Stellungnahme

Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 Telekommunikationsgesetz (TKG) Version 2.0

18. November 2019

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

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

Teresa Ritter
Bereichsleiterin Sicherheitspolitik
T +49 30 27576-203
t.ritter@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Achim Berg

Hauptgeschäftsführer
Dr. Bernhard Rohleder

www.bitkom.org

A. Allgemeine Erwägungen

Der Mobilfunk der Generationen 4G und 5G sowie digitale Infrastrukturen insgesamt werden zum Rückgrat der digitalen Wirtschaft, Gesellschaft und Verwaltung. Das gesetzte Ziel ist es, in Deutschland möglichst schnell leistungsfähige, bezahlbare und sichere 5G-Netze aufzubauen und die 4G-Netze zu verdichten und zu ertüchtigen. Einhergehend mit der wachsenden Bedeutung der Kommunikationsnetze für das Funktionieren unseres Gemeinwesens werden in jeder Hinsicht ambitioniertere Anforderungen an die Kommunikationsinfrastruktur gestellt. Gleichzeitig erwachsen aus der Diskussion um vertrauenswürdige Infrastrukturen auch weitere Anforderungen an die Gestaltung der Digitalen Souveränität Europas.

Um diese Ziele zu erreichen, sind ein fairer und innovationsstimulierender Wettbewerb mit gleichen Regeln für gleiche Dienste und Angebote sowie die Vielfalt von Technologien und Anbietern essenziell, damit wie beabsichtigt möglichst schnell leistungsfähige, bezahlbare und sichere 5G-Netze in Deutschland aufgebaut werden können.

Um aber, neben der notwendigen Markterschließungsgeschwindigkeit, dem Souveränitätsanspruch nachzukommen, ist die Politik aufgefordert, den Rechtsrahmen und seine Umsetzung so auszugestalten, dass die Netze jederzeit ein Höchstmaß an Sicherheit einschließlich der Verfügbarkeit gewährleisten und nicht kompromittiert werden können. Grundsätzlich gilt, dass für alle Hersteller – ganz gleich welcher Produkte und Angebote sowie unabhängig ihrer Herkunft – idealerweise mindestens europaweit die gleichen produkt- und angebotsspezifischen Prüfkriterien, Regeln und Verfahren gelten müssen. An dieser Stelle möchten wir auch darauf hinweisen, dass ein klarer und technikneutraler Ansatz, der den Einsatz von wirksamer Verschlüsselung fördert, auf der anderen Seite nicht durch staatliche Aktivitäten zur Schwächung von Verschlüsselung konterkariert werden darf.

Auch muss der Gesetzgeber eindeutig adressieren, welche Anforderungen er zur Gewährleistung eines entsprechenden Maßes an IT-Sicherheit stellt. Hier ist dem Cyber-

security Act, dem IT-Sicherheitsgesetz sowie der NIS-Richtlinie als horizontaler Regulierung eine bedeutende Rolle zuzuschreiben. In diesem Kontext sollte auch die Diskussion über § 109 TKG gesehen werden.

Grundsätzlich müssen folgende vier Prinzipien beachtet werden:

1. Transparenz ist die Grundlage für Vertrauen. Dies setzt einen kooperativen Ansatz mit klar definierten Regeln für alle Seiten voraus. So wird die Grundlage gelegt, nicht nur das jeweilige Produkt zu sichern, sondern auch die Erkenntnisse im sicheren Entwicklungslebenszyklus für zukünftige Produkte zu stärken. Alle Beteiligten sollten sicherstellen, dass sie frei von unangemessenem staatlichem Einfluss sind und mit den Standards und Zielen der OECD-Grundsätze für Corporate Governance übereinstimmen.

2. Prüfung und Zertifizierung: Innovation sichert den Wohlstand von morgen. Innovationen im IKT-Bereich werden zunehmend zur Triebfeder der Entwicklung von Wirtschaft und Gesellschaft. Dafür ist eine innovationsfreundliche Regulierung entscheidend. Staatlicherseits sollten vor allem die Zielsetzung und die Anforderungen der vorgeschlagenen Maßnahmen definiert werden. Dabei ist ein risikobasierter Ansatz zu wählen. Im Rahmen einer Zertifizierung ist die gegenseitige Anerkennung zumindest auf europäischer Ebene zu schaffen. Hierzu wie auch zur Frage der Transparenz gehört, dass jedwede Überprüfung von Quellcode und anderen relevanten Materialien, die von den zuständigen Behörden verlangt wird, an einem unter Kontrolle des Herstellers sich befindenden sicheren Ort in Europa durchgeführt wird. Deutschland besitzt nicht zuletzt aufgrund seiner wirtschaftlichen Kraft eine Vorbildfunktion für Staaten weltweit, der wir uns bewusst sein sollten.

