bitkom

Stellungnahme

16. Januar 2026

Überarbeitung des Katalogs von Sicherheitsanforderungen

Bitkom bedankt sich für die Gelegenheit, zum Entwurf des *Katalogs von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten* Stellung nehmen zu können.

Der Sicherheitskatalog nach § 167 TKG konkretisiert die technischen Vorkehrungen und sonstigen Maßnahmen, die die Betreiber von Telekommunikationsnetzen im Interesse der öffentlichen Sicherheit und Notfallvorsorge, der Wahrung des Fernmeldegeheimnisses, des Schutzes der Informationssicherheit der Nutzer und der Vermeidung von Betriebsstörungen bei der Erbringung von kritischen Dienstleistungen nach § 165 TKG zu beachten haben. Der gemeinschaftlich abgestimmte Rahmen von BNetzA, BSI und BfDI soll die ausbalancierten Interessen der Beteiligten gewährleisten und einen regulatorischen Rahmen für die sichere Diensteerbringung durch die Telekommunikationsindustrie darstellen. Dieser Multi-Stakeholder Ansatz aus Betreibern, Herstellern und Sicherheitsbehörden leistet seit vielen Jahren einen bestimmenden Beitrag zur sicheren Digitalisierung in Deutschland. Der Ansatz hat sich auch bei der Einführung und dem Betrieb von 5G in seinen verschiedenen Stufen bewährt. Die generellen Sicherheitskonzepte sind erprobt, die Sicherheitskooperation robust und die allgemeinen technischen Prinzipien wirksam.

Eine Konkretisierung der Sicherheitsanforderungen kann eine einheitliche Interpretation ermöglichen, die für ein durchgehend hohes Schutzniveau notwendig ist. Die Überarbeitung des Katalogs sollte aber nach Maßgabe dieser Betrachtung gezielt, behutsam, minimalinvasiv und proportional zur Effektivität der Erneuerungsvorschläge erfolgen. Vor diesem Hintergrund kann eine Neuauflage des Sicherheitskatalogs zweckmäßig sein.

Zu den vorgeschlagenen Änderungen möchte der Bitkom im Einzelnen wie folgt Stellung nehmen:

Bestimmung der Gefährdungspotenziale und Zweifel an der Verhältnismäßigkeit

Bitkom unterstützt die Maßnahmen der Bundesregierung und der EU, insbesondere die Telekommunikationssysteme in der EU sicherer zu machen. Die stärkere Anlehnung an Richtlinien des Europäischen Parlaments und des Rates, insbesondere an die Richtlinie (EU) 2022/2555 (NIS-2), ist grundsätzlich zu begrüßen, da sie zur Harmonisierung beiträgt, nationale Sonderwege reduziert und damit die regulatorische Komplexität senkt.

Gleichwohl bestehen Bedenken hinsichtlich der Verhältnismäßigkeit des aktuellen Entwurfs des Sicherheitskatalogs. Die zugrunde gelegten Gefährdungspotenziale sind nicht ausreichend konkretisiert. Dies birgt das Risiko einer faktischen Mehrfachregulierung, die keine zusätzliche Sicherheit erzeugt, gleichzeitig jedoch erhebliche operative und finanzielle Belastungen verursacht. Die vorgesehene pauschale Klassifizierung allein anhand von Umsatz- und Mitarbeiterzahlen ist nicht sachgerecht. Sie widerspricht den Grundprinzipien einer risikobasierten Regulierung. Unternehmensgröße oder Umsatzhöhe sind allein keine geeigneten Kriterien, um das tatsächliche Sicherheitsrisiko der Telekommunikationsdienste des Unternehmens bestimmen zu können. Eine pauschale Einordnung verfehlt daher die notwendige Zielgenauigkeit und führt in vielen Fällen zu unverhältnismäßigen Auflagen.

Entscheidend ist vielmehr eine fundierte Einstufung, die sich an den realen Gefährdungspotenzialen orientiert und die tatsächliche Art, kritische Bedeutung und Reichweite der erbrachten Dienste berücksichtigt. Die NIS-2-Richtlinie fordert explizit, dass Sicherheitsmaßnahmen risikoorientiert und an die konkrete Rolle der jeweiligen Einrichtung angepasst sein müssen. Eine schematische Anwendung von Schwellenwerten wird diesem Prinzip nicht gerecht und kann zu übermäßiger oder redundanter Regulierung führen. Insbesondere für Anbieter, deren Telekommunikationsdienste nur einen unterstützenden Bestandteil eines umfassenderen digitalen Angebots darstellen, ist es erforderlich, dass die Regulierung dem tatsächlichen Risikobeitrag dieser Leistungen Rechnung trägt. Nur eine klare, risikobasierte Differenzierung gewährleistet eine effektive und zugleich verhältnismäßige Regulierung.

