Resiliente Praxis-IT - Ratgeber für Ärztinnen und Ärzte

IT-Infrastruktur sicher und zuverlässig betreiben – für Arztpraxen und MVZ

Marc Dauenhauer

März 2026

Inhaltsverzeichnis

Impressum

Resiliente Praxis-IT - Ratgeber für Ärztinnen und Ärzte

Marc Dauenhauer

[Adresse] [PLZ Ort]

E-Mail: [email@example.de] Website: https://resiliente-praxis-it.de

Urheberrecht

1. Einleitung

IT-Sicherheit ist kein Thema, das Ärztinnen und Ärzte gerne angehen. Es kostet Zeit, es fühlt sich technisch an, und es scheint immer wichtigere Dinge zu geben. Patienten warten, Abrechnungen laufen, das Praxisteam braucht Anleitung. Wann soll man sich da noch mit Backups, Passwörtern und Datenschutzrichtlinien beschäftigen?

Diese Haltung ist verständlich. Aber sie ist falsch – und dieser Ratgeber erklärt, warum.

IT-Sicherheit in einer Arztpraxis ist kein IT-Problem. Es ist ein ärztliches Problem. Es geht um den Schutz Ihrer Patienten, um Ihre eigene rechtliche Sicherheit und um die Funktionsfähigkeit Ihrer Praxis. Wer das einmal verstanden hat, sieht das Thema anders.

Dieser Ratgeber ist entstanden, weil es zwar viel Material zu IT-Sicherheit gibt – aber kaum etwas, das wirklich auf die besondere Situation einer Arztpraxis eingeht. Die Anforderungen an niedergelassene Ärztinnen und Ärzte sind spezifisch: die Telematikinfrastruktur mit ihren Konnektoren und Karten, das Praxisverwaltungssystem als zentrales Nervensystem, die ärztliche Schweigepflicht als strafrechtliche Kategorie, die KBV-IT-Sicherheitsrichtlinie als geltendes Berufsrecht. Das alles existiert in dieser Form nur in Arztpraxen.

1.1. Für wen ist dieser Ratgeber?

Dieser Ratgeber ist für alle, die eine Praxis betreiben oder leiten – Hausärzte, Fachärzte, Zahnärzte, Psychotherapeuten, MVZ-Betreiber. Sie müssen keine IT-Kenntnisse haben. Sie müssen aber bereit sein, sich mit Dingen zu beschäftigen, die Sie vielleicht lieber ignorieren würden.

Vielleicht erkennen Sie sich hier wieder:

- Sie haben eine Praxissoftware, wissen aber nicht genau, wo Ihre Patientendaten liegen – ob auf dem lokalen Server oder in der Cloud.
- Ihr IT-Dienstleister kümmert sich um die technische Seite. Sie vertrauen darauf, dass er alles richtig macht – aber Sie hatten nie ein echtes Gespräch darüber, wie er geschützte Daten behandelt.
- Sie sichern Ihre Daten irgendwie – aber Sie haben nie überprüft, ob die Sicherung funktioniert.
- Sie haben schon von der KBV-Richtlinie gehört und sind unsicher, ob Ihre Praxis diese erfüllt.
- Sie nutzen die ePA und den TI-Konnektor – und fragen sich, welche Sicherheitsanforderungen das mit sich bringt.

Wenn Sie sich in einem dieser Punkte wiedererkennen: Dieser Ratgeber ist für Sie.

1.2. Was dieser Ratgeber ist – und was nicht

Dieser Ratgeber ist ein Orientierungsrahmen für Praxisverantwortliche ohne vertiefte IT-Kenntnisse. Er zeigt Ihnen, wo die kritischen Punkte liegen, welche Maßnahmen sinnvoll sind und warum sie wichtig sind. Er ersetzt aber weder eine individuelle IT-Beratung noch eine Rechtsberatung noch eine ärztliche Organisationsberatung.

Wo Fragen des Strafrechts, der DSGVO oder der Berufsordnung berührt werden, gibt dieser Ratgeber Orientierung. Eine individuelle Rechtsberatung ist das nicht. Wenn Sie konkrete rechtliche Fragen haben – etwa zur Auslegung eines Vertrags mit Ihrem IT-Dienstleister, zur Einhaltung der KBV-Richtlinie in Ihrer speziellen Situation, oder zur Frage, ob eine bestimmte Maßnahme ausreichend ist – wenden Sie sich an einen auf Medizinrecht oder Datenschutz spezialisierten Anwalt.

Auch ist dieser Ratgeber kein Hochsicherheitstrakt-Handbuch. Es geht nicht darum, das theoretisch Optimale zu erreichen – sondern das praktisch Erreichbare. Ein Schutz, den Sie umsetzen, hilft mehr als ein perfektes Konzept, das nur auf dem Papier steht. Deshalb lautet das Grundprinzip: Lieber 80 Prozent ehrlich und konsequent umgesetzt als 100 Prozent als guter Vorsatz.

> **Rechtlicher Hinweis:** Alle Ausführungen zu Strafrecht (§ 203 StGB), DSGVO, KBV-Richtlinie und anderen rechtlichen Fragen dienen der allgemeinen Orientierung. Sie ersetzen keine individuelle Rechtsberatung. Für Ihre konkrete Situation wenden Sie sich bitte an einen Anwalt, der auf Medizinrecht oder Datenschutz spezialisiert ist.

1.3. Wie Sie mit diesem Ratgeber arbeiten

Sie müssen diesen Ratgeber nicht von vorne bis hinten lesen. Wenn Sie ein akutes Problem haben – etwa weil Sie nicht wissen, ob Ihre Praxis die KBV-Anforderungen erfüllt – springen Sie direkt in das entsprechende Kapitel.

Wenn Sie von Grund auf anfangen und Ihre Praxis sicherer machen möchten, empfehle ich die Reihenfolge. Der Aufbau ist so gestaltet, dass jedes Kapitel auf dem vorherigen aufbaut.

Am Ende jedes Teils finden Sie eine Checkliste. Nutzen Sie diese. Drucken Sie sie aus, wenn das hilft. Haken Sie ab, was erledigt ist. Notieren Sie, was noch offen ist. Eine Checkliste, die Sie zur Hälfte abgehakt haben, ist unendlich besser als ein Ratgeber, den Sie gelesen, aber nicht umgesetzt haben.

Technische Begriffe werden beim ersten Auftreten erklärt. Wer tiefer einsteigen möchte, findet am Ende optional Deep-Dive-Abschnitte – freiwillig und nicht notwendig für das Grundverständnis.

> **Tipp:** Lesen Sie diesen Ratgeber mit einem Stift in der Hand oder einem offenen Notizdokument. Schreiben Sie auf, was Sie aufhorchen lässt. Das wird Ihre persönliche Aufgabenliste für die nächsten Wochen.

1.4. Was Sie erwartet

Dieser Ratgeber ist in zehn Teile gegliedert.

Teil 1: Grundlagen & Mindset legt die Basis. Warum ist IT-Sicherheit für Arztpraxen keine technische Nebensache, sondern eine ärztliche Pflicht? Welche Irrtümer halten viele Praxen zurück? Und wie stellen Sie fest, was Sie überhaupt an digitaler Infrastruktur in Ihrer Praxis haben?

Teil 2: Rechtlicher Rahmen erklärt die drei Ebenen von Pflichten: das Strafrecht (§ 203 StGB), die DSGVO und das Berufsrecht (KBV-IT-Sicherheitsrichtlinie). Keine Juristerei – sondern die konkrete Frage: Was bedeuten diese Regeln für meine tägliche Praxis?

Teil 3: Digitale Infrastruktur beschreibt die Grundmaßnahmen: sichere Passwörter, Zwei-Faktor-Authentifizierung, Backups, Verschlüsselung, sicherer Internetzugang, Cloud-Dienste und der Umgang mit Zugängen für externe Dienstleister.

Teil 4: Telematikinfrastruktur widmet sich den Besonderheiten der TI: Konnektor, elektronischer Heilberufsausweis, KIM, ePA, eRezept und elektronische Arbeitsunfähigkeitsbescheinigung – und was zu tun ist, wenn die TI ausfällt.

Teil 5: Praxisverwaltungssystem beleuchtet das Herzstück der Praxis-IT. Welche Sicherheitsanforderungen stellt das PVS? Was ist bei der Auswahl, dem Betrieb und dem Backup von Patientendaten zu beachten?

Teil 6: Medizinische Geräte am Netz behandelt ein oft übersehenes Risiko: vernetzte Medizintechnik, die mit dem Praxisnetzwerk verbunden ist. Wie segmentiert man das Netz, damit ein kompromittiertes Gerät nicht zur Gefahr für alle anderen wird?

Teil 7: KBV IT-Sicherheitsrichtlinie zeigt, welche Anforderungen die Richtlinie konkret stellt – gestaffelt nach Praxisgröße von der kleinen Einzelpraxis bis zur Gemeinschaftspraxis mit Großgeräten.

