

Alles, was  
uns verbindet.



# Was ist NIS-2?

Und was bedeutet die aktualisierte Richtlinie  
für Ihr Unternehmen?



# Was ist NIS-2?



Die NIS-2-Richtlinie (Network and Information Security Directive 2) ist die aktualisierte Version der europäischen Richtlinie über Netz- und Informationssicherheit (NIS), die darauf abzielt, ein höheres Sicherheitsniveau im Bereich der Netz- und Informationssysteme in der EU zu gewährleisten. Sie wurde 2022 verabschiedet und erweitert den Geltungsbereich und die Anforderungen an Unternehmen erheblich.

Die NIS-2 ist darauf ausgerichtet, die Cybersicherheit zu verbessern, indem sie verbindliche Maßnahmen für Unternehmen und Organisationen festlegt, die als „wesentlich“ oder „wichtig“ für die europäische Wirtschaft und Gesellschaft angesehen werden. Sie stärkt die Abwehr gegen Cyberbedrohungen und sorgt für eine stärkere Zusammenarbeit zwischen den EU-Mitgliedstaaten.



# Wen betrifft NIS-2?

Kriterien nach Unternehmenssektoren

Die NIS-2-Richtlinie gilt für eine Vielzahl von Branchen und Unternehmen, die als systemrelevant für die Wirtschaft und das Funktionieren der Gesellschaft angesehen werden. Grundsätzlich werden zur Einstufung zwei Kriterien geprüft: Unternehmenssektor und Unternehmensgröße.

## 1.

### Wesentliche Sektoren (Essential Entities):

- ▶ **Energie** (Strom, Gas, Öl, erneuerbare Energien)
- ▶ **Transport** (Luftfahrt, Eisenbahnen, Schifffahrt, Straßenverkehr)
- ▶ **Banken und Finanzmarktinfrastrukturen**
- ▶ **Gesundheit** (Krankenhäuser, Labore, Gesundheitsdienstleister)
- ▶ **Wasserwirtschaft**
- ▶ **Öffentliche Verwaltung**

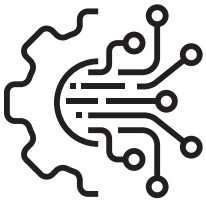
## 2.

### Wichtige Sektoren (Important Entities):

- ▶ **Digitale Infrastrukturen und Anbieter** (Rechenzentren, Content Delivery Networks, Marktplätze, Suchmaschinen, soziale Netzwerke)
- ▶ Hersteller von **Arzneimitteln und Medizinprodukten**
- ▶ **Lebensmittelproduktion** (Verarbeitung und Vertrieb)
- ▶ **Chemie** (Herstellung und Vertrieb)
- ▶ **Telekommunikationsanbieter** und Internetdienste
- ▶ **Entsorgungsunternehmen**
- ▶ **Post- und Kurierdienste**
- ▶ **Forschung** (Forschungsinstitute)

# Wen betrifft NIS-2?

## Kriterien nach Unternehmensgrößen



Die Unternehmen werden aber nicht ausschließlich nach ihrer Bedeutung für die wirtschaftliche und gesellschaftliche Infrastruktur oder nach ihrer Tätigkeit in kritischen oder wichtigen Sektoren klassifiziert. Auch die Größe eines Unternehmens spielt dabei eine ausschlaggebende Rolle.

Um in den Anwendungsbereich von NIS-2 zu fallen ist eine gibt es definierte Mindestanforderungen an die Unternehmensgröße. Man unterscheidet hier grundsätzlich zwischen **zwei verschiedenen Unternehmensgrößen** die nachfolgend beschrieben sind:

### 1.

**Mittelgroße und große Unternehmen in wesentlichen und wichtigen Sektoren sind automatisch von der NIS-2 betroffen. Nach der EU-Definition gilt Folgendes:**

- ▶ **Mittelgroße Unternehmen:**  
50–249 Mitarbeiter und ein Jahresumsatz oder eine Jahresbilanzsumme von nicht mehr als 50 Mio. Euro.
- ▶ **Große Unternehmen:**  
Mehr als 250 Mitarbeiter und ein Jahresumsatz oder eine Jahresbilanzsumme von über 50 Mio. Euro.

### 2.

**Kleinere Unternehmen (KMU)** sind in der Regel von der NIS-2 ausgenommen, **es sei denn, sie erbringen wesentliche oder wichtige Dienstleistungen in kritischen Sektoren.**

In diesen Fällen können auch kleine Unternehmen betroffen sein, wenn sie beispielsweise als Lieferanten oder Partner von größeren, systemrelevanten Unternehmen tätig sind.

