eco Stellungnahme zum notifizierten Sicherheitskatalog nach § 109 Abs. 6 TKG an die EU-Kommission – Ihr Zeichen 2020/496/D

Berlin, 28.09.2020

Die Bundesnetzagentur hat den Entwurf eines Sicherheitskataloges erstellt. Dieser soll die Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten vorgeben und ist bei der Erstellung von Sicherheitskonzepten zu Grunde zu legen.

eco und seine Mitgliedsunternehmen teilen mit den zuständigen Behörden das Interesse, die IT-Sicherheit von Telekommunikationsnetzen und -diensten zu verbessern und zu verstärken.

I. Allgemeines

Nachfolgend möchten wir die Gelegenheit ergreifen zu dem überarbeiteten Entwurf eines Sicherheitskatalogs, der zur Notifizierung bei der EU-Kommission vorgelegt wurde, nochmals im Rahmen einer Stellungnahme ausführlich die wesentlichen Aspekte zu adressieren.

eco erachtet es als positiv, dass die Bundesnetzagentur (BNetzA) einen angemesseneren Ansatz mit mehr Differenzierungen gewählt hat, als noch im Entwurf vom Herbst 2019 in Aussicht gestellt. Allerdings steht zu befürchten, dass die Pflichten für alle Telekommunikationsnetzbetreiber und Anbieter solcher Dienste in absehbarer Zeit wieder strenger werden. Im Rahmen der Umsetzung des Europäischen Kodexes für elektronische Kommunikation (EECC) soll das Telekommunikationsgesetz (TKG) komplett neugefasst werden. Dazu zählt nach bisherigerem Kenntnisstand auch eine Neufassung des § 109 TKG, dessen Absatz 6 Rechtsgrundlage des im Notifizierungsverfahren befindlichen Entwurfs ist. Diese Neufassung sieht deutliche Verschärfungen vor. Vorgesehen wird u. a. ein sehr komplexes Regelungswerk über verschiedene Gesetze neben TKG, einer Allgemeinverfügung des Bundesministeriums des Inneren und weiteren, anderen Rechtsvorschriften von Behörden. Bzgl. dieser avisierten Rechtsänderungen kommt der Eindruck auf, der notifizierte Entwurf wolle diese (Novellierungen) im Voraus berücksichtigen, bspw. eine technische Richtlinie des Bundesamts für Sicherheit in der Informationstechnik (BSI), vgl. IV.. Die Verabschiedung des Katalogs von Sicherheitsanforderungen vor Inkrafttreten von im Zusammenhang stehen Neuregelungen, die durch den Katalog konkretisiert werden sollen und die die Rechtsgrundlage für den Katalog bilden, hält eco für unzulässig, da es den Anbietern keine Planungs-, Investitions- und Rechtssicherheit bietet. eco fordert daher die Veröffentlichung alle geplanten Neuregelungen, damit eine gesamtheitliche Bewertung und Kommentierung durch die betroffenen Unternehmen erfolgen kann. Zudem sehen wir in dem Entwurf einen ungerechtfertigten Eingriff in die

unternehmerische Freiheit nach Art. 16 EU-Grundrechte-Charta, weil die geplanten Vorgaben weit über das erforderliche Maß zur Gewährleistung der Sicherheit von TK-Anlagen und Diensten hinausgehen und teilweise auch auf sachfremden Erwägungen beruhen.

II. Anwendungsbereich unklar

Der Entwurf verwendet den Begriff „erhöhter Kritikalität“. Der Listen-Entwurf (vgl. Nr. 16 Notifikations-Mitteilung) spricht hingegen von „erhöhtem Gefährdungspotential“. Es sollte eine Klarstellung erfolgen, ob mit den beiden unterschiedlichen Begriffen unterschiedliche Anwendungsbereiche gemeint sein sollen. Sofern das verneint wird, wäre es sinnvoll, in beiden Dokumenten denselben Begriff zu verwenden. Hinsichtlich der Anlage 2 des Sicherheitskatalogs und des zugehörigen Listen-Entwurfs ist die Betitelung unklar. Beide verwenden dort die Begriffe „erhöhtes Gefährdungspotential“. Auch aus dem Anwendungsbereich des Listen-Entwurfs wird nicht klar, worauf sich diese bezieht. Erst in der Gesamtschau des Sicherheitskatalog-Entwurfes lässt sich erkennen, dass unter „erhöhte Kritikalität“, S. 37f, 5.1.3, dass die Anlage 2 und der Listen-Entwurf die 5G-Mobilfunkanbieter adressieren sollen. Das derartige Verschränken, dass den Blick auf drei verschiedenen Seiten erfordert, um den Anwendungsbereich zu erkennen, ist unnötig und wenig hilfreich.

