NIS 2: Cybersecurity ist jetzt Chefsache

DIE NIS 2-RICHTLINIE VERSCHÄRFT DIE ANFORDERUNGEN AN DIE CYBERSECURITY VON UNTERNEHMEN UND SICHERT DEREN EINHALTUNG DURCH WEITREICHENDE SANKTIONSMECHANISMEN AB

Executive Summary

- Im Vergleich zur bisherigen Rechtslage weitet die NIS 2-Richtlinie den Kreis der verpflichteten Unternehmen von 7 auf 18 Sektoren erheblich aus.
- Die betroffenen Unternehmen haben zum einen weitreichende technische, operative und organisatorische Maßnahmen zur Begegnung von Cybersicherheitsrisiken zu ergreifen und diese ebenso zu dokumentieren. Zum anderen haben sie auch für die „Sicherheit der Lieferkette“ Sorge zu tragen, und insofern ihre bestehenden Verträge auf NIS 2-Compliance zu prüfen und ggf. anzupassen.
- Verstöße gegen den neuen Pflichtenkatalog können mit erheblichen Bußgeldern von bis zu 10 Millionen Euro geahndet werden. Geschäftsführer haften mitunter mit ihrem Privatvermögen.
- NIS 2-Compliance ist spätestens bis zum 17. Oktober 2024 zu erreichen.

1. Einleitung

Am 16. Januar 2023 ist die Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union („**Network-and-Information-Security-Richtlinie 2**“ / „**NIS 2-Richtlinie**“) in Kraft getreten. Sie ist spätestens bis zum **17. Oktober 2024** in nationales Recht umzusetzen; ein zweiter Referentenentwurf zur Umsetzung der NIS 2-Richtlinie liegt bereits vor.

Ziel der Richtlinie ist es, die unionsweite Cybersicherheit, und zwar sowohl im Bereich der öffentlichen Verwaltung als auch bei privaten Unternehmen, zu koordinieren und noch weiter zu stärken. Denn Hackerangriffe können nicht nur einen enormen, insbesondere finanziellen Schaden für das einzelne betroffene Unternehmen zur Folge haben, sondern auch volkswirtschaftliche und gesamtgesellschaftliche Schäden verursachen, wenn etwa ein zentraler Internetknotenpunkt aufgrund eines Cyberangriffs ausfällt, ein Ampelsystem attackiert oder ein Krankenhaus in seinem Betrieb gestört wird. Nicht zuletzt

bestehen aber auch Risiken aufgrund von (Wirtschafts-) Spionage, wenn sensible Informationen – etwa aufgrund unzureichend geschützter IT-Systeme – erlangt werden können.

Wenngleich es bereits schon jetzt – teilweise auch unionsweite – Vorgaben zur Cybersicherheit mit vergleichbarer Zielrichtung gibt, so gelten diese dennoch als unzureichend. Denn sie beschränken sich im Wesentlichen auf Kritische Infrastrukturen und digitale Dienste, während zugleich das bislang erreichte Schutzniveau in den EU-Mitgliedsstaaten deutliche Unterschiede aufzeigt.

Vor diesem Hintergrund, aber auch unter Berücksichtigung, dass das reibungslose Funktionieren von IT-Systemen längst Grundvoraussetzung für den gesellschaftlichen Austausch und vor allem für den Erfolg des EU-Binnenmarkts geworden ist und Bedrohungen für diese Systeme beständig zunehmen, sah sich die EU veranlasst, die bestehenden Vorschriften durch einen umfassenden Katalog von zu erfüllenden Mindestsicherheitsmaßnahmen zu verschärfen sowie den Kreis der Verpflichteten von bislang 7 auf 18 Sektoren wesentlich zu erweitern.

2. Betroffene Unternehmen

Betroffen von der NIS 2-Richtlinie bzw. von dem entsprechenden Umsetzungsgesetz sind all jene Unternehmen, die jedenfalls folgende Kriterien erfüllen:

- Beschäftigung von mehr als 50 Mitarbeitern und
- Jahresumsatz von mehr als 10 Millionen Euro und
- Zugehörigkeit zu einem der folgenden Sektoren:
  - Bankwesen und Finanzmarktinfrastrukturen
  - Digitale Infrastruktur
  - Anbieter digitaler Dienste (etwa Cloud-Services und Online-Marketplaces)
  - Verarbeitendes Gewerbe / Herstellung von Waren (insb. Maschinenbau / KFZ / EDV / Haushaltsgeräte / Unterhaltungselektronik)
  - Lebensmittel (Produktion, Verarbeitung und Vertrieb)
  - Energie
  - Chemie (Produktion, Herstellung und Handel)
  - Verkehrswesen
  - Gesundheitswesen
  - Verwaltung von IKT-Diensten (B2B)
  - Post- und Kurierdienste
  - Forschung
  - öffentliche Verwaltung
  - Trink- und Abwasser sowie Abfallwirtschaft
  - Weltraum

Unabhängig von ihrer Größe werden Unternehmen auch allein aufgrund ihrer wahrgenommenen Aufgabe bzw. angebotenen Dienstleistung verpflichtet, so etwa bestimmte IT-Dienstleister wie DNS-Diensteanbieter oder qualifizierte Vertrauensdienste, die digitale Signaturen bereitstellen.

