RTR

Wahrnehmungsbericht 2023

TLP-White-Version

www.rtr.at

TLP:WHITE

2023

Wahrnehmungsbericht 2023

des Fachbeirats für Sicherheit in elektronischen Kommunikationsnetzen

TLP-White-Version

Rundfunk und Telekom Regulierungs-GmbH

Mariahilfer Straße 77–79 | A-1060 Wien | Österreich
T: +43 1 58058-0 | E: rtr@rtr.at
www.rtr.at

TLP:WHITE

Geheimhaltung: Traffic Light Protocol

Das Traffic Light Protocol (TLP) ist eine standardisierte Vereinbarung zum Austausch von schutzwürdigen Informationen. Das TLP dient der Erhöhung der Sicherheit bei der Weitergabe sensibler Daten. Alle Dokumente werden in eine von vier Klassen eingeteilt, welche die Bedingungen für ihre Weitergabe regeln.

Für den vorliegenden Wahrnehmungsbericht wurde seitens des Fachbeirats eine Klassifizierung auf TLP:AMBER+STRICT gemäß TLP 2.0 vorgenommen. Davon abweichende Textstellen sind im Dokument explizit gekennzeichnet.

Das Traffic Light Protocol 2.0[1] sieht folgende Kategorien vor:

TLP:RED = nur für die Augen und Ohren einzelner Empfänger, keine weitere Offenlegung. Quellen können TLP:RED verwenden, wenn auf Informationen nicht effektiv reagiert werden kann, ohne dass ein erhebliches Risiko für die Privatsphäre, den Ruf oder den Betrieb der beteiligten Organisationen besteht. Empfänger dürfen daher TLP:RED-Informationen mit niemand anderem teilen. Beispielsweise sind im Kontext eines Meetings TLP:RED-Informationen auf die Teilnehmer des Meetings beschränkt.

TLP:AMBER = eingeschränkte Offenlegung, Empfänger können dies nur gemäß dem Need-to-Know-Prinzip innerhalb ihrer Organisation und deren Klienten verbreiten. Man beachte, dass TLP:AMBER+STRICT die Freigabe auf die Organisation selbst einschränkt. Quellen können TLP:AMBER verwenden, wenn Informationen zwar für eine effektive Reaktion Unterstützung erfordern, aber bei Weitergabe außerhalb der beteiligten Organisationen ein Risiko für die Privatsphäre, den Ruf oder den Betrieb bergen. Empfänger können TLP:AMBER-Informationen an Mitglieder ihrer eigenen Organisation und deren Klienten weitergeben, aber nur auf einer Need-to-Know-Basis, um ihre Organisation und deren Klienten zu schützen und weiteren Schaden zu verhindern. Hinweis: Wenn die Quelle die Freigabe auf die Organisation selbst beschränken will, muss sie TLP:AMBER+STRICT angeben. Informationen ohne TLP-Kennzeichnung gelten als TLP:AMBER+STRICT.

TLP:GREEN = eingeschränkte Offenlegung, Empfänger können dies in ihrer Community verbreiten. Quellen können TLP:GREEN verwenden, wenn Informationen nützlich sind, um das Bewusstsein in ihrer breiteren Community zu erhöhen. Empfänger können TLP:GREEN-Informationen an Fachkollegen und Partnerorganisationen innerhalb ihrer Community weitergeben, aber nicht über öffentlich zugängliche Kanäle. TLP:GREEN-Informationen dürfen nicht außerhalb der Community geteilt werden. Hinweis: Wenn „Community“ nicht definiert ist, kann als Community Cybersicherheit/Verteidigung verstanden werden.

TLP:CLEAR = Empfänger können dies weltweit verbreiten, es gibt keine Einschränkung der Offenlegung. Quellen können TLP:CLEAR in Übereinstimmung mit anwendbaren Regeln und Verfahren für die Veröffentlichung verwenden, wenn Informationen ein minimales oder kein vorhersehbares Missbrauchsrisiko bergen. Vorbehaltlich der urheberrechtlichen Zulässigkeit dürfen TLP:CLEAR-Informationen uneingeschränkt weitergegeben werden.

[1] Quelle: Wikipedia; https://de.wikipedia.org/wiki/Traffic_Light_Protocol

Wahrnehmungsbericht 2023 des Fachbeirats für Sicherheit in elektronischen Kommunikationsnetzen

TLP-White-Version

Vorwort

Sehr geehrte Damen und Herren,

das Thema „Sicherheit im Netz“ ist heute in aller Munde und ein zentraler Teil der Sicherheit unseres Staates und jedes einzelnen Menschen, der hier in Österreich lebt. Grundvoraussetzung für Sicherheit im Netz ist aber auch die Sicherheit der physischen mobilen und festen Netze, über die Zugang zum Netz sowie zum Internet als Ader unserer Wirtschaft und unseres gesamten gesellschaftlichen Lebens besteht.

Wenn es um die Sicherheit von Kommunikationsnetzen geht, sind zwei Faktoren zu beachten. Zum einen die technische Sicherheit, die anhand von technischen Standards überprüft werden kann, und zum anderen externe Effekte, die den Betrieb eines Netzes beeinflussen können. Gerade die Sicherheit der Lieferketten spielt hier eine besondere Rolle.

Auf europäischer Ebene wurde der Bereich Netzsicherheit schon seit 2009 und im Zusammenhang mit dem Einsatz von 5G-Technologie seit 2019 zum Thema gemacht. Damals wurden seitens der EU-Kommission erste Schritte eingeleitet, die im Ergebnis dann in den Empfehlungen der EU-5G-Toolbox („Cybersicherheit von 5G-Netzen – EU-Instrumentarium der Risikominderungsmaßnahmen“, Publikation der NIS-Kooperationsgruppe 01/2020) vom Jänner 2020 ihren Niederschlag fanden. Diese Toolbox gliedert sich im Wesentlichen in zwei Abschnitte, die sich einerseits der technischen Sicherheit und andererseits der generellen Betriebssicherheit bzw. damit zusammenhängenden geopolitischen Themen widmen. Wir waren in Österreich sehr schnell in der Umsetzung der technischen Vorgaben der Toolbox durch Erlassung der Telekom-Netzsicherheitsverordnung. Der zweite Teil der Toolbox wurde dann im Telekommunikationsgesetz 2021 (TKG 2021) umgesetzt. Wesentlich ist dabei die Risikoqualifikation bei Hochrisikolieferanten in § 45 TKG 2021 sowie der in dieser Bestimmung festgelegte Prozess, wie mit derartigen Risiken umzugehen ist. Dem Fachbeirat für Sicherheit in elektronischen Kommunikationsnetzen kommt dabei die Rolle zu, sich einen Überblick zu bestehenden und möglichen Risiken zu verschaffen und in seinem Wahrnehmungsbericht dem Bundesminister für Finanzen ein möglichst umfassendes Lagebild samt Empfehlungen abzugeben. Darüber hinaus soll der Fachbeirat bei Vorliegen eines konkreten Anlassfalles dem Bundesminister für Finanzen vor bescheidmäßiger Feststellung eines Hochrisikolieferanten durch diesen mit einem Gutachten eine fachlich fundierte Entscheidungsgrundlage bereitstellen.

Eine besondere Herausforderung ist es, sich ein faktenbasiertes und objektives Bild einer Risikoeinschätzung zu verschaffen und mit fundierter Expertise aus allen gesellschaftlich relevanten Bereichen eine gesicherte Meinung zu erarbeiten. In diesem Zusammenhang ist ganz besonders darauf zu achten, sich auf gesicherte Erkenntnisse zu verlassen und eine „cognitive bias“ möglichst zu vermeiden. Das ist gerade bei Themen mit großer öffentlicher Aufmerksamkeit von Bedeutung. Weil aber Entscheidungen, die sich beispielsweise gegen Erzeuger aus bestimmten als möglicherweise politisch kritisch zu bewertenden Regionen richten, viele direkte und indirekte Folgen auf andere Bereiche in unserer Wirtschaft und Gesellschaft haben können, ist bei solchen Maßnahmen holistisch an die Angelegenheit heranzugehen und eine faktenbezogene Beurteilung zu präferieren.

Aus diesem Grund macht es auch Sinn, dass wir mit dem „Fachbeirat für Sicherheit in elektronischen Kommunikationsnetzen“ ein Expertengremium haben, das mit seinen Mitgliedern ein breites Spektrum aus Vertretern der öffentlichen Verwaltung, der akademischen Welt und aus Wirtschaft und Sozialpartnerschaft abdeckt und damit Garant dafür ist, diesem ganzheitlichen Risikobewertungsansatz bestmöglich zu entsprechen.

Mit dem nunmehr vorliegenden ersten Wahrnehmungsbericht haben wir inhaltlich das Thema „Sicherheit in elektronischen Kommunikationsnetzen“ auch im Sinne des besseren Verständnisses dieser angesprochenen umfassenden Betrachtungsweise in drei Schwerpunktkapitel geclustert.

Dieser Bericht fasst die wesentlichen Wahrnehmungen entlang der einzelnen Themenabschnitte zusammen und bildet dann einen daraus abgeleiteten konkreten Katalog von Einzelmaßnahmen ab, die nach Ansicht des Fachbeirates einen Beitrag zur generellen Verbesserung der Risikolage liefern können. Dabei hervorzuheben sind einerseits die empfohlene Erweiterung des Prüfauftrages auf alle Netzwerktechnologien unabhängig davon, ob es sich um mobile, feste oder satellitengebundene Netze handelt. Das macht schon deswegen Sinn, weil es wenig nützt, potenzielle Anbieter in 5G-Netzen auszuschließen oder besonders zu beobachten, diesen aber im Bereich des Festnetzes oder in Satelliteninfrastrukturen keine Beachtung zu schenken. Risiken lassen sich nicht auf eine bestimmte Technologie beschränken, sondern betreffen ein ganzes Ökosystem von Technologien und Infrastrukturen.

