ℹ️ Du kannst dir ganz einfach eine Kopie dieser Checkliste zur weiteren Verwendung erstellen. Klicke dazu oben links auf **Datei** und wähle dann **Kopie erstellen**.

Checkliste, Hintergrundwissen & Umsetzungsratgeber für Entscheider

NIS2-Starter-Guide für KMU

Warum NIS2 auch dich betrifft

Auch wenn dein Unternehmen nicht direkt unter die NIS2-Richtlinie fällt, kann sie dich trotzdem betreffen. Viele deiner Kunden – insbesondere größere Organisationen oder solche aus kritischen Infrastrukturen – müssen ihre gesamte Lieferkette absichern. Das bedeutet: Sie erwarten von dir als Dienstleister oder Zulieferer klare, nachweisbare IT-Sicherheitsmaßnahmen.

> *Fazit: Ohne ein dokumentiertes Mindestniveau an Cybersecurity könnte dein Unternehmen als Lieferant in Zukunft nicht mehr infrage kommen – auch wenn du selbst keine NIS2-Pflichten hast.*

Ein weiterer wichtiger Punkt: Durch NIS2 entsteht ein „Sicherheitsdruck von oben". Große Kunden sind gezwungen, sicherzustellen, dass ihre gesamte Lieferkette bestimmten Mindeststandards genügt. Dieser Druck wird an kleine und mittlere Unternehmen weitergegeben – teils formal, teils durch Ausschreibungen oder Audits.

Zudem erhöht sich durch die allgemeine Bedrohungslage und die zunehmende Digitalisierung die Erwartung an Unternehmen aller Größen, verantwortungsbewusst mit Daten und IT-Risiken umzugehen. NIS2 ist damit auch ein Türöffner für strategische Weiterentwicklung deines Unternehmens.

🔹 Was ist NIS2?

Die "Network and Information Security Directive 2" (NIS2) ist eine überarbeitete EU-Richtlinie, die die Cybersicherheit von Unternehmen in kritischen Sektoren verbessern soll. Sie tritt die Nachfolge der bisherigen NIS-Richtlinie an und erweitert sowohl den Anwendungsbereich als auch die Anforderungen. Ziel ist es, ein einheitliches und höheres Sicherheitsniveau in ganz Europa zu schaffen.

Wesentliche Neuerungen im Überblick:

1. Erweiterte Anwendungsbereiche: Die Anzahl der betroffenen Sektoren wurde deutlich erhöht
2. Härtere Sanktionen: Bei Nichteinhaltung drohen empfindliche Geldbußen (bis zu 10 Mio. EUR oder 2% des weltweiten Jahresumsatzes)
3. Persönliche Haftung: Führungskräfte können persönlich zur Verantwortung gezogen werden
4. Lieferkettenverantwortung: Die Sicherheit muss auch bei externen Partnern gewährleistet sein
5. Konkretere Anforderungen: Die Vorgaben für technische und organisatorische Maßnahmen sind präziser

Zu den betroffenen Sektoren zählen:

- Energieversorgung und -erzeugung
- Verkehr und Logistik
- Finanzdienstleistungen und Versicherungen
- Digitale Dienste, Telekommunikation, Cloud-Anbieter
- Gesundheitswesen, medizinische Versorgung, Labordienstleistungen
- Öffentliche Verwaltung und Raumfahrt
- Abfallwirtschaft
- Herstellung von kritischen Produkten (Medizinprodukte, Pharmazeutika)
- Nahrungsmittelproduktion und -verteilung
- Digitale Infrastruktur (Rechenzentren, CDN-Anbieter)

Neu: Auch zahlreiche "wichtige Einrichtungen" (sog. "important entities") sowie deren Dienstleister und Lieferanten können betroffen sein. Damit sind auch viele KMU zumindest indirekt verpflichtet, die Anforderungen umzusetzen oder nachzuweisen. Besonders betroffen sind IT-Dienstleister, Systemhäuser, Marketing- und Kommunikationsagenturen sowie Zulieferer mit digitaler Schnittstelle zu Kunden.

