An die
Rundfunk und Telekom Regulierungs-GmbH
Mariahilfer Straße 77-79
1060 Wien

E-Mail: konsultationen@rtr.at

Wien, am 04. Juni 2020

ISPA STELLUNGNAHME ZUM 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)

Sehr geehrte Damen und Herren,

die ISPA erlaubt sich in Zusammenhang mit der öffentlichen Konsultation der RTR-GmbH zum 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) wie folgt Stellung zu nehmen:

Bei der Festlegung der Informationspflichten in § 3 sollte darauf geachtet werden, überschneidende Meldepflichten zu vermeiden. Außerdem erfordert die Definition von „beträchtlichen Auswirkungen“ in § 3 Abs. 2 einer näheren Klarstellung und sollte anstelle einer „unverzüglichen“ Meldung eine Frist zur Übermittlung der Erstmeldung von maximal 24 Stunden vorgesehen werden. Die ISPA weist zudem darauf hin, dass die Umsetzungsfrist der Mindestsicherheitsanforderungen in § 5 fehlt und ergänzt werden sollte. Hinsichtlich der Sicherheitsanforderungen an 5G-Netze in § 6 weist die ISPA darauf hin, dass die ausschließliche Bezugnahme auf „Teilnehmer“ zur Ermittlung des Schwellenwerts dem Grundgedanken der Verordnung widerspricht und daher zusätzlich eine neutralere Bezugsgröße verwendet werden sollte. Darüber hinaus sollten die als gleichwertig anerkannten Standards zum Nachweis eines Informationssicherheitsmanagementsystems weit ausgelegt werden und auch Selbstaudits zulassen. Die ISPA spricht sich zudem dafür aus, dass der Betrieb eines NOC/SOC nicht zwingend in „eigenen Räumlichkeiten“ zu erfolgen hat und fordert eine verfassungsgemäße Klarstellung des Erfordernisses einer Multi-Vendor Strategie.

ISPA – Internet Service Providers Austria
Währinger Straße 3/18, 1090 Wien, Austria
☎ +43 1 409 55 76
office@ispa.at
www.ispa.at

UniCredit Bank Austria AG
Konto-Nr.: 00660 491 705, **BLZ:** 12000
BIC: BKAUATWW
IBAN: AT59 1200 0006 6049 1705

UID-Nr.: ATU 54397807
ZVR-Zahl: 551223675

1) Überschneidende Meldepflichten sollten vermieden werden

In § 3 TK-NSiV 2020-E möchte die Regulierungsbehörde die Vorgehensweise bzw. Informationspflicht von Betreibern öffentlicher Kommunikationsnetze oder -dienste bei Sicherheitsverletzungen iSd § 16a Abs. 5 TKG näher festlegen. Wie bereits aus den EB zu § 1 hervorgeht, bedient sich der Gesetzgeber hierzu jedoch des Begriffs „Sicherheitsvorfall" anstelle von „Sicherheitsverletzung" um bereits Art 2 Z 42 der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (European Electronic Communications Code – EECC) zu entsprechen. Es ist unklar, ob sich durch diese weitergehende Formulierung als bisher auch zusätzliche überschneidende Meldepflichten ergeben. Da die Umsetzung des EECC im Rahmen der Novellierung des TKGs noch aussteht ist es noch nicht möglich auf etwaige Kollisionsregeln mit anderen Meldepflichten der Betreiber Bezug zu nehmen, wie diese beispielswiese bislang u.a. zum Teil in § 95a TKG enthalten sind.

Die ISPA ersucht daher um eine Klarstellung bereits in den EB der TK-NSiV 2020 wie sich die Informationspflichten nach § 3 zu anderen Meldepflichten verhalten. Dabei sollte darauf geachtet werden, dass Sicherheitsvorfälle wie etwa Datenlecks ausschließlich an die Datenschutzbehörde gemeldet werden müssen, und daher nicht in den Anwendungsbereich des § 3 TK-NSiV 2020-E fallen. Hierdurch sollen redundante doppelte Meldewege vermieden werden, speziell unter dem Gesichtspunkt der äußerst straffen Meldefristen, durch die bereits eine einzelne Meldung einen erheblichen Aufwand mit sich bringt. Ist die Datenschutzbehörde in Folge der Ansicht, es handle sich um einen Sicherheitsvorfall der auch über den datenschutzrechtlichen Aspekt hinaus Belang hat kann sie weiterhin die Regulierungsbehörde darüber informieren, sofern dies der Betreiber nicht ohnehin bereits getan hat (vgl. hierzu bislang § 95a Abs. 7 TKG).

