Swiss GRC AG

10.12.2025 – 08:00 Uhr

NIS2 tritt in Deutschland in Kraft: Eine fachliche Einordnung mit Blick auf über 30.000 betroffene Unternehmen

Frankfurt (ots) -

NIS2 erhöht die regulatorischen Anforderungen an Risikosteuerung, Meldeverfahren und Dokumentationspflichten und leitet damit einen substanziellen Wandel in der Sicherheitsarchitektur vieler Unternehmen ein.

Mit der Umsetzung der NIS2-Richtlinie gelten in Deutschland ab sofort deutlich erweiterte Anforderungen an Cybersicherheit, Risikomanagement und organisatorische Steuerung. Über 30.000 Unternehmen müssen künftig nachweisen, wie sie Risiken bewerten, Verantwortlichkeiten zuweisen und Sicherheitsvorfälle strukturiert melden.

Während die öffentliche Diskussion bisher vor allem technische Maßnahmen betonte, zeigt eine fachliche Betrachtung: NIS2 verlangt eine umfassende organisatorische Neuaufstellung, die weit über reine IT-Themen hinausgeht.

Die Richtlinie verlangt ein systematisches **Risikomanagement (Art. 21)**, klare **Verantwortlichkeiten der Unternehmensleitung (Art. 20)** und **verbindliche Meldepflichten bei Sicherheitsvorfällen (Art. 23)**. Dazu gehören Maßnahmen für Cyber-Hygiene, Supply-Chain Security, Business Continuity und Krisenreaktion sowie strukturierte Sicherheits- und Governance-Prozesse.

"Viele Anforderungen aus NIS2 greifen tief in die Steuerungs- und Verantwortungsstrukturen von Unternehmen ein", erklärt Dr. Fino Scholl, Geschäftsführer der in Frankfurt ansässigen Swiss GRC Germany GmbH. "Entscheidungen sind nachvollziehbar zu dokumentieren, Risiken systematisch zu bewerten und Verfahren zum Umgang mit sicherheitsrelevanten Vorfällen dauerhaft vorzuhalten. Dies stellt einen grundlegenden regulatorischen Wandel dar, da Sicherheitsverantwortung erstmals klar formalisiert und der Leitungsebene als Aufsichtspflicht zugewiesen wird."

Nach Einschätzung von Swiss GRC besteht die zentrale Herausforderung darin, Risikobewertungen, Maßnahmenumsetzung, Meldewege und Kontinuitätsverfahren in eine konsistente und prüfbare Struktur zu überführen. Viele Organisationen beginnen erst jetzt damit, diese Vorgaben methodisch zu operationalisieren und verbindliche Abläufe zu etablieren.

Die von Swiss GRC entwickelte GRC Toolbox unterstützt Unternehmen dabei, die NIS2-relevanten Anforderungen strukturiert abzubilden - von Risikobewertungen über Maßnahmenverfolgung und ISMS-Bausteine bis hin zu Workflows für den Umgang mit sicherheitsrelevanten Vorfällen und einer auditfesten Dokumentation.

"NIS2 schafft eine neue Erwartungshaltung an Governance und Transparenz", betont Gentian Ajeti, Chief Customer & Commercial Officer bei Swiss GRC. "Strukturierte Prozesse und verlässliche Nachweise werden künftig entscheidend sein - nicht nur für die Compliance, sondern für die gesamte Cyberresilienz eines Unternehmens."

Mit Inkrafttreten der Richtlinie gewinnen Themen wie Verantwortlichkeitszuordnung, Prozessdokumentation und Risikoüberwachung erheblich an Bedeutung. Frühzeitig strukturierte Umsetzungen stärken nicht nur die Compliance, sondern auch die langfristige Cyberresilienz.

Weitere Informationen zur praktischen Umsetzung der NIS2-Anforderungen: **www.swissgrc.com/nis2**

Pressekontakt:

Yahya Mohamed Mao
yahya.mao@swissgrc.com