Zeitplan für die Umsetzung:

- Oktober 2024: Umsetzung in nationales Recht (in Deutschland voraussichtlich durch ein neues IT-Sicherheitsgesetz)
- Anfang 2025: Erste Meldepflichten treten in Kraft
- Q3/Q4 2025: Umfassende Implementierungsfrist für betroffene Organisationen
- Ab 2026: Vollständige Anwendung und Durchsetzung

📋 NIS2 Checkliste für KMU

Diese Checkliste hilft dir, den aktuellen Stand deines Unternehmens im Hinblick auf IT-Sicherheit und NIS2-Konformität besser einzuschätzen:

Grundlegende Sicherheitsorganisation

1. Cybersicherheits-Governance etabliert?

- [ ] Gibt es eine verantwortliche Person für IT-Sicherheit im Unternehmen?
- [ ] Ist die Geschäftsführung aktiv in IT-Sicherheitsthemen eingebunden?
- [ ] Werden IT-Sicherheitsthemen in regelmäßigen Abständen auf Management-Ebene besprochen?

2. Sicherheitsrichtlinien dokumentiert?

- [ ] Existiert eine IT-Sicherheitsrichtlinie, die alle relevanten Bereiche abdeckt?
- [ ] Wird diese regelmäßig überprüft und aktualisiert?
- [ ] Sind die Richtlinien allen Mitarbeitern bekannt und zugänglich?

3. Risikomanagement etabliert?

- [ ] Werden IT-Risiken systematisch identifiziert und bewertet?
- [ ] Gibt es einen dokumentierten Prozess zur Risikobewertung?
- [ ] Werden Maßnahmen zur Risikominimierung umgesetzt und nachverfolgt?

Mitarbeiterschulung & Awareness

4. Mitarbeiterschulungen durchgeführt?

- [ ] Gibt es regelmäßige Schulungen zu IT-Sicherheitsthemen?
- [ ] Werden neue Mitarbeiter zu IT-Sicherheit eingewiesen?
- [ ] Sind die Schulungen dokumentiert und wird der Erfolg gemessen?

5. Awareness-Kampagnen umgesetzt?

- [ ] Werden Mitarbeiter regelmäßig über aktuelle Bedrohungen informiert?
- [ ] Gibt es ein Programm zur Sensibilisierung für IT-Sicherheit (z.B. Phishing-Tests)?
- [ ] Existieren klare Meldewege für verdächtige Aktivitäten?

Technische Maßnahmen

6. Grundlegende Schutzmechanismen implementiert?

- [ ] Sind alle Systeme mit aktueller Antiviren-Software geschützt?
- [ ] Ist eine professionelle Firewall im Einsatz?
- [ ] Werden regelmäßige Updates und Patches eingespielt?

7. Zugriffskontrollen & Passwortmanagement etabliert?

- [ ] Ist eine Zwei-Faktor-Authentifizierung für kritische Systeme aktiviert?
- [ ] Gibt es eine dokumentierte Passwortrichtlinie?
- [ ] Werden Zugriffsrechte nach dem Need-to-Know-Prinzip vergeben?

8. Datensicherung implementiert?

- [ ] Gibt es ein dokumentiertes Backup-Konzept?
- [ ] Werden Backups regelmäßig getestet?
- [ ] Werden Backup-Daten an einem sicheren Ort (auch offline) aufbewahrt?

Incident Response & Business Continuity

9. Notfallplan definiert?

- [ ] Existiert ein dokumentierter Plan für IT-Sicherheitsvorfälle?
- [ ] Sind die Verantwortlichkeiten im Notfall klar geregelt?
- [ ] Wird der Plan regelmäßig getestet und aktualisiert?

10. Vorfallmanagement etabliert?

- [ ] Gibt es einen Prozess zur Erkennung und Behandlung von Sicherheitsvorfällen?
- [ ] Werden Sicherheitsvorfälle dokumentiert und analysiert?
- [ ] Ist ein Kommunikationsplan für Sicherheitsvorfälle vorhanden?

Lieferanten- und Drittanbieter-Management

11. Lieferanten bewertet?

- [ ] Werden IT-Sicherheitsaspekte bei der Lieferantenauswahl berücksichtigt?
- [ ] Gibt es ein Verfahren zur regelmäßigen Überprüfung von Lieferanten?
- [ ] Werden IT-Sicherheitsanforderungen vertraglich festgelegt?