III. Vereinbarkeit mit Cyber Security Act fraglich

Nach Ansicht des eco steht der Entwurf des Katalogs nicht mit dem Cyber Security Act (CSA), EU-Verordnung 2019/881 in Einklang. Soweit keine Zertifizierungsschemata nach dem CSA verfügbar seien, wird vorbehalten, dass „pflichtige Netzbetreiber und Diensteerbringer beim Einsatz kritischer Komponenten vorübergehend sonstige geeignete und angemessene technische Vorkehrungen und sonstige Maßnahmen zur Gefahrenabwehr treffen müssen.“, vgl. S. 65, 2.4. Dies sind weitere sehr unbestimmte Begriffe, welche die BNetzA zusätzlich über die von § 109 TKG hinaus auslegen kann. Die unbestimmten Rechtsbegriffe in den § 109 TKG sollen aber durch den Sicherheitskatalog konkretisiert werden. Das Tatbestandsmerkmal „Gefahrenabwehr“ ist außerdem nicht hinreichend auf den Zweck von § 109 TKG begrenzt, wo es um technische Schutzmaßnahmen für Netze und TK-Dienste geht. Zudem fehlt eine Anknüpfung an globale und internationale Standards, wie unter anderen 3GPP. Weiter soll dem Entwurf zu Folge das BSI eine Technische Richtlinie zu Komponenten in Netzen mit erhöhter Kritikalität erlassen können. „Diese (Technische Richtlinie) enthält Anforderungen zur Zertifizierung von kritischen Komponenten einschließlich Anforderungen an die Einsatzumgebung und an den Betrieb als Voraussetzung für die Gültigkeit von Zertifikaten. Darüber hinaus beschreibt sie Auflagen zur Nachweiserbringung von Zertifikaten nach europäischen Zertifizierungsschemata (CSA).“

eco erachtet es diesbezüglich für sehr wichtig, dass die EU-Kommission und ENISA ihre Kontrollaufgaben bzgl. der EU-rechtskonformen Anwendung durch BNetzA und BSI wahrnimmt.

IV. Verstoß gegen EU-Binnenmarktprinzip

eco sieht in den Auflagen der Anlage 2 des Sicherheitskataloges einen Verstoß gegen das EU-Binnenmarktprinzip, im Sinne ungerechtfertigter Eingriffe in die Dienstleistungsfreiheit nach Art. 62 i. V. m. Art. 53 Abs. 1 AEUV, konkretisiert durch die Richtlinie 2006/123/EG. Indem die Bundesnetzagentur derart hohe Auflagen für 5G-Anbieter, die alle EU-weit tätig sind bzw. dies planen, festlegt, werden diese Anbieter faktisch gezwungen, technische Komponenten entsprechend den deutschen Anforderungen einzukaufen, obwohl andere Mitgliedsstaaten andere oder geringere Anforderungen stellen. Dies stellt nach Auffassung des eco eine diskriminierende Anforderung im Sinne von Art. 14 Nr. 1 der RL 2006/123/EG dar. Der BNetzA ist bewusst, dass die Anbieter den Einkauf konzernweit vornehmen, um betriebswirtschaftlich zu handeln und im Wettbewerb bestehen zu können. Dadurch nutzt die Behörde indirekt die faktischen Zwänge auf Grund der gegebenen Marktprinzipen aus. Dadurch kommt es zu einer mittelbaren Diskriminierung der deutschen 5G-Anbieter. Diese Ungleichbehandlung ist auch nicht sachlich gerechtfertigt. Dazu müssten zwingende Gründe des Allgemeininteresses wie die Öffentliche Sicherheit diese indirekte Diskriminierung erfordern, vgl. Art. 16 Abs. 1 lit. b) der RL 2006/123/EG. eco erkennt das Bestreben der BNetzA die öffentliche Sicherheit in elektronischen Kommunikationsnetzen durch die Vorgaben im notifizierten Entwurf zu steigern, an. Die Vorgaben übersteigen jedoch in vielen Punkten und Umfang das erforderliche Maß, z. B. die Anzeigepflicht bzgl. des Einbaus einzelner kritischer Komponenten (vgl. unten VIII.) und die Ausbauverpflichtung (s. u. IX.). Schließlich soll zudem die 5G-Tollbox der ENISA, das IT-Grundschutzkompendium des BSI, die Liste von BNetzA und BSI die Technische Richtlinie des BSI beachtet werden. Dieses Konglomerat an Vorgaben ist nicht mehr überschaubar und der Sicherheit nicht dienlich.

