Stellungnahme

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

29. September 2020

Vorbemerkung

Bitkom bedankt sich für die Gelegenheit zur Stellungnahme zum Entwurf der Liste der kritischen Funktionen für öffentliche Telekommunikationsnetze und -dienste mit erhöhtem Gefährdungspotenzial, die als 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, die mit Stand 29. April 2020 am 11. August 2020 zur Konsultation veröffentlich wurde.

Wie bereits in der Bitkom Stellungnahme zum Sicherheitskatalog vom 18. November 2019 dargestellt wird,[1] ist für die Bewertung der vorliegenden Aktualisierung [des Katalogs von Sicherheitsanforderungen nach § 109 TKG durch die Bundesnetzagentur] die Konkretisierung der Liste kritischer Netz- und Systemkomponenten entscheidend. Vor diesem Hintergrund ist es überaus bedauerlich, dass die Bundesnetzagentur, parallel zur Veröffentlichung des Entwurfs der ‘Liste der kritischen Funktionen für öffentliche Telekommunikationsnetze und -dienste mit erhöhtem Gefährdungspotenzial‘, bereits die Notifizierung eines veränderten Sicherheitskatalogs bei der Europäischen Kommission eingeleitet hat, ohne der Branche die Möglichkeit zu geben, die Ergebnisse der Konsultationsprozesses abzuwarten und diese entsprechend zu berücksichtigen. Dieses Vorgehen wird weder dem gepflegten Dialog von Telekommunikationsbranche und Bundesnetzagentur, noch den Vorgaben von § 109 Abs. 6 S. 2 TKG, gerecht.

Zusammenfassung

Bitkom begrüßt, dass mit der nun erfolgten Veröffentlichung der ‚Liste der kritischen Funktionen für öffentliche Telekommunikationsnetze und –dienste mit erhöhtem Gefährdungspotenzial‘ eine Konkretisierung des Anwendungsbereichs des neuen Sicherheitskatalogs gem. § 109 TKG erfolgt. Berücksichtigt werden müssen in diesem Zusammenhang jedoch zwingend die laufenden bzw. anstehenden Umsetzungs- bzw. Gesetzgebungsverfahren des Cybersecurity Acts, des IT-Sicherheitsgesetzes 2.0 und der

[1] Abrufbar unterhttps://www.bitkom.org/sites/default/files/2019-11/20191118_bitkom-stellungnahme_katalog-sicherheitsanforderungen.pdf.

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

Nick Kriegeskotte
Leiter Infrastruktur & Regulierung
T +49 30 27576-224
n.kriegeskotte@bitkom.org

Sebastian Artz
Referent IT-Sicherheit
T +49 151 27631531
s.artz@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Achim Berg

Hauptgeschäftsführer
Dr. Bernhard Rohleder

NIS-Richtlinie als horizontaler Regulierung sowie des TK-Modernisierungsgesetzes, die Änderungen an den hier in Rede stehenden Rechtsgrundlagen und Regelungszusammenhängen erwarten lassen. Das komplexe Zusammenspiel aus BSIG, KRITIS-V, TKG, Katalog von Sicherheitsanforderungen (insb. Anhang II), kritischer Funktionen, CSA, NIS 2.0, Zertifizierungsschemata, technischer Richtlinien und weiterer noch zu spezifizierender Rechtsverordnungen lässt sich zum jetzigen Zeitpunkt unmöglich in seiner Gesamtheit einschätzen und beurteilen. Da aber alle genannten Regelungen ineinandergreifen und gesamtheitlich betrachtet werden müssen, um den Adressatenkreis der Verpflichteten sowie den Inhalt und den Umfang der neuen Pflichten bestimmen zu können, ist das Vorgehen des Regelungsgebers einer scheibchenweisen Veröffentlichung und Anhörung der einzelnen Akte weder sachdienlich noch zeugt es von einer vertrauensvollen und transparenten Partnerschaft. Wir haben Zweifel, ob dem Anhörungserfordernis des § 109 Abs. 6 TKG mit dieser Vorgehensweise ausreichend Rechnung getragen wird. In diesem Punkt sehen wir notwendigen Verbesserungsbedarf. Keinesfalls dürfen diese absehbaren Initiativen in ihrer Gesamtheit dazu führen, dass Unternehmen vermeidbaren Aufwänden ausgesetzt werden. Insbesondere sind auch ausreichende Umsetzungsfristen zu berücksichtigen. Wir weisen unmissverständlich darauf hin, dass die Regelungsinhalte ohne rechtsunsicherheitsbefördernde Überlappungen nahtlos ineinandergreifen müssen.