3. Verantwortung: Staatliche Stellen und in staatlichem Auftrag Handelnde, Netzbetreiber und Hersteller tragen jeweils ihren Teil zur Verantwortung für sichere Netze bei und müssen hierfür ihren jeweiligen Rollen und Zuständigkeiten entsprechend alle erforderlichen Maßnahmen treffen. Gleichzeitig sind auch die Nutzer dafür zu sensibilisieren, ihren Beitrag für Sicherheit, Integrität und Verfügbarkeit von Daten zu leisten und beispielsweise bei kritischen Daten konsequent Verschlüsselung einzusetzen.

4. Europäischer Binnenmarkt: Der Europäische Binnenmarkt ist eine Erfolgsgeschichte für die wirtschaftliche Entwicklung in Deutschland. Deutschland und die Wirtschaft in Deutschland besitzen ein Eigeninteresse daran, diesen Binnenmarkt zu stärken und an seiner Innovationskraft teilzuhaben. Daher muss jedwede Festlegung von Sicherheitsanforderungen, auch die Zertifizierung von als »kritisch« zu bewertenden Kernkomponenten im europäischen Rahmen erfolgen und die darauf basierende Zertifizierung durch natio-

nale Prüfstellen europaweit anerkannt werden. Nationale Alleingänge schwächen die wirtschaftliche Entwicklung und bremsen die Innovationsfähigkeit.

Diese Prinzipien werden maßgeblich dazu beitragen, den Anspruch an sichere Kommunikationsnetze zu erfüllen.

B. Zum Entwurf des Katalogs für Sicherheitsanforderung Version 2.0 im Einzelnen:

Bitkom begrüßt, dass die Bundesnetzagentur die Aktualisierung des Katalogs von Sicherheitsanforderungen nach § 109 Abs. 6 Telekommunikationsgesetz (TKG) veröffentlicht hat und der dort beschriebene Ansatz beinhaltet, dass Sicherheitsanforderungen für alle Netzbetreiber, Hersteller und Diensteerbringer gleichermaßen und technikneutral gelten. Vorgeschlagene Prinzipien, wie beispielsweise die permanente Netzbetrieb-Überwachung, sind schon heute geübte Praxis. Auch die geforderte Vermeidung von Monokulturen ist heute Realität im Zuge der Multi-Vendor-Strategie der Netzbetreiber. Darüber hinaus sind Redundanzen im Netz eine geeignete Maßnahme, um dessen Sicherheit zu erhöhen.

Die Sicherheit der Netze hat oberste Priorität. Dazu passt die Idee einer umfassenden Sicherheitsarchitektur, wie sie die Bundesnetzagentur vorschlägt. Wünschenswert wäre es, wenn solche Vorstellungen auch EU-weit umgesetzt werden könnten. Hierauf sollte Deutschland hinwirken. Anstelle nationaler Sonderwege mit zusätzlichen Kosten könnten Effizienzgewinne im europäischen Binnenmarkt gehoben werden. Zudem muss auch klar sein, dass nicht die Netzbetreiber alleine die Verantwortung tragen, sondern auch die Hersteller ihren Teil dazu beitragen müssen.

1. Zu 3 Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung von personenbezogenen Daten

1.1 Zu 3.3.1 „Sicherer Umgang mit sensiblen Daten und Informationen“

Im Bereich der Telekommunikation sind Bestands- und vor allem Verkehrsdaten hoch sensible Daten. Sie unterliegen dem Datenschutz und dem Schutz des Fernmeldegeheimnisses. Es müssen daher Regelungen zum sicheren Umgang mit solchen Daten und Informationen getroffen werden. Insbesondere gilt:

- Umsetzung von angemessenen organisatorischen und technischen Vorkehrungen nach Stand der Technik,
- Umsetzung im Rahmen eines Managementsystems, z.B. Informationssicherheitsmanagementsystems (ISMS).

1.2 Zu 3.3.2 „Physische und elementare Schutzanforderungen“

Es werden neun Aufzählungspunkte als mindestens umzusetzende Maßnahmen benannt. Diese erscheinen willkürlich und entsprechen nicht der Grundlogik eines ISMS mit Risikomanagement, in dem man feststellt, welche Maßnahmen zu befolgen sind und welche nicht. Dazu ist die Wirtschaft bzw. der jeweils gültige Geltungsbereich des jeweiligen Betreibers zu heterogen, als dass man pauschale Mindestangaben vornehmen sollte. Hier eignet es sich eher, auf die bestehenden Sicherheitsstandards inkl. dem sog. Stand der Technik und einem ISMS zu verweisen, also beispielsweise dem BSI Grundschutz-Kompendium oder der ISO 27001.

Diese Auflistungen ziehen sind durch das Dokument, insbesondere natürlich durch Abschnitt 3.3.

