Aktuelle gesetzliche Entwicklung zur neuen NIS 2-Richtlinie der EU

Prof. Dr. Dennis-Kenji Kipker

Hamburg, 03.02.2022

VDE

EU NIS 2-Richtlinie: Übersicht Ursprungsfassung Stand 12/2020

- **Ursprungsfassung:** Zusammen mit der neuen EU-Cybersicherheitsstrategie am 16.12.2020 vorgestellt
- Wesentliche Neuerungen seinerzeit:
  - **Neufassung und Erweiterung des Anwendungsbereichs:** z.B. öffentliche Verwaltung und Raumfahrt als neue Sektoren; Fernwärme/Fernkälte und Wasserstoff als Teilsektoren
  - Pflicht zu Maßnahmen richtet sich danach, ob eine Einrichtung als **„wesentlich“** oder **„wichtig“** eingestuft wird
  - **Identifikations- und Überprüfungspflicht der Mitgliedstaaten** hinsichtlich Infrastrukturen, Übermittlung an EU-Kommission
  - **ENISA:** Erstellung eines Registers, in das Sicherheitslücken von IKT-Produkten und -Diensten eingetragen werden können
  - Kooperation im **„EU-CyCLONe“** zur Abwehr großangelegter Cybersecurity-Vorfälle
  - Sicherheitsrisikobewertung von **Versorgungsketten**, insb. im Bereich IKT
  - Verschärfung behördlicher **Aufsichts- und Durchsetzungsbefugnisse**

EU NIS 2-Richtlinie: Übersicht aktueller Stand 12/2021

- 03.12.2021: Einigung des Rates auf einen Standpunkt („allgemeine Ausrichtung“ bzw. **„General Approach“**)
- **Schwellenwert für die Größe für die Betreiber wesentlicher Dienste:** mittlere/große Unternehmen, die in den von der RL erfassten Sektoren tätig sind oder die unter die Richtlinie fallende Art von Diensten erbringen
- **Ausnahme:** RL gilt nicht für Bereiche Verteidigung, nationale Sicherheit, öffentliche Sicherheit, Strafverfolgung, Justiz, Parlamente, Zentralbanken
- **Streitthema öffentliche Verwaltung:**
  - Zunehmendes Ausmaß und Betroffenheit von Cyberangriffen, jedoch: unterschiedliche Standpunkte der MS
  - NIS 2 gilt für Einrichtungen der öffentlichen Verwaltung der Zentralregierungen
  - Geltung regionale/lokale Ebene: Abhängig vom Beschluss der Mitgliedstaaten
  - **Stand 10/2021:** „Education and research“ – „Higher education institutions and research institutions“ – entfallen → **aber:** Zugang über regionale/lokale Sonderregelungen beachten!
- Anpassung des Entwurfs an **sektorspezifische Rechtsvorschriften** für mehr Kohärenz (z.B. DORA)
- Freiwilliger **Peer-Learning-Mechanismus**; Straffung der **Meldepflichten**; mehr **Aufsicht und Durchsetzung**

EU NIS 2-Richtlinie: Anwendungsbereich

Öffentliche und private Einrichtungen gem. Anhang I (vgl. zur Konkretisierung Definitionen in Art. 4):

- Energie (inkl. Fernwärme und -kälte und Wasserstoff)
- Verkehr
- Bankwesen
- Finanzmarktinfrastruktur
- Gesundheitswesen
- Trinkwasser und Abwasser
- Digitale Infrastruktur (Internetknoten; DNS-Diensteanbieter, ausgenommen Root-Nameserver; TLD-Namenregister; Cloud Service Provider; RZ-Anbieter; Inhaltszustellnetze; Vertrauensdiensteanbieter nach eIDAS; öffentliche elektronische Kommunikationsnetze; öffentliche elektronische Kommunikationsdienste)
- Verwaltung von IKT-Diensten (B2B)
- Einrichtungen öffentlicher Verwaltung (von Zentralregierungen)
- Weltraum (Bodenstationen, Kommunikation grds. ausgenommen, s.o. digitale Infrastruktur)

EU NIS 2-Richtlinie: Anwendungsbereich

Öffentliche und private Einrichtungen gem. Anhang II (vgl. zur Konkretisierung Definitionen in Art. 4):

- Post- und Kurierdienste
- Abfallbewirtschaftung
- Chemische Industrie
- Lebensmittelindustrie
- Verarbeitendes Gewerbe (u.a. Medizinprodukte; EDV/elektronische/optische Erzeugnisse; elektrische Ausrüstungen; Maschinenbau; Kfz-Industrie; Fahrzeugbau)
- Digitale Dienste (Online-Marktplätze; Online-Suchmaschinen; soziale Netzwerke)

