Die NIS-2-Richtlinie der EU und ihre Umsetzung in nationales Recht – Neue Vorgaben zur Cybersicherheit in der Arztpraxis ab 2025

1. Einleitung

Cyberangriffe nehmen weltweit zu. Auch Gesundheitseinrichtungen sind vermehrt betroffen. Ein zentraler IT-Knotenpunkt des Gesundheitswesens ist die Telematikinfrastruktur (TI). Sie ist das Kommunikationsnetzwerk im deutschen Gesundheitssystem, wird regelmäßig kontrolliert und orientiert sich an strengen Spezifikationen. Die Sicherheitslage der IT-Infrastruktur von Arztpraxen in Deutschland hingegen wird bisher kaum erfasst, obwohl sie essenziell für die Verarbeitung sensibler Daten und direkt an die TI angeschlossen sind.

Bei Cyberangriffen unter Verwendung einer sog. Ransomware[1] beobachtet das Bundesamt für Sicherheit in der Informationstechnik („*BSI*“) insgesamt eine Verlagerung der Attacken. Waren früher meist nur große, zahlungskräftige Unternehmen betroffen, sehen sich nunmehr zunehmend auch kleine und mittlere Unternehmen mit einer Bedrohung durch Ransomware-Angriffe konfrontiert.[2] Abgesehen von Ransomware existieren weitere zahlreiche Schadprogramme, welche die IT-Sicherheit von Unternehmen bedrohen. Die Varianten der entwickelten Schadprogramme wachsen dabei täglich (▶ **Abb. 1**).

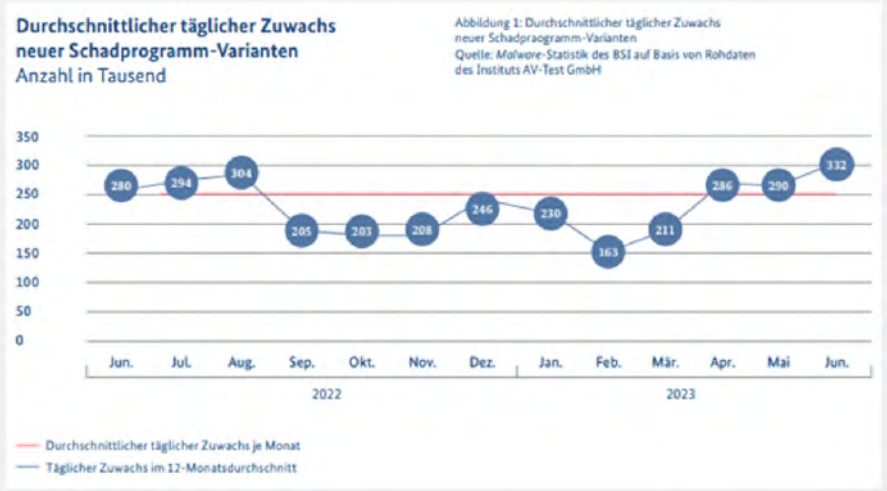
Mit der im Dezember 2022 im EU-Amtsblatt veröffentlichten zweiten EU-Richtlinie zur Netzwerk- und Informationssicherheit („*NIS-2-Richtlinie*“) erweitert die EU daher die Vorgaben an die Mitgliedsstaaten hinsichtlich der Anforderungen an die Cybersicherheit. Bis zum 17.10.2024 müssen alle EU-Mitgliedsstaaten die NIS-2-Richtlinie in nationales Recht implementieren. Die Bundesrepublik Deutschland kommt dieser Verpflichtung durch das NIS-2-Umsetzungs-und Cybersicherheitsstärkungsgesetz („*NIS2UmsuCG*“) nach. Das NIS2UmsuCG wurde noch nicht erlassen.[3] Es tritt nach abschließender Behandlung und Beschlussfassung im Bundestag zu dem im Gesetz genannten Termin in Kraft. Der genaue Termin des Inkrafttretens kann daher heute noch nicht genannt werden.

Der nachfolgende Beitrag beschäftigt sich mit der theoretischen und praktischen Bedeutung des NIS2UmsuCG, insbesondere mit Artikel 1, dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSIG), welches zukünftig auch für Einrichtungen im Gesundheitswesen gelten soll.

2. Betroffene medizinische Einrichtungen

Künftig sollen nicht mehr nur Krankenhäuser, Produktionsstätten für unmittelbar lebenserhaltende Medizinprodukte und ähnliches Einrichtungen[4] von Regulierungen in Bezug auf die IT-Sicherheit betroffen sein. Spätestens 2025 wird der Gesundheitssektor als „*Erbringer von Gesundheitsdienstleistungen im Sinne der Richtlinie (EU) 2011/24 des Europäischen Parlaments und des Rates vom 9. März 2011 über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung (ABl. L 88 vom 4.4.2011, S. 45)*“[5] auch Arztpraxen und Medizinische Versorgungszentren (MVZ) mitumfassen.

Bisher beinhaltet das aktuell geltende BSIG umfangreiche Vorgaben für Betreiber kritischer Infrastrukturen. Diese sind nach § 2 Abs. 10 BSIG Einrichtungen, Anlagen oder Teile davon, die dem Sektor Gesundheit



▶ **Abb. 1** Durchschnittlicher täglicher Zuwachs neuer Schadprogramm-Varianten.

1 Unter Ransomware wird eine spezielle Art schädlicher Software verstanden, die den Zugriff auf Geräte sperrt oder darauf enthaltene Daten verschlüsselt und anschließend vom Opfer ein Lösegeld für die Wiederherstellung verlangt.

2 Bundesamt für Sicherheit in der Informationstechnik, Bericht zur Lage der IT-Sicherheit in Deutschland 2023, S. 11.

3 Bislang liegt der Gesetzentwurf der Bundesregierung zum NIS2UmsuCG vom 22.07.2024 vor, der in Art. 33 kein Datum für ein Inkrafttreten benennt.

4 Teil 1 Ziffer 1 des Anhangs 5 zu § 1 Nummer 4 und 5; § 6 Abs. 6 Nummer 1 und 2 der BSI-Kritis-Verordnung.

5 Entwurf der Anlage 1 Nr. 4.1.1 BSIG.

Fortschr Röntgenstr 2024; 196: 1186–1190

angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind. Welche Infrastruktur konkret als kritisch anzusehen ist, bestimmt die BSI-Kritisverordnung (BSI-KritisV).

Nach der Regelung in § 6 Abs. 1 Nr. 1 BSI-KritisV werden wegen ihrer besonderen Bedeutung für das Funktionieren des Gemeinwesens im Sektor Gesundheit kritische Dienstleistungen im Sinne des § 10 Absatz 1 Satz 1 des BSIG folgende Gesundheitseinrichtungen angesehen:

„1. die stationäre medizinische Versorgung;
2. die Versorgung mit unmittelbar lebenserhaltenden Medizinprodukten, die Verbrauchsgüter sind;
3. die Versorgung mit verschreibungspflichtigen Arzneimitteln und Blut- und Plasmakonzentraten zur Anwendung im oder am menschlichen Körper;
4. die Laboratoriumsdiagnostik."

In der ambulanten Versorgung sind daher gegenwärtig lediglich Krankenhäuser und laborärztliche Praxen in den Geltungsbereich des BSIG einbezogen. Dies wird sich mit dem geplanten Inkrafttreten des neuen BSIG ändern. Erstmalig wird der Gesetzgeber auch die IT-Sicherheit von sog. „*wichtigen*" und „*besonders wichtigen Einrichtungen*" regulieren. Dies resultiert aus Artikel 3 der von der EU beschlossenen NIS-2-Richtlinie. Der nationale Gesetzgeber wurde durch die EU angewiesen, Einrichtungen in *besonders wichtig* und *wichtig* zu kategorisieren. Hierbei soll gemäß den Vorgaben der EU der Grad der Kritikalität in Bezug auf den Sektor, die Art der erbrachten Dienstleitungen sowie die Betriebsgröße berücksichtigt werden.[6]

Diesen Vorgaben der EU entsprechend werden in dem Gesetzesentwurf der Bundesregierung in § 28 BSIG (E-BReG[7]) die besonders wichtigen Einrichtungen und wichtige Einrichtungen aufgeführt. Nach § 28 Abs. 2 Nr. 3 BSIG (E-BReG) sollen folgende natürliche und juristische Personen als *wichtige Einrichtungen* gelten:

„natürliche oder juristische Personen oder rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft, die anderen natürlichen oder juristischen Personen entgeltlich Waren oder Dienstleistungen anbietet, die einer in den Anlagen 1 und 2 bestimmten Einrichtungsarten zuzuordnen sind und die Mindestens 50 Mitarbeiter beschäftigen oder einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro ausweisen."

Damit werden nach Inkrafttreten des NIS2UmsuCG nicht mehr nur Krankenhäuser von den Vorschriften über Cybersicherheit nach dem BSIG erfasst, sondern auch umsatzstarke Praxen, MVZ sowie Berufsausübungsgemeinschaften (BAG). Gerade ein kapitalintensives Fachgebiet wie die Radiologie wird daher durch die Anforderungen und möglichen Sanktionen des BSIG zukünftig betroffen sein.

3. Pflichten und Haftung

a. Registrierungspflicht wichtiger Einrichtungen

Unternehmen sollten die zukünftige Registrierungspflicht nach § 33 Abs. 1 BSIG (E-BReG) beachten. Spätestens drei Monate nachdem eine *wichtige Einrichtung* als solche gilt, hat diese sich über Registrierungsstellen zu registrieren, die nach Inkrafttreten des Gesetzes eingerichtet werden sollen.

Erfolgt eine Registrierung nicht innerhalb der dreimonatigen Frist, nicht richtig oder nicht vollständig, so kann gegen das Unternehmen ein Bußgeld in Höhe von bis zu 500.000,00 Euro nach § 61 Abs. 5 Nr. 4 BSIG (E-BReG) festgesetzt werden.

b. Maßnahmen des Risikomanagements

Insbesondere hinsichtlich des Risikomanagements stellt das BSIG (E-BReG) an die *wichtigen Einrichtungen* erhöhte Anforderungen.

Nach § 30 Abs. 1 BSIG (E-BReG) sind Praxen, MVZ und BAGs, die als besonders wichtige Einrichtungen oder wichtige Einrichtungen gelten, künftig verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen zu ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten. Geeignete Maßnahmen können beispielsweise ein Backup-Management, Konzepte in Bezug auf die Sicherheitsanalyse oder etwa grundlegende Verfahren im Bereich der Cyberhygiene sowie Schulungen im Bereich der Sicherheit in der Informationstechnik gemäß § 30 Abs. 2 BSIG (E-BReG) darstellen. Die Einhaltung dieser Verpflichtung ist zudem durch das Unternehmen zu dokumentieren. In der Praxis könnte es sich problematisch auswirken, dass das Gesetz die konkrete Ausgestaltung des Risikomanagements offenlässt. Eine Überprüfung der Geeignetheit der Maßnahmen durch eine Feststellung der zuständigen Bundesbehörde ist nach Absatz 8 der Norm lediglich für *besonders wichtige Einrichtungen* möglich.

Damit keine unverhältnismäßigen finanziellen und administrativen Belastungen für *wichtige Einrichtungen* entstehen, sollen nach der Gesetzesbegründung die im Gesetzesentwurf genannten Maßnahmen in einem angemessenen Verhältnis zu den Risiken stehen, denen das betroffene Netz- und Informationssystem ausgesetzt wird. Hierbei soll u. a. den Kosten der Umsetzung sowie der Größe der Einrichtung Rechnung getragen werden. Ebenfalls könnte in die Bewertung der Angemessenheit und Verhältnismäßigkeit wegen der unterschiedlichen Grade an Risikoexposition einfließen, ob es sich um eine *wichtige Einrichtung*, eine *besonders wichtige* im Vergleich zu einer *wesentlichen Einrichtung* oder einem Betreiber einer *kritischen Anlage* handelt.[8] In der Praxis könnte dies zu erheblichen Schwierigkeiten in der Umsetzung führen, da die Bewertung der Geeignetheit des Risikomanagement durch eine verantwortliche Person im Unternehmen zu erfolgen hat. Kommt das Unternehmen nämlich der Verpflichtung zur Ergreifung geeigneter Maßnahmen zum Risikomanagement oder

6 Absatz 15 der Erwägungsgründe der NIS-2-Richtlinie.

7 Der Gesetzestext liegt bislang lediglich als Gesetzentwurf der Bundesregierung vor (Bearbeitungsstand: 22.07.2024).

8 Gesetzesentwurf der Bundesregierung, NIS2UmsuCG, Bearbeitungsstand: 22.07.2024, S. 160.

der Pflicht zur Dokumentation der Maßnahmen vorsätzlich oder fahrlässig nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig nach, droht dem Unternehmen nach § 61 Abs. 2 Nr. 2, Abs. 5 Nr. 2b) BSIG (E-BReG) ein Bußgeld in einer Höhe von bis zu 7.000.000,00 Euro.

c. Pflichten und Haftung der Geschäftsleitung

Besonders weitreichend sind zudem die Pflichten der Geschäftsleitung besonders wichtiger Einrichtungen und wichtiger Einrichtungen ausgestaltet. Dieser obliegt nach § 38 BSIG (E-BReG) einer Umsetzungs-, Überwachungs- und Schulungspflicht. Der Geschäftsführer hat demnach die konkret zu ergreifenden Maßnahmen als geeignet zu billigen und deren Umsetzung zu überwachen. Auch bei Einschaltung von Hilfspersonen für die Umsetzung und Überwachung soll die Geschäftsleitung als Organ letztverantwortlich sein.[9]

Zudem hat die Geschäftsleitung regelmäßig an Schulungen teilzunehmen. Ziel der Schulungen soll die Vermittlung ausreichender Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie von Risikomanagementpraktiken im Bereich der Sicherheit der Informationstechnik sein. Des Weiteren soll künftig der Geschäftsführer befähigt sein, Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste zu beurteilen.

Kommt der Geschäftsführer seiner Umsetzungs- und Überwachungspflicht nicht in ausreichendem Maße nach, drohen nicht unerhebliche Haftungsrisiken. Grundsätzlich gestaltet das BSIG (E-BReG) die Haftung der Geschäftsleitung gegenüber der Gesellschaft als sog. Binnenhaftung nach den allgemeinen Grundsätzen der Haftung der jeweiligen gewählten Gesellschaftsform aus.[10] Medizinische Einrichtungen in der ambulanten Versorgung werden häufig als BAG[11] (vgl. § 33 Abs. 2 Ärzte-ZV) oder als MVZ in Trägerschaft einer Gesellschaft mit beschränkter Haftung (GmbH), einer Partnerschaftsgesellschaft (PartG) sowie als Gesellschaft bürgerlichen Rechts (GbR) betrieben (vgl. § 95 Abs. 1a S. 3 Sozialgesetzbuch 5 (SGB V)). Allen gemein ist, dass die Geschäftsleitung der Gesellschaft für vorsätzliches oder fahrlässiges Handeln haften soll.

aa. GmbH

Die Haftung des Geschäftsführers einer GmbH bestimmt sich im Allgemeinen[12] nach den Voraussetzungen des § 43 Abs. 1 GmbHG. Die Geschäftsführung schuldet der Gesellschaft die Sorgfalt, die ein ordentlicher Geschäftsmann in verantwortlich leitender Position bei ständiger Wahrnehmung fremder Vermögensinteressen zu wahren hat. Damit enthält § 43 Abs. 1 GmbHG einerseits einen allgemeinen Auffangtatbestand für alle Pflichtverletzungen des Geschäftsführers gegen die Gesellschaft und konkretisiert den allgemeinen Sorgfaltsmaßstab nach § 276 Abs. 1 S. 2 BGB, wonach der Schuldner Vorsatz und Fahrlässigkeit zu vertreten hat.[13] Bei Verletzung dieser Sorgfaltspflicht haftet der Geschäftsführer[14] gegenüber der Gesellschaft in Höhe des der Gesellschaft entstandenen Schadens mit seinem Privatvermögen, vgl. § 43 Abs. 2 GmbHG.

bb. PartG

Das Partnerschaftsgesellschaftsgesetz (PartGG) enthält hingegen keine Norm, welche die Haftung der Geschäftsleitung gegenüber der Partnerschaftsgesellschaft explizit regelt. Insoweit greift für diesen Fall zukünftig § 38 Abs. 2 BSIG (E-BReG) als sog. Auffangtatbestand.[15] Nach dem Wortlaut der Norm haftet die Geschäftsleitung der Gesellschaft für den *„schuldhaft verursachten Schaden“*. Der Begriff schuldhaft bzw. Verschulden ist hierbei als Oberbegriff für vorsätzliches oder fahrlässiges Verhalten zu verstehen.[16]

cc. GbR

Das Bürgerliche Gesetzbuch (BGB) enthält für die GbR keine Vorschriften hinsichtlich einer Haftung des geschäftsführenden Gesellschafters gegenüber der GbR. In diesem Fall gilt künftig, dass die Geschäftsleitung der Gesellschaft für den schuldhaft verursachten Schaden nach § 38 Abs. 2 BSIG (E-BReG) haftet.

d. Umfassende Meldepflichten

Das BSIG (E-BReG) sieht für den Eintritt eines sog. erheblichen Sicherheitsvorfalls umfassende Meldepflichten an das zuständige Bundesamt für Sicherheit in der Informationstechnik (BSI) nach § 32 BSIG (E-BReG) vor. Für jeden eingetretenen erheblichen Sicherheitsvorfall sind insgesamt mindestens drei Meldungen abzugeben.

Von einem erheblichen Sicherheitsvorfall ist nach § 2 Nr. 11 BSIG (E-BReG) auszugehen, wenn ein Sicherheitsvorfall schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat, verursachen kann oder andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann, sofern durch eine Rechtsverordnung nach § 56 Abs. 5 BSIG (E-BReG) keine konkretisierende Begriffsbestimmung erfolgt.

Das Unternehmen ist demnach verpflichtet, im Falle eines erheblichen Sicherheitsvorfalles unverzüglich, d. h. ohne schuldhafte Verzögerung nach Kenntniserlangung, spätestens innerhalb von 24 Stunden, eine Erstmeldung an das BSI abzugeben. Die Erstmeldung sollte enthalten:

9 Gesetzesentwurf der Bundesregierung, NIS2UmsuCG, Bearbeitungsstand: 22.07.2024, S. 168.

10 Gesetzesentwurf der Bundesregierung, NIS2UmsuCG, Bearbeitungsstand: 22.07.2024, S. 169.

11 Eine BAG nach § 18 Abs. 2a MBO-Ä und § 33 Abs. 2 Ärzte-ZV kann nur in den Rechtsformen einer GbR oder PartG betrieben werden.

12 Weitere Normen, welche die Haftung des Geschäftsführers gegenüber der Gesellschaft regeln, sind §§ 9a Abs. 1, 31 Abs. 6 57 Abs. 4, 64 Abs. 1 GmbHG.

