TaylorWessing

NIS2-Richtlinie: Neue IT-Sicherheits-anforderungen auf EU-Ebene

Mit der sogenannten **NIS2-Richtlinie** hat die EU ihre IT-Sicherheitsanforderungen aktualisiert. Im Vergleich zur früheren NIS(„1")-Richtlinie enthält die NIS2-Richtlinie weitaus detailliertere **Anforderungen an die IT-Sicherheit,** und der **Kreis** der erfassten Einrichtungen wurde erheblich **ausgeweitet**. Unternehmen sollten daher genau prüfen, ob sie der NIS2-Richtlinie unterliegen und welche Maßnahmen sie ergreifen müssen. Im Überblick die wesentlichen Aspekte der NIS2-Richtlinie:

1 **Eine umfassende Regelung der IT-Sicherheits-pflichten auf EU-Ebene** soll zu einer stärkeren Harmonisierung innerhalb der EU und zu mehr IT-Sicherheit führen

2 **Eine breite Abdeckung von Wirtschaftssektoren** soll angesichts der aktuell bestehenden Risiken eine umfassende IT-Sicherheit in kritischen Bereichen der Gesellschaft gewährleisten

3 **Die** von der NIS2-Richtlinie **betroffenen Einrichtungsarten** sind:

- **Energie** (Strom, Fernwärme und -kälte, Erdöl, Erdgas und Wasserstoff), z. B. Stromversorger, Stromerzeuger oder Übertragungs- und Verteilernetzbetreiber
- **Verkehr** (Luft, Schiene, Schifffahrt, Straßenverkehr)
- **Bankenwesen und Finanzmarktinfrastrukturen**
- **Gesundheitswesen** (z. B. Krankenhäuser, Labore, Forschungseinrichtungen, Hersteller von pharmazeutischen Erzeugnissen)
- **Trinkwasser und Abwasser**
- **Digitale Infrastruktur:**
  - Cloud Computing-Dienste
  - Rechenzentrumsdienste
  - Vertrauensdiensteanbieter
  - Internet-Infrastruktur (IXP, DNS, TLD, CDN)
  - Anbieter von Telekommunikations- und Internetdiensten
  - Managed Services und Managed Security Services Provider (auch wenn diese Dienste nur als „shared services" innerhalb eines Konzerns angeboten werden)
- **Öffentliche Verwaltung**
- **Weltraum**
- **Post- und Kurierdienste**
- **Abfallbewirtschaftung**
- **Produktion, Herstellung und Handel mit chemischen Stoffen**
- **Industrielle Produktion, Verarbeitung und Großhandel mit Lebensmitteln**
- **Herstellung von Waren:**
  - Medizinprodukte und Invitro-Diagnostika
  - Datenverarbeitungsgeräte, elektronische und optische Erzeugnisse, elektrische Ausrüstungen
  - Maschinenbau
  - Kraftwagen und Kraftwagenteile
  - Sonstiger Fahrzeugbau
- **Digitale Dienste** (Online-Marktplatzbetreiber, Online-Suchmaschinenbetreiber, Betreiber von Plattformen für soziale Netzwerkdienste)
- **Forschungseinrichtungen**

4 **Schwellenwerte:** Unternehmen in diesen Sektoren sind im Regelfall dann von der NIS2-Richtlinie betroffen, wenn sie:

- mind. 50 Mitarbeiter (vollzeitäquivalent) beschäftigen
- oder jeweils mind. 10 Mio. EUR Jahresumsatz und Jahresbilanzsumme erreichen.
- **Ausnahme für vernachlässigbare Tätigkeiten:** Wenn eine Geschäftstätigkeit im Lichte der Gesamtgeschäftstätigkeit eine untergeordnete Rolle spielt, kann sie unter Umständen außer Betracht bleiben.

- **Zurechnung im Konzern:** Die Schwellenwerte beziehen sich regelmäßig auf den Konzern, nicht nur das konkret betroffene Unternehmen.