▶ **Zusammengefasst sind vor allem mittelgroße und große Unternehmen in den betroffenen Sektoren direkt verpflichtet, die Anforderungen der NIS-2 umzusetzen. Kleinere Unternehmen können in speziellen Fällen ebenfalls unter die Regelungen fallen, insbesondere wenn sie als Lieferanten oder Dienstleister für betroffene Unternehmen fungieren.**

# Wen betrifft NIS-2?

## Ausnahmen



Unabhängig von der Unternehmensgröße und dem Umsatz gibt es spezielle Ausnahmen, beispielsweise für Unternehmen, die kritische Tätigkeiten ausüben oder Auswirkungen auf die öffentliche Ordnung haben. Auch Systemrisiken und grenzüberschreitende Folgen im Falle eines Ausfalls können dazu führen, dass diese Unternehmen unter den Anwendungsbereich der NIS-2 fallen, selbst wenn sie weniger als 50 Mitarbeiter haben oder einen Jahresumsatz von unter 10 Millionen Euro erzielen.

Ebenso kann ein Unternehmen in bestimmten Fällen vollständig von der NIS-2 ausgeschlossen sein:

Die NIS-2-Richtlinie findet keine Anwendung auf Einrichtungen, die in Bereichen wie Verteidigung, nationale Sicherheit, öffentliche Sicherheit und Strafverfolgung tätig sind. Auch Justizbehörden, Parlamente und Zentralbanken fallen nicht unter den Anwendungsbereich. Für öffentliche Verwaltungen auf zentraler und regionaler Ebene gilt jedoch die NIS-2-Richtlinie.

Darüber hinaus haben die Mitgliedstaaten die Möglichkeit zu entscheiden, dass die Richtlinie auch für lokale Einrichtungen Anwendung findet.

### **Auch Dienstleister oder Unternehmen, welche Teil der Lieferkette eines NIS-2 betroffenen Unternehmens sind, werden in den NIS-2-Prozess integriert.**

So werden auch in diesen, nicht unmittelbar betroffenen Unternehmen Kriterien wie Lieferantenbeziehung, Risikomanagement, Zugangs- und Datenmanagement, Krisenmanagement, Compliance und Berichterstattung, Zusammenarbeit und Informationsaustausch relevant.

### **Noch unsicher?**

Beim **BSI** (Bundesamt für Sicherheit in der Informationstechnik) können Sie eine **anonyme Eigenprüfung/Einstufung** nach o.g. Kriterien durchführen lassen.

Diese erstellt Ihnen anhand konkreter, am Gesetzentwurf orientierter Fragen eine automatisierte Ersteinschätzung, ob Ihr Unternehmen vom NIS-2 betroffen ist und erläutert Ihnen, was dieser Status bedeutet und welche Pflichten durch den Gesetzgeber vorgezeichnet sind. Die Nutzung der NIS-2-Betroffenheitsprüfung erfolgt anonym!

„NIS-2-Betroffenheitsprüfung“ unter:  
<https://www.bsi.bund.de>

# Was muss ich tun?



Unternehmen, die unter die NIS-2-Richtlinie fallen, müssen spezifische Maßnahmen ergreifen, um die Cybersicherheit zu erhöhen und sich auf Vorfälle vorzubereiten. Die wichtigsten Maßnahmen umfassen:

## 1.

### Risikomanagement und Sicherheitsmaßnahmen:

- ▶ Unternehmen müssen effektive Sicherheitsstrategien entwickeln und umsetzen, die technische, organisatorische und personelle Maßnahmen beinhalten.
- ▶ Es müssen Risiken für die Informationssicherheit identifiziert und gemanagt werden, und geeignete Maßnahmen zur Minimierung dieser Risiken müssen umgesetzt werden.

## 3.

### Cybersicherheits-Governance:

- ▶ Führungskräfte und Management müssen sich aktiv an der Cybersicherheitsstrategie beteiligen.
- ▶ Es muss sichergestellt werden, dass die Verantwortung für Cybersicherheit klar definiert ist, und die Unternehmensleitung trägt eine erweiterte Verantwortung für die Umsetzung der Sicherheitsmaßnahmen.

## 2.

### Meldung von Sicherheitsvorfällen:

- ▶ Wesentliche und wichtige Unternehmen sind verpflichtet, schwerwiegende Sicherheitsvorfälle innerhalb von 24 Stunden an die zuständigen nationalen Behörden zu melden.
- ▶ Eine detaillierte Analyse und ein umfassender Bericht müssen innerhalb von 72 Stunden erfolgen.

## 4.

### Sicherstellung der Lieferkettensicherheit:

- ▶ Unternehmen müssen sicherstellen, dass ihre Dienstleister und Partner entlang der Lieferkette ebenfalls robuste Sicherheitsvorkehrungen treffen.
- ▶ Dies beinhaltet auch die Zusammenarbeit mit Dritten, um Sicherheitsstandards zu überprüfen und zu überwachen.

## 5.

### Überprüfung und Auditierung:

- ▶ Regelmäßige Überprüfungen und Audits müssen durchgeführt werden, um sicherzustellen, dass die Sicherheitsmaßnahmen angemessen und effektiv sind.
- ▶ Behörden haben das Recht, Unternehmen auf Einhaltung der NIS-2 zu prüfen und bei Nichteinhaltung Sanktionen zu verhängen.