Ferner ermächtigt die Richtlinie die EU-Mitgliedsstaaten, den Adressatenkreis um Unternehmen zu erweitern, wenn zu befürchten ist, dass der Ausfall ihrer Dienste zu erheblichen gesamtgesellschaftlichen bzw. gesamtwirtschaftlichen Auswirkungen führt.

3. Pflichten der betroffenen Unternehmen

Alle von der NIS 2-Richtlinie erfassten Unternehmen werden zur **Ergreifung von technischen, operativen und organisatorischen Maßnahmen** verpflichtet, um die Risiken für die Sicherheit ihrer Netz- und Informationssysteme beherrschen und die Auswirkungen von möglichen Sicherheitsvorfällen verhindern oder möglichst gering halten zu können.

Zur Beurteilung, welche Maßnahmen zu ergreifen sind, sind zum einen die Eintrittswahrscheinlichkeit eines Sicherheitsvorfalls und zum anderen dessen potentielle Auswirkungen sowohl auf das Unternehmen als auch auf die Gesellschaft und die Wirtschaft insgesamt zu berücksichtigen. Je größer dieses Risiko und diese Auswirkungen sein können, um so weitreichendere Maßnahmen sind folglich vorzusehen. Jedenfalls haben diese Maßnahmen Folgendes zu umfassen:

- Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme

- Bewältigung von Sicherheitsvorfällen
- Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement
- Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit
- grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit
- Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung
- Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen
- Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Darüber hinaus haben die Unternehmen **regelmäßige Schulungen** ihrer Mitarbeiter vorzusehen, damit diese ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Begegnung von Cybersicherheitsrisiken erwerben.

Begleitet werden die zu treffenden Vorkehrungen ferner von **umfassenden Melde- und Berichtspflichten**: Sobald ein Sicherheitsvorfall eingetreten ist, der zu einer schwerwiegenden Betriebsstörung oder zu einem finanziellen Verlust des betroffenen Unternehmens geführt hat oder noch führen könnte, oder der natürliche oder juristische Personen geschädigt hat oder noch schädigen könnte, ist dies vom betroffenen Unternehmen innerhalb von 24 Stunden an die zuständige Behörde zu melden und es sind die Empfänger der vom Unternehmen angebotenen Dienstleistungen zu unterrichten. Hiernach ist die Meldung zu bestätigen bzw. zu aktualisieren und zu bewerten sowie ein ausführlicher Abschlussbericht zu verfassen.

Unternehmen, welche nach der Richtlinie als **wesentliche Einrichtungen** definiert werden, also etwa zur Kritischen Infrastruktur zählen oder die Schwellenwerte für mittlere Unternehmen überschreiten und sich bestimmten sensiblen Sektoren zuordnen lassen, trifft darüber hinaus eine **proaktive Nachweispflicht**, dass die von ihnen getroffenen Maßnahmen ausreichend sind. Diese Unternehmen können zudem anlasslos von der zuständigen Behörde auf NIS 2-Compliance überprüft werden.

4. Sanktionen und Haftung

Verstöße gegen die vorgenannten Pflichten sind sanktionsbewehrt. Je nach Einordnung des Unternehmens als wesentliche oder wichtige Einrichtung können Geldbußen in Höhe von bis zu zehn Millionen Euro oder zwei Prozent des Jahresumsatzes bzw. in Höhe von bis zu sieben Millionen Euro oder 1,4 Prozent des Jahresumsatzes verhängt werden – stets je nachdem welcher Betrag höher ist.
Neben dem Unternehmen unterliegen auch die Leitungsorgane selbst der Haftung. Sofern diese ihre – nicht delegierbaren – Überwachungspflichten verletzen, haften sie dem Unternehmen gegenüber persönlich auf den entstandenen Schaden.

Ferner sieht die Richtlinie vor, dass die zuständigen Behörden dazu ermächtigt werden, gegenüber wesentlichen Einrichtungen die Betriebsgenehmigung auszusetzen sowie zur vorübergehenden Absetzung des Leitungspersonals aufzufordern, sofern die Einrichtungen Anordnungen hinsichtlich der Cybersicherheit nicht nachgekommen sind.

5. Verhältnis zum Digital Operational Resilience Act

Mit dem Digital Operational Resilience Act (Verordnung [EU] 2022/2554; „**DORA**“) hat die EU als **lex specialis** einen weiteren Rechtsakt erlassen, der die digitale Resilienz erhöhen und EU-weit harmonisieren soll, und zwar für fast alle Unternehmen des Finanzsektors. Hinsichtlich dieser Unternehmen sollen nach der NIS 2-Richtlinie jene Vorschriften nicht anzuwenden sein, die sich auf das Cybersicherheitsrisikomanagement, die Berichtspflichten sowie auf die Aufsicht und die Durchsetzung beziehen. Stattdessen gelten die diesbezüglichen – und strengeren – Vorgaben von DORA. Nach den bereits vorliegenden Gesetzgebungsentwürfen und Diskussionspapieren zeichnet es sich zudem ab, dass der deutsche Gesetzgeber jene Unternehmen des Finanzsektors, welche bereits von DORA verpflichtet werden, komplett aus dem Adressatenkreis des NIS 2-Umsetzungsgesetzes nehmen möchte.

