RTR AKTUELL
Telekommunikation und Post

TK 02/2022 VOM 01.07.2022

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
F: +43 1 58058 – 9191

EDITORIAL

(©APA-Fotoservice/Martin Hörmandinger)

„Denn, wie ihr wisst, war Sicherheit des Menschen Erbfeind jederzeit Macbeth III, 5. (Hekate)“

Liebe Leser:innen!

Wie diese Worte in Zeiten, wie wir sie jetzt erleben, sich doch bewahrheiten. Wer hätte gedacht, dass eine Pandemie nun schon mehr als zwei Jahre die Welt in Schach hält, wer hätte aber auch gedacht, dass es ganz nahe an den Grenzen Europas zum Krieg kommt und wir nicht wissen, ob im kommenden Winter unsere Heizungen funktionieren. Ob unsere Industrie genügend Energie zur Verfügung hat. Was passiert mit all den Annehmlichkeiten, an die wir uns gewöhnt haben. Und vor allem was passiert mit unserer Umwelt.

Wir haben uns schon sehr sicher gefühlt, seit der Eiserne Vorhang und die Berliner Mauer 1989 gefallen sind. Seit Beginn des 21. Jahrhunderts konnte es eigentlich nur mehr besser werden. Fortschritt durch Digitalisierung und Wohlstand durch Handel. Aber das hatten wir ja gut hundert Jahre vorher auch schon einmal. Einfach nachzulesen im ersten Kapitel von Stefan Zweigs Autobiografie „Die Welt von gestern“, das die sinnige Überschrift trägt, „Die Welt der Sicherheit“. Alles was man über Sicherheit daher sagen kann, dass sie immer nur trügerisch ist, wenn man allzu sehr auf sie vertraut. Wir sollten uns also bewusst sein, dass wir in einer „Welt der Unsicherheit“ leben. Und diese Unsicherheit ist gerade dort, wo sich unser analoges Leben mit dem digitalen verbindet, zumeist größer als zuvor, wenn man sich nicht entsprechend vor potenziellen und realen Angriffen schützt. Vor allem im digitalen Leben gilt, am sichersten ist, wer sich unsicher fühlt. Nur so ist es möglich, Schwachstellen zu schließen, bevor andere sie ausnutzen können. Netzinfrastruktur mit allem, was danach kommt, bildet heute das zentrale Nervensystem unseres wirtschaftlichen und gesellschaftlichen Lebens. Dieses Nervensystem ist sehr verletzlich.

Netzsicherheit oder besser Netzunsicherheit und was man dagegen machen kann, ist daher das zentrale Thema in unserem „Nerven Newsletter“. Netzunsicherheit hat ganz unterschiedliche Auswirkungen und Angriffspunkte. Sind es auf der einen Seite geopolitische strategische Fragen, betrifft Sicherheit im Netz natürlich auch die ganz persönliche Privatsphäre von jedem und jeder einzelnen von uns allen. Im nachfolgenden Interview mit Vinzenz Heußler, dem Leiter des NIS Büros im Bundeskanzleramt, erfahren Sie mehr darüber, was es mit den neuen Regelungen von NIS 2 auf sich hat und wo der weitere Weg hingeht. Im neuen TKG wurde ein sogenannter Netzsicherheitsbeirat zur Beratung der Bundesregierung eingerichtet, um die Grundlagen dafür zu schaffen, im Einzelfall rechtssicher und rechtsstaatlich Entscheidungen über in Netzen zu verbauende Netzwerkkomponenten treffen zu können. Auch wollen wir uns ganz generell einmal der Frage widmen, was wir denn so unter Netzsicherheit verstehen dürfen. Dabei versuchen wir auch auf die Branchenrisikoanalyse, die von der RTR seit einigen Jahren gemacht wird, näher einzugehen. Auch die Risiken von klassischem Cybercrime, die vor allem private

EDITORIAL

Nutzer:innen treffen können, wie beispielsweise zuletzt die sogenannten FluBot-SMS, sollen bei unserer Analyse in diesem Newsletter nicht zu kurz kommen.

Daneben finden Sie in diesem Newsletter aber auch noch die neuesten Themen aus dem letzten BEREC-Plenum und einen Beitrag zu unserer zuletzt veröffentlichten Studie über Wechselbarrieren.

Und insofern ist eines sicher. Dieser Newsletter ist auf jeden Fall als spannende Sommerlektüre geeignet. Ich wünsche trotz der einleitend vielleicht etwas nachdenklich gestimmten Worte Ihnen allen einen schönen Sommer und eine gute Zeit.

Aber nehmen Sie das Thema Sicherheit auch in Zukunft ernst. Vor allem die digitale Welt ist kein Ponyhof.

In diesem Sinne verbleibe ich Ihr

Klaus M. Steinmaurer
Geschäftsführer der RTR
Fachbereich Telekommunikation und Post

NETZSICHERHEIT

Netzsicherheitsbeirat – Hersteller stärker im Fokus

Das im November vergangenen Jahres in Kraft getretene Telekommunikationsgesetz (TKG 2021) wartet im Bereich Netzsicherheit mit einer wesentlichen Neuerung auf. Galt der Schwerpunkt der gesetzlichen Auflagen im TKG bislang vorrangig den Netzbetreibern und Diensteanbietern, so sollen nunmehr auch die Hersteller von Netzequipment stärker in die Pflicht genommen werden. Eine tragende Rolle kommt einem neu einzurichtenden „Fachbeirat für Sicherheit in elektronischen Kommunikationsnetzen“ zu.

Die Entwicklung hatte sich schon mit der auf europäischer Ebene erarbeiteten und im Jahr 2020 veröffentlichten Cybersecurity Toolbox angekündigt, einem Kompendium von Empfehlungen für die EU-Mitgliedsstaaten im Umgang mit Sicherheitsaspekten bei Roll-Out und Betrieb von 5G-Netzen. In den Dokumenten wird auch die Verantwortung von Herstellern thematisiert, die sich nun – losgelöst von 5G und technologieagnostisch – im TKG 2021 widerspiegelt. Kann ein Hersteller gewisse Kriterien, insbesondere im Bereich der Informationssicherheit und des Datenschutzes, nicht oder nicht ständig erfüllen, so besteht nunmehr die Möglichkeit, den betreffenden Hersteller als sogenannten „Hochrisikolieferanten“ einzustufen und in seinen Möglichkeiten am österreichischen Markt einzuschränken.

Und hier kommt der eingangs erwähnte Netzsicherheitsbeirat ins Spiel. Zieht das zuständige Bundesministerium (derzeit BMLRT, zukünftig BMF) aus Gründen der nationalen Sicherheit die Einstufung eines Herstellers von Komponenten eines elektronischen Kommunikationsnetzes oder eines Bereitstellers von Dienstleistungen für solche Netze als Hochrisikolieferant in Erwägung, so hat sie vorher den Netzsicherheitsbeirat zu konsultieren, welcher binnen 12 Wochen ein Gutachten zu erstellen und an das Bundesministerium zu übermitteln hat. Eine allfällige Einstufung als Hochriskolieferant hätte seitens des verantwortlichen Bundesministeriums mittels Bescheid zu erfolgen, wobei das Gutachten des Netzsicherheitsbeirates im Ermittlungsverfahren zu berücksichtigen ist.

Drei Aspekte werden als wesentlich für die Beurteilung eines Herstellers herangezogen:
(1) Mängel in der Qualität der Produkte sowie bei den Cybersicherheitspraktiken des Herstellers, wobei insbesondere die Kontrolle über die eigene Zulieferkette und die Beachtung einschlägiger Sicherheitspraktiken und Schutzziele der Informationssicherheit (Vertraulichkeit, Verfügbarkeit und Integrität) genannt werden.
(2) Sicherheits- oder Datenschutz-Übereinkommen zwischen der EU und dem Sitzstaat des Lieferanten, sofern es sich dabei um einen Drittstaat handelt, wobei es insbesondere um die Vermeidung einer rechtswidrigen Übertragung von Benutzerdaten in Länder außerhalb der EU geht.
(3) Ausreichende Fähigkeit des Herstellers zur Gewährleistung einer durchgängigen Versorgung.

Neben der Erstellung von Gutachten im Zusammenhang mit einer Einstufung als Hochrisikolieferant, kommt dem Netzsicherheitsfachbeirat auch die Aufgabe der Beratung des zuständigen Bundesministeriums zu allgemeinen Aspekten der Sicherheit für Netze der elektronischen Kommunikation zu. Zu diesem Zwecke hat der Fachbeirat jährlich einen Wahrnehmungsbericht zu erstellen, der sich insbesondere der sicherheitstechnologischen Entwicklung von Netzkomponenten und von Dienstleistungen für Netze in- und außerhalb der Europäischen Union widmen soll.

