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

Das vorliegende Dokument enthält die geplante Telekom-Netzsicherheitsverordnung 2020 („TK-NSiV 2020“) zur öffentlichen Konsultation gemäß § 128 TKG 2003. Zur besseren Übersicht sind die Erläuternden Bemerkungen direkt nach den jeweiligen Bestimmungen zu finden.

Die TK-NSiV 2020 normiert einerseits Informationspflichten von Betreibern elektronischer Kommunikationsnetze und Anbietern elektronischer Kommunikationsdienste bei Sicherheitsvorfällen im Zusammenhang mit elektronischen Kommunikationsnetzen und -diensten, die zu beträchtlichen Auswirkungen auf den Netzbetrieb oder die Dienstebereitstellung geführt haben. Zudem regelt sie das Vorgehen der Regulierungsbehörde bei derartigen Sicherheitsvorfällen. Überdies legt sie Rahmenbedingungen einer Erstattung von Mitteilungen in Bezug auf Sicherheitsvorfälle ohne beträchtliche Auswirkungen auf Netzbetrieb oder Dienstebereitstellung fest.

Andererseits stellt sie Anforderungen an die von Betreibern elektronischer Kommunikationsnetze und Anbietern elektronischer Kommunikationsdienste zur Gewährleistung einer angemessenen Beherrschung der Risiken für elektronische Kommunikationsnetze und -dienste und Aufrechterhaltung des diesbezüglich geeigneten Sicherheitsniveaus zu ergreifenden Mindestsicherheitsmaßnahmen unter besonderer Berücksichtigung der Sicherheit von 5G-Netzen auf. Hinsichtlich der Sicherheit von 5G-Netzen werden einige der Vorgaben aus dem diesbezüglichen EU-Instrumentarium („5G-Toolbox“) umgesetzt.

Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH)
Mariahilfer Straße 77–79
1060 WIEN, ÖSTERREICH
www.rtr.at
E: rtr@rtr.at
T: +43 1 58058-0
F: +43 1 58058-9191
FN 208312t, HG Wien
UID-Nr.: ATU43773001

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

Aufgrund des § 16a Abs. 9 des Bundesgesetzes, mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2003 – TKG 2003, BGBl. I Nr. 70/2003 idF BGBl. I Nr. 23/2020), wird im Einvernehmen mit der Bundesministerin für Landwirtschaft, Regionen und Tourismus sowie dem Bundesminister für Inneres verordnet:

Zweck und Anwendungsbereich

§ 1. (1) Mit dieser Verordnung werden Informationspflichten von Betreibern elektronischer Kommunikationsnetze und Anbietern elektronischer Kommunikationsdienste bei Sicherheitsvorfällen im Zusammenhang mit elektronischen Kommunikationsnetzen und -diensten, die zu beträchtlichen Auswirkungen auf den Netzbetrieb oder die Dienstebereitstellung geführt haben, sowie das Vorgehen der Regulierungsbehörde bei derartigen Sicherheitsvorfällen festgelegt. Überdies werden Rahmenbedingungen einer Erstattung von Mitteilungen in Bezug auf Sicherheitsvorfälle ohne beträchtliche Auswirkungen auf Netzbetrieb oder Dienstebereitstellung geschaffen.

(2) Darüber hinaus werden Anforderungen an die von Betreibern elektronischer Kommunikationsnetze und Anbietern elektronischer Kommunikationsdienste zur Gewährleistung einer angemessenen Beherrschung der Risiken für elektronische Kommunikationsnetze und -dienste und Aufrechterhaltung des diesbezüglich geeigneten Sicherheitsniveaus zu ergreifenden Mindestsicherheitsmaßnahmen unter besonderer Berücksichtigung der Sicherheit von 5G-Netzen festgelegt.

(3) Diese Verordnung gilt für alle im Bundesgebiet betriebenen öffentlichen elektronischen Kommunikationsnetze mit Ausnahme von Rundfunknetzen und für alle im Bundesgebiet öffentlich angebotenen elektronischen Kommunikationsdienste mit Ausnahme von Übertragungsdiensten in Rundfunknetzen.

EB zu § 1

Abs. 1: Abweichend von § 3 Z 7 NISG wird hier der Begriff Sicherheitsvorfall konform zu Art 2 Z 42 der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (European Electronic Communications Code – EECC) verwendet.

Abs. 3: Für Rundfunknetze und für Übertragungsdienste in Rundfunknetzen besteht eine Zuständigkeit der Kommunikationsbehörde Austria.

