Ihre Checkliste zur NIS2-Richtlinie

Cybersicherheit im Griff? Machen Sie den Check ...

In Deutschland befindet sich das nationale Umsetzungsgesetz um NIS2 noch im Gesetzgebungsverfahren. Ziel der Richtlinie ist es, gesellschaftlich relevante Organisationen wirksam gegen Cyberangriffe zu wappnen. Wir zeigen Ihnen, wie Sie schon jetzt in elf Schritten zu wirkungsvollen Schutzmaßnahmen gelangen können.

1. Verantwortlichkeiten festlegen

Benennen Sie eine verantwortliche Person für die Umsetzung der NIS2-Richtlinie. Diese Person sollte nicht nur die Umsetzungsstrategie leiten, sondern auch die Unterstützung durch die Geschäftsleitung erhalten, um die nötige Durchsetzungskraft und Ressourcen zur Verfügung zu haben.

2. Strukturierten Projektplan erstellen

Planen Sie die Umsetzung der NIS2-Anforderungen anhand eines klaren, strukturierten Projektplans. Legen Sie Zeitrahmen, Meilensteine und Ressourcen fest, damit alle Schritte übersichtlich und geordnet durchgeführt werden können.

3. IT-Struktur analysieren

Dokumentieren Sie Ihre IT-Infrastruktur vollständig und erfassen Sie alle Assets. Eine transparente Übersicht hilft Ihnen, Schwachstellen frühzeitig zu erkennen und gezielte Sicherheitsmaßnahmen zu planen.

4. Schutzbedarf ermitteln

Bestimmen Sie, welche Ihrer Assets am meisten Schutz benötigen. Definieren Sie dabei klar, welche Systeme und Daten für Ihre Organisation unverzichtbar sind, um den angemessenen Schutzumfang festzulegen.

5. Risikobewertung durchführen

Analysieren Sie die Risiken, die für Ihre schützenswertesten Assets bestehen. Berücksichtigen Sie dabei mögliche Bedrohungen und Schwachstellen, um ein umfassendes Risikobild zu erhalten.

6. Vorbeugungsmaßnahmen entwickeln
Erarbeiten Sie auf Basis Ihrer Risikobewertung präventive und korrektive Maßnahmen. Damit mindern Sie die identifizierten Risiken und gewährleisten die Sicherheit Ihrer kritischen Assets.

7. Notfallmanagement etablieren
Erstellen Sie einen Notfallplan, um auf mögliche IT-Vorfälle vorbereitet zu sein. Simulieren Sie regelmäßig verschiedene Szenarien, um sicherzustellen, dass alle Beteiligten im Ernstfall wissen, wie sie reagieren müssen.

8. Dokumentation sicherstellen
Führen Sie eine detaillierte Nachweisdokumentation, in der Sie alle durchgeführten Schutzbedarf- und Risikoanalysen sowie die getroffenen Maßnahmen festhalten. Diese Dokumentation ist nicht nur für Ihre internen Prozesse wichtig, sondern auch für mögliche Prüfungen durch Aufsichtsbehörden.

9. Permanente Überwachung einrichten
Richten Sie eine kontinuierliche Überwachung Ihrer Systeminfrastruktur ein. Das hilft dabei, ungewöhnliche Aktivitäten frühzeitig zu erkennen und direkt darauf zu reagieren.

10. Kommunikation festlegen
Sensibilisieren Sie Ihre Mitarbeitenden für die Relevanz von IT-Sicherheit und definieren Sie klare Kommunikationswege für den Fall von Sicherheitsvorfällen. Stellen Sie sicher, dass im Falle eines Vorfalls alle Meldepflichten erfüllt werden.

11. PDCA-Zyklus anwenden
Etablieren Sie einen kontinuierlichen Verbesserungsprozess nach dem PDCA-Prinzip (Plan-Do-Check-Act). Überprüfen und optimieren Sie Ihre Sicherheitsmaßnahmen regelmäßig, um auf neue Bedrohungen und Veränderungen der Infrastruktur reagieren zu können.

Kontaktieren Sie uns