Kommunikation & Recht

K&R

3 | März 2024
27. Jahrgang
Seiten 157 - 228

www.kommunikationundrecht.de

dfv Mediengruppe
Frankfurt am Main

ligen Werbetreibenden aufgrund der vertraglichen Freistellungsklauseln schadlos halten. Eine solche Freistellung greift allerdings nicht, wenn es um Straftatbestände oder Ordnungswidrigkeiten geht. In diesen regulierten Bereichen wie der bereits behandelten Glücksspielwerbung oder dem Heilmittelwerberecht[39] gilt zwar ebenfalls die beschränkte Haftung der Presseunternehmen für entsprechende Anzeigen. Die Presseunternehmen werden jedoch wohl nicht umhinkommen, aufgrund einer fehlenden Richtschnur bezüglich der Evidenz der Rechtsverletzung diese Anzeigen rechtlich zu prüfen oder interne Richtlinien zu etablieren, die die Ausspielung „evidenter" Rechtverletzungen bestmöglich verhindern. Gleichermaßen bestehen Risiken dort, wo wegen fehlender direkter vertraglicher Beziehungen mit dem Werbekunden keine Freistellungen existieren, wie dies auf Fälle der programmatischen Ausspielung von Werbung zutreffen kann. Hier wird das Presseunternehmen allerdings gut beraten sein, jedenfalls mit den zwischengeschalteten Plattformen umfangreiche Freistellungen zu vereinbaren, oder auf anderem Wege zu versuchen, in direkten vertraglichen Kontakt mit dem Werbekunden zu treten und hierbei eine Freistellungsklausel zu vereinbaren.

Die vorstehenden Ausführungen haben außerdem gezeigt, dass das Haftungsprivileg der Presse bei der Anzeigenprüfung überall in gleichem Maße gelten sollte, unabhängig davon, auf welchem Weg oder Medium (Print, Rundfunk, Digital) die Anzeige ausgespielt wird. Außerdem bestehen auffallende Parallelen zwischen dieser Pressehaftung und der Störerhaftung bzw. im digitalen (Plattform-)Bereich dem Hostprovider-Privileg. Im Kern geht es stets um die Frage, welche Prüfpflichten für Anbieter zumutbar sind. Diese Frage stellt sich in sehr ähnlichem Umfang für Presse als Verbreiter von Drittanzeigen oder Plattformbetreibern als Verbreiter von nutzergenerierten Inhalten. Auf welcher dogmatischen Basis die beschränkte Haftung der Presse bei der Prüfung von Werbeanzeigen künftig stehen wird, und wie das Verhältnis zur Störerhaftung und zur Verletzung wettbewerblicher Verkehrspflichten ist, erscheint in diesem Kontext noch unklar. Es bleibt abzuwarten, ob die weiterhin zunehmende Online-Präsenz der Presse dazu führt, dass mehr Fälle, die das Anzeigenprivileg der Presse auf ihren Webseiten zum Gegenstand haben, vor Gericht landen. Das Glücksspielrecht könnte hierbei zum Präzedenzfall werden, zumal die ein Presseunternehmen treffenden Prüfungspflichten bei (digitaler) Glücksspielwerbung trotz der existierenden Rechtsprechung zur Rundfunkhaftung keineswegs klar sind.

Dr. Lars Querndt

1. Staatsexamen Bayreuth (2008), 2. Staatsexamen 2010 (Hessen), 2013 LL.M. Instituto de Empresa (Madrid), 2014 Dr. jur. (Universität Bayreuth), seit 2013 Rechtsanwalt im IP/IT- und Medienrecht, seit 2022 auch Syndikusrechtsanwalt im Axel Springer Konzern.

39 § 14 HWG enthält eine Strafvorschrift im Hinblick auf irreführende Heilmittelwerbung, siehe etwa *Doepner/Reese*, in: BeckOK HWG, 11. Ed., Stand: 1. 10. 2023, § 14 HWG Rn. 172 m. w. N.

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

Update IT-Sicherheitsrecht 2022/2023 – Teil 1

Kurz und Knapp

Die Autoren stellen anschließend an ihr Update aus den Vorjahren in K&R 2021, 689 ff. und K&R 2022, 794 ff. die Entwicklung des IT-Sicherheitsrechts im Zeitraum 2022/2023 dar. Der vorliegende Teil 1 stellt ausgewählte Akte der Gesetzgebung dar; in K&R Heft 4/2024 folgt Teil 2 mit dem Bericht zur Rechtsprechung.

I. Einführung und Gefährdungslage

Ende Januar 2024 vermeldete Microsoft, Opfer eines Cyberangriffs zu sein. Es seien zwar keine Quellcodes abgeflossen, wohl aber haben die Angreifer Zugriff auf E-Mail-Konten erlangt. Hinter dem Angriff stehe eine russische Hackergruppierung. In der IT-Sicherheitsszene gab es Häme, schließlich preist Microsoft seine Produkte als sicher an und nutzt sie selbst.[1]

Abgesehen von prominenten Opfern scheinen „Hackerangriffe" mittlerweile das Äquivalent von „Hund beißt Briefträger" zu sein: Zu normal, um überhaupt noch berichtenswert zu sein. Einige Spezialmedien versuchen noch, Hit-Listen der zehn gruseligsten, schlimmsten, gefährlichsten, teuersten oder sonstig superlativierten Angriffe zu generieren.[2]

Die Angriffe sind mittlerweile häufig weitgehend automatisiert, selten finden sich wirklich noch „echte" Hacker, die mit viel Geschick in die Systeme einbrechen. Denn nachlässige Qualitätssicherung in der Software-Entwicklung, fehlende Qualitäts-Zertifizierung durch messbare IT-Sicherheit und unzureichende Administration lassen genügend Lücken offen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stuft die Gefährdungslage der IT-Sicherheit in Deutschland im Jahr 2023 „so hoch wie nie zuvor" ein.[3] Ob die legislativen und

* Mehr über die Autoren erfahren Sie am Ende des Beitrags.

1 Siehe u. a. https://www.spiegel.de/netzwelt/russische-gruppe-hackt-microsoft-a-3fbce604-e772-410b-a99a-49d33caeb7f3, https://www.zeit.de/wirtschaft/2024-01/cyberangriff-microsoft-manager-emails-russland-spionage oder https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/; https://www.bleepingcomputer.com/news/security/microsoft-reveals-how-hackers-breached-its-exchange-online-accounts/.

2 So z. B. https://securityaffairs.com/156722/breaking-news/top-2023-security-affairs-stories.html und https://www.bleepingcomputer.com/news/security/the-biggest-cybersecurity-and-cyberattack-stories-of-2023/.

3 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html.

judikativen Entscheidungen der Jahre 2022/2023 diesen Gefahren auf die richtige Weise begegnen, bezweifeln die Autoren.[4] Sie halten es technisch für sinnvoller, die Qualität der eingesetzten Software nachhaltig zu verbessern. Eine strengere Haftung kommerzieller Softwareanbieter für Sicherheitslücken wäre ein Weg zu mehr IT-Sicherheit.

II. IT-Sicherheit in der Gesetzgebung

Die Gefährdungslage und die intensivere IT-Nutzung haben den europäischen und nationalen Gesetzgeber im Berichtszeitraum zu weiteren Rechtsakten motiviert.

