Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Evaluierung der IT-Sicherheitsrichtlinie in Arztpraxen

BSI-Projekt 598 - SiRiPrax

Änderungshistorie

Version	*Datum*	*Name*	*Beschreibung*
1.0	19.01.2024	BSI	Finalisierung

Tabelle 1: Änderungshistorie

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
E-Mail: referat-di24@bsi.bund.de
Internet: https://www.bsi.bund.de

Management Summary

Die IT-Sicherheitsrichtlinie gem. § 75b SGB V[1] definiert Mindestanforderungen an die IT-Sicherheit für einen sicheren Betrieb in Arztpraxen. Das Bundesamt für Sicherheit in der Informationstechnik führte im Rahmen der gesetzlich vorgeschriebenen Evaluation von März bis Mai 2023 eine Umfrage zur IT-Sicherheit in Praxen, vor dem Hintergrund dieser IT-Sicherheitsrichtlinie, durch. Die ca. 1.600 Rückmeldungen der Befragten stellen einen Einblick in die derzeitige Berücksichtigung von IT-Sicherheit im Versorgungsalltag dar.

Arztpraxen verfügen über eine recht große Anzahl an technischen, digitalen und medizinischen Geräten, die in einem Netzwerk eingebunden oder extern verwendet werden. Des Weiteren arbeiten sie mit unterschiedlichen Programmen und branchenspezifischer Software.

Die meisten Befragten sind um Sicherung und Schutz ihrer Daten bemüht und halten sich bei diesem Thema für gut informiert. In fast jeder Praxis gibt es einen IT-Sicherheitsbeauftragten.

Dennoch verweist die durchwachsene Bekanntheit der IT-Richtlinie nach § 75b SGB V und ihrer Umsetzung darauf, dass das Thema und seine Bedeutung viele Praxen noch nicht erreicht hat.

Dass die Vorgaben aktuell nur in einem Drittel der Praxen vollumfänglich umgesetzt wurden, scheint zum einen mit Verständnisproblemen hinsichtlich der Vorgaben und Zweifel an deren Nutzen zu tun zu haben, zum anderen mit fehlendem oder unzureichendem Budget, Personal und Zeit. Möglicherweise empfinden viele Praxen zudem keine große Dringlichkeit, da sie meistens noch keinen IT-Sicherheitsvorfall hatten.

Die flächendeckende Umsetzung der Richtlinie zur Etablierung eines Mindestschutzes bei den Arztpraxen bedarf weiterer Anstrengungen, damit bestehende Hürden, wie Verständnisprobleme oder unklare Umsetzungen ausgeräumt werden können.

[1] Nach Verabschiedung des Digital-Gesetzes wird der Sachverhalt (Richtlinie zur IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung) zukünftig nicht mehr unter § 75b SGB V aufgeführt, sondern unter § 390. Um Verwirrungen vorzubeugen, wird in diesem Dokument weiterhin von § 75b SGB V vor der Verabschiedung des Digital-Gesetzes gesprochen und die damit einhergehenden Richtlinien (Richtlinie nach § 75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit) der Kassenärztlichen Bundesvereinigung (KBV) und der Kassenzahnärztlichen Bundesvereinigung (KZBV) veröffentlichten Richtlinien thematisiert.

Inhalt

1 Einleitung

Die Digitalisierung im Gesundheitswesen wird nicht zuletzt seit der Einführung der Telematikinfrastruktur vorangetrieben. Unterschiedliche digitale Anwendungen sollen dabei eine Vielzahl an Verbesserungen für die Kostenträger, die Versicherten und die Leistungserbringer gewährleisten. Bei der Nutzung der Fülle an unterschiedlichen Anwendungen ist auch die Einhaltung ausreichender Sicherheitsmaßnahmen unabdingbar. Diese beginnen bereits bei der Entwicklung für Anwendungen im Gesundheitskontext. Die grundlegenden Sicherheitseigenschaften von Anwendungen müssen jedoch stets durch begleitende Maßnahmen bei Nutzenden ergänzt werden.

Im Kontext der gesetzlich zugesicherten Gesundheitsversorgung definieren die Kassenärztliche Bundesvereinigung (KBV) und die Kassenzahnärztliche Bundesvereinigung (KZBV) im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) angemessene Sicherheitsmaßnahmen für Leistungserbringer in der ambulanten Versorgung. Neben der Definition dieser Maßnahmen und Anforderungen in der „Richtlinie nach § 75b SGB V[2] über die Anforderungen zur Gewährleistung der IT-Sicherheit“ (vgl. KBV 2020 bzw. KZBV 2021) sind regelmäßige Evaluationen dieser Richtlinie gesetzlich vorgesehen.

Maßgeblich für die Etablierung einer ausreichenden und flächendeckenden IT-Sicherheit in Praxen ist neben der Angemessenheit der Anforderungen ebenfalls die Anwendbarkeit. Diese Anwendbarkeit ist stets auch von der allgemeinen Verständlichkeit der Anforderungen abhängig. Um einen Einblick in die bisherige Umsetzung und die Verständlichkeit der 2020 veröffentlichten IT-Sicherheitsrichtlinie zu erlangen, hat das BSI im Nachgang der belastenden Corona-Pandemie eine Befragung bei den Leistungserbringenden in der ambulanten Versorgung in Auftrag gegeben.

Das Vorgehen und die Ergebnisse, der von März bis Mai 2023 durchgeführten Befragung, werden in diesem Dokument vorgestellt. Hierzu wird zunächst die Ausgangslage und relevante Fragestellungen benannt, das Untersuchungsdesign der Befragung dargestellt und eine Einordnung der teilgenommenen Arztpraxen präsentiert. Anschließend werden die Ergebnisse zu einzelnen Fragestellungen dargelegt und schließlich eine Interpretation der Umfrageergebnisse vorgenommen.

[2] Nach Verabschiedung des Digital-Gesetzes wird der Sachverhalt (Richtlinie zur IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung) zukünftig nicht mehr unter § 75b SGB V aufgeführt, sondern unter § 390. Um Verwirrungen vorzubeugen, wird in diesem Dokument weiterhin von § 75b SGB V vor der Verabschiedung des Digital-Gesetzes gesprochen und die damit einhergehenden Richtlinien (Richtlinie nach § 75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit) der Kassenärztlichen Bundesvereinigung (KBV) und der Kassenzahnärztlichen Bundesvereinigung (KZBV) veröffentlichten Richtlinien thematisiert.

2 Hintergrund und Ausgangslage der Untersuchung

Die IT-Sicherheit in Arztpraxen soll durch die in der IT-Sicherheitsrichtlinie gem. § 75b SGB V definierten Mindeststandards erhöht werden. Damit diese Mindeststandards verbessert werden können, ist eine Betrachtung der aktuellen Umsetzung unabdingbar. Grundlegend für eine Verbesserung der vorherrschenden IT-Sicherheit sind Fragestellungen, die sich der bisherigen Umsetzung, der Verständlichkeit und der Hilfeleistung durch die Richtlinie widmen. Um Einblicke in die bisherige Umsetzung und die Verständlichkeit der Richtlinie bei den Leistungserbringern zu erlangen, hat das BSI eine Online-Befragung in deutschen Arztpraxen in Auftrag gegeben. Hierbei wurden die beiden folgenden Themenfelder inhaltlich abdeckt:

- Gewinnung von Informationen zur derzeitigen Umsetzung der IT-Sicherheitsrichtlinie nach §°75b°SGB V
- Erhebung grundsätzlicher Parameter zur IT-Sicherheit in den teilnehmenden Praxen.

2.1 Untersuchungsdesign

Bei der durchgeführten Online-Befragung konnten nicht mit vertretbarem Aufwand alle deutschlandweit tätigen Arzt- und Zahnarztpraxen befragt werden. Daher wurde aus dieser Grundgesamtheit eine Zufalls-Bruttostichprobe von 12.000 Praxen ausgewählt und schriftlich-postalisch angeschrieben. Die anschließende Befragung wurde online mittels eines Fragebogens durchgeführt (CAWI = Computer assisted Web Interviewing).

