Stellungnahme

BNetzA Entwurf (Stand 9. Oktober 2019)

zu Anlage 2 „Zusätzliche Sicherheitsanforderungen für öffentliche TK-Netze und -Dienste mit erhöhtem Gefährdungspotenzial“

zum

Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 TKG

(Anlage 2 zum Entwurf des erweiterten Sicherheitskatalogs zu §109 TKG**)**

Bundesverband der Deutschen Industrie e.V.

Stand: 12. November 2019

Inhaltsverzeichnis

Executive Summary

Für die deutsche Industrie ist ein leistungsfähiges, sicheres, souveränes, vertrauenswürdiges und verlässliches 5G-Netz von zentraler Bedeutung, um die Wettbewerbsfähigkeit der Industrie am Standort Deutschland nachhaltig zu stärken. 5G ist die Voraussetzung für die Implementierung zahlreicher neuer Anwendungen: Von Operationen per Telemedizin bis hin zu effizienteren Produktionsprozessen in Fabriken mittels Echtzeitanalyse von Daten.

Deutschland ist bei der digitalen Transformation auf technische Lösungen sowohl nationaler als auch internationaler Unternehmen angewiesen. Eine systematische Ausgrenzung von nicht-europäischen Anbietern beim Aufbau digitaler Infrastrukturen, bei Endgeräten sowie Dienstleistungen wäre daher weder technologisch, wirtschaftlich noch zeitlich zielführend. Digitale Souveränität darf nicht mit digitaler Autarkie verwechselt werden. Es ist vielmehr essenziell:

1. Sicherheitsanforderungen harmonisiert mit existierenden Regelungen und europaweit einheitlich auf Basis europäischer Werte und Anforderungen an die Integrität und Vertraulichkeit von Daten sowie die Verfügbarkeit von Netzen und Diensten zu erarbeiten und

2. die Einhaltung von Sicherheitsanforderungen selbstständig und kontinuierlich bewerten zu können.

Sicherheit hat oberste Priorität und muss sowohl auf europäischer als auch auf nationaler Ebene gedacht werden. Für alle Hersteller, unabhängig von Produkten, Angeboten und Herkunft, müssen europaweit die gleichen produkt- und angebotsspezifischen Prüfkriterien, Regeln und Verfahren gelten. **Ein *lex specialis* für einzelne Anbieter darf es nicht geben! Der BDI begrüßt daher ausdrücklich, den von der Bundesnetzagentur gewählten herstellerunabhängigen Ansatz. Die Gewährleistung von resilienten Produkten, Netzen und Dienstleistungen muss durch alle Hersteller, Lieferanten und Anbieter gleichermaßen sichergestellt werden.** 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. Daher bedarf es einer zusätzlichen adäquaten Regelung an anderer Stelle.

Mit Blick auf den von der BNetzA am 15. Oktober 2019 vorgestellten Anhang 2 „Zusätzliche Sicherheitsanforderungen für öffentliche TK-Netze und -Dienste mit erhöhtem Gefährdungspotenzial“ spricht sich die deutsche Industrie für folgende Anpassungen aus:

- Vertrauenswürdigkeitserklärung nicht wie aktuell geplant einführen, sondern wenn, dann nur mit einem rechtssicheren und durchsetzbaren

Haftungs- und Sanktionsregime: Statt einer wirkungslosen und bürokratischen Vertrauenswürdigkeitserklärung muss vertraglich die Einhaltung europäischer Sicherheitsanforderungen vereinbart werden. Dazu ist ein entsprechender regulatorischer Anker notwendig, der auch ein rechtssicheres und durchsetzbares Haftungs- und Sanktionsregime gegenüber den Herstellern beinhaltet adressiert und auch entsprechende Bedingungen (u.a. zertifizierte Typprüfungen und Haftungserfordernis) definiert. Dadurch kann die noch offene Fragestellung beantwortet werden, was geschehen soll, wenn ein Lieferant seine Vertrauenswürdigkeit einbüßt, obgleich bereits seine Technik Bestandteil der Infrastruktur ist. Zudem sollte die Einhaltung der in der Vertrauenswürdigkeitserklärung durch den Hersteller gemachten Angaben (zu mindestens in Teilen) durch staatliche Stellen überprüft werden.

