Die Cybersicherheits-Richtlinie NIS2

Mag. Verena Becker, BSc
Bundessparte Information und Consulting
Wirtschaftskammer Österreich

11. März 2024
Innovation und Digitalisierung WK Niederösterreich

WKO
WIRTSCHAFTSKAMMER ÖSTERREICH

Vorstellung Mag. Verena Becker, BSc (WU)

- Cybersicherheitsexpertin in der Bundessparte Information und Consulting/WKÖ
- Cofounderin des Frauennetzwerks Women4Cyber Austria
- Mitglied der ENISA Ad Hoc Working Group on Enterprise Security
- Juristin – Betriebswirtin - Wirtschaftstrainerin
- Information Security Managerin

11. März 2011

Quelle: filin174 | stock.adobe.com

Fehler in Fukushima

- Mythos Technik ist sicher
- bekannte Schwächen nicht ausgemerzt
- mangelndes Lernen aus anderen Vorfällen
- mangelnde Sicherheitskultur
- miserables Krisenmanagement

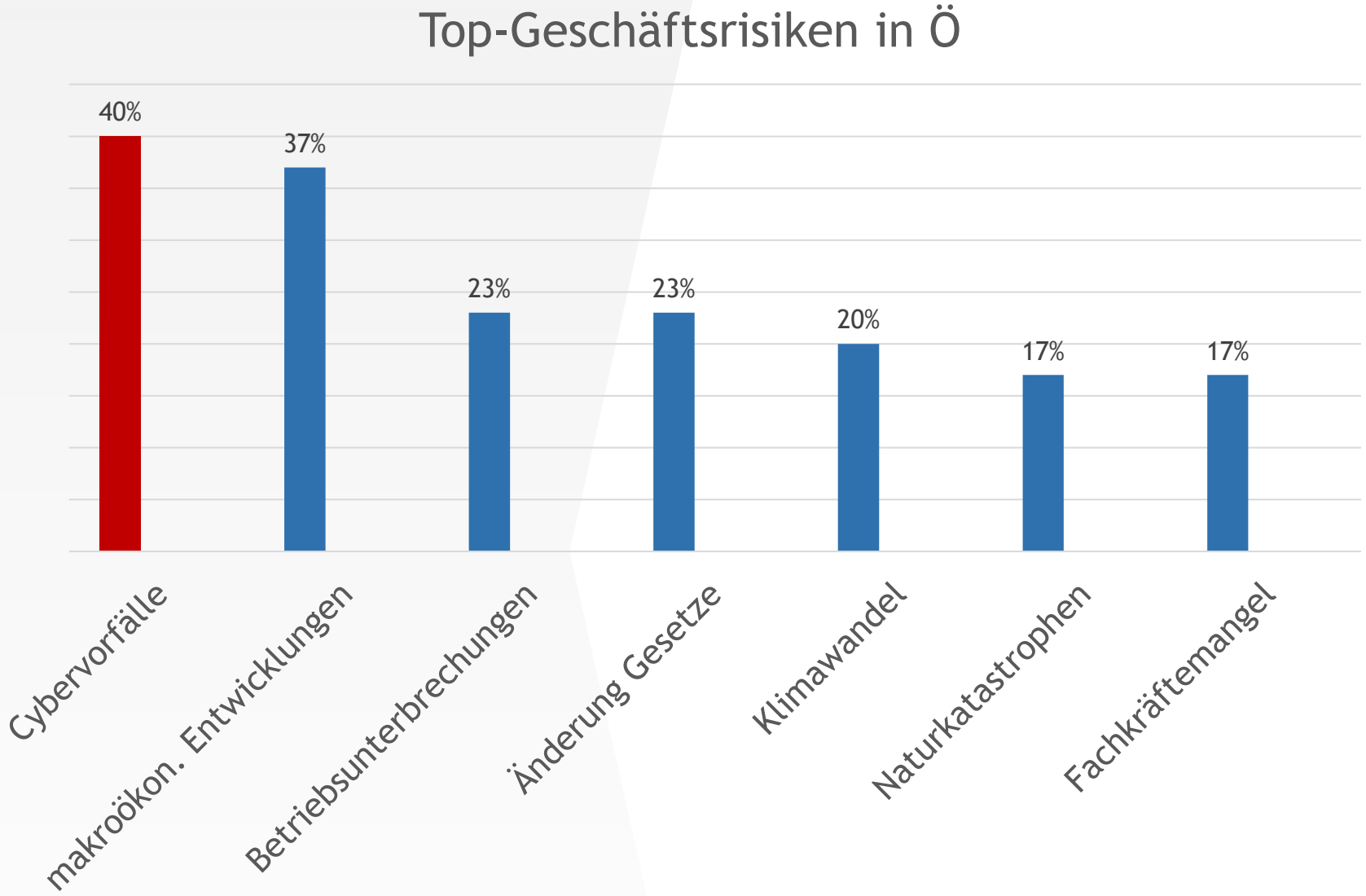
Lehren aus Fukushima

- Risikomanagement
- Standards einhalten
- ALLE einbeziehen
- Testen
- Krisenmanagement

Agenda

- Cybersecurity und NIS2 in Österreich
- NIS2 in a nutshell
- Bin ich betroffen?
- Was muss ich tun?
- Was ist wenn ich nichts tue?

Cybersecurity ist größtes Risiko für Unternehmen



Quelle: Allianz Risk Barometer 2024 Pressemitteilung | Allianz Commercial

NIS2 in a nutshell

- **NIS** – **S**icherheit von **N**etz- und **I**nformationssystemen
- Umsetzung bis 17. Oktober 2024 in nationales Gesetz
- **Risikomanagementmaßnahmen und Meldepflichten**
- betroffen: **große und mittlere Unternehmen bestimmter Sektoren**
- betroffen: **Digitale Infrastruktur**
- indirekt betroffen: **Lieferkette**

Wer fällt unter die neue NIS2-Gesetzgebung?

- **Energieunternehmen**

7.000 Beschäftigte; EUR 3 Mrd. Umsatz

- **Maschinenbauunternehmen**

32 Beschäftigte, EUR 12 Mio. Jahresumsatz

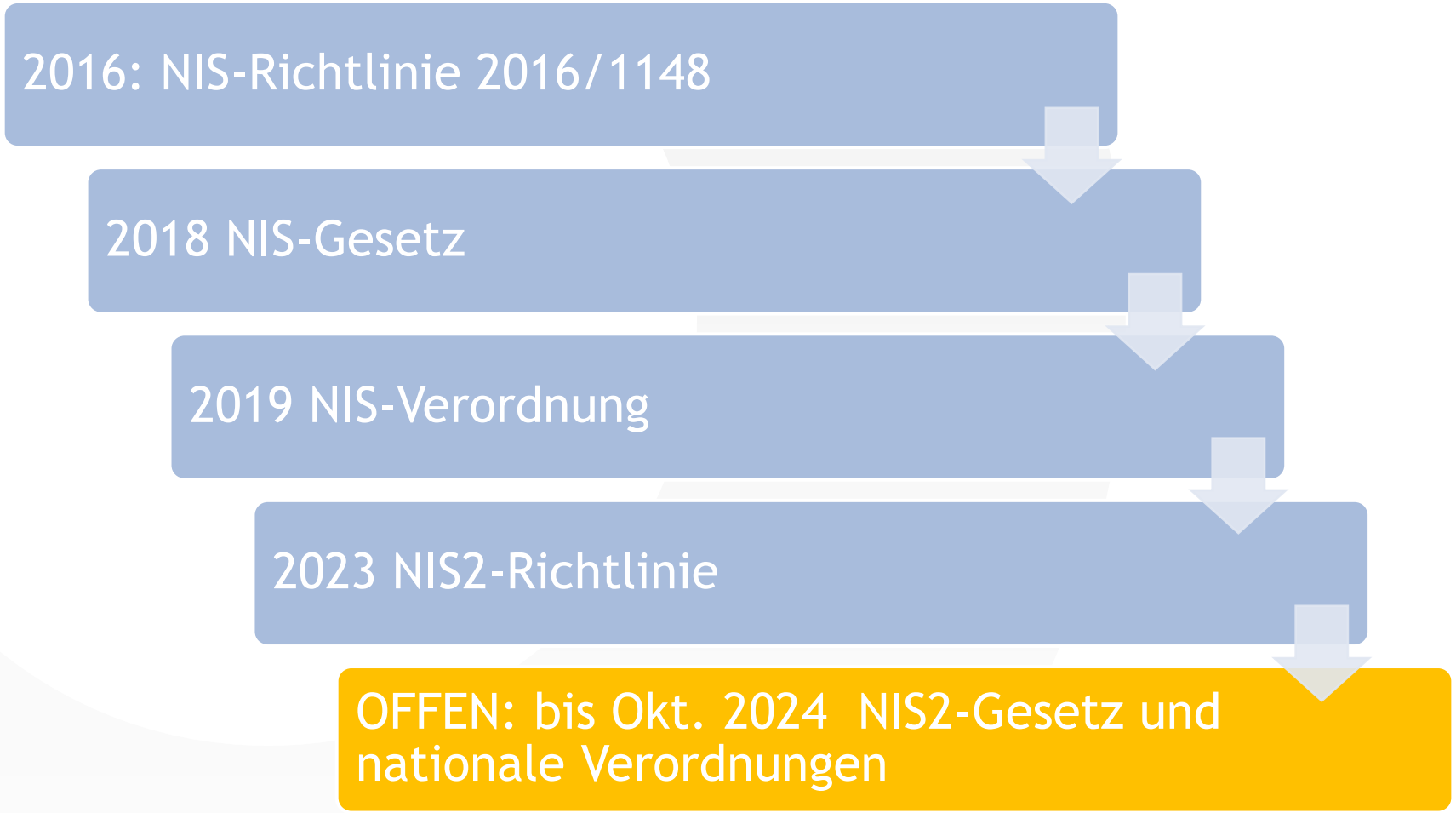
- **Fischzuchtbetrieb**

2 Beschäftigte, EUR 14 Mio. Umsatz

- **Rechenzentrum**

18 Beschäftigte, Tochter eines Unternehmens in China mit 3.000 Beschäftigten

NIS-Gesetzgebung – noch ohne NIS2-Gesetz



WKO WIRTSCHAFTSKAMMER ÖSTERREICH

Bin ich betroffen?

Betroffen sind mittlere und große Unternehmen bestimmter Sektoren

Prüfschema:

1. **EU ?**
2. **Sektor**: Anhang I und Anhang II ?
3. **mittleres oder großes Unternehmen ?***

Zusatzfrage: wesentliche oder wichtige Einrichtung?

*Sonderregeln für Digitale Infrastruktur oder wenn als kritisch eingestuft

Betroffen sind mittlere und große Unternehmen bestimmter Sektoren

Prüfschema:

1. **EU ?**
2. **Sektor: Anhang I und Anhang II ?**
3. **mittleres oder großes Unternehmen ?***

Zusatzfrage: wesentliche oder wichtige Einrichtung?

*Sonderregeln für Digitale Infrastruktur oder wenn als kritisch eingestuft

Betroffen sind mittlere und große Unternehmen bestimmter Sektoren

Anhang I - hohe Kritikalität

- Energie
- Verkehr
- Bankwesen
- Finanzmarktinfrastrukturen
- Gesundheitswesen
- Trinkwasser
- Abwasser
- Digitale Infrastruktur
- Verwaltung von IKT-Diensten (B2B)
- öffentliche Verwaltung
- Weltraum

Anhang II - sonstige Kritikalität

- Post- und Kurierdienste
- Abfallbewirtschaftung
- Chemie (Herstellung und Handel)
- Lebensmittel (Großhandel, ind. Produktion, und Verarbeitung)
- verarbeitendes Gewerbe/Herstellung von Waren
- Anbieter digitaler Dienste
- Forschung

Betroffen sind mittlere und große Unternehmen bestimmter Sektoren

Prüfschema:

1. **EU ?**
2. **Sektor**: Anhang I und Anhang II ?
3. **mittleres oder großes Unternehmen ?***

*Sonderregeln für Digitale Infrastruktur oder wenn als kritisch eingestuft

Betroffen sind mittlere und große Unternehmen

Größenklasse	Beschäftigte (VZÄ)	Jahresumsatz	Jahresbilanzsumme
Kleines Unternehmen (KU)	< 50 **und**	⩽ 10 Mio. Euro **oder**	⩽ 10 Mio. Euro
Mittleres Unternehmen (MU)	< 250 **und**	⩽ 50 Mio. Euro **oder**	⩽ 43 Mio. Euro
Großes Unternehmen (GU)	⩾ 250 **oder**	> 50 Mio. Euro **und**	> 43 Mio. Euro

Benutzerleitfaden der EU-Kommission zur Definition von KMU

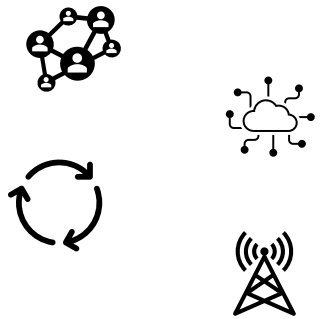
Empfehlung der Kommission Definition von KMU

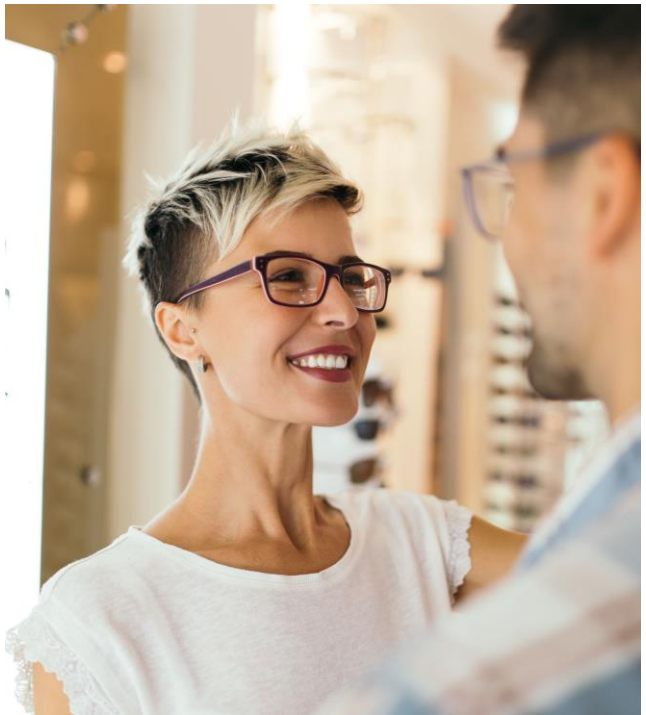
Kleine Unternehmen sind nicht betroffen

Kleinunternehmen

- bis 49 Beschäftigte UND
- Jahresumsatz/Jahresbilanz bis 10 Mio. EUR

- Ausnahmen:
  - verbundene oder Partner-Unternehmen
  - Digitale Infrastruktur
  - Lieferkette (indirekt über Kunden betroffen)
  - wichtig eingestuft





Fällt die „Metall Warrior GmbH“

Maschinenbauunternehmen

mit 32 Beschäftigten und EUR 12 Mio.

Jahresumsatz unter NIS2?

