Deutscher Bundestag **Drucksache 19/12117**

19. Wahlperiode 31.07.2019

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Heike Hänsel, Michel Brandt, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 19/11396 –

Europäische Initiativen zur Überwachung der 5G-Telefonie

Vorbemerkung der Fragesteller

Die fünfte Mobilfunkgeneration (5G) ermöglicht Telefonverbindungen mit etappenweiser Verschlüsselung. Deutsche Polizeien und Geheimdienste befassen sich deshalb seit längerer Zeit mit Möglichkeiten des Zugangs zu diesen sicheren Verbindungen (Bundestagsdrucksache 19/10535, Schriftliche Frage 18 des Abgeordneten Dr. Diether Dehm). Die Bundesregierung bezeichnet dies als „Herausforderungen“ für ihre Sicherheitsbehörden. Dies betreffe die Gefahrenabwehr und die Strafverfolgung (Schriftliche Frage 20 des Abgeordneten Dr. Diether Dehm auf Bundestagsdrucksache 19/10765).

Die technische Standardisierung von 5G ist noch nicht abgeschlossen und soll im Dezember 2019 finalisiert werden (Ratsdokument 8983/19). Daher ist es noch möglich, die Implementierung von Abhörschnittstellen bei der Einführung von 5G zu berücksichtigen. Die Bundesregierung beteiligt sich mit dem Bundesamt für Verfassungsschutz (BfV), der Bundesnetzagentur (BNetzA) und dem Zollkriminalamt (ZKA) an dem Europäischen Institut für Telekommunikationsnormen (ETSI) bzw. dort eingerichteten Arbeitsgruppen zu Abhörmöglichkeiten (Bundestagsdrucksache 17/11239, Frage 10). Das Bundeskriminalamt (BKA) nimmt nicht daran teil, stimmt sich aber mit dem ZKA inhaltlich zu gemeinsamen Positionen ab. Im März 2012 hatte das ETSI 759 Mitglieder aus 62 Ländern, im Jahr 2011 betrug das Budget 22 472 000 Euro (www.etsi.org/membership).

Zusammen mit der BNetzA nimmt das BfV seit 2003 außerdem am 3rd Generation Partnership Project (3GPP) zu „Lawful Interception“ (SA3-LI) teil. Das 3GPP, dem sich auch das ETSI angeschlossen hat, ist ein weltweiter Zusammenschluss von sieben Standardisierungsgremien. Zu ihnen gehören neben Behörden auch Netzwerkausrüster und Netzbetreiber sowie „Hersteller von Sicherheitstechnik und Überwachungslösungen“ (Bundestagsdrucksache 17/11239, Frage 10). Voraussetzung für die Mitarbeit in 3GPP ist die Mitgliedschaft in einem der dort zusammengeschlossenen Standardisierungsgremien (für die Bundesbehörden das ETSI). Laut einem Medienbericht hat die 3GPP-Arbeitsgruppe SA3-LI bereits dafür gesorgt, dass die Interessen der Behörden

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 29. Juli 2019 übermittelt.

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

„gewürdigt werden“ („Verschlüsselung in 5G: ‚Das Rennen ist verloren‘“, www.heise.de vom 6. Juni 2019). Bezüglich der Abhörschnittstellen für Behörden entsprechen die neuen 5G-Standards früheren Mobilfunkstandards.

Für mehr Sicherheit soll in 5G die Verschlüsselung der bislang unverschlüsselt übertragenen Teilnehmerkennungen (IMSI) sorgen. Daher sind sogenannte IMSI-Catcher, mit denen die Nummern von in der Nähe befindlichen Telefonen festgestellt oder mit einer fingierten Netzstation abgehört werden können, nutzlos. Das bestätigt auch die Bundesregierung (siehe oben) und prüft, mit welchen „technischen und rechtlichen Anpassungen“ diese „derzeitige Konfiguration“ des 5G-Standards im Rahmen des Standardisierungsprozesses im ETSI geändert werden könnte. Möglich wäre, dass die IMSI- oder IMEI-Daten zukünftig mit richterlichem Beschluss bei den Netzanbietern abgefragt werden können („Verschlüsselung in 5G: ‚Das Rennen ist verloren‘“, www.heise.de vom 6. Juni 2019).

Auch die EU-Justiz- und -Innenminister haben sich auf ihrer Tagung am 6. und 7. Juni 2019 mit Auswirkungen von 5G auf dem Gebiet der inneren Sicherheit befasst („Überwachungs-Overkill im EU-Ministerrat ab Donnerstag“, https://fm4. orf.at vom 2. Juni 2019). Diskussionsgrundlage war das erwähnte Papier des EU-Koordinators für Terrorismusbekämpfung. Gilles de Kerchove wurde dabei vom BKA unterstützt, wofür sich dieser ausdrücklich bedankt hat. Das BKA hatte bei einem Termin „Informationen zu möglichen Auswirkungen von 5G auf die Aufgabenwahrnehmung der Sicherheitsbehörden“ zur Verfügung gestellt (Schriftliche Frage 20 des Abgeordneten Dr. Diether Dehm auf Bundestagsdrucksache 19/10765).

Vorbemerkung der Bundesregierung

Zwar ist der parlamentarische Informationsanspruch grundsätzlich auf die Beantwortung gestellter Fragen in der Öffentlichkeit angelegt. Soweit parlamentarische Anfragen Umstände betreffen, die aus Gründen des Staatswohls geheimhaltungsbedürftig sind, hat die Bundesregierung zu prüfen, ob und auf welche Weise die Geheimhaltungsbedürftigkeit mit dem parlamentarischen Informationsanspruch in Einklang gebracht werden kann. Die Bundesregierung ist nach sorgfältiger Abwägung zu der Auffassung gelangt, dass für die oben genannten Bundesbehörden im Rahmen dieser Kleinen Anfrage eine Beantwortung sämtlicher Fragen in offener Form ganz oder teilweise nicht erfolgen kann.

Die Antworten zu den Fragen 2b, 3, 4 und 8 (mit Unterfragen) sind als Verschlusssache mit dem Geheimhaltungsgrad „VS – Nur für den Dienstgebrauch“ eingestuft.

