RTR

Wir stehen für Wettbewerb und Medienvielfalt

RTR-GmbH, Mariahilfer Straße 77 – 79, 1060 Wien | www.rtr.at

NIS2-Vorschlag der EK

Regulierungsdialog Mobilfunk

RTR-Netzsicherheitsteam: K. Reichinger, U. Latzenhofer, D. Jagar, J. Weber

Inhalt

- Hintergrund
- Vorschlag der EK
  - Motive; Kernpunkte
  - Sektoren
  - Sicherheitsmaßnahmen und Berichtspflichten
- RTR-Position
- Positionen in anderen EU-Staaten – gemeinsame Initiativen

Hintergrund

- Nov. 2009: RL-Paket 2009 fügte Art 13a, 13b in Rahmen-RL ein (neu: Meldepflicht bei Sicherheitsverletzungen, Mindestsicherheitsmaßnahmen)
- Nov. 2011: Umsetzung in TKG-Novelle 2011 als § 16a TKG 2003
- Ausfüllung Meldepflicht, MSM durch techn. Guidelines der ENISA
- Juli 2016: RL 1148/2016 („NIS-RL“) beschlossen
  - Ausweitung Art 13a/b Rahmen-RL auch auf Schutz von Netz- und Informationssystemen in anderen Sektoren wie Strom, Gas, Öl, Verkehr (Luft/Bahn/Schifffahrt/ Straße), Banken, Gesundheit, Wasser, digitale Infrastruktur wie z.B. Internetknoten, DNS-Anbieter, Online-Marktplätze, Suchmaschinen
  - Unterscheidung: Betreiber wesentlicher Dienste, Anbieter digitaler Dienste
- Dez. 2018: Umsetzung im NISG, Netz- und InformationssystemsicherheitsG

Inhalt

- Hintergrund
- Vorschlag der EK
  - Motive; Kernpunkte
  - Sektoren
  - Sicherheitsmaßnahmen und Berichtspflichten
- RTR-Position
- Positionen in anderen EU-Staaten – gemeinsame Initiativen

NIS2-Vorschlag (1) – Motive

- Dzt. nicht alle kritischen Sektoren erfasst
- Inkonsistenzen/Lücken, da unterschiedl. Identifikation Betroffener in MS
- Fehlende Harmonisierung bei Sicherheitsmaßnahmen & Meldepflichten
- Unzureichende Aufsicht, Informationsaustausch zwischen MS und zwischen Betreibern nur freiwillig bzw. ad-hoc
- Auseinanderfallen der Aufsicht bei Digital: Internetknoten, TLD-Registries & Digitale Dienste bei NIS-Behörde, el. Kommunikationsnetze/-dienste bei TK-Regulatoren
- Juli – Sept. 2020: EU-Konsultation zur Revision der NIS-RL
- → 16.12.2020: „Cybersecurity Package“ der EK, u.a. mit RL-Vorschlag „NIS2“ COM(2020)823 (https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52020PC0823)

NIS2-Vorschlag (2) – Kernpunkte

- zusätzliche Sektoren
- Auswahl Betroffener: Fokus auf größere und kritische Akteure; statt aktueller Identifikation nun Schwellenwerte für große/mittelgroße Unternehmen, d.h., Ausnahme für KMU iSd EK-KMU-Empfehlung 361/2003 v. 6.05.03 (< 250 AN, < 50 Mio. Jahresumsatz bzw. < 43 Mio. Bilanzsumme); keine Schwellenwerte für ECN/ECS, VDA, TLD-Registries & Rechtsträger iSd Art 2 Z 2 b – g (zB öff. Vw.)
- Kategorien „wesentliche“ bzw „wichtige“ Dienste, zusätzlich RL-Vorschlag „Resilienz kritischer Infrastrukturen“ (COM(2020)829, 16.12.2020)
- Angleichung von Meldepflichten & Anforderungen an Sicherheitsmaßnahmen
- Angleichung von Bestimmungen über nationale Aufsicht & Vollzug
- Verbesserung der Zusammenarbeit insb. beim Krisenmanagement

NIS2-Vorschlag (3) – Sektoren

Wesentliche Dienste	Wichtige Dienste
Energie (Elektrizität, Erdöl, Erdgas, Fernwärme)	Digitale Dienste (Suchmaschinen, Online-Marktplätze, soziale Netze)
Verkehr (Luft-, Schienen-, Schiffs-, Straßenverkehr)	Post & Zustelldienste
Banken & Finanzmarktinstitutionen	Abfallbeseitigung
Gesundheitswesen	Chemie (Herstellung & Distribution)
Medikamentenerzeugung	Lebensmittel (Herstellung, Verarbeitung & Verteilung)
Trinkwasserlieferung & -versorgung, Abwasser	Handwerk
Digitale Infrastruktur (Rechenzentren, Cloud-Computing-Dienste, CDN, ECN/S, Vertrauensdienste)	
Öffentliche Verwaltung	
Weltraum	