Begriffsbestimmungen

§ 2. Im Sinne dieser Verordnung bedeuten

1. Sicherheit von Netzen und Diensten: die Fähigkeit von Kommunikationsnetzen und -diensten, auf einem bestimmten Vertrauensniveau Ereignissen entgegenzuwirken, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit dieser Netze und Dienste, der gespeicherten, übermittelten oder verarbeiteten Daten oder der damit zusammenhängenden Dienste, die über diese Kommunikationsnetze oder -dienste angeboten werden bzw. zugänglich sind, beeinträchtigen;
2. böswilliger Angriff: Vorgang, bei dem sich eine Person oder ein Programm vorsätzlich ohne Berechtigung logischen oder physischen Zugang oder die Zugangsmöglichkeit zu einem Netz oder dessen Komponenten, einem System oder einer Anwendung, zu Daten oder zu anderen IT-Ressourcen verschafft oder die Funktion des angegriffenen Netzes oder Dienstes vorsätzlich beeinträchtigt;
3. menschliches Versagen: fahrlässiges Handeln (zB Falschkonfiguration oder fehlerhafter Einsatz von Netzelementen, Plattformen, Anwendungen [Software], Datensicherung und Datenbanken, irrtümliche Anwendung von Verfahren auf Abläufe betreffend Konfigurationsmanagement, Änderungsmanagement, Identitäts- und Zutrittskontrollabläufe sowie Fehlentscheidungen im Management);
4. Naturereignis: natürliches Phänomen mit Auswirkungen auf Kommunikationsinfrastrukturen wie Unwetter (zB Sturm, schwerer Schneefall, Hitzewelle), Erdbeben, epidemische Krankheit, Flut, Brand, Erdrutsch, Vulkanausbruch oder geänderte Umweltbedingungen durch Sonnenaktivität;
5. Systemfehler: Hardwarefehler, Softwarefehler und Fehler in Betriebsanleitungen, Verfahren oder internen Vorschriften;
6. Drittversagen: Vorgang, dessen Ursache sich außerhalb der direkten Kontrolle des Betreibers befindet (zB Vorfall bei einem Outsourcingpartner oder bei einer Organisation innerhalb der Lieferkette);
7. Sicherheitsvorfall: ein Ereignis mit nachteiliger Wirkung auf die Sicherheit von Kommunikationsnetzen oder -diensten;
8. unverzüglich: ohne schuldhaftes Zögern;
9. 5G-Netz: Mobilfunknetz der fünften Generation, dessen einschlägige Netzinfrastrukturelemente auf weltweit vereinbarten technischen Normen für die Mobilfunk- und Drahtloskommunikation beruhen und fortgeschrittene Leistungsmerkmale wie sehr hohe Datengeschwindigkeit und -kapazität, Kommunikation mit niedriger Latenzzeit, ultra-hohe Zuverlässigkeit oder Unterstützung einer großen Zahl verbundener Geräte aufweisen. Die Netzinfrastrukturelemente eines 5G-Netzes können auch vorhandene Netzbestandteile umfassen, denen frühere Generationen mobiler und drahtloser Kommunikationstechnik (4G oder 3G) zugrunde liegen.

EB zu § 2

Z 1: Da der Begriff „Sicherheit von Netzen und Diensten“ bislang nicht in den Begriffsbestimmungen des TKG 2003 enthalten war, wurde eine entsprechende EECC-konforme Definition aufgenommen.

Z 2: Beim böswilligen Angriff wurde die Möglichkeit einer vorsätzlichen Beeinträchtigung der Funktion des angegriffenen Netzes oder Dienstes vorgesehen, um auch DDoS-Attacken erfassen zu können.

Z 8: „Unverzüglich“ bedeutet ohne schuldhaftes Zögern, wobei die Informationspflichten jedenfalls nicht auf die Geschäftszeiten des Betreibers beschränkt sind. Die Informationspflicht besteht, sobald absehbar ist, dass der Vorfall beträchtliche Auswirkungen hervorrufen wird. Im Zweifel wird von einer Meldepflicht auszugehen sein.

Z 9: In Z 9 wurde eine Definition des Begriffs „5G-Netz“ aufgenommen, die jener in Punkt 2 lit. a der Empfehlung (EU) 2019/534 der Kommission vom 26. März 2019 „Cybersicherheit der 5G-Netze“ entspricht.

Informationspflichten

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

1. Datum und Uhrzeit des Beginns des Vorfalls;
2. Ursache des Vorfalls nach folgenden Kategorien: Naturereignis, menschliches Versagen, böswilliger Angriff, Systemfehler oder Drittversagen;
3. betroffenes Betriebsmittel (zB mobile Basisstation, Netzknoten, Home Subscriber Server, internationale Datenübertragungsanbindung);
4. betroffener Dienst (nach Kategorien: Festnetztelefonie, Mobiltelefonie, fester Internetzugang, mobiler Internetzugang) und zu Grunde liegende Technologie;
5. Anzahl der in der jeweiligen Dienstekategorie betroffenen Teilnehmer:
   a. bei Festnetztelefonie nach Anzahl der betroffenen Anschlüsse,
   b. bei Mobiltelefonie nach Anzahl der betroffenen aktivierten SIM-Karten,
   c. bei festen Internetzugängen nach Anzahl der betroffenen Anschlüsse,
   d. bei mobilen Internetzugängen nach Anzahl der betroffenen aktivierten SIM-Karten;
6. Auswirkungen auf die Erreichbarkeit von Notrufnummern (betroffene Notrufnummern, Anzahl der betroffenen Teilnehmer in der jeweiligen Dienstekategorie);
7. Anzahl der in allen Dienstekategorien insgesamt betroffenen Teilnehmer;
8. ergriffene Maßnahmen zur Behebung des Vorfalls und Wiederherstellung des Dienstes;

9. Vorgehen nach dem Vorfall (Risikominimierung in künftigen Fällen, Schätzung der Effizienz der ergriffenen Maßnahmen);
10. langfristig bedeutsame Erkenntnisse aus dem Vorfall;
11. Wiederherstellungszeitraum vom Beginn des Vorfalls bis zur Wiederherstellung des betroffenen Dienstes;
12. betroffene Zusammenschaltungen in Form der betroffenen Zusammenschaltungspartner und betroffenen Zusammenschaltungsstandorte;
13. Kurzbeschreibung und Analyse des Vorfalls;
14. gegebenenfalls Angaben über eine erfolgte oder geplante Information der Öffentlichkeit.

Erst- und Folgemeldungen sind über das Meldeportal der Regulierungsbehörde einzubringen. Bei Nichtverfügbarkeit des Meldeportals der Regulierungsbehörde können Meldungen in Bezug auf einen Sicherheitsvorfall mit beträchtlichen Auswirkungen abweichend von dem in Satz 1 und 2 beschriebenen elektronischen Format erfolgen.