Die erbetenen Auskünfte sind in Teilen geheimhaltungsbedürftig, weil sie Informationen enthalten, die im Zusammenhang mit der Arbeitsweise und Methodik der von der Kleinen Anfrage betroffenen Dienststellen des Bundes (Bundeskriminalamt, Bundespolizei, Zollkriminalamt, Bundesamt für Verfassungsschutz, Bundesamt für den Militärischen Abschirmdienst, Bundesnachrichtendienst) und insbesondere deren Aufklärungsaktivitäten und Analysemethoden stehen. Die Antworten auf die Kleine Anfrage beinhalten zum Teil detaillierte Einzelheiten zu ihren technischen Fähigkeiten und ermittlungstaktischen Verfahrensweisen. Aus ihrem Bekanntwerden könnten Rückschlüsse auf ihre Vorgehensweise, Fähigkeiten und Methoden gezogen werden, was wiederum nachteilig für die Aufgabenerfüllung der durchführenden Stellen und damit für die Interessen der Bundesrepublik Deutschland sein kann.

Deshalb sind die Antworten zu den genannten Fragen gemäß § 2 Absatz 2 Nummer 4 der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern, für Bau und Heimat zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA) in Teilen als Verschlusssache mit dem Geheimhaltungsgrad „VS – Nur für den Dienstgebrauch“ eingestuft und werden als nicht zur Veröffentlichung in einer Bundestagsdrucksache bestimmte Anlage übermittelt.*

1. Worin bestehen aus Sicht der Bundesregierung die „Herausforderungen“ für die Sicherheitsbehörden hinsichtlich der fünften Mobilfunkgeneration (5G), die sie in den Bereichen Gefahrenabwehr und Strafverfolgung feststellt und die den Zugang zu relevanten Informationen für die Behörden betreffen (Schriftliche Frage 20 des Abgeordneten Dr. Diether Dehm auf Bundestagsdrucksache 19/10765)?

Abschließende Feststellungen sind nach Auffassung der Bundesregierung vor dem Hintergrund der nicht abgeschlossenen Standardisierung noch nicht möglich. Absehbar ist jedoch, dass das Konzept „Privacy by Design“ als Kernforderung bei der Standardisierung von 5G durch Funktionalitäten wie Verschlüsselung, Virtualisierung und Anonymisierung zusätzliche technische Hürden bei der Überwachung der Telekommunikation und der Umsetzung technischer Ermittlungsmaßnahmen mit sich bringt.

2. Besteht aus Sicht der Bundesregierung die ernsthafte Gefahr, dass die vorhandenen Ermittlungsmaßnahmen im Bereich der Telekommunikation nach Einführung der 5G-Technologie faktisch nicht mehr oder nicht mehr im gleichen Umfang zur Verfügung stehen und dadurch Ermittlungslücken entstehen (vgl. Jumiko-Frühjahrskonferenz 2019, Beschluss zur „Sicherung der Möglichkeit der Telekommunikationsüberwachung bei Einführung der fünften Mobilfunkgeneration)?

   Falls ja, worin liegt diese Gefahr konkret?

   Falls nein, welche Ermittlungsmaßnahmen gemäß §§ 100a ff. der Strafprozessordnung werden aus Sicht der Bundesregierung mit der Einführung des 5G-Standards nach derzeitigem Stand nicht beeinträchtigt?

Auf die Antwort zu Frage 1 wird verwiesen.

a) Enthalten die vom ETSI und dem 3GPP entwickelten bzw. diskutierten Standards zu 5G nach Kenntnis der Bundesregierung nach derzeitigem Stand eine Option, eine Pflicht oder eine Empfehlung für Ende-zu-Ende-Verschlüsselung?

Auf die Antwort der Bundesregierung auf die Schriftliche Frage 18 auf Bundestagsdrucksache 19/10535 wird verwiesen.

* Das Bundesministerium des Innern, für Bau und Heimat hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

b) Welche Ermittlungslücken sieht die Bundesregierung hinsichtlich des Roamings mittels eines Endgeräts, das in Deutschland genutzt wird, aber bei einem ausländischen Netzbetreiber angemeldet ist?

Nach Maßgabe der Ausführungen in der Vorbemerkung der Bundesregierung wird auf den als Verschlusssache mit dem Geheimhaltungsgrad „VS – Nur für den Dienstgebrauch“ versehenen Antwortteil verwiesen.

c) Sieht die Bundesregierung Ermittlungslücken hinsichtlich der in 5G möglichen Aufteilung in eine Vielzahl virtueller Netze („Network Slicing“)?

Falls ja, wodurch kommen diese zustande?

Da die Standardisierung bei 3GPP bezogen auf Network Slicing noch nicht abgeschlossen ist, kann hierzu keine abschließende Aussage getroffen werden.

d) Inwiefern haben sich bereits unter 4G entsprechende Ermittlungslücken gezeigt, das nach Kenntnis der Fragestellerinnen und Fragesteller mit einem „Dedicated Core Network“ (DCN) ebenfalls in verschiedene Netze unterteilt werden kann (bitte erläutern)?

Der Bundesregierung sind keine Ermittlungslücken dieser Art bezogen auf 4G-Netze bekannt.

e) Handelt es sich bei dem in 5G genutzten „Multi-Access Edge Computing“ (MEC) am Endgerät aus Sicht der Bundesregierung um die Verarbeitung von Kommunikationsdaten oder um eine Datenverarbeitung auf dem Endgerät?

Aus technischer Sicht stellt „Multi-Access Edge Computing“ einen Kommunikationsvorgang zwischen Endgeräten dar, der ohne Nutzung des Kernnetzes auskommt. Dabei kann es sich auch um die Verarbeitung von Kommunikationsdaten handeln.

f) Welche Möglichkeiten kennt und nutzt die Bundesregierung zur Ausleitung dieser „Access Edge“-Daten?

Die Nutzung von Multi-Access Edge Computing (MEC) ist mit der Einführung von 5G vorgesehen. Insoweit bestehen bislang keine Möglichkeiten zur Ausleitung entsprechender Informationen. Nach den Vorschriften des Telekommunikationsgesetzes und der Telekommunikations-Überwachungsverordnung müssen Betreiber von Telekommunikationsanlagen, mit denen öffentlich zugängliche Telekommunikationsdienste erbracht werden, ab der Inbetriebnahme für die darüber erbrachten Telekommunikationsdienste Überwachungstechnik vorhalten. Mögliche technische Anforderungen zur Sicherstellung einer vollständigen Erfassung und Ausleitung der zu überwachenden Telekommunikation werden erforderlichenfalls in der Technischen Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation (TR TKÜV) zu beschreiben sein.

3. Inwiefern gelten die beschriebenen Gefahren oder Ermittlungslücken nach Kenntnis der Bundesregierung auch für Endgeräte, die neben 5G zunächst das 4G-Kernnetz verwenden oder über Schnittstellen für 4G, 3G bzw. 2G verfügen?

