von Aufklärungsfähigkeiten der NdBs ziehen. Dadurch könnten bereits ergriffene oder geplante Aufklärungsmaßnahmen erschwert oder gar vereitelt werden. Eine Bekanntgabe von Informationen zur Leistungsfähigkeit der NdBs und damit einhergehend die Kenntnisnahme durch Unbefugte würde damit erhebliche nachteilige Auswirkungen auf die Arbeit der NdBs und damit für die Sicherheit der Bundesrepublik Deutschland haben. Eine VS-Einstufung und Hinterlegung der angefragten Informationen in der Geheimschutzstelle des Deutschen Bundestages würde ihrer erheblichen Brisanz im Hinblick auf die Bedeutung für die Aufgabenerfüllung der NdBs nicht ausreichend Rechnung tragen. Die Fähigkeiten der NdBs sind für das Staatswohl von großer Bedeutung und zugleich in hohem Maße geheimhaltungsbedürftig. Die angefragten Inhalte beschreiben die Fähigkeiten und Arbeitsweise der NdBs so detailliert, dass eine Bekanntgabe auch gegenüber nur einem begrenzten Empfängerkreis ihrem Schutzbedürfnis nicht Rechnung tragen kann. Schon bei dem Bekanntwerden der schutzbedürftigen Informationen wäre kein Einsatz durch andere Instrumente der Informationsgewinnung mehr möglich. Aus dem Vorgesagten ergibt sich, dass die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, aufgrund derer das Staatswohl gegenüber dem parlamentarischen Informationsrecht wesentlich überwiegt. Insofern muss ausnahmsweise das Fragerecht der Abgeordneten gegenüber dem Geheimhaltungsinteresse der Bundesregierung zurückstehen.

10. Welche Vorgaben macht die Bundesregierung den Netzbetreibern hinsichtlich der Behandlung von Software- bzw. Firmware-Updates für sicherheitsrelevante Netzfunktionen, und inwieweit werden Updates für als kritisch eingestufte Komponenten vor Einspielung geprüft oder zertifiziert (bitte die einschlägigen Regelwerke, Zuständigkeiten und Prozesse benennen)?

§ 9b Absatz 1 BSIG a. F. sah vor, dass der Einsatz neuer kritischer Komponenten dem BMI vorher („ex-ante“) angezeigt werden muss. Hierunter fielen im Einzelfall auch Software-Updates. § 41 BSIG n.F. enthält keine derartige Anzeigeverpflichtung mehr. Der Wortlaut des § 165 Absatz 4 TKG enthält keine Ausführungen zu Software-Updates. Ob und inwieweit § 165 Absatz 4 TKG auch auf ein individuelles Software-Update anwendbar ist, bedarf daher einer individuellen Entscheidung, bei der insbesondere das jeweilige Zertifizierungsprogramm berücksichtigt werden kann.

11. Welche Maßnahmen hat die Bundesregierung ggf. ergriffen, um sicherzustellen, dass in Bundesnetzen oder bundesnahen Netzinfrastrukturen (z. B. Netze von Bundesbehörden oder bundeseigenen Unternehmen) kein Einsatz von Huawei-Komponenten erfolgt, soweit dies sicherheitsrelevant ist, und welche Bestandsaufnahmen liegen hierzu vor (bitte nach Kenntnisstand der Bundesregierung aufschlüsseln)?

Innerhalb der Bundesregierung ist jedes Ressorts selbst für die Cyber- und Informationssicherheit der jeweils eingesetzten IT-Infrastruktur verantwortlich. Dazu gehören u. a. auch Risikoanalysen im Hinblick auf das Risiko beim Ein-

satz von Komponenten nicht vertrauenswürdiger Hersteller. Die Ressorts berücksichtigen den Schutzbedarf der jeweiligen IT-Systeme und Netze im Hinblick auf das individuelle Risiko bei dem Ergreifen hinreichender IT-Sicherheitsmaßnahmen. Das BMI sensibilisiert die Ressorts fortlaufend im Hinblick auf die Cyber- und Informationssicherheit eingesetzter IT-Produkte, u. a. nach Abschluss der gegenüber Telekom, Vodafone und Telefónica auf Basis von § 9b Absatz 4 BSIG a. F. geführten Verwaltungsverfahren.

12. Welche Auswirkungen auf Kosten, Netzverfügbarkeit und Zeitpläne erwartet die Bundesregierung durch den Austausch der betroffenen Komponenten, und welche Vorkehrungen hat sie getroffen, um zu verhindern, dass daraus mittelbar finanzielle Belastungen des Bundes entstehen (bitte nach Kenntnis der Bundesregierung etwaige Szenarien, Vorsorgeinstrumente und Haushaltsvorsorge darstellen)?

Zu Auswirkungen bei den Mobilfunkprovidern und eventuell daraus resultierenden finanziellen Belastungen des Bundes liegen der Bundesregierung keine Erkenntnisse vor.

13. Inwieweit bezieht die Bundesregierung bei ihrer Risikobewertung und Maßnahmenplanung die EU-Vorgaben bzw. Empfehlungen zur 5G-Sicherheit (EU-Toolbox) ein?

Im Rahmen der nach § 9b BSIG a. F. durchgeführten Verfahren sind in der EU-5G-Toolbox enthaltenen Empfehlungen in die Bewertung des BMI eingeflossen. Im Übrigen hat die Bundesregierung mit der Schaffung von § 9b a. F. und § 41 BSIG n.F. sowie der LkRf die Empfehlungen der 5G-Toolbox in nationales Recht umgesetzt.

14. Welche Maßnahmen ergreift die Bundesregierung, um auch bei Netzen oder IT-Infrastrukturen im Zuständigkeitsbereich der Länder und Kommunen, soweit diese an bundesrelevante Kommunikations- oder Verwaltungsprozesse angebunden sind, Risiken durch den Einsatz potenziell kritischer Hersteller zu minimieren, und welche Erkenntnisse liegen ihr hierzu nach Kenntnis der Bundesregierung vor?

Die IT-Sicherheit von IT-Infrastrukturen der Länder und Kommunen liegt nicht im Zuständigkeitsbereich der Bundesregierung und/oder des BMI, sondern der Länder und Kommunen. Das BMI hat die Länder über den Abschluss und Ergebnisse der nach § 9b Absatz 4 BSIG a. F. geführten Verwaltungsverfahren bei der Herbstkonferenz der Innenminister im Jahr 2024 informiert.

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