Cybersicherheit und die NIS-2-Richtlinie der EU

Sara Nesler, Mag. iur. (Torino), LL.M. (Münster)

August 2024

Laut Statista waren rund 58 Prozent der deutschen Unternehmen im Jahr 2023 mindestens einmal Opfer eines Cyber-Angriffs. Die Folgen solcher Angriffe reichen von Betriebsunterbrechungen über Umsatzeinbußen, Datenwiederherstellungskosten und Reputationsschäden bis hin zu Schadenersatzforderungen betroffener Kunden, die schnell erhebliche Summen erreichen können. Sind Unternehmen oder Institutionen betroffen, die eine besonders wichtige Rolle in der Gesellschaft spielen, wie zum Beispiel Energieversorger oder Medikamentenhersteller, können die Folgen verheerend sein.

Vor diesem Hintergrund ist am 16. Januar 2023 die EU-Richtlinie NIS-2 in Kraft getreten, die auch als *Richtlinie zur Sicherheit von Netz- und Informationssystemen* bekannt ist. Sie ist bis zum 17. Oktober 2024 in nationales Recht der Mitgliedstaaten umzusetzen und ersetzt die NIS-Richtlinie aus dem Jahr 2016. Wesentliche Neuerungen betreffen insbesondere die Erweiterung des Anwendungsbereichs und die persönliche Haftung der Leitungsorgane.

Hintergrund

Mit der ursprünglichen NIS-RL, die 2016 in Kraft trat, wollte die EU ein hohes gemeinsames Sicherheitsniveau für Netz- und Informationssysteme schaffen. Sie diente als Grundlage für nationale Cybersicherheitsstrategien und die Einrichtung von *Computer Security Incident Response Teams* (CSIRTs) und verpflichtete bestimmte Diensteanbieter, Cybersicherheitsvorfälle zu melden.

Es zeigte sich jedoch bald, dass die sich rasch verändernde Bedrohungslage eine Erweiterung der Richtlinie erforderte. Um diesen neuen Herausforderungen gerecht zu werden, wurde die NIS-2-RL entwickelt. Sie zielt darauf ab, die Cybersicherheit in der EU durch einen umfassenden und risikobasierten Ansatz zu verbessern. Anstatt sich nur auf einzelne kritische Infrastrukturen zu konzentrieren, betrachtet die Richtlinie die Sicherheit eines Unternehmens als Ganzes. Dieser umfassende Ansatz führt dazu, dass ein breiteres Spektrum von Unternehmen höhere Anforderungen an ihr Risikomanagement stellen muss, um die Vorschriften zu erfüllen.

Erweiterung des Anwendungsbereichs

Sachlicher Anwendungsbereich

Die alte NIS-RL galt für Betreiber wesentlicher Sektoren (Energie, Verkehr, Bankwesen, Finanzinfrastruktur, Gesundheitswesen und Trinkwasserversorgung) sowie für Anbieter digitaler Dienste. Die NIS-2-RL

differenziert zwischen „wesentlichen“ und „wichtigen“ Einrichtungen. Alle Sektoren, die von der NIS-RL erfasst waren, hat die NIS-2-RL in der Liste der wesentlichen Einrichtungen übernommen. Der Anwendungsbereich der neuen Richtlinie ist jedoch weiter als der der alten und umfasst insgesamt 18 Sektoren, davon 11 wesentliche und 7 wichtige Sektoren (Art. 3 NIS-2-RL und Anhang 1). Damit sind allein in Deutschland ca. 25.000 Unternehmen zusätzlich erfasst.

Die Liste der wesentlichen Einrichtungen wurde um folgende Sektoren erweitert:

- Öffentliche Verwaltung
- Verwaltung von Informations- und Kommunikationstechnologie-Diensten (IKT-Dienste)
- Abwasserwirtschaft
- Raumfahrt

Die Liste der wichtigen Sektoren umfasst nun:

- Post- und Kurierdienste
- Lebensmittelversorgung
- Abfallwirtschaft
- Chemische Industrie
- Herstellung von Arzneimitteln und Medizinprodukten

Zu beachten ist, dass die Mitgliedstaaten den Anwendungsbereich der Richtlinie bei der Umsetzung in nationales Recht noch erweitern können. Im deutschen Referentenentwurf zum *NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz* (NIS2UmsuCG) fallen beispielsweise neben den wesentlichen und wichtigen Einrichtungen auch die „Betreiber kritischer Anlagen“ in den sachlichen Anwendungsbereich.

Schwellenwerte

Die NIS-2-RL gilt grundsätzlich nur für Unternehmen und Einrichtungen, die mindestens als mittelgroßes Unternehmen einzustufen sind. Dies ist der Fall bei 50 oder mehr Beschäftigten und einem Jahresumsatz von mehr als 10 Millionen Euro. Schwierig wird die Abgrenzung bei Unternehmen, deren Hauptgeschäftstätigkeit nicht unter eine Einrichtungskategorie fällt, eine Nebentätigkeit des Unternehmens aber darunter fallen könnte. Darüber hinaus führt die Anwendbarkeit der NIS-2-RL auf eine Tochtergesellschaft nicht automatisch dazu, dass die gesamte Unternehmensgruppe (auch außerhalb der EU) in den Anwendungsbereich der Richtlinie fällt. Die verbundenen Unternehmen müssen jedoch gegebenenfalls bei der Berechnung des Schwellenwerts berücksichtigt werden.