4. Welche dieser beschriebenen Gefahren existieren nach Auffassung der Bundesregierung in welchem Modell des Parallelbetriebs von EPC (4G Core) und 5G?

Die Fragen 3 und 4 werden gemeinsam beantwortet.

Nach Maßgabe der Ausführungen in der Vorbemerkung der Bundesregierung wird auf den als Verschlusssache mit dem Geheimhaltungsgrad „VS – Nur für den Dienstgebrauch“ versehenen Antwortteil verwiesen.

5. Steigt nach Ansicht der Bundesregierung durch Verfahren in 5G wie beispielsweise MEC die Wahrscheinlichkeit, dass überwachte Telekommunikationskundinnen und -kunden von laufenden Überwachungsmaßnahmen erfahren?

Nach Kenntnis der Bundesregierung besteht keine erhöhte Wahrscheinlichkeit im Sinne der Fragestellung.

6. Über welche Fähigkeiten, Ausrüstung und Kompetenzen verfügen Bundesbehörden bzw. nach Kenntnis der Bundesregierung auch Behörden der Länder zur Telekommunikationsüberwachung von Netzen auf Basis des Codemultiplexverfahrens (CDMA-/CDMA2000)?

Zum Trennen mehrerer räumlich verteilter, gleichzeitig sendender Teilnehmer einer Funkzelle werden im Mobilfunk verschiedene technische Multiplexverfahren („Multiple Access“) eingesetzt.

Bei Code Division Multiple Access-Verfahren (CDMA) werden die Funkübertragungen der Teilnehmer einer Funkzelle durch Zuweisung verschiedener mathematischer Codes voneinander getrennt. Alle Teilnehmer einer Funkzelle übertragen gleichzeitig auf der gleichen Frequenz. CDMA wird in den 3G-Mobilfunksystemen UMTS und CDMA2000, welches überwiegend in Amerika und Afrika genutzt wird, eingesetzt.

Sofern die Voraussetzungen gemäß § 3 TKÜV erfüllt und öffentliche Telekommunikationsdienste erbracht werden, sind Vorkehrungen gemäß der Technischen Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation (TR-TKÜV) durch den Betreiber zu treffen, um TKÜ-Maßnahmen umsetzen zu können. Wenn diese Voraussetzungen gegeben sind, ist eine Überwachung durch die Strafverfolgungs- und Ermittlungsbehörden des Bundes grundsätzlich möglich.

Mit Blick auf die Nachrichtendienste des Bundes betrifft die Frage 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 findet seine Grenzen in den gleichfalls Verfassungsrang genießenden schutzwürdigen Interessen des Staatswohls.

Arbeitsmethoden und Vorgehensweisen der Nachrichtendienste des Bundes sind im Hinblick auf deren künftige Aufgabenerfüllung besonders schutzwürdig. Eine Antwort der Bundesregierung auf diese Frage würde spezifische Informationen zur Tätigkeit, insbesondere zur Methodik und den konkreten technischen Fähig-

keiten der Nachrichtendienste des Bundes einem nicht eingrenzbaren Personenkreis nicht nur im Inland, sondern auch im Ausland zugänglich machen. Bereits die Auskunft darüber, ob die genannten Behörden zur Durchführung des beschriebenen Verfahrens im Bereich der informationstechnischen Überwachung befähigt sind, lässt Rückschlüsse auf die Leistungsfähigkeit der Nachrichtendienste des Bundes zu. Dabei würde die Gefahr entstehen, dass ihre bestehenden oder in der Entwicklung befindlichen operativen Fähigkeiten und Methoden aufgeklärt und damit der Einsatzerfolg gefährdet würde. Es könnten entsprechende Abwehrstrategien entwickelt werden. Dies könnte einen erheblichen Nachteil für deren wirksame Aufgabenerfüllung und damit für die Interessen der Bundesrepublik Deutschland bedeuten.

Die vorgenannten Informationen über Tätigkeiten und aktive und ggf. zukünftige Fähigkeiten der Nachrichtendienste des Bundes wären geeignet, die künftige Möglichkeit der betroffenen Behörden zur Gewinnung von Erkenntnissen im Wege der technischen Aufklärung, in erheblicher Weise negativ zu beeinflussen. Die Informationsgewinnung durch technische Aufklärung ist für die Sicherheit der Bundesrepublik Deutschland und für die Aufgabenerfüllung und Funktionsfähigkeit der Nachrichtendienste des Bundes jedoch unerlässlich.

Zur Erstellung möglichst vollständiger Lagebilder und zur Vermeidung von Informationsdefiziten sind die Nachrichtendienste auf die aus der technischen Aufklärung zu generierenden Informationen zwingend und zunehmend angewiesen. Diese stellen einen unentbehrlichen Beitrag zum Informationsaufkommen dar. Das sonstige Informationsaufkommen der Nachrichtendienste des Bundes wäre auch nicht ausreichend, um ein vollständiges Lagebild zu erhalten und Informationsdefizite im Bereich der technischen Aufklärung zu kompensieren.

Insofern birgt eine Offenlegung der angefragten Informationen die Gefahr, dass Einzelheiten zur konkreten Methodik und zu aus den vorgenannten Gründen im hohen Maße schutzwürdigen spezifischen technischen Fähigkeiten bekannt würden. Infolgedessen könnten sowohl staatliche als auch nichtstaatliche Akteure Rückschlüsse auf spezifische Vorgehensweisen und technische Fähigkeiten der Nachrichtendienste des Bundes sowie die Entwicklung derselben in den vergangenen Jahren gewinnen. Diese Kenntnisse würden es ihnen ermöglichen, ihr Kommunikationsverhalten so zu verändern, dass eine zukünftige Erhebung dieser Daten zumindest erschwert und in vielen Fällen in Gänze vereitelt werden würde. Dies wiederum würde folgenschwere Einschränkungen der Informationsgewinnung bedeuten, wodurch letztlich der gesetzliche Auftrag der Nachrichtendienste des Bundes nicht mehr sachgerecht erfüllt werden könnte. Sofern derartige Informationen wegfallen oder wesentlich zurückgehen sollten, würden empfindliche Informationslücken im Hinblick auf die Sicherheitslage der Bundesrepublik Deutschland drohen. Damit wäre das Staatswohl der Bundesrepublik Deutschland gefährdet.