EU NIS 2-Richtlinie: Anwendungsbereich

- **Erreichen oder Überschreiten der Schwellenwerte für mittlere Unternehmen gem. Empfehlung 2003/361/EG der Kommission:**
  - Beschäftigung von mindestens 50 Personen
  - Jahresumsatz bzw. Jahresbilanz übersteigt 10 Mio. EUR
- **Ausnahmen von Schwellenwertgrößen für den Anwendungsbereich u.a. für:**
  - Öffentliche elektronische Kommunikationsnetze/öffentlich zugängliche elektronische Kommunikationsdienste
  - Vertrauensdiensteanbieter (qualifiziert/nichtqualifiziert)
  - Namensregister der Domäne oberster Stufe
  - Einziger Anbieter in Mitgliedstaat mir Kritikalität
  - Eintritt wesentlicher Störungsfolgen bei Nichtfunktionieren des Dienstes
  - Öffentliche Verwaltung der Zentralregierungen der Mitgliedstaaten

EU NIS 2-Richtlinie: Pflichten für Betreiber und Anbieter

- Nach wie vor Unterscheidung zwischen **„wesentlichen“** und **„wichtigen“** Einrichtungen: Hier teilweise Überschneidungen mit KRITIS und UBI nach IT-SiG 2.0
  - **Aber zu beachten:** Über den teilweisen Ausschluss des Schwellenwertkriteriums können in bestimmten Sektoren auch kleine und Kleinstunternehmen erfasst sein!
- Ausdrückliche Bestimmung der **Cybersecurity-Verantwortung der Leitungsorgane** mit Blick auf Haftung/Teilnahme an regelmäßigen Schulungen!
- Pflicht zu geeigneten, verhältnismäßigen, risikoangemessenen TOM für wesentliche und wichtige Einrichtungen → **strengerer Maßstab für wesentliche Einrichtungen**
  - Ausdrückliche Einbeziehung von Sicherheit der (kritischen) **Lieferkette**
  - Indirekt **„Security by Design“**
  - **Vulnerability Disclosure**, Kryptografie und Verschlüsselung
- **Meldepflichten** ggü. Behörden und Leistungsempfängern für wesentliche und wichtige Einrichtungen
- Befugnis der EU-Kommission zu konkretisierenden **Durchführungsrechtsakten** für Betreiberpflichten

EU NIS 2-Richtlinie: Pflichten für die EU und für die Mitgliedstaaten

- Verabschiedung nationaler Cybersicherheitsstrategie inkl. **Cybersicherheit in der Lieferkette** und freiwilliger, koordinierter Offenlegung von Schwachstellen: Überarbeitung alle fünf Jahre
- Mitgliedstaatliche CSIRTs als Koordinatoren zur Offenlegung von Schwachstellen für Transparenz + Vertrauen
- ENISA entwickelt und pflegt ein **EU-Schwachstellenregister** → Informationsaustausch zwischen Betreibern
- Entwicklung eines nationalen behördlichen Rahmens inkl. Reaktionsplan für das **Cybersicherheitskrisenmanagement**
- Neue Aufgabe der CSIRTs: **proaktive Überprüfung** der Netz- und Informationssysteme
- Einsetzung einer Kooperationsgruppe bestehend aus Mitgliedstaaten, EU-Kommission und ENISA, u.a. Betreuung von **EU-CyCLONe** (operatives EU-Netzwerk für Cyberkrisen) und Erstellung eines 2-jährigen Arbeitsprogramms
- Errichtung eines europäischen **CSIRT-Netzwerks** (operativer Schwerpunkt)
- ENISA + EU-Kommission: Veröffentlichung eines 2-jährigen **Berichts zur Cybersicherheit** in der Union
- Freiwilliges **Peer-Learning-System** für die Mitgliedstaaten zur Umsetzung der NIS 2-Richtlinie

EU NIS 2-Richtlinie: Fazit und Ausblick

- Wesentliche Grundsätze und Anforderungen **scheinen materiellrechtlich nunmehr „festgezurrt“**, insb. Anwendungsbereich der Regelungen
- **Deutliche inhaltliche Überschneidung** zu neuen Vorgaben aus IT-SiG 2.0, bessere Verzahnung mit EU Cybersecurity Act (CSA) und aktive **Einbeziehung der Normung**
- **Schärfung der Sanktionsbefugnisse** mittels prozentualer Regelungen (vgl. EU DS-GVO)
- Änderungen auch am **General Approach** sind aber durchaus noch möglich und erwartbar
- **Ausgang und Dauer des Trilogs derzeit jedoch noch offen:** Standpunkt des Rates das eine, aber: Einigung mit EU-Parlament unter Vermittlung der EU-Kommission?
- **Blick in die Glaskugel:**
  - Einigung ggf. Ende 2022/Mitte 2023
  - Mitgliedstaatliche Umsetzungsfristen von zwei Jahren nach Inkrafttreten beachten: „IT-SiG 3.0“ wohl eher in Richtung 2024/2025 zu erwarten
  - **Zurzeit auch noch offen:** Umsetzung EU NIS 2-RL und Neuerungen IT-SiG 3.0 gemeinsam oder separat?

Vielen Dank für Ihre Aufmerksamkeit!

Wir gestalten die e-diale Zukunft.
Machen Sie mit.

Ihr Ansprechpartner:

Prof. Dr. jur. Dennis-Kenji Kipker
Legal Advisor
CERT@VDE + Cybersecurity

Tel. +49 151 40223163
dennis-kenji.kipker@vde.com

VDE