NIS-2-Richtlinie

NIS-2-Richtlinie: Auftrag für KRITIS-Schutz

Mit den überarbeiteten Vorgaben an kritische Einrichtungen im Bereich der Cybersicherheit hat die EU auf die geänderte Gefahrenlage reagiert. Bis 2024 müssen die EU-Staaten ihr nationales Recht anpassen.

Von Tobias Haar

-tract

- Die NIS-2-Richtlinie löst ihre Vorgängerin ab, EU-Mitgliedsstaaten müssen sie bis 2024 in nationales Recht umsetzen.
- Die neue Richtlinie hat zwei Schwerpunkte: das Erschaffen nationaler Cybersicherheitsstrategien samt den dafür nötigen Institutionen sowie die verbesserte Kommunikation zwischen den Mitgliedsstaaten und den Sicherheitsbehörden.
- Die NIS-2-Richtlinie erweitert den Anwendungsbereich auf zusätzliche Sektoren und Unternehmen.
- Hierzulande dürfte die Umsetzung im Rahmen eines überarbeiteten IT-Sicherheitsgesetzes, dann in Version 3.0, erfolgen. Dies hatte der Koalitionsvertrag der Bundesregierung ohnehin vorgesehen.

Das Ziel der NIS-2-Richtlinie zum Schutz von Netzwerk- und Informationssystemen ist die Verbesserung der Resilienz und Reaktionsfähigkeit im Bereich der Cybersicherheit der öffentlichen und privaten Sektoren sowie der EU insgesamt. Sie löst die Vorgängerregelung NIS-1-Richtlinie aus dem Jahr 2016

ab. Im Text der NIS-2-Richtlinie wird der Vorgängerin eine große Rolle bei der Stärkung der Cyberresilienz bescheinigt, zudem habe sie in diesem Bereich ein „erhebliches Umdenken bewirkt“. Zwischenzeitlich hätten sich allerdings „inhärente Mängel ergeben, die ein wirksames Vorgehen gegen aktuelle und neue Herausforderungen im Bereich Cybersicherheit verhindern“.

Bis zum 17. Oktober 2024 müssen EU-Mitgliedsstaaten die NIS-2-Richtlinie in nationales Recht umsetzen. So sieht es die „Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union … (NIS-2-Richtlinie)“ vor. Verordnungen, beispielsweise die Datenschutz-Grundverordnung (DSGVO), gelten im Gegensatz dazu unmittelbar nach Inkrafttreten für jeden Einzelnen und sind rechtlich verbindlich.

Artikel 1 der neuen NIS-2-Richtlinie beschreibt deren Ziele. In erster Linie gehe es darum, „nationale Cybersicherheitsstrategien zu verabschieden sowie zuständige nationale Behörden, Behörden für das Cyberkrisenmanagement, zentrale Anlaufstellen für Cybersicherheit und Computer-Notfallteams (CSIRT) zu benennen oder einzurichten“. Außerdem beschäftigt sie sich mit Regelungen zum Cybersicherheitsmanagement, einschließlich entsprechender Berichtspflichten, dem Austausch von Cybersicherheitsinformationen zwischen den EU-Staaten sowie mit der Art und Weise der Aufsicht in den einzelnen Mitgliedsstaaten. Sektorspezifische Spezialgesetze gehen ebenfalls aus der NIS-2-Richtlinie hervor.

Mehr Sektoren und Unternehmen betroffen

Die NIS-2-Richtlinie erweitert den Anwendungsbereich auf zusätzliche Sektoren und Unternehmen (siehe Abbildung). In Anhang I zur Richtlinie finden sich Auflistungen von „Sektoren mit hoher Kritikalität“ sowie „sonstige kritische Sektoren“. Zu ersteren zählen Unternehmen im Bereich Energie, Verkehr,

Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, Abwasser, digitale Infrastruktur, Verwaltung von IKT-Diensten, öffentliche Verwaltung und Weltraum. Zur zweiten Gruppe zählen die Sektoren Post- und Kurierdienste, Abfallbewirtschaftung, Produktion, Umgang und Handel mit chemischen Stoffen oder Lebensmitteln, bestimmte Unternehmen im Bereich des verarbeitenden Gewerbes, Anbieter digitaler Dienste sowie Forschung.