1. In Kraft getretene und geplante Rechtsakte im EU-Recht

a) NIS-2-RL

Die RL (EU) 2022/2555 (NIS-2-RL), 20 Tage nach ihrer Verkündung am 14. 12. 2022 am 16. 1. 2023 in Kraft getreten, verstärkt die Vorgaben zu den staatlichen Strukturen der IT-Sicherheit auf der Ebene der Mitgliedstaaten und der EU (Kapitel II und III sowie V bis VIII NIS-2-RL).[5] Nachfolgend ist dargestellt, welche neuen Pflichten die NIS-2-RL für wen mit sich bringt und ab wann diese zu befolgen sind.

aa) Zeitliche Geltung und Anwendungsbereich

Die NIS-2-RL löst die NIS-RL (EU) 2016/1148 mit Wirkung zum 18. 10. 2024 ab (Artt. 41, 44 NIS-2-RL). Bis dahin müssen die EU-Mitgliedstaaten die Neuregelungen gesetzlich umgesetzt haben (siehe zum BSIG-E unten Ziffer 2 lit. a); solange verbleibt es bei den bisherigen Regelungen.

Besonders relevant ist die NIS-2-RL für Unternehmen sowie Behörden, die gemäß den Artt. 2 und 3 NIS-2-RL als wesentliche oder wichtige Einrichtung gelten und die definierten Schwellenwerte als mittlere und große Unternehmen erreichen. Sie haben die erweiterten IT-Sicherheitspflichten gemäß den Artt. 20, 21 NIS-2-RL zu erfüllen. Die NIS-2-RL erfasst alle Einrichtungen der bisherigen NIS-RL, klassifiziert diese aber in den Anhängen I und II neu. Zusätzlich erfasst sind Einrichtungen aus den Sektoren Energie (betreffend Fernwärme, Erdölbevorratung und Wasserstoff), Abwasser und Verwaltung von IKT-Diensten und aus der öffentlichen Verwaltung (soweit nach nationalem Recht definiert). Die bisherigen Anbieter digitaler Dienste sind teilweise in Anhang I (Nr. 8) und in Anhang II (Nr. 6) gelistet. Vollständig neu erfasst sind alle Einrichtungen im Anhang II:[6] Post- und Kurierdienste, Abfallbewirtschaftung, Chemie- und Lebensmittelbereich sowie verarbeitendes Gewerbe und Forschung.[7]

In Bezug auf das verarbeitende Gewerbe (Teilsektoren Medizin, IT-Hardware, Elektronik und Optik, Maschinen- und Kfz-Herstellung) ist nicht nur die Aufnahme in die NIS-2-RL neu, sondern auch die Klassifizierung nach dem NACE-Code Rev. 2. Beim NACE-Code handelt es sich um die Systematik der EU zur Klassifizierung von Wirtschaftszweigen und -einheiten (z. B. Unternehmen) sowie ihrer Daten zu statistischen Zwecken. Bislang diente er v. a. der Wirtschafts- und Finanzgesetzgebung bei der Einteilung von Unternehmen, z. B. im Handels- und Dienstleistungsstatistikgesetz, in § 341r HGB oder in der EU-Taxonomie.[8]

Ob Unternehmen in Deutschland die NIS-2-Pflichten erfüllen müssen, wird sich nach der Neufassung des BSIG richten. Der aktuelle Stand der Gesetzesentwürfe ist nicht leicht nachzuvollziehen: Es gibt einen Referentenentwurf (BSIG-E, Stand 3. 7. 2023) und ein Diskussionspapier (BSIG-E-DP, Stand 27. 9. 2023), welche bei der Definition der betroffenen Einrichtungen voneinander abweichen. Während § 28 BSIG-E nebst Begründung zu § 57 BSIG-E auf eine Definition per Rechtsverordnung (= KritisV) abstellt, enthält das BSIG-E-DP zwei Anlagen, die wie die NIS-2-RL den NACE-Code heranziehen.[9] Unternehmen, die prüfen möchten, ob sie von der NIS-2-RL oder dem BSIG-E-DP betroffen sind, müssen sich daher mit den Grundregeln für die Klassifizierung von Wirtschaftszweigen des Eurostat befassen.[10]

Gemäß Art. 4 NIS-2-RL werden die NIS-2-Regelungen durch Spezialvorschriften („sektorspezifische Rechtsakte") verdrängt. Bereits nach bisheriger Rechtslage gehen die Spezialvorschriften den NIS-Vorgaben vor, z. B. verdrängen die §§ 165 ff. TKG die Pflichten gemäß § 8a BISG für Betreiber öffentlicher Telekommunikationsdienste oder -netze (Art. 1 Abs. 7 NIS-RL, § 8d BSIG; § 28 BSIG-E bzw. BSIG-E-DP sehen verschiedene Unterausnahmen vor). Ebenso gehen § 11 EnWG, § 311, 325, 327 SGB V und § 7 AtG vor, jedoch nur, soweit die Spezialregelungen reichen. Weitergehende Vorgaben des BSIG, z. B. beim Einsatz kritischer Komponenten gemäß § 9b BSIG, bleiben unberührt bestehen.[11] Neu ist § 4 Abs. 3 NIS-2-RL, wonach die EU-Kommission Leitlinien zur Abgrenzung des sektorspezifischen Vorrangs bereitstellt, was auch bereits erfolgt ist. Nach den aktuellen Leitlinien der Kommission gehen die DORA-Pflichten im Finanzsektor den NIS-2-Pflichten vor.[12]

bb) IT-Sicherheitspflichten der NIS-2-RL; Sanktionen

Die Artt. 20, 21 NIS-2-RL strukturieren die IT-Sicherheitspflichten der betroffenen Einrichtungen neu.

Art. 20 Abs. 1 NIS-2-RL (umgesetzt in den §§ 38 Abs. 1 und 43 Abs. 1 BSIG-E) verpflichtet die Leitungsorgane der Einrichtungen, die IT-Sicherheitsmaßnahmen zu billigen und zu überwachen. Was der Richtliniengeber mit „billigen" genau meint, bleibt für die Autoren fraglich.[13] Wer etwas „billigt", beurteilt im allgemeinen Sprachgebrauch das Werk oder die Äußerung

4 Siehe dazu: *Deusch/Eggendorfer*, K&R 2016, 152 ff. sowie K&R 2023, 781 ff.

5 Was einer gesonderten Untersuchung vorbehalten bleibt, z. B. bei *Ritter*, RDV 2023, 152.

6 Ausgenommen die Anbieter digitaler Dienste.

7 Siehe auch *Schmidt*, K&R 2023, 705, 706; *Deusch/Eggendorfer*, Beauftragte für Informationssicherheit und für IT-Sicherheit, 2024, Ziffer 3.1.3 und 3.1.4.

8 Der NACE-Code (Rev. 2) ist geregelt in der VO (EG) 1893/2006. Die Entsprechung in Deutschland ist die Klassifikation nach Wirtschaftszweigen Ausgabe 2008 (WZ 2008), siehe *Seidel*, Wirtschaft und Statistik 2010, 255, abrufbar https://www.destatis.de/DE/Methoden/WISTA-Wirtschaft-und-Statistik/2010/03/dienstleistungen-032010.pdf?__blob=publicationFile.

