Kommunikation & Recht

K&R
11 | November 2023
26. Jahrgang
Seiten 705 - 768

dfv Mediengruppe
Frankfurt am Main

Kommunikation & Recht

RA Stephan Schmidt*

Neue europäische Anforderungen im Cybersicherheitsrecht – die NIS2-Richtlinie im Überblick

Kurz und Knapp

Verschiedene neue Rechtsakte sollen das Gerüst einer neuen europäischen Cybersicherheitsarchitektur bilden. Neben dem Cyber Resilience Act ist dabei die NIS2-Richtlinie ein wichtiger Baustein. Die NIS2-Richtlinie baut inhaltlich auf der ersten NIS-Richtlinie aus dem Jahr 2016 auf, erweitert jedoch den bisher auf kritische Infrastrukturen und ausgewählte Sonderfälle beschränkten Anwendungsbereich auf große Teile der Wirtschaft. Der Beitrag stellt die sich aus der Richtlinie ergebenden Anforderungen vor.

I. Die NIS2-Richtlinie als Baustein des Europäischen Cybersicherheitsrechts

1. Einführung

Mit Vorstellung der neuen europäischen Cybersicherheitsstrategie im Jahr 2022 wurde die Resilienz zu einem wesentlichen regulatorischen Aspekt.[1] In der Folge wurden diverse neue Rechtsakte auf den Weg gebracht: die Richtlinie „über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union“ (NIS2),[2] der Vorschlag einer Verordnung über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen („Cyber Resilience Act“ oder „CER-Richtlinie“),[3] der Rechtsakt zur Cybersicherheit („Cybersecurity Act“),[4] der delegierte Rechtsakt zur Funkanlagenrichtlinie („RED“)[5] sowie der Entwurf einer KI-Verordnung.[6] Cyber Resilience Act[7] und NIS2-Richtlinie wurden beide Ende 2022 verabschiedet und müssen bis zum 17. 10. 2024 in den Mitgliedstaaten umgesetzt sein. Der Cyber Resilience Act wird voraussichtlich durch das Gesetz zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen (KRITIS-Dachgesetz),[8] die NIS2-Richtlinie durch das NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG)[9] in nationales Recht umgesetzt.

Ziel der NIS2-Richtline ist, ausweislich ErwG 5, die großen Unterschiede zwischen den Mitgliedstaaten hinsichtlich der auferlegten Anforderungen an die Cybersicherheit von solchen Einrichtungen, die Dienste erbringen oder wirtschaftlich signifikante Tätigkeiten ausüben, zu beseitigen. Dies soll insbesondere durch Mindestvorschriften für einen funktionierenden und koordinierten Rechtsrahmen und Mechanismen für die wirksame Zusammenarbeit zwischen den zuständigen Behörden in den einzelnen Mitgliedstaaten erreicht werden. Die Liste der Sektoren und Tätigkeiten, für welche Pflichten im Hinblick auf die Cybersicherheit gelten, wird aktualisiert und es werden Abhilfe- und Durchsetzungsmaßnahmen eingeführt. Neben den inzwischen üblichen Bußgeldern bei Verstößen, ist insbesondere auch eine direkte Haftung der Geschäftsleitung vorgesehen.

2. Aufbau und Systematik der NIS2-Richtlinie

Die NIS2-Richtline ist in neun Kapitel gegliedert und enthält insgesamt 46 Artikel und 3 Anhänge. Wie üblich enthält Kapitel I allgemeine Bestimmungen zum Gegenstand und Anwendungsbereich sowie Definitionen. Kapitel II beschäftigt sich mit dem koordinierten Rahmen für die Cybersicherheit und in Kapitel III wird die internationale Zusammenarbeit geregelt. In Kapitel IV werden Risikomanagementmaßnahmen beschrieben und in Kapitel V Zuständigkeiten und Vorgaben für die Registrierung erläutert. In den Kapiteln VI und VII werden der Informationsaustausch zwischen den Mitgliedstaaten, sowie Aufsicht und Sanktionsmöglichkeiten erläutert.

---

* Mehr über den Autor erfahren Sie am Ende des Beitrags. Alle zitierten Internetquellen wurden zuletzt abgerufen am 22. 9. 2023.

1 Abrufbar unter https://www.consilium.europa.eu/de/policies/cybersecurity/.

2 RL (EU) 2022/2555 des Europäischen Parlaments und des Rates v. 14. 12. 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der VO (EU) Nr. 910/2014 und der RL (EU) 2018/1972 sowie zur Aufhebung der RL (EU) 2016/1148 (NIS2), ABl. L 333/80 zur Ablösung der geltenden NIS-RL, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32022L2555.

3 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der VO (EU) 2019/1020, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A52022PC0454.

4 VO (EU) 2019/881 des Europäischen Parlaments und des Rates v. 17. 4. 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der VO (EU) Nr. 526/2013, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32019R0881.

5 Aktueller Stand abrufbar unter https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13847-Cybersicherheit-Schutz-der-Privatsphare-und-Schutz-vor-Betrug-Verlangerung-des-Geltungsbeginns-delegierter-Rechtsakt-zur-Funkanlagenrichtlinie-_de.

6 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52021PC0206.

7 Ausführlich zum CRA *Hessel/Callewaert*, K&R 2022, 789 f.

8 Referentenentwurf abrufbar unter https://ag.kritis.info/2023/07/18/referentenentwurf-des-bmi-kritis-dachgesetz-kritis-dachg/.

9 Referentenentwurf vom 3. 7. 2023 abrufbar unter https://ag.kritis.info/2023/07/19/referentenentwurf-des-bmi-nis-2-umsetzungs-und-cybersicherheitsstaerkungsgesetz-nis2umsucg/.

