eco Stellungnahme zu Sicherheitskatalog-Entwurf gem. § 109 Abs. 6 TKG

Berlin, den 22.11.2019

Am 15.10.2019 veröffentlichte die Bundesnetzagentur einen Entwurf eines Sicherheitskataloges nach § 109 Abs. 6 TKG. Diesen erstellte sie im Einvernehmen mit Bundesamt für Sicherheit in der Informationstechnik und dem Beauftragten für Datenschutz und Informationsfreiheit. Wir danken für die Gelegenheit zur Stellungnahme und nehmen diese gerne wahr.

eco und seine Mitgliedsunternehmen teilen mit den zuständigen Behörden das Interesse, die IT-Sicherheit von Telekommunikationsnetzen und -diensten zu verbessern und zu verstärken. Positiv an dem vorliegenden Entwurf bewerten wir insbesondere, dass die Anforderungen des Sicherheitskatalogs agnostisch von Herstellern und deren Herkunftsländern formuliert wurden.

Nach Auffassung des eco ist fraglich, ob die beabsichtigten Regelungen im TKG im richtigen Gesetz platziert sind. Das TKG adressiert im Wesentlichen die Betreiber von Telekommunikationsnetzen und -diensten, nicht aber die Zulieferer einzelner Hard- und Softwarekomponenten. Sämtliche aus den Regelungen des TKG folgende Verpflichtungen bzgl. der Sicherheit oder Verfügbarkeit von Netzelementen und Diensten richten sich in Folge an die Betreiber, nicht aber an die Hersteller, Distributoren oder Integratoren der Hard- und Softwarekomponenten. Letztere sind aber diejenigen, welche allein die Anforderungen an eine Zertifizierung oder der Sicherheit der Lieferkette umsetzen können, werden jedoch nicht wie die TK-Anbieter im TKG sanktioniert. Die Verantwortung wird daher unsachgemäß auf die TK-Anbieter verlagert.

Das TKG fußt, wie alle entsprechenden Gesetze in den europäischen Mitgliedstaaten auch, auf europäischen Vorgaben. Für die Beibehaltung harmonisierter Regelungen in den Mitgliedstaaten bedarf die Fortentwicklung dieser Regelungen eines EU-weiten Ansatzes. Ansonsten kommt es zu einer Schwächung des heutigen Harmonisierungsniveaus. Der aktuell vorgelegte Entwurf lässt nicht erkennen, inwiefern einer europaweiten Harmonisierung der Sicherheitsanforderungen Rechnung getragen wurde.

eco sieht in dem vorliegenden Entwurf eine gute Diskussionsgrundlage. An vielen Stellen sehen wir jedoch Präzisierungs- und Nachbesserungsbedarf.

eco bedauert, dass viele Aspekte seiner bereits in der Kommentierung und Anhörung zu den Eckpunkten neuer Sicherheitsanforderungen vorgebrachten Kritikpunkte bisher unberücksichtigt geblieben sind. Obschon sich manche der nun formulierten Vorgaben und Sicherheitsanforderungen prinzipiell eignen, die beabsichtigten Kontrollziele zu erreichen, ist deren Angemessenheit und Umsetzbarkeit teilweise zweifelhaft, vgl. § 109 Abs. 2 TKG.

eco sieht insbesondere hinsichtlich der folgenden Aspekte des Entwurfes einen dringenden Nachbesserungsbedarf:

- **Adressatenkreis zu unbestimmt und keine Bagatellgrenzen vorgesehen**
- **Rechts- und Planungsunsicherheit durch Auslagerung der Definitionen der kritischen Komponenten in eine unbestimmte Liste ab 2020**
- **Geplante Änderung des § 109 TKG verstärkt Rechts- und Planungsunsicherheit der Unternehmen**
- **Keine Differenzierungen zwischen Hard- und Software – sowie keine Unterscheidung zwischen Arten von Software, bspw. OpenSource und selbsthergestellte Software von Netzbetreibern**
- **Fehlen einer Notfalllösung um kurzfristig bei kritischen Vorfällen reagieren zu können**
- **kontinuierliche Überwachung durch eine „Monitoring Infrastruktur“ wirft datenschutzrechtliche Fragestellungen auf**

I. Adressatenkreis und Bagatellgrenze

eco sieht Präzisierungsbedarf hinsichtlich der Einstufung von Netzbetreibern und Diensteanbietern als solche mit gehobener Kritikalität und solche mit erhöhter Kritikalität und/oder erhöhtem Gefährdungspotential.

