VERBAND DER INTERNETWIRTSCHAFT E.V.

STELLUNGNAHME

zu dem von der BNetzA vorgelegten Entwurfs des Katalogs von Sicherheitsanforderungen nach § 167 TKG

Berlin, 16.01.2026

Die Bundesnetzagentur hat einen überarbeiteten Entwurf des Katalogs von Sicherheitsanforderungen nach § 167 Telekommunikationsgesetz (TKG) vorgelegt. Der Katalog definiert die verbindlichen technischen und organisatorischen Vorgaben, mit denen Anbieter öffentlicher Telekommunikationsnetze und -dienste die Sicherheit und Funktionsfähigkeit ihrer Infrastrukturen sicherstellen müssen.

Der Sicherheitskatalog wird auf Grundlage des § 167 Abs. 1 TKG im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik sowie der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit fortgeschrieben. Mit der aktuellen Überarbeitung verfolgt die Bundesnetzagentur das Ziel, die bestehenden Vorgaben weiterzuentwickeln und an veränderte Bedrohungslagen sowie an den fortgeschrittenen Stand der Technik anzupassen. Vor dem Hintergrund zunehmender Komplexität und Vernetzung moderner Telekommunikationsnetze kommt dieser Aktualisierung besondere Bedeutung zu.

Für die betroffenen Unternehmen entfaltet der Sicherheitskatalog erhebliche praktische Relevanz. Er ist maßgeblicher Referenzrahmen für die Erstellung unternehmensinterner Sicherheitskonzepte und konkretisiert die Anforderungen an technische Schutzmaßnahmen, organisatorische Prozesse und Risikomanagementstrukturen. Damit wirkt er nicht nur unmittelbar auf betriebliche Abläufe und Investitionsentscheidungen, sondern auch auf die regulatorische Ausgestaltung von Netz- und Dienstestrukturen ein.

eco bedankt sich für die Möglichkeit, den überarbeiteten Katalog von Sicherheitsanforderungen zu kommentieren und möchte folgende Punkte adressieren:

1. Grundsätzliches

- Es wird im Rahmen des Sicherheitskataloges eine weitere Einstufung der Anbieter vorgenommen. Diese ähnelt zwar der Einstufung nach NIS2 und KritisVO ist aber nicht identisch (und auch die Verpflichtungen unterscheiden sich erheblich). Dies führt zu unnötiger Rechtsunklarheit, die verfassungsrechtlichen Bedenken begegnet. Zudem kommt es zu unnötiger Doppelregulierung, da auch die Umsetzung der NIS2-RL schon Sicherheitsmaßnahmen, Risikoanalysen und Meldepflichten enthält. Dies führt zu weiterer, unnötiger Bürokratisierung im TK-Sektor durch erhebliche Dokumentationspflichten.

- Fehlen eines risikobasierten Ansatzes in der Zuordnung der Unternehmen zu den Gefährdungsklassen: Bestimmte Anbieter komplett in die höchste Kategorie zu stufen und die damit einhergehenden hohen Anforderungen an jeder Stelle der Telekommunikationsinfrastruktur anzulegen, ist nicht sachgerecht und auch nicht umsetzbar. Eine Gefährdung ist nicht an jeder Stelle gegeben. Deshalb ist es wichtig, nach Schutzbedarf der jeweiligen Anlage/Komponenten zu unterscheiden und nur da die hohen Anforderungen zu stellen, wo es tatsächlich notwendig ist. Hier wird bei der Bewertung der Gefährdung nicht mehr unterschieden nach der Anzahl der Kunden oder Standorte, und auch nicht welche Dienste oder Netze betrieben werden – die reine Einordnung nach Unternehmensgröße ist dafür nicht zweckmäßig.

  Zur Verdeutlichung soll folgendes Beispiel dienen:

  Ein Unternehmen fungiert als Vorlieferant für ein mit ihm verbundenes Unternehmen. Dieses verbundene Unternehmen erbringt VoIP-Dienstleistungen gegenüber Endkunden. Die Leistungen werden dabei über das öffentliche Internet erbracht. Weiterhin bietet das verbundene Unternehmen Mobilfunkleistungen im MVNO-Modell an. In dieser Konstellation ist festzustellen, dass sowohl VoIP-Anbieter wie auch MVNO nicht die Kontrolle über den gesamten Signalweg haben. Mangels Kontrolle über den gesamten Signalweg sind die Anforderungen für den Vorlieferanten nicht in vollem Umfang umzusetzen.

