Deutscher Bundestag **Drucksache 20/6271**

20. Wahlperiode 31.03.2023

Antwort

der Bundesregierung

auf die Kleine Anfrage der Fraktion der CDU/CSU
– Drucksache 20/6067 –

Zertifizierung eines Produktes für 5G-Mobilfunkausrüstung des chinesischen Telekommunikationsunternehmens Zhong Xing Telecommunication Equipment

Vorbemerkung der Fragesteller

Am 7. Februar 2023 vermeldete das chinesische Unternehmen Zhong Xing Telecommunication Equipment (ZTE), dass ihr Produkt 5G NR gNodeB durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifiziert wurde (www.zte.com.cn/global/about/news/20230207e2.html; cybersecurityasean.com/news-press-releases/zte%E2%80%99s-5g-nr-received-bsi-security-certification). Das BSI bietet seit dem 1. Juli 2022 eine Anerkennung als NESAS-Prüfstelle an. NESAS CCS-GI ist ein nationales Zertifizierungsschema für 5G-Mobilfunkausrüstung und ermöglicht es Herstellern, die Sicherheitsaussage ihres Produktes durch ein unabhängiges Zertifikat bestätigen zu lassen (www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Anerkennung-von-Stellen-und-Zertifizierung-IT-Sicherheitsdienstleister/NESAS/nesas_node.html). Bei dem zertifizierten Produkt handelt es sich um einen Verbindungspunkt in einem 5G-Funkzugangsnetz, das wiederum für die drahtlosen Verbindungen zu den Endgeräten im 5G-Standard zuständig ist und den Zugang zum Kernnetz des Telekommunikationssystems ermöglicht (www.bsi.bund.de/SharedDocs/Zertifikate_NESAS/NESAS-0002-2022.html?nn=1078996; www.ip-insider.de/was-ist-ein-ran-radio-access-network-a-16d3c3434b22c6e39bc56d482b897724/; www.itwissen.info/next-generation-core-5G-NGC.html).

In den USA erklärte die dortige Zulassungsbehörde für Kommunikationsgeräte Federal Communications Commission (FCC) am 30. Juni 2020 die chinesischen Telekommunikationsunternehmen ZTE und Huawei zu einem nationalen Sicherheitsrisiko für die Vereinigten Staaten. Das bedeutete gleichzeitig, dass die Behörde keine Subventionen an Telekommunikationsanbieter mehr für den Kauf, Erhalt, die Wartung, Verbesserung, Modifizierung oder zur anderweitigen Unterstützung von Geräten oder Dienstleistungen ausgegeben werden, die von Huawei oder ZTE hergestellt oder bereitgestellt werden. Der damalige Vorsitzende der FCC, Ajit Pai, führte zu dieser Entscheidung zudem aus, dass dem FCC-Präsidium eine gewichtige Beweiskraft dafür vorläge, dass die beiden Firmen Huawei und ZTE eng mit der Kommunistischen Partei Chinas (KPCh) und dem chinesischen Militär verbunden sind. Zudem unterliegen sie dem FCC zufolge dem chinesischen Gesetz. Damit seien sie zur Zusammenarbeit mit den chinesischen Geheimdiensten verpflichtet. Die damalige Entscheidung des FCC wurde auch damit begründet, dass es der KPCh nicht

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern und für Heimat vom 30. März 2023 übermittelt.

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

ermöglicht werden sollte, Schwachstellen in Netzwerken auszunutzen und kritische Kommunikationsinfrastruktur zu kompromittieren (docs.fcc.gov/public/attachments/DOC-365255A1.pdf).

Auf Anordnung der FCC am 25. November 2022 haben die USA ein Verbot von Verkauf und Import von Kommunikationsgeräten und Überwachungsausrüstung der chinesischen Technologiekonzerne Huawei und ZTE erlassen (www.dw.com/de/usa-verbannen-huawei-und-zte/a-63895829). Gleichzeitig ließ die Behörde die Möglichkeit offen, frühere Zulassungen rückgängig zu machen (www.spiegel.de/wirtschaft/usa-importverbot-fuer-zte-und-huawei-ausruestung-a-08bb91eb-72d6-40b8-be7f-73c0ecd4a1ff).