2) Die Definition von „beträchtlichen Auswirkungen" in § 3 Abs. 2 bedarf einer näheren Klarstellung

In § 3 Abs. 2 TK-NSiV 2020-E führt der Verordnungsgeber detailreich aus, unter welchen Voraussetzungen mit beträchtlichen Auswirkungen auf die Sicherheit von elektronischen Kommunikationsnetzen oder -diensten zu rechnen ist und eine Informationspflicht daher ausgelöst wird.

Dabei ist es nach Ansicht der ISPA jedoch unverständlich, weshalb zum einen ein absoluter Wert der betroffenen Nutzer im Bundesgebiet je Dienstekategorie angeführt wird und zum anderen auf einen entsprechenden Prozentsatz der Gesamtzahl der Nutzer Bezug genommen wird. Diese Formulierung führt jedenfalls zu Unklarheit und potentiell zu einer Ungleichbehandlung der Betreiber.

Generell lässt der Wortlaut wonach die „Anzahl der betroffenen Teilnehmer der jeweiligen Dienstekategorie gemäß Abs. 1 Z 5 X % der Gesamtzahl der Nutzer des Dienstes im Bundesgebiet" übersteigen muss zwei unterschiedliche Interpretationen zu. Zum einen kann es so verstanden werden, dass es sich dabei um einen Prozentsatz aller Nutzerinnen und Nutzer dieser

Dienstekategorie (also etwa alle Festnetznutzer) auf dem Bundesgebiet handelt. Andererseits aber kann man es auch als einen Prozentsatz der dem jeweiligen Anbieter zuzurechnenden Teilnehmer im Bundesgebiet verstehen. Hierauf lassen etwa auch die EB zu Abs. 2 leg cit. schließen, wonach der Bezugspunkt die dem Anbieter des betroffenen Kommunikationsdienstes zuzurechnenden Teilnehmer sind.

Letztere Interpretation hätte aufgrund des relativen Werts der betroffenen Nutzer zur Folge, dass gerade bei kleinen Unternehmen bereits bei einer geringen absoluten Anzahl an betroffenen Nutzern entsprechende Informationspflichten ausgelöst werden würden während bei der selben Anzahl an betroffenen Nutzern eines großen Betreibers im gleichen Gebiet keine Informationspflicht ausgelöst wird. Das erscheint nach Ansicht der ISPA als unverhältnismäßige Ungleichbehandlung und sollte daher vermieden werden.

Sofern sich der entsprechende Prozentsatz jedoch auf sämtliche Nutzer der Dienstekategorie im Bundesgebiet bezieht, führt die Angabe eines Prozentsatzes von der Gesamtzahl samt absolutem Schwellenwert in diesem Zusammenhang lediglich zu Rechtsunsicherheit, da das Unternehmen in der Regel keine Kenntnis über die Gesamtzahl an Nutzern im Bundesgebiet informiert ist. Zwar verweist der Verordnungsgeber in den EB zu Abs. 4 hierzu auf eine Tabelle der Regulierungsbehörde(https://www.rtr.at/de/tk/MitteilungVorflle), die dort angeführten Schwellenwerte scheinen jedoch nicht mit jenen in Abs. 2 übereinzustimmen. Beispielsweise beträgt der Schwellenwert bei einem Sicherheitsvorfall von mehr als vier Stunden in der Dienstekategorie Mobiltelefonie gemäß Tabelle 170 000 Teilnehmer während in Abs. 2 Z 5 des vorliegenden Entwurfs 150 000 als absolute Obergrenze angeführt wird.

Die ISPA spricht sich daher dafür aus, in der Verordnung ausschließlich absolute Schwellenwerte anzuführen und von einem relativen Wert, der nur mithilfe weiterer Unterlagen eruiert werden kann, abzusehen. Dies ist auch im vorliegenden Entwurf bereits in den § 3 Abs. 2 Z 1 u. 7 entsprechend umgesetzt, in welchen ausschließlich ein absoluter Wert genannt wird.

In diesem Zusammenhang möchte die ISPA außerdem darauf aufmerksam machen, dass bei der Erbringung von Diensten, die auf einer SIM-Karte basieren, SIM-Karten die ausschließlich für M2M-Dienste verwendet werden nicht in die Berechnung der Anzahl an betroffenen Teilnehmern einfließen sollen, sofern es dem Betreiber möglich ist, diese zu separieren. Solche SIM-Karten werden in der Regel in Geräten verbaut, die weltweit verwendet werden (z.B. Autos) und ein Ausfall dieser Dienste hätte daher nur bedingt Auswirkungen in Österreich.