Unabhängig von Größe und Umsatz eines Unternehmens sind bestimmte Ausnahmen vorgesehen, wenn das Unternehmen eine kritische Tätigkeit ausübt, Auswirkungen auf die öffentliche Ordnung hat oder Systemrisiken sowie grenzüberschreitende Auswirkungen bestehen.

Räumlicher Anwendungsbereich

Räumlich erfasst die NIS-2-RL Unternehmen, die in der EU Dienstleistungen erbringen oder sonst tätig sind, unabhängig von ihrem Sitz (Art. 2 NIS-2-RL). Das anwendbare Recht wird durch die Niederlassung eines Unternehmens in dem jeweiligen Mitgliedstaat bestimmt. Hat ein Unternehmen keine Niederlassung in der EU, erbringt jedoch Dienstleistungen in der EU oder ist dort sonst tätig, muss es einen Vertreter in der EU benennen. Das Recht der Niederlassung des Vertreters ist dann anwendbar.

Erhöhte Sicherheitsanforderungen

Die NIS-2-RL stellt erhöhte Sicherheitsanforderungen an die betroffenen Unternehmen und Organisationen, die durch die Umsetzungsgesetze der Mitgliedstaaten weiter konkretisiert werden. Diese umfassen:

- Die Implementierung eines umfassenden Risikomanagements, das auf die spezifischen Bedrohungen und Schwachstellen des jeweiligen Sektors zugeschnitten ist.
- Die Entwicklung und Umsetzung wirksamer Maßnahmen zur Reaktion auf sicherheitsrelevante Vorfälle (*Incident Response*).

- Die Durchführung regelmäßiger Sicherheitsüberprüfungen und Audits, um die Einhaltung der Richtlinie zu gewährleisten.

Lieferketten

Für Unternehmen sind besonders die Neuerungen im Bereich der Lieferketten relevant. Da diese als Schnittstellen zwischen mehreren Unternehmen besonders anfällig für Datenübermittlungen und Unternehmen dadurch besonders verwundbar sind, hält die Kommission einen verstärkten Schutz der Lieferketten für notwendig. Zu berücksichtigen sind unter anderem folgende Kriterien:

- Das Ausmaß, in dem wesentliche und wichtige Einrichtungen von kritischen IKT-Diensten, -Systemen oder -Produkten abhängig sind.
- Die Bedeutung dieser kritischen IKT-Dienste, -Systeme oder -Produkte für die Durchführung kritischer oder sensibler Funktionen.
- Die Verfügbarkeit alternativer Dienste, Systeme und Produkte.
- Die Widerstandsfähigkeit der gesamten Lieferkette gegenüber destabilisierenden Ereignissen.

Erweiterte Meldepflichten

Die NIS-2-RL erweitert auch die Meldepflichten für Cybersicherheitsvorfälle. Unternehmen und Organisationen sind verpflichtet, jede erhebliche Bedrohung ihrer Netz- und Informationssysteme innerhalb kurzer Zeit den zuständigen Behörden zu melden. Ein Sicherheitsvorfall gilt als erheblich, wenn er zu einer schwerwiegenden Beeinträchtigung der Funktionsfähigkeit von Diensten oder zu finanziellen Verlusten für die betroffene Organisation geführt hat oder führen kann oder anderen natürlichen oder juristischen Personen einen erheblichen materiellen oder immateriellen Schaden zugefügt hat oder zufügen kann.

Persönliche Haftung der Leitungsorgane

Eine weitere wichtige Änderung betrifft die Haftung für Verstöße gegen die Richtlinie. Nach Art. 20 Abs. 1 NIS-2-RL haften die Leitungsorgane, also Geschäftsführer, Vorstandsmitglieder usw., persönlich mit ihrem Privatvermögen. Nationale Haftungsregelungen im öffentlichen Sektor bleiben unberührt. Darüber hinaus sind die Leitungsorgane wesentlicher und wichtiger Einrichtungen verpflichtet, an Schulungen teilzunehmen und diese regelmäßig für alle Mitarbeiter anzubieten.

Sanktionen

Die Sanktionen bei Verstößen sind beträchtlich. Bei wesentlichen Einrichtungen beträgt der Höchstbetrag der Geldbuße 10 Mio. EUR oder 2 % des weltweiten Vorjahresumsatzes (Art. 34 Abs. 4 NIS-2-RL). Bei wichtigen Einrichtungen beträgt der Höchstbetrag 7 Mio. EUR oder 1,4 % des weltweiten Vorjahresumsatzes (Art. 34 Abs. 5 NIS-2-RL). Da die Richtlinie lediglich eine Mindestharmonisierung vorschreibt, können die Bußgelder in einzelnen Mitgliedstaaten noch höher ausfallen. Zudem haben die zuständigen Behörden Aufsichts- und Durchsetzungsbefugnisse.