Hinzu kommt, dass die Produkte und Dienste der deutschen 5G-Netzbetreiber EU-Weit teurer werden, da die Unternehmen faktisch gezwungen sind, in der ganzen EU Komponenten zu verwenden, welche den deutschen Sicherheitsanforderungen entsprächen. Die von der BNetzA aufgestellten Anforderungen sollen ihrem Sinn und Zweck nach nur dazu dienen, dass deutsche 5G-Netze sicher sind. Sie dürfen aber nicht dazu führen, auch nicht mittelbar, dass die Kosten für den Netzausbau EU-weit deutlich ansteigen. Dies führt außerdem zu einer Wettbewerbsverzerrung, da 5G-Anbieter aus anderen EU-Mitgliedsstaaten mit erheblich niedrigeren Sicherheitsanforderungen deutlich günstiger deren Leistungen anbieten können. Eine sachliche Rechtfertigung dieser mittelbaren Diskriminierung ist nicht ersichtlich, da die BNetzA mit ihren Anforderungen das erforderliche Maß überschreitet, siehe Absatz zuvor.

Letztlich werden Hersteller von Komponenten, die die Vorgaben des Katalogs nicht einhalten wollen oder können, vom deutschen Markt ausgeschlossen, ohne dass der Ausschluss sachlich gerechtfertigt würde. Wie oben ausgeführt, sind die Anforderungen nämlich für eine Gewährleistung der Sicherheit nicht oder nicht in dem geforderten Maße erforderlich.

V. Auswirkungen Internationaler Handel nicht hinreichend berücksichtigt

In Nr. 16 der Mitteilung zum notifizierten Entwurf gelangt das Bundesministerium für Wirtschaft und Energie zur Einschätzung, dass sich keine Auswirkungen auf den internationalen Handel ergäben. Konkret geht es um die Einhaltung des „Agreement on Technical Barriers to Trade“ der Welthandelsorganisation (TBT-Übereinkommen). Es zielt u.a. auf die Verhinderung unnötiger technischer Hemmnisse für den internationalen Handel und soll die Annahme protektionistischer Maßnahmen verhindern. Dem wird der notifizierte Entwurf nicht gerecht. Der Entwurf sieht den Punkt der Vertrauenswürdigkeit samt vielen zu prüfenden Unteraspekten vor.

eco sieht die Vertrauenswürdigkeit grundsätzlich als wichtigen Punkt an. Dieser Aspekt spielt aber schon zu einem deutlich früheren Zeitpunkt eine zentrale Rolle, und zwar vor dem Vertragsschluss zwischen 5G Mobilfunknetzbetreibern und den Herstellern. Keiner dieser Netzbetreiber würde einen Vertrag mit einem Hersteller abschließen, den er nicht als vertrauenswürdig erachtet, da sich die Netzbetreiber ihrer Verantwortung gegenüber Kunden und Gesellschaft sehr bewusst sind. In Bezug auf die Verhinderung der Annahme protektionistischer Maßnahmen gebieten rechtsstaatliche Prinzipien, dass nicht Vermutungen Grundlage für den Entzug des Vertrauens können sein, erst recht nicht sachfremde geostrategische, handels-, geo-, außen- oder sonstige politischen Erwägungen. Ein Ausschluss eines Unternehmens von einem Markt muss auf überprüfbaren Fakten beruhen, unabhängig davon, ob der Staat das Unternehmen selbst ausschließt oder indem den Netzbetreibern so strenge Vorgaben bzgl. Herstellern und Lieferanten auferlegt werden, um zu bewirken, dass die Netzbetreiber vom Einsatz der Komponenten von bestimmten Herstellern absehen. Bedauerlicherweise sieht eco diesen Fall in Deutschland als eine real bevorstehende Möglichkeit an.

