# NIS 2 umsetzen: So müssen Unternehmen sich vor Cyberattacken schützen

Die NIS-2-Richtlinie der EU soll für mehr Cybersicherheit für die wesentlichen Infrastrukturen sorgen und diesbezüglich ein einheitliches und deutlich höheres Schutzniveau in Europa schaffen. Die Mitgliedsstaaten sollten sie bis zum 17. Oktober 2024 in nationales Recht umsetzen. Der deutsche Gesetzgeber ist dieser Pflicht zwar noch nicht nachgekommen. Ein Entwurf des Umsetzungsgesetzes (NIS2UmsuCG) liegt aber seit Juli 2024 vor. Auch die kommende Regierung wird jedenfalls für die Umsetzung der Richtlinie Sorgen zu tragen haben. Die Richtlinie schreibt den wichtigen Infrastrukturunternehmen bestimmte Risikomanagement-Maßnahmen wie Tests vor und verschärft die Meldepflichten.

### NIS-2 erweitert Umfang der verpflichteten Unternehmen enorm

Maßnahmen für Cybersicherheit waren auch bisher schon vorgeschrieben. Die NIS-2-Richtlinie dehnt allerdings den Kreis der betroffenen Unternehmen deutlich aus. Die kritischen Sektoren im Vergleich zur im Jahr 2016 verabschiedeten NIS-Richtlinie wurde um elf Sektoren erweitert. Betroffen sind neben Betreibern wesentlicher Dienste nun auch Anbieter digitaler Dienste, die zuvor nicht unter die Regelungen fielen. Dazu zählen zum Beispiel Anbieter von Cloud-Diensten, Rechenzentren und Online-Marktplätzen. Letztlich kann künftig fast jedes größere Unternehmen in den Anwendungsbereich fallen. Hinzu kommt: Ob ein Unternehmen betroffen ist, ist dabei nicht immer auf den ersten Blick ersichtlich. Insbesondere in Konzernstrukturen kann durch Beteiligungen auch die Konzernmutter verpflichtet sein.

### Unternehmen müssen ihre Betroffenheit selbst ermitteln

Die NIS-2-Richtlinie bzw. das NISUmsuCG richten sich an Betreiber kritischer Infrastruktur, an besonders wichtige Einrichtungen und an wichtige Einrichtungen. In den letzten beiden Kategorien richtet sich die Betroffenheit nach dem Sektor sowie nach Kriterien wie Jahresumsatz und Jahresbilanzsumme. Ob eine Einrichtung von NIS 2 bzw. dem NISUmsuCG betroffen ist, muss es selbst ermitteln. Das Bundesamt für Sicherheit und Informationstechnik (BSI) bietet zur ersten Orientierung eine NIS-2-Betroffenheitsprüfung an.

Grundsätzlich können Unternehmen die Betroffenheit von NIS 2 in fünf Schritten bewerten:


**So sollen Unternehmen ihre Cybersicherheit erhöhen**

In Umsetzung der Richtlinie soll in Deutschland eine Reihe von Gesetzen geändert werden. Die meisten Änderungen betreffen das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG). Geplant sind vor allem strengere Cybersicherheitsanforderungen. Unternehmen sollen nicht nur technische, sondern auch organisatorische Maßnahmen ergreifen müssen, um den Schutz ihrer IT-Infrastruktur sicherzustellen. Insbesondere kommen diese zusätzlichen Pflichten auf die betroffenen Unternehmen zu:

- **Risikomanagement-Maßnahmen**

  Das Umsetzungsgesetz definiert einige Maßnahmen zum Risikomanagement. Dazu gehören unter anderem Konzepte zu Risikoanalysen, Backups, Tests, Verschlüsselungen und Schulungen.

- **Meldepflichten**

  Besonders wichtige Einrichtungen und wichtige Einrichtungen müssen Sicherheitsvorfälle an eine Meldestelle melden.

- **Registrierungspflicht**

  Betroffene Unternehmen müssen sich selbstständig als solche registrieren lassen.

- **Unterrichtungspflicht**

  Bei Sicherheitsvorfällen müssen betroffene Unternehmen andere von dem Vorfall betroffene Einrichtungen informieren.

- **Überwachung durch Geschäftsleitung**

Mitglieder der Geschäftsleitung werden persönlich verpflichtet, die Umsetzung der Risikomanagementmaßnahmen zu überwachen.

Für Betreiber kritischer Infrastrukturen gelten zusätzliche Nachweispflichten.

**Die Geschäftsleitung haftet persönlich**

Wenn betroffene Einrichtungen die Anforderungen nicht erfüllen, drohen Bußgelder von bis zu 10 Millionen Euro oder 2 Prozent des weltweiten Jahresumsatzes. Besonders brisant ist die persönliche Haftbarkeit der Geschäftsleitung.

Der Haftungsmaßstab des aktuellen Entwurfs des deutschen Umsetzungsgesetzes entspricht den Vorgaben der NIS-2 Richtlinie. Bereits jetzt haften die Geschäftsleitungen, wenn sie sorgfaltswidrig gegen Pflichten zur Sicherstellung der IT-Sicherheit verstoßen und es dadurch zu Schäden gekommen ist. Durch NIS 2 erhöht sich das faktische Haftungsrisiko für die Geschäftsleitungen signifikant: Leitungsorgane müssen die ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit billigen und ihre Umsetzung überwachen. Für Verstöße können sie haftbar gemacht werden. Der aktuelle Regierungsentwurf des NIS2UmsuCG verschärft die Verantwortung der Geschäftsleitungen dem Wortlaut nach womöglich noch, indem diese über die Überwachung hinaus die Risikomanagementmaßnahmen sogar umzusetzen haben.

**So sollten Unternehmen sich vorbereiten**

Betroffene Unternehmen sollten sich auch schon vor Inkrafttreten eines Umsetzungsgesetzes mit NIS 2 beschäftigen und angemessene und verhältnismäßige Maßnahmen ergreifen, die auf einem nachvollziehbaren Risikomanagement basieren. Alle Maßnahmen sollten auf einem ganzheitlichen und bedrohungsorientierten Management-Ansatz beruhen, der darauf abzielt, Sicherheitsvorfälle zu vermeiden oder deren Auswirkungen zu minimieren. Wir empfehlen folgende Schritte:

- Zunächst sollten alle Unternehmen eine Betroffenheitsanalyse durchführen.
- Ist es betroffen, ist der nächste Schritt ein Readiness Assessment. Unternehmen sollten prüfen, wie das Unternehmen in Bezug auf die IT-Sicherheit aufgestellt ist und welche Maßnahmen in Bezug auf NIS 2 noch notwendig sind.
- Aus dieser Analyse leitet es dann die noch notwenigen Maßnahmen ab und setzt diese um.
- Zur Sicherstellung aller Maßnahmen sollten Unternehmen eine NIS-2-Governance aufstellen.
- Unternehmen sollten die Geschäftsleitung und ihre Mitarbeitenden schulen (lassen), insbesondere in den Bereichen Recht, Datenschutz, Audit / Revision, CyberSecurity und Technologie.
- Schließlich sollte ein Prozess zu der verpflichtenden Berichterstattung an die Aufsichtsbehörde aufgesetzt werden.
- Die gesamte Umsetzung sollte einem regelmäßigen Monitoring unterzogen werden.

## Ansprechpartner:

Francois Heynike, LL.M. (Stellenbosch)

Tel: +49-69-951195770
fheynike@kpmg-law.com

Dr. Daniel Taraz
Tel: +49 40 360994-5483
danieltaraz@kpmg-law.com