NIS-2-Umsetzungsgesetz: Neue Compliance-Pflichten für zahlreiche Unternehmen

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

Nachdem der Bundestag das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz („**NIS2UmsuCG**“) im November 2025 beschlossen hat und der Bundesrat dem Gesetz am zustimmte, wurde es am 5. Dezember 2025 im Bundesgesetzblatt verkündet und trat am darauffolgenden Tag in Kraft. Das NIS2UmsuCG setzt die auf EU-Ebene beschlossene NIS2-Richtlinie (EU) 2022/2555 mit einiger Verspätung in nationales Recht um. Es sieht umfassende Änderungen insbesondere des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik („**BSIG**“) vor.

Mit dem NIS2UmsuCG werden neben den bereits zuvor regulierten Betreibern kritischer Anlagen („**KRITIS**“) nunmehr weitere Einrichtungen die im novellierten BSIG niedergelegten Pflichten im Bereich der Cybersicherheit erfüllen müssen. Der Anwendungsbereich des BSIG wird damit auf etwa 30.000 weitere Unternehmen in vielen Wirtschaftsbereichen erweitert.

1. Betroffene Unternehmen

Unternehmen müssen eigenständig prüfen, ob sie als „besonders wichtige Einrichtung“ oder eine „wichtige Einrichtung“ einzustufen und damit vom NIS2UmsuCG betroffen sind. Die Prüfung erfolgt grundsätzlich anhand der Zugehörigkeit zu bestimmten Sektoren und der Unternehmensgröße.

Als „besonders wichtige Einrichtungen“ gelten, unabhängig von der Unternehmensgröße, neben KRITIS-Betreibern auch qualifizierte Vertrauensdiensteanbieter, Top Level Domain Name Registries und DNS-Diensteanbieter. Erfasst werden darüber hinaus Anbieter von Telekommunikationsdiensten und Betreiber öffentlicher Telekommunikationsnetze, vorausgesetzt sie beschäftigen mindestens 50 Mitarbeiter oder weisen einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über EUR 10 Mio. auf. Zuletzt werden auch bestimmte Unternehmen aus den Sektoren Energie, Transport und Verkehr, Finanzwesen, Gesundheit, Wasser, digitale Infrastruktur und Weltraum erfasst, sofern sie mindestens 250 Mitarbeiter beschäftigen oder einen Jahresumsatz von über EUR 50 Mio. und zudem eine Jahresbilanzsumme von über EUR 43 Mio. aufweisen.

„Wichtige Einrichtungen“ sind zunächst sämtliche Vertrauensdiensteanbieter. Darüber hinaus sind auch Anbieter von Telekommunikationsdiensten und Betreiber von Telekommunikationsnetzen erfasst, die die Schwellenwerte für die Einstufung als besonders wichtige Einrichtung nicht erreichen. Ebenfalls als wichtige Einrichtungen gelten bestimmte Unternehmen in den Sektoren Energie, Transport und Verkehr, Finanzwesen, Gesundheit, Wasser, Abfallbewirtschaftung, Chemie,

Lebensmittel, verarbeitendes Gewerbe, digitale Infrastruktur, digitale Dienste und Weltraum, sofern sie mindestens 50 Mitarbeiter beschäftigen oder einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über EUR 10 Mio. aufweisen.

2. Pflichten betroffener Unternehmen

Betroffene Unternehmen werden zur Implementierung bestimmter Cybersicherheitsmaßnahmen verpflichtet, wobei die spezifischen Pflichten von der konkreten Einstufung (KRITIS-Betreiber; sonstige besonders wichtige Einrichtung; wichtige Einrichtung) abhängen.