Eindeutig ist bisher nur, dass Anbieter von Mobilfunkdiensten mit über 100.000 Teilnehmern von den Behörden als Anbieter mit „hoher“ Kritikalität (5.1.3) und erhöhtem Gefährdungspotential (Anlage 2) angesehen werden sollen. Die Entwurfsverfasser wollen sich an den Vorgaben des PSTG orientieren. Diesen Ansatz betrachtet eco als nicht als sachgerecht, da die Reglungen des PTSG primär auf Infrastrukturbetrieb abgestellt sind und eine Vielzahl von Telekommunikationsdiensten dem PTSG bewusst nicht unterworfen sind bzw. werden.

Für sinnvoll und erforderlich erachtet eco Ausführungen, ob die betroffenen Unternehmen hinsichtlich der Begriffe „Abstrakte, konkrete Gefahrenprognose und Gesamtprognose“ im Anwendungsbereich der Anlage 2 auf die Beschreibungen ab 5.1.3 des Entwurfs zurückgreifen können. Gegebenenfalls wäre ein entsprechender Verweis in der Einleitung der Anlage 2 angebracht.

Dazu sollten die Behörden auch Zahlenwerte zur Teilnehmerzahl für TK-Netze und Diensteanbieter von lokalen Netzen für Sprach- und Datenkommunikation, Anbieter von Internetzugängen oder Rundfunkverteildienste mit geringer bis mittlerer Teilnehmerzahl oder Anbieter reiner internetgestützter Kommunikationsdienste angeben, die der Standardkritikalität unterfallen sollen. Soweit unter 5.1.3 und in der Einleitung der Anlage 2 dieselben Größenordnungen gemeint sind, bitten wir ebenfalls um eine entsprechende Referenz im Text, anderenfalls um Klarstellungen an beiden genannten Textstellen.

Hinzu kommt, dass kein Schwellenwert für ein erhöhtes Gefährdungspotential und somit denklogisch auf gehobene Kritikalität bzw. erhöhte Kritikalität vorgesehen wird, unterstellt 5.1.3. gilt auch für den Anwendungsbereich der Anlage 2. Das Fehlen einer Bagatellgrenze führt den oben gewählten Ansatz, hauptsächlich die Anzahl der Kunden als erheblich für eine Gefährdung anzusehen ad absurdum.

In diesem Zusammenhang möchten wir an unsere Vorschläge aus unserer Stellungnahme vom 04.05.2019 zu den Eckpunkten hinweisen:

„Denkbar sind auf Umsatz bezogene Festlegungen, im Sinne von § 267 HGB oder entsprechend der Empfehlung der EU-Kommission 2003/361/EG (L 124/36 v. 20.05.2003), welche zusätzlich zum Umsatz die Mitarbeiterzahl miteinbezieht.“

Näher darzulegen ist auch der Unterschied zwischen gehobener Kritikalität und erhöhter Kritikalität hinsichtlich der geplanten Grundlagen einer Einstufung. Zur Unterscheidung zwischen gehobener und erhöhter Kritikalität bedarf es aus Sicht des eco weiterer verständlicher und insbesondere bestimmter Unterscheidungsmerkmale, welche insbesondere eine Vergleichbarkeit der Einstufungen zwischen den Unternehmen ermöglicht.

Unklar bleibt auch, welche zusätzlichen Anforderungen der Anlage 2 sich für Anbieter mit einer gehobenen Kritikalität oder erhöhter Kritikalität zu erfüllen hätten, im Sinne der dort genannten „ergänzenden Präventivanforderungen“.

