Stellungnahme von Telefónica Deutschland zum Diskussionsentwurf eines zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG 2.0)
Stand: 24. Februar 2021

Telefónica Deutschland (im weiteren Telefónica) ist mit 43,5 Millionen Mobilfunkanschlüssen und 2,2 Millionen Breitbandanschlüssen einer der führenden integrierten Telekommunikationsanbieter in Deutschland. Das Unternehmen bietet Mobilfunk- und Festnetzdienste für Privat- und Geschäftskunden an und betreibt eine eigene Mobilfunkinfrastruktur, die derzeit aus etwa 26.000 Mobilfunkstandorten sowie einem hochleistungsfähigen Verbindungs- und Kernnetz besteht. In den kommenden Jahren plant Telefónica, jährlich rund 1,3 Milliarden Euro in digitale Infrastruktur in Deutschland zu investieren.[1]

Telefónica begrüßt vor dem Hintergrund der aktuellen Bedeutung von Telekommunikationsnetzen für Wirtschaft und Gesellschaft in Deutschland eine steigende Sensibilität für Fragen der IT-Sicherheit.

Vor allem im Zuge der anstehenden Verabschiedung der NIS2 Richtlinie und der zwingenden Notwendigkeit eines stärker harmonisierten und zukunftsorientierten Cybersicherheitsrahmens auf europäischer Ebene weisen wir im Zusammenhang mit der nun diskutierten nationalen Regulierung jedoch ausdrücklich auf die Entwicklung und Umsetzung europaweit einheitlicher Standards hin. Vorgaben auf nationaler Ebene sollten zwingend mit den EU-Empfehlungen oder zukünftigen EU-Richtlinien harmonisiert werden.

Im vorliegenden Entwurf der Bundesregierung zum IT-Sicherheitsgesetz vom 16.12.2020 ist aus Sicht von Telefónica eine starke einseitige Belastung der betroffenen Mobilfunkunternehmen zu Grunde gelegt. Als Betreiberin einer kritischen Infrastruktur im Sinne des §2 Abs. 10 BSIG ist Telefónica unmittelbar von der geplanten Gesetzesänderung des IT-SiG 2.0 betroffen. Teile des vorliegenden Entwurfs der Bundesregierung haben Einfluss auf den Betrieb und Ausbau der digitalen Infrastruktur und die Geschäftstätigkeit von Telefónica.

In der vorliegenden Stellungnahme legt Telefónica einen Fokus auf ausgewählte Aspekte des Gesetzentwurfs und verweist im Übrigen auf die ausführlichen Stellungnahmen der Verbände Bitkom und VATM, zu deren Mitgliedern Telefónica zählt.

Im Speziellen legt Telefónica den Fokus dieser Kurzstellungnahme auf folgende Aspekte:

- **Massive rechtliche und ökonomische Risiken für die Betreiber von kritischen Infrastrukturen:** Sämtliche Folgen, die eine Untersagung der Nutzung einzelner Komponenten gemäß § 9b Abs. 3 BSIG-E hätte, sind im vorliegenden Gesetzentwurf nicht geregelt. Dringend erforderlich ist für das Szenario einer Untersagung eine Regelung, die eine mindestens fünfjährige Übergangsphase für den Rückbau und Austausch einzelner Komponenten vorsieht. Auch eine bisher gänzlich fehlende Regelung des Schadensersatzes sollte in das Gesetz aufgenommen werden. Es darf nicht sein, dass Betreiber, die in Deutschland private Mittel in den Ausbau kritischer Infrastrukturen investieren, den ökonomischen Schaden zu tragen haben, wenn der Bund aufgrund einer politischen Entscheidung Lieferanten dieser Betreiber als nicht vertrauenswürdig einstuft. Vor allem, wenn die infrage kommenden Komponenten zuvor durch eine Bundesbehörde geprüft und zertifiziert worden sind, der Betreiber der kritischen Infrastruktur also unverschuldet einen Schaden erleidet. Hier sollte im Falle einer potenziellen Untersagungsentscheidung dringend eine Kompensationsregelung gefunden werden, um einen stabilen Weiterbetrieb der Mobilfunknetze zu gewährleisten.
- **Keine Rechtssicherheit, da wesentliche Entscheidungen an Behörden ausgelagert werden:** Wesentliche Entscheidungen im Regime der Untersagung der Nutzung einzelner Komponenten würde der Gesetzgeber

[1] Weitere Fakten und Kennzahlen von Telefónica Deutschland finden Sie unter www.telefonica.de/unternehmen.html

mit dem vorliegenden Entwurf an die Verwaltung übertragen. Von den Anforderungen an die Garantieerklärung über die Liste kritischer Komponenten bis hin zum gesamten Ablauf und Inhalt des Zertifizierungsverfahrens sollen letztlich Behörden über Verordnungen, Verfügungen und Richtlinien das Sagen haben. Der vorliegende Gesetzentwurf bietet daher nicht die Rechtssicherheit, die für Betreiber kritischer Infrastrukturen dringend erforderlich wäre.

