NIS-Richtlinie 2.0 in der Praxis

OVE – Tagung zur Cybersicherheit industrieller Automatisierungssysteme

Inhalt: Mag. Vinzenz Heußler, LL.M.
Bundeskanzleramt, Abteilung I/8 (Cyber Security, GovCERT, NIS-Büro und ZAS)
Leiter NIS-Büro

Vortrag: Ing. Maximilian Schiessl, MSc. - CISSP, GPEN
Bundesministerium für Inneres, Abteilung IV/S/2 (Audit & Recht)
Wien, 6. Oktober 2022

Die neue NIS-Richtlinie (NIS2)

- **NIS 2**: Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148
  - Von EU-Kommission (DG CONNECT) am 16.12.2020 als Teil der neuen EU-Cybersicherheitsstrategie vorgelegt
- **NIS 2 ersetzt NIS 1** = Richtlinie (EU) 2016/1148 vom 6. Juli 2016
  - 1. Rechtsakt über Cybersicherheit in EU
  - Legt Maßnahmen fest, mit denen ein hohes gemeinsames Sicherheitsniveau von Netz- und Informationssystemen in der EU erreicht werden soll

NIS 1 – „Probleme“

- Unzureichendes Niveau der **Cyber-Resilienz** von Unternehmen aufgrund von
  - fehlenden Cybersicherheitsmaßnahmen (aufgrund der Nichtberücksichtigung)
  - **uneinheitlicher Behandlung** im gesamten Binnenmarkt (Diskrepanzen in den Ermittlungen der Betreiber)
- **Unterschiedlich starke** Resilienz der Mitgliedstaaten und Sektoren
- Schwach ausgeprägte **gemeinsame Lageerfassung** und mangelnde gemeinsame **Krisenreaktion**

Was will NIS 2 besser machen?

1. **Stärkung der Cyberresilienz eines alle relevanten Sektoren umfassenden Spektrums von Unternehmen,**
   - alle im gesamten Binnenmarkt, die wichtige Funktionen für die Wirtschaft und die Gesellschaft als Ganzes erfüllen, sollen verpflichtet werden, angemessene Cybersicherheitsmaßnahmen zu ergreifen
2. **Förderung einer gleich starken Resilienz bei den bereits unter die Richtlinie fallenden Sektoren im Binnenmarkt**, durch weitere Angleichung
   1. des De-facto-Anwendungsbereichs,
   2. der Sicherheitsanforderungen und Meldepflichten bei Sicherheitsvorfällen,
   3. der Bestimmungen für die nationale Aufsicht und Durchsetzung sowie
   4. der Kapazitäten der zuständigen Behörden in den Mitgliedstaaten.

Was will NIS 2 besser machen?

3. Verbesserung der gemeinsamen Lageerfassung und der kollektiven Vorsorge und Reaktionsfähigkeit

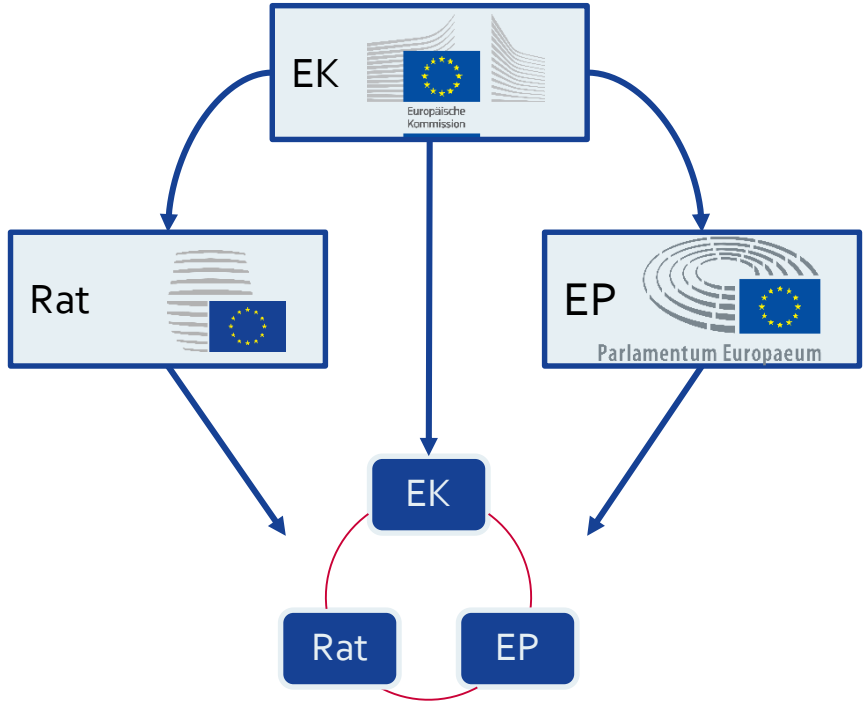
- Maßnahmen zur Stärkung des Vertrauens zwischen den zuständigen Behörden
- verstärkten des Informationsaustauschs
- Festlegung von Regeln und Verfahren im Falle weitreichender Sicherheitsvorfälle oder Krisen

