



Arno Spiegel

NIS 2 und CRA

NIS2

Mag. Arno Spiegel

Bundeskanzleramt, Abteilung I/8 (Technologie- und Datenmanagement, Cybersicherheit und Krisenrechenzentrum)

Wien, 25. Oktober 2023

2 Kernpflichten für Unternehmen

Risikomanagementmaßnahmen



Berichtspflichten

Risikomanagement

- **Governance**
 - Verantwortlichkeit des Top-Managements
 - Schulungen für Top-Management
- **Risikomanagementmaßnahmen**
 - Unternehmen müssen Maßnahmen ergreifen, um die Risiken für die Sicherheit ihrer Netz- und Informationssysteme zu beherrschen und die Auswirkungen von Sicherheitsvorfällen zu verhindern oder möglichst gering zu halten

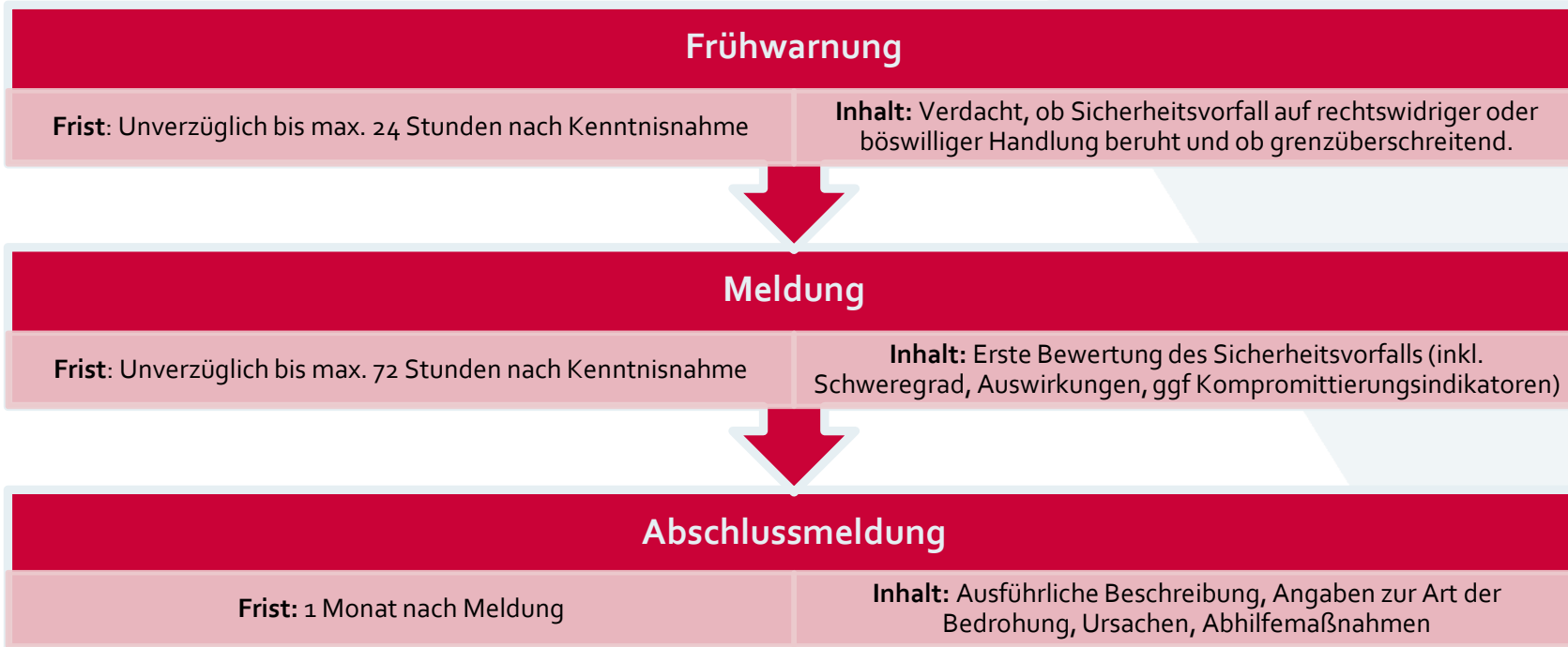
Risikomanagementmaßnahmen

- **All-Gefahren-Ansatz**
- **Risikobasierter Ansatz**
 - Angemessene und verhältnismäßige technische, operative und organisatorische Maßnahmen
 - Berücksichtigung des Stands der Technik und der Kosten der Umsetzung
 - Berücksichtigung des Ausmaßes der Risikoexposition und der Größe des Unternehmens
 - Berücksichtigung der Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen und deren Schwere (inkl. gesellschaftlichen und wirtschaftlichen Auswirkungen)

