NIS-2-Checkliste für Unternehmen

Diese Checkliste dient als praxisnahe Arbeitsgrundlage zur Vorbereitung, Bewertung und Umsetzung von NIS-2-Anforderungen in Unternehmen. Sie orientiert sich an aktuellen behördlichen und fachlichen Checklisten sowie Umsetzungsleitfäden und ist so strukturiert, dass sie für Gap-Analysen, interne Audits und Projektsteuerung verwendet werden kann.

1. Betroffenheit und Einstufung

- Prüfen, ob das Unternehmen einem von NIS-2 erfassten Sektor zuzuordnen ist, etwa Energie, Verkehr, Gesundheit, digitale Infrastruktur oder bestimmten Industrie- und Dienstleistungsbereichen.
- Prüfen, ob das Unternehmen nach Größe und Rolle als „wichtige Einrichtung“ oder „besonders wichtige Einrichtung“ einzuordnen ist.
- Die Entscheidung zur Anwendbarkeit schriftlich dokumentieren, einschließlich Begründung, Annahmen und Zuständigkeiten.

2. Registrierung und Ansprechpartner

- Prüfen, ob eine Registrierung bei der zuständigen nationalen Behörde erforderlich ist und welche Fristen gelten.
- Die erforderlichen Unternehmensdaten, Sicherheitsansprechpartner und Meldekontakte vollständig zusammenstellen.
- Eine verantwortliche Kontaktstelle für NIS-2-Meldungen und Behördenkommunikation benennen.

3. Governance und Management-Verantwortung

- Sicherstellen, dass die Geschäftsleitung ihre Verantwortung für die Umsetzung und Überwachung von Cybersicherheitsmaßnahmen kennt.
- Rollen und Verantwortlichkeiten für Informationssicherheit, Incident-Management, BCM, Lieferantenmanagement und Compliance eindeutig festlegen.
- Management-Schulungen zu Cyberrisiken, NIS-2-Pflichten und Aufsichtserwartungen durchführen und dokumentieren.

4. Scope und Asset-Management

- Den Geltungsbereich der NIS-2-relevanten Dienste, Prozesse, IT-Systeme, OT-Komponenten und Standorte definieren.
- Ein aktuelles Inventar kritischer Assets, Anwendungen, Schnittstellen, Datenflüsse und Dienstleister führen.
- Kritikalität und Schutzbedarf der relevanten Assets nachvollziehbar bewerten.

5. Risikoanalyse und ISMS

- Eine dokumentierte Methodik zur Informationssicherheits-Risikoanalyse festlegen und regelmäßig anwenden.
- Risiken bewerten, priorisieren und in einem Maßnahmen- oder Risikobehandlungsplan nachverfolgen.
- Ein ISMS aufbauen oder weiterentwickeln, das die NIS-2-Anforderungen in Richtlinien, Prozessen und Kontrollen abbildet.

6. Richtlinien und Awareness

- Relevante Sicherheitsrichtlinien erstellen, freigeben, kommunizieren und regelmäßig überprüfen, etwa für Zugriffsmanagement, Patch-Management, Backup, Incident-Management und Lieferantensteuerung.
- Zielgruppenspezifische Awareness- und Schulungsprogramme für Management, Administratoren und Mitarbeitende umsetzen.
- Die Wirksamkeit von Schulungen und Sensibilisierungsmaßnahmen messen, etwa durch Tests, Übungen oder Phishing-Simulationen.

7. Technische und organisatorische Maßnahmen

- Ein dokumentiertes Sicherheitskonzept mit risikobasierten technischen und organisatorischen Maßnahmen etablieren.
- Prozesse zur Erkennung, Behandlung und Nachbereitung von Sicherheitsvorfällen definieren und erproben.
- Maßnahmen zur Betriebsaufrechterhaltung umsetzen, darunter Backup-Strategien, Wiederanlaufplanung, Krisenmanagement und Notfallvorsorge.
- Sicherheitsanforderungen für Beschaffung, Entwicklung, Wartung und Änderung von Systemen festlegen.

- Ein geregeltes Schwachstellen- und Patch-Management einführen, einschließlich Priorisierung und Fristensteuerung.
- Die Wirksamkeit der Sicherheitsmaßnahmen regelmäßig überwachen, testen und verbessern.

