RTR AKTUELL
Telekommunikation und Post

RTR

TK 02/2024 VOM 19.07.2024

INHALT

Rundfunk und Telekom Regulierungs-GmbH (RTR)

Mariahilfer Straße 77–79
1060 Wien, Österreich
www.rtr.at

E: rtr@rtr.at

T: +43 1 58058 – 0

EDITORIAL

(©APA-Fotoservice/
Martin Hörmandinger)

Digitale Geschäftsmodelle leben von digitaler Kommunikation. Nur sichere digitale Kommunikation kann nachhaltig digitale Geschäftsmodelle sichern. Sichere Kommunikation beginnt bereits im Netz.

Sehr geehrte Damen und Herren!

Als ich vor fünf Jahren meine Tätigkeit als Geschäftsführer des Fachbereichs Telekommunikation und Post begonnen habe, war die Welt noch in Ordnung. Glaubten wir. Mit einer Pandemie und einen Krieg hier in Europa, später mit massiven geopolitischen und ökonomischen Auswirkungen, unglaublichen technologischen Entwicklungen in kürzester Zeit und einer Europäischen Kommission, die es ernst mit der von ihr ausgerufenen Digitalen Dekade gemeint hat, sieht diese Welt heute ganz anders aus. Kam das alles überraschend? Einiges sicher, aber dort, wo es den digitalen Raum betroffen hat, war vieles vorhersehbar.

In meinen Vorträgen über das Telekommunikationsrecht sage ich immer, der EECC (European Electronic Communication Code) war die letzte Richtlinie. Seither ist alles, was die digitale Welt betrifft, ein Act, also eine Verordnung, die direkt wirkt: Digital Markets Act, Digital Services Act, Artificial Intelligence Act, Data Act und Digital Governance Act. Aber das ist nicht ganz richtig. NIS II ist eine Richtlinie und die EU 5G Toolbox eine Empfehlung der Kommission. Und doch hängen alle diese Rechtsakte in gewisser Weise zusammen, allerdings scheint es, dass man sich beim Thema Sicherheit auf europäischer Ebene nicht ganz so viel zutraut, bzw. die Gemeinschaftsverträge hier die Möglichkeiten der Rechtsharmonisierung nicht so weit zulassen, wie in den vielen anderen Bereichen. In diesem für die Entwicklung und Sicherung einer digitalen Gesellschaft so wichtigen Bereich sind die nationalen Gesetzgeber gefordert und ist auch die nationale Regulierung weiterhin von Bedeutung. Wir haben das in der RTR in unserem Fachbereich bereits sehr bald erkannt und das Thema Sicherheit als Teil unserer Fachbereichsstrategie bereits 2019 verankert, als die ersten Diskussionen zu Netzausstattern aus Drittländern aufgekommen sind.

Aus diesem Grund widmet sich die aktuelle Ausgabe unseres Newsletters hier auch wieder diesem Thema, allerdings, und dabei darf ich auch das Leitthema unseres heurigen Salzburger Telekom-Forums hervorheben, aus dem Gesichtspunkt der „Sicheren Kommunikation“. Was verstehen wir unter sicherer Kommunikation? Nein, es geht heute nur mehr beschränkt um die Kommunikation zwischen Menschen. Es geht um die Interaktion von Menschen und Maschine, Maschine und Maschine und alle darauf aufbauenden Arten von Dienstleitungen, die damit ermöglicht werden. Auch elektronisches Payment ist digitale Kommunikation, genau so wie die Steuerung einer Drohne mit 5G Technologie. Unser gesamtes Wirtschaftssystem wird immer mehr von dieser Art der Kommunikation geprägt und damit das funktionieren kann, nämlich wirklich nachhaltig funktionieren kann, bedarf es einer sicheren Kommunikation. Diese Sicherheit zu erhalten, ist im Wesentlichen eine technische, aber auch eine regulatorische Herausforderung, die wahrscheinlich niemals zu Ende gebracht werden kann. Und diese Herausforderung beginnt immer im jeweiligen Telekommunikationsnetz. Egal, ob über mobile oder feste Technologie oder über Satelliten. Und es bedarf einer laufenden Abstimmung zwischen technologischen Möglichkeiten und dem,

EDITORIAL

was rechtlich und gesellschaftspolitisch erforderlich ist. Daran muss permanent gearbeitet werden und laufend der dahinter liegende regulatorische Rahmen aktualisiert werden. Genau an dieser Schnittstelle befinden wir uns heute auch in unserer Regulierungsarbeit, die mit dem Thema Netzsicherheit einen wichtigen neuen Schwerpunkt in den letzten Jahren bekommen hat und wo wir die Zeit genutzt haben, um entsprechende Expertise aufzubauen. Auch die Europäische Kommission hat diese Herausforderung erkannt und ist in ihrem aktuellen Weißbuch „How to master Europe's digital infrastructure needs?" darauf eingegangen. Sichere Netze sind für die Zukunft von uns allen die Basis und Grundlage für das Funktionieren all der bereits heute im täglichen Leben unverzichtbaren digitalen Dienstleistungen, für das Funktionieren von Wirtschaft und Gesellschaft. Und es ist noch kein Ende in Sicht. Es sei denn, das Vertrauen in die Sicherheit dieser Kommunikation geht verloren, was fatal wäre.