Personell wird sich der Fachbeirat aus Expertinnen und Experten der heimischen TK-Branche zusammensetzen, wobei sich der institutionelle Bogen von Bundesministerien über Interessenvertretungen bis zur Forschung und CERT.at spannt. Die RTR-GmbH (Fachbereich Telekommunikation und Post) übernimmt den Vorsitz im Fachbeirat, führt dessen Geschäfte und nimmt die Aufgaben einer Geschäftsstelle wahr. Mit einer Konstituierung des Fachbeirates ist in den nächsten Monaten zu rechnen.

Telekommunikationsbranche und Energiewirtschaft kooperieren bei Branchenrisikoanalysen

Seit 2017 werden unter Federführung der RTR sogenannte „Branchenrisikoanalysen“ für die Telekommunikationsbranche durchgeführt. Dabei handelt es sich um einen zyklischen Prozess, bei dem im Abstand von jeweils zwei bis drei Jahren Risiken identifiziert und bewertet werden, die allen Betreibern elektronischer Kommunikationsnetze oder -dienste gemein sind bzw. über den einzelnen Betreiber hinausgehen. Bislang wurden Berichte über die Branchenrisikoanalysen 2018 und 2020 veröffentlicht, darüber hinaus ein Bericht aus dem Jahr 2019 über spezifische Risiken für die Cybersicherheit von 5G-Netzen.[1] Solche Risikoanalysen werden auf Basis der Österreichischen Cybersicherheitsstrategie (ÖSCS) und des Österreichischen Programms zum Schutz kritischer Infrastrukturen (APCIP) für verschiedene Sektoren durchgeführt, u.a. auch für die Energiewirtschaft und die Finanzbranche.

Die Risikoanalysen umfassen auch Risiken, die nicht charakteristisch für eine bestimmte Branche sind, sondern mehrere Sektoren oder die Gesellschaft insgesamt betreffen. Überdies existieren zwischen verschiedenen Branchen Abhängigkeiten, sodass sich Beeinträchtigungen in einer Branche auf andere Branchen auswirken. In solchen Fällen spricht man von Kaskadeneffekten. Diese treten in besonderem Maß zwischen der Telekommunikationsbranche und der Energiewirtschaft auf.

Beispielsweise führen Stromausfälle innerhalb weniger Stunden zu Ausfällen von Basisstationen. Teile der Kommunikationsinfrastruktur, die sich in Rechenzentren befinden, können zwar bei guter Notstromversorgung länger in Betrieb gehalten werden, aber kaum länger als wenige Tage. Die Verfügbarkeit von

[1] https://www.rtr.at/TKP/was_wir_tun/telekommunikation/anbieterservice/netzsicherheit/Risikoanalysen.de.html.

Kommunikationsnetzen, insbesondere Mobilfunknetzen, kann also nur bei funktionierender Stromversorgung gewährleistet werden. Umgekehrt hängt auch die Stromversorgung von der Kommunikationsinfrastruktur ab, wenngleich wesentliche Einrichtungen auf nationaler und regionaler Ebene hinsichtlich der elektronischen Kommunikation autark sind.

Zur Behandlung branchenübergreifender Risiken arbeiten die Telekommunikationsbranche und die Energiewirtschaft seit zwei Jahren zusammen. Als besonderer Vorteil hat sich dabei erwiesen, dass die Risikoanalysen beider Sektoren auf derselben Norm beruhen und daher einander methodisch, auch in der Granularität und der Bewertung der erfassten Risiken, sehr ähnlich sind. In mittlerweile fünf mehrstündigen Workshops, an denen Vertreter beider Sektoren unter der Koordination von RTR und E-Control teilnahmen, wurden eine Reihe gemeinsamer Risiken und überdies mehrere Risiken mit Kaskadenpotenzial identifiziert. Im nächsten Schritt sollen risikomindernde Maßnahmen untersucht werden. Für gemeinsame Risiken genügt es, die von beiden Sektoren bereits festgelegten Maßnahmen zu vergleichen und eventuell voneinander zu lernen. Manche Maßnahmen zur Minderung von Risiken mit Kaskadenpotenzial bedürfen hingegen einer Abstimmung zwischen den beiden Sektoren, die durch die institutionelle Zusammenarbeit gefördert wird.

Die Kooperation zwischen Telekommunikationsbranche und Energiewirtschaft bei der Identifizierung gemeinsamer Risiken und Kaskadeneffekte hat sich schon in der kurzen Zeit ihres Bestehens bewährt. In Zukunft könnte sie sich auch zu einem Modell für die branchenübergreifende Betrachtung von Risikoanalysen entwickeln.

NIS 2 – alles aus einem Guss?

Im Jahr 2016 wurde mit der NIS-Richtlinie[2] ein rechtlicher Rahmen für die Netz- und Informationssicherheit bei Betreibern wesentlicher Dienste in den Sektoren Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasserlieferung und -versorgung sowie digitale Infrastruktur geschaffen. Mit dieser Richtlinie, die mit dem 2018 beschlossenen Netz- und Informationssystemsicherheitsgesetz[3] in österreichisches Recht umgesetzt wurde, wurde ein wichtiger Meilenstein für ein höheres Sicherheitsniveau von Netz- und Informationssystemen in der EU erreicht. Insbesondere haben die Mitgliedstaaten der EU (und in weiterer Folge auch die EWR/EFTA-Staaten) zu gewährleisten, dass Betreiber wesentlicher Dienste technische und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der von ihnen genutzten Netz- und Informationssysteme zu bewältigen und die Auswirkungen von Sicherheitsverletzungen so gering wie möglich zu halten. Weiters haben die Mitgliedstaaten zu gewährleisten, dass Betreiber wesentlicher Dienste der

[2] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl. L 194, 19.7.2016, S. 1–30.
[3] Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG), BGBl. I Nr. 111/2018.

zuständigen Behörde oder dem Computer-Notfallteam (CSIRT) Sicherheitsvorfälle mit erheblichen Auswirkungen unverzüglich melden. Die Richtlinie nimmt aber hinsichtlich dieser Pflichten zwei Bereiche explizit aus, in denen vergleichbare Vorschriften bereits zuvor existierten: Vertrauensdienste (z. B. Dienste zur Ausstellung von Zertifikaten für elektronische Signaturen) gemäß eIDAS-Verordnung[4] und elektronische Kommunikationsnetze und -dienste gemäß der früheren Rahmenrichtlinie[5] bzw. des derzeitigen EECC[6].

Ziel der NIS-Richtlinie war auch, einen einheitlichen organisatorischen Rahmen für die Behandlung von Angelegenheiten der Netz- und Informationssicherheit zu schaffen. Beispielsweise wurden auf Unionsebene ein CSIRTs-Netzwerk und eine Kooperationsgruppe eingerichtet, in der die zuständigen Behörden gemeinsam handeln. Zuständigkeiten innerhalb von Mitgliedstaaten können zwar auf verschiedene Behörden verteilt sein, jeder Mitgliedstaat hat aber eine für die Sicherheit von Netz- und Informationssystemen zuständige nationale Anlaufstelle zu benennen. Als auf europäischer Ebene ab 2019 die Cybersicherheit von 5G-Netzen zunehmend thematisiert wurde, zeigte sich eine gewisse Schwäche des Rechtsrahmens: Für die Sicherheit elektronischer Kommunikationsnetze und -dienste waren zwar in den meisten Mitgliedstaaten die nationalen Regulierungsbehörden zuständig, behandelt wurde das Thema aber in der Kooperationsgruppe, in der die nationalen Regulierungsbehörden selbst nicht vertreten sind, sondern bestenfalls von den für Netz- und Informationssicherheit zuständigen Behörden beigezogen wurden. Und nicht überall klappte die Zusammenarbeit zwischen NIS-Behörde und Regulierungsbehörde auf nationaler Ebene so reibungslos wie hierzulande zwischen BKA und RTR.

Mit der von der Europäischen Kommission im Dezember 2020 vorgeschlagenen NIS-2-Richtlinie7 soll dieses Manko behoben werden, indem auch Vertrauensdienste sowie elektronische Kommunikationsnetze und -dienste in den Anwendungsbereich dieser Richtlinie fallen. Somit sollen auch die Sicherheitserfordernisse der eIDAS-Verordnung und des EECC durch jene der NIS-2-Richtlinie ersetzt werden. Die Gesetzgebung ist zwar noch nicht abgeschlossen, aber im Mai 2022 haben sich der Rat und das Europäische Parlament über den Inhalt der Richtlinie (vorläufig) geeinigt.

4 Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, ABl. L 257 vom 28.8.2014, S. 73–114.
5 Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie), ABl. L 108 vom 24.4.2002, S. 33–50, in der Fassung der Richtlinie 2009/140/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/21/EG über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste, der Richtlinie 2002/19/EG über den Zugang zu elektronischen Kommunikationsnetzen und zugehörigen Einrichtungen sowie deren Zusammenschaltung und der Richtlinie 2002/20/EG über die Genehmigung elektronischer Kommunikationsnetze und -dienste, ABl. L 337 vom 18.12.2009, S. 37–69.
6 Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation, ABl. L 321 vom 17.12.2018, S. 36–214.
7 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148, COM(2020) 823 final.

