Kiteworks

NIS-2Compliance-Checkliste für Best Practices für britische Unternehmen

Die folgenden Best Practices helfen britischen Unternehmen, die Anforderungen der NIS-2Konformität zu erfüllen, und stärken gleichzeitig ihr Cybersicherheitsprogramm, um sich gegen Cyberangriffe und Datenpannen zu verteidigen.

- **1. Führen Sie eine umfassende Risikobewertung durch:** Identifizieren Sie potenzielle Bedrohungen und Schwachstellen in Ihrem Netzwerk und Informationssystemen. Bewerten Sie die Wahrscheinlichkeit und Auswirkungen dieser Risiken, um die Minderungsmaßnahmen zu priorisieren.
- **2. Implementieren Sie starke Zugriffskontrollen:** Führen Sie die Zwei-Faktor-Authentifizierung und rollenbasierte Zugriffskontrollen (RBAC) ein, um sicherzustellen, dass nur autorisiertes Personal Zugang zu kritischen Systemen und Daten hat.
- **3. Stellen Sie kontinuierliches Monitoring und Erkennung sicher:** Implementieren Sie fortschrittliche Überwachungswerkzeuge und -techniken, wie Intrusion Detection Systeme und Security Information and Event Management Lösungen, um Bedrohungen in Echtzeit zu identifizieren und darauf zu reagieren.
- **4. Führen Sie regelmäßige Mitarbeiterschulungen durch:** Organisieren Sie regelmäßige Schulungssitzungen, um Mitarbeiter über Best Practices im Bereich der Cybersicherheit zu informieren, wie das Erkennen von Phishing-Versuchen und den sicheren Umgang mit sensiblen Daten.
- **5. Klare Kommunikationskanäle etablieren:** Legen Sie Kommunikationsprotokolle für die Meldung von Vorfällen innerhalb Ihres Unternehmens und an zuständige Behörden fest, wie es die NIS-2Richtlinie erfordert.
- **6. Kooperieren Sie mit externen Experten:** Ziehen Sie in Erwägung, sich mit Spezialisten zu beraten, um Ihre Sicherheitslage zu bewerten, Lücken zu identifizieren und Verbesserungen zu empfehlen.
- **7. Investieren Sie in fortschrittliche Cybersicherheitstechnologien:** Setzen Sie Lösungen wie Next-Generation-Firewalls, Tools zur Erkennung und Reaktion auf Endpunkte ein, um Ihr Netzwerk und Ihre Daten zu schützen.

- **8.Sichern Sie die Lieferkette:** Führen Sie gründliche Bewertungen Ihrer Lieferanten und Drittanbieter durch, um sicherzustellen, dass sie robuste Cybersicherheitspraktiken einhalten. Entwickeln und implementieren Sie Richtlinien und Verfahren, um Risiken im Zusammenhang mit Beziehungen zu Dritten zu mindern.

- **9. Integrieren Sie Threat Intelligence:** Nutzen Sie Threat-Intelligence-Feeds und -Plattformen, um Echtzeitinformationen über potenzielle Risiken zu sammeln. Integrieren Sie diese Erkenntnisse in Ihre Überwachungs- und Reaktionsbemühungen, um Bedrohungen proaktiv anzugehen.