(2) Beträchtliche Auswirkungen liegen dann vor, wenn

1. der Vorfall bis zu einschließlich einer Stunde dauert und die Anzahl der betroffenen Teilnehmer der jeweiligen Dienstekategorie gemäß Abs. 1 Z 5 500 000 übersteigt oder
2. der Vorfall mehr als eine Stunde dauert und die Anzahl der betroffenen Teilnehmer der jeweiligen Dienstekategorie gemäß Abs. 1 Z 5 15% der Gesamtzahl der Nutzer des Dienstes im Bundesgebiet oder 500 000 übersteigt oder
3. der Vorfall mehr als zwei Stunden dauert und die Anzahl der betroffenen Teilnehmer der jeweiligen Dienstekategorie gemäß Abs. 1 Z 5 10% der Gesamtzahl der Nutzer des Dienstes im Bundesgebiet oder 250 000 übersteigt oder
4. der Vorfall mehr als vier Stunden dauert und die Anzahl der betroffenen Teilnehmer der jeweiligen Dienstekategorie gemäß Abs. 1 Z 5 5% der Gesamtzahl der Nutzer des Dienstes im Bundesgebiet oder 150 000 übersteigt oder
5. der Vorfall mehr als sechs Stunden dauert und die Anzahl der betroffenen Teilnehmer der jeweiligen Dienstekategorie gemäß Abs. 1 Z 5 2% der Gesamtzahl der Nutzer des Dienstes im Bundesgebiet oder 100 000 übersteigt oder
6. der Vorfall mehr als acht Stunden dauert und die Anzahl der betroffenen Teilnehmer der jeweiligen Dienstekategorie gemäß Abs. 1 Z 5 1% der Gesamtzahl der Nutzer des Dienstes im Bundesgebiet oder 50 000 übersteigt oder
7. der Vorfall mehr als 16 Stunden dauert und die Anzahl der betroffenen Teilnehmer der jeweiligen Dienstekategorie iSd Abs 1 Z 5 10 000 übersteigt oder
8. eine Notrufnummer aus einem Kommunikationsnetz für Teilnehmer eines verfügbaren öffentlichen Telefondienstes nicht erreichbar ist oder der Telefondienst für den Teilnehmer nur teilweise verfügbar und mindestens eine Notrufnummer nicht erreichbar ist. Beträchtliche Auswirkungen liegen auch dann vor, wenn der Telefondienst der Notrufleitstelle, an der ein Notruf terminiert, für passive Gespräche nicht verfügbar ist, unabhängig davon, ob die Notrufnummer erreichbar ist oder nicht.

(3) Liegt die Bekanntgabe des Vorfalls im öffentlichen Interesse, haben Betreiber von Kommunikationsnetzen und -diensten auf Verlangen der Regulierungsbehörde unverzüglich die Öffentlichkeit darüber zu informieren. Bei Gefahr in Verzug kann die Regulierungsbehörde die Öffentlichkeit auch unmittelbar informieren.

(4) Die Regulierungsbehörde hat Daten zur Ermittlung der in Abs. 2 angeführten Schwellwerte auf ihrer Website zu veröffentlichen.

(5) Die Regulierungsbehörde hat eine erfolgte Mitteilung nach Abs. 1 unverzüglich an den Bundesminister für Inneres weiterzuleiten (§ 16a Abs. 5a TKG 2003, BGBl I Nr. 70/2003 idF BGBl I Nr. 23/2020).

EB zu § 3

Abs. 1: Die von den Betreibern öffentlicher Kommunikationsnetze oder Anbietern öffentlicher Kommunikationsdienste zu übermittelnden Informationen ergeben sich aus dem von den Mitgliedstaaten der Europäischen Union unter Mitwirkung der ENISA verabschiedeten Dokument „Technical Guideline on Reporting Incidents", Version 2.1, Oktober 2014. Das Dokument liegt bei der Regulierungsbehörde zur Einsichtnahme auf und ist auf deren Website unter http://www.rtr.at/de/tk/Netzsicherheit/Article_13a_ENISA_Technical_Guideline_On_Incident_Reporting_v2_1.pdf allgemein zugänglich.

Abs. 1 Z 1: Ist der exakte Beginnzeitpunkt des Vorfalls nicht feststellbar, kann auch der Zeitpunkt angegeben werden, an dem der Betroffene erstmals vom Vorfall Kenntnis erlangt hat.

Abs. 1 Z 3: vgl hierzu ENISA-Guideline „Threats and Assets", https://www.rtr.at/de/tk/Netzsicherheit/Article_13a_ENISA_Technical_Guideline_On_Threats_And_Assets.pdf , Version 1.2, August 2015.

Abs. Z 5: Bei Erbringung von Diensten auf einer SIM-Karte, die zu mehr als einer Dienstekategorie gehören (Mobiltelefonie, mobiler Internetzugang), ist die Anzahl der betroffenen SIM-Karten jeweils in den Dienstekategorien lit. b und d anzugeben. Bei Erbringung von Diensten über einen Festnetzanschluss, die sowohl zur Dienstekategorie Festnetztelefonie als auch zur Dienstekategorie fester Internetzugang gehören, ist die Anzahl jeweils in den Dienstekategorien lit. a und c anzugeben.

Abs. 1 Z 5 lit. b und d: Falls die exakte Anzahl nicht ermittelbar ist, kann diese anhand des auf Erfahrungswerten basierenden Mittelwerts der Nutzer der betroffenen Funkzellen abgeschätzt werden.

Abs. 2: Unter den betroffenen Teilnehmern der jeweiligen Dienstekategorie sind nur jene Teilnehmer zu verstehen, die dem Anbieter des betroffenen Kommunikationsdienstes zuzurechnen sind.

Abs. 4: Bei der Ermittlung der Gesamtzahlen der Nutzer eines Dienstes im Bundesgebiet kann sich der Betreiber an den von der Regulierungsbehörde unter https://www.rtr.at/de/tk/MitteilungVorflle veröffentlichten Daten orientieren.

