ISiCO

inklusive Schnelltest-Checkliste

Praxis-Leitfaden zur neuen NIS2-Richtlinie der EU

In 9 einfachen Schritten zur NIS2-Compliance

Wie Sie sicher und ressourcenschonend die neuen Anforderungen an Ihre IT-Sicherheit erfüllen.

KUNDEN, DIE UNS BEREITS VERTRAUEN:

zalando CLARK SPIE CHARITÉ UNIVERSITÄTSMEDIZIN BERLIN fressnapf idealo trivago

Version: November 2025

Herzlich Willkommen!

Schön, dass Sie sich unseren Praxisleitfaden **„9 Schritte zur NIS2 Compliance“** heruntergeladen haben.

Ich habe ihn für Sie erstellt, um Ihnen dabei zu helfen, den Überblick und die Kontrolle über Ihre NIS2-Compliance zu behalten.

Der Leitfaden enthält **9 wichtige Punkte**, die Sie bei der Umsetzung der NIS2-Anforderungen in Ihrem Unternehmen beachten sollten.

Eine NIS2-Analyse ist ein wesentliches Instrument, um die Cybersicherheitskonformität zu bewerten und zu verbessern. Sie hilft, Risiken frühzeitig zu erkennen, Prozesse zu optimieren und gesetzliche Vorgaben zu erfüllen.

Dieser Leitfaden bietet eine **praxisnahe Schritt-für-Schritt-Anleitung** zur strukturierten Umsetzung der NIS2-Anforderungen.

Da die NIS2-Richtlinie durch das am 13. November 2025 beschlossene NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2-UmsuCG) nunmehr in Deutsches Recht umgesetzt wird, sollten Sie mit der Umsetzung nicht länger warten.

Ich wünsche Ihnen viel Freude und Erfolg bei der Umsetzung.

Dr. Jan Scharfenberg
Partner

Ich durfte bereits unzählige NIS2-Compliance-Überprüfungen für Unternehmen aller Größen durchführen und unterstütze viele Betriebe als externer Cybersicherheitsberater. Deshalb weiß ich genau, welche Herausforderungen bei der Umsetzung der NIS2-Anforderungen entstehen und worauf es bei einer effizienten Umsetzung ankommt. Außerdem beobachte ich häufig, dass Sicherheitsbeauftragte Schwierigkeiten haben, die Übersicht und Kontrolle über die Cybersicherheits-Infrastruktur zu behalten. Dieser Leitfaden soll Ihnen dabei helfen, einen Selbstcheck in Ihrem Unternehmen durchzuführen.

Bevor Sie loslegen: Wer ist im Unternehmen für die NIS2-Umsetzung verantwortlich?

Für die Umsetzung der NIS-2-Richtlinie ist im Unternehmen **primär die Unternehmensleitung** verantwortlich. Sie trägt die strategische Gesamtverantwortung und kann bei Verstößen persönlich haftbar gemacht werden.

Wenn Sie einen **Informationssicherheitsbeauftragten (ISB)** haben, sollte dieser die Koordination und Kontrolle der Umsetzung übernehmen. Die **Legal- bzw. Compliance-Abteilung** ist für die Überprüfung der Einhaltung gesetzlicher Vorgaben und die Integration der NIS-2-Anforderungen in bestehende Compliance-Strukturen zuständig. Die **IT-Abteilung** verantwortet die Implementierung und Wartung technischer Sicherheitslösungen sowie die Überwachung der Netz- und Informationssysteme.

Hier noch einmal in der Übersicht:

Unternehmensleitung

- strategische Gesamtverantwortung
- kann bei Verstößen persönlich haftbar gemacht werden

Legal-/Compliance-Abteilung

- Prüfung der NIS2-Betroffenheit
- Überprüfung der Einhaltung gesetzlicher Vorgaben
- Integration der NIS-2-Anforderungen in bestehende Compliance-Strukturen

IT-Abteilung

- Implementierung und Wartung technischer Sicherheitslösungen.
- Überwachung der Netz- und Informationssysteme.