  In derlei Konstellationen sollte für Anbieter eine ausdrückliche Ausnahme vorgesehen werden, die zwar nominell unter das erhöhte Gefährdungspotential fallen (durch MA-Anzahl und/oder Umsatz), bei denen es aber beispielsweise an der tatsächlichen (Ende-zu-Ende) Kontrolle über die Signalübertragung fehlt. In diesen Fällen ist das Risiko als geringer anzusehen als bei "herkömmlichen" TK-Diensten (vgl. auch EKEK, Erwägungsgrund 95). So können VoIP-Anbieter und MVNOs nicht in das erhöhte Gefährdungspotential fallen, da diesen Anbietern die tatsächliche Kontrolle (Ende-zu-Ende) über die Signalübertragung fehlt.

- Die Anforderungen sind insgesamt viel zu konkret und detailliert formuliert. Da die Technik schnell voranschreitet, besteht hier die Gefahr, dass die Anforderungen sehr schnell veralten (vorrangig in Teil C – technische Spezifikationen). Der Fokus sollte auf generelle Schutzziele (jeweilige Maßnahme zielführend für entsprechenden Schutzzweck) gelegt werden.

- Die Umsetzungsfrist von einem Jahr, auf die die BNetzA hinweist (S. 12 des Entwurfes) ist insgesamt zu kurz bemessen. Dies gilt insbesondere für Unternehmen, die erstmalig von den Festlegungen des Sicherheitskataloges betroffen sind. Bei der Bemessung der Umsetzungsfrist ist der erhebliche Umsetzungsaufwand für die betroffenen Unternehmen hinreichend zu berücksichtigen. Zwar enthält der § 167 Abs. 3 TKG dem Grunde nach eine Regelumsetzungsfrist von einem Jahr. Die Regelung sieht jedoch ebenfalls die Befugnis der BNetzA vor, die Umsetzungsfrist im Sicherheitskatalog zu verlängern und räumt der ihr in diesem Zusammenhang einen Ermessensspielraum ein. Dieses Ermessen sollte die BNetzA auch ausüben. Dem Entwurf ist allerdings nicht zu entnehmen, dass eine Auseinandersetzung mit der

Möglichkeit der Verlängerung der Umsetzungsfrist in Form einer Abwägung des Für und Wider stattgefunden hat. Vielmehr scheint die BNetzA von einer starren Umsetzungsfrist bzw. der Pflicht zur Festlegung der einjährigen Umsetzungsfrist ausgegangen zu sein, was in der Sache einen Ermessensausfall begründet. Eine auskömmliche - sämtliche betroffenen Interessen hinreichend in Ausgleich bringende - Umsetzungsfrist darf im vorliegenden Falle einen Zeitraum von mindestens 24 Monaten nicht unterschreiten.

2. Beurteilungsspielraum BNetzA

Anders als im Katalog unterstellt wird, steht der BNetzA kein Beurteilungsspielraum bei der Anwendung und Konkretisierung der einschlägigen unbestimmten Rechtsbegriffe zu. Denn die Anforderungen an einen solchen Beurteilungsspielraum sind nicht erfüllt. Vielmehr sind die Festlegungen des Kataloges gerichtlich vollumfänglich überprüfbar.

Der Katalog lässt außer Acht, dass exekutive Beurteilungsspielräume nach ständiger Rechtsprechung nur in eng umgrenzten Bereichen und unter besonderen Voraussetzungen, die restriktiv auszulegen sind, ausnahmsweise angenommen werden können. Denn anders als mit Blick auf den der Verwaltung auf Rechtsfolgenebene zustehenden Ermessensspielraum, hinsichtlich dessen bereits kraft des gesetzlichen Regelungskonzepts des § 40 VwVfG sowie § 114 VwGO nur eine beschränkte – auf Ermessensfehler zugeschnittene – Kontrolldichte der Verwaltungsgerichte besteht, entspricht es der gesetzlichen Regel, dass unbestimmte Rechtsbegriffe gerichtlich voll überprüfbar sind. Die Gerichte sind also bei der Auslegung und Anwendung unbestimmter Rechtsbegriffe nicht an die behördlichen Feststellungen und Wertungen gebunden und entscheiden abschließend über die richtige Auslegung der Begriffe. Anders als auf Rechtsfolgenseite besteht somit bei der Auslegung und Anwendung unbestimmter Rechtsbegriffe grundsätzlich kein Entscheidungsspielraum der Verwaltung im Sinne einer der gerichtlichen Kontrolle – partiell – entzogenen Letztentscheidungskompetenz. Dies gebietet letztlich auch der durch Art. 19 Abs. 4 GG garantierte effektive Rechtsschutz. Denn mit jeder Beschränkung der gerichtlichen Kontrolldichte gehen Rechtsschutzdefizite einher, die es zu rechtfertigen gilt (so etwa BVerfGE 129, 1 (22 f.) = NVwZ 2011, 1062).