Eine VS-Einstufung und Weiterleitung der angefragten Informationen an die Geheimschutzstelle des Deutschen Bundestages kommt angesichts ihrer erheblichen Brisanz im Hinblick auf die Bedeutung der technischen Aufklärung für die Aufgabenerfüllung der Nachrichtendienste des Bundes nicht in Betracht. Auch ein geringfügiges Risiko des Bekanntwerdens derart sensibler Informationen kann unter keinen Umständen hingenommen werden. Die angefragten Inhalte beschreiben die technischen Fähigkeiten der Nachrichtendienste des Bundes in einem Detaillierungsgrad, dass eine Bekanntgabe auch gegenüber einem begrenzten Kreis von Empfängern ihrem Schutzbedürfnis nicht Rechnung tragen kann. Dies gilt umso mehr, als sie Spezifika betreffen, deren technische Umsetzung nur

in einem bestimmten Verfahren erfolgen kann. Bei einem Bekanntwerden der schutzbedürftigen Information wäre kein Ersatz durch andere Instrumente möglich.

Aus dem Vorgesagten ergibt sich, dass die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht wesentlich überwiegt und einer Beantwortung der Kleinen Anfrage im Hinblick auf die Nachrichtendienste des Bundes im aktuellen Fall sowie (bei gleichlautender Anfrage und unverändertem Sachverhalt) in Zukunft entgegensteht. Insofern muss ausnahmsweise das Fragerecht der Abgeordneten gegenüber dem Geheimhaltungsinteresse der Bundesregierung zurückstehen.

7. Inwiefern bzw. mit welchen Einschränkungen können deutsche Sicherheitsbehörden die Abhörmöglichkeiten oder Schnittstellen zur Ausleitung von Telekommunikationsdaten, die hinsichtlich der Standards 4G, 3G bzw. 2G genutzt werden, für 5G weiter verwenden?

In der TR-TKÜV werden die Schnittstellen zur Ausleitung der überwachten Telekommunikation beschrieben. Die Verfahren sind grundsätzlich dafür geeignet, auch Telekommunikation aus 5G-Netzen an die berechtigten Stellen auszuleiten. Bei 5G ist mit einer wesentlich höheren Datenrate an den Dateneingangsschnittstellen zu rechnen. Die Schnittstellen werden daher voraussichtlich hard- und softwaretechnisch anzupassen sein.

8. Inwiefern trifft es aus Sicht der Bundesregierung zu, dass IMSI-Catcher unter 5G sämtlich nicht mehr nutzbar sind?

   a) Welche konkreten Informationen (etwa Inhalte, Zeit und Dauer des Gesprächs, Angerufene, IMSI- und IMEI-Nummer) sind mit den von Bundesbehörden genutzten IMSI-Catchern nicht mehr zu überwachen?

   b) Auf welche Weise können deutsche Behörden auch mit 5G an die „International Mobile Subscriber Identity“-Nummern (IMSI) der Telefone gelangen?

   c) Welche IMSI-Catcher kennt die Bundesregierung, die auch eine Überwachung von 5G-Telefonie ermöglichen?

   d) Welche Förderung oder Auftragsvergabe im Bereich der Forschung und Entwicklung von IMSI-Catchern gab es durch den Bund seit 2014?

Nach Maßgabe der Ausführungen in der Vorbemerkung der Bundesregierung wird auf den als Verschlusssache mit dem Geheimhaltungsgrad „VS – Nur für den Dienstgebrauch“ versehenen Antwortteil verwiesen.

9. Welche deutschen Behörden nehmen an Sitzungen des European Telecommunications Standards Institute (ETSI) und der Arbeitsgruppe „Strafverfolgung“ (SA3-LI) im 3rd Generation Partnership Project (3GPP) teil, bzw. welche Änderungen haben sich seit Beantwortung der Bundestagsdrucksachen 18/7466 und 17/11239 ergeben?

In den Arbeitsgruppen ETSI TC LI und 3GPP SA3 LI nehmen derzeit die folgenden Bundesbehörden teil:

– Bundeskriminalamt,

– Bundesamt für Verfassungsschutz,

– Bundesnetzagentur.

Seit Juli 2019 hat auch die Zentrale Stelle für Informationstechnik im Sicherheitsbereich teilgenommen.

Nach Kenntnis der Bundesregierung nehmen an Sitzungen der Arbeitsgruppe ETSI TC LI auch das Bayerische Landeskriminalamt und das Landeskriminalamt Niedersachsen teil.

a) Welche Arbeitsgruppentreffen (Plenary) und Rapporteurs-Sitzungen der Gruppe „Strafverfolgung“ (TC LI) des ETSI sowie der Arbeitsgruppe „Strafverfolgung“ des 3GPP haben nach Kenntnis der Bundesregierung im Jahr 2018 und 2019 stattgefunden, und wo wurden diese jeweils abgehalten?

Für die Arbeitsgruppe ETSI TC LI haben die nachfolgenden Treffen seit Januar 2018 stattgefunden:

ETSI TC LI#47 Plenary: 05.02.2018 - 07.02.2018, New Delhi, IND

ETSI TC LI-Rap#43 Rapporteurs: 14.03.2018 - 15.03.2018, Heathrow, GBR

ETSI TC LI#48 Plenary: 26.06.2018 - 28.06.2018, Bergen, NOR

ETSI TC LI-Rap#44 Rapporteurs: 29.08.2018 - 30.08.2018, Belfast, GBR

ETSI TC LI#49 Plenary: 25.09.2018 - 27.09.2018, Zagreb, HRV

ETSI TC LI-Rap#45 Rapporteurs: 10.12.2018 - 12.12.2018, Berlin

ETSI TC LI#50 Plenary: 05.02.2019 - 07.02.2019, Dubai, UAE

ETSI TC LI-Rap#46 Rapporteurs: 13.03.2019 - 14.03.2019, Heathrow, GBR

ETSI TC LI-Rap#47 Rapporteurs: 20.05.2019 - 21.05.2019, Rotterdam, NLD

ETSI TC LI#51 Plenary: 11.06.2019 - 13.06.2019, Texel, NLD

ETSI TC LI-Rap#48 Rapporteurs: 10.07.2019 - 11.07.2019, Mainz

Für die Arbeitsgruppe 3GPP SA3 LI haben die nachfolgenden Treffen seit Januar 2018 stattgefunden:

