Kommunikation & Recht

K&R
5 | Mai 2026
29. Jahrgang
Seiten 293 - 364

dfv Mediengruppe
Frankfurt am Main

Kommunikation & Recht

K&R 5/2026 293

RA Prof. Dr. Alexander Koch*

Nach der Umsetzung der NIS-2-Richtlinie ist vor der Reform der NIS-2-Richtlinie

Kurz und Knapp

Inzwischen liegen erste Erfahrungen mit der Umsetzung der NIS-2-RL vor und es haben sich verschiedene Probleme gezeigt. Gleichzeitig hat sich die Cybersicherheitslage weiterentwickelt. Die Kommission arbeitet deshalb an einer Reform des Cybersicherheitsrechts und hat hierfür Anfang 2026 Vorschläge vorgelegt, durch die u. a. die NIS-2-RL überarbeitet werden soll. Weitere Änderungen sind u. a. im Rahmen der Digital-Omnibus-Verordnung geplant.

I. Einleitung

Die bisherige Umsetzung der NIS-2-RL (EU) 2022/2555[1] in den Mitgliedstaaten hat gezeigt, dass in der Praxis mehr Unternehmen erfasst wurden, als von der Kommission ursprünglich beabsichtigt. Teilweise ist der Anwendungsbereich übermäßig weit ausgestaltet – so werden derzeit alle DNS-Diensteanbieter unabhängig von ihrer Größe erfasst –, teilweise haben sich schlicht Auslegungsprobleme gezeigt – etwa hinsichtlich der im Gesundheitssektor erfassten Unternehmen (hierzu unter II. 2. und II. 6.). Die Kommission erhofft sich von den nun vorgesehenen Änderungen erhebliche Kostenreduzierungen für die Wirtschaft.[2] Hierzu soll auch die Einführung neuer Schwellenwerte beitragen. Bislang werden Unternehmen – aus den relevanten Branchen –, die die KMU-Schwelle überschreiten, als „wesentliche" (Terminologie der NIS-2-RL) bzw. „besonders wichtige" (Terminologie des BSIG – im Folgenden wird die Terminologie der NIS-2-RL verwendet) Einrichtung erfasst. Künftig sollen erst Unternehmen oberhalb der Schwelle für Midcap-Unternehmen als wesentliche Einrichtungen erfasst werden (hierzu unter II. 1.). Die Kommission möchte den Anwendungsbereich der NIS-2-RL aber auch ausweiten. Sie reagiert hiermit auf Veränderungen in der Weltsicherheitslage. Exemplarisch hierfür ist die Erfassung von Untersee-Datenkabeln (hierzu unter III. 2.) oder von strategisch bedeutsamen zivilen Infrastrukturen, die für transeuropäische Truppentransporte benötigt werden (hierzu unter III. 3.). Schließlich nimmt die Kommission (vermeintliche) Detailanpassungen vor – etwa betreffend eine Informationspflicht über gezahlte Ransomware-Lösegelder (hierzu unter IV.).

II. Einschränkung des Anwendungsbereichs

1. Midcap-Unternehmen

Die NIS-2-RL erfasst bislang – unter Bezugnahme auf die KMU-Definition der Empfehlung 2003/361/EG – als „wesentliche" Einrichtung bestimmte „mittlere Unternehmen". Darunter fallen Unternehmen, die mindestens 250 Mitarbeitende beschäftigen oder einen Jahresumsatz von über 50 Millionen Euro und zudem eine Jahresbilanzsumme von über 43 Millionen Euro aufweisen.[3] Der Vorschlag der Kommission ersetzt den Begriff der „mittleren Unternehmen" nun durch Unternehmen, welche „die Obergrenzen für kleine Midcap-Unternehmen überschreiten".[4] Er nimmt dabei Bezug auf die Empfehlung (EU) 2025/1099. Erfasst werden sollen zukünftig – als wesentliche Einrichtung – erst Unternehmen ab einem Schwellenwert von 750 Beschäftigten oder einem Jahresumsatz von über 150 Millionen Euro oder einer Jahresbilanzsumme von über 129 Millionen Euro. Der Schwellenwert wird also deutlich nach oben verschoben und es kommt damit zu einer Umgruppierung von Unternehmen aus der Gruppe der wesentlichen in die Gruppe der wichtigen Einrichtungen. Für die betroffenen Unternehmen hat dies insbesondere Auswirkungen bei den Aufsichtsmaßnahmen, denen sie unterliegen.[5] Die Änderung wirkt sich also nicht darauf aus, *ob* Einrichtungen erfasst werden, sondern nur auf das „Wie" der Regulierung. Es fallen zukünftig also mehr Unternehmen in die Gruppe der „nur" wichtigen Einrichtungen und unterliegen damit nicht der strengeren Regulierung für wesentliche Einrichtungen.