3) Anstelle einer „unverzüglichen“ Meldung sollte eine Meldefrist von 24h vorgesehen werden

In Bezug auf den zeitlichen Horizont einer Meldung verweist der Verordnungsgeber lediglich darauf, dass diese „unverzüglich ab Kenntnis des Vorfalls“ zu erfolgen habe. In den EB zu § 2 Z 8 TK-NSiV 2020-E wird klargestellt, dass hierunter ohne „schuldhaftes Zögern“ zu verstehen sei, wobei „die Informationspflichten jedenfalls nicht auf die Geschäftszeiten des Betreibers beschränkt sind. Im Zweifel wird von einer Meldepflicht auszugehen sein.“

Die ISPA möchte an dieser Stelle darauf hinweisen, dass gerade kleine und mittelgroße Unternehmen, sofern sie von den Informationspflichten erfasst werden, über keine 24/7 technischen Bereitschaftsdienste verfügen und hierfür auch nicht das notwendige Personal haben. Um sicherzustellen, dass auch diese Unternehmen die Informationspflichten erfüllen können und nicht unverhältnismäßig benachteiligt werden ersucht die ISPA daher § 3 dahingehend zu novellieren, dass die Erstmeldung innerhalb von 24h zu erfolgen hat. Dies würde es den Unternehmen erlauben, auch mit einem gerade an Wochenenden nur beschränktem Servicedienst die Fristen einzuhalten.

Weiters besteht oftmals zu Beginn eines Sicherheitsvorfalls Unklarheit, ob die Schwellenwerte in Abs. 2 erreicht werden und damit die Informationspflicht gemäß Abs. 1 eintritt. Aufgrund dessen wird in einigen Fällen vermutlich zunächst nur ein Warnhinweis iSd § 4 abgegeben. Da hierdurch jedoch bereits die wesentliche Funktion der Informationspflicht iSd § 3 erfüllt wird – die Meldung erfolgt sogar ebenfalls über das Meldeportal der Behörde – ersucht die ISPA um Klarstellung, dass bei Abgabe eines Warnhinweises der Betreiber mit einer Erstmeldung im Sinne des § 3 Abs. 1 nicht in schuldhaften Verzug gerät. Eine entsprechende Folgemeldung, sofern sich herausstellt, dass die Schwellenwerte des § 3 Abs. 2 erfüllt sind, sollte innerhalb von 36h abgegeben werden können.

Um den Meldevorgang generell zu beschleunigen regt die ISPA zudem an, dass der Meldeweg selbst vereinfacht wird. Dabei sollte eine Meldung nicht nur mittels Zugriffes durch einen individuell benannten Nutzer auf das Meldeportal der RTR möglich sein, sondern auch durch eine vom Betreiber eingerichtete Netzbereitschaft (z.B. Security Operation Center) als Absender, die hierfür eine eigene E-Mail Adresse nutzt, wie dies beispielsweise auch bei einer Meldung an CERT der Fall ist.

4) Für die Umsetzung der Mindestsicherheitsmaßnahmen sollte eine Frist ergänzt werden

Anders als in Bezug auf die Sicherheitsanforderungen an 5G-Netze in § 6 TK-NSiV 2020-E fehlt in § 5 TK-NSiV 2020-E eine Frist bis zu der die vorgesehenen allgemeinen Mindestsicherheitsanforderungen umzusetzen sind. Mangels einer solchen Frist ist anzunehmen, dass bereits umgehend mit In-Kraft-Treten der Verordnung jedes unterworfene Unternehmen auf Aufforderung ein entsprechendes Sicherheitskonzept vorlegen können muss das sämtliche der in Abs. 1 Z 1 – 7 angeführten Bereiche abdeckt (§ 5 Abs. 2 TK-NSiV 2020-E).

Zwar geht die ISPA davon aus, dass die in § 5 Abs. 1 TK-NSiV 2020-E genannten Maßnahmen bereits durch bestehende Sicherheitskonzepte wie etwa dem ISPA Mustersicherheitskonzept zur Genüge abgedeckt sind. Dennoch ersucht die ISPA um eine über das In-Kraft-Treten der Verordnung hinausgehende Umsetzungsfrist um es den Unternehmen zu erlauben, ihre internen Sicherheitskonzepte anhand der Vorgaben zu evaluieren und in den erforderlichen Bereichen Verbesserungen vorzunehmen. Die ISPA regt daher an, der Frist zur Umsetzung der Erfordernisse in § 5 Abs. 1 sechs Monate nach In-Kraft-Treten der Verordnung anzusetzen.