VI. Vertrauenswürdigkeitserklärung stößt auf Bedenken

Der notifizierte Entwurf hat alle Punkte aus Entwurf vom Herbst 2019 entgegen der berechtigen Kritik und Präzisierungsbedarfen bedauerlicherweise unverändert beibehalten. Daher berücksichtigt der Entwurf nach Ansicht des eco weiterhin unzureichend, dass rechtliche Rahmenbedingungen eines Landes unabhängig von einzelnen Herstellern gelten. Insofern stellt sich die Frage, ob entsprechende Überprüfungen nicht vielmehr von einer zentralen behördlichen Stelle durchgeführt werden müssten. Es besteht aus Sicht des eco immer 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 Unternehmenssitzes auf Anordnung zur Auskunft verpflichtet sind.

Wir verweisen exemplarisch auf die deutsche 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 Polizeilichen 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 in den vorgenannten Staaten 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. In Bezug auf die fortgeschrittenen Verhandlungen zu einer E-Evidence-VO sieht eco Deutschland auch daran gehindert, den Zielen dieser Verordnung widersprechende Vorschriften zu erlassen. Das ergibt aus den Verträgen der EU, und insbesondere dem Effet Utile gem. Art. 4 Abs. 3 EUV.

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 die 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 Management-systemen durch jeden Hersteller zur Folge und dürfte geschätzt mehrere Jahre dauern. Gleichsam gravierend wären die Auswirkungen auf die bestehenden, branchen-üblichen 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 weiter insgesamt als dringend erforderlich an, damit betroffene Telekommunikationsunternehmen auch tatsächlich und rechtlich eine Vertrauenswürdigkeitserklärung erstellen und die jeweiligen Hersteller diese Erklärung unterschreiben können.

Schließlich fehlt bei dem Aspekt der Vertrauenswürdigkeitserklärung eine Rückbeziehung auf die Fristen aus dem Punkt 2.4 des Entwurfes, S. 66. Wegen des inneren Sachzusammenhangs beider Aspekte ist hier eine Anknüpfung geboten.

VII. Verstoß gegen Notifizierungspflicht oder nationales Recht

In Nr. 8 der Mitteilung zur Notifizierung wird ausgeführt, dass die Bundesnetzagentur und das Bundesamt für Sicherheit in der Informationstechnik im Einvernehmen eine "Liste der kritischen Funktionen für öffentliche Telekommunikationsnetze und –dienste mit erhöhtem Gefährdungspotenzial (Ergänzung zu Anlage 2 des Kataloges von Sicherheitsanforderungen)“ veröffentlichen wollen. Zudem soll das BSI eine Technische Richtlinie "Zertifizierung von TK- Komponenten" herausgeben, da insbesondere eine "Sicherheitszertifizierung" durch eine anerkannte Stelle ein wesentlicher Baustein sei.

Allerdings wurden weder der Listen-Entwurf noch die Technische Richtlinie des BSI bei der EU-Kommission zur Notifizierung vorgelegt.

a) Liste

Entweder ist die Liste rechtlicher Bestandteil des Verwaltungsaktes „Sicherheitskatalog“ (in Form einer Allgemeinverfügung). Wenn die Liste Teil dieser Allgemeinverfügung ist, unterliegt sie ebenso wie der Sicherheitskatalog der Notifizierungspflicht als technische Vorschrift im Sinne der Richtlinie EU/2015/1535. Dass die BNetzA die Liste als Teil einer verbindlichen, konkreten Regelung des Einzelfalles im Sinne Allgemeinverfügung ansieht, zeigt sich an den vielen Verpflichtungen der 5G-Netzbetreiber in Anlage 2, bspw. Verpflichtung zur Meldung des Einbaus kritischer Komponenten, Rückbauverpflichtung bei Wegfall der Zertifizierung nach Einbau, usw., die sie ausspricht und die ohne Liste keinen Regelungsgegenstand hätten.