NIS2-Vorschlag (4) – 2 regulatorische Regime

	Wesentliche Dienste („essential“)	Wichtige Dienste („important“)
Anwendungsbereich	NIS1-Sektoren & bestimmte neue Sektoren (Rechenzentren, Cloud-Computing-Dienste, Content Delivery Networks, Kommunikationsnetze & -dienste, Vertrauensdienste), Anhang 1	Großteil neuer Sektoren und bestimmter NIS1-Dienste, Anhang 2
Sicherheitsmaßnahmen	Risikobasierte Sicherheitsmaßnahmen; Vorstandsverantwortlichkeit, Art 17, 18	
Berichtspflichten	Vorfälle mit beträchtlichen Auswirkungen & Cyber-Bedrohungen, Art 20	
Aufsicht	Ex-ante (Art 29)	Ex-post (Art 30)
Sanktionen	Mindestliste administrativer Sanktionen einschl. Geldbußen, Art 31	
Jurisdiktion	Regelfall: Mitgliedstaat, in dem Dienst erbracht wird (Art 24 Z 1 & 2) Ausnahme: Hauptsitz & ENISA-Register bestimmter digitaler Infrastrukturen & Dienste (Art 24 Z 1 iVm Z 3)	

NIS2-Vorschlag (5) – Sicherheitsmaßnahmen

Grundsätze	Mindestsicherheitsmaßnahmen (Art 18 Z 2)
Vorstandsverantwortlichkeit für Nichteinhaltung von (Cyber-)Sicherheitsmaßnahmen, Art 17	Risikoanalyse & Informationssicherheitspolicies
Risikobasierter Ansatz: angemessene & verhältnismäßige technische & organisatorische Maßnahmen, Art 18 Z 1	Umgang mit Sicherheitsvorfällen
	Business continuity & Krisenmanagement
	Sicherheit der Lieferketten
	Sicherheit in Aufbau, Entwicklung und Wartung von Netz- und Informationssystemen einschl. Umgang mit Schwachstellen & deren Offenlegung
	Policies & Abläufe zur Bewertung der Wirksamkeit von Cybersicherheits-Risikomanagementmaßnahmen
	Nutzung von Kryptografie & Verschlüsselung

NIS2-Vorschlag (6) – Berichtspflichten, Art. 20

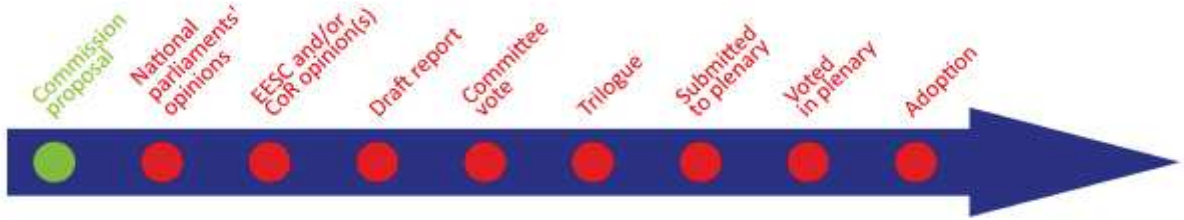
- Berichtspflicht sowohl für Sicherheitsvorfälle mit beträchtlichen Auswirkungen als auch für Bedrohungen
- Information an Nutzer der Dienste
- Berichtspflicht in drei Abschnitten:
  - Anfangsbericht
  - Zwischenbericht auf Anforderung von Aufsichtsbehörde oder CSIRT (Computer Security Incident Response Team)
  - Endbericht binnen eines Monats
- Mitgliedstaaten haben einander und ENISA über grenzüberschreitende Sicherheitsvorfälle zu informieren

NIS2-Vorschlag (7) – Institutionen

- Institutionen national
  - CSIRTs: Computer Security Incident Teams - Incident Handling, Threat Monitoring, Frühwarnsystem, Analyse von & Reaktion auf Sich'vorfälle,
  - Nationale Cybersicherheitsbehörde - Aufsicht gemäß NIS2-RL
  - SPOC: Single Point of Contact on Cybersecurity - grenzüberschreitender Kontakt
- Institutionen EU-Ebene
  - NIS Cooperation Group - Unterstützung von strateg. Zusammenarbeit & Informations-austausch zwischen MS; koord. Risikobewertung zur Sicherheit v. Lieferketten; Sek.: EK
  - CSIRT-Netzwerk – Förderung rascher & operativer Zusammenarbeit; Sek.: ENISA
  - EU-CyCLONe (European Cyber Crises Liaison Organisation Network) – koord. Bewältigung großer Cyberkrisen, Informationsaustausch MS – EU-Organe; Sek.: ENISA
  - ENISA – zweijährliche Herausgabe eines Berichts zur Cybersicherheitslage, Europäisches Schwachstellenregister etc