1.3 Zu 3.3.4 Zugriffs- und Zugangskontrolle auf Netzwerk- und Informationssystemen

„Gesicherte Bereiche“ waren in der Vergangenheit Vermittlungsstellen oder IT-Serverräume, die über einen zentralen Zugang geschützt, aber im Inneren Systemschränke ohne Türen und weiteren Zugangsschutz ausgebaut waren. Für diese ist die Anforderung aus 3.3.4 zielgerichtet. Heute gibt es dagegen komplexere physikalische Infrastrukturen, z. B. zentrale Rechenzentren, in denen verschiedene Schutzbedarfe mit unterschiedlichem Schutzniveau in gemeinsamen Räumlichkeiten untergebracht sind. Für eine angemessene Trennung gibt es hierfür eigene Käfigbereiche oder zumindest eigene abgeschlossene Serverschränke, die über individuelle Schlüssel- oder Kartensysteme gegen unbefugten Zugang geschützt sind. Jedoch stellen diese Absicherungen keine eigenen „gesicherte Bereiche“ dar, sondern „gesicherte technische Anlagen“ (als allgemeiner gefassten Begriff). Durch ein geeignetes Sicherheitskonzept (24/7 Sicherheitsdienst, Kameraüberwachung u. ä.) wird in solchen Umgebungen dennoch sichergestellt, dass der Zugriff für Personen mit berechtigtem Interesse möglich ist.

2. Zu Anlage 2: Weitergehende Sicherheitsanforderungen für Betreiber von Netzen mit erhöhtem Gefährdungspotenzial

2.1 Vorbemerkung

Im Sinne der stärkeren Etablierung des Europäischen (Digitalen) Binnenmarktes und der Entwicklung grenzüberschreitender 5G-basierter Anwendungen sollte zunehmend auf europäische, anstatt nationaler Ansätze abgezielt werden. Anstelle der vorgesehenen Vertrauenswürdigkeitserklärung, braucht es deshalb einen europaweit verbindlich geltenden Cybersecurity Scheme für 5G-Netzwerkkomponenten auf Basis des EU Cybersecurity Acts. Zudem gilt es Implikationen des IT-Sicherheitsgesetzes 2.0 auf das aktuelle Verfahren so vice versa zu berücksichtigen.

Ziel der Überarbeitung des Anforderungskatalogs, sowie darüber hinausgehender Initiativen wie der TKG-Novelle zur Umsetzung des Europäischen Kodex für elektronische Kommunikation oder der aktuellen Überarbeitung des IT-Sicherheitsgesetzes muss es sein Rechtssicherheit für die Telekommunikationsbranche zu schaffen und gleichzeitig die Unternehmen einzubeziehen, die ihrerseits für eine sicherere Infrastrukturausstattung unabdingbar sind. Dabei dürfen und können allgemeinpolitische Fragestellungen weder durch technisch-regulatorische Anforderungsdefinitionen beantwortet werden, noch kann die Beantwortung durch privatwirtschaftlich agierende Unternehmen erfolgen.

Das vorgesehene Verfahren sieht zwei Säulen vor: technische Überprüfungen und Vertrauenswürdigkeit. Neben der technischen Überprüfung von Komponenten, sollte die Bewertung der Vertrauenswürdigkeit von Herstellern ebenfalls eine staatliche Aufgabe sein und darf nicht delegiert werden. Dies können sowohl der Entwurf des Sicherheitskataloges nach §109 TKG, als auch das TKG nicht erfüllen, da nur Betreiber, nicht aber Zulieferer, adressiert werden. Eine entsprechende Rechtsgrundlage, die u.a. eine sachgerechte Verantwortungszuweisung regelt, muss geschaffen werden.

Um Rechtsunsicherheit bei den Betreibern zu vermeiden, muss des Weiteren geklärt werden, wie die Sicherheit und Vertrauenswürdigkeit von Dritten überprüft und gewährleistet werden kann. Der Regulierer muss die Frage beantworten, welche weiteren Prozesse er hiermit auslöst.

2.2 Zu 1. Anwendungsbereich

Die Definition des Anwendungsbereiches bzw. der Definition des „erhöhten Gefährdungspotenzials“ für die Festlegung der Adressaten der im Folgenden genannten weiteren Sicherheitsanforderungen lässt konkrete Kriterien für die Festlegung – abgesehen von den offensichtlich erfassten Mobilfunknetzbetreibern – vermissen. Im Sinne der Rechtssicherheit für betroffene Netzbetreiber und Diensteanbieter sollten hier konkretere Angaben gemacht werden.

Darüber hinaus weisen wir darauf hin, dass der Anwendungsbereich des Sicherheitskataloges auch im weiteren Kontext betrachtet werden muss:

1. Der Anwendungsbereich des TKG und des Sicherheitskatalogs nach §109 TKG richtet sich im Wesentlichen an die Betreiber. Gleichzeitig gilt, dass Sicherheit einen kooperativen Ansatz mit Pflichten und Verantwortungszuweisungen für alle Akteure voraussetzt.