Bitkom unterstützt das Bestreben der Bundesnetzagentur die Liste der kritischen Funktionen eng an der EU-Risikoanalyse und den Implementierungsempfehlungen der EU-Toolbox zu orientieren und technologieneutrale Funktionen für öffentliche Telekommunikationsnetze und -dienste mit erhöhtem Gefährdungspotenzial als Regelungsgegenstand zu beschreiben.

Das BSI erstellt und veröffentlicht in Abstimmung mit der Bundesnetzagentur einen "Technischen Leitfaden" für die betroffenen Netze im Rahmen der Anlage 2 zum "Sicherheitskatalog". Die "Technische Richtlinie" enthält Anforderungen für die Zertifizierung kritischer Komponenten einschließlich Anforderungen an die Betriebsumgebung und den Betrieb als Voraussetzung für die Gültigkeit von Zertifikaten. Darüber hinaus beschreibt der Leitfaden Anforderungen an den Nachweis von Zertifikaten nach europäischen Zertifizierungssystemen (CSA). Diese, aktuell vom BSI ausgearbeitete "Technische Richtlinie", sollte dem Network Equipment Security Assurance Scheme (NESAS) folgen, da NESAS, das gemeinsam von 3GPP und GSMA definiert wurde, einen branchenweiten Rahmen für die Sicherheitsgewährleistung bietet, um Verbesserungen des Sicherheitsniveaus in der gesamten Mobilfunkbranche zu erleichtern.

Die Definition von kritischen Komponenten muss sich mindestens auf europäische, im Idealfall internationale, anerkannte Standards berufen und nicht zu einer nationalen und deutschlandspezifischen Sonderlösung führen. Generell begrüßen wir daher die Akzeptanz

und die Berücksichtigung internationaler Standards und Analysen wie z. B. der ENISA oder BEREC. Auch begrüßen wir das Verfahren, die kritischen Komponenten über die Umsetzung der kritischen Funktionen zu definieren. Dies ist positiv, da ein Maß für positive Sicherheitsergebnisse, die Resilienz des Gesamtsystems darstellt. Grundsätzliche Standardfunktionen, dürfen dabei nicht als kritische Funktionen gelten. Kritische Komponenten müssen eindeutig identifizierbar festgelegt werden. Übergreifende Bezeichnungen, wie aktuell teilweise in der BSI-KritisV verwendet, oder Öffnungsklauseln sind hierfür nicht präzise genug. Es wäre grundlegend begrüßenswert, wenn die Definition eines 5G-Netzwerkes explizit anhand der 3GPP Definition entlang vorgenommen würde, um Unklarheiten und Ungenauigkeiten aufzulösen, und einem klaren, internationalen Standard zu folgen. Wir befürchten, dass die Zersplitterung zahlreicher Regelungsgegenstände in verschiedene Regelungsinstrumente nicht zur Normklarheit beiträgt. Dies kann die Rechtsanwender übermäßig belasten und zur Rechtsunsicherheit führen. Wir regen daher an, eine Konsolidierung der Regelungsgegenstände enger und widerspruchsfrei zu fassen und Redundanzen auszuschließen.

Im Einzelnen

Bitkom begrüßt grundsätzlich den Ansatz der Bundesnetzagentur kritische Komponenten über die Umsetzung der kritischen Funktionen zu definieren. Einerseits erscheint dieses Vorgehen zielführender, als eine Gesamtliste kritischer Komponenten zu erarbeiten und fortwährend zu pflegen. Anderseits garantiert eine solche Definition ein angemessenes und schwerlich zu unterlaufendes Verständnis kritischer Komponenten. Eine Unterteilung der Liste in ‚1 Kritische Funktionen und Komponenten' und ‚2 Liste der kritischen Funktionen' erscheint aus Sicht des Bitkom aber entbehrlich, da diese keinen Beitrag zu einer klaren Definition leistet. Ferner empfehlen wir, bestehende Redundanzen und inhärente Überlappungen, wie die zwischen Punkt 1 (Zugangsrechte und Authentifikation von Teilnehmern) und Punkt 3 (Zugangsrechte und Authentifizierung von Netzdiensten) zu vermeiden.