Sofern keine überraschenden Entwicklungen eintreten, kann mit einer Kundmachung der Richtlinie in einigen Monaten gerechnet werden.

Die Ausweitung des Anwendungsbereichs auf Normadressaten, die bisher von anderen Vorschriften umfasst waren, erweist sich in verschiedener Hinsicht als herausfordernd: Im Laufe der letzten Jahrzehnte wurden sowohl in der elektronischen Kommunikation als auch bei Vertrauensdiensten Vorgangsweisen etabliert und weiterentwickelt, die sich bewährt haben – gerade im Bereich der zu ergreifenden Sicherheitsmaßnahmen und der zu meldenden Sicherheitsverletzungen. Eine radikale Änderung dieser Vorgangsweisen könnte zumindest vorübergehend zu einer Schwächung der Cybersicherheit führen. Deshalb sollte ein Kontinuitätsbruch im Zuge der Umstellung des Rechtsrahmens jedenfalls vermieden werden. Andererseits haben die nationalen Regulierungsbehörden für elektronische Kommunikation und die Aufsichtsstellen für Vertrauensdienste umfassendes Know-how aufgebaut, das nach einer eventuellen Neuregelung der Zuständigkeiten auf nationaler Ebene nicht brachliegen sollte. Im Bereich der Vertrauensdienste besteht eine zusätzliche Schwierigkeit darin, dass sich Anforderungen der Cybersicherheit nur in beschränktem Maß von sonstigen Anforderungen separieren lassen, da alle durch dieselben technischen Normen vorgegeben werden und durch eine Vielzahl von Bezügen miteinander verknüpft sind. Hinzu kommt, dass Anforderungen einer in allen Mitgliedstaaten unmittelbar anwendbaren Verordnung durch 27 nationale Gesetze ersetzt werden und somit auch die Konformitätsbewertung für qualifizierte Vertrauensdienste (zumal als Dienstleistung im Binnenmarkt) um ein Vielfaches komplexer wird.

All diese Fragen und Probleme werden bei der Umsetzung in nationales Recht zu berücksichtigen sein, die sich somit als die eigentliche Herausforderung erweist.

Im Gespräch mit dem Leiter des NIS-Büros im BKA

Mag. Vinzenz Heußler (©BKA)

Wenn es um NIS 2 geht, dann führt hierzulande kein Weg am Leiter des Büros für strategische Netz- und Informationssystemsicherheit im Bundeskanzleramt(NIS-Büro), Mag. Vinzenz Heußler, vorbei. Er ist als federführender Jurist für die Legistik zur Umsetzung der NIS-Richtlinie in Österreich verantwortlich und vertritt Österreich in zahlreichen europäischen Gremien für Cybersicherheit. In dieser Funktion koordiniert Vinzenz Heußler auch die Verhandlungen zur NIS-2-Richtlinie für Österreich.

Wir konnten Herrn Mag. Heußler für ein Interview zum Thema NIS 2 und dessen Bedeutung für Österreich und die hiesige TK-Branche im Speziellen gewinnen.

RTR: Was bedeutet die am 13. Mai erfolgte politische Einigung zu NIS 2 speziell für Österreich?

Mag. Heußler: Bereits die „alte“ NIS-Richtlinie aus dem Jahr 2016 war eine wesentliche Treibkraft zur Erhöhung des Cybersicherheitslevels in Österreich. So

wurde mit dem Netz- und Informationssystemsicherheitsgesetz (NISG), das die NIS-Richtlinie umsetzt, erstmals in Österreich ein nationales Cybersicherheitsgesetz erlassen und es wurden Cybersicherheitsbehörden und Computer-Notfallteams formell eingerichtet und mit Befugnissen ausgestattet. Des Weiteren wurden formelle Strukturen und rechtliche Grundlagen zur Kooperation und Bewältigung von Cybervorfällen geschaffen. Von höchster Bedeutung war auch die Ermittlung der Betreiber wesentlicher Dienste, weil damit erstmals in rechtlich verbindlicher Weise für die Daseinsvorsorge relevante kritische Infrastrukturen identifiziert wurden, die aufgrund einer Risikobewertung Sicherheitsvorkehrungen implementieren mussten, wodurch die Cyber-Resilienz Österreichs maßgeblich gesteigert werden konnte.
Von der NIS-2-RL darf ein ähnlicher „Boost" für die österreichische und europäische Cybersicherheit erwartet werden. Wo mit der NIS-1-RL die Grundlagen geschaffen wurden, baut die NIS-2-RL darauf auf und verbessert all jene Bereiche, wo die NIS-1-RL nicht zum gewünschten Erfolg führte. Die NIS-2-RL modernisiert den bestehenden Rechtsrahmen und berücksichtigt dabei die zunehmende Digitalisierung des Binnenmarkts in den letzten Jahren (nicht zuletzt auch infolge der COVID-19 Pandemie) und der sich rasch weiterentwickelnden Bedrohungen für die Cybersicherheit. So wird sich die Anzahl der in Österreich von NIS betroffenen Einrichtungen stark erhöhen, um die gesamte Bandbreite der wirtschaftlich kritischen Aktivitäten, einschließlich der öffentlichen Verwaltung, zu schützen. Dabei wird ein nach objektiven Größenkriterien gerichteter Ansatz verfolgt, um in der EU ein Level-Playing-Field sicherzustellen, den Mitgliedstaaten aber auch ausreichend Spielraum gelassen, um nach risikobasierten Kriterien Prioritäten setzen und verhältnismäßig vorgehen zu können. Zeitgleich werden die Sicherheitsanforderungen granularer gestaltet und europäisch stärker harmonisiert. Auf diese Weise ist zu erwarten, dass die Cyber-Resilienz der österreichischen Unternehmen als Teil einer gesamteuropäischen Strategie sowohl in der Breite als auch in der Tiefe stark erhöht wird. Gleichzeitig werden auch die Fähigkeiten der Behörden stark ausgebaut, indem sie mit weitreichenderen Befugnissen ausgestattet werden, um die Anwendung der Richtlinie zu gewährleisten.

RTR: Wie wird sich NIS 2 auf die Telekommunikationsbranche auswirken?

Mag. Heußler: Das Funktionieren des Internets und der Telekommunikation ist für Österreich und den europäischen Binnenmarkt wichtiger denn je. Praktisch alle Dienstleistungen hängen von Diensten ab, die insbesondere über das Internet erbracht werden. Für die reibungslose Bereitstellung dieser Dienste ist es wichtig, dass für öffentliche elektronische Kommunikationsnetze geeignete Cybersicherheitsmaßnahmen bestehen und diesbezügliche Sicherheitsvorfälle gemeldet werden. Die NIS-2-RL verfolgt daher konsequenterweise das Ziel, die Telekommunikationsbranche näher an das „NIS-Ökosystem" heranzuführen.
Damit auch die Akteure der Telekommunikationsbranche (also Anbieter öffentlicher elektronischer Kommunikationsnetze und Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste) vom Regelwerk der NIS-2-RL profitieren können, werden sie in den Anwendungsbereich der NIS-2-RL aufgenommen. Die entsprechenden Bestimmungen der Richtlinie (EU) 2018/1972 (EECC), mit denen

diesen Akteuren bisher Sicherheitsanforderungen und Meldepflichten auferlegt werden, werden daher durch die NIS-2-RL aufgehoben bzw. ersetzt.
Ein Vorzug des Regelwerks der NIS-2-RL ist zum Beispiel die Möglichkeit, ein Computer-Notfallteam (CSIRTs) für die Bewältigung von Risiken und Vorfällen im Telekomsektor benennen zu können. Ferner können Akteure der Telekommunikationsbranche an Vereinbarungen über den Austausch von Informationen zur Cybersicherheit (zB über Cyberbedrohungen, Schwachstellen, Indicators of Compromise, etc.) teilnehmen.
Auch die für die Telekommunikationsbranche zuständigen Behörden und Stellen sollen vom Rechtsrahmen der NIS-2-RL profitieren können, indem sie beispielweise an der Arbeit der NIS-Kooperationsgruppe und des CSIRT-Netzwerks partizipieren können.
Durch das Überführen des Telekomsektors in die NIS-2-RL geht aber auch eine Straffung der rechtlichen Verpflichtungen, denen die Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste hinsichtlich der Sicherheit ihrer Netze und Informationssysteme unterliegen werden, einher. Auf diese Weise wird auch eine stärkere Harmonisierung mit den anderen der NIS-2-RL unterliegenden Sektoren erreicht und Interdependenzen können besser adressiert werden.
Um eine gewisse Kontinuität zu ermöglichen, können die Mitgliedstaaten bestehende nationale Leitlinien und nationale Rechtsvorschriften, die zur Umsetzung der Sicherheitsmaßnahmen und der Meldepflicht von Sicherheitsvorfällen aus dem EECC bereits bestehen, weiterhin anwenden und von den dafür zuständigen Behörden nach dem EECC vollziehen lassen, sofern möglich und sofern sie es für angebracht halten.

