Was bedeutet die Cybersicherheits-Richtlinie NIS 2 für Unternehmen?

Wirtschaftskammer Niederösterreich - Krisenresilienz für Unternehmen
29. November 2023

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

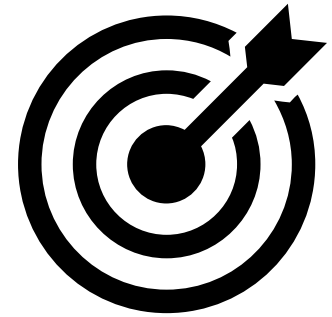
Mustermann GmbH, you are fucked.
DO NOT TOUCH ANYTHING!

Use Tor.
Password: N2OiN(Q66!{,Tw+

OK

Cybercrime in Österreich

33 % waren Opfer einer Ransomware-Attacke



55 % sagen, dass Cyberangriffe ihre geschäftliche Existenz bedrohen

201 % Zunahme von Cyberangriffen im Vorjahr

Quelle: Cybersecurity in Österreich; KPMG-Studie; veröffentlicht im Mai 2023 – Link zum Bestellen: info.kpmg.at/cyber-security-2023/

WKO INFORMATION · CONSULTING

Situation in der EU

- **EUR 250.000** sind die geschätzten direkten **Kosten** eines größeren Informationssicherheitsvorfalls (2022: EUR 200.000 im Jahr 2021)

- **1 Monat** benötigen 51 % der Organisationen um kritische **Schwachstellen** in IT- oder OT-Assets zu **schließen** (Transportsektor)

Quelle: ENISA investment report 2023

Warum tun die Unternehmen zu wenig für Cybersicherheit?

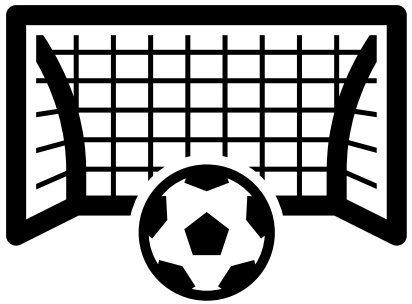
Die 7 größten Herausforderungen für Unternehmen 2023*

- Inflation und wirtschaftlicher Abschwung
- Sicherung der Lieferkette
- Steigende Kundenerwartungen
- Beschleunigte digitale Transformation
- Krieg um Talente
- Sicherheit von Daten und Geräten
- Nachhaltigkeit

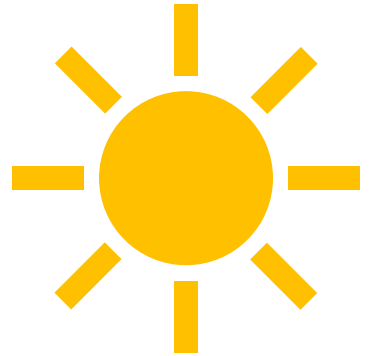
*The 7 Biggest Business Challenges Every Company Is Facing In 2023 (forbes.com)

kurzfristiger Erfolg versus Belohnungsaufschub

- kurzfristig:



langfristig:



Themen heute

Was ist NIS überhaupt?

