KPMG
Law

KPMG

NIS-2: Für ein höheres Sicherheitsniveau in Europa

Herausforderungen, Chancen, Lösungen

Inhalt

Einleitung

NIS-2 ist die Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Europäischen Union (EU). Das Ziel der NIS-2-Richtlinie ist es, ein einheitliches Schutzniveau für Netzwerk- und Informationssysteme kritischer Infrastrukturen zu schaffen.

Mit der NIS-2-Richtlinie wurde die Zahl der kritischen Sektoren im Vergleich zur im Jahr 2016 verabschiedeten NIS-Richtlinie um elf Sektoren erweitert und genauer definiert.

Die NIS-2-Richtlinie ist seit dem 16. Januar 2023 in Kraft und hätte bis zum 17. Oktober 2024 in nationales Recht umgesetzt werden müssen. In Deutschland wurde die geplante Umsetzung jedoch nicht fristgerecht abgeschlossen, sodass die Europäische Kommission ein Vertragsverletzungsverfahren eingeleitet hat.

Trotz der ausstehenden nationalen Umsetzung bietet die NIS-2-Richtlinie bereits heute konkrete Anforderungen, die Unternehmen zum Schutz ihrer Netzwerk- und Informationssysteme umsetzen sollten.

NIS-2 wird konkreter und betrifft mehr Unternehmen

Die NIS-2-Richtlinie birgt neben den umfangreichen Risikomanagement-Maßnahmen ein Bußgeldrisiko sowie ein erhebliches Haftungsrisiko für die Unternehmensleitung.

Unternehmen sollten jetzt handeln und auf Basis der vorliegenden Richtlinie die Betroffenheit und ihre NIS-2-Readiness bewerten. Die interdisziplinären KPMG-Experten und -Expertinnen unterstützten Sie gerne mit Ihrer Better Practice bei der Betroffenheitsanalyse sowie der Planung und Umsetzung der NIS-2-Anforderungen.

Sektorenausweitung

Durch die Ausweitung des Anwendungsbereichs auf neue Sektoren wird das Cybersicherheitsniveau von deren betroffenen Einrichtungen auf die Probe gestellt.

Zahlreiche Anforderungen

Diese Erweiterung bringt zahlreiche Anforderungen mit sich, die von der Organisation über die Personalsicherheit bis hin zu technischen Fähigkeiten reichen.

Umfangreiche Governance-Anforderungen

Es ist zu erwarten, dass umfangreiche Governance-Maßnahmen bezüglich der Sicherheit im Betrieb zu etablieren sind und in der Verantwortung der Unternehmensleitung liegen.

Befugnisse der Behörden

Die Befugnisse der zuständigen Aufsichtsbehörden wurden erweitert, was eine engere Zusammenarbeit zwischen Privatwirtschaft und Staat fordert. Für die Nichterfüllung der Anforderungen durch die betroffenen Einrichtungen sieht die NIS-2-Richtlinie Bußgelder von bis zu 10 Millionen Euro oder 2 % des weltweiten Jahresumsatzes vor, je nach dem, was höher ist.

Better Practices zur Vorbereitung und Umsetzung

Die neuen NIS-2-Vorgaben erfordern eine intensive Vorbereitung, beginnend mit einer Analysephase zur Feststellung der **Betroffenheit** eines Unternehmens und einem **Readiness Assessment** in den betroffenen Kernbereichen.

Auf dieser Grundlage können notwendige **Maßnahmen** festgelegt und effektiv umgesetzt werden. Maßnahmenpakete wie Governance, Berichterstattung und regulatorisches Monitoring sowie Workshops und Schulungen sorgen für eine anforderungsgerechte Umsetzung. Dies ist insbesondere vor dem Hintergrund der Geschäftsleitungshaftung unter NIS-2 relevant.

Auf Basis und als Ergebnis unserer vorstehend skizzierten Analyse erhalten Sie von uns einen Risiko-Bericht, der konkret aufzeigt, inwieweit Ihr Unternehmen von der NIS-2-Richtlinie betroffen ist, welche Bereiche besonders kritisch sind und welche Maßnahmen ergriffen werden sollten.

Der Bericht enthält den Vorschlag eines konkreten Maßnahmenplans zur Anpassung an die Anforderungen der Richtlinie, einschließlich technischer, organisatorischer und rechtlicher Schritte. Dadurch reagieren Sie gezielt auf die Anforderungen der NIS-2-Richtlinie und bereiten sich rechtzeitig auf die neuen Pflichten vor.