2. DNS-Diensteanbieter

Bislang erfasst Art. 3 Abs. 1 lit. b der NIS-2-RL DNS-Diensteanbieter unabhängig von Schwellenwerten als wesentliche Einrichtung. Das ist im deutschen Gesetzgebungsverfahren deutlich kritisiert worden. Es wurde befürchtet, die weite Fassung führe dazu, dass etwa Hotel-WLANs oder gemeinnützige Initiativen wie Freifunk nun unter das strenge Regime für wesentliche Einrichtungen fallen, wenn sie einen eigenen DNS-Dienst anbieten.[6] Der Vorschlag der Kommission streicht die DNS-Diensteanbieter aus der genannten Vorschrift.[7]

DNS-Diensteanbieter werden aber weiterhin in Anhang I Sektor „Digitale Infrastruktur" tir. 2 der NIS-2-RL als Einrichtung mit hoher Kritikalität aufgelistet. Das heißt, DNS-Diensteanbieter

* Mehr über den Autor erfahren Sie am Ende des Beitrags. Alle zitierten Internetquellen wurden zuletzt abgerufen am 17. 3. 2026.

1 Siehe hierzu *Koch*, N&R 2026, 13 sowie *Dittrich/Kipker*, NJW 2026, 193; *Karniyevich*, K&R 2026, 82; *Voigt/Schmalenberger*, CR 2026, 17. Siehe zur geplanten Reform auch *Schmidt*, K&R 2026, 226, 230.

2 Vorschlag der Kommission für einen Rechtsakt zur Cybersicherheit 2, COM(2026) 11 endgültig (im Folgenden „COM(2026) 11"), S. 187 f.

3 Vgl. die Definition in Art. 2 Abs. 1 Empfehlung 2003/361/EG und § 28 Abs. 1 Nr. 4 BSIG.

4 Art. 1 Abs. 2 (a) (i) des Vorschlags der Kommission zur Änderung der NIS-2-RL, COM(2026) 13 endgültig (im Folgenden „COM(2026) 13") zur Änderung von Art. 3 Abs. 1 lit. d der NIS-2-RL.

5 Vgl. ausführlicher zu den unterschiedlichen Regulierungsansätzen: *Koch*, N&R 2026, 13, 16 ff.

6 Etwa Stellungnahme *Kipker*, Ausschussdrucksache 21(4)062 D, 8; Stellungnahme AG KRITIS, Ausschussdrucksache 21(4)072, 13.

7 Art. 1 Abs. 2 (a) (i) COM(2026) 13.

bieter werden weiterhin von der NIS-2-RL erfasst, wenn sie die Voraussetzungen für wichtige Einrichtungen erfüllen.[8] Ausgenommen sind also lediglich „kleine" DNS-Diensteanbieter. Die Kommission geht davon aus, dass dies aber immerhin 6200 Einrichtungen betrifft, die zukünftig nicht mehr unter die NIS-2-Regulierung fielen.[9]

3. Stromerzeuger mit weniger als 1 MW

Ebenfalls eingeschränkt werden soll der Anwendungsbereich in Bezug auf Elektrizitätsunternehmen. Auch hierzu hatte es Kritik im deutschen Umsetzungsverfahren gegeben. Diese kam u. a. von der Immobilienwirtschaft, die darauf hinwies, dass lokale Photovoltaikanlagen zur Versorgung von Mietern trotz ihrer fehlenden Bedeutung für die allgemeine Versorgungssicherheit erfasst würden.[10]

Ausgenommen werden sollen zukünftig „Erzeuger, deren Gesamterzeugungskapazität 1 MW nicht überschreitet".[11] Anhang I Sektor „Energie" Teilsektor „Elektrizität" tir. 4 soll entsprechend angepasst werden. Die Kommission zielt hiermit vor allem auf mittelständische Unternehmen, die Solarparks zum Eigenverbrauch betreiben.[12] Der Schwellenwert von 1 MW soll nur noch solche Unternehmen erfassen, deren Störung Auswirkungen auf die Sicherheit und Stabilität des Stromnetzes haben könnte.[13]

4. Wasserstoffherstellung für kommerzielle Zwecke

Eine weitere Einschränkung wird in Bezug auf den Teilsektor „Wasserstoff" vorgeschlagen. Erfasst werden soll hier nur noch die Herstellung für kommerzielle Zwecke.[14] Zur Begründung verweist die Kommission auf – nicht weiter ausgeführte – Herausforderungen bei der Auslegung der entsprechenden Bestimmungen.[15] Der Hintergrund dürfte sein, dass der Wortlaut der NIS-2-RL bislang auch die Wasserstoffherstellung im Rahmen von Versuchsanlagen oder zur eigenen Verwendung (im Rahmen weiterer chemischer Prozesse) erfasst hat.[16]

5. Klarstellung für Anbieter intelligenter Verkehrssysteme

Anhang I Sektor „Verkehr" Teilsektor „Straßenverkehr" tir. 2 erfasst derzeit „Betreiber intelligenter Verkehrssysteme im Sinne des Art. 4 Nr. 1 der RL 2010/40/EU". Hier ist eine begriffliche Klarstellung geplant. Zukünftig soll die Vorschrift auf Art. 4 Nr. 5 der Richtlinie verweisen.[17] Statt auf die Legaldefinition für „‚intelligente Verkehrssysteme' oder ‚IVS' Systeme", soll zukünftig auf die Legaldefinition für „IVS-Diensteanbieter" verwiesen werden.