Teil 8: KI in der Arztpraxis gibt einen Überblick darüber, wie KI-Werkzeuge in der Praxis sinnvoll eingesetzt werden können – und welche Risiken bei Datenschutz und Schweigepflicht zu beachten sind.

Teil 9: Personal & Zugänge erklärt, wie Berechtigungen in einer Praxis sinnvoll vergeben werden, wie Onboarding und Offboarding von Mitarbeitenden geregelt sein sollten und was bei Praxisübergaben zu beachten ist.

Teil 10: Notfall & Resilienz schließt den Kreis: Was tun, wenn etwas wirklich schiefgeht? Wie erkennt man Social Engineering und Phishing? Wie sieht ein handhabbarer Notfallplan aus?

Am Ende finden Sie ein Glossar sowie ein Quellenverzeichnis mit weiterführenden Materialien.

Eine persönliche Anmerkung: IT-Sicherheit für Arztpraxen ist kein attraktives Thema. Es ist unbequem, zeitaufwendig und fühlt sich oft wie eine Last an. Aber wenn Sie verstanden haben, dass IT-Sicherheit in einer Arztpraxis nicht ein IT-Problem ist, sondern ein ärztliches Problem – dass es um den Schutz Ihrer Patienten und um Ihre eigene rechtliche Sicherheit geht – dann wird es plötzlich sinnvoll. Und plötzlich lohnt sich die Anstrengung.

2. Grundlagen – Warum Ihre Praxis IT-Sicherheit braucht

Was unterscheidet eine Arztpraxis von anderen Unternehmen – und welche Grundprinzipien helfen, die IT-Sicherheit dauerhaft auf solidem Fundament zu halten?

2.1. Morgens um acht Uhr – und nichts geht mehr

Stellen Sie sich diese Situation vor: Sie öffnen morgens die Praxistür. Der Praxismanager sitzt schon am Computer – und schaut Sie mit besorgter Miene an. "Die Praxissoftware antwortet nicht. Der Server ist aus. Und der TI-Konnektor blinkt rot." Sie probieren es selbst. Nichts. Kein Zugriff auf Patientendaten, keine Rezepte, keine eRezepte. Und die erste Patientin sitzt schon im Wartezimmer.

Das klingt nach Horror-Szenario. Es ist aber Alltag in vielen Praxen – und es passiert regelmäßig: Nicht weil Ärzte schlecht arbeiten, sondern weil digitale Systeme ausfallen, gehackt werden oder nicht richtig gepflegt werden. Und wer als Arzt nicht auf seine Daten zugreifen kann, kann auch nicht arbeiten. Nicht für eine Stunde, nicht für einen halben Tag – sondern für unbestimmte Zeit. Die Patienten müssen abgesagt werden. Rezepte können nicht ausgestellt werden. Notfallpatienten, die Sie sehen könnten, müssen Sie wegschicken.

Das ist nicht nur ein praktisches Problem. Es ist auch ein rechtliches Problem. Denn wenn Ihre Praxis-IT unsicher ist und Patientendaten in fremde Hände geraten – nicht weil Sie das wollten, sondern weil Sie ein Ransomware-Opfer wurden, weil ein Update fehlte oder weil Ihr Passwort zu schwach war – dann sind Sie nach deutschem Strafrecht haftbar. Das ist keine Frage von Schuld oder nicht schuld, sondern von strafrechtlicher Verantwortung.

2.2. Warum IT-Sicherheit für Arztpraxen eine besondere Qualität hat

Eine Steuerberaterin mit Datenleck bekommt ein Bußgeld. Ein IT-Dienstleister mit Ransomware verliert vielleicht Kunden. Aber eine Arztpraxis mit Datenleck oder Systemausfall – das ist etwas anderes. Das sind nicht irgendwelche Daten, die geflossen sind. Das sind Patientendaten. Und Patientendaten sind nach deutschem Recht besonders geschützt.

Das Strafgesetzbuch, § 203, schützt Berufsgeheimnisse. Wenn Sie als Arzt oder Ärztin ein Patientengeheimnis unbefugt offenbaren – sei es durch aktives Handeln oder durch

Unterlassen –, das ist eine Straftat. Keine Verwarnung, keine Ordnungswidrigkeit: Straftat, mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe.

Das ist nur eine Ebene. Daneben kommt die DSGVO – die Datenschutz-Grundverordnung. Sie sagt: Wer personenbezogene Daten verarbeitet, muss sie schützen. Technische Maßnahmen, organisatorische Maßnahmen, Verschlüsselung, Backups. Und bei Verstößen gibt es Bußgelder, die durchaus in fünfstelliger Höhe liegen können.

Und dann gibt es noch das Berufsrecht. Die KBV, die Kassenärztliche Bundesvereinigung, hat für alle Vertragsärzte eine IT-Sicherheitsrichtlinie erlassen. Diese Richtlinie ist nicht unverbindlicher Ratschlag – sie ist geltendes Recht mit Bußgeldandrohungen bis zu 100.000 Euro.

Das sind drei verschiedene Regelungsebenen. Sie ersetzen sich nicht gegenseitig. Sie stehen nebeneinander. Das heißt: Ihre Praxis muss gleichzeitig strafrechtliche Anforderungen, datenschutzrechtliche Anforderungen und berufsrechtliche Anforderungen erfüllen.

> **Merksatz:** Schlechte IT in einer Arztpraxis ist nicht ein technisches Problem, das man irgendwann beheben könnte. Es ist eine Verletzung der ärztlichen Sorgfaltspflicht, die Konsequenzen nach sich zieht – strafrechtlich, datenschutzrechtlich und berufsrechtlich.

Das bedeutet nicht, dass Sie zum IT-Sicherheits-Experten werden müssen. Es bedeutet aber, dass Sie verstehen müssen, was Ihre Verantwortung ist und wie Sie sie erfüllen.

2.3. Was ist Resilienz?

In diesem Ratgeber sprechen wir nicht von Perfektion. Wir sprechen von Resilienz.

Resilienz bedeutet: Ihre Praxis funktioniert auch wenn Dinge schiefgehen. Nicht, weil nichts schieflaufen kann – sondern weil Sie vorbereitet sind. Weil Ihre Patientendaten nicht an einem einzigen Ort existieren. Weil Ihre wichtigsten Systeme Backups haben. Weil Sie nicht hilflos sind, wenn Ihr Computer gehackt wird oder die Praxissoftware abraucht.

Resilienz bedeutet auch: Sie erfüllen Ihre Pflichten nicht perfekt nach Lehrbuch, sondern praktisch und konsequent. Es ist nicht schlimm, wenn Sie nicht alle allerneuesten Sicherheitsstandards haben. Es ist schlimm, wenn Sie wissen, dass Sie etwas nicht richtig machen, und es trotzdem nicht ändern.

> **Merksatz:** Resilienz heißt nicht: Keine Probleme. Resilienz heißt: Ich bin vorbereitet, wenn Probleme kommen – und ich kann damit umgehen.

2.4. Die vier Grundprinzipien dieses Ratgebers

Bevor wir in die konkreten Themen einsteigen, lohnt es sich, vier Prinzipien zu verstehen, die sich durch den gesamten Ratgeber ziehen.

2.4.1. Prinzip 1: Redundanz – Verlassen Sie sich nie auf ein einziges System

Redundanz bedeutet: Wenn etwas ausfällt, gibt es einen Ersatz. Nicht Panik, nicht Stillstand – nur ein Umschalten auf Plan B. In der Praxis heißt das: Ihre wichtigsten Patientendaten existieren an mehr als einem Ort. Ihre Praxissoftware lässt sich auch dann noch betreiben, wenn der Server temporär ausfällt. Sie haben einen definierten Notfallplan für den Fall, dass Ihre Praxis-IT stundenlang nicht erreichbar ist.

Redundanz ist nicht kompliziert – aber sie braucht Planung. Wer erst dann überlegt, wie die Praxis ohne ihre IT läuft, wenn gerade die IT zusammengebrochen ist, hat keinen Plan B.

2.4.2. Prinzip 2: Unabhängigkeit – Wer kontrolliert Ihre Infrastruktur wirklich?

Sie nutzen einen Praxis-Software-Anbieter, einen Cloud-Dienst für Backups, vielleicht einen IT-Dienstleister vor Ort. Diese Anbieter können ihre Geschäftsbedingungen ändern, den Dienst einstellen, den Preis erhöhen – oder in seltenen Fällen Ihr Konto sperren.

Das Prinzip der Unabhängigkeit bedeutet nicht, alle externen Dienste zu meiden. Es bedeutet: Verstehen Sie, wovon Sie abhängig sind. Stellen Sie sicher, dass Sie im Notfall an Ihre Daten herankommen – auch wenn ein Anbieter ausfällt. Ihre Patientendaten gehören Ihnen, nicht Ihrem IT-Dienstleister. Die Zugangsdaten zu kritischen Systemen sollten Sie kennen – nicht nur Ihr Praxismanager oder ein externer Techniker.