Die aus der Befragung resultierenden Rückmeldungen von 1.591 Arztpraxen wurden, im Rahmen der Datenaufbereitung und Auswertung, komplex nach den folgenden Merkmalen, an die aus der amtlichen Statistik sowie der Rohstichprobe bekannten Sollstrukturen, ausgewertet:

- Einzelpraxis/ Gemeinschaftspraxis/ Praxisgemeinschaft,
- Fachgebiet,
- Alter, Geschlecht
- und Bundesland

2.2 Soziogramm

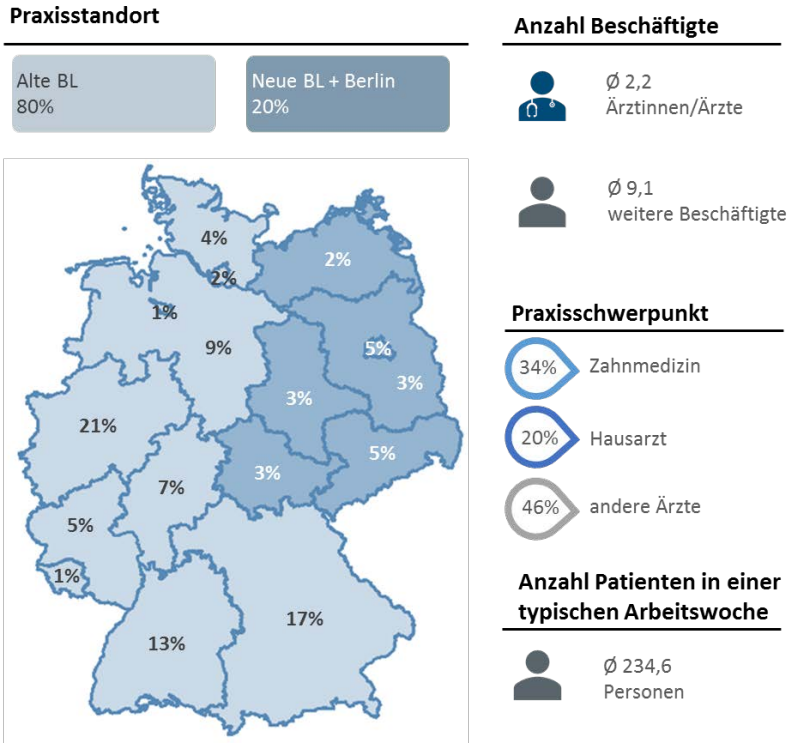

Abbildung 1:Informationen zu den befragten Praxen (Praxisstandort, Anzahl der Beschäftigten, Praxisschwerpunkt, Anzahl Patienten in einer typischen Arbeitswoche, n=1.591)

Bei der Auswertung zeigte sich eine hohe Beteiligung von Zahnarztpraxen. Diese sind mit 34 Prozent vertreten. In Abbildung 1 sind die Ergebnisse grafisch dargestellt. Des Weiteren nahmen 20 Prozent an Hausärztinnen und -ärzten an der Umfrage teil und 46 Prozent aus weiteren Arztpraxen. Fast alle Praxen (97°%) haben angegeben, dass sie sich eigenständig verwalten.

Da bei der Umfrage der Fokus auf den nach IT-Sicherheitsrichtlinie definierten ‚kleinen' Praxen liegt, sind bei den Befragten im Durchschnitt zwei Ärztinnen oder Ärzte und neun Mitarbeitende beschäftigt.

Bei der Teilnahme zeigte sich, dass die meisten Arztpraxen aus den drei einwohnerstärksten Bundesländern Nordrhein-Westfalen, Bayern und Baden-Württemberg kommen (siehe rote Markierung in Abbildung1). Diese drei Bundesländer sind mit 51°Prozent der befragten Praxen vertreten. Zudem zeigte sich bei der Erstellung des Soziograms, dass über 80°Prozent in Groß- oder Kleinstädten angesiedelt sind. Arztpraxen, die auf dem Land oder in Vororten von Städten liegen, haben nur sehr geringfügig an der Umfrage teilgenommen.

