NIS2 – Was bedeutet das für Ihr Unternehmen?

Eine verständliche Einordnung für mittelständische Betriebe

1. Einleitung

Mit der **NIS2-Richtlinie** (Network and Information Security Directive) hat die Europäische Union einen neuen Rahmen geschaffen, um die **IT-Sicherheit von Unternehmen** zu stärken.

Hintergrund sind die stark zunehmenden Cyberangriffe auf Unternehmen, Lieferketten und kritische Infrastrukturen.

Ziel von NIS2 ist **nicht**, Unternehmen mit Bürokratie zu überfordern, sondern die **Widerstandsfähigkeit gegen IT-Ausfälle und Sicherheitsvorfälle** zu erhöhen.

Diese Information soll eine **sachliche und verständliche Einordnung** geben:

- Wer ist betroffen?
- Was wird gefordert?
- Was bedeutet das konkret für Unternehmen?

2. Ab wann gilt NIS2?

NIS2 ist eine **EU-Richtlinie**.

Sie wird von den Mitgliedsstaaten in nationales Recht umgesetzt.

Für Deutschland bedeutet das:

- Die gesetzlichen Regelungen treten **schrittweise** in Kraft
- Unternehmen sind **nicht über Nacht vollständig umsetzungspflichtig**
- Der Fokus liegt zunächst auf **Vorbereitung, Struktur und Nachweisbarkeit**

Entscheidend ist:

Unternehmen sollen zeigen können, dass sie sich **systematisch mit IT-Sicherheit befassen**.

xeko GmbH
Marienthaler Str. 17
24340 Eckernförde
Amtsgericht Kiel HRB 14603 KI
Geschäftsführer Helge Haude

Kontakt
Telefon 04351 - 8 90 90 20
Telefax 04351 - 8 90 90 21
E-Mail: team@xeko.de
URL www.xeko.de

Bankverbindung
Commerzbank Eckernförde
IBAN: DE 56 2104 2076 0837 7566 00
BIC: COBADEFFXXX
USt-IdNr. DE287620113/St.-Nr.15/294/06949

3. Wer ist von NIS2 betroffen?

NIS2 richtet sich vor allem an **mittelständische Unternehmen**, die:

- **mindestens 50 Mitarbeiter** beschäftigen **oder**
- einen **Jahresumsatz von über 10 Mio. €** erzielen

und

- in bestimmten Wirtschaftssektoren tätig sind

Dazu zählen unter anderem:

- Groß- und Fachgroßhandel
- Logistik und Warenverteilung
- Lebensmittel- und Getränkeversorgung
- Industrie und Produktion
- Energie, Wasser, Versorgung
- Gesundheitswesen
- IT-Dienstleistungen

Viele klassische Mittelstandsunternehmen fallen damit **erstmals** unter eine gesetzliche IT-Sicherheitsregelung.

---

4. Kategorien innerhalb von NIS2

NIS2 unterscheidet zwei Gruppen:

- **Wesentliche Einrichtungen**
- **Wichtige Einrichtungen**

Der Unterschied liegt vor allem in:

- Umfang der Anforderungen
- Höhe möglicher Sanktionen

Wichtig:

Unternehmen außerhalb der klassischen „kritischen Infrastruktur“ unterliegen **vereinfachten Anforderungen**.
Es besteht **keine Pflicht** zu ISO-Zertifizierungen oder externen Audits, sofern die Anforderungen nachvollziehbar erfüllt werden.

