§ 6 TK-NSiV 2020 Sicherheitsanforderungen an 5G-Netze

TK-NSiV 2020 - Telekom-Netzsicherheitsverordnung 2020

Berücksichtigter Stand der Gesetzgebung:

1. (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. (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. (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. 1.Betrieb von Network Operation Center (NOC) sowie Security Operation Center (SOC) in eigenen Räumlichkeiten innerhalb der Europäischen Union;
    2. 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. 3.Schutz des Management-Verkehrs von Kommunikationsnetzen oder -diensten, um nicht autorisierte Änderungen von Netz- oder Dienstkomponenten zu verhindern;
    4. 4.physischer Schutz von kritischen Netzkomponenten und sensiblen Teilen der 5G-Netze mit risikobasiertem Ansatz für Multi-access Edge Computing (MEC) und Basisstationen;
    5. 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. 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. 7.Multi-Vendor-Strategie, die die technischen Beschränkungen und Interoperabilitätsanforderungen verschiedener Teile eines 5G-Netzes berücksichtigt.
4. (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.

In Kraft seit 04.07.2020 bis 31.12.9999