Fünf Schritte der Betroffenheitsanalyse

Betroffenheitsanalyse

Eine Betroffenheitsanalyse ist der erste Schritt, um in NIS-2-regulierten Sektoren direkte und indirekte Betroffenheiten zu konkretisieren. Dabei werden betroffene Einheiten, Geschäftsprozesse und verbundene Services unter Berücksichtigung übergreifender Prozesse, Lieferanten und Kunden ermittelt und damit der Betroffenheitsgrad identifiziert. Nutzen Sie unser Quick Assessment, um eine erste Einschätzung zu Ihrer Betroffenheit zu erhalten.

Readiness Assessment

Das Readiness Assessment bildet die Basis für einen Maßnahmenplan. Das Ziel des Assessment ist es, zu prüfen, wie das Unternehmen auf die kommenden Herausforderungen eingestellt ist und welche Maßnahmen noch notwendig sind.

NIS-2-Governance

Sicherstellen einer effizienten Steuerung der NIS-2-Maßnahmen zur effektiven Erfüllung der Anforderungen.

Berichterstattung an die Behörden

Design des Prozesses zur verpflichtenden Berichterstattung an die entsprechende Aufsichtsbehörde auf Basis bestehender Prozesse und Systeme für das Vorfalls- und Krisenmanagement.

NIS-2-Maßnahmen-Umsetzung

Unterstützung bei der effektiven Einhaltung der NIS-2-Richtlinie und Umsetzung aller notwendigen Maßnahmen und Anforderungen (wie z. B. IAM, Incident Response oder BCM).

Workshops und Schulungen

Durchführung von Schulungen und Workshops mit erfahrenen und interdisziplinären Experten und Expertinnen mit umfassenden Kenntnissen in den Bereichen Recht, Datenschutz, Audit/Revision, Cyber Security und Technologie.

Regulatory Monitoring in der Umsetzung

Das Ziel des Regulatory Monitoring ist es, die nationalen Besonderheiten wie zum Beispiel die regulatorische, behördliche Praxis in die Umsetzung einzubringen.

Risiko Geschäftsleitungshaftung unter NIS-2

Der Haftungsmaßstab des aktuellen Entwurfs des deutschen Umsetzungsgesetzes folgt dem Rahmen der NIS-2-Richtlinie. Bereits jetzt haften in Deutschland die Geschäftsleitungen, wenn sie grob fahrlässig gegen Pflichten zur Sicherstellung der IT-Sicherheit verstoßen.

Durch konkrete Normierung von Pflichten in der NIS-2 erhöht sich das faktische Haftungsrisiko für die Geschäftsleitungen signifikant. Wenn eine konkret benannte Pflicht nicht umgesetzt wird, liegt eine Pflichtverletzung nahe.

Aufgrund des konkretisierten Pflichtenkanons erhöht sich gleichzeitig das Risiko, dass Pflichtverletzungen auch als grob fahrlässig anzusehen sind.

Die EU bestätigt und festigt mit der NIS-2-Richtlinie somit die Haftung der Geschäftsleitungen („IT-Sicherheit ist Chefsache“).

Wer zählt zur Geschäftsleitung?

Bundesvorstand, die jeweiligen Vorstände und Direktorien/Geschäftsführungen der Träger sowie die Geschäftsführungen von Tochtergesellschaften.

Pflichtenkanon einer Geschäftsleitung

Gesetzlicher Maßstab ist die Verletzung der Sorgfalt IT-Sicherheit. Entsprechende Risikomanagement-maßnahmen (auch ohne Inkrafttreten des Umsetzungsgesetzes) gehören zum Pflichtenkanon einer Geschäftsleitung. Aufgrund der gemeinhin zunehmenden Bedrohungslage und der entsprechenden gesetzlichen Adressierung gilt dies in einem erhöhten Maße.

Haftungsmaßstab

Gesetzlicher Maßstab ist die Verletzung der Sorgfalt eines „ordentlichen und gewissenhaften Geschäftsleiters“ im Fall einer Aktiengesellschaft (AG) beziehungsweise „eines ordentlichen Geschäftsmannes“ im Fall einer Gesellschaft mit beschränkter Haftung (GmbH). Damit kann bereits einfache Fahrlässigkeit genügen.

Grobe Fahrlässigkeit

Je konkreter die Verhaltenspflichten geregelt sind, desto näher liegt der Vorwurf einer groben Fahrlässigkeit. Insbesondere, wenn es gesetzliche Regelungen gibt, die sich ausdrücklich an die Geschäftsleitung richten.

