Umsetzung der 5G Toolbox

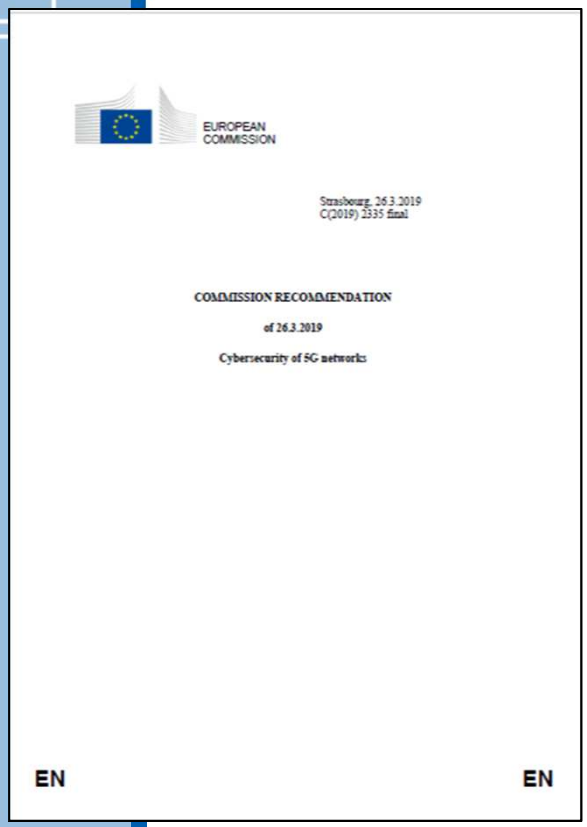
durch TK-Netzsicherheitsverordnung

Kurt Reichinger | RTR-GmbH

12.03.2020 – Regulierungsdialog

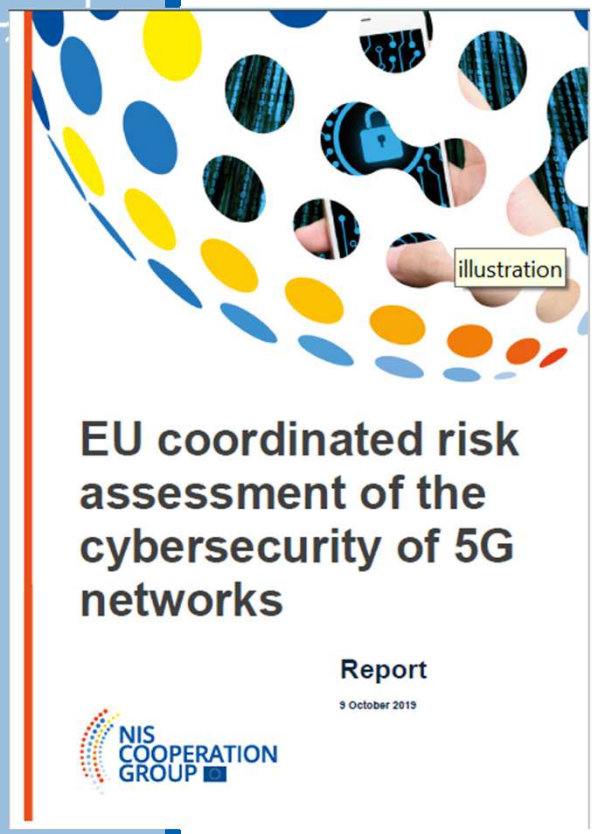
Inhalt

- 5G-Toolbox der EK
- Aufbau und Inhalt des Entwurfs einer TK-NSiV
  - Umfasste Themen
  - Nicht umfasste Themen
- Vorläufiger Zeitplan