Ein anderer wichtiger Punkt, der in Zukunft größere Aufmerksamkeit fordern wird, ist die Problematik von Lieferketten und damit zusammenhängend die Resilienz von Kommunikationsnetzen, wenn diese Lieferketten unterbrochen werden. Suezkanal-Blockade, Ukrainekrieg und Corona haben dazu in den letzten Jahren wesentliche Anhaltspunkte geliefert und uns unsere Abhängigkeit von globalen Lieferketten vor Augen geführt. Es geht also oft gar nicht darum, dass unsere Kommunikation ausspioniert wird, sondern darum, zu vermeiden, dass sie nicht mehr stattfinden kann, was ungleich schlimmere Folgen haben könnte.

Dem Bericht vorangestellt ist eine Einführung in die Rechtsgrundlagen, auf denen die Arbeit des Fachbeirates basiert. Im Anschluss werden die einzelnen für 2023 festgestellten Wahrnehmungen ausgehend von Beiträgen der Beiratsmitglieder dargestellt. Der Wahrnehmungsteil gliedert sich dabei in die Abschnitte „Recht und Politik", „Technologie und technische Risikoeinschätzung" und „Märkte und Verbraucher:innen". Die Wahrnehmungen des Beirats zu allgemeinen Aspekten der Sicherheit für Netze der elektronischen Kommunikation werden insbesondere durch Beobachtungen aus dem speziellen Blickwinkel der sicherheitstechnologischen Entwicklung von Komponenten oder Dienstleistungen in der Telekommunikation und allfälligen Risiken im Zusammenhang mit der Thematik von Hochrisikolieferanten ergänzt.

Darin spiegelt sich auch sehr gut die Fachexpertise im Beirat wider, die einen umfassenden Eindruck über die Risikolage bei elektronischen Kommunikationsnetzen liefert. Der Fachbeirat hat dabei bewusst darauf verzichtet, eine Aneinanderreihung von Einzelaufsätzen der Beiratsmitglieder vorzunehmen, sondern hat sich entschieden, thematisch in sich geschlossene Abschnitte zu schaffen, die sich dem Risikothema aus unterschiedlichen Perspektiven nähern. Damit besteht die Möglichkeit, einzelne identifizierte Problemfelder nach unterschiedlichen Gesichtspunkten zu bewerten und diese Wertungen einander gegenüberzustellen. In der Gesamtheit ergibt sich daraus ein umfassendes Bild, aus dem sich die konkreten Empfehlungen des Fachbeirates für das weitere Vorgehen ableiten lassen.

Im Anschluss finden sich die aus den Erhebungen und Beratungen gewonnenen und im Fachbeirat abgestimmten Maßnahmenempfehlungen, die sich – soweit nicht explizit anderes vorgesehen ist – an den Bundesminister für Finanzen richten.

Im Ergebnis versteht sich der vorliegende Bericht auch als Referenz für die Folgejahre, um darauf aufbauend die getroffenen Risikogewichtungen jeweils neu zu evaluieren, wegzulassen oder neu hinzuzufügen.

Zusammengefasst lässt sich für das Jahr 2023 festhalten, dass es mangels konkreter objektiver Fakten, die auf ein erhöhtes Risiko durch Netzkomponenten bestimmter Anbieter hindeuten würden, keinen Anlass gibt, tiefergehende Einzelprüfungen zur Sicherheit von verbauten bzw. angebotenen Systemkomponenten und Betriebssystemen einzelner Anbieter zu empfehlen. Allerdings ist jedenfalls weiteres Monitoring sowohl auf nationaler als auch auf internationaler Ebene angeraten.

Besonderes Augenmerk ist auf allgemeine geopolitische Entwicklungen zu legen. Generell ist im Hinblick auf die Verminderung eines grundsätzlich gegebenen Klumpenrisikos vor allem in der Lieferkette zu empfehlen, auf Betreiberseite kurz- bzw. mittelfristig die Diversifizierung ihrer Lieferanten sowohl für das Zugangsnetz als auch für das Kernnetz (im Fest- und Mobilnetzbereich gleichermaßen) voranzutreiben, um zukünftig bestehende Abhängigkeiten von Lieferanten außerhalb der Europäischen Union zu verringern. Seitens des Fachbeirates wird hierauf im folgenden Bericht ein Fokus gelegt. Details dazu sind den Wahrnehmungen in Teil II, Abschnitt 2, zu entnehmen.

Aus aktueller Sicht kann davon ausgegangen werden, dass der EU-Rechtsrahmen in Österreich vorbildlich sowohl unter sicherheitstechnischen als auch unter rechtsstaatlichen Gesichtspunkten umgesetzt ist und unsere Netze grundsätzlich als sicher nach dem aktuellen Stand der Technik eingestuft werden können.

Abschließend darf ich mich an dieser Stelle sehr herzlich bei allen Fachbeiratsmitgliedern und dem Supportteam der RTR bedanken, die gemeinsam in umfangreicher Kleinarbeit an diesem Bericht mitgewirkt haben und die einzelnen Positionen in guten, sehr sachlichen, aber manchmal auch durchaus hitzigen Diskussionen in zahlreichen Sitzungen erarbeitet haben. Ich freue mich, hier eine aus meiner Sicht sehr gelungene und informative Entscheidungsgrundlage für die Risikobeurteilung der elektronischen Kommunikationsinfrastruktur in Österreich vorlegen zu können.

Wien
im März 2024

Klaus M. Steinmaurer

Vorsitzender des Fachbeirates für Sicherheit in elektronischen Kommunikationsnetzen

01

Wahrnehmungen

01 Wahrnehmungen

Nachstehend sind die wesentlichen Inhalte der in diesem Bericht des Fachbeirats für Sicherheit in elektronischen Kommunikationsnetzen gemäß § 45 Abs. 7 TKG 2021 beschriebenen Wahrnehmungen **zusammengefasst**, gefolgt von Maßnahmenempfehlungen, die sich aus den Wahrnehmungen ergeben.

Kapitel I – Recht und Politik

a. Legistische Entwicklungen auf europäischer und nationalstaatlicher Ebene

Auf nationalstaatlicher Ebene wird im Wahrnehmungsbericht eine Zusammenfassung der derzeit für die Telekommunikation und Netzsicherheit relevanten Neuerungen durch EU-Legislativ-Vorhaben gegeben. Der Schwerpunkt liegt auf der bis zum 17.10.2024 umzusetzenden NIS-2-Richtlinie. Angerissen werden auch andere Vorhaben wie der Cyber Resilience Act (CRA) der – sehr vereinfacht gesagt – das Gegenstück der NIS Richtlinie darstellt; richtet sich die NIS Richtlinie (NIS-1 und NIS-2) auf die Sicherheit von Diensten (oder nun Einrichtungen), stellt der CRA zukünftig darauf ab, die Produkte (cyber-)sicher zu gestalten. In beiden Fällen wird in Zukunft eine Zertifizierung nach dem Cybersecurity Act (CSA) eine gewichtige Rolle spielen.

b. Cybersicherheits- und Cyberkriminalitätslage

Für die Cybersicherheits- und Cyberkriminalitätslage lassen sich unterschiedliche Themenbereiche für das Jahr 2023 ableiten, welche in Beziehung zur sicherheitstechnologischen Entwicklung von Komponenten von Netzen für elektronische Kommunikation oder für Dienstleistungen für solche Netze in und außerhalb der Europäischen Union stehen. Es herrscht weiterhin eine latente Bedrohungslage durch staatliche und nichtstaatliche Akteure z. B. im Kontext des Angriffskrieges Russlands gegen die Ukraine und den damit zusammenhängenden europäischen und internationalen Sanktionen. Des Weiteren wird international von einer steigenden Aktivität durch chinesische Cyber-Akteure berichtet. Für die meisten Organisationen ist Ransomware weiterhin die größte Bedrohung. Der Fokus der Ransomware-Gruppierungen liegt oft jedoch nicht mehr auf Verschlüsselung der Unternehmensdaten, sondern auf Daten-Exfiltration mit anschließender Erpressung. Weitere Themen wie DDoS-Angriffe, kritische Sicherheitslücken im Bereich von Netzwerkhardware oder auch in Open Source Libraries (welche in sehr vielen, auch kommerziellen Produkten eingesetzt werden) sowie Angriffe auf Cloud-Computing-Systeme standen im Jahr 2023 im Fokus.

c. Cyberverteidigung und hybride Kriegsführung

Aus Sicht der Landesverteidigung ist eine zunehmende Bedrohung durch Cyberangriffe im Kontext der fortschreitenden Digitalisierung zu konstatieren, wobei insbesondere die Auswirkungen hybrider Angriffstaktiken hervorzuheben sind. Die steigende Abhängigkeit von moderner Technologie macht Unternehmen, Organisationen und Behörden immer anfälliger für Angriffe aus dem Cyber-Raum. Dadurch steigt die Bedeutung nationaler und internationaler Zusammenarbeit sowie die Notwendigkeit der Mensch-Technologie-Interaktion bei der Bewältigung komplexer sicherheitspolitischer Herausforderungen.

Hervorzuheben sind die Herausforderungen durch aufkommende disruptive Technologien wie Quantencomputer, künstliche Intelligenz und Weltraumtechnologien im Verteidigungsbereich sowie die geopolitischen Dimensionen der Cyber-Sicherheit. Die Bekämpfung von Cyberbedrohungen erfordert eine umfassende Anstrengung auf politischer, gesellschaftlicher und technologischer Ebene. Die Zusammenarbeit zwischen EU-Mitgliedstaaten, das Engagement der Elemente der öffentlichen Hand, Privatwirtschaft und Forschungseinrichtungen sowie ein möglichst hohes Level an Autarkie sind dabei als Grundsätze zur Bewältigung dieser komplexen sicherheitspolitischen Herausforderungen zu sehen.

d. Cybersicherheit von Funkanlagen

Zur Steigerung der Cybersicherheit in Ergänzung der grundlegenden Anforderungen an Funkanlagen gemäß der Richtlinie 2014/53/EU über die Bereitstellung von Funkanlagen auf dem EU-Markt (RED – Radio Equipment Directive) wurde die Delegierte Verordnung 2022/30/EU erlassen. Diese behandelt u.a.