II. Die NIS2-Richtlinie im Überblick

1. Anwendungsbereich

Mit der NIS2 halten neue Begrifflichkeiten Einzug: die bisher bekannten Betreiber wesentlicher Dienste und Anbieter digitaler Dienste werden durch wesentliche und wichtige Einrichtungen (Art. 3 NIS2) ersetzt. Neben den wesentlichen und wichtigen Einrichtungen kennt die NIS2 noch die Einrichtung, welche Domänennamen-Registrierungsdienste erbringt (Art. 6 Nr. 22 NIS2). Diese sind nach Art. 28 NIS2 verpflichtet, die Domänennamen-Registrierungsdaten in der Domänennamen-Registrierungsdatenbank zu sammeln und zu pflegen sowie auf berechtigte Anträge hin den Zugang dazu zu ermöglichen (Art. 28 Abs. 5 NIS2). Zudem trifft diese Einrichtungen die Verpflichtung aus Art. 27 Abs. 2 NIS2, bis zum 17. 1. 2023 und danach bei Änderungen bestimmte Daten an die zuständigen Behörden zu übermitteln.

Während es bei der alten NIS-Richtlinie den Mitgliedstaaten überlassen war, zu bestimmen, welche Einrichtungen die Kriterien für die Einstufung als Betreiber wesentlicher Dienste erfüllen, wird mit NIS2 eine sogenannte „Size-Cap-Rule" eingeführt.[10] Dies bedeutet, dass alle mittleren und großen Unternehmen, die in den von der Richtlinie erfassten Sektoren tätig sind oder Dienstleistungen erbringen, in den Anwendungsbereich der Richtlinie fallen. Die nachfolgend näher erläuterten Sektoren, Teilsektoren und Einrichtungen sollen nach Art. 40 NIS2 erstmals bis zum 17. 10. 2027 und danach alle 36 Monate von der EU-Kommission überprüft und in Bezug auf Relevanz der Größe und der Arten für das Funktionieren der Wirtschaft und der Gesellschaft in Bezug auf die Cybersicherheit bewertet werden.

a) Sektoren

In Anhang I und II nennt die NIS2 Einrichtungsarten für 11 besonders kritische und 7 kritische Sektoren.[11] Die Anzahl der Sektoren wird also im Vergleich zur Vorgängerrichtlinie erhöht. Die Einordnung wirkt sich auch darauf aus, ob eine Einrichtung als wesentlich oder als wichtig angesehen wird. Dabei sind „Anbieter digitaler Dienste" nun ein eigener Sektor in Anhang II, wobei es zu einigen Verschiebungen kommt. So finden sich Anbieter von Cloud-Computing-Diensten nun im Sektor „Digitale Infrastruktur" (Anhang I Nr. 8). Zudem wurden drei Sektoren mit hoher Kritikalität neu aufgenommen. Dies betrifft den Sektor 9 „Verwaltung von IKT-Diensten (Business-to-Business)", Sektor 10 „öffentliche Verwaltung", der Einrichtungen der Zentralregierungen und der öffentlichen Verwaltung auf regionaler Ebene enthält, sowie Sektor 11 „Weltraum", welcher Betreiber von Bodeninfrastrukturen zur Unterstützung weltraumgestützter Dienste umfasst. Letzterer war allerdings im deutschen Recht bereits als kritische Infrastruktur nach Anhang 7 Teil 3 Spalte A Nr. 1.7.2. BSI-KritisV eingestuft. In einigen der Sektoren in Anhang I gibt es auch neue Teilsektoren.

Sämtliche in Anhang II aufgeführten sonstigen kritischen Sektoren sind, bis auf die bereits bekannten und erwähnten „Anbieter digitaler Dienste", neu. Zu den sonstigen kritischen Sektoren gehören nun Post- und Kurierdienste (1.), Abfallbewirtschaftung (2.), Produktion, Herstellung und Handel mit chemischen Stoffen (3.), Produktion, Verarbeitung und Vertrieb von Lebensmitteln (4.), Verarbeitendes Gewerbe/Herstellung von Waren (5.) und Forschung (7.). Insbesondere die Erweiterung auf Herstellung von Waren in den in Anhang II genannten Teilsektoren (Medizinprodukte, Datenverarbeitungsgeräte, elektronische und optische Erzeugnisse, elektrische Ausrüstung, Maschinenbau, Kraftwagen und Kraftwagenteile sowie sonstiger Fahrzeugbau) führt, selbst unter Berücksichtigung der Ausnahme für Klein- und Kleinstunternehmen, zu einer deutlichen Erweiterung des Anwendungsbereichs der Richtlinie.[12]

b) Einrichtungstypen

Nach Art. 3 Abs. 1 und 2 NIS2 bestimmen drei Faktoren, ob eine Einrichtung wesentlich oder wichtig im Sinne der NIS2 ist: 1. die Einstufung als KRITIS-Betreiber, 2. die Zugehörigkeit zu einem Sektor und 3. die Größe des Unternehmens.

Einrichtungen in den sonstigen kritischen Sektoren gem. Anhang II NIS2 gelten dann als wesentlich, wenn sie bisher als KRITIS galten oder unter der CER-Richtlinie als KRITIS gelten. Alle anderen Einrichtungen aus den in Anhang II NIS2 genannten Sektoren gelten dann als wichtig, wenn sie mehr als 50 Mitarbeiter oder mehr als 10 Mio. Euro Jahresumsatz bzw. Bilanzsumme haben.