Wir halten es zusätzlich, insbesondere vor dem Hintergrund der im Entwurf vorgesehenen Ausweitung des Anwendungsbereichs sowie des technischen Aufwandes, der mit der Umsetzung der inhaltlichen Vorgaben des Katalogs einhergeht, für sachgerecht, dass die BNetzA die ihr zustehenden Ermessensspielräume ausnutzt, vor allem die Ausweitung der Umsetzungsfrist auf 24 Monate in ihre Gesamtabwägung hinreichend berücksichtigt. Dies ist gem. § 167 Abs. 3 TKG grundsätzlich möglich.

Festlegung grundlegender Einzelheiten und sonstige Maßnahmen unter Berücksichtigung der verschiedenen Gefährdungspotenziale

Sicherheit bei Abhängigkeiten von Dritten

Der Ansatz des Entwurfs, Sicherheitsziele verbindlich in Verträgen mit Dritten zu verankern und deren Umsetzung, besonders im 5G-Kontext, sicherzustellen, ist grundsätzlich sinnvoll. Zielführend wäre jedoch eine ausgewogene Präzisierung, die nachvollziehbare Nachweise und objektive Bewertungskriterien erleichtert, ohne die praktische Handhabbarkeit zu beeinträchtigen. Bei der Bewertung von Gefährdungspotenzialen sollte besonderes Augenmerk auf die Transparenz hinsichtlich Entwicklungsprozessen, Lieferkettenintegrität, unabhängiger Sicherheitsprüfungen sowie auf eine vollumfängliche Einhaltung europäischer Sicherheits-, Transparenz- und Vertrauensanforderungen gelegt werden. Insgesamt trägt eine derart auf nachprüfbare Transparenz, unabhängige Prüfung und europäische Konformität ausgerichtete Ausgestaltung dazu bei, Abhängigkeiten von Dritten sachlich zu bewerten und die Resilienz der Netze gegenüber externen Einflüssen nachhaltig zu stärken.

Physische und umgebungsbezogene Sicherheit

Einer klarstellenden Präzisierung bedarf der Begriff der »unbemannten Standorte« im Zusammenhang mit den geforderten physischen Infrastrukturkontrollen. Es muss ausgeschlossen werden, dass davon sämtliche Mobilfunkmasten und Dachstandorte pauschal erfasst sind. Zwar werden diese in der Regel unbemannt betrieben, eine undifferenzierte Ausweitung auf diese Standorte würde jedoch zu sehr weitreichenden und unverhältnismäßigen Anforderungen führen – etwa der flächendeckenden Videoüberwachung sämtlicher Mobilfunkstandorte. Dies hätte neben rechtlichen Unwägbarkeiten auch unzumutbare wirtschaftliche Auswirkungen. Aus unserer Sicht sollte deshalb klargestellt werden, dass mit den »angemessenen physischen Infrastrukturkontrollen« keine generelle Pflicht zur Videoüberwachung oder zu vergleichbaren Maßnahmen für jeden einzelnen Mast- oder Dachstandort gemeint ist. Auch ist bereits unklar, ab welchem Zeitraum ein Standort als unbemannt gilt. Vielmehr sollte eine risikobasierte Betrachtung erfolgen, die Art, Nutzung, Lage und das Gefährdungspotenzial des jeweiligen Standorts berücksichtigt.

Zentrale Leitung bei anbieterübergreifenden Störungen

Die im Entwurf vorgesehene Verpflichtung zur Kooperation bei anbieterübergreifenden Störungen würde in der praktischen Umsetzung zu strukturellen Herausforderungen führen. Eine rein bilaterale Abstimmung zwischen betroffenen Telekommunikationsanbietern ist ineffizient, erzeugt doppelte Kommunikationsstrukturen und birgt das Risiko inkonsistenter oder widersprüchlicher Lagebilder.

Anstelle einer primär direkten Kooperation der Anbieter sollte der Sicherheitskatalog klar festlegen, dass eine zentrale Stelle die Koordinierung und Informationsverteilung bei anbieterübergreifenden Störungen übernimmt, während die Telekommunikationsanbieter weiter in einer operativen Rolle agieren. Dies schafft Verlässlichkeit, Rechtssicherheit und eine einheitliche Struktur im Störungsfall.