Triloge

2020

2021

2022



EK Vorlage am 16.12.2020

Ratsmandat (AA) am 3.12.2021

EP Mandat am 10.11.2021

Vorläufige Einigung am 12.05.

Zeitplan auf EU-Ebene

Vorläufige politische Einigung im 3. Trilog	12. Mai
Finalisierung des Textes auf technischer Ebene	Ende Mai - Mitte Juni
Konsolidierter Text von AStV I gebilligt	22. Juli
Bericht des Berichterstatters von ITRE-Ausschuss gebilligt	13. Juli
Sprachjuristische Prüfung und Finalisierung der EN Sprachfassung	August - Mitte Sept
Übersetzung in 23 Amtssprachen und Prüfung	September
Annahme durch Plenum des EP (1. Lesung)	Oktober
Finale Annahme durch Rat	Ende Oktober

Zeitplan auf EU-Ebene

Signatur, Übermittlung an Büro des ABl der EU & Veröffentlichung im ABl	November
Inkrafttreten 20 Tage nach Veröffentlichung im ABl	Ende Nov / Dez
21 Monate Umsetzungsfrist für Mitgliedstaaten	August / Sept 2024

Die drei Säulen von NIS2

Mitgliedstaaten	Kooperation und Informationsaustausch	Risikomanagement
Nationale Behörden	NIS-Kooperationsgruppe Peer-Review	Verantwortlichkeit des Top-Managements
CSIRTs	CSIRTs-Netzwerk	Trainings für Top-Managements
Krisenmanagement	CyCLONe	Unterscheidung wesentliche und wichtige Einrichtungen
Nationale Strategien	ENISA Cybersecurity Reports	Einrichtungen sind verpflichtet, Sicherheitsmaßnahmen zu ergreifen
Rahmen für CVD (Coordinated Vulnerability Disclosure)	Europäisches Schwachstellenregister	Einrichtungen sind verpflichtet, signifikante Vorfälle zu melden

Rot = Neuerungen gegenüber NIS1

NIS 2 – Verpflichtungen für Einrichtungen

Risikomanagementmaßnahmen im Bereich der Cybersicherheit

Meldepflichten

Sicherheitsanforderungen

- Verantwortung des **Top-Managements** bei Nichteinhaltung von Maßnahmen des CS Risikomanagements
- **Schulungen für Top-Management**
- **Risikobasierter Ansatz**: angemessene und verhältnismäßige technische und organisatorische Maßnahmen
- **All-Gefahren-Ansatz** (All-hazards approach) mit dem Ziel, Netz- und Informationssysteme sowie ihre physische Umgebung vor Störungen zu schützen

Sicherheitsanforderungen

a) Risikoanalyse und Sicherheitsrichtlinien für Informationssysteme

b) Behandlung von Vorfällen

c) Business Continuity (inkl. Backup-Management und Notfallwiederherstellung) und Krisenmanagement

d) Supply Chain Security (inkl. sicherheitsbezogene Aspekte der Beziehungen mit direkten Anbietern oder Diensteanbietern)

e) Sicherheit bei der Beschaffung, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Umgang mit Schwachstellen und deren Offenlegung