9 Der Referentenentwurf BSIG-E wird z. B. im Blog von *Kipker* unter https://intrapol.org/2023/07/20/offizieller-refe-zum-nis2umsucg-stand-juli-2023-ist-veroeffentlicht/ als „offiziell öffentlich" bezeichnet, auf der Website des Bundesinnenministeriums ist jedoch lediglich das zeitlich nachfolgende (und lückenhafte) Diskussionspapier (BSIG-E-DP) verfügbar: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/CI1/NIS-2-UmsetzungWirtschaft_DisP.html; näher zum Gesetzgebungsverfahren unten Ziffer 2 lit. a.

10 Ziffer 3.1 des Working Paper „NACE Rev 2" des Statistischen Amts der Europäischen Gemeinschaften (Eurostat) stellt die Methode der Klassifizierung mit Beispielen dar (https://ec.europa.eu/eurostat/de/web/products-manuals-and-guidelines/-/ks-ra-07-015).

11 *Beucher/Ehlen/Utzerath*, in: Kipker, Cybersecurity, 2. Aufl. 2023, Kap. 14 Rn. 152 - 155.

12 Leitlinien der Kommission zur Anwendung des Art. 4 Abs. 1 und 2 der RL (EU) 2022/2555 (NIS-2-Richtlinie) (2023/C 328/02), Abl. C 328/2 vom 18. 9. 2023, siehe dazu *Voigt/Schmalenberger*, CR 2023, 717, 719.

13 Die englische Textfassung verwendet in Erwägungsgrund 138 NIS-RL-2 und in Art. 20 NIS-2-RL „approve", was die deutsche Übersetzung der NIS-2-RL im Erwägungsgrund mit „genehmigen" und in Art. 20 mit „billigen" wiedergibt.

eines anderen. Die Organisation der IT-Sicherheit ist aber originäre Aufgabe der Leitung einer Einrichtung; sie ist kraft ihres Auftrags verpflichtet, über Maßnahmen zur IT-Sicherheit selbst zu entscheiden. Demzufolge dürfte „billigen" nach dem Telos der Norm als „beschließen" zu verstehen sein, z. B. im Sinne eines Vorstandsbeschlusses, der die Risikomanagementmaßnahmen als verbindlich festlegt. Die Leitung ist auch dafür verantwortlich, dass ihre Anordnungen dazu umgesetzt werden.[14] Folgerichtig ordnet Art. 20 Abs. 1 NIS-2-RL an, dass Leitung die Ausführung der IT-Sicherheitsmaßnahmen überwachen muss und für Verstöße gegen ihre Pflichten aus Art. 20 NIS-2-RL auch haftbar gemacht werden können.

Für die Leitung öffentlicher Einrichtungen ordnet Art. 20 Abs. 1 Unterabs. 2 NIS-2-RL jedoch an, dass die geltenden Haftungserleichterungen in den Mitgliedstaaten unberührt bleiben. Die persönliche Haftung von *behördlichen* Leitungsorganen bleibt somit auf Vorsatz und grobe Fahrlässigkeit begrenzt (Art. 34 GG i. V. m. den §§ 839 BGB, 75 BBG und 48 BeamtenStG; unklar noch: § 38 BSIG-E bzw. BSIG-E-DP).

Art. 20 Abs. 2 NIS-2-RL schreibt zudem vor, dass sich die Leitungsorgane zur IT-Sicherheit zu schulen und allen Mitarbeitern entsprechende Schulungsangebote zu unterbreiten haben.

Art. 21 Abs. 1 NIS-2-RL ordnet wie bislang Art. 14 Abs. 1 NIS-RL geeignete technische und organisatorische Schutzmaßnahmen an (umgesetzt in den §§ 30 f. BSIG-E-DP und §§ 30, 43 BSIG-E).[15] Art. 21 Abs. 2 NIS-2-RL geben vor, welche Bereiche diese Maßnahmen mindestens umfassen müssen. Ein Bereich von besonderer Relevanz ist die Sicherheit der Lieferkette gemäß Art. 21 Abs. 2 lit. d und Art. 22 NIS-2-RL; ISO-zertifizierte Unternehmen müssen sich damit bereits gemäß Kontrollpunkt 5.21 der neu gefassten ISO/IEC 27001:2022 befassen (siehe unten Ziffer 3). Für bestimmte Einrichtungen erlässt die EU-Kommission bis zum 17. 10. 2024 Durchführungsrechtsakte mit spezifischen Anforderungen an die Sicherheitsmaßnahmen (Art. 21 Abs. 5 NIS-2-RL).

Art. 23 NIS-2-RL (umgesetzt in § 31 BSIG-E bzw. § 32 BSIG-E-DP) verpflichtet die Einrichtungen, Sicherheitsvorfälle innerhalb vorgegebener Fristen bei den zuständigen Behörden zu melden. Art. 27 NIS-2-RL enthält eine Registrierungspflicht der Einrichtungen (§§ 32 BSIG-E bzw. 33 BSIG-E-DP).

Verstöße gegen die NIS-2-Pflichten sind mit Sanktionen einschließlich Bußgeldern zu belegen (Kapitel VII, Artt. 31 ff.). Gemäß Art. 35 Abs. 2 NIS-2-RL sollen Geldbußen, die aufgrund der DSGVO verhängt wurden, zusätzlichen Geldbußen nach der NIS-2-RL entgegenstehen. Offen bleibt, was im umgekehrten Fall gelten soll: Ist ein Bußgeldbescheid der Datenschutzbehörde ausgeschlossen, wenn bereits zuvor das BSI in Ausführung der NIS-2-RL (bzw. dem dann geltenden BSIG) eine Geldbuße verhängt hat?[16]

b) CER-RL

Zeitgleich zur NIS-2-RL ist die RL (EU) 2022/2557 (CER-RL) in Kraft getreten. Auch diese ist bis zum 18. 10. 2024 umzusetzen; Deutschland plant dazu das KRITIS-Dachgesetz.[17] Die CER-RL richtet sich an Einrichtungen, deren Leistungen für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen oder wirtschaftlicher Tätigkeiten im Binnenmarkt der EU unerlässlich sind (Art. 1 CER-RL). Betroffen ist ein Teilbereich der Einrichtungen, die die NIS-2-RL reguliert (Anhang zur CER-RL). Die CER-RL zielt darauf ab, die Fähigkeiten der betroffenen Einrichtungen zu stärken, Sicherheitsvorfälle zu verhindern und die Folgen eingetretener Vorfälle zu vermindern (Art. 1 Abs. 1b, 2 Nr. 2 CER-RL). Gemäß Art. 13 CER-RL sollen die betroffenen Einrichtungen verpflichtet werden, Maßnahmen zur Stärkung ihrer Resilienz zu ergreifen; die Pflichten der NIS-2-RL gehen jedoch den CER-Pflichten vor (Art. 1 Abs. 2 CER-RL). Im Fokus der CER-RL steht dabei der physische Schutz der Einrichtungen. Soweit Art. 13 Abs. 1b CER-RL dabei den Begriff „Zugangskontrollen" verwendet, besteht Verwechslungsgefahr zum Datenschutzrecht, welches zwischen dem Zutritt (physische Näherung) und dem Zugang (technische Nutzungsmöglichkeit) zu einer Datenverarbeitungsanlage unterscheidet.[18] Art. 13 Abs. 1b) CER-RL dürfte den Zutritt meinen.

c) DORA

Mit der NIS-2-RL und der CER-RL hat die EU am 14. 12. 2022 die VO (EU) 2022/2554 (Digital Operational Resilience Act – DORA) verabschiedet. Sie ist seit dem 16. 1. 2023[19] in Kraft, gilt aber erst nach einer Übergangsfrist von zwei Jahren, mithin ab dem 17. 1. 2025 (Art. 64 DORA). Ihr Zweck ist es, ein hohes gemeinsames Niveau an digitaler operationaler Resilienz auf dem Finanzsektor zu erreichen. Dazu legt der DORA einheitliche Anforderungen für die Sicherheit von Netzwerk- und Informationssystemen fest (Art. 1 DORA).

