EU stellt Deutschland vor Cyber-Challenge: NIS-2-Richtlinie in Gefahr!

EU stärkt Cybersicherheit mit der NIS-2-Richtlinie, die erweiterte Pflichten für Unternehmen und öffentliche Einrichtungen festlegt.

Deutschland - Die digitale Welt wird zunehmend komplexer, und mit ihr wachsen die Herausforderungen im Bereich der Cybersicherheit. Die NIS-2-Richtlinie, die am 16. Januar 2023 in Kraft trat, setzt einen entscheidenden Schritt in diesem Bereich. Diese europäische Richtlinie erfasst rund 30.000 Einrichtungen und Unternehmen, statt der 4.500, die 2016 unter der vorhergehenden NIS-Richtlinie standen. Ziel ist es, die Cybersicherheit innerhalb der EU erheblich zu stärken und einen einheitlichen Rechtsrahmen zu etablieren. Doch was heißt das konkret für Unternehmen und öffentliche Einrichtungen in Deutschland? Twobirds berichtet von einer ungewissen Umsetzung, da der nationale Gesetzgebungsprozess für das NIS-2-Umsetzungsgesetz aufgrund interner politischer

Schwierigkeiten noch keine Fortschritte gemacht hat.

Die Frist für die nationale Umsetzung war bereits für den 17. Oktober 2024 gesetzt, doch Deutschland hinkt hinterher. Der Koalitionsvertrag sieht eine Novellierung des BSI-Gesetzes vor, aber ein Kabinettsbeschluss steht noch aus. Ein aktualisierter Referentenentwurf wurde erst am 23. Juni 2025 veröffentlicht. Das betrifft nicht nur große Unternehmen: Die neuen Anforderungen werden auch kleinere Betriebe betreffen, die ab einer gewissen Größe oder einem bestimmten Umsatz unter die Richtlinie fallen. Nicht weniger als 18 Sektoren sind betroffen, verteilt auf „wesentliche" und „wichtige" Einrichtungen. OpenKritis hebt hervor, dass Unternehmen mit 50 oder mehr Mitarbeitern oder einem Umsatz über 10 Millionen Euro besonders gefordert sind.

Neuerungen durch NIS-2-Richtlinie

Was sind die wesentlichen Neuerungen? Zunächst einmal schlägt die NIS-2-Richtlinie mit strengen Mindestsicherheitsanforderungen zu. Einrichtungen müssen signifikante Sicherheitsvorfälle innerhalb von 24 Stunden melden, was im Falle einer Cyberattacke einen raschen und effektiven Umgang mit der Situation erfordert. Die Vorschrift erweitert auch das Pflichten- und Sanktionsregime. Bußgelder können bis zu 10 Millionen Euro betragen oder bis zu 2% des weltweiten Jahresumsatzes – da bleibt kein Platz für Nachlässigkeit.

Insgesamt wird die Cybersicherheitslage in Europa durch geopolitische Konflikte, etwa den Ukraine-Konflikt, beeinflusst. Diese Probleme machen klar, dass die Sicherheit im Cyberspace eine dringende Angelegenheit ist. Die NIS-2-Richtlinie ist nicht nur eine Antwort auf technische Bedrohungen, sondern auch auf die sich wandelnde geopolitische Landschaft. Fraunhofer IESE betont, dass Unternehmen systematisch Risiken analysieren und Notfallpläne erstellen müssen, um in der Lage zu sein, im Fall eines Vorfalls den Betrieb aufrechtzuerhalten.

Überwachung und Zusammenarbeit

Die Überwachung und Zusammenarbeit zwischen nationalen Behörden und Einrichtungen wird durch die NIS-2-Richtlinie verstärkt. Jedes Mitgliedsland muss nationale Cybersicherheitsstrategien und Computer-Notfallteams (CSIRTs) einrichten, die eine essenzielle Rolle bei der Reaktion auf Cybervorfälle spielen. Die NIS-2-Richtlinie gibt den Mitgliedstaaten bis zum 17. April 2025 Zeit, um Listen wesentlicher Einrichtungen zu erstellen. OpenKritis erwähnt zudem, dass dieser Rahmen das Potenzial hat, die Cybersicherheitsmaßnahmen deutlich zu verbessern und die Attacken auf kritische Infrastrukturen, wie sie in den letzten Jahren zugenommen haben, zu reduzieren.

Wie sieht die Zukunft aus? Die Transparenz und Kontrolle über Sicherheitsmaßnahmen müssen in den Geschäftsbeziehungen, insbesondere innerhalb der Lieferketten, kontinuierlich verbessert werden. Unternehmen sind aufgefordert, technische Lösungen wie Kryptografie und Multi-Faktor-Authentifizierung zu implementieren und Schulungen zur „Cyberhygiene“ durchzuführen. NIS-2 verpflichtet Einrichtungen, wie Banken oder die öffentliche Verwaltung, einen proaktiven Ansatz zur Cybersicherheit zu verfolgen – da liegt was an.

Die NIS-2-Richtlinie ist letztlich ein Aufruf an alle, die sich in der digitalen Welt bewegen. Ja, die Herausforderungen sind groß, aber Chancen für eine robuste Cybersicherheitsarchitektur sind für diejenigen, die bereit sind zu investieren, überall sichtbar. Bleiben Sie dran und halten Sie Ihre Infrastruktur sicher – es ist nicht nur eine rechtliche Verpflichtung, sondern auch entscheidend für das Überleben in der digitalen Ära.

Details	
Ort	Deutschland
Quellen	• www.twobirds.com

Details	
	• www.openkritis.de • www.iese.fraunhofer.de