Über die Hälfte der Befragten ist über 55 Jahre alt (54 %). 30 Prozent gehören der Altersgruppe 45 bis 54 Jahre an, jünger als 45 Jahre sind lediglich 17 Prozent.

3 IT-Sicherheitsrichtlinie und IT-Strukturen

Die Umfrage wurde jeweils von einer Person aus den teilnehmenden Arztpraxen beantwortet. Diese Antworten dienen einer realistischen Einschätzung bezüglich der verwendeten IT und der allgemeinen Berücksichtigung der IT-Sicherheitsrichtlinie im Versorgungskontext des ambulanten Gesundheitswesens. Dabei widmen sich die einzelnen Fragen der Umsetzung, Bekanntheit und Verständlichkeit der IT-Sicherheitsrichtlinie sowie der grundlegenden Ausstattung mit IT, der Nutzung vorhandener IT und bestehender digitaler Anwendungen für die Leistungserbringer.

Die vorliegende Auswertung gründet auf den Umfrageergebnissen zu diesen einzelnen Fragestellungen und kombiniert diese Erkenntnisse zu einzelnen Themenblöcken.

3.1 Umsetzung, Bekanntheit und Verständlichkeit

Mit Rückmeldungen von rund 1.600 Arztpraxen zeigte sich ein hohes Interesse, das Thema IT-Sicherheit in den Praxen zu verbessern. Mit 79 Prozent haben mehrheitlich Ärztinnen und Ärzte die Beantwortung des Fragebogens wahrgenommen. Die übrigen Befragten sind Praxismitarbeitende, vor allem medizinische Fachangestellte und Angestellte in der Verwaltung sowie dem Praxis-Management. Bei lediglich einem Prozent der Praxen antworteten externe Dienstleister. Die meisten Befragten haben den hohen Stellenwert der Sicherung und des Schutzes ihrer Daten erkannt und halten sich bei diesem Thema für gut informiert. In fast jeder Praxis widmet sich ein IT-Sicherheitsbeauftragter der Thematik. Diese Zuständigkeit beeinflusst die IT-Sicherheit in der Praxis positiv. Jedoch ist hierbei eindeutig hervorzuheben, dass die verantwortlichen Personen in der Regel fachfremd sind und die Aufgaben im Bereich der IT-Sicherheit neben ihrer beruflichen Tätigkeit erledigen. Obwohl die Befragten sich mehrheitlich als gut informiert einschätzen, zeigt die Umfrage, dass das Thema IT-Sicherheit und seine Bedeutung viele Praxen noch nicht erreicht hat. Aus den meisten Rückmeldungen geht hervor, dass eine eher geringe Bekanntheit der IT-Richtlinie nach §°75b SGB V und ihrer Umsetzung vorherrscht (vgl. Abbildung 2).

