ZTE Austria Stellungnahme zu dem

Entwurf einer Verordnung der Rundfunk und Telekom Regulierungs- GmbH über Verpflichtungen von Betreibern elektronischer Kommunikationsnetze und Anbietern elektronischer Kommunikationsdienste im Zusammenhang mit Mindestsicherheitsmaßnahmen unter Berücksichtigung von 5G-Netzen sowie mit Informationspflichten bei Sicherheitsvorfällen (Telekom- Netzsicherheitsverordnung 2020 – TK-NSiV 2020)

Als österreichisches Unternehmen und betroffener Marktteilnehmer möchte ZTE Austria im Rahmen der bis zum 5. Juni 2020 laufenden Konsultation der RTR-GmbH zur TK-NSiV 2020 folgendermaßen Stellung nehmen.

ZTE Austria GmbH, Tochter der ZTE Corporation, einem international führenden Anbieter von Lösungen für die Telekommunikationsbranche sowie für Unternehmens- und Privatkunden im Bereich mobiles Internet, begrüßt das Vorhaben der österreichischen Bundesregierung, die 5G-Vorreiterrolle weiter auszubauen und Anwendungen für neue, sowie Integration in neue Technologien voranzutreiben. Damit müssen auch die notwendigen Sicherheitsvorkehrungen für eine nachhaltige und leistungsfähige Infrastruktur einhergehen, diese sollten auf Basis anerkannter technologischer Grundlagen beurteilt und nicht mit handelspolitischen Zwecken vermengt werden. Im Zuge dessen dürfen die Bestimmungen den 5G-Ausbau und die ambitionierten Ziele Österreichs nicht konterkarieren, daher müssen diese Stränge immer gemeinsam betrachtet und durchdacht werden.

ZTE Austria begrüßt den Zugang der Regulierungsbehörde die TK-NSiV auf sachlich und technologisch fundierten Argumenten fußen zu lassen. Forderungen nach nicht gerechtfertigten Ausschlüssen von Marktteilnehmern auf Grund von etwaigen Eigeninteressen derer Konkurrenten unter Vorwand von politisch induzierten Risiken sollten hierbei keine Rolle spielen. Eine ausgewogene Markt Balance findet sich sinngemäß als wichtiges Element auch in der EU-Toolbox wieder.

Technologische Entwicklung, Wettbewerb um die fortschrittlichste Infrastruktur und damit zusammenhängende Produkte finden international statt, daher ist es wichtig in Europa ein plain level playing field mit einheitlichen Standards sowie Zeitlinien und EU-weit gültigen Vorgaben umzusetzen, um den Markt und seine Akteure wettbewerbsfähig zu halten und raschen Fortschritt und Weiterentwicklung zu ermöglichen.

Daher ist es essentiell, auch für die Umsetzung in Österreich einen engen Austausch mit den anderen Mitgliedstaaten und den EU-Institutionen zu pflegen, um Partikularlösungen und widersprüchliche Systeme in Europa zu vermeiden.

ZTE engagiert sich seit Beginn der Diskussionen zur Gestaltung der Rahmenbedingungen für sichere 5G Netze auf EU-Ebene, in mehreren Mitgliedstaaten wie in Österreich und steht weiterhin jederzeit für Gespräche zur Verfügung und bietet ihre Expertise als internationaler Technologievorreiter an.

Vor kurzem erhielt die ZTE Corporation von der British Standards Institution die ISO/IEC 27701:2019 Zertifizierung für die Bereitstellung von 5G-Diensten. Diese Norm umfasst einen ergänzenden Teilbereich der in der TK-NSiV 2020 zitierten ISO 27001, nach der die ZTE Corporation ebenfalls zertifiziert ist. Das Zertifikat der ISO 2701 bezieht sich auf die Bereitstellung von Forschung und Entwicklung sowie Wartungsdiensten von 5G NR und UME-Systemen. Es bestätigt, dass die Datenschutzvorgaben eingehalten werden und dass die 5G-Dienste von ZTE den internationalen Informationssicherheitsstandards in vollem Umfang entsprechen.

Zu den einzelnen Bestimmungen:

Einleitung und § 1 Zweck und Anwendungsbereich

Keine Anmerkungen.

