VERBAND DER INTERNETWIRTSCHAFT E.V.

eco Hauptkritik zum notifizierten Sicherheitskatalog-Entwurf gem. § 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 und der EU-Kommission zur Notifizierung vorgelegt. 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. Im Rahmen des Notifizierungsverfahrens möchten wir zu dem vorgelegten Entwurf unsere Hauptkritikpunkte an der Vereinbarkeit des vorgelegten Sicherheitskatalogs mit europäischen Vorgaben und Grundsätzen darlegen. Ergänzend möchten wir auf unsere ausführliche Stellungnahme zu dem Entwurf für einen Sicherheitskatalog verweisen.

- **Keine Rechtssicherheit auf Grund geplanter Änderungen**

Unter anderem soll § 109 TKG geändert werden. Dessen Absatz 6 ist Rechtsgrundlage für den notifizierten Entwurf. Die Norm soll dazu derart geändert werden, dass sie mit dem zukünftigen BSI-Gesetz, einer zukünftigen Allgemeinverfügung des Bundesministerium des Inneren (Garantieerklärung), der zukünftigen Liste der BNetzA (Entwurf in nationaler Konsultation) und BSI und einer zukünftigen Technischen Richtlinie (TR) des BSI einen Regelungskomplex bilden (vgl. zu Liste u. TR, Nr. 8 der Notifikationsmitteilung). Dieser noch ausstehende Reglungs-komplex ist mit einer erheblichen Rechts- und Planungsunsicherheit für die betroffenen Anbieter behaftet. Dies stellt einen ungerechtfertigten Eingriff in die unternehmerische Freiheit nach Art. 16 EU-Grundrechte-Charta dar.

- **Vereinbarkeit mit Cyber Security Act fraglich**

Nach Ansicht des eco ist eine Anwendung des notifizierten Entwurfs, welche mit dem Cyber Security Act (CSA), EU-Verordnung 2019/881 nicht in Einklang steht, möglich. Die BNetzA und das BSI haben einen sehr weiten Auslegungs- und Anwendungsspielraum außerhalb des CSA. Zudem fehlt eine Anknüpfung an globale und internationale Standards, wie unter anderen 3GPP.

- **Verstoß gegen EU-Binnenmarktprinzip**

eco sieht in den Auflagen der Anlage 2 des Sicherheitskataloges einen Verstoß gegen die Dienstleistungsfreiheit nach Art. 62 i. V. m. Art. 53 Abs. 1 AEUV, konkretisiert durch die Richtlinie 2006/123/EG. Die strengen Auflagen der BNetzA bedeuten derart hohe Auflagen für 5G-Anbieter, die EU-weit tätig sind bzw. dies planen, technische Komponenten entsprechend den deutschen Anforderungen einzukaufen, obwohl andere Mitgliedsstaaten andere Anforderungen stellen. Die Produkte und Dienste der deutschen 5G-Netzbetreiber würden europaweit teurer werden, da die Unternehmen faktisch gezwungen werden, europaweit in ihren TK-Infrastrukturen Komponenten einzusetzen und zu verwenden, welche den deutschen Sicherheitsanforderungen entsprächen. Dies führt außerdem zu einer Wettbewerbsverzerrung, da 5G-Anbieter aus anderen EU-

Mitgliedsstaaten mit erheblich niedrigeren Sicherheitsanforderungen deutlich günstiger ihre Leistungen anbieten können. Eine sachliche Rechtfertigung dieser mittelbaren Diskriminierung ist nicht ersichtlich, da die Vorgaben der BNetzA das erforderliche Maß überschreiten.

- **Auswirkungen Internationaler Handel nicht hinreichend berücksichtigt**

Der vorgelegte Entwurf verstößt entgegen der Einschätzung der vorlegenden Behörden gegen das Agreement on Technical Barriers to Trade-Übereinkommens, vgl. Nr. 16 Notifizierungsmitteilung. Es handelt sich um eine protektionistische Maßnahme, nach der Hersteller vom deutschen Markt ausgeschlossen werden, sofern die Vorgaben des Katalogs und seiner Anlagen nicht eingehalten werden. Anlass für die Regelungen sind Vermutungen gegenüber bestimmten Herstellern und keine tatsächlich belegten Beweise. Rechtsstaatliche Prinzipien gebieten, dass eben nicht Vermutungen Grundlage für den Entzug des Vertrauens sein können, erst recht nicht sachfremde geostrategische, handels-, geo-, außen- oder sonstige politischen Erwägungen.

- **Vertrauenswürdigkeitserklärung verstößt gegen europäische Rechtsgrundsätze**

Begriffe wie Dritte, Sicherheitsbehörden, vertrauliche Informationen sind zu unbestimmt. Einige Punkten können von keinem Hersteller unterzeichnet bzw. zugesichert werden, da rechtlich unmöglich. Dies ist ein Eingriff in die unternehmerische Freiheit, der über das absolut erforderliche Maß hinausgeht. Die Vorgaben stehen auch nicht mit den Zielen der geplanten E-Evidence-VO in Einklang. Mitgliedsstaaten sind jedoch auch an den Effet Utile gehalten, wenn sie absehen können, das nationale Vorschriften mit einer EU-Verordnung, die bereits so konkrete Formen wie die E-Evidence angenommen hat, nicht vereinbar sind. Dann obliegt den EU-Staaten diese kommende Verordnung weitestgehend zu berücksichtigen.

