Deutscher Bundestag **Drucksache 19/4804**

19. Wahlperiode 08.10.2018

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Matthias Büttner, Andreas Mrosek und der Fraktion der AfD
– Drucksache 19/4419 –

Nationale Sicherheit und digitale Infrastruktur

Vorbemerkung der Fragesteller

Einem starken Datenschutz muss nach Auffassung der Fragesteller in Zeiten der Digitalisierungen und der damit einhergehenden einfacheren Verbreitung und Missbrauch von sensiblen Daten ein hoher Stellenwert eingeräumt werden.

Die Fragesteller vertreten die Ansicht, dass bei sensibler Netzinfrastruktur sicherzustellen ist, dass die digitale Souveränität gewahrt bleibt. Nach Ansicht der Fragesteller gehört Telekommunikation (unter anderem Mobilfunk- und Glasfasernetze) zur kritischen Infrastruktur des Landes. Die australische Regierung ist hier der Ansicht, dass es mit der nationalen Sicherheit nicht zu vereinbaren ist, Mobilfunkkomponenten von Huawei Technologies Co. Ltd. und ZTE Corp in ihrem 5G-Mobilfunknetz zu verbauen. Laut der „IT-TIMES“ sind Regierungsvertreter in Beijing verärgert und bezeichnen das Vorgehen als schlechte Ausrede, ein chinesisches Unternehmen vom Markt gänzlich auszuschließen (www.it-times.de/news/australien-sperrt-huawei-und-zte-als-5g-technologie-lieferanten-nokia-und-ericsson-durfte-das-freuen-129629/).

Die australische Regierung teilt in ihrer Pressemitteilung mit, dass sie die nationalen Sicherheitsrisiken in Bezug auf 5G-Netze intensiv geprüft hat und dass 5G hier Änderungen benötigt im Vergleich zu früheren Mobilfunknetzen (www.minister.communications.gov.au/minister/mitch-fifield/news/government-provides-5g-security-guidance-australian-carriers).

Vor Australien hatten bereits die Vereinigten Staaten von Amerika Huawei und ZTE von ihrem 5G-Ausbau ausgeschlossen (www.focus.de/digital/handy/nach-den-usa-australien-verbietet-zte-und-huawei-5g-ausbau_id_9474378.html).

Alle drei großen in Deutschland tätigen Mobilfunk- und Internet-Service-Provider setzen überwiegen aus dem Ausland eingekaufte Produkte ein, die sie nur an der Oberfläche verstehen können (www.techrepublic.com/blog/it-security/researchers-create-nearly-undetectable-hardware-backdoor/). Ein Zugriff auf alle spezifischen Hardwarekomponenten oder auf die Firmware ist nur durch den Systemhersteller möglich. Nach Kenntnis der Fragesteller bestehen seitens Mitarbeitern der Deutschen Telekom AG Bedenken, dass im Mobilfunk mehr als zwei Drittel der Technikprodukte von Huawei zum Einsatz kommen und beim 5G-Ausbau Huawei ebenfalls den Löwenanteil erhalten wird. Nach Kenntnis der

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 4. Oktober 2018 übermittelt.

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

Fragesteller dürfte bei anderen Providern die Größenordnung ähnlich, eher noch höher sein (www.wiwo.de/unternehmen/it/huawei-aufstieg-mit-spionage/21115020.html).

1. Gehören für die Bundesregierung Mobilfunk- und Glasfasernetze zu den sicherheitskritischen Infrastrukturen?

In der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung) sind Netze zur Sprach- und Datenübertragung ab bestimmten Schwellwerten als Anlagen definiert, für die besondere Schutzmaßnahmen zu ergreifen sind. Angesichts der hohen Bedeutung Kritischer Infrastrukturen für das Gemeinwohl kommt dem Staat und den Betreibern eine besondere Verantwortung zu, die Anlagen vor Ausfällen und Beeinträchtigungen zu schützen.

