

# Die neue Cybersicherheits-Richtlinie NIS2

IT Security Fokustalk SIC Kärnten am 17. Mai 2023

**Mag. Verena Becker, BSc (WU)**

Bundessparte Information und Consulting/WKÖ

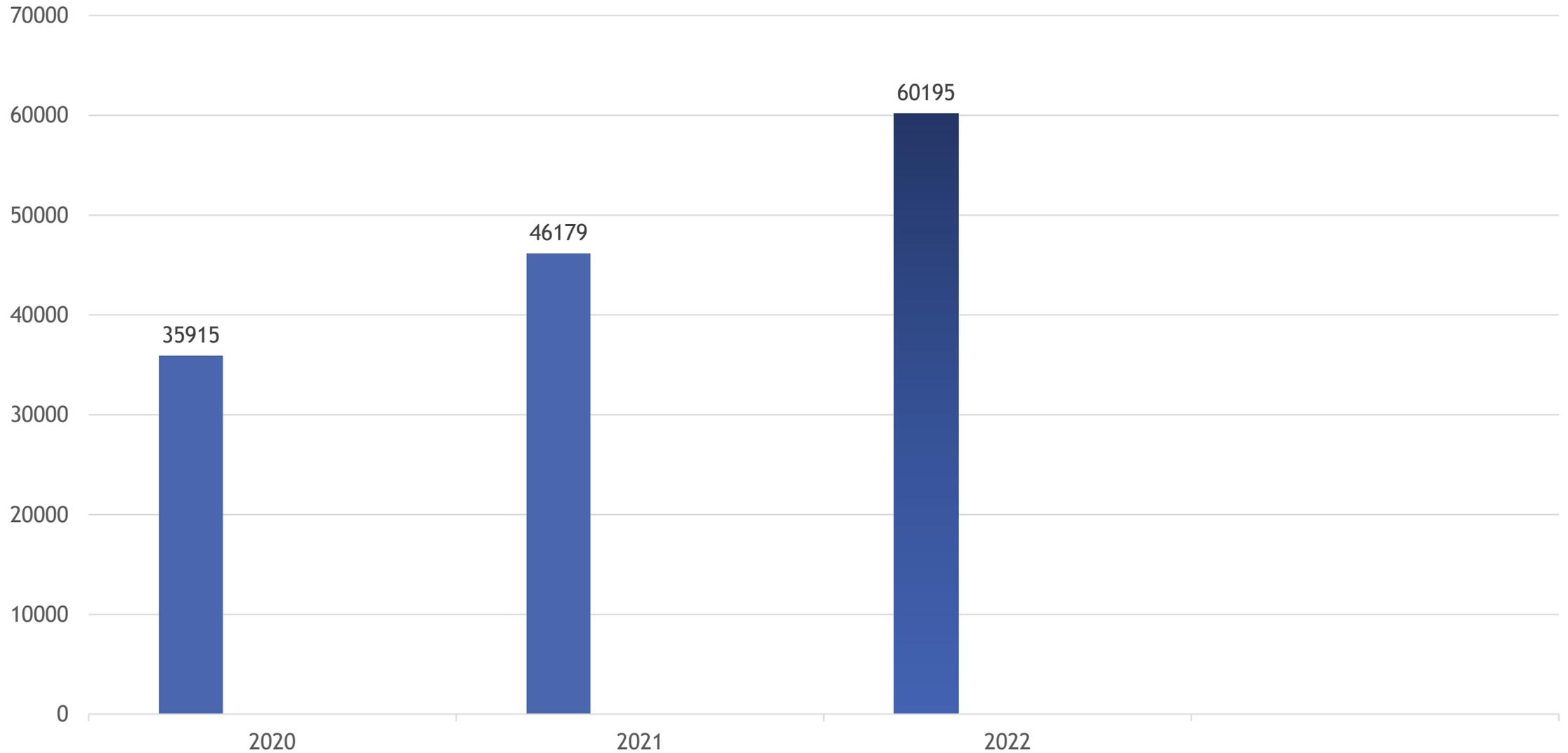
# WARNING!

09:53:15

All your important files are encrypted.  
Browse here to get an access to your system and files.  
Any attempt to restore the drives using other way will  
lead to inevitable data loss!!!  
Remember your ID:  
With its help a sign-in password will be generated.

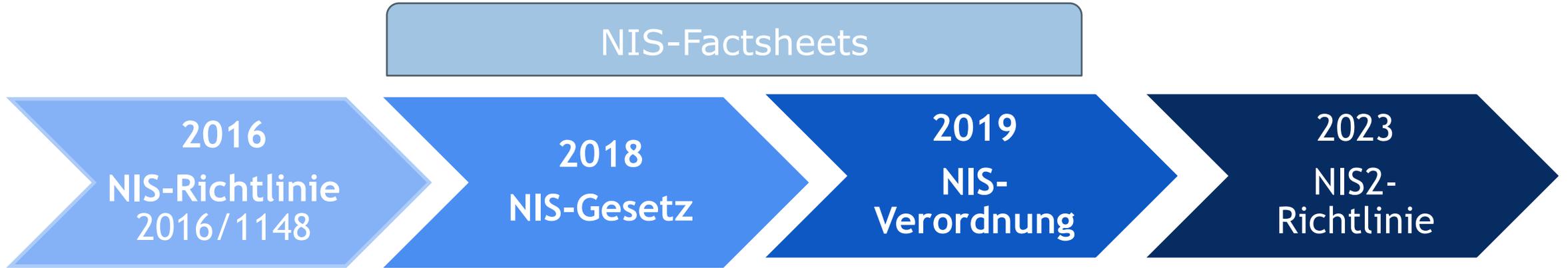
Enter password: \*\*\*\*\*

# Anzeigen Cybercrime



Quelle:  
PK Lagebericht Internetkriminalität 2022, 16.5.2023  
2020: Cybercrime Report BMI

# NIS - Netzwerk- und Informationssicherheit



Richtlinie (EU) 2022/2555 vom 14. Dezember 2022

über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau

in der Union

# NIS2 im Unternehmen

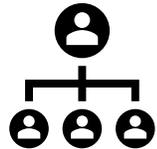


Risikomanagementmaßnahmen



Berichtspflichten

Verantwortlichkeit des Top-Managements



# Risikomanagementmaßnahmen



Risiken für die Sicherheit der Netz- und Informationssysteme beherrschen



Auswirkungen von Sicherheitsvorfällen verhindern oder möglichst gering zu halten

# Risikomanagementmaßnahmen

- Konzept **Risikoanalyse** und Sicherheit für Informationssysteme
- **Bewältigung** von Sicherheitsvorfällen
- **Business Continuity** und Krisenmanagement
- **Lieferkettensicherheit**
- Sicherheitsmaßnahmen bei **Erwerb/Entwicklung/Wartung** von IKT
- **Cyberhygiene** und **Schulungen** zur Cybersicherheit
- **Kryptografie** und ggf Verschlüsselung
- Sicherheit des **Personals**, Konzepte für die **Zugriffskontrolle**, **MFA**

# Lieferkette

**Sicherheit der Lieferkette** einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen Einrichtungen und unmittelbaren (Dienste-)Anbietern

- spezifische **Schwachstellen**
- **Gesamtqualität** der Produkte
- **Cybersicherheitspraxis** einschließlich der Sicherheit Entwicklungsprozesse

# Berichtspflichten



# Governance

Verantwortlichkeit des Top-Managements



Schulungen für Top-Management



## Durchsetzung

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



## Wer ist betroffen - Prüfschema



➤ **EU?**

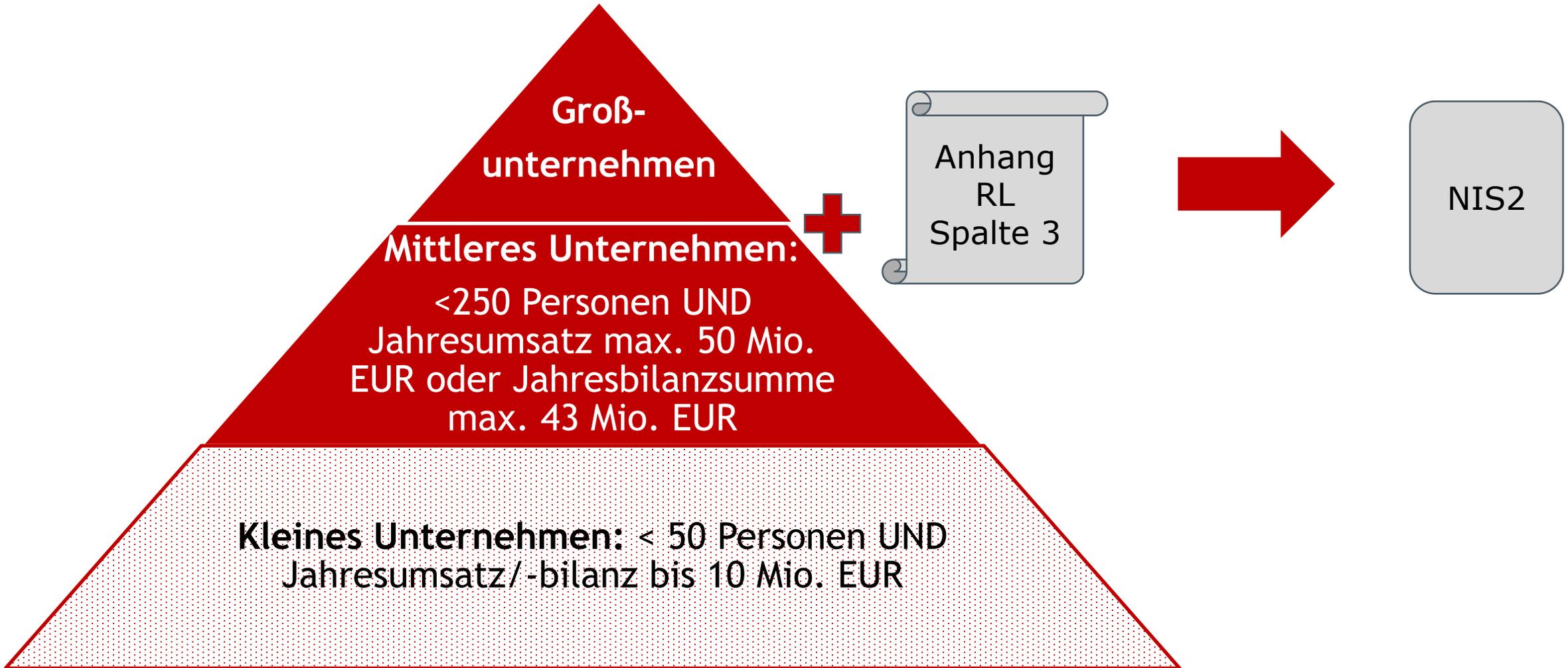
➤ **mittleres oder großes Unternehmen?**

Ausnahmen: Sektor **digitale Infrastruktur** oder wenn als **kritisch** eingestuft

➤ **Sektor:** Anhang I und Anhang II Spalte 3 ?

→ wesentliche oder wichtige Einrichtung?

# Große und mittlere Unternehmen betroffen



## 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 <sup>(1)</sup> , 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 <sup>(2)</sup>
		— 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 <sup>(3)</sup>
	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 <sup>(4)</sup>		

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

## wesentliche oder wichtige Einrichtung?

- **Wesentliche Einrichtungen**
  - große Einrichtungen laut Anhang I
- **Wichtige Einrichtungen**
  - alle anderen Einrichtungen
- **Sonderregeln:**
  - Sektor Digitale Infrastruktur

# Ist mein Unternehmen betroffen?

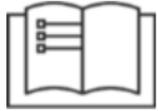
<https://ratgeber.wko.at/nis2>



## Cybersicherheitsrichtlinie - NIS2

Die neue Cybersicherheits-Richtlinie "**NIS2**" ist seit Jänner 2023 in Kraft, sie muss bis 17. Oktober 2024 in Österreich umgesetzt werden. Die Regelungen gelten ab diesem Zeitpunkt für die betroffenen Einrichtungen. Mit diesem Ratgeber können Sie feststellen, ob Ihr Unternehmen von den Regelungen erfasst ist.

Weiter



## Cybersicherheitsrichtlinie - NIS2

### Ihre Angaben

Ratgeber erneut starten

NIS1: Nein

### Fortschritt



## Schwellenwerte

### Wie groß ist Ihr Unternehmen? ⓘ

- Kleines Unternehmen, das weniger als 50 Personen beschäftigt und dessen Jahresumsatz bzw. Jahresbilanz 10 Mio. EUR nicht übersteigt

---

- Mittleres Unternehmen, das weniger als 250 Personen beschäftigt und das entweder einen Jahresumsatz von höchstens 50 Mio. EUR erzielt oder dessen Jahresbilanzsumme sich auf höchstens 43 Mio. EUR beläuft

---

- Großunternehmen (alle Unternehmen, sofern kein kleines oder mittleres Unternehmen)

---



## Cybersicherheitsrichtlinie - NIS2

### Ihre Angaben

Ratgeber erneut starten

NIS1: Nein

Schwellenwerte: Großunternehmen (alle Unternehmen, sofern kein kleines oder mittleres Unternehmen)

### Fortschritt



### Sektor

In welchem Sektor sind Sie tätig?

- Energie
- Verkehr
- Bankwesen ⓘ
- Finanzmarktinfrastrukturen
- Gesundheitswesen
- Trinkwasser ⓘ
- Abwasser ⓘ
- Digitale Infrastruktur
- Weltraum ⓘ Rechteckiges Ausschneiden
- Post- und Kurierdienste ⓘ
- Abfallbewirtschaftung ⓘ
- Produktion, Herstellung und Handel mit chemischen Stoffen ⓘ
- Produktion, Verarbeitung und Vertrieb von Lebensmitteln ⓘ
- Verarbeitendes Gewerbe/Herstellung von Waren
- In keinem der Angeführten

## 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
  - ✓ Betrugswarnungen
  - ✓ Suche nach [IT-Security-Expert: innen](#)



...Freitagmorgen, 18. Oktober 2024

*Was ist NIS2???*

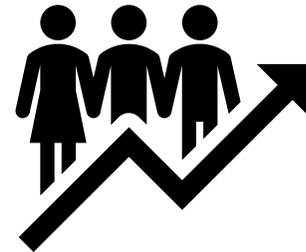


Oktober 2024

Expert:innen



gut vorbereitete Unternehmen





## Mag. Verena Becker, BSc

Bundessparte Information und Consulting  
Wirtschaftskammer Österreich

T 05 90 900-3176

E [verena.becker@wko.at](mailto:verena.becker@wko.at)

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