RTR: Welche Bestimmungen der künftigen NIS-2-RL sind aus Sicht des NIS-Büros besonders bedeutsam?

Mag. Heußler: Die NIS-2-RL dreht an vielen Stellen die richtigen Schrauben. Es darf nicht außer Acht gelassen werden, dass mit der Umsetzung der NIS-1-RL schon viel Erfahrung gesammelt werden konnte und sich eine wertvolle Zusammenarbeit auf europäischer Ebene herausgebildet hat. Es bestehen daher schon viele Grundlagen und ein hohes Vertrauen zwischen den Akteuren der NIS-1-RL und den Mitgliedstaaten. Die NIS-2-RL stärkt zum einen diese gut funktionierenden Elemente der NIS-1-RL, wie insbesondere das CSIRTs-Netzwerk, aber auch die NIS-Kooperationsgruppe. Zum anderen kann die NIS-2-RL aber dort einen größeren Wurf machen, wo die Zeit bei der NIS-1-RL noch nicht reif genug war. Beispielweise werden die Mitgliedstaaten viel umfangreichere und detailliertere nationale Cybersicherheitsstrategien verabschieden müssen. Als Teil dieser Strategien werden sie auch einen Rahmen für die koordinierte Offenlegung von Sicherheitslücken vorsehen müssen. Dabei handelt es sich um einen nicht zu vernachlässigenden Faktor im Auffinden und Schließen von Sicherheitslücken, der in vielen Mitgliedstaaten – so auch in Österreich – aktuell noch fehlt.

Des Weiteren sieht die NIS-2-RL auch viel mehr Bestimmungen vor, was große Cybersicherheitsvorfälle und -krisen mit europäischer Dimension betrifft. Denn alle Mitgliedstaaten müssen nunmehr einen nationalen Rahmen für das

Cybersicherheitskrisenmanagement schaffen, nationale Cyberkrisen-Behörden benennen und auf europäischer Ebene in einem neuen Netzwerk der Verbindungsorganisationen für Cyberkrisen (CyCLONe) zusammenarbeiten. Durch den vereinheitlichten Anwendungsbereich, die harmonisierten Bestimmungen zur Meldung von Sicherheitsvorfällen und das Schaffen gleicher Kapazitäten bei den Behörden sollte es der EU in Zukunft daher besser möglich sein, ein gesamteuropäisches Lagebild zu generieren.
Sinnvoll ist zudem, dass die NIS-2-RL vorschreibt, dass die Führungsebenen der in den Anwendungsbereich fallenden Einrichtungen die Risikomanagement-Maßnahmen genehmigen und spezielle Cybersicherheitsschulungen absolvieren müssen. Dadurch sollte es möglich sein, das für die Cybersicherheit essentielle Bewusstsein auf der Ebene der Leitungsorgane zu erzeugen. Dieses Bewusstsein bildet sich sonst leider allzu oft erst, nachdem es zu einem großen Cybervorfall bei der Einrichtung gekommen ist.

Darüber hinaus widmet sich die NIS-2-RL verstärkt dem immer wichtiger werdenden Thema der Sicherheit der Lieferketten. Dieses wird sowohl auf europäischer Ebene durch die Möglichkeit der NIS-Kooperationsgruppe, EU-weit koordinierte Risikobewertungen kritischer Lieferketten durchzuführen, als auch auf nationaler Ebene als Teil der Cybersicherheitsstrategien adressiert. Entscheidend ist auch, dass auf individueller Ebene die einzelnen in den Anwendungsbereich fallenden Einrichtungen die Sicherheit der Lieferkette im Rahmen der Risikomanagementmaßnahmen beachten müssen.

RTR: Mit welchem Zeitplan ist für die weitere Gesetzgebung auf Unionsebene und innerhalb Österreichs zu rechnen?

Mag. Heußler: In der Nacht von 12. auf 13. Mai konnte eine vorläufige politische Einigung zwischen den beiden Ko-Gesetzgebern, also dem Europäischen Parlament und dem Rat der EU, erzielt werden. Im Anschluss wurde der Text noch auf technischer Ebene finalisiert und konsolidiert und den Mitgliedstaaten Anfang Juni zur Prüfung übermittelt. Der finalisierte und konsolidierte Text wird nach Prüfung durch die Mitgliedstaaten dem Ausschuss ständiger Vertreter (AStV) am 22. Juni zur Billigung vorgelegt, um anschließend in die Amtssprachen der EU übersetzt zu werden. Nach der Prüfung der Übersetzungen muss das Europäische Parlament den Text annehmen, wovon im dritten Quartal 2022 auszugehen ist. In weiterer Folge wird der Rechtstext im Amtsblatt der EU veröffentlicht und tritt 20 Tage danach in Kraft.

Nach Inkrafttreten haben die Mitgliedstaaten anschließend 21 Monate Zeit, um die NIS-2-RL in nationales Recht umzusetzen. Das bedeutet, dass Österreich die Umsetzung voraussichtlich bis zum zweiten Quartal 2024 vornehmen wird müssen. Hierzu wird es einer Änderung der nationalen Rechtsgrundlagen, also insbesondere des Bundesgesetzes zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG), bedürfen.

RTR: Herzlichen Dank für das Gespräch!

NETZSICHERHEIT

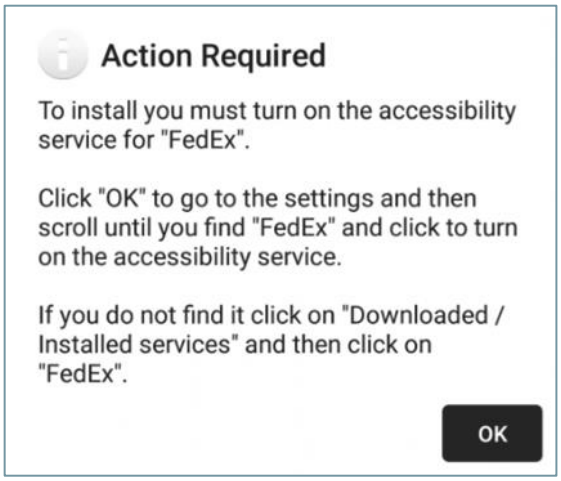
FluBot – ein lästiger Gast in TK-Netzen

Wenn es um Cyberkriminalität geht, kann man durchaus den Eindruck gewinnen, als technisch minderversierte:r Nutzer:in, dem Treiben hilflos ausgeliefert zu sein. Da gibt es Schwachstellen in Hard- und Software, da werden „Overflows" erzeugt und Zero-Day-Exploits ausgenützt, wo man selbst als Experte leicht den Überblick verlieren kann. Vergessen wird dabei allerdings, dass es für die Angreifer oftmals viel einfacher geht. Nämlich dann, wenn der angegriffene Endkunde die Schadsoftware selbst am Endgerät installiert und dieser auch noch Schritt für Schritt die notwendigen Berechtigungen erteilt.

Genau so passiert es mit FluBot, einer Android-Malware, die sich nun bereits seit mehr als einem Jahr auch in Österreich über SMS verbreitet und vor allem das Ausspähen von persönlichen Daten der Handy-Nutzer:innen zum Ziel hat. Oftmals ist es eine SMS-Nachricht eines vermeintlich vertrauenswürdigen Absenders (wie etwa ein Paketdienstleister, eine Bank oder der eigene Netzbetreiber), mit der der bzw. die Adressat:in aufgefordert wird, eine App zu installieren, um ein Paket nachverfolgen zu können, eine Sperre des Bankkontos oder des Internetzugangs zu vermeiden. Nachdem Schadsoftware in aller Regel im offiziellen App-Store nicht verfügbar ist, muss das Opfer zunächst die Berechtigung für „Sideloading" erteilen, sodass die App aus einer Quelle unbekannter Herkunft außerhalb des App-Stores bezogen werden kann. Ist diese Berechtigung erteilt und die Datei auf das Endgerät heruntergeladen, muss die App installiert werden. Erst wenn die Einstellungen etwa für Accessibility Service und Notification Access entsprechend angepasst sind, wird die vermeintlich hilfreiche App endgültig am Endgerät installiert. In Wirklichkeit befindet sich mit FluBot nun eine mächtige Malware am Endgerät, die den Angreifern die Übernahme zahlreicher Funktionen des Endgerätes ermöglicht: eine Vielzahl von Daten abzugreifen, SMS-Nachrichten zur Weiterverbreitung von FluBot versenden oder die Aktivitäten von FluBot vor dem bzw. der Endnutzer:in zu verbergen. Abhilfe schafft in der Regel nur ein komplettes Rücksetzen des Endgerätes auf Werkseinstellungen – eine Prozedur, die bei betroffenen Kunden verständlicherweise auf wenig Begeisterung stößt.