3GPP SA3 LI #68: 30.01. – 02.02.2018, New Delhi, IND

3GPP SA3 LI #69: 10.04. – 13.04.2018, Newport Beach, USA

3GPP SA3 LI #69-BIS: 14.05. – 15.05.2018, Sophia Antipolis, FRA

3GPP SA3 LI #70: 17.07. – 20.07.2018, Lecce, ITA

3GPP SA3 LI #70-BIS: 01.10. – 03.10.2018, Sophia-Antipolis, FRA

3GPP SA3 LI #71: 30.10. – 02.11.2018, Newport Beach, USA

3GPP SA3 LI #72: 22.01. – 25.01.2019, Sophia-Antipolis, FRA

3GPP SA3 LI #72-BIS: 26.02. – 28.02.2019, Düsseldorf

3GPP SA3 LI #73: 09.04. – 12.04.2019, La Jolla, USA

3GPP SA3 LI #74: 16.07. – 19.07.2019, Breslau, PLN

b) Welche Mitglieder der TC LI oder der SA3-LI haben nach Kenntnis der Bundesregierung die Arbeitsgruppentreffen (Plenary) und Rapporteurs-Sitzungen vorbereitet, und wer war für die Tagesordnung sowie die Organisation zuständig?

Die Tagesordnung wird in beiden Arbeitsgruppen vom jeweiligen Chairman auf Grundlage der eingereichten Beiträge erstellt. Die Organisation wird innerhalb ETSI TC LI und 3GPP SA3 LI von den jeweils zuständigen Sekretären übernommen.

c) Wer nahm an diesen Treffen teil (bitte wie auf Bundestagsdrucksache 17/11239 beantworten)?

Die Teilnehmerlisten stehen grundsätzlich nur Mitgliedern zur Verfügung und sind mit Blick auf die Persönlichkeitsrechte der Betroffenen nicht zur Weitergabe vorgesehen.

10. Welche konkreten Punkte standen nach Kenntnis der Bundesregierung jeweils auf der Tagesordnung von Treffen der TC LI oder der SA3-LI in den Jahren 2018 und 2019, und welche Dokumente wurden hierfür im Vorfeld oder am Tag der Treffen verteilt?

Was war der Inhalt der Tagesordnung?

Die jeweiligen Tagesordnungen zu den Sitzungen von 3GPP sowie zugehörige Dokumente sind unter dem angegeben Link auf der Homepage von 3GPP einsehbar: www.3gpp.org/dynareport/Meetings-S3.htm?Itemid=451 (zuletzt aufgerufen am 17. Juli 2019).

Eine Veröffentlichung der vergleichbaren Dokumente im Rahmen der ETSI-Zusammenarbeit erfolgt nicht. Vielmehr stehen die Tagungsdokumente nur den Mitgliedern zur Verfügung und sind nicht zur Veröffentlichung bestimmt.

a) Welche ILETS-Sitzungen haben hierzu im Vorfeld stattgefunden, und welche Bundesbehörden beteiligten sich daran?

Im Zeitraum Januar 2018 bis Juli 2019 fanden vier ILETS-Tagungen statt. Teilnehmer an diesen Sitzungen waren Vertreter des BKA, des BfV und der BNetzA. ILETS-Sitzungen finden turnusmäßig und ohne Bezug zu konkreten Standardisierungsgruppen oder -sitzungen statt.

b) Welche technischen Lösungen und Lösungsansätze unter Berücksichtigung verschiedener nationaler Gesetzgebungen wurden hinsichtlich von Schnittstellen zum Abhören von 5G bzw. der Nutzung von IMSI-Catchern bzw. vergleichbarer Verfahren in den ILETS-Gruppen, der TC LI und der SA3-LI vorgestellt und/oder diskutiert (bitte erläutern)?

Anlässlich der jeweiligen Sitzungen wurde zu den aktuellen Sachständen aus den Standardisierungsgremien von 3GPP und ETSI berichtet. Innerhalb der ILETS-Sitzungen wurden keine konkreten Lösungen bezüglich 5G vorgestellt und/oder diskutiert.

Die Nutzung von IMSI-Catchern liegt nicht in der Zuständigkeit der Standardisierungsgruppen ETSI TC LI und 3GPP SA3 LI.

11. Inwiefern haben sich das ZKA oder das BfV hinsichtlich der Standardisierung von 5G in den ILETS-Gruppen, der TC LI und der SA3-LI mit dem BKA abgestimmt?

Eine Bedarfsabstimmung der berechtigten Stellen zur Standardisierung von 5G findet regelmäßig statt.

Das Zollkriminalamt nimmt an den Sitzungen der genannten Gruppen nicht teil. Eine spezielle Abstimmung mit dem BKA zum Thema „Standardisierung von 5G“ im Vorfeld der Sitzungen erfolgte deshalb nicht.

a) Welche eigenen Diskussionspapiere oder Vorschläge zu Herausforderungen von 5G oder Lösungsmöglichkeiten haben deutsche Behörden in den ILETS-Gruppen, der TC LI und der SA3-LI verteilt?

Die teilnehmenden Behörden berichten regelmäßig zu Themen, die in Bezug zu den jeweiligen Sitzungen stehen. Durch das BKA und BfV wurden in TC LI und SA3 LI keine konkreten Diskussionspapiere erarbeitet oder verteilt.

b) Welche Berichte (Technical Reports) zu Möglichkeiten der Überwachung von 5G wurden nach Kenntnis der Bundesregierung in ILETS-Gruppen, der TC LI und der SA3-LI erstellt?

ETSI TC LI arbeitet derzeit an TR 103 656 „Study on high bandwidth delivery“ und 3GPP SA3 LI arbeitet derzeit an TR 33.842 „Study on lawful interception (LI) service in 5G“. Beide Dokumente befinden sich im Entwurfsstadium.

Sobald die Dokumente finalisiert sind, ist nach Kenntnis der Bundesregierung beabsichtigt, diese auf der jeweiligen Internetpräsenz von 3GPP bzw. ETSI zu veröffentlichen (3GPP: www.3gpp.org/specifications; ETSI: www.etsi.org/standards#Pre-defined%20Collections; zuletzt aufgerufen am 17. Juli 2019).

12. Wann sollen die nächsten Versionen des Standards zu 5G nach Kenntnis der Bundesregierung vom ETSI bzw. dem 3GPP veröffentlicht werden (Release #16), und welche technischen Spezifikationen zu Überwachungsmöglichkeiten stehen jetzt schon fest bzw. welche sollen nicht mehr verhandelt oder geändert werden (vgl. Ratsdokument 8983/19)?

    Werden bis zur Veröffentlichung nur noch Fehlerkorrekturen vorgenommen?