Ferner ersucht die ISPA in den EB zu § 5 Abs. 2 um Klarstellung, dass die der Regulierungsbehörde zu übermittelten Informationen bzw. Unterlagen sich ausschließlich auf eine generelle Darlegung

des Sicherheitskonzept begrenzen und nicht die Übermittlung von Unterlagen zu einzelnen Maßnahmen erforderlich ist. Insbesondere hinsichtlich der gemäß Abs. 1 Z 2 leg. cit. notwendigen Hintergrundüberprüfungen erscheint dies aus datenschutzrechtlicher Sicht zwingend geboten da hierbei oftmals sensible Details des Privatlebens des Betroffenen offengelegt werden müssten.

5) Die Bezugnahme auf „Teilnehmer" widerspricht dem Grundgedanken der TK-NSiV

Die umfangreichen Sicherheitsanforderungen an 5G-Netze sind gemäß § 6 Abs. 1, 2 u. 3 TK-NSiV-E auf Betreiber von 5G-Netzen mit insgesamt mehr als „100 000 Teilnehmern in allen von ihnen betriebenen Mobilfunknetzen begrenzt". Die ISPA begrüßt grundsätzlich diese Eingrenzung auf große Netze hinterfragt jedoch die Bezugnahme auf „Teilnehmer" als maßgebende Größe.

Denn hierunter versteht sich gemäß § 3 Z 19 TKG eine natürliche oder juristische Person mit welchen der Betreiber ein Vertragsverhältnis eingegangen ist. Gerade der Einsatz von 5G Technologie wird in Hinkunft jedoch auch zur Anbindung zahlreicher IoT-Sensoren verwendet werden, wobei der Vertrag dabei mit einer einzelnen natürlichen oder juristischen Person als Teilnehmer abgeschlossen wird (z.B. mit einer Gemeinde zur Errichtung einer Smart-City etc.).

Im Sinne der Gleichbehandlung der betroffenen Unternehmen und dem Grundgedanken der Verordnung einer angemessenen Beherrschung der Risiken für elektronische Kommunikationsnetze und -dienste entsprechend regt die ISPA an, dass die Größe des Netzes nicht nur anhand der Anzahl der angebundenen Teilnehmer bestimmt werden sollte. Vielmehr sollte eine neutrale Formulierung wie etwa „Anschlüsse" in § 6 samt eigenem Schwellenwert sowie eine entsprechende Begriffsdefinition in § 2 aufgenommen werden.

6) Der Nachweis eines Informationssicherheitsmanagementsystems sollte anhand zusätzlicher Standards und auch mittels Selbstaudit möglich sein

Gemäß § 6 Abs. 1 TK-NSiV-E sollen Betreiber von 5G-Netzen das Bestehen eines Informationssicherheitsmanagementsystems gemäß einer diesbezüglich anerkannten internationalen Norm durch Vorlage eines Auditberichts nachweisen.

Die Gewährleistung eines hohen Sicherheitsstandards der Mobilfunknetze liegt selbstverständlich im eigenen Interesse der Betreiber und ist daher auch für die ISPA von großer Bedeutung. Dennoch ersuchen wir darum, das Hauptaugenmerk weiterhin auf eine technisch und wirtschaftlich ausgewogene Gewährleistung der Netzsicherheit zu legen, und nicht auf die damit einhergehende Dokumentation, welche mit erheblichem bürokratischem Aufwand verbunden ist. Bereits heute wird von den Betreibern ein hoher Sicherheitsstandard der Netze gewährleistet, ohne, dass hierfür bürokratische Hürden in Form von Auditberichten, Konformitätserklärungen u.ä. notwendig erscheinen.

Die ISPA möchte darauf hinweisen, dass obwohl der Nachweis über die Einhaltung eines Informationssicherheitsmanagementsystems auch in Form eines Auditberichts für ausreichend

erachtet wird, und kein Nachweis einer (externen) Zertifizierung erforderlich ist, der interne Personalaufwand de facto der Gleiche bleiben würde. Denn durch den Entfall der Zertifizierung reduziert sich – neben den damit einhergehenden finanziellen Kosten – lediglich der Personalaufwand, welcher in den Tagen der Zertifizierung aufgebracht werden müsste.

