Kritische Infrastrukturen: Keine Umsetzung der NIS-2- und CER-Richtlinie noch vor der Bundestagswahl

Economic Security

Cattwyk Rechtsanwaltsgesellschaft mbH & Co. KG

Hohe Bleichen 8, 20354 Hamburg
Rue d'Arlon 25, B-1050 Brüssel

Kommanditgesellschaft | Sitz: Hohe Bleichen 8, 20354 Hamburg | Handelsregister HRA 131507 | Pers. haftende Gesellschafterin: Cattwyk Verwaltungs GmbH, HRB 188095 | Geschäftsführung: Dr. Katja Göcke, Dr. Lothar Harings, Dr. Hartmut Henninger, Franziska Kaiser, Marian Niestedt

Die Umsetzung der Richtlinien (EU) 2022/2555 (NIS-2-Richtlinie) und (EU) 2022/2557 (CER-Richtlinie) ist in Deutschland vorerst gescheitert. Wie nun bekannt geworden ist, konnten sich die bisherigen Ampel-Koalitionäre nach dem Bruch der Regierung nicht mehr auf eine Umsetzung der Richtlinien in das deutsche Recht einigen. Unternehmen sollten ungeachtet dessen prüfen, ob sie von den Umsetzungsgesetzen voraussichtlich betroffen sein werden und die Implementierung der damit einhergehenden Pflichten vorbereiten.

1. Was regeln die Richtlinien?

Gegenstand der NIS-2- und der CER-Richtlinie ist die Schaffung eines EU-weit einheitlichen Schutzniveaus im Hinblick auf die Sicherheit kritischer Infrastrukturen unter anderem in den Sektoren Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, Abwasser, Digitale Infrastruktur und Raumfahrt.

Mit der NIS-2-Richtlinie sollen betroffene Unternehmen zur Einhaltung eines hohen Cybersicherheitsniveaus verpflichtet werden. Der Anwendungsbereich ist deutlich weiter als beider Vorgängerrichtlinie (EU) 2016/1148 (NIS-1-Richtlinie), sodass zahlreiche Unternehmen erstmals von konkreten Cybersicherheitspflichten betroffen sein werden. Zudem gehen die Verpflichtungen weiter als unter der NIS-1-Richtlinie. Insbesondere sollen Unternehmen verpflichtet werden, auch innerhalb ihrer Lieferkette die Sicherheit zu prüfen und durch geeignete Maßnahmen zu gewährleisten.

In der CER-Richtlinie geht es hingegen um die Steigerung der physischen Resilienz kritischer Infrastrukturen vor dem Hintergrund hybrider Bedrohungen, Naturkatastrophen und durch den Klimawandel bedingter Wetterextreme. Betroffene Unternehmen sollen zur Ergreifung verschiedener Maßnahmen verpflichtet werden, um die physische Resilienz kritischer Einrichtungen sicherzustellen. Zu den in einem Resilienz-Plan zusammenzufassenden Maßnahmen gehören Präventionsmaßnahmen, die physische Absicherung, Krisenmanagementsysteme, Wiederherstellungsmaßnahmen, mitarbeiterbezogenes Sicherheitsmanagement sowie Sensibilisierungsmaßnahmen.

2. Umsetzung in deutsches Recht vorerst gescheitert

Die Richtlinien gelten nicht unmittelbar, sondern sind zunächst von den EU-Mitgliedstaaten in nationales Recht umzusetzen. Die hierfür vorgesehene Frist (17. Oktober 2024) ist bereits verstrichen.

In Deutschland sollte die CER-Richtlinie durch das KRITIS-Dachgesetz und die NIS-2-Richtlinie durch das gleichlautende Umsetzungsgesetz in das deutsche Recht umgesetzt werden. Unter der Federführung des Bundesministeriums des Innern und für Heimat (BMI) hatten die Verhandlungsführer von SPD, BÜNDNIS 90/DIE GRÜNEN und FDP die Regierungsentwürfe beraten, zunächst auch nach dem Aus der Regierung im November 2024. Allerdings kam es zu keiner Einigung, sodass es Aufgabe einer neuen Bundesregierung sein wird, die notwendigen Gesetze zu erarbeiten und durch das Gesetzgebungsverfahren zu bringen.

3. Das sollten Unternehmen jetzt tun

Wenngleich die Umsetzung der NIS-2-Richtlinie sowie der CER-Richtlinie in dieser Legislaturperiode gescheitert ist, darf nicht zuletzt wegen eines möglichen Vertragsverletzungsverfahrens gegen Deutschland davon ausgegangen werden, dass die nächste Bundesregierung die Richtlinien möglichst zeitnah in nationales Recht umsetzen wird.

Auch wenn die Umsetzung der Richtlinien vorerst zum Stillstand gekommen ist, sollten die betroffenen Unternehmen die Zeit nicht ungenutzt lassen und sich auf die zu erwartenden Regelungen einstellen. Anhand der Richtlinienvorgaben können bereits gewisse Anforderungen an die Unternehmen antizipiert und deren Umsetzung vorbereitet werden.

Unternehmen, die sich bislang nicht mit den voraussichtlichen Auswirkungen der neuen Regelungen beschäftigt haben, sollten zeitnah zunächst auf Grundlage der Richtlinien prüfen, ob sie in den Anwendungsbereich der Richtlinien fallen. Ist dies der Fall, wäre eine Risikoanalyse durchzuführen und zu prüfen, inwieweit bestehende IT- und physische Sicherheitsmaßnahmen verstärkt werden müssen. Auch bietet es sich an, bereits zu diesem Zeitpunkt mit der Erarbeitung oder Anpassung unternehmensinterner Richtlinien zu beginnen, in denen unter anderem Zuständigkeiten verteilt und Prozesse definiert werden, die der Umsetzung der in den nationalen Umsetzungsrechtsakten voraussichtlich enthaltenen Pflichten dienen.

Marian Niestedt, M.E.S.

Rechtsanwalt | Geschäftsführer

m.niestedt@cattwyk.com

Kahraman Altun, LL.M.

Rechtsanwalt | Associate

k.altun@cattwyk.com

Cattwyk Rechtsanwaltsgesellschaft mbH & Co. KG

Hohe Bleichen 8, 20354 Hamburg