Die NIS-2-Richtlinie weitet den Geltungsbereich ihrer Vorgängerin erheblich aus und deckt nun ebenfalls die rechts dargestellten Bereiche mit ab.
Unternehmen, die in mindestens einen der genannten Sektoren fallen, sind von der Richtlinie erfasst, wenn sie als „mittleres Unternehmen“ einzustufen sind. Das gilt für Firmen mit weniger als 250 Mitarbeitern und einem Jahresumsatz von unter 50 Millionen Euro beziehungsweise einer Jahresbilanz von unter 43 Millionen Euro. Ungeachtet ihrer Einstufung sind Anbieter öffentlicher Kommunikationsnetze und -dienste sowie Vertrauensdiensteanbieter und Namensregister der obersten Domäne einschließlich DNS-Diensteanbieter stets erfasst. Die Richtlinie führt weitere Kriterien für die Einstufung von Unternehmen als kritisch ein und erlaubt es den Mitgliedsstaaten, diese weiter zu verschärfen. So strebt sie

für die gesamte EU eine „Mindestharmonisierung“ an.

Kapitel 2 der Richtlinie legt Vorgaben für einen „Koordinierten Rahmen für die Cybersicherheit“ fest. Dazu zählt in erster Linie, dass sich jeder EU-Staat eine nationale Cybersicherheitsstrategie geben muss. Diese muss beispielsweise „die Bestimmung von Maßnahmen zur Gewährleistung der Vorsorge, Reaktionsfähigkeit und Wiederherstellung bei Sicherheitsvorfällen, einschließlich der Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor“ umfassen.

Ein Schwerpunkt in dieser nationalen Cybersicherheitsstrategie liegt auf IKT-Produkten und -Diensten. Ein weiterer auf „der allgemeinen Verfügbarkeit, Integrität und Vertraulichkeit des öffentlichen Kerns des offenen Internets“. Risikomanagementmaßnahmen sollen stets weiterentwickelt und auf dem neuesten Stand eingesetzt werden.

Die EU-Staaten müssen für die Cybersicherheit zuständige Behörden schaffen und dies der EU-Kommission mitteilen. Über sie sollen grenzüberschreitende Abstimmungen erfolgen. Sie sollen über „angemessene Ressourcen“ verfügen, um ihre Aufgaben wirksam und effizient wahrnehmen zu können, um die Ziele der NIS-2-Richtlinie zu erreichen.

Nationale Notfallteams

Die NIS-2-Richtlinie sieht außerdem die Schaffung von Computer-Notfallteams (CSIRTs) vor und beschreibt ausführlich, welchen Anforderungen diese genügen müssen. Sie müssen über eine hohe Erreichbarkeit verfügen und dafür redundante Kommunikationskanäle unterhalten. Sie sind an sicheren Standorten einzurichten, ihre Datenverarbeitung muss sicher und ihre Bereitschaft jederzeit gewährleistet sein. Zu ihren Aufgaben zählen die Überwachung und Analyse von Cyberbedrohungen, die Ausgabe von Frühwarnungen und Alarmmeldungen sowie die Information über Cyberbedrohungen,

die Reaktion auf Sicherheitsvorfälle, Lagebeurteilungen und Schwachstellenscans. Zudem soll es darüber im Rahmen des CSIRT-Netzwerks einen regelmäßigen Austausch geben.

Ein weiteres Ziel der Richtlinie ist es, die Zusammenarbeit zwischen den EU-Staaten im Bereich Cybersicherheit zu stärken. Eine Kooperationsgruppe soll beispielsweise Orientierungshilfen für die zuständigen Behörden ausarbeiten, den Austausch von Best Practices fördern, die EU-Kommission im Bereich der Cybersicherheit beraten oder den jeweils aktuellen Stand „in Bezug auf Cyberbedrohungen oder Sicherheitsvorfälle wie Ransomware“ beschreiben.

Die Abstimmung zwischen den EU-Staaten und ihren Behörden bildet einen klaren weiteren Schwerpunkt der NIS-2-Richtlinie. Zur Förderung einer raschen und wirksamen operativen Zusammenarbeit zwischen den CSIRTs soll ein Netzwerk entstehen. Darin geht es um Informationsaustausch, Technologietransfers und die gegenseitige Unterstützung. Über die Fortschritte beim Erreichen dieser Ziele sollen die Staaten regelmäßig berichten.

Des Weiteren werden die Aufgaben des Europäischen Netzwerks der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe) weiter konkretisiert. Es koordiniert künftig Maßnahmen bei „Cybersicherheitsvorfällen großen Ausmaßes und Krisen auf operativer Ebene und zur Gewährleistung eines regelmäßigen Austauschs relevanter Informationen zwischen den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der Union“. Auch hier soll eine regelmäßige Evaluierung der geleisteten Arbeit erfolgen.

