NIS2 – EU-Update zur Cybersicherheit

Prof. Dr. Dennis-Kenji Kipker

Offenbach a.M., 24.02.2023

VDE

A. Auf einen Blick

- **Richtlinie (EU) 2022/2555** des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148, abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32022L2555
- Beschluss durch das **EP am 10.11.2022** in erster Lesung
- Annahme durch den **Rat am 28.11.2022**
- Verkündung im **EU-Amtsblatt am 27.12.2022**
- Umsetzungsfrist für Mitgliedstaaten in **nationales Recht bis 17.10.2024**
- Aufhebung der Vorgängerregelung **NIS-1 zum 18.10.2024**
- **Wesentliche Anforderungen:** Ausweitung des Anwendungsbereichs, neue Vorgaben für Mitgliedstaaten und betroffene Einrichtungen, verschärftes Sanktionsregime
- Grundsatz der **Mindestharmonisierung** gilt
- Grds. **mitgliedstaatliche Zuständigkeit** für Einrichtungen, in dem sie niedergelassen sind

B. Erhebliche Ausdehnung des Anwendungsbereichs

- Cybersicherheit nicht nur für Kritische Infrastrukturen, sondern flächendeckend als allgemeine Compliance-Anforderung für die Wirtschaft (vgl. bereits nationales **IT-SiG 2.0**)
- NIS-2 grds. anwendbar auf **öffentliche + private Einrichtungen**, die ihre Dienste in der Union erbringen oder ihre Tätigkeiten dort ausüben
  - **Einschränkungen + Bereichsausnahmen** für öffentlichen Sektor
- Weitere Konkretisierung durch:
  - **Anhang I** (Sektoren mit hoher Kritikalität)
  - **Anhang II** (Sonstige kritische Sektoren)

B. Erhebliche Ausdehnung des Anwendungsbereichs

- Überschneidungen z.B. mit EU-Resilienz-Richtlinie 2022/2557
- **Sektorspezifische Vorschriften** und **DS-GVO** sind in ihrem Anwendungsbereich bei gleichwertigem Schutzniveau vorrangig
- EU-Kommission erstellt bis 17.07.2023 **Leitlinie zur Abgrenzung der Rechtsakte**
- Im Anwendungsbereich Unterscheidung zwischen **wesentlichen und wichtigen Einrichtungen** mit Auswirkungen auf mögliche Aufsichts- und Durchsetzungsmaßnahmen sowie bei der Ahndung gesetzlicher Verstöße
  - Berücksichtigung unterschiedlicher **wirtschaftlicher Leistungsfähigkeit**
  - Mitgliedstaaten erstellen bis zum **17.04.2025** eine Liste wesentlicher und wichtiger Einrichtungen

B. Erhebliche Ausdehnung des Anwendungsbereichs

Sektoren nach Anhang I	Sektoren nach Anhang II
Energie	Post- und Kurierdienste
Verkehr	Abfallbewirtschaftung
Bankwesen	Produktion, Herstellung und Handel mit chem. Stoffen
Finanzmarktinfrastrukturen	Produktion, Verarbeitung und Vertrieb von Lebensmitteln
Gesundheitswesen	Verarbeitendes Gewerbe/Herstellung von Waren
Trinkwasser	Anbieter digitaler Dienste
Abwasser	Forschungseinrichtungen
Digitale Infrastruktur	
Verwaltung von IKT-Diensten	
Öffentliche Verwaltung	
Weltraum	

B. Erhebliche Ausdehnung des Anwendungsbereichs

Mittlere Unternehmen gem. Empfehlung 2003/361/EG: Beschäftigung von min. 50 Personen und Jahresumsatz/Jahresbilanz übersteigt 10 Mio. EUR

Unternehmen, die die Schwellenwerte für mittlere Unternehmen nach EU-Recht überschreiten (min. 250 Beschäftigte und Jahresumsatz von mehr als 50 Mio. EUR oder Jahresbilanz von mehr als 43 Mio. EUR)

Von Unternehmensgröße unabhängig, soweit qualifizierende Faktoren erfüllt sind, z.B. wegen kritischer Tätigkeit, Auswirkungen auf öff. Ordnung, Systemrisiken, grenzüberschreitenden Auswirkungen

B. Erhebliche Ausdehnung des Anwendungsbereichs

Wesentliche Einrichtungen

- Unternehmen gem. NIS-2 Anhang I, die die EU-Schwellenwerte für mittlere Unternehmen überschreiten
- Unternehmen, die nach NIS-1 bzw. mitgliedstaatlich als wesentliche Einrichtungen eingestuft werden