- **Sicherheitsschemata nach dem EU Cybersecurity Act rasch für 5G-Netzwerkkomponenten entwickeln**: Dieses sollte neben technischen Anforderungen an das Produkt und dessen Lifecycle Prozess auch Kriterien zum Umgang mit Regulierungen im Heimatland des Herstellers in die Betrachtung und Überprüfung einbeziehen.

- **Zertifizierung**: Die Zertifizierung von Produkten, Prozessen und Dienstleistungen durch eine unabhängige dritte Stelle sollte auf Basis europaweit einheitlicher Sicherheitsanforderungen auch im Bereich kritischen TK-Infrastruktur (Netze und Dienste) zum Einsatz kommen. Die Bundesregierung und die BNetzA müssen sicherstellen, dass die Prüfung und Zertifizierung von kritischen Komponenten nicht deren Einsatz im Netz verzögern darf. Hierfür bedarf es ausreichend personeller Ressourcen sowie einer Zertifizierung von Prozessen zur sicheren Einbringung von Komponenten.

- **Sicherheitsanforderungen im laufenden Betrieb**: Es gilt zu konkretisieren, welche besonderen Merkmale eine MI (Monitoring Infrastruktur) haben muss und wie diese umgesetzt werden soll. Zudem muss sichergestellt sein, dass im Rahmen eines Monitorings keine staatlichen Aufgaben an die Betreiber delegiert werden.

- **Diversität:** Die Einführung einer verpflichtenden Multi-Vendor-Strategie begrüßt die deutsche Industrie ausdrücklich. Eine Maximalquoten für Komponente eines einzelnen Herstellers erscheint hingegen willkürlich und zur Stärkung der Cyberresilienz des 5G-Netzes nicht notwendig.

Die Wahrung der Integrität von Telekommunikationsnetzen sowie auch der darin verbauten Produkte sind von herausragender Bedeutung. Daher werden die von der BNetzA vorgeschlagenen Maßnahmen entlang des gesamten Produktlebenszyklusses begrüßt.

Maßnahmen zur Erhöhung der Sicherheit in Telekommunikationsnetzen sollten mindestens auf europäischer Ebene eingeführt werden. Nationale Alleingänge schwächen die wirtschaftliche Entwicklung und behindern die Innovationsfähigkeit. Wichtig ist zudem:

- **Gleiche Kriterien für alle Hersteller einführen**: Für alle Hersteller müssen idealerweise europaweit die gleichen produkt- und angebotsspezifischen Prüfkriterien, Regeln und Verfahren gelten. Falls ein Verdacht auf Spionage, Manipulation, o.ä. besteht, müssen die Vorwürfe eingehend geprüft werden. Fakt ist: Rechtstaatliche Verfahren bedürfen „harter Fakten“. Dies umfasst technologische, nachrichtendienstliche, wirtschaftliche und juristische Erkenntnisse.

Anmerkungen zur Anlage 2 des Entwurfs der Bundesnetzagentur für „Zusätzliche Sicherheitsanforderungen für öffentliche Telekommunikationsdienste mit erhöhtem Gefährdungspotenzial“

Die Sicherheit von Telekommunikationsdaten, die Wahrung des Fernmeldegeheimnisses sowie die Gewährleistung der Verfügbarkeit von Telekommunikationsdiensten müssen mit Blick auf das 5G-Netz höchste Priorität genießen. Daher begrüßt der BDI jede Maßnahme seitens der Behörden, die dafür geeignet ist, die Sicherheit von Telekommunikationsnetzen und -diensten nachhaltig zu stärken. Hierbei sollten jedoch im Sinne der stärkeren Etablierung des Europäischen (Digitalen) Binnenmarktes und der Entwicklung grenzüberschreitender 5G-basierter Anwendungen zunehmend auf europäische, anstatt nationaler Ansätze abgezielt werden. Konkret heißt das: Statt einer deutschen Vertrauenswürdigkeitserklärung braucht es einen europaweit verbindlich geltenden Cybersecurity Scheme für 5G-Netzwerkkomponenten auf Basis des EU Cybersecurity Acts und abgestimmt mit bereits existierenden Regelungen. Nur so kann die Diffusion von europäischen Cybersicherheitsanforderungen global skalieren.

