NIS-2-Umsetzung kommt!

01 August 2025

Mit der NIS-2-Richtlinie (EU) 2022/2555 will die EU das IT-Sicherheitsniveau in Europa deutlich erhöhen. Die Richtlinie richtet sich neben Einrichtungen der Bundesverwaltung sowie an sogenannte wichtige und besonders wichtige Einrichtungen aus als besonders schützenswert erachteten Sektoren. Für die Bestimmung, ob ein Unternehmen reguliert wird, ist erstens zu klären, ob es zu einem der betroffenen Sektoren gehört. Zweitens muss ein gewisser Schwellenwert erreicht werden, um als wichtige oder besonders wichtige Einrichtung zu gelten. Für die betroffenen Stellen werden strengere Anforderungen an Netz- und Informationssysteme, erweiterte Meldepflichten und mehr Verantwortung für die Geschäftsführung eingeführt. Die Richtlinie betrifft künftig deutlich mehr Unternehmen und Sektoren als bisher. Neben einer Ausweitung des Anwendungsbereichs in den bereits NIS-1-Richtlinie abgedeckten Sektoren wie Energie, Verkehr und Gesundheitswesen erfasst die NIS-2-Richtlinie nunmehr auch zusätzliche Bereiche wie digitale Dienste, Post- und Kurierdienste, Abwasser- und Abfallbewirtschaftung und „Hersteller kritischer Produkte“.

Nachdem die vorherige Bundesregierung es versäumt hat, die Richtlinie fristgerecht umzusetzen, wussten viele Unternehmen bis zuletzt nicht, welche konkreten Maßnahmen auf sie zukommen (siehe dazu im Einzelnen unser Briefing v. 7. Februar 2025). Infolge dieser Verzögerung hat die EU-Kommission Anfang Mai 2025 ein Vertragsverletzungsverfahren gegen Deutschland eingeleitet. Die neue Bundesregierung hat die Umsetzung der NIS-2-Richtlinie in den letzten Wochen und Monaten stark priorisiert und binnen weniger Wochen den ursprünglichen Entwurf des NIS-2 Umsetzungsgesetzes überarbeitet, zwischen den Ressorts abgestimmt und in die Verbändeanhörung gegeben. Am 30. Juli 2025 wurde der Entwurf eines „Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“ im Kabinett der Bundesregierung beschlossen. Der Bundesrat wird voraussichtlich im September und der Bundestag im Oktober mit dem Gesetzesentwurf befasst werden. Das Gesetz soll dann bis Ende des Jahres in Kraft treten, um eine Anrufung des EuGH durch die EU-Kommission noch zu vermeiden.

Veränderungen beim Anwendungsbereich

Der nunmehr verabschiedete Regierungsentwurf basiert in wesentlichen Teilen auf den Vorarbeiten der „Ampel“-Regierung. Allerdings setzt die neue Bundesregierung einige neue Akzente:

- Die Neufassung beinhaltet nunmehr Regelungen für sogenannte Betreiber digitaler Energiedienste. Diese Dienste ermöglichen einen zentralen Zugriff auf die

Steuerung von Energieanlagen oder dezentralen Energieverbrauchsanlagen. Betreiber solcher Dienste, deren Anlage an ein Energieversorgungsnetz angeschlossen sind, sind künftig verpflichtet, einen angemessenen Schutz gegen Bedrohungen für Telekommunikationssysteme sowie elektronische Datenverarbeitungssysteme zu gewährleisten, die für einen sicheren Anlagenbetrieb notwendig sind. Besonders relevant ist in diesem Zusammenhang das Gefahrenpotenzial, das von einer möglichen Fernsteuerung ausländischer Hersteller ausgeht. Das ist zum Beispiel bei der Errichtung von Windparks von hoher Bedeutung. Daher sollen das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die Bundesnetzagentur (BNetzA) gemeinsam Anforderungen für die Anschaffung der Anlagengüter in einem IT-Sicherheitskatalog festlegen. Ziel ist es, den angestrebten Schutz umfassend zu gewährleisten. Die Aktualisierung des Katalogs sowie die Kontrolle der Einhaltung obliegen der BNetzA. Mit dieser Ergänzung erhält die Behörde erweiterte Befugnisse.