13 *Schaal*, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, Werkstand: 252. EL Juni 2024, § 43 GmbHG, Rn. 2.

14 Bei mehreren Geschäftsführern haften diese als Gesamtschuldner, Vgl. § 43 Abs. 2 GmbHG.

15 Gesetzesentwurf der Bundesregierung, NIS2UmsuCG, Bearbeitungsstand: 22.07.2024, S. 169.

16 *Lorenz*, in: Hau/Poseck, BeckOK, 71. Edition, Stand: 01.08.2024, § 276 BGB, Rn. 5; BT-Drs. 14/6040, S. 131.

Fortschr Röntgenstr 2024; 196: 1186–1190

- Verdacht, dass der erhebliche Sicherheitsvorfall auf eine rechtswidrige oder böswillige Handlung zurückzuführen ist,
- ob aufgrund des Sicherheitsvorfalls grenzüberschreitende Auswirkungen drohen.

Unverzüglich, spätestens 72 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall, hat künftig eine Bestätigungsmeldung der zuvor genannten Verdachtsmeldung bei der Bundesbehörde zu erfolgen. Diese Meldung sollte folgende Informationen enthalten:

- Bestätigung über den Verdacht, dass der erhebliche Sicherheitsvorfall auf eine rechtswidrige oder böswillige Handlung zurückzuführen ist,
- Bestätigung, dass aufgrund des Sicherheitsvorfalls grenzüberschreitenden Auswirkungen drohen,
- eine erste Bewertung des erheblichen Sicherheitsvorfalls, einschließlich seines Schweregrades und seiner Auswirkungen,
- ggf. Angabe der Kompromittierungsindikatoren.

Spätestens einen Monat nach der Bestätigungsmeldung des erheblichen Sicherheitsvorfalls, hat künftig eine Abschlussmeldung zu erfolgen, welche folgenden Inhalt haben sollte:

- Ausführliche Beschreibung des Sicherheitsvorfalls, einschließlich des Schweregrades und der Auswirkungen,
- Angaben zur Art der Bedrohung und ihrer zugrundeliegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat,
- Angaben zu den getroffenen und laufenden Abhilfemaßnahmen,
- ggf. grenzüberschreitende Auswirkungen.

Für den Fall, dass der Sicherheitsvorfall noch andauert, sind Unternehmen nach § 32 Abs. 2 BSIG (E-BReG) verpflichtet, statt einer Abschlussmeldung eine Fortschrittsmeldung abzugeben.

Erfolgen die Meldungen nach § 32 Abs. 1 BSIG (E-BReG) oder entsprechende Abschlussmeldung für den Fall eines fortdauernden Sicherheitsvorfalls nach § 32 Abs. 2 S. 2 BSIG (E-BReG) nicht, nicht vollständig oder nicht rechtzeitig, kann die Ordnungswidrigkeit nach § 61 Abs. 2 Nr. 2, Abs. 5 Nr. 2b) BSIG (E-BReG) mit einem Bußgeld in Höhe von bis zu 7.000.000,00 Euro geahndet werden.

Auffallend ist, dass es bislang den verantwortlichen Personen im Unternehmen obliegt zu entscheiden, ob ein erheblicher Sicherheitsvorfall vorliegt. Die Norm enthält bisher keine Konkretisierung der Definition eines erheblichen Sicherheitsvorfalls. Auch entsprechende Rechtsverordnungen konkretisieren den Begriff bislang nicht. Gleichwohl stellt der Gesetzesentwurf klar, dass die Begriffsdefinition des erheblichen Sicherheitsvorfalls in § 2 Nr. 11 BSIG (E-BReG) einerseits der Umsetzung von Artikel 23 Abs. 3 und Abs. 11 UA 2 der NIS-2-Richtlinie dient und bei den genannten finanziellen Verlusten Bagatellschäden regelmäßig ausgeschlossen seien. Es wird offengelassen, bis zu welcher Grenze Bagatellschäden in Unternehmen mit einem Jahresumsatz von mehr als 10 Millionen Euro zu beziffern sind.[17]