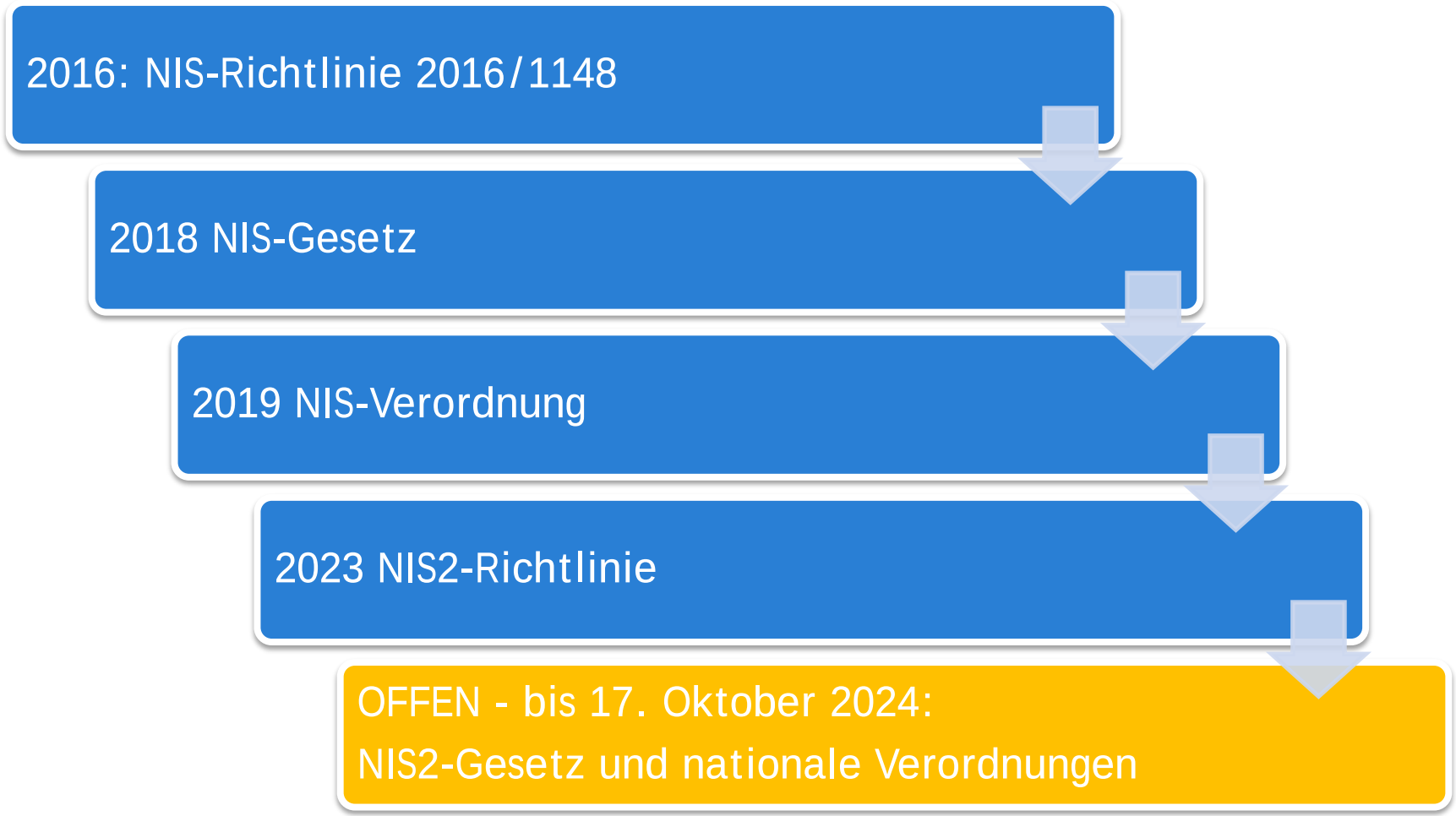
Wofür steht NIS?

NIS - Sicherheit von **N**etz- und **I**nformationssystemen

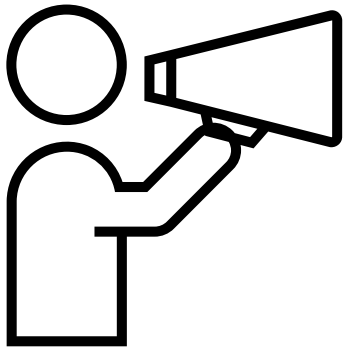
Cybersicherheits-Richtlinie NIS2 in a nutshell

- NIS – Sicherheit von Netz- und Informationssystemen
- Umsetzung bis 17. Oktober 2024 in nationales Gesetz
- **Risikomanagementmaßnahmen und Meldepflichten**
- betroffen: **große und mittlere Unternehmen bestimmter Sektoren**
- betroffen**: Digitale Infrastruktur**
- indirekt betroffen: **Lieferkette**

NIS-Gesetzgebung



Disclaimer



Informationen beruhen auf NIS2-Richtlinie vorbehaltlich der innerstaatlichen Umsetzung

Bin ich betroffen?

Anwendungsbereich

Artikel 2

Diese Richtlinie gilt

- *für **öffentliche oder private Einrichtungen***
- *der in den **Anhang I oder II genannten Art**,*
- *die […] als **mittlere Unternehmen** gelten oder die **Schwellenwerte für mittlere Unternehmen** […] **überschreiten** und*
- *ihre Dienste **in der Union** erbringen oder ihre Tätigkeiten dort ausüben.*

Wer ist unmittelbar betroffen - Prüfschema

1. **EU ?**
2. **Sektor**: Anhang I und Anhang II Spalte 3 ?
3. **mittleres oder großes Unternehmen ?***
4. wesentliche oder wichtige Einrichtung?

