ProcessForge

BLOG

NIS2-Checkliste für den Mittelstand: Nachweise, die du brauchst

NIS2 fragt nicht nur, ob du Prozesse hast — sondern ob du sie nachweisen kannst. Welche prozessbezogenen Nachweise gefragt sind und wie du sie aus dem, was du schon hast, in Tagen statt Quartalen erzeugst.

NIS2 verlangt für deine sicherheitsrelevanten Prozesse sechs prüffähige Nachweise: dokumentierte Prozesse, einen sichtbaren Risiko-Maßnahmen-Bezug, klare Verantwortlichkeiten, Aktualität, nachvollziehbare Vorfall- und Meldewege und Referenzierbarkeit auf die Quelle. Der Engpass ist fast nie das Wissen, sondern die prüffähige Form — und genau die erzeugst du aus dem, was du schon hast, in Tagen statt Quartalen.

NIS2 trifft vor allem mittlere und größere Unternehmen in kritischen oder wichtigen Sektoren — und die meisten von ihnen scheitern nicht am Wissen, sondern am Nachweis. Die Prozesse laufen, die Zuständigkeiten sind im Kopf geklärt, die Maßnahmen greifen. Was fehlt, ist die prüffähige Form: dokumentiert, referenziert, aktuell. Genau dafür ist diese Checkliste gedacht — als Orientierung, kein Ersatz für Rechtsberatung.

Welche Nachweise verlangt NIS2 für Prozesse?

1. **Dokumentierte Prozesse** — die sicherheitsrelevanten Abläufe schriftlich, nicht nur im Kopf der Verantwortlichen. Inklusive der Frage, wer was wann tut, wenn etwas schiefläuft.
2. **Risiko- und Maßnahmenbezug** — zu jedem erkannten Risiko die konkrete Maßnahme, die es adressiert. Die Verbindung muss sichtbar sein, nicht nur behauptet.
3. **Klare Verantwortlichkeiten** — wer trägt die Verantwortung für welche Kontrolle, welchen Prozess, welche Entscheidung. Namen oder Rollen, nicht „die IT“.
4. **Aktualität** — ein Stand, der das abbildet, was *heute* gilt, nicht der eingefroren wurde, als das Dokument zuletzt angefasst wurde.
5. **Vorfall- und Meldewege** — ein nachvollziehbarer Ablauf für das Erkennen, Behandeln und Melden von Sicherheitsvorfällen, inklusive der Zuständigen.
6. **Referenzierbarkeit** — jeder Nachweis sollte zurück auf seine Quelle zeigen. „Steht im Wiki“ reicht nicht; „steht hier, Stand soundso“ schon.

Wo ProcessForge ansetzt

Die ehrliche Schwierigkeit ist selten die erste Erstellung — es ist die Übersetzung des realen Ist-Zustands in genau diese Form, unter Zeitdruck. ProcessForge zieht den realen Ablauf aus dem, was du schon hast — Doku, Tickets, System-Exporte, Gespräche — und baut daraus das Ergebnis, das der Nachweis verlangt:

- **Input:** deine bestehenden Quellen, ungereinigt
- **System:** gleicht den realen Ablauf mit den geforderten Punkten ab und zeigt Lücken
- **Nachweis raus:** Prozess-Doku, Risiko-Maßnahmen-Bezug und Verantwortlichkeiten, referenziert auf die Quelle

> Aus dem lebenden Kontext, nicht aus der Doku von gestern.

Und der eigentliche Hebel zeigt sich beim nächsten Mal: Ändert sich ein Prozess, zieht dasselbe System die aktualisierte Version aus dem Stand, der dann gilt. Aus einem Quartals-Projekt wird ein Lauf — in Tagen statt Quartalen.

Zum Ausprobieren: Bring deinen anstehenden NIS2-Anlass mit ins Demo-Gespräch — wir bauen an einer realen Quelle live das erste Stück Nachweis daraus.