DIGITAL TRANSFORMATION

NIS 2 Anforderungen in der Informationssicherheit: Compliance Checkliste

DIGITAL TRANSFORMATION

CHECKLISTE ZUR NIS 2 COMPLIANCE

(Network and Information Security Directive 2 – EU-Richtlinie zur Cybersicherheit)

1. Sicherheitsrichtlinien & Physische Sicherheit

- [ ] Sicherheitsrichtlinien (Information, IT und phsysisce Sicherheit) und -verfahren schriftlich dokumentiert und regelmäßig überprüft
- [ ] Zugangskontrollen für physische Standorte eingerichtet (z. B. Zutrittskarten, Transponder, biometrische Systeme)
- [ ] Überwachungssysteme (z. B. CCTV, Alarmanlage) zur physischen Sicherheit implementiert
- [ ] Maßnahmen zur Umgebungs- und Gebäudesicherheit implementiert (z. B. Feuerschutz, Wasserschäden)
- [ ] Sichere Vernichtung sensibler Dokumente und Datenträger gewährleistet

2. Asset & Risikomanagement

- [ ] Vollständige und aktuelle Inventarisierung aller IT-Assets (Hardware, Software, Netzwerke, Infrastruktur usw.)
- [ ] Vollständige und aktuelle Inventarisierung aller Non-IT-Assets (geistiges Eigentum, Daten, Prozesse, Personal usw.)
- [ ] Durchführung regelmäßiger Risikoanalysen für IT- und Non-IT Assets
- [ ] Sicherheitsmaßnahmen für kritische Infrastrukturen priorisiert (Business Impact Analyse - BIA)
- [ ] Identifikation von Schwachstellen durch regelmäßige Penetrationstests und Security Audits
- [ ] Einhaltung gesetzlicher, verträglicher Vorgaben und Sicherheitsstandards (z. B. ISO 27001, TISAX)

DIGITAL TRANSFORMATION

3. Access Control & Kryptographie

- [ ] Prinzip der minimalen Rechte (Least Privilege) für alle Benutzer implementiert
- [ ] Starke Authentifizierung (z. B. MFA) für kritische Systeme und Anwendungen aktiviert
- [ ] Zugriffskontrollen regelmäßig überprüft und angepasst

- [ ] Verschlüsselung von Daten im Ruhezustand und bei der Übertragung sichergestellt
- [ ] Sichere Speicherung und Verwaltung von kryptografischen Schlüsseln gewährleistet

4. Beschaffung, Entwicklung, Wartung & Lieferkettensicherheit

- [ ] Sicherheitsanforderungen bei der Auswahl von Lieferanten und Dienstleistern berücksichtigt
- [ ] Vertragliche Sicherheitsanforderungen mit Lieferanten und Partnern definiert
- [ ] Sichere Entwicklungspraktiken (z. B. Secure Software Development Lifecycle) umgesetzt
- [ ] Regelmäßige Updates und Patches für Software und Systeme gewährleistet
- [ ] Überprüfung der Lieferkette auf potenzielle Schwachstellen oder Risiken

DIGITAL TRANSFORMATION

5. Personalwesen & Awareness

- [ ] Sicherheitsprüfungen für Mitarbeiter mit Zugang zu sensiblen Informationen durchgeführt
- [ ] Regelmäßige Awareness-Schulungen zur Cybersicherheit für alle Mitarbeiter implementiert
- [ ] Definition von Sicherheitsrichtlinien für den sicheren Umgang mit Unternehmensdaten
- [ ] Zugriff auf Systeme bei Austritt oder Rollenwechsel von Mitarbeitern zeitnah gesperrt
- [ ] Klare Verantwortlichkeiten und Eskalationsprozesse für Sicherheitsvorfälle definiert

6. Incident Management & BCM (Business Continuity Management)

- [ ] Notfallpläne und Business Continuity Strategien entwickelt und getestet
- [ ] **I**ncident Response Plan (IRP) vorhanden und regelmäßig überprüft
- [ ] Meldung von Sicherheitsvorfällen gemäß gesetzlichen Vorgaben sichergestellt
- [ ] Backups regelmäßig erstellt, getestet und sicher aufbewahrt
- [ ] Simulationen und Notfallübungen zur Reaktionsfähigkeit durchgeführt

DIGITAL TRANSFORMATION

NIS-2 Anforderungen in der Informationssicherheit

Mit der Einführung von NIS-2 müssen Unternehmen neue Cybersicherheitsstandards einhalten und eine Reihe von Maßnahmen ergreifen, um die Anforderungen der Richtlinie zu erfüllen. Diese Anforderungen betreffen mit NIS-2 eine größere Bandbreite an Branchen und stellen erweiterte Verpflichtungen im Bereich der Cybersicherheit dar.

Wenn Sie mehr über die Anforderungen von NIS-2 erfahren möchten, lesen Sie unseren **Blog-Beitrag zu diesem Thema**.

NIS-2 Anforderungen: Wie Unternehmen sich jetzt absichern

- Verantwortlichkeit auf Managementebene
- Maßnahmen zur Erhöhung der Widerstandsfähigkeit
- Technische und organisatorische Maßnahmen
- Erweiterte Dokumentations- und Nachweispflichten
- Angleichung und Integration mit anderen Sicherheitsstandards
- Zukünftige Entwicklungen und Anpassungsfähigkeit

Jetzt fundierte Erstberatung sichern

360 Digitale Transformation GmbH
Hettenshausenerstr. 3,
85304 Ilmmünster
https://360dt.de
info@360dt.de
+49 30 616 369 28