2. Hat die Bundesregierung eine umfassende Überprüfung der nationalen Sicherheitsrisiken für 5G-Netze durchgeführt?

   a) Wenn ja:

   Welche Tätigkeiten wurden durchgeführt (bitte nach Datum und Behörde listen)? Welchen Einfluss hatten die Ergebnisse der Tätigkeiten auf die 5G-Strategie der Bundesregierung? Welche konkreten Maßnahmen wurden auf Grund der Überprüfungen getroffen? Welchen Einfluss hatten die Ergebnisse der Tätigkeiten auf die Glasfaserstrategie der Bundesregierung? Welche konkreten Maßnahmen wurden auf Grund der Tätigkeiten getroffen?

   b) Wenn nein:

   Warum hat so eine Überprüfung noch nicht stattgefunden? Ist eine Überprüfung in Planung? Wurde die 5G-Strategie der Bundesregierung formuliert, ohne den Aspekt nationale Sicherheit der verbauten Hardwarekomponenten zu beachten? Wurde die Glasfaserstrategie der Bundesregierung formuliert, ohne den Aspekt nationale Sicherheit der verbauten Hardwarekomponenten zu beachten?

3. Teilt die Bundesregierung die Ansicht der australischen Regierung, dass 5G eine Änderung der Funktionsweise der Mobilfunknetze im Vergleich zu früheren Generationen von Mobilfunknetzen darstellt und diese Änderungen die Bedrohungspotentiale für Telekommunikationsnetze erhöhen?

   a) Wenn ja:

   Welche Maßnahmen hat die Bundesregierung getroffen um die Bedrohungspotentiale zu klassifizieren? Welche Bedrohungspotentiale sieht die Bundesregierung? Wie viele Mitarbeiter der Bundesregierung sind mit dem Aufgabenfeld Bedrohungspotentiale in Bezug auf Telekommunikationsnetze betraut (bitte getrennt nach Behörde listen)?

   b) Wenn nein:

   Wo weicht die Ansicht der Bundesregierung von der Sicht der australischen Regierung ab?

Die Fragen 2 und 3 werden im Zusammenhang beantwortet.

Die Standards für 5G werden von einer internationalen Kooperation von Standardisierungsgremien für die Standardisierung im Mobilfunk (3GPP) entwickelt. Die erste Phase der 5G-Spezifikation soll mit Release 15 im September 2018, die zweite (und entscheidende) Phase soll mit Release 16 und dessen Evaluation bis März 2020 abgeschlossen sein. Im Rahmen der Standardisierung spielt die Frage

der Sicherheit der 5G Netze eine erhebliche Rolle. Die endgültigen Spezifikationen im 5G Bereich stehen jedoch noch nicht zur Verfügung. Die Frequenzvergabe der für 5G relevanten Bereiche ist in Deutschland gleichfalls noch nicht abgeschlossen.

Die Bundesregierung hat entsprechend keine umfassende Untersuchung durchgeführt. Generell gelten jedoch für öffentliche Telekommunikationsnetze – und damit auch für die zukünftigen 5G Netze – verpflichtende gesetzliche Vorgaben. Ergänzende Ausführungen zum Schutz der 5G-Infrastruktur gegen IT-Angriffe enthält zudem auch die 5G-Strategie der Bundesregierung (S. 12).

Der § 109 des Telekommunikationsgesetzes (TKG) enthält technologieneutrale Vorgaben zur Sicherheit von Telekommunikationsnetzen. Nach § 109 Absatz 1, 2 TKG hat jeder Betreiber eines öffentlichen Telekommunikationsnetzes angemessene technische Vorkehrungen zum Schutz des Fernmeldegeheimnisses und gegen Störungen zu treffen.

Insbesondere sind Maßnahmen zu treffen, um Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu sichern. Die Netzbetreiber sind auch verpflichtet, ein Sicherheitskonzept zu erstellen, das der Bundesnetzagentur vorzulegen ist und von dieser geprüft wird. Die Bundesnetzagentur kann zudem anordnen, dass sich die Netzbetreiber einer Überprüfung durch eine qualifizierte unabhängige Stelle unterziehen.

Auch eine Aussage über eine Änderungen und Erhöhung der Bedrohungspotentiale für Telekommunikationsnetze durch 5G, kann auf Grund des laufenden Standardisierungsprozesses entsprechend nicht getroffen werden. Ferner kommentiert die Bundesregierung Ansichten fremder Regierungen grundsätzlich nicht.