Notfallübungen

Der Entwurf des Sicherheitskatalogs fordert die Durchführung realitätsnaher Notfallübungen unter Einbeziehung von Lieferanten, Dienstleistern und weiteren Betreibern. Mobilfunknetzbetreiber arbeiten mit einer Vielzahl von externen Partnern in unterschiedlichen Rollen und Abhängigkeiten zusammen. Eine undifferenzierte, vollständige Einbindung sämtlicher Partner in Übungen sowie umfangreiche Neuverhandlungen mit Dienstleistern wären mit erheblichen organisatorischen und wirtschaftlichen Aufwänden auf beiden Seiten verbunden und erscheinen nicht sachgerecht.

Es bedarf einer Klarstellung, welche Kategorien von Lieferanten verpflichtend, in welcher Tiefe und in welchen zeitlichen Intervallen in Notfallübungen einzubeziehen sind. Auch sind Branchenübungen denkbar, die vorher zum Beispiel in den BAK (Branchenarbeitskreisen) der UP-KRITIS geplant wurden.

Threat Intelligence

Die im Entwurf vorgesehene Verpflichtung zur Information von Nutzern über besondere Sicherheitsbedrohungen erfordert klar definierte und operationalisierbare Auslösekriterien, die im Entwurf des Sicherheitskatalogs bislang nicht hinreichend konkretisiert sind.

Es bedarf eindeutiger Kriterien dafür, welche Arten von Bedrohungen eine Informationspflicht gegenüber Endnutzern auslösen, welche Inhalte diese Information haben soll und welche Kommunikationswege dabei zulässig und vorgesehen sind.

Festlegung von zusätzlichen Einzelheiten und Maßnahmen für 5G-Netze und die Bestimmung von kritischen Komponenten

Entfall der Einzelfallentscheidung innerhalb der kritischen Funktionen

Der Entwurf des Sicherheitskatalogs sieht vor, dass die bisherige Einzelfallentscheidung zur Bewertung der Einsatzkritikalität bei Komponenten mit Zuordnung zu kritischen Funktionen der Kategorien C bis F entfällt. Damit würden künftig sämtliche in 5G-Netzen eingesetzten Komponenten den Anforderungen an

kritische Komponenten unterliegen, einschließlich solcher, die bislang, auch in Abstimmung mit der BNetzA und dem BSI, als »nicht in ihrem Einsatz kritisch« eingestuft wurden und für die bisher ausschließlich die Maßnahmen nach dem Sicherheitskatalog 2.0 sowie die einschlägigen Vorgaben aus Anlage 2 umzusetzen waren.

Ferner sollte der Sicherheitskatalog den in öffentlich-rechtlichen Verträgen getroffenen Vereinbarungen hinreichend Rechnung tragen.

Darüber hinaus erscheinen die Abgrenzungen der betroffenen Netzbereiche derzeit nicht hinreichend eindeutig geregelt. Eine klare und rechtssichere Definition ist unabdinglich, um festzulegen, welche RAN- und Transportnetzelemente künftig bei der Identifizierung kritischer Komponenten zu berücksichtigen sind und wie diese Abgrenzung mit den Vorgaben des § 167 TKG in Einklang gebracht werden kann.

Zertifizierung kritischer Komponenten

Die vorgesehene Zertifizierung kritischer Komponenten nach TR-03163 ist grundsätzlich sinnvoll. Dies sollte in Anlehnung an die Zertifizierungspflichten internationaler Standards EUCC, NESAS und CRA erfolgen. Um die Umsetzbarkeit sicherzustellen, sind angemessene Übergangsfristen erforderlich, die sich an der internationalen Standardisierung orientieren müssen. Nur so kann verhindert werden, dass der Markt durch nationale Fristen fragmentiert und unverhältnismäßig belastet wird und es nicht zu Verzögerungen beim Netzausbau kommt. Zudem könnte eine übermäßige Ausweitung der Zertifizierungspflicht auf eine Vielzahl weiterer Komponenten Innovations- und Einführungszyklen im Netzbetrieb deutlich verlängern. Dies würde sich nicht nur hemmend auf die technologische Weiterentwicklung und die zeitnahe Umsetzung von Sicherheitsmaßnahmen auswirken, sondern auch notwendige Erneuerungen zur Sicherstellung einer hohen Netzverfügbarkeit verzögern. In der Folge würde die Reaktionsgeschwindigkeit gegenüber neuen Bedrohungslagen sinken, obwohl gerade diese für ein dauerhaft hohes Sicherheitsniveau essenziell ist. Damit wäre die ursprüngliche Zielsetzung der Produktzertifizierung, die Erhöhung von Sicherheit und Vertrauenswürdigkeit, in wesentlichen Teilen konterkariert und könnte mittelbar selbst zur Gefährdung von Verfügbarkeit und Sicherheit der Netze beitragen.