Die Richtlinie beschreibt schließlich Grundsätze der internationalen Zusammenarbeit im Bereich der Cybersicherheit, die Erstellung zweijährlicher Berichte über den Stand der Cybersicherheit in der EU und Peer-Reviews innerhalb des CSIRT-Netzwerks.

Vorgaben beim Risikomanagement

Umfassende Vorgaben ergeben sich aus der NIS-2-Richtlinie an die jeweiligen nationalen Gesetzgeber im Bereich der Risikomanagementmaßnahmen. Dies beginnt mit Grundsätzen im Bereich der Governance. Leitungsorgane kritischer Einrichtungen müssen die ergriffenen Maßnahmen billigen, deren Umsetzung überwachen und für Verstöße verantwortlich gemacht werden können. Sie selbst müssen und ihre Mitarbeiter sollen regelmäßig an Schulungen teilnehmen, „um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben“.

Die Risikomanagementsysteme müssen geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen umfassen. Damit möchte man die Risiken für die genutzten Netz- und Informationssysteme bei Sicherheitsvorfällen verhindern oder zumindest minimieren. Dabei sind der Stand der Technik sowie geltende Vorschriften einzuhalten und ein „gefahrenübergreifender Ansatz“ zu wählen (siehe Kasten).

Risikomanagementmaßnahmen

Folgende Punkte müssen Risikomanagementsysteme nach der NIS-2-Richtlinie im Bereich der Cybersicherheit nach Artikel 21 Absatz 2 umfassen:

a. Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;
b. Bewältigung von Sicherheitsvorfällen;
c. Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;
d. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen

den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern;
e. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;
f. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;
g. grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;
h. Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;
i. Sicherheit des Personals, Konzepte für die Zugriffskontrolle und das Management von Anlagen;
j. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Bis 17. Oktober 2024 wird die EU-Kommission technische und methodische Anforderungen für die aufgelisteten Risikomanagementmaßnahmen erlassen. Diese gelten dann für „DNS-Diensteanbieter, TLD-Namenregister, Cloud-Computing-Dienstleister, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter von verwalteten Diensten, Anbieter von verwalteten Sicherheitsdiensten, Anbieter von Onlinemarktplätzen, Onlinesuchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter“.

Die Richtlinie schlägt den EU-Staaten vor, erfassten Unternehmen und Behörden bei eigenentwickelten und -genutzten IKT-Produkten und -Diensten eine Zertifizierung gemäß den Schemata für Cybersicherheitszertifizierungen vorzuschreiben. Bei der Sicherheit von Netz- und Informationssystemen sollen zudem internationale Normen und technische Spezifikationen gefördert werden. Nicht in der EU ansässige von der NIS-2-

Richtlinie erfasste Unternehmen müssen einen Vertreter innerhalb der EU benennen.

ENISA erstellt Register betroffener Einrichtungen

Die European Union Agency for Cybersecurity (ENISA) übernimmt die Aufgabe, ein EU-weites Register aller von der NIS-2-Richtlinie erfassten Einrichtungen im Bereich digitale Infrastruktur zu schaffen und zu pflegen, einschließlich Cloud-Anbieter, aber auch sozialer Netzwerke. Auf die Betreiber von TDL-Namensregistern und DNS-Registrierungsdienste sollen zusätzliche Pflichten zukommen. Sie müssen „genaue und vollständige Domänennamen-Registrierungsdaten in einer eigenen Datenbank im Einklang mit dem Datenschutzrecht der Union in Bezug auf personenbezogene Daten mit der gebotenen Sorgfalt sammeln und pflegen“.

Nationale Gesetze sollen es zusätzlich auch nicht von der Richtlinie erfassten Einrichtungen ermöglichen, „Informationen über Cyberbedrohungen, Beinahe-Vorfälle, Schwachstellen, Techniken und Verfahren, Kompromittierungsindikatoren, gegnerische Taktiken, bedrohungsspezifische Informationen, Cybersicherheitswarnungen und Empfehlungen für die Konfiguration von Cybersicherheitsinstrumenten zur Aufdeckung von Cyberangriffen“ auszutauschen. Aus kartellrechtlichen Gründen soll dies aber nur gelten, wenn es für das Management von Sicherheitsvorfällen erforderlich ist und der Informationsaustausch das Cybersicherheitsniveau erhöht.

