NIS 2

Aktuelle Entwicklungen

Ulrich Latzenhofer / Jan Weber

Cybersicherheitspaket vom 16.12.2020

- Gemeinsame Mitteilung der EK und des HV: **Die Cybersicherheitsstrategie der EU für die digitale Dekade,** JOIN(2020) 18 final
- Vorschlag für eine RL über **Maßnahmen für ein hohes Maß an Cybersicherheit in der gesamten Union [NIS 2],** COM(2020) 823 final
- Vorschlag für eine RL über die **Resilienz kritischer Einrichtungen [CER],** COM(2020) 829 final

- In weiterer Folge (03.06.2021): Vorschlag für eine VO zur **Änderung der Verordnung (EU) Nr 910/2014 [eIDAS] im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität,** COM(2021) 281 final

Cybersicherheitspaket: Hintergrund

Mitteilung **Gestaltung der digitalen Zukunft Europas,** COM(2020) 67 final

- Technologie im Dienste des Menschen
  - Europäische Cybersicherheitsstrategie
  - Überprüfung der NIS-RL
- Offene, demokratische und nachhaltige Gesellschaft
  - Überarbeitung der eIDAS-VO

Mitteilung **EU-Strategie für eine Sicherheitsunion,** COM(2020) 605 final

- Zukunftsfähiges Sicherheitsumfeld für Einzelpersonen
  - Stärkung von Rechtsvorschriften zu kritischen Infrastrukturen
  - Ausarbeitung einer EU-Cybersicherheitsstrategie

NIS 2: 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, ECN/ECS bei TK-Regulatoren
- → daher „Cybersecurity Package“ der EK v. 16.12.20 mit RL-Vorschlag „NIS2“ COM(2020)823

NIS 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
- 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

NIS 2: 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	

NIS 2: zwei regulatorische Regime

	Wesentliche Dienste („essential“)	Wichtige Dienste („important“)
Anwendungsbereich	NIS1-Sektoren & bestimmte neue Sektoren (Rechenzentren, Cloud-Computing-Dienste, Content Delivery Networks, Kommunikationsnetze & -dienste, qualif. 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)	

NIS 2: 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

NIS 2: 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
  - Endbericht binnen eines Monats
- Mitgliedstaaten haben einander und ENISA über grenzüberschreitende Sicherheitsvorfälle zu informieren

NIS 2: Auswirkungen auf andere Vorschriften

Ersatz bisheriger Bestimmungen von EECC und eIDAS-VO durch NIS 2

- Art 39: Streichung von Art 19 eIDAS-VO (Sicherheit von Vertrauensdiensten)
- Art 40: Streichung von Art 40 und 41 EECC (Sicherheit elektronischer Kommunikation)

Zuständige Behörde: NIS-Behörde statt TK-Regulierungsbehörde und eIDAS-Aufsichtsstelle

- EG 48aa und 49: Bisherige Regulierungsbehörden und Aufsichtsstellen können mit Aufgaben sektorspezifischer NIS-Behörden betraut werden
  - Kontinuität bei Anwendung von Vorschriften
  - Wahrung von Kenntnissen und Erfahrungen der bisher zuständigen Behörden

NIS 2: aktuelle Entwicklung

11.03.2021: Stellungnahme des Europäischen Datenschutzbeauftragten; insgesamt positiv, einige Empfehlungen, keine Kritik an Art 39 und 40

27.04.2021: Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses; insgesamt positiv, einige Empfehlungen, keine Kritik an Art 39 und 40

04.11.2021: Bericht des EP; diverse Änderungsanträge, ua zeitversetztes Inkrafttreten von Art 39 und 40

26.11.2021: allgemeine Ausrichtung des Rates

13.05.2022 politische Einigung zwischen Rat und Parlament

NIS 2: Ausblick

- Weiterer Verlauf des Gesetzgebungsverfahrens abhängig von Entscheidungen des Europäischen Parlaments und des Rates
- Kundmachung aus heutiger Sicht vermutlich im Spätsommer oder Herbst 2022
- Umsetzungsfrist 21 Monate

CER: Vorschlag der EK

- Erweiterung der RL 2008/114/EG über europäische kritische Infrastrukturen (EKI)
- Anwendbar auf zehn Sektoren, auch elektronische Kommunikation und Vertrauensdienste als Teile des Sektors digitale Infrastruktur
- Nationale Strategien zur Gewährleistung der Resilienz kritischer Infrastrukturen
- Regelmäßige Risikobewertungen auf nationaler Ebene sowie für kleinere Gruppen von Einrichtungen
- Unterstützung der Kommission durch Bestandsaufnahme von grenz- oder sektorübergreifenden Risiken, bewährte Verfahren, Schulungen, Übungen usw.

CER: Kernpunkte (1)

Anwendungsbereich: kritische Einrichtungen, insbesondere digitale Infrastruktur inkl elektronischer Kommunikation und Vertrauensdienste

Nationaler Resilienzrahmen für kritische Einrichtungen

- Resilienzstrategie von jedem Mitgliedstaat zu verabschieden (strategische Ziele, politische Maßnahmen)
- Erstellung einer Liste wesentlicher Dienste je Mitgliedstaat
- Bewertung aller Risiken mit potenziellen Auswirkungen auf wesentliche Dienste
- Ermittlung kritischer Einrichtungen, die wesentliche Dienste erbringen, und anderer Einrichtungen, die kritischen Einrichtungen gleichzuhalten sind (zB bestimmte Behörden)
- Festlegung von Kriterien für das Vorliegen erheblicher Störungen
- Benennung einer zuständigen Behörde und einer zentralen Anlaufstelle innerhalb dieser Behörde
- Unterstützung kritischer Einrichtungen durch die Mitgliedstaaten

CER: Kernpunkte (2)

Resilienz kritischer Einrichtungen

- Risikobewertungen und Resilienzmaßnahmen kritischer Einrichtungen
- Zuverlässigkeitsüberprüfungen für Personal kritischer Einrichtungen
- Meldung von Sicherheitsvorfällen, die den Betrieb erheblich stören (könnten)

Spezifische Aufsicht über kritische Einrichtungen, die für Europa von besonderer Bedeutung sind

- Wesentliche Dienste für mehr als ein Drittel der Mitgliedstaaten
- Beratungsmission (von EK organisiert, mit Vertretern der MS)

Zusammenarbeit und Berichterstattung: Gruppe für die Resilienz kritischer Einrichtungen

Aufsicht und Durchsetzung

CER: aktuelle Entwicklung

27.04.2021: Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses

01.07.2021: Stellungnahme des Ausschusses der Regionen

15.10.2021: Bericht des EP

07.12.2021: allgemeine Ausrichtung des Rates

Weiterer Verlauf des Gesetzgebungsverfahrens abhängig von Entscheidungen des Europäischen Parlaments und des Rates

RTR

Wir stehen für Wettbewerb und Medienvielfalt

Auf Wiedersehen!

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