WKO
WIRTSCHAFTSKAMMER ÖSTERREICH

Betroffen sind mittlere und große Unternehmen bestimmter Sektoren

Prüfschema:

- **EU ?**
- **Sektor**: Anhang I und Anhang II ?
- **mittleres oder großes Unternehmen ?**

Maschinenbau ist im Anhang II von NIS2

ANHANG II

SONSTIGE KRITISCHE SEKTOREN

Sektor	Teilsektor	Art der Einrichtung
5. Verarbeitendes Gewerbe/Herstellung von Waren	d) Maschinenbau	Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 28 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
	e) Herstellung von Kraftwagen und Kraftwagenteilen	Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 29 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben

WKO
WIRTSCHAFTSKAMMER ÖSTERREICH

„Metall Warrior GmbH“

Maschinenbauunternehmen mit 32 Beschäftigten und EUR 12 Mio. Jahresumsatz

- NIS2-Richtlinie Anhang II: Maschinenbau
- mittleres Unternehmen

→ ja, NIS2

- *https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555&qid=1674579731975&from=EN#d1e32-143-1

Betroffen sind mittlere und große Unternehmen bestimmter Sektoren

Prüfschema:

1. **EU ?**
2. **Sektor**: Anhang I und Anhang II ?
3. **mittleres oder großes Unternehmen ?***

Zusatzfrage: wesentliche oder wichtige Einrichtung?

Anhang II → „nur“ wichtige Einrichtung

NIS2 unterscheidet wesentliche und wichtige Einrichtungen

Wesentliche Einrichtungen

große Einrichtungen
laut Anhang I

- strengere Aufsicht
- Audits
- höhere Strafdrohung

Wichtige Einrichtungen

mittlere Einrichtungen Anhang I
große und mittlere Einrichtungen Anhang II

Digitale Infrastruktur

WKO
WIRTSCHAFTSKAMMER ÖSTERREICH

Sektor	Art der Einrichtung	groß	mittel	klein
Digitale Infrastruktur	**TLD-Namenregister** **qualifizierte Vertrauensdiensteanbieter**	wesentlich		
	DNS Diensteanbieter (ausgenommen Betreiber von Root-Nameserver)			
	Anbieter öffentlicher elektronischer **Kommunikationsnetze** oder elektronischer **Kommunikationsdienste**	wesentlich		wichtig
	Vertrauensdiensteanbieter	wesentlich	wichtig	
	Betreiber von **Internet-Knoten**	wesentlich	wichtig	
	Anbieter von **Cloud-Computing-Diensten**			
	Anbieter von **Rechenzentrumsdiensten**			
	Betreiber von **Content Delivery Networks** (CDN)			

Wer fällt unter die neue NIS2-Gesetzgebung?

