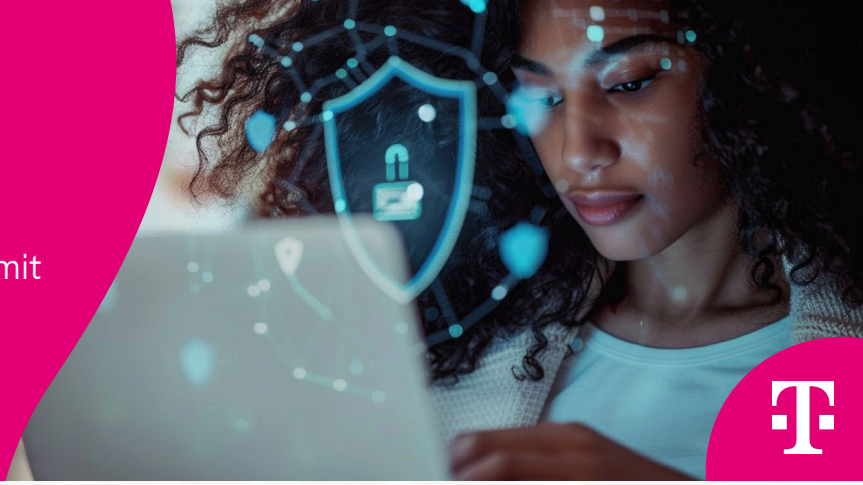
T Security

# NIS2-Richtlinie

Die Vorbereitung auf NIS2 beginnt mit Transparenz, Kontrolle und einem strukturierten Sicherheitsansatz.



## Was ist die NIS2-Richtlinie und wozu dient sie?

Die NIS2-Richtlinie ist der aktualisierte Cybersicherheitsrahmen der Europäischen Union mit dem Ziel, die Widerstandsfähigkeit kritischer Branchen und digitaler Dienste zu stärken. Sie erweitert den Geltungsbereich der ursprünglichen NIS-Richtlinie und führt strengere Anforderungen für Risikomanagement, Vorfallsmeldung, Governance und Lieferkettensicherheit ein. Für Organisationen in modernen, hybriden und Cloud-nativen Umgebungen macht NIS2 deutlich, dass Cybersicherheit nicht länger nur ein IT-Thema ist, sondern eine geschäftliche Priorität, mit Verantwortung auf operativer und Führungsebene.

## Wer ist von der NIS2-Richtlinie betroffen?

Ob und wie Unternehmen von der NIS2-Richtlinie betroffen sind, ist abhängig von ihrer **Unternehmensgröße** und dem **Tätigkeitsbereich.**

### Unternehmensgröße

- Mittelgroße Unternehmen mit mehr als 50 Mitarbeitenden und **über 10 Mio. € Jahresumsatz**
- Großunternehmen mit mehr als 250 Mitarbeitenden und **über 50 Mio. € Jahresumsatz**

### Tätigkeitsbereich

**Zu Sektoren mit hoher Kritikalität zählen Bereiche, in denen Störungen erhebliche gesellschaftliche oder wirtschaftliche Folgen hätten:**

Energie | Transport | Bankwesen | Finanzmarktinfrastrukturen | Gesundheitswesen | Trinkwasserversorgung | Abwasserwirtschaft | Digitale Infrastruktur | Verwaltung von IKT-Dienstleistungen | Öffentliche Verwaltung | Raumfahrt

**Weitere kritische Sektoren, die umfassendere Infrastrukturen und Betriebsabläufe unterstützen:**

Digitale Dienste | Produktion, Verarbeitung und Vertrieb von Lebensmitteln | Produktion, Verarbeitung und Vertrieb chemischer Erzeugnisse | Fertigung / Herstellung von Gütern | Abfallwirtschaft | Post- und Kurierdienste | Forschungseinrichtungen

Organisationen, die nicht direkt unter die Klassifizierung fallen, können dennoch durch Anforderungen innerhalb der Lieferkette betroffen sein, da regulierte Unternehmen zunehmend von ihren Partnern NIS2-konforme Sicherheitsstandards verlangen.

## Warum jetzt handeln

NIS2 steht für einen Wandel von grundlegender Compliance hin zu geschäftskritischem Risikomanagement. Unternehmen müssen hybride Umgebungen absichern, Risiken durch Dritte steuern und auf Vorfälle innerhalb strenger Fristen reagieren. Eine fehlende Anpassung beeinträchtigt nicht nur die Compliance, sondern auch Betriebsabläufe, Partnerschaften und das Vertrauen am Markt.