Im Einzelnen

Zu 1. Anwendungsbereich

Für die deutsche Industrie ist ein leistungsfähiges, sicheres, souveränes, vertrauenswürdiges und verlässliches 5G-Netz von zentraler Bedeutung, um die Wettbewerbsfähigkeit der Industrie am Standort Deutschland nachhaltig zu stärken. 5G ist die Voraussetzung für die Implementierung zahlreicher neuer Anwendungen von Operationen per Telemedizin bis hin zu effizienteren Produktionsprozessen in Fabriken. Gleichzeitig bedarf es eines zügigen Aufbaus der 5G-Netzwerkinfrastruktur.

Angesichts der potenziellen Anwendungsfelder, die sich aus dem Ausbau des 5G-Netzes für die deutsche Industrie ergeben, ist die gegenwärtige Fokussierung des Anwendungsbereiches auf Betreiber von öffentlichen Telekommunikationsnetzen und Anbietern von öffentlichen Telekommunikationsdiensten mit erhöhtem Gefährdungspotenzial nachvollziehbar. Gleichwohl muss absehbar sichergestellt werden, dass sog. 5G-Campusnetze, v.a. solche, die von KRITIS-Unternehmen genutzt werden sollen, grundsätzlich die gleichen Sicherheitsanforderungen erfüllen müssen, wie öffentliche 5G-Netze.

Zu 2. Zertifizierung von kritischen Kernkomponenten

Die Zertifizierung von Produkten, Prozessen und Dienstleistungen durch eine unabhängige dritte Stelle ist ein geübter und zielführender Ansatz, um die Sicherheit von kritischen Infrastrukturen basierend auf einer Prüfung der eingesetzten Komponenten sowie der Produktions- und Implementierungsprozesse dieser Komponenten durch einen unabhängigen Dritten zu gewährleisten.

Mit Blick auf Telekommunikationsnetze und -dienste sollte die Bundesregierung gemeinsam mit den zuständigen nachgeordneten Bundesbehörden die

Ausarbeitung von europaweit einheitlichen Sicherheitsanforderungen als Grundlage für die Zertifizierung von Komponenten und Prozessen forcieren. Der EU Cybersecurity Act bietet hierfür den geeigneten Rahmen. Daher sollte von der Ausarbeitung nationaler Technischer Richtlinien soweit als möglich Abstand genommen werden.

Die deutsche Industrie regt mit Blick auf die in Ziffer 2.2 eingeführte Definition von kritischen Komponenten die Präzisierung „Datenschutzverletzungen *mit und ohne Personenbezug* in erheblichem Ausmaß“ an. Da durch den neuen Mobilfunkstandard 5G insbesondere auch Anwendungen, die vordergründig auf der Analyse von hochgradig sensiblen nicht-personenbezogenen Daten basieren, ermöglicht werden, scheint diese Klarstellung nötig.

Die Bundesregierung und die BNetzA müssen sicherstellen, dass die Prüfung und Zertifizierung von kritischen Komponenten nicht deren Einsatz im Netz verzögern. Daher müssen jetzt rasch die für die Prüfung und Zertifizierung notwendigen personellen Ressourcen aufgebaut werden. Nur so kann sichergestellt werden, dass innovative, nach dem Stand der Technik sichere Technologie im deutschen Telekommunikationsnetz verbaut werden kann.

Zudem gilt es zu überlegen, wie sichergestellt werden kann, dass bei Bedarf (z.B. aufgrund der Identifikation von Schwachstellen in Komponenten) alternative Komponenten rasch eingebaut werden können, respektive eingesetzte Produkte zügig gepatcht/geupdatet werden können. Eine Möglichkeit könnte die Einführung eines Eilverfahrens bei der Prüfung und Zertifizierung von Komponenten bei hoher Kritikalität des Einsatzes einer neuen Komponente sein. Auch wäre es denkbar, dass – eine sich aus Sicherheitserwägungen ergebende besondere Dringlichkeit vorausgesetzt – eine Komponente direkt „unter Vorbehalt“ ins Netz eingebaut wird und erst im laufenden Betrieb geprüft und zertifiziert wird. Alternativ könnte die Zertifizierung eines Prozess zur sicheren Einbringung von Komponenten eine Option sein.

