NIS-2 Survival Kit

Incident-Meldecheckliste

Diese Checkliste stellt sicher, dass sicherheitsrelevante Vorfälle schnell, strukturiert und nachvollziehbar behandelt und – falls erforderlich – gemeldet werden. Sie ersetzt keine technische Analyse, sondern unterstützt Entscheidungsfähigkeit unter Zeitdruck.

1. Erstbewertung – Liegt ein sicherheitsrelevanter Vorfall vor?

☐ Beeinträchtigung der Verfügbarkeit, Integrität oder Vertraulichkeit

☐ Kritischer Geschäftsprozess betroffen oder potenziell betroffen

☐ Verdacht auf externen Angriff (z. B. Ransomware, Kompromittierung)

☐ Unklarer oder ungewöhnlicher Systemzustand mit möglicher Auswirkung

➞ Wenn mindestens ein Punkt zutrifft: Vorfall als relevant behandeln.

2. Sofortmaßnahmen (technisch & organisatorisch)

☐ Vorfall intern gemeldet (IT / NIS-2-Koordination)

☐ Zeitpunkt der Feststellung dokumentiert

☐ Erste Eindämmungsmaßnahmen eingeleitet

☐ Beweise gesichert (Logs, Systeme nicht unnötig verändert)

☐ Kommunikationsdisziplin sichergestellt

3. Einordnung der Meldepflicht

☐ Auswirkungen auf wesentliche Dienste möglich oder gegeben

☐ Externe Auswirkungen nicht auszuschließen

☐ Rechtliche / regulatorische Relevanz wahrscheinlich

➞ Wenn unklar:

☐ Vorfall vorläufig als meldepflichtig einstufen (konservativer Ansatz)

NIS-2 erlaubt unvollständige Erstmeldungen.

4. Zuständigkeiten geklärt

☐ Verantwortliche Entscheidungsrolle informiert

☐ Meldeentscheidung getroffen oder vorbereitet

☐ Vertretung geregelt (falls außerhalb der Geschäftszeiten)

5. Erstmeldung (innerhalb 24 Stunden)

☐ Meldung vorbereitet

☐ Folgende Informationen enthalten (soweit bekannt):

Art des Vorfalls

Zeitpunkt / Zeitraum

Betroffene Systeme oder Dienste

Erste Einschätzung der Auswirkungen

Aktueller Status der Maßnahmen

☐ Meldung freigegeben

☐ Meldung versendet

☐ Zeitpunkt der Meldung dokumentiert

6. Folgemeldung / Aktualisierung (bis 72 Stunden)

☐ Neue Erkenntnisse zusammengeführt

☐ Auswirkungen präzisiert

☐ Ursachen (vorläufig) benannt

☐ Weitere Maßnahmen beschrieben

☐ Meldung aktualisiert / ergänzt

7. Interne Nachbereitung (nach Stabilisierung)

☐ Vorfall intern dokumentiert

☐ Erkenntnisse in Risikoübersicht übernommen

☐ Maßnahmen angepasst oder ergänzt

☐ Verantwortlichkeiten überprüft

☐ Entscheidung zu Restrisiken dokumentiert

Mehr zum Thema NIS-2

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