WKO
WIRTSCHAFTSKAMMER WIEN
Unternehmensberatung · Buchhaltung · IT

NIS2 ohne Overkill - Wie Unternehmen Sicherheit sinnvoll und nachweisbar umsetzen

Philipp Mandl – 28.05.2026

Ihr Vortragender

Philipp Mandl, MSc.

Geschäftsführer - Zettasecure GMBH

- Zertifizierter Data & IT Security Expert
- Zertifizierter Information Systems Security Professional (CISSP)
- Zertifizierter Projektmanager der IPMA, Durchführung von über 120+ Einzelprojekten in den letzten Jahren
- Zertifizierter Incident Responder
- Zertifizierter ISO27001 Manager & Auditor
- Zertifizierter NIS 2 Directive Lead Implementer

Inhalt

- Ausgangslage - NIS2 & steigender Nachweisdruck
- Anforderungen an Unternehmen und Lieferketten
- Überblick - Welche Nachweise gibt es?
- Handlungsempfehlungen für Unternehmen

WIRTSCHAFTSKAMMER WIEN
Unternehmensberatung · Buchhaltung · IT

NIS2 verändert die Anforderungen an alle Unternehmen spürbar

- Regelt verbindliche Cybersecurity Pflichten für wesentliche und wichtige Einrichtungen
- der Anwendungsbereich wurde deutlich ausgeweitet
- Sicherheitsanforderungen betreffen nicht mehr nur direkt regulierte Unternehmen
- Sicherheitsniveau wird zunehmend zur Voraussetzung für Geschäftsbeziehungen
- IT-Sicherheit ist nicht mehr nur ein internes Thema sondern eine externe Erwartung.

WIRTSCHAFTSKAMMER WIEN
Unternehmensberatung · Buchhaltung · IT

Was wird von Unternehmen tatsächlich verlangt?

NIS2 verlangt **kein Zertifikat,** sondern ein nachweisbares Sicherheitsniveau.

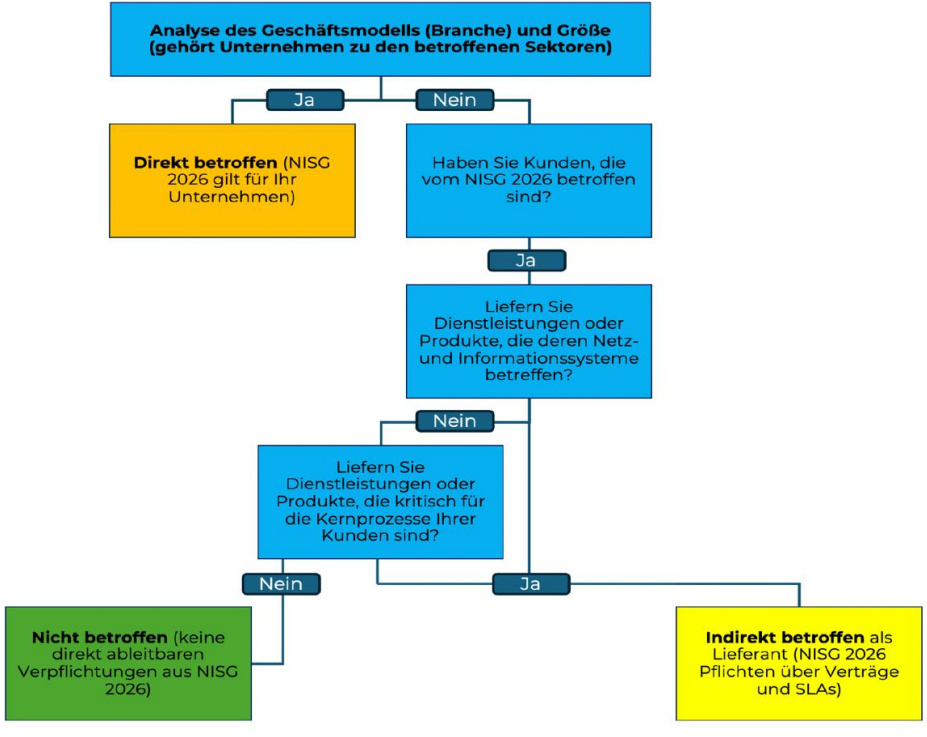
Fristen des NIS2 Gesetzes

23.12.2025	Veröffentlichung des Gesetzes im BGBl. I Nr. 94/2025
01.10.2026	• Inkrafttreten NISG 2026; NISG 2018 tritt zeitgleich außer Kraft • Bestimmungen zu den Risikomanagementmaßnahmen inklusive Sicherheit der Lieferkette und Meldepflichten gelten • Aufsicht- und Durchsetzungsmaßnahmen der Behörde sind möglich
01.01.2027	Registrierung muss erfolgt sein
01.10.2027	Selbstdeklaration muss erfolgt sein
01.10.2028	Cybersicherheitsbehörde kann Einrichtungen zur Prüfung auffordern

Was bedeutet das für nicht direkt betroffene Unternehmen?