Innerhalb 3GPP wurden bisher die Spezifikationen 3GPP TS 33.126 (Release 16) und 3GPP TS 33.127 (Release 16) mit Bezug zu 5G veröffentlicht. Die Überarbeitung der Spezifikation 3GPP TS 33.128 (Release 15) erfolgt derzeit. Die Spezifikationen werden entsprechend der Standardisierung neuer Funktionalitäten weiterentwickelt und unterliegen einer grundsätzlichen Fehlerkorrektur. Release #16 soll laut dem Release-Plan von 3GPP bis Ende 2019 finalisiert werden. Die dazugehörige Evaluation soll im März 2020 abgeschlossen werden.

ETSI erarbeitet keine Standards zu Überwachungsmöglichkeiten mit Bezug zu 5G, da die Zuständigkeit für die Erarbeitung der Standards zu 5G bei 3GPP liegt. Allerdings bestehen zwischen 3GPP und ETSI Kooperationen. In diesem Rahmen sind Modifizierungen bereits bestehender ETSI-Standards durch ETSI nach Anfrage/Aufforderung von 3GPP möglich, um diese bei der Standardisierung zu 5G durch 3GPP nutzen zu können.

13. Was ist der Bundesregierung über eine 5G-Arbeitsgruppe bei der EU-Polizeiagentur Europol bekannt (Ratsdokument 8983/19), wer nimmt daran teil, und wie oft trifft sich diese?

Im Februar 2019 hat bei Europol ein Expertentreffen "5G" mit Blick auf die Einführung des Mobilfunkstandards 5G und möglicher Auswirkungen auf die TKÜ-Fähigkeiten der Sicherheitsbehörden unter den EU-Mitgliedstaaten stattgefunden. Eingeladen waren die Leiter und stellvertretenden Leiter der für Telekommunikationsüberwachung zuständigen Organisationseinheiten bei den Strafverfolgungsbehörden der EU-Mitgliedstaaten. Eine zweite Expertensitzung zum Thema fand im Juni 2019 statt.

a) Was ist der Bundesregierung darüber bekannt, inwiefern Europol bereits an Treffen der ILETS-Gruppen, der TC LI und der SA3-LI teilnahm oder diese indirekt (etwa über das BKA oder das BfV) inhaltlich mitbestimmt hat?

Nach Kenntnis der Bundesregierung hat Europol an keiner Sitzung der genannten Gruppen teilgenommen.

b) Welche Haltung vertritt die Bundesregierung zum Vorschlag des EU-Koordinators für Terrorismusbekämpfung, dass Europol Mitglied des ETSI werden könnte, um darüber Einfluss auf die dort oder bei 3GPP angesiedelten Arbeitsgruppen „Strafverfolgung" zu nehmen?

Ein Engagement der Strafverfolgungsbehörden und damit auch von Europol bei ETSI und 3GPP wird von der Bundesregierung befürwortet.

14. Welche konkreten Mitarbeiterinnen und Mitarbeiter des BKA oder anderer Behörden beraten hierzu mit Europol, und inwiefern handelt es sich dabei um „heads of telecommunications interception units“ (Ratsdokument 8983/19)?

Eingeladen zu dem Expertentreffen waren die Leiter und stellvertretenden Leiter der für Telekommunikationsüberwachung zuständigen Organisationseinheiten bei den Strafverfolgungsbehörden der EU-Mitgliedstaaten. Für Deutschland erfolgte die Teilnahme durch Vertreter des BKA.

a) Welche „Informationen zu möglichen Auswirkungen von 5G auf die Aufgabenwahrnehmung der Sicherheitsbehörden“ hat das BKA dem EU-Koordinator für Terrorismusbekämpfung zur Verfügung gestellt?

b) Welche wesentlichen Bestandteile dieser BKA-Informationen sind aus Sicht der Bundesregierung in das Diskussionspapier des EU-Koordinators für Terrorismusbekämpfung eingeflossen (Ratsdokument 8983/19)?

Die Fragen 14a und 14b werden aufgrund des Sachzusammenhangs zusammen beantwortet.

Die im Diskussionspapier des EU-Koordinators für Terrorismusbekämpfung dargestellten Informationen zur Einführung von 5G und den Auswirkungen auf die TKÜ-Fähigkeiten der Sicherheitsbehörden geben im Wesentlichen die dem BKA und den europäischen Partnerdienststellen vorliegenden Informationen wieder.

c) Haben das BKA oder Europol Gespräche hinsichtlich der Standardisierung von 5G oder ETS nach Kenntnis der Bundesregierung mit den Netzbetreibern Ericsson und Nokia geführt?

Wenn ja, wie viele, und was waren die konkreten Gesprächsgegenstände?

Das BKA hatte keine Gesprächstermine mit den Unternehmen Ericsson und Nokia. Ob etwaige Gespräche von Europol mit beiden Firmen geführt wurden, ist der Bundesregierung nicht bekannt.

15. Welche Vorgaben plant die Bundesregierung bei der Vergabe von 5G-Lizenzen für die Netzbetreiber hinsichtlich der Implementierung von Schnittstellen zum Abhören oder Ausleiten von Kommunikation, der Einrichtung zentraler Kommunikationsknoten, der Fragmentierung des Netzes oder dem Grad der Verschlüsselung?

a) Sollen die Firmen eine komplette und entschlüsselte Kopie der Kommunikation bereithalten und/oder Schnittstellen hierfür einrichten?

b) Sollen die Firmen ihre Netzwerke so organisieren, dass jederzeit Geodaten zur Lokalisierung der Telefone protokolliert werden?

c) Sollen die Firmen dafür Sorge tragen, dass weiterhin IMSI-Catcher eingesetzt werden können?

Die Fragen 15 bis 15c werden wegen Sachzusammenhangs gemeinsam beantwortet.

Die Versteigerung von 5G-Frequenzen ging am 12. Juni 2019 zu Ende. Mit der Vergabe waren keine speziell für die 5G-Lizenzen vorgesehenen besonderen Vorgaben hinsichtlich der Telekommunikationsüberwachung verknüpft. Für die Betreiber von Telekommunikationsnetzen, mit denen öffentlich zugängliche Tele-

kommunikationsdienste erbracht werden, und die Erbringer von öffentlich zugänglichen Telekommunikationsdiensten gelten – unabhängig von der zugrundeliegenden Technologie – hinsichtlich der Telekommunikationsüberwachung die diesbezüglichen Regelungen des Telekommunikationsgesetzes und der Telekommunikations-Überwachungsverordnung.

