VERBAND DER INTERNETWIRTSCHAFT E.V.

Stellungnahme zur Liste der kritischen Funktionen für öffentliche Telekommunikationsnetze und -dienste mit erhöhtem Gefährdungspotenzial

Berlin, 30.09.2020

Die Bundesnetzagentur hat gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik den Entwurf einer Liste der kritischen Funktionen öffentlicher Telekommunikationsnetze veröffentlicht. Darin sollen kritische Funktionen in 5G-Mobilfunknetzen benannt werden.

eco und seine Mitgliedsunternehmen setzen sich für die Stärkung der Sicherheit und der Integrität von ITK-Systemen ein. Dieses Ziel verfolgen auch die Bundesnetzagentur und das Bundesamt.

Nachfolgend möchten wir unsere Bedenken an dem vorgelegten Entwurf für eine Liste, mit der kritische Funktionen in 5G-Mobilfunknetzen benannt werden sollen, darlegen.

I. Anwendungsbereich

Für eco ist nicht nachvollziehbar, warum der Anwendungsbereich des Listen-Entwurfs derart unklar geregelt ist. Im Titel wird von „erhöhtem Gefährdungspotential“ gesprochen. Die Anlage 2 des Sicherheitskataloges, welche durch die Liste ergänzt werden soll, verwendet ebenso den Begriff „erhöhtes Gefährdungspotential“.

Im Katalog selbst wird dann auf S. 37f, 5.1.3 erläutert, dass erhöhtes Gefährdungspotential“ dann besteht, wenn „erhöhte Kritikalität“ anzunehmen sei. Erhöhte Kritikalität hätten derzeit nur 5G-Mobilfunknetze, führt die BNetzA an vorgenannter Stelle aus.

Der Anwendungsfreundlichkeit und der Bestimmtheit wegen hält es eco für geboten, die Liste dementsprechend klar zu bezeichnen und vor allem den Anwendungsbereich klar zu beschreiben. Eine entsprechende Anpassung des Titels der Anlage 2 sollte insofern auch vorgenommen werden. Sollten allerdings die unklaren Bezeichnungen und die unbestimmten Anwendungsbereiche der Liste sowie der Anlage 2 des Sicherheitskataloges darauf abzielen, die Anwendungsbereiche auf weitere Netze neben den 5G- Mobilfunkanbieter auszudehnen, lehnt eco dies strikt ab. Dies wäre insbesondere bezogen auf kleine und mittlere Unternehmen eine Verletzung des Verhältnismäßigkeitsgrundsatzes.

II. Notifizierungsverfahren und Rechtsgrundlage

Nach Ansicht des eco hat die Bundesnetzagentur gegen die TRIS-Richtlinie EU/2015/1535 verstoßen. Der vorliegende Listen-Entwurf wurde nicht mit dem Entwurf des Sicherheitskatalogs notifiziert. Das hätte die Bundesnetzagentur aber tun müssen, da es sich um dieselbe Rechtsgrundlage wie beim Katalog selbst handelt, und zwar § 109 Abs. 6 TKG. Dafür spricht der Untertitel des Entwurfs „Ergänzung zur Anlage 2 des Katalogs von

Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 Abs. 4 Telekommunikationsgesetz“. Der Listen-Entwurf steht ausweislich des Titels im Zusammenhang mit § 109 Abs. 4 TKG. Diese Norm enthält in Satz 2 die Pflicht für Netzbetreiber zur Vorlage eines Sicherheitskonzepts. Normadressat sind die Netzbetreiber. Die Befugnis der BNetzA beschränkt sich auf die Prüfung der Sicherheitskonzepte und die nachträgliche Aufforderung zur Beseitigung von Mängeln oder bei dessen Umsetzung. Auch die anderen Absätze von § 109 enthalten keine Ermächtigungsgrundlage zum Erlass der Liste, insbesondere nicht Absätze 1 und 2. Beide adressieren alleine die Unternehmen mit Pflichten. Der Inhalt des Sicherheitskonzeptes wird maßgeblich bestimmt durch den Katalog von Sicherheitsanforderungen gem. § 109 Abs. 6 TKG. Demzufolge wäre, wenn überhaupt, § 109 Abs. 6 i. V. m. Absatz 4 S.2 TKG eine Rechtsgrundlage. Die Liste wäre insofern rechtlich Teil des Verwaltungsaktes (in Form einer Allgemeinverfügung) des Sicherheitskataloges.

Zudem hat eco erhebliche Zweifel, dass § 109 Abs. 4 bzw. Absatz 6 i. V. m. Abs. 4 S. 2 TKG eine ausreichende Rechtsgrundlage darstellt. Erstens hätte der Bundesbeauftrage für Datenschutz und Informationsfreiheit an der Erstellung des Listen-Entwurfes beteiligt werden müssen, wenn § 109 Absatz 6 i. V. m. Abs. 4 S. 2 TKG die Ermächtigungsgrundlage sein soll. Das ergibt sich aus dem Wortlaut von 109 Abs. 6 TKG. Nach Plänen des Gesetzgebers soll er auch in Zukunft beteiligt werden, vgl. § 109 Abs. 4 S. 4 TKG-E (Gesetzesvorhaben IT-SiG 2.0, Stand 12.05.2020). Des Weiteren soll die Liste kritische Funktionen in 5G Netzen benennen und in Verbindung mit einer noch nicht erstellten Technischen Richtlinie des BSI wesentliche Vorgaben zur Zertifizierung von Komponenten machen. Eine solche Zertifizierung ist gesetzlich aber noch nicht geregelt. Hierzu soll vielmehr erst zukünftig eine gesetzliche Regelung geschaffen werden, dies entweder in einem Gesetzesvorhaben zum TKG oder dem eines IT-Sicherheitsgesetzes.

