NIS-2 kommt – Wie können sich Unternehmen vorbereiten?

Die NIS-2-Richtlinie (EU 2022/2555, „**NIS-2**") wird wesentliche Neuerungen in Bezug auf IT-Sicherheit für in der EU tätige Unternehmen bringen. Nach ihrem Inkrafttreten im Januar 2023 müssen die Mitgliedstaaten NIS-2 bis zum 17. Oktober 2024 in nationales Recht umsetzen. Unternehmen sollten nun prüfen, ob NIS-2 für sie gilt, um die verbleibende Zeit effizient zu nutzen und gegebenenfalls ihr Budget für Cybersicherheit zu erhöhen.

Hintergrund

Ziel von NIS-2 ist die Schaffung eines einheitlicheren Cybersicherheits-Niveaus in der EU gegenüber ihrer noch geltenden Vorgängerrichtlinie (EU 2016/1148, „**NIS-1**"). Zehntausende Unternehmen (auch kleine und mittelständische) werden in der Zukunft nun erstmals zur Einhaltung von IT-Sicherheit verpflichtet. Und auch Unternehmen, für die bereits jetzt NIS-1 gilt, müssen prüfen, ob noch *weitere* ihrer Tätigkeiten unter NIS-2 fallen. Zudem enthält NIS-2 strengere Pflichten für betroffene Unternehmen und deren Geschäftsleitungen.

Welche Sektoren unterfallen NIS-2?

18 (hochkritische und kritische) Sektoren werden von NIS-2 erfasst:

Elf Sektoren hoher Kritikalität: Energie; Verkehr; Banken; Finanzmarkt: Gesundheitswesen; Trink- und Abwasser, Digitale Infrastruktur; Verwaltung von IKT-Diensten (B2B); ausgewählte Einrichtungen der öffentlichen Verwaltung; Weltraum.

Sieben kritische Sektoren: Post- und Kurierdienste; Abfallwirtschaft; Herstellung und Handel mit chemischen Stoffen, Produktion; Verarbeitung und Vertrieb von Lebensmitteln; ausgewählte Gewerbetreibende; Anbieter digitaler Dienste; Forschung.

Für wen gilt NIS-2?

NIS-2 gilt insbesondere für

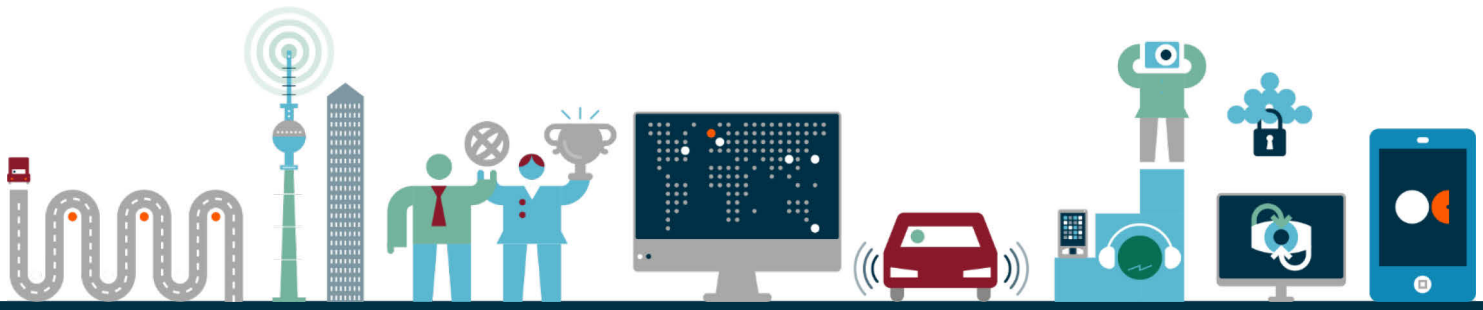
- öffentliche oder private Einrichtungen,
- in einem der 18 Sektoren,
- mit (i) ≥ 50 Beschäftigten und (ii) einem Jahresumsatz und/oder einer Jahresbilanzsumme ≥ EUR 10 Mio., welche
- ihre Dienste innerhalb der EU erbringen oder ihre Tätigkeiten dort ausüben.