Die Rechtsprechung hat verschiedene Fallgruppen entwickelt, in denen die Annahme eines Beurteilungsspielraums gerechtfertigt erscheint. Der Katalog stützt die Annahme des Beurteilungsspielraums vorrangig auf die Fallgruppe der Entscheidungen unabhängiger Sachverständiger und pluralistisch besetzter Ausschüsse bzw. Gremien (S. 17 des Entwurfs). Die Rechtsprechung stellt jedoch selbst bei solchen Entscheidungen hohe Anforderungen an die Annahme eines Beurteilungsspielraums. In abstrahierter Betrachtung kann ein Beurteilungsspielraum nämlich nur dann angenommen werden, wenn es sich um eine besonders komplexe – vor Gericht auch unter Einholung sachverständiger Hilfe nicht ohne Weiteres rekonstruierbare – Entscheidungsfindung handelt (so etwa BVerwGE 153, 129 = NVwZ-RR 2016, 142 Rn. 37) und die mit der Einschränkung der verwaltungsgerichtlichen Kontrolldichte einhergehende Beeinträchtigung des effektiven Rechtsschutzes durch besondere Elemente auf der Ebene

der Gremienentscheidung kompensiert wird. Dies ist allerdings nur dann der Fall, wenn das Gremium derartig pluralistisch besetzt ist, dass mögliche Auffassungsunterschiede bereits in sich zum Ausgleich gebracht werden und die zu treffende Entscheidung damit zugleich versachlicht wird (vgl. BVerwG, NVwZ 2008, 575; NJW 2008, 2135; NVwZ 2007, 1431 m.w. Nachw.), oder, wenn das Gremium aufgrund seiner Aufgabenstellung, Unabhängigkeit und Sachkunde Elemente einer kompensatorischen demokratischen Repräsentation und Kontrolle aufweist.

Diese Voraussetzungen sind jedoch nicht erfüllt. Die BNetzA entscheidet der Erläuterung im Katalog nach „zusammen mit den Sachverständigen für Informationstechnik und Datenschutz“ über die Auslegung der unbestimmten Rechtsbegriffe aus den §§ 165 ff. TKG. Weder ist klar, wie dieses entscheidende Gremium konkret zusammengesetzt ist; eine pluralistische – einen Interessenausgleich und eine Versachlichung der Entscheidung bereits auf exekutiver Ebene sicherstellende – Besetzung würde nämlich gerade auch eine operative Beteiligung der Unternehmensseite voraussetzen, da die Unternehmen als unmittelbare Adressaten fungieren. Noch ist ersichtlich, dass das entscheidende Gremium Elemente einer kompensatorischen demokratischen Repräsentation und Kontrolle aufweist; vielmehr handelt es sich offensichtlich schlichtweg um eine Beteiligung von Sachverständigen an einer einseitig hoheitlichen Maßnahme der BNetzA. In diesem Falle einen Beurteilungsspielraum anzunehmen, würde zu einer empfindlichen – nicht gerechtfertigten – Beschneidung der betroffenen Unternehmen in der ihnen nach Art. 19 Abs. 4 GG zustehenden Garantie auf effektiven Rechtsschutz führen. Es entstünde ein aus der Perspektive der in Art. 19 Abs. 4 GG verankerten Rechtsschutzgarantie nicht hinnehmbares Vakuum exekutiver Letztentscheidungskompetenz ohne effektive Schranken, die einen funktionalen Grundrechtsschutz zugunsten der betroffenen Unternehmen zu gewährleisten tauglich wären. Dies wird nicht zuletzt verstärkt durch den Umstand, dass sämtliche technisch-inhaltlichen Wertungen und Einschätzungen, die die BNetzA im Rahmen der Festlegung vornimmt, vor Gericht vollumfänglich rekonstruierbar und – unter Beteiligung von Sachverständigen – auch nachvollziehbar sind (hierzu BVerwGE 81, 12 (17) = NVwZ-RR 1990, 134, 136), mithin insgesamt kein Anlass für die Annahme eines Beurteilungsspielraums besteht.

Ein Beurteilungsspielraum lässt sich auch nicht etwa auf den Umstand stützen, dass es sich um eine Prognoseentscheidung bzw. Risikobewertung handelt (so im Entwurf auf S. 17 beiläufig erwähnt). Denn auch solche Prognoseentscheidungen und Risikobewertungen sind grundsätzlich vollumfänglich gerichtlich überprüfbar; Ausnahmen sind nach der Rechtsprechung nur in eng umgrenzten Fällen denkbar, wenn die gesetzliche Ermächtigungsgrundlage eine solche Beurteilungsermächtigung enthält und es sich um komplexe Sachverhalte und weit in die Zukunft reichende Entwicklungen handelt, die zudem ein hohes Maß an Unsicherheit aufweisen, mithin vor Gericht nicht ohne Weiteres rekonstruierbar sind. Hier ist jedoch – abgesehen von der bereits erwähnten hinreichenden Rekonstruierbarkeit der Entscheidung – keine Beurteilungsermächtigung in der gesetzlichen Ermächtigungsgrundlage erkennbar. Denn die von der BNetzA hervorgehobene Formulierung, dass sie in dem Sicherheitskatalog „Einzelheiten der nach § 167 Abs. 1 bis 7 TKG zu treffenden technischen Vorkehrungen und sonstigen Maßnahmen unter Beachtung der verschiedenen Gefährdungspotenziale“ festlegt, ist

nichts weiter als eine normative Spezifikation des Inhaltes und der Reichweite der Festlegungskompetenz.