Das Thema Sicherheit im digitalen Raum und in Kommunikationsnetzen im Speziellen ist daher ein regulatorischer „Dauerbrenner", dem wir uns hier in dieser Ausgabe widmen und zu dem wir im Rahmen unseres Salzburger Telekom-Forums, zu dem ich recht herzlich einladen darf (der Hinweis auf das Programm dazu auch nachfolgend in dieser Ausgabe), mit unseren Vortragenden hoffentlich einige interessante Aspekte präsentieren dürfen.

In diesem Sinne wünsche ich Ihnen mit Sicherheit interessante Einblicke zu einem spannenden Themengebiet und natürlich auch noch einen schönen Sommer!

Beste Grüße

Ihr Klaus M. Steinmaurer
Geschäftsführer der RTR
Fachbereich Telekommunikation und Post

ZUM THEMA

©freepik.com

Telekom-Branchenrisikoanalyse 2023 erfolgreich abgeschlossen

(Kurt Reichinger)

Die Regulierungsbehörde RTR hat nach 2018 und 2020 erneut eine Risikoanalyse für den Telekommunikationssektor durchgeführt und diese vor kurzem erfolgreich abgeschlossen. Die regelmäßige Überarbeitung der Risikoanalyse ist notwendig, damit die Aktualität der identifizierten Risiken sowie der abgeleiteten Maßnahmen gewährleistet bleibt und ein hohes Schutzniveau im Sektor erhalten bleibt. Gleichzeitig wird sichergestellt, dass die Maßnahmenempfehlungen in regelmäßigen Abständen auf den Prüfstand gestellt und an die veränderten Rahmenbedingungen angepasst werden.

Der Fachbereich Telekommunikation und Post (TKP) der RTR ist eine jener Institutionen im nationalen Sicherheitsgefüge, die laufend dazu beiträgt, die Sicherheit und Integrität von Kommunikationsnetzen und-diensten in Österreich nachhaltig zu gewährleisten. Einen wichtigen Baustein stellt die sogenannte „Branchenrisikoanalyse“ dar, die die Regulierungsbehörde seit 2017 im Rahmen eines PPP-Prozesses gemeinsam mit den für die Sicherheit verantwortlichen Ressorts BKA, BMI, BMLVS und BMF, mit Betreibern und deren Interessenvertretung sowie mit Proponenten der Internet-Community durchführt und daraus gemeinsame Empfehlungen der Branche zur Risikominimierung ableitet. Die gute Nachricht vorweg: Die kürzlich veröffentlichte Branchenrisikoanalyse 2023 stellt der Sicherheit der österreichischen Telekommunikationsnetze erneut ein gutes Zeugnis aus.

Der Sicherheit und Integrität von Netzen und Diensten kommt in modernen Wissensgesellschaften mittlerweile eine immense Bedeutung zu. Kaum ein Lebensbereich kommt heute ohne die Notwendigkeit einer hohen Verfügbarkeit von Kommunikationsnetzen und Kommunikationsdiensten aus. Die ständige Verfügbarkeit von Telekommunikationsdiensten und Internet ist für die meisten von uns schon längst zur Selbstverständlichkeit geworden. Dieses Bewusstsein hinsichtlich der Bedeutung von sicheren und verfügbaren Netzen und Diensten spiegelt sich in einer Reihe von Initiativen auf europäischer und nationaler Ebene wider.

Von Beginn weg waren sich die beteiligten Expertinnen und Experten aus der Branche einig, dass neben den TK-spezifischen Risiken auch die Abhängigkeiten zu anderen Branchen, insbesondere zwischen Telekommunikation und Energieversorgung, zu berücksichtigen sind. Zudem haben sich seit der ersten Risikoanalyse im Jahr 2017 mit der Einführung von 5G und der damit einhergehenden Harmonisierung von Sicherheitsanforderungen, beispielsweise einer auf EU-Ebene koordinierten Risikobewertung der Cybersicherheit von 5G-Netzen, neue Aspekte für die Risikobewertung ergeben. Diese wurden in einer zweiten, im Jahr 2021 abgeschlossenen Phase der Branchenrisikoanalyse berücksichtigt. Die nunmehr dritte Risikoanalyse für den Sektor hat erneut anhand von mehreren Gefahrenkatalogen hunderte von potenziellen Gefahren identifiziert, die in weiterer Folge zu Einzelrisiken zusammengefasst und bewertet wurden.

ZUM THEMA

Der von der RTR initiierte und von der Branche durchwegs positiv aufgenommene partnerschaftliche Prozess der Branchenrisikoanalyse hat sich im Telekom-Sektor längst etabliert und trägt zu einer regelmäßigen gemeinsamen Befassung der Branche mit Sicherheitsfragen wesentlich bei. Umso erfreulicher ist es, dass sich dieses bewährte Instrument auch im Entwurf zum zukünftigen NIS-Gesetz wiederfindet. Damit bleibt gewährleistet, dass die involvierten Institutionen auch in Zukunft gemeinsam daran arbeiten, das hohe Sicherheitsniveau der österreichischen Kommunikationsnetze und -dienste auch im Fluss des technologischen Fortschritts zu wahren.

