NIS-2-EINFÜHRUNGSLEITFADEN

Zusammenfassung

Einführung

Die NIS-2-Richtlinie (Netz- und Informationssicherheit) stellt eine wichtige Entwicklung in der europäischen Gesetzgebung zur Cybersicherheit dar. Sie erlegt einem breiten Spektrum von Organisationen, die als wesentlich oder wichtig für das Funktionieren von Gesellschaft und Wirtschaft gelten, spezifische Verpflichtungen auf. Ihre Umsetzung erfordert einen methodischen Ansatz, um die Einhaltung der Vorschriften zu gewährleisten, Cyberrisiken zu verringern und kritische Infrastrukturen zu schützen.

Dieser Leitfaden wurde erstellt, um Unternehmen bei der Umstellung auf NIS 2 zu unterstützen, wobei der Schwerpunkt auf den Unterschieden zwischen Organisationen liegt, die bereits nach ISO/IEC 27001 zertifiziert sind, und solchen, die es nicht sind. Das Ziel ist es, einen klaren und praktischen Weg für jeden Kontext zu bieten.

Teil 1: ISO-zertifiziertes Unternehmen 27001

Organisationen, die bereits nach ISO 27001 zertifiziert sind, haben einen erheblichen Vorteil, da viele der in NIS 2 geforderten Praktiken mit den Anforderungen von ISO/IEC 27001 übereinstimmen. Allerdings ist ein strategischer Ansatz erforderlich, um etwaige Lücken zu schließen und zusätzliche rechtliche Verpflichtungen zu integrieren.

Erste Vorteile für zertifizierte Unternehmen:

- Etablierte Struktur: Das Vorhandensein eines genau definierten Informationssicherheitsmanagementsystems (ISMS) erleichtert die Anpassung an die spezifischen Anforderungen der NIS 2.
- Teilweise Einhaltung: Prozesse wie Risikoanalyse, Schwachstellenmanagement und kontinuierliche Überwachung sind bereits vorhanden.
- Sicherheitskultur: Die Zertifizierung setzt ein erhöhtes internes Bewusstsein für IT-Sicherheit voraus.

Die wichtigsten Schritte zur Anpassung:

1. Abbildung der zusätzlichen Anforderungen der NIS 2: Identifizierung der Unterschiede zu den Anforderungen der ISO 27001, z. B. Lieferkettenmanagement und Berichterstattung an die zuständigen Stellen.
2. Einbindung von Interessengruppen: Verstärkte Zusammenarbeit mit Lieferanten, Partnern und Behörden, um die Anforderungen der NIS 2 in Bezug auf Berichterstattung und Widerstandsfähigkeit zu erfüllen.
3. Aktualisierung der Dokumentation: Integration bestehender Prozesse mit neuen Anforderungen, z. B. Krisenmanagement und Reaktionspläne.
4. Konformitätsprüfung: Vergleich des aktuellen Zustands des ISMS mit dem NIS-2-Rahmen, um etwaige Lücken zu ermitteln und zu beheben.