3. Stand der Technik

Der im Katalog verwendete Begriff des „Stands der Technik“ ist als unbestimmter Rechtsbegriff auslegungsbedürftig und bedarf daher einer präzisen, am deutschen Rechtsverständnis orientierten Konkretisierung. Nach gefestigter Rechtspraxis ist der Stand der Technik nicht mit der jeweils besten verfügbaren Technik gleichzusetzen. Vielmehr beschreibt er den Entwicklungsstand fortschrittlicher technischer Verfahren, Einrichtungen oder Betriebsweisen, der sich in der Praxis bewährt hat und dessen Eignung zur Erreichung des jeweiligen Schutzziels allgemein anerkannt ist. Entscheidend ist dabei eine verhältnismäßige, risikoorientierte und praktikable Umsetzung, die sich am realistisch Zumutbaren für die verpflichteten Unternehmen orientiert.

Der Gesetzgeber hat sich bewusst gegen den strengeren Maßstab des „Stands von Wissenschaft und Technik“ entschieden, der regelmäßig die jeweils neuesten, teilweise noch nicht hinreichend erprobten Erkenntnisse erfassen würde.

Rechtsterminologisch ist klar zwischen den Begriffen „anerkannte Regeln der Technik“, „Stand der Technik“ und „Stand von Wissenschaft und Technik“ zu differenzieren. Dabei gehen mit den verschiedenen Begriffen jeweils verschiedene technische Anforderungsprofile einher. Während die „anerkannten Regeln der Technik“ die Einhaltung des allgemein wissenschaftlich Anerkannten umfassen, stellt der „Stand von Wissenschaft und Technik“ auf die neuesten technischen und wissenschaftlichen Erkenntnisse ab, nimmt also weniger eine auf den status quo ausgerichtete, sondern vielmehr eine zukunftsorientierte Perspektive ein. Der „Stand der Technik“ steht zwischen diesen Begriffen, verzichtet zwar auf die schon erreichte allgemeine Anerkennung, die für die „anerkannten Regeln der Technik“ gefordert ist, erfordert jedoch gleichwohl eine praktische Bewährtheit. Der „Stand der Technik“ beschreibt damit einen fortgeschrittenen Entwicklungsstand, der zur Erreichung bestimmter praktischer Schutzzwecke als gesichert angesehen werden darf und gibt wieder, was technisch notwendig, geeignet, angemessen und vermeidbar ist. Was zum Stand der Technik gehört, wird durch das Heranziehen vergleichbarer Verfahren, Einrichtungen und Betriebsweisen, die mit Erfolg in der Praxis erprobt worden sind, festgelegt.

Eine Auslegung des Stands der Technik als zwingende Verpflichtung zur stets besten verfügbaren Technik liefe dieser Differenzierung zuwider und würde den gesetzlich vorgesehenen Abwägungsspielraum der Unternehmen bei der Wahl der dem Stand der Technik entsprechenden Umsetzungsmethode unterlaufen. Vor diesem Hintergrund sollte der Katalog klarstellen, dass der Stand der Technik dynamisch zu verstehen ist und technologische Entwicklungen nur insoweit berücksichtigt werden, als sie sich in der Praxis bewährt haben und unter Berücksichtigung von Aufwand, Nutzen und Risiko angemessen implementierbar sind.

4. Bestimmung von Gefährdungspotenzialen

- Das dreistufige Gefährdungspotential des Entwurfs weicht von der Vfg. Nr. 63/2021 ab. Dort war nur 5G mit Netz als erhöhter Kritikalität eingestuft. Jetzt sind alle Netze von Betreibern mit mind. 50 Mitarbeitern und mehr Jahresumsatz als 10 Millionen erfasst. Daraus folgt Ausweitung auf alle Netze, was sehr weitreichend ist.

- Jedoch sollte nicht die gesamte Unternehmensgröße als Maßstab dienen, sondern vielmehr die Größe der TK-Service-Bereiche. An dieser Stelle wäre eine Korrelation mit NIS2 sinnvoll, wonach von einem normalen Gefährdungspotenzial bei einem Wert von unter 50 MA bzw. wichtigen Einrichtungen auszugehen ist. Gehobenes Gefährdungspotenzial läge dementsprechend bei einem Wert von über 50 MA bzw. wesentlichen Einrichtungen vor. Ein erhöhtes Gefährdungspotenzial wäre dann bei Betreibern kritischer Anlagen, die auch unter die KRITIS-VO fallen würden, allerdings unabhängig von der Unternehmensgröße, sondern nach ihrer Bedeutung für das Gemeinwesen, anzunehmen.