Um den Gesamtaufwand, der mit der Umsetzung dieser Bestimmung einhergeht, daher im Rahmen zu halten ersucht die ISPA, dass die Regulierungsbehörde, wie auch in den EB bereits angedeutet, nicht nur die angeführten ISO Standards, sondern auch andere internationale Normen als gleichwertig anerkennt. Damit würde man es auch kleinen und mittelgroßen Unternehmen, welche durch innovativen Einsatz von 5G-Technologie den Wettbewerb beleben möchten, ermöglichen an der Nutzung dieser Zukunftstechnologie teilzunehmen. Denkbar wäre es etwa, die bereits den Mindestsicherheitsanforderungen in § 5 des vorliegenden Entwurfs zugrundeliegenden „ENISA Technical Guideline on Security Measures v. 2.0“ auch hier heranzuziehen, und einen Nachweis über die Erfüllung der darin genannten security objectives auch für 5G-Netze als ausreichend zu erachten. Denn diese erfordern in vielerlei Hinsicht bereits eine ähnliche Tiefe in der internen Überprüfung wie nach den genannten ISO Standards.

Des Weiteren ist es nach Ansicht der ISPA unklar, ob die in den EB enthaltene Formulierung, dass zur Erstellung von Auditberichten „gegebenenfalls“ externe Dienstleister herangezogen werden können im Umkehrschluss Selbstaudits ausschließt. Die ISPA ersucht von einem solchen Ausschluss von Selbstaudits jedenfalls abzusehen, da diese eine weitere Möglichkeit für Unternehmen darstellen den Gesamtaufwand in einem verhältnismäßigen Rahmen zu halten.

7) Hinsichtlich der Umsetzung der ENISA „Indispensable Baseline Security Requirements for the Procurement of Secure ICT Products and Services“ ist es unklar ob dies auch bereits vorhandene Netzkomponenten betrifft

Als einen der Anhang 1 angeführten Standards haben Betreiber von 5G-Netzen den ENISA Standard „Indispensable Baseline Security Requirements for the Procurement of Secure ICT Products and Services“ zu erfüllen. Dieser soll die Einhaltung von Sicherheitsstandards im Beschaffungsprozess bei IKT-Komponenten und Dienstleistungen gewährleisten.

Angesichts der in Abs. 2 enthaltenen Umsetzungsfrist bis 30. Juni 2021 geht die ISPA davon aus, dass bis zu diesem Zeitpunkt die Einkaufszyklen der normunterworfenen Unternehmen auf die in den angeführten ENISA Richtlinien angeführten Mindestanforderungen hin überprüft und gegebenenfalls angepasst werden müssen, sodass Produkte die nach dem 30. Juni 2021 erworben werden jedenfalls die Anforderungen erfüllen.

Die ISPA ersucht jedoch um Klarstellung, dass hiermit keinesfalls eine entsprechende Evaluierung sämtlicher bereits erworbener Netzkomponenten gemeint sein kann, da für diese ein entsprechender Nachweis, dass der jeweilige Hersteller sämtliche der enthaltenen Anforderungen erfüllt, nicht mehr oder nur mit unverhältnismäßigem Aufwand möglich ist. Eine solche Interpretation würde auch klar über die korrespondierende Anforderung in der EU 5G-Toolbox hinausgehen, die nur auf eine Angleichung des Mindestsicherheitsniveaus in den (zukünftigen) Einkaufszyklen Bezug

nimmt und keine generelle Evaluierung des Bestands an Netzkomponenten vorschreibt.[1] Letzteres würde vielmehr einer de-facto effektiven Rückwirkung der Norm gleichkommen und ist daher abzulehnen.

8) Die Umsetzung neuer Versionen sollte erst nach Novellierung der Verordnung erforderlich sein

Da Abs. 2 auf die in Anhang 1 angeführten Standards jeweils in der geltenden Fassung Bezug nimmt, ist es nach Ansicht der ISPA fraglich, wie in Hinkunft mit Updates der 29 Standards umgegangen werden soll. Keinesfalls kann es die Aufgabe der Unternehmen sein, ständig sämtliche Standards zu verfolgen und auf etwaige Updates umgehend zu reagieren. Vielmehr ersucht die ISPA, dass sofern die Regulierungsbehörde der Ansicht ist, dass ein Standard in einer aktualisierten Fassung umzusetzen sei, hierfür die Verordnung entsprechend novelliert und eine neue Umsetzungsfrist festgesetzt wird.