- **Verstoß gegen Notifizierungspflicht oder nationales Recht**

Liste der BNetzA/BSI und Technische Richtlinie des BSI sind entweder rechtlicher Bestandteil des Sicherheitskataloges (Verwaltungsakt in Form der Allgemeinverfügung). Dann gäbe es zumindest eine Rechtsgrundlage mit § 109 Abs. 6 TKG. Dann hätten sie notifiziert werden müssen. Da dies nicht erfolgt ist, hätte die BNetzA gegen die TRIS-RL EU/2015/1535 verstoßen. Sind beide aber nicht Bestandteil des Sicherheitskataloges, gibt es keine Rechtsgrundlagen für beides, weder im EU- noch im nationalen Recht. Das ist ein offensichtlicher Verstoß. In diesem Fall ist EU-Kommission gehalten, Deutschland aufzufordern den notifizierten Entwurf zu ändern oder zurück zu ziehen. Sonst würde das TRIS-Verfahren ad absurdum geführt. Es müsste nach Aufhebung des Entwurfs erneut durchgeführt werden. 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.

- **Vertrauensschutz nicht gewährleistet**

Für die Verpflichtung einzelne Komponenten aus dem Netz entfernen zu müssen (2.4 des Entwurfs, S. 66), falls die Zertifizierung auf Grund behördlicher Entscheidung nachträglich entzogen wird, existiert weder im EU- noch im deutschen Recht eine ausreichende Rechtsgrundlage. Eine solche Rechtsgrundlage müsste zudem ob ihrer Eingriffsintensität den Parlamentsvorbehalt erfüllen. Offen bleibt zudem, wie betroffenen Netzbetreibern Rechtsschutz gewährt wird, wenn sie zur Ersetzung einzelner Komponenten verpflichtet sein sollen, sollte nach Einbau die Zertifizierung der Komponente entfallen. 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. Die Nachvollziehbarkeit des Verwaltungshandelns der zertifizierenden Behörde ist auch offen. Denn oft dürften geheimdienstliche Informationen eine Rolle spielen, die der Behörde nicht zugänglich sind. Darüber hinaus ist dies ein Eingriff in das Eigentum des Netzbetreibers für das er keinen Anlass gegeben hat und nicht in seiner Verantwortung liegt. Dafür ist der betroffene Netzbetreiber durch den Staat zu entschädigen, wie bei einem enteignungsgleichen Eingriff. Eine solche Entschädigungsregel ist bisher nicht vorgesehen.

- **Anhörung nicht erfolgt**

Der hier notifizierte Entwurf wurde nicht angehört. Es wurde lediglich eine Anhörung zu einem Entwurf des Sicherheitskataloges im Herbst 2019 durchgeführt. Dieser unterschied sich jedoch wesentlich und in erheblichem Umfang vom notifizierten Entwurf. Der zur Notifizierung vorgelegte Entwurf ist daher nicht angehört worden, bevor er notifiziert wurde. Dies stellt einen Verstoß gegen Art. 41 Abs. 2 lit. a) der EU-Grundrechtecharta dar.

- **Längere Umsetzungsfristen für OTT-Anbieter geboten**

Mit Umsetzung des EECC ins nationale Recht ist bereits absehbar, dass der Kreis der Verpflichteten hinsichtlich der Sicherheitsanforderungen im Sinne von § 109 Absätze 6, 4, 2 und 1 TKG deutlich ausgeweitet wird, bspw. auf OTT-Anbieter. Die BNetzA gewährt klassischen Telekommunikationsunternehmen 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. Entsprechend müssen sie 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. Dies erfordert eine angemessene Umsetzungsfrist. Wir schlagen eine Frist bis zum 31.12.2025 vor, wie auch auf S. 65 des notifizierten Entwurfs. Nach Auffassung des eco gebietet das der Grundsatz der Verhältnismäßigkeit nach Art. 52 Abs. 1 S. 2 EU-Grundrechte-Charta.

Über eco: Mit über 1.100 Mitgliedsunternehmen ist eco der größte Verband der Internetwirtschaft in Europa. Seit 1995 gestaltet eco maßgeblich das Internet, fördert neue Technologien, formt Rahmenbedingungen und vertritt die Interessen seiner Mitglieder gegenüber der Politik und in internationalen Gremien. Leitthemen sind Zuverlässigkeit und Stärkung der digitalen Infrastruktur, IT-Sicherheit und Vertrauen sowie Ethik und Selbstregulierung. Deshalb setzt sich eco für ein freies, technikneutrales und leistungsstarkes Internet ein.