Deutscher Bundestag **Drucksache 19/12959**

19. Wahlperiode 03.09.2019

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Uwe Schulz, Joana Cotar und der Fraktion der AfD
– Drucksache 19/12269 –

Stand der nationalen Risikobewertung der 5G-Netzinfrastruktur

Vorbemerkung der Fragesteller

Die vom Bundesministerium für Wirtschaft und Energie (BMWi) am 17. Juni 2019 vorgelegte Ausschussdrucksache 19(23)053 trägt den Titel „Bericht der Bundesregierung zum aktuellen Stand der nationalen Risikobewertung der 5G-Netzinfrastruktur und ggf. erster Schlussfolgerungen daraus auf Grundlage der Empfehlung der Kommission vom 26. März 2019 Cybersicherheit der 5G-Netze“.

Nach Ansicht der Fragesteller werden in diesem Bericht allerdings zum aktuellen Stand der nationalen Risikobewertung der 5G-Netzinfrastruktur überhaupt keine Aussagen getroffen, sondern lediglich zum Stand des nach § 109 des Telekommunikationsgesetzes (TKG) aufzustellenden Katalogs von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen und für die Verarbeitung personenbezogener Daten. Der Bericht entspricht damit wortgleich dem bereits mit Ausschussdrucksache 19(23)041 am 12. März 2019 vorlegten „Sachstandsberichts des Bundesministerium für Wirtschaft und Energie zu 5G-Sicherheitsaspekte“, lediglich ergänzt um einige Erläuterungen zu den Empfehlungen der EU-Kommission vom 26. März 2019 zur Cybersicherheit von 5G-Netzen.

In dem aktuellen BMWi-Bericht (Ausschussdrucksache 19(23)053) heißt es wie folgt: „Die von der EU-Kommission bis zum 30. Juni 2019 geforderte nationale Risikobewertung und anschließende Aktualisierung der Sicherheitsmaßnahmen haben wir mit der Veröffentlichung der Eckpunkte für den zukünftigen Katalog an Sicherheitsanforderungen bereits begonnen. Die von der BNetzA am 7. März 2019 veröffentlichten Eckpunkte beinhalten bereits die Kernpunkte der Empfehlung“.

Nach Auffassung der Fragesteller wurden mit diesem Verfahren offenbar Maßnahmen zum Risikomanagement am 7. März 2019 vorgeschlagen, noch bevor die Phase der Risikobewertung am 30. Juni 2019 abgeschlossen wurde.

In dem aktuellen, am 17. Juni 2019 vorgelegten BMWi-Bericht (Ausschussdrucksache 19(23)053), wird ferner mehrfach auf die Frist zum 30. Juni 2019 zur Durchführung der nationalen Risikoanalyse explizit hingewiesen, darunter mit unterstrichener und fettgedruckter Schriftart. Dennoch behauptete eine Vertreterin des BMWi vor dem Bundestagsausschuss Digitale Agenda am

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums für Wirtschaft und Energie vom 30. August 2019 übermittelt.

Die Drucksache enthält – in kleinerer Schrifttype – den Fragetext.

26. Juni 2019, es gäbe diese Frist nicht bzw. sie wäre verschoben. Konkret wurde nur die weitere Frist 15. Juli 2019 genannt, bis zu der der Kommission und der Agentur der Europäischen Union für Cybersicherheit (ENISA) die nationalen Risikobewertungen übermittelt werden sollen.

Eine Methodik zur Analyse und Bewertung von Risiken hat beispielsweise das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe bereits im Jahr 2010 entwickelt und dem Deutschen Bundestag vorlegt (http://dipbt.bundestag.de/ dip21/btd/17/041/1704178.pdf). Auf Basis des § 18 des Zivilschutz- und Katastrophenhilfegesetzes (ZSKG) vom 2. April 2009 führt der Bund im Zusammenwirken mit den Ländern seit 2012 jährlich eine bundesweite, ressortübergreifende Risikoanalyse zu unterschiedlichen Szenarien im Bevölkerungsschutz mit Hilfe dieser Methodik durch. Dabei werden Schadensausmaß und Eintrittswahrscheinlichkeit analysiert und das Risiko dementsprechend mit einem Schadenserwartungswert bewertet und in die Kategorien „sehr hoch“, „hoch“, „mittel“, „niedrig“ eingeteilt.