Klarstellende Erläuterungen vermissen wir in diesem Zusammenhang ebenfalls zu den unbestimmten Rechtsbegriffen wie „Gemeinwohl“ oder „Bestand der Bundesrepublik Deutschland als Industrie- und Technologiestandort“ mit Blick auf eine hervorgehobene Bedeutung von

Netzbetreibern und Dienstanbietern und deren deswegen angenommener erhöhten Kritikalität.

Nach Ansicht des eco folgt daraus auch die Pflicht der Behörden zu begründen, warum entweder das Gemeinwohl oder der Bestand der Bundesrepublik Deutschland als Industrie- und Technologiestandort durch welche konkrete Gefährdung betroffen sein soll. Zudem sehen wir es als präzisierungsbedürftig, ob Gefahr oder Gefährdung gemeint ist. Im zweiten Fall bedarf es der Definition, was die Verfasser unter Gefährdung verstehen.

eco hält die Vermutung eines erhöhten Gefährdungspotentials bei über 100.000 Anschlüssen außerhalb des Anwendungsbereichs des PTSG für nicht zulässig. Bei 100.000 Anschlüssen handelt es sich um nicht einmal 0,057% der mehr als 38.800.000 Festnetz- und 137 Millionen Mobilfunk-Anschlüsse (2018: https://de.statista.com / www.bnetza.de). Das Gemeinwohl wird nicht entscheidend gefährdet sein, wenn 0,057 % der Bevölkerung vorübergehend keinen Zugang zu einzelnen TK-Anschlüssen haben - insbesondere da Bürger und Unternehmen in aller Regel über mehr als einen einzelnen TK-Anschluss (Festnetz & Mobilfunk) verfügen.

Konkret ist dem Entwurf nicht zu entnehmen, welche Umstände außer der Teilnehmerzahl in eine Einstufung einzubeziehen und somit zur Zusprechung der hervorgehobenen Bedeutung führen können. Dazu sollten entsprechende nachvollziehbaren und sachgerechten Kriterien genannt werden, sowie konkrete Beispiele für die jeweilige Einstufung von Betreibern.

Nach unserer Einschätzung werden einige Unternehmen ohne die hier geforderten Differenzierungen der Sicherheitsanforderungen im Sinne einer verhältnismäßigen Belastung in ihrer Existenz bedroht.

II. Rechts- und Planungsunsicherheit

Anfang März 2019 haben BNetzA, BMWi und BMI angekündigt, dass Bedarf für die Aktualisierung des Sicherheitskataloges bestünde. Dies hat zur Verunsicherung sowohl bei Anbietern als auch bei Nachfragern geführt. Nun, Mitte Oktober 2019, veröffentlicht man einen Entwurf, entscheidet sich aber dafür die Definitionen der kritischen Komponenten in einer separaten Liste festlegen zu wollen, welche nicht Bestandteil des Entwurfes ist. Diese soll vielmehr erst am 01.01.2020 im Amtsblatt der BNetzA veröffentlicht werden. Unklar ist, ob die Liste als Entwurf oder finales Dokument veröffentlicht wird. Ein solches Vorgehen hinsichtlich eines der relevantesten Punkte für die Unternehmen verlängert die Rechts- und Planungsunsicherheit weiter.

Für notwendig erachtet eco die vorherige Konsultation einer solchen Liste bei der ersten Erstellung sowie bei jeder Aktualisierung. Anderenfalls sähen

wir es als Verstoß gegen die Konsultationspflicht nach § 109 Abs. 6 TKG und gegen den Zweck dieser Norm, dass die Behörden die kritischen Funktionen festlegen wollen, ohne dass die Auswahl der und Funktion und deren Bewertung mit den gesetzlich zu beteiligenden Marktakteuren diskutiert wird. Dabei erwartet eco auch eine Beteiligung an der Ausarbeitung und der Berücksichtigung seiner Eingaben.