- **Bestandsnetze dürfen nicht von neuer Regulierung erfasst sein:** Es fehlen in dem Gesetzentwurf wichtige Überleitungsvorschriften, die festlegen, dass der Regulierungsmechanismus sowie die Folgen des § 9b BSIG-E nur für Komponenten angewendet werden, deren Nutzung zukünftig beim BMI angezeigt wird. Eine Rückwirkung auf Bestandsnetze muss schon aus Gründen des Investitions- und Vertrauensschutzes dringend ausgeschlossen werden.
- **Fehlende Rechtsfolgen:**

Im Einzelnen

1. Ausweitung der Aufgaben des BSI, § 3 BSIG-E

Der Gesetzentwurf intendiert die Einführung eines Parallelsystems, bei dem das BSI für den Bereich IT-Sicherheit mehrere zuvor voneinander getrennte Kompetenzen wie Standardisierung, Prüfung und Zertifizierung sowie typische Aufgaben von Sicherheits- und Strafverfolgungsbehörden gleichzeitig übernehmen soll. Ein derartiges Kompetenzgeflecht schafft unnötige zusätzliche Bürokratie, doppelte und längere Verfahren und verspielt das Potenzial für zügiges Verwaltungshandeln. Es steht zu befürchten, dass die Arbeit des BSI aufgrund des geplanten Wachstums der Behörde zur Innovationsbremse wird. Bürokratie und langsames Verwaltungshandeln würden letztlich zu weniger Rechtssicherheit und in letzter Konsequenz zu erheblichen Verzögerungen beim Ausbau von Netzen mit kritischen Komponenten führen. Telefónica plädiert aus diesen Erwägungen heraus dafür, dass die Aufgaben des BSI gesetzlich auf Schutzziele beschränkt werden.

2. Adressat der Zertifizierungspflicht, § 9 BSIG

Adressaten der Zertifizierungspflicht müssen die Hersteller kritischer Komponenten selbst sein. Dies sollte im IT-Sicherheitsgesetz klar festgelegt werden. Bisher ist im Gesetzesentwurf lediglich geregelt, dass kritische Komponenten von Betreibern nur eingesetzt werden dürfen, wenn eine Garantieerklärung der Hersteller über deren Vertrauenswürdigkeit vorliegt, die Komponente zertifiziert wurde und die Nutzung der Komponente beim BMI angezeigt wurde. Hier scheint der vorliegende Gesetzentwurf darauf zu vertrauen, dass die Betreiber von Infrastrukturen mit kritischen Komponenten die Frage, wer für die Zertifizierung einer Komponente überhaupt verantwortlich ist, auf vertraglicher Ebene mit den Herstellern klären. Da für die Durchführung der Zertifizierung jedoch zwingend die Mitwirkung sowie Dokumentationen und Fachkenntnisse des Herstellers erforderlich sind, sollte die Pflicht einer Zertifizierung klar an den Hersteller adressiert werden. Telefónica regt daher an, eine gesetzliche Regelung zu schaffen, die klarstellt, dass ein Hersteller, der kritische Komponenten in den Verkehr bringt, diese auch zertifizieren lassen muss. Adressat des Zertifizierungs-Regimes sollte nicht der Betreiber sein, sondern der Hersteller!

3. Voraussetzungen für Anmeldung kritischer Komponenten sind nicht hinreichend gesetzlich geregelt, § 9b Abs. 1, 2 BSIG-E

Zahlreiche Voraussetzungen und Definitionen, die für eine rechtssichere Anwendung des § 9b BSIG-E erforderlich sind, sollen später von Behörden auf untergesetzlicher Ebene definiert werden. Dies führt dazu, dass die potenziellen Folgen des § 9b BSIG-E basierend auf dem vorliegenden Entwurf nicht abschließend beurteilt werden können und die Wirksamkeit und Wirkungsweise des Mechanismus auch nach Abschluss des Gesetzgebungsverfahrens jederzeit von den Behörden geändert werden kann, indem einzelne Verordnungen geändert werden. Die Betreiber kritischer Infrastrukturen werden so auch nach

Inkrafttreten des IT-SiG 2.0 weiterhin keine Rechtssicherheit betreffend der Nutzung kritischer Komponenten zu erwarten haben.