Bei der Festlegung von Zertifizierungspflichten sollte der Fokus weiterhin auf Komponenten und Kategorien liegen, die unmittelbar und nachweislich für die Steuerung, Authentifizierung und den sicheren Betrieb des 5G-Mobilfunknetzes verantwortlich sind.

Die Erläuterung des Einsatzes von Bestandskomponenten muss deutlicher klargestellt werden. Unser Verständnis ist, dass ein »erstmaliger Einsatz« dann vorliegt, wenn eine neue Software (»update« oder »upgrade«) oder eine neue Hardware-Komponente in das bestehende Produkt eingebaut oder eingebracht werden soll. Es wird empfohlen, diese Klarstellung in den Katalog aufzunehmen.

Der Sicherheitskatalog sieht ferner vor, dass bereits im Einsatz befindliche Bestandskomponenten nicht nachträglich zertifiziert werden müssen. Dies begrüßt der Bitkom.

Technische Maßnahmen für die Sicherheit in 5G-Netzen

Die Sicherheitsanforderungen für 5G-Netze sind im Entwurf in der vorgesehenen Detailtiefe zu stark ausgestaltet. Wir befürworten, dass das Schutzniveau zukunftsweisend an die Bedrohung und den Stand der Technik als Maßstab ausgerichtet werden kann.

Beispiele aus Kapitel 5.5 wie die regelmäßige Erneuerung der Kurzzeit-Benutzerkennung, der Schutz der Vertraulichkeit der Nutz- und Signalisierungsdaten sowie der Schutz des Zugriffs auf Netzwerkfunktionen im 5G-Kernnetz zeigen, dass der Entwurf nicht nur Schutzziele oder Mindeststandards vorgibt, sondern sehr detaillierte technische Maßnahmen und Konfigurationen vorschreibt. Dies unterstreicht die Bedeutung, die Anforderungen so zu gestalten, dass sie sich an die Evolution internationaler Standards (3GPP), technischer Erkenntnisse (GSMA) oder besserer technischer Implementierungen orientieren und somit zukunftsweisend im Katalog von Sicherheitsanforderungen verankert werden.

Es ist daher wesentlich, dass nationale Vorgaben mit internationalen Standards kompatibel bleiben. Eine übermäßige Detaillierung technischer Maßnahmen auf nationaler Ebene erhöht die Gefahr divergierender Interpretationen und erschwert die Umsetzung global einheitlicher Sicherheitsarchitekturen. Eine noch engere Orientierung an 3GPP- und GSMA-Spezifikationen würde sicherstellen, dass Sicherheitsanforderungen weltweit konsistent interpretiert und umgesetzt werden können.

Sicherheitsbewertung und Exit-Strategie für Cloud-Services – technische Realisierbarkeit

Die Annahme des Entwurfs, dass Sicherheitsziele bei der Nutzung von Public-Cloud-Diensten grundsätzlich nicht mit gleichwertigen Mitteln wie im Eigenhosting erreicht werden könnten, ist fachlich nicht hinreichend belegt und in dieser Allgemeinheit nicht haltbar. Sie wird der Vielfalt moderner Cloud-Architekturen und Betriebsmodelle nicht gerecht.

Public-Cloud-Umgebungen verfügen über Sicherheits- und Resilienzmechanismen, die im Eigenbetrieb nur mit erheblichem Zusatzaufwand oder nicht wirtschaftlich realisierbar sind, insbesondere geo-redundante Architekturen, automatisierte Failover-Konzepte, hochverfügbare Plattformdienste und kurzfristige Skalierbarkeit. Diese Faktoren sind zwingend in eine risikobasierte Bewertung einzubeziehen.

Die Anforderungen an Exit-Strategien müssen sich an der technischen Machbarkeit orientieren. Dabei ist zwischen einem vollständigen Exit und der Sicherstellung eines funktionsfähigen Notbetriebs bzw. einer Resilienzfähigkeit zu unterscheiden. Ein vollständig getesteter Exit würde den parallelen Betrieb einer vollständigen Spiegelarchitektur erfordern und ist weder wirtschaftlich noch technisch realistisch umsetzbar.