Die Ankündigung der Gesetzesänderung von § 109 TKG in den Pressemitteilungen des BMWi und BMI zur Veröffentlichung des Sicherheitskatalog-Entwurfs sorgt für weitere Verunsicherung und vermindert Rechts- und Planungssicherheit der Unternehmen zusätzlich. Zudem dürfte die geplante Gesetzesänderung eine erneute Aktualisierung des Sicherheitskataloges nach sich ziehen.

eco regt daher ein zeitlich und inhaltlich abgestimmtes Handeln der Verwaltung und des Gesetzgebers an.

IV. Fehlende Differenzierung

Nach Ansicht des eco ist es weder sachgerecht noch angemessen, dass in dem Entwurf keine Unterscheidungen zwischen Hard- und Software im Hinblick auf Kritikalität vorgenommen wird. Dies gilt insbesondere bei den verschiedenen Arten von Software. So wird nicht zwischen vom Hersteller bereitgestellter Software, OpenSource und vom Netzbetreiber selbst entwickelter Software differenziert. Bei vom Netzbetreiber selbst entwickelter Software stellt sich die Frage, wie diese denn sinnvoll zertifiziert werden soll, da es keine Referenzen oder Vergleichssoftware gibt. Grundsätzlich gilt das ebenfalls für OpenSource-Software und zwar vom Hersteller bezogener, danach aber speziell und konkret vom Netzbetreiber bzw. Dienste-Anbieter für die jeweiligen unternehmensinternen Architekturen angepasste Software, welche nicht mehr der vom Hersteller zertifizierten Basissoftware entspricht.

Bzgl. Free and Open Source Software (FOSS) erscheint es relevant, dass durch die Offenlegung von Quelltext in der Öffentlichkeit es erheblich erschwert ist, gezielt einzelne Unternehmen zu sabotieren. Außerdem ergibt sich "post-mortem" eine Nachvollziehbarkeit, wie es zu einer Manipulation kam.

V. Zertifizierung

Klar geregelt werden sollte, welche Technologien in den Anwendungsbereich des Katalogs fallen. Soweit Bestandstechnologien wie etwa 2G,3G oder IP-Kernnetze erfasst werden sollen, ist ein Bestandsschutz auch dieser

kritischen Komponenten und/oder mehrjährige Übergangsfristen zu gewähren.

Bei vom Betreiber selbst entwickelter Software sollte eine Ausnahmeregelung von der Zertifizierungspflicht gelten, denn in Ermangelung eines externen Herstellers ist eine gezielte Manipulation dieser Software, z.B. vor dem Hintergrund gesetzlicher Auflagen dritter Staaten ausgeschlossen. Weiter sollte ein Unternehmen, welches als Netzbetreiber oder Diensteanbieter von der Bundesnetzagentur offenkundig als vertrauenswürdig erachtet wird, auch als Hersteller von Software als vertrauenswürdig gelten. Eine Zertifizierungspflicht für selbst entwickelte Software würde prinzipiell dazu führen, das Unternehmen Ihre komplette Softwareabteilung inklusive aller Zulieferer, verwendeten Module, Libraries und Compiler zertifizieren müssten. Ein solcher Prozess wäre nicht nur mit überbordenden Aufwendungen verbunden, welche den Rahmen des wirtschaftlich zumutbaren signifikant überschreiten, sondern würde in der Praxis keinen oder nur einen geringen Sicherheitsvorteil bieten.

eco empfiehlt daher dringend, dass nicht für jedes Software-Update ein umfassendes Prüfungs- und Zertifizierungsverfahren durchzuführen ist. Stattdessen sollte festgelegt werden, ab welcher Art von maßgeblichen Änderungen eine neue Prüfung und Zertifizierung erforderlich ist. Ein derartiges Vorgehen ist heute beispielsweise bereits im Bereich der IT-Grundschutzzertifizierung gelebte Praxis.

Die avisierte Zertifizierung darf in keinem Fall aktuelle Arbeitsmethoden wie agile Entwicklung unmöglich machen, welchem dem Stand der Technik entsprechen. Mit solchen Methoden setzt sich Anlage 2 aber nicht auseinander. So ist nicht erkennbar wie etwa im Rahmen von “Continuous Deployment” (kontinuierliche, azyklische Aktualisierung) von Software, sondern in Form von Microupdates einzelner Module geschieht, eine Zertifizierung im Sinne des Entwurfes sichergestellt werden kann. Diese Methodik bildet die Grundlage moderner Softwareentwicklung in zahlreichen Betrieben und ist im Gegensatz zu monolithischen Entwicklungen geeignet, kurzfristig auf neu bekanntwerdende Schwachstellen zu reagieren und diese zu beheben.

Es stellt sich darüber hinaus die Frage, wie eine Zertifizierung bei häufigen Releases zeitlich umgesetzt werden soll. Manche Hersteller liefern in vorbildlicher Weise mehrere Sicherheits- oder Funktionsupdates pro Monat aus, dies zudem pro angebotener Plattform. Es ist nicht zu erwarten, dass für diese Module eine ebenso zeitnahe Zertifizierung erfolgt. Denn ein Großteil der Hersteller als nicht eigenständig verpflichtete Unternehmen werden sich realistisch gesehen nicht auf eine geeignete Zertifizierung im Sinne der Anlage einlassen wird. Gleichzeitig ist jedoch das Einspielen

vorliegender Sicherheitsupdates der Hersteller zu dann als bereits bekannt anzusehenden Lücken elementar für einen sicheren Betrieb nach dem Stand der Technik im Sinne des Gesetzes.

Aus Sicht des eco ist insofern eine gesetzliche Regelung zu der Frage, wer die aus der zeitlichen Verzögerung einer zwingenden Zertifizierung von Softwarekomponenten zwangsläufig anwachsenden Risiken trägt, dringend erforderlich. Entsprechend sollte im Sicherheitskatalog klar zum Ausdruck gebracht werden, dass die Zertifizierung durch den Hersteller erfolgt, d. h. ein Herstellerzertifikat. Somit werden Unklarheiten bezüglich der Verantwortlichkeiten vermieden.

VI. Fehlen von Notfalllösungen

Im Falle eines zeitlich kritischen Vorfalls ist es dringend geboten, dass Netzbetreiber und Dienste-Anbieter ein Update vornehmen können, ohne zunächst auf Prüfung und Zertifizierung warten zu müssen. Anderenfalls sind erhebliche Schäden für Unternehmen, deren Kunden und für Dritte absehbar, wenn aufgrund einer fehlenden Zertifizierung keine kurzfristigen Abhilfemaßnahmen ergriffen werden können (siehe hierzu auch die Ausführungen unter V. „Zertifizierung“).

VII. Überwachung und Datenschutzkonformität

eco sieht erheblichen Nachbesserungsbedarf hinsichtlich konkreter Empfehlungen und Umsetzungshinweise auf eine daten- und grundrechtsschutzkonforme Ausführung der Überwachung von Datenverkehren durch die nun zwingend vorgesehene Monitoring Infrastruktur (MI). Der abstrakte Hinweis, dass eine MI daten- und grundrechtsschutzkonform sein soll, ist nicht hilfreich und weiterführend um die damit verbundenen Fragestellungen für die Beteiligten verbindlich zu beantworten. Dies ist verwunderlich, da der Beauftragte für Datenschutz und Informationsfreiheit an der Erstellung des Entwurfs des Sicherheitskataloges beteiligt war.

Ebenfalls mit Sorge sehen wir den Zwang zum Erkennen von Botnetzen in Anlage 1. So wurde hier keine Ausnahme für kleine Provider geschaffen, die schon allein mangels vorhandener Edge-Bandbreite keine relevante Gefahr darstellen. Im Entwurf fehlt die konkrete Definition eines Botnetzes sowie die Frage, ob der Detektion als logische Konsequenz eine automatische Abschaltung der erkannten Teilnehmer folgen soll bzw. eine solche erfolgen darf, da mit einer reinen Detektion kein Sicherheitsgewinn verbunden ist.

