NIS-2-Richtlinie zur Verbesserung der Cybersicherheit in der EU

Die NIS-2-Richtlinie vom Dezember 2022 löst die Vorgängerregelung NIS-1-Richtlinie aus dem Jahr 2016 ab. Ihr Ziel ist die Verbesserung der Resilienz und Reaktionsfähigkeit im Bereich der Cybersicherheit der öffentlichen und privaten Sektoren sowie der Europäischen Union insgesamt. Hierfür schreibt sie „Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union“ vor. Bis zum 17. Oktober 2024 müssen alle EU-Mitgliedsstaaten die Richtlinie in nationales Recht umsetzen. Spätestens dann gelten die Vorgaben insbesondere im Bereich des Cyberrisikomanagements auch direkt für „öffentliche und private Einrichtungen“ aus bestimmten Sektoren, unter anderem also für Behörden und Unternehmen. Bis dahin greifen die Regelungen der NIS-1-Richtlinie.

Ziele der NIS-2-Richtlinie

Zur Verbesserung der Cybersicherheit in der EU sollen nationale Cybersicherheitsstrategien verabschiedet und zuständige nationale Behörden, Behörden für das Cyberkrisenmanagement, zentrale Anlaufstellen für Cybersicherheit und Computer-Notfallteams (CSIRT) benannt oder eingerichtet werden. Für das Cybersicherheitsmanagement werden Vorgaben gemacht, einschließlich entsprechender Berichtspflichten, dem Austausch von Cybersicherheitsinformationen zwischen den EU-Staaten sowie über Art und Weise der Aufsicht in den einzelnen Mitgliedsstaaten.

Erweiterung des Anwendungsbereichs

Die NIS-2-Richtlinie erweitert den Anwendungsbereich um zusätzliche Sektoren. In Anhang I zur Richtlinie finden sich Auflistungen von „Sektoren mit hoher Kritikalität“ sowie „sonstige kritische Sektoren“:

Sektoren mit hoher Kritikalität	Sonstige kritische Sektoren
Energie	Post- und Kurierdienste
Verkehr	Abfallbewirtschaftung
Bankwesen	Produktion
Finanzmarktinfrastrukturen	Umgang und Handel mit chemischen Stoffen

Sektoren mit hoher Kritikalität	Sonstige kritische Sektoren
Gesundheitswesen	Umgang und Handel mit Lebensmitteln
Trinkwasser	Verarbeitendes Gewerbe
Digitale Infrastruktur	Anbieter digitaler Dienste
Abwasser	Forschung
Verwaltung von IKT-Diensten	
Öffentliche Verwaltung	
Weltraum	

Durch die NIS-2-Richtlinie neu hinzugekommene Sektoren sind blau markiert.

Unternehmen, die in mindestens einen der genannten Sektoren fallen, sind von der Richtlinie erfasst, wenn sie als „mittleres Unternehmen“ einzustufen sind. Das sind Unternehmen mit zwischen 50 und 249 Mitarbeitenden sowie einem Jahresumsatz zwischen 10 und 50 Millionen Euro. Ungeachtet ihrer Einstufung sind Anbieter öffentlicher Kommunikationsnetze und -dienste sowie Vertrauensdiensteanbieter und Namensregister der obersten Domäne einschließlich DNS-Diensteanbieter stets erfasst. In bestimmten Fällen können auch Klein- und Kleinstunternehmen unter die NIS-2-Richtlinie fallen.

Pflichtenkatalog

Auf betroffene Einrichtungen kommen umfassende Pflichten zu:

- → Leitungsorgane werden für das Risikomanagement im Bereich Cybersicherheit in die Pflicht genommen. Sie müssen entsprechende Maßnahmen billigen, deren Umsetzung überwachen und werden für Verstöße zur Verantwortung gezogen.
- → Leitungsorgane und Mitarbeitende müssen an Schulungen zur Cybersicherheit teilnehmen.
- → Wesentliche und wichtige Einrichtungen müssen geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen zur IT-Sicherheit ergreifen (Risikomanagementmaßnahmen).
- → Es greifen umfassende Berichts- und Meldepflichten bei Sicherheitsvorfällen.
- → Behörden können Pflicht zur Verwendung spezieller IKT-Produkte, -Dienste und -Prozesse mit Cybersicherheitszertifizierung anordnen.
- → Für Einrichtungen bestimmter Sektoren bestehen Registrierungspflichten.
- → Einrichtungen sollen untereinander Informationen zur Cybersicherheit austauschen.