Ist die Liste hingegen kein Teil der Allgemeinverfügung „Sicherheitskatalog“ ist § 109 Abs. 6 TKG keine Rechtsgrundlage für den Erlass der Liste. Im Übrigen ist auch keine auch andere Rechtsgrundlage für diese Liste im TKG ersichtlich. Somit handelte es sich um einen offensichtlichen Verstoß gegen nationales Recht. In diesem Fall ist EU-Kommission gehalten, Deutschland aufzufordern den notifizierten Entwurf zu ändern oder zurück zu ziehen. Das Verfahren zur Notifizierung technischer Vorschriften würde ad absurdum geführt, wenn die EU-Kommission offensichtlich rechtswidriges nationales Recht der Mitgliedstaaten akzeptieren würde. Nach einer Aufhebung des rechtswidrigen nationalen Rechtsakt, wäre ein Entwurf des Sicherheitskataloges erneut zu notifizieren. Die Annahme eines offensichtlich gegen nationales Recht verstoßenden Entwurfes durch die EU-Kommission entspräche auch nicht dem Effet Utile nach Art. 4 Abs. 3 EUV in Bezug auf die Richtlinie EU/2015/1535. Der Effet Utile bindet auch die EU-Kommission nach Art. 4 Abs. 3 i. V. m. Art. 17 Abs. 1 S. 2 EUV. Er verlangt die Durchsetzung des EU-Rechts in der Art und Weise, wie es dem Zweck des jeweiligen Rechts am besten Geltung verleiht. Es widerspricht dem Zweck des Notifizierungsverfahrens der Richtlinie EU/2015/1535, wenn offensichtlich rechtswidrige, nationale Vorschriften darin ohne Widerspruch angenommen würden, da

dieses Notifizierungsverfahren absehbar zur selben notifizierten Regelung wiederholt werden müsste.

b) Technische Richtlinie des BSI

Gleiches gilt für die unter Nr. 8 genannte Technische Richtlinie des BSI. Entweder ist sie notifizierungspflichtig, weil sie entweder ein Teil des Sicherheitskatalogs ist oder sie verstößt offensichtlich gegen nationales Recht. Denn § 109 Abs. 6 TKG ist keine Rechtsgrundlage für das BSI, eine Technische Richtlinie zu Komponenten in Netzen mit erhöhter Kritikalität erlassen zu dürfen. In dieser Norm wird allein die Bundesnetzagentur ermächtigt, den Sicherheitskatalog zu erlassen. Auch dann wäre es geboten, dass die EU-Kommission Deutschland auffordert, den Entwurf zu ändern oder zurückziehen, um das TRIS-Verfahren nicht ad absurdum zu führen und dem Effet Utile Rechnung zu tragen., vgl. Punkt zuvor.