Sicherheitsanforderungen

f) Richtlinien und Verfahren zur Bewertung der Wirksamkeit von Cyber-Risikomanagementmaßnahmen

g) Grundlegende Praktiken der Cyberhygiene und Schulungen zur Cybersicherheit

h) Richtlinien und Verfahren zum Einsatz von Kryptografie und, wo angemessen, Verschlüsselung

i) Sicherheit der Humanressourcen, Zugangskontrollmaßnahmen und Vermögensverwaltung

j) Verwendung von Lösungen für die **MFA** oder die kontinuierliche Authentifizierung, die gesicherte Sprach-, Video- und Textkommunikation sowie ggf gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung

Meldepflichten

Stärker harmonisierte Meldepflichten

- Einrichtungen müssen signifikante Cybersicherheits-Vorfälle melden
- Einrichtungen müssen Dienst-Empfänger über signifikante Cybersicherheits-Vorfälle und –Bedrohungen informieren, wenn angemessen
- Meldeprozess:

Meldepflichten

- Ein Sicherheitsvorfall gilt als signifikant, wenn

  a) er erhebliche **Betriebsstörungen** oder **finanzielle Verluste** für die betreffende Einrichtung verursacht hat oder verursachen kann;

  b) er andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Verluste geschädigt hat oder schädigen kann.

- EU-Kommission kann (und muss im Sektor digitale Infrastruktur) in Durchführungsrechtsakten festlegen, wann ein Vorfall signifikant ist.

Aufsicht

- Mindestliste an **Aufsichtsmaßnahmen** (regelmäßige & gezielte Audits, Vor-Ort- & Off-Site-Kontrollen, Sicherheitsscans) und **Mittel**, die den **zuständigen Behörden** zur Verfügung stehen (Ersuchen um Informationen & Zugang zu Beweismitteln).

- **Differenzierung des Aufsichtssystems** zwischen wesentlichen und wichtigen Unternehmen, um ein faires Gleichgewicht zwischen den Verpflichtungen der Einrichtungen und der zuständigen Behörden zu gewährleisten:
  - vollwertige Aufsicht (**ex ante & ex post**) für wesentliche Einrichtungen und
  - **ex post** Aufsicht für wichtige Einrichtungen.
- Risikobasierte Aufsicht möglich

Durchsetzung

- Mindestliste von **Verwaltungssanktionen** (z. B. verbindliche Anweisungen, Verwaltungsstrafen)
- Maximale **Bußgeldhöhe**:
  - mind. 10.000.000 EUR oder 2% des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres für wesentliche Einrichtungen
  - mind. 7.000.000 EUR oder 1,4% für wichtige Einrichtungen
- Natürliche Personen (leitende Angestellte) können für Pflichtverletzungen haftbar gemacht werden

Anwendungsbereich: Betroffene Sektoren

Anhang I	Anhang II
Energie (Elektrizität, Fernwärme/Kälte, Öl, Gas und Wasserstoff)	Post- und Kurierdienste
Verkehr (Luft, Schiene, Schifffahrt, Straße)	Abfallbewirtschaftung
Bankwesen	Chemie (Herstellung und Handel)
Finanzmarktinfrastrukturen	Lebensmittel (Produktion, Verarbeitung, Vertrieb)
Gesundheitswesen (Gesundheitsdienstleister, EU-Referenzlaboratorien, Forschung und Herstellung von pharmazeutischen und medizinischen Produken und Geräte)	Verarbeitendes / Herstellendes Gewerbe (Medizinprodukten; Datenverarbeitungs-, elektronische und optische Geräte und elektronische Ausrüstungen; Maschinenbau; Kraftwagen und Kraftwagenteile und sonstiger Fahrzeugbau)
Trinkwasser	Anbieter digitaler Dienste (Suchmaschinen, Online-Marktplätze und soziale Netzwerke)
Abwasser	Forschung
Digitale Infrastruktur (IXP, DNS, TLD, Cloud-Computing, Rechenzentren, Inhaltszustellnetzen, VDA und öffentliche elektronische Kommunikationsnetze- und dienste)	
IKT-Service Management	
Öffentliche Verwaltung	
Weltraum	