Risiko

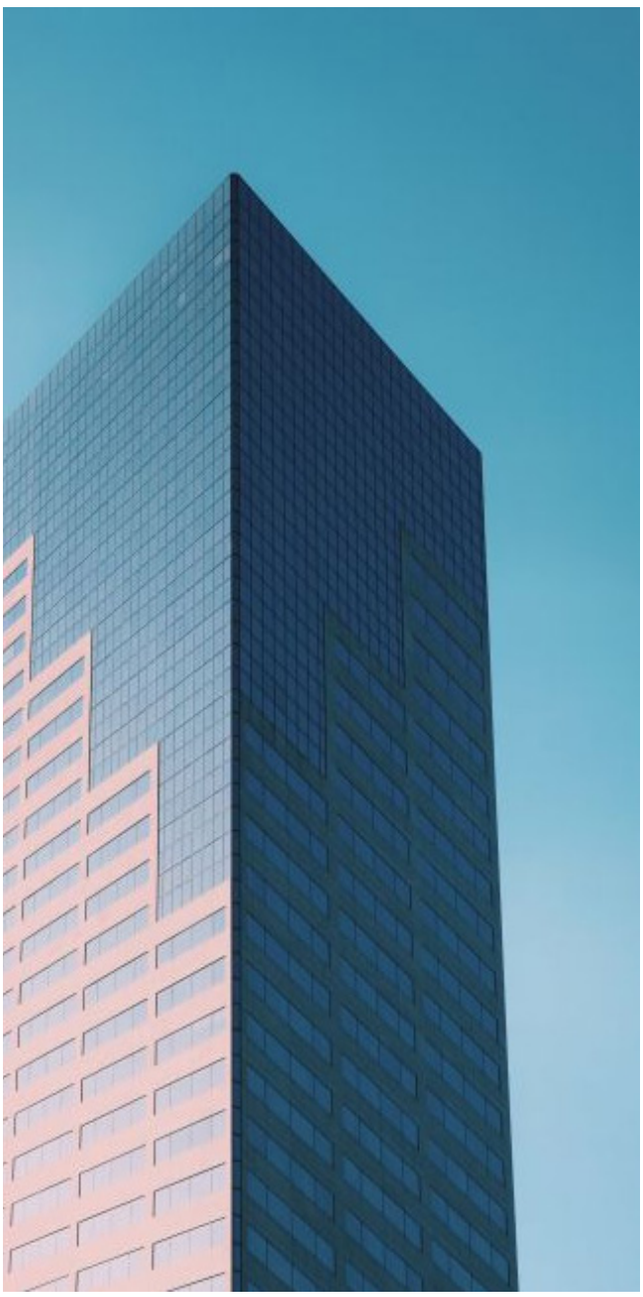
Sofern die Geschäftsleitung bei einer unternehmerischen Entscheidung nicht vernünftigerweise annehmen durfte, auf der Grundlage angemessener Informationen zum Wohle der Gesellschaft gehandelt zu haben, wird die Sorgfaltspflicht verletzt. Damit muss nachweislich eine sorgfältige und interessengerechte Entscheidung – unter Berücksichtigung der IT-Sicherheit – getroffen worden sein.

NIS-2-Richtlinie: Verantwortung auch ohne nationales Umsetzungsgesetz

Die NIS-2-Richtlinie setzt neue Maßstäbe für die Cybersicherheit und sollte bis zum 17. Oktober 2024 in nationales Recht umgesetzt werden. Da die Umsetzung in Deutschland nicht fristgerecht abgeschlossen wurde, bleibt die rechtliche Situation unklar – die Anforderungen der Richtlinie bestehen jedoch weiterhin.

Durch das Inkrafttreten der Umsetzungsgesetze in vielen Ländern der EU dürften die Pflichten für viele Unternehmen bereits gelten. Auch in Deutschland können konkrete Anforderungen an Cybersicherheit aus NIS-2 bereits aufgrund des am Stand der Technik und an allgemein anerkannten Standards auszurichtenden Sorgfaltsmaßstabs zum Tragen kommen, sodass NIS-2 faktisch bereits Wirkung unabhängig von einem nationalen Umsetzungsgesetz entfalten kann. Unternehmen sollten sich daher nicht auf eine verzögerte Gesetzgebung verlassen, sondern sich frühzeitig mit den bestehenden Vorgaben auseinandersetzen.

Die NIS-2-Richtlinie macht die Umsetzung der Cybersicherheit zur unternehmerischen Pflicht. Wer frühzeitig Maßnahmen ergreift, kann nicht nur regulatorische Risiken minimieren, sondern vor allem die Resilienz des eigenen Unternehmens stärken.



Unmittelbare Wirkung

Konkrete Anforderungen an Cybersicherheit aus der NIS-2-Richtlinie wirken bereits jetzt aufgrund des am Stand der Technik und an allgemein anerkannten Standards auszurichtenden Sorgfaltsmaßstabs, welcher für die Beurteilung der persönlichen Haftung der Geschäftsleitung zum Tragen kommen wird. Im Fall von Security-Vorfällen stellen sich unmittelbar rechtliche Haftungsfragen – auch im Zusammenhang mit den Maßgaben des Datenschutzes.