NIS2-Vorschlag (8) – weiteres Vorgehen

- Zuleitung des NIS2-RL-Vorschlags der EK an Europäischen Rat und Europ. Parlament, ITRE-Ausschuss, zur weiteren Beratung (GZ: 2020/0359(COD), vgl. https://www.parlament.gv.at/PAKT/EU/XXVII/EU/04/75/EU_47548/



Inhalt

- Hintergrund
- Vorschlag der EK
  - Motive; Kernpunkte
  - Sektoren
  - Sicherheitsmaßnahmen und Berichtspflichten
- RTR-Position
- Positionen in anderen EU-Staaten – gemeinsame Initiativen

RTR-Position (1)

- Aufsicht über Sicherheit von ECN/ECS war vor Inkrafttreten des EECC durch sog. „Rahmen-RL“ den TK-Regulierungsbehörden zugewiesen
- Art 40, 41 EECC verlagern diese Zuständigkeit auf „competent authority“ → MS entscheidet über innerstaatliche Aufgabenzuweisung
- Art 40 NIS2-Vorschlag sieht Streichung von Art 40, 41 EECC vor; Problem: EECC bis Ende Umsetzungsfrist NIS2-RL schon nat. umgesetzt
- Folgen bei Inkrafttreten NIS2-RL
  - Wegfall Rechtsgrundlage für nationale Umsetzung (§ 44 TKG-E)
  - Wegfall Rechtsgrundlage für TK-NSiV 2020 (Fortgeltung, § 212 Abs 12 TKG-E)
  - Anpassung des TKG erforderlich

RTR-Position (2)

- Zuständigkeit für Sicherheit elektronischer Kommunikationsnetze & -dienste („ECN/ECS“) wird seit 2011 von den TK-Regulierungsbehörden (TKK/RTR) wahrgenommen, die entsprechendes Know-How aufgebaut haben (bei NIS-Behörde nicht vorhanden)
- Synergieeffekte aufgrund der wettbewerblichen & sonstigen TK-spezifischen Aufsicht über ECN/ECS (RTR fungiert als „One-Stop-Shop“) → kostengünstige Wahrnehmung der Aufsichtsfunktion (Mehrkosten bei Auseinanderfallen)
- NIS-Behörden fokussieren auf Cybersecurity; Gefahr einer Vernachlässigung konventioneller Bedrohungen („Bagger“-Fall, Ausfall Notrufe etc.)
- Meldungen über Sicherheitsvorfälle gehen an NIS-Behörde oder CSIRT
- Wegfall Konsultation mit Stakeholdern bei Neuregelungen zur Netzsicherheit
- Nahtloser Zuständigkeitsübergang wäre derzeit mangels personeller Ressourcen der NIS-Behörde nicht möglich → Verunsicherung Stakeholder

RTR-Position (3)

EU-Ebene

- El. Kommunikationsnetze und –dienste auch künftig aus NIS-RL auszunehmen

Nationale Ebene

- Einrichtung von TKK/RTR als sektorspezifische NIS-Behörden für el. Kommunikation

Inhalt

- Hintergrund
- Vorschlag der EK
  - Motive; Kernpunkte
  - Sektoren
  - Sicherheitsmaßnahmen und Berichtspflichten
- RTR-Position
- Positionen in anderen EU-Staaten – gemeinsame Initiativen

Position von BEREC / Initiativen von NRAs

- Memorandum on certain proposed changes to the NIS Directive SE
- Non-paper on NIS regulatory framework BE, BG, HR, CZ, HU, IRL, LV, LIT, POL, SLO, SLV
- Opinion on proposed NIS 2 Directive and its effect on El. Communications BEREC
  - Fehlende Evaluierung vor Streichung von Art 40/41 EECC
  - Gesamtheitlicher Regulierungsansatz für ECN / ECS geht verloren
  - Fokus geht weg von ECN / ECS in Richtung Datensicherheit und “related services”
    - Öffentliche Komm.netze und -dienste sollen nicht von NIS2 umfasst sein
    - Art 40/41 EECC sollen bestehen bleiben
    - Derzeitige Praxis soll beibehalten und Disruptionen vermieden werden
    - Know-how von NRAs soll nicht verloren gehen
    - BEREC soll eine aktivere Rolle zugewiesen werden

RTR

Wir stehen für Wettbewerb und Medienvielfalt

Vielen Dank!

nis@rtr.at

RTR-GmbH, Mariahilfer Straße 77 – 79, 1060 Wien | www.rtr.at