Es ist derzeit unbekannt, welche Komponenten tatsächlich als kritische Komponenten im Sinne des Gesetzes anzusehen sind, da eine Liste der Komponenten gemäß § 2 Abs. 13 BSIG-E nachgelagert von BNetzA, BSI und BfDI festgelegt wird. Auch die Anforderungen an die Garantieerklärung sollen nach § 9b Abs. 2 BSIG-E erst zu einem späteren Zeitpunkt im Zuge der Allgemeinverfügung durch das BSI festgelegt werden. Schließlich werden auch Ablauf und Inhalt des zwingend zu durchlaufenden Zertifizierungsverfahrens durch das BSI festgelegt, ohne dass diese schon jetzt bekannt wären, siehe § 9 Abs. 4 BSIG-E. Da all diese Voraussetzungen für die Anmeldung der Nutzung kritischer Komponenten beim BSI im Sinne des § 9b Abs. 1 BSIG-E jedoch zwingend bekannt sein müssen, ist das aktuell vorgesehene Regime der Untersagung stark von Entscheidungen der Behörden und faktischem Verwaltungshandeln abhängig.

Während bei der Erstellung der Liste kritischer Komponenten sowie bei der Ausgestaltung des Zertifizierungsverfahrens für eine Ermächtigung der Behörden sprechen könnte, dass auf diese Weise ein innovationsoffener und technologieneutraler Ansatz in der Gesetzgebung gewählt wird, ist es nicht ersichtlich, warum Anforderungen an die Garantieerklärung nicht von vornherein gesetzlich geregelt werden können. Aus Sicht von Telefónica sollte der Gesetzgeber sich daher nicht davor drücken, über entscheidende Definitionen und Voraussetzungen selbst zu entscheiden.

4. Fehlende Regelung zu den Folgen im Falle einer Untersagung führen zu unverhältnismäßiger Belastung der Betreiber, § 9b Abs. 3, 4 BSIG-E

a. Pflichten des § 9b belasten einseitig die Betreiber

Die Auferlegung sämtlicher Pflichten und Risiken des § 9b BSIG-E auf die Schultern des Betreibers - von der Einholung der Garantieerklärung für kritische Komponenten und deren Administration über die potenziellen betrieblichen und wirtschaftlichen Folgeschäden durch die Einbeziehung von Behörden bis hin zur Untersagung eines Komponenteneinsatzes - ist unverhältnismäßig. Das Vorgehen greift durch die Zwangsvorgaben auch in das EU-Ausschreibungsrecht zu Lasten der betroffenen Unternehmen ein und führt ggf. zu Marktverzerrungen wegen Ungleichbehandlung.

b. Übergangsregelung für den Phase-Out

Für den Fall, dass es aufgrund mangelnder Vertrauenswürdigkeit ultima-ratio zu einer Untersagung der Nutzung einer kritischen Komponente kommt, ist dringend eine Übergangsregelung von mindestens fünf Jahren erforderlich, die einen Rückbau bzw. Austausch der Komponenten ermöglicht, ohne dass der Betrieb und der weitere Ausbau der Infrastruktur dadurch massiv beeinträchtig werden. Neben den angemessenen Übergangsfristen für einen eventuellen Rückbau bereits verbauter Komponenten muss eine Norm für die Risikoübernahme bzw. entsprechende Entschädigungen für die Aufwendungen vorgesehen werden.

c. Kompensationsregelung

Nach der derzeitigen Regelung kann es im Falle einer potenziellen Untersagung zur unverhältnismäßigen Belastung von Betreibern der kritischen Infrastrukturen kommen. Die potenziellen wirtschaftlichen sowie betrieblichen Folgeschäden dürfen auf keinen Fall zu Lasten der Betreiber gehen. Sollte es trotz einer Zertifizierung der Komponenten und einer wirksam erteilten Garantieerklärung dennoch aufgrund einer später festgestellten fehlenden Vertrauenswürdigkeit zu einer politisch beschlossenen Untersagung kommen, sollte eine spezialgesetzliche Regelung die verschuldensabhängige Herstellerhaftung festlegen. Eine solche Regelung allein kann die wirtschaftlichen Risiken der Betreiber jedoch nicht ausreichend kompensieren. Wenn ein Hersteller tatsächlich aufgrund fehlender Vertrauenswürdigkeit de facto vom deutschen Markt ausgeschlossen werden würde, so würde er sich vermutlich binnen kurzer Zeit sehr hohen Schadensersatzforderungen ausgesetzt sehen. Das Risiko der Insolvenz des Herstellers wäre in diesem Fall unkalkulierbar groß, was wiederum zu einem nicht tragbaren Risiko für die Betreiber werden würden. Aus diesem Grund sollte als zweite Stufe, wenn