Die DORA-Pflichten gelten für die Unternehmen der Finanzbranche, welche in Art. 2 Abs. 1 DORA gelistet sind, insbesondere Kredit- und Zahlungsinstitute, Wertpapierfirmen, Anbieter von Krypto-Dienstleistungen usw.

Eine Sonderrolle nehmen Versicherungsvermittler ein, für die die DORA-Pflichten vollkommen neu sind. Ausgenommen von den DORA-Pflichten sind jedoch alle Versicherungsvermittler mit weniger als 250 Mitarbeitern und einem Jahresumsatz von weniger als 50 Mio. Euro bzw. einer Jahresbilanzsumme von weniger als 43 Mio. Euro (Art. 2 Abs. 3 lit. e DORA). Diese Ausnahme dürfte den Großteil der Versicherungsvermittler betreffen.[20]

Eine weitere Sonderrolle erhalten IKT[21]-Drittdienstleister (Art. 2 Abs. 1 lit. u DORA). Für sie gibt es Vorschriften zur Gestaltung ihres Auftragsverhältnisses zu ihren Kunden aus der Finanzbranche (Artt. 28 bis 30 DORA); darüber hinaus können sie als kritische Dienstleister der unmittelbaren Aufsicht der DORA-Überwachungsbehörde (Bundesanstalt für Finanzdienstleistungsaufsicht – BaFin) unterliegen (Artt. 31 bis 43 DORA).

Die DORA-Pflichten bestehen auf folgenden Ebenen, wobei insgesamt ein risikobasierter Ansatz und das Verhältnismäßigkeitsprinzip gelten (Art. 4 DORA):[22]

14 *Schmidl/Thannen*, in: Kipker (Fn. 11), Kap. 8 Rn. 28 - 43; *Deusch/Eggendorfer*, in: Taeger/Pohle (Hrsg.), Computerrechts-Handbuch, 38. Aufl. 2023, Kap. 50.1 Rn. 398. *Deusch/Eggendorfer*, Beauftragte für Informationssicherheit und für IT-Sicherheit, 2024, Ziffern 1.5, 3.1.1 und 5.1.

15 *Wegmann*, BB 2023, 835 - 837. Zu Recht wirft *Schmidt* (K&R 2023, 705, 707) die Frage auf, weshalb es sich gemäß Art. 21 Abs. 1 NIS-2-RL ergänzend zu Art. 14 NIS-RL um „operative" Maßnahmen handeln muss.

16 Zu Recht diskutiert von *Voigt/Schmalenberger*, CR 2023, 717, 721.

17 https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/KRITIS-DachG.html; dazu *Voigt/Schmalenberger*, CR 2023, 717 sowie unten Ziffer 2 lit. b.

18 *Freund*, in: Schuster/Grützmacher, IT-Recht, Kommentar, 2020, Art. 32 Rn. 78, 79.

19 20 Tage nach ihrer Verkündung.

20 *Kahlscheuer*, AssCompact 2023, 102.

21 IKT = Informations- und Kommunikationstechnologie [Art. 1 lit. a i) DORA].

22 *Voigt/Ritter-Döring*, CR 2023, 82 - 90; *Pohle*, VersR 2023, 273 - 283.

aa) IKT-Risikomanagement

Die betroffenen Unternehmen haben ein IKT-Risikomanagement zu installieren (Artt. 5 bis 16 DORA). Dabei wird Art. 5 Abs. 2 lit. a DORA hinterfragt, wonach das Leitungsorgan die letztendliche Verantwortung für das Management der IKT-Risiken trägt, was der bisherigen Systematik entgegenstehe, Aufgaben zu delegieren und die Haftungsverantwortung in der Unternehmensleitung auf angemessene Kontrolle zu beschränken.[23] Art. 6 DORA gibt detaillierte Anforderungen an die Ausgestaltung des Risikomanagements; ob die herkömmliche Funktion des Informationssicherheitsbeauftragten (ISB) geeignet ist, um die Kontrollfunktion gemäß Art. 6 Abs. 4 DORA zu erfüllen, wird die Praxis zeigen.[24]

bb) Erfassung und Meldung von IKT-bezogenen Vorfällen

Die Artt. 17 bis 23 DORA geben vor, dass und wie die Finanzunternehmen IKT-bezogene Vorfälle (Art. 3 Nr. 8 DORA; gemeint sind sogenannte „Incidents" im Sinne der Controls A 5.24 bis A 5.29 und A 6.8 der ISO/IEC 27001:2022) erfassen, klassifizieren und behördlich zu melden haben.

cc) Testpflicht

Das Testen der digitalen operationellen Resilienz schreiben die Artt. 24 bis 27 DORA vor mit entsprechenden Vorgaben bis hin zu Penetrationstests.

dd) Management des IKT-Drittparteienrisikos

Vom Management des IKT-Drittparteienrisikos gemäß Kapitel V sind auch die IKT-Dienstleister betroffen. Ähnlich wie Art. 28 DSGVO gibt Art. 30 DORA Inhalte für die Verträge vor, die Finanzunternehmer mit IKT-Dienstleistern abschließen, allerdings weitaus detaillierter. Artt. 31ff. DORA unterwerfen „kritische IKT-Dienstleister" der unmittelbaren Aufsicht der DORA-Aufsichtsbehörden. IT-Dienstleistungsverträge mit Bezug zu Finanzinstituten sind daher anzupassen.

ee) Behörden und Sanktionen

Kapitel VII DORA regelt die Zuständigkeit und Befugnisse der Behörden sowie die Sanktionen bei Verstößen.

Auf der Website der BaFin sind Informationen zur Umsetzung des DORA in Deutschland enthalten, unter anderem der Verweis auf das geplante Finanzmarktdigitalisierungsgesetz (Referentenentwurf).[25] Hiernach sind Änderungen an den BAIT und VAIT zu erwarten, die laut Referentenentwurf höhere Risk-Management-Anforderungen als DORA stellen (Seiten 188, 208 des Referentenentwurfs).

d) Data Act

Der Data Act (VO (EU) 2023/2854) ist am 13. 12. 2023 beschlossen, am 22. 12. 2023 verkündet, gemäß Art. 50 Data Act am 11. 1. 2024 in Kraft getreten und ist ab dem 12. 9. 2025 zu befolgen. Er regelt, wie mit Daten umzugehen ist, die bei der Nutzung von vernetzten Produkten (bzw. mit diesen verbundenen Diensten) generiert werden. Interesse an diesen Daten haben einerseits der Hersteller bzw. Entwickler des Produkts und andererseits der Nutzer. Der Data Act strebt einen fairen Ausgleich dieser Interessen an (ErwG 6 Data Act).