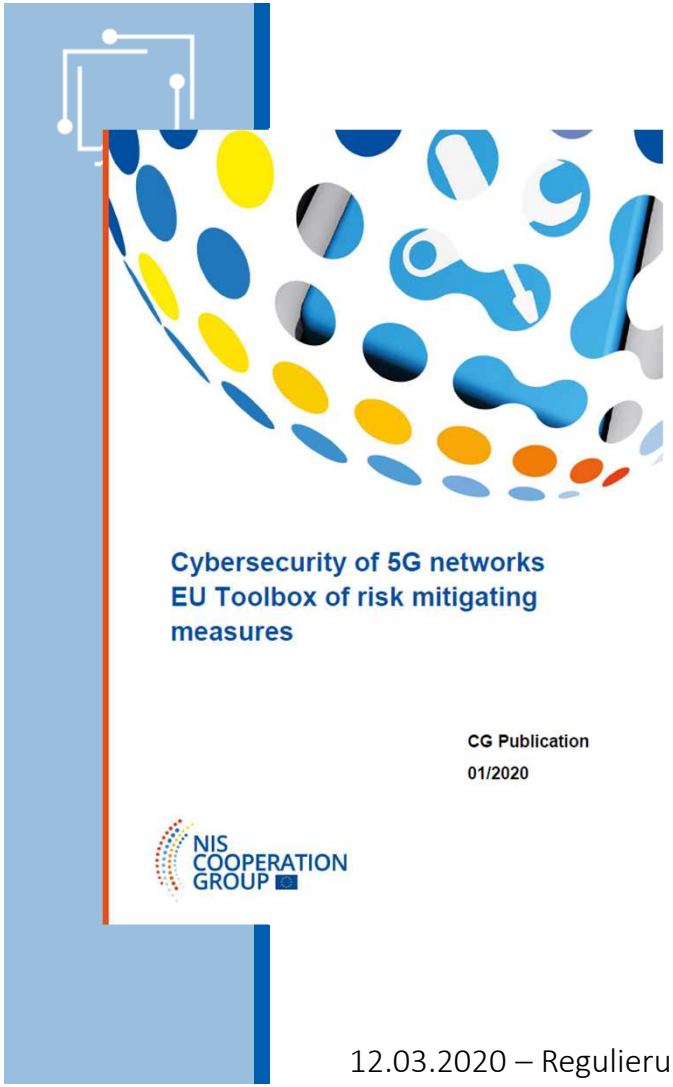
März.2019: Empfehlung der EK zur Cybersicherheit von 5G-Netzen

- Durchführung nationaler Risikobewertungen mit Schwerpunkt auf 5G-Netze
- Überprüfung der nationalen Maßnahmen im Hinblick auf 5G-Netze
- Forcierung der Zusammenarbeit auf EU-Ebene und Durchführung einer EU-weit koordinierten Risiko-bewertung
- Schaffung eines gemeinsamen Instrumentariums von Maßnahmen zur Risikominderung



Okt.2019: Koordinierte europ. Risikobewertung

- Überprüfung unionsweiter Exposition gegenüber Risiken durch die Mitgliedstaaten
- Erfassung der Bedrohungslage durch ENISA
- Unterstützung durch NIS-Kooperationsgruppe
  - Österreich durch BKA + RTR vertreten
- Veröffentlichung des Berichts im Okt.2020



Jan.2020: EU Toolbox

- Risikomanagementmaßnahmen zur Minderung der auf nationaler und Unionsebene ermittelten Cyber-sicherheitsrisiken
- Ausarbeitung der Tool Box im Rahmen der NIS-CG unter Beteiligung von BKA und RTR
- Veröffentlichung 29.01.2020
- Toolbox nennt eine Reihe von Risiken im Zusammenhang mit 5G-Netzen (auf Basis der europäischen Risikoanalyse) sowie mögliche Abhilfemaßnahmen (strategisch/technisch/unterstützend)
- Es bleibt dem Mitgliedstaat überlassen, welche Maßnahmen für die nationale Situation am besten geeignet angesehen und eingesetzt werden
- Evaluierung der Anwendung der Toolbox über die Europäische Union hinweg bis Oktober 2020

EU-Toolbox: Strategische Maßnahmen

- Stärkung der Rolle der nationalen Behörden um Sicherheitsmaßnahmen auf verschiedenen Ebenen einfordern zu können. Hier geht es u.a. auch um Einflussnahme von Drittstaaten auf die Sicherheit der 5G Supply Chain und der Abhängigkeit von einzelnen Herstellern
- Durchführung von Sicherheits-Audits bei Betreibern
- Erstellung eines Risiko-Profils von Herstellern inklusive der Möglichkeit der Anwendung von Restriktionen für Hochrisiko-Lieferanten bis hin zum Ausschluss
- Überprüfung des Einsatzes von Managed Service Providers (also der Auslagerung von Funktionen) und ggf. Anwendung von Restriktionen bei kritischen Funktionen
- Forcierung von Multi-Vendor-Strategien um die Abhängigkeit von einem Hersteller zu reduzieren
- Aufbau eines 5G Ökosystems und Forcierung europäischer Hersteller um die Abhängigkeit von non-EU Herstellern mittelfristig zu reduzieren
- Stärkung der Resilienz auf nationaler Ebene
- Ausbau der Diversität und der Kapazitäten in der EU für künftige Netztechnologien