Auch bei den Sektoren mit besonders hoher Kritikalität gem. Anhang I NIS2 gelten alle Einrichtungen als wesentlich, die bisher als KRITIS galten oder unter der CER-Richtlinie als KRITIS gelten. Bei den übrigen Einrichtungen richtet sich die Einstufung nach den Sektoren und der Einrichtungsart sowie der Unternehmensgröße.

„Qualifizierte Vertrauensdiensteanbieter", „DNS-Diensteanbieter (ohne Root-Namensserver)", „TLD-Namensregister" und „Zentralregierungen" sind jeweils unabhängig von ihrer Größe wesentliche Einrichtungen. In den Sektoren des Anhang I, außer „Digitale Infrastruktur" (8.) und „öffentliche Verwaltung" (10.), wo Einrichtungen auf regionaler Ebene als wichtige Einrichtung gelten, gelten Einrichtungen dann als wesentlich, wenn sie mehr als 250 Mitarbeiter oder einen Jahresumsatz von mehr als 50 Mio. Euro bzw. eine Bilanzsumme von mehr als 43 Mio. Euro haben, also Großunternehmen sind. Mittlere Unternehmen in diesen Sektoren gelten als wichtig i. S. d. Richtlinie.

Im Sektor „Digitale Infrastruktur" (8.) ist die Einteilung etwas unübersichtlich. Anbieter öffentlicher elektronischer Telekommunikationsnetze und öffentlich zugänglicher Telekommunikationsdienste sind anders als in den übrigen Sektoren des Anhang I NIS2 schon dann wesentliche Einrichtungen, wenn sie mittlere Unternehmen sind. Wenn sie Klein- oder Kleinstunternehmen sind, fallen sie unter „wichtige Einrichtungen", sofern die Mitgliedstaaten keine abweichenden Regelungen treffen. Betreiber von Internetknoten, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten und Betreiber von Content-Delivery-Netzwerken (CDN) gelten, vergleichbar zu den anderen Sektoren, nur dann als wesentliche Einrichtungen, wenn sie Großunternehmen sind. Mittlere Unternehmen gelten auch hier als wichtige Einrichtungen. Bei Anbietern nicht-qualifizierter Vertrauensdienste gibt es wiederum nur zwei Stufen. Sie gelten dann als wesentlich, wenn sie Großunternehmen sind, und alle anderen Unternehmen gelten unabhängig von ihrer Größe als wichtig.

Die Einordnung als wesentliche oder wichtige Einrichtung wirkt sich nach der NIS2 vor allem auf den Umfang der

10 *Ritter*, RDV 2023, 152 ff.

11 Eine übersichtliche Darstellung der Sektoren mit Verweisen auf NACE und RCE ist abrufbar unter https://www.openkritis.de/it-sicherheitsgesetz/eu-nis-2-sektoren-rce-cer.html.

12 *Wegmann*, BB 2023, 835 f.

staatlichen Aufsicht und die Sanktionsmöglichkeiten, aber nur in Einzelfällen auf die zu treffenden Maßnahmen aus.

2. Ausnahmen vom Anwendungsbereich

Für Sektoren, die bereits einer cybersicherheitsrechtlichen Regulierung unterliegen und wenn die entsprechenden Anforderungen in ihrer Wirkung den in der NIS2 festgelegten Verpflichtungen zumindest gleichwertig sind, sieht Art. 4 NIS2 eine Ausnahme vom Anwendungsbereich der Richtlinie vor.[13] So legt ErwG 28 NIS2 beispielsweise die Verordnung über die Betriebsstabilität digitaler Systeme des Finanzsektors (DORA)[14] als sektorspezifische Regelung im Sinne der NIS2 fest.[15] In Art. 4 Abs. 3 NIS2 ist die Bereitstellung von Leitlinien der Europäischem Kommission zur Klärung des Verhältnisses zwischen den Normen bis zum 17. 10. 2024 vorgesehen.

3. Vorgaben für Einrichtungen

Wie bereits die Vorgängerrichtlinie sieht die NIS2 diverse Pflichten für die wesentlichen und wichtigen Einrichtungen vor, allerdings ohne dabei zwischen wesentlichen oder wichtigen Einrichtungen zu unterscheiden. Die Einstufung als wesentlich oder wichtig wird, wie bereits erwähnt, erst bei den Maßnahmen der Aufsichtsbehörden relevant.

a) Risikomanagement

Art. 21 NIS2 regelt, ähnlich der DSGVO, dass die betroffenen Einrichtungen „geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen und die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten“. Was die neu eingeführten „operativen“ Maßnahmen in Abgrenzung zu den technischen und organisatorischen Maßnahmen sein sollen, ergibt sich leider weder aus der Richtline selbst, noch aus den Erwägungsgründen.[16] Deutlich wird jedoch, dass die betroffenen Einrichtungen nunmehr hinsichtlich der gesamten IT, welche für den Betrieb oder die Erbringung der Dienste notwendig ist, verpflichtet werden. Bisher galt dies nach § 8a Abs. 1 BSIG nur für die Teile der IT, die für die Funktionsfähigkeit der betriebenen Kritischen Infrastrukturen maßgeblich sind.

Aus Art. 21 Abs. 2 NIS2 ergibt sich, dass es nicht nur um Gefahren geht, die sich aus Cyberbedrohungen ergeben, sondern auch um physische Gefahren für Netz- und Informationssysteme, sowie die Umwelt dieser Systeme. Die Richtlinie sieht dann ein Potpourri an Mindestmaßnahmen vor, bei dem nicht recht zu erkennen ist, welches System hinter der Aufzählung steckt. Zu den Maßnahmen gehören Risikoanalyse- und Sicherheitskonzepte, Maßnahmen zur Vorfallsbewältigung, Business Continuity und Krisenmanagement, Lieferkettensicherheit, Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Systemen, einschließlich Schwachstellenmanagement und -offenlegung, Konzepte und Verfahren zur Wirksamkeitsbewertung der Maßnahmen, Verfahren im Bereich der Cyberhygiene, Kryptografie, Multi-Faktor-Authentifizierung, Notfallkommunikationssysteme sowie Schulungen und weitere Maßnahmen zur Sicherheit des Personals.

