NIS-2 ohne Panik – aber mit Plan

Wie die IT jetzt die richtigen Weichen stellt

Know-how to go | 10. Juni 2026

Marius Wiersch, Philipp Lottis

Agenda

- Problem und Ausgangslage
- NIS-2 im Überblick
- Typische Anti-Pattern
- Der smarte Weg

Problem und Ausgangslage

Doppelter Druck: Technologie und Regulatorik

Technologischer Wandel

- Cloud-Transformation
- Künstliche Intelligenz
- Post-Quantum-Kryptografie
- IT/OT-Konvergenz

IT

Regulatorischer Druck

- NIS-2-Umsetzungsgesetz
- KRITIS-Dachgesetz
- Cyber Resilience Act
- DORA & Branchenvorgaben

Die nächsten Herausforderungen kommen unabhängig davon, ob die IT bereit ist.

NIS-2 im Überblick

NIS-2: Wer ist betroffen?

~30.000	18	50+	10 Mio. EUR
betroffene Unternehmen in DE	kritische & wichtige Sektoren	Mitarbeitende oder >10 Mio. EUR Umsatz (+ Ausnahmen)	oder höhere Bußgelder

Zwei Stufen der Betroffenheit + KRITIS

Wichtige Einrichtungen

Grundlegende Pflichten, Bußgelder 7 Mio. EUR oder höher

Besonders wichtige Einrichtungen

Höhere Anforderungen, strengere Aufsicht, Bußgelder 10 Mio. EUR oder höher

KRITIS

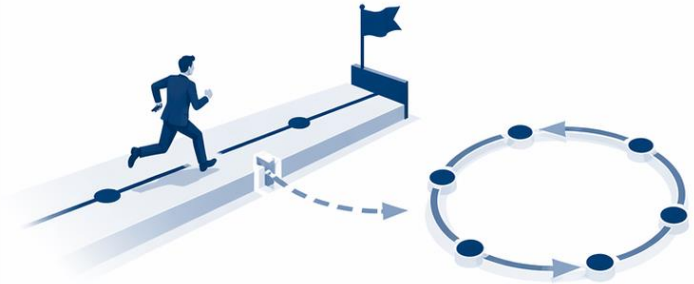
Strengste Anforderungen, proaktive Behördenaufsicht, Bußgelder 10 Mio. EUR oder höher

Was NIS-2 verlangt

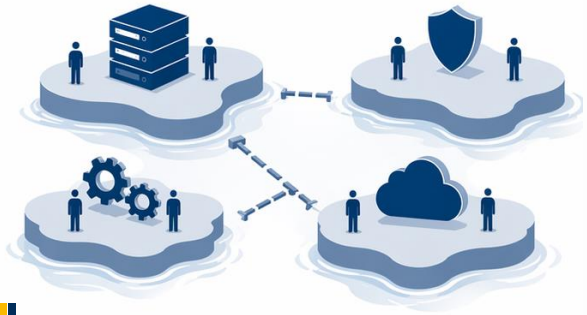
Fünf Kernanforderungen – die sich auswirken und abhängen von der IT-Organisation