Warnhinweis

§ 4. (1) Unbeschadet von § 23 des Bundesgesetzes zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG, BGBl. I Nr. 111/2018), können Betreiber elektronischer Kommunikationsnetze und Anbieter elektronischer Kommunikationsdienste von ihnen als sicherheitsrelevant erachtete Risiken und

Vorfälle, die nicht der Meldepflicht nach § 3 Abs. 1 unterliegen, der Regulierungsbehörde übermitteln. Dieser Warnhinweis darf keine personenbezogenen Daten natürlicher Personen (abgesehen von jenen des Einmelders) enthalten.

(2) Der Warnhinweis soll sämtliche relevanten Angaben zum Risiko bzw. zum Vorfall und zu den technischen Rahmenbedingungen, die im Mitteilungszeitpunkt bekannt sind, enthalten, insbesondere die vermutete oder tatsächliche Ursache und die betroffenen Betriebsmittel. Angaben über später bekanntgewordene Umstände zum Risiko oder Vorfall sind in Folgemitteilungen zu übermitteln. Warnhinweis und Folgemitteilungen sind in dem für verpflichtende Meldungen vorgegebenen elektronischen Format über das Meldeportal der Regulierungsbehörde einzubringen; § 3 Abs 1, letzter Satz, gilt entsprechend. Die Regulierungsbehörde hat den Warnhinweis sowie die jeweilige Mitteilung an das zuständige Computer-Notfallteam gemäß § 23 Abs. 3 NISG und mit Einwilligung des Einmelders an den Bundesminister für Inneres weiterzuleiten. Das zuständige Computer Notfallteam kann den Warnhinweis und die Mitteilungen zusammengefasst an den Bundesminister für Inneres weiterleiten.

EB zu § 4

Die Bestimmungen in Bezug auf Warnhinweis und Folgemitteilungen in Bezug auf Risiken oder Vorfälle, die nicht der Meldepflicht nach § 3 Abs 1 unterliegen, sind den §§ 19 Abs. 3, 23 NISG nachgebildet und enthalten diesbezügliche Rahmenbedingungen.

Mindestsicherheitsmaßnahmen

§ 5. (1) Zur Gewährleistung eines angemessenen Sicherheitsniveaus und im Interesse einer Vermeidung von Sicherheitsvorfällen haben Betreiber von elektronischen Kommunikationsnetzen und Anbieter von elektronischen Kommunikationsdiensten Maßnahmen gemäß § 16a Abs 1 TKG 2003 zu konzipieren, zu ergreifen und zu dokumentieren sowie eine Information Security Policy festzulegen. Diese Maßnahmen sollen ein Sicherheitsniveau der Netze und Dienste gewährleisten, das angesichts des bestehenden Risikos angemessen ist. Insbesondere haben die Maßnahmen und die Information Security Policy dem Stand der Technik zu entsprechen und folgende Bereiche abzudecken:

1. Governance und Risikomanagement (Information Security Policy, Risikomanagementsystem, Sicherheitsrollen und -verantwortung, Umgang mit Dritten),
2. Sicherheit im Hinblick auf Personal (Hintergrundüberprüfung, Sicherheitswissen und -training, Personalwechsel, Disziplinarmaßnahmen bei Verstößen),
3. Sicherheit von Systemen und Betriebsstätten (physische Sicherheit, Sicherheit des Umfelds, Sicherheit des Materials, Versorgungssicherheit, Zutrittskontrolle, Informationssicherheit),
4. Betriebsmanagement (Betriebsabläufe, Änderungsmanagement, Umgang mit Betriebsmitteln),
5. Störfallmanagement (Abläufe, Feststellung, Reaktion, Eskalation, Berichtswesen),
6. Betriebliches Kontinuitätsmanagement (Verfügbarkeit und Aufrechterhaltung der Dienste, Notfallpläne & Notfallwiederherstellung),

7. Monitoring, Audits, Tests (Monitoring/Protokollierung, Stellvertretungs- und Notfallsübungen, Systemtests, Sicherheitsbewertung, Konformitätsüberwachung und Auditierungsverfahren).

(2) Betreiber elektronischer Kommunikationsnetze und Anbieter elektronischer Kommunikationsdienste haben Unterlagen über die Maßnahmen gemäß Abs. 1 vorzuhalten und der Regulierungsbehörde auf Anforderung in einem allgemein lesbaren elektronischen Format Informationen zur Beurteilung der Sicherheit ihrer Netze und Dienste sowie über die von ihnen ergriffenen und dokumentierten Sicherheitsmaßnahmen gemäß Abs. 1 und ihre Information Security Policy zu übermitteln.

EB zu § 5

Abs. 1: Die Bereiche, die Betreiber öffentlicher Kommunikationsnetze oder Anbieter öffentlicher Kommunikationsdienste durch Sicherheitsmaßnahmen abdecken müssen, ergeben sich aus dem von den Mitgliedstaaten der Europäischen Union unter Mitwirkung der ENISA verabschiedeten Dokument „Technical Guideline on Security Measures", Version 2.0, Oktober 2014. Das Dokument liegt bei der Regulierungsbehörde zur Einsichtnahme auf und ist auch auf deren Website unter https://www.rtr.at/de/tk/Netzsicherheit/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf allgemein zugänglich. Zu den Sicherheitsmaßnahmen zählt auch die Festlegung einer Information Security Policy. Darunter ist eine von der Führung einer Organisation approbierte Richtlinie zu verstehen, die den Ansatz der Organisation zur Erreichung von Informationssicherheitszielen darlegt. Eine Information Security Policy sollte Anforderungen adressieren, die sich aus der Geschäftsstrategie, Gesetzen und Vereinbarungen sowie gegenwärtigen und zu erwartenden Bedrohungen für die Informationssicherheit ergeben. Die Information Security Policy sollte folgende Angaben enthalten:

a) Definition der Informationssicherheit, Ziele und Grundsätze, von denen man sich bei allen Tätigkeiten betreffend Informationssicherheit leiten lässt;
b) Zuweisung von allgemeinen und spezifischen Verantwortlichkeiten für das Informationssicherheitsmanagement an definierte Rollen;
c) Prozesse zur Behandlung von Abweichungen und Ausnahmen.