8. Identitäts- und Zugriffsmanagement

- Prozesse für Benutzeranlage, Rollenwechsel, Rezertifizierung und Entzug von Berechtigungen verbindlich regeln.
- Multi-Faktor-Authentifizierung oder vergleichbar starke Authentisierung für kritische Zugriffe umsetzen.
- Das Least-Privilege-Prinzip, Rollenmodelle und gegebenenfalls Netzsegmentierung technisch absichern.

9. Kryptografie und Kommunikation

- Geeignete kryptografische Verfahren nach Stand der Technik für Datenübertragung, Datenspeicherung und Schlüsselverwaltung einsetzen.
- Sichere Kommunikationskanäle für den Regelbetrieb und für Krisen- oder Notfalllagen bereitstellen.

10. Personal und physische Sicherheit

- Sicherheitsanforderungen für besonders kritische Rollen festlegen, einschließlich Vertraulichkeit, Berechtigungsprüfung und Eskalationswegen.
- Physische Schutzmaßnahmen für kritische Räume, Infrastrukturen und Systeme umsetzen, etwa Zutrittskontrollen und Besucherprozesse.

11. Incident-Management und Meldepflichten

- Einen dokumentierten Prozess zur Bewertung und Behandlung erheblicher Sicherheitsvorfälle festlegen.
- Die Meldewege für Frühwarnung, Folgemeldung und Abschlussmeldung organisatorisch und technisch vorbereiten.
- Interne und externe Kommunikationswege zu Management, CERT/CSIRT, Behörden und relevanten Partnern regelmäßig testen.

12. Resilienz und Wiederherstellung

- Backups kritischer Systeme regelmäßig erstellen, schützen und auf Wiederherstellbarkeit prüfen.
- Business-Continuity- und Krisenmanagementprozesse dokumentieren und durch Übungen validieren.
- Wiederanlauf- und Restore-Tests durchführen und daraus Verbesserungsmaßnahmen ableiten.

13. Lieferkettensicherheit

- Alle relevanten IT-, OT-, Cloud- und sonstigen Sicherheitsdienstleister identifizieren und bewerten.
- Sicherheitsanforderungen vertraglich absichern, etwa zu Meldepflichten, Mindeststandards, Audit-Rechten und Subunternehmern.
- Kritische Lieferanten regelmäßig überwachen und Nachweise zur Sicherheitsreife einfordern.

14. Audits und Wirksamkeitsnachweise

- Interne Audits, Kontrolltests und Management-Reviews zur Wirksamkeit der Maßnahmen planen und durchführen.
- Bestehende Zertifizierungen wie ISO 27001 auf ihre Abdeckung der NIS-2-Anforderungen überprüfen.
- Auditfest dokumentieren, welche Nachweise, Kennzahlen und Kontrollen für Behörden oder Prüfer verfügbar sind.

15. Dokumentation und Reporting

- Alle relevanten Richtlinien, Prozesse, Nachweise und Entscheidungen versioniert und nachvollziehbar dokumentieren.
- Regelmäßiges Reporting an Geschäftsleitung und Verantwortliche zur Umsetzungsreife, Risikolage und offenen Maßnahmen etablieren.
- Erkenntnisse aus Vorfällen, Tests und Audits systematisch in den Verbesserungsprozess überführen.

16. Sanktionen und Haftungsrisiken

- Management und Compliance-Verantwortliche über mögliche Sanktionen und Aufsichtsmaßnahmen informieren.
- Organisatorisch sicherstellen, dass Ressourcen, Zuständigkeiten und Entscheidungswege der regulatorischen Verantwortung entsprechen.

17. Praktische Verwendung

Diese Checkliste eignet sich besonders als Grundlage für folgende Einsatzbereiche:

- Initiale Gap-Analyse vor einem NIS-2-Umsetzungsprojekt.
- Reifegradbewertung bestehender Sicherheits- und Governance-Strukturen.
- Vorbereitung interner Audits, Management-Reviews oder externer Prüfungen.
- Überführung in ein operatives Maßnahmenregister mit Verantwortlichen, Fristen, Nachweisen und Prioritäten.

Haben Sie weitere Fragen?

Sie erreichen uns unter:

CONSUVATION GmbH
Tilsiter Str. 6
71065 Sindelfingen
www.consuvation.com

Telefon: +49 7031 4181-860
E-Mail: contact@consuvation.com