Gemeinsamkeiten und Unterschiede zwischen NIS2 und DORA

In den letzten Jahren hat die Europäische Union ihre Cyber-Resilienz durch zwei zentrale Regelwerke deutlich gestärkt: die NIS2-Richtlinie und den Digital Operational Resilience Act (DORA). Beide zielen darauf ab, Schäden durch Cyberangriffe und IT-Störungen zu begrenzen, verfolgen jedoch unterschiedliche Ziele und gelten für verschiedene Sektoren.

Für Sicherheits- und Risikoverantwortliche ist es entscheidend, sowohl die Gemeinsamkeiten als auch die Unterschiede dieser Regelwerke zu verstehen. Diese Klarheit ermöglicht fundierte Investitionsentscheidungen, die Gestaltung robuster Governance-Modelle und die Vermeidung von Compliance-Lücken, die zu regulatorischen Risiken führen können.

Wer fällt unter die DORA- und NIS2-Konformität?

Der Digital Operational Resilience Act (DORA) richtet sich in erster Linie an den Finanzsektor. Die Vorgaben gelten für Banken, Versicherungen, Zahlungsdienstleister, Wertpapierfirmen und andere Finanzinstitute, die unter EU-Finanzmarktregulierungen fallen. Darüber hinaus erstreckt sich DORA auch auf kritische Drittanbieter, die diese Institute unterstützen, etwa Anbieter von Risikomanagement-Software oder Penetrationstests.

Im Gegensatz dazu hat NIS2 einen deutlich breiteren Anwendungsbereich und umfasst zahlreiche Sektoren. Die Richtlinie gilt für wesentliche Einrichtungen wie Energie-, Verkehrs-, Gesundheits- und Wasserversorgungsunternehmen sowie für wichtige Einrichtungen, darunter Hersteller, Anbieter digitaler Infrastrukturen und Cybersicherheitsunternehmen.

Im Kontrast dazu ist NIS2 nicht auf einen einzelnen Sektor beschränkt, sondern konzentriert sich auf Branchen, die für das Funktionieren der Gesellschaft von zentraler Bedeutung sind.

Wie wirken sich NIS2 und DORA auf Ihr Unternehmen aus?

Mit NIS2 und DORA rückt das Risikomanagement in den Mittelpunkt der Unternehmensaktivitäten, da beide Regelwerke eine proaktive Identifikation und Minimierung von Cyber- und Betriebsrisiken verlangen. Sie erhöhen zudem die Verantwortung der Führungsebene, die direkt für die Einhaltung der Vorschriften und die Resilienz verantwortlich ist. Unternehmen müssen die geforderten Maßnahmen umsetzen, sonst drohen erhebliche Geldstrafen und Sanktionen, was zeigt, dass verpflichtende Compliance sowohl eine rechtliche als auch strategische Notwendigkeit darstellt.

www.patecco.com | Lothringer Straße 36 | 44805 Bochum |+49 (0) 23 23 - 9 87 97 96 | info@patecco.com

NIS2- und DORA-Gemeinsamkeiten

Gemeinsamer Fokusbereich	NIS2	DORA
Cybersicherheitsstandards	Erfordert strenge technische und organisatorische Maßnahmen zum Schutz von Netzwerken und Informationssystemen	Verlangt strenge Sicherheitskontrollen zum Schutz der Finanzsysteme
Risikomanagement und Governance	Etabliert ein risikobasiertes Sicherheitsmanagement und die Verantwortlichkeit der Führungskräfte	Erfordert formelle Risikomanagement-Rahmenwerke und Aufsicht auf Vorstandsebene
Vorfallmeldung	Legt strenge Fristen für die Meldung schwerwiegender Cybervorfälle an die Behörden fest	Legt detaillierte und zeitlich festgelegte Meldepflichten für ICT-Vorfälle fest
Operative Resilienz	Fokus auf die Sicherstellung der kontinuierlichen Betriebsfähigkeit wesentlicher und kritischer Einrichtungen	Legt den Schwerpunkt auf digitale Betriebs Resilienz und die Wiederherstellbarkeit von Systemen
Regulatorische Aufsicht	Durch nationale Aufsichtsbehörden mit Sanktionsbefugnis durchgesetzt	Unter Aufsicht der EU und nationaler Finanzaufsichtsbehörden mit Sanktionsmechanismen

NIS2- und DORA-Unterschiede

Aspekt	NIS2	DORA
Art der Gesetzgebung	EU-Richtlinie, die einen Mindeststandard festlegt und in nationales Recht umgesetzt werden muss, bevor sie für Unternehmen gilt	EU-Verordnung, die Pflichtvorgaben direkt definiert und ohne nationale Umsetzung sofort für Unternehmen anwendbar ist.
Anwendungsbereich	Gilt für wesentliche und wichtige Unternehmen in mehreren kritischen Sektoren	Gilt in erster Linie für Finanzinstitute und ihre kritischen IKT-Drittanbieter.
Fokus und Zweck	Stärkt die allgemeine Cybersicherheit und Widerstandsfähigkeit kritischer Dienste in der gesamten EU	Gewährleistet digitale operative Resilienz speziell im Finanzsektor
Kernkomponenten	Cyber-Risikomanagement, Vorfallmeldung, Governance-Verpflichtungen und Aufsicht	ICT-Risikomanagement, Resilienz Tests, Vorfallmeldung und Überwachung von Drittanbietern
Compliance-Ansatz	Risikobasiert und ergebnisorientiert, von den nationalen Behörden durchgesetzt	Vorgeschrieben und harmonisiert, mit direkter Aufsicht

www.patecco.com | Lothringer Straße 36 | 44805 Bochum |+49 (0) 23 23 - 9 87 97 96 | info@patecco.com