NIS-2 Survival Kit

Quiz für die Mitarbeitersensibilisierung

Dieses Quiz dient dazu, grundlegende Kenntnisse zur NIS-2-Richtlinie und deren praktischer Umsetzung zu überprüfen und zu vertiefen. Die Fragen basieren auf zentralen Prinzipien wie Risikoorientierung, Verantwortlichkeit, Incident Handling und Lieferkettensicherheit.

Modul 1 – NIS-2 Grundlagen (20 Fragen)

Frage 1: Ziel von NIS-2

Welche Ziele verfolgt NIS-2?

☑ Erhöhung der Resilienz von Organisationen
☑ Verbesserung der Reaktionsfähigkeit bei Vorfällen
☑ Klärung von Verantwortlichkeiten
☐ Einführung eines einheitlichen IT-Tools
☐ Abschaffung von Cyberangriffen

Frage 2: Grundprinzip von NIS-2

Was steht im Mittelpunkt der NIS-2-Logik?

☑ Nachvollziehbare Entscheidungen
☑ Risikobasierter Ansatz

☑ Organisatorische Beherrschbarkeit

☐ Maximale technische Absicherung

☐ Vollständige Risikovermeidung

Frage 3: NIS-2 als Konzept

Wie ist NIS-2 grundsätzlich zu verstehen?

☑ Als dauerhafte Managementaufgabe

☑ Als organisatorischer Rahmen

☐ Als einmaliges Projekt

☐ Als rein technisches Sicherheitsprogramm

☑ Als Bestandteil von Governance und Resilienz

Frage 4: Betroffenheit

Wann ist ein Unternehmen von NIS-2 betroffen?

☑ Wenn es kritische Dienstleistungen erbringt

☑ Wenn es Teil einer relevanten Lieferkette ist

☑ Wenn ein Ausfall Auswirkungen auf andere hat

☐ Nur wenn es ein KRITIS-Betreiber ist

☐ Nur bei Unternehmen > 1000 Mitarbeiter

Frage 5: Lieferkette

Welche Aussagen zur Lieferkette sind korrekt?

☑ Betroffenheit kann indirekt entstehen

☑ Dienstleister können NIS-2-relevant sein

☑ Auswirkungen auf Kunden sind entscheidend

☐ Nur direkte Betreiber sind relevant

☐ Lieferanten spielen keine Rolle

Frage 6: Fehlannahmen

Welche Aussagen sind typische Fehlannahmen?

☑ NIS-2 ist ein reines IT-Projekt

☑ NIS-2 erfordert Zertifizierung

☑ Nur große Unternehmen sind betroffen

☐ NIS-2 basiert auf Risikoanalyse

☐ NIS-2 verlangt Dokumentation

Frage 7: Risikoanalyse

Was verlangt NIS-2 bei der Risikoanalyse?

☑ Identifikation kritischer Assets

☑ Bewertung von Risiken

☑ Ableitung von Maßnahmen

☐ Mathematisch exakte Bewertung

☐ ISO-zertifizierte Methodik

Frage 8: Sicherheitsvorfälle

Was ist im Kontext NIS-2 wichtig?

☑ Vorfälle erkennen können

☑ Vorfälle bewerten können

☑ Meldeprozesse definieren

☐ 24/7 SOC betreiben müssen

☐ Jeder Vorfall muss gemeldet werden

Frage 9: Meldepflicht

Wann ist ein Vorfall potenziell meldepflichtig?

☑ Bei Auswirkungen auf Kunden

☑ Bei kritischen Systemausfällen

☑ Bei Störung wesentlicher Dienstleistungen

☐ Bei jedem IT-Fehler

☐ Bei geplanten Wartungen

Frage 10: Business Continuity

Was fordert NIS-2 in Bezug auf Business Continuity?

☑ Wiederanlaufplanung

☑ Priorisierung kritischer Prozesse

☑ Definition von Wiederherstellungszeiten

☐ Vollständige Ausfallsicherheit

☐ Hochverfügbarkeitsarchitektur zwingend

Frage 11: Backup

Welche Aussagen zu Backups sind korrekt?

☑ Backup ist Voraussetzung

☑ Backup ersetzt keine Wiederanlaufplanung

☑ Backups müssen getestet werden

☐ Backup allein erfüllt NIS-2

☐ Backups sind optional

Frage 12: Verantwortlichkeit

Wer trägt die Hauptverantwortung?

☑ Geschäftsführung

☑ Unternehmensleitung

☐ IT-Abteilung allein

☐ Externer Dienstleister

☑ Organisation insgesamt

Frage 13: Delegation

Was gilt für Verantwortung?

☑ Aufgaben sind delegierbar

☑ Verantwortung ist nicht delegierbar

☑ Überwachungspflicht bleibt bestehen

☐ Verantwortung kann vollständig übertragen werden

☐ IT trägt alleinige Verantwortung

Frage 14: Rolle der IT

Welche Aufgaben hat die IT-Leitung?

☑ Umsetzung technischer Maßnahmen

☑ Bewertung technischer Risiken

☑ Unterstützung der Entscheidungsfindung

☐ Finale Risikoentscheidungen treffen

☐ Haftung übernehmen

Frage 15: Dokumentation

Warum ist Dokumentation wichtig?

☑ Nachvollziehbarkeit von Entscheidungen

☑ Schutz der Geschäftsführung

☑ Transparenz über Maßnahmen

☐ Ersatz für Sicherheitsmaßnahmen

☑ Unterstützung von Audits

Frage 16: Priorisierung

Warum ist Priorisierung entscheidend?

☑ Ressourcen sind begrenzt

☑ Nicht alle Risiken sind gleich relevant

☑ Maßnahmen müssen wirksam sein

☐ Alle Maßnahmen sind gleich wichtig

☐ Vollständigkeit ist wichtiger als Wirkung

Frage 17: Sicherheitsmaßnahmen

Was verlangt NIS-2 bei Maßnahmen?

☑ Angemessenheit

☑ Nachvollziehbarkeit

☑ Risikoorientierung

☐ maximale technische Komplexität

☐ vollständige Absicherung

Frage 18: NIS-2 und Zertifizierung

Welche Aussage ist korrekt?

☑ Zertifizierung ist nicht vorgeschrieben

☑ Maßnahmen müssen begründbar sein

☐ ISO 27001 ist Pflicht

☐ Zertifikat ersetzt Umsetzung

☐ Audit ersetzt Risikoanalyse

Frage 19: Zielzustand

Was ist der Zielzustand von NIS-2?

☑ Handlungsfähigkeit im Ernstfall

☑ Klare Entscheidungsstrukturen

☑ Beherrschbarkeit von Risiken

☐ 100% Sicherheit

☐ vollständige Kontrolle aller Systeme

Frage 20: Grundverständnis

Welche Aussage trifft NIS-2 am besten?

☑ „Nicht Perfektion, sondern Angemessenheit“

☑ „Struktur statt Aktionismus“

☑ „Verantwortung statt Technikfokus“

☐ „Technologie löst alle Probleme“

☐ „Sicherheit ist ein Projekt“

Mehr zum Thema NIS-2

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