Luther.

Strengere Vorgaben an die IT-Sicherheit: Der Bundestag setzt die NIS2-Richtlinie um

Mit der Verabschiedung des Gesetzes zur Umsetzung der NIS2-Richtlinie und zur Stärkung der Cybersicherheit (NIS2UmsuCG) hat der Bundestag am 13. November 2025 den entscheidenden Schritt zur Überführung der europäischen Richtlinie (EU) 2022/2555 („NIS2-Richtlinie“) in nationales Recht vollzogen. Die Richtlinie war bereits Anfang 2023 in Kraft getreten und verpflichtete die Mitgliedstaaten, die Vorgaben bis Oktober 2024 umzusetzen. Nachdem sich die Umsetzung in Deutschland zuletzt deutlich verzögert hatte, erfolgt sie nun zeitnah. Das NIS2UmsuCG bringt insbesondere eine umfassende Neufassung des BSI-Gesetzes (BSIG) und damit weitreichende neue Anforderungen an IT-Sicherheitsstrukturen und Governance-Prozesse mit sich.

I. Hintergrund

Mit dem NIS2UmsuCG verschärft der Gesetzgeber die Anforderungen an die IT-Sicherheit in Deutschland erheblich. Das Gesetz dient der nationalen Umsetzung der europäischen NIS2-Richtlinie (EU) 2022/2555 und verfolgt das Ziel, die Cyberresilienz in Wirtschaft und Verwaltung zu erhöhen. Damit einher geht eine deutliche Ausweitung des Anwendungsbereichs und eine substanzielle Stärkung der Aufsichts- und Eingriffsbefugnisse des Bundesamts für Sicherheit in der Informationstechnik (BSI).

II. Anwendbarkeit

Bisher sind in Deutschland insbesondere Betreiber kritischer Infrastrukturen auf Grundlage des bestehenden BSI-Gesetzes (BSIG) und der BSI-Kritisverordnung zur Einhaltung besonderer IT-Sicherheitsvorgaben verpflichtet. Neben den KRITIS-Betreibern werden künftig auch zahlreiche weitere Unternehmen aus zentralen Wirtschafts- und Gesellschaftsbereichen der Aufsicht und Meldepflicht des BSI unterstellt. Maßgeblich sind dabei zwei neue Kategorien, die sich an den Vorgaben der NIS2-Richtlinie orientieren:

- **Besonders wichtige Einrichtungen:** Dies sind insbesondere Unternehmen aus den in Anlage I der Richtlinie genannten Sektoren, also etwa Energie, Verkehr, Gesundheitswesen oder digitale Infrastruktur, die zugleich als Großunternehmen gelten (mindestens 250 Beschäftigte oder über 50 Mio. EUR Jahresumsatz und 43 Mio. EUR Jahresbilanzsumme) sowie KRITIS-Betreiber.
- **Wichtige Einrichtungen:** Insbesondere Unternehmen der in Anlage I und II genannten Sektoren, die als mittlere Unternehmen einzustufen sind (mindestens 50 Beschäftigte oder über je 10 Mio. EUR Jahresumsatz und Bilanzsumme).

Durch diese weite Definition müssen künftig auch zahlreiche mittelständische Unternehmen die neuen Cybersicherheitsanforderungen erfüllen. Der Kreis der betroffenen Einrichtungen vergrößert sich damit erheblich.

unyer GLOBAL ADVISORS

III. Pflichten

Mit dem NIS2UmsuCG gehen zugleich strengere Anforderungen an das Risikomanagement der betroffenen Einrichtungen einher. Sie müssen künftig technische, organisatorische und operative Maßnahmen treffen, die dem Stand der Technik entsprechen, um ein angemessenes Sicherheitsniveau zu gewährleisten. Diese Pflicht umfasst insbesondere die Implementierung eines wirksamen Risikomanagementsystems, das alle relevanten IT- und OT-Systeme sowie Lieferketten einbezieht. Dazu zählen u.a. die folgenden Maßnahmen:

- Konzepte und Richtlinien zur Steuerung von Informationssicherheitsrisiken,
- Notfall- und Wiederherstellungspläne (Business Continuity & Incident Response),
- Sicherheitsmaßnahmen in Entwicklung und Lieferkette,
- Zugriffs-, Identitäts- und Berechtigungskonzepte,
- sowie Schulungs- und Sensibilisierungsmaßnahmen für Führungskräfte und Beschäftigte.