Während sich Endkunden also durch erhöhte Vorsicht im Umgang mit verdächtigen Nachrichten oder Links schützen können, stellt sich die Frage, inwieweit die Betreiber der Verbreitung von FluBot und anderer Malware einen Riegel vorschieben könnten. Die Antwort ist – wie oft in diesem Bereich – vielschichtig. Rein technisch betrachtet, bestünde die Möglichkeit, SMS-Nachrichten einer Analyse zu unterziehen, nach potenzieller Schadwirkung zu klassifizieren und verdächtige Nachrichten auszufiltern. Sieht man sich allerdings die rechtlichen Rahmenbedingungen an, so gibt es – aus guten Gründen – einige Hürden, die ein allzu forsches Herangehen recht rasch in die Schranken weisen. Fernmeldegeheimnis und Datenschutz sind hohe Güter, sodass zunächst abzuwägen ist, welche gelinderen Mittel ebenfalls zu einer Eindämmung von FluBot und anderer Malware beitragen könnten.

Abbildung 01: Das Opfer erhält genaue Anweisungen, welche Berechtigungen die Malware benötigt und wie diese zu erteilen sind.



Die RTR steht seit dem ersten Auftreten von FluBot mit den Mobilnetzbetreibern und zuletzt auch betroffenen Unternehmen (Banken) im Austausch und unternimmt ein gemeinsames Monitoring. Nachdem sich die zwischenzeitliche Hoffnung eines Rückgangs der FluBot-Angriffe nicht erfüllt hat, wurde seitens der RTR die Branchenrisikoanalysegruppe einberufen, um sich auf Expertenebene gemeinsam des Themas anzunehmen und nach Ansatzpunkten für eine Lösung zu suchen. Zusätzlich konnte seitens der RTR die für Fragen des Datenschutzes zuständige Datenschutzbehörde (DSB) für eine Teilnahme an den Gesprächen gewonnen werden.

Während also auf nationaler Ebene Behörden und Betreiber nach Lösungen suchten, waren auch Strafverfolgungsbehörden auf internationaler Ebene aktiv. Koordiniert vom European Cybercrime Center (E3C) von Europol, haben Behörden aus Australien, Belgien, Finnland, Irland, den Niederlanden, Schweden, der Schweiz, Spanien, Ungarn und den Vereinigten Staaten zusammengewirkt. Dabei gelang es der holländischen Polizei offenbar, die FluBot-Malware-Infrastruktur zu übernehmen und den FluBot-Kampagnen vorerst den Wind aus den Segeln zu nehmen. Inwieweit dieser Schlag den heimischen Anbietern und Kunden zumindest eine Atempause verschafft oder ob er vielleicht sogar nachhaltige Abhilfe bedeutet, bleibt abzuwarten. Die RTR wird das Thema jedenfalls weiterhin beobachten und gemeinsam mit den anderen Stakeholdern nach Maßnahmen gegen FluBot und andere Malware suchen.

5G-Cybersicherheitszertifizierungsschema

Die Zertifizierung von Produkten, Diensten und Prozessen ist grundsätzlich ein probates Mittel, die Sicherheit zu erhöhen. Gleichzeitig ist darauf Bedacht zu nehmen, in einer Industrie mit häufigen Produkt- und Update-Zyklen nicht Dynamik und

Innovationskraft zu reduzieren. Die RTR wirkt in den europäischen Arbeitsgruppen zum Thema einer 5G-Cybersicherheitszertifizierung mit. Nachfolgend ein kurzes Update zur Entwicklung eines EU-5G-Schemas.

Die Agentur der Europäischen Union für Cybersicherheit (ENISA) hat sich der Erreichung eines hohen gemeinsamen Niveaus an Cybersicherheit verschrieben. Die 2004 gegründete und durch den Rechtsakt zur Cybersicherheit („Cybersecurity Act" CSA, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0881) gestärkte Agentur leistet einen Beitrag zur EU-Cybersicherheitspolitik, stärkt die Vertrauenswürdigkeit von IKT-Produkten, -Diensten und -Prozessen mit Cybersicherheits-Zertifizierungssystemen, arbeitet mit Mitgliedstaaten und EU-Einrichtungen zusammen und hilft Europa, sich auf die Cyber-Herausforderungen von morgen vorzubereiten. Um die Cybersicherheit im Bereich 5G zu unterstützen und zu verbessern, hat die EU-Kommission die Agentur – im Einklang mit dem Mandat der ENISA gemäß Artikel 8 (1) (b) des CSA – aufgefordert, diesen Kandidaten für ein europäisches Cybersicherheitszertifizierungsschema für 5G-Netze vorzubereiten („EU 5G Scheme"). In diesem Rahmen hat die ENISA im Juni 2021 einen Aufruf zur Interessenbekundung an der 5G-Ad-hoc-Arbeitsgruppe („Ad Hoc Working Group" AHWG) gemäß Artikel 49 (4) des CSA und des entsprechenden Beschlusses des ENISA-Vorstands veröffentlicht (https://www.enisa.europa.eu/topics/standards/adhoc_wg_calls/ad-hoc-working-group-on-5g-cybersecurity-certification).

In Bezug auf den Kontext, in dem die Zertifizierung angewendet werden soll, konzentriert sich das 5G-Schema der EU auf zertifizierte Sicherheit für teilnehmerbezogene Anwendungsfälle des 5G-Ökosystems, wie z.B. die Lieferung und Bereitstellung von 5G-Netzausrüstung, Verwaltung von Teilnehmeridentitäten, ferngesteuerte SIM-Bereitstellung, 5G-Authentifizierung (inkl. Roaming) und Konnektivitätsdienste für Teilnehmer.

Das Programm zur Vorbereitung des EU-5G-Schemas besteht aus zwei Phasen. Die erste Phase umfasst die „Ist"-Übersetzung von Elementen bestehender Schemata in ihre EU-Äquivalente, die Identifizierung von Sicherheits- und Zertifizierungsanforderungen für die relevanten Anwendungsfälle, Komponenten und Prozesse auf der Grundlage der Risikobewertung ihrer beabsichtigten Verwendung und die Identifizierung von Lücken sowie ein erster Aufriss über die notwendigen Erweiterungen und/oder Verbesserungen der „Ist"-Versionen der Zertifizierungsmittel. Hier ist die Arbeit der AHWG in drei Work Streams (WS) unterteilt: WS1: „Ist"-Übersetzung bestehender Systemelemente in ein EU-Äquivalent auf Basis von GSMA NESAS (https://www.gsma.com/security/network-equipment-security-assurance-scheme/); WS2: „Ist"-Übersetzung bestehender Systemelemente in ein EU-Äquivalent auf Basis von GSMA SAS-SM und SAS-UP (https://www.gsma.com/security/security-accreditation-scheme/) und eUICC (eSIM) Zertifizierungssystem (https://www.gsma.com/services/gsma-euicc-security-assurance-test-trust-assure/); WS3: Risikobasierte Definition von Sicherheits- und Zertifizierungsanforderungen für Komponenten, die die oben genannten Anwendungsfälle unterstützen und dazugehörige Gap-Analyse.

In der zweiten Phase ist die Implementierung von Erweiterungen und Verbesserungen und die Vorbereitung und Ausarbeitung des EU 5G-Schemas vorgesehen, die maßgeblich durch die Ergebnisse der Gap-Analyse am Ende der Phase 1 festgelegt wird.
Die in die AHWG berufenen Mitglieder vertreten verschiedene 5G-Interessenvertreter:innen mit unterschiedlichen Fachgebieten wie Verbraucherinteressengruppen, Standardentwicklungsorganisationen, Mobilfunknetzbetreiber und -diensteanbieter, Netzwerkausrüstungslieferanten, eUICC/eSIM-Lieferanten, Anbieter von Teilnehmerverwaltungsplattformen und -diensten (SM-DP+, SM-DS), Anbieter von Mobilfunkendgeräten sowie Konformitätsbewertungsstellen und Prüflabors. Darüber hinaus sind in der AHWG auch ernannte Beobachter aus den Mitgliedstaaten vertreten, die ein Interesse daran haben, die Entwicklungen des 5G-Cybersicherheitszertifizierungsschema zu verfolgen.

Wie lange dauert es nun noch, bis 5G tatsächlich zertifiziert werden kann? Die Arbeiten am 5G-Cybersicherheitszertifizierungschema sind derzeit am Anfang und bis zum Abschluss wird es realistisch betrachtet wohl noch das eine oder andere Jahr dauern. Die seitens ENISA Anfang Juni 2022 veranstaltete „Cybersecurity Certification Conference 2022“ (https://www.enisa.europa.eu/events/enisa-cybersecurity-certification-conference-2022/eccc2022-hybrid-conference) konnte einige Einblicke in das spannende aber auch hochkomplexe Thema der Entwicklung und Zukunft der EU-weiten Zertifizierungsschemata preisgeben.