1. Wann und von wem wurde der Hausleitung des BMWi die laut Empfehlung der EU-Kommission vom 26. März 2019 zur Cybersicherheit der 5G-Netze (https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019H0534&rid=1) gesetzte Frist zum 30. Juni 2019 zur Durchführung der nationalen Risikobewertungen übermittelt?

Die Empfehlung (EU) 2019/534 der Kommission vom 26. März 2019 zu Cybersicherheit der 5G-Netze und dementsprechend auch die darin enthaltene Frist zur Durchführung der nationalen Risikobewertungen wurde der Leitung des Bundesministeriums für Wirtschaft und Energie am 27. März 2019 übermittelt.

2. Wann und durch welche Behörden wurde mit der nationalen Risikobewertungen der 5G-Netzinfrastruktur begonnen?

Die Arbeiten zur Durchführung der nationalen Risikobewertung entsprechend der Empfehlung (EU) 2019/534 der Kommission vom 26. März 2019 wurden von der hierfür federführend zuständigen Bundesnetzagentur und dem Bundesamt für Sicherheit in der Informationstechnik umgehend aufgenommen.

3. Welche Risikofaktoren wurden bei der nationalen Risikobewertung der 5G-Netzinfrastruktur berücksichtigt?

Es wurde das von der Kooperationsgruppe nach Artikel 11 der Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union erarbeitete Risk Assessment Template genutzt. Darin wurden die Risikofaktoren „Kompromittierung der Integrität der Dienste“, „Verlust der Vertraulichkeit von Daten“ sowie „Verlust der Verfügbarkeit“ berücksichtigt.

4. Zu welchem Ergebnis hat die nationale Risikobewertung der 5G-Infrastrutur geführt?

Die nationale Risikobewertung setzt sich mit den aus der Gesamtkomplexität künftiger 5G-Netzwerke resultierenden Sicherheitsimplikationen auseinander. Es ist vorgesehen, dass die nationalen Risikobewertungen der Mitgliedstaaten von der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) konsolidiert werden und in der Folge als Grundlage für die Ableitung von Maß-

nahmen auf EU-Ebene dienen. Die Einzelheiten zu diesem Prozess können der Empfehlung (EU) 2019/534 der Kommission vom 26. März 2019 entnommen werden.

Auf den die nationale Risikobewertung zusammenfassenden Abschlussbericht (Guidelines on common elements for 5G cybersecurity risk assessments and structured template for reporting on findings) wird verwiesen.

5. Welches Verfahren wurde für die nationale Risikobewertung der 5G-Infrastruktur benutzt?

   a) Wurde dieses Verfahren neu entwickelt, und wenn ja, warum wurde nicht auf bereits bewährte Verfahren anderer Bundesbehörden zurückgegriffen?

Es wurde das für diesen Zweck von der Kooperationsgruppe nach Artikel 11 der Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union erarbeitete Risk Assessment Template genutzt. Das Verfahren musste neu entwickelt werden. Ein Rückgriff auf bestehende Analyseverfahren war aufgrund des spezifischen Analysegegenstandes und fehlender Vergleichbarkeit nicht angezeigt.

   b) Entspricht das genutzte Verfahren zur Risikobewertung den Empfehlungen der EU-Kommission vom 26. März 2019 zur Cybersicherheit der 5G-Netze, und falls nein, warum nicht?

Die Empfehlung (EU) 2019/534 der Kommission vom 26. März 2019 sieht kein bestimmtes Analyseverfahren zur nationalen Risikobewertung vor, beinhaltet aber einen Auftrag an die Kooperationsgruppe und die Computer-Notfallteams, die mit der Richtlinie (EU) 2016/1148 eingerichtet wurden, diesen Vorgang zu unterstützen. Dies ist mit der Erarbeitung der strukturierten Vorlage für die Risikobewertung geschehen.