2.4.3. Prinzip 3: Worst-Case-Denken – Was passiert, wenn X morgen ausfällt?

Stellen Sie sich schlimmstmögliche Szenarien vor – nicht um Angst zu haben, sondern um vorbereitet zu sein. Was tun Sie, wenn Ihr Praxis-Software-Server nicht mehr hochfährt? Was tun Sie, wenn Ransomware Ihre Festplatte verschlüsselt? Was tun Sie, wenn der IT-Dienstleister unerwartet die Zusammenarbeit beendet? Diese Fragen haben konkrete Antworten – wenn Sie sie sich vorher gestellt haben.

2.4.4. Prinzip 4: Pragmatismus – Fertig ist besser als perfekt

IT-Sicherheit kann immer besser sein. Aber eine Maßnahme, die Sie heute konsequent umsetzen, schützt Sie mehr als ein perfektes System, das Sie nächstes Jahr irgendwann mal anfangen wollen. In diesem Ratgeber gilt: Lieber eine einfache Maßnahme, die Sie konsequent durchziehen, als eine aufwendige Lösung, die Sie nicht umsetzen.

2.5. Mindset: Warum IT-Sicherheit vernachlässigt wird – und wie Sie das ändern

Bevor die Technologie kommt, kommt die Haltung. Und die richtige Haltung ist der Anfang für alles andere.

2.5.1. Die drei Irrtümer im Praxisalltag

In Ihrem Arbeitsalltag werden Sie regelmäßig mit diesen Sätzen konfrontiert:

Irrtum 1: "Das macht unser IT-Dienstleister. Der kümmert sich darum."

Das ist beruhigend. Es ist aber falsch. Ja, ein guter IT-Dienstleister setzt die Sicherheitsmaßnahmen technisch um. Aber er trägt nicht die Verantwortung für die Praxis. Sie tun das. Die Ärztliche Schweigepflicht nach § 203 StGB ist eine persönliche Pflicht – Sie als Praxisinhaber oder Leitender Arzt haften dafür, dass Patientendaten geschützt sind. Das gilt auch, wenn Sie die technische Umsetzung outgesourct haben. Wenn Ihr IT-Dienstleister schlecht arbeitet und das zu einem Datenleck führt, können Sie nicht sagen: "Der ist schuld." Sie sind schuld – weil Sie die Verantwortung haben zu überprüfen, dass er gut arbeitet.

Ein Vergleich hilft: Wenn Sie Ihr Auto zur Reparatur geben und der Mechaniker macht einen Fehler, der zu einem Unfall führt, können Sie nicht sagen: "Das ist sein Problem." Nein – Sie haften, weil Sie die Kontrolle haben.

Irrtum 2: "Uns passiert das nicht. Kleine Praxen werden nicht gehackt."

Das ist einer der gefährlichsten Irrtümer. Es ist auch statistisch falsch. Die Zahl der Ransomware-Angriffe auf Arztpraxen ist in den letzten Jahren dramatisch gestiegen – gerade auf mittlere und kleine Praxen. Warum? Weil große Unternehmen oft gut geschützt sind. Kleine Praxen wirken wie ein leichtes Ziel. Ein unverschlüsselter Server, ein schwaches Passwort, veraltete Software – und schon ist eine Praxis ein Ransomware-Opfer.

Das heißt nicht, dass Sie paranoid werden sollen. Es heißt nur: Der Gedanke, Ihnen könne das nicht passieren, ist naiv. Es kann jeder passieren.

Irrtum 3: "Wir haben schon immer so gemacht – und es ist gut gegangen."

Das ist ein Überlebensirrtum. Ja, es ist gut gegangen – bisher. Das bedeutet aber nicht, dass es sicher ist. Ein Auto ohne Airbags ist auch 50 Jahre gut gegangen – bis zum ersten ernsthaften Unfall. Die Digitalisierung in Arztpraxen ist noch neu. Die Angriffe werden raffinierter. Die rechtlichen Anforderungen verschärfen sich. "Das haben wir immer so gemacht" ist keine Sicherheitsstrategie.

2.5.2. Die wahren Gründe, warum IT-Sicherheit vernachlässigt wird

Wenn diese drei Irrtümer so verbreitet sind, liegt das nicht daran, dass Ärzte dumm sind. Es liegt an realen Gründen:

Zeitmangel: Sie haben einen vollen Praxisalltag. Patienten sehen, Dokumentation, Administration. IT-Sicherheit fühlt sich wie noch eine Aufgabe an, für die Sie keine Zeit haben. Das ist verständlich.

Abstrakte Gefahr: Sie können das Risiko nicht anfassen. Ein Patient mit Herzinfarkt ist eine konkrete Gefahr. Ein mögliches Datenleck ist etwas, das vielleicht passiert, vielleicht

nicht. Das menschliche Hirn reagiert auf unmittelbare Bedrohungen, nicht auf statistische Wahrscheinlichkeiten.

Verantwortung delegiert: Sie haben einen IT-Dienstleister. Sie haben eine Praxissoftware. Sie vertrauen darauf, dass diese sich kümmern. Das ist menschlich – und teilweise sinnvoll. Aber es ist auch gefährlich, wenn Sie dabei Ihre eigene Verantwortung aus den Augen verlieren.

Kein unmittelbarer Nutzen: Wenn Sie einen neuen EKG-Monitor kaufen, können Sie sehen, dass die Patienten davon profitieren. Wenn Sie Ihre Festplatte verschlüsseln, passiert erst mal nichts – außer dass alles langsamer wird. Der Nutzen ist unsichtbar.

Kostengefühl: Sicherheitsmaßnahmen kosten Geld. Oft ist unklar, welche Maßnahmen notwendig sind und welche rausgeworfen Geld sind. Hinzu kommt, dass manche IT-Dienstleister mit Angst verkaufen und überdimensionierte Lösungen anbieten.

Das alles ist nachvollziehbar. Aber es ist kein Grund, es nicht zu ändern.

2.5.3. Die richtige Haltung: IT-Sicherheit ist Teil der ärztlichen Sorgfaltspflicht

Hier ist der Perspektivwechsel: IT-Sicherheit in der Arztpraxis ist kein IT-Problem. Es ist ein ärztliches Problem.

Sie sind Arzt oder Ärztin. Das bedeutet, Sie haben Patienten, die Ihnen ihre Geheimnisse anvertrauen. Sie vertrauen Ihnen mit ihrer Gesundheit, mit ihren Diagnosen, mit vertraulichen Informationen. Sie vertrauen Ihnen – und im Gegenzug haben Sie die Pflicht, dieses Vertrauen zu schützen.

Das ist nicht nur eine moralische Pflicht. Es ist eine rechtliche Pflicht, verankert in § 203 StGB: Die ärztliche Schweigepflicht ist Strafrecht. Und sie gilt nicht nur für aktive Handlungen – sie gilt auch für Unterlassen. Wenn Sie fahrlässig zulassen, dass Patientendaten nach außen dringen, weil Sie Ihre IT-Infrastruktur nicht geschützt haben, haben Sie gegen die Schweigepflicht verstoßen. Das ist eine Straftat.

Das bedeutet: IT-Sicherheit ist nicht optional. Sie ist ein essentieller Teil der ärztlichen Sorgfaltspflicht.

Es ist, als würde Ihnen jemand sagen: “Sie könnten ja Ihre Sprechstunde ohne Handschuhe machen – und es ist wahrscheinlich OK.” Es ist zwar wahr, dass es häufig OK gehen würde. Aber als Arzt wissen Sie, dass es nicht OK ist – weil es gegen Ihre Standards verstößt und Ihre Patienten gefährdet.

Genauso ist es mit IT-Sicherheit. Ja, Sie könnten die Praxis ohne verschlüsselte Server betreiben. Ja, Sie könnten unsichere Passwörter verwenden. Ja, Sie könnten auf Backups verzichten. Technisch ist das alles möglich. Aber ethisch und rechtlich ist es nicht in Ordnung.

> **Merksatz:** IT-Sicherheit ist nicht eine technische Zusatzaufgabe. Sie ist ein Teil Ihrer Sorgfaltspflicht als Ärzte oder Ärztin, genauso wie die medizinische Fachliteratur auf dem neusten Stand zu halten oder mit Instrumenten steril zu arbeiten.

2.5.4. Die praktischen Konsequenzen – und warum das Ändern sich lohnt

Was passiert, wenn Sie diese Haltung verankern?

Erst mal passiert wahrscheinlich nicht viel im täglichen Arbeitsalltag. Ihre Patientenversorgung wird nicht besser. Ihre Abrechnungsquoten ändern sich nicht.