Das NIS2UmsuCG sieht zunächst die Verpflichtung zur Implementierung von Risikomanagementmaßnahmen vor. Dazu gehören insbesondere Konzepte zur kontinuierlichen Bewertung von Risiken, Bewältigungsmaßnahmen im Falle eines Sicherheitsvorfalls und die Dokumentation ergriffener Maßnahmen. Die Umsetzung sowie Überwachung der Umsetzung dieser Maßnahmen obliegt der Geschäftsleitung. Das Gesetz sieht auch vor, dass die Geschäftsleitung, soweit sie ihre Pflichten aus dem NIS2UmsuCG verletzt, dem Unternehmen für entstandene Schäden haftet, vorausgesetzt die für das Unternehmen maßgeblichen gesellschaftsrechtlichen Bestimmungen enthalten keine Haftungsregelung.

Betroffene Unternehmen sind insbesondere auch verpflichtet, bei ihren Risikomanagementmaßnahmen etwaige Schwachstellen in der Lieferkette zu berücksichtigen. Das Bundesamt für Sicherheit in der Informationstechnik („**BSI**“) empfiehlt insoweit, Zulieferer vertraglich zur Einhaltung von IT-Sicherheitsstandards zu verpflichten und sich die Einhaltung nachweisen zu lassen. Zulieferer, die selbst nicht in den Anwendungsbereich des Gesetzes fallen, werden daher voraussichtlich über vertragliche Verpflichtungen gegenüber ihren Kunden mittelbar vom NIS2UmsuCG betroffen sein und ihre IT-Sicherheit gegebenenfalls stärken müssen.

Darüber hinaus haben sich betroffene Unternehmen beim BSI zu registrieren. Hierbei sind bestimmte Unternehmensdaten, die Sektorenzuordnung, Standortinformationen und die Benennung von Kontakten für Cybersicherheitsfragen zu übermitteln. Die Registrierung hat innerhalb von drei Monaten nach Inkrafttreten des NIS2UmsuCG oder nachdem die Einrichtung erstmals in den Anwendungsbereich des Gesetzes fällt, zu erfolgen. Das BSI-Portal, über das die Registrierung erfolgen soll, wird voraussichtlich Anfang Januar 2026 freigeschaltet.

Auch sind betroffene Unternehmen verpflichtet, den Behörden erhebliche Sicherheitsvorfälle in einem dreistufigen Verfahren zu melden. Dem BSI ist in einem solchen Fall innerhalb von 24

Stunden eine erste Warnmeldung, innerhalb von 72 Stunden eine detaillierte Meldung mit Bewertung des Vorfalls und innerhalb eines Monats ein Abschlussbericht zu übermitteln. KRITIS-Betreiber sind verpflichtet, im Rahmen der Meldung weitergehende Angaben zu machen.

Die Geschäftsleitung des betroffenen Unternehmens ist zudem verpflichtet, regelmäßig an Schulungen teilzunehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Cybersicherheit zu erlangen sowie um die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können.

Versäumnisse bei der Umsetzung der Cybersicherheitspflichten stellen Ordnungswidrigkeiten dar und können grundsätzlich mit einem Bußgeld in Höhe von bis zu EUR 10 Mio. oder, bei Unternehmen mit einem Gesamtumsatz von mehr als EUR 500 Mio., bis zu 2 % des Gesamtumsatzes geahndet werden.

3. Was Unternehmen jetzt tun sollten

Unternehmen sollten zeitnah prüfen, ob sie in den Anwendungsbereich des NIS2UmsuCG fallen. Die Prüfung sowie ihre Ergebnisse sollten sorgfältig dokumentiert werden. Führt die Prüfung zu dem Ergebnis, dass das Unternehmen eine „besonders wichtige Einrichtung“ oder eine „wichtige Einrichtung“ im Sinne des BSIG ist, hat das Unternehmen sich beim BSI zu registrieren und die auf sie anwendbaren Pflichten umzusetzen. Hierbei kann gegebenenfalls auf bereits existierende interne Systeme aufgesetzt werden.

Marian Niestedt, M.E.S.

Rechtsanwalt | Geschäftsführer

m.niestedt@cattwyk.com

Kahraman Altun, LL.M. (Edinburgh)

Rechtsanwalt | Associate

k.altun@cattwyk.com

Cattwyk Rechtsanwaltsgesellschaft mbH & Co. KG
Hohe Bleichen 8, 20354 Hamburg