- Darüber hinaus besteht dringender Klarstellungsbedarf hinsichtlich des Anwendungsbereichs von Kapitel 5.1 des Sicherheitskatalogs. Die in der Allgemeinverfügung in Teil A unter Nr. 3 c) (S. 12) getroffene Formulierung legt nahe, dass die im Sicherheitskatalog (Abschnitt B) Kapitel 5.1 genannten Anforderungen und insbesondere die Tabelle 1 („Liste der festgelegten kritischen Funktionen“ gemäß § 167 Abs. 1 Nr. 2 TKG) für alle Unternehmen mit erhöhtem Gefährdungspotenzial – also sowohl für Betreiber nach i) als auch für Betreiber nach ii) – gelten sollen.

  Eine solche Auslegung stünde jedoch im klaren Widerspruch zur Struktur des Sicherheitskatalogs, der die Anwendbarkeit von Kapitel 5 primär an den Betrieb eines 5G-Netzes knüpft. Zwar enthält Kapitel 5.1 Regelungen und Funktionsbeschreibungen, die technisch auch in 3G-, 4G- und modernen Festnetzen vorkommen; dies kann jedoch nicht implizieren, dass die bisher ausschließlich für die vier 5G-Netzbetreiber geltenden besonders strengen Anforderungen künftig stillschweigend auf eine große Zahl weiterer Telekommunikationsnetzbetreiber sowie – über die Verweisung auf Artikel 2 Nr. 1 CER-RL – zusätzlich auf Betreiber kritischer Einrichtungen ausgeweitet werden sollen.

  Sollte eine solche weite Anwendung tatsächlich intendiert sein, hätte dies erhebliche regulatorische, technische und wirtschaftliche Konsequenzen. Aus Sicht der betroffenen Wirtschaft ist daher eine präzise Abgrenzung unerlässlich.

  Es sollte klarstellt werden, dass Kapitel 5.1 ausschließlich für Betreiber eines öffentlichen Mobilfunknetzes der 5. Generation (i) gelten soll – oder alternativ deutlich gemacht werden, falls tatsächlich eine Ausweitung auf die Betreiber nach ii) beabsichtigt ist. Eine solche Transparenz ist notwendig, um Rechts- und Planungssicherheit zu gewährleisten und unbeabsichtigte regulatorische Ausweitungen zu vermeiden.

- Die Anzahl von Mitarbeitern und/oder Umsatzzahlen spiegeln nicht die Bedeutung für das Gemeinwohl wider. So ist der prozentuale Anteil am Gesamtmarkt trotz Erreichens der Umsatzgrenze für das erhöhte Gefährdungspotential sehr gering. Hier bestehen gegen die alleinige Heranziehung der Merkmale MA-Anzahl/Umsatz erhebliche Bedenken vor dem Hintergrund des Gleichbehandlungsgrundsatzes aus Art. 3 GG.

5. Unternehmensführung und Sicherheitsmanagement

- 4.2. des Katalogs sieht im Rahmen der Erforderlichkeit vor, dass im Falle von Unternehmen mit gehobenem und erhöhtem Gefährdungspotenzial das gesamte Personal über die Festlegung detaillierter Netz- und Informationssicherheitsrichtlinien zu informieren ist. Sinnvoller wäre es, lediglich mit der Technik betraute Personen entsprechend zu informieren.

- Eine Definition zu Sicherheitsfunktionen, in die das Personal förmlich einzusetzen ist, ist im Entwurf nicht enthalten.

- Auch hinsichtlich der gesicherten Nachvollziehbarkeit der Lieferkette in sicherheitsbezogenen Aspekten fehlt es an einer Konkretisierung, was Sicherheitsaspekte in diesem Zusammenhang sind. Beispielsweise für Hardware-Lieferketten ist dies überhaupt nicht zu leisten, da es keine Durchgriffsmöglichkeiten über alle Instanzen gibt.

- In Bezug auf die Sicherheit bei Abhängigkeiten von Dritten ist dem Entwurf nicht klar zu entnehmen, ob Sicherheitsziele und Sicherheitsstandards, die für das verpflichtete Unternehmen gelten, für „Lieferanten von Dritten“ oder für „Lieferanten als Dritte“ verpflichtend und vertraglich sicherzustellen sind.

6. Sicherheit im Personalmanagement

- Im Rahmen des Personalmanagements ist je nach Aufgabe und Verantwortlichkeit eine angemessene Überprüfung der Vertraulichkeit, Unabhängigkeit und Integrität des Personals durchzuführen. Eine solche Überprüfung kann sich im Einzelfall schwierig gestalten, vor allem bei Lieferanten im Ausland. Hier wird das verpflichtete Unternehmen wenig realistische Möglichkeiten zur Umsetzung der Anforderungen haben.