2. Der Beibehalt und die Stärkung harmonisierter Regelungen zwischen den Mitgliedstaaten der EU bedarf eines europäischen Ansatzes mit mindestens europäischen, wenn nicht globalen Standards. Andernfalls tritt eine Schwächung der bisher erreichten Harmonisierung, damit von Wettbewerb und Sicherheit ein. Wir begrüßen dennoch das Vorhaben, die Fortentwicklung der Sicherheitsanforderungen schnellstmöglich zu betreiben, wenn eine deutsche Fortentwicklung zu keinem Sonderweg, sondern abgestimmt und mit Vorbildcharakter zu einer rascheren europäischen Lösung führt.

2.3 Zu 2. Zertifizierung von kritischen Kernkomponenten

Es bedarf zunächst einer Klärung zusammen mit der Wirtschaft, welche Netz- und Systemkomponenten als »kritisch« eingestuft werden. Eine vollständige Bewertung des Katalogs kann ohne eine solche Festlegung nicht erfolgen. Weiterhin zu klären ist, wie eine Zusicherung der Vertrauenswürdigkeit in geeigneter Weise und rechtssicher erfolgen soll.

Dies und eine Zertifizierung von kritischen Kernkomponenten sollten sich mindestens auf europäische, im Idealfall internationale, anerkannte Standards berufen und existierende Gremien weitestgehend berücksichtigen. Die Regulierung und insbesondere eine mögliche

Zertifizierung sollten nicht zu einer losgelösten nationalen Sonderlösung[1] führen, die die Einführung von 5G in Deutschland verzögert und mit Mehrkosten belastet.

Des Weiteren, weisen wir darauf hin, dass Netz- und Systemkomponenten einer hohen Entwicklungsdynamik unterliegen. Prüfungs- und Zertifizierungsverfahren dürfen keinen Engpass darstellen und v.a. bei Personalengpässen in den Prüf- und Zertifizierungsstellen zu keinem verzögerten Einsatz der kritischen Kernkomponenten führen. Gerade softwaretechnische Anpassungen, die sicherheitskritische Komponenten beinhalten, müssen zeitnah eingebracht werden. Hier könnten europäische oder internationale IT-Managementstandards als Vorlage dienen, um den Prüfungsaufwand risikoorientiert zu priorisieren bzw. den Aufwand in einem angemessenen Rahmen zu belassen – Ziel kann nicht sein, dass jedes Update zu einer Rezertifizierung führt.

Bitkom begrüßt daher, dass der Katalog eine breitere Basis an Prüfstellen, die durch das BSI zu zertifizieren sind, vorsieht, um möglichen Engpässen auf behördlicher Seite effektiv zu begegnen. Entsprechende Sicherheitskontrollen durch vom BSI zertifizierte Prüfstellen sind laut §2 Abs. 7 des BSI-Gesetzes vorgesehen: Die »Zertifizierung im Sinne dieses Gesetzes ist die Feststellung durch eine Zertifizierungsstelle, dass ein Produkt, ein Prozess, ein System, ein Schutzprofil (Sicherheitszertifizierung), eine Person (Personenzertifizierung) oder ein IT-Sicherheitsdienstleister bestimmte Anforderungen erfüllt«. Testverfahren für »kritische« Komponenten sollten an einem unter Kontrolle des Herstellers sich befindenden sicheren Ort in Europa durchgeführt werden.

In diesem Kontext ist zu beachten, dass ein Rahmen für die gegenseitige Anerkennung innerhalb Europas notwendig ist, um Skalierbarkeit, Wirksamkeit und Effizienz zu gewährleisten. Es sollten Genehmigungsbehörden benannt werden, die eine verbindliche, robuste Prüfmethode anwenden – wie das BSI und ANSSI. Ohne diese wird jedes Land die Tests zu hohen Kosten wiederholen und die Anforderungen an die rechtzeitige Erprobung neuer Technologien nicht erfüllen können. Das BSI-Gesetz bietet die Mittel für eine solche gegenseitige Anerkennung im europäischen Kontext. §9(7) stellt klar, dass grundsätzlich »Sicherheitszertifikate anderer anerkannter Zertifizierungsstellen aus dem Bereich der Europäischen Union vom Bundesamt anerkannt werden«.

Hinsichtlich des von der Bundesnetzagentur und dem BSI zu erstellenden Dokuments, welches in einem ersten Teil die kritischen Funktionen und in einem zweiten Teil die kriti-

[1] Das BSI sollte z. B. davon absehen, „neben der IT-Sicherheitszertifizierung im Kontext internationaler Abkommen [...], nach einer Technischen Richtlinie zu zertifizieren“, um einen harmonisierten, europäischen Ansatz nicht zu fragmentieren.