§ 2 Begriffsbestimmungen

Original Text: § 2 Z 9 5G-Netz: Mobilfunknetz der fünften Generation, dessen einschlägige Netzinfrastrukturelemente auf weltweit vereinbarten technischen Normen für die Mobilfunk- und Drahtloskommunikation beruhen und fortgeschrittene Leistungsmerkmale wie sehr hohe Datengeschwindigkeit und -kapazität, Kommunikation mit niedriger Latenzzeit, ultra-hohe Zuverlässigkeit oder Unterstützung einer großen Zahl verbundener Geräte aufweisen. Die Netzinfrastrukturelemente eines 5G-Netzes können auch vorhandene Netzbestandteile umfassen, denen frühere Generationen mobiler und drahtloser Kommunikationstechnik (4G oder 3G) zugrunde liegen.
Kommentar: Der Begriff Netzwerkinfrastrukturelemente ist in diesem Kontext nicht ausreichend detailliert, ein Verweis auf „Anhang 2 Liste von Funktionen der Komponenten von 5G-Netzen iSd § 6 Abs. 4“ wäre angebracht, des Weiteren ist anzumerken, dass ein *nicht abschließender* Verweis auf frühere Generationen mobiler Kommunikationstechnik vor 4G entfernt werden sollte.
Text Vorschlag: § 2 Z 9 5G-Netz: Mobilfunknetz der fünften Generation, dessen einschlägige Netzinfrastrukturelemente *(Verweis auf Anhang 2 „ Liste von Funktionen der Komponenten von 5G-Netzen iSd § 6 Abs. 4“)* auf weltweit vereinbarten technischen Normen für die Mobilfunk- und Drahtloskommunikation beruhen und fortgeschrittene Leistungsmerkmale wie sehr hohe Datengeschwindigkeit und -kapazität, Kommunikation mit niedriger Latenzzeit, ultra-hohe Zuverlässigkeit oder Unterstützung einer großen Zahl verbundener Geräte aufweisen. Die Netzinfrastrukturelemente eines 5G-Netzes können auch vorhandene Netzbestandteile umfassen, denen frühere Generationen mobiler und drahtloser Kommunikationstechnik *(4G oder 3G)* zugrunde liegen.

§ 3 Informationspflichten

Original Text: § 3. (1) Bei Sicherheitsvorfällen, die zu beträchtlichen Auswirkungen auf die Sicherheit von elektronischen Kommunikationsnetzen oder -diensten geführt haben oder noch führen, haben Betreiber elektronischer Kommunikationsnetze und Anbieter elektronischer Kommunikationsdienste die Regulierungsbehörde unverzüglich ab Kenntnis des Vorfalls hiervon unter Übermittlung der im Hinblick auf die Datenlage verfügbaren Angaben gemäß Z 1 bis 12 in einem von der Regulierungsbehörde vorgegebenen elektronischen Format zu informieren („Erstmeldung“). Darüber hinaus sind der Regulierungsbehörde in dem von ihr vorgegebenen elektronischen Format binnen maximal 24 Stunden ab Wiederherstellung der betroffenen Dienste folgende Informationen zu übermitteln („Folgemeldung“):
Kommentar: 1. Verweis beinhaltet nur Z 1 bis 12 statt 1 bis 14
Text Vorschlag: § 3. (1) Bei Sicherheitsvorfällen, die zu beträchtlichen Auswirkungen auf die Sicherheit von elektronischen Kommunikationsnetzen oder -diensten geführt haben oder noch führen, haben Betreiber elektronischer Kommunikationsnetze und Anbieter elektronischer Kommunikationsdienste die Regulierungsbehörde unverzüglich ab Kenntnis des Vorfalls hiervon unter Übermittlung der im Hinblick auf die Datenlage verfügbaren Angaben gemäß Z 1 bis *14* in einem von der Regulierungsbehörde vorgegebenen elektronischen Format) zu informieren („Erstmeldung“). Darüber hinaus sind der Regulierungsbehörde, in dem von ihr vorgegebenen elektronischen Format binnen maximal 24 Stunden ab Wiederherstellung der betroffenen Dienste folgende Informationen zu übermitteln („Folgemeldung“):

§ 4 Warnhinweis

Keine Anmerkungen.