6. Sieht die Bundesregierung die Aggregation nationaler Risikobewertungen bei Verwendung nicht EU-konformer und damit uneinheitlicher Verfahren zur Risikobewertung als möglich an, und falls ja, wie?

Um ein möglichst einheitliches Verfahren zur Risikobewertung zu gewährleisten, wurde für diesen Zweck von der Kooperationsgruppe nach Artikel 11 der Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union eine strukturierte Vorlage (Risk Assessment Template) erstellt und die Mitgliedstaaten wurden dazu angehalten, sich bei der Durchführung der nationalen Risikobewertungen hieran zu orientieren.

7. Teilt die Bundesregierung die Auffassung der Fragesteller, dass mit den am 7. März 2019 veröffentlichten Eckpunkten offenbar bereits Maßnahmen zum Risikomanagement vorgeschlagen wurden, noch bevor die Phase der Risikobewertung am 30. Juni 2019 abgeschlossen war, und als wie zielführend bewertet die Bundesregierung diesen zeitlichen Ablauf?

Die zeitnahe Veröffentlichung der Eckpunkte für die zukünftige Fassung des Katalogs von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 Absatz 4 des Telekommunikationsgesetzes am

7. März 2019 war im Hinblick auf die anstehende Versteigerung der 5G-Frequenzen in Deutschland erforderlich. Die Risikobewertung im Rahmen der Empfehlung (EU) 2019/534 der Kommission vom 26. März 2019 ist ein Vorhaben auf EU-Ebene, ergänzt das nationale Vorgehen und wird daher ebenfalls als zielführend betrachtet.

8. Werden die geplanten detaillierten Neuformulierungen im Katalog von Sicherheitsanforderungen vorliegen, bevor die Telekommunikationsunternehmen ihre Verträge mit 5G-Ausrüstern abschließen, und wann wird das sein?

Der Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten wird derzeit entsprechend den Vorgaben von § 109 Absatz 6 des Telekommunikationsgesetzes von der Bundesnetzagentur im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit überarbeitet. Über die Details der Verträge der Telekommunikationsunternehmen mit potenziellen 5G-Ausrüstern hat die Bundesregierung keine Erkenntnisse.

9. Warum wurde der geplante neue Katalog von Sicherheitsanforderungen nicht bereits zum Start der Versteigerung der 5G-Frequenzen vorgelegt, um den Bietern volle Transparenz für ihre Geschäftsmodelle zu ermöglichen?

Der Katalog von Sicherheitsanforderungen hat sich am Stand der Technik zu orientieren. 5G-Systemtechnik kommt bislang ausschließlich in Versuchsumgebungen zum Einsatz. Auf entsprechende Erkenntnisse der Anwender kann daher noch nicht zurückgegriffen werden. Den zur Vorlage eines Sicherheitskonzeptes verpflichteten Unternehmen sollte dennoch frühzeitig eine Grundlage für zu erwartende zukünftige zusätzliche Anforderungen zur Verfügung gestellt werden. Mit Veröffentlichung der Eckpunkte dieser beabsichtigten zusätzlichen Sicherheitsanforderungen am 7. März 2019 wurde den potenziellen Teilnehmern an der Frequenzauktion insofern die zu diesem Zeitpunkt mögliche Transparenz verschafft.

10. Wann und aus welchen Quellen hat die Bundesregierung erstmals von möglichen Risiken für die deutsche 5G-Infrastruktur durch ausländische Netzwerkausrüster erfahren?

Die Bundesregierung betreibt eine regelmäßige Analyse dieser und vergleichbarer Risiken, auch ohne Anlass.

11. Seit wann hat die Bundesregierung Kenntnis von dem Huawei Cyber Security Evaluation Centre (HCSEC), das aufgrund von „ungewöhnlichen Aktivitäten“ der Huawei-Komponenten (core switches) im britischen Telekommunikationsnetzwerk bereits im Jahre 2010 durch die britische Sicherheitsbehörde Government Communications Headquarters (GCHQ) etabliert wurde (www.wired.co.uk/article/huawei-gchq-security-evaluation-uk)?