Der Data Act gilt im unternehmerischen Rechtsverkehr und gegenüber Verbrauchern. Das vernetzte Produkt kann z. B. ein PKW, ein Lkw, eine landwirtschaftliche Maschine oder eine vernetzte Maschine in einem Produktionsprozess sein, ebenso wie Verbraucherprodukte (vernetzter Kühlschrank, smarte Heizkörperthermostate oder Staubsaugerroboter).[26]

Aus Sicht der IT-Sicherheit sind insbesondere die Artt. 3, 4, 5, 11 und 33 relevant.

Gemäß Art. 3 Abs. 1 Data Act sollen vernetzte Produkte und verbundene Dienste so konzipiert sein, dass die Produkt- und Dienstdaten für den Nutzer einfach, sicher, unentgeltlich und in einem gängigen maschinenlesbaren Format direkt zugänglich sind. Damit wird der Hersteller verpflichtet, die Ansprüche von Nutzern nach dem Data Act „by design" bereits in der Entwicklung zu berücksichtigen.[27] Insoweit ist die Regelung vergleichbar mit der „Privacy by design"-Forderung des Art. 25 Abs. 1 DSGVO. Welche Anforderungen an die Sicherheit der Datenzugänglichkeit in concreto zu stellen sind, lässt die Regelung offen.

Die Sicherheit des Datenzugangs ist auch in Art. 4 Abs. 1 Data Act gefordert, der den Anspruch des Nutzers auf den Zugriff bzw. die Bereitstellung der Daten festlegt. Gleiches gilt für Art. 5 Data Act, welcher den Anspruch des Nutzers auf die „sichere" Weitergabe der Daten an einen Dritten regelt, vergleichbar zur Datenportabilität gemäß Art. 20 DSGVO.[28] Zu den Rechten aus den Artt. 4 und 5 Data Act ist mit ähnlichen Problem zu rechnen wie sie zu Art. 20 DSGVO bestehen: für den Nutzer sind sie nur werthaltig, wenn nicht nur Datenformate, sondern auch die Strukturen der Daten für seine Zwecke passend sind.[29] Auch die Sicherheit einer Datenübertragung – sei es an den Nutzer oder an einen Dritten – ist davon abhängig, dass Absender und Empfänger Einigkeit zur Übermittlung hergestellt haben, z. B. durch den Schlüsselaustausch bei Ende-zu-Ende-verschlüsselter E-Mail-Kommunikation. Hier fehlen Vorgaben für verpflichtende einheitliche Standards. Dieses Problem wird auch nicht durch Art. 33 Data Act behoben, der zwar Vorgaben zur Interoperabilität für Datenräume[30] festlegt, aber keine einheitlichen Standards zum Datenaustausch.

Offen ist auch, wie Art. 4 Abs. 2 Data Act angewendet werden wird. Hiernach können Zugang zu sowie Nutzung von Daten vertraglich beschränkt werden, wenn dies eine im Unionsrecht oder im nationalen Recht festgelegte Sicherheitsanforderung des vernetzten Produkts beeinträchtigt.

Gemäß Art. 11 Data Act dürfen die Dateninhaber Schutzmaßnahmen gegen unberechtigte Zugriffe auf die Daten treffen. Die Nutzer dürfen diese Schutzmaßnahmen nicht ändern oder umgehen (Art. 11 Abs. 1 S. 2 Data Act).

e) Maschinenverordnung

Die VO (EU) 2023/1230 (Maschinenverordnung – MV) ist am 14. 6. 2023 beschlossen, am 29. 6. 2023 verkündet und gemäß Art. 54 am 19. 7. 2023 in Kraft getreten. Sie löst mit Wirkung zum 14. 1. 2027 die bis dahin gültige Maschinenrichtlinie

23 *Siglmüller*, in: Bernzen/Fritzsche/Heinze/Thomsen (Hrsg.), Das IT-Recht vor der (europäischen) Zeitenwende, 2023, S. 339, 345.

24 ISBe sind gemäß §§ 25a KWG, 80 WpHG i. V. m. Ziffer 4.4 KAIT, § 27 ZAG i. V. m. Ziffer 4.4 ZAIT und § 28 KAG i. V. m. Ziffer 4.42 KAIT zu bestellen, siehe dazu und zu den DORA-Neuerungen *Deusch/Eggendorfer* (Fn. 7), Ziffer 3.1.6.

25 https://www.bafin.de/DE/Aufsicht/DORA/DORA_node.html;jsessionid=4D142DFF4226D031DFD8EE35AE2022EF.internet012.

26 *Funk*, CR 2023, 421, 425.

27 *Antoine*, CR 2024, 1, 4.

28 *Antoine*, CR 2024, 1, 2 bezeichnet den Data Act unter Berufung auf ErwG 35 als „Datenportabilität 2.0".

29 Zu Art. 20 DSGVO: *Deusch/Eggendorfer*, K&R 2020, 105, 106; derselbe Gedanke zum Data Act *Funk*, CR 2023, 421, 425.

30 Gemeint sind damit Cloud-Anbieter.

2006/42/EG ab (Art. 51 MV). Gemäß Art. 1 MV regelt die Verordnung die Sicherheits- und Gesundheitsschutzanforderungen an Konstruktion und Bau von Maschinen, dazugehörigen Produkten und unvollständigen Maschinen und deren Bereitstellen auf dem Markt.

Im Gegensatz zur bisherigen Maschinenrichtlinie will die MV Regelungslücken in Bezug auf die Nutzung digitaler Technologien schließen (ErwG 12) sowie die Risiken regeln, die böswillige Dritte in diesem Zusammenhang hervorrufen (ErwG 25 und 51 MV). Es geht mithin um IT-Security-Anforderungen.[31]

Gemäß Art. 8 MV dürfen Maschinen und dazugehörige Produkte sowie unvollständige Maschinen nur dann auf dem Markt bereitgestellt oder in Betrieb genommen werden, wenn sie die grundlegenden Sicherheits- und Gesundheitsschutzanforderungen nach Anhang III der Verordnung erfüllen. Anhang III enthält einen umfassenden Katalog an Sicherheits- und Gesundheitsanforderungen. Aus Sicht der IT-Security sind die Ziffern 1.1.9 und 1.2.1 des Anhangs III relevant. Hiernach muss die Maschine vor Korrumpierung geschützt sein, insbesondere bei Fernzugriffen (Ziffer 1.1.9). Außerdem definiert Ziffer 1.2.1 Anforderungen an die Sicherheit und Zuverlässigkeit von Steuerungen der Maschinen. Diese Anforderungen gelten als erfüllt, wenn für die betreffende Maschine ein Cybersicherheitszertifikat oder eine Konformitätserklärung gemäß dem Cybersecurity Act (VO (EU) 2019/881) existiert.[32]

f) Vorschläge der EU-Kommission

Folgende EU-Rechtsakte befinden sich im Legislativverfahren, sind aber noch nicht verabschiedet:

aa) Cyber Resilience Act

Der Cyber Resilience Act ist als Verordnung vorgeschlagen und soll Anforderungen zur IT-Sicherheit an alle Produkte mit digitalen Elementen vorgeben.[33] Mit dem Abschluss des Trilogs (30. 11. 2023) ist die Anwendung der Verordnung erweitert worden auf Identitätsmanagementsysteme, Passwort Manager, biometrische Lesegeräte, Smart Home Assistenten und private Überwachungskameras. Am 10. 4. 2024 steht die erste Lesung im Europäischen Parlament an.[34]