Zusätzlich dazu stellt sich die Frage nach dem Gegenstand der Zertifizierung: Die genauere Beschreibung der einzelnen Funktionen, möglichst ohne Überschneidung, würde Klarheit darüber schaffen, welche besonders kritischen Einzelkomponenten künftig einem dezidierten Zertifizierungsprozess unterliegen müssen. Bei der Beschreibung nach Funktionalität würde dadurch die Subsumption der zu zertifizierenden Komponenten erleichtert. Gleichwohl bedarf es natürlich einer ausgewogenen Balance. Ansonsten könnte die Anknüpfung an Funktionalitäten im Extremfall dazu führen, dass womöglich alle der eingesetzten Komponenten als „kritisch" zu bewerten wären. Dies würde zu einer „Bottom-Up"-Regulierungskette führen, d. h. die über ihre Funktionen als kritisch eingestuften Kompo-

nenten würden nach dem IT-SiG 2.0 dem Anwendungsbereich des § 9b BSIG-E unterliegen. Sie wären zu zertifizieren und ihr Einsatz müssten gegenüber dem BMI angezeigt werden, was eine erhebliche Bürokratie und Rechtsunsicherheit für die Unternehmen bedeuten würde.

Zum jetzigen Zeitpunkt wirft der bestehende Interpretationsspielraum weitere Folgefragen auf: Wird es möglich sein, Teilfunktionen als komplettes Teilsystem zertifizieren zu lassen, sodass ein Teilsystem bestimmte Funktionalität vollständig abbildet, aber nur für sie auch zertifiziert wird? Oder erstreckt sich die Zertifizierung auch auf Funktionalität, die außerhalb des zertifizierungspflichtigen Umfangs liegt? Wäre im ersten Fall dann eine komplette Re-Zertifizierungen erforderlich, wenn es zum Austausch von nur einer Teilkomponente kommt? Grundsätzlich sollte eine Zertifizierung durch anerkannte Testzentren und unabhängige Zertifizierungsstellen möglich sein.

Zu Punkt 1 Kritische Funktionen und Komponenten

Hier leistet der Punkte der „erheblichen Datenschutzverletzungen“ keinen Beitrag zu einer klaren Ausgestaltung und bedarf der Präzisierung, beispielsweise durch Verweis auf andere Regelungen.

Das Kriterium der „erheblichen Datenschutzverletzungen“ ist unklar. Der Begriff der Erheblichkeit ist nicht ausdrücklich definiert. Nach unserer Auffassung lässt sich das Maß der Erheblichkeit jedoch anhand der Aufzählung der weiteren Folgen einer technischen Kompromittierung, „systematische Ausforschung des Fernmeldeverkehrs oder beträchtliche Sicherheitsverletzung nach § 109 Abs. 5 TKG“ durch Auslegung ermitteln. Danach müssen die Folgen einer erheblichen Datenschutzverletzung vergleichbar sein mit den Folgen einer systematischen Ausforschung und einer beträchtlichen Sicherheitsverletzung.

Zu Punkt 2 Liste der kritischen Funktionen

Die unter 2 genannte Liste bildet überwiegend die Empfehlungen der EU-Risikoanalyse und die Implementierungsempfehlungen der EU-Toolbox ab, berücksichtigt aber darüber hinaus auch die Vorgaben zu Lawful Interception. Bitkom unterstützt im Grundsatz die hier genannten Funktionalitäten und damit die Kritikalität der für die Realisierung dieser Funktionalitäten erforderlichen Komponenten. Es gilt jedoch zu berücksichtigen, dass die

Bewertung einer hier gelisteten Funktion als kritisch im Sinne des Abschnittes 1 der Ergänzung zur Anlage 2 des Katalogs von Sicherheitsanforderungen auch von der konkreten Realisierung eines Netzes bzgl. Design, Architektur und Topologie abhängt. Diese Dimensionen spannen quasi den Kritikalitätsraum auf. Zur Bestimmung kritischer Funktionen und Komponenten dürfen die relevanten Gestaltungsparameter somit nicht gänzlich unberücksichtigt bleiben.

Zur Gewährleistung von Rechts- und Anwendungssicherheit ist die Liste der (potenziell) kritischen Funktionen abschließend zu formulieren. Nur so würde klar und bestimmt, für welche (gelisteten) Funktionen besondere Anforderungen (in Abhängigkeit von der gewählten Realisierung) gelten und für welche (nicht gelisteten) Funktionen die allgemeinen Sicherheitsanforderungen des § 109 TKG zu Anwendung kommen sollen.

Grundsätzlich wäre es ratsam, den 3GPP-Standard der 5G-Architektur zu nutzen, um Knoten, Funktionen und Schnittstellen eindeutig zu definieren. Außerdem sollten die Abhängigkeiten zwischen der Virtualisierungsinfrastruktur und Netzwerkfunktionen, z. B. die Verknüpfung von 3GPP-Funktionen mit der NFVi-Infrastruktur in der Risiko-Analyse berücksichtigt werden. Auf längere Sicht ist die Einhaltung von 3GPP-Definitionen und Architekturen notwendig, um das Risiko der Intransparenz und zunehmender Fragmentierung zu verringern.