*Sonderregeln für Digitale Infrastruktur
oder wenn als kritisch eingestuft

WKO INFORMATION · CONSULTING

Anhang I

Sektoren mit hoher Kritikalität

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

Anhang II

Sektoren mit sonstiger Kritikalität

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

rot=neu gegenüber NIS1
blau=Ergänzungen im Sektor
schwarz=NIS1

Ist das Unternehmen eine Einrichtung entsprechend Spalte 3 des Anhangs I oder II?

SEKTOREN MIT HOHER KRITIKALITÄT

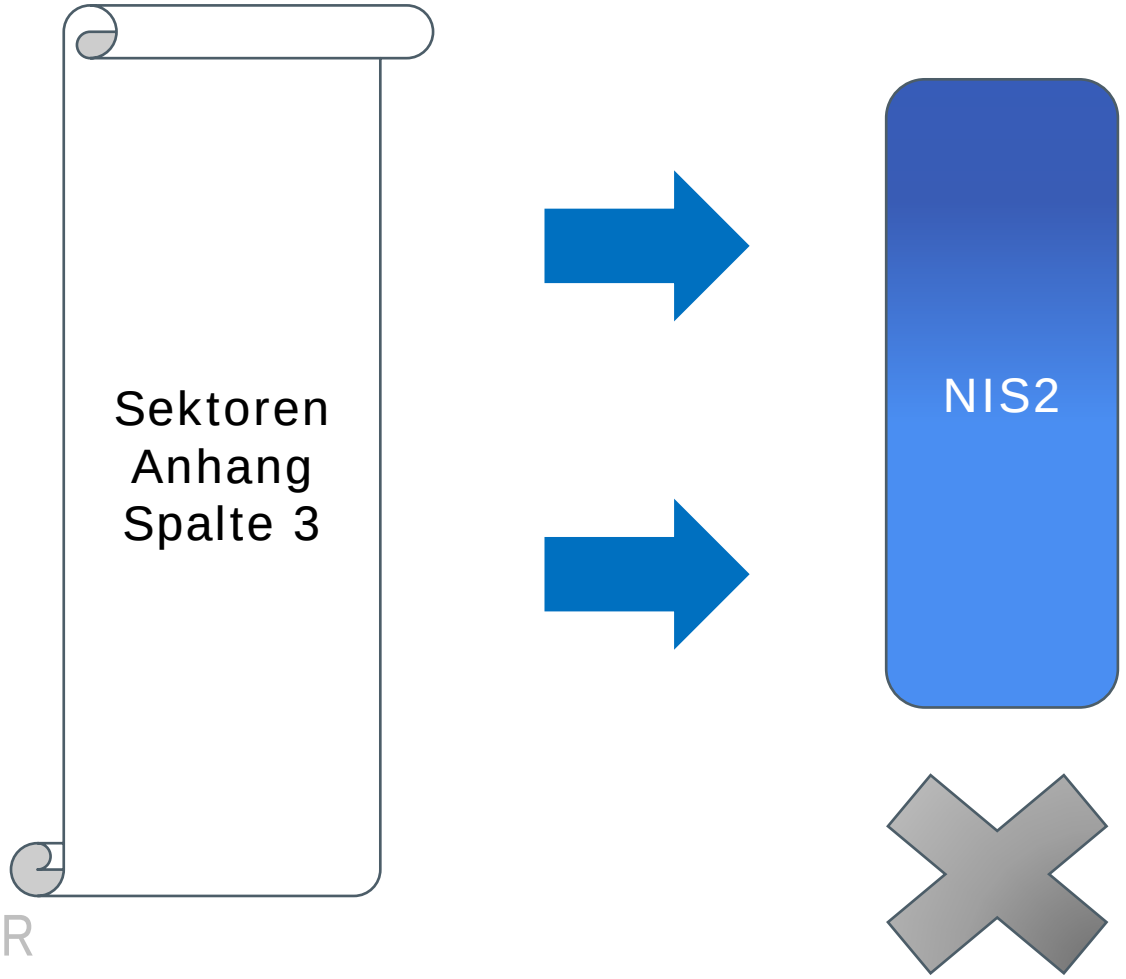
Sektor	Teilsektor	Art der Einrichtung
1. Energie	a)Elektrizität	— Elektrizitätsunternehmen im Sinne des Artikels 2 Nummer 57 der Richtlinie (EU) 2019/944 des Europäischen Parlaments und des Rates ([1]), die die Funktion „Versorgung“ im Sinne des Artikels 2 Nummer 12 jener Richtlinie wahrnehmen
		— Verteilernetzbetreiber im Sinne von Artikel 2 Nummer 29 der Richtlinie (EU) 2019/944
		— Übertragungsnetzbetreiber im Sinne des Artikels 2 Nummer 35 der Richtlinie (EU) 2019/944
		— Erzeuger im Sinne des Artikels 2 Nummer 38 der Richtlinie (EU) 2019/944
		— nominierte Strommarktbetreiber im Sinne des Artikels 2 Nummer 8 der Verordnung (EU) 2019/943 des Europäischen Parlaments und des Rates ([2])
		— Marktteilnehmer im Sinne des Artikels 2 Nummer 25 der Verordnung (EU) 2019/943, die Aggregierungs-, Laststeuerungs- oder Energiespeicherungsdienste im Sinne des Artikels 2 Nummern 18, 20 und 59 der Richtlinie (EU) 2019/944 anbieten
		— Betreiber von Ladepunkten, die für die Verwaltung und den Betrieb eines Ladepunkts zuständig sind und Endnutzern einen Aufladedienst erbringen, auch im Namen und Auftrag eines Mobilitätsdienstleisters
	b)Fernwärme und -kälte	— Betreiber von Fernwärme oder Fernkälte im Sinne des Artikels 2 Nummer 19 der Richtlinie (EU) 2018/2001 des Europäischen Parlaments und des Rates ([3])
	c)Erdöl	— Betreiber von Erdöl-Fernleitungen
		— Betreiber von Anlagen zur Produktion, Raffination und Aufbereitung von Erdöl sowie Betreiber von Erdöllagern und Erdöl-Fernleitungen
		— zentrale Bevorratungsstellen im Sinne des Artikels 2 Buchstabe f der Richtlinie 2009/119/EG des Rates ([4])

