NIS2
Die neue Ära der Cyber-Sicherheit

Was ist NIS2?

Die EU-Richtlinie NIS2 **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 wird dies mit dem **NIS2UmsuCG** (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes) geschehen, welches u.a. das BSI- (Bundesamt für Sicherheit und Informationstechnik) Gesetz ändert.

Schützen Sie Ihr Unternehmen vor Cyber-Angriffen

Seit Jahren nehmen Cyber-Angriffe und der Schaden hierdurch zu. Die Europäische Union schuf deshalb mit der **EU-Richtlinie NIS2 (N**etwork & **I**nformation **S**ecurity) einen Mindeststand für **höhere Cyber-Sicherheit** in der gesamten EU. NIS2 bedeutet **neue und strengere Vorschriften** für etwa **160.000 Unternehmen und Institutionen in Europa.**

2016: NIS1

Ziel: hohe Cyber-Sicherheit für große Organisationen der kritischen Infrastruktur

2022: NIS2

Ziel: EU-weite und höhere Mindeststandards für IT- und Cyber-Sicherheit auf breiter Basis

2021: BSI-Gesetz (BSIG)

durch IT-Sicherheitsgesetz 2.0, KRITIS-V

Etwa 1.800 KRITIS Unternehmen

2024: BSIG neue Fassung

durch NIS-2-Umsetzungs- und Cybersicherheits-Stärkungsgesetz

Etwa 30.000 betroffene Institutionen

Wann kommt NIS2?

Ab 18. Oktober 2024 müssen Sie NIS2 anwenden

NIS soll laut EU-Vorgabe ab dem **18. Oktober 2024** in den **Mitgliedsstaaten im nationalen Gesetz umgesetzt** werden.
Deutschland befindet sich aktuell mitten im Gesetzgebungsverfahren. Am 24.07.2024 wurde der Regierungsentwurf durch das Bundeskabinett verabschiedet, womit der Bundesrat dem Gesetz final zustimmen kann.

Zeitplan der EU-Richtlinie NIS2*

Ende 2022
EU-Direktive NIS2 (EU 2022/2555) beschlossen

Oktober 2024
EU-Vorgabe: bis 17. Oktober Überführung ins deutsche Recht

Ab Inkrafttreten
Umsetzung muss sofort erfolgen

Oktober 2027
Kontrollen zur Umsetzung starten

* Die finale Verabschiedung des deutschen Umsetzungsgesetzes verzögert sich wahrscheinlich um wenige Monate.
Mit der Veröffentlichung des Gesetzes beginnt dann sofort die Umsetzungsfrist und nach 3 Jahren die Dokumentationspflicht.

Stand 08/2024

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 oder den Hersteller von Autositzen mit 65 Mitarbeitenden und 15 Mio. € Jahresumsatz.

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

Folgende Branchen sind vom Geltungsbereich der NIS2 Richtlinie betroffen

- 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

Medien; Staat & Verwaltung Öffentliche Verwaltung (nur Zentralregierung); ebenfalls besonders wichtig: qTSP, TLD, DNS, TK-Anbieter < 100k Teilnehmer

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 möglichen, hohen Bußgeldern eine explizite Haftung der Geschäftsführung vorgesehen und in gravierenden Fällen sogar ein temporäres Absetzen der Geschäftsleitung möglich ist.

Welche Größe hat Ihr Unternehmen? Welche Bußgelder drohen?

Unternehmen	Mitarbeitende		Umsatz / Bilanzsumme	Bußgelder
Mittelgroß (wichtige)	50 - 249	**oder**	>10 Mio. € / > 10 Mio.	Bis 7 Mio. € oder 1,4% weltweiter Jahresumsatz*
Groß (besonders wichtige)	≥250	**oder**	> 50 Mio. € / >43 Mio.	Bis 10 Mio. € oder 2% weltweiter Jahresumsatz*

+ **Betreiber kritischer Anlagen** und Auswirkung auf öffentliche Ordnung, Systemrisiken oder grenzüberschreitenden Auswirkungen. Schon im UP KRITIS umgesetzt.

*Mögliche Sanktionen für Unternehmen mit einem Jahresumsatz >500 Mio. €.

Stand 08/2024

Was sind die Anforderungen von NIS2?

Unternehmen und Organisationen müssen sich im Rahmen von NIS2 sowohl mit **konzeptionellen Themen** wie z.B. den Inhalten eines Information Security Management System (ISMS) auseinandersetzen, als auch mit **praktischen Details** wie dem Umgang von konkreten Sicherheitsvorfällen oder dem Test der eigenen Security Maßnahmen, u.a. durch Pen-Test und Schwachstellen-Management. Weitere wichtige Punkte sind Back-Up Maßnahmen, Cyber Security Trainings für Mitarbeitende oder die Absicherung von Zugriffsrechten z.B. durch Multi-Faktor-Authentifizierung.

Der Gesetzgeber gibt dabei eine **Registrierungspflicht** vor, nach der sich Unternehmen, die in den Geltungsbereich des Gesetzes fallen, **selbstständig** als „**wichtige“** oder „**besonders wichtige**“ **Einrichtung** bei einer behördlichen Zentralstelle registrieren müssen.

Darüber hinaus werden alle Unternehmen dazu verpflichtet, nach einem **3-stufen Modell** ihre **erheblichen Sicherheitsvorfälle** an eine **behördliche Stelle** zu melden und dabei detailliert dazustellen, was passiert ist und wie dieser Vorfall im Detail zu bewerten ist sowie welche Abwehrmaßnahmen unternommen worden.

Geforderte Cybersicherheitsmaßnahmen (§30 BSIG)

- Risikoanalyse & -management
- Bewältigung von Sicherheitsvorfällen (Incident Management)
- Business Continuity (u.a. Back-Up Management, Wiederherstellung) & Krisenmanagement
- 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

Strenge Meldepflichten

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

Wie bereiten Sie Ihr Unternehmen vor?

Erreichen Sie NIS2-Compliance – mit Vodafone Business.

Unsere **Cyber Security-Expert:inn**en 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 Managed Services NIS2-konform ab.

Sprechen Sie uns an. Wir helfen Ihnen gerne.

Stand 08/2024