6. Folgen und Ausblick

Die Bedeutung der NIS 2-Richtlinie und ihre Auswirkungen sind kaum zu unterschätzen. Cybersecurity ist nun aufgrund der vorgesehenen persönlichen Geschäftsführerhaftung „Chefsache“; die zu treffenden Maßnahmen sind umfangreich und erfordern eine strukturierte Implementierung von Cybersecurity-Vorkehrungen und eine entsprechende Dokumentation. Neben diesen zu ergreifenden technischen, operativen und organisatorischen Maßnahmen sind darüber hinaus auch die Verträge mit Geschäftspartnern innerhalb einer Lieferkette auf NIS 2-Konformität zu prüfen und gegebenenfalls anzupassen.

Zwar hat der deutsche Gesetzgeber noch bis zum **17. Oktober 2024** Zeit, die Richtlinie umzusetzen. Da die zu ergreifenden Maßnahmen aber derart umfassend sind, sollte bereits frühzeitig damit begonnen werden, die eigenen Strukturen und Verträge auf NIS 2-Compliance zu prüfen und gegebenenfalls anzupassen. Dies kann erhebliche Kosten verursachen. Noch höhere Kosten dürften jedoch mögliche Geldbußen bei fehlender NIS 2-Compliance verursachen und erst recht ein „erfolgreicher“ Angriff auf die Netzwerk- und Informationssicherheit des Unternehmens.

Dr. Jörg Wünschel
Rechtsanwalt, Senior Associate
Standort Berlin
Tel +49 30 2039070
joerg.wuenschel@gsk.de

Dr. Jonathan Jung
Rechtsanwalt, Associate
Standort Berlin
Tel +49 30 2039070
jonathan.jung@gsk.de

GSK
STOCKMANN

Haftungsausschluss
Diese Mandanteninformation enthält ausschließlich allgemeine Informationen, die nicht geeignet sind, den besonderen Umständen eines Einzelfalles gerecht zu werden. Sie hat nicht den Sinn, Grundlage für wirtschaftliche oder sonstige Entscheidungen jedweder Art zu sein. Sie stellt keine Beratung, Auskunft oder ein rechtsverbindliches Angebot auf Beratung oder Auskunft dar und ist auch nicht geeignet, eine persönliche Beratung zu ersetzen. Sollte jemand Entscheidungen jedweder Art auf Inhalte dieser Mandanteninformation oder Teile davon stützen, handelt dieser ausschließlich auf eigenes Risiko.

GSK Stockmann und auch die in dieser Mandanteninformation namentlich genannten Partner oder Mitarbeiter übernehmen keinerlei Garantie oder Gewährleistung, noch haftet GSK Stockmann und einzelne Partner oder Mitarbeiter in irgendeiner anderen Weise für den Inhalt dieser Mandanteninformation. Aus diesem Grund empfehlen wir, in jedem Fall eine persönliche Beratung einzuholen.

www.gsk.de

GSK Stockmann
Rechtsanwälte Steuerberater Partnerschaftsgesellschaft mbB

BERLIN
Mohrenstraße 42
10117 Berlin
T +49 30 203907 - 0
F +49 30 203907 - 44
berlin@gsk.de

HEIDELBERG
Mittermaierstraße 31
69115 Heidelberg
T +49 6221 4566 - 0
F +49 6221 4566 - 44
heidelberg@gsk.de

FRANKFURT/M.
Bockenheimer Landstr. 24
60323 Frankfurt am Main
T +49 69 710003 - 0
F +49 69 710003 - 144
frankfurt@gsk.de

MÜNCHEN
Karl-Scharnagl-Ring 8
80539 München
T +49 89 288174 - 0
F +49 89 288174 - 44
muenchen@gsk.de

HAMBURG
Neuer Wall 69
20354 Hamburg
T +49 40 369703-0
F +49 40 369703-44
hamburg@gsk.de

LUXEMBURG
GSK Stockmann SA
44, Avenue John F. Kennedy
L - 1855 Luxemburg
T +352 271802 - 00
F +352 271802 - 11
luxembourg@gsk-lux.com

LONDON
GSK Stockmann International
Rechtsanwaltsgesellschaft mbH,
Zweigniederlassung London
Queens House, 8-9 Queen Street
London EC4N 1SP
United Kingdom
T +44 20 4512687-0
london@gsk-uk.com

Sitz der GmbH: München,
Amtsgericht München
HRB 281930
Geschäftsführer:
Dr. Mark Butt, Andreas Dimmling

YOUR PERSPECTIVE.
GSK.DE | GSK-LUX.COM