In diesem Zuge stellt sich jedoch die Folgefrage, ob eine derartig weitreichende Maßnahme, die faktisch den Aufbau einer Überwachungs- und insbesondere einer Sperrinfrastruktur vonnöten macht, ohne relevanten gesellschaftlichen Diskurs in einer nachgelagerten Norm erzwungen werden und dies nicht zumindest eine gesetzliche Verankerung erfahren sollte.

VIII. Fachpersonal

Abhängig von der Art der ausgelagerten systemrelevanten Prozesse ist zu berücksichtigen, dass dafür Dritte als Auftragnehmer in Betracht kommen, welche nicht Hersteller oder Lieferant sind. Es kann aber nicht davon ausgegangen werden, dass solche Betreiber der ausgelagerten Prozesse grundsätzlich unabhängig von den Telekommunikationsunternehmen sind. Dies ist insbesondere dann nicht der Fall, wenn das in Deutschland ansässige und nach TKG verpflichtete Telekommunikationsunternehmen und der Auftragnehmer einem Konzernverbund angehören.

Fraglich ist, ob ein Auftragnehmer automatisch oder nur dann als „zuverlässig“ gilt, wenn dieser „vertrauenswürdig“ im Sinne dieser Regelung ist. Hier ist Präzisierung erforderlich, insbesondere auch hinsichtlich EU-weiter Regelungen zur Eignungs- und Sicherheitsüberprüfung von eingesetztem Personal

IX. Verfehlen des Schutzzieles

Die in Anlage 2 beschriebenen Auflagen haben weitreichende Auswirkungen auf die betroffenen Unternehmen. Überschlägig berechnete Kosten einer Zertifizierung können das Betriebsergebnis von KMUs ohne weiteres übersteigen.

Trotz signifikanter Kosten wird das Schutzziel aber verfehlt, da nach unserer Einschätzung erhebliche Lücken verbleiben. Es ist technisch so gut wie unmöglich, dass ein Hersteller einen Betreiber in die Lage versetzt, die Integrität von Komponenten zu verifizieren.

Einerseits dürfte eine ernsthafte Überprüfung der Integrität einer Komponente nach unserer Einschätzung von den am Markt tätigen Unternehmen fachlich nicht zu leisten sein, andererseits kann man einen Hersteller nicht verpflichten, einen fachlich kompetenten Betreiber in die Lage zu versetzen, die von ihm selbst gelieferten Komponenten zu überprüfen. Denn eine derartige Überprüfung durch den Betreiber kann realistischer Weise nur durchgeführt werden, wenn neben dem eingesetzten Produkt zumindest auch die gesamte Toolchain in Quellcode vorliegt. Bei einem solchen Verfahren würden zudem Lücken geschaffen und ließen sich

ausnutzen, bspw. durch die Einbettung von Schadcode im Compiler oder durch den Einsatz von Hardwareimplantaten.

Das Erreichen des Schutzziels wird bereits dadurch verhindert, indem sich die Zertifizierung auf die gelieferten Hard- und Softwarekomponenten beschränkt. Um das Einbringen von jeglichen Implantaten zu verhindern, müssten sämtliche bei der Produktion genutzten Werkzeuge wie die verwendeten Compiler oder Komponenten zur Herstellung von Silizium ebenfalls zertifiziert werden. Ansonsten wäre auch hier eine Lücke gegeben.

X. Vertrauenswürdigkeit

eco bewertet die erläuternden Ausführungen zur Vertrauenswürdigkeit unter 3. in Anlage 2 als erläuternde Anhaltspunkte. Allerdings bezweifelt eco sehr stark, dass eine nennenswerte Zahl an KMUs in der Lage sein wird, Hersteller in Verträgen rechtlich zur Beachtung der hieraufgeführten Pflichten binden zu können. Das ist ob deren Verhandlungsgewicht, Auftragsvolumen, langfristige Abnahmemenge, usw. nicht realistisch.

Darüber hinaus gelten rechtliche Rahmenbedingungen eines Landes unabhängig von einzelnen Herstellern. Insofern stellt sich die Frage, ob entsprechende Überprüfungen nicht vielmehr von einer zentralen behördlichen Stelle durchgeführt werden müssten.