Darüber hinaus ist unklar, innerhalb welcher Frist Unternehmen, die den Schwellenwert von 100 000 Teilnehmern überschreiten sämtliche der angeführten Standards zu erfüllen haben. Auch hierfür ersucht die ISPA um Aufnahme einer entsprechenden Frist.

9) Der Betrieb eines NOC sowie eines SOC sollte nicht zwingend in „eigenen Räumlichkeiten“ erfolgen

Gemäß § 6 Abs 3 Z 1 TK-NSiV-E hat der Betreiber eines 5G-Netzes den Betrieb von Network Operation Center (NOC) sowie Security Operation Center (SOC) in eigenen Räumlichkeiten innerhalb der Europäischen Union nachzuweisen. Wie aus den entsprechenden EB hervorgeht ist dies so auszulegen, dass NOC und SOC nicht in Räumlichkeiten externer Dienstleister betrieben werden dürfen. Hierdurch soll gewährleistet werden, dass „Anomalien entdeckt und Bedrohungen (wie z.B. durch kompromittierte Endgeräte inkl. IoT-Komponenten) identifiziert und verhindert werden.“

Nach Ansicht der ISPA führt dies zu einem de facto Verbot der Heranziehung externer Dienstleister für den Betrieb von SOC/NOC ohne, dass es hierfür eine ausreichende Begründung gäbe bzw. dies zur Erfüllung des angegebenen Zwecks erforderlich erscheint. Denn gerade zum Betrieb solcher SOC/NOC ist in der Regel speziell geschultes, und hochqualifiziertes Personal erforderlich. Gerade aus diesem Grund übernehmen solche Aufgaben bislang zum Großteil externe darauf spezialisierte IT-Dienstleister, die hierfür auf eigene Räumlichkeiten zurückgreifen können, in welchen die notwendige kostenintensive Infrastruktur zur Verfügung steht.

Ohne der Möglichkeit auf solche Dienstleister zurückzugreifen, wäre der Betreiber selbst zu den Investitionen in diese Infrastruktur verpflichtet und müsste darüber hinaus auch jedes Unternehmen

[1] NIS Cooperation Group „Cybersecurity of 5G networks EU Toolbox of risk mitigating measures” (2020) CG Publication 01/2020 26.

eigens das dafür notwendige Personal einstellen wobei aufgrund der spezifischen Qualifikationsanforderungen zwingend mit Personalengpässen zu rechnen wäre. Hiervon wären gerade kleinere Unternehmen stärker betroffen, welche nicht über ausreichende Ressourcen verfügen, um in die notwendige Infrastruktur zu investieren und darüber hinaus auch aufgrund der erwähnten Engpässe nicht umgehend auf das notwendige Personal zurückgreifen könnten. Diese Unternehmen wären damit erheblich in der Nutzung von 5G Technologie und in weiterer Folge ihrem Fortkommen am Breitbandmarkt gehindert wodurch die bereits seit Jahren zu beobachtende Konzentration des Breitbandmarktes in Österreich, welchem sich die ISPA klar entgegenstellt, vorangetrieben werden würde.

Um die Kosten im Rahmen zu halten ist aus ökonomischen Gesichtspunkten zudem absehbar, dass das Sicherheitsniveau nicht zwingend jenem entsprechen würde welches durch den Betrieb eines NOC/SOC durch einen externen Dienstleister gewährleistet wäre. Es ist daher nachvollziehbar, dass auch die 5G Toolbox der EU zwar vorsieht, dass NOC und SOC in Räumlichkeiten innerhalb der EU betrieben werden sollen, nicht jedoch, dass es sich um „eigene Räumlichkeiten“ des Betreibers zu handeln hat.[2]

Aus den genannten Gründen erachtet die ISPA den durch diese Vorgabe erfolgten Eingriff in das Recht auf freie Erwerbsausübung iSd Art 6 StGG der normunterworfenen Unternehmen als nicht nur nicht geeignet zur Erreichung des angestrebten Ziels, sondern in jedem Fall auch als unverhältnismäßig und daher unzulässig.

Die ISPA ersucht daher, im Einklang auch mit den bestehenden Empfehlungen auf EU-Ebene den Passus „in eigenen Räumlichkeiten“ aus § 6 Abs 3 Z 1 TK-NSiV-E zu streichen.

Darüber hinaus sollte es auch möglich sein, NOC/SOC in gemeinsamen Räumlichkeiten zu betreiben, um zu ermöglichen, das notwendige interdisziplinäre Knowhow an einem Ort zu bündeln.