- Darüber hinaus ist auch nicht klar, wie die jeweiligen Überprüfungen ausgestaltet sein sollen. Eine Definition der Überprüfungsmaßnahmen oder des -rahmens gibt der Entwurf nicht vor.

- Jedenfalls sollen Überprüfungen des Personals in Schlüsselpositionen erfolgen, sofern erforderlich. Auch hier mangelt es an einer Definition, wann das Kriterium einer Schlüsselposition anzunehmen ist. Vorschlag: Orientierung an dem Begriff der Fokusgruppen nach NIS2

- Insbesondere die Ausweitung der Pflichten zur Überprüfung von Personal bei Auftragnehmern/Dritten ist kritisch zu beurteilen. Es stellt sich einerseits die Frage, ob nicht ein Verweis auf die Pflichten gem. NIS2-Umsetzung ausreichend wäre: Alle vom neuen Sicherheitskatalog adressierten Unternehmen dürften zweifelsfrei auch unter die NIS2-Pflichten mit der jeweiligen Einstufung fallen.

7. Sicherheit von Daten, Systemen und Einrichtungen

- Die unter 4.4.1 vorgegebenen Schutzmaßnahme der Umgebungskontrollen ist nicht für alle Netzebenen umsetzbar und insbesondere für gNodeB-Standorte nicht realisierbar.

- Unternehmen mit erhöhtem Gefährdungspotenzial sind angehalten, aktive Kühlung und Notstromgeneratoren bereitzuhalten, um zu gewährleisten, dass die Versorgung jederzeit sichergestellt ist. Dabei sollte berücksichtigt werden, dass Netzbetreiber von öffentlichen Stromversorgern abhängig sind. Aufgrund dieser Abhängigkeit kann eine jederzeitige Sicherstellung der Versorgung nicht ausnahmslos gewährleistet werden. Dies sollte im Rahmen der Verhältnismäßigkeit nach 2.3.3 geprüft werden.

- Die Anforderung der Führung von Nachweisen über Zugangskontrollen in der Form, dass Personen, die Räumlichkeiten betreten, sicherheitsüberprüft, geschult und qualifiziert sind und dass jeglicher Zugang, insbesondere durch Dritte streng überwacht wird, ist realistischerweise nicht umsetzbar. Diese Anforderung sollte gestrichen, mindestens aber klargestellt oder ins Ermessen der Behörde gestellt werDen.

8. Kritische Komponenten

- Ausweitung der kritischen Funktionen Ziffer B.5.1: Ziff. B 5.1 sieht eine Erweiterung der Liste der kritischen Funktionen, u.a. in Bezug auf RAN Funktionen (gNodeB) vor. Hiervon wären alle Komponenten in den Mobilfunkbasisstationen erfasst. Diese Ausweitung ist nicht sachgerecht, da es keine Änderungen in der Technik gibt, die diese notwendig machen. Der gNodeB erfüllt gemäß ETSI/3GPP-Standard weiterhin nur begrenzte Funktionen (Funkressourcensteuerung, Signalverarbeitung) am Netzrand, verarbeitet keine Nutzerdaten und besitzt in der Ende-zu-Ende-Verschlüsselungsarchitektur keinen Zugriff auf Verkehrsdaten. Sein Gefährdungspotenzial ist daher gering. Hierdurch werden ansonsten nur unverhältnismäßig hohe Aufwände verursacht (Zertifizierungspflicht, § 165 Abs. 4 TKG, die Aufwände der Hersteller werden an die Betreiber weiter gereicht) und der Netzausbau verlangsamt.

- Auch die Untersagungsmöglichkeit und Auflagenanordnung durch BMI gem. § 41 BSIG-E erstreckt sich auf sämtliche Komponenten der Mobilfunkbasisstationen, sofern sie auch 5G dienen. Dies verschlechtert die Planungs- und Investitionssicherheit.

- Hinzu kommt, dass die gemäß Ziff. B 5.2 gelisteten Funktionen grundsätzlich kritisch sind, es gibt die Ausnahmemöglichkeit nicht mehr, die in der vorangegangenen Liste der kritischen Funktionen für diese Kategorie noch vorgesehen war. Die Betreiber haben somit nicht mehr die Möglichkeit, durch geeignete risikominimierende Maßnahmen im Rahmen eines umfassenden Sicherheitskonzepts das Gefährdungspotenzial einer kritischen Funktion erfolgreich zu mitigieren. Ein solches Vorgehen ist jedoch in der Telekommunikationsindustrie weltweit erfolgreich etabliert und bewährt und sollte entsprechend auch weiter inzentiviert werden.