schen Komponenten auflistet, begrüßen wir die vorgesehene Berücksichtigung von Ergebnissen internationaler Analysen wie zum Beispiel der ENISA oder BEREC. Aus unserer Sicht muss eine Zertifizierung kritischer Komponenten auf europäischen oder globalen Standards aufzubauen, da die Normierung und Standardisierung ebenfalls auf supranationaler Ebene stattfinden. Hier begrüßen wir den Bezug auf die Verordnung (EU) 2019/881 (Cybersecurity Act) am 27.06.2019 mit welcher ein einheitliches europäisches Rahmenwerk in der Cybersicherheitszertifizierung eingeführt wurde, in dem die Anerkennung von europäischen Schemata für die Cybersicherheitszertifizierung geregelt ist. Zur Beteiligung von Herstellern, Verbänden der Betreiber öffentlicher Telekommunikationsnetze und Verbände der Anbieter öffentlich zugänglicher Telekommunikationsdienste wird in Anlage 2 unter Punkt 2.3 darauf verwiesen, dass es die Gelegenheit zu einer Stellungnahme gibt. Bitkom empfiehlt eine aktive Beteiligung der Wirtschaft bei der Erstellung und Aktualisierung des Dokuments, um Vorschläge bzw. Eingaben einreichen zu können. Im Zuge dieser aktiven Beteiligung sollten die zu erfassenden Kernkomponenten brancheneinheitlich identifiziert und benannt werden.

Um den Betrieb und die Weiterentwicklung neuer Technologien (wie z.B. des 5G-Mobilfunknetzes) zu gewährleisten, halten wir eine Präzisierung des vorliegenden Entwurfs dahingehend für sinnvoll, dass Ausnahmen und Sonderfälle berücksichtigt werden. Die 5G-Technologie wird z.B. Software-Updates in kurzen Zeitintervallen erforderlich machen. Hier sollte definiert werden, welche Kategorie von Software-Updates einer erneuten Zertifizierung bzw. Prüfung unterzogen werden müssen. Aus unserer Sicht ist eine Zertifizierung jedes Software-Updates nicht sinnvoll und auch im Betrieb nicht abbildbar. Zudem sehen wir hier einen erheblichen Einfluss auf die Ressourcenverfügbarkeit des BSI. Generell sollte es aus unserer Sicht neben dem Regelprozess der Zertifizierung für Ausnahme- bzw. Notfälle die Möglichkeit eines alternativen, beschleunigten Prüf-/Zertifizierungsverfahrens geben, welches z.B. den Betrieb einer kritischen Kernkomponente kurzfristig ermöglicht und ein paralleles oder nachgelagertes Prüf-/Zertifizierungsverfahren vorsieht.

Desweitern sollte präzisiert werden, wie mit kritischen Kernkomponenten von Bestandstechnologien (z.B. 2G/3G) verfahren werden soll. Aus Sicht des Bitkom kann sich eine Zertifizierungspflicht nur auf neu in Betrieb genommene Systemkomponenten erstrecken und keine Rückwirkung entfalten. Unter Punkt 2.5 in Anlage 2 (Übergangsfristen) wird hierzu ausgeführt, dass für Komponenten, die im Sinne von 2.3 als kritische Komponenten zu betrachten sind und vor dem 01.01.2021 ausgeliefert wurden, eine Übergangsfrist zur Erlangung eines gültigen Zertifikats bis zum 31.12.2025 gewährt wird. Voraussetzung für die Gewährung einer Übergangsfrist ist die Aufnahme der entsprechenden Komponenten

in die Liste der kritischen Komponenten vor dem 01.01.2021. Aus unserer Sicht sollten hier zusammen mit den Netzbetreibern im Rahmen der Erstellung der Liste angemessene Übergangsfristen anhand der ausgewählten Komponenten festgelegt werden.

In diesem Zusammenhang muss auch die Frage geklärt werden, was geschieht, wenn eine Zertifizierung nachträglich entzogen wird, z. B. durch nicht vorhanden sein von Software-Updates. Wer trägt hierfür die Kosten?

2.3.1 Zu 2.3 Liste kritischer Funktionen und Komponenten

Generell begrüßen wir die Akzeptanz und die Berücksichtigung internationaler Standards und Analysen wie z.B. der ENISA oder BEREC. Insbesondere bei der Entwicklung und Aktualisierung der Liste „kritischer Funktionen und Komponenten“. 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 Kernkomponenten müssen eindeutig identifizierbar festgelegt werden. Übergreifende Bezeichnungen, wie aktuell teilweise in der BSI-KritisV verwendet, sind nicht präzise genug. Wir schlagen vor, Betreiber von Telekommunikationsnetzen und -diensten an der Festlegung zu beteiligen und eine gemeinsame Arbeitsgruppe aus Behörden und Telekommunikationsunternehmen unter Leitung der BNetzA zu bilden oder den Branchenarbeitskreis Telekommunikation (BAK TK) im UP KRITIS zu nutzen.

In Anlage 2 Punkt 2.3 erhalten auch die Betreiber der Telekommunikationsdienste die Möglichkeit einer Stellungnahme. Hier erwarten wir nicht nur die Möglichkeit der Stellungnahme, sondern auch die Möglichkeit einer Beteiligung an der Ausarbeitung und der Berücksichtigung unserer Eingaben.