Risikomanagementmaßnahmen

- Konzepte in Bezug auf die **Risikoanalyse** und Sicherheit für Informationssysteme
- **Bewältigung** von Sicherheitsvorfällen
- **Business Continuity** und Krisenmanagement
- **Lieferkettensicherheit**
- Sicherheitsmaßnahmen bei **Erwerb**, Entwicklung und Wartung von IKT
- Grundlegende Praktiken der **Cyberhygiene** und **Schulungen** zur Cybersicherheit
- Konzepte und Verfahren für den Einsatz von **Kryptografie** und ggf Verschlüsselung
- Sicherheit des **Personals**, Konzepte für die **Zugriffskontrolle, MFA**
-

Berichtspflichten



Aufsicht

- **Aufsichtsmaßnahmen und Befugnisse**
 - 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).
- **2 Aufsichtssysteme (!)**
 - Vollwertige Aufsicht (**ex ante & ex post**) für wesentliche Einrichtungen
 - Abgeschwächte Aufsicht (**ex post**) für wichtige Einrichtungen

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

Betroffene Sektoren

Anhang I (= Sektoren mit hoher Kritikalität)	Anhang II (= sonstige kritische Sektoren)
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 Produkten 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, CDN, TSP und Anbieter öffentlicher elektronischer Kommunikationsnetze- und dienste)	
Verwaltung von IKT-Diensten (B2B)	
Öffentliche Verwaltung	
Weltraum	

Anwendungsbereich

- Anwendungsbereich durch Größenschwellenwert („**size cap rule**“) bestimmt:
 - Mittlere und große Unternehmen erfasst
 - Kleinunternehmen nur in bestimmten Ausnahmefällen umfasst
 - Level-Playing-Field
 - Öffentliche oder private Einrichtungen
 - Arten von Einrichtungen nach Spalte 3 von Anhang I & II ausschlaggebend

Prüfschema

1. Erbringt das Unternehmen seine Dienstleistungen in der EU oder übt seine Tätigkeiten in der EU aus?
2. Entspricht das Unternehmen einer in Spalte 3 von Anhang I und Anhang II genannten Art?
3. Ist das Unternehmen größer als ein Kleinunternehmen?
 - Ausnahmen und Sonderregeln: Kleinunternehmen insb. im Sektor digitale Infrastruktur erfasst und wenn sie als kritisch eingestuft werden (!)
4. Ist das Unternehmen eine wesentliche oder wichtige Einrichtung?

2. Entspricht das Unternehmen einer in Spalte 3 von Anhang I & 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

- Anhang I: 53 Arten
- Anhang II: 14 Arten

3. Ist das Unternehmen größer als ein Kleinunternehmen?

- Empfehlung 2003/361/EG der EU-Kommission
 - **Kleines Unternehmen:** ein Unternehmen, das **weniger als 50 Personen** beschäftigt **und** dessen Jahresumsatz bzw. Jahresbilanz **10 Mio. EUR** nicht übersteigt.
 - **Mittleres Unternehmen:** ein Unternehmen ab **50 bis 249 Mitarbeiter** **oder** dessen Jahresumsatz **über 10 Mio. EUR** bis **50 Mio. EUR** bzw. dessen Jahresbilanz **über 10 Mio. EUR** bis **43 Mio. EUR** ausmacht.
 - **Großunternehmen:** ein Unternehmen **ab 250 Mitarbeiter** **oder** **über 50 Mio. EUR** Jahresumsatz bzw. **über 43 Mio. EUR** Jahresbilanz.
- Benutzerleitfaden der EU-Kommission zur Definition von KMU

4. Ist das Unternehmen eine wesentliche oder wichtige Einrichtung?

- **Wesentliche Einrichtungen**
 - Alle im Anhang I angeführten Arten von Unternehmen, die groß sind.
- **Wichtige Einrichtungen**
 - Alle anderen Einrichtungen.
- **Sonderregeln:**
 - Sektor Digitale Infrastruktur

Grundregel Anwendungsbereich Anhang I

Sektoren	Große Unternehmen	Mittlere Unternehmen	Kleinunternehmen
Anhang I			
Energie / Verkehr / Bankwesen / Finanzmarktinfrastrukturen / Gesundheitswesen / Trinkwasser / Abwasser / Verwaltung von IKT-Diensten / Weltraum	wesentlich	wichtig	

- Große Unternehmen: Wesentlich
- Mittlere Unternehmen: Wichtig
- Kleinunternehmen: Grundsätzlich nicht im Anwendungsbereich