4. Teilt die Bundesregierung die Ansicht der Regierungsvertreter in Beijing, dass es sich bei der Vorgehensweise der australischen Regierung um eine Ausrede handelt, um chinesische Unternehmen vom Markt auszuschließen?

5. Teilt die Bundesregierung die Ansicht der australischen Regierung, dass es keine Kombination von technischen Sicherheitskontrollen gibt, die die neu auftretenden Risiken ausreichend mildern?

   Wenn nein, welche Kombination bzw. Maßnahme wird aus Sicht der Bundesregierung als erfolgreich angesehen?

Die Fragen 4 und 5 werden gemeinsam beantwortet.

Die Bundesregierung kommentiert die Ansichten fremder Regierungen grundsätzlich nicht.

6. Teilt die Bundesregierung die Ansicht der australischen Regierung, dass die Beteiligung von Hardwareanbietern, die wahrscheinlich außergerichtlichen Anweisungen einer ausländischen Regierung unterliegen, die mit nationalem Recht kollidieren, das Risiko bergen, dass der Netzbetreiber das 5G-Netz nicht ausreichend vor unbefugtem Zugriff oder Eingriffen schützen kann?

   a) Wenn ja, welche Schlussfolgerungen, Anweisungen und Maßnahmen ergeben sich daraus für die Bundesregierung und für private Internetunternehmen in Deutschland?

   b) Wenn nein, warum nicht?

Die Bundesregierung nimmt zu spekulativen Fragestellungen und zu Ansichten fremder Regierungen nicht Stellung.

7. Die Hardware welcher Anbieter für Mobilfunk- und Glasfaserhardware ist nach Kenntnis der Bundesregierung in den Telekommunikationsnetzen in Deutschland verbaut (bitte nach Technik, Prozentzahl und Anbieter listen)?

   Wenn nicht beantwortet werden kann, welche Hardware verbaut ist, wie wurde die Überprüfung der Telekommunikationsnetze auf Übereinstimmungen mit den Zielen digitale Souveränität und nationale Sicherheit durchgeführt?

Die Bundesregierung hat keine umfassende Einzelfallkenntnis von den in TK-Netzen eingesetzten Technologien und Produkten. Des Weiteren unterfallen derartige Informationen ggf. dem Geschäftsgeheimnis der Unternehmen. Die grundlegenden Anforderungen an die Funktionsweise und Sicherheitseigenschaften der eingesetzten Technologien ergeben sich aus den gesetzlichen Grundlagen (TKG). Der Digitalfunk BOS und Netze des Bundes nutzen die Netzinfrastruktur der TSI.

8. Welcher Anbieter von Hardware ist nach Kenntnis der Bundesregierung für den 5G-Ausbau relevant?

Die Beschaffung der Netzinfrastruktur im 5G Bereich ist Sache derjenigen Unternehmen, welche den 5G Aufbau vorantreiben werden. Da die eingesetzten Technologien frei am Markt eingekauft werden, ist grundsätzlich jeder Anbieter von Netzinfrastruktur potentiell relevant. Bzgl. der genauen Anforderungen an die 5G Infrastruktur und die Frequenznutzung kann auf Grund des laufenden Prozesses der Frequenzvergabe keine Aussage getroffen werden.

9. Welche Hardware welcher Anbieter wird nach Kenntnis der Bundesregierung in den digitalen Testfeldern (www.bmvi.de/DE/Themen/Digitales/Digitale-Testfelder/Digitale-Testfelder.html) genutzt (bitte getrennt nach Projekt auflisten)?

Auf digitalen Testfeldern können Wirtschaft und Wissenschaft Innovationen und Forschungsfragen für den Straßenverkehr der Zukunft im Realverkehr erproben, weiterentwickeln und validieren. Erprobungsprojekte auf den digitalen Testfeldern werden in Eigenverantwortung der Projektbeteiligten durchgeführt. Entscheidungen für die Nutzung bestimmter IT-Hardware liegen in der Verantwortung der Projektbeteiligten. Es handelt sich dabei häufig um Eigenentwicklungen im Entwicklungsstadium, welche von den Projektbeteiligten auf den digitalen Testfeldern er-probt werden. Im Bundesministerium für Verkehr und digitale Infrastruktur wird kein Verzeichnis über die genutzte IT-Hardware geführt.