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 muss es sein, dass die eingebauten Komponenten jederzeit auf dem Stand der Technik sind und maximale Sicherheit garantieren. Zudem sollten Updates keine zwingende Rezertifizierung verursachen.

Bei der Erarbeitung der Liste der kritischen Funktionen und Komponenten (Ziffer 2.3) bedarf es einer verpflichtenden öffentlichen Konsultation mit Herstellern, Betreibern von TK-Netzen und -Diensten sowie deren jeweiliger Verbände. Zudem sollte die so eingebrachte Expertise der Betreiber von TK-Netzen und -Diensten sowie der Hersteller entsprechender Komponenten auch durch staatliche Stellen bei der Erarbeitung der Liste der kritischen Funktionen und Komponenten berücksichtigt werden.

Um eine rasche Umsetzung der Sicherheitsanforderungen gewährleisten zu können, spricht sich die deutsche Industrie für eine schnellstmögliche Veröffentlichung der Liste der kritischen Funktionen und Komponenten aus. Eine Veröffentlichung vor dem 1. Januar 2020 wäre wünschenswert, um alsbald Planungssicherheit zu haben. Dies ist umso bedeutender, als dass es rasch Investitionssicherheit für im Ausbau befindliche TK-Netze geben sollte.

Der Entwurf sieht vor, dass vor dem 01.01.2021 gelistete kritische Komponenten ohne Einschränkung nur bis zum 31.12.2025 eingesetzt werden dürfen. Für die weitere Nutzung ab dem 01.01.2026 bedarf es hingegen eines gültigen Zertifikats, andernfalls ist die Weiternutzung untersagt.

Die deutsche Industrie fordert den Gesetzgeber auf, rasch die gesetzlichen sowie die anwendungspraktischen Grundlagen zu schaffen, damit Hersteller und Lieferant dieser Komponente frühzeitig den Zertifizierungsprozess analog zu neuen Komponenten einleiten können. 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.

Zu 3. Vertrauenswürdigkeit von Herstellern und Lieferanten

Für die deutsche Industrie ist ein leistungsfähiges, sicheres, souveränes, vertrauenswürdiges und verlässliches 5G-Netz von zentraler Bedeutung, um die Wettbewerbsfähigkeit der Industrie am Standort Deutschland nachhaltig zu stärken. Es stellt sich jedoch die Frage, ob dieses Ziel mit dem Instrument der Vertrauenswürdigkeitserklärung nachhaltig erreicht werden kann. So sind die genannten zehn Anforderungen an vertrauenswürdige Hersteller, wie beispielsweise die Pflicht, Schwachstellen sofort zu melden und mit einem Lösungsvorschlag zu liefern sowie die Bereitschaft der Hersteller zur Durchführung einer Sicherheitsüberprüfung ihrer Produkte, sinnvolle Schritte. Es bleibt jedoch zu klären, welchen Mehrwert für Unternehmen und der Allgemeinheit eine gesonderte Vertrauenswürdigkeitserklärung gegenüber der Aufnahme dieser Anforderungen in den Vertrag zwischen Hersteller und Betreiber haben wird.

Solch eine Vertrauenswürdigkeitserklärung hätte nur dann einen Mehrwert, wenn die BNetzA gemeinsam mit dem BSI sowie den deutschen Nachrichtendiensten die Einhaltung der darin zugesicherten Anforderungen überprüfen würden und bei Nichteinhaltung entsprechende Maßnahmen einleiten könnten. Dazu ist ein entsprechender regulatorischer Anker notwendig, der auch ein rechtssicheres und durchsetzbares Haftungs- und Sanktionsregime gegenüber den Herstellern beinhaltet und auch entsprechende Bedingungen (u.a. zertifizierte Typprüfungen, Einhaltung von (europäischen) Cybersicherheitsschemes) definiert. Dadurch kann die noch offene Fragestellung beantwortet werden, was geschehen soll, wenn ein Lieferant seine Vertrauenswürdigkeit einbüßt, obgleich bereits seine Technik Bestandteil der Infrastruktur ist. Nur mittels eines eindeutigen Haftungs- und Sanktionsregimes bei Nichteinhaltung der in der Vertrauenswürdigkeitserklärung gemachten Zusagen wird der Sicherheitskatalog seine Wirkung entfalten