Grundregel Anwendungsbereich Anhang II

Sektoren	Große Unternehmen	Mittlere Unternehmen	Kleinunternehmen
Anhang II			
Post- und Kurierdienste / Abfallbewirtschaftung / Lebensmittel / Verarbeitendes Gewerbes bzw. Herstellung von Waren / Anbieter digitaler Dienste / Forschung	wichtig	wichtig	

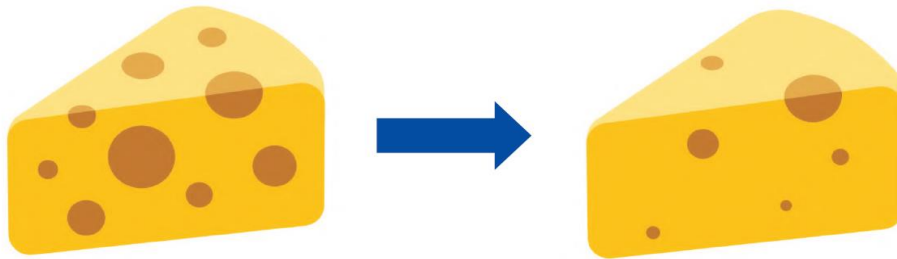
- Große Unternehmen: **Wichtig**
- Mittlere Unternehmen: **Wichtig**
- Kleinunternehmen: **Grundsätzlich nicht im Anwendungsbereich**

Hinweis

- WKÖ Online-Ratgeber „ist mein Unternehmen betroffen“
 - <https://ratgeber.wko.at/nis2>
- Sonstige Hinweise (inkl. Fact-Sheets):
 - <https://www.nis.gv.at/>

Cyber Resilience Act (CRA)

| CRA in a nutshell



(© European Commission)

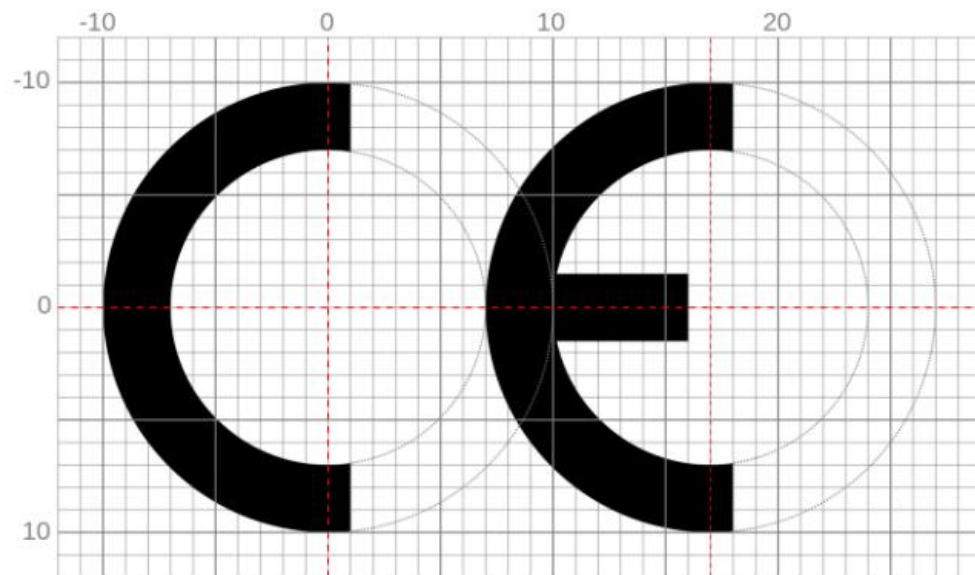
CRA I

- Einführung Cybersicherheitsregeln für die auf-den-Marktbringung von Produkten mit digitalen Elementen
- Beinhaltet Verpflichtungen für Hersteller, Distributoren und Einführer
- Verpflichtende Konformitätsbewertungen je nach Risikoniveau
- Strafen bis zu 15 Millionen, oder 2,5% des weltweiten Umsatzes.

CRA II

- Risikoniveaus:
 - 90% aller Produkte (default category): Self-Assessment
 - 10% entweder
 - Critical „Class I“ (Standard oder Third-Party Assessment)
 - Critical „Class II“ (Third-Party Assessment)

CRA III - Ziel



Danke für Ihre Aufmerksamkeit!

Bundeskanzleramt, Abteilung I/8 (Technologie- und Datenmanagement, Cybersicherheit und
Krisenrechenzentrum)
Wien, 25. Oktober 2023