- die missbräuchliche Nutzung von Netzressourcen und Beeinträchtigung eines Dienstes, wobei schädliche Auswirkungen auf das Netz unter Art. 3 Abs. 3 (d) RED noch zusätzlich angeführt sind;
- Sicherheitsvorrichtungen, die sicherstellen, dass personenbezogene Daten und die Privatsphäre des Nutzers und des Teilnehmers geschützt werden;
- Unterstützung bestimmter Funktionen zum Schutz vor Betrug.

e. Europäische und internationale Dimension

Vor dem Hintergrund eines größeren Bewusstseins innerhalb der EU über die Auswirkungen von kritischen Abhängigkeiten auf die Sicherheit und Versorgungssicherheit Europas strebt die EU eine umfassende Strategie der offenen strategischen Autonomie, der wirtschaftlichen Sicherheit und damit verbunden des De-Risking, d.h. der Verringerung von Abhängigkeiten von Drittstaaten in kritischen Technologiebereichen, an. In diesem Kontext ist auch die Warnung der Europäischen Kommission vor einer Gefährdung der Sicherheit der EU und die Aufforderung zur Einführung von Beschränkungen von Hochrisikoanbietern aus Drittstaaten im Telekommunikationsbereich im Einklang mit der 5G- Toolbox zu sehen.

In seinen Schlussfolgerungen vom 1. und 2. Oktober 2020 fordert der Europäische Rat die EU und die Mitgliedstaaten auf, das am 29. Januar 2020 angenommene Instrumentarium für die 5G-Cybersicherheit in vollem Umfang zu nutzen und insbesondere bei wichtigen Anlagen und Einrichtungen, die in den von der EU koordinierten Risikobewertungen als kritisch und sensibel eingestuft werden, die einschlägigen Beschränkungen für Hochrisikolieferanten anzuwenden.

Europäische Initiativen zur Verringerung von kritischen Abhängigkeiten sind auch im Zusammenhang mit der von einigen Drittstaaten verfolgten Politik der globalen technologischen Vorreiterschaft unter enger Verzahnung des militärischen und zivilen Bereichs („military-civil fusion“) zu sehen. Auf Grundlage von Gesetzen von Drittstaaten zur nationalen Sicherheit werden auch Privatunternehmen dieser Staaten als ein Instrument genutzt, um wirtschaftliche und technologische Abhängigkeiten zu erzeugen und deren Einflussbereich auszudehnen. Die derzeit in Europa wahrgenommenen Abhängigkeiten von bestimmten Drittstaaten im kritischen IKT-Infrastrukturbereich gefährden nach Wahrnehmung von Expert:innen die nationale Sicherheit und technologische Souveränität der EU und ihrer Mitgliedstaaten. In einigen EU-Mitgliedstaaten werden bestimmte 5G-Anbieter bereits in Anwendung der 5G-Toolbox als Hochrisikolieferanten eingestuft.

f. Hochrisikolieferanten

In Übereinstimmung mit der 5G-Toolbox sieht § 45 TKG 2021 Regeln hinsichtlich des Umgangs mit allfälligen Hochrisikolieferanten vor, also solchen Lieferanten, bei denen sich der Firmensitz bzw. der Firmensitz der Muttergesellschaft in einem Drittstaat befindet, bei dem die Einhaltung bestimmter in der EU üblicher maßgeblicher Standards im Bereich der Informationssicherheit oder des Datenschutzes durch den Hersteller oder Managed Service Provider („MSP“) nicht als gewährleistet betrachtet werden kann. Diese Regeln dienen primär dem Schutz der 5G-Mobilfunknetze, da dort die Abhängigkeit von allfälligen Hochrisikolieferanten besonders groß ist. Eine Nichteinhaltung der vorerwähnten Standards ist insbesondere dann wahrscheinlich, wenn – vor allem in Drittstaaten mit einem unzureichenden Ausmaß an Schutz demokratischer Grund- und Freiheitsrechte – Anlass zu der Vermutung besteht, dass geschützte Informationen, die über elektronische Kommunikationsnetze transportiert werden, mittels sog. „backdoors“ unter Bruch des Kommunikationsgeheimnisses an Institutionen dieser Drittstaaten wie etwa Geheimdienste übermittelt werden, die diese Informationen für unzulässige Zwecke missbrauchen.

In dem am 15.06.2023 veröffentlichten zweiten Fortschrittsbericht der NIS-Kooperationsgruppe über die Implementierung der 5G-Toolbox in den EU-Mitgliedstaaten wird hinsichtlich der die Hochrisikolieferanten und MSP betreffenden strategischen Maßnahmen festgehalten, dass 21 Mitgliedstaaten gesetzliche Regelungen in Kraft gesetzt haben, die nationale Behörden zur Einschränkung von Hochrisikolieferanten ermächtigen. Im Übrigen haben die Mitgliedstaaten bei der nationalen Umsetzung unterschiedliche Wege beschritten. Während einige EU-Mitgliedstaaten Vorschriften erlassen haben, nach denen Netzbetreiber den Einsatz bestimmter kritischer Komponenten in ihrem Netz einer behördlichen Vorabgenehmigung unterziehen müssen, haben andere Mitgliedstaaten Herstellern derartiger Komponenten eine Verpflichtung zu deren Vorabzertifizierung auferlegt. In den letzten Monaten wird in den Mitgliedstaaten zunehmend intensiver diskutiert, inwieweit die allfällige Auferlegung einer Verpflichtung zur Entfernung kritischer Komponenten von Hochrisikolieferanten eine Schadenersatzpflicht nach sich ziehen könnte.

Kapitel II – Technologie und Risikoeinschätzung

a. Betriebssicherheit von Telekommunikationsnetzen

Für eine nachhaltige Betrachtung der Betriebssicherheit von Telekommunikationsnetzen wäre es deutlich zu kurz gegriffen, nur die technischen Kernsysteme und deren Lieferanten zu betrachten. Vielmehr muss man auch die Sicherheit – sowohl aus technischer Sicht als auch aus dem Blickwinkel von Verfügbarkeit und Abhängigkeiten – aller anderen IT-Systeme der Betreiber mitbedenken. Das reicht von klassischer Office-IT über Systeme zur Kundenverwaltung und -verrechnung bis hin zu Webportalen und allgemeiner Netzwerktechnik. Auch die Geräte, die von den Betreibern an ihre Kund:innen verteilt werden (CPEs) oder die von Endkund:innen selbst gekauft werden, können ein Sicherheitsrisiko darstellen und die Netzintegrität gefährden. Auch die NIS-2-Richtlinie ist zu einem deutlich breiteren Sicherheitsbegriff übergegangen: es geht nicht mehr nur um die IT-Systeme für die Kernprozesse.

Mit der Verlagerung vieler Prozesse in die Cloud, der Online-Lizenzierung und Online-Wartung von Software, dem Outsourcing von Dienstleistungen inkl. Netzbetrieb und „sale and lease-back"-Aktionen ist die Verzahnung vieler Telekommunikations-Anbieter mit ihren Lieferanten sehr eng geworden. Für die Sicherheit sowohl im Sinne der Verfügbarkeit als auch aus dem Blickwinkel der Integrität und Vertraulichkeit des Netzbetriebes ist daher ein umfassendes Supply-Chain-Management essenziell geworden. Dieses muss weit über die technische Sicherheit der eingekauften Produkte hinausgehen.

b. Konformitätsprüfung von Endgeräten im Rahmen der Marktüberwachung

Aus dem Blickwinkel der Konformitätsprüfungen des Fernmeldebüros bei der Kontrolle von Endgeräten am Markt (Marktüberwachung) ist festzuhalten, dass die nationalen Marktüberwachungsbehörden dafür sorgen müssen, dass nur sichere und konforme Produkte am Markt erhältlich sind. Die Marktüberwachungsbehörde überprüft, ob ein Produkt zum Zeitpunkt des Inverkehrbringens bzw. der Inbetriebnahme den geltenden rechtlichen Anforderungen entspricht. Das Fernmeldebüro bedient sich akkreditierter (oder notifizierter) Prüfstellen, welche im Verdachtsfall entsprechende Analysen bzw. Tests durchführen.

c. Schwachstellen in Telekommunikations-Equipment

Im Zusammenhang mit Schwachstellen in Hard- und Software von Telekommunikations-Equipment ergeben sich mit der Einführung von 5G-Netzen sowohl neue Geschäftsmöglichkeiten als auch neue Sicherheitsbedrohungen. Einige der Hauptbedrohungen für die Cybersicherheit von 5G-Netzen sind aus anderen Domänen hinlänglich bekannt (z. B. Identitätsdiebstahl, Malwareverbreitung oder DDoS-Angriffe), während eine Reihe neuartiger 5G-spezifischer Bedrohungen aufgrund der einzigartigen Eigenschaften dieser Infrastruktur hinzukommen, wie beispielsweise Network-Slicing-Angriffe oder Angriffstechniken, die erst durch

den massiven Ausbau dieser Technologie ermöglicht werden, wie z. B. im IoT-Bereich, wo die Anbindung einer großen Anzahl von IoT-Geräten neue Gefahren bei Ausnutzung weit verbreiteter Sicherheitslücken nach sich zieht.

