finlex.io

Finlex

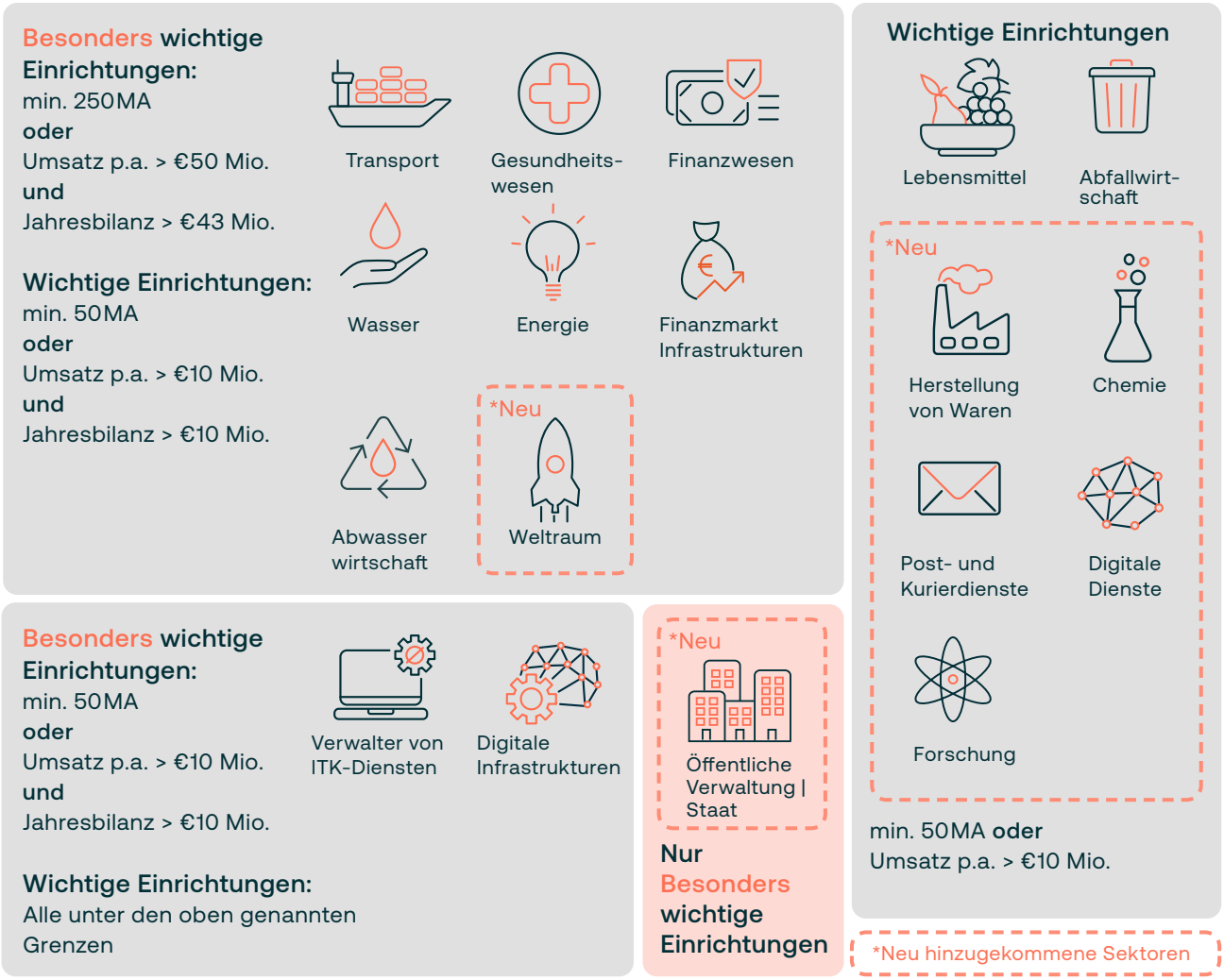
NIS-2-Richtlinie zur Netzwerk- und Informationssicherheit

Was ist NIS-2?

- Die NIS-2-Richtlinie (EU 2022/2555) ist eine EU-Richtlinie, die darauf abzielt, die Cybersicherheit von Unternehmen innerhalb der EU zu harmonisieren und zu verbessern und so die Sicherheit und das Vertrauen in digitale Dienste und Infrastrukturen in der Europäischen Union zu gewährleisten. Sie ersetzt die frühere NIS-Richtlinie von 2016 und stellt höhere Anforderungen an die Sicherheit von Netzwerk- und Informationssystemen.
- Die neue Regulierung betrifft deutlich mehr Unternehmen als die bisherige NIS-Richtlinie. Der Anwendungsbereich wurde auf zusätzliche Sektoren erweitert, um die Widerstands- und Handlungsfähigkeit sowohl staatlicher als auch nichtstaatlicher Akteure zu stärken.
- Die EU-Richtlinie wird durch die Mitgliedstaaten in nationales Recht umgesetzt. In Deutschland erfolgt dies durch das NIS-2-Umsetzungsgesetz (NIS2UmsuCG), das im Oktober 2024 in Kraft treten soll.