EU-Toolbox: Technische Maßnahmen

- Sicherstellung der Anwendung von baseline security requirements in Netzdesign und -architektur
- Evaluierung der Anwendung von 5G Sicherheitsstandards bei MNOs
- Überprüfung von strikten Zugangskontrollen
- Erhöhung der Sicherheit bei virtualisierten Netzfunktionen
- Sicherheit bei 5G Netzmanagement, Betrieb und Monitoring
- Sicherstellung von Software-Integrität und Patch-Management
- Verbesserung der Sicherheit im Bestell-Prozess
- EU-Zertifizierung für 5G Netzkomponenten, Kundenequipment und Prozesse bei Herstellern
- EU-Zertifizierung für weitere Non-5G Komponenten und Dienste (wie connected devices und cloud services)
- Stärkung der physischen Sicherheit
- Stärkung von Resilienz- und Kontinuitätsplänen

EU-Toolbox: Unterstützende Maßnahmen

- Überarbeitung oder Entwicklung von Leitfäden und Best Practices zur Netzsicherheit
- Stärkung des Potenzials für Tests und Audits auf nationaler und EU-Ebene
- Gestaltung und Unterstützung der 5G-Standardisierung
- Entwicklung von Leitfäden zur Umsetzung von Sicherheitsmaßnahmen in bestehenden 5G-Standards
- Gewährleistung technischer und organisatorischer Sicherheitsmaßnahmen durch ein spezifisches EU-weites Zertifizierungsschema
- Erfahrungsaustausch zur Umsetzung strategischer Maßnahmen, insbesondere des nationalen Rahmens zur Bewertung des Risikoprofils von Herstellern
- Verbesserung der Koordination bei der Behandlung von Sicherheitsvorfällen und im Krisenmanagement
- Überprüfung gegenseitiger Abhängigkeiten zwischen 5G-Netzen und anderen kritischen Diensten
- Ausweitung von Mechanismen zur Kooperation, Koordination und zum Informationsaustausch
- Berücksichtigung der Cybersicherheit in öffentlich geförderten Projekten zur 5G-Bereitstellung.

TK-Netzsicherheitsverordnung (TK-NSiV)

Rechtsgrundlage: § 16a Abs 9 TKG 2003 (idgF)

Die Regulierungsbehörde kann im Einvernehmen mit dem Bundesminister für Verkehr, Innovation und Technologie* und mit dem Bundesminister für Inneres unter Bedachtnahme auf die relevanten internationalen Vorschriften, auf die Art des Netzes oder des Dienstes, auf die technischen Möglichkeiten, auf den Schutz personenbezogener Daten und auf sonstige schutzwürdige Interessen von Nutzern mit Verordnung die näheren Bestimmungen zur Umsetzung der §§ 16 und 16a über

1. die Sicherheit des Netzbetriebes,
2. die Aufrechterhaltung der Netzintegrität,
3. die Interoperabilität von Diensten,
4. vorbeugende Sicherheitsmaßnahmen,
5. die Ausgestaltung von Sicherheitsrichtlinien, insbesondere Identitäts-, Zutritts- und Zugriffsverwaltung, sowie
6. die Vorgehensweise bei Sicherheitsverletzungen von Betreibern öffentlicher Kommunikationsnetze oder -dienste festlegen.

* nunmehr BMLRT, § 17 BMG

Aufbau und Inhalt der geplanten TK-NSiV

- Zweck und Anwendungsbereich
- Begriffsbestimmungen
- Inhaltliche Festlegungen
  - Meldepflicht bei Sicherheitsvorfällen mit beträchtlichen Auswirkungen
  - Möglichkeit von freiwilligen Meldungen
  - Umfang und Ausgestaltung von Mindestsicherheitsmaßnahmen
  - Maßnahmen aus dem Unionsinstrumentarium zur Cybersicherheit von 5G-Netzen („Toolbox“)
- Anhang
- Erläuternde Bemerkungen

Sicherheit von Netzen und Diensten allg.