6. Gesundheitsdienstleister

Eine weitere Präzisierung ist in Bezug auf Gesundheitsdienstleister geplant. Bislang erfasst der Anhang I der NIS-2-RL „Gesundheitsdienstleister im Sinne des Artikels 3 lit. g der RL 2011/24/EU". Hier soll zukünftig klargestellt werden, dass die Einschränkung in Art. 3 lit. a RL 2011/24/EU – „[d]iese Richtlinie gilt nicht für (…) Dienstleistungen im Bereich der Langzeitpflege, deren Ziel darin besteht, Personen zu unterstützen, die auf Hilfe bei routinemäßigen, alltäglichen Verrichtungen angewiesen sind" – auch für die NIS-2-RL gilt. Es soll deshalb ein Halbsatz „ausgenommen Dienstleistungserbringer, für die die RL 2011/24/EU gemäß Art. 1 Abs. 3 lit. a nicht gilt" in Anhang I Sektor „Gesundheitswesen" tir. 1 aufgenommen werden.[18] Die entsprechende Ausnahme ließe sich zwar auch im Wege einer systematischen Auslegung ermitteln; eine gesetzgeberische Klarstellung ist dennoch zu begrüßen, weil sie die Rechtsanwendung erleichtert.

7. Chemische Industrie

Ebenfalls eine klarstellende Einschränkung ist in Bezug auf die Produktion, Herstellung und den Handel mit chemischen Stoffen geplant. Hier erfasst die NIS-2-RL – als sonstige kritische Sektoren – bislang die Hersteller und Händler von chemischen Erzeugnissen i. S. d. REACH-VO (EG) Nr. 1907/2006. Der Anwendungsbereich soll in Zukunft auf die Hersteller beschränkt werden. Zudem werden nur noch die Hersteller von chemischen Erzeugnissen erfasst, die einer Registrierungspflicht nach Art. 6 bzw. einer Meldepflicht nach Art. 7 Abs. 2 der REACH-VO (EG) Nr. 1907/2006 unterliegen.[19]

III. Erweiterung des Anwendungsbereichs

Die Kommission plant aber nicht nur Klarstellungen und Einschränkungen des Anwendungsbereichs der NIS-2-RL, sondern auch Erweiterungen.

1. Anbieter von EUDI-Wallets und EU-Business Wallets

Die NIS-2-RL soll zukünftig auch für die Anbieter von EUDI-Wallets[20] und EU-Business Wallets gelten. Die entsprechenden Anbieter sollen unabhängig von ihrer Größe als wesentliche Einrichtung gelten.[21] Die entsprechenden Dienste werden in Zukunft eine zentrale Rolle bei der Identifizierung und Authentifizierung von EU-Bürgern und -Unternehmen spielen.[22] Hierüber soll zudem ein sicherer Austausch von Dokumenten möglich sein. Ein Ausfall der entsprechenden digitalen Infrastrukturen kann weitreichende Folgen für das Gemeinwesen haben.[23] Da es sich hierbei letztlich um eine Meta-Infrastruktur handelt, die zukünftig für verschiedenste – staatliche oder private – Dienste genutzt werden wird, ist es auch sinnvoll, die entsprechenden Dienstleister unabhängig von ihrer Größe zu erfassen.

2. Unterwasser-Datenübertragungsinfrastruktur

Geplant ist außerdem eine Erweiterung der wesentlichen Einrichtungen um die Betreiber von Unterwasser-Datenübertragungsinfrastrukturen.[24] Die entsprechenden Infrastrukturen

8 Vgl. den Anwendungsbereich in Art. 2 Abs. 1 NIS-2-RL „Diese Richtlinie gilt für (…) Einrichtungen, (…) die nach Art. 2 des Anhangs der Empfehlung 2003/361/EG als mittlere Unternehmen gelten". Art. 2 Abs. 1 der in Bezug genommenen Empfehlung grenzt die kleinen und mittleren Unternehmen nach oben ab (250 Personen und 50 Mio. Euro Jahresumsatz oder 43 Mio. Euro Jahresbilanzsumme). Abs. 2 grenzt hiervon die „kleine[n]" Unternehmen ab (50 Mitarbeiter und 10 Mio. Euro Jahresumsatz bzw. Jahresbilanz).
9 Commission, Impact Assessment Report, SWD(2026) 11 final (im Folgenden „SWD(2026) 11"), S. 81.
10 Stellungnahme Zentraler Immobilien Ausschuss e. V., Ausschussdrucksache 21(4)065, 3.
11 Ziff. 1. (a) Annex COM(2026) 13.
12 SWD(2026) 11 final, S. 34.
13 Erwägungsgrund 4 COM(2026) 13.
14 Ziff. 1 (b) Annex COM(2026) 13.
15 Erwägungsgrund 3 COM(2026) 13.
16 Der Deutsche Wasserstoff-Verband hatte in seiner Stellungnahme v. 3. 7. 2025 etwa kritisiert: „Der Geltungsbereich des Gesetzes ist mit Blick auf komplexe Lieferketten und Projektstrukturen unklar". Die Stellungnahme ist abrufbar unter https://ruw.link/2026/95 (dwv-info.de).
17 Ziff. 1. (c) Annex COM(2026) 13.
18 Ziff. 1. (d) Annex COM(2026) 13.
19 Ziff. 2. Annex COM(2026) 13.
20 *Frey*, K&R 2026, Heft 3, Editorial.
21 Art. 1 Abs. 1 (a) (ii) COM(2026) 13 und Ziff. 1. (e) Spiegelstriche 1 u. 2. Annex COM(2026) 13.
22 Vgl. ausführlich hierzu: *Frey*, K&R 2026, Editorial; *Lapp*, ZD 2026, 1.
23 Siehe auch Erwägungsgrund 5 COM(2026) 13.
24 Ziff. 1. (e) Siegelstrich 3 Annex COM(2026) 13.