§ 5 Mindestsicherheitsmaßnahmen

Keine Anmerkungen.

§ 6 Sicherheitsanforderungen an 5G-Netze

Original Text:

§ 6. (1) Zur Gewährleistung eines angemessenen Sicherheitsniveaus für 5G-Netze haben Betreiber derartiger Netze mit insgesamt mehr als 100 000 Teilnehmern in allen von ihnen betriebenen Mobilfunknetzen der Regulierungsbehörde das Bestehen eines Informationssicherheitsmanagementsystems gemäß einer diesbezüglich anerkannten Norm durch Vorlage entsprechender Auditberichte erstmals bis 31. Dezember 2021 und danach regelmäßig im Abstand von höchstens drei Jahren nachzuweisen. Die Festlegung und Umsetzung von allgemeinen und telekommunikationsspezifischen Informationssicherheitsmaßnahmen hat ebenfalls diesbezüglich anerkannten Normen zu entsprechen. Jede Nichtkonformität mit einer Anforderung aus diesen Normen ist jeweils zu begründen.

Kommentar:

1. Zur besseren Konkretisierung und als Verweis und Kontinuität zu §§ 1 bis § 5 wird empfohlen auch für §6 den Begriff des Diensteanbieters zu verwenden.
2. Die Beilage einer Liste anerkannter Zertifizierungsstellen wäre zu begrüßen
3. Zum voll-umfänglichen Verständnis wird eine Anpassung der Konformitätsanforderung empfohlen

Text Vorschlag:

§ 6. (1) Zur Gewährleistung eines angemessenen Sicherheitsniveaus für 5G-Netze haben Betreiber derartiger *Netze oder Diensteanbieter* mit insgesamt mehr als 100 000 Teilnehmern in allen von ihnen betriebenen Mobilfunknetzen der Regulierungsbehörde das Bestehen eines Informationssicherheitsmanagementsystems gemäß einer diesbezüglich anerkannten Norm durch Vorlage entsprechender Auditberichte *oder Zertifikate anerkannter Zertifizierungsstellen*, erstmals bis 31. Dezember 2021 und danach regelmäßig im Abstand von höchstens drei Jahren nachzuweisen. Die Festlegung und Umsetzung von allgemeinen und telekommunikationsspezifischen Informationssicherheitsmaßnahmen hat ebenfalls diesbezüglich anerkannten Normen zu entsprechen. Jede Nichtkonformität mit *einer Anforderungen* aus diesen Normen ist jeweils zu begründen.

Absatz 2:

Original Text:

§ 6. (2) Überdies haben die Betreiber von 5G-Netzen mit insgesamt mehr als 100 000 Teilnehmern in allen von ihnen betriebenen Mobilfunknetzen der Regulierungsbehörde die Erfüllung der in Anhang 1 angeführten Standards durch Vorlage einer Konformitätserklärung des Betreibers erstmals bis 30. Juni 2021 und danach regelmäßig im Abstand von höchstens drei Jahren nachzuweisen. Eine Nichtkonformität mit optionalen Bestimmungen der im Anhang angeführten Standards ist jeweils zu begründen.

Kommentar:

1. Zur besseren Konkretisierung und als Verweis und Kontinuität zu §§ 1 bis § 5 wird empfohlen auch für § 6 den Begriff des Diensteanbieters ebenfalls zu verwenden.
2. Es wird vorgeschlagen, den letzten Satz bez. Nichtkonformität zu löschen

Text Vorschlag:

§ 6. (2) Überdies haben die Betreiber von 5G-Netzen *und Diensteanbieter* mit insgesamt mehr als 100 000 Teilnehmern in allen von ihnen betriebenen Mobilfunknetzen der Regulierungsbehörde die Erfüllung der in Anhang 1 angeführten Standards durch Vorlage einer Konformitätserklärung des Betreibers erstmals bis 30. Juni 2021 und danach regelmäßig im Abstand von höchstens drei Jahren nachzuweisen. *Eine Nichtkonformität mit optionalen Bestimmungen der im Anhang angeführten Standards ist jeweils zu begründen.*