Sicherheit von 5G Netzen spez.

TK-NSiV: Meldepflicht, freiwillige Meldung

- Meldung unverzüglich bei Sicherheitsvorfall mit beträchtlichen Auswirkungen
  - Betroffene KNB*/KDB**: Sprache fest/mobil, Breitband fest/mobil
  - beträchtlich: bei Überschreitung Schwellwert (Ausnahme: Notruf)
  - Schwellwert: vgl. RTR-Website, Relation Anzahl betroffener Teilnehmer/Dauer des Vorfalls, max. 1 Mio. Nutzerstunden
  - unverzüglich: ohne schuldhaftes Zögern ab Vorfall bzw. ab Kenntnis
  - Basis: ENISA „Technical Guideline on Reporting Incidents“ (Okt. 2014)
- Unverzügliche Weiterleitung der Meldung an BMI (BVT)
- Bei sicherheitsrelevantem Risiko/Vorfall unter Schwellwert: freiwillige Meldung möglich, bei Einwilligung des Einmelders Weiterleitung an BMI und CSIRT

*KNB = Kommunikationsnetzbetreiber
**KDB = Kommunikationsdienstebetreiber

TK-NSiV: Mindestsicherheitsmaßnahmen

- KNB/KDB müssen
  - Mindestsicherheitsmaßnahmen konzipieren, ergreifen & dokumentieren, wodurch ein nach Stand der Technik angemessenes Sicherheitsniveau gewährleistet wird
  - eine Information Security Policy festlegen
  - 7 Domains
    - Governance/Risikomanagement, Sicherheit des Personals, Sicherheit von Systemen und Betriebsstätten, Betriebsmanagement, Störfallmanagement, Business Continuity Managment, Monitoring/Audits/Tests
  - Unterlagen auf Anforderung an RTR übermitteln
  - Basis: ENISA „Technical Guideline on Minimum Security Measures“ (Okt. 2014)
    - Überarbeitung der Guideline durch ENISA im Laufe des Jahres 2020 zu erwarten
  - Mindestsicherheitsmaßnahmen mit Sophistication Level „Basic“ für kleine Betreiber
    - Gemeinsame Überarbeitung des Templates durch RTR und ISPA bereits vereinbart