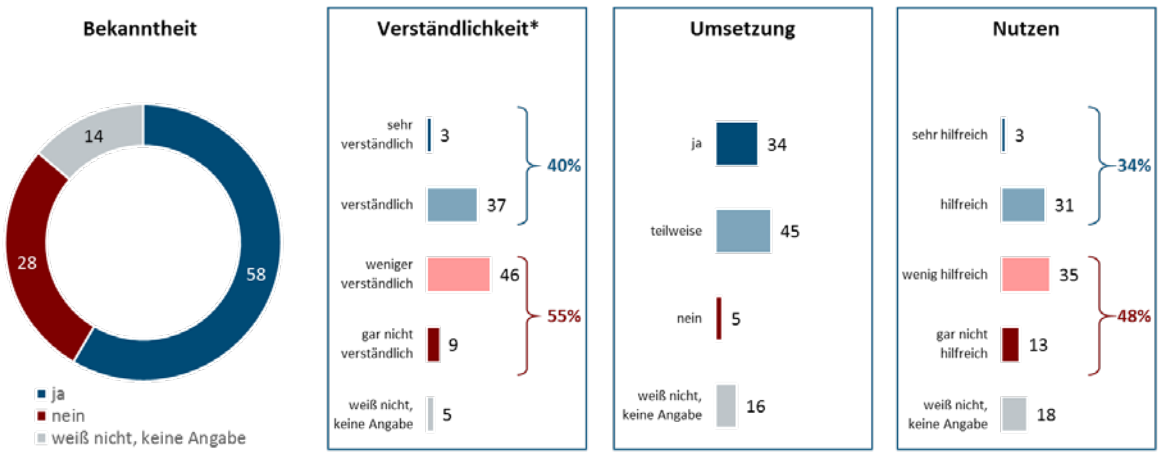

*Abbildung 2: Überblick der IT-Sicherheitsrichtlinie nach § 75b SGB V nach Bekanntheit, Verständlichkeit, Umsetzungsgrad und Nutzen (Angaben in %, n=1.591, *n=957)*

Die Anforderungen und Maßnahmen, die in der IT-Sicherheitsrichtlinie vorgegeben sind, sind derzeit nur in einem Drittel der Praxen vollumfänglich umgesetzt, obwohl es sich hierbei um gesetzliche Vorgaben handelt, die bis Juli 2022 hätten umgesetzt werden müssen. Die Antworten der Befragten verdeutlichen maßgeblich bestehende Schwierigkeiten bei der Umsetzung der IT-Sicherheitsrichtlinie für die verantwortlichen Praxisinhaber und Leistungserbringer. Einerseits bestehen Verständnisprobleme hinsichtlich der Vorgaben sowie grundsätzliche Zweifel am Nutzen der IT-Sicherheitsrichtlinie. Zum anderen mangelt es am Budget bei den Ärztinnen und Ärzten zur Ertüchtigung der jeweiligen IT-Infrastruktur, da Kosten, die durch die Realisierung einer effizienten/ausreichenden IT-Sicherheit anfallen,

eigenständig von der jeweiligen Praxis getragen werden müssen. Des Weiteren mangelt es an notwendigem Fachwissen sowie Zeit für die Umsetzung durch das Personal. Viele der befragten Praxen empfinden bei der Umsetzung der IT-Sicherheitsrichtlinie keine große Dringlichkeit, da sie meistens noch von keinem IT-Sicherheitsvorfall betroffen waren.

> *Für IT-Sicherheit im Versorgungskontext muss ein größeres Problembewusstsein geschaffen, sowie die Bekanntheit der IT-Sicherheitsrichtlinie gefördert werden. Um dies zu erreichen und somit auch eine Realisierung der Umsetzung, müssen die Anforderungen und Maßnahmen verständlich und anschaulich vermittelt werden.*

3.2 IT-Ausstattung und deren Nutzen

Mit Blick auf die IT-Ausstattung und deren Nutzung zeigt sich, dass die meisten Praxen erste Sicherheitsvorkehrungen getroffen haben.

In der IT-Sicherheitsrichtlinie gem. § 75b SGB V wird eine regelmäßige Datensicherung gefordert, ob dies jedoch manuell oder automatisch und wie oft erfolgen soll, ist nicht beschrieben. Die Studie hat gezeigt, dass fast jede Praxis regelmäßig automatisiert sowie manuell Sicherungskopien von wichtigen Daten anlegt.

> *Eine regelmäßige und richtige Datensicherung ist essentiell, um im Ernstfall, beispielsweise aufgrund eines IT-Sicherheitsvorfalls, wieder schnellstmöglich auf alle Daten zugreifen zu können und den Datenverlust zu minimieren.*

Schützenswerte Daten, wie es Gesundheitsdaten sind, müssen besonders vertraulich behandelt werden. Dies bedeutet, dass sie mit Hilfe einer Datenverschlüsselung so geschützt werden, dass Dritte diese Daten nicht mitlesen oder ausspionieren können. Nach den Ergebnissen der Umfrage verschlüsseln zwei Drittel aller Praxen ihre Daten regelmäßig, bevor diese lokal gespeichert oder versendet werden. Bei lediglich vier von zehn Praxen ist die Datenverschlüsselung ein Standardvorgehen. Es zeigt sich, dass besonders Zahnarztpraxen und Praxen mit sehr gutem IT-Informationsstand am engagiertesten bei der Verschlüsselung von Daten sind.