Schadensersatzansprüche der Betreiber nicht aus einer Herstellerhaftung befriedigt werden können, auch eine Haftung des Staates für die Folgen des Ausschlusses geregelt werden. Nach Ansicht von Telefónica sollte dieser Aspekt dringend unmittelbar im BSIG geregelt werden. Daher wird vorgeschlagen, einen neuen §14b in das Gesetz aufzunehmen, der folgend lauten könnte:

> *§14b Zur Entschädigung verpflichtende Maßnahmen*
>
> *(1) Ein Hersteller, der sich nach § 9b Abs. 4, Abs. 5 als nicht vertrauenswürdig erwiesen hat, ist dem Betreiber zum Ersatz des daraus entstandenen Schadens verpflichtet. Satz 1 kann nicht vertraglich ausgeschlossen werden.*
>
> *(2) Erhält der Betreiber keinen Ersatz für den Schaden nach Abs. 1 oder auf andere Weise, so ist ihm der Schaden zu ersetzen, der infolge einer Inanspruchnahme nach § 9b Abs. 4 entstanden ist, gleichgültig, ob das BMI ein Verschulden trifft oder nicht.*
>
> *(3) Soweit die Entschädigungspflicht wegen rechtmäßiger Maßnahmen der Ordnungsbehörden in anderen gesetzlichen Vorschriften geregelt ist, finden diese Anwendung.*
>
> *(4) Die Entschädigung nach Abs. 2 wird für entgangenen Gewinn und alle Vermögensschäden gewährt, unabhängig davon, ob sie in einem unmittelbaren Zusammenhang mit der zu entschädigenden Maßnahme stehen oder nicht.*
>
> *(5) Hat bei der Entstehung des Schadens ein Verschulden des Betreibers mitgewirkt, so ist das Mitverschulden bei der Bemessung der Entschädigung zu berücksichtigen.*
>
> *(6) Soweit die zur Entschädigung verpflichtende Maßnahme auch eine Amtspflichtverletzung darstellt, bleiben die weitergehenden Ersatzansprüche unberührt.*
>
> *(7) Für die Verjährung des Entschädigungsanspruchs gelten die Bestimmungen des Bürgerlichen Gesetzbuchs über die Verjährung von Schadensersatzansprüchen entsprechend.*
>
> *(8) Entschädigungspflichtig ist die Bundesrepublik Deutschland.*
>
> *(9) Über die Entschädigungsansprüche nach dieser Vorschrift entscheiden im Streitfall die ordentlichen Gerichte.*

Anderenfalls sind die Betreiber, die aus privaten Mitteln die Digitalisierung und die Positionierung Deutschlands als 5G-Leitmarkt vorantreiben, unverhältnismäßig und einseitig belastet.

Analog der Regelung zur Entschädigung der Energiewirtschaft bei der Energiewende sollte für betroffene Mobilfunkunternehmen ein **Netzbetriebs-Stabilitätsfonds** eingerichtet werden, um eine reibungslose, stabile Weiterversorgung sowie den flächendeckenden Ausbau der Mobilfunknetze der nächsten Generation zu gewährleisten. Dies wäre insbesondere dann dringend erforderlich, wenn die von den Folgen der Untersagung negativ betroffenen Betreiber kritischer Infrastrukturen rechtlich und tatsächlich keine Möglichkeit haben, ihren Schaden durch Ansprüche gegenüber den Lieferanten der entsprechenden Komponenten zu kompensieren, beispielsweise weil Lieferanten in Deutschland in Folge des Marktausschlusses insolvent sind.

5. Technische Zertifizierung kritischer Komponenten, § 2 Abs. 13 BSIG-E, § 109 Abs. 2 TKG-E

Grundsätzlich bewertet Telefónica den Ansatz positiv, dass kritische Komponenten einer Zertifizierung unterzogen werden sollen und ist bereit, sich im Dialog mit dem BSI in die Entwicklung und regelmäßige Evaluation des Zertifizierungsverfahrens einzubringen.