Aber längerfristig passiert Folgendes: Sie schlafen besser, weil Sie wissen, dass Sie Ihre Verantwortung erfüllen. Wenn eine Datenpanne vorkommt – und statistisch wird sie irgendwann kommen –, sind Sie nicht völlig unvorbereitet. Sie wissen, welche Maßnahmen getroffen wurden, welche Daten wie geschützt sind. Sie können schneller reagieren. Und Sie können einem Staatsanwalt oder einer Datenschutzbehörde gegenüber überzeugend darlegen, dass Sie alles Notwendige getan haben.

Noch wichtiger: Sie sind nicht von Ihrem IT-Dienstleister abhängig. Sie verstehen, was er tut. Sie können überprüfen, ob er gut arbeitet. Und wenn nicht – können Sie das ändern.

2.5.5. Die Bestandsaufnahme: Der erste konkrete Schritt

Der Perspektivwechsel ist wichtig. Aber dann braucht es konkrete Schritte. Der erste ist eine ehrliche Bestandsaufnahme: Was habe ich? Wovon hänge ich ab?

Das klingt langweilig. Es ist aber der wertvollste Schritt, den Sie tun können.

Mit einer Bestandsaufnahme beantworten Sie für Ihre Praxis folgende Fragen:

Welche Systeme und Geräte habe ich? Wo laufen die Patientendaten? Auf einem lokalen Server? In der Cloud? Auf dem Laptop des Praxismanagers? Auf mobilen Geräten?

Welche Dienstleister sind involviert? Wer hostet Ihre Praxissoftware? Wer macht die Backups? Wer sitzt beim IT-Support vor Ort? Wer hat Zugriff zu Ihren Systemen?

Wo sind meine Patientendaten wirklich? Das ist eine einfache Frage mit oft sehr komplizierter Antwort. Sie werden überrascht sein, an wie vielen Orten gleichzeitig Ihre Patientendaten liegen – manche Kopien sind verschlüsselt, manche nicht. Manche sind gesichert, manche nicht.

Wovon bin ich abhängig? Was passiert morgen, wenn Ihr Server nicht hochfährt? Wenn der Cloud-Anbieter der Praxissoftware überfallen wird? Wenn Ihr IT-Dienstleister unerwartet die Zusammenarbeit beendet? Wenn Ihr Praxismanager ausfällt?

Habe ich einen Notfallplan? Wie lange kann die Praxis ohne ihre IT-Systeme funktionieren? Was ist Plan B? Wo sind die Notfalldaten? Wer weiß, wo kritische Passwörter stehen?

2.5.6. Die Bestandsaufnahme: Konkrete Checklisten

Gehen Sie die folgenden Fragen durch. Sie brauchen keine Perfektion – aber eine ehrliche Antwort. Drucken Sie diese Seite aus und halten Sie fest, wo es noch Lücken gibt.

2.5.6.1. Teil A: Ihre Systeme

- ☐ Ich weiß, wo meine Praxissoftware läuft – lokal, Cloud, Hybrid.
- ☐ Ich kenne den Anbieter meiner Praxissoftware und weiß, wie Daten gespeichert werden.
- ☐ Ich weiß, ob meine Systeme verschlüsselt sind.
- ☐ Ich weiß, wo meine Backups liegen – und wann sie das letzte Mal getestet wurden.
- ☐ Ich verstehe, wer von meinem Team auf welche Systeme Zugriff hat.
- ☐ Ich kenne alle Passwörter für kritische Systeme – oder weiß zumindest, wo sie sicher verwahrt sind.

2.5.6.2. Teil B: Ihre Dienstleister

- ☐ Ich habe eine Liste aller IT-Dienstleister, die Zugriff auf meine Systeme haben.
- ☐ Ich weiß, welche Auftragsverarbeitungsverträge (AVV) mit meinen Dienstleistern bestehen.
- ☐ Ich kenne die Reaktionszeiten meines IT-Supports bei Notfällen.
- ☐ Ich weiß, wie lange die Behebung eines Systemausfalls typischerweise dauert.
- ☐ Ich habe in den letzten sechs Monaten mit meinem IT-Dienstleister ein Gespräch über Sicherheit geführt.

2.5.6.3. Teil C: Ihre Abhängigkeiten

- ☐ Ich weiß, wie lange die Praxis ohne Praxissoftware arbeiten kann.
- ☐ Ich habe einen Plan für den Fall, dass die Praxissoftware einen Tag ausfällt.
- ☐ Ich habe einen Plan für den Fall, dass alle Daten auf dem Server gelöscht werden (Ransomware, Hardwaredefekt).
- ☐ Ich weiß, wer in der Praxis notfallmäßig entscheidungsfähig ist, wenn ich ausfalle.
- ☐ Ich habe Zugang zu kritischen Kontoinformationen dokumentiert und sicher verwahrt.

2.5.6.4. Teil D: Ihre Anforderungen

- ☐ Ich habe die KBV IT-Sicherheitsrichtlinie gelesen oder zumindest überflogen.
- ☐ Ich weiß, welche Anforderungen für meine Praxisgröße gelten.
- ☐ Ich habe überprüft, ob meine Praxis diese Anforderungen erfüllt.
- ☐ Falls Lücken bestehen: Ich habe eine Prio-Liste, was ich zuerst beheben will.

2.5.7. Ihr persönlicher nächster Schritt

Sie müssen nicht alles heute klären. Aber wenn Sie diese Checkliste durchgehen und feststellen, dass Sie auf mindestens fünf Fragen keine gute Antwort haben, dann ist das Ihr Signal: Es ist Zeit, genauer hinzuschauen.

Ihr nächster Schritt:

1. **Drucken Sie diese Checkliste aus.** Nicht nur mental – physisch ausdrucken, auf den Schreibtisch legen.
2. **Blockieren Sie sich zwei Stunden Zeit** – gerne mit Ihrem Praxismanager oder Ihrem IT-Dienstleister – und gehen Sie diese Fragen durch.
3. **Schreiben Sie die Antworten auf.** Nicht im Kopf, nicht vage – sondern konkret. "Praxissoftware läuft bei Anbieter XYZ auf deren Servern in Frankfurt, mit täglichem Backup, Backup wird jährlich getestet" statt "Irgendwo in der Cloud".
4. **Schreiben Sie auch die Lücken auf.** "Ich weiß nicht, ob die Backups verschlüsselt sind. Ich weiß nicht, wie lange ein Systemausfall dauert. Ich habe kein Notfallpapier für den Fall, dass ich ausfalle."
5. **Sortieren Sie: Was ist kritisch?** Was sind die drei Dinge, bei denen Sie am wenigsten sicher sind und die am meisten Schaden machen könnten?

Das ist Ihre persönliche Aufgabenliste für die nächsten Wochen. Und damit Sie in den folgenden Kapiteln dieses Ratgebers nicht verloren sind: Jedes Kapitel wird Ihnen helfen, mindestens einen dieser Punkte besser zu verstehen und zu verbessern.

3. Der Rechtsrahmen: Drei Ebenen von Pflichten

Auf welcher rechtlichen Grundlage beruhen die Anforderungen an IT-Sicherheit in einer Arztpraxis? Und warum gibt es gleich drei verschiedene Regelungssysteme?

3.1. Das Szenario: Eine Praxis wird gehackt

Es ist Samstagnacht. Sie erhalten einen Anruf von Ihrem IT-Dienstleister: "Ihre Praxissysteme wurden gehackt. Patientendaten liegen offen im Internet. Ransomware hat die Festplatte verschlüsselt."

Jetzt geht Ihnen nicht nur ein Gedanke durch den Kopf: "Das ist ein technisches Desaster." Sie denken auch: "Das wird teuer. Und es wird rechtliche Konsequenzen haben."

Welche? Das ist nicht so einfach zu sagen, weil nämlich nicht eine, sondern gleich drei verschiedene rechtliche Systeme anfangen zu spielen.

Es kommt eine Strafanzeige. Ein Staatsanwalt prüft, ob Sie die ärztliche Schweigepflicht verletzt haben. Es kommt eine Mitteilung der Datenschutzbehörde: Sie sollen nach DSGVO eine Datenpanne melden und Betroffene informieren. Und Ihre Ärztekammer wird Sie auffordern, die KBV-Richtlinie einzuhalten. Drei verschiedene Behörden, drei verschiedene Regelungssysteme, drei verschiedene potenzielle Konsequenzen.

3.2. Die drei Ebenen

Für Ärzte gilt nicht eines dieser Systeme – es gelten alle drei gleichzeitig. Und sie ersetzen sich nicht gegenseitig. Sie stehen nebeneinander.

3.2.1. Ebene 1: Strafrecht – § 203 StGB

Das Strafgesetzbuch § 203 stellt das unbefugte Offenbaren von fremden Geheimnissen unter Strafe. Als Arzt unterliegen Sie und alle, die mit Ihnen arbeiten, einer absoluten Schweigepflicht für alles, was Ihnen im Rahmen Ihrer ärztlichen Tätigkeit bekannt geworden ist.

Das ist nicht nur eine moralische Pflicht. Das ist Strafrecht. Ein Verstoß ist kein Verwarnungsgeld und keine Ordnungswidrigkeit – es ist eine Straftat mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe.

Entscheidend ist: Die Schweigepflicht gilt nicht nur für aktives Handeln – also für den Fall, dass Sie selbst Patientendaten veröffentlichen. Sie gilt auch für Tun durch Unterlassen. Das heißt: Wenn Sie fahrlässig oder grob fahrlässig zulassen, dass Patientendaten nach außen dringen, weil Sie Ihre IT-Infrastruktur nicht richtig geschützt haben, dann haben Sie gegen die Schweigepflicht verstoßen.

Unverschlüsselte Server, schwache Passwörter, fehlende Backups, nicht aktualisierte Software – das sind keine technischen Fehler. Das sind potenzielle Straftaten, wenn sie dazu führen, dass Patientendaten offenbar werden.

3.2.2. Ebene 2: Datenschutzrecht – DSGVO und BDSG

Die Datenschutz-Grundverordnung (DSGVO) regelt, wie personenbezogene Daten verarbeitet werden. Sie gilt für alle, die Daten von EU-Bürgern verarbeiten – also auch für Arztpraxen.

Nach der DSGVO müssen Sie technische und organisatorische Maßnahmen (TOMs) ergreifen – Verschlüsselung, Zugangsschutz, Backups. Mit Dienstleistern müssen Sie entsprechende Auftragsverarbeitungsverträge abschließen. Bei Datenpannen die Behörde melden (Meldefrist: 72 Stunden). Betroffene informieren, wenn ein hohes Risiko besteht.

Die DSGVO sieht Bußgelder bis zu 20 Millionen Euro vor – das klingt dramatisch, ist aber für Großkonzerne gemeint. In der Praxis belegen deutsche Datenschutzbehörden kleinere Unternehmen mit Bußgeldern im Bereich von einigen Hundert bis einigen Tausend Euro.

Wichtig: DSGVO ist kein Entweder-Oder. Die DSGVO-Anforderungen gelten zusätzlich zu § 203 StGB. Sie können nicht sagen: “Ich habe die DSGVO erfüllt, also ist die Schweigepflicht OK.” Beide müssen erfüllt sein.

3.2.3. Ebene 3: Berufsrecht – KBV-Richtlinie und Heilberufsgesetze

Auf der dritten Ebene stehen die berufsrechtlichen Vorgaben. Für Vertragsärzte und Psychotherapeuten in der gesetzlichen Krankenversicherung ist das besonders wichtig: die IT-Sicherheitsrichtlinie der Kassenärztlichen Bundesvereinigung (KBV).

Diese Richtlinie ist nicht ein unverbindlicher Leitfaden. Sie ist geltendes Recht mit Sanktionen. Die Anforderungen sind nach Praxisgröße gestaffelt und umfassen sichere Passwörter, Verschlüsselung, regelmäßige Backups, Virenscutz, IT-Sicherheitsschulungen und Verschwiegenheitsverpflichtungen für externe Dienstleister.

Die Nichterfüllung kann zu Bußgeldern bis zu 100.000 Euro führen.

3.3. Wie die drei Ebenen zusammenhängen

Das ist die gute Nachricht: Die drei Ebenen verlangen in der Sache oft dieselben Maßnahmen. Wer seine Praxis so aufstellt, dass sie die § 203 StGB-Anforderungen erfüllt, erfüllt damit auch die DSGVO und meist auch die KBV-Richtlinie.

Ein und dieselbe technische Maßnahme erfüllt also alle drei rechtlichen Anforderungen gleichzeitig.

> **Merksatz:** Wer die Anforderungen von § 203 StGB sorgfältig erfüllt, erfüllt damit automatisch auch einen großen Teil der DSGVO und der KBV-Richtlinie.

3.4. Die zentrale Unterscheidung: Strafrechtliche Garantenpflicht

Es gibt eine wichtige Unterscheidung zwischen den drei Ebenen: Bei § 203 StGB geht es um die Garantenpflicht des Arztes. Das heißt: Sie können diese Verantwortung nicht vollständig an Dienstleister delegieren.

Wenn Sie einen IT-Dienstleister einstellen und dieser macht schlechte Arbeit, können Sie nicht sagen: “Der ist schuld.” Sie sind schuld – weil Sie dafür hätten sorgen müssen, dass dieser Dienstleister gute Arbeit leistet.

3.5. Die praktische Konsequenz: Dokumentation ist nicht optional

Aus dieser Verantwortung ergibt sich eine praktische Konsequenz: Sie müssen dokumentieren, dass Sie Ihre Verantwortung erfüllen.

Das bedeutet nicht, dass Sie ein hundertseítiges Compliance-Buch schreiben müssen. Es bedeutet aber:

- Sie sollten aufschreiben können, welche IT-Sicherheitsmaßnahmen Sie getroffen haben.
- Sie sollten nachweisen können, dass Sie Ihr Team geschult haben.
- Sie sollten dokumentieren, welche Verträge mit Dienstleistern bestehen.
- Sie sollten einen Notfallplan haben.

Warum? Weil Sie im Schadensfall zeigen müssen, dass Sie “alles Notwendige getan haben”.

3.6. Was Sie jetzt wissen sollten

Am Ende dieses Kapitels sollte Ihnen klar sein:

- Es gibt drei unterschiedliche rechtliche Systeme, die alle für Ihre Praxis gelten.
- Sie ersetzen sich nicht gegenseitig – sie ergänzen sich.
- Eine saubere IT-Sicherheitsmaßnahme erfüllt meist alle drei gleichzeitig.
- Sie persönlich als Arzt tragen die strafrechtliche Verantwortung.
- Dokumentation ist der Nachweis, dass Sie Ihre Verantwortung erfüllen.

In den nächsten Kapiteln werden wir uns diese drei Ebenen einzeln anschauen.

3.7. § 203 StGB: Strafrechtliche Schweigepflicht und IT-Sicherheit

Dieses Kapitel erklärt eine einzelne Vorschrift – aber sie ist existenziell für Ihren Praxisalltag.

3.7.1. Was § 203 StGB schützt

§ 203 Abs. 1 Nr. 1 StGB stellt das unbefugte Offenbaren von fremden Geheimnissen unter Strafe. Konkret heißt das für Ärzte:

"Ärzte, Zahnärzte und andere Heilpersonen, die zur Berufsausübung berechtigt sind, dürfen Geheimnisse, insbesondere Patientengeheimnisse, die ihnen in dieser Eigenschaft bekannt geworden sind, nicht verraten."

Das ist eine personale Schweigepflicht. Ein Arzt in der Praxis, in der Klinik, in einer Beratung unterliegt der Schweigepflicht.

Die Strafe: Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bis zu 360 Tagessätze. Eine einjährige Haftstrafe bedeutet: Ihre Approbation ist weg. Ihre Praxis ist zu. Ihr ganzes berufliches Leben ist damit beschädigt.

3.7.2. Was als „Geheimnis" gilt – eine weite Definition

Das Zentrale ist die Definition von "Geheimnis". Der Gesetzgeber hat das weit definiert – es ist nicht nur eine bestimmte Datenkategorie, sondern alles, das eine Person dem Arzt im Vertrauen offenbaren würde.

Das gilt: Diagnose und Prognose, Behandlung und Medikation, Befunde und Untersuchungsergebnisse, Therapieverlauf, Anamnese. Selbst die bloße Tatsache, dass jemand Patient bei Ihnen ist, kann ein Geheimnis sein.

Zeitlich gilt die Schweigepflicht unbegrenzt. Auch wenn ein Patient lange verstorben ist oder die Behandlung Jahre zurückliegt – die Schweigepflicht bleibt bestehen.

3.7.3. Garantenpflicht und Tun durch Unterlassen

Hier kommt der zentrale Punkt für IT-Sicherheit: Die Schweigepflicht ist nicht nur eine Verpflichtung, selbst kein Geheimnis zu verraten. Sie ist auch eine Garantenpflicht.

Das heißt konkret: Wenn Sie fahrlässig dafür sorgen, dass ein Patientengeheimnis nach außen dringt – nicht, weil Sie es selbst verraten, sondern weil Sie es zulassen –, dann haben Sie eine Straftat begangen.

Beispiele: Sie lassen Ihren Server unverschlüsselt. Ransomware bricht ein. Sie verwenden ein einfaches Passwort. Ein Hacker bricht ein. Sie haben keinen Notfallplan. Der IT-Dienstleister fällt weg. Sie haben das Geheimnis nicht selbst "verraten" – aber durch Unterlassen die Offenbarung ermöglicht.

> **Merksatz:** Unzureichende IT-Sicherheit kann selbst dann eine Verletzung der Schweigepflicht darstellen, wenn Sie persönlich kein Patientengeheimnis weitergegeben haben.