12. Verträge mit Sicherheitsklauseln versehen?

- [ ] Enthalten Dienstleisterverträge spezifische IT-Sicherheitsklauseln?
- [ ] Sind Meldepflichten bei Sicherheitsvorfällen vertraglich geregelt?
- [ ] Gibt es Audit-Rechte gegenüber wichtigen Dienstleistern?

Compliance & Dokumentation

13. Regelmäßige Überprüfungen geplant?

- [ ] Finden regelmäßige interne Audits der IT-Sicherheitsmaßnahmen statt?
- [ ] Werden externe Überprüfungen (z.B. Penetrationstests) durchgeführt?
- [ ] Werden die Ergebnisse dokumentiert und Maßnahmen abgeleitet?

14. Datenschutz und IT-Sicherheit zusammen gedacht?

- ☐ Erfolgt eine Abstimmung zwischen Datenschutz und IT-Sicherheit?
- ☐ Werden gemeinsame Maßnahmen koordiniert umgesetzt?
- ☐ Sind die Verantwortlichkeiten und Schnittstellen klar definiert?

🚀 Praktische Umsetzungstipps

Quick Wins für mehr IT-Sicherheit

Diese Maßnahmen kannst du schnell und mit überschaubarem Aufwand umsetzen:

1. Passwort-Manager einführen
   Stelle allen Mitarbeitern einen professionellen Passwort-Manager zur Verfügung und definiere klare Regeln für sichere Passwörter.

2. Multi-Faktor-Authentifizierung aktivieren
   Aktiviere MFA für alle geschäftskritischen Anwendungen, insbesondere E-Mail, Cloud-Speicher und VPN-Zugänge.

3. Backup-Strategie überprüfen
   Stelle sicher, dass deine Backups regelmäßig durchgeführt werden, verschlüsselt sind und auch offline verfügbar sind.

4. Phishing-Simulationen durchführen
   Teste regelmäßig, ob deine Mitarbeiter Phishing-E-Mails erkennen, und schulde gezielt nach.

5. Regelmäßige Awareness-Trainings einführen
   Etabliere ein kontinuierliches Schulungsprogramm zu Sicherheitsthemen für alle Mitarbeiter (z.B. monatliche Micro-Learnings (Kurz-Schulungen) zu wechselnden Themen).

6. Sicherheitsverantwortlichen benennen
   Lege fest, wer in deinem Unternehmen für Informations-Sicherheit verantwortlich ist – auch wenn es kein Vollzeit-Job ist.

Mittel- bis langfristige Maßnahmen

Für eine nachhaltige Verbesserung deiner IT-Sicherheit:

1. IT-Sicherheitsrichtlinie erstellen
   Dokumentiere deine Grundsätze und Maßnahmen zur IT-Sicherheit in einer formellen Richtlinie.

2. Notfallplan entwickeln
   Lege fest, wie bei einem IT-Sicherheitsvorfall vorzugehen ist und wer welche Verantwortung trägt.

3. Inventar kritischer Systeme anlegen
   Dokumentiere alle wichtigen IT-Systeme, Anwendungen und Datenbestände.

4. Risikobewertung durchführen
   Identifiziere und bewerte systematisch die IT-Risiken für dein Unternehmen.

5. Sicherheitsaudits durchführen
   Plane regelmäßige interne oder externe Überprüfungen deiner Sicherheitsmaßnahmen.

🤝 So unterstützen wir dich

Ich weiß: Für viele KMU ist Cybersecurity kein Selbstläufer – es fehlen oft Zeit, Ressourcen und spezialisiertes Know-how. Genau hier setze ich an:

IT-Sicherheits-Check nach DIN SPEC 27076

Mein IT-Sicherheits-Check nach DIN SPEC 27076 ist speziell für kleine Unternehmen bis 50 Mitarbeiter konzipiert und bietet dir:

- Eine strukturierte Analyse deiner aktuellen IT-Sicherheit
- Einen detaillierten Bericht mit konkreten Handlungsempfehlungen
- Eine klare Priorisierung der notwendigen Maßnahmen
- Ein anerkanntes Qualitätsniveau, das du gegenüber Kunden nachweisen kannst