VIII. Anzeigepflicht bzgl. Einbau kritischer Komponenten rechtswidrig

Nach Ansicht des eco ist die Meldepflicht des Einbaus kritischer Komponenten in 2.3 der Anlage 2, S. 65 rechtswidrig. Sowohl im Hinblick auf das nationale Recht als auch auf das EU-Recht. Eine solche Anzeigepflicht ist als Eingriff im Sinne der nationalen als auch europäischen Rechtsordnung zu werten, da die 5G-Netzbetreiber durch das Melden jeder betroffenen Komponente sowohl an BNetzA und BSI zugleich erheblich in ihrer unternehmerischen Freiheit eingeschränkt und belastet werden, da es sehr viele Komponenten sein dürften. Dies sind Eingriffe in die Berufsausübung Art. 12 Abs. 1 GG i. V m. Art. 19 Abs. 4 GG und in das Recht am eingerichteten und ausgeübten Gewerbebetrieb nach Art. 14 Abs. 1 i. V. m. Art. 19 Abs. 4 GG, sowie in das Grundrecht der unternehmerischen Freiheit gem. Art 16 EU-Grundrechte-Charta. Erhebliche Eingriffe des Staates müssen sich auf ein Gesetz stützen können, das vom Parlament erlassen wurde (Wesentlichkeitstheorie und Parlamentsvorbehalt). Da eine Anzeigepflicht nicht in Zuständigkeit der EU fällt, gibt es auch keine EU-Rechtsgrundlage, vgl. Empfehlung d. EU-Kommission 534/2019, 26.03.2019. Im TKG ist für eine Meldepflicht des Einbaus kritischer Komponenten keine Rechtsgrundlage vorhanden. Allenfalls könnte man hierzu § 109 Abs. 4 S. 5 TKG heranziehen (§ 109 Abs. 6 TKG ist Grundlage des Sicherheitskataloges). Allerdings beinhaltet § 109 Abs. 4 S. 5 TKG nur die Befugnis an die BNetzA bei der Feststellung von Mängeln im Sicherheitskonzepts oder bei dessen Umsetzung, die Beseitigung dieser Mängel verlangen zu können. Dabei handelt es sich um eine nachträgliche Kontrolle. Entweder liegt das Sicherheitskonzept schon vor, und es wird von der Behörde geprüft oder dessen Umsetzung wird behördlich kontrolliert. Eine Vorab (Ex-Ante)-Anzeige einzelner Komponenten lässt sich aus dieser Norm nicht herleiten und eine solche Auslegung verstößt gegen den Wortlaut von § 109 Abs. 4 S. 5 TKG. Auch eine historische Auslegung macht dies deutlich. In der Gesetzesbegründung, als die Regelung erstmalig eingeführt wurde, heißt es: „Die Regulierungsbehörde kann Nachbesserungen verlangen, wenn sie Mängel erkennt“, vgl. BT-Drs. 13/3609; S. 54. Das BSI wird in § 109 Abs. 4 S. 5 TKG gar nicht genannt.

Nach Auffassung des eco ist die EU-Kommission auch hinsichtlich dieses Aspekts gehalten, Deutschland aufzufordern, den Entwurf zu ändern oder zurückziehen, um das TRIS-Verfahren nicht ad absurdum zu führen und dem Effet Utile Rechnung zu tragen., vgl. ausführlich oben.

IX. Vertrauensschutz bzgl. eingebauter Komponenten nicht gewährleistet

eco sieht die Rückbauverpflichtung hinsichtlich kritischer Komponenten bei nachträglichem, behördlichem Entzug der Zertifizierung sehr kritisch. Ein Netzbetreiber schließt ein Vertrag zur Lieferung von Netzkomponenten nur mit einem Hersteller seines Vertrauens. Letzteres stellt Grundlage für Investition und für den Einbau der Komponenten dar. Die Verpflichtung in 2.4 des Entwurfes, S. 66 bedeutet aber dementgegen, dass Netzbetreiber einzelne Komponenten aus dem Netz entfernen zu müssen für den Fall das die Zertifizierung auf Grund behördlicher Entscheidung nachträglich entzogen wird. Der Entwurf weist auch ausdrücklich darauf hin, dass diese Vorgabe auch für Bestandskomponenten gelte. Eine solche Verpflichtung zur Ersetzung für Bestandskomponenten stellt einen noch erheblich intensiveren Eingriff als die Anzeigepflicht (vgl. Punkt zuvor) in die oben genannten Grundrechte der Unternehmen dar. Die entsprechende Planung, den Betrieb der Netze weiter aufrecht zu erhalten, das Einsetzen der Austauschkomponenten – dies alles sind sehr einschneidende Maßnahmen sich die unmittelbar auf die Geschäftstätigkeit und betrieblichen Abläufe der betroffenen Unternehmen auswirken. Hierbei handelt es sich um einen enteignungsgleichen Eingriff. Folglich hat der Regelungsgeber für einen angemessenen wirtschaftlichen Ausgleich zu sorgen im Falle der Untersagung des Betriebs von zuvor bewilligten technischen Komponenten., da die Netzbetreiber für die Entziehung eines Zertifikats keinen Anlass geben und Gründe hierfür nicht in seinem Verantwortungsbereich liegen.