Die Erhebung potenzieller Angriffstechniken zusammen mit deren möglichen Auswirkungen auf die Vertraulichkeit, Integrität und Verfügbarkeit geben Aufschluss darüber, in welchen Bereichen Angriffe grundsätzlich möglich sind. Die meisten Angriffstechniken zielen auf die Offenlegung und das Abgreifen von Nutzerdaten ab. Eine Reihe spezialisierter Angriffstechniken zielt hingegen darauf ab, die Erbringung der Telekommunikationsdienste an sich zu unterbinden, wie beispielsweise Radio Jamming, Denial-of-Service-Angriffe gegen das Kernnetz oder die Ausnutzung von Designschwächen in telekomspezifischen Protokollen. Diese Angriffe konnten in den letzten Jahren auch bereits beobachtet werden. Dabei ist festzuhalten, dass vor allem (Distributed) Denial-of-Service-Angriffe und Angriffe mittels „Legacy Protokollen" wie SS7 beobachtet werden konnten, während direkte Angriffe auf moderne Cloud Infrastrukturen (derzeit noch) nicht öffentlich bekannt sind.

Neben der Vielzahl an technischen Problemen, die erfolgreiche Angriffe unterstützen können, kämpfen Telekom-Anbieter derzeit auch noch mit etlichen weiteren Herausforderungen, die direkten Einfluss auf die Cybersicherheit haben können. Hierzu zählen beispielsweise die Maximierung der Interoperabilität und Offenheit von 5G bei gleichzeitig hinreichender Absicherung der Infrastrukturen, das erhöhte Interesse von Angreifergruppen an Telekom-Betreibern aufgrund diverser Multiplikatoreffekte bei erfolgreicher Kompromittierung (Betreiber als Einfallstor zu Kunden; vgl. Supply-Chain-Angriffe) sowie eine Verknappung von kompetentem Personal im Cybersicherheitsumfeld.

d. Supply-Chain-Security

Was die wissenschaftliche Befassung mit Supply-Chain-Security betrifft, muss grundsätzlich konstatiert werden, dass die Lieferkette im Bereich Kommunikation für technische Gerätschaften (Devices), wie sie die österreichischen Kommunikationsdienstleister in Verwendung haben, vollständig außerhalb des Einflussbereiches der Europäischen Union liegt. Die Technologieabhängigkeit für den Nachkauf fokussiert stark in den asiatischen Raum, aber auch in die USA, wenngleich letztere die technische Assemblierung aus Kostenüberlegungen ebenso in den außer-amerikanischen Raum verlegt haben. Auf der Dienstleistungsebene gibt es Kompetenzen in Österreich, insbesondere bei Betrieb und Wartung der technischen Komponenten. Ein erfolgreich ausgenutzter Angriffsvektor auf Device-Ebene kann jedoch hier nur schwer kompensiert werden. Hinzu kommt die Tatsache, dass durch die globalen Ausrichtungen der Kommunikationsausstatter mitunter die Transformation von einer Lieferkette zu einem Wertschöpfungsnetzwerk vollzogen wurde.

Die bevorstehende Umsetzung der NIS-2-Richtlinie adressiert dabei auch die Supply-Chain-Security, da sie die NIS-2-pflichtigen Unternehmen auffordert, die Lieferketten und ihre Abhängigkeiten zu analysieren, um diese letztlich resilienter zu gestalten. Das führt auch dazu, dass die Lieferanten selbst Compliance nachweisen müssen. Auf der anderen Seite werden die Angriffe auf Produktions- und Lieferketten auch immer wahrscheinlicher. 39 Prozent der heimischen Unternehmen berichten bereits von einem Angriff auf ihre Lieferkette. Für die Kommunikationsanbieter bedeutet die globalisierte Supply-Chain einen gewissen Analyseaufwand und die Erarbeitung von Resilienzstrategien.

Auf Device-Ebene motiviert der Cyber Resilience Act die Stärkung der Cybersicherheit sowie die proaktive Analyse, Identifikation und Adressierung technischer Schwachstellen.

e. Forschungsförderung im Bereich Cybersicherheit

Digitalisierung ist ein bleibender Trend und der Grundpfeiler moderner, wettbewerbsfähiger Gesellschaften. Im Jahr 2022 wurde seitens des für Sicherheits- und Verteidigungsforschungsförderung zuständigen BMF ein eigenständiges Cybersicherheitsforschungsprogramm unter der Bezeichnung Kybernet-Pass (K-PASS)

umgesetzt. K-PASS unterstützt (primär) österreichische Unternehmen und Forschungseinrichtungen bei der Entwicklung neuer Technologien zur Gewinnung des erforderlichen Wissens zur Erhöhung der digitalen Sicherheit Österreichs und Generierung von Wertschöpfung. Ziel ist dabei die Schaffung marktnaher Forschungsergebnisse zu digitaler Sicherheit für Sicherheitsanwender (Bedarfsträger wie Polizei, Feuerwehr, Behörden, Gemeinden, aber auch sicherheitsrelevante Unternehmen wie Mobilfunknetzbetreiber, Elektrizitätsversorgungsunternehmen oder Flughafen Wien).

f. Identifizierung und Authentifizierung

Identifizierung und Authentifizierung sind Grundfunktionen der Informationssicherheit und die Grundlage des Zugangs zu geschützten Ressourcen oder des Auslösens kritischer Aktionen. Dies betrifft sowohl interne Bereiche und Komponenten der Telekommunikationsanbieter samt Fernzugriff sowie Zugang für deren Nutzer:innen zur Selbstverwaltung ihrer Konten. Mehr-Faktor-Authentifizierung ist hier Stand der Technik und sowohl über die technische Ausstattung moderner Computer und Smartphones unterstützt, etwa über Passkeys, als auch über staatliche Initiativen wie ID Austria breit verfügbar.

Mit der eIDAS-Verordnung (EU) 910/2014 ist Rechtssicherheit für die Identifikation und elektronische Unterschrift sowie für die technisch hochwertige Authentifizierung sowohl national als auch grenzüberschreitend gegeben. Aus der vor dem Abschluss stehenden eIDAS-Novelle wird mit der EUid-Brieftasche nicht nur weitere Verbreitung erwartet und europaweite Nutzung auch in der Privatwirtschaft geregelt, es werden Anwendungen, die gesetzlich oder vertraglich starke Authentifizierung benötigen, auch zur Unterstützung der EUid-Brieftasche verpflichtet. Diese sollen im Rahmen des Großpilotprojektes POTENTIAL schon vor der gesetzlichen Notwendigkeit dieser Verpflichtungen erprobt werden.

g. Zertifizierung als Grundpfeiler von Cybersicherheit

Technische Prüfung durch unabhängige Dritte ist ein probates Mittel, um die Sicherheit von IKT-Produkten, -Diensten oder -Prozessen zu bewerten. Dabei stellen Zertifizierungen die typisch rigideste Form solch unabhängiger Prüfung über verbindliche Standards, Prüfmethodik und international harmonisierte Kriterien der Prüf- und Zertifizierungsstellen dar. Hier stehen Tiefe der Prüfung, Entwicklungsdauer der Prüfschemata, Durchlaufzeit und Kosten der Zertifizierung mit der Dynamik der technischen Entwicklung und letztlich dem Aufgriff durch den Markt im Wechselspiel, sofern es zu keinen Verpflichtungen gesetzlich oder in der Beschaffung kommt. Im Bereich der Telekommunikationsnetze haben sich bereits Industriestandards aus GSMA und 3GPP entwickelt.

In der 5G-Toolbox sind Zertifizierungen von Kundenkomponenten, Netzwerkgeräten und Lieferantenprozessen vorgesehen. Gleichzeitig wird Cybersicherheitszertifizierung in der Europäischen Union über den Cyber Security Act harmonisiert, was nationale Spezifika einschränkt oder zumindest zeitlich bis zur Verfügbarkeit harmonisierter Zertifizierungsschemata begrenzt. Ein solches Schema zu 5G ist in Erarbeitung. Mit einem Entwurf zur breiteren Diskussion, der auch auf Industriestandards aus GSMA und 3GPP aufbauen soll, ist erst 2024 zu rechnen. Die konkrete Anwendbarkeit wird von der Dauer der Verabschiedung und dem Aufbau der konkreten Zertifizierungsmöglichkeiten in der EU abhängen.

Zertifizierung muss sich auf den Endnutzer auswirken. Dabei ist in nicht monopolähnlich geregelten Bereichen darauf zu achten, dass Umgehungen möglichst vermieden werden. Solche Umgehungen können durch Billigprodukte, den Online-Handel usw. nur durch umfassende Bewusstseinsbildung eingegrenzt werden, insbesondere im IoT-Bereich und bei zunehmend auf Cloud basierenden Strukturen. Dies kann besonders in der Kombination und bei entsprechender Durchdringung ein kritisches Risiko darstellen und auch im Sinne der Souveränität und Erpressbarkeit eine beachtliche Rolle spielen.

h. Funktionen und Hersteller in 5G-Netzen

Anhand der vorliegenden Daten kann festgestellt werden, dass rund 42% der Netz-Funktionen von chinesischen Herstellern bezogen wird.

Ferner sind chinesische Hersteller in 4G- und 5G-Zugangsnetzen, 4G- und 5G-Kernnetzen, IP-Multimedia-Subsystemen sowie bei der Virtualisierung von Netzfunktionen stark vertreten. Bei den restlichen Komponenten, die eher weniger komplexe Funktionen wie Richtfunk, Router, Switches, Cloud-Speicher, Server usw. beherbergen, haben auch Hersteller außerhalb von China wesentliche Anteile in den heimischen Mobilfunknetzen.

i. Business Continuity Management und Multivendor-Strategie bei 5G-Betreibern

Zur Fragestellung, welche Konsequenzen ein Ausfall oder Ausschluss eines Herstellers potenziell haben könnten, sind aus den Business-Continuity-Plänen sowie den Multi-Vendor-Strategien der Betreiber Anhaltspunkte abzuleiten.