Jedoch sieht NIS-2 eine Reihe zusätzlicher Anwendbarkeitskriterien sowie Ausnahmen und Rückausnahmen vor. Meistens bedarf es daher einer Einzelfallprüfung bezüglich der Anwendbarkeit von NIS-2.

Pflichten nach NIS-2

Betroffene Unternehmen müssen u.a.

- bestimmte technische und organisatorische Mindestmaßnahmen umsetzen, um IT-Sicherheitsvorfälle zu verhindern bzw. deren Folgen zu minimieren;
- staatliche Computer-Notfallteams/Behörden, ggf. auch Kunden unverzüglich benachrichtigen;
- eine Registrierung bei dem Bundesamt für Sicherheit in der Informationstechnik vornehmen (nur bestimmte Unternehmen).



NIS-2 verlangt weiter, dass Leitungsorgane die genannten Risikomanagementmaßnahmen genehmigen und bei Verstößen haftbar gemacht werden können. Leitungsorgane müssen außerdem an Schulungen zur Cybersicherheit teilnehmen. Anders als NIS-1 sieht NIS-2 vor, dass Cybersicherheitszertifizierungen für bestimmte IKT-Produkte/-Dienste/-Verfahren verpflichtend werden können, wenn die Mitgliedsstaaten und die EU-Kommission dies beschließen (zu Deutschland siehe unten).

Durchsetzungsmaßnahmen und Sanktionen

Unter NIS-2 erhalten Aufsichtsbehörden weitreichende Befugnisse, wie z.B. die Befugnis, Inspektionen vor Ort durchzuführen oder Zugang zu Daten und Dokumenten zu verlangen. Aufsichtsbehörden können Unternehmen verbindlich anweisen, bestimmte Cybersicherheitsmaßnahmen zu ergreifen oder bestimmtes Verhalten einzustellen, das sie als Verstoß gegen NIS-2 bewerten. Für wesentliche Einrichtungen können Behörden sogar einen vorübergehenden "Überwachungsbeauftragten" ernennen, der die Einhaltung relevanter Vorschriften überwacht.

Geldbußen für die Nichteinhaltung von NIS-2 können erheblich sein, d.h. abhängig von der Art der Einrichtung bis zu EUR 10 Mio. oder 2 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres.

Umsetzung in Deutschland

Zur Umsetzung von NIS-2 in Deutschland liegen bislang nur zwei außerparlamentarische Referentenentwürfe des BMI vor. Der aktuellste Entwurf datiert vom Juli 2023. Dieser sieht eine umfassende Überarbeitung und Neustrukturierung des bislang geltenden BSI-Gesetzes vor.

Der aktuelle Entwurf verweist jedoch noch stark auf (noch zu erstellende) Verordnungen, welche das Gesetz mit Leben füllen müssen. Es zeichnet sich jedoch jetzt schon ab, dass der deutsche Gesetzgeber – wie bislang auch – teilweise strenger regulieren möchte, als es die NIS-2 für eine Mindestharmonisierung verlangt.

Unklar ist bislang, welche Umsetzungsspiel-räume der Gesetzgeber nutzen möchte. Für bestimmte IKT-Produkte könnte er z.B. **verpflichtende** Cybersicherheitszertifizierungen einführen. Der aktuelle Referentenentwurf deutet darauf hin, dass er dies tun wird. Welche Produkte konkret betroffen sein könnten, ist allerdings noch offen.

Empfehlung und nächste Schritte

Auch wenn noch kein parlamentarischer Gesetzentwurf vorliegt, sollten Unternehmen bereits jetzt schon prüfen, ob sie unter NIS-2 fallen und welche Maßnahmen sie ggf. umsetzen müssen, um genügend Zeit zu haben, auf Geschäftsführungsebene strategische Entscheidungen zu fällen.

Anne Leßner
Senior Associate

T +49 30726218049
M +49 15777691360
anne.lessner@osborneclarke.com

Dr. Florian Eisenmenger
Senior Associate

T +49 8954348108
M +49 163 518 4737
florian.eisenmenger@osborneclarke.com