Wer ist betroffen?

große Unternehmen

mittlere Unternehmen

kleine Unternehmen:
bis 49 Beschäftigte oder
Jahresumsatz/Jahresbilanz bis 10 Mio. EUR



Benutzerleitfaden der EU-Kommission zur Definition von KMU

Sind kleine Unternehmen betroffen?

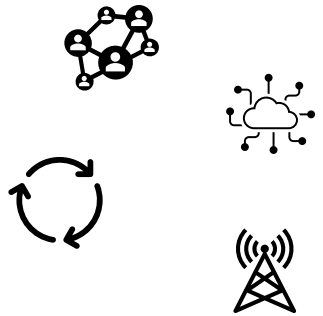
Kleinunternehmen nicht unter NIS2:

bis 49 Beschäftigte UND

Jahresumsatz/Jahresbilanz bis 10 Mio. EUR

Ausnahmen:

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



Unternehmensgrößen

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

Beispiel Anwendungsbereich

„Ostbahn GmbH“

Eisenbahnunternehmen mit 320 Beschäftigten und 80 Mio Jahresbilanzsumme

→ NIS2 Richtlinie Anhang I Spalte 3:

2. Verkehr	a)Luftverkehr	— Luftfahrtunternehmen im Sinne des Artikels 3 Nummer 4 der Verordnung (EG) Nr. 300/2008, die für gewerbliche Zwecke genutzt werden
		— Flughafenleitungsorgane im Sinne des Artikels 2 Nummer 2 der Richtlinie 2009/12/EG des Europäischen Parlaments und des Rates ([6]), Flughäfen im Sinne des Artikels 2 Nummer 1 jener Richtlinie, einschließlich der in Anhang II Abschnitt 2 der Verordnung (EU) Nr. 1315/2013 des Europäischen Parlaments und des Rates ([7]) aufgeführten Flughäfen des Kernnetzes, und Einrichtungen, die innerhalb von Flughäfen befindliche zugehörige Einrichtungen betreiben
		— Betreiber von Verkehrsmanagement- und Verkehrssteuerungssystemen, die Flugverkehrskontrolldienste im Sinne des Artikels 2 Nummer 1 der Verordnung (EG) Nr. 549/2004 des Europäischen Parlaments und des Rates ([8]) bereitstellen
	b)Schienenverkehr	— Infrastrukturbetreiber im Sinne des Artikels 3 Nummer 2 der Richtlinie 2012/34/EU des Europäischen Parlaments und des Rates ([9])
		— Eisenbahnunternehmen im Sinne des Artikels 3 Nummer 1 der Richtlinie 2012/34/EU, einschließlich Betreiber einer Serviceeinrichtung im Sinne des Artikels 3 Nummer 12 jener Richtlinie