- Basierend auf Standarddefinitionen und Industriepraxis wird daher empfohlen, den gNodeB nicht als kritische Funktion zu klassifizieren

9. Technische Spezifikationen für paketvermittelte Netze zum Katalog der Sicherheitsanforderungen

a) Domain Name System – Resolver

Die Vorgaben nach 4.2 a) zu DNSSEC sollten wie folgt ergänzt werden:

- Ein DNS-Resolver muss elliptische kryptografische Verfahren (ECDSA, EDDSA) unterstützen
- DNS-Resolver müssen per default prüfen, ob eine DNS-Zone DNSSEC-aktiviert ist
- DNS-Resolver müssen per default prüfen, ob die DNS-Replies einer DNSSEC-aktivierten DNS-Zone verifiziert sind
- DNS-Resolver müssen nicht verifizierbare DNS-Replies DNSSEC-aktivierter DNS-Zonen unterdrücken und stattdessen eine Fehlermeldung an den anfragenden Client zurückgeben
- Fehlermeldungen des DNS-Resolvers müssen den Vorgaben des RFC 8914 Extended DNS Errors entsprechen.

Die Vorgaben nach 4.3 a) sollten wie folgt ersetzt werden:

- DNS-Resolver sollen die Vorgaben der BSI Studie IP Fragmentierung und Maßnahmen gegen „Cache-Poisoning“ (siehe 5. Recommendation) unterstützen.

b) Domain Name System - Autoritative DNS-Server

Die Vorgaben nach 5.1 a), Bullet 3 sollten wie folgt ersetzt werden:

- Autoritative DNS-Server sollen die Vorgaben der BSI Studie IP Fragmentierung und Maßnahmen gegen „Cache-Poisoning“ (siehe 5. Recommendation) unterstützen.

c) E-Mail-Sicherheit

Allgemein

Der Entwurf lässt eine Definition des Begriffs des E-Mail Dienstanbieters vermissen. Im vorliegenden Entwurf wird der Begriff nur einseitig verwendet und ausschließlich der Empfängerseite zugeordnet. Das Thema E-Mail-Sicherheit kann allerdings nur dann effektiv behandelt werden, wenn auch die Versenderseite einbezogen wird. Für die Praxis bestehen bereits umfangreiche Kataloge mit best-practice-Beispielen für die Versenderseite (z.B. die Kriterien der Certified Senders Alliance), die praxisnah und mit den Unternehmen abgestimmt sind. Diese könnten als Hilfestellung dienen.

Zu 6.1.1

Hinsichtlich des Scans von E-Mails auf Malware (Viren, Würmer, Trojaner) und zu Hinweisen auf Spam oder Phishing sollten die Schutzmaßnahmen in Bezug auf die Prüfung eingehender Mails wie folgt ersetzt werden:

- Nachrichten sollten auf Grundlage der Vorhaben der Technischen Richtlinie BSI TR-03108 Sicherer E-Mail-Transport verarbeitet werden.

Zu 6.1.3

Die Maßnahmen nach 6.1.3 a) sollten wie folgt ersetzt werden:

- Access Provider müssen ausgehende SMTP-Verbindungen anlassbezogen auf Port 25/tcp für Privatkunden sperren, wenn bei einem solchen Account Spam und/oder Malware versendet wird
- Access- und Service-Provider müssen Privatkunden ausgehenden SMTP-Verkehr über SMTP-Submission(s)-Server ermöglichen
- Ausgehender Mailverkehr muss auf Malware-Gehalt geprüft werden
- Bei Malware-Verdacht darf eine Nachricht nicht zur Destination transportiert werden
- Bei Malware-Verdacht muss der Sender mindestens mit einem SMTP-Reject über den Verdacht benachrichtigt werden und die Malware darf nicht an den Sender zurückgegeben werden.

Zu 6.1.4

Die Schutzmaßnahmen in Bezug auf den Umgang mit verdächtigen E-Mails sollten angepasst werden. Infizierte Nachrichten sollten rejected oder im Einzelfall den Empfängern nur über einen Release-Mechanismus zur Verfügung gestellt werden, welcher eine bewusste Aktion erfordert. Das bloße Verschieben in einen separaten Ordner birgt die Gefahr, dass Malware über den Umweg einer „separaten Mailbox“ dennoch ihre schädigende Wirkung entfaltet.

Liegt eine hohe Anzahl von ausgehenden infizierten E-Mails vor, muss das Senden unterbunden werden. Der Nutzer der Mailbox sollte idealerweise über einen anderen Kanal (Medienbruch), auf den Angreifende keinen Zugriff haben informiert werden.