10) Eine Multi-Vendor-Strategie sollte nicht unverhältnismäßig in das Grundrecht auf Erwerbsfreiheit der Betreiber eingreifen

In § 6 Abs. 3 Z 7 sieht der Verordnungsgeber einen verpflichtenden Nachweis über eine „Multi-Vendor Strategie“ vor wobei die EB hierzu ergänzend ausführen, es handle sich dabei um die „Auswahlmöglichkeit eines Betreibers unter zumindest zwei Lieferanten für Netzinfrastrukturelemente eines 5G-Netzes“. Leider lässt diese Formulierung auch samt den weiteren Ergänzungen in den EB zahlreiche Interpretationsmöglichkeiten offen.

Die ISPA lehnt eine „Multi-Vendor Strategie“ sowohl im Sinne einer grundsätzlichen Pflicht für Unternehmen, Netzkomponenten von zumindest zwei Herstellern zu beziehen sowie auch im Sinne eines Verbots des Bezugs von Netzkomponenten, die nur von einem einzigen Lieferanten bezogen werden können entschieden als unverhältnismäßigen Eingriff in das Recht auf freie

[2] NIS Cooperation Group „Cybersecurity of 5G networks EU Toolbox of risk mitigating measures” (2020) CG Publication 01/2020 25.

Erwerbsausübung (Art 6 StGG) sowie die Privatautonomie (Art 5 StGG) der betroffenen Unternehmen ab.

Eine solche Multi-Vendor Strategie wäre nicht zur Erfüllung des öffentlichen Interesses nach Sicherheit der Netzinfrastruktur geeignet und würde diesem Interesse sogar entgegenlaufen. Denn der verpflichtende Einsatz von Netzkomponenten verschiedener Hersteller schafft zusätzliche Sicherheitsrisiken, die durch mangelnde Interoperabilität bzw. Kompatibilität der Netzinfrastrukturelemente geschaffen werden. Damit einhergehend würde auch das Management von Sicherheitsvorfällen erheblich erschwert werden da die Lokalisierung eines Problems in einem Netz mit Komponenten zahlreicher Hersteller sich weitaus schwieriger und aufwendiger gestaltet. Dies betrifft gleichermaßen auch den Betrieb der in § 6 Abs. 3 Z 1 vorgesehenen NOC/SOC. Denn auch das hierfür notwendige spezialisierte IT-Personal müsste Wissen über die Komponenten mehrerer Hersteller mitbringen, worunter zum einen das technische Detailwissen leiden würde sowie zum anderen der in Pkt. 9 genannte Mangel an entsprechendem Personal mit den notwendigen Fähigkeiten noch weiter verstärkt werden würde. Letztlich ergeben sich im Fall von Sicherheitsvorfällen auch Produkthaftungsfragen, die sich beim Bezug von Komponenten mehrere Lieferanten höchst komplex gestalten würden.

Ein entsprechender Gegenwert für die Sicherheit der Netze ist hingegen nicht erkennbar. Vielmehr müsste davon ausgegangen werden, dass sowohl die Netzwerkkomponenten, welche die Betreiber beziehen, als auch deren Lieferanten, bereits aufgrund der Vorgaben des ENISA Standards „Indispensable Baseline Security Requirements for the Procurement of Secure ICT Products and Services“ (vgl. Pkt 7) ausreichende Sicherheitsstandards erfüllen müssen.

Angesichts des erheblichen Eingriffs in die Privatautonomie und freie Erwerbsausübung der betroffenen Unternehmen, die ihre Lieferanten nicht mehr aus ökonomischen Gründen und aufgrund von internen Sicherheitsüberlegungen sondern vielmehr basierend auf staatlichen Vorgaben aussuchen müssten, und des geringen wenn nicht sogar kontraproduktiven Nutzens einer solchen Maßnahme zur Gewährleistung der öffentlichen Sicherheit, ist eine solche Multi-Vendor-Strategie von Seiten der ISPA klar als unverhältnismäßig abzulehnen.

Die ISPA geht vielmehr im Sinne einer verfassungskonformen Interpretation dieser Vorgabe davon aus, dass § 6 Abs. 3 Z 7 den Nachweis von alternativen Lieferanten erfordert, auf die im Bedarfsfall zur Lieferung einer bestimmten Gruppe von Netzwerkkomponenten zurückgegriffen werden kann, ohne, dass hierfür bereits ein Rahmenvertrag vorgelegt werden muss. Eine solche Auflistung möglicher Alternativen würde bereits ausreichend dem Gedanken der 5G Toolbox der EU-Kommission entsprechen, die durch eine solche Multi-Vendor Strategie lediglich die Abhängigkeit von einem einzigen Lieferanten im Sinne des business continuity managements begrenzen möchte.[3] Denn für den Fall, dass es Probleme (Lieferverzug, Sicherheitsbedenken etc.) hinsichtlich des Lieferanten erster Wahl gibt könnte jederzeit auf eine der angeführten Alternativen zurückgegriffen werden.

