Neue EU-Cyberrichtlinie NIS-2 betrifft zahlreiche Unternehmen

HDI Global SE → Cyber

Digitale Infrastrukturen und Systeme werden immer komplexer: Ein Cyberangriff betrifft heute häufig nicht nur ein Unternehmen, sondern ganze Wertschöpfungsketten.

Cybervorfälle sind inzwischen zu einer ernsthaften Bedrohung für die globale Wirtschaft geworden. Verschärfte europäische Sicherheitsstandards sollen diese Risiken reduzieren.

Um die Cybersicherheit in Europa zu erhöhen, hat die EU deshalb am 27. Dezember 2022 die neue Cyberrichtlinie NIS-2 (Network and Information Security Directive 2) zur Sicherheit von Netz- und Informationssystemen verabschiedet und aus 2016 erweitert, welche am 16. Januar in Kraft getreten ist. Eine Vielzahl von Unternehmen muss jetzt mehr für ihre Cybersicherheit tun und dies im Ernstfall auch nachweisen. Wer das nicht kann, muss mit Geldstrafen in Millionenhöhe rechnen. **Die Umsetzung in nationales Recht hat dabei bis zum 17. Oktober 2024 zu erfolgen.**

Herausforderungen für Unternehmen

Betroffene Unternehmen werden nicht informiert und zum Handeln aufgefordert, sondern müssen sich **selbst erkundigen**, ob sie in den Anwendungsbereich fallen. Mit Blick auf den **baldigen Ablauf der Umsetzungsfrist**, gilt es dann, umgehend mit den Vorbereitungen zu beginnen und sich frühzeitig Unterstützung an Bord zu holen. Denn die neue Richtlinie ist insbesondere **für kleinere Unternehmen eine Herausforderung**, da sie oft nicht über die nötigen Ressourcen verfügen, um die Anforderungen umzusetzen. Dazu kommt, dass nun vermehrt Dienstleister und Cybersicherheitsexperten benötigt werden, deren Kapazitäten begrenzt sind.

Welche Unternehmen müssen jetzt handeln?

Während in der Vergangenheit nur einige Unternehmen gefordert waren, bestimmte Cyberregularien zu erfüllen, ist jetzt ein größerer Teil betroffen. Unternehmen mit **mindestens 50 Mitarbeitenden** und einem **Jahresumsatz oder einer Bilanzsumme von mehr als 10 Millionen Euro** können in den Anwendungsbereich der NIS-2-Richtlinie fallen, wenn sie gleichzeitig zu den wesentlichen oder wichtigen Einrichtungen gehören:

Wesentliche Einrichtungen

Energie	Verkehr & Transport	Bankwesen & Finanzmärkte	Gesundheitswesen	Trinkwasser
Abwasser	Digitale Infrastruktur	ITK-Services (B2B)	Öffentliche Verwaltung	Weltraum

■ bereits unter NIS-1 betroffen.

Wichtige Einrichtungen

Post- und Kurierdienste	Abfallwirtschaft	Produktion, Herstellung und Handel mit chemischen Stoffen	Forschungseinrichtungen
Verarbeitendes Gewerbe, Herstellung von Waren*		Produktion, Verarbeitung und Handel von Lebensmitteln	Anbieter digitaler Dienste

* pharmazeutische Erzeugnisse (NACE 21); Elektronik/optische Erzeugnisse (NACE 26/27); Maschinenbau (NACE 28); Kraftwagen und Teile/Zubehör (NACE 29/30).

Die betroffenen Einrichtungen werden künftig folgenden Pflichten unterliegen:

1 **Meldepflicht für Zwischenfälle**
Betroffene Einrichtungen müssen erhebliche Cyberincidents innerhalb von 72 Stunden an die nationalen Behörden melden. Dies ermöglicht es den Behörden, schnell auf Bedrohungen zu reagieren und die Auswirkungen zu minimieren.