> *Verschlüsselung von Daten, ganz gleich wie die weitere Verarbeitung der Daten aussieht, sollte das Standardvorgehen in jeder Arztpraxis sein. Hierzu müssen die verschiedenen Verfahren transparent beschrieben und nutzerfreundlich angeboten werden. Der Praxisinhaber sowie alle Mitarbeitenden müssen diese Verfahren verstehen und sicher anwenden können.*

Das Betreiben von separaten Netzwerken begrenzt nach erfolgreichem Kompromittieren die Schadenswirkungen. Diese sinnvolle Maßnahme nutzen bereits 42 Prozent der Befragten. Derzeit wird ein separates Patienten WLAN bei 20 Prozent der Befragten eingesetzt. Hierbei handelt es sich um ein Netzwerk, über das Patientinnen und Patienten innerhalb der Praxis einen Internetzugang erhalten können, jedoch nicht in das eigentliche Praxisnetzwerk eingebunden werden müssen. Jeweils neun Prozent nutzen ein separates Server-Netz sowie ein Netzwerk für medizinisches Gerät. Durchschnitt sind bei 92 Prozent der Befragten zehn medizinische Geräte in den Arztpraxen in Betrieb, wobei hiervon durchschnittlich sechs an das Praxisnetzwerk angeschlossen sind.

> *Der Praxisinhaber muss sicherstellen, dass die sensiblen Bereiche, wie beispielsweise medizinische Geräte von schädlichen und öffentlichen Netzwerken getrennt und zusätzlich abgesichert werden.*

Grundlegend für die Absicherung der Praxis ist eine Bestandsaufnahme, welche Netzteilnehmer (bspw. Computer, Router, medizinische Geräte, Bürogeräte) in das Netzwerk der Arztpraxis wie eingebunden sind und wie deren Netzwerkkommunikation (IP-Adressen etc.) erfolgt. Zu diesem Zweck fordert die IT-Sicherheitsrichtlinie gem. § 75b SGB V das Erstellen eines Netzwerkplanes von allen Praxisbetreibern. Die Umfrageergebnisse legen nahe, dass diese notwendige Grundkenntnis für eine erfolgreiche Absicherung fehlt (vgl. Abbildung 3). So geben lediglich 60 Prozent der Befragten an, einen solchen Netzwerkplan aktuell

zu besitzen. Bei den verbleibenden 40 Prozent fehlt dieser oder es ist der Befragten oder dem Befragten nicht bekannt, ob ein solcher Plan für die jeweilige Praxis existiert.

> *Den Praxisinhabern muss die Notwendigkeit eines Netzwerkplanes verdeutlicht und dessen Erstellung erleichtert werden.*
> *Jederzeit sollte eine Übersicht über das gesamte Praxisnetzwerk bestehen. Einerseits bietet sie den Einstiegspunkt in Absicherungsmaßnahmen (Präventiv). Andererseits erleichtert es die Behebung eines Vorfalls (Reaktiv).*

Die Kenntnisse über die Anbindung an die Telematikinfrastruktur, dem Kernelement der gesetzlichen

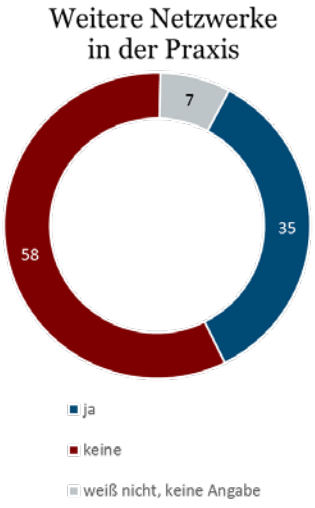

Abbildung 4: Weitere Netzwerke in der Praxis (Angaben in Prozent, n=1.591)

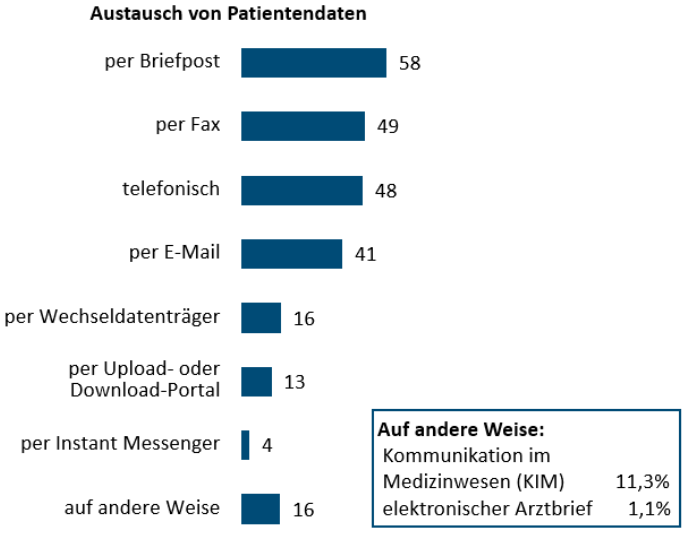

Abbildung 3: Austausch von Patientendaten mit anderen Leistungserbringern/ Praxen (Angaben in %, n=1.591)

Gesundheitsanwendungen bieten ebenfalls Grund zur Ernüchterung. In 93 Prozent der Praxen wird der Konnektor zur Anbindung an die Telematikinfrastruktur verwendet. Doch geben 60 Prozent der Befragten an, keine Kenntnisse über die Anschlussart ihres Konnektors zu haben. Die übrigen 40 Prozent geben an, ihren Konnektor seriell (19 %) oder parallel (21 %) zu betreiben. Die Schutzfunktionen des Konnektors kommen somit lediglich in 19 Prozent den Arztpraxen nach Angabe der Befragten zum Tragen.

> *Die Schutzmechanismen, die ein Konnektor im seriellen Betrieb aufweist, müssen in verständlicher Art kommuniziert werden, damit diese auch flächendeckend in den deutschen Arztpraxen genutzt werden. Andernfalls müssen konkrete Maßnahmen definiert und vor Ort umgesetzt werden, sodass derselbe Schutz auch bei einem parallelen Betrieb gewährleistet ist.*

Für die große Mehrheit der Befragten ist es selbstverständlich, dass es Zugangsbeschränkungen zu den in der Praxis genutzten Geräten gibt. Am meisten wird hier die Passwortsperre eingesetzt, gefolgt von PIN-Sperren. Weitere Beschränkungen sind allerdings eher selten und werden am ehesten von Praxen mit sehr gutem IT-Sicherheitsinformationsstand oder mit Unterstützung eines IT-Sicherheitsbeauftragten eingesetzt. Auch bei dem zeitbasierten Sperren (automatische Abmeldung) des Zugriffs wird am häufigsten ein Bildschirmschoner mit Passwort-Sicherung von den meisten Praxen umgesetzt. Die größten Defizite bei der Umsetzung von Schutzmaßnahmen gibt es in Praxen ohne IT-Sicherheitsbeauftragten.

> *Alle Geräte in den Praxen müssen mit Zugriffsbeschränkungen versehen werden. Eine gute Passwortregelung und zeitliche Zugriffsbeschränkungen sollten überall eingerichtet werden. Durch die Verwendung einer Zwei-Faktor-Authentifizierung kann der Schutz gesteigert werden.*

Der Austausch von Patientendaten mit anderen Leistungserbringern oder Praxen gehört zum Praxisalltag. Die in Abbildung 4 dargestellte Auswertung zeigt, dass der Austausch weiterhin in der Regel per Briefpost,

Fax oder Telefon oder – etwas seltener – per E-Mail erfolgt. In Zahnarztpraxen spielen die klassischen (analogen) Kommunikationswege eine deutlich geringere Rolle. Diese setzen vor allem auf E-Mails und überdurchschnittlich häufig auf Wechseldatenträger und den medizinischen Kommunikationsdienst KIM.