Bei einem plötzlichen Ausfall eines Lieferanten wird der Betrieb hauptsächlich durch geografische Redundanz der wichtigen Netzkomponenten sowie Vorhaltung von Ersatzteilen für in der Regel bis zu zwölf Monate gemäß betrieblichen Kontinuitätsmanagementplänen sichergestellt, wobei dies abhängig von der Schwere und Komplexität der möglicherweise auftretenden Probleme verkürzt werden kann.

Als Grundpfeiler der Multi-Vendor-Strategie der Mobilfunknetzbetreiber wäre im Falle eines Ausfalls eines Herstellers der Austausch mit einem alternativen Hersteller prinzipiell technisch möglich, wiewohl die Mobilfunknetzbetreiber dabei auf erhebliche Kosten, Implementierungsaufwände und Laufzeiten, die sich über mehrere Jahre erstrecken können, hingewiesen haben. Lediglich bei den Komponenten, die eher weniger komplexe Funktionen wie Richtfunk, Switches, Router, Server und Cloud-Speicher beherbergen, sind in der Regel mehrere Hersteller in 5G-Mobilfunknetzen vertreten. Hier ist ein Zusammenspiel von Komponenten verschiedener Hersteller aufgrund von standardisierten und weniger komplexen Schnittstellen und funktionalen Abhängigkeiten eher gegeben.

j. Branchenrisikoanalyse

Die 2023 ebenfalls unter Federführung der RTR-GmbH durchgeführte Risikoanalyse der österreichischen Telekommunikationsbranche basiert auf der vorherigen Version aus dem Jahr 2020 und entstand in einer Public-private-Partnership mit verschiedenen Akteuren, darunter Anbieter elektronischer Kommunikationsnetze und -dienste, Ministerien, Regulierungsbehörden und Branchenexperten. Sie entspricht den Vorgaben der österreichischen Strategie für Cybersicherheit sowie des österreichischen Programms zum Schutz kritischer Infrastrukturen und berücksichtigt die Entwicklung von Risikomanagementmaßnahmen gemäß der NIS-2-Richtlinie. Insgesamt wurden sieben halbtägige Workshops genutzt, um Einzelrisiken zu bewerten, diese zu Aggregationsrisiken zusammenzufassen und daraus einen Katalog von 28 Empfehlungen abzuleiten.

Die Analyse reflektiert den Fortschritt in der Gesetzgebung und zeigt, dass einige Risiken aufgrund obligatorischer Maßnahmen oder bereits umgesetzter Empfehlungen gestrichen werden konnten. Neue Risiken entstanden aufgrund der veränderten politischen Sicherheitslage und gestiegener Cyberkriminalität. Die Risikoverteilung hat sich verschoben, wobei mehr Risiken mittlerer Höhe vorhanden sind. Die Bewältigung komplexer Cybercrime-Szenarien ist nun ein Hauptfokus, was einen verstärkten branchenübergreifenden Informationsaustausch und verbesserte gesetzliche Rahmenbedingungen erfordert.

Als Schlussfolgerung empfiehlt die Analyse die Priorisierung von vier zentralen Empfehlungen: die rechtliche und technische Förderung des Informationsaustauschs zur Bekämpfung von Cybercrime, die verstärkte Zusammenarbeit zwischen Branchen zur Erhöhung der Resilienz, die Berücksichtigung von Vorgaben der NIS-2-Richtlinie im nächsten Analysezyklus und die Integration von Erkenntnissen aus der Risikoanalyse bei der Umsetzung von Vorgaben der NIS-2-Richtlinie. Die RTR-GmbH soll hier eine wesentliche Rolle für Unternehmen der Telekommunikationsbranche übernehmen.

Kapitel III – Märkte und Verbraucher:innen

a. Cybersicherheit für Konsument:innen

Sichere Datenverarbeitung und Nutzung digitaler Produkte, Dienste und Geräte setzt sichere Infrastruktur voraus. Umgekehrt wirkt sich digitaler Konsument:innenschutz auch günstig auf die Netzsicherheit aus. Konsument:innenrelevante Cybersicherheit ließe sich aktuell besonders in folgenden Bereichen verbessern:

Mobilfunknetzbetreiber kommunizieren Datensicherheitsverletzungen meist korrekt, selten aber Abhilfemaßnahmen, mit denen Konsument:innen schädliche Folgen minimieren können. Hervorzuheben sind kostenlose Sicherheitsservices (etwa von Apple und Google) für Konsument:innen. Mobilfunkanbieter bieten nur kostenpflichtige Zusatzservices für den Identitäts-, Viren- und Onlineschutz an und begründen dies mit netzneutralitätsbedingten Lizenzkosten.

Datenübermittlungen ohne EU-adäquatem Sicherheitsniveau setzt die DSGVO Grenzen. Grundrechtssensibel verhalten sich Anbieter, die auf Datentransfers in unsichere Drittstaaten verzichten. Datenspeicherung innerhalb des EWR stärkt auch die Resilienz der Kommunikationsnetze. Die Datenschutzerklärungen der Mobilfunkanbieter offenbaren diesbezüglich noch eine Abhängigkeit von Drittstaaten ohne geeignetes Datenschutzniveau.

Smarte Haushaltsgeräte gelten als Einfallstor für Sicherheitsbedrohungen. Der EU-Entwurf zu einem Cyber Resilience Act regelt Sicherheitsaspekte des Internets der Dinge. Gerätehersteller schließen Sicherheitslücken nicht immer unverzüglich durch Softwareaktualisierung. Nach dem EU-Entwurf müssen sie automatisch und zeitnah erfolgen. Diese für die Netzintegrität wichtige Maßnahme erfordert ambitionierte Marktbeobachtung und Vollziehung.

Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) ist seit 2021 mit sicherheitsbezogenem Verbraucherschutz betraut. In Österreich fehlen Einrichtungen, die sich so einschlägig mit sicherheitsrelevantem digitalen Verbraucher:innenschutz befassen. Arbeiterkammer, Internet-Ombudsstelle, Verein für Konsumenteninformation usw. informieren und helfen Konsument:innen – allerdings ohne Einbindung in die Behördenarbeit.

b. Hochrisikolieferanten aus Sicht der Telekommunikationsbranche

Bislang liegen dem Fachbeirat keine konkreten Anhaltspunkte vor, die eine negative Bewertung einzelner Anbieter von Telekommunikationsausrüstung zum derzeitigen Zeitpunkt gerechtfertigt erscheinen ließen. Damit wird umgekehrt nicht in Abrede gestellt, dass umfangreiche Evaluierungen der Sicherheitslage sinnvoll und geboten sind. Die Einstufung einzelner Lieferanten in anderen EU-Mitgliedstaaten als Hochrisikolieferanten kann eine Anregung zur Erörterung sein, darf aber redlicherweise nicht automatisch zu einer solchen Einstufung in anderen Mitgliedstaaten führen.

Die Telekommunikationsanbieter unterliegen seit jeher allgemeinen wie sektorspezifischen Regeln, die die Datensicherheit und die Integrität des Netzbetriebes sicherstellen. Eine Einstufung einzelner Lieferanten als Hochrisikolieferanten kann zur Folge haben, dass ein Telekommunikationsanbieter mit nicht geringen Kosten für einen allfälligen Umbau seiner Infrastruktur belastet wird. Bislang hat es keine Anhaltspunkte für die Einstufung eines Lieferanten als Hochrisikolieferanten gegeben. Im wettbewerbsintensiven Telekommunikationsmarkt Österreich führt die Lieferantenvielfalt auch zu einem Technologiewettbewerb mit entsprechend positiven Folgen für die Weiterentwicklung der Telekommunikationstechnik wie auch der Services für die Nutzer:innen.

c. Cyber- und Lieferkettensicherheit aus Sicht der Industrie

Die Lage im europäischen Telekommunikationssektor ist derzeit von großem Innovationsgeist, aber auch von Risikobewusstsein und Sensibilität geprägt. Um Sicherheitsrisiken, insbesondere in der Lieferkette, begegnen zu können, ist ein EU-weites Vorgehen auch auf regulatorischer Ebene notwendig. Grundsätzlich gibt es hierfür unterschiedliche Ansätze, wobei sowohl auf die Eigenverantwortung der Telekommunikationsanbieter als auch auf die Aufsicht durch staatliche Organe und/oder Organe der EU gesetzt werden kann. Auf der einen Seite besteht ein Eigeninteresse der Unternehmen aus Kosten- und Reputationsgründen, auf der anderen Seite ist ein öffentliches Interesse durch staatliche Institutionen zu wahren. In Österreich wurden bereits regulatorische Maßnahmen ergriffen, welche auf EU-Ebene als „Anschauungsbeispiel" hervorgehoben wurden. Auf europäischer Ebene gibt es jedoch insbesondere beim Thema Hochrisikolieferanten noch keinen einheitlichen Ansatz bzw. wurden noch nicht in allen Mitgliedstaaten entsprechende Gesetze verabschiedet. Demgegenüber wurde die NIS-2-Richtlinie auf EU-Ebene bereits beschlossen, die sich mit Lieferkettensicherheit, dem Ausbau von Kommunikation und Koordination zwischen den Verantwortlichen sowie der Umsetzung wichtiger strategischer Maßnahmen für mehr Cybersicherheit befasst. Darüber hinaus ist zu erwähnen, dass auf europäischer Ebene Bewegung in das Thema mit den Vorschlägen zum „European Chips Act" oder dem Cyber Resilience Act gekommen ist, mit denen auch die Themen Lieferkettensicherheit bei Chips/Halbleitern und die Sicherheit aller IKT-Komponenten durch ihre gesamte Lebensdauer hindurch angegangen werden. Zudem arbeitet die Europäische Agentur für Netz- und Informationssicherheit (ENISA) mit Unterstützung von Stakeholdern und Mitgliedstaaten an einer einheitlichen Zertifizierung für 5G-Netzwerkkomponenten und 5G-spezifische Dienstleistungen.