Neben den USA haben auch andere Staaten, wie Großbritannien, Kanada, Frankreich oder Schweden, die chinesischen Hersteller Huawei und ZTE vom Aufbau ihrer 5G-Netze ausgeschlossen (www.tagesschau.de/ausland/amerika/kanada-huawei-101.html; www.handelsblatt.com/technik/it-internet/mobilfunk-schweden-schliesst-huawei-und-zte-vom-5g-ausbau-aus/26290668.html).

Darüber hinaus hatten die USA im April 2018 Strafmaßnahmen gegen ZTE verhängt, weil das chinesische Unternehmen gegen Iran- und Nordkorea-Sanktionen verstoßen haben soll. US-Zulieferern wie Qualcomm und Intel wurde daraufhin für sieben Jahre verboten, Bauteile oder Software an ZTE zu verkaufen (www.handelsblatt.com/unternehmen/it-medien/sanktionsverstoesse-usa-einigen-sich-mit-chinesischem-tech-konzern-zte-auf-eine-milliarde-dollar-strafe/22657646.html).

In Deutschland wurde im Sommer 2016 ein Spionageangriff gegen die Deutsche Telekom durch das chinesische Unternehmen ZTE bekannt. Konkret sollen Manager des chinesischen Konzerns ZTE einen Telekom-Mitarbeiter bestochen haben, um geheime Infos über das gemeinsam mit Orange betriebene Einkaufsunternehmen Buyin zu erhalten. In diesem Zusammenhang wurden auch die Büroräumlichkeiten von ZTE in Bonn durchsucht (rp-online.de/wirtschaft/unternehmen/zte-unter-verdacht-spionageangriff-gegen-telekom_aid-18166383).

1. Ist es zutreffend, dass das Produkt 5G NR gNodeB des Unternehmens ZTE durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifiziert wurde?

   Wenn ja,

Ja.

   a) aus welchen Gründen hat die dem Bundesministerium des Innern und für Heimat (BMI) nachgeordnete Behörde, BSI, die in Rede stehende Komponente 5G NR gNodeB von ZTE sicherheitszertifiziert,

Die Zertifizierung wurde erteilt, da die rechtlichen und technischen Voraussetzungen dafür erfüllt waren.

   b) gab es bezüglich des Vorgangs Zertifizierung des Produkts 5G NR gNodeB von ZTE Kontakt zwischen dem BSI und der Bundesnetzagentur (bitte Kontakte auflisten),

Nein.

   c) dürfen aufgrund der BSI-Sicherheitszertifizierung in der Folge alle Mobilfunknetzbetreiber und öffentlichen Stellen in der Bundesrepublik Deutschland die entsprechenden 5G-Produkte von ZTE nutzen,

Nach § 165 Absatz 4 des Telekommunikationsgesetzes (TKG) dürfen Betreiber öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotenzial kri-

tische Komponenten im Sinne von § 2 Absatz 13 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) nur dann einsetzen, wenn sie vor dem erstmaligen Einsatz von einer anerkannten Zertifizierungsstelle überprüft und zertifiziert wurden. Die Zertifizierung der kritischen Komponenten hat auf der Grundlage der Technischen Richtlinie TR-03163 des BSI zu erfolgen. Sollte zum Zeitpunkt des erstmaligen Einsatzes einer kritischen Komponente keine Möglichkeiten zur Zertifizierung verfügbar sein, so können die Komponenten ohne Zertifikat eingesetzt werden. Für die Möglichkeit der Zertifizierung bedarf es sowohl der Veröffentlichung der TR-03163, wie auch der Verfügbarkeit produktbezogener Anforderungsdokumente.

Die Veröffentlichung der TR-03163 und der Verweis auf die entsprechenden Anforderungsdokumente mit Benennung des für den Produkttyp geltenden Stichtages erfolgt auf der Webseite des BSI (www.bsi.bund.de). Diese Übergangsregelung entfällt zum 1. Januar 2026. Bis dahin können grundsätzlich auch kritische Komponenten, die keine Zertifizierung aufweisen, in den öffentlichen 5G-Telekommunikationsnetzen verbaut werden. Ein Verbot gibt es nur dann, wenn das BMI den Einsatz nach § 9b BSIG untersagt hat. Dies ist wiederum von der Zertifizierung unabhängig.

d) welche Auswirkungen hat die benannte Sicherheitszertifizierung auf den Marktzugang ZTEs mit seinen 5G-Produkten in der Bundesrepublik Deutschland?