Kritische Komponenten bzw. Komponenten mit kritischen Funktionen können i. S. dieses Gesetzes nur dann kritisch sein, wenn ihre Funktionalitäten in Bezug auf die Einsatzumgebung im Falle ihrer Beeinträchtigung den KRITIS-Schutzzielen zuwiderlaufen. Daher sollte die Zertifizierung sich nur auf ausgewählte Elemente des Kernnetzes konzentrieren, da hier die Datenströme aus dem Zugangsnetz zusammenlaufen sowie zentrale Netzfunktionalitäten und Datenbanken angesiedelt sind, wodurch diese primär zum Ziel eines Angriffs werden

könnten. Eine Einbeziehung der Zugangsnetze dürfte Zertifizierungsverfahren und Vertrauenswürdigkeitsprüfung zu einem Bottleneck machen. Die in § 2 Abs. 13 BSIG-E zugrunde gelegte Definition kritischer Komponenten sollte nach Auffassung von Telefónica daher dringend auf solche Komponenten beschränkt werden, die in zentralen Netzwerkebenen zum Einsatz kommen.

Ebenfalls wichtig ist, dass Zertifizierungen anderer EU-Behörden ohne weitere Hürden anerkannt werden. Wenn eine Komponente von einer Behörde eines anderen EU-Mitgliedsstaates zertifiziert wurde, sollte diese nicht erneut beim BSI vorgelegt werden müssen.

6. Keine rückwirkende Belastung für Bestandsnetze, § 9b Abs. 4 BSIG-E

Eine Untersagung des Einsatzes von bereits eingesetzten Komponenten zum Zeitpunkt des Inkrafttretens des Gesetzes muss ausgeschlossen werden (Bestandsschutz). Im Sinne eines Investitionsschutzes dürfen die Folgen einer möglicherweise festgestellten mangelnden Vertrauenswürdigkeit sich nicht auf Komponenten erstrecken, die bereits vor Inkrafttreten des IT-SiG 2.0 verbaut wurden. Es bedarf zudem einer Klarstellung, dass auch die Pflicht zur Meldung des Einsatzes kritischer Komponenten an das BMI sich nicht auf bereits im Netz verbaute Komponenten beziehen darf (die z. B. im Rahmen einer Wartung oder Fehlerbehebung ausgetauscht werden müssen), sondern nur auf solche Komponenten, die erstmals neu im Netz in Betrieb genommen werden. Im Gesetz bedarf es daher dringend einer entsprechenden Überleitungsvorschrift, die klarstellt, dass das gesamte Regelungsregime des § 9b BSIG-E nur für Komponenten einschlägig ist, die zukünftig neu im Netz verbaut werden.

7. Ermächtigung zum Erlass von Rechtsverordnungen, § 10 Abs. 6 BSIG-E

Telefónica begrüßt den hier angestrebten Ansatz, IT-Security als einen dynamischen Prozess und nicht als ein starres Konstrukt zu begreifen. Das gesuchte Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie sowie die Einbeziehung der Wirtschaftsverbände begrüßen wir ebenfalls.

Dennoch sehen wir es als äußerst kritisch an, dass die Interoperabilität und Schnittstellenkompatibilität von Komponenten und Systemen pauschal und unabhängig von deren Kritikalität und/oder Funktionalität über eine Verordnung geregelt werden kann. Dies konterkariert die Bestrebungen des vorliegenden Gesetzentwurfs, der im Wesentlichen auf kritische Komponenten bzw. kritische Funktionen abstellt. Zudem steht es im krassen Widerspruch zu einer EU-weiten Harmonisierung der IT-Sicherheitsregulierung, dass hier die nationalen Behörden unabhängig von EU-Standards selbst Vorgaben zu technischen Standards machen können. Diese sehr weit und unbestimmt gefasste Vorschrift muss im Sinne des Bestimmtheitsgrundsatzes, sowie um Rechts- und Planungssicherheit für die betroffenen Unternehmen zu ermöglichen, zwingend angepasst und konkretisiert werden. Denkbar wäre hier eine Eingrenzung auf die Liste der kritischen Funktionen und Komponenten nach § 109 Abs. 6 TKG-E und die Einbeziehung der Maßnahmen nach der EU-5G-Tool-Box.

Ansprechpartner
Philippe Gröschel, Head of Government Relations, philippe.groeschel@telefonica.com