Die Vollversion des Abschlussberichts zur Branchenrisikoanalyse 2023 steht nur den am Prozess beteiligten Institutionen zur Verfügung; eine für die Öffentlichkeit freigegebene TLP:CLEAR-Version des Abschlussberichts steht auf der Website der RTR zum Download zur Verfügung: www.rtr.at/tkbranchenrisikoanalyse2023

©freepik.com

Aus der Tätigkeit des Fachbeirats für Sicherheit in elektronischen Kommunikationsnetzen

(Jan Weber)

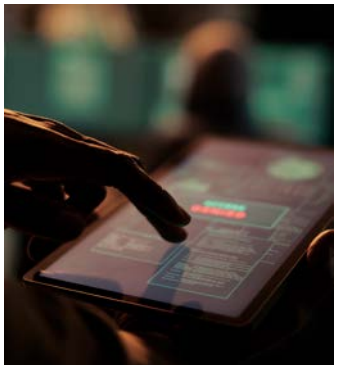
Mit Inkrafttreten des TKG 2021 wurde ein Fachbeirats für Sicherheit in elektronischen Kommunikationsnetzen eingerichtet. Dieser Fachbeirat ist ein Expertengremium, welches zwei- bis viermal jährlich zusammentritt und das für Telekommunikationsfragen (nicht: Digitalisierung) zuständige Bundesministerium – derzeit Bundesministerium für Finanzen – in Fragen der Netzsicherheit berät.

Vorsitzender des Fachbeirats ist RTR-Geschäftsführer des Fachbereichs Telekommunikation und Post, Dr. Klaus Steinmaurer. Die zwölf Mitglieder wurden von mehreren Bundesministerien, den Sozialpartnern und einschlägigen Fachorganisationen (Austrian Institute of Technology, kurz „AIT“, sowie Computer-Notfallteam, kurz „CERT“) benannt und von der Bundesregierung auf vier Jahre ad personam bestellt.

Hauptaufgaben des Fachbeirats sind neben der Beratung des Bundesfinanzministeriums zu allgemeinen Aspekten der Sicherheit für Netze der elektronischen Kommunikation die Erstellung von allfälligen Gutachten in Verfahren zur Einstufung eines Herstellers von Netzkomponenten als Hochrisikolieferant (jemand, der mit hoher Wahrscheinlichkeit die für ihn in der EU geltenden einschlägigen Normen, insbesondere im Bereich der Informationssicherheit und des Datenschutzes, nicht oder nicht ständig einzuhalten in der Lage ist). Darüber hinaus beobachtet der Fachbeirat die sicherheitstechnologische Entwicklung von Netzkomponenten und von Dienstleistungen für solche Netze in- und außerhalb der Europäischen Union und berichtet dem Bundesministerium zumindest einmal jährlich über seine diesbezüglichen Wahrnehmungen.

Der Fachbeirat trat am 21.11.2022 zu seiner konstituierenden Sitzung zusammen und hat im Jahr 2023 drei Sitzungen und im Jahr 2024 bislang zwei Sitzungen abgehalten. Neben der Erörterung der laufenden Entwicklung in Netzsicherheitsfragen war ein Großteil der Arbeit des Fachbeirats im Jahr 2023 der Erstellung des ersten Wahrnehmungsberichts für das Jahr 2023 gewidmet. Der Wahrnehmungsbericht besteht im Wesentlichen aus Wahrnehmungen der einzelnen Mitglieder, in denen diese die von ihnen in ihrem jeweiligen fachlichen Umfeld beobachteten Entwicklungen, Trends und Einschätzungen mitteilen und Empfehlungen für mögliche Maßnahmen zur Verbesserung der Sicherheit im Bereich der elektronischen Kommunikation aussprechen. Nach Einführung und Executive Summary behandeln die drei Hauptkapitel des Berichts die Themenbereiche „Recht und Politik", „Technologie und technische Risikoeinschätzung" sowie „Märkte und Verbraucher:innen". Darüber hinaus wird auf Einzelthemen wie etwa „Schwachstellen in Hard- und Software von Telekommunikationsnetzausstattung und Supply-Chain-Security", „Identifizierung und Authentifizierung in Kommunikationsnetzen" oder „Netzsicherheit und Zertifizierung" eingegangen.

Der Bericht wurde dem Bundesfinanzministerium im Frühsommer 2024 übergeben; dem Bundesfinanzministerium obliegt es nunmehr, zu entscheiden, ob der Bericht ganz oder teilweise veröffentlicht werden soll.