Cybersicherheit in Open RAN Netzen

5G-Mobilfunknetze bieten neue Funktionen und benützen neue Technologien in Kernnetz, Transportnetz und Funkzugangsnetz (Radio Access Netz - RAN - das die Verbindung zwischen mobilem Endgerät und Kernnetz in einem Mobilfunknetz ermöglicht), die seitens 3GPP (https://www.3gpp.org) für 3G-, 4G- und 5G-Technologien standardisiert wurden. 3GPP ist eine Partnerschaft, die maßgebliche Standardisierungsgremien aus verschiedenen Weltregionen wie ETSI (Europa), ATIS (USA), CCSA (China), ARIB und TTC (Japan), TTA (Korea) und TSDSI (Indien) zusammenbringt. In Open Radio Access Netzen (Open RAN) sollen einige dieser neuen Technologien, wie z. B. Cloudifizierung und Virtualisierung, Einsatz von herstellerneutraler Hardware, offener Software und Schnittstellen, verwendet werden, um mehr Interoperabilität zwischen verschiedenen Netzwerkkomponenten zu ermöglichen und eine Diversifizierung der Anbieter im RAN zu fördern. Es gibt mehrere Open-RAN-Konzepte, -Initiativen und -Spezifikationsbemühungen, die von verschiedenen Gruppen vorangetrieben werden, jedoch jeweils einen etwas anderen Ansatz verfolgen. Darunter sind virtualisiertes RAN (v-RAN), Telecom Infra Project (TIP) und insbesondere die O-RAN Alliance (https://www.o-ran.org) zu nennen, deren Spezifikationen diejenigen der 3GPP ergänzen, indem sie neue Anforderungen und Anwendungsfälle, Profile, zusätzliche Schnittstellen und neue Komponenten im RAN definieren.

NETZSICHERHEIT

Da die rechtzeitige Bereitstellung sicherer 5G-Netze für die Europäische Union eine hohe Priorität hat, haben die EU-Mitgliedstaaten mit Unterstützung der Europäischen Kommission und der ENISA einen konzertierten Ansatz für die Cybersicherheit von 5G-Netzen entwickelt. Im Rahmen dieses Vorgehens bewerteten die EU-Mitgliedstaaten gemeinsam die wichtigsten Risiken im Zusammenhang mit 5G-Netzen („EU Coordinated risk assessment“, https://digital-strategy.ec.europa.eu/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security) und definierten einen umfassenden und risikobasierten Ansatz in Form der im Januar 2020 verabschiedeten „EU 5G Toolbox“ (https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures). Da Open RAN als vielversprechender Markttrend in der Entwicklung von 5G- und 6G-Architekturen gesehen wird, haben die EU-Mitgliedstaaten beschlossen, eine eingehende Analyse der Auswirkungen von Open RAN auf die Cybersicherheit durchzuführen, um die vorhin erwähnte koordinierte Risikoanalyse zu 5G zu ergänzen, was zu einem in Mai 2022 veröffentlichten Bericht führte (https://digital-strategy.ec.europa.eu/en/library/cybersecurity-open-radio-access-networks).

Der Bericht stellt fest, dass die Cybersicherheit eine erhebliche Herausforderung für das Open-RAN-Konzept im Allgemeinen darstellt und dass insbesondere die von der O-RAN Alliance erstellten Spezifikationen, zusätzlich zu ihren Governance-Mängeln, nicht ausreichend ausgereift und durch Design abgesichert sind. Aufgrund des neuen Ansatzes von Open RAN würden, insbesondere kurzfristig, neue Schnittstellen und neue Arten von RAN-Komponenten, die möglicherweise von mehreren Anbietern stammen, eine Reihe von Sicherheitsrisiken von 5G-Netzen verschärfen und die Angriffsfläche im Bereich des Funkzugangsnetzes vergrößern.

Um diese Risiken zu mindern und die potenziellen Chancen von Open RAN zu nutzen, werden zusätzlich zu jenen der EU 5G Toolbox weitere Maßnahmen für Netze auf Basis von Open RAN empfohlen, wie z.B: Nutzung von Regulierungsbefugnissen, um die Pläne von großangelegter Bereitstellung von Open-RAN-Netzen zu prüfen und gegebenenfalls Einschränkungen, Verbote und/oder spezifische Anforderungen oder Bedingungen diesbezüglich aufzuerlegen; Verstärkung wichtiger technischer Kontrollen, wie Authentifizierung und Autorisierung, und Anpassung der Überwachung der Komponenten an eine modulare Umgebung; Bewertung des Risikoprofils von Open-RAN-Anbietern, externen Diensteanbietern im Zusammenhang mit Open RAN, Cloud-Dienst- bzw. -Infrastrukturanbietern und Systemintegratoren und Ausweitung der Kontrollen und Beschränkungen für Bereitsteller von Dienstleistungen; Behebung von Mängeln bei der Entwicklung technischer Spezifikationen: Der Prozess sollte die Gründungsprinzipien der Welthandelsorganisation für die Entwicklung internationaler Standards erfüllen, und Sicherheitsmängel sollten behoben werden; Aufnahme von Open-RAN-Komponenten zum frühestmöglichen Zeitpunkt in das zukünftige EU 5G Cybersicherheitszertifizierungsschema, das sich derzeit in der Entwicklung befindet.
Die Maßnahmen können je nach Konkretisierung direkt auf nationaler und/oder EU-Ebene umgesetzt werden, im Einklang mit den jeweiligen Zuständigkeiten. Bei der Auswahl der erforderlichen Maßnahmen entscheiden die einzelnen Mitgliedstaaten

über die Eignung der Maßnahme, zuzüglich der Überprüfung der verfügbaren Ressourcen und einer daraus abgeleiteten Notwendigkeit allfälliger Zusammenarbeit mit anderen Mitgliedstaaten und/oder auf EU-Ebene.

Zusammenfassend wird eine umsichtige Herangehensweise an die neue Architektur des Open RAN empfohlen. Jeder Übergang von und Koexistenz mit bestehenden Technologien sollte mit ausreichendem Zeit- und Ressourcenbudget erfolgen, um Risiken im Voraus zu bewerten, geeignete Minderungsmaßnahmen umzusetzen und die Verantwortlichkeiten im Falle eines Ausfalls oder Vorfalls klar zu definieren. Bei der Suche nach Kosten-Leistungs-Kompromissen durch Open RAN sollten Betreiber und andere Interessensgruppen der Gewährleistung der Sicherheit, die erhebliche Investitionen erfordern kann, zusätzlich zu den bestehenden 5G-Cybersicherheitsmaßnahmen genügend Aufmerksamkeit schenken.

Die RTR wirkt bei diesen europäischen Aktivitäten zu Sicherheitsaspekten von Open RAN auf unterschiedlichen Ebenen mit und bringt ihre Expertise in den betreffenden Arbeitsgruppen ein, sei es in der NIS-Kooperationsgruppe in Unterstützung des BKA, in der ENISA oder bei BEREC.

INTERNATIONALES

Neuigkeiten von BEREC: offenes Internet, Roaming und Ukraine

Vor dem Sommer veröffentlichte BEREC noch eine Reihe von Berichten und lud zu öffentlichen Konsultationen. So gibt es aktualisierte Guidelines zum Offenen Internet, den allerersten Nachhaltigkeitsbericht und konsultiert werden Retail Roaming Guidelines. Außerdem wird die ukrainische Regulierungsbehörde BEREC-Mitglied ohne Stimmrecht.

Die Europäische Kommission fasste den Beschluss, der ukrainischen Regulierungsbehörde für elektronische Kommunikation (NCEC) die Mitarbeit bei BEREC zu ermöglichen. Dadurch kann sie am Board of Regulators teilnehmen und Expertinnen und Experten in die BEREC-Arbeitsgruppen entsenden. Als „Member without voting rights" hat NCEC aber kein Stimmrecht.

Schon seit Kriegsbeginn arbeiten die EU und die Ukraine zusammen, um erschwingliche, grenzüberschreitende Kommunikation zu gewährleisten. Denn Konnektivität ist unerlässlich, damit Menschen auf der Flucht im In- und Ausland in Verbindung bleiben können. BEREC hat die Europäische Kommission unterstützt und die Situation beobachtet. Der Aufnahme-Beschluss wird eine stabile Entwicklung der Zusammenarbeit ermöglichen.

Angepasste Open Internet Guidelines veröffentlicht

Im September des Vorjahres entschied der Europäische Gerichtshof (EuGH) in Sachen offenes Internet. Das führte dazu, dass BEREC im Rahmen seines Mandats die Open Internet Guidelines anpassen musste. Nach einer öffentlichen Konsultation dieser modifizierten Guidelines wurden diese finalisiert und jetzt veröffentlicht.
Sie spiegeln das Urteil des EuGHs wider, dass Zero-Rating-Angebote mit der Verpflichtung zur Gleichbehandlung des Datenverkehrs in der Open-Internet-Verordnung unvereinbar sind.