Auf einer darunter befindlichen Ebene sollte die Information Security Policy durch themenspezifische Policies unterstützt werden, die die Umsetzung von Sicherheitsmaßnahmen konkretisieren und typischerweise so strukturiert sind, dass sie die Bedürfnisse bestimmter Zielgruppen innerhalb der Organisation adressieren oder bestimmte Themen abdecken (vgl ISO/IEC 27002:2013, 5.1.1).

Sicherheitsanforderungen an 5G-Netze

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

Informationssicherheitsmaßnahmen hat ebenfalls diesbezüglich anerkannten Normen zu entsprechen. Jede Nichtkonformität mit einer Anforderung aus diesen Normen ist jeweils zu begründen.

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

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

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

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

EB zu § 6

§ 6 setzt die Empfehlung (EU) 2019/534 der Europäischen Kommission vom 26. März 2019 zur Cybersicherheit der 5G-Netze um und enthält hinsichtlich der von Betreibern öffentlicher Kommunikationsnetze oder Anbietern öffentlicher Kommunikationsdienste zu ergreifenden Sicherheitsmaßnahmen ergänzende Bestimmungen, die unter Berücksichtigung der diesbezüglich auf EU-Ebene nach Durchführung einer entsprechenden Risikoabschätzung zusammengefassten Empfehlungen („EU-Instrumentarium", vgl. das Dokument CG 01/2020 der NIS Cooperation Group „Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures", https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures) sowie die Mitteilung der Europäischen Kommission COM(2020)50 vom 29.01.2020 an das Parlament, den Rat, den Wirtschafts- und Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: „Sichere 5G-Einführung in der EU – Umsetzung des EU-Instrumentariums") sicherstellen sollen, dass erhöhten Sicherheitsrisiken, die mit dem Betrieb von 5G-Netzen verbunden sind, angemessen begegnet werden kann.

Abs. 1: Da die von den Betreibern zu ergreifenden Sicherheitsmaßnahmen ein Sicherheitsniveau gewährleisten müssen, das zur Beherrschung der Risiken geeignet ist, und die Risiken von der Eintrittswahrscheinlichkeit und den potenziellen Auswirkungen eines Sicherheitsvorfalls abhängen, ist es gerechtfertigt, das Ausmaß des Risikos unter Berücksichtigung der Anzahl der Teilnehmer zu bewerten. Da vergleichbare Vorschriften wie zB § 10 Abs. 1 Z 2 lit. a Netz- und Informationssicherheitssystemverordnung („NISV"), BGBl. II Nr. II 215/2019, eine Zahl von 88.000 Teilnehmern bei Kommunikationsdiensten im Bereich des Betriebs von DNS-Diensten als wesentlichen Diensten im Sektor „Digitale Infrastruktur" heranziehen, ist es gerechtfertigt, auch zur Bewertung des erhöhten Risikos durch den Betrieb von 5G-Netzen in einer zukunftsgerichteten Betrachtung unter Berücksichtigung der Entwicklung der Teilnehmerzahlen bis zum ersten Nachweiszeitpunkt von einem entsprechend höheren Wert auszugehen.

Um dem erhöhten Risiko zu begegnen, sind ein funktionierendes Informationssicherheitsmanagement sowie allgemeine und telekommunikationsspezifische Informationssicherheitsmaßnahmen erforderlich. Das funktionierende Informationssicherheitsmanagement kann durch Vorlage eines Auditberichts über die Einhaltung der Anforderungen gemäß „ÖVE/ÖNORM EN ISO/IEC 27 001:2017, Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmanagementsysteme - Anforderungen (ISO/IEC 27 001:2013 + Cor 1:2014 + Cor 2:2015)" nachgewiesen werden. Die Festlegung und Umsetzung allgemeiner Informationssicherheitsmaßnahmen kann durch eine Anwendbarkeitserklärung iSv. ISO 27 001, Abschnitt 6.1.3, lit. d, dokumentiert werden. Die Festlegung und Umsetzung telekommunikationsspezifischer Informationssicherheitsmaßnahmen kann durch eine analoge Erklärung zur Festlegung und Umsetzung der in „ÖVE/ÖNORM EN ISO/IEC 27 011:2020, Informationstechnik - Sicherheitsverfahren - Leitfaden für Informationssicherheitsmaßnahmen auf Grundlage von ISO/IEC 27002 für Telekommunikationsorganisationen" angeführten Sicherheitsmaßnahmen dokumentiert werden.

Anstelle der vorerwähnten Normen können auch von der Regulierungsbehörde als gleichwertig angesehene Standards wie zB die Standards 200-1, 200-2, 200-3 des dt. Bundesamts für Sicherheit in der Informationstechnik iVm. ITU-T-Empfehlung X.1051 angewandt werden. Zur Erstellung von Auditberichten können gegebenenfalls diesbezüglich akkreditierte Prüfstellen oder qualifizierte Stellen gemäß § 3 Z 11 NISG herangezogen werden. Der für den erstmaligen Nachweis genannte Zeitpunkt soll jenen Betreibern, die die Normen derzeit nicht erfüllen, ermöglichen, die diesbezüglichen Voraussetzungen für eine Zertifizierung zu schaffen und den Zertifizierungsprozess zu durchlaufen. Die Dreijahresfrist für die Wiedervorlage entspricht üblichen Auditzyklen.

