NIS2

Die neue Ära der Cybersicherheit

NIS2 ist da!

Seit dem 6. Dezember 2025 gelten die Anforderungen des neuen BSIG.

Die Anforderungen des BSIG (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik) müssen ohne Übergangsfristen umgesetzt werden. Betroffene Unternehmen müssen sich innerhalb von **drei Monaten nach Inkrafttreten**, also bis spätestens **März 2026**, beim **BSI registrieren**, Meldungen machen und Vorgaben wie Risikomanagement erfüllen.

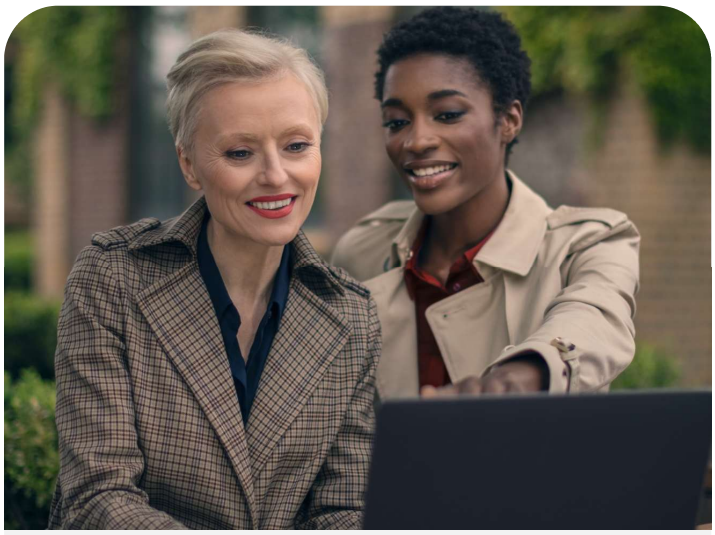
Was ist NIS2?

Die EU-Richtlinie NIS2 **(N**etwork & **I**nformation **S**ecurity) **regelt die Sicherheit von Netzen und Informationstechnologien** in der EU. NIS2 ist eine Weiterentwicklung der NIS-Richtlinie von 2016, sowohl inhaltlich als auch in Bezug auf die erheblich wachsende Anzahl der betroffenen Unternehmen und Institutionen. NIS2 muss **von jedem EU-Mitglied in nationales Gesetz übertragen werden,** wodurch auch kleine, nationale Unterschiede entstehen werden.

In Deutschland ist dies mit dem **NIS2UmsuCG** (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz) geschehen, welches u. a. das BSI-Gesetz ändert.

Schützen Sie Ihr Unternehmen vor Cyber-Angriffen

Seit Jahren nehmen Cyber-Angriffe und der Schaden durch sie zu. Die Europäische Union schuf deshalb mit der **EU-Richtlinie NIS2** einen Mindeststandard für **höhere Cybersicherheit** in der gesamten EU. NIS2 bedeutet **neue und strengere Vorschriften.** In Deutschland werden ca. **29.500 – 30.000 Organisationen** aus Wirtschaft und Staat **betroffen sein.**



Wer ist betroffen?

Die Richtlinie NIS2 betrifft nun nicht mehr nur große, kritische Infrastrukturen, sondern geht weit darüber hinaus. Sie umspannt nach der **Erweiterung** verschiedene neue **Wirtschaftssektoren,** so z. B. auch den kleinen Chemie-Produzenten mit 150 Mitarbeitenden und 20 Mio. € Jahresumsatz.

Darüber hinaus müssen Lieferketten abgesichert werden, z. B. muss der Energiesektor ebenfalls prüfen, ob wichtige Zulieferer, wie die Hersteller von Turbinen, abgesichert sind.

Stand 12/2025

NIS2

Relevante Branchen im Überblick

Die folgende Übersicht zeigt die Wirtschaftssektoren, für die die NIS2-Richtlinie konkrete Cybersicherheitsanforderungen definiert.