An folgenden Stellen besteht aus Sicht des Bitkom allerdings Konkretisierungsbedarf:

Zunächst ist die Regelung „Die gelisteten Funktionen stellen keine abgeschlossene Menge dar…“ unter dem Gesichtspunkt der Normklarheit problematisch. Die Kategorien stehen, wie der Entwurf ja offenbar zu verstehen ist, fest, und es darf bei der Definition der Funktionalitäten nicht dazu kommen, dass der Katalog der beispielhaft (dies ist allerdings nicht genannt) aufgeführten Funktionen in einer Weise ungeschrieben erweitert wird, die die Normadressaten nicht vorwegnehmen können. Besser als eine reine beispielhafte und nicht abschließende Aufzählung wäre es daher, zu jeder Kategorie die Grundsätze und Kriterien anzugeben, nach denen sich das Maß an Kritikalität bestimmt, und dann die Funktionen, die anhand dieser Grundsätze beispielhaft zu nennen sind, aufzuzählen. Die Grundsätze und Kriterien können dabei als Schutzziele formuliert werden, und mehrere Kategorien können auch auf gemeinsame Grundsätze und Kriterien Bezug nehmen.

Zu Punkt 2 – einzelne Kategorien:

- Kategorie 1:
  "sofern Bestandteil des Netzes" ist unklar. Schutzzweck ist offenbar der Schutz gegen Kompromittierung der kryptographischen Infrastruktur, die auch durch netzfremde Bestandteile beeinflusst werden kann. Klarer dürfte „sofern Bestandteil des Netzes oder in sonstiger Weise an das Netz angebunden" oder eine vergleichbare Regelung sein.

  Unter dem Begriff der Kategorie 1 „kryptographische Mechanismen (sofern Bestandteil des Netzes)" kann zu viel hinzugezählt werden. Die definitive Abgrenzung der Systeme, die zur internen Verwaltung & Management der internen Netze (OSS & BSS) dienen wie z. B. Admin-Login oder User-Management fehlt.
  Diese sollte enthalten sein damit die o. g. Systeme nicht unter die Kategorie 1 fallen und somit auch dem ganzen Vertraulichkeitserklärung & Zertifizierungsprozedere unterliegen.

- Kategorie 3:
  Netzwerkdienste müssen auf Funktionsebene geklärt werden. Es besteht Klarstellungsbedarf, welches Netzwerkelement und welche Infrastrukturfunktionen zu dieser Kategorie gehören. Konkret stellt sich bspw. die Frage, was genau mit der Funktionalität „Exponierung von Netzwerkfunktionen gegenüber externen Anwendungen" gemeint ist.

- Kategorie 4:
  Die Funktionalität „Managementfunktionen zur Orchestrierung und Konfiguration von NVF" ist insofern unklar, als dass das genaue Verständnis von Orchestrator und Hypervisor durch die jeweils gewählte Struktur eines 5G-Netzes bedingt wird. Dieser Aspekt bedarf einer differenzierteren Ausführung. Dieser Punkt gilt analog für die Funktionalität "Management- und andere Unterstützungssysteme" in Kategorie 5.

- Kategorie 6:
  Die Funktionalität ist unklar. Ist hier die bevorzugte Behandlung bestimmter Teilnehmer- und Verkehrsklassen gemeint? In diesem Fall kann es sich anbieten, klarzustellen, dass beispielsweise bedarfsträgerbezogene Verkehrsbeeinflussung gemeint ist, beispielsweise die besondere Bevorzugung von Blaulichtorganisationen im Katastrophenfall oder in Fällen gemeiner Gefahr. Die Rechtsanwender benötigen hier bessere Erläuterungen. Der Teil „Edge Computing Core Routing" am Ende der Erläuterung 6 ist nicht verständlich; es scheint sich um einen Bear-

beitungsfehler zu handeln. Es muss klargestellt werden, was durch diesen Zusatz gemeint ist.

- Kategorie 7:
  Hierzu sollte auch die eigentliche Durchführung der Überwachungsmaßnahmen genannt sein. Schutzzweck ist nicht nur, dass die bei Überwachungsmaßnahmen gewonnenen Daten gegen unbefugten Zugriff geschützt sind, sondern dass unzulässige Überwachungsmaßnahmen und die Ausleitung von Daten überhaupt verhindert werden. Dies ergibt sich auch aus den Erläuterungen, und es sollte in der Tabelle klarer sein.