2.3.2 Zu 2.5 Übergangsregelungen

Hierzu muss die rechtliche Grundlage geschaffen werden, dass der Hersteller/Lieferant dieser Komponente frühzeitig den Zertifizierungsprozess analog zu neuen Komponenten einleitet. Es ist dabei zu beachten, dass dieses ausgehend vom Betreiber im Rahmen bestehender Verträge nicht möglich ist und somit einen erheblichen Risikofaktor für die Aufrechterhaltung des Betriebes bedeuten kann.

2.4 Zu 3. Vertrauenswürdigkeit von Herstellern und Lieferanten

Hersteller und Lieferanten leisten bereits heute einen großen Beitrag zu einer sicheren Netzinfrastruktur. Dass der vorliegende Entwurf gemäß Ziffer 3 vorsieht, diese Verantwortung auch schriftlich entlang der hier aufgeführten Anforderungen beurkunden zu müssen, unterstützen wir.

Die Vertrauenswürdigkeit eines Hersteller/ Lieferanten dürfte sich primär an der Qualität einer transparenten und offenen Informationspolitik festmachen, die ein Hersteller/ Lieferanten bzgl. der Umsetzung der genannten Bestimmungen und Gesetze an den Tag legt sowie entsprechender Erkenntnisse und Erfahrungen aus der Vergangenheit. Auch im Kontext der Vertrauenswürdigkeit bleibt offen, was geschehen soll, wenn ein Lieferant seine Vertrauenswürdigkeit einbüßt, obgleich bereits seine Technik Bestandteil der Infrastruktur ist. Hier müssen klare Verantwortlichkeiten, Ausstiegsszenarien und Übergangsfristen Rechtssicherheit bieten.

Wird einem bereits eingesetzten Hersteller/Lieferanten die Vertrauenswürdigkeit aberkannt, muss sichergestellt sein, dass die Beweislast für den Grund der Aberkennung nicht durch den Netzbetreiber, sondern durch eine staatliche Institution/Behörde idealerweise auf europäischer Ebene erbracht wird. Dazu gehören z.B. mögliche Korrekturen des Netzes und die Wiederherstellung der Sicherheit in diesem operativen Netz.

Um die rechtliche Asymmetrie zwischen technischer Zertifizierung und Erklärung der Vertrauenswürdigkeit aufzuheben, ist es erforderlich, dass auch die Bewertung der Vertrauenswürdigkeit durch unabhängige, staatliche Stellen erfolgt. Den Netzbetreibern die Evaluation der Vertrauenswürdigkeit zu überlassen, entlässt den Staat aus der Pflicht, eine solche, politische und sachliche Bewertung zu treffen.

2.4.1 Zu Punkt 4:

Hier sollte die Verpflichtungen der Hersteller geklärt werden. Die vorliegende Fassung führt zu einer unlösbaren Situation und steht beispielsweise im Widerspruch zum Ansatz der EU-Kommission, die europäischen Strafverfolgungs- und Justizbehörden in die Lage zu versetzen, elektronische Beweismittel im Rahmen der E-Evidence-Richtlinie zu sichern.

2.4.2 Zu Punkt 10:

Hier sollte der Begriff "unverzüglich" weiter geklärt werden. Es ist notwendig, dass Hersteller sämtliche Kunden bzw. Nutzer rechtzeitig sowie gleichzeitig und damit gleichberechtigt über Sicherheitsrisiken informieren. Die Benachrichtigung von Betreibern, bevor eine Schwachstelle vom Hersteller nach Bedeutung, Auswirkung und Ausnutzbarkeit priorisiert wurde, und ihm die Behebung, ein Workaround oder eine Eingrenzung ermöglicht wurde, würde zu einer weniger sicheren Situation führen.

2.5 Zu 4. Produktintegrität

Neu zu beschaffende, kritische Komponenten unterliegen einer Prüfung und Zertifizierung des BSI. Insofern gehen wir grundsätzlich davon aus, dass der Auslieferungszustand von Hard- bzw. Software dem geprüften und zertifizierten Zustand entspricht.

Im Hinblick auf die benannten kritischen Phasen des Lebenszyklus einer Komponente unterstützen wir die Verpflichtung der Hersteller, technische Methoden/Verfahrensweisen zur Prüfung der Produktintegrität in das Produkt zu integrieren und die Herangehensweise zur Durchführung der Verifikation gegenüber dem Betreiber geeignet zu dokumentieren. Ebenso begrüßen wir die weitern Mitwirkungsverpflichtungen der Hersteller, welche aber inkl. notwendiger Schutzmaßnahmen regulatorisch eindeutig zu verankern ist. Wir begrüßen die Entwicklung eines solchen Ansatzes, weisen aber darauf hin, dass ein solch komplexes Instrument, einige Jahre Entwicklung beanspruchen wird.