©freepik.com

Gefahr aus dem digitalen Raum: E-SIM-Swapping und Identitätsdiebstahl

(Gregor Goldbacher)

In der zunehmend vernetzten Welt des 21. Jahrhunderts sind Mobiltelefone nicht nur Kommunikationsmittel, sondern auch zentrale Knotenpunkte unserer digitalen Existenz. Während Fortschritte wie die Einführung der eSIM (embedded SIM) die Mobilität und Flexibilität erhöhen, öffnen sie gleichzeitig neue Türen für Cyberkriminelle. Eine besonders bedrohliche Methode ist das sogenannte „eSIM-Swapping". Diese Technik ist eng mit dem Identitätsdiebstahl verbunden und birgt erhebliche Risiken sowohl für Einzelpersonen als auch für Unternehmen.

Was ist eSIM-Swapping?

Das eSIM-Swapping ist eine Methode, bei der Kriminelle die Kontrolle über die Telefonnummer eines Opfers übernehmen, indem sie diese auf eine neue, von ihnen kontrollierte eSIM übertragen. Sobald sie die Kontrolle über die Nummer erlangt haben, können sie Zwei-Faktor-Authentifizierungen umgehen, die auf dem Empfang von SMS-Codes basieren. Dies ermöglicht es ihnen, unbefugt auf Bankkonten, soziale Medien und weitere persönliche Daten zuzugreifen, was bei den Opfern oft zu erheblichen finanziellen Schäden und emotionalen Belastungen führt.

Wie funktioniert der Angriff?

Der Angriff beginnt meist mit dem Sammeln von persönlichen Informationen. Dies kann durch Phishing, Social Engineering oder Datenlecks geschehen. Hat der Angreifer genügend Informationen über das Opfer gesammelt, kontaktiert er den Mobilfunkanbieter und weist sich mit der Identität des Opfers aus. Mit überzeugenden Argumenten und oft detaillierten persönlichen Daten überzeugt er den Kundenservice, die Telefonnummer auf eine neue eSIM zu übertragen. Von diesem Moment an erhält der Angreifer alle eingehenden Anrufe und SMS. Nach dem Kenntnisstand der RTR sind sich die Mobilfunkanbieter dieses Risikos bewusst und haben Maßnahmen ergriffen, dieses Risiko zu minimieren.

Die Bedeutung des Identitätsdiebstahls

Identitätsdiebstahl spielt beim eSIM-Swapping eine zentrale Rolle. Indem der Angreifer Identitätsdaten des Opfers wie Namen, Geburtsdatum und sogar Sozialversicherungsnummern stiehlt, kann er sich erfolgreich als das Opfer ausgeben. Die Kombination aus gestohlenen Identitätsinformationen und der Kontrolle über die Telefonnummer ermöglicht es den Kriminellen, Zugang zu diversen Konten und Diensten zu erhalten, die sich auf Telefonnummern als primäres Sicherheitsmerkmal stützen.

Schutzmaßnahmen für Einzelpersonen und Unternehmen

Der Schutz vor eSIM-Swapping erfordert sowohl technische als auch verhaltensbezogene Maßnahmen. Hier sind einige Empfehlungen:

1. Starke Passwörter und Multifaktor-Authentifizierung: Verwenden Sie für alle wichtigen Konten starke, einzigartige Passwörter und, wo möglich, Multifaktor-Authentifizierung, die nicht auf SMS basiert, wie etwa Authentifizierungs-Apps oder Hardware-Token.
2. Schutz persönlicher Informationen: Seien Sie vorsichtig, welche persönlichen Informationen Sie online teilen und wie Sie diese speichern. Social Media Konten sollten regelmäßig überprüft und entsprechende Privatsphäre-Einstellungen aktiviert werden.
3. Alarmierungsdienste: Nutzen Sie Dienste, die ungewöhnliche Aktivitäten in Ihren Konten überwachen und Sie im Verdachtsfall benachrichtigen.
4. Schulung und Sensibilisierung: Sowohl Privatpersonen als auch Mitarbeiter:innen in Unternehmen sollten sich regelmäßig weiterbilden bzw. informieren, um Phishing-Angriffe und Social Engineering-Versuche zu erkennen und abzuwehren.
5. Kontakt mit Mobilfunkanbietern: Nutzen Sie alle möglichen Sicherheitsfragen oder PINs bei Ihrem Mobilfunkanbieter, um eine unzulässige Verifizierung zu erschweren.

Was tun, wenn man Opfer von eSIM-Swapping wird?

Wenn Sie die Vermutung haben, dass jemand Ihre SIM-Karte „gekapert“ hat, kontaktieren Sie unverzüglich Ihren Mobilfunkanbieter. Dieser kann anhand seiner Systemeinträge den Verdacht überprüfen.

Wenn andere Dienste bereits betroffen sind, insbesondere Ihr Onlinebanking, veranlassen unverzüglich die notwendigen Sperren bzw. das Zurücksetzen der Zugangsparameter.
Schalten Sie auch gleich die Polizei ein. Je schneller diese tätig werden kann, desto wahrscheinlicher können von den Tätern bereits eingeleitete Aktionen (z.B. Banküberweisungen) unterbrochen werden.

Fazit:

E-SIM-Swapping und Identitätsdiebstahl sind ernsthafte Bedrohungen in unserer digitalen Welt. Der Schutz vor diesen Angriffen erfordert ein Bewusstsein für die Risiken und eine proaktive Herangehensweise an die Sicherheit. Durch die Kombination aus technologischen Lösungen und aufmerksamen Verhaltensweisen können wir die Chancen der Kriminellen verringern und unsere digitalen Identitäten besser schützen.

Bleiben Sie wachsam und schützen Sie, was Ihnen wichtig ist!

INTERNATIONALES

BEREC und die EU: internationale Neuigkeiten

(Gregor Gradnig)

Mit großer Freude waren wir Gastgeber des zweiten BEREC Contact Network Meetings (CN) des Jahres. Das CN setzt sich aus hochrangigen Vertreter:innen der BEREC-Mitglieder und -Beobachter zusammen. Hier werden beispielsweise die Dokumente abstimmungsfit gemacht, die beim BEREC-Plenum wenige Wochen später verabschiedet werden sollen. Die wichtigsten Dokumente und Neuigkeiten vom CN in Wien und dem anschließenden BEREC-Plenum in Jurmala, Lettland, von Anfang Juni stellen wir in diesem Beitrag vor.

©RTR/Nelli Wallner

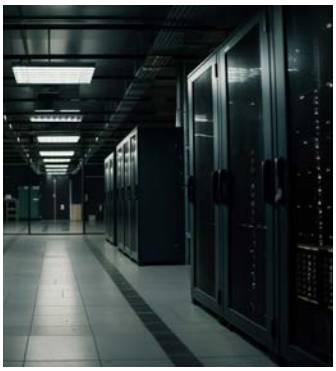
Abbildung 01: Hochrangige Vertreter:innen der europäischen Telekomregulierungsstellen machten beim BEREC Contact Network Meeting in Wien wichtige Dokumente abstimmungsfit für das nachfolgende BEREC-Plenum

Neue Direktorin für das BEREC Office

Seit 1. Juli hat das BEREC Office eine neue Direktorin. Verena Weber leitet nunmehr diese EU-Agentur, die die Arbeit von BEREC unterstützt. Sie folgt László Ignéczi, der die maximal mögliche Dauer der Leitung von zweimal fünf Jahren bereits ausgeschöpft hatte. Außerdem ist BEREC dabei zu wachsen: Die nationale Regulierungsbehörde der Republik Moldavien (ANRCETI) wird als ein weiterer „BEREC Participant without voting rights“ dazu kommen.

INTERNATIONALES

BEREC-Input zum White Paper zur Zukunft der digitalen Infrastruktur



©freepik.com

Die Europäische Kommission (EK) veröffentlichte im Februar ihren Vorschlag für ein White Paper namens „How to master Europe's digital infrastructure needs?". BEREC verabschiedete nun einen Input dazu.

Das White Paper selbst befasst sich mit den Trends und Herausforderungen im Bereich der digitalen Infrastruktur und schlägt unter Berücksichtigung der ermittelten Probleme zwölf mögliche Szenarien zur Bewältigung des Übergangs zu den digitalen Netzen der Zukunft vor. BERECs Input zielt darauf ab, über mehrere im White Paper enthaltene Begriffe und Vorschläge nachzudenken. Dabei stellt BEREC einerseits in einem „High-Level Input" den Kern seiner Standpunkte in kondensierter Form dar: BEREC analysiert Zielsetzung und Anwendungsbereich des aktuellen Rechtsrahmens für die elektronische Kommunikation und stellt Überlegungen zum Binnenmarkt, zur Marktregulierung sowie zum institutionellen Aufbau des Sektors an.

Andererseits legt BEREC diesem Dokument seine ausführliche Expertenmeinung bei. Darin konzentriert es sich auf die Analyse der skizzierten Vorschläge zu den technologischen Herausforderungen, dem Anwendungsbereich und den Zielen, der Allgemeinengenehmigung, dem Bereich der Frequenzen, der Kupferabschaltung, der Zugangsregulierung, dem Universaldienst, der Nachhaltigkeit sowie den sicheren und widerstandsfähigen digitalen Netzen.

Daneben weist BEREC auf die laufenden Arbeiten und aktuellen Ansichten hin: zur IP-Zusammenschaltung, zum Regime der Allgemeingenehmigung und über die bisherige Umsetzung der EECC-Bestimmungen über Co-Investments und Wholesale-only-Unternehmen (Lesen Sie mehr darüber in diesem Newsletterbeitrag).

Darüber hinaus ist BEREC an mehreren Aktivitäten beteiligt, die sich auf den breiteren digitalen Sektor beziehen, einschließlich der Umsetzung des Digital Markets Act und Untersuchungen in Bereichen wie den Investitionen der CAPs in ECS/ECN und dem Ausbau von Unterseekabeln. In seinem BEREC Action Plan for 2030 hat es seine Vision für BERECs Beitrag und Rolle im regulatorischen Umfeld der EU entwickelt, das für das digitale Zeitalter und den globalen Kontext geeignet ist.