Absatz 3:

Original Text:

§ 6. (3) Darüber hinaus haben die Betreiber von 5G-Netzen mit insgesamt mehr als 100 000 Teilnehmern in allen von ihnen betriebenen Mobilfunknetzen die Erfüllung folgender Anforderungen auf Verlangen der Regulierungsbehörde nachzuweisen:

1. Betrieb von Network Operation Center (NOC) sowie Security Operation Center (SOC) in eigenen Räumlichkeiten innerhalb der Europäischen Union;
2. effektives Monitoring aller kritischen Netzkomponenten und sensibler Teile der 5G Netze durch NOC/SOC, um Anomalien zu entdecken und Bedrohungen zu identifizieren und zu verhindern;
3. Schutz des Management-Verkehrs von Kommunikationsnetzen oder -diensten, um nicht autorisierte Änderungen von Netz- oder Dienstkomponenten zu verhindern;
4. physischer Schutz von kritischen Netzkomponenten und sensiblen Teilen der 5GNetze mit risikobasiertem Ansatz für Multi-access Edge Computing (MEC) und Basisstationen;
5. Einschränkung des Zugriffs auf befähigtes und qualifiziertes Personal, das einer Sicherheitsüberprüfung unterzogen wurde; ein Zugang durch Dritte ist zu beschränken und zu überwachen;
6. Einsatz adäquater Werkzeuge und Prozesse zur Gewährleistung der Software-Integrität bei Software-Aktualisierung und Anwendung von Sicherheits-Patches, zuverlässige Identifikation und Nachvollziehbarkeit von Änderungen und Patch-Status;
7. Multi-Vendor-Strategie, die die technischen Beschränkungen und Interoperabilitätsanforderungen verschiedener Teile eines 5G-Netzes berücksichtigt.

Kommentar:

1. Zur besseren Konkretisierung und als Verweis und Kontinuität zu §§ 1 bis § 5 wird empfohlen auch für § 6 den Begriff des Diensteanbieters zu verwenden.
2. Für Z1 wird auf Grund des nicht eindeutigen Wortlautes vorgeschlagen, das Wort „eigene“ vor Räumlichkeiten zu streichen. Es muss möglich bleiben, spezialisierte Dienstleister mit der die Bereitstellung von NOC und SOC zu beauftragen. Alternativ dazu könnte in den EB die Klarstellung erfolgen, dass eine Auslagerung an Spezialisten rechtskonform ist.
3. Z7 verordnet den Nachweis einer Multi-Vendor-Strategie, welche die technischen Beschränkungen und Interoperabilitätsanforderungen verschiedener Teile eines 5G-Netzes berücksichtigen soll. Der aktuelle VO-Text ist nicht ausreichend klar und zu weitreichend formuliert. Betreiber von 5G-Netzen brauchen eine Strategie, diese verpflichtet unserer Ansicht nach grundsätzlich nicht zur Implementierung von Ausrüstung mehrerer Vendoren. Die EB sorgen in diesem Kontext eher für Verwirrung als für Klarheit. In der EU Toolbox zu 5G Cybersecurity von Netzwerken ist auf S. 18 angeführt, dass im Rahmen der Multi-Vendor Strategie auch eine adäquate Balance von Herstellern auf nationaler Ebene sicherzustellen ist. Eine Multi-Vendor Equipment-Implementierung bringt nicht zwingend höhere Netzsicherheit, führt aber ausnahmslos und völlig ungerechtfertigt zu deutlich höheren und überschießenden Kosten. Auch dazu enthält die EU Toolbox zu 5G Cybersecurity von Netzwerken auf S. 34 iZm SM05 Hinweise, dass im Rahmen der Multi-Vendor-Strategie mit sektor-spezifischen und darüber hinausgehenden höheren ökonomischen Auswirkungen für Operatoren, Hersteller sowie Gesamtwirtschaft und Gesellschaft zu rechnen sei.