Mitarbeiter-Trainings & Awareness-Kampagnen

- E-Learning-Module, Live-Workshops oder monatliche Micro-Trainings
- Themen: Phishing, Passwortsicherheit, Remote Work, sichere Geräteverwendung, Social Engineering
- Optional: Prüfungen, Zertifikate und Teilnahme-Nachweise für dein Audit

Aufbau eines ISMS (Informationssicherheits-Managementsystems)

- Schritt-für-Schritt-Begleitung, speziell für kleine und mittlere Unternehmen
- Auswahl geeigneter Tools, Systeme und Templates
- Erstellung relevanter Dokumente (z.B. Richtlinien, Risikobewertungen, Prozessbeschreibungen)
- Regelmäßige Reviews zur Sicherstellung der Wirksamkeit

Vorbereitung auf ISO 27001-Zertifizierung

- Systematischer Aufbau eines ISO 27001-konformen ISMS
- Pragmatische Umsetzung der Anforderungen, maßgeschneidert für dein Unternehmen
- Durchführung von internen Audits zur Vorbereitung
- Begleitung während der Zertifizierung durch eine akkreditierte Zertifizierungsstelle
- Unterstützung bei der Behebung von Abweichungen

Begleitung bei der TISAX-Vorbereitung

- Durchführung einer Gap-Analyse nach VDA-ISA
- Entwicklung eines Maßnahmenplans zur Erfüllung der Anforderungen

- Unterstützung bei der internen Kommunikation, Dokumentation und Audit-Vorbereitung

Beratung zur NIS2-Compliance

- Identifikation von Schwachstellen im Kontext von NIS2
- Integration von IT-Sicherheitsanforderungen in bestehende Prozesse und Verträge
- Unterstützung bei der Kommunikation mit Kunden und Auftraggebern

DigimojoCOMPLY – Die Komplettlösung für NIS2-Compliance

Mit DigimojoCOMPLY biete ich dir eine integrierte Plattform, die speziell entwickelt wurde, um den Herausforderungen eines ISMS und anderen Sicherheitsanforderungen effizient zu begegnen. Anstatt mit unzähligen Excel-Tabellen, verstreuten Dokumenten und manuellen Prozessen zu jonglieren, erhältst du eine zentrale Lösung, die alle sicherheitsrelevanten Informationen bündelt und automatisiert.

Was DigimojoCOMPLY besonders macht:

- **Alles an einem Ort:** Von der Risikobewertung bis zur Maßnahmenverfolgung – alle Informationen sind zentral verfügbar und miteinander verknüpft
- **Automatisierte Workflows:** Intelligente Prozesse führen dich durch alle notwendigen Schritte und erinnern dich an fällige Aufgaben
- **Revisionssichere Dokumentation:** Alle Maßnahmen werden automatisch dokumentiert und sind jederzeit prüfungsbereit
- **Sofort einsatzbereit:** Vorkonfigurierte Templates und Best-Practice-Vorlagen ermöglichen einen schnellen Start
- **Kontinuierliche Verbesserung:** Dashboards und Reports zeigen dir auf einen Blick, wo du stehst und wo Handlungsbedarf besteht

DigimojoCOMPLY wächst mit deinen Anforderungen und ist dank Cloud-Hosting in einem ISO 27001-zertifizierten Rechenzentrum in Deutschland stets aktuell und sicher. Die modulare Struktur erlaubt es dir, genau die Funktionen zu nutzen, die du wirklich brauchst – ohne für unnötige Features zu bezahlen.

📑 NIS2 Anforderungen im Detail

Die NIS2-Richtlinie stellt konkrete Anforderungen in folgenden Bereichen:

Risikomanagement-Maßnahmen

- Risikobewertung und Informationssicherheitsrichtlinien
- Behandlung von Sicherheitsvorfällen
- Business Continuity und Krisenmanagement
- Lieferkettenmanagement
- Sicherheit bei der Beschaffung, Entwicklung und Wartung von Netzen und Informationssystemen
- Grundlegende Cyberhygiene-Maßnahmen
- Verschlüsselung und Kryptografie

