# CYBERsicher informiert:

## Die NIS-2-Richtlinie: Eine europaweite Maßnahme zur Steigerung des Gesamtniveaus der Cybersicherheit in der EU

### Was ist NIS-2?

NIS-2 ist eine neue Richtlinie für die Cybersicherheit von kritischen Infrastrukturen in der Europäischen Union. Sie setzt sich zum Ziel, dass innerhalb der EU alle Mitgliedsstaaten enger zusammenarbeiten und den gleichen Standard in der Cybersicherheit abbilden. Darüber hinaus wird ein einheitliches Meldesystem und Meldeverfahren von Sicherheitsvorfällen etabliert. Das Ziel ist die schnellere Reaktion und Einheitlichkeit im Vorgehen zur Behebung über Landesgrenzen hinaus.

Im deutschen Recht findet die Umsetzung über das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) statt. Mit dem 17. Oktober 2024 wird das Gesetz offiziell in Krafttreten und aktuell liegt hier der zweite Referentenentwurf zur weiteren Abstimmung vor.

### Was ist der Unterschied zur bisherigen Richtlinie?

Bisher gab es noch keine einheitliche EU-Richtlinie bzw. die bisherigen Richtlinien wurden sehr unterschiedlich umgesetzt. Dadurch ist das Cybersicherheitsniveau von Land zu Land sehr unterschiedlich. Die neue Richtlinie betrifft ca. 15 Mal so viele Unternehmen wie bisher und somit ca. 30.000 allein in Deutschland. (Quelle: https://www.openkritis.de/it-sicherheitsgesetz/index.html)

Bisher lag der Fokus vor allem auf der Reaktion bei Sicherheitsvorfällen. Zukünftig steht die Sensibilisierung der Mitarbeitenden in den Unternehmen im Mittelpunkt, um eventuelle Vorfälle schneller zu erkennen.



Gefördert durch: Bundesministerium für Wirtschaft und Klimaschutz aufgrund eines Beschlusses des Deutschen Bundestages

## Welche Unternehmen sind von der neuen Regelung betroffen?

### Kriterium 1: Größe

Zunächst unterscheidet der Gesetzgeber nach der Größe: Unternehmen, die Unternehmen mindestens 50 Mitarbeiterinnen und Mitarbeitern und einem Jahresumsatz von über 10 Mio. Euro können unter den Anwendungsbereich der NIS-2-Richtlinie fallen, wenn Kriterium 2 auch erfüllt ist.

### Kriterium 2: Sektor

Die Zuordnung erfolgt nach der Unterscheidung in wesentliche und wichtige Sektoren für das öffentliche Leben, wie Sie hier nachvollziehen können:

| Wesentliche Einrichtungen |
| --- |
| • Energie |
| • Verkehr |
| • Bankwesen |
| • Finanzmarktinfrastrukturen |
| • Gesundheitswesen |
| • Trinkwasser |
| • Abwasser |
| • Digitale Infrastruktur |
| • Verwaltung von IKT-Diensten (B2B) |
| • Öffentliche Verwaltung |
| • Weltraum |

| Wichtige Einrichtungen |
| --- |
| • Post- und Kurierdienste |
| • Abfallbewirtschaftung |
| • Produktion, Herstellung und Handel mit chemischen Stoffen |
| • Produktion, Verarbeitung und Vertrieb von Lebensmitteln |
| • Verarbeitendes Gewerbe/Herstellung von Waren |
| • Anbieter digitaler Dienste |
| • Forschung |

Für einzelne o.g. Sektoren gelten aktuell keine Größenbeschränkungen. Davon betroffen sind die digitalen Infrastrukturen (z.B. Rechenzentren, Online-Suchmaschinen, Marktplätze) und öffentliche Verwaltung.

**Achtung:**

1. Selbst wenn ihr Unternehmen unter die Grenze von 50 Mitarbeitenden fällt, jedoch einen Jahresumsatz größer als 10 Millionen erwirtschaftet, greift bei Ihnen die NIS-2-Richtlinie.

2. Sollten Sie indirekt für ein Unternehmen arbeiten, also bspw. Dienstleistungen für ein Großunternehmen verrichten, welches in den dargestellten Sektoren tätig ist, fällt ihr Unternehmen automatisch auch unter die NIS-2-Richtlinie.

3. Sie sind bereits als sogenanntes KRITIS-Unternehmen eingestuft? Dann fallen Sie höchstwahrscheinlich ebenfalls unter die NIS-2-Richtlinie.

**Was muss ich als Unternehmen tun?**

Der Gesetzgeber sieht vor, dass die Unternehmen selbstständig prüfen müssen, ob sie die Richtlinie erfüllen und sich ggf. melden müssen. Für jeden Sektor wurden spezifische Werte im Rahmen der KRITIS-Verordnung festgelegt und bieten eine erste Orientierung. Zum besseren Verständnis ein Beispiel aus dem Sektor Luftverkehr: Wenn ein Flughafen pro Jahr mehr als 20 Mio. Passagiere abfertigt, fällt dieser unter die Richtlinie.

Wenn Sie bereits nach den Normen ISO2700x arbeiten, oder sich am IT-Grundschutz nach dem Bundesamt für Sicherheit in der Informationstechnik (BSI) richten, sind sie bereits auf einen guten Weg und verfolgen den Allgefahrenansatz. Weitere Maßnahmen und Überlegungen im Vorfeld könnten die folgenden sein:

**Jetzt wissen Sie was tun ist, aber wie fangen Sie an?**

Die Transferstelle Cybersicherheit im Mittelstand steht Ihnen als zentrale Anlaufstelle für Cybersicherheit mit Rat und Tat zur Seite. Unsere Angebote orientieren sich an der Praxis, sind verständlich für Sie aufbereitet und stehen Ihnen kostenfrei zur Verfügung.

Durch unseren CYBERsicher Check können Sie sich in wenigen Minuten über die Bedarfe Ihres Unternehmens informieren. Des Weiteren steht Ihnen mit unserem CYBERdialog ein persönlicher Kontakt mit anschließenden konkreten Handlungsempfehlungen zur Verfügung.

Mehr Informationen finden Sie unter www.transferstelle-cybersicherheit.de!



Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages