Kommunikation & Recht

K&R

5 | Mai 2024
27. Jahrgang
Seiten 301 - 372

dfv Mediengruppe
Frankfurt am Main

schäftsmodellen ausgenutzt wird, hatte die BNetzA bereits 2017 eine Ansagepflicht für Anrufe zu bestimmten ausländischen Destinationen angeordnet, um Anrufer darauf hinzuweisen, dass es sich um einen Anruf zu einer ausländischen Rufnummer handelt. Die bisherige Verpflichtung zu einer Ansage lief zum 1. 3. 2024 aus und wurde von der BNetzA nun verlängert.

Die BNetzA hat eine vorläufige Bedarfsermittlung für den Vermittlungsdienst für gehörlose und hörgeschädigte Endnutzer gemäß § 51 Abs. 4 S. 2 i. V. m. § 207 TKG durchgeführt.[93] Diese Bedarfsermittlung gilt für das Jahr 2024. Hierin ist eine Versorgung rund um die Uhr mit Gebärden- und Schriftdolmetschern erfasst sowie im privaten Bereich eine kostenlose Grundversorgung für Nutzer des Dienstes von 30 Minuten monatlich. Aktuell führt die BNetzA eine Anhörung zum Entwurf einer Bedarfsermittlung für die Jahre 2025 bis 2028 durch.[94] Inhaltlich neu ist in dem Entwurf eine schrittweise Ausweitung der kostenfreien Nutzung des Vermittlungsdienstes. Derzeit kann jeder Endnutzer den Vermittlungsdienst monatlich 30 Minuten kostenfrei nutzen. Dies ist auch für das Jahr 2025 vorgesehen. Im Jahr 2026 sollen dann monatlich 40 Minuten, im Jahr 2027 monatlich 50 Minuten und im Jahr 2028 monatlich 60 Minuten pro Endnutzer kostenfrei sein.

Erstmals haben Endnutzer im neuen TKG nach § 156 Abs. 1 TKG einen Anspruch auf Versorgung mit TK-Diensten, die auch Breitbandinternet umfassen. In der TK-Mindestversorgungsverordnung (TKMV) legt die BNetzA die Parameter eines Breitbandanschlusses fest, auf dessen Verfügbarkeit ein Endnutzer Anspruch hat. Dieser Anschluss muss zudem noch zu einem erschwinglichen Preis angeboten werden.[95] Die Unterversorgung nach § 160 Abs. 1 TKG hat die BNetzA nunmehr für einige Gegenden festgestellt.[96] Wesentlich ist, dass die BNetzA entsprechend der Formulierung von § 156 Abs. 1 TKG die Geschwindigkeitsverfügbarkeit eines Anschlusses „an" der Hauptwohnung eines betroffenen Endnutzers misst und nicht „in" der Wohnung. Damit fallen Geschwindigkeitseinbußen durch Inhouse-Verkabelung und Gebäudeabschirmung bei Mobilfunk nicht in die Betrachtung ein.[97] Das Recht auf Versorgung mit schnellem Internet war auch Gegenstand einer kleinen Anfrage im Bundestag.[98]

Im März 2024 hat die BNetzA erstmals einen Anbieter nach § 160 Abs. 2 TKG verpflichtet, einen Haushalt in Niedersachsen gem. § 156 Abs. 1 TKG mit TK-Diensten im Umfang von § 157 Abs. 2 TKG zu versorgen.[99] Zwar sind am Wohnsitz des betroffenen Endnutzers TK-Dienste verfügbar, die die Bandbreiten- und Latenzanforderungen von § 2 TKMV erfüllen. Die Preise dieser Dienste entsprechen jedoch nicht den Vorgaben der Erschwinglichkeit nach § 158 Abs. 2 TKG.[100]

Dr. Thomas Sassenberg
ist als Rechtsanwalt und Fachanwalt für Medien- und Urheberrecht in Frankfurt a. M. tätig. Er berät und vertritt Unternehmen in den Bereichen des IT- und TK-Rechts.

Dr. Reto Mantz
ist nach einer Tätigkeit als Rechtsanwalt im Bereich des gewerblichen Rechtsschutzes und Patentrechts seit 2012 Richter am LG Frankfurt a. M.

Dr. Gerd Kiparski
ist General Counsel der 1&1 AG, Montabaur; Vorstandsmitglied der DGRI und Co-Vorsitzender des Fachausschusses Telekommunikation und IT-Sicherheit sowie Vorsitzender des Arbeitskreises Wettbewerbs- und Verbraucherrecht des BITKOM.

93 BNetzA, Vfg. Nr. 111/2023, ABl. 19/2023 v. 11. 10. 2023.
94 Der Entwurf ist abrufbar unter: https://www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/Unternehmenspflichten/Vermittlungsdienstfuer Gehoerlose/BedarfsfeststellungEntwurf.pdf?__blob=publicationFile&v=3.
95 Grundsätze über die Ermittlung erschwinglicher Preise für Telekommunikationsdienste hat die BNetzA ebenfalls veröffentlicht: https://www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/Grundversorgung/GrundsaetzeErschwinglichkeit.pdf?__blob=publicationFile&v=4.
96 Siehe BNetzA, Vfg. Nr. 9/2024 – 24/2024, ABl. 2/2024 v. 24. 1. 2024.
97 Siehe BNetzA, Vorgangsnummer 2022-06-13-0002.
98 BT-Drs. 20/8044.
99 https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2024/20240311_VerpflichtungTK.html.
100 Die Erschwinglichkeit hat die BNetzA ausdefiniert: https://www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/Grundversorgung/GrundsaetzeErschwinglichkeit.pdf?__blob=publicationFile.

RA Alexander Weidenhammer*

Die Meldepflicht – insbesondere nach § 168 TKG – als Instrument des IT-Sicherheitsrechts

Kurz und Knapp

Mit der voranschreitenden Regulierung des IT-Sicherheits- bzw. Cybersicherheitsrechts werden immer neue Meldepflichten bei Sicherheitsvorfällen (und Datenschutzverletzungen) in bestimmten Bereichen und Sektoren eingeführt. Hierdurch entstehen zugleich zahlreiche rechtliche Fragestellungen. Dies gilt gleichwohl für den Telekommunikationssektor.

* Mehr über den Autor erfahren Sie am Ende des Beitrags. Alle zitierten Internetquellen wurden zuletzt abgerufen am 11. 4. 2024.

I. Bedrohungslage im Telekommunikationssektor

Die Bedrohungen für die Sicherheit von IT-Systemen – z. B. durch Cyberangriffe – sind vielfältig und können unterschiedliche Lebensbereiche betreffen, so auch die Telekommunikation.[1] Für den Telekommunikationssektor bedeutsame Arten von Cyberangriffen sind durch Bots und Botnetze bzw. DoS- und DDoS-Angriffe zu sehen. Faktoren für steigende Zahlen sind im Breitbandausbau, der steigenden Nutzung des öffentlichen Internets durch Arbeiten im Homeoffice bzw. der Mobilen Arbeit sowie den Einsatz veralteter Technologie auszumachen. Mit zunehmender Vernetzung steigt gleichzeitig das Bedürfnis an Sicherheit von Netzen und Diensten und mit dieser Bedürfniszunahme wächst gleichwohl die Bedeutung IT-sicherheitsrechtlicher Aspekte.[2] Das IT-Sicherheitsrecht kennt zur Stärkung der IT-Sicherheit einen breiten Instrumentenkasten, z. B. das Aufstellen von Anforderungen an Systeme, Nachweis von Sicherheitseigenschaften oder -management durch Zertifizierungen und Auditierungen, Meldepflichten bei Eintritt von Sicherheitsvorfällen, Haftung als Steuerungselement sowie Erweiterung der Behördenbefugnisse.[3] Stellen Organisationen Beeinträchtigungen der IT-Sicherheit fest, rücken vermehrt gesetzliche Meldepflichten ins Blickfeld, welche bei Sicherheitsvorfällen zu einer Informationsübermittlung an zuständige staatliche Stellen verpflichten.[4] Nicht selten bestehen Unklarheiten, welche Vorfälle oder Ereignisse meldepflichtig sind und ob zugleich für die Erforderlichkeit einer Meldung das Überschreiten einer Erheblichkeitsschwelle notwendig ist.[5]

II. Die Meldepflicht als Instrument des IT-Sicherheitsrechts

Meldepflichten bei Sicherheitsvorfällen sind in den letzten Jahren zu einem Standardinstrument des IT-Sicherheitsrechtes geworden.[6] Sie existieren über die gesamte Rechtsordnung verteilt für eine Vielzahl unterschiedlicher Szenarien.[7] Die Normierung sowohl auf internationaler als auch auf nationaler Ebene dient vorrangig der Schaffung einer adäquaten Wissensbasis seitens staatlicher Stellen, um ein valides Lagebild der IT-Sicherheit zu ermitteln, um wiederum sachgerechte Entscheidungen treffen zu können, bspw. in Form von Sicherheits-, Kontroll- oder Sanktionsmaßnahmen.[8] Die Bedeutungszunahme ist auf den zunehmenden Einsatz von IT-Systemen und die damit einhergehenden Informationsgewinnung und -verarbeitung zurückzuführen. Die gesetzlichen Grundlagen und die Ausgestaltung der jeweiligen Meldepflicht unterscheiden sich mitunter stark nach dem betroffenen Regelungsgebiet.[9]

1. Rechtliche Grundlagen

Eine einheitliche Begriffsführung für die IT-Sicherheit oder das IT-Sicherheitsrecht existiert weder in der Informatik noch in der Rechtswissenschaft.[10] Ähnlich gelagert besteht diese Problematik auch beim Verständnis der Meldepflicht. Verwendung finden u. a. die Begriffe der Anzeige-, Benachrichtigungs-, Informations-, Melde-, Mitteilungs-, und Unterrichtungspflicht.[11] Unter einer Meldepflicht ist im Folgenden eine Handlungspflicht zu verstehen, die bei Erfüllung der jeweiligen Tatbestandvoraussetzungen unmittelbar kraft Gesetzes entsteht und daher keiner gesonderten Aufforderung bedarf, um die geforderte Informationsübermittlung gegenüber dem Staat bzw. einer oder mehrerer staatlicher Stellen vorzunehmen.[12] Unterschiede zeigen sich zuweilen hinsichtlich der die Meldung auslösenden Ereignisse.[13] Die gesetzlichen Meldepflichten werden entscheidend durch die Grundrechte, Rechtsgrundsätze und Rechtsgüter geprägt, in die durch das Auslösen besagter Handlungspflicht durch die Informationsübermittlung eingegriffen wird.[14] Ein Eingriff bzw. eine Einschränkung dieser Rechtsgüter ist nur möglich, wenn eine gesetzliche und hinreichend bestimmte Rechtsgrundlage vorliegt, die ein legitimes Ziel verfolgt und keine unverhältnismäßige Beeinträchtigung festgestellt werden kann. Allen voran kommt im Zusammenhang mit Meldepflichten bei IT-Sicherheitsvorfällen dem Datenschutz besondere Bedeutung zu, da der Schutz personenbezogener Daten zum einen das angestrebte Schutzziel der Meldepflichten darstellen kann, diesen aber andererseits jedoch auch klare Grenzen setzt.[15]

Im Zusammenhang mit der IT-Sicherheit bei Telekommunikationsanbietern kann zudem das Fernmeldegeheimnis eine Rolle spielen, welches ebenfalls eng mit dem Schutz personenbezogener Daten verknüpft ist.[16] Ebenso entfaltet der Schutz von Geschäfts- und Betriebsgeheimnissen Relevanz, da Organisationen im Rahmen bestehender Meldepflichten dazu verpflichtet sein können, Interna zu offenbaren, z. B. wenn basierend auf den konkret übermittelten Inhalten der Meldungen Rückschlüsse auf die Ausgestaltung und das Niveau der IT-Infrastruktur des Unternehmens gezogen werden können.[17] Auf diese Weise kann es zu einer Gefährdung der Reputation der Organisation kommen.[18] Ins Blickfeld rückt zudem die Berufsausübungsfreiheit bzw. unternehmerische Freiheit.[19]

Rechtfertigungsgründe für Eingriffe in die vorgenannten Rechtsgüter sind allem voran die öffentliche Sicherheit, die Verhütung von Straftaten und der Schutz der Rechte und Freiheiten anderer, d. h. im Datenschutzrecht der Schutz der Persönlichkeitsrechte Dritter oder mit Blick auf die Kritischen Infrastrukturen der Schutz des Gemeinwesens vor den Folgen möglicher Beeinträchtigungen der betroffenen Infrastrukturen.[20] Im Bereich der Meldepflichten darf zudem nicht außer Acht bleiben, dass die Verpflichtung zur Meldung eines Sicherheitsvorfalls zugleich auch einen Eingriff in das Recht, sich nicht selbst belasten zu müssen, den sog. Nemo-teneturGrundsatz, ist.[21] Eine Beeinträchtigung kann vorliegen, wenn die betroffene Organisation sich durch die (verpflichtende) Erfüllung einer Meldepflicht im Rahmen eines Verfahrens mit Sanktionsfolge selbst belasten müsste.[22] Eine Einschränkung dieses Rechtsgrundsatzes ist insbesondere dann mög-

1 *Hornung*, NJW 2015, 3334.
2 *Schneider*, Meldepflichten im IT-Sicherheitsrecht – Datenschutz, Kritische Infrastrukturen und besondere IT-Dienste, 2017, S. 36.
3 *Hornung/Schallbruch*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 2021, § 1 Einführung, Rn. 38.
4 *Winter*, CR 2020, 576.
5 *Schneider* (Fn. 2), S. 36.
6 *Hornung/Schindler*, in: Hornung/Schallbruch (Fn. 3), § 21 Telekommunikation und Telemedien, Rn. 74.
7 *Müllmann/Volkamer*, ZD 2021, 8, 9.
8 *Roos*, MMR 2015, 636, 639; *Schneider* (Fn. 2), S. 48.
9 *Müllmann/Volkamer*, ZD 2021, 8, 9.
10 *Hornung/Schindler*, in: Hornung/Schallbruch (Fn. 3), § 1 Einführung, Rn. 10.
11 *Schneider* (Fn. 2), S. 47.
12 *Schneider* (Fn. 2), S. 47.
13 *Winter*, CR 2020, 576, 578.
14 *Bräutigam/Wilmer*, ZRP 2015, 38, 39; *Schneider* (Fn. 2), S. 88.
15 *Schneider* (Fn. 2), S. 89.
16 *Schneider* (Fn. 2), S. 91.
17 *Schneider* (Fn. 2), S. 94.
18 *Hornung*, NJW 2015, 3334, 3338; *Roos*, MMR 2015, 636, 639.
19 *Schneider* (Fn. 2), S. 94.
20 *Schneider* (Fn. 2), S. 148.
21 *Eckhardt*, in: Geppert/Schütz (Hrsg.), Beck'scher TKG-Kommentar, 4. Aufl. 2013, § 109 Rn. 79; *Eckhardt/Schmitz*, CR 2011, 436, 442; *Schneider* (Fn. 2), S. 95.
22 *Schneider* (Fn. 2), S. 96.

lich, wenn der Wesensgehalt dieses Justizgrundrechtes nicht wesentlich ausgehöhlt wird.[23] Die Meldepflichten dürften demnach verhältnismäßig sein, wenn ein entsprechendes Verwertungsverbot für die übermittelten Informationen besteht.[24] Derartige Auskunftsverweigerungsrechte oder Verwertungsverbote sind im Rahmen der gesetzlichen Meldepflichten mittlerweile stets ebenfalls normiert. Anhand der vorstehenden Betrachtungen wird ersichtlich, dass gesetzliche Meldepflichten bei IT-Sicherheitsvorfällen insbesondere auf den Gebieten des Datenschutzes sowie den Kritischen Infrastrukturen, so auch der Telekommunikation, besondere Relevanz entfalten und lassen sich mit der Bedeutung der Sicherheit der IT-Systeme entsprechend rechtfertigen.[25] IT-Systeme und deren Funktionsfähigkeit sind u. a. im Bereich des Telekommunikationssektors essenziell für die Erbringung von Telekommunikationsdienstleistungen und mithin für die Versorgung der Bevölkerung und die Funktion des Gemeinwesens.[26]

2. Meldepflichten im TKG

Das Telekommunikationsgesetz in der aktuellen Fassung ist am 1. 12. 2021 in Kraft getreten und setzt die europarechtlichen Vorgaben der Richtlinie über den europäischen Kodex für die elektronische Kommunikation (EKEK) im nationalen Recht um. Im Telekommunikationsrecht sind grundlegend zwei Typen von Meldepflichten zu unterscheiden: § 168 TKG, der trotz inhaltlicher Abweichungen der allgemeinen Logik der Meldepflichten bei Sicherheitsvorfällen bzw. -verletzungen in Kritischen Infrastrukturen folgt und § 169 TKG, der dem Datenschutz dient.[27]

a) Mitteilungspflicht zu Sicherheitsvorfällen nach § 168 TKG

Im Zuge der nationalen Umsetzung der EKEK wurden die Vorschriften im Bereich der öffentlichen Sicherheit aktualisiert, was dazu geführt hat, dass die „Mitteilungs- und Informationspflicht“ des § 109 Abs. 5 TKG a. F. in § 168 TKG fortgeschrieben, präzisiert und erweitert wurde.[28] Unternehmen, die öffentliche Telekommunikationsnetze betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen, müssen gemäß § 168 Abs. 1 S. 1 TKG der Bundesnetzagentur (BNetzA) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) Sicherheitsvorfälle mit beträchtlichen Auswirkungen auf den Betrieb der Netze oder die Erbringung der Dienste unverzüglich mitteilen. Hierdurch soll sichergestellt werden, dass die von der Mitteilungspflicht betroffenen Organisationen zu einem validen und vollständigen Lagebild der IT-Sicherheit beitragen.[29] Die Begrifflichkeiten des öffentlichen Telekommunikationsnetzes (Nr. 42) und des öffentlich zugänglichen Telekommunikationsdienstes (Nr. 44) ergeben sich hierbei aus § 3 TKG. Die Einzelheiten der Mitteilung und des Verfahrens werden gemäß § 168 Abs. 4 S. 1 TKG durch die BNetzA festgelegt. Diese hat ein Meldekonzept veröffentlicht, welches zur Auslegung bei der Beurteilung des Vorliegens einer Meldepflicht herangezogen werden sollte.[30]

aa) Meldepflichtige Ereignisse

Meldepflichtig sind Sicherheitsvorfälle mit beträchtlichen Auswirkungen auf den Betrieb eines öffentlichen Telekommunikationsnetzes oder die Erbringung eines öffentlichen Telekommunikationsdienstes. Gemäß § 3 Nr. 53 TKG ist ein Sicherheitsvorfall ein Ereignis mit nachteiliger Wirkung auf die Sicherheit von Telekommunikationsnetzen oder -diensten. Sicherheitsrelevant in diesem Sinne ist ein Vorfall dann, wenn die Fähigkeit von Telekommunikationsnetzen oder -diensten, auf einem bestimmten Vertrauensniveau alle Angriffe abzuwehren, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit dieser Netze und Dienste, der gespeicherten, übermittelten oder verarbeiteten Daten oder der damit zusammenhängenden Dienste, die über diese Telekommunikationsnetze oder -dienste angeboten werden oder zugänglich sind, beeinträchtigen wird.[31] Demnach können als meldepflichtige Ereignisse potenziell alle vom Anbieter nicht gewollten, negativen Auswirkungen auf IT-Systeme, Komponenten und Prozesse verstanden werden.[32] Letztlich wird man allgemein IT-Sicherheitsvorfälle in Netzen und Diensten erfassen müssen.[33] Mithin kommen Manipulationen der Internet-Infrastruktur und der Missbrauch einzelner Server oder Anschlüsse, etwa zum Errichten oder Betreiben eines Botnetzes sowie ganz allgemein der Verfügbarkeit der Netze und der Verlässlichkeit und Funktionsfähigkeit der IT einzelner Nutzer oder etwa Denial-of-Service-Attacken in Betracht.[34] Die BNetzA führt in einem auf der Webseite bereitgestellten Meldeformular des Weiteren Diebstahl, Fehlbedienung, Social Engineering, Fehlkonfiguration, unautorisierte Nutzung von Ressourcen, Netzwerküberlastung, Softwarefehler, Sicherheitslücken in Hard- und Softwarekomponenten, gezielte Angriffe und informationstechnische Angriffe wie z. B. DDoS, Phishing, Angriffe durch Innentäter usw. als meldepflichtige Ereignisse an.[35]

Allein das Vorliegen bzw. die Feststellung eines Sicherheitsvorfalles führt jedoch noch nicht zum Auslösen der Mitteilungspflicht nach § 168 Abs. 1 TKG. Vielmehr müssen die Vorfälle zumindest das Potential einer beträchtlichen Auswirkung bergen.[36] Durch die europarechtlichen Vorgaben der EKEK wurde im Rahmen der Modernisierung des Telekommunikationssektors auch die Normierung bestimmter Bewertungskriterien vorgenommen.[37] Gemäß § 168 Abs. 2 Nr. 1 - 5 TKG ist das Ausmaß der Auswirkungen, d. h. der konkrete Gefährdungsgrad, insbesondere anhand der Zahl der von dem Sicherheitsvorfall betroffenen Nutzer, der Dauer des Sicherheitsvorfalls, der geographischen Ausdehnung des von dem Sicherheitsvorfall betroffenen Gebietes, dem Ausmaß der Beeinträchtigung des Telekommunikationsnetzes oder -dienstes sowie dem Ausmaß der Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten zu beurteilen. Die Kriterien des § 168 Abs. 3 TKG sind jedoch nicht abschließend. Die eigenverantwortliche Bewertung des Vorfalls durch den Pflichten-

23 *Schneider* (Fn. 2), S. 94.
24 *Eckhardt*, in: Geppert/Schütz (Fn. 21), § 109, Rn. 78 ff.; *Eckhardt/Schmitz*, CR 2011, 436, 443.
25 *Bräutigam/Wilmer*, ZRP 2015, 38, 40; *Schneider* (Fn. 2), S. 147.
26 *Bräutigam/Wilmer*, ZRP 2015, 38, 40; *Schneider* (Fn. 2), S. 147.
27 *Hornung/Schindler*, in: Hornung/Schallbruch (Fn. 3), § 21 Telekommunikation und Telemedien, Rn. 74.
28 *Filusch/Sowa*, PinG 2024, 1, 9.
29 BT-Drs. 18/4096, S. 36.
30 BNetzA, Meldekonzept für die Mitteilung von beträchtlichen Sicherheitsvorfällen nach § 168 TKG v. 28. 2. 2022, abrufbar unter: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/mitteilungeinersicherheitsverletzung/EntwurfMeldekonzept168TKG.pdf?__blob=publicationFile&v=1.
31 BNetzA (Fn. 30), S. 4.
32 *Voigt*, IT-Sicherheitsrecht, 2. Aufl. 2022, Rn. 405.
33 *Hornung/Schindler*, in: Hornung/Schallbruch (Fn. 3), § 21 Telekommunikation und Telemedien, Rn. 76.
34 BT-Drs. 18/4096, S. 36.; OLG Köln, 14. 12. 2015 – 12 U 16/13, K&R 2016, 194.
35 Formular zur Mitteilung eines Sicherheitsvorfalls zu § 168 TKG v. Dezember 2021, abrufbar unter: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/mitteilungeinersicherheitsverletzung/EntwurfMeldeformular168TKG.pdf?__blob=publicationFile&v=1.
36 *Voigt* (Fn. 32), Rn. 405.
37 BNetzA (Fn. 30), S. 5.

adressaten führt u. U. zur Berücksichtigung weiterer Kriterien, sofern diese zur Einschätzung der Sicherheitsrelevanz geeignet sind.[38] Als Anhaltspunkte zur Bestimmung des Ausmaßes der Auswirkungen sind unter Rückgriff auf die bisherige Mitteilungspraxis und in Anlehnung und an die „Technical Guideline on Incident Reporting under the EECC" der Agentur der Europäischen Union für Cybersicherheit Europäischen Union für Cybersicherheit (ENISA) entsprechende Schwellenwerte zu bestimmen.[39] Im Einzelnen zu den ausdrücklich normierten Bewertungskriterien sowie den jeweiligen Schwellenwerten gilt Folgendes:

Die Anzahl der betroffenen Nutzer im Sinne des § 3 Nr. 41 TKG ergibt sich aus der Anzahl aller natürlichen und juristischen Personen im Wirkbereich des Sicherheitsvorfalls. Die Dauer des Sicherheitsvorfalls sollte – soweit möglich bzw. feststellbar – ab dem tatsächlichen Eintritt des Sicherheitsvorfalls, hilfsweise ab dem Zeitpunkt der Kenntnisnahme bis zu dessen vollständiger Behebung, mithin mit Abschluss der letzten Maßnahme, ermittelt werden.[40] Da zwischen beiden vorgenannten Kriterien ein direkter Zusammenhang besteht, ist der Schwellenwert aus dem Produkt zu bilden: Ein Sicherheitsvorfall ist demnach beträchtlich, wenn die betroffenen Nutzerstunden einen Wert von einer Million Nutzerstunden überschreiten.[41] Zur Beurteilung der geographischen Reichweite können u. a. die Grenzüberschreitung des Sicherheitsvorfalls, die Größe sowie die Art des betroffenen Gebietes (ländliche Region, Inseln oder Hauptstädte) sowie eine mögliche Betroffenheit der internationalen Zusammenschaltung herangezogen werden.[42] Entsprechend der Technical Guideline on Incident Reporting under the EECC werden Konkretisierungen der Sicherheitsvorfälle mit länderübergreifenden Auswirkungen getroffen, wonach jeglicher Sicherheitsvorfall meldepflichtig ist.[43] Eine Beeinträchtigung des Telekommunikationsnetzes oder -dienstes soll möglichst anhand der Bedeutung der Komponenten und System und der Anzahl der prozentualen Betroffenheit beziffert werden.[44] Ebenso kann die Verminderung der Servicequalität als Indikator herangezogen werden.[45] Die Auswirkungen auf die wirtschaftlichen und gesellschaftlichen Tätigkeiten schließlich können mittels der Auswirkungen auf die Notruflenkung, durch außergewöhnliche IT-Störungen sowie öffentliche Warnsysteme gemessen werden, oder aber durch Gefahren für die öffentliche Sicherheit und Ordnung, durch materielle oder immaterielle Verluste wie z. B. Produktivitätseinbußen oder Rufschädigung sowie einer Berichterstattung in den Medien bestimmt werden.[46] Besondere Bedeutung kommt hier der Notruflenkung zu. Ausschlaggebend ist eine Beeinträchtigung der Hard- und/oder Software, die dezidiert zur Notruflenkung benötigt wird. Sofern die Notruflenkung betroffen ist, liegt stets ein meldepflichtiger Sicherheitsvorfall vor.[47] Ferner kann auch das Kriterium der außergewöhnlichen IT-Störungen einen Indikator zur Bewertung der beträchtlichen Auswirkungen darstellen. Dies ist der Fall, wenn die Ursache der Beeinträchtigung außergewöhnlich oder zum Zeitpunkt der Mitteilung nicht nachvollziehbar ist und die Beeinträchtigung nicht mehr im Rahmen des Tagesgeschäfts durch übliche Maßnahmen bewältigt werden kann.[48] Eine Ursache ist außergewöhnlich, wenn sie z. B. in Folge von Softwareupdates oder Systemfehlern zu einer unerwarteten Beeinträchtigung führt oder auf einen nicht alltäglichen technischen Angriff wie bspw. DoS- bzw. DDoS-Attacken, die aufgrund der Bandbreite bzw. der Vorgehensweise oder bisher unbekannter Sicherheitslücken außergewöhnlich sind, zurückzuführen ist.[49] Derartige Sicherheitsvorfälle sind ebenfalls stets meldepflichtige Vorfälle. Neben den vorbezeichneten Kriterien können auch die betroffene Person (z. B. Politiker) oder das Unternehmen (z. B. Banken), der Zeitpunkt (z. B. Wahlen) oder der Sektor (z. B. staatliche Einrichtungen) von Bedeutung sein.[50]

bb) Inhalt der Meldung

Der Inhalt der Meldung wird durch § 168 Abs. 3 TKG präzisiert. Die Mitteilung muss Angaben zum Sicherheitsvorfall und zu den Kriterien nach § 168 Abs. 2 TKG sowie zu den betroffenen Systemen und zu der vermuteten oder tatsächlichen Ursache enthalten. Zur Meldung sollte das durch die BNetzA bereitgestellte Meldeformular genutzt werden.[51] Mittels dieses Formulars werden allem voran Ausführungen zu dem Sicherheitsvorfall erhoben, welche in erster Linie der Bereitstellung allgemeiner Informationen dienen, und Angaben, ob es sich um eine initiale Kurzmitteilung oder eine vollständige Mitteilung handelt.[52] Hinsichtlich der Angaben die Ursachen betreffend ist zu berücksichtigen, dass derer theoretisch eine Vielzahl möglich sind, weshalb diese so genau wie möglich zu identifizieren, zu analysieren und entsprechend darzulegen sind.[53] Über die gesetzlich geforderten Angaben hinaus können bereits ergriffene Sicherheitsmaßnahmen geschildert werden.

cc) Verfahrensablauf

Das Meldeverfahren nach § 168 TKG folgt weitestgehend demjenigen nach dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG).[54] Hervorzuheben sind in diesem Zusammenhang insbesondere der Zeitpunkt der Mitteilung, die Mitteilungsformen sowie die Vertraulichkeit und der Umgang mit einer Mitteilung.[55] In Bezug auf die Feststellung des Sicherheitsvorfalls muss die Rechtzeitigkeit der Mitteilung in geeigneter Weise sichergestellt werden, d. h. Informationsmängel innerhalb der Organisation gehen zu Lasten der Verpflichteten, was gleichwohl beim Einsatz Dritter bzw. beim Outsourcing der Fall ist.[56] Eine Meldung ist erforderlich, wenn eine entsprechende Kenntnislage vorliegt und weiteres Zuwarten nach den Umständen des Einzelfalls nicht weiter geboten wäre.[57] Erfolgt eine derartige Feststellung, hat unverzüglich, d. h. „ohne schuldhaftes

38 BNetzA (Fn. 30), S. 5.
39 BNetzA, Mitteilung nach § 109 Abs. 5 TKG – Umsetzungskonzept Version 4.0 v. 10. 11. 2017, abrufbar unter: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/mitteilungeinersicherheitsverletzung/Umsetzungskonzept_%C2%A7_109_(5)_TKG_Mitteilung_Sicherheitsverletzung.pdf?__blob=publicationFile&v=9; ENISA, Technical Guideline on Incident Reporting under the EECC, v. März 2021, abrufbar unter: https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc/@@download/fullReport.
40 ENISA (2016) Security incident indicators – measuring the impact of incidents affecting electronic communications, S. 25 ff., abrufbar unter: https://www.enisa.europa.eu/publications/security-incidents-indicators/@@download/fullReport.
41 BNetzA (Fn. 30), S. 6.
42 ENISA (Fn. 40), S. 21.
43 ENISA (Fn. 40), S. 21.
44 BNetzA (Fn. 30), S. 5.
45 ENISA (Fn. 40), S. 42.
46 BNetzA (Fn. 30), S. 6.
47 BNetzA (Fn. 30), S. 6.
48 BNetzA (Fn. 30), S. 7.
49 BNetzA (Fn. 30), S. 8.
50 ENISA (Fn. 40), S. 21 f.
51 BNetzA (Fn. 35).
52 BNetzA (Fn. 30), S. 8.
53 BNetzA (Fn. 30), S. 8.
54 *Voigt* (Fn. 32), Rn. 409.
55 BNetzA (Fn. 30), S. 8.
56 BNetzA (Fn. 30), S. 8.
57 BNetzA (Fn. 30), S. 9.

Zögern“ (vgl. § 121 BGB), eine Mitteilung an die BNetzA und das BSI zu erfolgen. Es empfiehlt sich, dass Telekommunikationsdienstleister eine mehrstufige Meldung vornehmen, d. h. zunächst eine unverzügliche Kurzmitteilung an die BNetzA und das BSI vornehmen und zu einem späteren Zeitpunkt eine vollständige Meldung nachholen.[58] Die BNetzA legt in ihrem Meldekonzept zudem fest, dass Betreiber öffentlicher Telekommunikationsnetze und Anbieter öffentlich zugänglicher Telekommunikationsdienste mit erhöhtem Gefährdungspotenzial im Sinne des § 167 Abs. 1 Nr. 3 TKG eine Meldung unverzüglich, in jedem Fall eine erste Meldung als Frühwarnung aber innerhalb von drei Stunden nach Kenntnisnahme absetzen müssen und auch angeben, ob der Sicherheitsvorfall vermutlich auf eine rechtswidrige oder böswillige Handlung zurückzuführen ist.[59] In der Folge sind dann Zwischenberichte über relevante Statusaktualisierungen abzugeben, die Angaben zur Beschreibung, Erkenntnisse zu Schweregrad und Art der Bedrohung sowie getroffenen und laufenden Abhilfemaßnahmen enthalten. Ferner ist in derartigen Fällen unverzüglich, spätestens jedoch drei Tage nach der vollständigen Behebung des Sicherheitsvorfalls, ein Abschlussbericht mit einer ausführlichen Beschreibung des Vorfalls, seines Schweregrades und der Auswirkungen inklusive Angaben zur Art der Bedrohung und den zugrundeliegenden Ursachen sowie zu den getroffenen und laufenden Abhilfemaßnahmen vorzulegen. Zur Durchführung der Mitteilung ist bei der BNetzA ein ständiger Bereitschaftsdienst eingerichtet. Nach § 168 Abs. 4 S. 2 TKG kann die BNetzA zudem einen detaillierten Bericht über den Sicherheitsvorfall und die ergriffenen Abhilfemaßnahmen verlangen.

dd) Benachrichtigung der Öffentlichkeit

Die aus den nationalen Mitteilungsverfahren gewonnenen Daten werden im Rahmen des länderübergreifenden Mitteilungsverfahrens zwischen den nationalen Behörden der EU-Mitgliedstaaten und der ENISA ausgetauscht, vgl. § 168 Abs. 5 TKG. Liegt nach Ansicht der BNetzA der Sicherheitsvorfall zudem im öffentlichen Interesse, so kann diese nach § 168 Abs. 5 S. 2 TKG die Öffentlichkeit über den Vorfall informieren oder die zur Meldung verpflichtete Organisation zu einer entsprechenden Unterrichtung der Öffentlichkeit auffordern. Im Rahmen dieser Benachrichtigung der Öffentlichkeit hat die Bundesnetzagentur jedoch den Grundsatz der Verhältnismäßigkeit zu wahren und darf davon ausgehend nur bei besonders gravierenden Sicherheitsverletzungen mit potenziellen Auswirkungen auf die Verfügbarkeit und Integrität der gegenständlichen Telekommunikationsdienstleistung in Betracht kommen.[60] Darüber hinaus kann sich nach § 168 Abs. 6 TKG in den Fällen einer besonderen und erheblichen Gefahr eines Sicherheitsvorfalls eine Informationspflicht der Betreiber und Anbieter gegenüber den von dieser Gefahr potenziell betroffenen Nutzer über alle möglichen Schutz- oder Abhilfemaßnahmen, die von den Nutzern ergriffen werden können, ergeben. Nach § 168 Abs. 7 TKG legt die BNetzA der Kommission, der ENISA und dem BSI einmal pro Jahr einen zusammenfassenden Bericht in anonymisierter Form über die eingegangenen Meldungen und die ergriffenen Abhilfemaßnahmen vor.

b) Benachrichtigungspflichten nach § 169 TKG

Wie eingangs bereits erwähnt, sieht das Telekommunikationsgesetz in § 169 TKG eine bereichsspezifische Datenschutznorm mit IT-Sicherheitsbezug vor.[61] Diese dient insoweit der Umsetzung von Art. 4 Abs. 3 E-Privacy-Richtlinie und bleibt mithin neben der DSGVO anwendbar. Anbieter von Telekommunikationsdiensten treffen in den Fällen der Verletzung des Schutzes personenbezogener Daten Melde- und Dokumentationspflichten.

aa) Benachrichtigungspflichten bei Datenschutzverletzungen

Zunächst besteht nach § 169 Abs. 1 S. 1 TKG im Falle einer Verletzung des Schutzes personenbezogener Daten im Sinne des § 3 Nr. 71 TKG eine Pflicht zur unverzüglichen Meldung an die Bundesnetzagentur und die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Die Benachrichtigung muss dabei mindestens Angaben über die Art der Verletzung des Schutzes personenbezogener Daten, zu den Kontaktstellen, bei denen weitere Informationen erhältlich sind und Empfehlungen zu Maßnahmen, die mögliche nachteilige Auswirkungen der Verletzung des Schutzes personenbezogener Daten begrenzen, enthalten. Die Benachrichtigungspflicht entfällt nach § 169 Abs. 1 S. 3 TKG jedoch, wenn der Anbieter des Telekommunikationsdienstes über sein Sicherheitskonzept im Sinne des § 167 TKG nachweisen kann, dass die von der Verletzung betroffenen Daten durch geeignete technische Vorkehrungen gesichert, insbesondere unter Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens gespeichert wurden. Hiervon ist die Meldepflicht nach Art. 33 DSGVO zu unterscheiden. Das Meldeverfahren nach § 169 TKG ist als Umsetzung der E-Privacy-Richtlinie nach Art. 95 DSGVO anwendbar, wenn personenbezogene Daten den bereichsspezifischen Sektor der Telekommunikation betreffen. In Mischfällen, in denen durch denselben Lebenssachverhalt sowohl der Anwendungsbereich der DSGVO als auch die Datenschutzregelungen des Telekommunikationsbereichs betroffen sind, ist nur eine Meldung nach § 169 TKG erforderlich, was bspw. bei Verkehrs- oder Bestandsdaten der Fall sein kann.

bb) Dokumentationspflichten bei Datenschutzverletzungen

Neben den Benachrichtigungspflichten tritt nach § 169 Abs. 3 TKG die Pflicht, Datenschutzverletzungen in einem Verzeichnis zu dokumentieren. Dokumentiert werden müssen die Umstände der Verletzungen, deren Auswirkungen sowie die ergriffenen Abhilfemaßnahen. Das Verzeichnis muss zumindest Datenschutzverletzungen der letzten fünf Jahre berücksichtigen.

c) Verletzungsfolgen

Erfolgen die Meldungen nach §§ 168 Abs. 1 oder 169 Abs. 1 TKG nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig, kann dies gemäß § 228 Abs. 2 Nr. 39, Abs. 7 Nr. 6 bzw. Abs. 2 Nr. 40, Abs. 7 Nr. 4 TKG mit einem Bußgeld in Höhe von 10 000 Euro bzw. 100 000 Euro geahndet werden. Erfolgt die Dokumentationsverpflichtung gemäß § 169 Abs. 3 TKG nicht, nicht richtig oder nicht vollständig, ist nach § 228 Abs. 2 Nr. 41, Abs. 7 Nr. 6 TKG eine Sanktionierung in Höhe von 10 000 Euro denkbar. Neben den Bußgeldern können Anbieter von öffentlich zugänglichen Telekommunikationsdiensten zusätzlich zivilrechtliche Haftungsrisiken treffen. Inhalt und Umfang des Schadensersatzanspruchs richten sich nach den allgemeinen Grundsätzen der §§ 249 ff. BGB, wobei die Anspruchsgrundlage die Verträge mit den Kunden oder auch das Deliktsrecht bieten können.[62]

58 *Voigt* (Fn. 32), Rn. 409 f.
59 BNetzA (Fn. 30), S. 9.
60 *Voigt* (Fn. 32), Rn. 411.
61 *Voigt* (Fn. 32), Rn. 413.
62 *Voigt* (Fn. 32), Rn. 423.

3. Meldepflichten für Betreiber Kritischer Infrastrukturen

Das BSIG sieht verschiedene Meldepflichten vor: § 8b Abs. 4 und § 8c Abs. 3, § 8f Abs. 7 BSIG. Das Gesetz knüpft hierbei u. a. an die besondere Bedeutung des betroffenen Unternehmens für die Funktion des Gemeinwesens an.[63] Betrachtet werden soll im Folgenden insbesondere die Meldepflicht für Betreiber Kritischer Infrastrukturen gemäß § 8b Abs. 4 BSIG. Kritische Infrastrukturen sind nach § 2 Abs. 10 BSIG u. a. Einrichtungen, Anlagen oder Teile davon, die dem Sektor Telekommunikation angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Hierdurch wird bereits ersichtlich, dass nicht jede Infrastruktur aus dem Telekommunikationssektor als kritisch zu qualifizieren ist.[64]

a) Meldepflichtige Ereignisse

Die sicherheitsrechtlichen Regelungen im Bereich der Kritischen Infrastrukturen sehen für die Betreiber zwei Kardinalpflichten vor. Eine ist die Meldepflicht aus § 8b Abs. 4 BSIG für den Fall des Eintritts von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von betriebenen Kritischen Infrastrukturen geführt haben.[65] Unter den Begriff der Störung fallen alle Sicherheitslücken, Schadprogramme sowie erfolgte, versuchte oder erfolgreich abgewehrte Angriffe auf die Sicherheit in der Informationstechnik, entscheidend ist die Erheblichkeit der Beeinträchtigung der Funktionsfähigkeit der IT-Systeme.[66] Eine Beeinträchtigung ist dann als erheblich anzusehen, wenn die betroffene Infrastruktur nicht mehr in der Lage ist, ihre Versorgungsleistung wie geplant oder wie erwartet zu erbringen.[67] Ob eine Beeinträchtigung erheblich ist, obliegt der Prognose des Betreibers und solange ein solcher Störungserfolg nicht eingetreten ist, besteht diesbezüglich keine Meldepflicht.[68] Eine Verpflichtung zur Meldung besteht jedoch nicht nur dann, wenn tatsächlich eine Störung eingetreten ist, sondern auch bereits die Möglichkeit eines Ausfalls kann den Eintritt der Verpflichtung für den betroffenen Betreiber begründen.[69] In diesem Fall ist das Vorliegen einer erheblichen Störung erforderlich. Wiederrum ist der Eintritt eines Störungserfolges für das Entstehen der Meldepflicht nicht erforderlich. Es genügt, wenn die erhebliche Störung potenziell zu einem Störungserfolg führen kann.[70] Mit Blick auf das zuvor Gesagte wird deutlich, dass an das meldepflichtige Ereignis andere Voraussetzungen geknüpft werden als im Rahmen der Meldepflicht des § 168 TKG. Insbesondere geht der Wortlaut mit „Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse“ nach § 8b Abs. 4 BSIG und „Sicherheitsvorfälle mit beträchtlichen Auswirkungen auf den Betrieb eines öffentlichen Telekommunikationsnetzes oder die Erbringung eines öffentlichen Telekommunikationsdienstes“ nach § 168 Abs. 1 TKG auseinander. Nicht deutlich wird, ob mit dieser unterschiedlichen Wortwahl weitergehende Anforderungen erforderlich sind.[71]

b) Umfang und Inhalt der Meldung

Die Meldung muss unverzüglich, d. h. ohne schuldhaftes Zögern nach Eintritt der Störung erfolgen, d. h. der Betreiber muss die entsprechenden Ermittlungen die Störung betreffend in einer Weise durchführen, die nicht zu vermeidbaren Verzögerungen der Meldung führen.[72] Die entsprechenden Meldungen werden durch das BSI analysiert und mögliche Störungen für die Verfügbarkeit kritischer Infrastrukturen abgeleitet sowie ein Lagebild erstellt.[73] Es besteht zudem nach § 8b Abs. 4 S. 3 BSIG die Möglichkeit einer Meldung in anonymisierter Form, sofern die Störung nicht zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat, um den Betreibern die Bedenken im Hinblick auf mögliche Reputationsschäden zu nehmen.[74] Nach § 14 Abs. 2 Nr. 7, Abs. 5 BSIG ist ein Verstoß mit einer Geldbuße bis zu 500 000 Euro sanktionsfähig.

c) Abgrenzung des Anwendungsbereiches

§ 8d BSIG enthält eine allgemeine Vorrangregelung. Hiernach werden die IT-Sicherheits- und Meldepflichten – insbesondere auch § 8b BSIG – durch spezialgesetzliche Regelungen insoweit verdrängt, als diese mit den Anforderungen vergleichbar oder weitergehend sind.[75] Dies gilt z. B. für Art. 33 DSGVO, welcher eine Meldepflicht bei der Beeinträchtigung von personenbezogenen Daten auslöst.[76] Soweit Betreiber ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen, kommt die Meldepflicht des § 8b Abs. 4 BSIG gemäß § 8d Abs. 3 Nr. 1 BSIG zur Vermeidung einer Doppelregulierung nicht zur Anwendung.[77] Es sollen im Wesentlichen die bereichsspezifischen gleichen Anforderungen gelten, um eine Vereinheitlichung der IT-Sicherheitsregelungen zu erreichen.[78] Diesbezüglich muss jedoch die Frage aufgeworfen werden, ob hier eine vollständige Verdrängungswirkung angenommen werden kann, da wie aufgezeigt Unterschiede hinsichtlich des Adressatenkreises sowie des die Meldung auslösenden Ereignisses bestehen. Angesichts der Pflicht zur Implementierung aufwändiger Meldeverfahren ist der Anwendungsbereich für betroffene Organisationen von erheblicher Bedeutung.[79] Ebenso kann der Sanktionshöhe bei Verstoß gegen die jeweils einschlägige Meldepflicht Bedeutung zukommen.

4. Ausblick auf die Rechtsänderung

Am 16. 1. 2023 ist die NIS-2-Richtlinie (NIS-2-RL)[80] in Kraft getreten und muss nunmehr durch die nationalen Gesetzgeber bis zum 17. 10. 2024 umgesetzt werden. Mit der NIS-2-Richt-

63 *Winter*, CR 2020, 576.
64 *Winter*, CR 2020, 576.
65 *Fischer*, in: Hornung/Schallbruch (Fn. 3), § 13 Kritische Infrastrukturen, Rn. 27.
66 BT-Drs. 19/26106, S. 82.
67 *Ritter/Schulte*, CR 2019, 617, 619.
68 *Winter*, CR 2020, 576, 578.
69 *Beucher/Ehlen/Utzerath*, in: Kipker, Cybersecurity – Handbuch, 2. Aufl. 2023, Kap. 14 Kritische Infrastrukturen, Rn. 112.
70 *Ritter/Schulte*, CR 2019, 617, 619.
71 *Hornung*, NJW 2015, 3334, 3337.
72 *Beucher/Ehlen/Utzerath*, in: Kipker (Fn. 69), Kap. 14 Kritische Infrastrukturen, Rn. 116.
73 *Beucher/Ehlen/Utzerath*, in: Kipker (Fn. 69), Kap. 14 Kritische Infrastrukturen, Rn. 103.
74 *Fischer*, in: Hornung/Schallbruch (Fn. 3), § 13 Kritische Infrastrukturen Rn. 91.
75 *Beucher/Ehlen/Utzerath*, in: Kipker (Fn. 69), Kap. 14 Kritische Infrastrukturen, Rn. 153.
76 *Beucher/Ehlen/Utzerath*, in: Kipker (Fn. 69), Kap. 14 Kritische Infrastrukturen, Rn. 153.
77 BT-Drs. 19/26108, S. 362; BT-Drs. 18/4096, S. 29.
78 *Bräutigam/Wilmer*, ZRP 2015, 38, 39.
79 *Hornung*, NJW 2015, 3334, 3335.
80 RL (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. 12. 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der VO (EU) Nr. 910/2014 und der RL (EU) 2018/1972 sowie zur Aufhebung der RL (EU) 2016/1148 (NIS-2-Richtlinie).

linie hat der europäische Gesetzgeber eine europaweite Gesetzgebung zur Cybersicherheit durch eine Reihe rechtlicher Anforderungen und Maßnahmen geschaffen, welche darauf abzielen, das bestehende Cybersicherheitsniveau in der Europäischen Union zu erhöhen.

Relevanz entfaltet die NIS-2-RL für Unternehmen und Behörden die gemäß Art. 2 und Art. 3 NIS-2-RL als wesentliche oder wichtige Einrichtungen zu qualifizieren sind und die definierten Schwellenwerte erreichen.[81] Durch die auf diese Weise betroffenen Organisationen sind die erweiterten IT-Sicherheitspflichten zu erfüllen.[82]

In Deutschland ist für die Umsetzung die Verabschiedung des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) vorgesehen. Diesbezüglich existiert ein Referentenentwurf mit Bearbeitungsstand vom 22. 12. 2023.[83] Darüber hinaus liegt ein Diskussionspapier des Bundesministeriums des Inneren und für Heimat vor.[84] Das NIS2UmsuCG wird als Änderungsgesetz die Vorschriften diverser Gesetze adressieren.[85] Primär von den Änderungen betroffen sind die Vorgaben des BSIG. Eine Vielzahl der Vorgaben aus der NIS-2-RL und dem NIS2UmsuCG sind bereits im deutschen Recht verankert, so auch die Meldepflichten bei Sicherheitsvorfällen.[86] Entsprechende Vorgaben zur Meldung von Sicherheitsvorfällen sind in Art. 23 NIS-2-RL und in dessen Umsetzung in § 32 BSIG-E vorgesehen. Hervorzuheben ist hier, dass im Unterschied zur bisher geltenden Rechtslage ein mehrstufiges Meldeverfahren vorgesehen ist.[87] Weiterhin weicht der melderelevante Begriff in § 32 BSIG-E inhaltlich vom bisher die Meldepflicht auslösenden Ereignis nach § 8b Abs. 4 BSIG ab, weshalb eine inhaltliche Erweiterung der Meldepflicht anzunehmen sein wird.[88]

Die Regelungen der NIS-2 werden gemäß Art. 4 NIS-2-RL durch sog. sektorspezifische Rechtsakte verdrängt.[89] Für den Bereich des Telekommunikationssektors sieht § 28 Abs. 4 BSIG-E Ausnahmen vor. In Bezug auf das TKG enthält der aktuelle Referentenentwurf lediglich aktualisierte Verweise und noch keine inhaltlichen Veränderungen. Dennoch wird es aller Voraussicht nach zur Aktualisierung des TKG und insbesondere des § 168 TKG kommen.[90]

III. Fazit

Die unterschiedlichen gesetzlichen Pflichten, die bei Eintritt eines IT-Sicherheits- oder Datenschutzvorfalls eine Meldung an eine oder mehrere staatliche Stellen auslösen, sind, wie auch andere Bestandteile des IT-Sicherheitsrechts, weit über die gesamte Rechtsordnung verstreut. Zuweilen erfolgt im Rahmen der unterschiedlichen Meldepflichten eine uneinheitliche Begriffsführung, z. B. hinsichtlich des die Meldung auslösenden Ereignisses (Sicherheitsvorfall, Störung, Verletzung der Datensicherheit usw.). Diese terminologischen Unterschiede sind jedoch auf die verschiedenen gesetzlichen Schutzzwecke zurückzuführen, denen die einzelnen Meldepflichten dienen. Ein sicherheitsrelevantes Ereignis kann somit mehrere Meldepflichten auslösen. Es lässt sich ohne Weiteres festhalten, dass aufgrund der sich stetig zuspitzenden IT-Sicherheitslage eine Stärkung der Melde- und mithin der IT-Sicherheitspflichten zu begrüßen ist. Nur durch die Einführung und Umsetzung derartiger Pflichten wird der Aufbau eines validen Lagebildes zur IT-Sicherheit und ggf. das Ergreifen sich daran anschließender Maßnahmen seitens staatlicher Stellen ermöglicht. Verpflichtete sind angehalten, die für sie einschlägigen Pflichten zu kennen und entsprechend umzusetzen. Zu beachten ist allerdings, dass bei der Normierung der Meldepflichten stets ein Eingriff in die Rechtssphäre der gesetzlichen Adressaten vorliegt, weshalb die betroffenen Rechtsgüter in einen schonenden Ausgleich, bspw. durch das Eingreifen von Verwertungsverboten, zu bringen sind.

Alexander Weidenhammer
ist als Rechtsanwalt im Dresdner Institut für Datenschutz als externer Datenschutz- und Informationssicherheitsbeauftragter tätig. Zu den Beratungsschwerpunkten zählt das Recht der Informationssicherheit, insbesondere das Datenschutzrecht.

81 *Deusch/Eggendorfer*, K&R 2024, 169, 170.
82 *Deusch/Eggendorfer*, K&R 2024, 169, 170.
83 Referentenentwurf v 3. 7. 2023, abrufbar unter: https://ag.kritis.info/2024/03/07/referentenentwurf-des-bmi-nis-2-umsetzungs-und-cybersicherheitsstaerkungsgesetz-nis2umsucg/.
84 Diskussionspapier des BMI, Wirtschaftsbezogene Regelungen zur Umsetzung der NIS-2-Richtlinie in Deutschland v. 27. 9. 2023, abrufbar unter: https://ag.kritis.info/wp-content/uploads/2023/09/Anlage-2-Diskussionspapier.pdf.
85 *Schmidt*, K&R 2023, 705, 709.
86 *Voigt/Schmalenberger*, CR 2023, 717.
87 *Kipker/Dittrich*, MMR 2023, 481, 484.
88 *Kipker/Dittrich*, MMR 2023, 481, 484.
89 *Deusch/Eggendorfer*, K&R 2024, 169, 170.
90 *Deusch/Eggendorfer*, K&R 2024, 169, 174.

Prof. Dr. Tobias Gostomzyk und Dr. Jan Martin Rensinghoff*

Zehn Jahre Recht auf Vergessenwerden – Alles klar beim digitalen Neustart?

Kurz und Knapp

Jahrestage bieten Gelegenheit, voraus- und zurückzuschauen. Das gilt auch für das Recht auf Vergessenwerden. Es feiert sein zehnjähriges Bestehen. Der Beitrag möchte an diese Rechtsentwicklung erinnern und einen Ausblick geben – zumal die Geschichte des Rechts auf Vergessenwerden unter digitalen Netzwerkbedingungen weiter fortgeschrieben werden wird.

* Mehr über den Autor erfahren Sie am Ende des Beitrags. Alle zitierten Internetquellen wurden zuletzt abgerufen am 17. 4. 2024.