Meldepflichten

- Signifikante Vorfälle (binnen 24 Stunden erste Meldung, vollständiger Bericht innerhalb von 72 Stunden)
- Umfassende Dokumentationspflichten
- Zusammenarbeit mit Behörden bei Untersuchungen

Governance und Verantwortung

- Direkte Verantwortung des Managements für die Einhaltung der Maßnahmen
- Regelmäßige Schulungen für alle Mitarbeiter
- Kontinuierliche Überprüfung und Verbesserung der Maßnahmen

Besonderheit für KMU in der Lieferkette

Wenn dein Unternehmen Dienstleistungen für betroffene Organisationen erbringt, können diese verlangen, dass du:

- Bestimmte Mindestanforderungen erfüllst
- Die Einhaltung nachweisen kannst (durch Audits oder Zertifizierungen)
- Sicherheitsvorfälle meldest, die ihre Systeme oder Daten betreffen könnten

📢 Nächste Schritte

1. Nutze meine Checkliste als ersten Selbsttest für dein Unternehmen.
2. Melde dich für ein kostenloses Erstgespräch – wir analysieren gemeinsam deinen aktuellen Stand.
3. Erhalte individuelle Empfehlungen und einen Fahrplan für sinnvolle nächste Schritte.

Je früher du handelst, desto besser kannst du dein Unternehmen absichern – und dich als zuverlässigen Partner positionieren.

❓ Braucht dein Unternehmen Unterstützung?

Informationssicherheit kann komplex sein – ich helfe dir gerne weiter!

Mein Ziel mit Digimojo: Aus deiner Cybersecurity-Initiative wird ein echter Marktvorteil. Wir unterstützen dich mit klarer Kommunikation, Team Enablement und einer Positionierung, die Vertrauen schafft – intern wie extern.

Ich bin Thorsten Wälde, Berater aus Leidenschaft für Datenschutz, Informationssicherheit und Cybersecurity – speziell für kleine und mittlere Unternehmen. Ich weiß, wie herausfordernd gesetzliche Vorgaben und

Sicherheitsanforderungen im Alltag sein können. Deshalb unterstütze ich dich mit klaren, praxisnahen Lösungen, die wirklich funktionieren – damit dein Unternehmen sicher, compliant und zukunftsstark bleibt.

📧 Schreib mich an: hallo@digimojo.de
📅 Buche ein kostenloses Erstgespräch: Termin vereinbaren

Über Digimojo

Digimojo ist mehr als ein Beratungsunternehmen – wir sind dein Sparringspartner auf dem Weg zu mehr Sicherheit und Compliance. Wir kennen die Herausforderungen, vor denen KMU stehen, und liefern keine Konzepte von der Stange, sondern pragmatische Lösungen, die sich im Alltag bewähren. Gemeinsam machen wir dein Unternehmen cybersicher, gesetzeskonform und bereit für die digitale Zukunft.

Digimojo

🔗 **digimojo.de**

🧰 Glossar der wichtigsten Begriffe

Asset Management
Die systematische Erfassung und Verwaltung aller IT-Assets (Hardware, Software, Daten, Systeme), um Risiken besser bewerten und Schutzmaßnahmen gezielt umsetzen zu können.

Awareness
Das Sicherheitsbewusstsein der Mitarbeitenden – zentraler Erfolgsfaktor für IT-Sicherheit im Unternehmen.

Awareness-Trainings
Maßnahmen zur kontinuierlichen Sensibilisierung und Schulung von Mitarbeitenden im Bereich Informationssicherheit und Cybersecurity.

Business Continuity Management (BCM)
Maßnahmen und Prozesse zur Aufrechterhaltung des Geschäftsbetriebs in Krisensituationen.

Business Impact Analysis (BIA)
Analyseverfahren zur Bewertung der Auswirkungen eines Ausfalls von Geschäftsprozessen – Grundlage für BCM und Notfallpläne.

Compliance
Die Einhaltung gesetzlicher, regulatorischer und interner Anforderungen – zentral für die Umsetzung von NIS2.

Cybersecurity
Gesamtheit der Technologien, Prozesse und Maßnahmen, die dem Schutz von Computersystemen, Netzwerken und Daten vor Angriffen, Schäden und unbefugtem Zugriff dienen.

