Checkliste zur NIS2-Richtlinie

Die NIS2-Richtlinie, formal „Richtlinie (EU) 2022/2555“, ist eine von der EU erlassene Rechtsvorschrift, die die Anforderungen an die IT-Sicherheit in diversen Branchen verschärft. Sie baut auf der ursprünglichen NIS-Richlinie für die Sicherheit von Netzwerken und Informationssystemen auf und hat das Ziel, die IT-Sicherheitsstandards in der gesamten EU zu verbessern.

NIS2 gilt für „wesentliche“ und „wichtige“ Einrichtungen, deren Ausfall weitreichende negative Auswirkungen auf die Wirtschaft hätte.

- „**Wesentliche**“ Einrichtungen gelten als unverzichtbar für Gesellschaft und Wirtschaft. Darunter fallen Branchen wie Energieversorgung, Gesundheitswesen, Transport und Finanzdienstleistungen.
- „**Wichtige**“ Einrichtungen sind unter anderem Post- und Kurierdienste, die Lebensmittelbranche und die chemische Industrie.

Erfüllt Ihr Unternehmen die NIS2-Vorgaben? Mithilfe dieser Checkliste können Sie prüfen, ob noch weitere Compliance-Maßnahmen erforderlich sind. Weitere NAVEX-Ressourcen zum Thema Compliance mit NIS2 finden Sie hier.

Haben Sie die folgenden Punkte schon erledigt?

- ☐ Risikomanagementmaßnahmen implementiert, unter anderem Sicherheitsprüfungen, Verschlüsselung und regelmäßige Mitarbeiterschulungen
- ☐ Zeitnahe Meldung von Cybervorfällen sichergestellt und einen klaren Ablauf definiert, wie Vorfälle erkannt, beurteilt und fristgemäß den Behörden gemeldet werden
- ☐ Steuerung, Verantwortlichkeiten, Richtlinien und Verfahren definiert, um IT-Sicherheit auf höchster Ebene Priorität einzuräumen und klare Zuständigkeiten festzulegen
- ☐ Ihre Lieferkette abgesichert und dafür die Sicherheitsmaßnahmen Ihrer Lieferanten geprüft und festgestellt, ob diese die notwendigen IT-Sicherheitsstandards erfüllen
- ☐ Maßnahmenpläne entwickelt und getestet sowie einen Geschäftskontinuitätsplan aufgestellt, der regelmäßig getestet und aktualisiert wird, um Ausfallzeiten möglichst gering zu halten
- ☐ Compliance-Tools einrichten, wie zum Beispiel die NAVEX One-Plattform

Falls Sie in einem dieser Punkte mit Nein geantwortet haben, empfehlen wir Ihnen, auf zusätzliche Ressourcen zur NIS2-Compliance zurückzugreifen. Weitere Informationen finden Sie hier.

Unternehmen, die gegen die Bestimmungen verstoßen, können zu entsprechenden Maßnahmen verpflichtet und mit Strafzahlungen belegt werden. Diese können bis zu 10 Mio. Euro oder mindestens 2 % des weltweiten Umsatzes im vorangegangenen Geschäftsjahr betragen.

Die Aufsichtsbehörden in der EU sind angehalten, die oben genannten Maßnahmen bei der Umsetzung von NIS2 mit Nachdruck zu handhaben.

Diese Inhalte dienen ausschließlich der Information. Sie stellen keine Rechtsberatung dar und sollten nicht als solche genutzt werden. Für eine Beratung, die Ihre spezifische Situation berücksichtigt, wenden Sie sich bitte an Ihren Anwalt.

Erfahren Sie mehr über NIS2-Compliance

WWW.NAVEX.COM | info@navex.com | U.S. +1 866 297 0224 | EMEA +44 (0) 20 8939 1650