Ähnlich gravierend sind die Auswirkungen auf die bestehenden branchenüblichen Prozesse hinsichtlich Lieferung, Lagerung, Inbetriebnahme und Retirement, welche vollständig neu entwickelt werden müssten und ebenfalls in den bestehenden vertraglichen Beziehungen Niederschlag finden müssten. Insbesondere vor dem Hintergrund, dass eine Zertifizierung/Prüfung, gepaart mit den hier aufgeführten Kontrollmechanismen einer präventiven Kontrolle darstellt, welche den Einsatz von integren Produkten gewährleistet und so grundsätzlich aus Risikoaspekten zu bevorzugen wäre.

In der Zusammenarbeit mit vertrauenswürdigen Lieferanten/ Herstellern sollte vielmehr davon ausgegangen werden, dass die vom BSI zertifizierten kritischen Kernkomponenten genau in der geprüften und zertifizierten Hardware- und Softwarekombination zum Einsatz kommen. Eine weitere Nachweisverpflichtung erscheint in der Anwendung nicht

praktikabel. Um sich zu vergewissern, dass die auf der Netzwerkinfrastruktur laufende Software mit der vom Hersteller gelieferten übereinstimmt, ist das Konzept der binären Äquivalenz ein grundlegender Test. Das ist eine Herausforderung – es ist zu überlegen, ob der Anbieter die Tools bereitstellen muss, damit der Betreiber dies unabhängig überprüfen kann.

Zyklus, Inhalt und Form der regelmäßigen Sicherheitsüberprüfungen sind festzulegen, idealerweise mit längeren Intervallen für kritische Kernkomponenten im Vergleich zu besonders kritischen Kernkomponenten (vgl. Redundanz-Anforderung). Jegliche Form der zusätzlichen Abnahmeprüfungen und regelmäßigen Sicherheitsüberprüfungen binden neue Ressourcen bei den verpflichteten Unternehmen. Die Vorgaben dazu sollten daher dem Angemessenheitsgrundsatz des TKGs folgen. Inhalt und Form der Abnahmeprüfungen sollten außerdem mit den Prüfungsinhalten zur BSI-Zertifizierung abgestimmt sein, damit nur die Punkte zur Abnahme im Fokus stehen, die nicht bereits überprüft wurden.

Grundsätzlich bestehen Zweifel an der Angemessenheit (vgl. § 109 Abs. 2 TKG) und Umsetzbarkeit dieser Anforderung aufgrund der Komplexität und Vielfalt der Netz- und Systemkomponenten und der Entwicklungsdynamik in den unterschiedlichen Technologien.

2.6 Zu 5. Sicherheitsanforderungen im laufenden Betrieb

2.6.1 Zu 5.1.: Sicherheitsmonitoring

Im Fokus dieser Forderung stehen alle Arten des internen und externen Monitorings um Angriffe oder Fehler zu erkennen. Grundsätzlich wird der Netzverkehr über die Netz- und Systemkomponenten bereits jetzt auf Auffälligkeiten beobachtet. Es ist zu konkretisieren, welche besonderen Merkmale eine MI (Monitoring Infrastruktur) hat. Hierfür bestehen bereits branchenspezifische Vorgaben. Dabei ist zu beachten, dass eine Erkennung nach Art der Störung bzw. des Angriffs implementiert werden muss, so gibt es z.B. die Kommunikation infizierter Endgeräte, die Ausnutzung gehackter Telefonanalgen sowie die Anrufe ausländischer bzw. gefälschter Infrastrukturkomponenten.

Gerade die gesetzlichen Vorgaben zum Schutz des Fernmeldegeheimnisses dürften es praktisch schwierig machen, unautorisierte und gezielte Abgriffe von Kommunikationsdaten bei Anwendung von Verschleierungstechniken erkennen zu können. Aus diesem Grund erscheinen die nun geforderten MI in Teilen als schwer umsetzbar und unverhältnismäßig. Sinnvoller wäre ein Sicherheitsmonitoring, welches sich an den Schutzzielen orientiert.

Grundsätzlich muss außerdem sichergestellt sein, dass im Rahmen eines Monitorings keine staatlichen Aufgaben an die Betreiber delegiert werden.

2.7 Zu 6. Eingewiesenes Fachpersonal

Nachdem hier in der Version geklärt ist für welche Art von Fachpersonal diese Anforderung bestehen soll (zur Aufrechterhaltung des Betriebes der kritischen Kernkomponenten) regen wir an, die in Anlage 2 Punkt 6 angebrachten Anforderung als Rahmenbedingungen in einem Rollenprofil einzubringen.

Ebenso ist detaillierter zu beschrieben, für welche gesetzlichen Vorgaben eine Nachweispflicht besteht, wer Verpflichteter ist, die Nachweise vorzuhalten hat und wem gegenüber den Nachweisen zu erbringen sind. In diesem Zusammenhang ist auch eine genauere spezifizierte Definition der Sanktionen erforderlich.