Wichtige Einrichtungen

- NIS-2 Anhang I und II zugehörige Unternehmen, die nicht als wesentliche Einrichtungen gelten bzw. die mitgliedstaatlich als wichtige Einrichtungen eingestuft wurden

C. Koordinierter Rahmen für die europäische Cybersicherheit: Pflichten der Mitgliedstaaten

- Entwicklung **nationaler Cybersicherheitsstrategie** inkl. Steuerungsrahmen für NIS-2
- Einbeziehung der Cybersicherheit in der **Lieferkette** von IKT
- **Koordinierte Offenlegung von Schwachstellen**
- Alle 5 Jahre sind die nationalen Cybersicherheitsstrategien zu **evaluieren**
- Benennung mitgliedstaatlicher NIS-2 **Ausführungsbehörden**
- Benennung von Behörden für das **Cyberkrisenmanagement**
- Errichtung von Computer-Notfallteams **(CSIRTs)**
- Aktive Beteiligung am Europäischen Netzwerk der Verbindungsorganisationen für Cyberkrisen **(EU-CyCLONe): Bewältigung massiver Cybersicherheitsvorfälle**

D. Nationale, europäische und internationale Kooperation: CSIRT-Verbund und EU-CyCLONe

- ENISA: Errichtung einer **europäischen Schwachstellendatenbank**
  - Informationen zur Beschreibung von Schwachstellen + deren Ausmaß
  - Betroffene Produkte und Dienste
  - Patches, Abhilfemaßnahmen zur Risikominderung etc.
  - Zugang eröffnet für alle „Interessenträger“
- **Umfassende behördliche Zusammenarbeit** inkl. Strafverfolgung und Datenschutz
- **„Kooperationsgruppe“** bestehend aus Mitgliedstaaten, EU-Kommission + ENISA
- Netzwerk nationaler CSIRTs zur Förderung **operativer EU-Zusammenarbeit**
- Freiwilliger mitgliedstaatlicher **Cybersecurity Peer Review**

E. Risikomanagementmaßnahmen und Berichtspflichten im Bereich der Cybersicherheit: Unternehmerische Pflichten

- Explizite Einbeziehung der **Leitungsorgane** mit Überwachungs- und Weiterbildungspflichten
- Weitergehende Anforderungen an Cybersecurity-Prävention durch TOM gem. **„Stand der Technik“**, Angemessenheit und individuelle Risikoexposition
- **Berücksichtigung hybrider Bedrohungslage:** Nicht nur Digitalschutz, sondern ebenso physische Infrastruktur der IT-Systeme
- **„Minimalkonsens“ TOM** u.a.: Krisenmanagement, Cyberhygiene, Kryptografie, Personalsicherheit, Authentifizierungstechnologien, Notfallkommunikation
  - EU erlässt konkretisierende Durchführungsrechtsakte bis 17.10.2024
  - Bezugnahme auf internationale Normen + Standards

E. Risikomanagementmaßnahmen und Berichtspflichten im Bereich der Cybersicherheit: Meldepflichten

Erheblicher Sicherheitsvorfall I:
Schwerwiegende Betriebsstörung der Dienste oder finanzielle Verluste wurden verursacht oder können verursacht werden

Erheblicher Sicherheitsvorfall II:
Natürliche oder juristische Person kann oder wird durch erhebliche materielle oder immaterielle Schäden beeinträchtigt

E. Risikomanagementmaßnahmen und Berichtspflichten im Bereich der Cybersicherheit: Meldefristen

24 Stunden: Frühwarnung, in der ggf. angegeben wird, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte

72 Stunden: Ggf. Aktualisierung der in der Frühwarnung enthaltenen Informationen und erste Bewertung des erheblichen Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen, sowie ggf. Angabe der Kompromittierungsindikatoren

Abschlussbericht (spätestens ein Monat nach initialer Meldung):

Ausführliche Beschreibung des Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen

Angaben zur Art der Bedrohung bzw. zugrundeliegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat

Angabe zu den getroffenen und laufenden Abhilfemaßnahmen

Grenzüberschreitende Auswirkungen des Sicherheitsvorfalls, falls vorhanden

F. Aufsicht und Durchsetzung: Behördliche Befugnisse

- Mitgliedstaatliche Anforderung zu wirksamer und risikobasierter Beaufsichtigung erfordert Unterscheidung zwischen wesentlichen + wichtigen Einrichtungen
- **„Wirksam, verhältnismäßig und abschreckend“**
- **Umfassende Kompetenzen u.a.:** Vor-Ort-Kontrollen, Stichprobenüberprüfungen, regelmäßige Sicherheitsprüfungen und Anforderungen des Informations- und Datenzugangs
- **Behördliche Befugnisse:** Warnungen, Anweisungen, Geldbußen, vorübergehender Ausschluss von Leitungspersonen, Haftungsrecht gilt unverändert fort
- **Wichtige Einrichtungen:** Nachträgliche behördliche Aufsichtsmaßnahmen möglich