Zudem besteht noch weitergehender Klarstellungsbedarf im Hinblick auf mehrere Begriffe und den konkret gemeinten Inhalt mancher Unterpunkte.

- Zu 3 Nr. 2: „Keine Informationen aus Vertragsverhältnissen an Dritte“. Sind Zoll- und Steuerbehörden des Landes, indem die Bezugsquelle verzollt und/oder versteuert, Dritte? eco regt an, dass eine ausdrückliche Klarstellung im Text, dass gesetzliche Auskunftspflichten beispielsweise bzgl. Steuer und Zoll unberührt bleiben, erfolgt.

- Zu 3 Nr. 3ff: „vertrauliche Informationen“. Was fällt darunter und was nicht? eco regt an, die abstrakte Formulierung durch entsprechende Erläuterungen, Begründung und konkrete Beispiele zu konkretisieren.

- Zu 3 Nr. 4 insgesamt: Aus unserer Sicht kann kein Hersteller diese Zusage hinsichtlich der Formulierung dieses Unterpunktes abgeben. Selbst in den meisten europäischen Ländern gibt es anders als in Deutschland kein Trennungsgebot zwischen Polizei und Geheimdiensten, exemplarisch seien der Großteil von Skandinavien, die Schweiz, Österreich und Frankreich genannt. Auch außerhalb der EU ist in keinem der Heimatländer der großen Technologiekonzerne wie in den USA oder China eine derartige Trennung gesetzlich verankert.

Daraus folgt, dass nicht ausgeschlossen werden kann, dass Erkenntnisse, die ein Hersteller zu Strafverfolgungszwecken wegen seiner gesetzlichen Auskunftspflicht den zuständigen Strafverfolgungsbehörden mitteilt, nicht auch den jeweiligen Geheimdiensten zugänglich sind. Zudem gibt es außer oben bereits genannten gesetzlichen Pflichten zur Auskunft wegen Zoll und Steuer auch noch viele weitere, europa- und völkerrechtlich zwingende gesetzliche Pflichten, u. a. zur Gefahrenabwehr.

Es ist deutlich herauszustellen das fast alle Unternehmen der Welt, auch europäische und amerikanische, den Geheimdiensten ihres Unternehmens-sitzes auf Anordnung zur Auskunft verpflichtet sind. Wir verweisen exemplarisch auf unsere eigene Gesetzgebung, welche bestimmte Arten von Unternehmen gegenüber
- dem BND gem. § 8 BND-G (https://www.gesetze-im-internet.de/bndg/__8.html),
- dem BfV nach §§ 8, 8a, 8d BVerfSchG (https://www.gesetze-im-internet.de/bverfschg/).
- den LfVs (Bay. LVerfSchG, Art. 14-16 (https://www.gesetze-bayern.de/Content/Document/BayVSG)
- und dem MAD gem. §§ 4a, 4b MAD-G (https://www.gesetze-im-internet.de/madg/).
entsprechend verpflichtet.

In der Schweiz gilt die besondere Auskunftspflicht von Unternehmen nach Art. 25 i. V. m. Art. 19 des Schweizer Nachrichtendienstgesetz (https://www.admin.ch/opc/de/federal-gazette/2015/7211.pdf, S. 9).
In Österreich nach § 11 Abs. 1 Nr. 5 i. V. m. § 6 des österreichischen Polizeiliches Staatsschutzgesetz – PStSG (https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2016_I_5/BGBLA_2016_I_5.pdfsig, S. 4).

Im Kontext des fehlenden Trennungsgebot möchten wir außerdem auf das Europäische Gesetzgebungsverfahren für die sog. „E-Evidence-Verordnung“ hinweisen. Dieses geplante Regelwerk soll Ermittlungsbehörden grenzüberschreitend Zugriff auf Daten geben. Insoweit dürfte angesichts der avisierten E-Evidence-VO im Grunde künftig niemand die Anforderung des Nr. 4 erfüllen können. Nach unserer Auffassung liegt dem Grunde nach bereits eine generelle rechtliche Unmöglichkeit vor. Diesbezüglich ist der in Nr. 4 verwendete Begriff der „Sicherheitsbehörden“ erheblich zu unbestimmt. Eine Legaldefinition von „Sicherheitsbehörden“ gibt es im TKG nicht. Zudem würde auch dies zu kurz greifen, da die hier gemeinten Hersteller insgesamt nicht dem TKG unterfallen. Diese Ungenauigkeit hindert verpflichtete TK-Unternehmen an der Erstellung einer Vertrauenswürdigkeitserklärung und ebenso den jeweiligen Hersteller an einer Unterschrift.