Verbesserte Kooperation und Koordination

Die NIS-2-RL betont die Bedeutung von Kooperation und Koordination zwischen den Mitgliedstaaten sowie zwischen öffentlichen und privaten Akteuren. Dazu gehören die Einrichtung und Stärkung von CSIRTs in allen Mitgliedstaaten und deren Zusammenarbeit auf europäischer Ebene (CSIRT-Netzwerk) sowie die Einrichtung einer Kooperationsgruppe zur Förderung der strategischen Zusammenarbeit und des Informationsaustauschs zwischen den Mitgliedstaaten. Außerdem ist die Einrichtung eines Frühwarnsystems vorgesehen, um die Mitgliedstaaten frühzeitig über potenzielle Bedrohungen und Vorfälle zu informieren.

Verhältnis zu anderen Regelungen

Die Datenschutz-Grundverordnung bleibt von der neuen NIS-2-RL unberührt. Die nach der NIS-2-RL zuständigen Behörden sollen mit den Datenschutzbehörden zusammenarbeiten und müssen Datenschutzverstöße nach Art. 33 DSGVO melden.

Die *Richtlinie über die Resilienz kritischer Einrichtungen* (CER-Richtlinie) stellt einen weiteren Baustein des Cybersicherheitskonzepts der EU dar und muss bis zum 17. Oktober 2024 von den Mitgliedstaaten umgesetzt werden. Sie ist *lex spezialis* zur NIS-2-RL und bleibt unberührt.

Empfehlung

Die Mitgliedstaaten müssen die NIS-2-RL bis zum 17. Oktober 2024 in nationales Recht umsetzen. Betroffene Unternehmen sollten sich daher rechtzeitig mit der NIS-2-RL und den Entwürfen der Umsetzungsgesetze der jeweiligen Mitgliedstaaten auseinandersetzen, denn diese konkretisieren die Vorgaben der Richtlinie umfassend. Insbesondere für Unternehmen, die bisher nicht in den Anwendungsbereich der Richtlinie fallen, dürfte dies mit erheblichem Aufwand verbunden sein. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet auf seiner Website eine NIS-2-Betroffenheitsprüfung für Unternehmen an, die unsicher sind, ob sie von der Richtlinie betroffen sind.

Ein Vergleich zeigt, dass die *ISO-Norm 27001:2022* (Informationstechnik–IT-Sicherheitsverfahren–Informationssicherheits-Managementsysteme–Anforderungen) bereits viele Anforderungen der NIS-2-RL erfüllt. Einige Übereinstimmungen gibt es auch mit der *ISO-Norm 27002:2022* (Informationstechnik–IT-Sicherheitsverfahren–Leitfaden für das Informationssicherheits-Management). So finden sich beispielsweise die Governance-Anforderungen des Art. 20 NIS-2-RL in Art. A.5 ISO 27001:2022.

Eine GAP-Analyse, die die Abweichung des Ist-Zustands vom Soll-Zustand aufzeigt, ist sinnvoll. Das BSI empfiehlt als erste Schritte eine zuständige Person zu benennen, als Unternehmensleitung Verantwortung zu übernehmen, eine erste Bestandsaufnahme zu tätigen, die Informationssicherheit zu verbessern und sich auf die Meldepflichten vorzubereiten.

+ + +

IMPRESSUM

HERAUSGEBER

HERFURTH & PARTNER Rechtsanwaltsgesellschaft mbH
Luisenstr. 5, D-30159 Hannover
Fon 0511-307 56-0 Fax 0511-307 56-10
Mail info@herfurth.de, Web www.herfurth.de
Hannover · Göttingen · Brüssel
Member of the ALLIURIS GROUP, Brussels

REDAKTION

Leitung: Ulrich Herfurth, Rechtsanwalt, zugelassen in Hannover und Brüssel (verantw.)

Mitarbeit: Angelika Herfurth, Rechtsanwältin, FA Familienrecht; Sibyll Hollunder-Reese, M.B.L. (HSG), Rechtsanwältin; Günter Stuff; Xiaomei Zhang, Juristin (China), Mag. iur. (D); Thomas Gabriel, Rechtsanwalt; JUDr. Yvona Rampáková, Juristin (CR); Dr. Jona Aravind Dohrmann, Rechtsanwalt; Prof. Dr. jur. Christiane Trüe LL.M. (East Anglia); Konstantin Kuhle, Rechtsanwalt; Antonia Herfurth, Rechtsanwältin, LL.M. (Göttingen); Sara Nesler, Mag. iur. (Torino), LL.M. (Münster).

KORRESPONDENTEN

u.a. Amsterdam, Athen, Brüssel, Budapest, Helsinki, Istanbul, Kopenhagen, Lissabon, London, Luxemburg, Mailand, Madrid, Moskau, Paris, Stockholm, Warschau, Wien, Zug, New York, Toronto, Mexico City, Sao Paulo, Buenos Aires, New Delhi, Peking, Tokio.

VERLAG

CASTON GmbH, Law & Business Information
Luisenstr. 5, D-30159 Hannover,
Fon 0511-307 56-50 Fax 0511-307 56-60
Mail info@caston.info; Web www.caston.info