In einem bekannt gewordenen inoffiziellen Referenten-Entwurf wird eine Neufassung des § 109 TKG wie folgt vorgeschlagen: *„Darüber hinaus sind auch Einzelheiten der Festlegung kritischer Funktionen und der Bestimmung der kritischen Komponenten im Sicherheitskatalog festzulegen. Dabei legen die zuständigen Behörden insbesondere fest, welche Funktionen eines Netzes /Dienstes als kritisch eingestuft werden und wie die Netzbetreiber und Diensteerbringer ausgehend von dieser behördlichen Festlegung ableiten, ob eine bestimmte Komponente eine kritische Funktion erfüllt und folglich der Zertifizierungspflicht unterfällt.“*

Mit der geplanten Neuregelung kommt zum Ausdruck, dass auch die Entwurfsverfasser gesetzliche Regelungen zu Festlegungen kritischer Komponenten im Sicherheitskatalog als erforderlich ansehen. Wenn § 109 Absatz 6 i. V. m. Abs. 4 S. 2 TKG eine ausreichende Ermächtigungsgrundlage wäre, bedürfte es keiner noch zu erfolgenden Neuregelung.

Festzuhalten ist, dass gegen die Notifizierungspflicht verstoßen wurde, indem die Liste nicht mitangemeldet wurde. Zudem gibt es de lege lata keine Rechtsgrundlage für den Erlass der Liste durch die BNetzA/BSI.

III. Eignung der Liste

eco sieht kritisch, dass der Umfang der Liste in unvorhersehbarer Weise erweitert werden könnte. Im Entwurf heißt es dazu: „*gelisteten Funktionen stellen keine abgeschlossene Menge dar, sondern sind als Mindestanforderung zu verstehen*“. Wenn dies als eine Verbindung zu den o. g. Gesetzesvorhaben zu sehen sein soll, ist das nicht sachdienlich und zu unbestimmt, zudem gefährdet es weiter die Planungs- und Investitionssicherheit der ausbauenden Unternehmen und hemmt so den Ausbau.

Nicht nachvollziehbar ist insofern auch die Begrifflichkeit einer „Mindestanforderung“. Inwiefern kann eine Liste eine „Mindestanforderung“ darstellen, obschon sie nur kritische Funktionen nennt. Hier sehen wir Änderungs- bzw. Präzisierungsbedarf.

Zudem eignet sich die Liste nach Auffassung des eco nur bedingt zur Verbesserung der Sicherheit von Kommunikationsnetzen. Denn es werden abstrakt Funktionen benannt, ohne zu differenzieren in welchem Bereich eines Netzes Komponenten mit den genannten Funktionen konkret als kritisch anzusehen sind. Dieser Ansatz ist nicht zielführend.

Ohne Kenntnis, um welche Netzebene bzw. -bestandteile es sich konkret handelt, kann vielmehr keine zutreffende Risikoanalyse vorgenommen werden. Sachgerechter und zielführender wäre es, wenn je Funktionskategorie eine Benennung von Kriterien und deren Ausprägungen durch die Behörden erfolgt, anhand derer bewertet werden kann, ob und inwieweit die von einem Netzbetreiber oder Dienstanbieter gewählten Gestaltungsoptionen bei der Realisierung einer Funktion diese als kritisch, weniger kritisch oder unkritisch erscheinen lassen.

Im Hinblick auf Angriffe gegen die Vertraulichkeit und Integrität von Fernmeldeverkehr sieht eco als Kriterien mit Relevanz an:

- Relative Aggregation der Verarbeitung von Fernmeldeverkehr in einzelnen Knoten eines Telekommunikationsnetzes oder einer Dienstplattform.

- Klassifizierung der von einem Knoten verarbeiteten Fernmeldedaten hinsichtlich ihrer Vertraulichkeit.

- Weiterhin ist zu berücksichtigen, dass ein aus Anwendersicht über das Fernmeldegeheimnis hinausgehender Schutzbedarf beim Transport über öffentliche Telekommunikationsnetze auf Applikationsebene durch geeignete technische Mittel zu realisieren ist und somit diese Daten vor einem unautorisierten Zugriff über die am Transport beteiligten Netzknoten in der Regel geschützt sind.

Bezogen auf das Angriffsszenario einer Verfügbarkeit von Telekommunikationsdiensten wären nach Ansicht des eco als relevante Kriterien zu nennen:

- der Umfang der technischen Diversität funktional identischer Knoten eines Netzes oder einer Dienstplattform und die damit zusammenhängenden Auswirkungen eines absichtlich herbei geführten Ausfalls von Knoten gleicher technischer Bauweise auf die Versorgung der

Bevölkerung mit Telekommunikationsdiensten (z. B. lokale, regionale oder landesweite Betroffenheit).

- die Arten von Telekommunikationsdiensten, die von einem solchen angenommenen Ausfall betroffenen wären (z. B. mobile Sprachdienste, mobile Datendienste).

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, schafft Rahmenbedingungen und vertritt die Interessen seiner Mitglieder gegenüber der Politik und in internationalen Gremien. Die Zuverlässigkeit und Stärkung der digitalen Infrastruktur, IT-Sicherheit und Vertrauen sowie eine ethisch orientierte Digitalisierung bilden Schwerpunkte der Verbandsarbeit. eco setzt sich für ein freies, technikneutrales und leistungsstarkes Internet ein.