Beispiel Anwendungsbereich

„Ostbahn GmbH“;

Eisenbahnunternehmen mit 320 VZÄ und 80 Mio Jahresbilanzsumme

- NIS2-Richtlinie*
- Anhang I Z 2 Spalte 3: Eisenbahnunternehmen
- großes Unternehmen (≥250 VZÄ)

→ ja, fällt unter NIS2

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

Unterscheidungsmerkmal: wesentlich vs. wichtig

Wesentliche Einrichtungen

große Einrichtungen
laut Anhang I

Wichtige Einrichtungen

mittlere Einrichtungen Anhang I
große und mittlere Einrichtungen Anhang II

Digitale Infrastruktur

Grundregel Anhang I
Sektoren mit hoher Kritikalität

Sektor	groß	mittel	klein
Energie / Verkehr / Bankwesen / Finanzmarkt / Gesundheit / Trinkwasser / Abwasser / Verwaltung von IKT-Diensten / Weltraum	wesentlich	wichtig	--

- Große Unternehmen → wesentlich
- Mittlere Unternehmen → wichtig
- Kleinunternehmen → nicht im Anwendungsbereich

Grundregel Anwendungsbereich Anhang II – sonstige kritische Sektoren

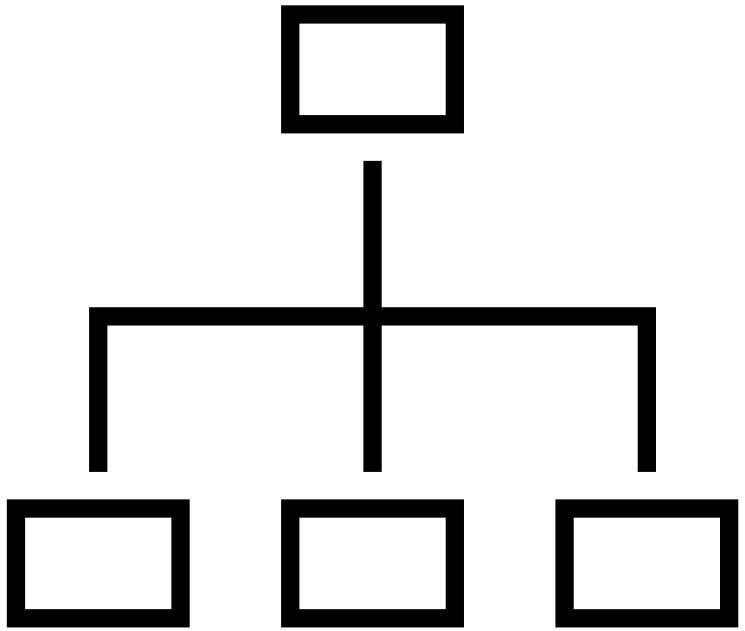
Sektor	groß	mittel	klein
Post und Kurier / Abfall / Chemie / Lebenmittel / Produktion / Digitale Dienste / Forschung	wichtig	wichtig	--

- Große Unternehmen → wichtig
- Mittlere Unternehmen → wichtig
- Kleinunternehmen → nicht im Anwendungsbereich

wesentliche Einrichtung	wichtige Einrichtung
Aufsicht:	
ex-ante Aufsicht und ex-post	**ex-post**
• regelmäßige Sicherheitsprüfungen • Stichprobenkontrollen	• nur bei begründetem Verdacht
Sanktionen	
• bis zu EUR 10 Mio oder 2 Prozent des weltweiten Umsatzes	• bis zu EUR 7 Mio oder bei 1,4 Prozent des weltweiten Umsatzes