Text Vorschlag:

§ 6. (3) Darüber hinaus haben die Betreiber von 5G-Netzen *und Diensteanbieter* mit insgesamt mehr als 100 000 Teilnehmern in allen von ihnen betriebenen Mobilfunknetzen die Erfüllung folgender Anforderungen auf Verlangen der Regulierungsbehörde nachzuweisen:

1. Betrieb von Network Operation Center (NOC) sowie Security Operation Center (SOC) in *eigenen* Räumlichkeiten innerhalb der Europäischen Union;
2. effektives Monitoring aller kritischen Netzkomponenten und sensibler Teile der 5G Netze durch NOC/SOC, um Anomalien zu entdecken und Bedrohungen zu identifizieren und zu verhindern;
3. Schutz des Management-Verkehrs von Kommunikationsnetzen oder -diensten, um nicht autorisierte Änderungen von Netz- oder Dienstkomponenten zu verhindern;

4. physischer Schutz von kritischen Netzkomponenten und sensiblen Teilen der 5GNetze mit risikobasiertem Ansatz für Multi-access Edge Computing (MEC) und Basisstationen;
5. Einschränkung des Zugriffs auf befähigtes und qualifiziertes Personal, das einer Sicherheitsüberprüfung unterzogen wurde; ein Zugang durch Dritte ist zu beschränken und zu überwachen;
6. Einsatz adäquater Werkzeuge und Prozesse zur Gewährleistung der Software-Integrität bei Software-Aktualisierung und Anwendung von Sicherheits-Patches, zuverlässige Identifikation und Nachvollziehbarkeit von Änderungen und Patch-Status;
7. Multi-Vendor-Strategie, die die technischen Beschränkungen und Interoperabilitätsanforderungen verschiedener Teile eines 5G-Netzes berücksichtigt.

Absatz 4:

Original Text:

§ 6. (4) Schließlich haben Betreiber von 5G-Netzen mit insgesamt mehr als 100 000 Teilnehmern in allen von ihnen betriebenen Mobilfunknetzen der Regulierungsbehörde halbjährlich jeweils mit Stand zum Ende des ersten und dritten Quartals bis 30. April und 31. Oktober des Jahres sowie auf begründetes Verlangen der Regulierungsbehörde eine Aufstellung von Funktionen und Herstellern der für den Betrieb des 5G-Netzes eingesetzten sicherheitsrelevanten Komponenten gemäß Anhang 2 sowie gegebenenfalls weiterer von ihnen verwendeter Komponenten zu übermitteln. Hierbei sind Funktionen und Hersteller in dem von der Regulierungsbehörde vorgeschriebenen elektronischen Format anzugeben. Die Regulierungsbehörde ist berechtigt, die ihr bekanntgegebenen Daten für die Dauer der Verwendung der Komponenten zu speichern und zu verarbeiten.

Kommentar:

1. Zur besseren Konkretisierung und als Verweis und Kontinuität zu §§ 1 bis § 5 wird empfohlen auch für §6 den Begriff des Diensteanbieters zu verwenden.
2. Unserem Verständnis nach umfasst der Anhang nicht nur die Liste der sicherheitsrelevanten Komponenten, mehr jedoch die Liste der 5G Netzkomponenten generell, aus diesem Grund ersuchen wir um Einschränkung des Anhangs 2 auf sicherheitsrelevante Komponenten.

Original Vorschlag:

§ 6. (4) Schließlich haben Betreiber von 5G-Netzen *sowie Diensteanbieter* mit insgesamt mehr als 100 000 Teilnehmern in allen von ihnen betriebenen Mobilfunknetzen der Regulierungsbehörde halbjährlich jeweils mit Stand zum Ende des ersten und dritten Quartals bis 30. April und 31. Oktober des Jahres sowie auf begründetes Verlangen der Regulierungsbehörde eine Aufstellung von Funktionen und Herstellern der für den Betrieb des 5G-Netzes eingesetzten sicherheitsrelevanten Komponenten gemäß Anhang 2 sowie gegebenenfalls weiterer von ihnen verwendeter Komponenten zu übermitteln. Hierbei sind Funktionen und Hersteller in dem von der Regulierungsbehörde vorgeschriebenen elektronischen Format anzugeben. Die Regulierungsbehörde ist berechtigt, die ihr bekanntgegebenen Daten für die Dauer der Verwendung der Komponenten zu speichern und zu verarbeiten.