BEREC stimmt den im Weißbuch angestellten Überlegungen zu, wonach sich die jüngsten Markt- und Technologietrends auf die elektronische Kommunikation und den digitalen Sektor auswirken und somit möglicherweise einschlägige regulatorische Anpassungen erforderlich machen. Es ist der Ansicht, dass solche Anpassungen im Rahmen einer ganzheitlichen Perspektive für die Regulierung der elektronischen Kommunikation im Lichte ihrer immer stärker werdenden Wechselwirkung mit dem breiten Korpus der europäischen Rechtsvorschriften im digitalen Bereich angegangen werden müssen.

Eine Überprüfung der Funktionsweise des Europäischen Kodex für elektronische Kommunikation (EECC) ist durch die Europäische Kommission bis Ende 2025 vorgesehen. Nach Ansicht von BEREC wäre es daher wichtig, zunächst eine gründliche Analyse der Funktionsweise der derzeit verfügbaren Maßnahmen durchzuführen, einschließlich einer Bewertung der Anforderungen, die aufgehoben werden könnten, bevor neue Vorschläge vorgelegt werden, die für den Sektor strukturell störend wirken und die wiederum langfristige Investitionen aus dem Gleichgewicht bringen könnten. BEREC weist auch darauf hin, dass das Weißbuch relevante Bereiche des derzeitigen Rechtsrahmens für die elektronische Kommunikation nicht abdeckt, wie z. B. das offene Internet und den Schutz der Endnutzer:innen, die aber unbedingt beibehalten werden müssen.

Was die Vorzüge der skizzierten Ideen angeht, so stimmt BEREC mit der Europäischen Kommission darin überein, dass die Verfügbarkeit einer hochwertigen, zuverlässigen, sicheren und nachhaltigen Konnektivität für alle und überall in der Union von zentraler Bedeutung ist, auch in ländlichen und abgelegenen Gebieten.

BEREC steht weiterhin zur Verfügung, um zu künftigen Initiativen der Europäischen Kommission beizutragen, die in seinen Zuständigkeitsbereich fallen, einschließlich der Governance des digitalen Sektors, wo es der Ansicht ist, dass unabhängige nationale Regulierungsbehörden, die mit den notwendigen sektoralen Aufgaben und Befugnissen ausgestattet sind, weiterhin eine zentrale Rolle spielen und eine ungerechtfertigte Zentralisierung des Prozesses vermieden werden sollte.

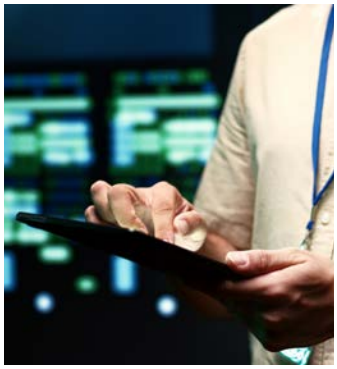
©freepik.com

Machine-to-Machine-Kommunikation und Roaming

Machine-to-Machine-Kommunikation (M2M) wird in zahlreichen Branchen zunehmend eingesetzt und wird voraussichtlich angesichts des technologischen Fortschritts künftig an Bedeutung gewinnen. M2M-Anwendungen dienen häufig der Standortverfolgung, der proaktiven Wartung und Statusabfragen von Industriemaschinen sowie der Meldung technischer Zwischenfälle. Vorbehaltlich der vorgesehenen Beschränkungen des dauerhaften Roamings fällt die M2M-Kommunikation in den Geltungsbereich der EU-Roamingverordnung mit den betreffenden Verpflichtungen zur Gewährung des Roamingvorleistungszugangs. Gerade eine Nutzung im dauerhaften Roaming ist jedoch bei zahlreichen M2M-Anwendungen ein häufiger Fall, da viele Geräte über längere Zeiträume mit einem ausländischen Netzwerk verbunden bleiben.

Im Hinblick auf die Überprüfung der Roamingverordnung im Jahr 2025 hat BEREC eine umfassende Analyse des Vorleistungsmarkts für M2M-Kommunikationsdienste durchgeführt, mit besonderem Augenmerk auf die Nutzung im dauerhaften Roaming. Der veröffentlichte Berichtsentwurf basiert auf einem Call for Input und auf den regelmäßig durch BEREC gesammelten Daten im Kontext des Roaming-Benchmark-Berichts. Unter den behandelten Themen sind die aktuellen Entwicklungen im Vorleistungsmarkt für M2M-Kommunikationsdienste, häufige Klauseln in den Roamingvereinbarungen sowie die von Stakeholdern wahrgenommenen Hindernisse und Herausforderungen. Der Berichtsentwurf ist nun für die öffentliche Konsultation freigegeben. Schriftliche Kommentare können bis zum 23. August 2024 eingereicht werden.

INTERNATIONALES



©freepik.com

Ökosystem der IP-Zusammenschaltung: „Evolution statt Revolution“

Die Zusammenschaltung von Netzwerken im Internet ist eine zentrale Vorleistung für die Bereitstellung von Breitbandzugängen und die Erbringung digitaler Dienste. Sie ermöglicht den Austausch von Daten zwischen Netzwerken auf Basis des Internet Protocol (IP).

Bereits 2012 und 2017 zeigte BEREC relevante technische und ökomische Entwicklungen sowie rechtliche Rahmenbedingungen im Bereich der IP-Zusammenschaltung in Berichten auf. In ihrem jüngsten Berichtsentwurf bewerteten BEREC-Expert:innen seitherige Marktentwicklungen. Dieser stellt auch seine früheren Schlussfolgerungen auf den Prüfstand.

Der Entwurf des Berichts stellt fest, dass die Entwicklungen auf den Märkten der IP-Zusammenschaltung weiterhin eher als Evolution statt Revolution beschrieben werden können. Der Datenverkehr steigt, Wettbewerb und technologischer Fortschritt ermöglichen jedoch, Änderungen in der Nutzung des Internetanschlusses sowie in der Nachfrage nach Inhalten im Ökosystem der IP-Zusammenschaltung erfolgreich zu integrieren.

Das Ökosystem ist weiterhin von Wettbewerb geprägt, auch wenn seit 2017 einzelne Konflikte zwischen Marktteilnehmern zu beobachten waren. BEREC wird Konflikte in diesem Bereich in Zukunft verfolgen. Es ermöglicht nun, in einer öffentlichen Konsultation Beiträge zu dem Berichtsentwurf abzugeben. Die Stakeholder haben dazu bis zum 26. Juli 2024 Zeit. Nach der Konsultation werden die eingegangenen Stellungnahmen eingearbeitet und der finale Bericht zum Ökosystem der IP-Zusammenschaltung Ende 2024 veröffentlicht.

Wirksamkeit der EU-Allgemeingenehmigungsregelung

Nachdem BEREC Informationen von den nationalen Regulierungsbehörden eingeholt hat, sammelt es nun Daten von Interessengruppen, um die Wirksamkeit der derzeitigen EU-Allgemeingenehmigungsregelung und ihre Auswirkungen auf den Binnenmarkt zu bewerten. Der Europäischen Kodex für elektronische Kommunikation (EECC) verlangt alle drei Jahre eine Stellungnahme zur Umsetzung der Allgemeingenehmigungsregelung und ihrer Funktionsweise auf nationaler und europäischer Ebene.

Nach Erhalt der BEREC-Stellungnahme kann die Europäische Kommission einen Bericht über die Anwendung der Bestimmungen veröffentlichen. Sie kann auch Änderungen der Rechtsvorschriften vorschlagen, um etwaige Hindernisse für das reibungslose Funktionieren des Binnenmarktes zu beseitigen. BEREC verabschiedete bereits im Dezember 2021 eine Stellungnahme zu diesem Thema. Der nun zweite Entwurf wird bis zum 26. Juli 2024 öffentlich konsultiert.

INTERNATIONALES

Externer BEREC-Workshop zur Ex-ante-Regulierung

©freepik.com

Zum Austausch von Meinungen und Best Practices bei der Anwendung der neuen Ex-ante-Regulierungsinstrumente aus dem EECC hielt BEREC einen öffentlichen Workshop in Bezug auf Ko-Investitionen, Verpflichtungserklärungen, Wholesale-only-Unternehmen sowie die Auswirkungen von kommerziellen Vereinbarungen über den Netzzugang ab.

Die Redner:innen vertraten verschiedene Betreiber (sowohl etablierte Unternehmen als auch Zugangssuchende) aus den Ländern, in denen einige Erfahrungen gesammelt wurden mit der Anwendung der in Betracht gezogenen alternativen Abhilfemaßnahmen; nämlich Italien, Dänemark, Irland, Finnland und Frankreich, sowie aus Ländern, in denen die Berücksichtigung bestehender kommerzieller Vereinbarungen zur (teilweisen) Deregulierung der Märkte führte, wie in Österreich (A1 Telekom Austria) und Zypern. Es zeigte sich, dass es bisher nur wenige Erfahrungen mit diesen neuen Regulierungsoptionen gibt und es daher meist noch zu früh war, Schlussfolgerungen über die Wirksamkeit dieser Instrumente zu ziehen. Die Zusammenfassung des Workshops finden Sie auf der BEREC Website.

Für September 2024 ist ein weiterer interner BEREC-Workshop mit Vorträgen der nationalen Regulierungsbehörden geplant, um die Ansichten und Meinungen zu prüfen, die während dieses externen Workshops im April geäußert wurden. Die dabei gezogenen Schlussfolgerungen könnten schließlich in die Bewertung der Wirksamkeit der betreffenden Maßnahmen des EECC einfließen. Sie könnten auch zu einer Neubewertung der BEREC Guidelines für Co-Investments beitragen, falls dies als notwendig erachtet wird.

Öffentliche Konsultation der RTR zum Entwurf der 1. Novelle der Post-Erhebungs-Verordnung 2019 (PEV 2019)

Die Bestimmung des § 52 Postmarktgesetz (PMG) ermächtigt die Rundfunk und Telekom Regulierungs- GmbH (RTR), für die Beobachtung und Überwachung der Markt- und Wettbewerbsentwicklung auf dem Gebiet des Postwesens die Erstellung von Statistiken anzuordnen. 2019 wurde daher von der RTR die Post-Erhebungs-Verordnung (PEV 2019) erlassen.