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)			

komplexe Unternehmensstrukturen - Konzern



bei Beteiligungen ab 25%

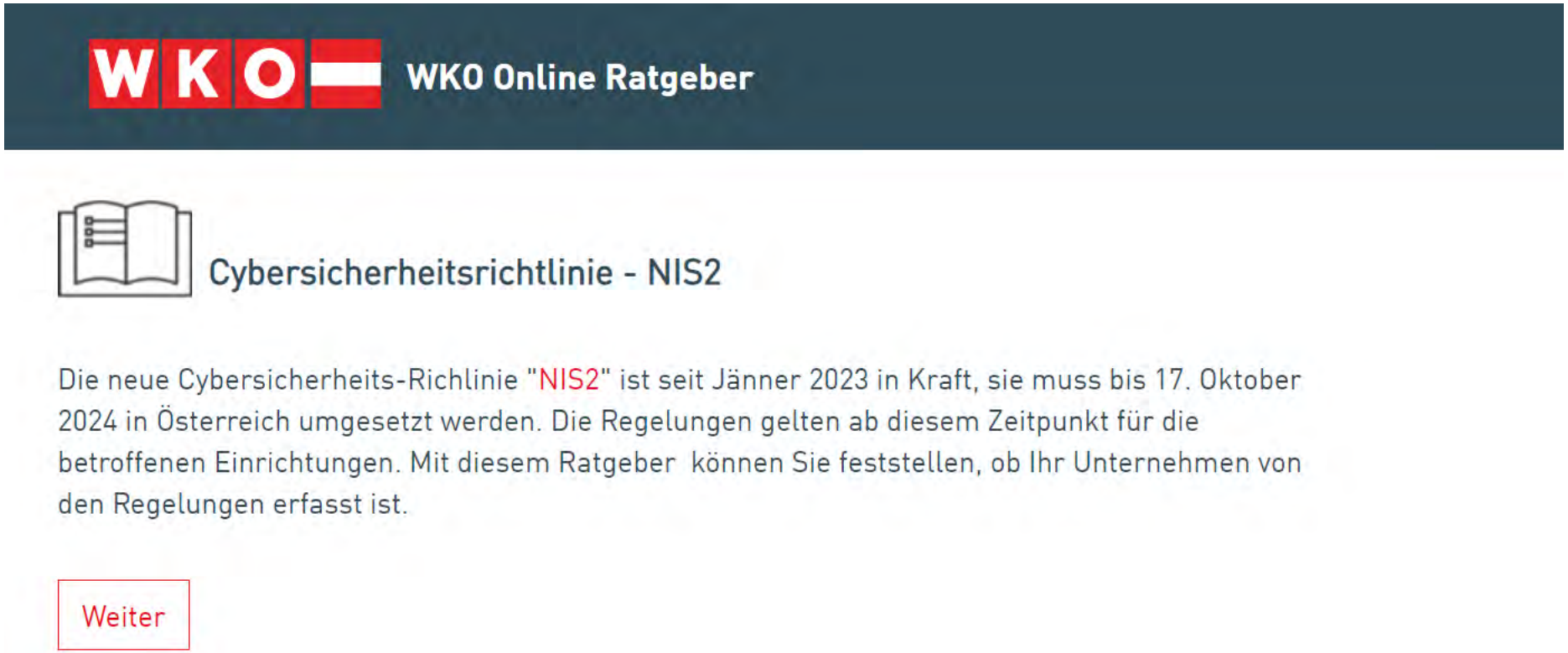
Verhältnismäßigkeitsprüfung betreffend

Grad der **Unabhängigkeit**

Empfehlung der EU-Kommission
Benutzerleitfaden der EU-Kommission zur Definition von KMU

Ist mein Unternehmen betroffen?

www.ratgeber.wko.at/nis2



Was muss ich tun?

Identifikation betroffener Unternehmen?

vorbehaltlich Gesetzesentwurf!!!

- **Unternehmen muss sich selbst als wesentlich oder wichtige Einrichtung einstufen**

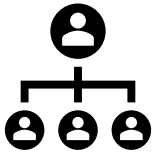
- Bescheid (wie unter NIS-Gesetz derzeit) nur mehr in Ausnahmefällen

NIS2 im Unternehmen

Risikomanagementmaßnahmen

Berichtspflichten

Verantwortlichkeit des Top-Managements



Risikomanagementmaßnahmen

Risiken für die Sicherheit
der Netz- und Informationssysteme beherrschen

Auswirkungen von Sicherheitsvorfällen verhindern
oder möglichst gering zu halten

10 Risikomanagementmaßnahmen – Art. 21 Abs. 2

- Konzept **Risikoanalyse** und Sicherheit für Informationssysteme
- **Bewältigung** von Sicherheitsvorfällen
- **Business Continuity** und Krisenmanagement
- **Lieferkettensicherheit**
- Sicherheitsmaßnahmen bei **Erwerb/**Entwicklung/Wartung von IKT
- Konzepte und Verfahren zur Bewertung 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