EB zu §6

Original Text:

……haben sowie die Mitteilung der Europäischen Kommission COM(2020)50 vom 29.01.2020 an das Parlament, den Rat, den Wirtschafts- und Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: „Sichere 5G-Einführung in der EU – Umsetzung des EU-Instrumentariums“) sicherstellen sollen, dass erhöhten Sicherheitsrisiken, die mit dem Betrieb von 5GNetzen verbunden sind, angemessen begegnet werden kann.

Kommentar:

Das Einfügen von Link Verweisen für COM (2020)50 wie auch „Sichere 5G Einführung in der EU- …“ ist dem Verständnis und der der Lesbarkeit zuträglich

Text Vorschlag:

……haben sowie die Mitteilung der Europäischen Kommission COM(2020)50 *(VERWEIS LINK)* 29.01.2020 an das Parlament, den Rat, den Wirtschafts- und Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: „Sichere 5G-Einführung in der EU – Umsetzung des EU-Instrumentariums“) *(VERWEIS LINK)* sicherstellen sollen, dass erhöhten Sicherheitsrisiken, die mit dem Betrieb von 5GNetzen verbunden sind, angemessen begegnet werden kann.

Original Text:

Die Multi-Vendor-Strategie (Auswahlmöglichkeit eines Betreibers unter zumindest zwei Lieferanten für Netzinfrastrukturelemente eines 5G-Netzes gemäß § 2 Z 9) soll Abhängigkeiten von einem einzigen Lieferanten (oder Lieferanten mit ähnlichem Risikoprofil) vermeiden oder beschränken und Abhängigkeiten von Lieferanten, die als hohes Risiko angesehen werden, vermeiden.

Kommentar:

1. Die erläuternden Bemerkungen zu § 6 Abs. 3 Z 7 bedürfen einer Präzisierung und genauen Beschreibung. Eine potentielle Redundanz von einzelnen Netzinfrastrukturelementen durch zumindest einen weiteren Ausstatter führt zu erheblichen Kosten im Aufbau und in Folge auch im regulatorisch gewünschten Ausbau des 5G Netzes. Eine Verschlechterung der Bedingungen zum Ausbau des 5G Netzes halten wir für fahrlässig, da der Ausbau bereits sehr investitionsintensiv ist, gemäß Zielen der Bundesregierung raschestmöglich erfolgen soll und keine weiteren Hürden dabei aufgestellt werden sollten.
2. Wie oben in den Kommentaren zu § 6 Abs. 3 Z 7 sollte in den EB dazu klargestellt sein, dass das Bestehen einer Strategie, bei der zumindest zwei Vendoren bei der Planung im Evaluierungsprozess zum Aufbau eines 5G Netzes in Betracht gezogen werden, eine ausreichende und ökonomisch sinnvolle Maßnahme im Sinne der EU Toolbox darstellt, um langfristige Abhängigkeiten zu vermeiden.
3. Die generelle Berücksichtigung von Systemvendoren im Planungsprozess sowie auch deren getroffene *Sicherheitsmaßnahmen sollten aus* unserer Sicht die Grundlage einer sicherheitsrelevanten Multi-Vendor Einschätzung sein, nicht jedoch die Festlegung der Anzahl von Vendoren.

Text Vorschlag:

Die Multi-Vendor-Strategie *(Durchführung einer strategischen Bewertung eines Betreibers eines 5G Netzes hinsichtlich einer Auswahlmöglichkeit unter zumindest zwei Lieferanten für Netzinfrastrukturelemente eines 5G-Netzes gemäß § 2 Z 9)* soll Abhängigkeiten von einem einzigen Lieferanten (oder Lieferanten mit ähnlichem Risikoprofil) *aufzeigen* und Abhängigkeiten von Lieferanten, *die ein hohes Risiko bringen können*, *ersichtlich machen und nach Möglichkeit auf langfristige Sicht vermeiden.*

Anhang 1

Keine Anmerkungen.

Anhang 2

Vorschlag zur Einschränkung auf sicherheitsrelevante Netzkomponenten, s.o. Kommentare zu § 6 Abs. 4.