Wenn nein, aus welchen Gründen wird nach Kenntnis der Bundesregierung berichtet, dass ZTE die genannte Sicherheitszertifizierung erhalten hat (cybersecurityasean.com/news-press-releases/zte%E2%80%99s-5g-nr-received-bsi-security-certification)?

Die Zertifizierung hat keine Auswirkungen auf den Marktzugang in Deutschland. Die Gründe für die Presseberichterstattung Dritter sind der Bundesregierung nicht bekannt.

2. Hat die Bundesregierung Kenntnis von einer Verbindung des Unternehmens ZTE zur KPCh, und wenn ja, wie stellt sich diese Verbindung dar?

5. Hat die Bundesregierung Kenntnis von einer Verbindung des Unternehmens Huawei zur KPCh, und wenn ja, wie stellt sich diese Verbindung dar?

Die Fragen 2 und 5 werden gemeinsam beantwortet.

Ja, beide Unternehmen stehen auf verschiedenen Ebenen unter Kontrolle der KPCh (Aufsichtsbehörden, Parteigremien, Parteizellen in den Firmen etc.).

Gemäß Kapitel V der Statuten der KPCh sind in jedem Unternehmen Parteizellen zu etablieren, die in die Hierarchie der Parteiorganisation eingebettet sind. Gemäß Artikel 19 des chinesischen Gesellschaftsrechtsgesetzes ist die KPCh berechtigt, Parteizellen zur Ausübung von Parteiaktivitäten in Unternehmen einzurichten.

Hierdurch verfügt die KPCh rechtlich und tatsächlich über die Möglichkeit, durch Einwirkung auf die Geschäftsführung und Unternehmenspolitik die Erfüllung politischer Zielvorgaben effektiv sicherzustellen.

Huawei wie ZTE unterhalten nach Kenntnis der Bundesregierung einen solchen KPCh-Parteiarm innerhalb des Unternehmens. Huawei-Gründer Ren Zhengfei sowie der Chair of the Board of Directors, Lian Hua, sind Mitglieder der KPCh.

3. Hat die Bundesregierung Kenntnis von einer Verbindung des Unternehmens ZTE mit dem chinesischen Militär, und wenn ja, wie stellt sich diese Verbindung dar?

6. Hat die Bundesregierung Kenntnis von einer Verbindung des Unternehmens Huawei mit dem chinesischen Militär, und wenn ja, wie stellt sich diese Verbindung dar?

Die Fragen 3 und 6 werden gemeinsam beantwortet.

Die sogenannte Strategie zur Entwicklung der zivil-militärischen Integration ist laut Präambel der Statuten der KPCh eines der zentralen Ziele im Prozess der Modernisierung der Volksrepublik China. Sie zielt auf den Transfer zivilen Wissens in den militärischen Bereich.

4. Unterliegt die chinesische Firma ZTE nach Kenntnis der Bundesregierung dem chinesischen Gesetz, und wenn ja, wäre die chinesische Firma ZTE nach Kenntnis der Bundesregierung damit zur Zusammenarbeit mit chinesischen Geheimdiensten verpflichtet?

7. Unterliegt die chinesische Firma Huawei nach Kenntnis der Bundesregierung dem chinesischen Gesetz, und wenn ja, wäre die chinesische Firma Huawei nach Kenntnis der Bundesregierung damit zur Zusammenarbeit mit den chinesischen Geheimdiensten verpflichtet?

Die Fragen 4 und 7 werden gemeinsam beantwortet.

Sämtliche in der Volksrepublik China ansässige Unternehmen unterliegen dem dortigen Recht. Nach Artikel 7 des Geheimdienstgesetzes der Volksrepublik China sollen alle Organisationen und Bürger der Volksrepublik China die Geheimdienstbehörden entsprechend dem Gesetz unterstützen und mit den Behörden kooperieren.