können. Es ist dabei von zentraler Bedeutung, dass nicht der TK-Netz- und Dienste-Betreiber alleinig die Vertrauenswürdigkeit überprüfen muss. Vielmehr sollten TK-Betreiber und staatliche Stellen die Einhaltung mindestens gemeinsam vornehmen: Der Betreiber könnte die Analyse der technischen Sicherheitskriterien sowie der Anforderungen an die Kooperation mit dem Hersteller prüfen, während auf Basis nachrichtendienstlicher und politischer Erkenntnisse staatliche Stellen die allgemeine (geopolitisch und rechtliche) Vertrauenswürdigkeit bewerten würden.

Aus Sicht der deutschen Industrie würde die von der Bundesregierung im Rahmen des veröffentlichten Referentenentwurfs zum IT-Sicherheitsgesetz 2.0 sowie jetzt erneut von der Bundesnetzagentur vorgeschlagene Vertrauenswürdigkeitserklärung in ihrer aktuellen Form vielmehr (1) unkalkulierbare Folgen für Unternehmen haben und gleichzeitig (2) wahrscheinlich folgenlos für internationale Zulieferer bleiben.

1. Im schlimmsten Fall könnte eine Vertrauenswürdigkeitserklärung, ohne zur Stärkung der Cyberresilienz beizutragen, die Wettbewerbsfähigkeit der deutschen Industrie schwächen. Die Vertrauenswürdigkeitserklärung wird zu hohen Erfüllungsaufwendungen bei deutschen Unternehmen führen, da Unternehmen verpflichtet werden, entlang der gesamten, häufig hochkomplexen Wertschöpfungskette von allen Zulieferern eine Vertrauenswürdigkeitserklärung einzufordern. Es muss geklärt werden, wer die Richtigkeit der in der Vertrauenswürdigkeitserklärung gemachten Angaben zu prüfen hat und wie eine Nichteinhaltung der entsprechenden Zusicherungen aus der Vertrauenswürdigkeitserklärung mit Sanktionen bestraft werden können.

2. Zum anderen werden sich internationale Zulieferer in einer Abwägung zwischen der Einhaltung gesetzlicher Vorgaben in ihrem Heimatmarkt oder der Vertrauenswürdigkeitserklärung gegenüber ihrem deutschen Handelspartner, stets für eine Rechtstreue gegenüber ihrer nationalen Regierung entscheiden. Es stellt sich die Frage, ob solch eine Vertrauenswürdigkeitserklärung im Endeffekt lediglich zu einer „Scheinsicherheit“ beiträgt. Zu klären ist zudem, wie die Versorgung mit bestimmten kritischen Komponenten sichergestellt werden wird, sofern die potenziellen Anbieter aus Drittstaaten eine deutsche Vertrauenswürdigkeitserklärung mit Blick auf die Gesetzeslage auf ihrem Heimatmarkt nicht unterzeichnen können (siehe Punkte 3 und 4 in Ziffer 3) oder widerrufen müssen (siehe Punkt 5 in Ziffer 3).