- Anbieter digitaler Dienste
- Abfallbewirtschaftung
- Bank-/ Finanzwesen (Dienstleistungen)
- Chemie
- Energie
- Digitale Infrastruktur
- Finanzmarktinfrastruktur
- Forschung (kommerziell)
- Gesundheit
- Industrie (verarbeitendes Gewerbe)
- Lebensmittel
- Post- & Kurierdienste
- Produktion
- Transport & Verkehr
- Wasserversorgung & Abwasser
- Weltraum

Sonderfälle
Bundeseinrichtungen (ausgenommen BMVg; AA; BND, BfV & Bundesländer); ebenfalls besonders wichtig: qTSP, TLD, DNS, TK-Anbieter ab mittlerer Größe aber <100k Teilnehmer. Weitere Infos

Neben der **„Branche“** wird als zweites Kriterium die Unternehmensgröße herangezogen. Dabei wird zwischen **„besonders wichtigen Einrichtungen“** und **„wichtigen Einrichtungen“** unterschieden. Der Hauptunterschied besteht darin, dass für **„wichtige Einrichtungen“** geringere Geldstrafen vorgesehen sind und die Behörde etwas weniger Durchgriffsmöglichkeiten hat. Bzgl. der behördlichen Möglichkeiten ist zu erwähnen, dass neben den hohen Bußgeldern eine explizite Haftung der Geschäftsführung vorgesehen ist.

Welche Größe hat Ihr Unternehmen? Welche Bußgelder drohen?

Unternehmen	Mitarbeitende		Umsatz / Bilanzsumme	Bußgelder
Mittelgroß (wichtige)	ab 50	oder	>10 Mio. € /> 10 Mio.	Bis 7 Mio. € oder 1,4 % weltweiter Jahresumsatz*
Groß (besonders wichtige)	ab 250	oder	> 50 Mio. € />43 Mio.	Bis 10 Mio. € oder 2 % weltweiter Jahresumsatz*

+ **KRITIS-Unternehmen** mit kritischen Anlagen sind ebenfalls **besonders wichtige Unternehmen** und werden derzeit bereits in der KRITIS-Verordnung reguliert. Weitere Infos

Stand 12/2025

Was sind die Anforderungen von NIS2?

Unternehmen und Organisationen müssen sich im Rahmen von NIS2 neben organisatorischen und rechtlichen Maßnahmen mit technischen Anforderungen auseinandersetzen. Hierzu zählen:

- **konzeptionelle Themen,** wie z. B. Inhalte eines Information Security Management Systems (ISMS)
- **praktische Details**, wie der Umgang mit konkreten Sicherheitsvorfällen oder der Test der eigenen Security Maßnahmen, u. a. durch Pen-Test und Schwachstellen-Management.
- **Weitere wichtige Punkte** sind Backup-Maßnahmen, Cybersecurity-Trainings für Mitarbeitende oder die Absicherung von Zugriffsrechten z. B. durch Multi-Faktor-Authentifizierung.

Der Gesetzgeber gibt dabei eine **Registrierungs-pflicht** vor, nach der sich Unternehmen, die in den Geltungsbereich des Gesetzes fallen, **selbstständig** als „**wichtige**“ oder „**besonders wichtige**“ **Einrichtung** beim **BSI registrieren** müssen.

Geforderte Cybersicherheitsmaßnahmen (§30 BSIG)

- Risikoanalyse & -management
- Bewältigung von Sicherheitsvorfällen (Incident Management)
- Business Continuity (u. a. Backup-Management, Wiederherstellung) & Krisenmanagement
- Sicherheit in der Lieferkette
- Sicherheit in der Lieferkette
- Sichere Entwicklung, Beschaffung & Wartung von IT
- Wirksamkeitsprüfungen der Risiko- & IT-Sicherheitsmaßnahmen
- Cyber-Hygiene & Schulungen
- Kryptographie & Verschlüsselung
- Sicherheit des Personals & Zugriffskontrolle
- MFA oder kontinuierliche Authentifizierung sowie gesicherte Kommunikationskanäle

Höhere Maßstäbe für KRITIS-Unternehmen (§31 BSIG)

Strenge Meldepflichten

- Bis 24 Stunden: initiale Erstmeldung Vorfall
- Bis 72 Stunden: Folgemeldung mit Bewertungsdetails
- Bis einen Monat nach Abschluss des Vorfalls: Abschlussbericht

Wie setzten Sie NIS2 um?

Erreichen Sie NIS2-Compliance – mit Vodafone Business.

Unsere **Cyber-Security-Expert:innen** unterstützen Sie vom **ersten Kickoff-Workshop** an. Zusammen mit Ihnen setzen wir Ihre NIS2-Lösungen um – bis hin zum Regelbetrieb. Sie erarbeiten mit uns Ihre **GAP-Analyse**. Zusammen mit Ihnen erstellen wir Ihre **persönliche NIS2-Roadmap**. Dazu gehört die Einführung eines für Sie passenden Managementsystems für Informationssicherheit (ISMS) – sofern sie noch keins haben.

Sichern Sie Ihre Organisation mit unseren Cyber-Security-Produkten und Security Services NIS2-konform ab.

Sprechen Sie uns an. Wir helfen Ihnen gerne.

Stand 12/2025