Die Guidelines wurden nur im Rahmen der Rechtsprechung des Gerichtshofs aktualisiert. Sie bieten damit aber auch mehr Klarheit in acht Paragraphen und stärken Endnutzerrechte. BEREC wird auch in Zukunft für die Koordinierung zwischen den nationalen Regulierungsbehörden sorgen. Sie finden die Übersicht der veröffentlichten Berichte auf der BEREC-Webseite.

Veröffentlicht wird auch der Bericht zum Thema „consistent approach to migration and copper switch-off". Dieser ist Teil des BEREC-Ziels, die volle Konnektivität zu unterstützen. Er rührt daher, dass durch den Glasfaserausbau das traditionelle Kupfer-basierte Anschlussnetz zunehmend an Bedeutung verliert, Betreiber daher dieses außer Betrieb nehmen und beispielsweise Hauptverteilerstandorte abschalten wollen. Der Bericht identifiziert auf Basis der Regelungen und Erfahrungen von nationalen Regulierungsbehörden in 17 europäischen Staaten einen konsistenten Ansatz für die Regulierung dieser Migration und Kupfernetzabschaltung.

Auch im Bereich der Cybersicherheit veröffentlichte BEREC einen Bericht über die Resilienz von nationalen Netzen. Da die Ergebnisse daraus für die nationale Sicherheit und den sicheren Betrieb relevant sind, können sie nicht veröffentlicht werden. Dennoch gibt es eine öffentliche Version, die BERECs Arbeit beschreibt, um zu den Ergebnissen zu gelangen.

So viel kann aber gesagt werden: Es gab zwei Erhebungen, die Einblicke in die nationale Organisation und den Betrieb von einigen sicherheitsrelevanten Funktionen in den Netzen von MNOs bieten.

Erster ICT-Nachhaltigkeitsbericht veröffentlicht

BEREC erkannte die Wichtigkeit einer umweltgerechten elektronischen Kommunikation. Nicht zuletzt, um den Green Deal der Europäischen Kommission zu unterstützen, erarbeitet sich BEREC eine Expertise innerhalb des Mandats im Sektor.
Entstanden ist dadurch der erste Nachhaltigkeitsbericht, dessen Entwurf wir schon im vorigen Newsletter vorgestellt haben. Dieser wird jetzt nach der öffentlichen Konsultation in der Endfassung veröffentlicht. Bei näherem Interesse empfehlen wir die Aufzeichnung des Stakeholder Workshops zur ICT-Nachhaltigkeit.

Im Bereich neuer Gesetzesinitiativen begrüßt BEREC die Ziele des neuen Data Acts, den die Europäischen Kommission vorgeschlagenen hatte. Der Entwurf sieht ein Datengesetz mit harmonisierten Regeln für den Zugang zu und die faire Nutzung von Daten vor. BEREC überprüft die Relevanz des Gesetzesentwurfs für die Arbeitsbereiche der Regulierungsbehörden für elektronische Kommunikation einschließlich angrenzender Bereiche wie Datenschutz und Privatsphäre.

Sie sind am Wort: öffentliche Konsultationen

Welche Rolle spielen Wettbewerb und Offenheit im Ökosystem Internet? In einer breit angelegten Analyse möchte BEREC verstehen helfen, wie das Internet-Erlebnis der Nutzer:innen durch die verschiedenen Elemente des Internetökosystems beeinflusst wird. Gleichzeitig stellt der Analysebericht dar, wie sich die Wechselwirkungen zwischen diesen Elementen auf potenzielle Regulierungsmaßnahmen auswirken können.

Die Idee dahinter war es, sich dieses Ökosystem ganzheitlich anzusehen. Dafür wurde es zuerst analysiert und nach Elementen geordnet. Zu den Elementen gehören etwa Hardware, CDNs, Hosting und OTTs. Danach wurde festgestellt, welche Praktiken im Zusammenhang mit diesen Elementen für den Wettbewerb relevant sind.
Klar war bereits, dass Big Tech und Internet Service Provider wesentliche Akteure sind. Jetzt wird aber dargelegt, inwiefern sie für das Ökosystem Internet relevant sind und wie man sowohl Wettbewerbsverhältnisse als auch Partnerschaftsverhältnisse darstellen kann.
Dadurch sieht man auch, dass Big-Tech-Unternehmen am stärksten auf der Client- und Serverseite vertreten sind. ECS-Anbieter hingegen sind hauptsächlich auf IAS und Infrastruktur konzentriert.

Die zunehmenden Investitionen von Big-Tech-Unternehmen in die Telekommunikationsinfrastruktur, wie virtualisierte Netzdienste, Cloud-Computing oder Unterseekabeln, könnten jedoch die Wettbewerbsdynamik im Telekomsektor beeinflussen.

Der Bericht ist eine Basis für eine intensivere Auseinandersetzung mit Digitalthemen und bietet auch einen guten Einstieg, wenn Sie sich im Bereich Internetökosystem einlesen wollen. Derzeit können Sie zu dem Bericht Stellung nehmen. Eine finale Fassung wird nach dem letzten Plenum 2022 veröffentlicht.

Konsultiert wird des Weiteren ein Entwurfsbericht zu Satelliten-Breitbandinternet innerhalb des Universaldienstes. Darin zu finden sind etwa Informationen über die verschiedenen „Satcom"-Lösungen sowie wichtige dazugehörige Aspekte wie Preis, Qualität, Marktrolle oder regulatorische Überlegungen.

Retail Roaming Guidelines werden konsultiert

Die Europäische Union veröffentlichte heuer eine angepasste Roaming-Verordnung. Diese verlangt von BEREC sowohl Wholesale als auch Retail Roaming Guidelines. Erstere sollen schon im Oktober veröffentlicht werden. Der Entwurf beider Leitlinien ist bereits fertig und wird jetzt öffentlich konsultiert.

Bei den Retail Guidelines sieht der Entwurf vor allem Anpassungen bei „Quality of Service" vor. Durch die angepasste Verordnung können Endkundinnen und Endkunden im Rahmen von „Roam Like at Home" jetzt ja auch die gleiche Verbindungsqualität wie daheim genießen. Außerdem müssen Notrufe kostenlos möglich sein.

In den angepassten Retail Roaming Guidelines finden sich auch die Definition von nicht-terrestrischen Netzwerken und freiwillige Maßnahmen der Betreiber, um ungewolltes oder versehentliches Roaming außerhalb von „Roam Like at Home" zu verhindern.

Öffentlich konsultiert wird daneben auch ein Bericht zu Maßnahmen, um Endkundinnen bzw. Endkunden mit Behinderungen gleichen Zugang und Wahlmöglichkeiten zu Telekommunikationsdiensten zu ermöglichen. Er baut auf vorangegangenen Berichten auf und zielt darauf ab, Informationen von den nationalen Regulierungsbehörden zusammenzutragen. Daraus soll eine Sammlung von Maßnahmen und Initiativen werden, um den Bedürfnissen von Menschen mit Behinderung gerecht zu werden. Gleichzeitig unterstützt er damit die Behörden in der Umsetzung solcher Maßnahmen.

Der Bericht enthält Informationen über die Art und Weise, wie die Mitgliedstaaten die Maßnahmen aus Artikel 111 EECC zur Verfügbarkeit und Erschwinglichkeit spezieller Geräte und spezieller Dienste umsetzen, die den gleichwertigen Zugang verbessern. Davon umfasst sind auch vollständige Gesprächsdienste und Relaisdienste.

Laufende und abgeschlossene Konsultationen finden Sie auf der BEREC-Webseite. Das nächste BEREC-Plenum findet Anfang Oktober in Salzburg statt.

INTERNATIONALES

Neuigkeiten aus dem Bereich Postdienste

Von 30. Juni bis 01. Juli 2022 findet das erste ERGP-Plenum statt. Auf der Tagesordnung steht unter anderem die Mid-Term-Strategy 2023-2025, die sich mit den Themen der Digitalisierung und Nachhaltigkeit beschäftigt. Darüber hinaus steht nach wie vor die Frage der Überarbeitung der Postdiensterichtlinie zur Diskussion. Dieser Rechtsrahmen besteht seit rund 20 Jahren beinahe unverändert.