4 Schlussfolgerung und Erkenntnisse aus der Umfrage

Die Ergebnisse der Umfrage verdeutlichen, dass die IT-Sicherheit bei den Praxen aktuell kein primärer Fokus ist, obgleich sie sich in diesem Bereich gut aufgestellt sehen. Diese Einschätzung verwundert vor dem Hintergrund der unzureichenden Bekanntheit der dafür vorgesehenen Richtlinie. Die Selbsteinschätzung kann ebenfalls dadurch zustande kommen, dass bisher wenige Arztpraxen von einem IT-Sicherheitsvorfall betroffen waren. Dieser positive Umstand gibt jedoch keinen Anlass zur Beruhigung, sondern sollte als Ansporn angesehen werden, die IT-Sicherheit bei den Ärztinnen und Ärzten fortwährend zu steigern. Hierzu muss primär die bereits bestehende IT-Sicherheitsrichtlinie bei allen Verantwortlichen bekannt sein. Dass die Vorgaben zudem aktuell nur in einem Drittel der Praxen vollumfänglich umgesetzt wurden, scheint zum einen mit Verständnisproblemen hinsichtlich der Vorgaben und Zweifel an deren Nutzen zu tun zu haben. Zum anderen scheint der Umsetzungsrückstand mit fehlendem Budget, Personal und Zeit einherzugehen. Die Befragung zeigt, dass bereits der Einsatz eines Sicherheitsverantwortlichen einen positiven Effekt auf die IT-Sicherheit der Praxis hat. So gibt es in diesen Praxen häufiger einen Netzwerkplan und eine redundante Stromversorgung des Servers, die Daten werden häufiger verschlüsselt gespeichert und versendet, und die Zugangsbeschränkungen und Schutzmaßnahmen vor unberechtigten Zugriffen gehen häufiger über eine Passwortsperre hinaus. Somit kommen hier die grundlegenden Schutzmaßnahmen der IT-Sicherheitsrichtlinie häufiger zum Tragen.

Die Verbreitung der bestehenden Richtlinie und deren Umsetzung sollte zudem durch begleitende Maßnahmen ergänzt werden. Hierbei sollte der Fokus auf einer Erleichterung der Realisierung liegen. Dafür sollten die Informationen niedrigschwellig und anschaulich vermittelt werden. Hilfreich könnten klare Vorgaben, etwa in Form einer Checkliste, sowie persönliche Beratungen oder Schulungen von IT-Sicherheitsbeauftragten sein.

Darüberhinausgehend bedarf der Schutz der Arztpraxen einer Evaluation und Anpassung der unterschiedlichen Anforderungen und Maßnahmen. Diese Evaluation muss vor dem Hintergrund der allgemein angespannten IT-Sicherheitslage und mit dem speziellen Fokus der Rolle der ambulanten Versorgung regelmäßigen erfolgen. Erfolgsentscheidend sind die Aspekte der Angemessenheit und Umsetzbarkeit der Schutzmaßnahmen bei der Absicherung deutscher Praxen.

Die diskutierten Ergebnisse der Umfrage verdeutlichen, dass die bisherigen Maßnahmen verbessert werden sollten, damit die Richtlinie ihre präventive Wirkung entfalten kann und der fortwährende Schutz in der ambulanten Versorgung Deutschlands verbindlich und ausreichend etabliert wird.

5 Literaturverzeichnis

Kassenärztliche Bundesvereinigung (KBV). 2020. *Richtlinie nach § 75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit*, https://www.kbv.de/media/sp/RiLi__75b_SGB_V_Anforderungen_Gewaehrleistung_IT-Sicherheit.pdf

Kassenzahnärztliche Bundesvereinigung (KZBV). 2021. *Richtlinie nach § 75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit*, https://www.kzbv.de/it-sicherheitsrichtlinie-75b-kzbv-v1-01-0121.download.e97ec0837147f4639f3b4c32e5775c84.pdf