Unternehmen müssen daher z. B. über ein funktionierendes Incident Response Management verfügen, welches zum einen Präventionsmaßnahmen und zum anderen angemessene Notfallmaßnahmen und einen gesicherten Prozess für den Umgang mit Sicherheitsvorfällen sicherstellt.

Die Maßnahmen müssen insgesamt dem Risiko angemessen sein, wobei der Stand der Technik, EU- und internationale Normen sowie die Umsetzungskosten zu berücksichtigen sind (Art. 2 Abs. 1 S. 2 NIS2).

Gemäß Art. 21 Abs. 5 NIS2 muss die Kommission bis zum 17. 10. 2024 Durchführungsrechtsakte für die technischen und methodischen Anforderungen an die Maßnahmen für DNS-Diensteanbieter, TLD-Namensregister, Cloud-Computing-Dienstleister, Anbieter von Rechenzentrumsdiensten, CDN-Betreiber, Anbieter verwalteter Dienste und verwalteter Sicherheitsdienste, Anbieter von Online-Marktplätzen, Suchmaschinen und Plattformen für Dienste sozialer Netzwerke sowie Vertrauensdiensteanbieter erlassen. Für die übrigen Sektoren können Durchführungsrechtsakte erlassen werden, dies ist jedoch nicht verpflichtend. Es bleibt abzuwarten, ob sich durch Durchführungsrechtsakte die durch die NIS2 geforderten, recht allgemeinen Maßnahmen noch konkretisieren.

b) Nutzung europäischer Cybersicherheitszertifizierungssysteme

Nach Art. 24 NIS2 können die Mitgliedstaaten Einrichtungen zudem dazu verpflichten, spezielle IKT-Produkte, -Dienste und -Prozesse zu verwenden, die von der Einrichtung entwickelt oder von Dritten beschafft werden und die im Rahmen europäischer Schemata für die Cybersicherheitszertifizierung zertifiziert[17] sind, um die Erfüllung bestimmter in Art. 21 NIS2 genannter Anforderungen nachzuweisen. Sofern ein unzureichendes Cybersicherheitsniveau festgestellt wird, ist die Kommission nach Art. 24 Abs. 2 NIS2 ermächtigt, im Rahmen von Durchführungsrechtsakten festzulegen, welche Kategorien wesentlicher und wichtiger Einrichtungen zur Nutzung vorgenannter Produkte, Verfahren und Dienste zu verpflichten sind.

Art. 29 NIS2 gibt Einrichtungen zudem auf, untereinander sowie mit Lieferanten und Dienstleistern auf freiwilliger Basis relevante Cybersicherheitsinformationen austauschen. Grundlage dieses Informationsaustausches sollen nach der Richtlinie Vereinbarungen über den Informationsaustausch im Bereich der Cybersicherheit sein (Art. 29 Abs. 2 NIS2), über deren Abschluss und Beendigung die Einrichtungen die Behörden informieren müssen (Art. 29 Abs. 4 NIS2).

c) Melde- und Informationspflichten

Der NIS2 unterliegende Einrichtungen müssen erhebliche Sicherheitsvorfälle nach Art. 23 NIS2 melden. Erheblich ist ein Sicherheitsvorfall dann, wenn er erhebliche Auswirkungen auf die Erbringung der Dienste hat, also gemäß Art. 23 Abs. 3 NIS2 schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann oder Dritte durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann.

Die Richtlinie sieht für die Meldung ein dreistufiges Verfahren[18] vor, nachdem unverzüglich, in jedem Fall aber inner-

13 *Voigt/Bastians*, CR 2022, 768, 773 f.
14 Abrufbar unter https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595.
15 Siehe auch ErwG 16 DORA, wonach DORA als lex specialis gegenüber der NIS anzusehen ist.
16 So auch *Ritter*, RDV 2023, 152 ff.
17 Siehe Art. 49 der VO (EU) 2019/881.
18 Auch in DORA ist ein Stufenkonzept für die Meldepflicht bei Cybervorfällen vorgesehen, dazu *Dittrich/Heinelt*, RDi 2023, 164, 167.

halb von 24 Stunden eine Frühwarnung (frühe Erstmeldung) mit einer Einschätzung dazu abgegeben wird, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte. Unverzüglich, in jedem Fall aber innerhalb von 72 Stunden, muss dann eine aktualisierte Meldung (bestätigende Erstmeldung) mit einer ersten Vorfallsbewertung erfolgen. Spätestens einen Monat nach Übermittlung der aktualisierten Meldung ist ein Abschlussbericht (Abschlussmeldung) vorzulegen, welcher eine ausführliche Vorfallsbeschreibung mit Angaben zu Schweregrad und Auswirkungen, der Art der Bedrohung bzw. Vorfallsursache, zu Abhilfemaßnahmen und etwaigen grenzüberschreitenden Auswirkungen enthalten muss.

Auf Ersuchen eines CSIRT oder gegebenenfalls der zuständigen Behörde muss zudem ein Zwischenbericht (Zwischenmeldung) über relevante Statusaktualisierungen vorgelegt werden. Dies gilt auch dann und ohne Aufforderung durch eine Behörde, wenn ein Vorfall nach einem Monat noch andauert und daher innerhalb dieser Frist kein Abschlussbericht vorgelegt werden kann (sogenannte Fortschrittsmeldung).

Zwar ist zu begrüßen, dass durch kurze Fristen und ein sehr früh ansetzendes Meldeverfahren dem Bedürfnis nach möglichst schnellen Informationsflüssen Rechnung getragen wird, allerdings wird dies insbesondere bei mittleren Unternehmen zu erhöhten Aufwänden und (Personal-)Kosten führen, da die 24 Stunden für eine Frühwarnung nicht nur an Werktagen, sondern auch am Wochenende oder an Feiertagen laufen. Auf der anderen Seite bleibt jedoch völlig unklar, wie die Behörden mit diesen Meldungen umzugehen haben. Regelungen dazu gibt es in der NIS2 nicht.

In besonders schweren Fällen, dann wenn der erhebliche Sicherheitsvorfall die Erbringung des jeweiligen Dienstes beeinträchtigen kann, müssen auch die Nutzer (Empfänger der Dienste – Art. 23 Abs. 2 NIS2) und ggfs. sogar die Öffentlichkeit (Art. 23 Abs. 7 NIS2) informiert werden. Betroffene Einrichtungen müssen daher prüfen, ob die vorhandene Krisenkommunikation die gesetzlichen Pflichten erfüllen kann. Die NIS2 trifft jedoch keine Aussage dazu, wann genau eine „Sensibilisierung der Öffentlichkeit" i. S. d. Art. 23 Abs. 7 NIS2 erforderlich ist. Der Wortlaut „um einen erheblichen Sicherheitsvorfall zu verhindern oder einen laufenden erheblichen Sicherheitsvorfall zu bewältigen" bietet keine weiteren Anhaltspunkte. Und auch wann der Sicherheitsvorfall im öffentlichen Interesse liegt, erläutert die Richtlinie nicht. Zu beachten ist jedoch insoweit, dass es nach dem Wortlaut nicht auf eine Abwägung mit etwaigen Geheimhaltungsinteressen der Einrichtungen ankommt.[19]

d) Einrichtungen ohne Niederlassung in der Union

Bestimmte Einrichtungen, welche Dienste innerhalb der EU anbieten, ohne eine Niederlassung in der EU zu haben, müssen nach Art. 26 Abs. 3 NIS2 einen Vertreter in einem der Mitgliedstaaten benennen. Die Pflicht trifft nur die in Art. 26 Abs. 1 lit. b NIS2 genannten Einrichtungen, also DNS-Diensteanbieter, TLD-Namenregister, Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter von verwalteten Diensten, Anbieter von verwalteten Sicherheitsdiensten sowie Anbieter von Online- Marktplätzen, Online-Suchmaschinen oder Plattformen für Dienste sozialer Netzwerke.

Die von der Vertreterbenennung betroffenen Einrichtungen müssen sich außerdem nach Art. 27 NIS2 bei den Behörden registrieren und für das Einrichtungsregister bei der ENISA folgende Daten übermitteln: Name, Anschrift und Kontaktdaten der Einrichtung, Informationen zum Sektor, Teilsektor und Art der Einrichtung, Anschrift des Vertreters nach Art. 26, Benennung der Mitgliedstaaten, in denen die Einrichtung Dienste erbringt, und der IP-Adressbereiche der Einrichtung. Bei unterlassener Registrierung trotz bestehender Verpflichtung kann ein Bußgeld drohen.[20]

e) Chefsache Cybersecurity

Nach NIS2 trägt die Geschäftsleitung des Unternehmens die zentrale Verantwortung für das Risikomanagement und die Umsetzung von Cybersicherheitsmaßnahmen. Sie muss daher verpflichtend an Cybersicherheits-Schulungen teilnehmen und sicherstellen, dass Awareness-Maßnahmen durchgeführt und auch allen Mitarbeitenden entsprechende Schulungen angeboten werden. Die Mitgliedstaaten müssen nach Art. 20 Abs. 1 NIS2 sicherstellen, dass die Leitungsorgane von Unternehmen, die über die Maßnahmen zur Einhaltung der Cybersicherheitspflichte gemäß Art. 21 NIS2 entscheiden, direkt haftbar gemacht werden können. Nach dem derzeitigen Entwurf des NIS2UmsuCG und der Entwurfsfassung des § 2 Abs. 1 Nr. 11 BSIG zählen diejenigen natürlichen Personen zur Geschäftsleitung, die nach Gesetz, Satzung oder Gesellschaftsvertrag zur Führung der Geschäfte und zur Vertretung einer Einrichtung berufen sind. Dies umfasst u. a. den Vorstand einer AG, Geschäftsführer der GmbH, Vorstände oder besondere Vertreter eines Vereins sowie die Leitungspersonen in öffentlichen Einrichtungen, etwa die Behördenleitung.

Neben Art. 20 enthalten auch Art. 32 Abs. 6 und 33 Abs. 5 NIS2 Regelungen zur persönlichen Haftung von Leitungsorganen. Was den konkreten Sorgfaltsstandard angeht, wird es jedoch im besonderen Maße auf die konkrete nationale Umsetzungsgesetzgebung ankommen, da NIS2 einen solchen nicht festlegt.[21]

III. Überwachung und Sanktionen

Mit NIS2 erhalten die nationalen Behörden eine Vielzahl an Kontroll- und Sanktionsmöglichkeiten. Die Aufsichtsbefugnisse sind dabei insgesamt deutlich umfassender als bislang z. B. in den §§ 8a ff. BSIG geregelt und lassen sich in Aufsichts- und Durchsetzungsmaßnahmen unterteilen.

1. Aufsichtsmaßnahmen

In Art. 32 Abs. 2 NIS2 sind die Aufsichtsmaßnahmen für wesentliche Einrichtungen beschrieben, während sich die fast deckungsgleichen Maßnahmen für wichtige Einrichtungen in Art. 33 Abs. 2 finden. Grundsätzlich gilt, dass wesentliche Einrichtungen auch anlasslos kontrolliert werden können, während bei wichtigen Einrichtungen die Aufsicht eher nachträglich und (nur) anlassbezogen erfolgen soll. Vorgesehen sind bei wesentlichen Einrichtungen unter anderem Vor-Ort-Kontrollen, externe Aufsichtsmaßnahmen, einschließlich von geschulten Fachleuten durchgeführte Stichprobenkontrollen, Sicherheitsprüfungen und Ad-hoc-Prüfungen, einschließlich solcher, die aufgrund eines erheblichen Sicherheitsvorfalls oder Verstoßes gegen die Richtlinie gerechtfertigt sind. Bisher

19 *Voigt/Bastians*, CR 2022, 768, 772.
20 Zu einem aktuellen Bußgeldverfahren wegen Verstoßes gegen die Registrierungspflicht nach § 14 Abs. 2 Nr. 5 BSI vgl. *Dittrich*, MMR-Aktuell 2023, 457211.
21 *Wegmann*, BB 2023, 835 f.

hatte das BSI konkrete Betretungs- und Kontrollrechte nur im Hinblick auf die Kommunikationstechnik des Bundes (vgl. § 4a Abs. 1 - 3 BSIG) und gegenüber den Betreibern kritischer Infrastrukturen (§ 8a Abs. 4 BSIG). Die Befugnisse der Behörden werden hier also deutlich erweitert.

Nachweise, Hinweise oder Informationen, wonach eine wichtige Einrichtung mutmaßlich den Vorgaben der NIS2 nicht nachkommt, können Anlass für nachträgliche Kontrollen sein. Erlaubt sind bei derartigen Kontrollen auch durch die Behörde oder eine unabhängige Stelle durchgeführte Sicherheitsüberprüfungen.

Sicherheitsscans dürfen Aufsichtsbehörden bei allen Einrichtungen durchführen, erforderlichenfalls in Zusammenarbeit mit der jeweiligen Einrichtung (Art. 32 Abs. 2 lit. d bzw. Art. 33 Abs. 2 lit. c NIS2). Ebenfalls für alle Einrichtungsarten ist ein Recht der Aufsicht auf Zugang zu aufsichtsrelevanten Daten, Dokumenten und sonstigen Informationen vorgesehen sowie die Befugnis, Nachweise für die Umsetzung der Cybersicherheitskonzepte zu verlangen. Bei wesentlichen Einrichtungen können anlasslos auch Informationen für die Bewertung der ergriffenen Cybersicherheitsmaßnahmen und Überprüfung der Verpflichtung zur Datenübermittlung nach Art. 27 NIS2 verlangt werden. Für wichtige Einrichtungen sieht die Richtlinie diese Bewertung nur anlassbezogen vor.

2. Durchsetzungsmaßnahmen

Zusätzlich zu den Aufsichtsmaßnahmen sehen Art. 32 Abs. 4 und 5 NIS2 gegenüber wesentlichen Einrichtungen und Art. 33 Abs. 4 NIS2 gegenüber wichtigen Einrichtungen Durchsetzungsmaßnahmen vor. Die nationalen Behörden werden aufgrund dieser Regelungen befugt sein, Warnungen über Verstöße herauszugeben oder Einrichtungen anzuweisen, Aspekte der Verstöße öffentlich bekannt zu machen.

Nach Abs. 4 lit. b NIS2 dürfen Behörden verbindliche Anweisungen zur Beseitigung von Mängeln und Verstößen gegen die Richtlinie erlassen sowie Anweisungen erteilen, das entsprechende Verhalten einzustellen und nicht zu wiederholen (Abs. 4 lit. c NIS2). Gegenstand einer Anweisung kann auch sein, nach bestimmten Vorgaben sicherzustellen, dass die Art. 21- und Art. 23-Pflichten erfüllt werden (Abs. 4 lit. d NIS2), oder die Empfehlungen aus einer Sicherheitsüberprüfung umzusetzen (Abs. 4 lit. f NIS2).

Gegenüber wesentlichen Einrichtungen kann zudem nach Art. 32 Abs. 4 lit. b NIS2 eine Anweisung erteilt werden, fristgebundene Maßnahmen zur Verhütung und Behebung eines Sicherheitsvorfalles vorzunehmen und darüber Bericht zu erstatten.

Wenn eine wesentliche Einrichtung den Anweisungen einer Behörde nicht folgt, kann die Behörde nach Art. 32 Abs. 5 NIS2 als weitere Eskalationsstufe Zertifizierungen oder Genehmigungen für manche oder alle von der Einrichtung erbrachten entsprechenden Dienste oder Tätigkeiten vorübergehend aussetzen und einzelnen leitenden Personen ein Tätigkeitsverbot auferlegen, indem untersagt werden kann, Leitungsaufgaben in der Einrichtung wahrzunehmen. Beide Durchsetzungsmaßnahmen sind jedoch zeitlich bis zu dem Zeitpunkt begrenzt, in dem das Ziel, also die Umsetzung der Anweisung, erreicht wird. Gegenüber Einrichtungen der öffentlichen Verwaltung können diese Maßnahmen nicht ergriffen werden. Während noch nachvollziehbar ist, dass die öffentliche Verwaltung in Deutschland von Bußgeldern ausgenommen wird (basierend auf Art. 34 Abs. 7 NIS2), ist diese Ausnahme wenig verständlich, da so jedes Druckmittel zur Durchsetzung von Cybersicherheitsmaßnahmen gegenüber der öffentlichen Verwaltung fehlt.

3. Bußgelder

War die konkrete Gestaltung der Bußgeldvorschriften durch die NIS-RL noch den Mitgliedstaaten überlassen, ähneln die Bußgeldvorschriften nun den Vorschriften aus anderen EU-Rechtsakten (z. B. Art. 83 DSGVO, Art. 52 DSA). Bei Verstößen drohen wesentlichen Einrichtungen Bußgelder von bis zu 10 Mio. Euro oder 2 % des weltweiten Jahresumsatzes. Wichtigen Einrichtungen drohen Bußgelder bis zu 7 Mio. Euro oder 1,4 % des weltweiten Jahresumsatzes (Art. 34 Abs. 4, 5 NIS2). Die Bußgelder liegen damit unter dem bisher aus dem BSIG resultierenden Rahmen, welcher Bußgelder bis zu 20 Mio. Euro zuließ. Nach Art. 34 Abs. 1 NIS2 sind die Mitgliedstaaten verpflichtet, die Bußgeldregelungen und damit auch die nach dem weltweiten Jahresumsatz berechnete Geldbuße in nationales Recht umzusetzen. Die Mitgliedstaaten können jedoch bei den Bußgeldhöhen nach oben von den Regelungen abweichen.

IV. Das deutsche NIS2-Umsetzungsgesetz

Seit dem 3. 7. 2023 liegt der aktuelle Referentenentwurf des NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG)[22] vor. Die zusätzliche Bezeichnung „Cybersicherheitsstärkungsgesetz“ lässt erkennen, dass der Entwurf des NIS2UmsuCG über die Vorgaben der NIS2 hinausgeht und für Deutschland spezifische Neuerungen bringt. Dies ist möglich, weil die NIS2 den Ansatz der Vollharmonisierung, anders als noch die NIS-RL, aufgibt und sich auf eine Mindestharmonisierung beschränkt (Art. 5 NIS2).

Das NIS2UmsuCG wird als komplexes Änderungsgesetz die Vorschriften verschiedener Gesetze und insbesondere des BSIG ändern und ergänzen. Da es sich derzeit nur um einen Referentenentwurf handelt, soll auf einzelne Regelungen an dieser Stelle nicht im Detail eingegangen werden. Allerdings zeigen die geplanten Änderungen bereits jetzt, dass der deutsche Gesetzgeber seinen Spielraum nutzen möchte, dabei allerdings teilweise auch die Regelungen der NIS2 verschärft und durch die Einführung eigener Definitionen und Abgrenzungen leider nicht immer für mehr Klarheit sorgt.

So führt der Entwurf eine, der NIS2 nicht bekannte, weitere Kategorie von Einrichtungen ein. Zu den wichtigen und wesentlichen (in der deutschen Umsetzung: „besonders wichtigen“) Einrichtungen kommen nach § 28 Abs. 1 BSIG-E in Deutschland die Betreiber kritischer Anlagen. Nach § 2 Abs. 1 Nr. 19 BSIG-E sind dies Anlagen, die für das Funktionieren des Gemeinwesens von hoher Bedeutung sind, da durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Der Begriff „Kritische Anlage“ ersetzt den Begriff der Kritischen Infrastrukturen i. S. d. BSIG. Grund dieser stärkeren Aufgliederung ist wohl der sektoren- und gefahrenübergreifende Ansatz des Gesetzes zum Schutz Kritischer Infrastrukturen („KRITIS-Dachgesetz“) und der Bedarf des deutschen Gesetzgebers die Begrifflichkeiten dort einordnen zu können.[23]

Auch Schwellenwerte und Sektoren im NIS2UmsuCG sind etwas anders als in der NIS2. So werden Einrichtungen nach

22 Referentenentwurf vom 3. 7. 2023 abrufbar unter https://ag.kritis.info/2023/07/19/referentenentwurf-des-bmi-nis-2-umsetzungs-und-cybersicherheitsstaerkungsgesetz-nis2umsucg/.

23 *Nardone*, ITRB 2023, 182 f.

Unternehmensgröße unterschieden – die Definitionen im NIS2UmsuCG von Großunternehmen (§ 2 Abs. 1 Nr. 12) und mittleren Unternehmen (§ 2 Abs. 1 Nr. 23) weichen jedoch von Art. 3 NIS2 und der Empfehlung 2003/361/EG[24] ab. Bei mittleren Unternehmen müssen die Schwellenwerte für Mitarbeiter und Umsatz oder Bilanz erfüllt sein, bei Großunternehmen reicht bereits die Überschreitung eines Schwellenwerts, also Mitarbeiterzahl oder Umsatz und Bilanz.

Eine weitere wesentliche Abweichung von NIS2 ergibt sich nach dem vorliegenden Entwurf aus § 38 Abs. 3 BSIG-E, wonach ein Verzicht einer Einrichtung auf Ersatzansprüche gegen die Geschäftsleitung nach § 38 Abs. 2 BSIG-E oder ein Vergleich der Einrichtung über diese Ansprüche unwirksam sein soll.[25] Dies soll nur dann nicht gelten, wenn der Ersatzpflichtige zahlungsunfähig ist und sich zur Abwendung des Insolvenzverfahrens mit seinen Gläubigern vergleicht oder wenn die Ersatzpflicht in einem Insolvenzplan geregelt wird.

Auch der Rahmen der Bußgelder liegt mit einem Maximalwert von 20 Mio. Euro über den Anforderungen der NIS2.

V. Fazit und Ausblick

Die NIS2-Richtlinie ist zwar nicht ganz mit dem breiten Anwendungsbereich der DSGVO vergleichbar und für bisherige KRITIS-Betreiber bringt sie wenig Neues, dennoch ist sie nicht nur eine kleine Anpassung der bereits vorhandenen Cybersicherheitsgesetzgebung. Die Richtline erfasst viele Unternehmen erstmals aufgrund ihrer Größe und ihrer Leistungen oder Produkte und diese Unternehmen müssen nun allgemeine Cybersicherheitspflichten erfüllen und insoweit auch ihre IT-Verträge anpassen.[26] Viele Details der zu treffenden Maßnahmen werden jedoch davon abhängen, wie der deutsche Gesetzgeber seinen Entscheidungsspielraum nutzt und die NIS2 konkret umsetzt.[27] Der derzeit vorliegende Entwurf geht davon aus, dass das Änderungsgesetz im Frühjahr 2024 verabschiedet wird. Zudem wird abzuwarten sein, wie die Konkretisierung der Maßnahmen durch EU, BSI oder Verbände insbesondere zum Stand der Technik aussehen wird und wie sich die zu treffenden Maßnahmen in bestehende Cybersecurity Standards wie ISO 27001 oder C5 einfügen lassen.

Stephan Schmidt
ist Gründungspartner bei TCI Rechtsanwälte in Mainz und Fachanwalt für IT-Recht. Er berät nationale und internationale Mandanten im IT-, Technologie- und Datenschutzrecht. Er ist Mitglied des Geschäftsführenden Ausschusses der davit.

24 Abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32003H0361.
25 *Kipker/Dittrich*, MMR 2023, 481, 486, die in dieser Regelung eine Verbotsnorm i. S. d. § 134 Abs. 1 BGB sehen.
26 Dazu ausführlich *Hessel/Callewaert/Klose*, MMR 2023, 471.
27 Siehe dazu den Referentenentwurf vom 3. 7. 2023, abrufbar unter https://ag.kritis.info/2023/07/19/referentenentwurf-des-bmi-nis-2-umsetzungs-und-cybersicherheitsstaerkungsgesetz-nis2umsucg/.

RA Dr. Timo Handel*

Medien- und IT-Strafrecht 2022/2023

Kurz und Knapp

Der vorliegende Beitrag beschäftigt sich mit ausgewählten aktuellen und aus Sicht des Verfassers interessanten Entwicklungen des Medien- und IT-Strafrechts in den Jahren 2022 und 2023, wobei auch das Ordnungswidrigkeitenrecht umfasst ist. Dargestellt werden Entwicklungen in Gesetzgebung, Verwaltung und Rechtsprechung.

I. Gesetzgebung

Aus dem Bereich der Gesetzgebung sind die E-Evidence-VO (siehe 1.) und der Digital Services Act (DSA; siehe 2. a) der EU hervorzuheben. Eingegangen wird zudem auf den Referentenentwurf eines Digitale-Dienste-Gesetzes (DDG-RefE; siehe 2. b) und den Referentenentwurf eines KRITIS-DachG (siehe 3.).

1. E-Evidence-VO

Am 28. 7. 2023 wurde die sog. E-Evidence-Verordnung[1] im Amtsblatt der EU veröffentlicht.[2] Sie gilt ab dem 18. 8. 2026 unmittelbar (Art. 34 Abs. 2 E-Evidence-VO) und betrifft Diensteanbieter, die Dienste in der Europäischen Union anbieten (Art. 2 Abs. 1 E-Evidence-VO). Solche sind natürliche und juristische Personen als Anbieter von elektronischen Kommunikationsdiensten,[3] Internetdomänennamen- und IP-Nummerierungsdiensten[4] oder anderen Diensten der Informationsgesellschaft,[5] wobei Finanzdienstleistungen i. S. d. Art. 2 Abs. 2 lit. b RL 2006/123/EG ausgenommen sind (Art. 3 Nr. 3 E-Evidence-VO).

Ziel der Verordnung ist die europaweit einheitliche Einholung und Sicherung von elektronischen Beweismitteln zur Kriminalitätsbekämpfung in grenzüberschreitenden Konstellationen (vgl. ErwG 2 E-Evidence-VO). Vor diesem Hintergrund regelt sie eine Europäische Herausgabeanordnung und eine

* Mehr über den Autor erfahren Sie am Ende des Beitrags. Alle zitierten Internetquellen wurden zuletzt abgerufen am 9. 10. 2023.
1 VO (EU) 2023/1543 des Europäischen Parlaments und des Rates vom 12. 7. 2023 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren.
2 ABl. L 191/118 v. 28. 7. 2023.
3 Art. 2 Nr. 4 RL (EU) 2018/1972.
4 Bspw. Dienste der IP-Adressenzuweisung und der Domänennamen-Registrierung, Domänennamen-Registrierungsstellendienste und mit Domänennamen verbundene Datenschutz- und Proxy-Dienste (Art. 3 Nr. 3 lit. b E-Evidence-VO).
5 Im Sinne des Art. 1 Abs. 1 lit. b RL (EU) 2015/1535, die es ihren Nutzern ermöglichen, miteinander zu kommunizieren, oder die es ermöglichen, für Nutzer, für welche die Dienstleistung erbracht wird, Daten zu speichern oder auf sonstige Weise zu verarbeiten, sofern die Speicherung von Daten ein bestimmender Bestandteil der für den Nutzer erbrachten Dienstleistung ist (Art. 3 Nr. 3 lit. c E-Evidence-VO).