- Eine weitere Besonderheit im neuen Referentenentwurf ist die Streichung von Verweisen auf das KRITIS-Dachgesetz. Dieses Gesetz soll die parallel zu NIS-2 verabschiedete Richtlinie über die Resilienz kritischer Einrichtungen (sogenannte CER-Richtlinie) der EU umsetzen und Schutzmaßnahmen gegen physische Gefahren wie Naturgewalten oder Sabotage regeln. Unabhängig davon bleibt jedoch das Ziel bestehen, eine gemeinsame Meldeplattform des BSI und des Bundesamtes für Bevölkerungsschutz zu etablieren.

- Neu ist zudem, dass Geschäftsfelder eines Unternehmens nur berücksichtigt werden sollen, sofern sie nicht ausdrücklich als „vernachlässigbar“ eingestuft werden können (siehe § 28 Abs. 3 BSIG-E). Auf diese Weise soll eine als unverhältnismäßig empfundene Regulierung nach den NIS-2 Anforderungen vermieden werden, wenn Unternehmen nur geringfügige Nebentätigkeiten in den regulierten Bereichen ausüben.

Präzisierung der Unschärfen bei Unternehmenseinstufung auf den letzten Metern

Nach der Veröffentlichung des ersten Referentenentwurfs des Bundesinnenministeriums (Stand: 23.06.2025) hat insbesondere der unbestimmte Begriff der „vernachlässigbaren Geschäftstätigkeiten“ für erhebliche Rechtsunsicherheiten gesorgt. Kritisiert wurde in der Verbändeanhörung insbesondere, dass weder das NIS-2-Umsetzungsgesetz noch dessen Begründung klare Kriterien dafür lieferten, wann eine Tätigkeit als „vernachlässigbar” eingestuft werden kann. Daraufhin wurde noch kurzfristig nachgebessert und im Entwurf der Gesetzesbegründung ergänzt, dass mögliche Anhaltspunkte für diese Einstufung etwa

- die Anzahl der in diesem Bereich tätigen Mitarbeiter,

- der durch diese Geschäftstätigkeit erwirtschaftete Umsatz,

- die Bilanzsumme für diesen Bereich sowie
- eine Nennung in einem Gesellschaftervertrag, einer Satzung oder einem vergleichbaren Gründungsdokument der Einrichtung

sein können (so ausdrücklich im Regierungsentwurf, S.162). Diese Auslegungshilfen sind grundsätzlich zu begrüßen. Allerdings werden aufgrund der Ausnahme für „vernachlässigbare Geschäftstätigkeiten" nun möglicherweise von NIS-2 befreite Unternehmen sorgfältig überprüfen müssen, ob sie wirklich nicht unter die neuen Regularien fallen.

NIS-2-Start ohne Schonfrist

Abschließend ist besonders hervorzuheben: Das neue Umsetzungsgesetz zur NIS-2-Richtlinie sieht keine Übergangsfrist vor. Alle neuen Anforderungen und Bußgeldandrohungen gelten ab dann (d.h. vermutlich spätestes ab 1. Januar 2026) unmittelbar. Ab diesem Zeitpunkt laufen dann auch die Fristen für Nachweispflichten gegenüber dem BSI, wie z.B. die dreijährige Frist für Betreiber kritischer Anlagen aus § 39 BSIG-E.

Unternehmen, die potenziell von NIS-2 betroffen sind, müssen sich – sofern noch nicht geschehen – jetzt dringend vorbereiten, um rechtliche Risiken und Sanktionen zu vermeiden. Darüber hinaus sollten IT-Dienstleister, die gegenüber nunmehr regulierten Stellen Leistungen erbringen, sich darauf einstellen, dass einzelne IT-Sicherheitspflichten an sie weitergegeben werden.

***

BLOMSTEIN wird die weiteren Entwicklungen bei der NIS-2-Umsetzung aufmerksam verfolgen. Wenden Sie sich bei Fragen zum Umgang mit den Entwicklungen im deutschen IT-Sicherheitsrecht jederzeit gerne an Christopher Wolters, Leonard von Rummel und Moritz Schuchert.

BLOMSTEIN | Wir beraten unsere internationalen Mandanten in den Gebieten Kartell-, Vergabe-, Außenwirtschafts- und Beihilferecht sowie ESG in Deutschland, Europa und – über unser globales Netzwerk – weltweit.