Die Bundesregierung hat durch das Bundesamt für Sicherheit in der Informationstechnik seit 2010 Kenntnis von der Existenz des HCSEC.

12. Warum behauptet das BMWi in seinem am 17. Juni 2019 vorgelegten Bericht (Ausschussdrucksache 19(23)053), die Bundesnetzagentur (BNetzA), das Bundesamt für Sicherheit in der Informationstechnik (BSI) und der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) hätten „unverzüglich“ im Zuge der in den vergangenen Wochen geführten Diskussionen um die Netzwerksicherheit gehandelt und die Eckpunkte für den zu überarbeitenden Katalog von Sicherheitsanforderungen abgestimmt, obwohl nach Ansicht der Fragesteller „Diskussionen um die Netzwerksicherheit“ der Bundesregierung schon deutlich länger hätten bekannt sein müssen als nur ein paar Wochen (www.spiegel.de/netzwelt/netzpolitik/5g-in-deutschland-usa-fordern-verzicht-auf-huawei-technik-a-1240977.html)?

    Sieht die Bundesregierung vor diesem Hintergrund eine Bewertung der Abstimmung der Eckpunkte als „unverzügliches“ Handeln als gerechtfertigt an?

Es wird auf die Antwort zu Frage 9 verwiesen.

13. Wird der Katalog von Sicherheitsanforderungen auch Sanktionen enthalten, und wenn ja, welche?

Eine Sanktion kann nur auf der Grundlage eines Gesetzes erfolgen, hier auf Basis des Telekommunikationsgesetzes. Der Katalog von Sicherheitsanforderungen kann daher keine Sanktionen enthalten.

14. Wie soll nach Ansicht der Bundesregierung mit den dem BSI vorzulegenden „Nachweisen der Vertrauenswürdigkeit“ des Herstellers umgegangen werden, wenn diese Nachweise mit existierenden Vertrauenswürdigkeitsbewertungen deutscher Sicherheitsbehörden kollidieren?

Die Details zu den möglichen Wirkungsweisen der geplanten Vertrauenswürdigkeitszusicherung werden derzeit noch bearbeitet, die Abstimmung zwischen den betroffenen Ressorts ist noch nicht abgeschlossen.

15. Mit welchem technischen, organisatorischen, personellen und finanziellen Mehraufwand bei dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und bei der Bundesnetzagentur (BNetzA) ist durch die Umsetzung der gesteigerten Anforderungen des Katalogs zu rechnen?

Da die Überarbeitung des Kataloges derzeit noch nicht abgeschlossen ist, kann ein etwaiger Mehraufwand noch nicht abgeschätzt werden. Die langfristigen technischen, organisatorischen, personellen und finanziellen Implikationen für die betroffenen Behörden sind Bestandteil einer sich an den Anforderungen des zukünftigen Katalogs orientierenden entsprechenden Bedarfsabschätzung.

16. Ist das BSI und die BNetzA bereits technisch, organisatorisch, personell und finanziell in die Lage versetzt worden, die gesteigerten Anforderungen des Katalogs umzusetzen, und wenn nein, wann wird damit begonnen?

Sobald der überarbeitete Katalog an Sicherheitsanforderungen vorliegt, sollen das Bundesamt für Sicherheit in der Informationstechnik und die Bundesnetzagentur entsprechend dem sich hieraus ergebenden Bedarf (siehe Antwort zu Frage 15) zeitnah mit den erforderlichen Ressourcen ausgestattet werden.

17. Beabsichtigt die Bundesregierung überhaupt, die Produktprüfungen unmittelbar durch das BSI selbst durchführen zu lassen, oder soll das Prüfverfahren, vergleichbar mit dem britischen Modell der Prüfung durch das HCSEC unter Aufsicht des GCHQ, durch das in Bonn ansässige Huawei Security Lab unter Aufsicht des BSI durchgeführt werden?

Seitens des Bundesamtes für Sicherheit in der Informationstechnik ist es nicht beabsichtigt, Produktevaluierungen durch das Huawei Security Lab durchführen zu lassen.

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