Der Artikel 14 des Geheimdienstgesetzes der Volksrepublik China räumt den genannten Behörden die Befugnis ein, bei ihrer Arbeit Organe, Organisationen und Bürger um Unterstützung, Hilfe und Kooperation zu ersuchen.

8. Sind der Bundesregierung Sicherheitsvorfälle in Deutschland mit Bezug zu Telekommunikationsnetzwerken und kritischer Telekommunikationsinfrastruktur im Zusammenhang mit Komponenten chinesischer Unternehmen bekannt (bitte einzeln auflisten)?

Nein.

9. Erwägt die Bundesregierung, ein Verbot von Verkauf und Import von Kommunikationsgeräten und Überwachungsausrüstung der chinesischen Technologiekonzerne Huawei und ZTE zu erlassen?

Nein, für ein solches Verbot ist aktuell keine Rechtsgrundlage erkennbar. Das Außenwirtschaftsrecht enthält sehr hohe Hürden für den Erlass nationaler Import- oder Exportverbote. Nur unter engen Voraussetzungen und im Einklang mit europa- und völkerrechtlichen Vorgaben sind Einschränkungen des Warenverkehrs zulässig.

10. Hält es die Bundesregierung weiterhin für unbedenklich, den Einsatz kritischer Komponenten aus chinesischer Herstellung wie der Firma ZTE in 5G-Mobilfunknetzen zuzulassen, obwohl Staaten wie die USA, Großbritannien, Kanada, Frankreich oder Schweden die Hersteller Huawei und ZTE vom Aufbau ihrer 5G-Mobilfunknetze ausgeschlossen haben?

Eine gesetzliche Grundlage für den Ausschluss bestimmter Komponenten aus öffentlichen 5G-Telekommunikationsnetzen aufgrund fehlender Vertrauenswürdigkeit des jeweiligen Herstellers besteht derzeit nur in Form des § 9b BSIG. Der deutsche Gesetzgeber hat sich dabei für einen technologie- und herstellerneutralen Ansatz entschieden. Einen pauschalen Ausschluss einzelner Produkte oder Hersteller aus 5G-Netzen sieht § 9b BSIG – mit Ausnahme schwerwiegender Fälle nach Absatz 7 – nicht vor.

Dementsprechend wird der Einsatz jeder Komponente im Einzelfall durch das BMI unter Berücksichtigung aller maßgeblichen Umstände und unter Beteiligung der betroffenen Ressorts darauf geprüft, ob der Einsatz die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland voraussichtlich beeinträchtigt. Hierbei wird auch der staatliche Einfluss auf den Hersteller berücksichtigt.

11. Sind der Bundesregierung über den in der Vorbemerkung der Fragesteller genannten Vorfall bei der Deutschen Telekom hinaus weitere Spionageangriffe oder Spionageversuche chinesischer Telekommunikationsunternehmen in Deutschland bekannt (bitte einzeln auflisten)?

12. Sind der Bundesregierung über den in der Vorbemerkung der Fragesteller genannten Vorfall bei der Deutschen Telekom hinaus weitere Spionageangriffe oder Spionageversuche chinesischer Telekommunikationsunternehmen in den EU-Staaten bekannt (bitte einzeln auflisten)?

13. Sind der Bundesregierung über den in der Vorbemerkung der Fragesteller genannten Vorfall bei der Deutschen Telekom hinaus weitere Spionageangriffe oder Spionageversuche chinesischer Telekommunikationsunternehmen in den NATO-Staaten bekannt (bitte einzeln auflisten)?

Die Fragen 11 bis 13 werden gemeinsam beantwortet.

Es sind nachstehende Fälle bekannt, in denen chinesische Telekommunikationsunternehmen oder deren Beschäftigten Konkurrenzausspähung bzw. Spionage vorgeworfen wird. Die US-Justiz warf Huawei im Jahr 2019 vor, Konkurrenzausspähung gegen T-Mobile betrieben zu haben. In Polen wurde im Jahr 2019 ein Mitarbeiter von Huawei festgenommen, der im Auftrag eines chinesischen Nachrichtendienstes Spionage betrieben haben soll.

14. Sind der Bundesregierung Verstöße von ZTE Deutschland gegen die bestehenden Russland-Sanktionen bekannt (bitte Verstöße auflisten)?