Zusammenfassung

Zum Abschluss kann festgehalten werden, dass generell in Österreichs Telekommunikationsnetzen von einem hohen Sicherheitsniveau auszugehen ist. Auf Basis der aktuellen Wahrnehmungen besteht zum Zeitpunkt der Verfassung dieses Berichtes kein konkreter Anhaltspunkt, der die Bestimmung eines in den österreichischen Netzen, insbesondere in 5G Netzen verwendeten Systemausstatters als Hochrisikolieferant nach § 45 TKG 2021 erforderlich erscheinen lässt.

Allerdings ist zu empfehlen, aufgrund aktueller geopolitischer Entwicklungen auch in den Folgejahren die Beobachtung zu forcieren. Empfohlen wird insbesondere eine Erweiterung der nach der 5G-Toolbox festgelegten Maßnahmen auf alle Arten von Kommunikationsnetzen, vor allem auf Glasfasernetze. Dies wäre bei einer Evaluierung der Telekom-Netzsicherheitsverordnung 2020 zu berücksichtigen. Dabei ist ganz besonders auf Möglichkeiten der Diversifizierung im Bereich von Kern- und Zugangsnetzen zur Vermeidung von Klumpenrisiken zu achten. Dem Thema Netzresilienz einschließlich Supply-Chain ist dabei besondere Beachtung zu schenken.

Auf die Ausführungen unter Punkt 2.2.6 (Kontinuitätsmanagement und Multi-Vendor Strategie in österreichischen 5G-Netzen) sowie die Maßnahmenempfehlungen aus der Branchenrisikoanalyse 2023 unter Punkt 2.2.7.5 sowie die nachstehenden allgemeinen Empfehlungen des Fachbeirates in diesem Wahrnehmungsbericht wird gesondert hingewiesen.

Ausdrücklich festgehalten wird, dass die in den einzelnen Abschnitten festgestellten Wahrnehmungen die Diversität in der Zusammensetzung des Fachbeirats reflektieren. Daraus abgeleitet ergibt sich ein gemeinsam erarbeiteter und beschlossener Katalog von Maßnahmenempfehlungen, der gleich anschließend dargestellt ist.

02

Maßnahmenempfehlungen

02 Maßnahmenempfehlungen

Die Wahrnehmungen des Beirats zu allgemeinen Aspekten der Sicherheit für Netze der elektronischen Kommunikation werden mit Beobachtungen aus dem speziellen Blickwinkel der sicherheitstechnologischen Entwicklung von Komponenten oder Dienstleistungen in der Telekommunikation und allfälligen Risiken im Zusammenhang mit der Thematik von Hochrisikolieferanten ergänzt.

Die aus den Erhebungen und Beratungen gewonnenen und im Fachbeirat abgestimmten Maßnahmenempfehlungen sind thematisch in die drei Kapitel „Recht und Politik", „Technologie und Risikoabschätzung" sowie „Märkte und Verbraucher:innen" gegliedert.

Empfehlungen betreffend Kapitel I – Recht und Politik

- Aufgrund der latent hohen und konstanten Bedrohungslage im Bereich der Cybersicherheit sowie der Cyberkriminalität durch staatliche und nichtstaatliche Akteure sind verstärkte Ressourcen im Bereich der Vorbeugung, der Reaktion und der Aufklärung von Cybersicherheitsvorfälle sicherzustellen. Überdies sind eine weiterhin laufende engmaschige Lagebetrachtung sowie eine starke Kooperation der staatlichen Institutionen (sowohl national als auch international) miteinander und mit der Öffentlichkeit zu gewährleisten. Dies hat im Rahmen der NIS-2-, CRA- und CSA-Entwicklungen zu erfolgen.

- Für die Gewährleistung der Sicherheit und der Erbringung wesentlicher Dienste durch kritische Telekommunikationsinfrastrukturen sollten auf nationaler und europäischer Ebene verstärkt Anstrengungen unternommen werden, um technologische Abhängigkeiten von einzelnen Drittstaaten zu reduzieren und dadurch Souveränität und Handlungsfähigkeit zu gewährleisten.

- Für den Einsatz von KI in Telekommunikationsnetzen sind risikobasierte sicherheitstechnische Vorgaben zur Umsetzung der europäischen Gesetzgebung (z. B. AI Act) zu berücksichtigen.

- Sicherheitspolitische und geopolitische Fragen sollten bei Regelungen zur Auswahl und Beschaffung von Produkten und Dienstleistungen der Telekommunikationsinfrastruktur berücksichtigt werden. Konkrete Maßnahmen sind im Rahmen der Umsetzung der europäischen Rechtsakte national zu evaluieren.

- Die Notwendigkeit einer Verordnung gemäß § 3 Abs. 3 FMaG betreffend die Sicherheit von Produkten im Telekommunikationssektor sollte evaluiert werden.

- Die Zusammenarbeit mit den Prüfstellen, die nach der RL 2014/53/EU für Cybersicherheit akkreditiert sind, sollte verstärkt werden.

Empfehlungen betreffend Kapitel II – Technologie und Risikoabschätzung

- NIS-2 sollte auf Unternehmensebene bereits jetzt berücksichtigt werden. Insbesondere das Thema Supply Chain Management wird für das Risikomanagement im Unternehmen, insb. betreffend Dienstleister, adressiert.

- Zur Stärkung der Netzsicherheit und generell sollte auf geeignete Mehrfaktor-Verfahren zur Authentifizierung sowohl im Fernzugriff als auch im internen Netz der Telekommunikationsanbieter hingewirkt werden.

- Telekommunikationsanbieter sollten in den Zugängen der Kund:innen hochsichere Identifizierung und Authentifizierung aus der EU-eIDAS-Verordnung wie über ID Austria ermöglichen.

- Es wird empfohlen, die Verpflichtungen in Bezug auf 5G-Netze aus der Telekom-Netzsicherheitsverordnung 2020 auf alle Netzwerktechnologien auszuweiten.

- Auf die Empfehlungen aus der Branchenrisikoanalyse 2023 (Punkt 2.2.7.5) wird gesondert hingewiesen.

Empfehlungen betreffend Kapitel III – Märkte und Verbraucher:innen

- Telekommunikations-Netzbetreiber und -Diensteanbieter sollten für den Fall von Datensicherheitsverletzungen unter Mitwirkung der RTR-GmbH Guidelines dazu erarbeiten, mit welchen konkreten Gefahren Konsument:innen bei Datensicherheitsverletzungen zu rechnen haben und wie sie diese Gefahren vermeiden können.

- Die Basiskommunikationsdienste Telefonanruf, SMS und E-Mail werden von vielen Dienstleistern im Internet als zweiter Faktor für die Anmeldung oder für eine Passwort-Neuvergabe benutzt. Kommunikationsnetzbetreiber, die diese Medien bereitstellen, tragen daher eine zusätzliche Verantwortung für ihre Kunden. Die Integrität dieser Kommunikationswege muss daher gegen Angriffe wie SIM-Swapping, SMS-Interception, Credential-Stuffing, etc. bis hin zu Social Engineering am Helpdesk abgesichert werden.

- Es wird empfohlen, auf europäischer Ebene darauf einzuwirken, dass Konsument:innen eine durchgehende Ende-zu-Ende-Verschlüsselung zur Verfügung zu stellen ist. Weiters wird empfohlen, darauf einzuwirken, dass in Zukunft Sicherheitsupdates unabhängig von funktionsändernden Updates im Rahmen der technischen und wirtschaftlichen Möglichkeiten zur Verfügung zu stellen sind.

- Vernetzte Produkte, die Netzsicherheit und Privatsphäre besonders gefährden können, sollten auf europäischer Ebene einer externen Zertifizierung der Produktsicherheit unterworfen werden.

- Es wird empfohlen, für den Fall einer Einstufung von Lieferanten als Hochrisikolieferanten eine konkrete Handlungsempfehlung zu entwickeln, die den Zusammenhang zwischen §§44 und 45 TKG 2021 transparent macht.

- Es wird empfohlen, generelle Leitlinien für das Thema der Lieferkettensicherheit zu entwickeln, insbesondere auch in nicht direkt von NIS-2 betroffenen Sektoren.

03

Rechtsgrundlagen

03 Rechtsgrundlagen

Aufgaben des Fachbeirats für Sicherheit in elektronischen Kommunikationsnetzen

Mit § 45 Abs. 7 des am 1.11.2021 in Kraft getretenen Telekommunikationsgesetzes („TKG 2021“) wurde ein Fachbeirat für Sicherheit in elektronischen Kommunikationsnetzen („Netzsicherheitsbeirat“) eingerichtet. Der Netzsicherheitsbeirat setzt sich aus zwölf Mitgliedern zusammen. Diese Mitglieder sind Expertinnen und Experten, die von Ministerien (Bundeskanzleramt, BM für Äußeres, BM für Finanzen, BM für Gesundheit/Soziales/Pflege/Konsumentenschutz, BM für Inneres, BM für Landesverteidigung, BM für Wirtschaft und Arbeit) und Sozialpartnern (Wirtschaftskammer, Arbeiterkammer, Industriellenvereinigung) sowie vom Computer-Notfallteam (CERT) und dem Austrian Institute of Technology (AIT) benannt und von der Bundesregierung am 5.10.2022 für vier Jahre bestellt wurden. Den Vorsitz im Netzsicherheitsbeirat nimmt der Geschäftsführer des Fachbereichs Telekommunikation und Post der RTR-GmbH wahr; letztere fungiert als Geschäftsstelle des Netzsicherheitsbeirats. Zu den Aufgaben des Netzsicherheitsbeirats gehören

- die Beratung des für Telekommunikationsagenden zuständigen Bundesministeriums für Finanzen zu allgemeinen Aspekten der Sicherheit für Netze der elektronischen Kommunikation,
- die laufende Beobachtung der sicherheitstechnologischen Entwicklung von Komponenten oder Dienstleistungen für derartige Netze,
- die Erstellung eines jährlichen Wahrnehmungsberichts sowie
- die Erstellung von Gutachten in Verfahren vor dem BM für Finanzen zur allfälligen Einstufung eines Herstellers von Netzkomponenten oder eines Bereitstellers von Dienstleistungen für solche Netze als Hochrisikolieferant (das ist jemand, bei dem davon auszugehen ist, dass er mit hoher Wahrscheinlichkeit die für ihn in der EU geltenden einschlägigen Normen – insbesondere in den Bereichen Informationssicherheit und Datenschutz – nicht oder nicht ständig einzuhalten in der Lage ist).