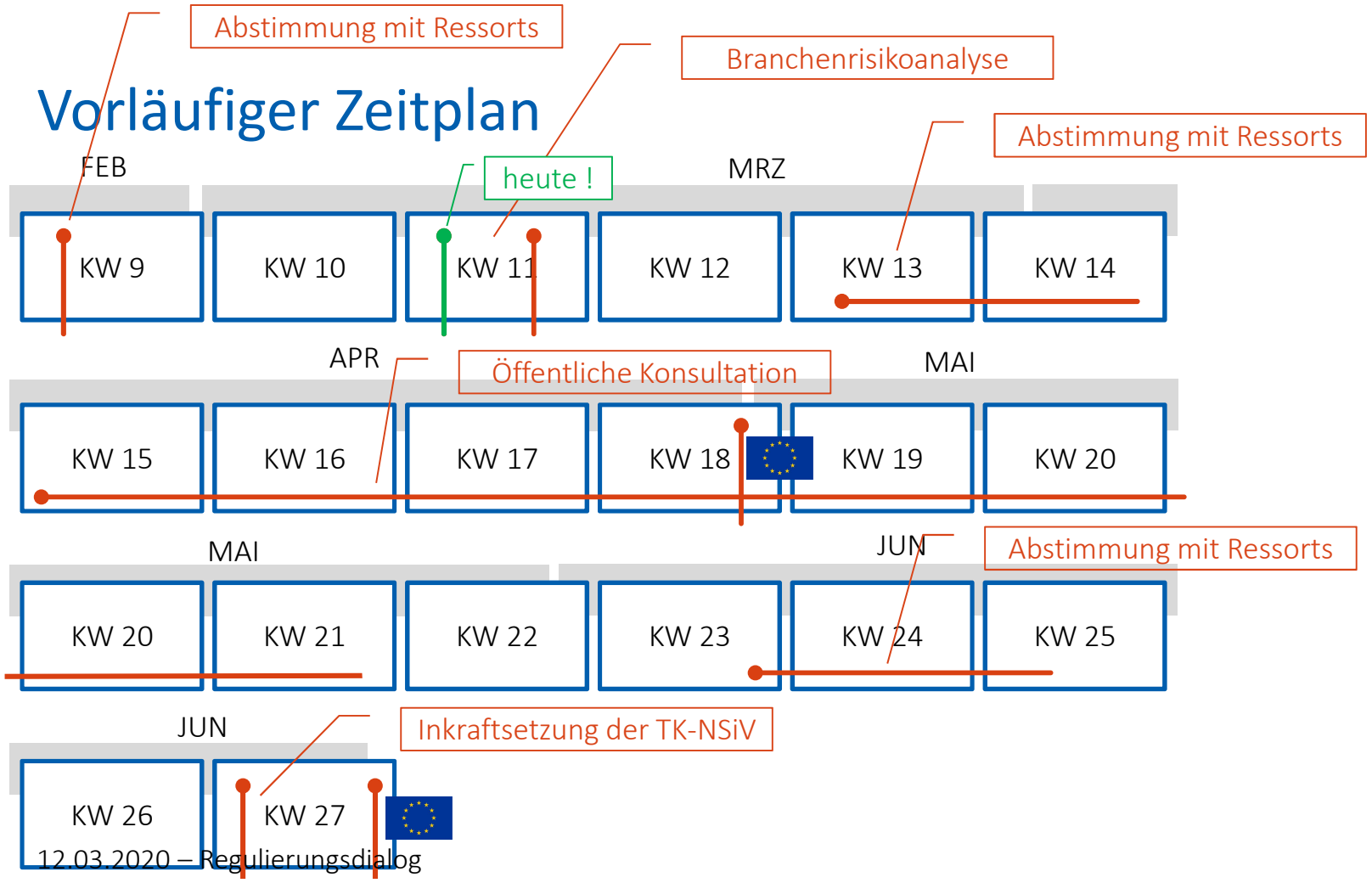
TK-NSiV: Sicherheitsmaßnahmen für 5G-Netze

- **Erhöhte Sicherheitsanforderungen an Betreiber von 5G-Netzen: KNB mit > 100.000 Teilnehmern in allen von ihnen betriebenen Mobilfunknetzen müssen**
  - Erfüllung der Standards ISO 27001/27002/27011 durch Auditberichte/Zertifikate bis 31.12.2021 nachweisen;
  - Erfüllung der Standards im Anhang (3GPP, ETSI, ENISA Indispensable Baseline Security Requirements for Procurement of Secure ICT Products and Services) durch Konformitätserklärung bis 30.06.2021 nachweisen;
  - Erfüllung zusätzlicher Anforderungen auf Verlangen der RTR nachweisen (NOC/SOC in eigenen Räumen in EU, Monitoring & phys. Schutz krit. Netzkomponenten, Schutz des Mgmt.verkehrs, Zugriff nur für qual. Personal, sichere Prozesse für Software-Aktualisierung & Sicherheitspatches, Multi-Vendor-Strategie);
  - Aufstellung sicherheitsrelevanter Komponenten für Betrieb des 5G-Netzes halbjährlich bzw. auf begründetes Verlangen unter Angabe von Hersteller, Typenbezeichnung sowie Hard- bzw Software- oder Firmwareversion übermitteln.

TK-NSiV: Was derzeit nicht inkludiert ist

- 5G Toolbox
  - High Risk Supplier List
  - EU-weite Zertifizierung
    - Vorläufig über Konformitätserklärung abgedeckt; später Novellierung der VO
  - Redundanz von Herstellern auf nationaler Ebene
    - Keine Aufnahme aufgrund zu hoher Eingriffsintensität
  - Monitoring von Foreign Direct Investment (FDI)
    - Keine Aufnahme aufgrund fehlender Zuständigkeit der RTR

Vorläufiger Zeitplan



Umsetzung der 5G Toolbox

durch TK-Netzsicherheitsverordnung

Kurt Reichinger | RTR-GmbH

12.03.2020 – Regulierungsdialog