Verantwortlichen Personen eines Unternehmens ist daher zu raten, jeden Angriff auf die IT-Infrastruktur als erheblichen Sicherheitsvorfall zu bewerten, da potentiell jeder Angriff geeignet sein könnte, schwerwiegende Betriebsstörungen oder finanzielle Verluste herbeizuführen.

e. Unterrichtungspflichten

Im Falle eines erheblichen Sicherheitsvorfalls kann das BSI gegenüber der betroffenen medizinischen Einrichtung zudem zukünftig gemäß § 35 BSIG (E-BReG) anordnen, die Empfänger ihrer Dienste unverzüglich über diesen Vorfall zu unterrichten. Hintergrund ist die Möglichkeit der Empfänger der jeweiligen Dienste selbst entsprechende Maßnahmen umzusetzen, um weitere Schadensauswirkungen auf eigene Dienste möglichst zu vermeiden.[18]

17 Gesetzesentwurf der Bundesregierung, NIS2UmsuCG, Bearbeitungsstand: 22.07.2024, S. 139.

18 Gesetzesentwurf der Bundesregierung, NIS2UmsuCG, Bearbeitungsstand: 22.07.2024, S. 166.

4. IT-Sicherheitsrichtlinie in Vertragsarztpraxen nach § 75b SGB V

Für Vertragsarztpraxen gilt daneben weiterhin die Regelung in § 75b SGB V, die durch das Digitale-Versorgungsgesetz (DVG) vom 09.12.2019[19] eingeführt worden ist. Bei vielen Vertragsarztpraxen handelt es sich um kleinere oder mittlere Unternehmen, die nicht in den Anwendungsbereich der Regeln des BSIG fallen, das die Gewährleistung der Sicherheit kritischer Infrastrukturen zum Ziel hat. Diese Lücke schließt § 75b SGB V, indem in den zu erlassenden Richtlinien verbindliche Vorgaben zur IT-Sicherheit in Arztpraxen zu treffen sind, die nach § 75b Abs. 2 S. 1 SGB V für die vertragsärztlichen Leistungserbringer verbindlich sind. Die Richtlinie der Kassenärztlichen Bundesvereinigung (KBV)[20] nach § 75b Abs. 1 SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit vom 16.12.2020 ist am 01.01.2021 in Kraft getreten.[21] Sie definiert, abgestuft nach der Größe der Praxis und abhängig von der Nutzung medizinischer Großgeräte, einzuhaltende Anforderungen. Diese ergeben sich je nach Praxis aus einer oder mehrerer Anlagen der Richtlinie. Aufgrund einer Evaluierung der IT-Sicherheitsrichtlinie durch das BSI im Jahr 2023 wurde festgestellt, dass die Anforderungen und Maßnahmen, die in der IT-Sicherheitsrichtlinie vorgegeben sind, derzeit nur in einem Drittel der Praxen vollumfänglich umgesetzt sind, obwohl es sich hierbei um gesetzliche Vorgaben handelt, die bis Juli 2022 hätten umgesetzt werden müssen.[22] Interessant dürfte daher sein, wie die Vorgaben in § 75b SGB V und dem noch zu verabschiedenden NIS2UmsuCG bei Arztpraxen, BAGs und

19 BGBl. I, S. 2562.

20 Für den vertragszahnärztlichen Bereich gilt die Richtlinie der KZBV: https://www.kzbv.de/datenschutz.91.de.html# (abgerufen am 01.10.2024).

21 https://www.kbv.de/html/it-sicherheit.php#:~:text=IT-Systeme%20und%20sensible%20Daten%20in%20den%20Praxen%20noch%20besser%20sch%C3%BCtzen: (abgerufen am 01.10.2024).