    Hat die Bundesregierung prüfen lassen, ob ZTE Deutschland gegen die bestehenden Russland-Sanktionen verstößt?

Der Bundesregierung sind keine Verstöße von ZTE Deutschland GmbH gegen die bestehenden Russland-Sanktionen bekannt.

Zu Ermittlungen von Staatsanwaltschaften der Länder nimmt die Bundesregierung schon aus Gründen der bundesstaatlichen Kompetenzverteilung keine Stellung.

15. Könnte die Bundesregierung aufgrund von Sanktionsverstößen anderen Unternehmen eine Belieferung von ZTE mit Produkten untersagen, und wenn ja, auf Basis welcher Rechtsgrundlage beziehungsweise mit welchen Instrumenten?

Die Rechtsfolgen von Sanktionsverstößen ergeben sich aus den §§ 17 ff. des Außenwirtschaftsgesetzes sowie den §§ 80 ff. der Außenwirtschaftsverordnung. Verfolgt werden die Verstöße von den zuständigen Strafverfolgungsbehörden.

16. Wird die in Erarbeitung befindliche China-Strategie der Bundesregierung den Umgang mit chinesischen Herstellern von kritischen Komponenten für Mobilfunknetze adressieren, und wenn ja, inwiefern?

Die umfassende China-Strategie der Bundesregierung befindet sich aktuell in der Ressortabstimmung, eine ins Detail gehende Antwort zu den Inhalten der Strategie ist daher zu diesem Zeitpunkt nicht möglich.

17. Werden Komponenten chinesischer Hersteller in den Kommunikationsinfrastrukturen der Bundeswehr eingesetzt?

a) Wenn ja, wie viel Prozent der Komponenten in der Kommunikationsinfrastruktur der Bundeswehr stammen von chinesischen Herstellern (bitte zusätzlich die Hersteller auflisten)?

b) Wenn ja, unterliegen die bei der Bundeswehr eingesetzten Komponenten anderen (beispielsweise strengeren) Kriterien?

c) Wenn nein, war dies eine bewusste Entscheidung, denen Sicherheitsbedenken zugrunde lagen?

Die Fragen 17 bis 17c werden zusammen beantwortet.

Die Kommunikationsinfrastrukturen der Bundeswehr werden in der Regel durch Industrieunternehmen im Auftrag der Bundeswehr und nach Maßgabe der geltenden Vorgaben und Richtlinien des BSI realisiert.

Dabei ist nicht auszuschließen, dass Komponenten chinesischer Hersteller genutzt werden.

18. Sind der Einbau und die Verwendung von Komponenten chinesischer Hersteller in den Kommunikationsinfrastrukturen der Bundeswehr aus Sicht der Bundesregierung zulässig?

19. Was sind aus Sicht der Bundesregierung die Kriterien für die Zulassung zu Einbau bzw. Verwendung von Komponenten chinesischer Hersteller in den Kommunikationsinfrastrukturen der Bundeswehr?

Die Fragen 18 und 19 werden zusammen beantwortet.

Die Kommunikationsinfrastrukturen der Bundeswehr werden mit Blick auf gegebenenfalls vorhandene, die Cyber- und Informationssicherheit betreffende, Zertifizierungs- oder Zulassungsanforderungen nach den Vorgaben des BSI beschafft und genutzt.

20. Werden Komponenten chinesischer Hersteller in den Kommunikationsinfrastrukturen des BSI eingesetzt, und wenn ja, wie viel Prozent der Komponenten in der Kommunikationsinfrastruktur des BSI stammen von chinesischen Herstellern (bitte zusätzlich die Hersteller auflisten)?

Die folgenden Komponenten in der Kommunikationsinfrastruktur (Netzwerk-/Telefoninfrastruktur) des BSI stammen von chinesischen Herstellern:

– 1 LTE-Router von HUAWEI für externe Präsentationen (Demos) über eine offene Internetverbindung (< 0,1 Prozent) sowie

– die Telekommunikationskomponenten der Firma Alcatel-Lucent Enterprise (100 Prozent der BSI-Festnetztelefonanlage, keine Betroffenheit der Daten- oder Mobilfunkkommunikationsinfrastruktur).

21. Welche Mobilfunknetzbetreiber verwenden nach Kenntnis der Bundesregierung 5G-Technologie von ZTE in ihren Mobilfunknetzen?