- indirekte Betroffenheit über Kunden und Auftraggeber
- steigende Anforderungen an Sicherheitsnachweise in der Lieferkette
- vertragliche Verpflichtungen und Audits nehmen zu
- ohne Nachweis drohen Wettbewerbsnachteile oder Ausschluss

Bin ich als Unternehmen indirekt betroffen?



Welche Möglichkeiten existieren?

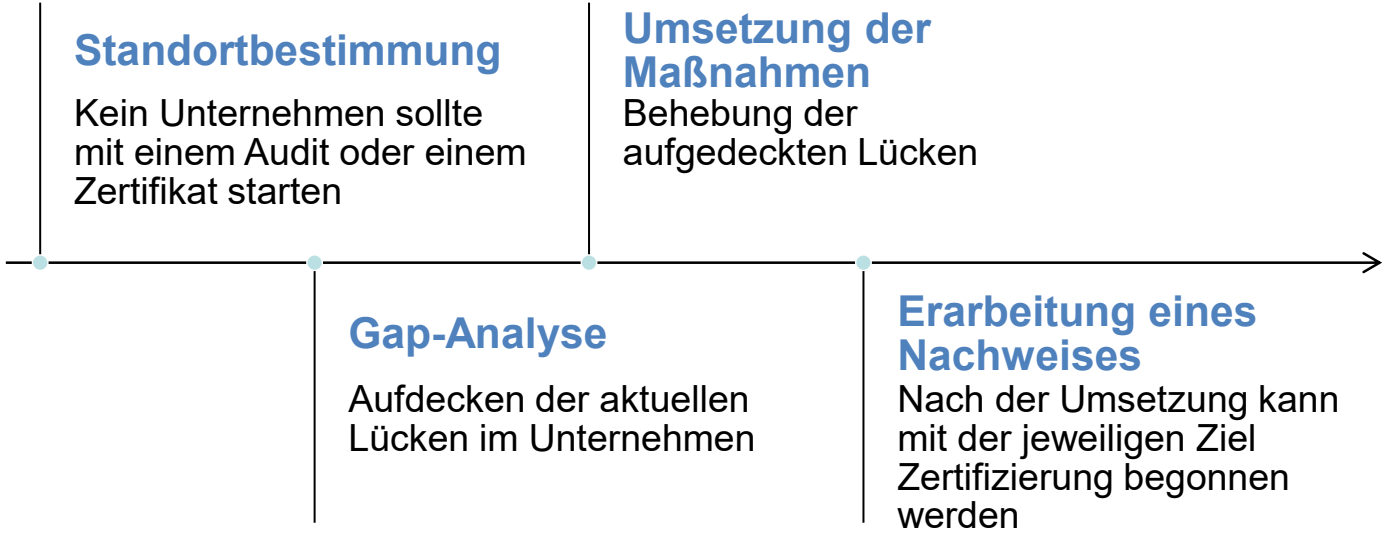
Lieferanten müssen sicherstellen, dass ihre IT- und Sicherheitsprozesse den Anforderungen der NISG 2026-regulierten Unternehmen entsprechen.

- ÖISHB: Zusammenarbeit mit Externen, Evaluierung von Zertifizierungen, Lieferantenbeziehungen
- **ISO/IEC 27001: Information security in supplier relationships**
- **IEC 62443 2-1: Supply chain security**
- CIS CSC v8.0: Service Provider Management
- **KSÖ Cyber Risk Rating: Anforderungen für A bzw. B Rating**
  - Cyber Trust Austria Label
  - KSV CyberRisk Rating

Was ist für KMU in Österreich realistisch?

- ISO/IEC 27001 – meist nur bei größeren oder kritischen Dienstleistern realistisch
- strukturierte Sicherheitsmaßnahmen + dokumentierte Prozesse
- **Cyber Trust Austria/Europe Label oder KSV RiskRating** als pragmatischer Nachweis
- Sicherheitsfragebögen als Mindestanforderung in vielen Projekten
- Cyber Risk Ratings zunehmend als ergänzende Bewertung

Wie gehe ich als Unternehmen vor?



Typische Fallstricke

- zu spät beginnen (erst bei Kundenanforderung reagieren)
- direkt auf ISO 27001 springen und dann überfordert sein
- fehlende Dokumentation
- kein klar definierter Zielzustand
- direkt mit der Zertifizierung beginnen (Security kann man nicht kaufen)

Fragen?

NIS2 ohne Overkill – 28.05.2026