Zu den Risikomanagementmaßnahmen zählen Risikoanalyse- und Sicherheitskonzepte, Business Continuity-, Backup- sowie Krisen-Management, Multi-Faktor-Authentifizierungen, Konzepte für Zugriffskontrollen und Mitarbeitersicherheit, Verschlüsselungskonzepte, Schwachstellenanalysen sowie Sicherheitsaspekte der Lieferkette und in Beziehungen zu anderen Lieferanten oder Dienstleistern.

Neben den allgemeinen Vorschriften zur Cybersicherheit definiert die NIS-2-Richtlinie auch spezifische Anforderungen für einzelne Sektoren. Dazu gehören beispielsweise Anforderungen an die Sicherheit von Energie- und Verkehrssystemen oder die Anforderungen an die Sicherheit von Gesundheitsdaten im Gesundheitswesen.

Aufsicht und Bußgelder

Die zuständigen Behörden sollen gegenüber den betroffenen Einrichtungen wirksame, verhältnismäßige und abschreckende Aufsichts- und Durchsetzungsmaßnahmen ergreifen. Der Bußgeldrahmen beträgt mindestens 7 Millionen Euro oder 2 % des weltweiten Vorjahresumsatzes einer betroffenen Einrichtung.

Acht Fragen und Antworten rund um NIS-2

1. Die Umsetzung der NIS-2-Richtlinie in nationales Recht erfolgt voraussichtlich erst im Jahr 2024. Ab wann sollte man sich aktiv darauf vorbereiten?

Von der NIS-2-Richtlinie betroffene öffentliche und private Einrichtungen sollten sich bereits jetzt mit der Umsetzung der Pflichten aus der Richtlinie in nationales Recht beschäftigen. Hierzu können sie sich am Text der Richtlinie orientieren, denn er dient den EU-Staaten als Vorlage für die Umsetzung der Vorgaben in jeweils nationales Recht. Die NIS-2-Pflichten gelten zwingend ab 18. Oktober 2024. Die Zeit bis dahin ist knapp. Mehr Zeit haben betroffene Einrichtungen nicht. Die EU-Staaten dürften diese Pflicht auch nicht verlängern. In Deutschland gelten einige Vorgaben aus der NIS-2-Richtlinie bereits heute, da sie bereits im IT-Sicherheitsgesetz 2.0 enthalten sind.

2. Welche Vorgaben aus der NIS-2-Richtlinie sollten mit höchster Priorität behandelt werden?

Die höchste Priorität sollte das Risikomanagement bekommen. Die NIS-2-Richtlinie stellt das Risikomanagement im Bereich Cybersicherheit in den Vordergrund. Hierfür werden „geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen“ gefordert. Sie müssen jeweils dem Stand der Technik sowie einschlägigen internationalen und europäischen Normen entsprechen. Der Aufbau entsprechender Strukturen und Prozesse, einschließlich entsprechender personeller Ressourcen, nimmt oftmals viel Zeit in Anspruch und sollte deswegen Vorrang haben.

3. Inwiefern gilt es weiterhin die Datenschutz-Grundverordnung (DSGVO) zu berücksichtigen?

Die NIS-2-Richtlinie ändert nichts an der Geltung der Datenschutz-Grundverordnung und der Zuständigkeit von Datenschutzbehörden für die Verarbeitung von personenbezogenen Daten. Das bedeutet beispielsweise, dass ein Datenleck im Rahmen eines Sicherheitsvorfalls Meldepflichten nach DSGVO, aber auch Pflichten nach den

NIS-2-Gesetzen der EU-Staaten auslösen kann. Die NIS-2-Aufsichtsbehörden sind zudem verpflichtet, die Datenschutzbehörden über datenschutzrechtlich relevante Vorfälle zu unterrichten. Für von der NIS-2-Richtlinie betroffene Einrichtungen ist es zudem richtig, den betrieblichen Datenschutzbeauftragten bei der Umsetzung der Vorgaben einzubeziehen.

4. Wird es einen Übergangszeitraum der kulanten Handhabe geben oder ist zum Stichtag unmittelbar mit Bußgeldern zu rechnen?

Mit Inkrafttreten der nationalen Gesetze zur Umsetzung der NIS-2-Richtlinie werden die Pflichten, aber auch die Bußgeldregelungen scharfgestellt. Im Grunde besteht ein Übergangszeitraum nur zwischen jetzt und dem 18. Oktober 2024. Er sollte von den betroffenen Einrichtungen genutzt werden. Dies gilt insbesondere für Einrichtungen aus Sektoren, die erstmals erfasst werden.