Schließlich umfasst die NIS-2-Richtlinie Anweisungen zur Aufsicht und Durchsetzung der Vorgaben. Der Katalog an Kompetenzen für die zuständigen Behörden ist lang. Er reicht von Vor-Ort-Kontrollen bei den betroffenen Einrichtungen über Sicherheitsscans bis hin zu Vorgaben für die Nachweise zur Umsetzung der Cybersicherheitskonzepte. Die betroffenen Einrichtungen sind zur umfassenden Mitwirkung zu verpflichten.

Bei Rechtsverstößen sollen Warnungen und Handlungs- oder Unterlassungsanweisungen einschließlich Fristsetzungen möglich sein.

Bußgelder für Verstöße gegen die Vorgaben sollen „wirksam, verhältnismäßig und abschreckend“ sein. Bei Verstößen gegen die Pflichten im Bereich des Risikomanagements sollen Bußgelder für wesentliche Einrichtungen bei mindestens 10 Millionen Euro oder 2 Prozent des weltweiten Vorjahresumsatzes gedeckelt sein. Bei wichtigen Einrichtungen liegt die Grenze bei 7 Millionen Euro beziehungsweise 1,4 Prozent des weltweiten Vorjahresumsatzes.

EU-Maßnahmen-Portfolio

Die NIS-2-Richtlinie fügt sich in eine ganze Reihe von gesetzgeberischen Maßnahmen der EU ein. Sie ist Teil der „Gestaltung der digitalen Agenda Europas“, die sich die EU-Kommission 2020 als Vorhaben in ihrer Amtszeit bis zur Europawahl im Jahr 2024 gesetzt hat. Dazu gehören auch der derzeit diskutierte AI Act zur Regulierung des Einsatzes von künstlicher Intelligenz, der Cyber Resilience Act, der Digital Operational Resilience Act und weitere. Wegen der anstehenden Europawahl befinden sich zahlreiche Gesetzeswerke im Jahr 2023 auf der Zielgeraden (siehe „IT-Recht 2023: Viele neue EU-Regeln“ in iX 1/2023, S. 86).

Die NIS-2-Richtlinie adressiert die EU-Staaten, die die Vorgaben nun umsetzen müssen. Zahlreiche Regelungen beinhalten daher Aufforderungen wie „Die Mitgliedsstaaten stellen sicher …“ oder „Die Mitgliedstaaten können …“. In Deutschland dürfte es zu einer Überarbeitung des 2021 in Kraft getretenen IT-Sicherheitsgesetzes 2.0 kommen. Dies passt auch zur Vereinbarung im Koalitionsvertrag der Bundesregierung. Dort heißt es: „Die Cybersicherheitsstrategie und das IT-Sicherheitsrecht werden weiterentwickelt.“ Dort ist auch von „ehrgeiziger Cybersicherheitspolitik“ die Rede. Die Cybersicherheit bezeichnet der Koalitionsvertrag als „digitale

Schlüsseltechnologie“.

Fazit

Mit der Umsetzung der NIS-2-Richtlinie will die EU ein hohes gemeinsames Cybersicherheitsniveau sicherstellen, „um so das Funktionieren des Binnenmarkts zu verbessern“. So lautet das übergreifende Ziel. Um das zu erreichen, hat die EU den Anwendungsbereich der Richtlinie und die Aufgaben der zuständigen Behörden wesentlich erweitert und neue Behörden geschaffen. Die Mitgliedsstaaten sollen sich zudem besser austauschen und die Überwachung verschärfen.

Die ausdrücklichen Regelungen zur persönlichen Verantwortlichkeit der Leitungsorgane und die gleichzeitig signifikant erhöhten Bußgeldrahmen dürften für Zündstoff sorgen. Die EU unterstreicht damit die große Bedeutung der Cybersicherheit und reagiert auf steigende Risiken. Das Thema bleibt spannend und ein Dauerbrenner. In der EU sind nun erst einmal wieder die einzelnen EU-Staaten an der Reihe. Von der Richtlinie erfasste Unternehmen tun aber gut daran, den Gesetzgebungsprozess zu beobachten und zu begleiten. Sich früh auf anstehende Änderungen einzustellen ist für sie eine kluge Strategie. (jvo@ix.de)

1. Quellen
2. Tobias Haar; IT-Recht 2023: Viele neue EU-Regeln; iX 1/2023, S. 86
3. NIS-2-Richtlinie online verfügbar unter ix.de/z3zm