In den letzten Jahren hat sich gezeigt, dass im Hinblick auf Änderungen des Postmarktes sowie geänderte Anforderungen bei Berichts- und Auskunftspflichten auf EU-Ebene eine Novellierung der Post-Erhebungs-Verordnung geboten erscheint. Hinzu kommen Anregungen des Rechnungshofes im Zuge der Überprüfung des Universaldienstes sowie die Notwendigkeit, in Zusammenhang mit der Handhabung von Beschwerden zu Postdiensteanbietern über bessere Informations- und Entscheidungsgrundlagen zu verfügen.

Die vorliegende Novelle sieht daher neben gewissen Erleichterungen in Bezug auf die Frequenz der Erhebungen zusätzliche Datenabfragen hinsichtlich Erstzustellquote, Paketboxen, verloren gegangenen Sendungen, Anzahl von Beschwerden und Kennzahlen zu Nachhaltigkeit vor.

Der Entwurf der 1. Novelle der Post-Erhebungs-Verordnung 2019 (PEV 2019) wird bis 7. August 2024 konsultiert. Detaillierte Infomationen zur Konsultation sind unter https://www.rtr.at/TKP/aktuelles/veroeffentlichungen/veroeffentlichungen/konsultationen/konsultation_1nov_pev2019.de.html veröffentlicht.

IN EIGENER SACHE

Publikationen

Folgende Publikationen wurden in den letzten Wochen auf der Website der RTR veröffentlicht:

Kommunikationsbericht 2023

Der Kommunikationsbericht 2023 stellt die Aufgaben und Tätigkeiten der in Österreich für die Regulierung der Medien-, Post- und Telekommunikationsmärkte zuständigen Einrichtungen Kommunikationsbehörde Austria (KommAustria), Post-Control-Kommission (PCK), Telekom-Control-Kommission (TKK) sowie der Rundfunk und Telekom Regulierungs-GmbH (RTR) für das Berichtsjahr 2023 dar und dient der umfassenden Transparenz über die national wie international geleistete Arbeit.

Der Bericht ist in Deutsch und Englisch unter www.rtr.at/rtr/publikationen/Kommunikationsbericht/KBericht_2023.de.html veröffentlicht.

Netzneutralitätsbericht 2024

Der (mittlerweile) achte Netzneutralitätsbericht der RTR zur Offenheit des Internets in Österreich bietet der interessierten Öffentlichkeit für den Zeitraum April 2023 bis Mai 2024 einen umfassenden Überblick über die Aktivitäten zur Sicherung der Netzneutralität in Österreich.

Der Netzneutralitätsbericht 2024, verfügbar in Deutsch und Englisch, ist auf der Website der RTR unter www.rtr.at/nnbericht2024 veröffentlicht.

RTR Telekom Monitor Jahresbericht 2023

Der RTR Telekom Monitor Jahresbericht basiert auf umfangreichen Marktdaten zu Mobilfunk, Breitband, Festnetz, Mietleitungen und Glasfaser und bietet Jahresvergleiche sowie Analysen auf Quartalsbasis bis inklusive 4. Quartal 2023.

Der Jahresbericht (interaktive Grafiken und PDF-Dokument) ist unter https://www.rtr.at/telekom-monitor-2023 veröffentlicht, die Daten zu den Grafiken sind im Open Data Bereich unter www.rtr.at/rtr/service/opendata/OpenData.de.html veröffentlicht.

IN EIGENER SACHE

RTR Post Monitor Jahresbericht 2023

Der RTR Post Monitor Jahresbericht enthält Daten zum österreichischen Postmarkt sowie internationale Vergleiche. Der Jahresbericht (interaktive Grafiken und PDF-Dokument) ist unter www.rtr.at/post-monitor-2023 veröffentlicht, die Daten zu den Grafiken sind im Open Data Bereich unter www.rtr.at/rtr/service/opendata/OpenData.de.html veröffentlicht.

Veranstaltungshinweis

25. Salzburger Telekom-Forum

„Sichere elektronische Kommunikation im Spannungsfeld zwischen Technik und Recht" – so lautet das Motto des heurigen Salzburger Telekom-Forums. Die hochkarätig besetzte Fachtagung, an der jedes Jahr mehr als 100 Expertinnen und Experten teilnehmen, findet am 20. und 21. August auf der Edmundsburg statt.

Das Programm ist unter https://www.rtr.at/TKP/aktuelles/veranstaltungen/veranstaltungen/veranstaltungen_2024/Programm_2024.pdf abrufbar.

Da die Anzahl der Plätze im Tagungsraum der Edmundsburg begrenzt ist, ist eine Teilnahme an der Fachtagung nur nach Anmeldung (bis 8. August unter veranstaltungen@rtr.at) und nach Erhalt einer Bestätigung möglich.