Im europäischen Recht gibt es dafür mangels Regelungskompetenz keine Ermächtigungsgrundlage. Im nationalen Recht käme unter Umständen § 109 Abs. 4 S. 5, 2. Alt. TKG in Betracht. Danach kann die BNetzA die unverzügliche Beseitigung von Mängeln verlangen, wenn sie solche (Mängel) bei der Umsetzung des Sicherheitskonzeptes feststellt. Das Sicherheitskonzept wiederum ist von Netzbetreibern auf Grundlage des Sicherheitskataloges zu erstellen, vgl. § 109 Abs. 4, Abs. 6 TKG. Sowohl die Liste von BNetzA und BSI sowie die technische Richtlinie des BSI (Nr. 16 Notifizierungsmitteilung) sind entweder Teil des Sicherheitskataloges. Wenn § 109 Abs. 4, Abs. 6 TKG die Rechtsgrundlagen sein sollen, dann wären Liste von BNetzA und BSI sowie die technische Richtlinie des BSI zeitgleich mit dessen Entwurf zu notifizieren gewesen. Allerdings enthält § 109 Abs. 4, S. 5 TKG keine tatbestandliche Anknüpfung an die Zertifizierung oder einer Pflicht dazu. Somit fehlen für Liste und Technische Richtlinie nationale Rechtsgrundlagen, um verbindliche Regelungen für Netzbetreiber festlegen zu können. Diese Rechtsgrundlagen müssten ob ihrer Eingriffsintensität den Parlamentsvorbehalt erfüllen. Schließlich ist der Eintritt der konkreten Verpflichtung zur Ersetzung einer Komponente für den Netzbetreiber in

keiner Weise vorhersehbar. Dieser staatlich vorgesehene, erhebliche Eingriff gefährdet selbst den Betrieb der kritischen Infrastruktur und zieht mindestens Nutzungseinschränkungen nach sich, bzw. kann den kompletten Ausfall von Netzelementen und Diensten zur Folge haben.

Offen bleibt zudem, wie betroffenen Netzbetreibern Rechtsschutz gewährt wird, wenn sie zum Ausbau einzelner Komponenten verpflichtet sein sollen, weil nach Einbau die Zertifizierung der Komponente entzogen wird. Die Netzbetreiber sind nicht Adressat der Zertifizierungspflicht, sondern die Hersteller. Die Entscheidungen, die zum Wegfall einer Zertifizierung führen könnten, sind den Netzbetreibern auch nicht ohne weiteres zugänglich. In diesem Zusammenhang steht auch die Nachvollziehbarkeit des Verwaltungshandelns. Den Netzbetreibern wird sich das nur erschließen, wenn ihnen die vollständigen behördlichen Entscheidungen zum Wegfall einer Zertifizierung mitgeteilt werden. Das hierfür zu führende Verwaltungsverfahren betrifft aber nur die zertifizierende Behörde und Hersteller. Erschwerend kommt hinzu, dass im 5G-Bereich ein erheblicher Teil an Erkenntnissen, die ggf. zum Wegfall der Zertifizierung führen könnten, aus nachrichtendienstlichen (geheimdienstlichen) Quellen stammen kann, so dass unter Umständen bereits die Behörde, welche das Zertifikat entzieht, nur eine entsprechende Weisung zur Entziehung bekommt, ohne die sachlichen Gründe zu kennen. Damit wäre die Nachvollziehbarkeit des Verwaltungshandels auch in Bezug auf Verpflichtung zum Ausbau in keiner Weise gegeben und effektiver Rechtsschutz nicht möglich. Dies ist weder mit dem EU-Recht noch dem nationalen Recht vereinbar. Zudem haben die Netzbetreiber keinen Einfluss auf die Schaffung und den Erhalt der Zertifizierungsvoraussetzungen.