DORA
(Digital Operational Resilience Act) – Europäische Verordnung zur Stärkung der digitalen Resilienz im Finanzsektor. Verpflichtet Finanzunternehmen und ihre IT-Dienstleister zur Einführung robuster Risikomanagement- und Cybersecurity-Strukturen.

Incident Response
Maßnahmen zur Erkennung, Eindämmung und Behebung von Sicherheitsvorfällen.

Incident-Management
Strukturierter Prozess zur Erkennung, Bearbeitung, Meldung und Nachverfolgung von sicherheitsrelevanten Vorfällen.

Integrität (Integrity)
Sicherstellung, dass Daten und Systeme nicht unbemerkt manipuliert werden können.

ISMS
Informationssicherheits-Managementsystem – Ein Managementsystem zur systematischen Verwaltung, Steuerung und Verbesserung der Informationssicherheit im Unternehmen.

Kritische Infrastruktur (KRITIS)
Sektoren und Unternehmen, deren Ausfall erhebliche Auswirkungen auf das Gemeinwesen haben kann. Mit NIS2 wurde die Definition erweitert – viele KMU könnten nun ebenfalls betroffen sein.

Logging & Monitoring
Protokollierung und Überwachung von IT-Systemen, um sicherheitsrelevante Ereignisse rechtzeitig zu erkennen und analysieren zu können.

Mehr-Faktor-Authentifizierung (MFA)
Sicherheitsmaßnahme, bei der mindestens zwei unabhängige Authentifizierungsfaktoren (z. B. Passwort + App) für den Zugang benötigt werden – häufig verpflichtend im Rahmen von NIS2.

NIS2
EU-Richtlinie zur Stärkung der Cybersicherheit kritischer und digitaler Infrastrukturen, erweitert um Pflichten entlang der Lieferkette.

Notfallmanagement (Incident Handling)
Umfassende Planung und Prozesse, wie ein Unternehmen auf schwerwiegende Störungen oder Angriffe reagieren soll – über Incident Response hinausgehend.

Patch-Management
Der Prozess zur Verwaltung und Implementierung von Software-Updates und Sicherheitspatches.

Penetrationstest
Eine kontrollierte Simulation eines Hackerangriffs, um Schwachstellen in Systemen oder Anwendungen zu identifizieren.

Phishing
Betrugsversuche, meist per E-Mail, sollen Mitarbeitende zur Preisgabe von Zugangsdaten oder zur Ausführung von Schadsoftware verleiten.

Ransomware
Schadsoftware, die Daten verschlüsselt und für deren Entschlüsselung ein Lösegeld gefordert wird.

Resilienztests
Simulierte Angriffe und Tests zur Überprüfung der Widerstandsfähigkeit von IT-Systemen und Sicherheitsprozessen gegen Cyberbedrohungen.

Risk Assessment
Die strukturierte Bewertung von IT-Risiken, z. B. für Systeme, Prozesse oder Lieferanten.

Risikoanalyse (Risk Analysis)
Bewertung potenzieller Bedrohungen und Schwachstellen – oft als Teil des ISMS und für NIS2 verpflichtend.

Security by Design
IT-Systeme und Prozesse werden von Anfang an so gestaltet, dass Sicherheit integraler Bestandteil ist.

Supply Chain Security
Die Absicherung der gesamten Lieferkette gegen IT-Sicherheitsrisiken.

Third-Party Risk Management
Verfahren zur Identifikation, Bewertung und Steuerung von Risiken, die durch externe Dienstleister und Lieferanten entstehen können.

TISAX
"Trusted Information Security Assessment Exchange" – branchenspezifischer Standard für die Automobilindustrie, entwickelt vom VDA.

Verfügbarkeit (Availability)
Eines der drei Grundprinzipien der Informationssicherheit (neben Vertraulichkeit und Integrität). Bedeutet: Systeme und Daten müssen im Bedarfsfall erreichbar und funktionsfähig sein.

Vertraulichkeit (Confidentiality)
Schutz von Informationen vor unbefugtem Zugriff – ein zentraler Aspekt von IT-Sicherheit.

Zugriffsmanagement
Steuerung, wer auf welche Systeme und Informationen zugreifen darf – oft mit Rollenverteilung und Mehrfaktor-Authentifizierung.