Die Bundesregierung prüft derzeit, welche technischen und rechtlichen Anpassungen erforderlich sind, um zu gewährleisten, dass die Sicherheitsbehörden auch vor dem Hintergrund der Einführung des 5G-Standards ihren gesetzlichen Aufgaben nachkommen können (vgl. Antwort der Bundesregierung auf die Schriftliche Frage 18 auf Bundestagdrucksache 19/10535).

16. Auf welche Weise könnte die Europäische Union aus Sicht der Bundesregierung die Bedürfnisse der Sicherheitsbehörden nach Abhörmöglichkeiten bei der Standardisierung von 5G unterstützen (vgl. Ratsdokument 8983/19)?

a) Welche Ratsarbeitsgruppen sind nach Kenntnis der Bundesregierung derzeit mit der Überwachung von 5G befasst, und welche ist hierzu federführend, und wer sitzt dort von Seiten der Bundesregierung?

Die Fragen 16 und 16a werden gemeinsam beantwortet.

Hierzu liegen der Bundesregierung keine Erkenntnisse vor.

b) Welche Unterstützung leisten nach Kenntnis der Bundesregierung die Agentur der Europäischen Union für Cybersicherheit (ENISA) oder das Gremium Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK) hinsichtlich der Bedürfnisse der Sicherheitsbehörden nach Abhörmöglichkeiten bei der Standardisierung von 5G und ETS?

Das Gremium Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK) befasst sich nach Kenntnis der Bundesregierung nicht mit Bedürfnissen der Sicherheitsbehörden bei der Standardisierung von 5G.

c) Sollte die Überwachung von 5G-Telefonie aus Sicht der Bundesregierung in die geplanten EU-Verordnungen zur Sicherung und Herausgabe elektronischer Beweismittel aufgenommen werden oder ist diese davon aus ihrer Sicht bereits umfasst?

Der Entwurf einer Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen ist diensteanbieter- und datenkategoriebezogen und knüpft hinsichtlich der Anwendungsvoraussetzungen nicht an spezifische Übertragungsstandards an. Die Bundesregierung geht daher derzeit davon aus, dass auch mittels 5G übertragene Daten in den Anwendungsbereich des Verordnungsentwurfs fallen.

Der Verordnungsentwurf betrifft jedoch nur Maßnahmen von Strafverfolgungsbehörden im Wege der Europäischen Herausgabe- und Sicherungsanordnungen und eröffnet damit nicht die Möglichkeit einer Echtzeitüberwachung.

17. Welche Position vertritt die Bundesregierung im ETSI hinsichtlich der Bereitstellung einer „Cloud Lawful Interception Function“ für Polizeien und Geheimdienste (Bundestagsdrucksache 17/11239, Frage 16)?

Auf die Antwort der Bundesregierung zu Frage 16 auf Bundestagsdrucksache 17/11239 wird verwiesen.

a) Inwieweit befassen sich die ILETS-Gruppen, die TC LI und die SA3-LI nach Kenntnis der Bundesregierung auch mit dem Zugriff von Polizeien und Geheimdiensten auf Cloud-Daten, und welche Standardisierungen wurden hierzu verabredet oder diskutiert?

ETSI TC LI hat zu dieser Thematik die Studie TR 101 567 „Cloud / Virtual Services for Lawful Interception (LI) and Retained Data (RD)“ erarbeitet.

b) Welche der hierzu in der Vergangenheit diskutierten Standards zur Überwachung von Clouddaten, die in einem Draft Technical Report veröffentlicht wurden, sind nach Kenntnis der Bundesregierung in Deutschland umgesetzt?

Nach Kenntnis der Bundesregierung wurden bisher keine der genannten Standards umgesetzt.

18. Welche Bedeutung misst die Bundesregierung der vom Massachusetts Institute of Technology vorgenommen Einstufung des vom ETSI entwickelten Protokolls Enterprise Transport Security (ETS) als Schwachstelle bei („Transport-Verschlüsselung: ETS aka eTLS ist laut MITRE-Schwachstellenliste ein Bug“, www.heise.de vom 12. Juni 2019), und wird sie sich deshalb für den Verschlüsselungsstandard TLS 1.3 einsetzen?

MITRE führt die von ETSI entwickelte TLS-Variante ETS (ursprünglich eTLS genannt) als Schwachstelle. Dies wird damit begründet, dass ETS im Gegensatz zu TLS 1.3 keine Perfect Forward Secrecy (PFS) bietet. PFS zählt bei kryptographischen Protokollen heute zum Stand der Technik, ist jedoch nicht in allen Konfigurationen verbreiteter Protokolle enthalten (darunter auch bestimmte Konfigurationen von TLS 1.2 und TLS 1.3). Protokolle ohne PFS als Schwachstelle zu bezeichnen entspricht nach Kenntnis der Bundesregierung nicht dem allgemeinen Sprachgebrauch.

Das BSI empfiehlt in der „Technischen Richtlinie TR-02102-2 (Kryptographische Verfahren: Empfehlungen und Schlüssellängen – Teil 2 - Verwendung von Transport Layer Security (TLS)), Version 2019-01“ die von der IETF standardisierten TLS-Versionen 1.2 und 1.3 mit geeigneten Cipher-Suiten. Dabei werden grundsätzlich Cipher-Suiten mit PFS empfohlen, es werden aber auch Empfehlungen für Cipher-Suiten ohne der PFS-Eigenschaft gegeben, wenn der Einsatz von PFS-Verfahren nicht möglich ist. Der „Mindeststandard des BSI zur Verwendung von Transport Layer Security (TLS), Version 2.0“ macht TLS 1.2 mit PFS oder TLS 1.3 mit PFS für die Bundesverwaltung verpflichtend.

19. Mit welchen Behörden nimmt die Bundesregierung an der „Internet Engineering Task Force“ (IETF) teil, die sich mit der sicheren Verschlüsselung in zukünftigen Kommunikationsstandards befasst?

Für die Bundesregierung nehmen Vertreter der Bundesnetzagentur an der „Internet Engineering Task Force“ (IETF) teil.

20. Wer nimmt an den auf Bundestagsdrucksache 19/10803, Antwort zu Frage 5 genannten Projekten des Forschungsinstituts Cyber Defence (CODE) an der Universität der Bundeswehr München im Handlungsfeld „Künstliche Intelligenz“ teil, und wann sollen die Ergebnisse vorliegen?