---

xeko GmbH
Marienthaler Str. 17
24340 Eckernförde
Amtsgericht Kiel HRB 14603 KI
Geschäftsführer Helge Haude

Kontakt
Telefon 04351 - 8 90 90 20
Telefax 04351 - 8 90 90 21
E-Mail: team@xeko.de
URL www.xeko.de

Bankverbindung
Commerzbank Eckernförde
IBAN: DE 56 2104 2076 0837 7566 00
BIC: COBADEFFXXX
USt-IdNr. DE287620113/St.-Nr.15/294/06949

5. Was fordert NIS2 konkret?

NIS2 verlangt **keine perfekten Systeme**, sondern **strukturierte Maßnahmen** in sieben Kernbereichen:

1. Verantwortlichkeiten

- IT-Sicherheit ist **Chefsache**
- Zuständigkeiten müssen klar benannt sein
- IT darf nicht isoliert handeln

---

2. Risikobewertung

- Welche IT-Systeme sind kritisch?
- Welche Auswirkungen hätte ein Ausfall?
- Welche Risiken bestehen realistisch?

Eine **überschaubare, praxisnahe Betrachtung** ist ausreichend.

---

3. Technische Schutzmaßnahmen

Beispiele:

- Firewall- und Netzwerkschutz
- Aktuelle Systeme & Patch-Management
- Benutzer- und Rechtekonzepte
- Viren- und Schadsoftware-Schutz

---

4. Backup & Wiederanlauf

- Regelmäßige Datensicherungen
- Getestete Wiederherstellung
- Klarer Plan für den Ernstfall

---

5. Umgang mit Sicherheitsvorfällen

- Definition, was ein relevanter Vorfall ist
- Interne Meldewege
- Unterstützung bei Bewertung und Reaktion

Nicht jeder IT-Fehler ist meldepflichtig.

---

xeko GmbH
Marienthaler Str. 17
24340 Eckernförde
Amtsgericht Kiel HRB 14603 KI
Geschäftsführer Helge Haude

Kontakt
Telefon 04351 - 8 90 90 20
Telefax 04351 - 8 90 90 21
E-Mail: team@xeko.de
URL www.xeko.de

Bankverbindung
Commerzbank Eckernförde
IBAN: DE 56 2104 2076 0837 7566 00
BIC: COBADEFFXXX
USt-IdNr. DE287620113/St.-Nr.15/294/06949

6. Lieferketten & Dienstleister

- IT-Dienstleister gelten als Teil der Sicherheitskette
- Verträge, Zuständigkeiten und Sicherheitsstandards müssen nachvollziehbar sein

---

7. Sensibilisierung der Mitarbeiter

- Grundverständnis für IT-Sicherheit
- Phishing, Passwörter, E-Mails
- Praktische Verhaltensregeln

Kurze Schulungen sind ausreichend.

---

8. Was NIS2 nicht verlangt

- Keine sofortige Vollumsetzung
- Keine ISO-Zertifizierungspflicht
- Keine lückenlose Überwachung
- Keine vollständige Auslagerung an externe Berater

Der Ansatz ist:

Angemessen, verhältnismäßig und nachvollziehbar

---

9. Fazit

NIS2 ist kein Grund zur Panik.

Viele Unternehmen erfüllen bereits heute einen Großteil der Anforderungen – oft ohne es bewusst zu dokumentieren.

Der Schlüssel liegt in:

- Klaren Zuständigkeiten
- Strukturierter Vorgehensweise
- Realistischen Maßnahmen
- Verständlicher Dokumentation

IT-Sicherheit wird damit **kein Sonderthema**, sondern ein **normaler Bestandteil der Unternehmensführung**.

Falls Sie Fragen haben oder Unterstützung benötigen, sprechen sie uns bitte an!

xeko GmbH
Marienthaler Str. 17
24340 Eckernförde
Amtsgericht Kiel HRB 14603 KI
Geschäftsführer Helge Haude

Kontakt
Telefon 04351 - 8 90 90 20
Telefax 04351 - 8 90 90 21
E-Mail: team@xeko.de
URL www.xeko.de

Bankverbindung
Commerzbank Eckernförde
IBAN: DE 56 2104 2076 0837 7566 00
BIC: COBADEFFXXX
USt-IdNr. DE287620113/St.-Nr.15/294/06949