10. Ist die Bundesregierung der Ansicht, dass durch das Verbauen von Hardware des Anbieters Huawei Technologies Co. Ltd. in Glasfasernetzen ein Risiko für die nationale Sicherheit oder digitale Souveränität ausgeht?

11. Ist die Bundesregierung der Ansicht, dass durch das Verbauen von Hardware des Anbieters Huawei Technologies Co. Ltd. in 5G-Mobilfunknetzen ein Risiko für die nationale Sicherheit oder digitale Souveränität ausgeht?

12. Ist die Bundesregierung der Ansicht, dass durch das Verbauen von Hardware des Anbieters ZTE Corp. in Glasfasernetzen ein Risiko für die nationale Sicherheit oder digitale Souveränität ausgeht?

13. Ist die Bundesregierung der Ansicht, dass durch das Verbauen von Hardware des Anbieters ZTE Corp. in 5G-Mobilfunknetzen ein Risiko für die nationale Sicherheit oder digitale Souveränität ausgeht?

14. Gibt es Hersteller von Hardware, bei denen die Bundesregierung der Ansicht ist, dass ein Verbauen ihrer Technologie in Mobilfunk- oder Glasfasernetzen ein Sicherheitsrisiko in Bezug auf die nationale Sicherheit oder digitale Souveränität darstellt (bitte alle betroffenen Hersteller getrennt nach Land listen)?

15. Hat die Bundesregierung geprüft, ein Verbot für die Nutzung von Hardware bestimmter Hersteller beim Aufbau von Mobilfunk-, 5G- und Glasfasernetzen in Deutschland auszusprechen?

    a) Wenn ja:

    War die Prüfung allgemeiner Natur? War die Prüfung konkret auf Hardware einiger Hersteller bezogen?

    b) Wenn nein:

    Ist so eine Prüfung in Planung? Wenn eine Prüfung in Planung ist, wird diese Prüfung allgemeiner Natur sein, oder sich konkret auf Hardware einiger Hersteller beziehen?

Die Fragen 10 bis 15 werden im Zusammenhang beantwortet.

Der Einsatz von Informationstechnik aus Drittstaaten geht immer einher mit der Frage nach digitaler Souveränität und den eigenen Möglichkeiten.

In einer weit entwickelten digitalisierten Welt ist dabei aus Sicht der Bundesregierung die generelle Abschottung öffentlicher Netzinfrastrukturen gegen bestimmte Anbieter jedenfalls kein adäquater Schutzmechanismus. Vielmehr muss – um eine hinreichende Souveränität zu gewährleisten – der Einsatz kritischer Komponenten sehr sorgfältig evaluiert und bewertet werden. Die Anbieter öffentlicher Netze arbeiten in diesem Zusammenhang sehr intensiv mit dem Bundesministerium des Innern, für Bau und Heimat (BMI) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zusammen, um durch gemeinsame Bewertungen, Evaluationen und ggf. Zertifizierungen sowie den daraus abgeleiteten Maßnahmen, die Risiken nicht vertrauenswürdiger IT zu minimieren und möglichst auch auszuschließen. Diese Grundsätze gelten damit auch für die Risikobewertung in den von Ihnen angesprochenen Szenarien.

16. Die Hardware welcher Hersteller für Mobilfunk-, 5G-, und Glasfaserausbau ist nach Kenntnis der Bundesregierung am preisgünstigsten und würde erwartungsgemäß den Zuschlag bei öffentlichen Ausschreibungen erhalten (bitte nach Herkunft des Herstellers nach Preis aufsteigend listen)?

Die Bundesregierung hat keine Kenntnis darüber, welche Hardware im 5G Bereich am günstigsten bzw. am wirtschaftlichsten sein wird. Die Beschaffung der Hardware ist Sache der Unternehmen. Entsprechend kann auch nicht über den möglichen Einsatz spekuliert werden.

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.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