Konkrete Anforderungen aus NIS-2

Zu den bereits umzusetzenden Maßnahmen zählen insbesondere die Durchführung regelmäßiger Risikoanalysen, die Implementierung technischer und organisatorischer Cybersicherheitsmaßnahmen (z. B. Firewalls, Intrusion Detection System (IDS)/Intrusion Response System (IRS), Verschlüsselung), die Etablierung eines Vorfallmanagementsystems sowie die Dokumentation und Nachweisführung über diese Maßnahmen, selbst wenn das Gesetz noch nicht in Kraft ist.

Verantwortung der Unternehmen

Frühzeitige, angemessene Umsetzung schützt vor regulatorischen Unsicherheiten.

Klare interne Prozesse zur Erfüllung der Anforderungen sind entscheidend.

Risiken bei Untätigkeit

Verzögerungen erhöhen die Gefahr von Compliance-Risiken. Das deutsche NIS-2-Umsetzungsgesetz wird voraussichtlich keine Übergangsfristen für die Umsetzung der Pflichten enthalten. Sobald das Gesetz in Kraft tritt, gelten die NIS-2-Pflichten unmittelbar für betroffene Unternehmen.

Warum KPMG?

KPMG unterstützt Organisationen dabei, die Komplexität der NIS-2-Richtlinie sowie der entsprechenden Umsetzungsgesetze zu bewältigen.

KPMG Law steht für umfassendes juristisches Fachwissen kombiniert mit fundierten Branchenkenntnissen und einem globalen Netzwerk.

Unsere Anwälte und Anwältinnen verfügen über fundierte Kenntnisse in den Bereichen IT-Recht, Datenschutz und Cybersicherheit. Unsere Kunden profitieren von unserer Fähigkeit, komplexe technologische Fragen in einen klaren rechtlichen Rahmen zu übersetzen und dabei stets die Unternehmensziele im Auge zu behalten.

KPMG bietet eine umfassende Beratung an, um Ihre Netzwerk- und Informationssicherheit zu stärken.

Unsere Cyber-Security-Experten und -Expertinnen bieten Ihnen eine umfassende Beratung und Unterstützung in Bezug auf NIS-2, Cyber Resilience Act (CRA) sowie Cyber Incidents.

Wir führen Risikobewertungen durch, implementieren maßgeschneiderte Sicherheitslösungen und schulen Ihr Personal, um die Cybersicherheit Ihres Unternehmens zu stärken.

Gemeinsam

Die enge Zusammenarbeit zwischen KPMG und KPMG Law ermöglicht es, die rechtlichen Anforderungen praktisch zu übersetzen und umzusetzen sowie umgekehrt Erkenntnisse aus der Beratung nahtlos in die rechtlichen Strategien zu integrieren. Damit kann eine ganzheitliche Sicht auf die Risikolandschaft und die Compliance-Anforderungen unserer Kunden erreicht werden. Dieser kooperative Ansatz hat sich als besonders effektiv erwiesen, da er unseren Kunden nicht nur hilft, Compliance-Anforderungen zu erfüllen, sondern auch, ihre Geschäftsprozesse zu optimieren und ihre Wettbewerbsfähigkeit zu stärken.

Durch unser fundiertes Fachwissen und unser Engagement für Spitzenleistungen können wir unseren Kunden nicht nur Rechtssicherheit bieten, sondern auch einen echten strategischen Vorteil in einem zunehmend komplexen und wettbewerbsintensiven Marktumfeld. KPMG bietet Lösungen für Organisationen, die sich den dynamischen Herausforderungen von Cybersicherheit, Datenschutz und Compliance stellen müssen.

Kontakt

KPMG Law
Rechtsanwaltsgesellschaft mbH

Francois Maartens Heynike
LL.M. Rechtsanwalt, Partner
Technology, Media & Telecommunication
T +49 69 95119-5770
fheynike@kpmg-law.com

Dr. Daniel Taraz,
Rechtsanwalt, Senior Manager
IT/Data/Digital
T +49 40 360994-5483
danieltaraz@kpmg-law.com

KPMG AG
Wirtschaftsprüfungsgesellschaft

Wilhelm Dolle
Consulting,
Cyber Security & Resilience
T +49 30 2068-2323
wdolle@kpmg.com

Marko Vogel
Partner
Consulting, Cyber Security & Resilience
T +49 201455-8838
mvogel@kpmg.com

Dr. Michael Falk
Partner
Consulting, Cyber Security & Resilience
T +49 69 9587-3680
mfalk@kpmg.com

Jan Stoelting
Partner
Consulting, Cyber Security & Resilience
T +49 711 90604-2774
jstoelting@kpmg.com

kpmg.de/socialmedia

kpmg.de