PRAXISTIPP

Bestimmen Sie eine oder mehrere Personen für die Koordination und Kontrolle der Umsetzung – am besten den **Informationssicherheitsbeauftragten (ISB)**. Der ISB kann auch **extern besetzt** werden.

Schritt 1: Durchführung einer Betroffenheitsprüfung

Die NIS2-Richtlinie betrifft Unternehmen, die als **„wesentliche“** oder **„wichtige“** Einrichtungen in bestimmten Sektoren eingestuft werden. Zu den relevanten Sektoren zählen unter anderem Energie, Transport, Gesundheit, digitale Infrastruktur und öffentliche Verwaltung. Ein Unternehmen gilt als betroffen, wenn es mindestens **50 Mitarbeiter** beschäftigt und einen **Jahresumsatz oder eine Jahresbilanzsumme von mindestens 10 Millionen Euro** aufweist.

Ob Ihr Unternehmen betroffen ist, können Sie mit unserem NIS2-Online-Checker herausfinden:

Wichtig: Die Geschäftsleitung steht in besonderer Verantwortung. Neben der Bereitstellung notwendiger finanzieller Ressourcen für die Einführung der von NIS2 geforderten Maßnahmen, ist sie dazu verpflichtet die Maßnahmenumsetzung zu überwachen, notwendige Richtlinien und Prozesse zu billigen und sich regelmäßig zu NIS2 schulen zu lassen.

Schritt 2: Durchführung einer Risikobewertung

Beginnen Sie mit der Identifikation aller kritischen Netz- und Informationssysteme Ihres Unternehmens. Analysieren Sie potenzielle Bedrohungen und Schwachstellen, die diese Systeme beeinträchtigen könnten. Bewerten Sie die Wahrscheinlichkeit des Eintretens dieser Bedrohungen sowie deren potenzielle Auswirkungen auf den Geschäftsbetrieb. Dokumentieren Sie die Ergebnisse und entwickeln Sie Strategien zur Risikominderung.

Beispiele für mögliche Bedrohungen und Schwachstellen:

Unzureichender Schutz von Gebäuden

- **Schwachstelle:** Fehlende physische Sicherheitsmaßnahmen wie Zutrittskontrollen oder Überwachungssysteme.
- **Mögliche Bedrohung:** Unbefugter physischer Zugriff auf Serverräume oder Büroräume, was zu Diebstahl oder Sabotage führen kann.

Unverschlüsselte Speicherung sensibler Daten:

- **Schwachstelle:** Speicherung vertraulicher Informationen ohne angemessene Verschlüsselung.
- **Mögliche Bedrohung:** Abfangen oder Diebstahl von Daten durch Cyberkriminelle, was zu Datenlecks und Compliance-Verstößen führen kann

Veraltete oder ungepatchte Software:

- **Schwachstelle:** Einsatz von Software mit bekannten Sicherheitslücken aufgrund fehlender Updates.
- **Mögliche Bedrohung:** Ausnutzung dieser Schwachstellen durch Malware oder Hackerangriffe, die zu Systemkompromittierungen führen können.

PRAXISTIPP

Ein wichtiger Schritt ist die regelmäßige Aktualisierung Ihrer Risikobewertung – **idealerweise jährlich oder nach größeren Systemänderungen**. Bedrohungen und Technologien entwickeln sich stetig weiter. Der Austausch mit anderen Unternehmen oder die Teilnahme an Fachforen hilft, neue Risiken frühzeitig zu erkennen.

Schritt 3: Implementierung von Sicherheitsmaßnahmen

Setzen Sie technische und organisatorische Maßnahmen (TOM) um, um identifizierte Risiken zu minimieren. Zum Beispiel:

- **Netzsegmentierung:** Teilen Sie Ihr Netzwerk in isolierte Segmente auf, um im Falle eines Sicherheitsvorfalls die Ausbreitung von Schadsoftware zu verhindern.
- **Zugriffsmanagement:** Implementieren Sie strikte Zugriffskontrollen, sodass Mitarbeiter nur auf die für ihre Arbeit notwendigen Daten und Systeme zugreifen können.
- **Sicherheitsupdates:** Stellen Sie sicher, dass alle Systeme und Anwendungen regelmäßig aktualisiert werden, um bekannte Sicherheitslücken zu schließen.
- **Überwachungssysteme:** Nutzen Sie Intrusion Detection und Prevention Systeme (IDPS), um ungewöhnliche Aktivitäten frühzeitig zu erkennen und darauf zu reagieren.

PRAXISTIPP

Der Aufbau eines Informationssicherheitsmanagementsystems (ISMS) ist das zentrale Element einer Compliance mit NIS2. Die Grundlagen branchenüblicher Standards der Informationssicherheit wie der ISO:IEC 27001 können wichtige Anhaltspunkte für den Aufbau einer NIS2-Compliance und eines ISMS liefern.

Schritt 4: Entwicklung eines Incident Response Plans

Erstellen Sie einen Plan zur Erkennung, Meldung und Behebung von Sicherheitsvorfällen. Dazu gehört unter anderem:

- **Kommunikationsstrategie:** Definieren Sie klare Kommunikationswege und -verantwortlichkeiten für den Fall eines Sicherheitsvorfalls, sowohl intern als auch extern.
- **Rollen und Verantwortlichkeiten:** Legen Sie fest, welche Mitarbeiter für welche Aufgaben im Falle eines Vorfalls zuständig sind.
- **Maßnahmenkatalog:** Erstellen Sie eine detaillierte Liste von Schritten zur Eindämmung, Untersuchung und Behebung von Sicherheitsvorfällen.
- **Dokumentation:** Sorgen Sie für eine lückenlose Aufzeichnung aller Vorfälle und der ergriffenen Maßnahmen, um aus vergangenen Ereignissen zu lernen und Compliance-Anforderungen zu erfüllen.

Schritt 5: Einhaltung der Meldepflichten

Der Incident Response Plan sollte auch die Einhaltung der Meldepflichten berücksichtigen. Erhebliche Sicherheitsvorfälle müssen unverzüglich, spätestens jedoch **innerhalb von 24 Stunden** nach deren Feststellung, an die zuständige nationale Behörde gemeldet werden. Die Meldung sollte eine detaillierte Beschreibung des Vorfalls, der betroffenen Systeme, der vermuteten oder bekannten Ursachen sowie der bereits ergriffenen oder geplanten Gegenmaßnahmen enthalten. Diese Transparenz ermöglicht es den Behörden, angemessen zu reagieren und gegebenenfalls Unterstützung bereitzustellen.

Wichtig: Prüfen Sie genau, ob ein Vorfall meldepflichtig ist. Ein Sicherheitsvorfall gilt als **„erheblich“**, wenn er eine schwerwiegende Betriebsstörung verursacht oder andere Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt.

Schritt 6: Erstellung eines Notfallplans

Entwickeln Sie Strategien zur Aufrechterhaltung des Geschäftsbetriebs bei Cyberangriffen oder Systemausfällen. Wichtige Bestandteile sind zum Beispiel:

- **Business Continuity Plan (BCP):** Entwickeln Sie Strategien und Verfahren, um kritische Geschäftsprozesse auch während und nach einem Sicherheitsvorfall aufrechtzuerhalten.
- **Disaster Recovery Plan (DRP):** Definieren Sie Maßnahmen zur Wiederherstellung von IT-Systemen, Daten und Infrastruktur nach einem schwerwiegenden Vorfall.
- **Regelmäßige Tests:** Führen Sie regelmäßig Übungen und Simulationen durch, um die Effektivität Ihrer Notfallpläne

Schritt 7: Sicherstellung der Lieferkettensicherheit

Überprüfen Sie die Sicherheitsmaßnahmen Ihrer Lieferanten und Dienstleister und integrieren Sie spezifische Sicherheitsanforderungen in Verträge mit Ihren Lieferanten und Dienstleistern. Dies kann die Verpflichtung zur Einhaltung bestimmter Sicherheitsstandards, regelmäßige Sicherheitsüberprüfungen und das Recht auf Audits umfassen. Stellen Sie sicher, dass Ihre Partner ähnliche Sicherheitsmaßnahmen implementieren, um die Integrität der gesamten Lieferkette zu gewährleisten.