## Wie die Einhaltung sichergestellt wird

NIS2 führt strengere Aufsicht und Durchsetzung in den EU-Mitgliedstaaten ein. Behörden können Audits durchführen, Sicherheitsdokumentationen anfordern und die Reaktionsfähigkeit auf Vorfälle bewerten. Korrekturmaßnahmen können angeordnet werden. Der Aufsichtsprozess unterscheidet sich nach Organisationstyp.

**Wesentliche Einrichtungen:** Große Organisationen mit Tätigkeit in einem Sektor hoher Kritikalität

**Wichtige Einrichtungen:** Große und mittelgroße Organisationen in anderen kritischen Sektoren

Wesentliche Einrichtungen unterliegen proaktiver Aufsicht, während wichtige Einrichtungen meist nach Vorfällen oder identifizierten Risiken überprüft werden.

### Sanktionen und geschäftliche Auswirkungen

- Wesentliche Einrichtungen müssen mit Geldbußen von **über 10 Mio. € oder 2 % des weltweiten Jahresumsatzes** rechnen
- Wichtige Einrichtungen müssen mit Geldbußen von **über 7 Mio. € oder 1,4 % des weltweiten Jahresumsatzes** rechnen

Über Geldbußen hinaus drohen Betriebsunterbrechungen, Vertragsverluste und Reputationsschäden.

## Ein praxisnaher Ansatz zur NIS2-Readiness

Die Erfüllung der NIS2-Anforderungen erfordert einen strukturierten und schrittweisen Ansatz, abgestimmt auf die bestehende Umgebung.

Organisationen sollten zunächst ihren aktuellen Reifegrad bewerten, Lücken identifizieren und risikoreiche Bereiche wie Identitäten, Zugriffe und Incident Response priorisieren. Anschließend sollten Sicherheitsmaßnahmen über Systeme und Nutzer hinweg gestärkt, kontinuierliches Monitoring etabliert sowie klare Governance- und Verantwortungsstrukturen geschaffen werden.

## Vorteile für die Branchen

**Risk Management**
Definition von Sicherheitsrichtlinien und Risikobewertung

**Incident Reporting**
Kontinuierliches Monitoring und Reporting

**Business Continuity**
Backup- und Wiederherstellungsprozesse sowie Krisenmanagement

**Supply Chain Security**
Risikomanagement für Anbieter, Partner und externe Dienstleistungen

**Identity and Access Control**
Sichere Authentifizierung und konsequente Zugriffskontrollen

**Vulnerability Management**
Kontinuierliche Identifikation, Behebung und Verwaltung von Systemschwachstellen

## Wo Unternehmen an ihre Grenzen stoßen

Viele Unternehmen stehen bei der Umsetzung der NIS2-Anforderungen vor ähnlichen Herausforderungen:

- Begrenzte Transparenz über hybride IT-Umgebungen hinweg
- Unklare oder verzögerte Prozesse zur Reaktion auf Sicherheitsvorfälle
- Unzureichende Konzepte für Identity and Access Control
- Begrenzte Kontrolle über Risiken durch Drittanbieter und Lieferketten

Diese Schwachstellen erhöhen sowohl Compliance-Risiken als auch die Anfälligkeit für betriebliche Störungen.

## T Security unterstützt Sie auf Ihrem Weg zur NIS2 Readiness

**NIS2-Readiness Assessment**
Identifizieren Sie Schwachstellen, Risiken und Compliance-Prioritäten in Ihrer gesamten IT-Umgebung

**Sichere Infrastruktur und Cloud**
Aufbau und Betrieb sicherer IT-Umgebungen gemäß europäischen Vorgaben

**Identity and Access Management**
Sichere Zugriffe durch Zero Trust gewährleisten

**Threat Detection and Response**
Kontinuierliches Monitoring, Detection und Incident Response sicherstellen

**Compliance & Audit Support**
Reporting, Governance und Audit Readiness effizient gestalten

**Resilienzplanung**
Klare Prozesse für Reporting und Recovery im Einklang mit den NIS2-Anforderungen etablieren

**Unsere Expert:innen beraten Sie gerne**
*cyber.security@t-systems.com*

**Herausgeber**
Deutsche Telekom AG
Friedrich-Ebert-Allee 140
53113 Bonn, Germany
security.telekom.de
t-systems.com