Stellungnahme

Aktualisierung des Katalogs von Sicherheitsanforderungen nach § 109 TKG durch die Bundesnetzagentur

29. März 2019

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.

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

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

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

Dr. Nabil Alsabah
Bereichsleiter IT-Sicherheit
T +49 30 27576-242
n.alshbah@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Achim Berg

Hauptgeschäftsführer
Dr. Bernhard Rohleder

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 entsprechend ihren jeweiligen Rollen und Zuständigkeiten 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 nationale 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.

Zu den Eckpunkten der Bundesnetzagentur im Einzelnen

Bitkom begrüßt, dass die Bundesnetzagentur Eckpunkte zusätzlicher Sicherheitsanforderungen 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.

- *»Der Netzverkehr muss ständig auf Auffälligkeiten hin beobachtet werden und im Zweifelsfall sind geeignete Maßnahmen zum Schutz zu ergreifen (z. B. Netzverkehr unterbinden, Verkehr zu Störern einschränken oder unterbinden). Die Detektionsmaßnahmen müssen dem Stand der Technik entsprechen.«*

Auffälligkeiten im Netzverkehr sind aus Sicht des Bitkom Eingriffe in die ordnungsgemäße Funktionsfähigkeit der Netztechnik bzw. betreffen den Abgriff oder die Manipulation von Kommunikationsdaten jeglicher Art. Entsprechende Mechanismen sind bereits heute vorgesehen und implementiert.

Die aktuellen Sicherheitslösungen auf dem neuesten Stand der Technik umfassen die Fähigkeit, fortgeschrittene Bedrohungen mit Hilfe von Algorithmen des maschinellen Lernens zu überwachen und zu erkennen, um Anomalien des normalen Netzwerkbetriebs zu erkennen und eine Kontrolle auf der Grundlage von Richtlinien zur Abwehr von Angriffen nahe der Quelle bereitzustellen.

Der Ausdruck »ständig« bedarf der Konkretisierung. Abhängig von der jeweiligen Interpretation kann eine Auslegung von permanent (im Sinne von ständig = fortlaufend) bis sporadisch (z. B. regelmäßige Stichproben in größeren Zeitabständen) reichen.

- *Die Festlegung der sicherheitsrelevanten Netz- und Systemkomponenten (kritische Kernkomponenten) erfolgt einvernehmlich zwischen BSI und BNetzA.*

- *»Sicherheitsrelevante Netz- und Systemkomponenten (kritische Kernkomponenten) dürfen nur eingesetzt werden, wenn sie von einer vom BSI anerkannten Prüfstelle auf IT-Sicherheit überprüft und vom BSI zertifiziert wurden. Kritische Kernkomponenten dürfen nur von solchen Lieferanten/Herstellern bezogen werden, die in geeigneter Weise ihre Vertrauenswürdigkeit zusichern. Die Verpflichtung soll für die gesamte Lieferkette gelten und Voraussetzung für die notwendige Zertifizierung der Komponenten sein. Diese Vorgaben werden im Katalog weiter konkretisiert werden. Die hierfür zugrundeliegenden Standards werden vom BSI im Benehmen mit der BNetzA veröffentlicht. Um die Verbindlichkeit der Anforderungen sicherzustellen und konkrete Anforderungen wie etwa die Zertifizierungspflicht rechtlich eindeutig abzusichern, planen die zuständigen Ministerien entsprechende gesetzliche Absicherungen, insbesondere im Rahmen der laufenden großen Novelle des Telekommunikationsgesetzes.«*

- *»Sicherheitsrelevante Netz- und Systemkomponenten (kritische Kernkomponenten) dürfen nur nach einer geeigneten Abnahmeprüfung bei Zulieferung eingesetzt werden und müssen regelmäßig Sicherheitsprüfungen unterzogen werden. Sollten bei den Prüfungen Abweichungen gegenüber den Leistungsvorgaben der Netzbetreiber oder Erbringer auftreten, sind diese zu dokumentieren und einem Risikobehandlungsprozess zuzuführen. Bei Abweichungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen und -diensten führen können, sind die BNetzA und das BSI über die zur Minderung des Risikos ergriffenen Maßnahmen umgehend zu informieren.«*

Es bedarf zunächst einer Klärung zusammen mit der Industrie, welche Netz- und Systemkomponenten als »kritisch« eingestuft werden. Eine vollständige Bewertung der Eckpunkte 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 sollte nicht zu einer nationalen und deutschlandspezifischen Sonderlösung führen, die die Einführung von 5G in Deutschland verzögert und mit Mehrkosten belastet.

Bitkom begrüßt daher, dass die Eckpunkte 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.

Ein Rahmen für die gegenseitige Anerkennung innerhalb Europas ist notwendig, 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«.