bb) KI-Verordnung

Die Trilog-Verhandlungen zum Vorschlag der KI-Verordnung haben im Dezember 2023 eine vorläufige Einigung erbracht; der Rat der EU erwartet nunmehr die Verabschiedung durch das EU-Parlament.[35] *Wagner* weist auf den Zusammenhang der geplanten KI-Verordnung mit dem weiteren Kommissionsvorschlag für eine *Richtlinie über KI-Haftung* hin, welche keine Haftungsgründe regelt, sondern lediglich die Beweislast bei der Geltendmachung außervertraglicher Ansprüche vor nationalen Gerichten in Bezug auf Schäden, die durch ein KI-System verursacht wurden.[36]

cc) EU Cyber Solidarity Act

Ein Europäischer Cyber Schutzschild („European Cyber Shield“) soll entwickelt werden, um Cyberbedrohungen und Vorfälle zu entdecken, zu analysieren und zu bearbeiten; dabei sollen die nationalen Cyberabwehrzentren mit grenzüberschreitenden Sicherheitszentren zusammenarbeiten (Kapitel 2, Artt. 3 - 8). Weiter definiert der Verordnungsvorschlag Mechanismen bzw. Vorgehensweisen, wie die neu gebildeten Kapazitäten in Cybernotfällen abgerufen werden können und wie Nachbetrachtungen („Reviews“) von Cybervorfällen und Cyberbedrohungen durchgeführt werden können (Kapitel 3 und 4 des Verordnungsvorschlags).[37]

dd) eIDAS-Verordnung

Zum Reformvorschlag der eIDAS-Verordnung[38] wurde im November 2023 eine Einigung im Trilog erzielt. Kritisch zu hinterfragen sind dabei die jüngsten Änderungen, wonach staatliche Stellen spezielle Authentifizierungszertifikate ausstellen dürfen, die Webbrowser anerkennen müssen (Qualified Website Authentication Certificate – QWAC). Denn dies ermöglicht es staatlichen Stellen, die Verbindung zwischen einer Website und dem Rechner des Website-Besuchers auszuspähen.[39] Aus Sicht der IT-Sicherheit ist dieser Regelungsvorschlag daher kontraproduktiv.

ee) Chatkontrolle

Die aktuelle Regelung zur sogenannten „Chatkontrolle“ ermächtigt Anbieter digitaler Kommunikationsdienste – befristet bis zum 3. 8. 2024 – dazu, die Kommunikation ihrer Kunden zu überwachen, um Kindesmissbrauch zu verhindern (VO (EU) 2021/1232); danach sollte aus der Kontrollbefugnis eine Kontrollpflicht werden.[40] Da der politische Entscheidungsprozess zur Kontrollpflicht noch nicht abgeschlossen ist, hat die EU-Kommission im November 2023 vorgeschlagen, die derzeitige Rechtslage bis zum 3. 8. 2026 zu verlängern.[41] In technischer Hinsicht ist unklar, wie eine Kontrollpflicht zu realisieren ist, wenn der Anbieter, wie von der IT-Sicherheit gefordert und z. B. in Signal, Wire oder Threema implementiert, eine Verschlüsselung von Nutzer zu Nutzer implementiert hat. In dem Fall hat der Anbieter nur Zugriff auf verschlüsselte Datenströme und keine Möglichkeit, Inhal-

31 Ein wesentlich breiterer Teil der MV befasst sich dagegen mit Safety-Anforderungen.

32 Allerdings gewährleistet auch ein solches Zertifikat nur mäßige IT-Sicherheit, siehe zur Kritik am Cybersecurity Act und seiner derzeitigen Anwendung *Deusch/Eggendorfer*, K&R 2023, 781, 784.

33 *Deusch/Eggendorfer*, K&R 2022, 794, 796; *Piltz/Weiß/Zwerschke*, CR 2023, 154 - 162; *Voigt/Falk*, MMR 2023, 88 - 93; *Hessel/Callewaert*, K&R 2022, 789; kritisch *Siglmüller*, in: Bernzen/Fritzsche/Heinze/Thomsen (Fn. 23), S. 339, 341, dort auch *Schöttle*, in: Bernzen/Fritzsche/Heinze/Thomsen (Fn. 23), S. 651 ff.

34 Zum Abschluss des Trilogs mit der Erweiterung des Anwendungsbereichs die Pressemitteilung des Europäischen Parlaments vom 1. 12. 2023: https://www.europarl.europa.eu/news/en/press-room/20231106IPR09007/cyber-resilience-act-agreement-with-council-to-boost-digital-products-security; zur Lesung am 10. 4. 2024 die Übersicht zum Legislativverfahren: https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2022/0272(COD)&l=en.

35 Pressemitteilung des Rats der EU vom 9. 12. 2023 (https://www.consilium.europa.eu/de/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/); generell zur vorgeschlagenen KI-Verordnung *Schneider/Streitz*, ITRB 2023, 266 - 268; *Denga*, CR 2023, 277 ff.; *Deusch/Eggendorfer* in: Taeger/Pohle (Fn. 14), Kap. 50.1 Rn. 232 l (grundsätzlich zur KI), 280 c, 337 und 385.

36 Richtlinienvorschlag: COM(2022) 496 final, dazu *Wagner*, in: Baumgärtel/Kiparski, DGRI Jahrbuch 2021/2022, 2023, S. 249, 278 – Haftungsregeln für das digitale Zeitalter.

37 Verordnungsvorschlag: COM(2023) 209 final vom 18. 4. 2023; zur Einbindung in die Politik der EU-Kommission: https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity.

38 *Deusch/Eggendorfer*, K&R 2022, 794, 796.

39 Zur Trilog-Einigung: Pressemitteilung der EU-Kommission vom 9. 11. 2023: https://digital-strategy.ec.europa.eu/de/news/commission-welcomes-final-agreement-eu-digital-identity-wallet; zur Kritik an der staatlichen QWAC-Erstellung: *Eggendorfer/Schmidt-Wudy*, K&R 2024, 13 - 18; ebenso die Position der Stiftung Forschungszentrum Informatik (FZI): https://www.fzi.de/2023/12/18/position-eidas/.

40 *Deusch/Eggendorfer*, K&R 2022, 794, 797.

41 COM(2023) 777 final vom 30. 11. 2023 (https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2023)777&lang=de).

te zu prüfen. Selbst wenn Hintertüren in die Verschlüsselung entgegen jedem guten Rat der IT-Sicherheit eingebaut würden, es hindert niemand die Täter daran, ausländische Dienste zu nutzen, die keine Überwachung implementieren. Technisch ist daher vermutlich die plausibelste Möglichkeit, eine Überwachung auf Smartphones zu installieren, wie es Apple bereits zur Erkennung von CSAM macht. Juristisch wiederum ist das nicht unumstritten.[42]

ff) Reform der Produkthaftungsrichtlinie

Der Entwurf zur Reform der Produkthaftungsrichtlinie (bislang RL 85/374/EWG) unterwirft auch Software den Produkthaftungsregelungen, was bislang streitig war. Zudem legt Art. 6 Nr. 1 lit. f des Richtlinienvorschlags fest: Ein Produkt ist fehlerhaft, wenn es nicht die Sicherheit bietet, die die breite Öffentlichkeit unter Berücksichtigung der „sicherheitsrelevanten Cybersicherheitsanforderungen" erwarten darf. Fraglich ist, welche IT-Sicherheit eine breite Öffentlichkeit angesichts der desolaten IT-Sicherheitslage mit täglichen Vorfällen[43] erwartet. Erstaunlich ist, dass die Kommission in ihrem Vorschlag nur in Erwägungsgrund 43 an den Stand der Wissenschaft und Technik anknüpft und nicht bei der Definition der Fehlerfreiheit in Art. 6. Stattdessen wird dort eine kaum prüf- und messbare „allgemeine Erwartungshaltung" herangezogen. Damit würde die Richtlinie letztlich sogar einen Anreiz für Anbieter schaffen, weiterhin unsichere Software anzubieten, denn dann steigen die Erwartungen der breiten Öffentlichkeit nicht.

Art. 10 Nr. 2 des Richtlinienvorschlags ordnet zudem an, dass der Hersteller, Händler bzw. Anbieter („Wirtschaftsakteur") auch dann haftet, wenn ein Update nach dem Inverkehrbringen unterlassen wurde, obwohl es zur Aufrechterhaltung der Sicherheit des Produkts erforderlich war, was praktisch zu einer gesetzlichen Updatepflicht zu den betreffenden Produkten führt.[44]

2. Neuerungen in der nationalen Gesetzgebung

Die nationale Gesetzgebung verzeichnet insbesondere folgende Neuerungen:

a) NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG)

Das NIS2UmsuCG soll die NIS-2-RL umsetzen. Bislang existiert ein Referentenentwurf („BISG-E") und ein Diskussionsentwurf dazu („BISG-E-DP"), wie oben in Ziffer 1 lit. a ausgeführt.[45]

Das NIS2UmsuCG ist ein Artikelgesetz, welches in Art. 1 eine vollständige Neufassung des BSIG enthält und in den weiteren Artikeln andere Gesetze anpasst, z. B. das BND-Gesetz, das TTDSG, das EnWG, das SGB V und das TKG.

Teil 1 BSIG-E benennt das BSI als zentrale Stelle für Informationssicherheit auf nationaler Ebene und enthält Begriffsdefinitionen. Teil 2 regelt die Aufgaben und Befugnisse des BSI. Für die Unternehmen und öffentlichen Stellen ist Teil 3 (§§ 28 - 42 BSIG-E) relevant, sie setzen die IT-Sicherheitspflichten der NIS-2-RL um, wie oben in Ziffer 1. lit. a dargestellt. Sonderregelungen gibt es für die Einrichtungen der Bundesverwaltung (§§ 44 ff. BSIG-E). Zum Beispiel schreibt § 45 BSIG-E verpflichtend für Einrichtungen der Bundesverwaltung vor, einen Informationssicherheitsbeauftragten zu benennen.

Teil 4 BSIG-E verpflichtet Top Level Domain Name Registries und Domain-Name-Registry-Dienstleister in Umsetzung von Art. 28 NIS-2-RL, genaue und vollständige Domain-Namen-Registrierungsdaten in einer eigenen Datenbank zu sammeln und zu pflegen. Unklar bleibt, wie diese Forderung für Domains außerhalb Europas durchgesetzt werden soll. Täter werden dorthin ausweichen. So nutzen viele IT-Projekte den Top-Level „.io", der nach „Input/Output" klingt, aber tatsächlich Britischen Überseegebieten zugeordnet ist, eine Zeit war „.ag" (Antigua) so beliebt, dass sogar die Rechtsprechung feststellte, dass eine GmbH sie nicht nutzen dürfe, sie sei irreführend über die Rechtsform.[46]

Teil 5 enthält die Regelungen zur Zertifizierung durch das BSI einschließlich des IT-Sicherheitskennzeichens.[47] Praxisrelevant in Teil 6 ist v. a. § 57 BISG-E mit der Ermächtigung des BMI, Rechtsverordnungen zu weiteren Inhalten zu regeln; hierunter fällt insbesondere die sogenannte „KRITIS-Verordnung" mit ihren Regelungen, welche Unternehmen und sonstigen Stellen als „kritische Infrastrukturen" die besonderen Sicherheitspflichten des BISG erfüllen müssen (bislang § 10 BSIG). Teil 7 BSIG-E schließt mit den Sanktionsbefugnissen, welche jedoch erheblich erweitert sind. Wer z. B. nach aktueller Rechtslage als Betreiber kritischer Infrastrukturen entgegen § 8a BSIG keine organisatorischen und technischen Vorkehrungen zur IT-Sicherheit trifft, kann gemäß § 11 Abs. 5 BSIG mit einem Bußgeld bis zu € 2,0 Mio. belegt werden. Derselbe Verstoß wird gemäß § 60 Abs. 6 BSIG-E für wichtige Einrichtungen mit einem Bußgeld bis zu € 7,0 Mio. (oder 1,4 % des Jahresumsatzes) bzw. gemäß § 60 Abs. 7 BSIG-E für besonders wichtige Einrichtungen und Betreiber kritischer Anlagen mit einem Bußgeld bis zu € 10,0 Mio. (oder 2 % des Jahresumsatzes) bedroht.

b) Systeme zur Angriffserkennung in KRITIS-Unternehmen; KRITIS-Verordnung

Kohpeiß/Schaller weisen auf § 8a Abs. 1a BSIG hin, der in seiner bereits derzeit gültigen Fassung Betreiber Kritischer Infrastrukturen seit dem 1. 5. 2023 zum Einsatz von Angriffserkennungssystemen verpflichtet (künftig gemäß § 31 Abs. 2 BSIG-E-DP).[48]

Zudem gab es mehrfache Änderungen in der KRITIS-Verordnung, in der das Bundesinnenministerium gemäß § 10 BSIG die Adressaten der IT-Sicherheitspflichten des BSIG festlegt: Infolge der 2. Änderung der KRITIS-Verordnung gelten reduzierte Schwellenwerte für Stromerzeuger, was die Anzahl der Energieunternehmen, die die KRITIS-Pflichten nach BSIG und EnWG befolgen müssen, erhöht hat. Die 3. Änderung hat mit Wirkung zum 2. 3. 2023 in den Anhängen der KRITIS-Verordnung sogenannte LNG-Anlagen (Flüssiggas) zu den KRITIS-

42 Siehe hierzu auch *Eggendorfer/Schmidt-Wudy*, ZD 2021, 674 ff.
43 Siehe oben die Einleitung in Abschnitt I.
44 Reformvorschlag COM(2022) 495 final vom 28. 9. 2022, dazu *Wagner* (Fn. 32), S. 260ff.; *Bronner/Ziegler*, jurisPR-ITR 1/2023 Anm. 2.
45 Nähere Auskünfte zum Stand des Gesetzgebungsverfahrens waren nicht zu erhalten. Das BMI hat auf Anfrage der Autoren per E-Mail vom 8. 1. 2024 mitgeteilt: „Das BMI strebt ein Inkrafttreten des NIS2UmsuCG innerhalb der Richtlinienumsetzungsfrist an, welche am 17. 10. 2024 endet." Ob die Frist eingehalten werden kann, ist daher schwer zu prognostizieren. Zum NIS2UmsuCG siehe auch *Kipker*, MMR 2023, 481 ff.
46 OLG Hamburg, 16. 6. 2004 – 5 U 162/03, K&R 2004, 492.
47 Bislang §§ 9 ff. BSIG, dazu *Deusch/Eggendorfer*, K&R 2023, 781, 783 - 785.
48 *Kohpeiß/Schaller*, CR 2023, 635; dieselben in CR 2024, 22 - 29 mit Bezug zu KI-Angriffserkennung als Stand der Technik unter Berücksichtigung der geplanten KI-Verordnung; *Deusch/Eggendorfer*, K&R 2018, 753 ff., zur Technik der Systeme *Deusch/Eggendorfer* (Fn. 7), Ziffer 2.7.2.3.

Energieversorgern und Anlagen zur Anbindung von Seekabeln für die Kommunikation dem KRITIS-Bereich der IT zugeordnet. Die 4. Änderung der KRITIS-Verordnung gilt seit 1. 1. 2024 und hat in § 9 KRITIS-Verordnung den Sektor Siedlungsabfallentsorgung aufgenommen.[49]

c) Kritis-Dachgesetz

Zur Umsetzung der CER-RL (oben Ziffer 1 lit. b) existiert ein Referentenentwurf für ein KRITIS-Dachgesetz (KRITIS-DachG-E).[50] Gemäß dem Ziel der Richtlinie soll das KRITIS-DachG-E v. a. den physischen Schutz von Anlagen und Dienstleistungen sichern, welche für die Aufrechterhaltung wirtschaftlicher Tätigkeiten und Funktionen unerlässlich sind (§ 1 KRITIS-DachG-E). Das Gesetz gilt gemäß den Begriffsbestimmungen in § 2 für Betreiber kritischer Anlagen und Anbieter kritischer Dienstleistungen sowie für wichtige und besonders wichtige Einrichtungen (allesamt in Umsetzung der CER-RL). Zudem gilt das KRITIS-DachG-E für kritische Infrastrukturen i. S. d. § 2 Nr. 2 KRITIS-DachG-E, wobei dieser Begriff auf nationalem Recht beruht (siehe die Gesetzesbegründung Seite 32). Zuständige nationale Behörde ist gemäß § 3 Abs. 1 KRITIS-DachG-E das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK). Die Pflichten des KRITIS-DachG-E bestehen im Wesentlichen aus Registrierungen (§ 8 KRITIS-DachG-E), einem Risikomanagement (§ 10 KRITIS-DachG-E) mit technischen, sicherheitsbezogenen und organisatorischen Maßnahmen zur Gewährleistung der Resilienz (§ 11 KRITIS-DachG-E) und einer Meldepflicht bei Störungen (§ 12 KRITIS-DachG-E).

3. Untergesetzliche Normen

Im Bereich der untergesetzlichen Normen sind folgende Neuerungen relevant:

a) ISO/IEC 27001:2022

Die Norm ISO 27001 beschreibt, wie ein Informations-Sicherheits-Management-System einzurichten und zu betreiben ist. Aufgrund ihrer internationalen Anerkennung[51] hat die Norm große Bedeutung in der Praxis. Im Oktober 2022 hat die International Organization for Standardization (ISO) die nun aktuelle Version ISO/IEC 27001:2022 herausgegeben.[52] Dafür gilt eine *Umsetzungsfrist bis zum 30. 10. 2025*. Zertifikate, die aufgrund der bisherigen Fassung ISO/IEC 27001:2013[53] erteilt wurden, sind ab dem 1. 11. 2025 ungültig.[54]

Die ISO/IEC 27001:2022 besteht aus einem Normteil mit 10 Normen und einem Anhang mit 93 „Controls“. Dies sind Kontrollfragen, deren Beantwortung Aufschluss darüber geben soll, ob und wie das jeweilige Risiko behandelt wird. Dabei sind einige der bislang 114 Controls zusammengefasst worden, so dass sich die Anzahl reduziert hat, ohne dass auf inhaltliche Belange verzichtet wurde. Neu sind die Controls 5.19 bis 5.23 mit den Fragen zur Informationssicherheit in der Lieferkette von Zulieferern und Dienstleistern, zu Cloud Computing und zu Remote-Anwendungen.[55]

b) 7. MaRisk-Novelle

Die Mindestanforderungen an das Risikomanagement (MaRisk) sind ein Rundschreiben der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin). Darin legt die BaFin dar, welche Anforderungen sie an die Unternehmen stellt, die die Pflichten zum Risikomanagement gemäß den §§ 25a und 25b KWG erfüllen müssen. Zur Umsetzung der Leitlinien für die Kreditvergabe und Überwachung der European Banking Authority (EBA/GL/2020/06) hat die BaFin am 29. 6. 2023 die 7. MaRisk-Novelle veröffentlicht. Mit Blick auf die IT-Sicherheit ist von Belang, dass das Risikomanagement (einschließlich IT-Sicherheit) auch für Geschäfte der Banken mit eigenen Immobilien gilt (BTO 3 der MaRisk). Zudem sind in BTO 2.2.1 Anforderungen an die Abwicklung von Wertpapiergeschäften im Homeoffice formuliert. Die Umsetzungsfrist für die Anwendung der neuen MaRisk endete am 1. 1. 2024.[56]

Dr. Florian Deusch
ist Rechtsanwalt und Fachanwalt für Informationstechnologierecht in der Anwaltskanzlei Dr. Gretter in Ravensburg. Er ist zudem als Datenschutzbeauftragter tätig.

Prof. Dr. Tobias Eggendorfer
ist Professor für Sicherheit in verteilten Anwendungen an der TH Ingolstadt, davor war er als Abteilungsleiter „Sichere Systeme“ an der Agentur für Innovation in der Cybersicherheit für die Weiterentwicklung der Forschung im Bereich der IT-Sicherheit zuständig. Er ist zudem als IT-Berater und Datenschutzbeauftragter tätig.

49 BGBl. I 2023 Nr. 339 vom 6. 12. 2023.
50 https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/KRITIS-DachG.html; dazu im Einzelnen *Kipker/Dittrich*, ZRP 2023, 230 ff.
51 Die Anerkennung derartiger Akkreditierungen ist durch internationale Abkommen geregelt; in Deutschland ist die Deutsche Akkreditierungsstelle GmbH (Dakks) für die Anerkennung von Akkreditierungen zuständig (https://www.dakks.de/de/home.html).
52 https://www.iso.org/standard/27001.
53 Dazu existiert eine deutsche Übersetzung mit der Bezeichnung ISO/IEC 27001:2017, die inhaltlich aber mit der Fassung aus 2013 übereinstimmt.
54 *Deusch/Eggendorfer* (Fn. 7), Ziffer 3.3.3; https://www.dakks.de/de/aktuelle-meldung/dakks-empfiehlt-fruehzeitige-umstellungen-bei-akkreditierungen-im-bereich-iso-iec-27001.html.
55 *Deusch/Eggendorfer* (Fn. 7), Ziffer 3.3.3.
56 Neufassung abrufbar unter https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2023/meldung_2023_06_29_BaFin_veroeffentlicht_siebte_MARisk_Novelle.html, dazu siehe z. B., *Schulte-Mattler, Markus/Schulte-Mattler, Herrmann*, WM 2023, 1678 ff. sowie aus der Sicht eines Informations- bzw. IT-Sicherheitsbeauftragten: *Deusch/Eggendorfer* (Fn. 7), Ziffer 3.1.6.

Hinweis der Redaktion:
Teil 2 des Beitrags lesen Sie in Heft 4/2024.