# Wie gehe ich jetzt vor?



  
**ISO 27001**  
Information Security Management Systems

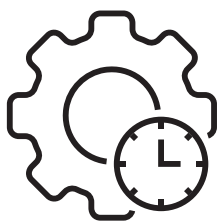


Die beste Art, die Cyber-Sicherheit eines Unternehmen zu verbessern bzw. zu gewährleisten, ist die Einführung eines sog. ISMS-Systems. Ein ISMS (Information Security Management System) bietet einen systematischen Ansatz zur Verwaltung und Sicherung von Informationen innerhalb einer Organisation. Risikomanagement, Zuständigkeiten und Notfallpläne sind dabei die zentralen Elemente.

Das ISMS sorgt dafür, dass geeignete Sicherheitsmaßnahmen implementiert werden, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu schützen und Risiken durch Cyberangriffe zu minimieren.

ISMS werden häufig nach dem anerkannten Standard ISO 27001 eingerichtet, der international gültig ist. Diese Norm bietet einen bewährten Rahmen für die Einrichtung, Umsetzung, Überwachung und Verbesserung eines effektiven ISMS. Durch die Implementierung eines ISMS gemäß ISO 27001 können Unternehmen eine nachhaltige Grundlage schaffen, um die Anforderungen der NIS-2-Richtlinie zu erfüllen.

# Fristen und Umsetzungszeitplan



**Die Fristen für die Umsetzung der NIS-2-Richtlinie sind klar festgelegt:**

## Ende 2024:

Alle EU-Mitgliedstaaten müssen die NIS-2-Richtlinie in nationales Recht umgesetzt haben. Unternehmen müssen dann mit den Vorbereitungen beginnen, um die neuen Anforderungen zu erfüllen.

## 2025:

Unternehmen müssen alle geforderten Maßnahmen umgesetzt haben, um die Anforderungen der NIS-2 zu erfüllen. Es wird erwartet, dass bis spätestens Mitte 2025 alle notwendigen Vorkehrungen getroffen sind, um Sanktionen zu vermeiden.

## Nach Umsetzung:

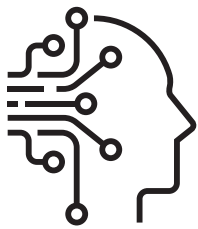
Regelmäßige Überprüfungen und Kontrollen durch die nationalen Behörden werden durchgeführt, um die Einhaltung sicherzustellen. Unternehmen, die die Vorschriften nicht einhalten, müssen mit erheblichen Bußgeldern und Sanktionen rechnen.

## Was passiert, wenn die Richtlinie nicht umgesetzt wird?

Unternehmen, die die Anforderungen der NIS-2 nicht erfüllen, müssen mit strengen Strafen rechnen. Diese können von finanziellen Bußgeldern bis hin zu vorübergehenden oder dauerhaften Verboten von Dienstleistungen reichen. Die Höhe der Bußgelder hängt vom Sektor und der Schwere des Verstoßes ab, kann jedoch in schweren Fällen Millionenbeträge erreichen.



# Wer unterstützt mich bei der Umsetzung der neuen NIS-2 Richtlinien?



Mit KEVAG Telekom sind sie auf der sicheren Seite – Schritt für Schritt.

## Schritte zur Vorbereitung:

- ▶ 1. Durchführung einer umfassenden Risikobewertung der Netzwerksicherheit.
- ▶ 2. Investition in neue Cybersicherheitsmaßnahmen und Schulung der Mitarbeiter.
- ▶ 3. Einführung eines Meldesystems für Sicherheitsvorfälle.
- ▶ 4. Zusammenarbeit mit externen Sicherheitsanbietern, um die Einhaltung der Richtlinie zu gewährleisten.
- ▶ 5. Sicherstellung der Cybersicherheit in der gesamten Lieferkette und bei Partnern.

## Fazit

Die NIS-2 stellt einen bedeutenden Schritt zur Verbesserung der Cybersicherheit in Europa dar. **Unternehmen**, die in wesentlichen oder wichtigen Sektoren tätig sind, **sollten sich bereits jetzt auf die Umsetzung der Richtlinie vorbereiten**, um Risiken zu minimieren und ihre Geschäftsabläufe zukunftssicher zu gestalten.

Aus der Region.  
Für die Region.



### **Kontaktieren Sie uns**

Falls Sie Unterstützung bei der Umsetzung der NIS-2 benötigen oder Fragen zu den Anforderungen haben, zögern Sie nicht, uns zu kontaktieren. Wir bieten maßgeschneiderte Beratungs- und Unterstützungsdienste, um sicherzustellen, dass Ihr Unternehmen alle Vorschriften rechtzeitig und effizient erfüllt.



**Alles, was uns verbindet.**

---

#### **KEVAG Telekom GmbH**

Cusanusstraße 7  
56073 Koblenz

Telefon: +49 261 201 622-212  
E-Mail: [vertrieb-gk@kevag-telekom.de](mailto:vertrieb-gk@kevag-telekom.de)  
[www.kevag-telekom.de](http://www.kevag-telekom.de)