fallen zu einem großen Teil zwar schon bisher in den Anwendungsbereich der Richtlinie – insbesondere, soweit es sich um „Anbieter öffentlicher elektronischer Kommunikationsnetze" handelt.[25] Nicht erfasst werden bislang die Anbieter nichtöffentlicher Kommunikationsnetze oder Unternehmen, die lediglich die Infrastruktur bereitstellen und diese an die Anbieter öffentlicher Kommunikationsnetze vermieten.[26] Die Kommission formuliert hier sehr vorsichtig, dass angesichts „zunehmender Risiken" die Untersee-Kommunikationsinfrastruktur besser geschützt werden muss.[27] Hintergrund der entsprechenden Überlegungen dürften verschiedene Vorfälle seit dem Angriffskrieg Russlands auf die Ukraine sein, bei der „europäische" Unterseekabel beschädigt oder zerstört wurden. Stellt man in Rechnung, dass 99 % des interkontinentalen Internetverkehrs über Unterseekabel abgewickelt werden,[28] besteht hier ein immenses öffentliches Interesse an einer Absicherung dieser Infrastruktur. Erschwerend kommt hinzu, dass Europa beim Betrieb dieser Infrastrukturen in Teilen vollständig von außereuropäischen Herstellern abhängig ist. So gibt es etwa keinen einzigen europäischen Hersteller für Glasfasern, wie sie in Unterseekabeln verwendet werden.[29]

3. Strategische Infrastruktur mit doppeltem Verwendungszweck

Schließlich plant die Kommission eine Ausdehnung der wesentlichen Einrichtungen auf die Eigentümer, Verwalter und Betreiber strategischer Infrastrukturen mit doppeltem Verwendungszweck. Solche Einrichtungen sollen unabhängig von ihrer Größe erfasst werden.[30] Auch diese Änderung dürfte der geänderten Weltlage geschuldet sein. Um Truppen – Personen und Material – innerhalb der Union bewegen zu können, sind die Streitkräfte auf zivile Infrastrukturen – insbesondere Straßen, Schienen, Bahnhöfe, See-, Binnen- und Flughäfen – angewiesen. Diese Infrastrukturen haben also nicht nur eine zivile, sondern auch eine strategisch-militärische Bedeutung. Die Kommission arbeitet derzeit an einer Verordnung zur Schaffung eines Rahmens für Maßnahmen zur Erleichterung des Transports von militärischer Ausrüstung, militärischen Gütern und militärischem Personal innerhalb der Union.[31] Hiermit soll die NIS-2-RL verzahnt werden. Auch diese Erweiterung ist sinnvoll. Der russische Angriff auf die Ukraine und die Neuausrichtung der US-amerikanischen Außen- und Verteidigungspolitik haben gezeigt, dass die europäischen Staaten zukünftig in der Lage sein müssen, auf militärische Bedrohungen eigenständig zu reagieren und hierfür ggf. große Truppenkontingente nebst Ausrüstung innerhalb der Union kurzfristig verlegen zu können. Dementsprechend müssen die hierfür benötigten und in Friedenszeiten vorwiegend zivil genutzten strategischen Infrastrukturen besonders geschützt werden. Da die geplante Militärtransport-Verordnung einen Prozess zur Bestimmung der relevanten strategischen Infrastruktur vorsieht,[32] bedarf es keiner weiteren Eingrenzung in der NIS-2-RL.

IV. Ransomware-Angriffe

Der Kommissionsvorschlag sieht außerdem erweiterte Berichtspflichten bei Ransomware-Angriffen vor. Bei solchen Angriffen werden üblicherweise Daten verschlüsselt und eine Entschlüsselung nur gegen Zahlung eines Lösegelds in Aussicht gestellt. Eine andere Angriffsvariante sieht vor, dass Daten kopiert und mit Veröffentlichung gedroht wird, sollte kein Lösegeld gezahlt werden. Die von solchen Angriffen betroffenen Unternehmen sollen zukünftig melden müssen, ob und ggf. von wem sie Lösegeldforderungen erhalten haben. Sollte ein Lösegeld bezahlt worden sein, müssen die betroffenen Unternehmen hierzu detaillierte Angaben – etwa Betrag, Zahlungsmittel, Empfänger, Krypto-Asset – machen.[33] Die Auskunftspflicht setzt allerdings eine explizite Aufforderung voraus.