Abs. 2: Betreiber von 5G-Netzen mit mehr als 100 000 Teilnehmern haben aufgrund des EU-Instrumentariums überdies auch die in den im Anhang angeführten relevanten 3GPP- und ETSI-Technologiestandards (vgl. https://www.3gpp.org/DynaReport/33-series.htm) vorgesehenen Sicherheitsmaßnahmen zu ergreifen und durch eine Konformitätserklärung des Betreibers zu dokumentieren. Der Anforderung des EU-Instrumentariums, in angemessener Weise auch eine Umsetzung optionaler Teile der 3GPP-Technologiestandards sicherzustellen, wird dadurch Rechnung getragen, dass der Betreiber Abweichungen hinsichtlich der optionalen Teile zB durch vergleichbare Sicherheitsmaßnahmen, mit denen dasselbe Sicherheitsziel erreicht wird, zu begründen hat. Die Notwendigkeit zur Einhaltung der angeführten ETSI-Standards zu Network Function Virtualisation („NFV“, vgl. https://www.etsi.org/standards#page=1&search=&title=1&etsiNumber=1&content=1&version=0&onApproval=0&published=1&historical=0&startDate=&endDate=&harmonized=0&keyword=&TB=799&stdType=&frequency=&mandate=&collection=&sort=1) ergibt sich aus dem Umstand, dass die durch die Virtualisierung herbeigeführte Komplexität auch erhöhte Risiken in sich birgt, und der Anforderung des EU-Instrumentariums, dass 5G-Betreiber in Bezug auf NFV gute Praktiken befolgen sollen. Die Notwendigkeit zur Einhaltung der im ENISA-Dokument „Indispensable Baseline Security Requirements for the Procurement of Secure ICT Products and Services“ (vgl. https://www.enisa.europa.eu/publications/indispensable-baseline-security-requirements-for-the-procurement-of-secure-ict-products-and-services) angeführten Empfehlungen folgt der Anforderung im EU-Instrumentarium zur Einhaltung spezifischer Sicherheitsstandards im Beschaffungsprozess bei IKT-Komponenten und Dienstleistungen.

Abs. 3: Die angeführten Sicherheitsmaßnahmen entsprechen zusätzlichen Sicherheitsmaßnahmen im EU-Instrumentarium, die sich nicht aus den Anforderungen in Abs. 1 und 2 ergeben.

So soll etwa der Betrieb des Network Operation Centers und Security Operation Centers in eigenen Räumlichkeiten (Räume unter Kontrolle des Betreibers eines 5G-Netzes, zB auch selbst angemietete Rechenzentren, nicht aber Räume externer Dienstleister) und das effektive Monitoring aller kritischen Netzkomponenten und sensibler Teile der 5G-Netze sicherstellen, dass Anomalien entdeckt und Bedrohungen (wie zB durch kompromittierte Endgeräte inkl IoT-Komponenten) identifiziert und verhindert werden.

Der Schutz des Management-Verkehrs von Kommunikationsnetzen oder -diensten soll nicht autorisierte Änderungen von Netz- oder Dienstkomponenten verhindern.

Der physische Schutz von kritischen Netzkomponenten und sensiblen Teilen der 5G-Netze mit risikobasiertem Ansatz hat auch Netzkomponenten außerhalb des Kernnetzes wie zB Basisstationen zu umfassen, die zur Erreichung niedrigerer Latenzzeichen miteinander kommunizieren („Multi-access Edge Computing").

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

Das Risikoprofil von Lieferanten kann auf Basis verschiedener Faktoren bewertet werden wie insbesondere die Wahrscheinlichkeit einer Einflussnahme aus Nicht-EU-Staaten, die Lieferfähigkeit des Lieferanten und die Gesamtqualität seiner Produkte und Sicherheitspraktiken. Dies bedürfte aus Sicht der RTR-GmbH jedoch einer gesonderten rechtlichen Grundlage.

Abs. 4: Sicherheitsrelevante Komponenten, die bei Betrieb des 5G-Netzes eingesetzt werden, sind – gruppiert und nach Funktionen – in Anhang 2 angeführt.

Schlussbestimmungen

§ 7. Alle in dieser Verordnung verwendeten personenbezogenen Bezeichnungen gelten gleichermaßen für alle Geschlechter.

Inkrafttreten

§ 8. Diese Verordnung tritt am XX.XX.2020 in Kraft.

Anhang 1

3GPP-Standards:

- 3GPP TS 33.116 V15.0.0 (2018-06), Security Assurance Specification (SCAS) for the MME network product class
- 3GPP TS 33.117 V16.3.0 (2019-12), Catalogue of general security assurance requirements
- 3GPP TS 33.216 V16.2.0 (2019-12), Security Assurance Specification (SCAS) for the evolved Node B (eNB) network product class
- 3GPP TS 33.250 V15.1.0 (2019-09), Security assurance specification for the PGW network product class
- 3GPP TS 33.401 V16.1.0 (2019-12), 3GPP System Architecture Evolution (SAE); Security architecture
- 3GPP TS 33.402 V15.1.0 (2018-06), 3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses
- 3GPP TS 33.501 V16.1.0 (2019-12), Security architecture and procedures for 5G System
- 3GPP TS 33.511 V16.2.0 (2019-12), Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class
- 3GPP TS 33.512 V16.1.0 (2019-12), 5G Security Assurance Specification (SCAS); Access and Mobility management Function (AMF)
- 3GPP TS 33.513 V16.1.0 (2019-12), 5G Security Assurance Specification (SCAS); User Plane Function (UPF)
- 3GPP TS 33.514 V16.1.0 (2019-12), 5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) network product class
- 3GPP TS 33.515 V16.1.0 (2019-12), 5G Security Assurance Specification (SCAS) for the Session Management Function (SMF) network product class
- 3GPP TS 33.516 V16.1.0 (2019-12), 5G Security Assurance Specification (SCAS) for the Authentication Server Function (AUSF) network product class
- 3GPP TS 33.517 V16.1.0 (2019-12), 5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) network product class
- 3GPP TS 33.518 V16.1.0 (2019-12), 5G Security Assurance Specification (SCAS) for the Network Repository Function (NRF) network product class
- 3GPP TS 33.519 V16.1.0 (2019-12), 5G Security Assurance Specification (SCAS) for the Network Exposure Function (NEF) network product class