Je nach Art der ausgelagerten systemrelevanten Prozesse ist zu beachten, dass auch Lieferanten-/ Hersteller-unabhängige Auftragnehmer dafür in Betracht kommen. Es kann aber nicht davon ausgegangen werden, dass die Betreiber der ausgelagerten Prozesse grundsätzlich unabhängig von den Telekommunikationsunternehmen sind. Das ist insbesondere dann nicht der Fall, wenn das in Deutschland ansässige und nach TKG verpflichtete Telekommunikationsunternehmen und der Auftragnehmer einem Konzernverbund angehören.

Fraglich ist, ob ein Auftragnehmer automatisch oder nur dann als „zuverlässig“ gilt, wenn dieser „vertrauenswürdig“ im Sinne dieser Regelung ist. Auch das bedarf der Klarstellung.

2.8 Zu 7. Redundanzen

Zum Schutz vor Störungen bzw. Ausfällen kritischer Komponenten wird als eine mögliche Präventivmaßnahme die Schaffung von Redundanzen benannt. Bitkom begrüßt hier, dass die Schaffung von Redundanzen einer angemessenen, unternehmensinternen Risikobewertung unterliegen soll und nicht als einzige Maßnahme pauschal für alle kritischen Komponenten gefordert wird. Eine pauschale Forderung hätte in nicht unerheblichen Umfang steigende Betriebsaufwände und Wartungskosten zur Folge.

2.9 Zu 8. Diversität

Es bedarf der Klarstellung, worauf sich die Forderung »nach ausreichender Diversität durch Einsatz von Netz- und Systemkomponenten unterschiedlicher Hersteller« bezieht. Grundsätzlich gilt mit der damit implizierten Forderung nach einer Mehr-Lieferanten-Strategie zu beachten, dass eine solche Konstellation erfahrungsgemäß zu einer erhöhten Systemkomplexität und damit zu neuen Quellen für funktionale Instabilitäten und Sicherheitsschwachstellen führt. D. h., eine Entscheidung über den Einsatz von einem oder mehreren Herstellern zur Realisierung kritischer Netzfunktionen bedarf einer detaillierten Abwägung von funktionalen, betrieblichen und sicherheitstechnischen Aspekten und ist in jedem Einzelfall separat vorzunehmen.

Die im Markt aktiven Netzbetreiber verfolgen bereits heute eine »Multi-Vendor«-Strategie. Durch eine Fortschreibung dieser Betreiberstrategien kann auch im 5G-Kontext das Risiko einseitiger Abhängigkeiten vermieden werden. Allein eine »Multi-Vendor«-Strategie aber führt nicht zu mehr Sicherheit. Wenn die Produkte aller Anbieter nicht gleichermaßen vertrauenswürdig sind, kann die Logik eines risikobasierten Ansatzes tatsächlich zu dem gegenteiligen Effekt führen und die Anzahl der Anbieter begrenzen, die für sensible Teile des Netzwerks zur Verfügung stehen. Die Forderung nach einem »Multi-Vendor«-Ansatz in bestimmten Architekturbereichen, wie beispielsweise dem Kernpaketnetz oder Teilen davon, könnte die Implementierung weniger sicher und aus architektonischer und betrieblicher Sicht wesentlich komplexer machen. Es erhöht die notwendige Anzahl und das notwendige Know-how der Fachkräfte, die für die Wartung des Netzwerks erforderlich wären – was in Zeiten des Fachkräftemangels schwierig ist – und die Betriebskosten erhöht. Außerdem wird es bereits heute durchgeführt.

Kritisch sehen wir in diesem Kontext auch die allgemeine Forderung hinsichtlich der Verwendung von mindestens zwei Herstellern im Core-/Access-Netz sowie die zwei Drittel Regelung im Hinblick auf das Gesamtnetz. Neben operativen Problemen, welche sich aus dem Betrieb von Netz- und Systemkomponenten unterschiedlicher Hersteller ergeben, sehen wir aus einer solch starren Anforderung Risiken im Hinblick auf den sicheren Betrieb des Netzes erwachsen. Die praktische Erfahrung zeigt, dass trotz internationaler Standardisierung die Konfiguration unterschiedlicher Herstellerkomponenten aufwendig und störanfällig ist.

Die Diversitätsaufteilung 1:2 gem. Ziffer 8 scheint hingegen willkürlich und trifft nicht die Bedürfnisse einer funktionalen Netzarchitekturplanung. Diese Aufteilung sollte ein Richt-

wert sein bzw. empfehlenden Charakter haben. Um Monokulturen grundsätzlich zu vermeiden ist die Festlegung eines Prozentanteils überdies entbehrlich.

Grundsätzlich sollte an dieser Stelle auch präzisiert werden, ob sich diese Forderungen ausschließlich auf den Einsatz von als kritisch definierten Komponenten beziehen oder pauschal alle Netz- und Systemkomponenten umfasst.