Hierzu liegen der Bundesregierung keine eigenen Informationen vor.

22. Benutzt die Deutsche Bahn 5G-Technologie von ZTE in ihrem Mobilfunknetz, und wenn ja, in welchem Umfang?

Bei der Deutschen Bahn AG wird derzeit noch keine 5G-Technologie im Wirknetz eingesetzt. Auf einer Teststrecke mit 5G-Technologie ist der Hersteller ZTE nicht beteiligt.

23. Erwägt die Bundesregierung, in den Beschaffungsprozessen der Sicherheitsbehörden des Bundes das Vergabekriterium „Digitale Souveränität“ aufzunehmen?

Unter digitaler Souveränität versteht die Bundesregierung die Fähigkeiten und Möglichkeiten von Staaten oder Staatengemeinschaften, ihre Rolle in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können, von der technologischen Souveränität (kritische Komponenten) über Datensouveränität bis hin zu Cybersicherheit und digitalen Infrastrukturen. Digitale Souveränität bedeutet dabei, im Rahmen offener Märkte und des regelbasierten Handels eigene Stärken auszubauen und strategische Schwächen zu reduzieren. Auf die Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der AfD auf Bundestagsdrucksache 20/4500 wird verwiesen.

Die Bundesregierung stärkt die digitale Souveränität der Öffentlichen Verwaltung, stellt Wahlmöglichkeiten sicher und reduziert dadurch die Abhängigkeit von einzelnen Anbietern, insbesondere durch die Schaffung von Alternativen und eines offenen, wettbewerbsfähigen Marktes.

Eine generelle Planung der Bundesregierung, die digitale Souveränität als Vergabekriterium selbst bzw. Kriterien, die die digitale Souveränität fördern, als Kriterien für Vergabeverfahren aufzunehmen, besteht derzeit nicht. Jedes Vergabeverfahren im Bereich Software, Hardware oder IT-Services wird durch die jeweils zuständige Vergabestelle gemäß den jeweiligen Bedarfsforderungen konzipiert und aufgesetzt.

Gesichtspunkte der digitalen Souveränität werden vorranging bei Festlegung und Beschreibung des Beschaffungsbedarfs einschließlich der vertraglichen Anforderungen berücksichtigt. Die Gesichtspunkte lassen sich nicht in einem Kriterium zusammenfassen, sondern sind vielgestaltig. Je nach Beschaffungsgegenstand können hier beispielsweise Punkte der Informationssicherheit,

rechtliche Unsicherheiten, Lieferverfügbarkeiten, sonstige Abhängigkeiten, fremdgesteuerte Innovationen oder eine eingeschränkte Flexibilität ausschlaggebend sein.

24. Sollte die Bundesregierung nachträglich den Einbau von ZTE-Komponenten im Mobilfunknetz untersagen (www.br.de/nachrichten/deutschland-welt/5g-ausbau-wie-deutschland-den-einfluss-chinas-eindaemmen-will,TXpleLY) und die Mobilfunknetzbetreiber müssten diese ZTE-Komponenten wieder ausbauen, wer müsste die Kosten für den Ausbau tragen?

§ 9b BSIG enthält keine Rechtsgrundlage für Entschädigungsleistungen für den Fall einer Untersagung oder Anordnung des Einsatzes kritischer Komponenten. Im Übrigen handelt es sich um eine hypothetische und abstrakte Fragestellung ohne hinreichend konkreten Bezugspunkt und Anlass, die von der Bundesregierung nicht zu beantworten ist.

25. Bezugnehmend auf die Antwort zu den Fragen 1 bis 4, 6 bis 9 und 11 auf Bundestagsdrucksache 20/5598, erwägt die Bundesregierung, sich künftig von den Mobilfunknetzbetreibern berichten zu lassen, welche Komponenten aus undemokratischen Drittstaaten diese in den kritischen Infrastrukturen verbauen, und wenn ja, erwägt die Bundesregierung, auch dem Deutschen Bundestag darüber künftig regelmäßig zu berichten?