Bei den auf Bundestagsdrucksache 19/10803, Antwort zu Frage 5 benannten Projekten des ressorteigenen Forschungsinstituts CODE an der Universität der Bundeswehr München handelt es sich um laufende Forschungsschwerpunkte und Forschungsgebiete, die im Rahmen der allgemeinen universitären Forschungsaufgabe durch Wissenschaftlerinnen und Wissenschaftler am Forschungsinstitut CODE wahrgenommen werden. Eine Berichterstattung über etwaige Ergebnisse erfolgt in Abhängigkeit des erzielten Forschungsfortschritts.

21. Welche Rahmenbedingungen existieren heute, um eine „aktive Cyber-Abwehr“ zu gestalten, und welche weiteren Rahmenbedingungen wären nötig, um diese auszubauen (http://gleft.de/2Ye, bitte ausführen, welche Haltung das Bundesministerium der Verteidigung bzw. dessen Generalleutnant Ludwig Leinhos hierzu vertritt)?

Zur Beantwortung wird auf die Vorbemerkung der Bundesregierung und die Antwort zu Frage 1 der Kleinen Anfrage der Fraktion der FDP auf Bundestagsdrucksache 19/2645 verwiesen.

22. Welche Cybersicherheitsrisiken sind der Bundesregierung in 5G-Netzen bekannt, und wie werden diese von der Europäischen Kommission konkret adressiert (vgl. Empfehlung 2019/534 der Kommission vom 26. März 2019 zur Cybersicherheit der 5G-Netze)?

a) Welche Risiken von 5G-Netzen hat die Bundesregierung auf nationaler Ebene identifiziert?

Die Fragen 22 und 22a werden wegen Sachzusammenhangs gemeinsam beantwortet.

Die Risiken von 5G-Netzen orientieren sich derzeit an den Risiken, die auch bei bestehenden Netzen (2G/3G/4G) anzunehmen sind. Die Verfügbarkeit und Integrität der Netze sowie die Integrität und Vertraulichkeit der übermittelten Daten und anfallenden Metadaten stehen, neben dem Schutz personenbezogener Daten, im Fokus der Risikobetrachtungen.

b) Mit welchen EU-Institutionen trifft die Bundesregierung eine gemeinsame Risikoeinschätzung, und wie bringt sie sich hierzu auf EU-Ebene ein?

Das BSI ist über das BMI an dem Prozess beteiligt, der in der Empfehlung 2019/534 der Kommission vom 26. März 2019 beschrieben ist. Dieser sieht regelmäßige Treffen der Kooperationsgruppe nach Artikel 11 der Richtlinie (EU) 2016/1148 („NIS-Richtlinie“) vor, hier im Work Stream „5G“.

23. Welche Maßnahmen unternimmt nach Kenntnis der Bundesregierung die Kooperationsgruppe für Netz- und Informationssicherheit (NIS), um die Risiken für die „Infrastrukturen, die dem digitalen Ökosystem zugrunde liegen“ – insbesondere 5G Netze – abzuschwächen (vgl. Empfehlung 2019/534 der Kommission vom 26. März 2019 zur Cybersicherheit der 5G-Netze)?

Auf Basis des in der Antwort zu Frage 22b dargestellten Arbeitsprozesses soll in der Kooperationsgruppe nach Artikel 11 NIS-Richtlinie als Ausfluss der gemeinsamen Risikobewertung auf europäischer Ebene die Entwicklung eines Werkzeugkastens („tool box“) auf der Basis von „best practices“ der MS vorangetrieben werden. Dieser Werkzeugkasten soll durch darin enthaltene Lösungsansätze einen Beitrag dazu leisten, identifizierte Risiken zu minimieren. Dies soll bis zum 31. Dezember 2019 erfolgen.

24. Welche „sensibelsten Elemente, bei denen Sicherheitsvorfälle [in 5G-Netzen] erhebliche negative Auswirkungen nach sich ziehen würden“, will die Bundesregierung der Europäischen Kommission bis 30. Juni 2019 mitteilen (vgl. Empfehlung 2019/534 der Kommission vom 26. März 2019 zur Cybersicherheit der 5G-Netze)?

Der deutsche Beitrag zur koordinierten europäischen Risikobewertung i. S. d. Empfehlung (EU) 2019/534 der Kommission vom 26. März 2019 zur Cybersicherheit der 5G-Netze ist am 15. Juli 2019 entsprechend Nr. 9 der Empfehlung an die Kommission und die Agentur der Europäischen Union für Cybersicherheit (ENISA) übermittelt worden.

Die Anbieter von Telekommunikationsdiensten und die Betreiber von öffentlichen Telekommunikationsnetzen sind nach § 109 Absatz 1, 2 des Telekommunikationsgesetzes (TKG) verpflichtet, angemessene technische Vorkehrungen und sonstige Maßnahmen zu treffen zum Schutz gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen und -diensten führen, und zur Beherrschung der Risiken für die Sicherheit von Telekommunikationsnetzen und -diensten. Insbesondere sind Maßnahmen gegen unerlaubte Zugriffe vorzusehen.

Die BNetzA hat am 7. März 2019 die Eckpunkte für eine Erweiterung des Katalogs an Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten veröffentlicht. Sie wurden im Einvernehmen mit dem BSI und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) entwickelt.

Im Rahmen ihrer Sicherheitskonzepte müssen Unternehmen zukünftig die erweiterten Sicherheitsanforderungen erfüllen. Das gilt insbesondere auch für den anstehenden Ausbau des 5G-Netzes in Deutschland, das eine zentrale kritische Infrastruktur für Zukunftstechnologien darstellt.

Angesichts der Bedeutung von 5G für die künftige Wettbewerbsfähigkeit des Standortes muss die Technik, die beim Ausbau von 5G zum Einsatz kommt, höchste Sicherheitsstandards erfüllen. Sicherheitsbedenken müssen so weit wie möglich ausgeschlossen werden. Das gilt für die eingesetzte Hard- und Software gleichermaßen.

In den veröffentlichten Eckpunkten ist bereits vorgesehen, dass sicherheitsrelevante Netz- und Systemkomponenten (kritische Kernkomponenten) nur nach einer geeigneten Abnahmeprüfung bei Zulieferung eingesetzt werden dürften und regelmäßig und kontinuierlich Sicherheitsprüfungen unterzogen werden müssten. Die Definition der sicherheitsrelevanten Komponenten (kritische Kernkomponenten) wird einvernehmlich zwischen BNetzA und BSI erfolgen.

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