Die zuständigen Behörden müssen die Verhängung etwaiger Bußgelder von den jeweiligen Umständen des Einzelfalls abhängig machen. Dabei spielt der Grundsatz der Verhältnismäßigkeit eine entscheidende Rolle. Die NIS-2-Richtlinie listet zudem Kriterien auf, die bei der Bußgeldbemessung zu berücksichtigen sind. Hierzu zählen Schwere und Dauer des Verstoßes, frühere Verstöße, der verursachte Schaden, Fahrlässigkeit oder Vorsatz der verantwortlichen Personen, Schadensbegrenzungsmaßnahme und Art und Weise der Kooperation mit den Behörden. Behörden wenden zunächst meist mildere Mittel an, bevor Bußgelder verhängt werden. Eine gewisse „Kulanz“ dürfte es daher auch nach dem 18. Oktober 2024 geben, ein Rechtsanspruch darauf besteht jedoch nicht.

5. Welche zusätzlichen Dienstleistungen können Systemhäuser / IT-Berater anbieten, um ihren Kunden entsprechend zu wappnen?

Betroffene Einrichtungen müssen die Pflichten der NIS-2-Richtlinie erfüllen. Zum Aufbau der Prozesse, Teams, Sicherheitstechnik et cetera können sie sich externer Systemhäuser und IT-Berater bedienen. Das ist auch ratsam, wenn die entsprechenden Fähigkeiten intern nicht vorhanden sind. Fehlende Ressourcen genügen gegenüber den Behörden nicht, um sich von den NIS-2-Pflichten insgesamt freizuzeichnen.

6. Welche Art risikobasierter Sicherheitsstrategien wird erforderlich sein, um den voraussichtlichen Auflagen Genüge zu tun?

Die NIS-2-Richtlinie verlangt die Einhaltung des Standes der Technik, sowie internationaler wie europäischer Normen. Der IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik, aber auch die ISO-Normenwerke 27001 und 9001 verfolgen risikobasierte Ansätze der Informations- und Cybersicherheit. Die konkrete Umsetzung in einer betroffenen Einrichtung hängt vom Einzelfall ab. Risikobasiert kann eine Sicherheitsstrategie aber nur dann sein, wenn zunächst die Risiken jeweils einrichtungsbezogen und konkret bestimmt wurden.

7. Welche Rolle spielen IT-Sicherheits-Audits?

Die NIS-2-Richtlinie schreibt IT-Sicherheits-Audits nicht unmittelbar vor. Sie sind aber beispielsweise in ISO 27001 genannt und können als internes wie externes Audit durchgeführt werden. Sie dienen allgemein zur Feststellung, ob ein Cyber- oder IT-Sicherheitssystem einer Einrichtung den an sie gestellten Vorgaben genügt und wo Nachbesserungsbedarf besteht. Zu diesen Vorgaben zählen auch die Gesetze zur Umsetzung der NIS-2-Richtlinie.

IT-Sicherheits-Audits helfen den Verantwortlichen auch dabei, zu überprüfen, ob sie ihren NIS-2-Pflichten gerecht werden und können das Risiko behördlicher Maßnahmen reduzieren. Mitunter verlangen Versicherer, aber auch Vertragspartner über die gesetzlichen Vorgaben hinaus die regelmäßige Durchführung von IT-Sicherheits-Audits.

8. Es wird ein sehr breites Spektrum adressiert, so etwa auch das verarbeitende Gewerbe und Anbieter digitaler Dienste. Welche Branchen und Unternehmen werden von den zu erwartenden Regelungen nicht betroffen sein?

Die Pflichten nach der NIS-2-Richtlinie richten sich an Einrichtungen aus insgesamt 18 Sektoren, unterteilt in Sektoren mit hoher Kritikalität und „sonstige kritische Sektoren". Diese Sektorenauflistung ist abschließend. Unternehmen, die nicht mindestens einem dieser Sektoren angehören, sind nicht betroffen.

Betroffen sind zudem grundsätzlich nur mittlere und große Unternehmen. Klein- und Kleinstunternehmen sind aber beispielsweise dann erfasst, wenn sie systemrelevant oder „für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Tätigkeiten unerlässlich" sind.

Über den Autor

Tobias Haar
LL.M. (Rechtsinformatik), MBA (Kellogg-WHU)
Rechtsanwalt
Vogel & Partner Rechtsanwälte mbB
www.vogel-partner.eu