Die geplante Regelung dürfte für die Praxis sehr weitreichende Folgen haben. Die Zahlung von Lösegeldern erfüllt nach der deutschen Rechtsordnung regelmäßig den Tatbestand der Unterstützung (ausländischer) krimineller Vereinigungen nach § 129, § 129b StGB. Hinzu können Taten nach § 18 Abs. 1 AWG kommen. Die wohl herrschende Meinung versagt in diesen Konstellationen – des Nötigungsnotstandes – auch eine Rechtfertigung und Entschuldigung.[34] Das Unionsrecht erfasst die Zahlung von Lösegeldern sogar ausdrücklich – etwa in Art. 2 Abs. 2a der VO (EG) 881/2002 – als Unterstützungshandlung von Terrorgruppen (Al-Qaida im Falle der genannten Verordnung).

Gleichzeitig ist die Zahlung eines Lösegeldes in vielen Fällen die einzige Möglichkeit, wieder Zugang zu verschlüsselten Daten zu erhalten und/oder die Veröffentlichung von – ggf. sehr sensiblen – Daten (Betriebs- und Geschäftsgeheimnisse, Informationen über Patienten etc.) zu verhindern. Auch wenn Behörden grundsätzlich davon abraten, Lösegelder zu bezahlen, sehen sich viele Unternehmen daher gezwungen, auf entsprechende Forderungen einzugehen. Das BSI schätzt, dass mehr als 25 % der betroffenen Opfer von Ransomware Lösegelder zahlen, und zwar in einer Höhe von über einer Million US-Dollar im arithmetischen Mittel.[35]

Die Zahlung von Lösegeldern ist also in der Praxis weit verbreitet. Gleichzeitig laufen die handelnden Personen Gefahr, strafrechtlich verfolgt zu werden, wenn eine Lösegeldzahlung öffentlich wird. Den Unternehmen drohen ggf. zusätzliche Bußgelder über § 30 OWiG. Die Kommission erkennt dieses Problem durchaus. In den Erwägungsgründen werden deshalb die Mitgliedstaaten aufgefordert, auf mögliche Risiken für die Betroffenen einzugehen, die sich aus einer Meldung von Ransomware-Vorfällen ergeben können.[36] Den Erwägungsgründen kommt aber kein Regelungscharakter zu. Zudem dürfte die Kommission übersehen, dass es nicht nur die nationalen Rechtsordnungen sind, aus denen sich ein entsprechendes Risiko ergibt, sondern gerade auch das Unionsrecht.

Hier bedarf es einer klaren Regelung, um zu verhindern, dass die betroffenen Personen und Unternehmen sich einem straf- oder ordnungsrechtlichen Verfolgungsrisiko aussetzen, wenn sie gegenüber den Behörden wahrheitsgemäße Angaben zu einer Lösegeldzahlung machen.

Das Problem ist im Übrigen deutlich grundsätzlicher: Nicht selten wird ein meldepflichtiger Angriff nämlich nur deshalb erfolgreich sein, weil die betroffenen Einrichtungen zuvor

25 Anhang I Ziff. 8 Spiegelstrich 8 NIS-2-RL.
26 Erwägungsgrund 6 COM(2026) 13.
27 Erwägungsgrund 6 COM(2026) 13.
28 SWD(2026) 11, S. 28.
29 SWD(2026) 11, S. 28.
30 Art. 1 Abs. 1 (b) u. Abs. 2 (a) (ii) COM(2026) 13.
31 Kommission, Vorschlag für eine Verordnung zur Erleichterung von Militärtransporten innerhalb der Union, COM(2025) 847 final.
32 Art. 33 COM(2025) 847.
33 Art. 1 Abs. 8 COM(2026) 13.
34 *Rückert*, GWuR 2021, 103; *Salomon*, MMR 2016, 575; siehe auch *Heinelt*, K&R 2025, Beilage 1 zu Heft 9, 37, 39, der darauf hinweist, dass kein Fall bekannt sei, in dem Anklage gegen ein Erpressungsopfer erhoben wurde.
35 BSI, Lagebericht 2025, S. 8; abrufbar unter https://ruw.link/2026/96 (medien.bsi.bund.de).
36 Erwägungsgrund 11 COM(2026) 13.

pflichtwidrig Sicherheitsmaßnahmen vernachlässigt haben. Auch hier sind straf- und ordnungsrechtliche Sanktionen denkbar, wenn Unternehmen pflichtgemäß melden.[37] Die Grundkonstellation ist dabei keine Besonderheit des IT-Sicherheitsrechts. Vergleichbare Fragen stellen sich etwa im Datenschutzrecht. Hier hat der nationale Gesetzgeber beispielsweise in § 43 Abs. 4 BDSG Beweisverwertungsverbote vorgesehen. Entsprechende Vorschriften fehlen im BSIG.[38]