Anwendungsbereich

- NIS1: Mitgliedstaaten hatten großen Ermessensspielraum bei der Ermittlung der Betreiber wesentlicher Dienste.
- NIS2: Anwendungsbereich durch „**size cap rule**“ grds vorgegeben.
  - NIS2 gilt für alle öffentliche oder private wesentliche und wichtige Einrichtungen der in Anhang I und Anhang II genannten Art, die ihre Dienstleistungen in der EU erbringen oder ihre Tätigkeiten in der EU ausüben und die den Schwellenwert für mittlere Unternehmen iSd Empfehlung 2003/361/EG der EU-Kommission erreichen oder überschreiten
  - Kleinunternehmen nur in bestimmten Fällen umfasst.

Anwendungsbereich

- Prüfschema („Bin ich betroffen?“ „Bin ich wesentlich oder wichtig?“):
  - Erbringt die Einrichtung ihre Dienstleistungen in der EU oder übt ihre Tätigkeiten in der EU aus? („Serviciere ich den Binnenmarkt“?)
  - Entspricht die Einrichtung einer in Spalte 3 von Anhang I und Anhang II genannten Art? („Führt mich die NIS2 an?“ „In welchem Anhang“?)
  - Erreicht oder überschreitet die Einrichtung den Schwellenwert für mittlere Unternehmen? („Wie groß bin ich?“)
- Achtung: Es gibt Ausnahmen und Sonderregeln!

1. Erbringt die Einrichtung ihre Dienstleistungen in der EU oder übt ihre Tätigkeiten in der EU aus?

- „Serviciere ich den Binnenmarkt“?

2. Entspricht die Einrichtung einer in Spalte 3 von Anhang I und Anhang II genannten Art?

- „Führt die NIS2 meine Art von Einrichtung an?“
- „Wenn ja, in welchem Anhang wird meine Einrichtung genannt?“

Entspricht die Einrichtung einer in Spalte 3 von Anhang I und II genannten Art?

Sektor	Teilsektor	Art der Einrichtung
1. Energie	a) Elektrizität	— Elektrizitätsunternehmen im Sinne des Artikels 2 Nummer 57 der Richtlinie (EU) 2019/944[1], die die Funktion „Versorgung“ im Sinne des Artikels 2 Nummer 12 jener Richtlinie wahrnehmen
		— Verteilernetzbetreiber im Sinne des Artikels 2 Nummer 29 der Richtlinie (EU) 2019/944
		— Übertragungsnetzbetreiber im Sinne des Artikels 2 Nummer 35 der Richtlinie (EU) 2019/944

3. Erreicht oder überschreitet die Einrichtung den Schwellenwert für mittlere Unternehmen?

- „Wie groß bin ich?“
- „Bin ich ein kleines, mittleres oder großes Unternehmen?“

Schwellenwerte

- Empfehlung 2003/361/EG der EU-Kommission
  - **Großunternehmen**: Alle Unternehmen, sofern kein KMU.
  - **Mittleres Unternehmen**: ein Unternehmen, das weniger als 250 Personen beschäftigen und die entweder einen Jahresumsatz von höchstens 50 Mio. EUR erzielen oder deren Jahresbilanzsumme sich auf höchstens 43 Mio. EUR beläuft.
  - **Kleines Unternehmen**: ein Unternehmen, das weniger als 50 Personen beschäftigt und dessen Jahresumsatz bzw. Jahresbilanz 10 Mio. EUR nicht übersteigt.

Wesentliche und wichtige Einrichtungen

- Wesentliche Einrichtungen
  - Alle im Anhang I angeführten Einrichtungen, welche die Schwellenwerte für **mittlere Unternehmen überschreiten**.
- Wichtige Einrichtungen
  - Alle anderen Einrichtungen.
- Ausnahmen:
  - Sektoren Digitale Infrastruktur und Öffentliche Verwaltung
  - Immer wesentlich: Nach CER-Richtlinie als kritische Einrichtung ermittelt.