Neben einer rechtlichen Verankerung einer klaren Verantwortungszuweisung im nationalen Recht, die Grundvoraussetzung für die Wirksamkeit einer Vertrauenswürdigkeitserklärung wäre, spricht sich die deutsche Industrie für die rasche Entwicklung eines Sicherheitsschemas für 5G-Netzwerkkomponenten auf Basis des EU Cybersecurity Acts aus. Betreiber von TK-Netzen und -Diensten könnten dann in Verträgen mit Herstellern und Lieferanten von Komponenten die Einhaltung der im Scheme geforderten und durch eine Zertifizierung bestätigten Anforderungen verlangen. Damit TK-Netzbetreiber die Einhaltung des Schemes wirksam einfordern können, müsste es als

verpflichtende Anforderung eingeführt werden. Ein entsprechender Scheme sollte sowohl die Einhaltung bestimmter technischer Sicherheitskriterien (u.a. als auch die Überprüfung von regulatorischen Vorgaben, die der Hersteller/Lieferant im Heimatland erfüllen muss, beinhalten. Nur eine ganzheitliche Betrachtung von technischen und regulatorischen Sicherheitsanforderungen wird langfristig die Integrität, Verfügbarkeit und Vertrauenswürdigkeit von Telekommunikationsnetzen und -diensten sicherstellen.

Sollten die regulatorischen Anforderungen eines Staates als unvereinbar mit europäischen Vorgaben gelten oder es geopolitische Entwicklungen geben, die die Vertrauenswürdigkeit eines Herstellers einschränken, so sollte nicht der einzelne Betreiber dies feststellen müssen. Vielmehr sollte dies auf Basis vorab klar definierter Kriterien durch staatliche Stellen (mind. Kooperation von BSI, BNetzA und Nachrichtendiensten) in Deutschland oder am besten in Europa erfolgen. Dies würde den Erfüllungsaufwand, der sich aus der Implementierung von Anhang 2 für die Betreiber von TK-Netzen und -Diensten ergibt, signifikant reduzieren und gleichzeitig das Instrument der Vertrauenswürdigkeit in seiner Wirksamkeit erheblich stärken. Bei Nicht-Einhaltung der in der Vertrauenswürdigkeitserklärung gemachten Zusagen, müssten staatliche Stellen das betreffende Unternehmen mit (empfindlichen) Sanktionen belegen können.

Zu 4. Produktintegrität

Aus Sicht der deutschen Industrie ist die Wahrung der Integrität von Telekommunikationsnetzen sowie der darin verbauten Produkte von herausragender Bedeutung. Daher werden die von der BNetzA vorgeschlagenen Maßnahmen entlang des gesamten Produktlebenszyklusses begrüßt. Um die Umsetzbarkeit der in Kapitel 4 genannten Anforderungen gewährleisten zu können, empfiehlt der BDI die Berücksichtigung der folgenden Punkte:

- **Abnahme**: Inhalt und Form der Abnahmeprüfungen sollten mit den Prüfungsinhalten zur Zertifizierung abgestimmt sein, damit nur die Punkte zur Abnahme im Fokus stehen, die nicht bereits überprüft wurden.

- **Wirkbetrieb**: Zyklus, Inhalt und Form der regelmäßigen Sicherheitsüberprüfungen sind festzulegen, idealerweise mit längeren Intervallen für kritische Kernkomponenten im Vergleich zu besonders kritischen Kernkomponenten. Es kann sinnvoll sein, sich an die Release-Zyklen der Hersteller anzupassen.

Zu 5. Sicherheitsanforderungen im laufenden Betrieb

Wir begrüßen die nach Stand-der-Technik geforderten Monitoring-Funktionen (MI) der Netzverkehre unter Ziffer 5. Allerdings dürften es die gesetzlichen Vorgaben zum Schutz des Fernmeldegeheimnisses jedoch 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.

Zudem ist zu konkretisieren, welche besonderen Merkmale eine MI (Monitoring Infrastruktur) haben muss und wie diese umgesetzt werden soll.

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

Zu 6. Eingewiesenes Fachpersonal

Gut geschultes Personal ist eine der elementaren Grundvoraussetzungen, um die nunmehr definierten Sicherheitsanforderungen umzusetzen. Bereits heute investieren Betreiber von Telekommunikationsnetzen und -diensten viel in die Aus- und Weiterbildung ihrer Mitarbeiterinnen und Mitarbeiter. Dies ist umso bedeutender, als dass in vielen Fällen der Mensch eines der größten Sicherheitsrisiken darstellt. Auch weiterhin werden die verpflichteten Unternehmen in Fortbildungsmaßnahmen investieren, um Ihren Mitarbeiterinnen und Mitarbeitern Wissen auf dem Stand der Technik zu ermöglichen.