V. Verzahnung mit den geplanten Änderungen im Cybersicherheitsgesetz 2

Parallel zur Überarbeitung der NIS-2-RL arbeitet die Kommission an einer Reform des Cybersicherheitsgesetzes (Cybersecurity Act – CSA).[39] Dort ist unter anderem die Einführung von Zertifikaten über das Cybersicherheitsniveau („cyber posture of entities") vorgesehen. Bislang beziehen sich die Zertifikate vorrangig auf Produkte oder Prozesse. Der Vorschlag für ein Cybersicherheitsgesetz 2 sieht nun die Einführung von Zertifikaten über das Cybersicherheitsniveau ganzer Unternehmen vor. Die Zertifikate sollen dabei nicht auf die NIS-2-RL beschränkt sein, sondern modular aufgebaut sein und etwa auch die Anforderungen nach der DSGVO erfassen.[40] Hierdurch sollen nicht zuletzt die Verwaltungskosten für die betroffenen Unternehmen gesenkt werden.[41]

Der Kommissionsvorschlag für die NIS-2-RL sieht nun vor, dass die Mitgliedstaaten wesentliche und wichtige Einrichtungen verpflichten können, entsprechende Zertifikate zu erwerben. Verfügt ein Unternehmen über ein entsprechendes Zertifikat, soll es keinen weiteren Nachweispflichten in Bezug auf die Verpflichtungen aus Art. 21 Abs. 1 und 2 der NIS-2-RL unterliegen.[42]

VI. Harmonisierung

Die NIS-2-RL verpflichtet die Mitgliedstaaten bislang zu einer „Mindestharmonisierung", hindert sie aber ausdrücklich nicht daran, Vorschriften zu erlassen, durch die ein höheres Cybersicherheitsniveau erreicht werden soll.[43] Hier sieht der Kommissionsvorschlag eine Einschränkung vor: Soweit die Kommission Durchführungsrechtsakte zur Bestimmung der technischen und methodischen Anforderungen nach Art. 21 NIS-2-RL erlässt, dürfen die Mitgliedstaaten zukünftig keine strengeren Vorgaben mehr vorsehen.[44]

VII. Sicherheit der Lieferkette

Die NIS-2-RL erfasst unmittelbar nur wichtige und wesentliche Unternehmen aus ausgewählten Sektoren und Branchen. Allerdings müssen diese bei der Umsetzung von Risikomanagementmaßnahmen nach Art. 21 Abs. 2 lit. d die „Sicherheit der Lieferkette" berücksichtigen.[45] Das führt in der Praxis dazu, dass die von der NIS-2-RL erfassten Unternehmen die sich aus der Richtlinie ergebenden Cybersicherheitsverpflichtungen zunächst nach unten in der Lieferkette weiterreichen müssen und dann gezwungen sind, die Einhaltung der entsprechenden Verpflichtungen zu überprüfen. Das ist in der Praxis mit einem erheblichen Verwaltungsaufwand verbunden. Bislang muss jedes betroffene Unternehmen eigene Fragebögen, Prozesse etc. entwickeln, um die Cybersicherheit entlang der Lieferkette nachzuverfolgen und sicherzustellen. Das ist eine volkswirtschaftlich unsinnige Bindung von Ressourcen in zehntausenden betroffenen Unternehmen, weil immer die gleichen Probleme zu adressieren sind. Hier möchte die Kommission zukünftig mit Leitlinien weiterhelfen, aus denen sich Detailliertheit, Struktur und Format für entsprechende Informationsanfragen ergeben sollen.[46]

VIII. Single-Entry-Point für die Meldung von Vorfällen

Eine weitere Änderung der NIS-2-RL soll im Rahmen der Digital-Omnibus-Verordnung erfolgen. Hierdurch soll eine zentrale Anlaufstelle – „Single-Entry Point" – für die Meldung von Sicherheitsvorfällen eingerichtet werden.

Das EU-IT-Sicherheitsrecht sieht in verschiedenen Rechtsakten – NIS-2-RL, DSGVO, DORA, eIDAS-Richtlinie, CER-Richtlinie – Meldepflichten für Sicherheitsvorfälle vor. Die betroffenen Einrichtungen müssen also ggf. den gleichen Sicherheitsvorfall an verschiedene Behörden melden, was zu einem erheblichen Verwaltungsaufwand führt.[47] Verschärft wird das Problem, wenn Einrichtungen in mehreren Mitgliedstaaten tätig sind. Sie müssen dann ggf. Meldungen in all diesen Ländern an unterschiedliche Behörden abgeben.