Zu 6.2

a) Zur Transportverschlüsselung

Kommunikationsvorgänge im Kontext von E-Mails sind unter Heranziehung der BSI TR 02101-2 zu verschlüsseln. Die Technische Richtlinie 3108 inkludiert und adaptiert die Spezifikationen der BSI TR 02102 speziell auf die Bedürfnisse von E-Mail und wurde in Zusammenarbeit mit dem für die BSI TR 02102 zuständigen Referat erarbeitet. Dementsprechend sollte hier die BSI TR 3108 angeführt werden.

b) Zur Ende-zu-Ende-Verschlüsselung (E2EE)

Ende-zu-Ende-Verschlüsselung ist keine Eigenschaft des E-Mail-Transports oder der E-Mail-Infrastruktur, sondern eine Funktion der Endpunkte der Kommunikation. Sie wird ausschließlich durch die eingesetzten Clients, Erweiterungen oder externen Werkzeuge der Kommunikationspartner realisiert und entzieht sich damit dem unmittelbaren Einfluss des E-Mail-Diensteanbieters.

Vor diesem Hintergrund ist die Formulierung, dass „für den Kunden die Option bestehen sollte, für seine E-Mails selbst eine Ende-zu-Ende-Verschlüsselung vorzunehmen“, ausschließlich dahingehend sachgerecht, dass E-Mail-Diensteanbieter die Übertragung Ende-zu-Ende-verschlüsselter Inhalte nicht unterbinden.

Die Möglichkeit, Ende-zu-Ende-verschlüsselte Inhalte zu versenden, ergibt sich bereits daraus, dass E-Mail-Diensteanbieter den Transport solcher Inhalte nicht blockieren oder technisch einschränken. Ein darüberhinausgehender Regelungsbedarf besteht aus sicherheitstechnischer Sicht nicht.

Der Hinweis, dass bei Ende-zu-Ende-verschlüsselten E-Mails eine serverseitige Virenprüfung nicht möglich ist, greift fachlich zu kurz. Bei Ende-zu-Ende-Verschlüsselung ist jegliche inhaltliche Prüfung ausgeschlossen, einschließlich der Erkennung von Schadsoftware, Spam oder Phishing.

In diesen Fällen übernimmt der E-Mail-Diensteanbieter ausschließlich den Transport der verschlüsselten Daten, ohne Möglichkeit zur inhaltlichen Analyse oder Bewertung. Eine Verpflichtung zur Kennzeichnung solcher E-Mails verändert weder die Risikolage noch erhöht sie das Sicherheitsniveau und ist daher kein geeigneter Bestandteil eines Sicherheitskatalogs für E-Mail-Infrastrukturen.

10. Fazit

Der vorgelegte Entwurf des Sicherheitskatalogs nach § 167 TKG verfolgt das nachvollziehbare Ziel, die Sicherheitsanforderungen an Telekommunikationsnetze an veränderte Bedrohungslagen und den Stand der Technik anzupassen. In seiner derzeitigen Ausgestaltung wirft der Entwurf jedoch erhebliche fachliche, rechtliche und praktische Fragen auf.

Besonders kritisch ist die vorgesehene Systematik zur Bestimmung des Gefährdungspotenzials zu bewerten. Die pauschale Anknüpfung an Unternehmensgröße, Mitarbeiterzahl und Umsatz bildet weder die tatsächliche sicherheitsrelevante Bedeutung einzelner Netze, Dienste oder Komponenten ab noch spiegelt sie das reale Risiko für das Gemeinwesen wider. Hier besteht dringender Klärungs- und Anpassungsbedarf. Erforderlich ist ein konsequent risikobasierter Ansatz, der sich an Schutzbedarf, Funktion und tatsächlicher Kontrolle über die jeweilige Infrastruktur orientiert und zugleich eine bessere Kohärenz mit bestehenden Regimen wie NIS2 und der KRITIS-Systematik herstellt.

Darüber hinaus führen die sehr detaillierten und teils technologisch spezifischen Vorgaben zu einem hohen Umsetzungsaufwand und bergen die Gefahr schneller Überalterung. Auch die vorgesehene Umsetzungsfrist von einem Jahr erscheint vor diesem Hintergrund nicht sachgerecht und sollte unter Ausübung des der Bundesnetzagentur zustehenden Ermessens auf mindestens 24 Monate verlängert werden. Schließlich bestehen grundlegende Bedenken gegen die Annahme eines behördlichen Beurteilungsspielraums sowie hinsichtlich der Anwendung und Auslegung zentraler Rechtsbegriffe wie des „Stands der Technik“.

Insgesamt sollte der Sicherheitskatalog stärker auf übergeordnete Schutzziele und eine verhältnismäßige und praktische Umsetzbarkeit ausgerichtet werden. Eine Überarbeitung, insbesondere bei der Bestimmung der Gefährdungspotenziale und der Abgrenzung kritischer Funktionen, ist notwendig, um Rechtssicherheit zu schaffen, Doppelregulierung zu vermeiden und ein hohes Sicherheitsniveau mit realistischen und wirksamen Maßnahmen zu erreichen.