Grundregel Anwendungsbereich Anhang I

Sektoren	Groß-unter-nehmen	Mittlere Unter-nehmen	Kleinst- und Klein-unternehmen
Anhang I			
Energie / Verkehr / Bankwesen / Finanzmarktinfrastrukturen / Gesundheitswesen / Trinkwasser / Abwasser / IKT-Service Management / Weltraum	wesentlich	wichtig	

- Großunternehmen: wesentlich.
- Mittlere Unternehmen: Wichtig, außer falls ermittelt als wesentlich.
- Kleinst- und Kleinunternehmen: Nicht im Anwendungsbereich, außer falls ermittelt als wesentlich oder wichtig

Grundregel Anwendungsbereich Anhang II

Sektoren	Groß-unter-nehmen	Mittlere Unter-nehmen	Kleinst- und Klein-unternehmen
Anhang II			
Post- und Kurierdienste / Abfallbewirtschaftung / Lebensmittel / Verarbeitendes Gewerbes bzw. Herstellung von Waren / Anbieter digitaler Dienste / Forschung	wichtig	wichtig	

- Großunternehmen: Wichtig, außer falls ermittelt als wesentlich.
- Mittlere Unternehmen: Wichtig, außer falls ermittelt als wesentlich.
- Kleinst- und Kleinunternehmen: Nicht im Anwendungsbereich, außer falls ermittelt als wesentlich oder wichtig

Sonderregeln

- Kleinunternehmen
- Sektor Digitale Infrastruktur
- Sektor öffentliche Verwaltung

Wann fallen Kleinunternehmen unter die NIS2?

- Bestimmte Arten von Einrichtungen im Sektor Digitale Infrastruktur.
- Nach CER-Richtlinie als kritische Einrichtung ermittelt.
- Staat stuft Kleinunternehmen als wichtig oder wesentlich ein. Kriterien:
  - Einziger Erbringer eines Dienstes, der für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Tätigkeiten wesentlich ist.
  - Unterbrechung der Dienstleistung könnte erhebliche Auswirkungen auf die öffentliche Sicherheit, die öffentliche Ordnung oder die öffentliche Gesundheit haben.
  - Unterbrechung der Dienstleistung könnte ein erhebliches Systemrisiko mit sich bringen (insb. grenzüberschreitende Auswirkungen).
  - Besondere Bedeutung auf regionaler oder nationaler Ebene für den betreffenden Sektor oder die betreffende Art von Dienstleistung oder für andere voneinander abhängige Sektoren kritisch.

Sektor Digitale Infrastruktur

Sektor	Art der Einrichtung	Große Unternehmen	Mittlere Unternehmen	Kleinunternehmen
Anhang I				
Digitale Infrastruktur	TLD-Namenregister	Wesentlich		
	DNS-Diensteanbieter (ausgenommen Betreiber von Root-Nameserver)			
	Qualifizierte Vertrauensdiensteanbieter			
	Anbieter öffentlicher elektronischer Kommunikationsnetze oder Anbieter elektronischer Kommunikationsdienste, soweit deren Dienste öffentlich zugänglich sind	Wesentlich		Wichtig, außer falls ermittelt als wesentlich
	Vertrauensdiensteanbieter	Wesentlich	Wichtig, außer falls ermittelt als wesentlich	
	Betreiber von Internet-Knoten	Wesentlich	Wichtig, außer falls ermittelt als wesentlich	Nicht im Anwendungsbereich, außer falls ermittelt als wesentlich oder wichtig
	Anbieter von Cloud-Computing-Diensten			
	Anbieter von Rechenzentrumsdiensten			
	Betreiber von Inhaltszustellnetzen			

Danke für Ihre Aufmerksamkeit!

Inhalt: Mag. Vinzenz Heußler, LL.M.
Bundeskanzleramt, Abteilung I/8 (Cyber Security, GovCERT, NIS-Büro und ZAS)
Leiter NIS-Büro

Vortrag: Ing. Maximilian Schiessl, MSc. - CISSP, GPEN
Bundesministerium für Inneres, Abteilung IV/S/2 (Audit & Recht)
Wien, 6. Oktober 2022