ETSI-Standards:

- ETSI GS NFV-SEC 001 V1.1.1 (2014-10), Network Functions Virtualisation (NFV); NFV Security; Problem Statement
- ETSI GS NFV-SEC 002 V1.1.1 (2015-08), Network Functions Virtualisation (NFV); NFV Security; Cataloguing security features in management software
- ETSI GS NFV-SEC 003 V1.1.1 (2014-12), Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance
- ETSI GS NFV-SEC 004 V1.1.1 (2015-09), Network Functions Virtualisation (NFV); NFV Security; Privacy and Regulation; Report on Lawful Interception Implications
- ETSI GS NFV-SEC 006 V1.1.1 (2016-04), Network Functions Virtualisation (NFV); Security Guide; Report on Security Aspects and Regulatory Concerns

- ETSI GS NFV-SEC 009 V1.1.1 (2015-12), Network Functions Virtualisation (NFV); NFV Security; Report on use cases and technical approaches for multi-layer host administration
- ETSI GS NFV-SEC 010 V1.1.1 (2016-04), Network Functions Virtualisation (NFV); NFV Security; Report on Retained Data problem statement and requirements
- ETSI GS NFV-SEC 012 V3.1.1 (2017-01), Network Functions Virtualisation (NFV) Release 3; Security; System architecture specification for execution of sensitive NFV components
- ETSI GS NFV-SEC 013 V3.1.1 (2017-02), Network Functions Virtualisation (NFV) Release 3; Security ; Security Management and Monitoring specification
- ETSI GS NFV-SEC 014 V3.1.1 (2018-04), Network Functions Virtualisation (NFV) Release 3; NFV Security; Security Specification for MANO Components and Reference points
- ETSI GS NFV-SEC 021 V2.6.1 (2019-06), Network Functions Virtualisation (NFV) Release 2; Security; VNF Package Security Specification
- ETSI GS NFV-SEC 022 V2.7.1 (2020-01), Network Functions Virtualisation (NFV) Release 2; Security; Access Token Specification for API Access

ENISA-Dokumente:

- ENISA Indispensable Baseline Security Requirements for the Procurement of Secure ICT Products and Services, Version 1.0, December 2016

Anhang 2

Liste von Funktionen der Komponenten von 5G-Netzen iSd § 6 Abs 4

Zugangsnetz

(gemäß 3GPP TS 23.002 V15.0.0 (2018-03), Network architecture)

- 4G-Basisstation Evolved Node B (eNodeB, eNB)
- Home eNodeB Subsystem (HeNS)

(gemäß 3GPP TS 38.401 V16.0.0 (2019-12), NG-RAN; Architecture description)

- 5G-Basisstation gNB inklusive gNB Central Unit (gNB-CU) und gNB Distributed Unit (gNB-DU)

Paketvermitteltes Kernnetz

(gemäß 3GPP TS 23.002 V15.0.0 (2018-03), Network architecture)

- 3GPP Authentication, Authorization and Accounting (AAA) Proxy
- 3GPP Authentication, Authorization and Accounting (AAA) Server
- Access Network Discovery and Selection Function (ANDSF)
- Application Front Ends (AFE)
- Application Function (AF)
- Border gateway (BG)
- Closed Subscriber Group (CSG) List Server
- Closed Subscriber Group (CSG) Subscriber Server (CSS)
- Equipment Identity Register (EIR)
- Evolved Packet Data Gateway (ePDG)
- Home Agent (HA)
- Home Subscriber Server (HSS)
- Local Gateway (L-GW)
- Mobility Management Entity (MME)
- Packet Data Gateway (PDG)
- Packet Data Network Gateway (PDN GW) inklusive PDN GW Control Plane (PGW-C) und PDN GW User Plane (PGW-U)
- Policy and Charging Rules Function (PCRF)
- Security Gateway (SEG)
- Serving Gateway (S-GW) inklusive S-GW Control Plane (SGW-C) und S-GW User Plane (SGW-U)
- Signalling Gateway Function (SGW)
- User Data Repository (UDR)
- WLAN Access Gateway (WAG)

(gemäß 3GPP TS 23.501 V16.3.0 (2019-12), System architecture for the 5G System (5GS))

- 5G-Equipment Identity Register (5G-EIR)
- Access and Mobility Management Function (AMF)
- Application Function (AF)
- Authentication Server Function (AUSF)
- Charging Function (CHF)
- Data Network (DN)
- Intermediate NEF (I-NEF)
- Location Management Function (LMF)

- Network Data Analytics Function (NWDAF)
- Network Exposure Function (NEF)
- Network Repository Function (NRF)
- Network Slice Selection Function (NSSF)
- Non-3GPP InterWorking Function (N3IWF)
- Policy Control Function (PCF)
- Security Edge Protection Proxy (SEPP)
- Service Communication Proxy (SCP)
- Session Management Function (SMF)
- Short Message Service Function (SMSF)
- Trusted Non-3GPP Gateway Function (TNGF)
- UE radio Capability Management Function (UCMF)
- Unified Data Management (UDM)
- Unified Data Repository (UDR)
- Unstructured Data Storage Function (UDSF)
- User Plane Function (UPF)
- Wireline Access Gateway Function (W-AGF)

IP Multimedia Subsystem (IMS)

(gemäß 3GPP TS 23.002 V15.0.0 (2018-03), Network architecture)