Wer ein öffentliches Telekommunikationsnetz betreibt, hat nach § 166 Absatz 2 und 4 Satz 2 TKG der Bundesnetzagentur ein Sicherheitskonzept vorzulegen und dieses bei Änderung der Gegebenheiten anzupassen. Hierbei erlangt die Bundesnetzagentur auch Kenntnis von verwendeten kritischen Komponenten im Sinne des § 2 Absatz 13 BSIG. Eine Unterscheidung nach Herkunftsstaaten im Sinne der Fragestellung sieht das Gesetz dabei nicht vor. Auch für eine Unterrichtung des Deutschen Bundestages über die Inhalte der Sicherheitskonzepte ist keine Rechtsgrundlage ersichtlich.

Darüber hinaus erlangt 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.

26. Bis wann wird die Bundesregierung voraussichtlich die von den Mobilfunknetzbetreibern Anfang April 2023 vorzulegende Liste geprüft haben (www.faz.net/aktuell/politik/inland/bmi-prueft-huawei-komponenten-bei m-5-g-ausbau-auf-sicherheit-18730170.html), und bis wann können die Mobilfunknetzbetreiber mit einem Bescheid der Bundesregierung rechnen, ob Komponenten wieder ausgebaut werden müssen (bitte Quartal bzw. Jahr angeben)?

Das BMI beabsichtigt, im April 2023 eingehende Stellungnahmen von Mobilfunknetzbetreibern zu den bei ihnen eingesetzten kritischen Komponenten im Sinne des § 2 Absatz 13 BSIG bis zum Beginn des dritten Quartals 2023 zu prüfen. Ob es daraufhin zu Bescheiden kommt, ist derzeit nicht absehbar, sodass dafür auch keine Zeitplanung besteht.

27. Welche nachgeordnete Behörde wird unter Federführung welches Bundesministeriums die Liste der Komponenten prüfen (www.faz.net/aktuell/politik/inland/bmi-prueft-huawei-komponenten-beim-5-g-ausbau-auf-sicherheit-18730170.html)?

    Welche Rolle und welche Aufgabe hat die Bundesnetzagentur bei diesem Verfahren?

    Wird das Auswärtige Amt an dem Verfahren beteiligt?

Prüfverfahren nach § 9b BSIG werden federführend durch das BMI durchgeführt. Dieses prüft auch in diesem Zusammenhang eingehende Stellungnahmen. An der Prüfung beteiligt BMI die Ressorts: Auswärtiges Amt, Bundesministerium für Digitales und Verkehr (BMDV), Bundesministerium für Wirtschaft und Klimaschutz und das Bundeskanzleramt sowie die nachgeordneten Behörden: BSI, Bundesamt für Verfassungsschutz und Bundesnetzagentur über BMDV.

Die Bundesnetzagentur bringt die dort vorliegenden einschlägigen Erkenntnisse in das Verfahren ein und unterstützt die Prüfung durch die bestehende technische Expertise im Bereich Telekommunikation.

28. Nach welchen Kriterien wird die angekündigte Prüfung der Komponenten durchgeführt (www.faz.net/aktuell/politik/inland/bmi-prueft-huawei-komponenten-beim-5-g-ausbau-auf-sicherheit-18730170.html)?

    Werden externe Unternehmen an der Prüfung beteiligt?

    Wie viele Personentage nimmt eine durchschnittliche Prüfung in Anspruch?

    Wie ist eine „Komponente“ definiert, und welchen Umfang hat eine „Komponente“?

Prüfungen nach § 9b Absatz 4 BSIG werden nach dem dort festgelegten gesetzlichen Prüfmaßstab („voraussichtliche Beeinträchtigung der öffentlichen Ordnung oder Sicherheit“) durchgeführt. Eine Beteiligung externer Unternehmen an der Prüfung ist nicht beabsichtigt. Da der Umfang einzelner Prüfverfahren sehr unterschiedlich sein kann und zudem bisher keine ausreichende Anzahl von Prüfverfahren für die Bildung eines Durschnitts vorliegt, lässt sich die Frage nach der durchschnittlichen Bearbeitungszeit nicht beantworten.

Was eine kritische Komponente ist, ist in § 2 Absatz 13 BSIG legaldefiniert. Daraus ergibt sich auch der Umfang einer Komponente.

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.betrifft-gesetze.de
ISSN 0722-8333