X. Anhörung nicht erfolgt

Zu dem zur Notifizierung vorgelegten Entwurf hat bislang keine Anhörung nach § 109 Abs. 6 TKG stattgefunden. Es wurde lediglich eine Anhörung zu einem Entwurf des Sicherheitskataloges im Herbst 2019 durchgeführt. Dieser unterschied sich jedoch wesentlich und in erheblichem Umfang vom in die Notifizierung gegebenen Entwurf. Nach Auffassung des eco sind die Liste von BNetzA/BSI und die technische Richtlinie rechtliche Bestandteile des Sicherheitskataloges. Daher hätten sie beide zugleich mit dem vorliegenden Entwurf notifiziert werden müssen. Der Listen-Entwurf wird gerade erst national konsultiert. Über eine Anhörung der Technischen Richtlinie des BSI ist nichts bekannt. Zu spät oder nicht erfolgte Anhörungen stellen nach Auffassung des eco Verstöße gegen Art. 41 Abs. 2 lit. a) i. V. m. Art. 16 der EU-Grundrechte-Charta dar. Das Recht auf gute Verwaltung umfasst insbesondere das Recht jedes Unternehmens, gehört zu werden, bevor ihm gegenüber eine für es nachteilige individuelle Maßnahme getroffen wird. (Der Vollständigkeit halber wird nochmals darauf hingewiesen, dass soweit man Liste und Technischen Richtlinie nicht als Bestandteil des Sicherheitskatalogs ansieht, keine Rechtsgrundlagen für beides vorhanden sind.)

XI. Längere Umsetzungsfristen für OTT-Anbieter geboten

Mit Umsetzung des EECC ins nationale Recht ist bereits absehbar, dass der der Kreis der Verpflichteten hinsichtlich der Sicherheitsanforderungen im Sinne von § 109 Absätze 6, 4, 2 und 1 TKG deutlich ausgeweitet wird. Dies beinhaltet unter anderen OTT-Anbieter. Die BNetzA gewährt an mehreren Stellen im notifizierten Entwurf Anbietern eine Jahresfrist ab Veröffentlichung des Katalogs, bspw. auf S. 65. Diese Frist richtet sich an klassische Telekommunikationsunternehmen, die bereits über praktische Erfahrung und Wissen und mit den Sicherheitsanforderungen verfügen. Demgegenüber trifft dies auf die erstmalig verpflichteten OTT-Anbieter nicht zu. Die vorgegebenen Sicherheitsanforderungen sind komplex, umfangreich und diffizil zu implementieren. Die betroffenen Unternehmen müssen sich entsprechend zunächst ein ausreichendes Verständnis der technischen Anforderungen erarbeiten und darauf aufbauend ein entsprechendes Umsetzungskonzept, das auf ihre individuellen Anforderungen und Gegebenheiten abgestimmt ist, entwickeln. eco fordert eine angemessene Umsetzungsfrist, bspw. bis 31.12.2025, wie an anderer Stelle im Entwurf, S. 66. Hinzu kommen die Herausforderungen der Implementierung der erforderlichen technischen Vorkehrungen. Auch diesbezüglich fehlen einschlägige Erfahrungen und standardisierte Lösungen und Konzepte. Die bestehenden technischen Systeme der erstmalig betroffenen Unternehmen sind ihrerseits komplex. Implementierungsprozesse in diesem Umfang sind sehr anspruchsvoll und müssen bestmöglich geplant, vorbereitet und gegengetestet werden.

Bei den betroffenen OTT-Anbietern wird allenfalls ein Teil des erforderlichen und notwendigen Personals vorhanden sein, um die notwendigen technischen Vorkehrungen zu installieren, auf die Bestandsysteme anzupassen, zu betreiben und zu warten. Dies führt zu einem neuen, bisher nicht vorhandenen Bedarf bei der Personalbeschaffung, der in einem so speziellen Bereich, schwierig ist und entsprechende Zeit voraussetzt. Dies gilt auch, wenn Teile der erforderlichen Prozesse zur Implementierung an Dritte vergeben werden sollten, da es in diesem Bereich nur wenige Anbieter gibt und somit ein Auftragsstau vorhersehbar der bei Festlegung von längeren Umsetzungsfristen zu berücksichtigen ist.

Nach Auffassung des eco gebietet das der Grundsatz, Ungleiches nicht gleich zu behandeln, Art. 20 i. v. m. Art. 16 EU-Grundrechte-Charta und der Grundsatz der Verhältnismäßigkeit nach Art. 52 Abs. 1 S. 2 EU-Grundrechte-Charta. Die OTT-Anbieter sind im Sinne ungleich zu den klassischen Telekommunikationsunternehmen, da es ob deren erstmaliger Verpflichtung an Wissen, Erfahrung und Best Practices fehlt. Entsprechend ist es konkret verhältnismäßig diesen Anbietern längere Umsetzungszeiten zuzugestehen.
