By PwC Deutschland | 19. September 2023

NIS2 – Umsetzung der neuen EU-Vorgaben zur Cybersicherheit in Deutschland

Mit der zunehmenden Digitalisierung und Automatisierung steigt auch die Bedrohungslage durch Cyberkriminalität kontinuierlich an. Insbesondere kritische Infrastrukturen oder jene Unternehmen und Bundeseinrichtungen, die gesellschaftlich und wirtschaftlich relevante (digitale) Dienste erbringen, sind daher inzwischen einem erheblichen Cyber-Risiko ausgesetzt.

Content

Zugleich wird der Rechtsrahmen im Bereich der Cybersicherheit zunehmend komplexer. Gerade der öffentliche Sektor ist besonders betroffen, da häufig öffentliche Unternehmen Betreiber von kritischen Infrastrukturen (KRITIS) sind. Ein Ausfall bestimmter (kritischer) Anlagen und Dienste kann schwerwiegende Folgen für das Funktionieren unserer Gesellschaft, Wirtschaft und die öffentliche Sicherheit haben. Das Ausmaß der Bedrohungslage spiegelt sich in der weiter ansteigenden Zahl an Cyberangriffen auf (kritische) Infrastrukturen bzw. IT-Systeme von Unternehmen und Bundeseinrichtungen wider. Die daraus entstandenen Schäden in deutschen Unternehmen werden auf mehr als 200 Milliarden Euro allein für das Jahr 2022 geschätzt. Hiervon erfasst sind vor allem Schäden durch sogenannte Ransomware, DDoS-Angriffe und weitere Cyberattacken auf IT-Systeme der Unternehmen.

Die NIS2-EU-Richtlinie

Um im gesamten europäischen Raum ein entsprechendes Cybersicherheitsniveau gewährleisten zu können, wurde Ende 2022 durch das Europäische Parlament und den Rat der EU die zweite Fassung der Network-and-Information-Security-Richtlinie (NIS2) verabschiedet. Die NIS2 gibt den Mitgliedstaaten einen Regelungsrahmen an die Hand, der bestimmt, welche Unternehmen betroffen sind und welche Pflichten diese Unternehmen zu erfüllen haben, um ein ausreichendes Cybersicherheitsniveau gewährleisten zu können. Die Länder sind dazu verpflichtet, die Richtlinie bis zum 17. Oktober 2024 in nationales Recht umzusetzen.

Das NIS2-Umsetzungsgesetz

In Deutschland werden die Regelungen der NIS2 mit dem NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) in nationales Recht umgesetzt. Jüngst wurde dazu der Referentenentwurf des BMI veröffentlicht, der einen Ausblick gibt, wie betroffene Unternehmen identifiziert werden sollen und welche Pflichten auf diese Unternehmen zukommen. Erste Schätzungen gehen davon aus, dass neben den bisher geltenden kritischen Infrastrukturen (KRITIS) künftig rund 29.000 zusätzliche Unternehmen von den Regelungen erfasst werden. Die Identifizierung und Betroffenheit der Unternehmen wird sich nach den NIS2-Maßgaben in Kritische Infrastrukturen, Anbieter digitaler Dienste, besonders wichtige Einrichtungen, wichtige Einrichtungen und Bundeseinrichtungen untergliedern.

Auch die damit einhergehenden Pflichten und die bei Verstößen zu zahlenden Bußgelder wurden maßgeblich erweitert bzw. erhöht. Bei Verstößen können nunmehr Bußgelder zwischen 100.000 und 20 Millionen Euro verhängt werden. Geschäftsführer werden stärker in die Verantwortung genommen und können zukünftig persönlich für die Umsetzung der Sicherheitsmaßnahmen in ihren Unternehmen haftbar gemacht werden.

Spätestens ab Inkrafttreten der nationalen Regelungen durch das NIS2UmsuCG gilt es daher für Unternehmen, eine sogenannte Betroffenheitsanalyse durchzuführen, um zu prüfen, ob sie von dem Anwendungsbereich der NIS2 erfasst sind. Im zweiten Schritt sind ggf. die entsprechenden Pflichten zu identifizieren, die die Unternehmen nach der jeweilig einschlägigen Kategorisierung zu erfüllen haben. Mit

Durchführung der Betroffenheitsanalyse kommt die Geschäftsführung ihren Pflichten hinsichtlich der Erfüllung einer ordnungsgemäßen Cyber Compliance nach.

Sind Sie an Details interessiert? Unser Experte **Dr. Nicolas Sonder** berät Sie gerne.

Schlagwörter

Gesetzgebung