BUNDESGESETZBLATT
FÜR DIE REPUBLIK ÖSTERREICH

Jahrgang 2020 **Ausgegeben am 3. Juli 2020** **Teil II**

301. 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 – Telekom-Netzsicherheitsverordnung 2020 (TK-NSiV 2020)

Auf Grund des § 16a Abs. 9 des Bundesgesetzes, mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2003 – TKG 2003), BGBl. I Nr. 70/2003 in der Fassung 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.

Begriffsbestimmungen

§ 2. Im Sinne dieser Verordnung bedeutet

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.

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 14 in einem von der Regulierungsbehörde vorgegebenen elektronischen Format zu informieren („Erstmeldung“). Die Wiederherstellung der betroffenen Dienste ist der Regulierungsbehörde unverzüglich mitzuteilen. 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 den Erst- und Folgemeldungen muss der Einmelder auf einen allfälligen von ihm zuvor übermittelten Warnhinweis gemäß § 4 Bezug nehmen. 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 gemäß 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).

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. 2 iVm. Abs. 3 NISG und mit Einwilligung des Einmelders an den Bundesminister für Inneres weiterzuleiten.

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 (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.

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 entsprechend dem Stand der Technik in angemessenem Umfang 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.

Schlussbestimmungen

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

Steinmaurer

Unterzeichner	serialNumber=932783133,CN=Bundeskanzleramt,C=AT
Datum/Zeit	2020-07-03T16:16:41+02:00
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: https://www.bundeskanzleramt.gv.at/verifizierung
Hinweis	Dieses Dokument wurde amtssigniert.