grosse-hornke

NIS-2 RUFT

JETZT FITNESS AUFBAUEN FÜR DIE NEUE EU-RICHTLINIE

- Finden und **beheben Sie Schwachstellen** im IT-Risikomanagement
- Wappnen Sie Ihr Unternehmen gegen **neue Bedrohungen**
- Sichern Sie sich ab gegen **persönliche Haftung** und Strafen in Höhe von **Millionen Euro**

Neuland für tausende Firmen

EU erweitert ihre Regeln zur Cybersicherheit

Unsere Wirtschaft ist verwundbar

Cyberattacken können die Volkswirtschaft schwer treffen, wenn systemrelevante Sektoren ihre Aufgaben nicht mehr erfüllen.

NIS-1 regelt Cyberschutz in der EU

Seit 2018 verpflichtet die EU ausgewählte Branchen dazu, ihre digitale Infrastruktur zu schützen: mit der Richtlinie zur Netzwerk- und Informationssicherheit, kurz NIS-1.

NIS-2: mehr Unternehmen betroffen

Aus EU-Sicht ließ NIS-1 zu viel Raum zur Interpretation. NIS-2 legt die Sektoren präziser fest und schließt auch mittlere Unternehmen ein. Damit nimmt die EU zehntausende weitere Firmen in die Pflicht.

Strengere Vorgaben

Auch Unternehmen, die NIS-1 bereits erfüllen, müssen mehr tun: NIS-2 sieht zum Beispiel vor, das Firmen kritische Vorfälle umgehend melden und Berichte dazu vorlegen.

Schmerzhafte Strafen

Bei einem Verstoß kann der Staat verantwortliche Führungskräfte persönlich haftbar machen. Es drohen Geldbußen von 7 Millionen Euro oder mehr.

Ist Ihr Unternehmen betroffen?

NIS-2 gilt für 2 Kategorien systemrelevanter Branchen

Sektoren mit hoher Kritikalität	Sonstige kritische Sektoren
Energie	Post- und Kurierdienste
Verkehr	Abfallbewirtschaftung
Banken	Chemie (Produktion, Herstellung & Handel)
Finanzmarktinfrastruktur	Verarbeitendes Gewerbe & Herstellung von Waren (Medizinprodukte, EDV-Erzeugnisse, elektrische Ausrüstung, Maschinenbau, Fahrzeugbau)
Gesundheitswesen	Anbieter digitaler Dienste
Trinkwasser	Forschung
Abwasser	
Digitale Infrastruktur	
IKT-Dienste-Verwaltung	
Öffentliche Verwaltung	
Weltraum	

Ist die Firmengröße relevant?

Das kommt darauf an. NIS-2 unterscheidet wichtige und wesentliche Einrichtungen.

Größere Unternehmen mit hoher Kritikalität gelten als wesentlich und müssen im Allgemeinen strengere Regeln befolgen.

	Mittlere Unternehmen > 10 Beschäftigte + > 10 Mio. € Bilanzsumme / Umsatz	**Größere Unternehmen** > 250 Beschäftigte + > 50 Mio. € Bilanzsumme / 43 Mio. € Umsatz
Sektoren mit hoher Kritikalität	**Wichtige Einrichtung**	**Wesentliche Einrichtung** im Dt. auch „sehr wichtige Einrichtung“
Sonstige kritische Sektoren	**Wichtige Einrichtung**	**Wichtige Einrichtung**

Ist Ihre Firma ein Sonder- oder Grenzfall?

Wenn Ihr Unternehmen überragend wichtige Leistungen erbringt, kann eine Sonderregel greifen – unabhängig von der Firmengröße.

Sonderregeln sind auch dann zu beachten, wenn Ihr Unternehmen temporär wächst oder schrumpft.

Risikomanagement: 3 Ebenen

Die EU nimmt das Top-Management in die Verantwortung und setzt einheitliche Standards in allen Mitgliedstaaten für:

Governance

Die Unternehmensführung muss Maßnahmen für die Cybersicherheit in die Hand nehmen, prüfen und überwachen. Bei Verstößen haften Verantwortliche persönlich. Mitarbeitende aller Ebenen sind zum Thema Cybersicherheit zu schulen.

Operatives Risikomanagement

NIS-2 fordert von Unternehmen robuste Pläne und Systeme, unter anderem um …

- Vorfälle zu bewältigen
- den Betrieb aufrechtzuerhalten
- Lieferketten abzusichern
- sensible Daten zu verschlüsseln
- Zugriffe auf Systeme zu kontrollieren
- sicher zu kommunizieren

Meldepflicht

Unternehmen müssen die zuständige Behörde innerhalb von 24 Stunden über erhebliche Vorfälle informieren. Innerhalb von 3 Tagen muss eine Bewertung vorliegen, nach einem Monat eine Abschlussmeldung.

