



Holger Reibold

# NIS-2 Survival Kit

Der Praxisleitfaden mit

Sofortmaßnahmen,

Checklisten und Vorlagen zur

rechtssicheren Umsetzung

BRAIN-MEDIA DE

# NIS-2 Survival Kit

Audit-Readiness-Check

Die Audit-Readiness-Checkliste dient dazu, Organisationen prüfungsfähig, nicht prüfungspfekt zu machen. Ihr Zweck ist es, sicherzustellen, dass zentrale NIS-2-relevante Entscheidungen, Maßnahmen und Nachweise auffindbar, erklärbar und konsistent sind – unabhängig davon, ob tatsächlich ein Audit ansteht.

NIS-2-Audits bewerten nicht die Existenz einzelner Technologien, sondern die Fähigkeit einer Organisation, Risiken strukturiert zu steuern. Genau hier setzt die Audit-Readiness-Checkliste an. Sie hilft, vorhandene Informationen zu bündeln und sichtbar zu machen, ohne neue Dokumentationspflichten zu erzeugen. Das reduziert Unsicherheit und verhindert hektische Nacharbeiten.

Ein weiterer zentraler Zweck liegt in der Selbstkontrolle. Die Checkliste ermöglicht eine realistische Einschätzung des eigenen Reifegrads. Sie zeigt, ob Entscheidungen nachvollziehbar dokumentiert sind, Zuständigkeiten klar geregelt sind und technische Maßnahmen begründet umgesetzt wurden. Lücken werden frühzeitig sichtbar – bevor sie extern thematisiert werden.

Darüber hinaus dient die Audit-Readiness-Checkliste als Kommunikationshilfe. Sie strukturiert Gespräche mit Prüfern, Kunden oder Aufsichtsstellen, indem sie einen roten Faden vorgibt. Statt sich in Details zu verlieren, kann die Organisation ihre Steuerungslogik erklären und belegen. Hier ein Beispiel für eine solche Checkliste:

## **1. Einordnung und Betroffenheit**

- Betroffenheit nach NIS-2 wurde strukturiert geprüft
- Entscheidung ist dokumentiert
- Entscheidungsgrundlage ist nachvollziehbar begründet
- Regelmäßige Überprüfung der Einordnung ist vorgesehen

## **2. Governance und Verantwortung**

- Gesamtverantwortung ist benannt (Management)
- NIS-2-Koordinationsrolle ist definiert
- Operative Zuständigkeiten sind klar
- Entscheidungswege sind dokumentiert
- Vertretungsregelungen existieren

## **3. Risikoübersicht und Priorisierung**

- Kritische Geschäftsprozesse sind identifiziert
- Zentrale IT-Abhängigkeiten sind bekannt
- Risiken sind grob eingeordnet (keine Detailanalyse)
- Prioritäten sind gesetzt und Restrisiken akzeptiert und dokumentiert

#### **4. Technische Maßnahmen**

- Backup- und Wiederherstellungsmechanismen existieren
- Wiederherstellbarkeit wurde zumindest stichprobenartig geprüft
- Grundlegende Netzwerkstruktur ist bekannt (keine Blackbox)
- Zugriffsschutz für kritische Systeme ist geregelt
- Maßnahmen sind begründet, nicht zufällig

#### **5. Incident-Handling und Meldebereitschaft**

- Definition sicherheitsrelevanter Vorfälle vorhanden
- Interne Meldewege sind bekannt
- Entscheidung über Meldepflicht ist geregelt
- 24h-/72h-Fristen sind bekannt
- Kontaktinformationen sind aktuell

#### **6. Lieferkette und Dienstleister**

- Kritische Dienstleister sind identifiziert
- Mindestanforderungen sind definiert
- Informationen zur Sicherheitslage liegen vor

- Abhängigkeiten sind bekannt
- Entscheidungen zum Umgang mit Restrisiken sind dokumentiert

## **7. Dokumentation und Nachweise**

- Zentrale Dokumente sind gebündelt auffindbar
- Dokumente widersprechen sich nicht
- Entscheidungen sind erklärbar
- Aktualisierungen sind datiert

## **8. Kontinuität und Weiterentwicklung**

- Regelmäßige Überprüfung vorgesehen und Anpassungen geplant
- Erkenntnisse aus Vorfällen fließen ein
- NIS-2 ist im Regelbetrieb verankert

## **Gesamtbewertung**

- auditbereit
- mit Einschränkungen auditbereit
- aktuell nicht auditbereit

## Mehr zum Thema NIS-2

Das vollständige Buch „NIS-2 Survival Kit – Praxisleitfaden mit Sofortmaßnahmen, Checklisten und Vorlagen zur rechtssicheren Umsetzung“

 [Jetzt bei Amazon bestellen](#)