F. Aufsicht und Durchsetzung: Geldbußen

Wesentliche Einrichtungen:

Entweder 10 Mio. Euro oder 2 % des weltweiten Jahresumsatzes, je nachdem, welcher Betrag höher ist

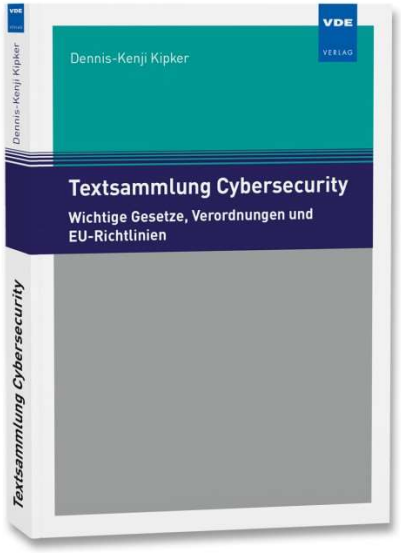
Wichtige Einrichtungen:

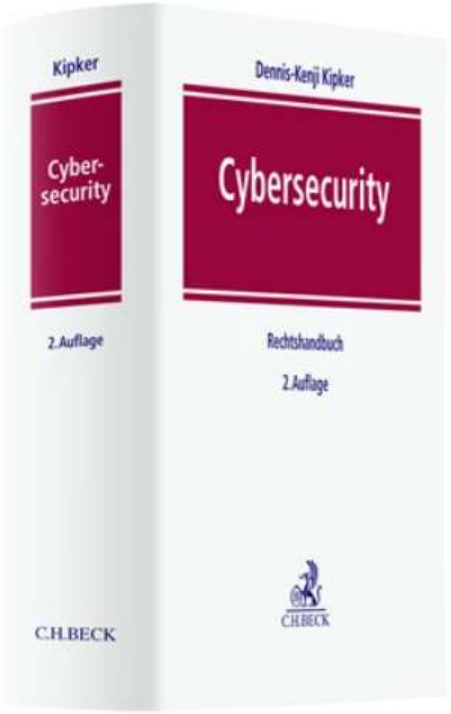
Entweder 7 Mio. Euro oder 1,4 % des weltweiten Jahresumsatzes, je nachdem, welcher Betrag höher ist

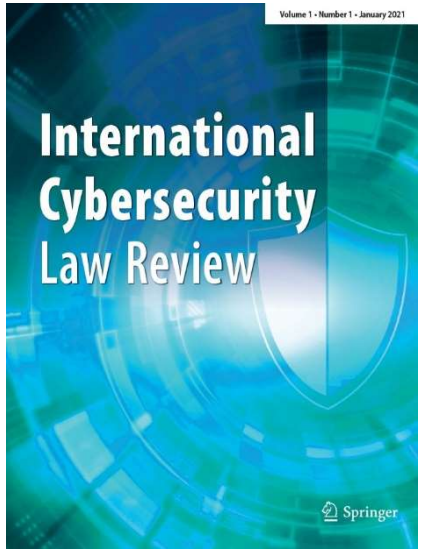
G. Fazit und Ausblick

- **Mitgliedstaatliche Umsetzung** NIS-2 bis 17.10.2024, Aufhebung NIS-1 zum 18.10.2024
- **EU KOM Impact Assessment:** Erhöhung des unternehmerischen Cybersecurity-Budgets um 22% (neue Unternehmen) bzw. 12% (Bestandsunternehmen)
- Zwar erhebliche Ausdehnung des Anwendungsbereichs und deutlich stärkere europäische Überformung, eigentlich zu treffende TOM jedoch wenig überraschend (vgl. auch **IT-SiG 2.0, 2021**)
- **Komplexes Zusammenspiel mit weiteren EU-Regelungen** (z.B. CRA, CSA, DS-GVO), Durchführungsrechtsakten, Normen + Standards
- Umfassende Regulierung der **Privatwirtschaft**, aber nur zaghaftes Vorgehen im **öffentlichen Sektor**

Weiterführende Literatur







Vielen Dank für Ihre Aufmerksamkeit!

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

Ihr Ansprechpartner:

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

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