In diesem Zusammenhang wird auch die Verantwortung der Geschäftsleitung ausdrücklich betont: Die Unternehmensleitung muss die Umsetzung der Risikomanagementmaßnahmen ausdrücklich fördern und überwachen sowie selbst an Schulungen zur Cybersicherheit teilnehmen.

Neu eingeführt wird zudem ein dreistufiges Meldesystem für Sicherheitsvorfälle, das eine zeitnahe und abgestufte Kommunikation mit dem BSI sicherstellen soll. Parallel erhält das BSI erweiterte Überwachungs- und Eingriffsbefugnisse, um die Einhaltung der Pflichten zu kontrollieren und bei Sicherheitsvorfällen unmittelbar reagieren zu können.

Verstöße gegen die neuen Vorgaben können künftig mit erheblich höheren Bußgeldern sanktioniert werden:

- bis zu 10 Mio. EUR für besonders wichtige Einrichtungen,
- bis zu 7 Mio. EUR für wichtige Einrichtungen,
- alternativ bis zu 2 % des weltweiten Jahresumsatzes bei sehr großen Unternehmen mit über 500 Mio. EUR Umsatz.

Mit dem NIS2UmsuCG werden die Anforderungen an die Cybersicherheit in Deutschland somit deutlich verschärft und breiter gefasst. Unternehmen aller Größenordnungen – insbesondere auch solche des Mittelstands – sind gefordert, ihre internen Sicherheitsprozesse, Meldewege und technischen Schutzmaßnahmen rechtzeitig zu überprüfen und an die neuen gesetzlichen Vorgaben anzupassen.

IV. Handlungsempfehlung: NIS2-Compliance vorbereiten

Unternehmen sollten die Umsetzung des NIS2UmsuCG so frühzeitig wie möglich aktiv angehen. Zentrale Schritte sind:

- **Anwendbarkeitsprüfung:** Unternehmen sollten jetzt prüfen, ob sie von den Anforderungen des NIS2UmsuCG betroffen sind. Denn zusätzliche Übergangsfristen sind im Gesetz nicht vorgesehen.
- **Registrierung:** Betroffene Unternehmen haben ab Inkrafttreten drei Monate Zeit, sich als betroffene Einrichtung beim BSI zu registrieren.
- **Bestandsaufnahme und Gap-Analyse:** Sicherlich haben die meisten Unternehmen bereits Maßnahmen zur IT-Sicherheit implementiert. Daher sollten die betroffenen Einrichtungen zunächst die bestehenden Sicherheitsmaßnahmen, Prozesse und Meldewege erfassen und etwaige Lücken identifizieren.
- **Implementierung technischer, organisatorischer und operativer Maßnahmen:** Umsetzung von Sicherheitsrichtlinien, Incident-Response-Plänen, Lieferkettenkontrollen und Mitarbeiterschulungen.
- **Anpassung von Governance-Strukturen:** Besonders wichtig ist die Einbindung der Geschäftsleitung, da diese letztverantwortlich für die Umsetzung der Anforderungen und die Akzeptanz von Risiken ist. Verantwortlichkeiten müssen daher klar benannt und Kommunikationswege für Sicherheitsvorfälle errichtet werden.

Luther unterstützt Sie bei der Prüfung und Umsetzung der NIS2-Anforderungen umfassend und praxisnah: von der Anwendbarkeitsprüfung und Durchführung von Gap-Analysen über die Entwicklung maßgeschneiderter Richtlinien und Konzepte sowie die Anpassung von Verträgen bis hin zur Schulung von Mitarbeitenden und Geschäftsleitung. Unser interdisziplinäres Expertenteam vereint tiefgehendes Wissen in Cybersecurity, Datenschutz und IT-Recht. Dabei setzen wir nicht nur auf unser exzellentes juristisches Know-how, sondern verfügen auch über Kooperationspartner, die Sie bei der technischen Umsetzung unterstützen können. So können Sie die neuen gesetzlichen Anforderungen effizient umsetzen und gleichzeitig Ihre Cyberresilienz nachhaltig stärken.

V. Ihre Ansprechpartner

Dr. Michael Rath
Rechtsanwalt, Certified Information Privacy Professional/Europe (CIPP/E), Partner, Fachanwalt für IT-Recht, Certified ISO/IEC 27001 Lead Auditor
Köln
+49 221 9937 25795
michael.rath@luther-lawfirm.com

Christian Kuß, LL.M.
Rechtsanwalt, Partner
Köln
+49 221 9937 25686
christian.kuss@luther-lawfirm.com

Franziska Tilgner
Rechtsanwältin, Senior Associate
Köln
+49 221 9937 25790
franziska.tilgner@luther-lawfirm.com

Stand: November 2025