NIS-2 Compliance für Unternehmen

Betroffenheit und notwendige Maßnahmen zur Compliance mit der neuen EU-weiten Richtlinie für Cybersicherheit

Mit der Novelle der Network and Information Security Richtlinie (NIS-2 Richtlinie) werden der Kreis der betroffenen Unternehmen deutlich erweitert und die Vorgaben für Cybersicherheit deutlich verschärft. Spätestens ab dem 18. Oktober 2024 müssen die Vorgaben über nationale Gesetze in den Mitgliedstaaten der EU angewandt werden.

Wer ist betroffen?

Die NIS-2 Richtlinie richtet sich an sog. „wesentliche“ und „wichtige“ Einrichtungen. Dies sind Unternehmen und Einrichtungen in insgesamt 18 Wirtschaftssektoren wie dem Energiesektor, dem Transportsektor, der digitalen Infrastruktur oder der Herstellung von Produkten. Betroffen sind bereits Unternehmen ab 50 Beschäftigten mit einem Jahresumsatz von 10 Mio. Euro. Teilweise können Unternehmen auch aufgrund anderer Kriterien als wesentlich bzw. wichtig qualifiziert werden. In Deutschland werden nach diesen Kriterien ca. 30.000 bis 40.000 Unternehmen erfasst, von denen Schätzungen zufolge derzeit noch knapp 80 % nicht wissen, dass sie betroffen sind.

Was ist umzusetzen?

Die Vorgaben der NIS-2 Richtlinie lassen sich in drei Gruppen zusammenfassen. Die erste Gruppe betrifft den Bereich Governance & Awareness. Leitungsorgane müssen ergriffene Maßnahmen im Bereich der Cybersicherheit billigen und überwachen und haften für Verstöße.

Die zweite Gruppe betrifft die Durchführung von Risikomanagementmaßnahmen. Bei unternehmensbezogenen Entscheidungen und Maßnahmen sind stets die Risiken für die Netz- und Informationssysteme zu bewerten. Ermittelte Risiken müssen durch geeignete technische und organisatorische Maßnahmen beherrschbar gemacht werden.

Die dritte Gruppe von Vorgaben betrifft schließlich einzuhaltende Meldepflichten. Bei erheblichen Sicherheitsvorfällen müssen die zuständigen Aufsichtsbehörden unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach dem Vorfall informiert werden.

Was droht bei Verstößen?

Bei Verstößen drohen neben Bußgeldern auch Weisungen der Aufsichtsbehörde, die bis hin zu einer Untersagung der Wahrnehmung von Leitungsfunktionen durch die Leitungsorgane des jeweiligen Unternehmens reichen. Darüber hinaus sind öffentliche Warnungen möglich.

Unsere Unterstützung

Wir unterstützen Sie bei der Umsetzung der Anforderungen der NIS-2 Richtlinie u.a. mit folgenden Leistungen:

- Rechtliche Prüfung der Betroffenheit Ihres Unternehmens
- Ableitung der konkreten Vorgaben für Ihr Unternehmen
- Rechtliche Unterstützung bei der Umsetzung und Dokumentation
- Einführung eines Cybersecurity Compliance Managements

Next step: Kontaktaufnahme

Gerne erläutern wir Ihnen unser Vorgehen ausführlich in einem persönlichen Gespräch. Nehmen Sie jetzt unverbindlich Kontakt auf!

T + 49 681 / 859 160 0
E info@reuschlaw.de