- **Fischzuchtbetrieb**

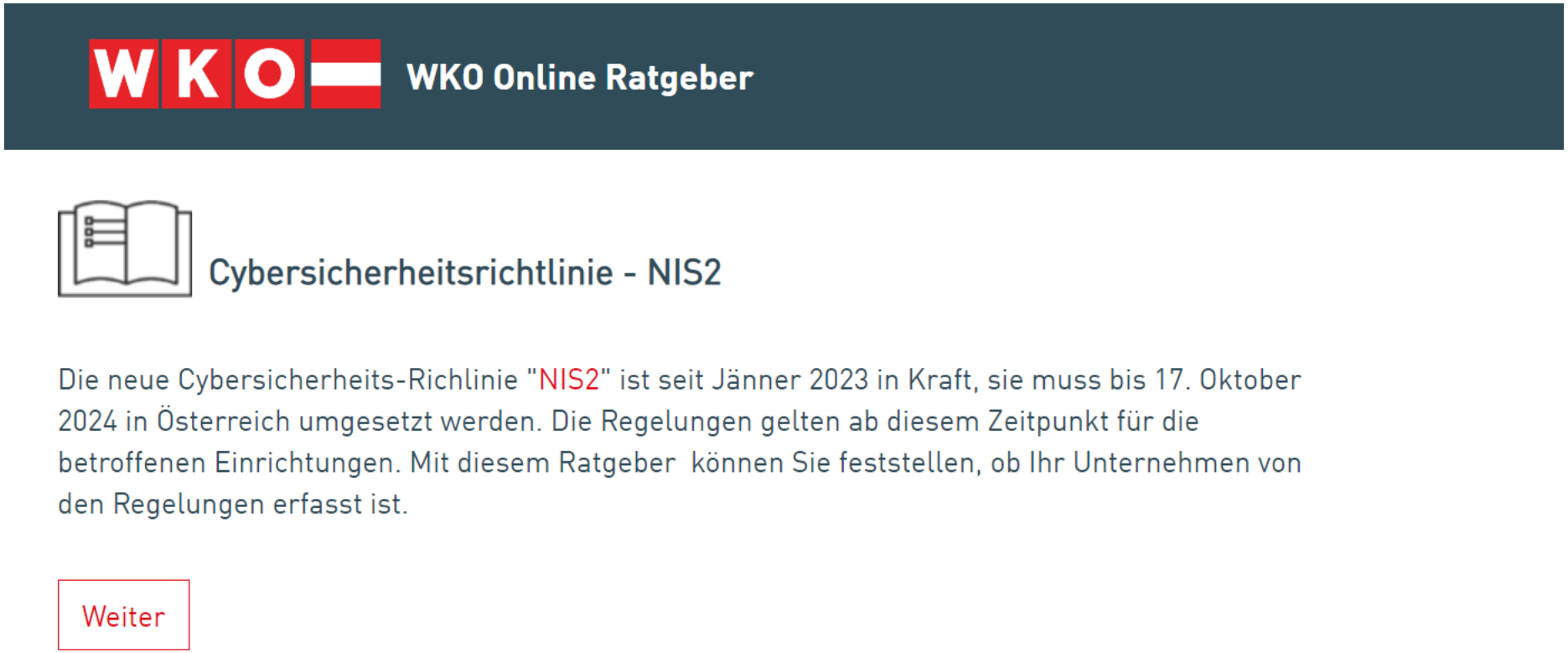
2 Beschäftigte, EUR 14 Mio. Umsatz

- **Rechenzentrum**

2 Beschäftigte, Tochter eines Unternehmens in China mit 3.000 Beschäftigten

Ist mein Unternehmen betroffen?

www.ratgeber.wko.at/nis2



Was muss ich tun?

NIS2 verpflichtet Einrichtungen

- Risiken zu beherrschen
- Auswirkungen von Sicherheitsvorfällen zu verhindern bzw. möglichst gering zu halten
- Meldepflichten
- Governance

10 Risikomanagementmaßnahmen

- Konzept **Risikoanalyse** und Sicherheit für Informationssysteme
- **Bewältigung** von Sicherheitsvorfällen
- **Business Continuity** und Krisenmanagement
- **Lieferkettensicherheit**
- Sicherheitsmaßnahme[illegible]ung/Wartung von IKT
- Konzepte und Verfahren[illegible]ertung der Wirksamkeit von Risikomanagementmaßnahmen
- **Cyberhygiene** und **Schulungen** zur Cybersicherheit
- **Kryptografie** und ggf Verschlüsselung
- Sicherheit des **Personals**, Konzepte für die **Zugriffskontrolle**
- **Multi-Faktor-Authentifizierung** oder kontinuierliche Authentifizierung

- dem Risiko angemessen
- Kosten

3-stufiges Meldeverfahren bei erheblichen Sicherheitsvorfällen

01 **Frühwarnung**
unverz. bis 24h nach Kenntnis

02 **Meldung**
bis 72h nach Kenntnis

03 **Abschlussmeldung -**
bis 1 Monat nach Meldung

Leitungsorgane sind verantwortlich

Verantwortlichkeit des
Top-Managements

Schulungen für das
Top-Management

Was ist wenn ich nichts tue?

Sanktionen

- 10 Mio EUR oder 2% des weltweiten Jahresumsatzes (wesentlich)
- 7 Mio EUR oder 1,4% des weltweiten Jahresumsatzes (wichtig)
- persönliche Haftung für Leitungsorgane

Cybersecurity ist unverzichtbar im Unternehmen

WKO WIRTSCHAFTSKAMMER ÖSTERREICH

17. Oktober 2024

Mag. Verena Becker, BSc

Bundessparte Information und Consulting
Wirtschaftskammer Österreich
T 05 90 900-3176
E verena.becker@wko.at
W https://wko.at/nis2
W https://it-safe.at