ZUM THEMA

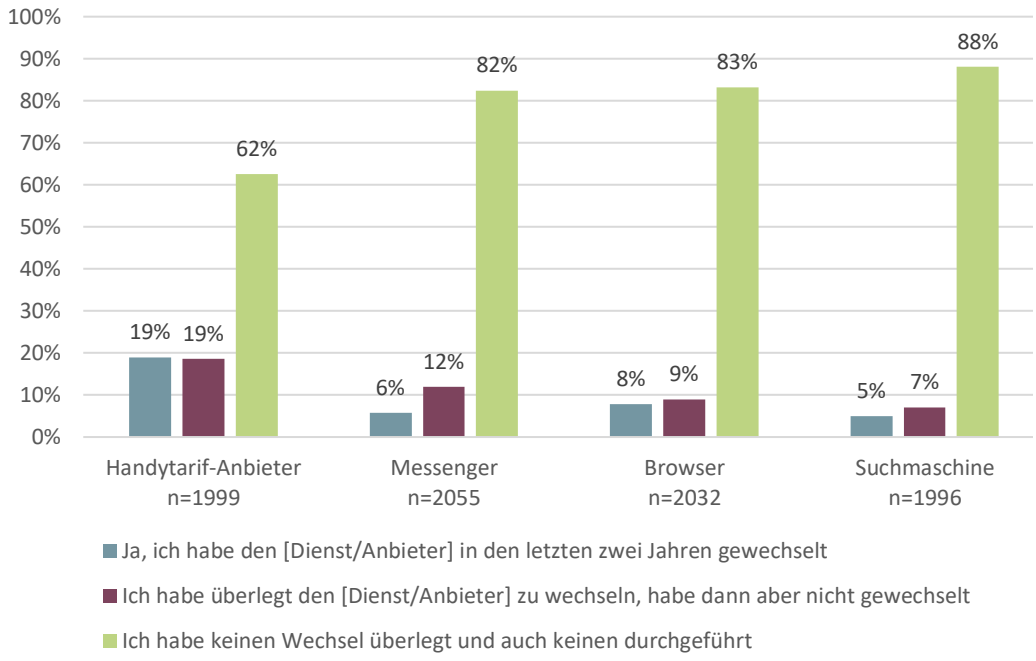
Wechselbarrieren bei wesentlichen Diensten des Internets

Der Fachbereich Telekommunikation und Post der RTR untersuchte Barrieren beim Wechsel von Messengern, Browsern, Suchmaschinen und Handytarif-Anbietern anhand einer repräsentativen Befragung österreichischer Nutzer:innen.

1. Handytarif-Anbieter wird öfter gewechselt als der Messenger, Browser oder die Suchmaschine

Die Märkte für Messenger, Browser und Suchmaschinen werden von wenigen Unternehmen dominiert. Obwohl zahlreiche Dienste am Handy verfügbar sind, entscheiden sich viele Nutzerinnen und Nutzer, bewusst oder unbewusst, für denselben Anbieter. Chrome ist in Österreich Marktführer bei Browsern, Google bei Suchmaschinen und WhatsApp bei Messengern. Abbildung 1 zeigt das Wechselverhalten von Nutzern in den letzten 2 Jahren im Vergleich über die betrachteten Dienste. In diesem Zeitraum haben 19% der Befragten ihren Handytarif-Anbieter gewechselt („Wechsler"), hingegen nur zwischen 5% und 8% ihren Messenger, ihren Browser oder ihre Suchmaschine.

Abbildung 1: Die Verteilung von Wechslern, Überlegern und Nicht-Überlegern (Einfachnennung, Q26, Q43, Q53, Q63), Quelle: RTR



ZUM THEMA

2. Messenger: Netzwerkeffekte entscheidend, Multi-Homing etabliert

Bei Messengern ist das wichtigste Auswahlkriterium jenes der Netzwerkeffekte. Nutzende verwenden oft jenen Messenger, mit dem sie die meisten ihrer Kontakte erreichen können. Dies begünstigt klar die großen Dienste, die schon eine hohe Marktdurchdringung haben und ist letztlich auch ein wesentlicher Grund für die Dominanz von WhatsApp. Auch Funktionalitäten, insbesondere unter Snapchat-Nutzenden, und Gewohnheitseffekte spielen eine wichtige Rolle. Jeder fünfte Nutzende, welcher den Messenger wechselte, nannte die notwendige Überzeugung von Kontakten als Barriere für einen Wechsel. Gleichzeitig betreiben rund 80% der Nutzer Multi-Homing, also die parallele Nutzung von verschiedenen Messengern, sodass ein Wechsel des Messengers anlassbezogen möglich ist.

3. Browser und Suchmaschinen: Gewohnheit und Vorinstallationen wesentlich, Beurteilung von Sicherheit und Datenschutz schwierig

Bei Browsern und Suchmaschinen spielt Gewohnheit eine große Rolle bei der Auswahl des Dienstes. Die meisten Nutzer erhalten über Vorinstallationen oder Voreinstellungen Zugang zu ihrem Browser und ihrer Suchmaschine. Der Markt für Browser wird daher stark von Chrome (Google) und Safari (Apple) dominiert. Für Firefox-Nutzer sind Sicherheits- und Datenschutzaspekte besonders wichtig – sie installieren den Browser gezielt selbst. Bei der Nutzung von Suchmaschinen dominiert Google deutlich. Die Nutzung einer alternativen Suchmaschine ist häufig mit einer stärkeren Präferenz für Sicherheit und einem besseren Datenschutz verbunden. Die wichtigste Barriere beim Wechsel des Browsers oder der Suchmaschine ist die Beurteilung von Sicherheit und Datenschutz bei alternativen Anbietern.

4. Adressierung von Netzwerkeffekten und Vorinstallationen bleibt Herausforderung

Interoperabilitätsverpflichtungen, wie sie im Digital Markets Act der EU geplant sind, kann die Dominanz eines Messengers mindern, indem Netzwerkeffekte über etablierte und neue Anbieter realisiert werden. Gleichzeitig kann Interoperabilität zu vermehrtem Single-Homing, d.h. der Nutzung ausschließlich eines Messengers, und einem Verlust an Innovation und Investitionsbereitschaft führen, was dem Wettbewerb letztlich auch schaden könnte. Die Wirksamkeit der kürzlich eingeführten Auswahlmenüs bei Android, welche eine bewusste Auswahl für einen Browser oder eine Suchmaschine und Markteintritt von alternativen Anbietern erleichtern sollen, ist vorerst nicht eindeutig und weiter zu beobachten.

5. Bericht auf der Website der RTR veröffentlicht

Der Bericht „Wechselbarrieren bei wesentlichen Diensten des Internets“ untersucht anhand einer repräsentativen Befragung österreichischer Nutzenden wettbewerbliche Aspekte beim Wechsel von Messengern, Browsern, Suchmaschinen und Handytarif-Anbietern. Der Bericht, der Fragebogen der Umfrage sowie die erhobenen Rohdaten sind auf der Website der RTR abrufbar. Die Daten sind als Open-Data frei zugänglich und nutzbar.

PUBLIKATIONEN

Kommunikationsbericht 2021

Der Kommunikationsbericht 2021 erfüllt die gesetzlich festgelegten Berichtspflichten nach dem KommAustria-Gesetz sowie nach dem Telekommunikationsgesetz und dokumentiert die behördliche Sacharbeit. Darüber hinaus bietet er einen Einblick in die Entwicklung der von der Regulierung umfassten Märkte.

RTR Roaming Monitor - 1. Ausgabe 2022

Die erste Ausgabe der aktualisierten Publikationsreihe RTR Roaming Monitor enthält Daten bis zum 3. Quartal 2021 und steht als interaktive Datenvisualisierung zur Verfügung.

RTR Telekom Monitor Jahresbericht 2021

Der RTR Telekom Monitor Jahresbericht enthält umfangreiche Marktdaten zu Mobilfunk, Breitband, Festnetz und Mietleitungen bis einschließlich 4. Quartal 2021 und gibt überdies einen Einblick in internationale Entwicklungen.

RTR Post Monitor Jahresbericht 2021

Der RTR Post Monitor Jahresbericht gibt einen Einblick in aktuelle Trends und enthält Daten zum österreichischen Post-Markt sowie zu internationalen Entwicklungen bis einschließlich 4. Quartal 2021.

RTR Netzneutralitätsbericht

Der Bericht, der spätestens mit 30. Juni zu veröffentlichen ist, gibt Auskunft über den Stand der Offenheit des Internets in Österreich im Zeitraum vom 1. Mai 2021 bis 30. April 2022 und darüber, ob bzw. welche Maßnahmen von der RTR/TKK ergriffen werden mussten, um die Offenheit des Internets in Österreich sicherzustellen.

REMINDER

23. Salzburger Telekom Forum

Das 23. Salzburger Telekom Forum, unter dem Motto Netzsicherheit, findet am 5. und 6. September statt:

Montag, 5. September, 10:30 Uhr bis 17:00 Uhr
1. Themenfeld: Cybersecurity als Gebot der Stunde
2. Themenfeld: Netzsicherheit in Österreich

Networking ab 18:30 Uhr

Dienstag, 6. September, 9:00 Uhr bis 12:30 Uhr
3. Themenfeld: Netzsicherheit im Recht

Das detaillierte Programm wird voraussichtlich Ende Juli auf der Website der RTR veröffentlicht.

Anmeldungen sind ab sofort unter daniela.andreasch@rtr.at möglich.

Wir freuen uns auf Ihre Teilnahme und auf spannende Gespräche!

Autoren

Die Beiträge der aktuellen Ausgabe von RTR AKTUELL 2/2022 des Fachbereichs Telekommunikation und Post wurden verfasst von:

Gregor Gradnig
Dubravko Jagar
Robert Kiraly
Ulrich Latzenhofer
Kurt Reichinger
Klaus Steinmaurer