- *»In sicherheitsrelevanten Bereichen darf nur eingewiesenes Fachpersonal mit vertieften Systemkenntnissen zur Bewertung von Gefährdungen und Schutzmaßnahmen eingesetzt werden. Dieses Personal ist in ausreichendem Umfang vorzuhalten.«*

Diese Anforderung bedarf der Klarstellung, was mit sicherheitsrelevanten Bereichen gemeint ist und was Gegenstand und Inhalt einer Einweisung von Fachpersonal sind. In diesem Zusammenhang sind auch physische Zugangsberechtigungen (z. B. Zugangskontrollsysteme) zu berücksichtigen. Eine allgemeine Verpflichtung für Betreiber, geschulte und vertrauenswürdige Fachleute, unabhängig davon, ob es sich um Mitarbeiter oder Personen gemäß eines Dienstleistungsvertrags handelt, für sicherheitsrelevante Aufgaben einzusetzen, ist grundsätzlich richtig. Hier sollte dennoch sehr vorsichtig/umsichtig vorgegangen werden, bevor empfohlen wird, dass diese Personen vom BSI zertifiziert werden oder anderweitig allgemein eine Sicherheitsfreigabe erhalten. Die durch den Zertifizierungsprozess verursachte Verzögerung erschwert es den Unternehmen, effektiv auf die Nachfrage zu reagieren und könnte das Angebot an solchen Dienstleistungen verringern. Angesichts des derzeitigen Mangels an Sicherheits- und Netzwerkexperten auf breiter Front könnten zusätzliche Einschränkungen, beispielsweise in Bezug auf die Nationalität, das Problem noch verschärfen.

- *»Es ist nachzuweisen, dass die für ausgewählte, sicherheitsrelevante Komponenten geprüfte Hardware und der Quellcode am Ende der Lieferkette tatsächlich in den verwendeten Produkten zum Einsatz kommen.«*

Es bedarf zunächst einer grundsätzlichen Klarstellung und Definition der hier vorgesehenen Komponenten und Maßnahmen, u. a. der »*ausgewählten, sicherheitsrelevanten Komponenten*«. Dabei und für die daran anknüpfenden Testverfahren sollte ein risikobasierter Ansatz verfolgt werden, der eine robuste und dynamische Schwachstellenanalyse beinhaltet.

Die Tests hierfür sollten an einem unter Kontrolle des Herstellers sich befindenden sicheren Ort in Europa durchgeführt werden. Die Einsicht in die Quellcodes sowie der Zugang zu diesen durch Dritte in einer Umgebung außerhalb der kontrollierten und sicheren Umgebung des jeweiligen Ausrüsters hingegen birgt Risiken und unkontrollierte sowie nichtintendierte Konsequenzen für die Sicherheit kritischer Infrastrukturen.

- *»Bei Planung und Aufbau der Netze ist eine ausreichende Diversität durch Einsatz von Netz- und Systemkomponenten unterschiedlicher Hersteller sicherzustellen. Diese Vorgabe wird von der BNetzA konkretisiert und kann etwa für das Core- bzw. Access-Network unterschiedlich ausfallen.«*

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.

Eine »Multi-Vendor«-Strategie allein 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 beispiels-

weise 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 erhöht die Betriebskosten. Außerdem wird es bereits heute durchgeführt.

- *»Die Netzbetreiber und Erbringer müssen bei Auslagerung von systemrelevanten Prozessen sicherstellen, dass unabhängige, fachkompetente und zuverlässige Auftragnehmer ausgewählt werden und die Einhaltung von gesetzlichen Vorgaben gewährleistet bleibt. Sie haben dies nachzuweisen.«*

Die Anforderung bedarf der Klarstellung, um welche »systemrelevanten Prozesse« es sich hier handelt. Bzgl. einer Beurteilung von Zuverlässigkeit und Vertrauenswürdigkeit eines Auftragnehmers gilt analog der oben festgestellte Klärungsbedarf .

- *»Für kritische, sicherheitsrelevante Netz- und Systemkomponenten (kritische Kernkomponenten) müssen ausreichend Redundanzen vorgehalten werden. Hierfür wird eine Liste besonders kritischer Netzkomponenten (z. B. Home Location Register, Core Network, Backbone, Portierungsserver) erstellt.«*

Es bedarf einer Klarstellung, ob die hier genannten »kritischen, sicherheitsrelevanten Netz- und Systemkomponenten (kritische Kernkomponenten)« mit den oben genannten »kritischen Kernkomponenten« identisch sind. Dann ist eine Klarstellung nötig, in welchem Umfang diese Redundanzen aufgebaut werden sollen. Dabei ist zu berücksichtigten, dass eine »ausreichende Diversität durch Einsatz von Netz- und Systemkomponenten unterschiedlicher Hersteller«, wie weiter oben erwähnt, keine Strategie zur Schaffung von Redundanzen darstellt.

Die im Markt aktiven Netzbetreiber verfolgen bereits heute eine »Multi-Vendor«-Strategie. Allein der Fakt, dass unterschiedliche Netzbetreiber jeweils eigene Netze betreiben, ist ohnehin eine redundante Infrastruktur. Durch eine Fortschreibung dieser Betreiberstrategien kann auch im 5G-Kontext das Risiko einseitiger Abhängigkeiten vermieden werden.

- *»Bei der Umsetzung der Sicherheitsanforderungen sind nationale Sicherheitsbestimmungen sowie Bestimmungen zum Fernmeldegeheimnis und zum Datenschutz einzuhalten.«*

Die Vertrauenswürdigkeit eines Lieferanten dürfte sich primär an der Qualität einer transparenten und offenen Informationspolitik festmachen, die ein Lieferant bzgl. der Umsetzung der genannten Bestimmungen und Gesetze an den Tag legt sowie entsprechender Erkenntnisse und Erfahrungen aus der Vergangenheit.