Eine Regelung, welche jedoch keinem der potentiellen Zulieferer geeigneter Systemkomponenten eine gesetzeskonforme Erklärung ermöglicht, ist aus Sicht des eco abzulehnen.

Außerdem werden in Punkt 4 Hersteller in die Pflicht genommen, in ihre Produkte technische Methoden/Verfahrensweisen zu integrieren, die die Betreiber dazu befähigen, die Produkte hinsichtlich Integrität zu verifizieren. Die Überprüfung des Produktes soll während des ganzen Lebenszyklus erfolgen und dokumentiert werden. eco bezweifelt daher an der Angemessenheit im Sinne von § 109 Abs. 2 TKG und der Umsetzbarkeit dieser Anforderung aufgrund der Anzahl der Netz- und Systemkomponenten sowie deren Entwicklungsdynamik. Eine Umsetzung dieser Forderung, welche derzeit in keinem Produkt enthalten ist, hätte bspw. eine vollständige Neuentwicklung von Kernnetzkomponenten und Managementsystemen durch jeden Hersteller zur Folge und dürfte geschätzt mehrere Jahre dauern. Gleichsam gravierend wären die Auswirkungen auf die bestehenden, branchenüblichen Prozesse bzgl. Lieferung, Lagerung, Inbetriebnahme und dem Austausch von Komponenten, welche komplett neu entwickelt werden müssten und ebenso in den bestehenden, vertraglichen Beziehungen Niederschlag finden müssten.

Entsprechend sieht eco eine Neuformulierung von 3 Nr. 4 insgesamt als dringend erforderlich an, damit betroffene Telekommunikationsunternehmen auch tatsächlich und rechtlich eine Vertrauenswürdigkeitserklärung erstellen und die jeweiligen Hersteller diese Erklärung unterschreiben können.

XI. Übergangsfristen

eco erachtet die unter 2.5 in Anlage 2 vorgeschlagenen Übergangsfristen als sehr sinnvoll und sachgerecht, soweit diese Übergangfrist auch für bereits getätigte Bestellungen gilt. So wird Investitionsstau vermieden. In diesem Kontext ist es von erheblicher Bedeutung, dass die Liste im Sinne von 2.3 der Anlage 2 möglichst lange keiner Aktualisierung bedarf.

XII. Harmonisierte Rahmenbedingungen

eco erachtet die ersten Ansätze zur EU-Harmonisierung, die sich im Entwurf finden, positiv. Dementsprechend sollte zur Grundlage der Liste im Sinne von 2.4 und 2.5 der Anlage nicht die nationale Risikobewertung zu 5G, sondern das „Risk Assessment 5G“ der NIS Cooperation Group vom 09.10.2019 werden.

XIII. Bezugnahme bisherige Kritik

Im Übrigen verweisen wir ergänzend auf die bereits in unserer Stellungnahme vom 04.05.2019 dargelegten Kritikpunkte zu den Eckpunkten der Bundesnetzagentur (https://www.eco.de/download/93658/).

Über eco
eco - Verband der Internetwirtschaft e.V. ist Interessenvertreter und Förderer aller Unternehmen, die mit oder im Internet wirtschaftliche Wertschöpfung betreiben. Der Verband vertritt derzeit mehr als 1100 Mitgliedsunternehmen.

Hierzu zählen unter anderem ISP (Internet Service Provider), Carrier, Hard- und Softwarelieferanten, Content- und Service-Anbieter sowie Kommunikationsunternehmen. eco ist der größte nationale Internet-Service-Provider-Verband Europas.