5 **Registrierungspflicht:** Registrieren Sie Ihre Einrichtung innerhalb von drei Monaten, nachdem sie erstmals oder erneut unter die NIS2-Richtlinie fällt, bei der zuständigen Aufsichtsbehörde

6 **Die Verpflichtung zur Umsetzung umfassender Risikomanagementmaßnahmen im Bereich der Cybersicherheit** beinhaltet die Ergreifung geeigneter und verhältnismäßiger technischer, operativer und organisatorischer Maßnahmen in Bezug auf:

- Risikoanalyse und Konzepte für die Sicherheit von Informationssystemen (einschließlich der Entwicklung von Bewertungsverfahren für die Effektivität der durchgeführten Risikomanagementmaßnahmen)
- Lieferkettensicherheit
- Bewältigung von Sicherheitsvorfällen
- Business Continuity (einschließlich Backup-Management)
- Prozesse für Cyberhygiene und Schulungen im Bereich der IT-Sicherheit
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netzwerken und Informationssystemen
- Sicherheit des Personals (einschließlich Zugangskontrolle und Anlagenmanagement)
- Konzepte und Verfahren für den Einsatz von Kryptographie
- Krisenmanagement
- Verwendung von Lösungen für die Multi-Faktor- oder kontinuierliche Authentifizierung, gesicherte Sprach-, Video- und Textkommunikationskanäle sowie gesicherte Notfallkommunikationssysteme

Ihr Experte

Dr. Paul Voigt, Lic. en Derecho, CIPP/E
Partner, Berlin
+49 30 885636-408
p.voigt@taylorwessing.com

7 **Strengere Vorschriften für die Meldung von erheblichen Sicherheitsvorfällen:** Übermitteln Sie an die zuständige Behörde

- eine Frühwarnung innerhalb von 24 Stunden
- eine Meldung über den Sicherheitsvorfall innerhalb von 72 Stunden, einschließlich einer ersten Bewertung
- einen Abschlussbericht innerhalb eines Monats nach der Meldung

8 **Mögliche Unterrichtungspflichten gegenüber Vertragspartnern und Nutzern in Bezug auf:**

- erhebliche Cyberbedrohungen (einschließlich potenzieller Schutz- oder Abhilfemaßnahmen, die ergriffen werden können)
- erhebliche Sicherheitsvorfälle (die Aufsichtsbehörde kann bei öffentlichem Interesse den Vorfall zusätzlich öffentlich machen)

9 **Haftung der Leitungsorgane und besondere Pflichten:**

- Haftung der Leitungsorgane einer Einrichtung (auch gegenüber der Einrichtung) für die ordnungsgemäße Umsetzung von Risikomanagementmaßnahmen im Bereich der Cybersicherheit, einschließlich der Auswahl und Überwachung von Personal im Fall der Delegation von Aufgaben
- Verpflichtung zur regelmäßigen Teilnahme an IT-Sicherheitsschulungen

10 **Die Aufsichts- und Durchsetzungsmaßnahmen der Aufsichtsbehörden umfassen unter anderem:**

- Audits und Vor-Ort-Kontrollen
- Anforderung von Informationen
- Ernennung eines Überwachungsbeauftragten
- Vorübergehende Aussetzung von Zertifizierungen oder Genehmigungen für einen Teil oder alle von einer Einrichtung erbrachten Dienste, die unter die NIS2-Richtlinie fallen
- Antrag gegenüber der zuständigen Stelle oder dem Gericht auf eine vorübergehende Untersagung der Wahrnehmung von Leitungsaufgaben auf Geschäftsführungs- bzw. Vorstandsebene

11 **Geldbußen:** bis zu 10 Mio. EUR (in Deutschland: bis zu 20 Mio. EUR) oder 2 % des gesamten Jahresumsatzes, je nachdem, welcher Betrag höher ist