3.7.4. Die Reform von 2017: Externe Dienstleister werden legal

Bis 2017 war die Lage problematisch: Die Beauftragung eines externen IT-Dienstleisters konnte als "Offenbaren" eines Geheimnisses gewertet werden.

Mit der Reform 2017 hat der Gesetzgeber das geändert. Der neue § 203 Abs. 3 Satz 2 StGB sagt: "Das Offenbaren eines Geheimnisses ist nicht strafbar, wenn…die Offenbarung für die ordnungsgemäße Erbringung der Leistung erforderlich ist."

Das heißt: Es ist legal, einen IT-Dienstleister zu beauftragen.

Aber: Es gibt eine zentrale Bedingung – der Berufsgeheimnisträger muss dafür sorgen, dass dieser Dienstleister "zur Geheimhaltung verpflichtet werden".

3.7.5. Die Hilfspersonenvereinbarung nach § 203 Abs. 4 StGB

Das ist das zentrale Dokument: die Hilfspersonenvereinbarung.

Viele Praxisinhaber meinen, ein Auftragsverarbeitungsvertrag (AVV) nach Art. 28 DSGVO reiche aus. Das ist falsch. Der AVV ist eine datenschutzrechtliche Anforderung. Aber § 203 StGB ist Strafrecht – und Strafrecht und Datenschutzrecht sind zwei separate Regelungssysteme.

§ 203 Abs. 4 Satz 2 StGB macht es explizit: Der Berufsgeheimnisträger wird strafbar, "wenn eine mitwirkende Person ein ihr bekanntes Geheimnis unbefugt offenbart und der Berufsgeheimnisträger nicht bereits zuvor dafür gesorgt hatte, dass diese Person zur Geheimhaltung verpflichtet [wurde]."

Das Wort "bereits zuvor" ist entscheidend. Die Verpflichtung muss erfolgen, bevor der Dienstleister überhaupt Zugriff auf Patientendaten bekommt – nicht nachträglich.

Eine Hilfspersonenvereinbarung nach § 203 StGB muss mindestens folgendes enthalten:

- Die ausdrückliche Verpflichtung zur Geheimhaltung aller Patientengeheimnisse
- Die Belehrung über die strafrechtlichen Folgen einer Verletzung
- Das Need-to-know-Prinzip: Der Dienstleister hat nur Zugriff, der notwendig ist
- Eine Regelung, wie Subunternehmer eingesetzt werden dürfen – und müssen verpflichtet sein

  Merksatz: AVV (Datenschutz) + Hilfspersonenvereinbarung (Strafrecht) = Mindestanforderung für externe Dienstleister.

3.7.6. Praktische Konsequenz: Der IT-Dienstleister-Check

Das heißt für Ihre Praxis konkret: Für jeden externen Dienstleister, der möglicherweise Zugriff auf Patientendaten bekommt, brauchen Sie:

1. Einen gültigen AVV nach Art. 28 DSGVO
2. Eine Verschwiegenheitsverpflichtung nach § 203 Abs. 4 StGB

Das gilt für: Den lokalen IT-Dienstleister vor Ort, den Cloud-Anbieter der Praxissoftware, den Anbieter der Backup-Lösung, den Softwarewartungsdienst, jeden Anbieter mit Fernwartungs-Zugriff.

Praktisches Vorgehen:

- Erstellen Sie eine Liste aller Dienstleister
- Prüfen Sie für jeden: Liegt ein AVV vor? Liegt eine Verschwiegenheitsverpflichtung vor?
- Fehlende Dokumente: Fordern Sie sie an
- Dokumentieren Sie, dass die Verpflichtung vor dem Zugriff erfolgt ist
- Überprüfen Sie regelmäßig, dass die Verträge noch aktuell sind

---

3.7.7. Checkliste: § 203 StGB und IT-Sicherheit

- ☐ Ich verstehe, dass § 203 StGB eine persönliche strafrechtliche Verpflichtung ist.
- ☐ Ich habe eine Liste aller Dienstleister mit Zugriff auf Patientendaten.
- ☐ Für jeden Dienstleister prüfe ich: Liegt ein AVV vor? Liegt eine Verschwiegenheitsverpflichtung nach § 203 vor?
- ☐ Die Verpflichtungen liegen VOR dem ersten Zugriff vor.
- ☐ Meine Dienstleisterverträge enthalten das Need-to-know-Prinzip.
- ☐ Wenn ein Dienstleister Subunternehmer einsetzt, sind diese ebenfalls vertraglich verpflichtet.
- ☐ Bei externen Dienstleistern mit Sitz außerhalb der EU habe ich überprüft, ob ein vergleichbares Schutzniveau besteht.
- ☐ Ich habe einen Plan, wie ich die Zusammenarbeit beende, wenn ein Dienstleister die Anforderungen nicht erfüllt.
- ☐ Die Verträge werden mindestens jährlich überprüft.

3.8. DSGVO in der Arztpraxis – Datenschutz neben der Schweigepflicht

Die DSGVO gilt zusätzlich zu § 203 StGB, nicht statt dessen. Was das bedeutet, und wo die praktischen Anforderungen für Ihre Praxis liegen.

3.8.1. DSGVO und § 203 StGB sind unterschiedlich – aber nicht gegensätzlich

Hier ist eine Quelle der Verwirrung: Viele meinen, wenn sie die DSGVO erfüllen, erfüllen sie automatisch auch die Schweigepflicht. Das stimmt nicht ganz.

Die DSGVO regelt, wie personenbezogene Daten verarbeitet werden – wer sie erheben darf, zu welchem Zweck, wie lange sie gespeichert werden dürfen.

§ 203 StGB regelt, ob Geheimnisse offenbart werden dürfen – gar nicht, wenn nicht mit Einwilligung.

Beide Systeme verlangen also Schutzmaßnahmen. Praktisch verlangen sie oft die gleichen Maßnahmen. Aber die rechtliche Grundlage ist unterschiedlich.

> **Merksatz:** DSGVO und § 203 StGB sind zwei separate Regelungssysteme. Sie konkurrieren nicht – sie ergänzen sich.

3.8.2. Warum Gesundheitsdaten in der DSGVO besonders sind

Die DSGVO unterscheidet zwischen normalen personenbezogenen Daten und "besonderen Kategorien" nach Art. 9 DSGVO. Gesundheitsdaten gehören zu den besonderen Kategorien.

Das heißt konkret: Die Verarbeitung von Gesundheitsdaten ist grundsätzlich verboten – es sei denn, es gibt einen Ausnahmegrund. Für Arztpraxen ist der Ausnahmegrund klar: Art. 9 Abs. 2 lit. h DSGVO erlaubt die Verarbeitung "zur Sicherstellung oder Verbesserung der Gesundheitsversorgung durch einen Angehörigen eines medizinischen Berufs."

Das heißt: Sie dürfen Gesundheitsdaten verarbeiten – aber nur für Patienten, die Sie behandeln, und nur zu dem Zweck der Behandlung.

3.8.3. Art. 32 DSGVO: Technische und organisatorische Maßnahmen (TOMs)

Art. 32 DSGVO verpflichtet Sie, angemessene technische und organisatorische Maßnahmen zu ergreifen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Das klingt juristisch kompliziert. Praktisch bedeutet es: Ihre IT-Sicherheitsmaßnahmen müssen dem Risiko entsprechen, das von der Verarbeitung Ihrer Daten ausgeht.

Für eine Arztpraxis sind Gesundheitsdaten hochrisikant. Das heißt: Der Schutzbedarf ist hoch. Art. 32 konkretisiert:

- **Vertraulichkeit** – Verschlüsselung, Passwörter, Zugangsschutz
- **Integrität** – Backups, Prüfsummen
- **Verfügbarkeit** – Redundante Systeme, Notfallpläne
- **Fähigkeit zur raschen Wiederherstellung** – Backup-Strategien, Disaster Recovery

Das ist nicht alles theoretisch abstrakt. Es bedeutet konkret für Ihre Praxis: Sie brauchen Verschlüsselung, sichere Passwörter, Backups, regelmäßige Updates.

3.8.4. Das Verzeichnis von Verarbeitungstätigkeiten (VVT) – Art. 30 DSGVO

Art. 30 DSGVO verpflichtet Sie, ein Verzeichnis zu führen, in dem dokumentiert ist, welche personenbezogenen Daten Sie verarbeiten, zu welchem Zweck, auf welcher Rechtsgrundlage.

Das klingt nach Bürokratie. Es ist aber praktisch wertvoll. Denn wenn Sie wissen, welche Daten Sie haben und wo sie liegen, können Sie im Schadensfall schnell reagieren, der Behörde nachweisen, dass Sie Ihre Pflichten erfüllen, und beurteilen, welche Sicherheitsmaßnahmen notwendig sind.

Das VVT muss für Arztpraxen folgende Punkte dokumentieren:

- Verarbeitungstätigkeiten: Patientenverwaltung, Rechnungsstellung, Abrechnung
- Zweck: Behandlung, Abrechnung, Buchhaltung
- Betroffene: Patienten, Rechnungsempfänger
- Datenkategorien: Name, Adresse, Gesundheitsdaten, Abrechnungsdaten
- Speicherdauer: 10 Jahre für Medikationen und Befunde (nach § 630g BGB)
- Empfänger: Krankenkassen, Steuerberater, Buchhaltungssoftware-Anbieter
- Technische Maßnahmen: Verschlüsselung, Zugangsschutz, Backup

Das VVT kann eine einfache Tabelle sein – muss nicht in juristischem Deutsch verfasst sein. Es muss aber vollständig und aktuell sein.

3.8.5. Datenpannen – Art. 33 und 34 DSGVO

Das ist der Punkt, an dem Theorie und Praxis zusammentreffen. Wenn bei Ihnen eine Datenpanne vorkommt – Ransomware, Diebstahl eines Laptops, gehacktes Praxis-System – müssen Sie reagieren.

Art. 33: Meldung an die Behörde (72-Stunden-Frist)

Wenn eine Datenpanne voraussichtlich ein Risiko für die Rechte und Freiheiten natürlicher Personen birgt, müssen Sie sie der zuständigen Datenschutzbehörde melden – innerhalb von 72 Stunden nach Kenntnis der Panne.

72 Stunden sind nicht viel. Sie müssen wissen, welche Daten betroffen sind, wie viele betroffene Personen es gibt, was die möglichen Folgen sind, welche Maßnahmen Sie ergriffen haben.

Art. 34: Benachrichtigung betroffener Personen

Wenn eine Datenpanne ein hohes Risiko für betroffene Personen birgt – etwa wenn unverschlüsselte Patientendaten gestohlen wurden – müssen Sie diese Personen benachrichtigen.

Wichtig: Wenn die Daten verschlüsselt waren und der Schlüssel nicht kompromittiert wurde, ist die Benachrichtigungspflicht entfallen. Das ist ein konkretes Argument für Verschlüsselung.

3.8.6. Checkliste: DSGVO in der Arztpraxis

- ☐ Ich habe ein Verzeichnis von Verarbeitungstätigkeiten (VVT) erstellt oder überprüft.
- ☐ Das VVT dokumentiert alle wesentlichen Verarbeitungen: Patientenverwaltung, Rechnungsstellung, Abrechnung.
- ☐ Für jede Verarbeitung ist eine Rechtsgrundlage benannt.
- ☐ Aufbewahrungsfristen sind dokumentiert – besonders die 10-Jahres-Frist für medizinische Dokumentation.
- ☐ Mit allen Dienstleistern liegt ein AVV vor, der TOMs konkretisiert.
- ☐ Falls Website vorhanden: Aktuelle Datenschutzerklärung ist vorhanden.

- ☐ Ich weiß, wie ich im Fall einer Datenpanne reagiere – insbesondere die 72-Stunden-Frist.
- ☐ Ich kenne die Kontaktdaten meiner zuständigen Landesdatenschutzbehörde.

3.9. Die Hilfspersonenvereinbarung – Das vergessene Dokument

Ein Dokument, das Tausende von Praxen übersehen – und das im Schadensfall den Unterschied macht zwischen strafrechtlicher Haftung und Rechtssicherheit.

3.9.1. Was ist der Unterschied zwischen AVV und Hilfspersonenvereinbarung?

Das ist die zentrale Verwirrung: Viele Praxisinhaber meinen, ein Auftragsverarbeitungsvertrag (AVV) nach Art. 28 DSGVO sei ausreichend. Das ist falsch.

Ein AVV ist ein datenschutzrechtliches Dokument. Es regelt, wie der Auftragnehmer personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Eine Hilfspersonenvereinbarung ist ein strafrechtliches Dokument. Sie regelt, dass ein Dienstleister, der möglicherweise Zugriff auf Patientengeheimnisse hat, zur Geheimhaltung verpflichtet wird.

Das ist kein semantischer Unterschied. Es ist ein rechtlicher Unterschied.

Ohne Hilfspersonenvereinbarung ist die Beauftragung des IT-Dienstleisters strafrechtlich fragwürdig – und Sie als Praxisinhaber tragen die Verantwortung.

> **Merksatz:** AVV = Datenschutz. Hilfspersonenvereinbarung = Strafrecht. Beides ist erforderlich.

3.9.2. Wer braucht eine Hilfspersonenvereinbarung?

Die Antwort ist einfach: Jede Person oder Firma, die möglicherweise Zugriff auf Patientendaten oder andere Patientengeheimnisse bekommt.

Das umfasst: IT-Dienstleister vor Ort, Cloud-Anbieter, Backup-Anbieter, Software-Wartungsdienste, Fernwartungs-Software-Anbieter, Cyber-Security-Dienstleister, Datenlösch-Dienste.

Das ist nicht begrenzt auf große Firmen. Auch ein Freelancer-Programmierer braucht eine Hilfspersonenvereinbarung, wenn er dabei möglicherweise Patientendaten sieht.

3.9.3. Die Vertragskette – Subunternehmer und Sub-Subunternehmer

Hier wird es kompliziert: Ein IT-Dienstleister hat oft selbst Subunternehmer. Sie beauftragt IT-Dienstleister A mit dem lokalen Support. A beauftragt Cloud-Provider B mit dem Hosting. B nutzt Sicherheitsdienst C.

Alle drei haben potenziellen Zugriff auf Ihre Patientendaten. Und § 203 StGB sagt: Sie sind verantwortlich, dass die ganze Kette verpflichtet ist.

Das heißt konkret: - Sie schließen mit IT-Dienstleister A eine Hilfspersonenvereinbarung - A verpflichtet Cloud-Provider B vertraglich zur Geheimhaltung - B verpflichtet Sicherheitsdienst C vertraglich zur Geheimhaltung - Das muss alles dokumentiert und überprüft sein

Wenn die Kette bricht – etwa weil C nicht verpflichtet ist und dann Patientendaten nach außen dringen – dann haftet am Ende auch Sie.

3.9.4. Was muss in einer Hilfspersonenvereinbarung stehen?

§ 203 Abs. 4 Satz 2 StGB schreibt vor, dass der Dienstleister "zur Geheimhaltung verpflichtet" sein muss. Konkret sollte die Vereinbarung folgendes enthalten:

3.9.4.1. 1. Explizite Verpflichtung zur Geheimhaltung

"Der Dienstleister verpflichtet sich, alle Patientengeheimnisse im Sinne des § 203 StGB vertraulich zu behandeln und nicht weiterzugeben."

3.9.4.2. 2. Belehrung über strafrechtliche Folgen

"Eine unbefugte Offenbarung eines Patientengeheimnisses ist eine Straftat nach § 203 Abs. 4 StGB und wird mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe geahndet."

Das ist nicht Einschüchterung – das ist rechtliche Klarheit.

3.9.4.3. 3. Need-to-know-Prinzip

"Der Dienstleister darf sich nur insoweit Kenntnis von Patientengeheimnissen verschaffen, als die Erbringung seiner Leistung das erfordert."

3.9.4.4. 4. Regelung von Subunternehmern

"Der Dienstleister darf Subunternehmer nur mit vorheriger schriftlicher Zustimmung einschalten. Subunternehmer müssen ebenfalls schriftlich zur Geheimhaltung verpflichtet werden."

3.9.4.5. 5. Zeitliche Geltung

"Die Verschwiegenheitspflicht besteht zeitlich unbegrenzt – auch nach Beendigung der Zusammenarbeit."

3.9.4.6. 6. Rückgabe und Löschung

"Nach Beendigung der Zusammenarbeit werden alle Patientendaten gelöscht oder zurückgegeben."

3.9.5. Praktisches Vorgehen: Schritt für Schritt

Schritt 1: Liste aller Dienstleister erstellen

Machen Sie eine Liste aller Dienstleister, die momentan mit Ihrer Praxis arbeiten. IT-Support, Cloud-Hosting, Backup, Softwarewartung, ggf. Webdesigner, ggf. Rechtsanwalt, ggf. Steuerberater.

Schritt 2: Für jeden Dienstleister prüfen

Prüfen Sie: Liegt ein AVV vor? Liegt eine Hilfspersonenvereinbarung vor? Wenn beide vorhanden sind: Sind sie aktuell?

Schritt 3: Fehlende Dokumente anfordern

Schreiben Sie dem Dienstleister: "Für die Zusammenarbeit brauchen wir einen Auftragsverarbeitungsvertrag nach Art. 28 DSGVO und eine Verschwiegenheitsverpflichtung nach § 203 Abs. 4 StGB."

Die meisten größeren Dienstleister haben Standarddokumente.

Schritt 4: Unterschreiben und archivieren

Wenn die Vereinbarungen vorliegen, unterschreiben Sie und archivieren Sie sicher. Sie brauchen diese Dokumente, wenn die Behörde Sie fragt oder ein Schadensfall eintritt.