Die deutsche Industrie sieht es jedoch als notwendig an, dass im Rahmen des Anhangs 2 Ziffer 6 klarer spezifiziert wird, was konkret unter „sicherheitsrelevante Aufgaben“ fällt.

Zudem sollte genauer spezifiziert werden, welche Sanktionen bei Nichteinhaltung der Anforderungen an geschultes Fachpersonal dem pflichtigen Unternehmen drohen.

Zu 7. Redundanzen

Das Vorhalten redundanter Netzinfrastrukturen ist aus Nutzersicht ein wichtiger Beitrag, um die Verfügbarkeit von Telekommunikationsnetzen und -dienstleistungen sicherzustellen. Gleichzeitig ist zu beachten, dass Redundanzen grundsätzlich zu höheren Ausbau- und Wartungskosten führen, die wiederum Auswirkungen auf die Preise der angebotenen Telekommunikationsdienste haben werden.

Zu 8. Diversität

Grundsätzlich kann eine Multi-Vendor-Strategie das Sicherheitsrisiko minimieren. Es ist allerdings zu berücksichtigen, dass eine Mehr-Lieferanten-/ Herstellerstrategie die Komplexität erhöht und auch zu zusätzlichen Schwachstellen führen kann. So muss beispielsweise die Kompatibilität und Interoperabilität zwischen den Produkten unterschiedlicher Hersteller sichergestellt werden. Eine Entscheidung über den Einsatz von einem oder mehreren Herstellern zur Realisierung kritischer Netzfunktionen bedarf einer detaillierten Abwägung von funktionalen, betrieblichen und sicherheitstechnischen Aspekten.

Der nunmehr vorgeschlagene Grenzwert von maximal zwei Drittel, die ein Anbieter eines Telekommunikationsnetzes und -dienstes von ein und demselben Hersteller beziehen darf, scheint hingegen willkürlich und trifft nicht die Bedürfnisse einer funktionalen Netzarchitekturplanung. Diese Aufteilung sollte ein Richtwert sein bzw. empfehlenden Charakter haben. Um

Monokulturen grundsätzlich zu vermeiden ist die Festlegung eines Prozentanteils überdies entbehrlich. Im weiteren Diskurs ist auch die etwaige Idee einer paritätischen Verteilung entlang der Hersteller im Sinne einer sicheren Infrastruktur nicht förderlich, da eine daraus resultierende Quotenbildung nicht zu mehr Sicherheit führt, sondern die Gefahr einer marktanteilsbedingten Sorglosigkeit steigt. Zudem sollte berücksichtigt werden, dass im Zweifel eine kompromittierte Komponente ausreichen würde, um die Sicherheit von TK-Netzen und -Diensten nachhaltig zu schwächen.

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.

Über den BDI

Der BDI transportiert die Interessen der deutschen Industrie an die politisch Verantwortlichen. Damit unterstützt er die Unternehmen im globalen Wettbewerb. Er verfügt über ein weit verzweigtes Netzwerk in Deutschland und Europa, auf allen wichtigen Märkten und in internationalen Organisationen. Der BDI sorgt für die politische Flankierung internationaler

Markterschließung. Und er bietet Informationen und wirtschaftspolitische Beratung für alle industrierelevanten Themen. Der BDI ist die Spitzenorganisation der deutschen Industrie und der industrienahen Dienstleister. Er spricht für 39 Branchenverbände und mehr als 100.000 Unternehmen mit rund 8 Mio. Beschäftigten. Die Mitgliedschaft ist freiwillig. 15 Landesvertretungen vertreten die Interessen der Wirtschaft auf regionaler Ebene.

Impressum

Bundesverband der Deutschen Industrie e.V. (BDI)
Breite Straße 29, 10178 Berlin
www.bdi.eu
T: +49 30 2028-0

Ansprechpartner

Steven Heckler
T: +49 (0)30 2028-1523
S.Heckler@bdi.eu

Carolin Proft
T: +49 (0)30 2028-1529
C.Proft@bdi.eu

BDI Dokumentennummer: D 1106