Die im Entwurf vorgesehene Nachweispflicht, dass die Nutzung von Diensten Dritter weder die Verfügbarkeit noch das Sicherheitsniveau des 5G-Netzes beeinträchtigt, bleibt ohne praktikable Konkretisierung und sollte daher entfallen.

Die zusätzliche Forderung, ausgelagerte Funktionen und Daten für Netzadministration und -konfiguration auch im Eigenbetrieb vorzuhalten, würde eine vollständige Spiegelung cloudbasierter Netzmanagementsysteme erfordern und käme faktisch einem Ausschluss von Cloud-Service-Modellen gleich. Angesichts bestehender Abhängigkeiten in den Lieferketten ist diese Anforderung derzeit selbst im Eigenhosting nicht durchgängig erfüllbar und greift unverhältnismäßig in unternehmerische Gestaltungsentscheidungen ein, ohne einen erkennbaren zusätzlichen Sicherheitsmehrwert zu bieten.

E-Mail-Sicherheit

Bitkom zweifelt an der Angemessenheit der für die E-Mail-Sicherheit herangezogenen Mechanismen. Ausgehend von der aktuellen Tatsachenlage, bei der schon jetzt jeder sachgerecht arbeitende E-Mail-Dienstanbieter organisatorische und technische Maßnahmen zur Gefahrenabwehr implementiert hat, dürften die Vorgaben aufgrund des hohen Detailgrades die Grenzen der Angemessenheit in vielen Anwendungsfällen überschreiten. Möchte man an den Mechanismen festhalten, so sollten sie lediglich als Empfehlungen formuliert werden.

Abschließende Hinweise und Empfehlungen

Der Entwurf des Sicherheitskatalogs bewirkt eine deutliche Erweiterung seines Anwendungsbereichs, da er als unternehmensweites Sicherheits- und Compliance-Regelwerk ausgestaltet ist. Der Wegfall der Einzelfallentscheidungen führt zu einer übermäßigen Ausweitung des Kreises der als kritisch einzustufenden Komponenten, welche wir strikt ablehnen. Die weitreichende Ausdehnung der Zertifizierungspflichten ist mit erheblichen und zusätzlichen Aufwänden und Unsicherheiten für große Mobilfunknetzbetreiber verbunden.

Abschließend empfehlen wir unter Bezugnahme auf die grundsätzlichen Anmerkungen zu den Gefährdungspotenzialen folgenden Lösungsansatz:

1. Schwellenwerte nur als initiale Orientierung nutzen

Die im Entwurf vorgesehenen Schwellenwerte für Umsatz und Mitarbeiterzahl sollten ausschließlich als erste Orientierung dienen. Für die endgültige Einstufung ist eine vertiefte und konkrete Risikobewertung der angebotenen TK-Dienste erforderlich. Diese sollte klare qualitative und operative Kriterien umfassen, etwa:

a) potenzielle Ausfall- und Störungsfolgen,
b) Abhängigkeit kritischer Dienste von den jeweiligen Leistungen,
c) sicherheitsrelevante Marktstellung oder Systemrelevanz.

Eine solche risikobasierte Differenzierung entspricht den Grundsätzen der NIS-2-Richtlinie und gewährleistet eine verhältnismäßige Regulierung.

2. Anerkennung bestehender Sicherheitszertifizierungen und -nachweise

Wir empfehlen die Berücksichtigung und Anerkennung bereits bestehender Compliance-Nachweise (beispielsweise Zertifizierungen nach ISO/IEC-Normen oder bereits implementierte Maßnahmen gemäß NIS-2 bzw. EU-weiten Sicherheitsanforderungen). Ein solches »Anerkennungs- oder Äquivalenzprinzip« verhindert Doppelregulierung, erhöht die Effizienz und bündelt Ressourcen auf tatsächliche Sicherheitsverbesserungen.

3. Einführung eines transparenten Verfahrens zur Überprüfung und Herabstufung

Es sollte ein klar definierter Prozess vorgesehen werden, über den betroffene Unternehmen eine Neubewertung oder Herabstufung beantragen können. Dies stärkt die Rechtssicherheit und ermöglicht eine sachgerechte Anpassung, wenn die tatsächlichen Risiken geringer ausfallen als eine pauschale Schwellenzuordnung vermuten lässt.

4. Beibehaltung des Ableitungsprozesses und der Einzelfallentscheidung

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner
Nick Petersen | Referent für digitale Infrastrukturen
M +49 151 14824830 | n.petersen@bitkom.org

Verantwortliches Bitkom-Gremium
AK Telekommunikationspolitik