22 Bundesamt für Sicherheit in der Informationstechnik, Tätigkeitsbericht Gesundheit Cybersicherheit im Gesundheitswesen 2023, Stand April 2024, S. 17.

MVZ unterschiedlicher Größe zukünftig Geltung beanspruchen werden.

Das neue BSIG wird seine Geltung neben der IT-Sicherheitsrichtlinie der KBV nach § 75b SGB V beanspruchen. Während die Richtlinie der KBV nach § 75b SGB V den Schutz sensibler Gesundheitsdaten, Verpflichtungen zur regelmäßigen Überprüfung der Sicherheitsmaßnahmen sowie Schulungspflichten und Sensibilisierung des Personals, um Sicherheitslücken im IT-System durch menschliches Versagen zu minimieren, beinhaltet die Umsetzung der NIS-2-Richtlinie neue europaweite Standards für die IT-Sicherheit. Zweck des neuen BSIG ist nicht der Schutz sensibler Daten im Gesundheitswesen, vielmehr soll der Aufbau einer erhöhten Resilienz der IT-Systeme durch umfangreiche Verpflichtungen und Haftungstatbestände vorangetrieben werden. Das noch zu verabschiedende NIS2UmsuCG wird in den Anwendungsbereich fallende Unternehmen künftig zum Aufbau robuster IT-Systeme verpflichten, sodass diese auch bei Cyberangriffen und technischen Ausfällen funktionsfähig bleiben. Über diverse Meldeverpflichtungen, Kooperationen und Informationsaustausch von Bedrohungsinformationen zwischen den EU-Mitgliedstaaten wird sich die EU über NIS-2 zur gemeinsamen Abwehr von Cyberangriffen zusammenschließen. Für Vertragsarztpraxen, die auch dem Anwendungsbereich des neuen BSIG unterfallen, gilt daher, dass weitere Vorschriften betreffend die IT-Sicherheit zu beachten sein werden.

5. Fazit

Das im Rahmen des NIS2UmsuCG novellierte BSIG wird für Arztpraxen und MVZ, die dem Anwendungsbereich unterfallen, in naheliegender Zukunft umfassende Sicherheitsmaßnahmen im Bereich der Cybersicherheit vorschreiben. Gemeinsam mit neuen Dokumentations- und Meldepflichten sowie der Schaffung erweiterter Sanktionsvorschriften mit neuen Bußgeldtatbeständen greift das BSIG umfassend in den betrieblichen Ablauf und die Organisation betroffener Praxen und MVZ ein. Erstmalig werden sich nun auch mittlere Gesundheitseinrichtungen mit Vorschriften zur Cybersicherheit auseinandersetzen müssen. Daneben sind die Vorgaben der IT-Sicherheitsrichtlinie der KBV nach § 75b SGB V zu beachten. Im Hinblick auf die Verantwortlichkeit der Geschäftsleitung sollten sich Geschäftsführer sowie Gesellschafter bereits jetzt Gedanken zur praktischen Umsetzung der Regelungen innerhalb des Praxisalltages machen. Insbesondere die vorgesehenen Sanktionen sollten Verantwortliche betroffener medizinischer Einrichtungen anhalten, bereits jetzt Maßnahmen zum Qualitätsmanagement und zum Umgang mit den künftigen gesetzlichen Regelungen zu treffen, da das neue BSIG Praxen und MVZ sowohl vor personelle, organisatorische und technische Herausforderungen stellen wird.

Prof. Dr. Peter Wigge
Rechtsanwalt
Fachanwalt für Medizinrecht

Stefanie Kath
Rechtsanwältin

Rechtsanwälte Wigge
Großer Burstah 42
20 457 Hamburg
Telefon: (040) 33 98 705–90
Telefax: (040) 33 98 705–99
E-Mail: kanzlei@ra-wigge.de
www.ra-wigge.de

Fortschr Röntgenstr 2024; 196: 1186–1190