- Access Transfer Control Function (ATCF)
- Access Transfer Gateway (ATGW)
- Application Server (AS) inklusive Session Initiation Protocol (SIP) Application Server, Open Service Access (OSA) Application Server und Customised Applications for Mobile network Enhanced Logic IP Multimedia Service Switching Function (CAMEL IM-SSF)
- Breakout Gateway Control Function (BGCF)
- Call Session Control Function (CSCF) inklusive Emergency CSCF (E-CSCF), Interrogating CSCF (I-CSCF), Proxy CSCF (P-CSCF) und Serving CSCF (S-CSCF)
- Cellular Text Modem (CTM) inklusive CTM Special Resource Function (CTM-SRF)
- Emergency Access Transfer Function (EATF)
- Home Subscriber Server (HSS)
- IMS Access Gateway (IMS-AGW)
- IMS Media Gateway (IMS-MGW)
- Interconnection Border Control Function (IBCF)
- IP Multimedia Service Switching Function (IM-SSF)
- Location Retrieval Function (LRF)
- Media Gateway Control Function (MGCF)
- Media Resource Broker (MRB)
- Multimedia Resource Function Controller (MRFC)
- Multimedia Resource Function Processor (MRFP)
- Open Service Access Service Capability Servers (OSA SCS-s)
- Service Centralization and Continuity Application Server (SCC AS)
- Subscription Locator Function (SLF)
- Telephony Application Server (TAS)
- Transition Gateway (TrGW)

Dienstekomponenten

(gemäß 3GPP TS 23.002 V15.0.0 (2018-03), Network architecture)

- Bearer Binding and Event Reporting Function (BBERF)
- Broadcast-Multicast Service Centre (BM-SC)
- Cell Broadcast Centre (CBC)
- Cell Broadcast Entity (CBE)
- Customised Applications for Mobile network Enhanced Logic (CAMEL) Service Enviroment (CSE)
- Evolved Serving Mobile Location Centre (E-SMLC)
- Gateway Mobile Location Centre (GMLC)
- Generic User Profile (GUP) Server
- Group Communication Service Application Server (GCS AS)
- IP-Short-Message-Gateway (IP-SM-GW)
- Machine Type Communication- Authentication, Authorization and Accounting (MTC-AAA)
- Machine Type Communication-InterWorking Function (MTC-IWF)
- Mission Critical Push To Talk Application Server (MCPTT AS)
- Multi-cell/multicast Coordination Entity (MCE)
- Multimedia Broadcast Multicast Service Gateway (MBMS-GW)
- Packet Flow Description Function (PFDF)
- Packet Switched Streaming Service Server (PSS Server)
- Proximity-based services (ProSe) Function
- Radio Access Network (RAN) Congestion Awareness Function (RCAF)
- Service Capability Exposure Function (SCEF)
- Short Message Service Router
- Short Message Service Service Centre (SMS-SC)
- Subscription Profile Repository (SPR)
- TCP Proxy Function
- Traffic Detection Function (TDF)
- Traffic Steering Support Function (TSSF)
- Web Real-Time Communication (WebRTC) Web Server Function (WWSF)

Number Portability

(gemäß 3GPP TS 23.002 V15.0.0 (2018-03), Network architecture)

- Mobile Number Portability/Signalling Relay function (MNP-SRF)
- Number Portability Database (NPDB)

Lawful Intercept

(gemäß 3GPP TS 23.002 V15.0.0 (2018-03), Network architecture)

- Administration Function (ADMF)
- Law Enforcement Monitoring Facility (LEMF)
- Mediation and Delivery Function (MDF)

Charging und Billing

(gemäß 3GPP TS 23.002 V15.0.0 (2018-03), Network architecture)

- Billing Domain
- Charging Data Function (CDF)
- Charging Gateway Function (CGF)

- Offline Charging System (OFCS)
- Online Charging Function (OCF)
- Online Charging System (OCS)

Network Function Virtualisation (NFV), Network Slicing, Software Defined Networking (SDN) und Management and Network Orchestration (MANO)
(gemäß ENISA Threat Landscape for 5G Networks, Version 1.0, November 2019)

- Element Management (EM)
- Network Function Lifecycle Management
- Network Functions (NF)
- Network Services Catalogue
- Network Slice Management Function (NSMF)
- NFV Audit Database (NFV-AUD-DB)
- NFV Infrastructure (NFVI)
- NFV Instances repository
- NFV Orchestrator (NFVO)
- NFV Security Controller (SC)
- NFV Security Manager (NSM)
- NFV Security Monitoring Database (NFVSecM DB)
- NFV Security Services Agent (SSA)
- NFV Security Services Provider (SSP)
- NFVI Resources repository
- NFVI Security Manager (ISM)
- NFVI-based Security Function (ISF)
- Operations Support System/Business Support System (OSS/BSS)
- Physical Security Function (PSF)
- SDN Application
- SDN Controller
- SDN Resource
- Security Element Manager (SEM)
- Security Monitoring Analytics System
- Virtual Network Functions (VNF)
- Virtual Security Function (VSF)
- Virtual Security Function VNF Catalog Database (VSF-VNF-CAT)
- Virtualised Infrastructure Manager (VIM)
- VNF Catalogue
- VNF Manager (VNFM)

Multi-access Edge Computing (MEC)
(gemäß ENISA Threat Landscape for 5G Networks, Version 1.0, November 2019)

- Customer facing service (CFS) portal
- MEC host inklusive MEC applications, MEC platform und Virtualisation infrastructure
- MEC host level management inklusive MEC platform manager und Virtualised Infrastructure Manager (VIM)
- Multi-access edge orchestrator
- User application life-cycle management (LCM) proxy

Physische aktive Vermittlungs- und Übertragungssysteme

- Richtfunk, Switches, Router etc

Komponenten mit physischen Rechner-, Speicher- und Netzwerkressourcen

- Server, Cloud-Speicher etc

Telecommunication Management

(gemäß 3GPP TS 32.101 V15.0.0 (2017-09), Telecommunication management; Principles and high level requirements)

- Element Manager (EM)
- Domain Manager (DM)
- Network Manager (NM)
- Network Management Layer Service (NMLS)