Kiteworks

NIS -2 Compliance Best Practices Checkliste für kleine Unternehmen

Anders als bei der ersten NIS-Richtlinie umfasst der Geltungsbereich der NIS-2Richtlinie nun auch kleine und mittlere Unternehmen (KMU), da sie eine entscheidende Rolle in der Lieferkette essenzieller Dienste spielen. Um KMU bei der Einhaltung der NIS-2Vorschriften zu unterstützen, finden Sie hier einige maßgeschneiderte Best Practices, die auf ihre Ressourcen und Kapazitäten zugeschnitten sind:

- **1. Führen Sie eine Risikobewertung durch:** Identifizieren Sie Schlüsselressourcen, potenzielle Bedrohungen und Schwachstellen. Priorisieren Sie Risiken basierend auf Wahrscheinlichkeit und potenziellem Einfluss, unter Verwendung von Methodologien wie ISO/IEC 27005 oder ENISA-Richtlinien.
- **2. Implementieren Sie ein Governance-Framework für Cybersicherheit:** Übernehmen Sie eine vereinfachte Version bestehender Frameworks (ISO/IEC 27001, NIST CSF), um Rollen, Verantwortlichkeiten und Richtlinien rund um die Cybersicherheit festzulegen.
- **3. Schulen Sie Mitarbeiter in Bezug auf Cybersicherheitsbewusstsein:** Bilden Sie regelmäßig Mitarbeiter über Phishing-Angriffe, Social Engineering, Passwortmanagement und sichere Online-Praktiken weiter.
- **4. Stellen Sie eine starke Zugriffskontrolle und Authentifizierung sicher:** Setzen Sie die Zwei-Faktor-Authentifizierung (2FA) in wichtigen Systemen durch. Beschränken Sie Benutzerprivilegien durch ein Modell der minimalen Rechtevergabe, um Insider-Bedrohungen zu reduzieren.
- **5. Entwickeln Sie einen Incident-Response-Plan:** Erstellen Sie einen Incident-Response-Plan, der Verfahren zur Erkennung, Meldung und Reaktion auf Cybersicherheitsvorfälle skizziert. Testen Sie den Plan durch Tabletop-Übungen, um Lücken und Schwachstellen zu identifizieren.
- **6. Üben Sie regelmäßiges Patchen und Schwachstellenmanagement:** Implementieren Sie automatisierte Patch-Management-Prozesse, um sicherzustellen, dass Systeme und Software regelmäßig aktualisiert werden. Verwenden Sie Tools zum Scannen von Schwachstellen, um Sicherheitsschwächen zu identifizieren.
- **7. Plan für Geschäftskontinuität und Notfallwiederherstellung (BC/DR):** Entwickeln Sie BC/DR-Pläne, die wichtige Systeme und die Wiederherstellung von Daten nach einem Sicherheitsvorfall abdecken. Testen Sie regelmäßig Backup-Prozesse, um sicherzustellen, dass kritische Daten effizient wiederhergestellt werden können.
- **8. Überwachen und Protokollieren der Netzwerkaktivität:** Setzen Sie Netzwerküberwachungstools ein, um ungewöhnliche Aktivitäten zu erkennen. Führen Sie Protokolle, um die Erkennung von Vorfällen zu erleichtern und die Einhaltung der Berichterstattungsanforderungen gemäß NIS2 zu gewährleisten.