Zukünftig sollen Einrichtungen Vorfälle nur noch einmal an eine neu zu schaffende zentrale Anlaufstelle melden müssen. Hierfür soll die Agentur der Europäischen Union für Cybersicherheit (ENISA) eine entsprechende Meldeplattform aufbauen.[48] Der ENISA kommt dabei nur die Rolle eines technischen Dienstleisters zu, der die Meldeplattform bereitstellt. Die ENISA soll nämlich keinen Zugang zu den übermittelten Meldungen erhalten.[49] Praktisch bedeutet das, dass die betroffenen Einrichtungen zukünftig einen Sicherheitsvorfall nur noch über die von der ENISA betriebene zentrale Anlaufstelle melden.[50] Die ENISA leitet die Meldung dann – ohne hierzu Zugang zu haben – an die nationalen Stellen weiter. Ab diesem Punkt bleibt es bei der bisherigen Systematik: D. h. die nationalen Behörden treten mit den meldenden Einrichtungen in Kontakt (etwa Art. 23 Abs. 5 NIS-2-RL). Die vorgesehene Änderung betrifft also nur die Erstmeldung. Ist diese erfolgt, müssen die meldenden Einrichtungen weiterhin mit ggf. verschiedenen Behörden in ggf. verschiedenen Mitgliedstaaten kommunizieren. Es soll sich auch nichts an der Meldekette ändern. Geht eine Meldung bei einer nationalen Stelle ein, muss diese bei einem staatenübergreifenden Angriff die nationalen Stellen der anderen betroffenen Mitgliedstaaten informieren – eine Änderung von Art. 23 Abs. 6 NIS-2-RL ist nicht geplant. Ebenfalls keine Änderungen sind in Bezug auf die Meldungen hin zur ENISA geplant. Die Meldungen erfolgen zwar über die ENISA, diese hat aber keinen Zugang hierzu. Die nationalen Stellen sollen die ENISA weiterhin bei grenzüberschreitenden Vorfällen sofort

37 Siehe zum Strafrecht auch *Dittrich*, MMR 2026, 273, 275 f.
38 Hierauf wurde bereits im Gesetzgebungsverfahren hingewiesen. Vgl. die Stellungnahme von *Kipker*, Ausschussdrucksache 21(4)062 D, 21.
39 Ausführlich *Schmidt*, K&R 2026, 226.
40 COM(2026) 13, S. 3 des Einführungstextes (nach „GDPR" suchen), Erwägungsgrund 93 Kommission, Vorschlag für ein Cybersicherheitsgesetzes 2, COM(2026) 11.
41 COM(2026) 13, S. 2.
42 Art. 1 Abs. 9 COM(2026) 13.
43 Art. 5 NIS-2-RL.
44 Art. 1 Abs. 8 (b) COM(2026) 13.
45 Siehe hierzu *Rosensaft*, MMR 2026, 261, 264.
46 Erwägungsgrund 9 COM(2026) 13.
47 Kommission, Vorschlag für eine Digital-Omnibus-Verordnung, S. 8 f., COM(2025) 837 final (im Folgenden „Digital-Omnibus-VO"). Siehe auch *Lienemann*, K&R 2026, 155.
48 Art. 6 Digital-Omnibus-VO soll einen entsprechenden Art. 23a in die NIS-2-RL einfügen.
49 Art. 23a Abs. 4 NIS-2-Richlinie in der Fassung nach Art. 6 Nr. 1 Digital-Omnibus-VO.
50 Art. 23 Abs. 1 NIS-2-RL in der Fassung nach Art. 6 Nr. 2 Digital-Omnibus-VO.

und im Übrigen nur alle drei Monate in anonymisierter und aggregierter Form informieren.[51]

IX. Fazit

Die vorgesehenen Änderungen betreffen zunächst sinnvolle Anpassungen des Anwendungsbereichs der NIS-2-RL. Unausgereift scheinen bislang aber die Vorschriften zu Informationspflichten über Lösegeldzahlungen. Hier wird es rechtsgebietsübergreifender Regelungen im nationalen wie unionalen Recht bedürfen, um Strafverfolgungsrisiken für die handelnden natürlichen Personen und ordnungs- und verwaltungsrechtliche Sanktionen für die betroffenen Unternehmen auszuschließen.

Grundsätzlich zu begrüßen ist der Ansatz in der Digital-Omnibus-Verordnung, die betroffenen Einrichtungen bei der Meldung von Sicherheitsvorfällen zu entlasten. Allerdings sollte erneut erwogen werden, ob eine zentrale Meldestelle bei der ENISA der richtige Weg ist. Hierüber wird ein einzelner Angriffspunkt („Single-Point-of-Failure") geschaffen, über den ein Angreifer sämtliche Meldungen in der EU verhindern kann. Das ist ein Risiko, welches es überaus sorgfältig gegenüber dem Nutzen für die betroffenen Einrichtungen abzuwägen gilt. Dabei ist zu bedenken, dass der bisherige Vorschlag ohnehin nur die Erstmeldung adressiert. Die Einrichtungen sind weiterhin mit einer Vielzahl von Rechtsvorschriften und Aufsichtsbehörden konfrontiert. Zu erwägen wäre deshalb, zentrale Anlaufstellen auf nationaler Ebene vorzuschreiben und vorzusehen, dass Einrichtungen nur noch in einem Mitgliedstaat eine Meldung abzugeben haben.