Typische Anti-Pattern

Die häufigsten Fehler bei der NIS-2-Umsetzung



1 NIS-2 als Projekt statt als Prozess



2 Insellösungen ohne Integration

3 2nd Line erzeugt Papiertiger

4 1st Line diktiert Best Practice

Stau in der IT: Ein Strukturproblem

Was passiert

Anforderungen aus NIS-2, DORA, IT-Grundschutz treffen gebündelt ein

Ressourcen auf zu viele Baustellen verteilt

Keine abgestimmte Priorisierung zwischen ISB und IT

Maßnahmen werden panisch und isoliert umgesetzt

Wirksamkeit wird nicht erreicht, Sicherheitslücken bleiben

ISB wird als Blockierer wahrgenommen

Ursache

→ Ungeklärtes Rollenverständnis zwischen ISB und IT

→ Fehlende tragfähige Prozesse und Steuerungsstrukturen

→ Kein gemeinsames Zielverständnis

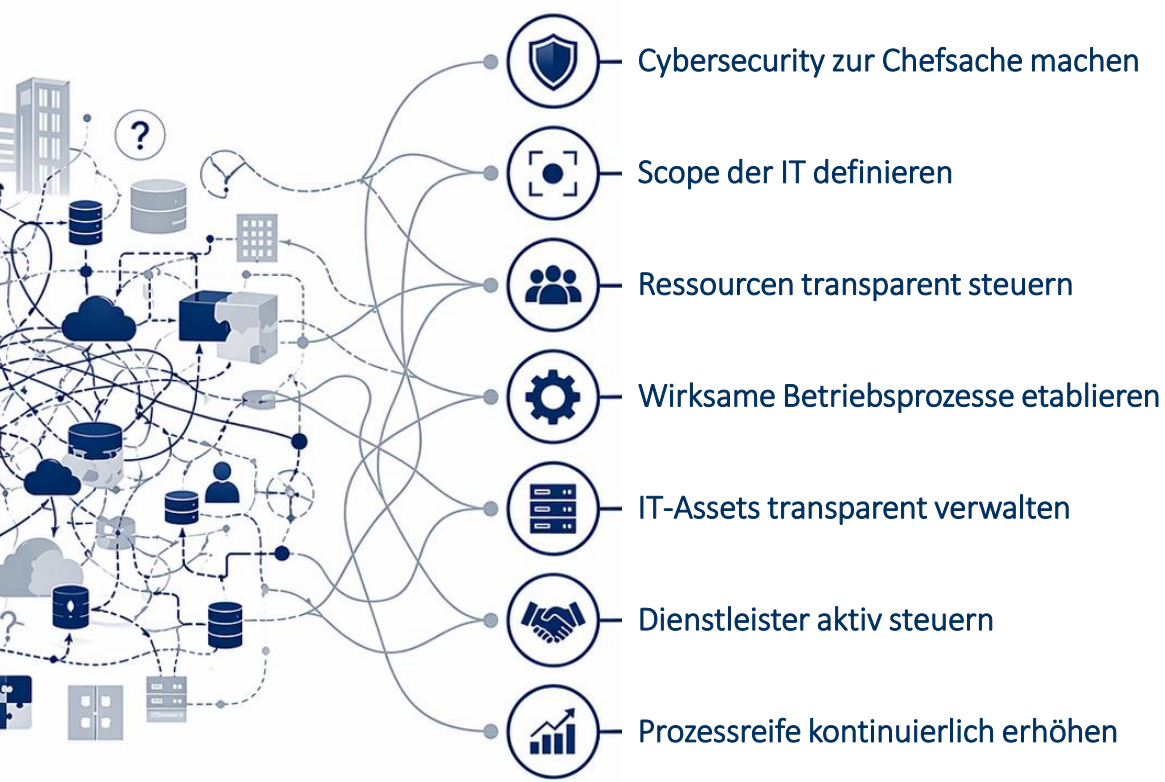
→ Anforderungen werden weitergereicht statt eingebettet

→ Security als Zusatzaufwand statt integraler Bestandteil

→ Bereiche werden zu spät eingebunden

Der smarte Weg

Die richtigen Weichen stellen: 7 Hebel für **IT-Reife** und **NIS-2-Konformität**



- Cybersecurity zur Chefsache machen
- Scope der IT definieren
- Ressourcen transparent steuern
- Wirksame Betriebsprozesse etablieren
- IT-Assets transparent verwalten
- Dienstleister aktiv steuern
- Prozessreife kontinuierlich erhöhen

These: **Resilienz** gegen **Regulatorik**

Wer NIS-2 nur als Compliance-Pflicht versteht, verpasst die eigentliche Chance:
Die eigene IT-Organisation zukunftsfähig und widerstandsfähig aufzustellen.

NIS-2 ist nicht das Ziel – NIS-2 ist der Anlass.

Kontakt

Marius Wiersch
Senior Manager

Philipp Lottis
Senior Consultant