10 Risikomanagementmaßnahmen

- Konzept **Risikoanalyse** und Sicherheit für Informati[illegible]systeme
- **Bewältigung** von Sicherheitsvorfällen
- **Business Continuity** und Krise[illegible]
- **Lieferkettensicherh[illegible]**
- Sicherheits[illegible]artung von IKT
- Konzepte u[illegible]er Wirksamkeit von Risikomanagementmaßnahmen
- **Cyberhygien[illegible]** zur Cybersicherheit
- **Kryptografie** u[illegible] Verschlüsselung
- Sicherheit des **Personals**, Konzepte für die **Zugriffskontrolle**
- **Multi-Faktor-Authentifizierung oder kontinuierliche Authentifizierung**

- Stand der Technik*
- Normen
- dem Risiko angemessen
- Kosten

* Stand der Technik - TeleTrusT - Bundesverband IT-Sicherheit e.V. / IT Security Association Germany

WKO INFORMATION · CONSULTING

NIS2 für alle – die Sicherheit der Lieferkette

Beziehung zu DL/Lieferant

- spezifische **Schwachstellen**
- **Gesamtqualität** der Produkte
- **Cybersicherheitspraxis**

WKO INFORMATION · CONSULTING

Berichtspflichten bei erheblichen Sicherheitsvorfällen

Frühwarnung

unverz. bis 24h nach Kenntnis

Verdacht, ob Sicherheitsvorfall auf rechtswidriger oder böswilliger Handlung beruht und ob grenzüberschreitend

Meldung

bis 72h nach Kenntnis

Erste Bewertung des Sicherheitsvorfalls (inkl. Schweregrad, Auswirkungen, ggf Kompromittierungsindikatoren)

Abschlussmeldung –

bis 1 Monat nach Meldung

Ausführliche Beschreibung, Angaben zur Art der Bedrohung, Ursachen, Abhilfemaßnahmen

Governance

Verantwortlichkeit des Top-Managements

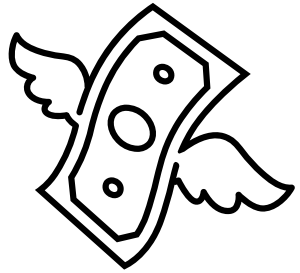
Schulungen für Top-Management

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

Kosten und Schäden bei Sicherheitsvorfällen

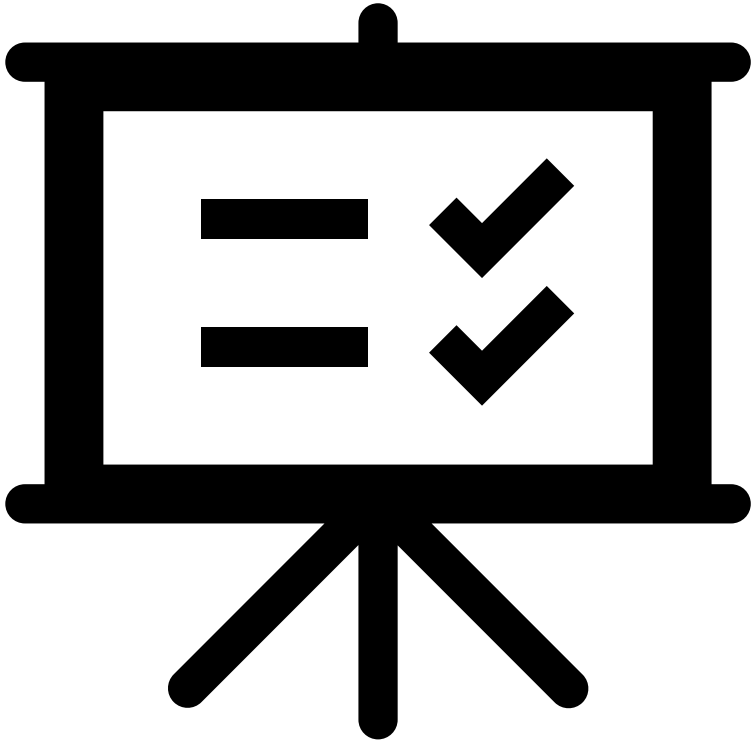


- **Security Kosten**: Datenwiederherstellung, Forensik, Hard- und Software)
- **Betriebsunterbrechung**: Mehrkosten Aufrechterhaltung und Wiederherstellung, entgangener Gewinn
- **finanzieller Schaden**: durch Hacking, Zahlen von Lösegeldern, etc.
- **Krisenmanagement**: PR-Beratung, Krisenmanager, etc.
- **Haftung und Schadenersatzansprüche**: Weiterleitung Schadsoftware, Verletzung von Geheimhaltungspflichten, Vertragsstrafen, etc.
- **Data Breach**: Datenschutzverletzung, Rechts- und PR-Beratung, Benachrichtigungskosten
- **Strafen**