PRAXISTIPP

Nutzen Sie einen risikobasierten Ansatz bei der Auswahl Ihrer Lieferanten und Dienstleister. Bewerten Sie deren Sicherheitspraktiken durch Cybersicherheits-Risikoanalysen und stellen Sie sicher, dass kritische Partner die erforderlichen Sicherheitsstandards erfüllen.

- ✓ **Risikoabschätzungen:** Prüfen Sie, wie die Sicherheitsmaßnahmen eines Partners Ihre Prozesse beeinflussen könnten.
- ✓ **Sicherheitsklassifizierung:** Wählen Sie Partner basierend auf festgelegten Sicherheitsstufen.
- ✓ **IT-Integration:** Binden Sie Ihre IT-Abteilung frühzeitig in die Auswahl ein.

Dieser Ansatz minimiert das Risiko von Sicherheitslücken in der gesamten Lieferkette.

Schritt 8: Mitarbeiterschulungen durchführen

Schulen Sie Ihre Mitarbeiter regelmäßig zu Cybersicherheitsrisiken und -maßnahmen. Schulungsinhalte könnten sein:

- **Erkennung von Phishing-Angriffen:** Schulen Sie Ihre Mitarbeiter darin, betrügerische E-Mails und andere Social-Engineering-Techniken zu erkennen und angemessen darauf zu reagieren.
- **Sicherer Umgang mit Passwörtern:** Vermitteln Sie Best Practices zur Erstellung und Verwaltung sicherer Passwörter, einschließlich der Nutzung von Passwort-Managern.
- **Verhalten bei Sicherheitsvorfällen:** Legen Sie klare Anweisungen fest, wie Mitarbeiter Verdachtsmomente melden und sich im Falle eines Sicherheitsvorfalls verhalten sollten.

Schritt 9: Dokumentation und Berichterstattung

Führen Sie detaillierte Aufzeichnungen über alle implementierten Sicherheitsmaßnahmen, durchgeführten Schulungen, Sicherheitsvorfälle und die entsprechenden Reaktionen darauf. Diese Dokumentation sollte regelmäßig überprüft und aktualisiert werden, um sicherzustellen, dass sie den aktuellen Gegebenheiten entspricht und bei Bedarf den zuständigen Behörden vorgelegt werden kann.

Bonus-Tipp: Tätigkeit im EU-Ausland?

Auch, wenn Ihr Unternehmen im EU-Ausland tätig ist, kann für Sie die Pflicht bestehen, die eigene Informationssicherheit, das Lieferkettenmanagement und die Behandlung von Zwischenfällen NIS2-konform auszugestalten. Die meisten Europäischen Länder haben die Richtlinie bereits in nationales Recht umgesetzt. Das gilt insbesondere für Tätigkeiten in Belgien, Griechenland, Italien, Kroatien, Lettland, Litauen, Slowakei, Rumänien und Ungarn. Diese Mitgliedsstaaten haben die Umsetzung bereits abgeschlossen.

Schnelltest-Checkliste zur NIS2-Readyness

1.	Haben Sie geprüft, ob Ihr Unternehmen unter die NIS2-Richtlinie fällt?	ja ☐	nein ☐
2.	Gibt es eine aktuelle Risikobewertung Ihrer Netz- und Informationssysteme?	ja ☐	nein ☐
3.	Haben Sie dokumentierte Maßnahmen zur Risikominderung und IT-Sicherheit implementiert?	ja ☐	nein ☐
4.	Existiert ein Notfallplan (Business Continuity / Disaster Recovery) für IT-Sicherheitsvorfälle?	ja ☐	nein ☐
5.	Gibt es einen dokumentierten Incident-Response-Plan, der Verantwortlichkeiten und Abläufe klar definiert?	ja ☐	nein ☐
6.	Haben Sie Lieferantenverträge überprüft und um Sicherheitsanforderungen ergänzt?	ja ☐	nein ☐
7.	Gibt es interne Richtlinien, die Anforderungen an Informationssicherheit und Cybersicherheit klar vorgeben?	ja ☐	nein ☐
8.	Haben alle relevanten Mitarbeitenden eine Schulung zur IT- und Cybersicherheit erhalten?	ja ☐	nein ☐
9.	Gibt es klare Zuständigkeiten für das Thema Cybersicherheit (z. B. einen Informationssicherheitsbeauftragten)?	ja ☐	nein ☐
10.	Erfassen und dokumentieren Sie systematisch alle umgesetzten Sicherheits-maßnahmen?	ja ☐	nein ☐
11.	Werden Ihre Netzwerke und IT-Systeme regelmäßig auf Schwachstellen geprüft (z. B. durch Penetrationstests)?	ja ☐	nein ☐
12.	Sind Sie in der Lage, die Sicherheit in Ihrer Lieferkette durch Audits oder Anfragen nachzuweisen?	ja ☐	nein ☐
13.	Werden alle IT-Systeme, Softwarelösungen und Cloud-Dienste regelmäßig aktualisiert (Patch-Management)?	ja ☐	nein ☐
14.	Wird die Effektivität Ihrer IT-Sicherheitsmaßnahmen regelmäßig überprüft und bewertet (z. B. durch interne Audits)?	ja ☐	nein ☐
15.	Ist Ihr Informationssicherheitsmanagementsystem (ISMS) ISO 27001-zertifiziert?	ja ☐	nein ☐

AUSWERTUNG:

- **Wenn Sie überall „Ja“ angekreuzt haben:** Super! Sie sind auf einem sehr guten Weg in Richtung NIS2-Compliance!
- **Wenn Sie mindestens einmal „Nein“ angekreuzt haben:** Handlungsbedarf vorhanden. Einzelne Maßnahmen sollten zeitnah verbessert werden.
- **Mehr als drei „Nein“?** Dringender Handlungsbedarf! Es sollte schnell ein strukturiertes NIS2-Compliance-Projekt gestartet werden

Über ISiCO

Datenschutz und Informationssicherheit sind mehr als nur Compliance – sie sind der Schlüssel zu langfristigem Unternehmenserfolg. Seit 2011 unterstützen wir Unternehmen aus allen Branchen dabei, Datenschutz, Informationssicherheit und Datenstrategie ganzheitlich und wirtschaftlich sinnvoll zu gestalten. Mit tiefgehendem Fachwissen, strategischer Beratung und einem klaren Verständnis für digitale Geschäftsmodelle entwickeln wir Lösungen, die praxisnah und zukunftssicher sind.

Unser Ansatz: Als eine der führenden Unternehmensberatungen in Deutschland bieten wir Unternehmen jeder Größe maßgeschneiderte Strategien und begleiten sie als Informationssicherheits- und externe Datenschutzbeauftragte. Namhafte Unternehmen, internationale Verbände und Institutionen aus stark regulierten Branchen vertrauen auf unsere Expertise.

Unsere Mission: Individuell. Unternehmerisch. Zukunftsorientiert. Keine Copy&Paste-Konzepte, sondern passgenaue Lösungen für Datenschutz und Informationssicherheit.

Warum ISiCO?

- führende Beratung in Datenschutz & IT-Sicherheit
- nur praxisnahe & wirtschaftlich sinnvolle Lösungen
- tiefes Branchenverständnis & strategische Weitsicht
- Expertise für digitale Geschäftsmodelle & neue Technologien
- juristische, technische und strategische Expertise vereint – für innovative, interdisziplinäre Lösungen

Sie kommen nicht weiter?

Vereinbaren Sie Ihr kostenfreies Erstgespräch zu den NIS2-Vorgaben direkt mit mir.

Nutzen Sie die Gelegenheit, ohne Aufwand und vollkommen unverbindlich herauszufinden, bis wann und wie Sie die NIS2-Richtlinie umsetzen müssen.
Sprechen Sie mit uns.

Anfrage Erstgespräch zu NIS2

DR. JAN SCHARFENBERG
Partner

T **+49 (0)30 21 30 028-0**
E **scharfenberg@isico.de**