Übersicht der NIS-2-Sektoren

Neben den bestehenden 5.000 KRITIS-Unternehmen in Deutschland betrifft die NIS-2-Richtlinie auch weitere Sektoren. NIS-2 unterscheidet dabei zwischen „Wichtigen Einrichtungen“ und „Besonders wichtigen Einrichtungen“, wobei die Einteilung sowohl von der Sektor-Zugehörigkeit, als auch von der Unternehmensgröße (sog. Size-Cap Regelung) abhängt.



Wichtig: Eine Aufforderung durch die Aufsichtsbehörden erfolgt nicht. Unternehmen müssen eigenständig prüfen, ob sie unter NIS-2 fallen. Hierzu kann die NIS-2-Betroffenheits-prüfung des Bundesamts für Sicherheit in der Informationstechnik (BSI) genutzt werden.

Zur Prüfung

Wie ist der Zeitplan für die Umsetzung?

Die NIS-2-Richtlinie wurde im Dezember 2022 verabschiedet und ist seit dem 16. Januar 2023 in Kraft. Die EU-Mitgliedstaaten müssen diese Richtiline bis zum 17. Oktober 2024 in nationales Recht umsetzen. Ob diese zeitliche Umsetzungsfrist in Deutschland eingehalten

werden kann, ist aktuell (Stand September 2024) allerdings ungewiss. Der aktuelle Gesetzentwurf des NIS-2-Umsetzungsgesetzes (NIS2UmsuCG) lässt eine Umsetzung in nationales Recht erst Anfang 2025 vermuten. Die nationale Gesetzgebung wird spezifische Anforderungen an die Registrierungs-, Umsetzungs- und Nachweispflichten festlegen.

Eine Übergangsfrist für die Umsetzung der Maßnahmen ist derzeit nicht vorgesehen. Unternehmen sollten sich daher umgehend mit den bekannten Anforderungen und Pflichten vertraut machen.

Sanktionen und Bußgelder?

Die NIS-2-Richtlinie sieht vor, dass Unternehmen, die die festgelegten Anforderungen und Pflichten nicht erfüllen, mit Geldbußen und Sanktionen belegt werden können. Im Vergleich zur bisherigen Regulierung in Deutschland sollen die Bußgelder für Unternehmen der Kategorie „Besonders wichtige Einrichtungen“ beispielsweise auf bis zu 10 Mio. EUR oder zwei Prozent des weltweiten Jahresumsatzes erhöht werden. „Wichtige Einrichtungen“ haben mit Bußgeldern von bis zu 7 Mio. EUR oder 1,4 % des weltweiten Jahresumsatzes zu rechnen (maßgeblich ist jeweils der höhere Betrag).

Welche Anforderungen stellt NIS-2?

Die NIS-2-Richtlinie verpflichtet betroffene Unternehmen zur Einhaltung von Mindeststandards in der Cybersicherheit. Diese umfassen Risikomanagement und die Implementierung von Maßnahmen wie Richtlinien, Incident Management, Business Continuity Management, Sicherheit in der Lieferkette, Schwachstellenmanagement, Kryptographie, Personalsicherheit, Zugangskontrollen und mehr. Abhängig von der Einstufung eines Unternehmens können zusätzliche Pflichten wie verpflichtende Audits oder Registrierungs- und Meldepflichten gegenüber Aufsichtsbehörden oder der Öffentlichkeit hinzukommen.

Gänzlich neu sind die Anforderungen aus NIS-2 für Unternehmen nicht, dennoch fallen sie weitreichender als bisher aus. Dazu kommt die umgedrehte Meldepflicht der Richtlinie, was bedeutet, dass Unternehmen proaktiv prüfen müssen, ob sie unter die NIS-2-Richtlinie fallen und entsprechend Nachweise über die Sicherheitsstandards proaktiv einreichen müssen. Hier kommen demnach erhöhte Anforderungen auf die Geschäftsführung zu.

Welche Rolle spielt die Cyber-Versicherung hierbei?

Eine unmittelbare Verbindung zwischen der NIS-2-Richtlinie und der Cyber-Versicherung besteht erstmal nicht. Doch gerade in Bezug auf die gestellten Anforderungen an die

Unternehmen zeigen sich große Paralellen zwischen der NIS-2-Richtlinie und den Anforderungen, die die Cyber-Versicherer im aktuellen Marktumfeld an ihre Kunden stellen.

Das im Rahmen des Abschlusses einer Cyber-Versicherung durchgeführte Risiko-Assessment kann daher unterstützen, Lücken in der IT-Sicherheit zu identifizieren und diese gezielt anzugehen.