Es ist zu hoffen, dass der Gesetzgebungsprozess auf Unionsebene zügig abgeschlossen wird und die nationalen Gesetzgeber dann für eine schnelle Umsetzung sorgen. Die unionsweiten Verzögerungen bei der Umsetzung der NIS-2-RL dürfen sich angesichts der Bedeutung der Cybersicherheit unter einer massiv veränderten Weltsicherheitslage nicht wiederholen.

Der deutsche Gesetzgeber sollte nicht auf die Kommission warten, bis er erste Korrekturen der NIS-2-Umsetzung angeht. Die Umsetzung weist einige handwerkliche Fehler auf, die schnellstmöglich korrigiert werden sollten. Das beginnt bei kleineren Fehlern, wie Verweise auf nicht mehr existierende Paragraphen – die Verweise auf § 3 EnWG in Ziffer 1 der Anlage beziehen sich auf den EnWG-Gesetzesstand bis Dezember 2025. Hier dürften sich die Gesetzgebungsvorhaben schlicht überschnitten haben. Schwerer wiegen – vermutlich unbeabsichtigte – Systembrüche bei den Bußgeldern: Während das BSIG – wie von Art. 34 der NIS-2-RL vorgesehen – Bußgelder für unterlassene Meldungen bis 10 Millionen Euro oder 2 % des Gesamtumsatzes vorsieht, ist der Bußgeldrahmen für entsprechende Verstöße nach dem TKG nicht angepasst worden und liegt weiterhin bei lediglich 10 000 Euro.[52] Das sollte Anlass zu einer grundsätzlichen Überprüfung der deutschen Regelungstechnik geben. Historisch ist es nachvollziehbar, weshalb die Verpflichtungen für TK- und Energieunternehmen im TKG bzw. dem EnWG geregelt wurden. Das führt nun aber dazu, dass Änderungen am Cybersicherheitsrecht in jeweils drei Gesetzen – dem TKG, dem EnWG und BSIG – umgesetzt werden müssen. Das ist nicht nur fehleranfällig, sondern auch unnötig. Es sollte deshalb erwogen werden, das Cybersicherheitsrecht für alle Unternehmen in einem einheitlichen Gesetz zu regeln und die Sonderregelungen aus dem TKG und EnWG herauszulösen.

Schließlich ist es wenig hilfreich, wenn die Terminologie des deutschen Rechts von der Terminologie des Unionsrechts abweicht. So ist unverständlich, warum das deutsche Recht zwischen besonders wichtigen und wichtigen Einrichtungen unterscheidet, während das Unionsrecht auf wesentliche und wichtige Einrichtungen abstellt. Hier wäre eine Anpassung der Terminologie sinnvoll.

Prof. Dr. Alexander Koch
Rechtsanwalt und Partner in der Kanzlei Koch & Neumann, einer der Geschäftsführer des Instituts für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie (IRNIK) und Honorarprofessor an der Philipps-Universität Marburg, wo er (IT-) Strafrecht lehrt, und Dozent an der Westfälischen Hochschule Gelsenkirchen für IT-Recht, Datenschutz und Ethik.

51 Art. 23 Abs. 6 und 9 NIS-2-RL.
52 Siehe hierzu schon *Koch*, N&R 2026, 13, 22, Fn. 96.

RA Dr. Florian Deusch und Prof. Dr. Tobias Eggendorfer*

Update IT-Sicherheitsrecht 2026

Kurz und Knapp

Die Autoren stellen anschließend an ihr Update aus den Vorjahren in K&R 2024, 169 ff. und 242 ff. die Entwicklung des IT-Sicherheitsrechts im Zeitraum 2024 - 2026 anhand ausgewählter Akte der Gesetzgebung und der Rechtsprechung dar. Aufgrund der Betriebsamkeit der legislativen Ebenen liegt der Schwerpunkt auf der Gesetzgebung.

I. Einführung und Gefährdungslage

Die Gefährdungslage aus dem Cyberraum für gewerbliche und private IT-Nutzer ist im Berichtszeitraum ungebrochen angespannt geblieben. An der Tagesordnung stehen für viele Unternehmen nach wie vor arbeitsteilig orchestrierte Ransomware-Attacken (80 % der Opfer in Deutschland waren kleine und mittlere Unternehmen). Die Täter nutzen zahlreiche Sicherheitslücken in gängiger Software für ihre Zwecke aus, z. B. indem sie die Opfer durch teilweise mit KI erzeugten Phishingmails überzeugen, ihre Schadsoftware zu installieren,[1] was sichere Betriebssysteme selbständig verhindern sollten.

* Mehr über die Autoren erfahren Sie am Ende des Beitrags. Alle zitierten Internetquellen wurden zuletzt abgerufen am 25. 3. 2026.
1 ENISA Threat Landscape 2025, https://ruw.link/2026/79 (enisa.europa.eu); BSI-Lagebericht zur IT-Sicherheit 2025 (https://medien.bsi.bund.de/lagebericht/de/index.html).