[3] NIS Cooperation Group „Cybersecurity of 5G networks EU Toolbox of risk mitigating measures” (2020) CG Publication 01/2020 28.

In keinem Fall sollte jedoch im Einzelfall eine Begründung für die Heranziehung eines bestimmten Lieferanten erforderlich sein, da dies einen unverhältnismäßigen Aufwand darstellen würde, grundsätzlich im Ermessen des Unternehmens liegen sollte und über den genannten Zweck der Norm deutlich hinausgeht. Können bestimmte Netzkomponenten nur von einem einzigen Lieferanten bezogen und daher keine Alternative genannt werden, so hätte der Betreiber dies kurz zu begründen, etwa wenn es sich dabei um Spezialkomponenten handelt bzw. es aufgrund mangelnder Interoperabilität keine Alternativen anderer Hersteller gibt. Die ISPA ersucht im Sinne der Rechtssicherheit um entsprechende Klarstellung der Auslegung dieser Bestimmung durch den Verordnungsgeber.

Aus dem Wortlaut des Abs. 3 („[…] auf Verlangen der Regulierungsbehörde nachzuweisen“) ist zudem nicht ableitbar, wie häufig eine entsprechende Liste mit Alternativen zu aktualisieren ist, da sich das Angebot der Lieferanten selbstverständlich stets ändern kann. Die ISPA ersucht hier von einer periodischen Überprüfung jedenfalls abzusehen und es den Betreibern zu ermöglichen bei Nachfrage der Behörde die Liste entsprechend zu aktualisieren.

11) Die Zugangsbeschränkung von Dritten sollte sich am Stand der Technik orientieren

§ 6 Abs. 3 Z 5 enthält die Anforderung, den Zugriff auf Netzwerkinfrastruktur auf befähigtes und qualifiziertes Personal zu beschränken, das einer Sicherheitsüberprüfung unterzogen wurde sowie den Zugang durch Dritte zu beschränken und zu überwachen. Dabei handelt es sich um eine grundlegende Sicherheitsanforderung, die bereits jetzt aufgrund anderer gesetzlicher Verpflichtungen durch die Unternehmen umgesetzt wird. Zum besseren Verständnis regt die ISPA jedoch an in den EB hervorzuheben, dass beide Maßnahmen sich jeweils am Stand der Technik zu orientieren haben, wie dies auch in der zugrundeliegenden Gesetzesbestimmung (§ 16a Abs. 2 TKG) festgehalten wird, und darüber hinaus selbstverständlich nur im Einklang mit anderen Anfordernissen, insbesondere datenschutzrechtlichen Grundsätzen, ergriffen werden können.

Die ISPA hofft auf die Berücksichtigung ihrer Bedenken und Anregungen.

Für Rückfragen (und weitere Auskünfte) stehen wir jederzeit gerne zur Verfügung

Mit freundlichen Grüßen,

ISPA - Internet Service Providers Austria

Dr. Maximilian Schubert, LL.M.

Generalsekretär

Die ISPA – Internet Service Providers Austria – ist der Dachverband der österreichischen Internet Service-Anbieter und wurde im Jahr 1997 als eingetragener Verein gegründet. Ziel des Verbandes ist die Förderung des Internets in Österreich und die Unterstützung der Anliegen und Interessen von über 200 Mitgliedern gegenüber Regierung, Behörden und anderen Institutionen, Verbänden und Gremien. Die ISPA vertritt Mitglieder aus Bereichen wie Access, Content und Services und fördert die Kommunikation der Marktteilnehmerinnen und Marktteilnehmer untereinander.

ISPA – Internet Service Providers Austria
Währinger Straße 3/18, 1090 Wien, Austria
☎ +43 1 409 55 76
office@ispa.at
www.ispa.at

UniCredit Bank Austria AG
Konto-Nr.: 00660 491 705, **BLZ:** 12000
BIC: BKAUATWW
IBAN: AT59 1200 0006 6049 1705

UID-Nr.: ATU 54397807
ZVR-Zahl: 551223675