Mittels des Finlex Ökosystems steht Unternehmen außerdem ein umfangreiches Partner-Netzwerk zur Verfügung, das die Suche nach Dienstleistern zur Behebung der identifizierten IT-Sicherheitslücken erleichtert.

Welche Anpassungen Cyber-Versicherer auf Basis des finalen NIS-2-Umsetzungsgesetzes ggf. an ihren Produkten vornehmen – beispielsweise Angleichung der technischen Obliegenheiten an die Anforderungen der NIS-2-Richtlinie oder Harmonisierung des Risiko-Assessments – bleibt abzuwarten.

Welche Rolle spielt die D&O-Versicherung hierbei?

Die NIS-2-Richtlinie verpflichtet Mitgliedsstaaten, sicher zu stellen, dass Leitungsorgane wesentlicher und wichtiger Einrichtungen zur Einhaltung und Überwachung der Umsetzung der vorgeschriebenen Risikomanagementmaßnahmen verpflichtet sowie für Verstöße gegen die Vorschriften der NIS-2-Richtlinie verantwortlich gemacht werden können. Dies setzt die nationale Gesetzgebung um, indem sie bestimmt, dass Geschäftsleiter besonders wichtiger Einrichtungen und wichtiger Einrichtungen verpflichtet sind,

- die von diesen Einrichtungen zu ergreifenden Risikomanagementmaßnahmen im Bereich der Cybersicherheit zu billigen und
- ihre Umsetzung zu überwachen.

Die Einhaltung der mit der NIS-2-Richtlinie einhergehenden Pflichten ist also Teil unternehmerischer Compliance. Eine Regelung der Haftung erfolgt nicht spezialgesetzlich, vielmehr ergibt sich die Binnenhaftung der Leitungsorgane bei Verletzung von Pflichten nach dem BSI-Gesetz aus den allgemeinen Grundsätzen (bspw. § 93 AktG). Der Unterschied zu anderen Managerhaftungsfällen besteht aber darin, dass es den betroffen Unternehmen nach § 38 Abs. 2 BSI-Gesetz verwehrt ist, auf die Geltendmachung von Schadensersatzansprüchen gegen die handelnden Organe zu verzichten. Damit verlieren neben Verzichten auch zwischen den Leitungsorganen und den Unternehmen vereinbarte Haftungsfreistellungen oder -begrenzungen ihre Wirkung. Ein umfassender Versicherungsschutz stellt dementsprechend die einzige Möglichkeit dar, das Risiko der persönlichen Haftung von Organen zu beschränken.

Es sollte daher gewährleistet sein, dass eine D&O-Versicherung mit einem weiten Deckungsschutz, einer adäquaten Versicherungssumme und auskömmlichen Nachmeldefristen zu Gunsten der Organe betroffener Unternehmen besteht. Zur Gewährleistung eines adäquaten Versicherungsschutzes sollte diese durch eine Persönliche D&O-Versicherung, eine Strafrechtsschutzversicherung sowie eine Vertrauensschadenversicherung ergänzt werden.

Ihr Ansprechpartner bei Finlex

Für alle Fragen rund um das Thema D&O Broking steht Ihnen gerne zur Verfügung:

Beata Drenker
Vice President Management Liability
M +49 151 150 716 65
E beata.drenker@finlex.de

Für alle Fragen rund um das Thema Cyber Broking steht Ihnen gerne zur Verfügung:

Andrea Kotter
Vice President Cyber
M +49 151 150 716 78
E andrea.kotter@finlex.de

IT-Sicherheitspflichten

Auszug aus

Gesetzentwurf des Bundesministeriums des Innern und für Heimat Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz) Bearbeitungsstand: 22.07.2024

§ 30

Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

(1) Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen, die nach Absatz 2 konkretisiert werden, zu ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten. Bei der Bewertung der Verhältnismäßigkeit der Maßnahmen nach Satz 1 sind das Ausmaß der Risikoexposition, die Größe der Einrichtung, die Umsetzungskosten und die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen zu berücksichtigen. Die Einhaltung der Verpflichtung nach Satz 1 ist durch die Einrichtungen zu dokumentieren.

(2) Maßnahmen nach Absatz 1 sollen den Stand der Technik einhalten, die einschlägigen europäischen und internationalen Normen berücksichtigen und müssen auf einem gefahrenübergreifenden Ansatz beruhen. Die Maßnahmen müssen zumindest Folgendes umfassen:

1. Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik,
2. Bewältigung von Sicherheitsvorfällen,
3. Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,
4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern,
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und

Offenlegung von Schwachstellen,

6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik,
7. grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Sicherheit in der Informationstechnik,
8. Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung,
9. Sicherheit des Personals, Konzepte für die Zugriffskontrolle und für das Management von Anlagen,
10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung