www.betriebs-berater.de

Betriebs Berater

BB

16 | 2023

Recht ... Wirtschaft ... Steuern ... Recht ... Wirtschaft ... Steuern ... Recht ... Wirtschaft ...

17.4.2023 | 78. Jg.
Seiten 833–896

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

Simon Clemens Wegmann, RA*

Too much of a good thing? Erweiterung und Verschärfung von Cybersicherheitspflichten durch die NIS2-Richtlinie

Am 16.1.2023 ist die Richtlinie (EU) 2022/2555, besser bekannt als NIS2-Richtlinie (auch „NIS2"), in Kraft getreten. Sie erweitert den bisher auf kritische Infrastrukturen und ausgewählte Sonderfälle beschränkten Anwendungsbereich der europäischen Cybersicherheitsgesetzgebung auf große Teile der Wirtschaft. Das betrifft auch Unternehmen, deren Geschäftsmodelle nicht als solche „digital" oder datenintensiv sind. Verstöße können – wie in der europäischen Datenregulatorik inzwischen üblich – mit erheblichen Bußgeldern geahndet werden und sogar eine direkte Haftung der Geschäftsleitung ist vorgesehen. Dieser Beitrag gibt einen ersten Ausblick auf die neuen oder erweiterten Cybersicherheitspflichten, auf die sich Unternehmen einstellen müssen, die in der EU bzw. in Deutschland niedergelassen sind oder ihre Dienste dort erbringen.

I. Einleitung

Dem Thema der Cybersicherheit[1] widmete sich die EU zum ersten Mal ernsthaft mit der NIS1-Richtlinie,[2] die am 8.8.2016 in Kraft trat und in Deutschland im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik („BSIG") umgesetzt ist. In ihrer Evaluation der NIS1-Richtlinie bemängelte die Europäische Kommission jedoch, dass die Richtlinie und ihre Umsetzung in den Mitgliedstaaten nicht zu einem hinreichenden Niveau an Cybersicherheit geführt hätten. Insbesondere sei das Maß an Cybersicherheit in gesellschaftlich wichtigen Wirtschaftszweigen zu niedrig, die Umsetzung der Richtlinie in den Mitgliedstaaten divergiere z. T. dramatisch, und damit einher gehe ein Mangel an Koordinations- und Reaktionsfähigkeit.[3] Dabei spielte auch eine Rolle, dass sich bedingt durch die Kontaktbeschränkungen im Rahmen der COVID-19-Pandemie große Teile des wirtschaftlichen und gesellschaftlichen Lebens fast über Nacht in den digitalen Raum verlagert hatten.[4] Am 16.12.2020 schlug die Kommission daher als Teil ihrer Cybersicherheitsstrategie eine Reform der NIS1-Richtlinie vor.[5]

Diese Reform in Gestalt der Richtlinie (EU) 2022/2555 oder NIS2-Richtlinie ist nunmehr in Kraft getreten. Die Mitgliedstaaten müssen sie bis zum 17.10.2024 in nationales Recht umsetzen und stehen dabei unter kaum weniger Druck als die Kommission im Winter 2020: Mit dem Angriffskrieg der Russischen Föderation auf die Ukraine löst eine neue Bedrohungslage im digitalen Raum den Digitalisierungsschub der Pandemie fast nahtlos als regulatorischen „Motivator" ab.[6]

Die NIS2-Richtlinie bettet sich ein in die übergreifende Digitalstrategie der Europäischen Kommission,[7] die mit einer Vielzahl an Maßnahmen den Weg in eine „digitale Dekade" ebnen soll. Zu diesen Maßnahmen gehört ein ganzer Blumenstrauß gesetzgeberischer Initiativen, von denen sich die Mehrzahl an Unternehmen richtet, die digitale Dienstleistungen erbringen[8] oder digitale Produkte entwickeln bzw. vertreiben.[9] Eine erste Ausnahme von dieser Regel bildete die Datenschutz-Grundverordnung (Verordnung (EU) 2016/679, „DS-GVO"), deren Umsetzung die gesamte Wirtschaft auch kurz vor ihrem fünften Geburtstag noch vor erhebliche Herausforderungen stellt.[10]

Die NIS2-Richtlinie ist zwar nicht derart breit in ihrem Anwendungsbereich wie die DS-GVO. Dennoch bedeutet sie deutlich mehr als eine bloß inkrementelle Anpassung der Cybersicherheitsgesetzgebung. Dementsprechend ist die Diskussion zwischen Verbänden, Politik und Wissenschaft um ihre sachgerechte Umsetzung bereits in vollem

* Der Verfasser dankt *Celine Biela*, Wiss. Mitarb., für die Unterstützung bei der Erstellung des Beitrags.

1 Bereits in den Erwägungsgründen der NIS1-Richtlinie erwähnt, findet sich der Begriff der Cybersicherheit nun auch in der offiziellen Übersetzung des Normtextes der NIS2-Richtlinie. Daher sieht sich der Verfasser zur Verwendung dieses unschönen Begriffs gezwungen und wähnt sich dabei in guter Gesellschaft (vgl. etwa *Kipker*, MMR-Aktuell 2023, 455199). Wie der Begriff des *Metaverse* (hierzu *Klar/Wegmann/Galandi*, BB 2022, 2691) stammt auch der Begriff des *Cyberspace* aus der Science Fiction-Literatur (*Coe*, Where does the word cyber come from?, Oxford University Press Blog vom 28.3.2015, https://blog.oup.com/2015/03/cyber-word-origins/ (Abruf: 27.3.2023)) und der Wortbestandteil *cyber* behauptet sich tapfer in der Diskussion digitaler Phänomene. Im Kontext der NIS2-Richtlinie wird hierdurch immerhin deutlich, dass es nicht nur um die Sicherheit von Daten als Schutzobjekt, sondern um die Sicherheit von Informations- und Kommunikationssystemen insgesamt geht.

2 Der Name leitet sich aus dem englischen Gebrauchsnamen der Richtlinie (EU) 2016/1148, der sog. *Network and Information Security Directive* („NIS1-Richtlinie") ab.

3 Vgl. *European Commission*, Executive Summary of the Impact Assessment Report zum Entwurf der NIS2-Richtlinie vom 16.12.2022, SWD(2020) 344 final, https://digital-strategy.ec.europa.eu/en/library/impact-assessment-proposal-directive-measures-high-common-level-cybersecurity-across-union (Abruf: 27.3.2023).

4 *Bundesministerium für Wirtschaft und Energie*, Digitalisierung in Deutschland – Lehren aus der Corona-Krise, 12.2.2021, https://www.bmwk.de/Redaktion/DE/Publikationen/Ministerium/Veroeffentlichung-Wissenschaftlicher-Beirat/gutachten-digitalisierung-in-deutschland.html (Abruf: 27.3.2023).

5 *European Commission*, PM vom 16.12.2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391 (Abruf: 27.3.2023).

6 *Kleine/Barthel*, Kritische Infrastruktur. Gesetzentwurf vor der Sommerpause?, tagesschau vom 25.1.2023, https://www.tagesschau.de/inland/innenpolitik/kritische-infrastruktur-gesetzentwurf-101.html (Abruf: 27.3.2023); schon vor der Invasion *Kolbe/Morrow/Zabierek*, The Cybersecurity Risks of the Escalating Russia-Ukraine Conflict, Harvard business Review vom 24.2.2022, https://hbr.org/2022/02/the-cybersecurity-risks-of-an-escalating-russia-ukraine-conflict (Abruf: 27.3.2023); *Bundesamt für Sicherheit in der Informationstechnik*, Die Lage der IT-Sicherheit in Deutschland 2022, Oktober 2022, S. 67.

7 *European Commission*, C(2022) 4388 final vom 30.6.2022, https://commission.europa.eu/system/files/2022-06/c_2022_4388_1_de_act.pdf (Abruf: 27.3.2023).

8 Etwa der sog. *Digital Services Act* (Verordnung (EU) 2022/2065, s. Art. 2 Abs. 1, 3 lit. g) und der sog. *Digital Markets Act* (Verordnung (EU) 2022/1925, s. Art. 1 Abs. 2, 2 Nr. 2), überwiegend auch der sog. *Data Governance Act* (Verordnung (EU) 2022/868, s. Art. 1 Abs. 1 lit. b, c, 2 Nr. 11, 15, 16) und teilweise der sog. *Data Act* (s. Art. 1 Abs. 2 lit. a Var. 2, b, e, 2 Nr. 3, 12 des Kommissionsentwurfs, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52022PC0068&from=EN (Abruf: 27.3.2023).

9 Etwa der sog. *Artificial Intelligence Act* (s. Art. 2 Abs. 1 lit. a des Kommissionsentwurfs, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52021PC0206&from=EN (Abruf: 27.3.2023)) und wiederum teilweise der sog. *Data Act* (s. Art. 1 Abs. 2 lit. a Var. 1 des Kommissionsentwurfs, vgl. Fn. 8). S. zu den diversen Gesetzgebungsinitiativen auch den Überblick bei *Ohrtmann/Golland*, DSB 2023, 43.

10 So die Ergebnisse einer Umfrage durch den Branchenverband bitkom, s. PM vom 27.9.2022, https://www.bitkom.org/Presse/Presseinformation/Datenschutz-deutsche-Wirtschaft-2022-DS-GVO-wenig-Wettbewerbsvorteile (Abruf: 27.3.2023).

Gange.[11] Während die Stärkung von Cybersicherheit als Ziel unisono begrüßt wird, warnen einige Wirtschaftsverbände den Gesetzgeber davor, zu viel des Guten zu tun.[12]

Im Folgenden werden kurz die wesentlichen Cybersicherheitspflichten dargestellt, denen deutsche Unternehmen aktuell unterliegen (s. unter Ziff. II.). Darauf aufbauend wird erläutert, welche Änderungen sich durch die NIS2-Richtlinie ergeben werden – insbesondere, welche Unternehmen zukünftig unter die neuen Cybersicherheitspflichten fallen werden und welche Folgen ein Verstoß gegen diese Pflichten haben kann (s. unter Ziff. III.). Schließlich wird auf andere relevante Gesetzgebungsvorhaben in diesem Bereich hingewiesen (s. unter Ziff. IV.). Der Beitrag schließt mit einem Ausblick auf die Zeit bis zur Umsetzung der NIS2-Richtlinie in nationales Recht (s. unter Ziff. V.).

II. Wesentliche aktuelle Cybersicherheitspflichten für deutsche Unternehmen

Aktuell ergeben sich Cybersicherheitspflichten für deutsche Unternehmen im Wesentlichen aus dem BSIG (s. unter Ziff. II. 1.), der DS-GVO (s. unter Ziff. II. 2.) und dem Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien („TTDSG", s. unter Ziff. II. 3.). Für die besonderen Bereiche der Telekommunikation, Energieversorgung, Atomkraft und Telematik enthalten die jeweiligen Spezialgesetze ebenfalls Cybersicherheitspflichten. Besondere Cybersicherheitspflichten können sich zudem aus Produktsicherheitsrecht ergeben (s. unter Ziff. II. 4.).

1. Cybersicherheitspflichten unter dem BSIG

Das BSIG ist das zentrale Cybersicherheitsgesetz in Deutschland und dient wie erwähnt auch der Umsetzung der europäischen Cybersicherheitsgesetzgebung. Es findet nur auf einen begrenzten Kreis von Unternehmen Anwendung, der nicht immer leicht zu bestimmen ist (s. unter II. 1. a)). Diese Unternehmen unterliegen dann vergleichsweise strengen Cybersicherheitspflichten (s. unter II. 1. b)).

a) Anwendungsbereich

Das BSIG sieht Cybersicherheitspflichten für drei Kategorien von Unternehmen vor: Betreiber Kritischer Infrastrukturen (§ 8a BSIG), Anbieter digitaler Dienste (§ 8c BSIG) und Unternehmen im besonderen öffentlichen Interesse (sog. „UBI", § 8f BSIG).

aa) Betreiber Kritischer Infrastrukturen

Der gesetzlich definierte Begriff der Kritischen Infrastrukturen umfasst Einrichtungen oder Anlagen der folgenden Sektoren, die aufgrund der erheblichen Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit, die durch ihren Ausfall oder ihre Beeinträchtigung verursacht würden, für das Gemeinwesen von erheblicher Bedeutung sind (§ 2 Abs. 10 BSIG):

– Energie,
– Informationstechnik und Telekommunikation,
– Transport und Verkehr,
– Gesundheit,
– Wasser,
– Ernährung,
– Finanz- und Versicherungswesen, und
– Siedlungsabfallentsorgung.

Diese Voraussetzungen werden in der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSIG (sog. KRITIS-Verordnung) näher definiert (§ 2 Abs. 10 S. 2 BSIG), sowohl durch eine Operationalisierung der unbestimmten Rechtsbegriffe der Definition als auch durch eine Definition von Bemessungskriterien und Schwellenwerten zur Bestimmung der Kritikalität.

bb) Anbieter digitaler Dienste

Digitale Dienste sind als bestimmte Dienste der Informationsgesellschaft definiert, nämlich Online-Marktplätze, Online-Suchmaschinen und Cloud-Computing-Dienste, die nicht zum Schutz grundlegender staatlicher Funktionen eingerichtet worden sind oder für diese genutzt werden (§ 2 Abs. 11 BSIG).[13]

cc) Unternehmen im besonderen öffentlichen Interesse

Die Kategorie der UBI soll Unternehmen erfassen, die zwar keine Betreiber Kritischer Infrastrukturen sind, deren Informationssicherheit aber aus anderen Gründen von Bedeutung ist. Sie umfassen daher Unternehmen, die (i) Güter nach § 60 Abs. 1 Nr. 1, 3 Außenwirtschaftsverordnung („AWV") herstellen oder entwickeln, (ii) nach ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören und daher von erheblicher volkswirtschaftlicher Bedeutung sind, bzw. für ein solches Unternehmen als Zulieferer wegen ihrer Alleinstellungsmerkmale von wesentlicher Bedeutung sind, oder (iii) Betreiber eines Betriebsbereich der oberen Klasse der sog. Störfall-Verordnung („SVO") oder diesen gleichgestellt sind (§ 2 Abs. 14 BSIG).

Die erste Unterkategorie umfasst aufgrund des explizit dynamischen Verweises in § 2 Abs. 14 S. 1 Nr. 1 BSIG auf den kürzlich angepassten § 60 Abs. 1 Nr. 1, 3 AWV Unternehmen, die entweder Produkte mit IT-Sicherheitsfunktionen zur Verarbeitung staatlicher Verschlusssachen oder wesentliche Komponenten solcher Produkte herstellen oder u. U. hergestellt haben, oder Güter im Sinne des Teils I Abschnitt A der Ausfuhrliste – d. h. nicht nur Kriegswaffen als solche, sondern diverse Waffen, Munition und weiteres Rüstungsmaterial – entwickeln, herstellen, modifizieren oder besitzen. Es geht hier also primär um die öffentliche Sicherheit (daher im Folgenden „ÖffSi-UBI").

Die Methode zur Bestimmung der zweiten Unterkategorie, der volkswirtschaftlich bedeutsamen UBI (im Folgenden „VWi-UBI"), muss noch durch eine Rechtsverordnung bestimmt werden (§ 2 Abs. 14 S. 1 Nr. 2, S. 2 BSIG), die bislang nicht verabschiedet wurde.

Bei der dritten Unterkategorie von UBI hatte der Gesetzgeber die Gefahren von gesundheitsschädlichen Immissionen im Auge (daher im Folgenden „Immi-UBI"): Die obere Klasse der Störfall-Verordnung umfasst Betriebe, bei denen die in der Verordnung definierten gefährlichen Stoffe in Mengen oberhalb der ebenfalls in der Verordnung festgelegten Schwellenwerte vorhanden sind (§§ 1, 2 Nr. 2, 4 SVO). Die zuständige Behörde kann Betriebsbereiche unterhalb der Schwellenwerte der oberen Klasse im Hinblick auf drohende Störfälle gleichstellen (§ 1 Abs. 2 SVO).

11 Vgl. *Steger*, NIS-2-Richtlinie. Industrie veröffentlicht Erwartungen an die Politik, Tagesspiegel Background vom 22.2.2023, https://background.tagesspiegel.de/cybersecurity/industrie-veroeffentlicht-erwartungen-an-die-politik (Abruf: 27.3.2023).

12 Vgl. *Steger* (Fn. 11); vgl. auch *SPECTARIS – Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik*, PM vom 16.1.2023, https://www.spectaris.de/verband/aktuelles/detail/nis-2-richtlinie-cybersicherheitsanforderungen-an-unternehmen-muessen-verhaeltnismaessig-bleiben/ (Abruf: 27.3.2023).

13 Diese Art digitaler Dienste ist bei der Nutzung des Internets besonders relevant, wie auch die Regelung dieser Dienste im Digital Services Act zeigt, vgl. dort insb. Art. 11 ff., 29 ff., 33 ff.

b) Cybersicherheitspflichten

Die Cybersicherheitspflichten des BSIG sind nach den unterschiedlichen Kategorien von normunterworfenen Unternehmen gestaffelt.

aa) Cybersicherheitspflichten für Betreiber Kritischer Infrastrukturen

Betreiber Kritischer Infrastrukturen unterliegen den strengsten Cybersicherheitspflichten des BSIG, sofern es sich nicht um Kleinstunternehmen[14] handelt (vgl. § 8d Abs. 1 BSIG). Sie müssen unter Einhaltung des Stands der Technik „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse … treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind" (§ 8a Abs. 1 BSIG).

Am 1.5.2023 wird zudem die Pflicht des § 8a Abs. 1a BSIG „scharf geschaltet", als Teil der o. g. Maßnahmen „Systeme zur Angriffserkennung" einzusetzen. Diese sollen durch eine laufende Überwachung des Betriebs eine (automatische) Protokollierung und Detektion von sowie Reaktion auf Störungen ermöglichen.[15] Hierfür genügt jedoch nicht allein die Beschaffung einer bestimmten Software – Unternehmen müssen auch sicherstellen, dass die erforderlichen technischen, organisatorischen und personellen Rahmenbedingungen zu ihrem effektiven Einsatz gegeben sind, und die relevanten Systeme so konfiguriert sind, dass sie das Anforderungsprofil erfüllen.[16]

Verfahrensmäßig abgesichert wird die Einhaltung dieser Anforderungen durch eine Pflicht, diese Einhaltung alle zwei Jahre dem Bundesamt für Sicherheit in der Informationstechnik („BSI") nachzuweisen (§ 8a Abs. 3 BSIG). Allerdings kann das BSI die Einhaltung auch kontrollieren oder durch Dritte kontrollieren lassen – erfolgt eine solche Kontrolle auf Grund von konkreten Verdachtsmomenten, kann das BSI sogar Gebühren für ihre Durchführung erheben (§ 8a Abs. 4 BSIG).

Die Verletzung der Cybersicherheits- und Nachweispflichten ist bußgeldbewehrt (§ 14 Abs. 1, 2 Nr. 2, 3, 4, Abs. 3 BSIG). Das Bußgeld kann bis zu 1 Mio. Euro betragen (vgl. § 14 Abs. 5 S. 1 BSIG).

bb) Cybersicherheitspflichten für Anbieter digitaler Dienste

Für Anbieter digitaler Dienste, eine in Umsetzung der NIS1-Richtlinie geschaffene Kategorie, gelten ebenfalls Cybersicherheitspflichten, sofern es sich nicht um Kleinst- oder Kleinunternehmen[17] handelt (vgl. § 8d Abs. 4 BSIG). Sie müssen „geeignete und verhältnismäßige technische und organisatorische Maßnahmen … treffen, um Risiken für die Sicherheit der Netz- und Informationssysteme, die sie zur Bereitstellung der digitalen Dienste innerhalb der Europäischen Union nutzen, zu bewältigen" (§ 8c Abs. 1 S. 1 BSIG). Dazu gehören auch Maßnahmen, um Sicherheitsvorfällen vorzubeugen bzw. ihre Folgen zu begrenzen.[18]

Die relevanten Aspekte der o. g. Maßnahmen, etwa System- und Anlagensicherheit, Vorfallmanagement und Betriebskontinuität sind in § 8c Abs. 2 BSIG näher aufgeführt, allerdings ist das Umsetzungsgesetz hier nicht detaillierter als die NIS1-Richtlinie selbst (vgl. dort. Art. 14). Dafür hat die Europäische Kommission die notwendigen Maßnahmen in der Durchführungsverordnung (EU) 2018/151 der Kommission vom 30.1.2018 („NSI-DVO") näher beschrieben.

Darüber hinaus sind Anbieter digitaler Dienste verpflichtet, Sicherheitsvorfälle mit erheblichen Auswirkungen auf die Bereitstellung ihrer Dienste unverzüglich an das BSI zu melden, vorausgesetzt, sie können die Erheblichkeit einschätzen (§ 8c Abs. 3 S. 1, 3 BSIG). Die Erheblichkeit eines Vorfalls setzt gemäß Art. 4 NSI-DVO eine der folgenden Auswirkungen voraus: (i) einen Ausfall von 5 Mio. Nutzerstunden, (ii) eine Verletzung der Integrität, Authentizität oder Vertraulichkeit mit über 100 000 betroffenen Nutzern, (iii) eine öffentliche Gefahr, ein Risiko für die öffentliche Sicherheit oder den Verlust von Menschenleben, (iv) einen Sachschaden von über 1 Mio. Euro.

Auch für Anbieter digitaler Dienste kann die Verletzung ihrer Cybersicherheitspflichten ein Bußgeld nach sich ziehen, allerdings „nur" in einer Höhe bis zu 500 000 Euro (§ 14 Abs. 5 S. 2 BSIG).

cc) Cybersicherheitspflichten für Unternehmen im besonderen öffentlichen Interesse

Die Cybersicherheitspflichten für UBI sind verfahrensmäßig besonders ausgestaltet. Für ÖffSi- und VWi-UBI ist Ausgangspunkt die Verpflichtung, sich beim BSI zu registrieren und dabei die getroffenen IT-Sicherheitsmaßnahmen sowie entsprechende Zertifizierungen und Audits zu melden (§ 8f Abs. 1, 5 BSIG). Für ÖffSi-UBI greift diese Pflicht ab dem 1.5.2023, VWi-UBI haben hierfür noch Zeit, bis die Rechtsverordnung zu ihrer Bestimmung in Kraft getreten ist und zwei Jahre vergangen sind (§ 8f Abs. 4 S. 1 BSIG).[19] Für Immi-UBI ist die Registrierung freiwillig (§ 8f Abs. 4 S. 2 BSIG).

Nach verbindlicher Registrierung sind ÖffSi- und VWi-UBI außerdem verpflichtet, erhebliche Störungen unverzüglich an das BSI zu melden (§ 8f Abs. 7 BSIG). Für Immi-UB gilt diese Pflicht bereits seit dem 1.11.2021 (§ 8f Abs. 8 BSIG).

Auch UBI droht ein Bußgeld in Höhe von bis zu 500 000 Euro bei Verletzung ihrer Cybersicherheitspflichten (§ 14 Abs. 5 S. 2 BSIG).

2. Cybersicherheitspflichten unter der DS-GVO

Sowohl sog. Verantwortliche als auch sog. Auftragsverarbeiter und damit letztlich alle personenbezogene Daten verarbeitenden Unternehmen in Deutschland müssen gemäß Art. 32 Abs. 1 DS-GVO unter „Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen … ein dem Risiko angemessenes Schutzniveau … gewährleisten".

Cybersicherheit im Sinne der DS-GVO ist *Daten*sicherheit. Das Maß datenschutzrechtlich erforderlicher Cybersicherheitsmaßnahmen richtet sich damit vor allem nach dem Risiko für die betroffenen Personen, etwa aufgrund der Sensibilität der über die Personen verarbeiteten

14 Ein Kleinstunternehmen ist gemäß § 8d Abs. 1 BSIG i.V.m. Art. 2 Abs. 3 der Empfehlung 2003/361/EG der Europäischen Kommission vom 6.5.2003 ein Unternehmen, „das weniger als 10 Personen beschäftigt und dessen Jahresumsatz bzw. Jahresbilanz 2 Mio. EUR nicht überschreitet".

15 *Bundesamt für Sicherheit in der Informationstechnik*, Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung, Version 1.0, 26.9.2022, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-sza.html (Abruf: 27.3.2022).

16 *Bundesamt für Sicherheit in der Informationstechnik*, s. Fn. 15, S. 8.

17 Für die Schwelle, ab der ein Unternehmen nicht mehr als Kleinst- oder Kleinunternehmen, sondern (mindestens) als mittleres Unternehmen gilt, verweist das BISG (vgl. § 8d Abs. 1a, 4) – wie schon unter Fn. 14 erwähnt – auf Empfehlung 2003/361/EG. Nach deren Art. 2 Abs. 2 sind Klein- und Kleinstunternehmen nur solche, die weniger als 50 Personen beschäftigen und deren Jahresumsatz bzw. Jahresbilanz nicht höher ist als 10 Mio. Euro.

18 Die entsprechende Vorschrift des § 8c Abs. 1 S. 2 BSIG ist allerdings nicht unter den Bußgeldtatbeständen aufgeführt, vgl. § 14 BSIG.

19 Diese Regelung wird daher voraussichtlich durch die Umsetzung der NIS2-Richtlinie überholt, s. dazu noch unter Ziff. III.

Daten.[20] Es steht also der Schutz der Persönlichkeitsrechte der konkreten betroffenen Personen im Vordergrund,[21] einen Schutz öffentlicher Güter bzw. gesamtgesellschaftlicher Interessen leisten die datenschutzrechtlichen Cybersicherheitspflichten nur als Reflex. Dennoch werden über den allgemeinen Verweis auf die „Rechte und Freiheiten" natürlicher Personen eine Reihe an nicht im engeren Sinne datenschutzbezogenen Schutzgütern relevant – so kann etwa eine Datenpanne gemäß Art. 33 Abs. 1, 34 Abs. 1 DS-GVO meldepflichtig sein, wenn zwar nur persönlichkeitsrechtlich selten als sensibel zu bezeichnende personenbezogene Daten wie Namen und Geschlecht bekannt werden, dadurch aber finanzielle Schäden drohen.[22]

3. Cybersicherheitspflichten unter dem TTDSG

Nach § 19 Abs. 1 TTDSG sind Anbieter von Telemedien verpflichtet, „durch technische und organisatorische Vorkehrungen sicherzustellen, dass der Nutzer von Telemedien die Nutzung des Dienstes jederzeit beenden kann und er Telemedien gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann". Soweit technisch möglich und wirtschaftlich zumutbar, muss er zudem unerlaubte Zugriffe auf die genutzten technischen Einrichtungen verhindern und sie gegen Störungen sichern (§ 19 Abs. 4 S. 1–3 TTDSG).

Bereits eine Website stellt ein sog. Telemedium dar.[23] Da Websites/Homepages als digitaler Öffentlichkeitsauftritt beinahe allgegenwärtig sind, treffen diese Pflichten folglich beinahe jedes Unternehmen.

Gerade im Vergleich mit den oben unter Ziff. II. 1. b) beschriebenen Cybersicherheitspflichten sind die Pflichten des § 19 Abs. 1, 4 S. 1 TTDSG allerdings erkennbar niedrigschwellig. Insbesondere ist – wohlgemerkt nur bei Maßnahmen nach Abs. 4 – der Stand der Technik zwar zu berücksichtigen (§ 19 Abs. 4 S. 2 TTDSG; indes nicht notwendigerweise „einzuhalten", vgl. § 8a Abs. 1 S. 2 BSIG), Maßnahmen müssen allerdings wirtschaftlich zumutbar sein. Grundlegende Maßnahmen wie die Nutzung von HTTPS und SSL-Verschlüsselung, allgemein übliche Security Header und eine regelmäßig aktualisierte Firewall dürften zur Wahrung der Anforderungen des § 19 Abs. 1, 4 TTDSG auf Unternehmenswebsites grundsätzlich genügen,[24] zumal ein Websitenutzer den Besuch der Website selbstverständlich jederzeit selbst beenden kann.

4. Cybersicherheitspflichten in besonderen Bereichen und im Produktsicherheitsrecht

Trotz ihrer gesellschaftlichen Bedeutung sind einige Bereiche von der Anwendung der Cybersicherheitspflichten des BSIG ausgenommen, da insoweit bereits spezialgesetzliche Cybersicherheitspflichten gelten. Dies gilt insbesondere für die Bereiche Telekommunikation (vgl. §§ 168 ff. Telekommunikationsgesetz), Energieversorgung (§ 11 Energiewirtschaftsgesetz), Atomkraft (§§ 7, 41 ff. Atomgesetz) und Telematik (§§ 323 ff. Fünftes Buch Sozialgesetzbuch). Auch in diesen Bereichen ist das Bundesamt für Sicherheit in der Informationstechnik eng in die Bestimmung und Überwachung des erforderlichen Cybersicherheitsstandards eingebunden (vgl. § 168 Abs. 7 TKG; § 11 Abs. 1d EnWG; § 44b AtG; § 323 Abs. 5 SGB V).

Darüber hinaus enthält das Produktsicherheitsrecht Cybersicherheitspflichten, etwa im Bereich Funkanlagen (vgl. Art. 3 Abs. 3 der sog. Funkanlagenrichtlinie (EU) 2014/53/EU i.V.m. der Delegierten Verordnung (EU) 2022/30) oder Kraftfahrzeuge.[25]

Eine detaillierte Darstellung der jeweiligen spezialgesetzlichen Cybersicherheitspflichten geht jedoch über den Zweck dieses Beitrags hinaus.

III. Cybersicherheitsreform durch die NIS2-Richtlinie

Die NIS2-Richtlinie überholt den Anwendungsbereich der Cybersicherheitspflichten und erweitert ihn dadurch erheblich (s. unter Ziff. III. 1.). Die eigentlichen Cybersicherheitspflichten sind umfassend, aber vergleichsweise abstrakt (s. unter Ziff. III. 2.). Verstöße gegen Cybersicherheitspflichten werden streng sanktioniert (s. unter Ziff. III. 3.).

1. Erweiterung des Anwendungsbereichs

Die NIS2-Richtlinie teilt Unternehmen, die aufgrund ihrer Bedeutung Cybersicherheitspflichten unterworfen werden, in die zwei Kategorien der „wesentlichen" und „wichtigen" Einrichtungen auf (vgl. Art. 3 NIS2). Die Kategorie der Anbieter digitaler Dienste wird aufgegeben.

Unter die „wesentlichen" Einrichtungen fallen nach der NIS2-Richtlinie neben Vertrauensdiensteanbietern, bestimmten Telekommunikationsanbietern, öffentlichen Einrichtungen und bislang schon als kritisch eingestuften Einrichtungen alle mindestens mittelgroßen[26] Unternehmen folgender Sektoren (s. Art. 3 Abs. 1 und Anhang I NIS2), neu hinzugekommene Sektoren sind *kursiv gedruckt*):

- Energie,
- Verkehr,
- Bankwesen,
- Finanzmarktinfrastruktur,
- Gesundheitswesen,
- Trinkwasser,
- Abwasser,
- Digitale Infrastruktur,
- *Verwaltung von Diensten der Informations- und Kommunikationstechnologie (Business-to-Business),*
- *Öffentliche Verwaltung,*
- *Weltraum.*

Schon hierdurch wird der Anwendungsbereich des europäischen Cybersicherheitsrechts folglich erweitert. Noch deutlich weiter geht die Ausdehnung des Anwendungsbereichs allerdings durch die Sektoren der „wichtigen" Einrichtungen (s. Art. 3 und Anhang II NIS2):

- Post- und Kurierdienste,
- Abfallbewirtschaftung,
- Produktion, Herstellung und Handel mit chemischen Stoffen,
- Produktion, Verarbeitung und Vertrieb von Lebensmitteln,
- Verarbeitendes Gewerbe/Herstellung von Waren,
- Anbieter digitaler Dienste,
- Forschung.

Von besonderer Bedeutung ist der Sektor Verarbeitendes Gewerbe/Herstellung von Waren (sog. *Manufacturing*). Selbst unter Berücksichtigung der Ausnahme für Klein- und Kleinstunternehmen[27] wer-

20 *Paulus*, in: Wolff/Brink, BeckOK Datenschutzrecht, 42. Edition, DSGVO Art. 32, Rn. 10.
21 *Piltz*, in: Gola/Heckmann (Hrsg.), Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 32, Rn. 41, 44; *Jandt*, in: Kühling/Buchner (Hrsg.), DS-GVO BDSG, 3. Aufl. 2020, Art. 32, Rn. 31; vgl. außerdem die Ableitung des Datensicherheitsgebots aus dem Grundrecht auf Datenschutz gemäß Art. 8 der Grundrechtecharta, *Piltz*, ebd., Art. 32, Rn. 5 f.
22 Vgl. Erwägungsgrund 85 zur DS-GVO.
23 *Micklitz/Schirmbacher*, in: Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl. 2019, TMG § 5, Rn. 7.
24 Vgl. *Schneider*, in: Assion, TTDSG, 2022, § 19, Rn. 18 ff.: „erheblicher Einschätzungsspielraum".
25 Speziell zu Kraftfahrzeugen ausführlich *Seufert*, CR 2023, 73.
26 Art. 2 Abs. 1 NIS2 verweist ebenso wie das BSIG für die Bestimmung der Schwellenwerte auf die Empfehlung 2003/361/EG, s. daher Fn. 17.
27 S. Fn. 17.

den sich hierdurch viele Unternehmen erstmals umfassend mit Cybersicherheitscompliance auseinandersetzen müssen.

Die Erweiterung der Sektoren ergibt sich vor allem daraus, dass künftig eine Unterscheidung zwischen wesentlichen und wichtigen Einrichtungen vorgenommen wird. Beide Einrichtungstypen werden in der Richtlinie auch so konkretisiert, dass abzusehen ist, dass eine deutlich größere Anzahl an Unternehmen unter den Begriff der wesentlichen oder wichtigen Einrichtung fallen werden.

Für ohnehin schon cybersicherheitsrechtlich regulierte Sektoren sieht Art. 4 NIS2-Richtlinie vor, dass neben gleichwertigen sektorspezifischen Regelungen nicht auch noch die Regelungen der NIS2-Richtlinie gelten. Bis zur Verabschiedung der in Art. 4 Abs. 3 NIS2-Richtlinie vorgesehenen Leitlinien der Europäischem Kommission zur Klärung dieses Verhältnisses besteht erhebliche Rechtsunsicherheit, mit einiger Wahrscheinlichkeit werden sich aber Unternehmen des Finanzsektors hierauf berufen können.[28]

2. Neue Cybersicherheitspflichten

Im Vergleich zur NIS1-Richtlinie sieht die NIS2-Richtlinie einen deutlich umfassenderen Katalog von Cybersicherheitssicherheitspflichten vor.[29] Gemäß Art. 21 Abs. 1 NIS2-Richtlinie müssen wesentliche und wichtige 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". Dabei sind der Stand der Technik, EU- und internationale Normen sowie die Umsetzungskosten zu berücksichtigen, letztlich müssen die Maßnahmen aber dem Risiko angemessen sein (Art. 2 Abs. 1 S. 2 NIS2). Die NIS2-Richtlinie schreibt einen holistischen Ansatz zur Gefahrenabwehr vor, der mindestens Folgendes umfasst (Art. 21 Abs. 2 NIS2, dessen offizielle deutsche Übersetzung etwas misslungen ist):

- Risikoanalyse- und Informationssicherheitskonzepte, einschließlich Berechtigungskonzepte und Verfahren zur Bewertung der Wirksamkeit des Risikomanagements;
- Sicherheitsvorfall-Management;
- Betriebskontinuitätsmanagement einschließlich Backups und Notfallpläne;
- Sicherheitsmanagement des eigenen Personals (einschließlich Cybersicherheitsvorgaben und -trainings), der Lieferkette, insbes. bei Lieferanten/Dienstleistern;
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung;
- Kryptografie und gegebenenfalls Verschlüsselung;
- Authentifizierungsverfahren und gesicherte Kommunikationskanäle.

Verschärft wird insbesondere die Pflicht zur Meldung von – erheblichen – Sicherheitsvorfällen. Anders als bei den Sicherheitsmaßnahmen beschränkt sich die NIS2-Richtlinie hier nicht auf einen Beispielskatalog, sondern gibt eine konkrete Abfolge von bestimmten Meldungen vor (Art. 23 Abs. 1, 3 NIS2):

1. Zuerst müssen die wesentlichen und wichtigen Einrichtungen jeden erheblichen Sicherheitsvorfall unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnisnahme, dem Computer-Notfallteam (eng. *Computer Security Incident Response Team* oder „CSIRT") oder den zuständigen Behörden[30] melden (sog. Frühwarnung). Diese Frühwarnung soll bereits mitteilen, ob der Verdacht besteht, dass der Sicherheitsvorfall rechtswidrig oder böswillig herbeigeführt wurde oder grenzüberschreitende Auswirkungen haben könnte.
2. Ebenfalls unverzüglich und jedenfalls innerhalb von 72 Stunden muss die Frühwarnung aktualisiert werden (sog. Meldung). Die Meldung muss eine erste Bewertung der Schwere und Auswirkungen des Sicherheitsvorfalls und der Hinweise auf eine Kompromittierung der Sicherheit enthalten.
3. Auf Nachfrage des CSIRT oder der zuständigen Behörde ist zudem ein Zwischenbericht über relevante Status-Updates abzugeben. Innerhalb eines Monats nach der Meldung muss ein Abschlussbericht eingereicht werden. Der Abschlussbericht muss den Sicherheitsvorfall ausführlich beschreiben, insbesondere seine Schwere, (grenzüberschreitende) Auswirkungen, Art und Ursachen. Ebenfalls im Abschlussbericht zu beschreiben sind etwaige Abhilfemaßnahmen.
4. Schließlich sind selbst nach dem Abschlussbericht noch weitere Folgeberichte und ein Monat nach Abschluss der Gegenmaßnahmen ein weiterer Abschlussbericht verpflichtend. Dieser muss eine ausführliche Beschreibung des Sicherheitsvorfalls, Angaben zu der Art der Bedrohung bzw. der zugrundeliegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat, Angaben zu den getroffenen und laufenden Abhilfemaßnahmen und gegebenenfalls zu den grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls enthalten.[31]

Im Übrigen muss es wesentlichen und wichtigen Einrichtungen auch ermöglicht werden, Sicherheitsvorfälle, Cyberbedrohungen und Beinahe-Vorfälle *freiwillig* dem CSIRT oder der zuständigen Behörde zu melden (Art. 30 Abs. 1 lit. a NSI2). Für Unternehmen außerhalb des Anwendungsbereichs gilt das ebenfalls mit der Einschränkung, dass etwaige Sicherheitsvorfälle erheblich sein müssen (Art. 30 Abs. 1 lit. b NIS2). Eine freiwillige Meldung darf (ausgenommen im Bereich der Verhinderung und Verfolgung von Straftaten) nicht zu zusätzlichen Pflichten für das freiwillig meldende Unternehmen führen (Art. 30 Abs. 2 S. 3 NIS2).

Insgesamt sind die Aufsichtsbefugnisse umfassender als bislang in den §§ 8a ff. BSIG geregelt (vgl. Art. 31 ff. NIS2). Insbesondere konkrete Betretungs- und Kontrollrechte hat das BSI bislang nur im Hinblick auf die Kommunikationstechnik des Bundes (vgl. § 4a Abs. 1–3 BSIG) und gegenüber den Betreibern kritischer Infrastrukturen (§ 8a Abs. 4 BSIG).

Aufgrund der Pflicht der Mitgliedstaaten, eine aktuelle Liste wesentlicher und wichtiger Einrichtungen (sowie Einrichtungen, die Domänennamen-Registrierungsdienste erbringen) zu unterhalten (vgl. Art. 3 Abs. 3, 4 NIS2-Richtlinie), werden sich diese Einrichtungen in Zukunft bei der zuständigen Behörde registrieren müssen (ähnlich bislang für UBI in § 8f BISG geregelt).[32]

28 *Voigt/Bastians*, CR 2022, 768, 773 f.

29 Darüber hinaus enthält die NIS2-Richtlinie auch zahlreiche Regeln zur institutionellen Stärkung der Aufsichtsbehörden und ihrer grenzüberschreitenden Kooperation (vgl. hierzu *Kopker u. a.*, MMR 2021, 214, 215, 217). Da sich hieraus aber keine unmittelbaren Pflichten für Unternehmen ergeben, wird in diesem Beitrag darauf nicht weiter eingegangen.

30 Jeder Mitgliedstaat ist nach Art. 8 Abs. 1 NSI2 verpflichtet, eine zuständige Behörde für Cybersicherheit und die in der Richtlinie vorgesehenen Aufsichtsaufgaben zu benennen bzw. einzurichten. Nach Art. 10 Abs. 1 NIS2 müssen sie außerdem ein oder mehrere CSIRTs einrichten, entweder innerhalb oder außerhalb der zuständigen Behörde.

31 Damit sind die NIS2-Richtlinie jedenfalls aus operativer Sicht komplexer als die Meldepflichten für Verletzungen des Schutzes personenbezogener Daten (sog. Datenpannen) gemäß Art. 33 f. DS-GVO.

32 Für folgende Unternehmen erstellt und führt zudem die *European Union Agency for Cybersecurity* (ursprünglich *European Network and Information Security Agency* – „ENISA") ein Register: 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 Netz-

3. Sanktionen

Wie zahlreiche andere Rechtsakte der europäischen Digitalstrategie (vgl. Art. 83 DS-GVO, Art. 52 *Digital Services Act*) sieht auch die NIS2-Richtlinie strenge Bußgeldtatbestände für Pflichtverletzungen vor: Wesentlichen Einrichtungen drohen Bußgelder bis zu 10 Mio. Euro oder 2 % des weltweiten Jahresumsatzes, wichtigen Einrichtungen „lediglich" Bußgelder bis zu 7 Mio. Euro oder 1,4 % des weltweiten Jahresumsatzes (Art. 34 Abs. 4, 5 NIS2).

Einen besonderen Akzent setzt zudem Art. 20 Abs. 1 NIS2, wonach die Mitgliedstaaten sicherstellen müssen, dass die Leitungsorgane von Unternehmen, die über die Maßnahmen zur Einhaltung der Cybersicherheitspflichte gemäß Art. 21 NIS2 entscheiden, direkt haftbar gemacht werden können (vgl. außerdem Art. 32 Abs. 6, 33 Abs. 5 NIS2). Anders als etwa bei der DS-GVO, bei der bei Fehlentscheidungen des Managements grundsätzlich nur das Unternehmen haftet, wird im Zusammenhang mit Cybersicherheitspflichten also auch eine persönliche Haftung in Frage kommen. Einen konkreten Sorgfaltsstandard legt die NIS2-Richtlinie jedoch nicht fest, sodass es hier im besonderen Maße auf die konkrete nationale Umsetzungsgesetzgebung ankommen wird.

IV. Weitere Cybersicherheitsgesetzgebung

Komplementiert wird die NIS2-Richtlinie durch die Richtlinie (EU) 2022/2557 über die Resilienz kritischer Einrichtung (*Critical Entities Resilience*- oder „CER-Richtlinie" bzw. „CER"), die wie die NIS2-Richtlinie bis zum 17.10.2024 in nationales Recht umzusetzen ist. Der Fokus der CER-Richtlinie liegt darauf, die Regeln zur Bestimmung kritischer Einrichtungen zu vereinheitlichen und die behördliche Aufsicht über sie zu verbessern, um so die Widerstandsfähigkeit der kritischen Einrichtungen gegen diverse Gefahren zu verbessern. Dabei geht es gerade nicht nur um „digitale", sondern auch um „analoge" Gefahren wie Naturkatastrophen, terroristische Anschläge oder Sabotage, und entsprechend auch „analoge" Gegenmaßnahmen – Cybersicherheit ist daher nur inzident berührt.

Kritische Einrichtungen im Anwendungsbereich der CER-Richtlinie müssen insbesondere eine Risikobewertung durchführen (Art. 12 CER), auf dieser Grundlage geeignete und verhältnismäßige Resilienzmaßnahmen ergreifen (Art. 13 CER) und erhebliche Sicherheitsvorfälle melden (Art. 15 CER). Allerdings ist der Anwendungsbereich auf folgende Sektoren beschränkt:

– Energie,
– Verkehr,
– Bankwesen,
– Finanzmarktinfrastruktur,
– Gesundheitswesen,
– Trinkwasser,
– Abwasser,
– Digitale Infrastruktur,
– Öffentliche Verwaltung,
– Weltraum,
– Produktion, Verarbeitung und Vertrieb von Lebensmitteln.

Die CER-Richtlinie regelt folglich auch die Bestimmung kritischer Einrichtungen aus den Sektoren Banken, Finanzmarktinfrastruktur und digitale Infrastruktur – diese sind allerdings explizit vom Anwendungsbereich der inhaltlichen Resilienzpflichten (insbes. Kapitel III CER) ausgenommen (Art. 8 CER), da für sie wiederum spezielle Vorschriften gelten. Für den Finanzbereich ist das die Verordnung (EU) 2022/2554 (*Digital Operational Resilience Act*, „DORA"),[33] für den Bereich digitale Infrastruktur die oben beschriebene NIS2-Richtlinie (vgl. Erwägungsgrund 20 f. CER).

Auf der Ebene des Produktsicherheitsrechts ziehen die Cybersicherheitsanforderungen zukünftig voraussichtlich ebenfalls an, insbesondere durch den *Artificial Intelligence Act,*[34] den *Data Act* sowie den sog. *Cyber Resilience Act.*[35]

V. Zusammenfassung und Ausblick

Der erweiterte Anwendungsbereich der Cybersicherheitspflichten nach der NIS2-Richtlinie führt dazu, dass eine Reihe von Unternehmen, insbesondere aus dem verarbeitenden oder herstellenden Gewerbe, zum ersten Mal einem umfassenden Cybersicherheitsregime unterworfen werden. Sie müssen ihre Prozesse und Vorkehrungen zur Cybersicherheit entsprechend anpassen, um aufsichtsbehördliche Maßnahmen wie etwa hohe Bußgelder zu vermeiden. Die direkte Haftung der Geschäftsleitung hat hier eine zusätzliche Anreizfunktion.

Auch Unternehmen, die bereits im Hinblick auf die DS-GVO Konzepte zum Umgang mit Cybersicherheit entwickelt haben, werden diese im Hinblick auf die Anforderungen der NIS2-Richtlinie überarbeiten müssen. Zum einen sind nun nicht mehr nur personenbezogene Daten zu schützen, sondern auch reine Sachdaten sowie – unabhängig von den verarbeiteten Daten – die Informations- und Kommunikationssysteme, die zur Aufrechterhaltung des Geschäftsbetriebs erforderlich sind. Die veränderte Risikobetrachtung wird regelmäßig auch zu einem veränderten Katalog verpflichtender Maßnahmen führen. Zum anderen legt sich neben die Anforderungen zur Meldung von Verletzungen des Schutzes personenbezogener Daten (in Unternehmen oft in sog. *Data Security Incident Policies* oder Datenpannenmelderichtlinien geregelt) die detailliert durchstrukturierte Meldepflicht der NIS2-Richtlinie im Hinblick auf erhebliche Sicherheitsvorfälle.

Die Europäische Kommission schätzt, dass Unternehmen, die durch die Erweiterung des Anwendungsbereichs der Cybersicherheitspflichten erstmalig unter die NIS2-Richtline fallen, ihr Budget für Cybersicherheitsmaßnahmen um 22 % steigern müssen. Für Unternehmen, die bereits der NIS1-Richtlinie unterfielen, schätzt sie eine Budgetsteigerung von 12 %.[36] Sie erwartet jedoch, dass sich diese Investitionen über das nächste Jahrzehnt amortisieren, insbesondere durch eine Verhinderung ebenfalls kostspieliger[37] oder sogar existenzvernichtender[38] Cybersicherheitsvorfälle.

werke. Um dies zu ermöglichen, sollen diese Unternehmen verpflichtet werden, den zuständigen Behörden bestimmte Kontaktdaten zu übermitteln (vgl. Art. 27 NIS2).

33 Einen ersten Überblick geben *Voigt/Ritter-Döring*, CR 2023, 82.

34 Zum *Artificial Intelligence Act* ausführlich *Ruttloff/Wagner/Schulz-Kunth*, BB 2022, 2499.

35 S. den Vorschlag der Europäischen Kommission vom 15.9.2022 für eine Verordnung für horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Komponenten, COM(2022) 454 final, https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act (Abruf: 27.2.2023); vgl. eine Übersicht bei *Zirnstein*, CR 2022, 707; zur Interaktion mit der NIS2-Richtlinie *Voigt/Bastians*, CR 2022, 768, 774.

36 *European Commission* (Fn. 3).

37 Im Jahr 2022 schätzte der Branchenverband bitkom den volkswirtschaftlichen Schaden auf 203 Mrd. Euro, s. PM vom 31.8.2022, https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022 (Abruf: 27.3.2023).

38 *Knop*, Fahrradbauer Prophete: Erste Details zum Cyber-Angriff, auf heise online, https://www.heise.de/news/Fahrradbauer-Prophete-Erste-Details-zum-Cyber-Angriff-7457031.html (Abruf: 27.3.2023).

Für Unternehmen, die in der EU bzw. in Deutschland niedergelassen sind oder ihre Dienste dort erbringen, hängt indes noch viel davon ab, wie der deutsche Gesetzgeber die NIS2-Richtlinie und die anderen cybersicherheitsrelevanten EU-Richtlinien umsetzt und mit dem nach den entsprechenden Verordnungen verbleibenden Entscheidungsspielraum umgeht. Industrie- und Verbraucherschutzverbände sind sich einig, dass eine Bündelung der Zuständigkeiten der unter den verschiedenen Rechtsakten vorgesehenen Aufsichtsbehörden oder jedenfalls eine Zentralisierung der Melde- und Kontaktstellen für Unternehmen und Bürger sinnvoll wäre.[39]

Die Umsetzungsfrist ist jedenfalls nicht nur für den Gesetzgeber, sondern auch für die zukünftig verpflichteten Unternehmen knapp bemessen – die Einführung oder Überarbeitung eines ganzheitlichen Cybersicherheitssystems ist insbesondere angesichts der beschriebenen regulatorischen Komplexität eine enorme Aufgabe. Auch wenn die Einzelheiten der Datensicherheitspflichten sich erst durch die Umsetzungsgesetzgebung klären werden, sollten Unternehmen daher jetzt schon prüfen, ob bzw. inwieweit sie dem neuen NIS2-Cybersicherheitsregime unterfallen werden, und mit den Vorbereitungen für etwaig erforderliche Anpassungen beginnen.

Simon Clemens Wegmann ist Rechtsanwalt bei der Kanzlei Gleiss Lutz am Standort Berlin. Er berät nationale und internationale Mandanten insbesondere aus den USA und Asien im deutschen und europäischen Datenschutzrecht und bei anderen Aspekten der öffentlich-rechtlichen Datenregulierung.

39 *Steger* (Fn. 11), *Rudl*, Umsetzung des Digital Services Act – Mehr Schlagkraft, weniger Kompetenzgerangel, https://netzpolitik.org/2022/umsetzung-des-digital-services-act-mehr-schlagkraft-weniger-kompetenzgerangel/ (Abruf: 27.3.2023).

Robin Kienitz, RA, und Prof. Dr. Hervé Edelmann, RA

Der Sicherungseigentümer als Zustandsstörer i.S.v. § 1004 Abs. 1 S. 1 BGB

Das vom Reichsgericht entwickelte und seither anerkannte Sicherungseigentum ist aus dem heutigen Wirtschaftsleben nicht mehr wegzudenken. Der fiduziarische Charakter und die damit verbundene Sonderform des Sicherungseigentums erlangt u. a. im Rahmen des negatorischen Beseitigungsanspruchs gem. § 1004 Abs. 1 S. 1 BGB Bedeutung. In der bankrechtlichen Praxis kann sich das Problem stellen, dass der vermietende Grundstückseigentümer gegenüber dem lediglich mittelbar besitzenden Sicherungseigentümer – meist der kreditgewährenden Bank – die Beseitigung des Sicherungsgutes verlangt, dies deshalb, weil beispielsweise der Mieter nach Kündigung des Mietverhältnisses entweder nicht gewillt oder nicht in der Lage ist, das Sicherungsgut aus dem Mietobjekt zu entfernen. Dann stellt sich die Frage, ob der mittelbar besitzende Sicherungseigentümer ohne Weiteres als Störer i. S. v. § 1004 Abs. 1 S. 1 BGB angesehen werden kann, mit der Folge, dass er dann gegenüber dem Vermieter hieraus zur Beseitigung der Sicherungsgegenstände verpflichtet wäre.

I. Einleitung

Das vom Reichsgericht[1] praeter legem entwickelte und seither in Rechtsprechung und Literatur anerkannte Sicherungseigentum ist aus dem heutigen Wirtschaftsleben nicht mehr wegzudenken. Im Gegensatz zum Faustpfand gemäß §§ 1204 ff. BGB bietet es dem Sicherungsgeber die Möglichkeit, den unmittelbaren Besitz am Sicherungsgut zu behalten und so die Betriebsmittel weiterhin zur Gewinnerzielung zu nutzen. Denn die betriebliche Nutzung des Sicherungsgutes bildet in vielen Fällen erst die Grundlage, ein durch die Sicherungsübereignung besichertes Darlehen zurückzuführen. Das Sicherungseigentum entspricht daher dem Verkehrsbedürfnis und hat so das Faustpfand bei der Sicherung von Geldkrediten weitgehend ersetzt.[2]

Wesensprägend für das Sicherungseigentum ist die aus der Sicherungsabrede folgende funktionale Aufteilung der Eigentumsfunktionen und der damit verbundene fiduziarische Charakter des Sicherungseigentums.[3] Dem Sicherungseigentümer steht aufgrund der getroffenen Sicherungsabrede regelmäßig nur die Sicherungsfunktion des Eigentums zu, der Sicherungsgeber hingegen behält die Nutzungsfunktion und übt unter Beachtung der treuhänderischen Bindung die tatsächliche Sachherrschaft aus.[4] So wird dem Sicherungseigentümer regelmäßig nur ein Verwertungsrecht an der Sache für den Fall des Eintritts der Verwertungsreife eingeräumt. Dem Sicherungsnehmer ist es aufgrund seiner ihn treffenden Treuepflichten gegenüber dem Sicherungsgeber in der Regel untersagt, ohne Eintritt der Verwertungsreife die Sicherungsgegenstände an sich zu nehmen oder deren Herausgabe vom Sicherungsgeber zu verlangen.

Der fiduziarische Charakter und die damit verbundene Sonderform[5] des Sicherungseigentums erlangt unter anderem im Rahmen des negatorischen Beseitigungsanspruchs gemäß § 1004 Abs. 1 S. 1 BGB Bedeutung. Mitunter kann sich in der bankrechtlichen Praxis das Problem stellen, dass der vermietende Grundstückseigentümer gegenüber dem lediglich mittelbar besitzenden Sicherungseigentümer – meist der kreditgewährenden Bank – die Beseitigung des Sicherungsgutes verlangt, dies deshalb, weil beispielsweise der Mieter nach Kündigung

1 RG, 8.11.1881 – III 48/81, RGZ 5, 181, 184; RG, 10.1.1885 – I 431/84, RGZ 13, 200, 201.
2 *Oechsler*, in: MünchKomm. BGB, 8. Aufl. 2020, Anh. §§ 929–936, Rn. 2.
3 *Oechsler*, in: MünchKomm. BGB, 8. Aufl. 2020, Anh. §§ 929–936, Rn. 1.
4 Vgl. *Larenz/Canaris*, Lehrbuch des Schuldrechts, Bd. II/2, 13. Aufl. 1994, § 86 III, S. 690.
5 *Wiegand*, in: Staudinger, Kommentar zum BGB, Neubearbeitung 2017, Anh. zu §§ 929 ff., Rn. 211, *Oechsler*, in: MünchKomm. BGB, 8. Aufl. 2020, Anh. §§ 929–936, Rn. 1.