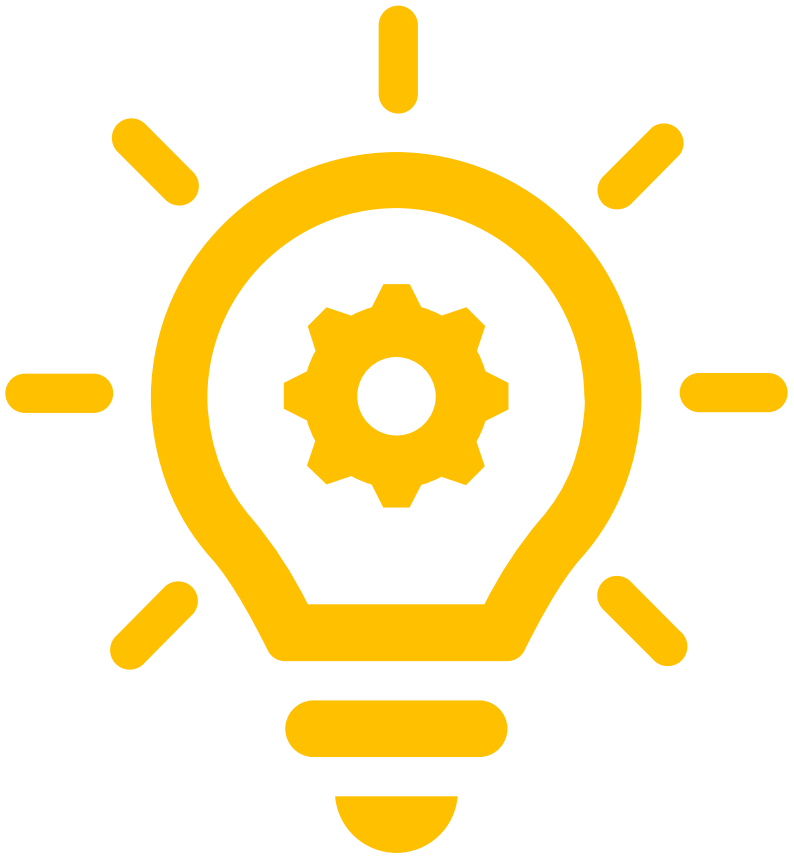
Wie geh ich´s an?

NIS2 – wie geh ich´s an?

1. Betroffenheit klären
2. Ressourcen einplanen
3. Assetmanagement
4. Risikoanalyse und Lücken in Bezug auf NIS2
5. Maßnahmen ermitteln und umsetzen



Nutzen



- Identifizierung von Schwachstellen
- bessere Abwehrfähigkeit von Angriffen
- Transparenz
- Vermeidung Beeinträchtigung des Geschäftsbetriebs
- Erfüllung der gesetzlichen Vorgaben/Compliance
- Vermeiden von Haftungen, Strafen, Reputationsverlust, etc.
- ...

Wie unterstützt die WKO Unternehmen?

- Informationen zu NIS2 - https://wko.at/nis2
- Online-Ratgeber NIS2 – https://ratgeber.wko.at/nis2
- Informationen zu Cybersicherheit – https://it-safe.at
  - ✓ Förderungen: Cyber Security Schecks (FFG)
  - ✓ Suche nach IT-Security-Expert: innen und
  - ✓ NIS2-Berater:innen https://mein.wko.at/ unter Produkte

Cyber Security Schecks – NIS2 Förderung für KMU

- Wer: KMU im direkten NIS2-Anwendungsbereich
- Was: Kosten für Technologien sowie für technische Beratungsleistungen
- Höhe: maximal 40%, maximal EUR 10.000

https://www.ffg.at/ausschreibung/CyberSecuritySchecks2023

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://it-safe.at | W https://wko.at/nis2