2 **Sicherheitsmaßnahmen**
Betroffene Einrichtungen müssen geeignete technische und organisatorische Maßnahmen zur Gewährleistung der Cybersecurity umsetzen. Dies umfasst die Sicherung von Netzwerken und Systemen sowie die Implementierung von Sicherheitsrichtlinien.

3 **Verantwortung der Geschäftsführung**
Die Geschäftsführung ist dazu angehalten, die Umsetzung der Maßnahmen zu überwachen. Dabei haftet sie für Verstöße. Die Teilnahme an entsprechenden Schulungen ist verpflichtend und diese müssen auch den Mitarbeitenden angeboten werden.

Sanktionen bei Verstößen

Bei **Verstößen gegen die Risikomanagementmaßnahmen (Art. 21) oder Meldepflicht von Sicherheitsvorfällen (Art. 23) der NIS-2-Richtlinie**, können Geldstrafen und andere Sanktionen verhängt werden. Die Pflichten der wesentlichen Einrichtungen (s. Übersicht oben) sind grundsätzlich gleich, jedoch unterscheiden sie sich in der Intensität der Überwachung und der Höhe der Bußgelder bei Nichteinhaltung. Es drohen Höchstbeträge von **mindestens 10 bzw. 7 Millionen Euro bzw. 2 % oder 1,4 % des weltweiten Umsatzes im Vorjahr**.

Wie kann HDI hier unterstützen?

Neben dem Angebot einer klassischen Cyberversicherung hat die HDI Global SE ihr Angebot um den Bereich **„Cyber-Services"** erweitert. **Dieses Angebot richtet sich sowohl an Neu- als auch Bestandskunden.** Der Serviceumfang besteht dabei aus dem **1:1 Support** (Unterstützung und Expertise von HDI Cyber-Risikoingenieuren) und diversen vorausgewählten und geprüften Dienstleistern aus dem Spektrum der **Value Added Services**. Der Kunde profitiert hierbei von Sonderkonditionen durch bestehende Rahmenverträge mit der HDI Global SE.

Das Thema NIS-2 kann sowohl ganzheitlich als auch selektiv durch den HDI Service-Bereich unterstützt werden:

Sicherheitsanforderungen nach NIS-2 inkl. Service-Angebot der HDI Global SE

Thema	NIS-2 Vorgabe	Serviceleistung von HDI Global SE
Policies	Richtlinien für Risiken und Informationssicherheit	✔
Incident Management	Prävention, Detektion und Bewältigung von Cybervorfällen	✔
Business Continuity	BCM mit Backup Management, Disaster Recovery, Krisenmanagement	✔
Training	Cybersecurity-Hygiene	✔
Kryptographie	Vorgaben für Kryptographie und – wo möglich – Verschlüsselung	✔
Asset Management	Information Security Management System (ISMS)	✔
Authentifizierung	Einsatz von Multi-Faktor und Single-Sign-On (SSO)	✔
Notfallkommunikation	Einsatz gesicherter Systeme (Sprache, Video und Text)	✔

Weiteren Anforderungen nach NIS-2 auf Anfrage:
Supply Chain (Sicherheit in der Lieferkette), Einkauf (Beschaffung von IT- und Netzwerksystemen), Effektivität (Vorgaben zur Messung von Cyber- und Risikomaßnahmen), Personal (HR-Security), Zugangskontrolle (Zugriffskontrolle), Kommunikation (Sichere Kommunikationstools)

Sie sind sich unsicher, ob Sie als Unternehmen in den Anwendungsbereich fallen oder wissen nicht, wo und wie Sie anfangen sollen? Die HDI Cyberexperten helfen Ihnen gerne bezüglich Fragen zur neuen Cyberrichtlinie und entwickeln gemeinsam mit Ihnen einen Plan mit konkreten Handlungsempfehlungen.

Ihre Ansprechpartner:

Larissa Schrader
Head of Cyber
Risk Engineering Services
Larissa.Schrader@hdi.global

Florian Köhler
Risk Engineering Services
Cyber & Financial Lines
Florian.Koehler@hdi.global

HDI Global SE
HDI-Platz 1
30659 Hannover
www.hdi.global

404-FL026-202404