Empfindliche Strafen

Aufsichtsbehörden werden Unternehmen in Zukunft stichprobenartig kontrollieren, etwa durch:

- Abfrage des Cybersicherheits-Konzepts
- Abfrage von Nachweisen über Security-Checks
- Inspektionen vor Ort

Bei Verstößen drohen teils erhebliche Strafen. Sie schaden dem Ruf und können sogar die Existenz bedrohen:

Warnungen und verbindliche Anweisungen

Veröffentlichung von Verstößen

Hohe Geldbußen
7 / 10* Mio. € oder mehr (1,4 % – 2 %* vom Jahresumsatz)

Entzug von Zulassungen*

Führungsverbot für Verantwortliche*

*Nur wesentliche Einrichtungen

Enger Zeitplan

NIS-1	NIS-2
	EU-Beschluss 14.12.2022
Gültig	**Umsetzung in nationale Gesetzgebung** bis 17.10.2024
Ungültig 18.10.2024	**Gültig** 18.10.2024

Was gilt in Deutschland?

Der deutsche Gesetzgeber überträgt NIS-2 bis 17. Oktober 2024 in nationales Recht:

1. **NIS-2-Umsetzungs- und Cybersicherheitsstärkungs-gesetz** (NIS2UmsuCG)
2. **KRITIS-Dachgesetz** mit ergänzenden Regelungen zum Schutz sensibler Infrastrukturen

Aufsicht:
Bundesamt für Sicherheit in der Informationstechnik (BSI).

Starten Sie frühzeitig, um NIS-2 sicher zu erfüllen

Jetzt zu handeln lohnt sich

Nutzen Sie NIS-2 als Chance. Denn Cybersecurity ist mehr als eine Pflicht. Sie ist ein strategischer Vorteil:

Wappnen Sie sich gegen KI-Angriffe

Künstliche Intelligenz macht u. a. Phishing-Mails noch glaubwürdiger und stößt laut Gartner das Einfallstor für Cyberkriminelle weiter auf.

Vermeiden Sie teure Ausfälle

Incident-Management und Business-Continuity-Pläne helfen Ihnen, Vorfälle schnell einzudämmen und Ihr Geschäft am Laufen zu halten.

Machen Sie Ihre IT produktiver

Sichere Prozesse wie z. B. ein Identity and Access Management (IAM) reduzieren zugleich interne Bürokratie und Supportanfragen.

Halten Sie im Wettbewerb mit

Laut einer IBM-Studie verursacht ein Datenleck im Schnitt über 4,3 Millionen US-Dollar Schaden. Viele betroffene Unternehmen geben die Kosten an ihre Kunden weiter. Sichern Sie Ihre Daten ab und vermeiden Sie Wettbewerbsnachteile.

Schützen Sie Ihre Reputation

Überlassen Sie Cyber-Vorfälle der Konkurrenz und verschaffen Sie sich einen Vertrauensvorsprung bei Kunden und Partnern.

Die sicherste Route finden

Von der Gap-Analyse zum Aktionsplan

Erfassen relevanter Bereiche, Planung

- Welche Organisationseinheiten müssen mitwirken?
- Welche Arbeitspakete sind zu erledigen?
- Wer sind die Stakeholder des Projekts?

Interviews mit Stakeholdern

- Wie sehen aktuelle Prozesse des IT-Risikomanagements aus?
- Welche IT-Projekte sind zu berücksichtigen?
- Bestehen Ressourcenkonflikte?

Analyse vorhandener Dokumente

- Sind Prozesse des IT-Risikomanagements NIS-2-konform dokumentiert?
- Müssen wir interne Leitlinien überarbeiten?

Abstimmung Gap-Analyse-Resultate

- Welche Anmerkungen haben die Verantwortlichen für IT und weiterer relevanter Fachbereiche?
- Gibt die Unternehmensführung grünes Licht für die Umsetzung?

Priorisieren der Maßnahmen

- Welche Arbeiten haben Vorrang mit Blick auf Relevanz, Umfang und Verfügbarkeit von Ressourcen?

Ihre Roadmap

- Detaillierter Projekt- und Zeitplan
- Inklusive Vorlaufzeiten, so dass Ihr Unternehmen alle Vorgaben pünktlich umsetzt

Guide gesucht?

Wir bringen Sie sicher ans Ziel

Sturmerprobtes IT-Projekt-Management für Konzerne und große Mittelständler

Erfahren in Regulatorik-Projekten und IT-Security-Themen kritischer Branchen

Wachsames Auge für Risiken und Ihr Budget

Stark im Change-Management bei komplexen Fachthemen

NIS-2 angehen: Fragen dazu?

Kontaktieren Sie uns gerne unverbindlich:

Silke Grosse-Hornke

+49 (0)2501 59435-10
silke.grosse@grosse-hornke.de

www.grosse-hornke.de

Herausgeber

grosse-hornke
Am Dornbusch 54
48163 Münster

Die Inhalte dieser Broschüre sind dazu gedacht, Unternehmen für das Thema NIS-2 zu sensibilisieren und erste Orientierung zu geben. Sie ersetzen nicht die detaillierte Auseinandersetzung mit den (künftigen) Regelungen und stellen keine juristische Beratung dar.