Nach Kundmachung einer Verordnung, mit der eine Geschäftsordnung für den Fachbeirat für Sicherheit in elektronischen Kommunikationsnetzen gemäß § 45 Abs. 12 TKG 2021 erlassen wird, am 21.10.2022 (BGBl II Nr. 393/22) trat der Netzsicherheitsbeirat erstmals am 21.11.2022 zu seiner konstituierenden Sitzung zusammen. In weiteren Sitzungen am 22.03., 19.06., 13.11.2023 und am 15.01.2024 erörterte der Netzsicherheitsbeirat aktuelle Fragen der Sicherheit elektronischer Kommunikationsnetze und -dienste.

Rechtsgrundlagen für die Sicherheit elektronischer Kommunikationsnetze

Während der Schwerpunkt des TKG 1997 ausgehend auf entsprechenden Richtlinien des Europarechts zur „Open Network Provision“ (ONP) auf Bestimmungen zur Öffnung der zu liberalisierenden Telekommunikationsmärkte lag, wurde nach Umsetzung der Marktöffnungsregelungen in der Arbeit der nationalen Regulierungsbehörden der Aspekt der Sicherheit elektronischer Kommunikationsnetze und -dienste zunehmend bedeutsam, weshalb die Richtlinie 2002/21/EG (Rahmen-Richtlinie) im Jahr 2009 durch Einfügung der Artikel 13a und 13b ergänzt wurde, die u.a. Meldepflichten bei Sicherheitsvorfällen sowie Mindestsicherheitsmaßnahmen von Betreibern elektronischer Kommunikationsnetze und -dienste vorsahen. Die Regelungen wurden am 22.11.2011 durch eine entsprechende TKG-Novelle (BGBl I Nr. 102/2011) in § 16a TKG 2003 umgesetzt und den jeweils zuständigen Regulierungsbehörden (Telekom-Control-Kommission und RTR-GmbH für Betreiber elektronischer Kommunikationsnetze und -dienste, Kommunikationsbehörde Austria für Betreiber von Rundfunknetzen) zum Vollzug anvertraut. § 16a TKG 2003 idF BGBl I Nr. 102/2011 enthielt auch eine Ermächtigung an das damals zuständige Bundesministerium für Verkehr, Innovation und Technologie sowie in Bezug auf Rundfunknetze an die KommAustria zum Erlass einer entsprechenden Verordnung, von der jedoch zunächst nicht Gebrauch gemacht wurde.

Im Jahr 2013 publizierte die bereits im Jahr 2004 eingerichtete Europäische Agentur für Netz- und Informationssicherheit („ENISA") zwei technische Richtlinien zur Handhabung der Berichtspflicht bei Sicherheitsvorfällen und zur Ergreifung von Sicherheitsmaßnahmen, die von den Regulierungsbehörden und den Betreibern in den folgenden Jahren als Richtschnur herangezogen wurden. Durch eine Novellierung wurde die Verordnungsermächtigung in § 16a TKG 2003 am 27.11.2015 hinsichtlich elektronischer Kommunikationsnetze und -dienste mit Ausnahme von Rundfunknetzen vom damaligen Bundesministerium für Verkehr, Innovation und Technologie auf die RTR-GmbH übertragen (BGBl I Nr. 134/2015).

Mit Inkrafttreten der RL 1148/20216 vom 6.07.2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union („NIS-RL", ABl L 194/1 vom 19.07.2016) wurden die Meldepflicht für Sicherheitsvorfälle und die Pflicht zur Gewährleistung bestimmter Mindestsicherheitsmaßnamen aus Art. 13 a/b Rahmen-RL auf zusätzliche Sektoren wie z. B. Strom, Gas, Öl, Verkehr (Luft/Bahn/Schifffahrt/ Straße), Banken, Gesundheit, Wasser sowie digitale Infrastruktur (also z. B. Internetknoten, DNS-Anbieter, Online-Marktplätze und Suchmaschinen) ausgeweitet; zusätzlich wurde zwischen Betreibern wesentlicher Dienste (Betreiber wichtiger bzw. wesentlicher Dienste, Anbieter digitaler Dienste) unterschieden.

Eine entscheidende Entwicklung in Bezug auf die Sicherheit elektronischer Kommunikationsnetze und -dienste ergab sich aus der Empfehlung der Europäischen Kommission 534/2019 zur Cybersicherheit der 5G-Netze (ABl L 88/42 vom 29.03.2019). Nach Ansicht der EK werden die 5G-Netze nach ihrer Einführung das Rückgrat eines breiten Spektrums von Diensten bilden, die für das Funktionieren des Binnenmarkts, die Aufrechterhaltung und Ausführung wichtiger gesellschaftlicher und wirtschaftlicher Funktionen — wie Energie, Verkehr, Bank- und Gesundheitswesen — sowie industrieller Steuerungssysteme unverzichtbar sind (ErwGr. 3). Aufgrund der Vernetzung und des transnationalen Charakters der Infrastrukturen, die dem digitalen Ökosystem zugrunde liegen, sowie des grenzübergreifenden Charakters der betreffenden Bedrohungen würden sich alle erheblichen Schwachstellen und/oder Cybersicherheitsvorfälle, die 5G-Netze in einem Mitgliedstaat betreffen, auf die Union als Ganzes auswirken. Deshalb sollten Maßnahmen zur Gewährleistung eines hohen gemeinsamen Cybersicherheitsniveaus der 5G-Netze getroffen werden (ErwGr. 4). Auf der Grundlage dieser Empfehlung hatten die Mitgliedstaaten bis zum 30.06.2019 eine Risikobewertung der 5G-Netzinfrastruktur durchzuführen, einschließlich der Bestimmung jener sicherheitskritischen Elemente, bei denen Sicherheitsvorfälle erhebliche negative Auswirkungen nach sich ziehen würden (Rz. 3). In Österreich erfolgte dies durch eine Ergänzung der Ergebnisse der Branchenrisikoanalyse im Telekommunikationsbereich (vgl. hierzu auch Kapitel 2.2.7). Die Ergebnisse hatten die Mitgliedstaaten der EK und der ENISA bis zum 15.07.2019 zu übermitteln (Rz. 9).

Darüber hinaus wurden die Mitgliedstaaten aufgefordert, ein gemeinsames Konzept zur Bewältigung der Cybersicherheitsrisiken in Bezug auf 5G-Netze zu entwickeln und bis zum 30. April 2019 diesbezügliche Arbeiten in einem eigenen Bereich der Kooperationsgruppe aufzunehmen (Rz. 7). Mit Unterstützung der Kommission und gemeinsam mit ENISA sollten die Mitgliedstaaten bis zum 1. Oktober 2019 eine gemeinsame Überprüfung der unionsweiten Exposition gegenüber Risiken im Zusammenhang mit Infrastrukturen, die dem digitalen Ökosystem, insbesondere 5G-Netzen, zugrunde liegen, durchführen (Rz. 11). Diese gemeinsame Risikobewertung („EU coordinated risk assessment of the cybersecurity of 5G networks") hat die NIS-Kooperationsgruppe (ein gemäß Art. 11 der Richtlinie 2016/1148 vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, sog. „NIS-RL" eingerichtetes Gremium) am 9.10.2019 veröffentlicht.

Die Empfehlung sah vor, auf der Grundlage national bewährter Verfahren und Maßnahmen bis zum 31. Dezember 2019 ein Instrumentarium mit geeigneten, wirksamen und angemessenen möglichen Risikomanagementmaßnahmen zur Minderung der auf nationaler und Unionsebene ermittelten Cybersicherheitsrisiken („Cybersicherheit von 5G-Netzen EU-Instrumentarium der Risikominderungsmaßnahmen") zu vereinbaren, um die Kommission bei der Ausarbeitung gemeinsamer Mindestanforderungen für die weitere Gewährleistung eines hohen Cybersicherheitsniveaus von 5G-Netzen in der gesamten Union zu unterstützen (Rz. 14). Diese sogenannte „EU 5G-Toolbox" (kurz „5G-Toolbox") hat die NIS-Kooperationsgruppe am 29.01.2020 veröffentlicht.

Die Toolbox stellt eine Reihe von Risiken im Zusammenhang mit 5G-Netzen (auf Basis der europäischen Risikoanalyse) sowie mögliche Abhilfemaßnahmen dar; jedoch bleibt es dem Mitgliedstaat überlassen, welche Maßnahmen für die nationale Situation als am besten geeignet angesehen und eingesetzt werden. Die Anwendung der Toolbox über die Europäische Union hinweg sollte bis 1.10.2020 evaluiert werden (Rz. 19). In dieser Toolbox wird zwischen strategischen, technischen und unterstützenden Maßnahmenempfehlungen unterschieden.

Die strategischen Maßnahmen umfassen

- Stärkung der Rolle der nationalen Behörden, um Sicherheitsmaßnahmen auf verschiedenen Ebenen einfordern zu können. Hier geht es u.a. auch um Einflussnahme von Drittstaaten auf die Sicherheit der 5G Supply Chain und der Abhängigkeit von einzelnen Herstellern
- Durchführung von Sicherheits-Audits bei Betreibern
- Erstellung eines Risiko-Profils von Herstellern inklusive der Möglichkeit der Anwendung von Restriktionen für Hochrisiko-Lieferanten bis hin zum Ausschluss
- Überprüfung des Einsatzes von Managed Service Providers (also der Auslagerung von Funktionen) und ggf. Anwendung von Restriktionen bei kritischen Funktionen
- Forcierung von Multi-Vendor-Strategien, um die Abhängigkeit von einem Hersteller zu reduzieren
- Aufbau eines 5G Ökosystems und Forcierung europäischer Hersteller, um die Abhängigkeit von Nicht-EU-Herstellern mittelfristig zu reduzieren
- Stärkung der Resilienz auf nationaler Ebene
- Ausbau der Diversität und der Kapazitäten in der EU für künftige Netztechnologien

Die technischen Maßnahmen umfassen

- Sicherstellung der Anwendung von Baseline Security Requirements in Netzdesign und -architektur
- Evaluierung der Anwendung von 5G Sicherheitsstandards bei MNOs
- Überprüfung von strikten Zugangskontrollen
- Erhöhung der Sicherheit bei virtualisierten Netzfunktionen
- Sicherheit bei 5G Netzmanagement, Betrieb und Monitoring
- Sicherstellung von Software-Integrität und Patch-Management
- Verbesserung der Sicherheit im Bestell-Prozess
- EU-Zertifizierung für 5G Netzkomponenten, Kundenequipment und Prozesse bei Herstellern
- EU-Zertifizierung für weitere Nicht-5G-Komponenten und -Dienste (wie Connected Devices und Cloud Services)
- Stärkung der physischen Sicherheit
- Stärkung von Resilienz- und Kontinuitätsplänen

Die unterstützenden Maßnahmen umfassen

- Überarbeitung oder Entwicklung von Leitfäden und Best Practices zur Netzsicherheit
- Stärkung des Potenzials für Tests und Audits auf nationaler und EU-Ebene,
- Gestaltung und Unterstützung der 5G-Standardisierung,
- Entwicklung von Leitfäden zur Umsetzung von Sicherheitsmaßnahmen in bestehenden 5G-Standards,
- Gewährleistung technischer und organisatorischer Sicherheitsmaßnahmen durch ein spezifisches EU-weites Zertifizierungsschema,
- Erfahrungsaustausch zur Umsetzung strategischer Maßnahmen, insbesondere des nationalen Rahmens zur Bewertung des Risikoprofils von Herstellern,
- Verbesserung der Koordination bei der Behandlung von Sicherheitsvorfällen und im Krisenmanagement,
- Überprüfung gegenseitiger Abhängigkeiten zwischen 5G-Netzen und anderen kritischen Diensten,
- Ausweitung von Mechanismen zur Kooperation, Koordination und zum Informationsaustausch,
- Berücksichtigung der Cybersicherheit in öffentlich geförderten Projekten zur 5G-Bereitstellung und Entwicklung von Leitfäden zur Umsetzung von Sicherheitsmaßnahmen in 5G-Standards.

Einen großen Teil dieser Empfehlungen hat die RTR-GmbH noch vor Inkrafttreten des TKG 2021 mit dem Erlass der Verordnung 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" bzw. „TK-NSiV 2020") am 4.07.2020 (BGBl I Nr. 301/2020) umgesetzt. Der in den strategischen Maßnahmen SM 03 und SM 04 der 5G-Toolbox geforderten Möglichkeit zur Anwendung von Restriktionen für Hochrisiko-Lieferanten (SM 03) bis hin zum Ausschluss sowie zur Überprüfung des Einsatzes von Managed Service Providern (also der Auslagerung von Funktionen) und ggf. Anwendung von Restriktionen bei kritischen Funktionen (SM 04) wurde in § 45 TKG 2021 Rechnung getragen. Eine allfällige bescheidmäßige Verhängung einschränkender Maßnahmen gegenüber potenziellen Hochrisikolieferanten oder risikobehafteten Managed Service Providern nach Erstattung eines diesbezüglichen Gutachtens durch den Netzsicherheitsbeirat obliegt dem Bundesminister für Finanzen.

04

Schlussbemerkungen

04 Schlussbemerkungen

Wir versichern, den Bericht nach bestem Wissen und Gewissen und aufgrund sorgfältiger Untersuchungen sowie der uns zur Verfügung stehenden Informationen erstellt zu haben.

Klaus M. Steinmaurer

Vorsitzender des Fachbeirates für Sicherheit in elektronischen Kommunikationsnetzen

05

Glossar

05 Glossar

3GPP	3G Partnership Project
ACS	Auto-Configuration Server
AI	Artificial Intelligence
AIT	Austrian Institute for Technology
APCIP	Österreichisches Programm zum Schutz kritischer Infrastrukturen
APT	Advanced Persistent Threat
BSI	Deutsches Bundesamt für Sicherheit in der Informationstechnik
BTS	Base Transceiver Station
CA	Carrier Aggregation
CC-MRA	Common Criteria Mutual Recognition Agreement
CDR	Call Detail Record
CEN/CENELEC	Comité Européen de Normalisation Électrotechnique
CERT	Computer Emergency Response Team
CERT-EU	Computer Emergency Response Team for the EU
COTS	Commercial off-the-shelf
CPE	Customer Premises Equipment
CRA	Cyber Resilience Act
CSA	Cyber Security Act
CSIRT	Computer Security Incident Response Team
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DC4EU	Digital Credentials for Europe Project
DDoS	Distributed Denial of Service
DSGVO	Datenschutz-Grundverordnung
ECCG	European Cybersecurity Certification Group
ECCG	European Cybersecurity Certification Group
EDA	European Defence Agency
EDT	Emerging Disruptive Technology
EECC	European Electronic Communications Code
EFTA	Europäische Freihandelsassoziation

eIDAS	Electronic Identification, Authentication and Trust Services
ENISA	Europäische Agentur für Netz- und Informationssicherheit
ETSI	European Telecommunications Standards Institute
EUCC	European Union Common Criteria Scheme
EUCS	European Union Cybersecurity Certification Scheme on Cloud Services
eUICC	embedded Universal Integrated Circuit Card
EUid	European Digital Identity
EWC	European Wallet Consortium
FBS	Fake Base Station
FFG	Forschungsförderungsgesellschaft
FIDO	Fast Identity Online
FMaG	Funkanlagen-Marktüberwachungs-Gesetz
FORTE	Österreichisches Verteidigungsforschungsprogramm
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GSMA	GSM Association
HLR	Home Location Register
HSM	Hardware Security Module
http	Hyper Text Transfer Protocol
IKDOK	Innerer Kreis der Operativen Koordinierungsstruktur
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
ISMS	Information Security Management System
ISPA	Internet Service Providers Austria
ITSEC	Information Technology Security Evaluation Criteria
KI	Künstliche Intelligenz
KIRAS	Österreichisches Förderungsprogramm für Sicherheitsforschung
LTE	Long Term Evolution
MEC	Multi Access Edge Computing
MNO	Mobile Network Operator
MSC	Mobile Switching Centre
MSP	Managed Service Provider
MVNO	Mobile Virtual Network Operator
NAS	Network Attached Storage
NATO	North Atlantic Treaty Organisation
NCCA	National Cybersecurity Certification Authority
NESAS	GSMA Network Equipment Security Assurance Scheme

NISG	NIS-Gesetz
NISV	NIS-Verordnung
OpKoord	Operative Koordinierungsstruktur
ÖSCS	Österreichische Strategie für Cybersicherheit
PUAS	Potentially Unwanted Accessible System
RAN	Radio Access Network
RAT	Radio Access Technology
RCS	Rich Communication Suite
RDP	Remote Desktop Protocol
RED	Radio Equipment Directive
RIPE NCC	Réseaux IP Européens Network Coordination Centre
RRC	Radio Resource Control
SAS	GSMA Security Accreditation Scheme
SBOM	Software Bill of Materials
SCCG	Stakeholder Cybersecurity Certification Group
SDN	Software Defined Networking
SIM	Subscriber Identification Module
SMS	Short Message Service
SMSC	SMS Centre
SNMP	Simple Network Monitoring Protocol
SOG-IS	Senior Officials Group – Information Systems Security
SS7	Signalisierungssystem Nr. 7
TCP	Transfer Control Protocol
TLP	Traffic Light Protocol
TSEC	Trusted Computer System Evaluation Criteria
UDP	User Datagram Protocol
UE	User Equipment
ULV	Umfassende Landesverteidigung
VDA	Vertrauensdiensteanbieter
VoLTE	Voice over LTE
WLAN	Wireless LAN
WTO	World Trade Organisation

Impressum

Eigentümerin, Herausgeberin und Verlegerin
Rundfunk und Telekom Regulierungs-GmbH
Mariahilfer Straße 77–79
A-1060 Wien,
T: +43 1 58058-0 | E: rtr@rtr.at
www.rtr.at

Für den Inhalt verantwortlich
Dr. Klaus M. Steinmaurer
Vorsitzender des Fachbeirates für Sicherheit in elektronischen Kommunikationsnetzen
Geschäftsführer Telekommunikation und Post, RTR-GmbH

Konzept, Text und Abbildungen
Rundfunk und Telekom Regulierungs-GmbH

Umsetzung und Layout
Mag. Johannes Bulgarini Werbeagentur
Gföhl 8, A-3053 Laaben

RTR

Rundfunk und Telekom Regulierungs-GmbH

Mariahilfer Straße 77–79 | A-1060 Wien | Österreich
T: +43 1 58058-0 | E: rtr@rtr.at

www.rtr.at