Schritt 5: Jährlich überprüfen

Überprüfen Sie mindestens jährlich, ob alle Dokumente noch vorhanden und aktuell sind.

3.9.6. Bitkom-Mustervorlage

Der Bitkom e.V. hat Musterdokumente zur Verfügung gestellt, die einen guten Ausgangspunkt bieten. Sie finden Sie auf: `bitkom.org` (Suche: "Muster § 203 StGB")

3.9.7. Checkliste: Hilfspersonenvereinbarungen in Ihrer Praxis

- ☐ Ich habe eine Liste aller Dienstleister, die Zugriff auf Patientendaten haben.
- ☐ Für jeden Dienstleister prüfe ich: Liegt ein AVV vor? Liegt eine Verschwiegenheitsverpflichtung nach § 203 vor?
- ☐ Die Vereinbarungen sind unterschrieben und archiviert.
- ☐ Jede Vereinbarung enthält explizit die Verpflichtung zur Geheimhaltung nach § 203 StGB.
- ☐ Jede Vereinbarung enthält eine Belehrung über strafrechtliche Folgen.
- ☐ Jede Vereinbarung regelt das Need-to-know-Prinzip.
- ☐ Falls der Dienstleister Subunternehmer einsetzt, ist vertraglich geregelt, dass diese ebenfalls verpflichtet werden.
- ☐ Ich habe einen Plan, wie die Zusammenarbeit beendet wird, wenn ein Dienstleister Anforderungen nicht erfüllt.
- ☐ Die Vereinbarungen werden mindestens jährlich überprüft.

4. Teil 3: Die digitale Infrastruktur einer Arztpraxis

4.1. Die Praxis ist mehr als ein Netzwerk

Stellen Sie sich vor: Eine Ihrer Arzthelferinnen kommt morgens herein, startet ihren Laptop, und er bootet nicht. Der Bildschirm bleibt schwarz. Sie greifen zum nächsten Computer – auch dort ein Problem. Dann merken Sie: Der Server geht nicht mehr auf. Die Praxisverwaltungssoftware ist unerreichbar. Patientendaten lassen sich nicht abrufen. Der ganze Betrieb steht still.

Das ist keine Fantasie. Es passiert regelmäßig – und meist nicht durch einen spektakulären Hacker-Angriff, sondern durch etwas viel Alltäglicheres: Ein Laptop wurde gestohlen. Eine externe Festplatte fiel und zerbrach. Ransomware verschlüsselte die Festplatte eines Praxis-PCs. Der Internet-Router fiel aus. Ein Datensicherungs-Gerät, das eigentlich die Rettung sein sollte, war seit Monaten nicht getestet worden.

Eine Arztpraxis ist ein IT-System – auch wenn die meisten Ärztinnen und Ärzte sich selbst nicht als IT-Profis verstehen. Diese Infrastruktur ist nicht optional. Sie ist heute so kritisch wie der Stromkreis oder das Telefonnetz. Und wie bei diesen Systemen gilt: Man denkt darüber erst nach, wenn etwas ausfällt.

Dieses Kapitel behandelt die **digitale Grundinfrastruktur** einer Arztpraxis – was vorhanden ist, warum es kritisch ist, und wie Sie es stabil und sicher halten.

4.2. Was gehört zur Praxis-Infrastruktur?

Die Infrastruktur einer niedergelassenen Praxis besteht typischerweise aus mehreren Komponenten, die alle zusammenhängen:

Die Endgeräte – Laptop, Desktop-PCs, Drucker, Scanner, möglicherweise Tablets für Hausbesuche. Das sind die Arbeitsplatzrechner, auf denen täglich Patientendaten verarbeitet werden. Jedes dieser Geräte ist potenziell ein Einfallstor für Sicherheitsprobleme.

Das Netzwerk – WLAN und kabelgebundene Verbindungen verbinden die Geräte miteinander. In einer modernen Praxis ist das WLAN oft sowohl für Mitarbeiter als auch für Patienten vorhanden – was eine Trennung erfordert.

Der Internet-Anschluss – DSL, Glasfaser oder mobiles Internet. Das ist die Verbindung nach draußen – zum TI-Konnektor (Telematik-Infrastruktur), zu Cloud-Diensten, zu E-Mail-Servern. Ein Ausfall hier lahmt die ganze Praxis.

Der Server oder die Server-Lösung – Wenn es einen zentralen Server gibt (oft bei mittleren oder größeren Praxen), speichert dieser die Praxisverwaltungssoftware und zentrale Datenbestände. Bei kleineren Praxen kann das auch eine Cloud-Lösung sein. Der Server ist das Rückgrat.

Datensicherungs-Systeme – Backups auf externe Festplatten, auf einem NAS, in der Cloud oder einer Kombination aus allem. Das ist die Versicherung gegen Datenverlust.

Sicherheitsgeräte und -software – Router mit integrierter Firewall, eventuell eine dedizierte Firewall, Antivirus-Software, der eHBA (elektronischer Heilberufsausweis) mit PIN-Verwaltung, Verschlüsselung.

Zusatzdienste – Der TI-Konnektor für die sichere Verbindung zur Telematik-Infrastruktur, optional Cloud-Dienste für Terminkalender oder Buchhaltung, VPN für sichere Fernverbindungen.

Alle diese Komponenten müssen zusammenpassen. Ein modernes Antivirus-Programm hilft nicht, wenn die Festplatte nicht verschlüsselt ist. Ein perfektes Backup ist nutzlos, wenn es nie getestet wird. Ein sicherer eHBA bringt nichts, wenn das Passwort auf einem Post-it am Monitor steht.

4.3. Warum die Infrastruktur kritisch ist

Patientendaten sind geschützt – durch das Strafgesetzbuch (§ 203 StGB), durch die Datenschutzgrundverordnung (DSGVO), durch die Berufsordnung. Wer mit sensiblen Gesundheitsdaten umgeht, trägt auch eine rechtliche Verantwortung für deren Sicherheit. Ein Datensicherungsbruch ist nicht nur ein technisches Problem – es ist eine Straftat.

Betriebsfähigkeit ist existenzbedrohend – Wenn die Praxis-IT ausfällt, kann niemand arbeiten. Kein Zugriff auf Patientenakten bedeutet auch keine Abrechnung mit der Krankenkasse. Mehrere Tage Ausfall gefährden nicht nur den Betrieb, sondern auch das Vertrauen von Patienten.

Der Schaden ist exponentiell – Ein Sicherheitsproblem, das klein beginnt, kann sich schnell ausbreiten. Ransomware breitet sich in wenigen Stunden über das ganze Netzwerk aus. Ein mit Schadsoftware infizierter PC kann zum Ausgangspunkt für einen Kettenbrief werden, der auch die Systeme von Laborpartnern oder überweisenden Kollegen befällt.

Die Abhängigkeiten sind unterschätzt – Viele Praxen wissen nicht genau, von wem ihre Systeme abhängen. Wer betreut den Server? Wer aktualisiert die Software? Was passiert, wenn der externe IT-Dienstleister nicht mehr erreichbar ist? Diese fehlende Dokumentation ist selbst schon ein Risiko.

4.4. Die Kapitel dieses Teils

Die nächsten acht Kapitel adressieren die kritischen Bereiche der Praxis-Infrastruktur:

Kapitel 3-01: Passwörter & Zwei-Faktor-Authentifizierung. Im Praxis-Alltag kompliziert: mehrere Helferinnen an einem PC, individuelle eHBA-PINs, Passwort-Manager im Netzwerk. Wie organisiert man das sicher?

Kapitel 3-02: Backups & Datensicherung. Was muss alles gesichert werden – PVS-Daten, Bilddaten, TI-Konfiguration? Die 3-2-1-Regel gilt auch hier, aber mit gesetzlichen Aufbewahrungsfristen für Patientenakten.

Kapitel 3-03: Endgeräte absichern. Von automatischer Sperrung über Updates bis zur sicheren Entsorgung.

Kapitel 3-04: Verschlüsselung. Warum Festplattenverschlüsselung ein Muss ist, und welche zusätzlichen Verschlüsselungsschichten sinnvoll sind.

Kapitel 3-05: Internetzugang absichern. TI-Verbindung, Fallback-Lösungen bei Ausfällen, sicheres WLAN.

Kapitel 3-06: Cloud-Dienste in der Arztpraxis. Welche Cloud-Dienste für welche Daten erlaubt sind – und welche nicht.

Kapitel 3-07: Zugänge für Dritte. IT-Dienstleister, Wartungstechniker, Labore – sichere Fernwartung und Rechteverwaltung.

Kapitel 3-08: Firewall. Was die Fritz!Box leisten kann, und wann eine echte Firewall notwendig wird.

Jedes dieser Kapitel behandelt ein spezifisches technisches Thema – aber immer mit dem Blick auf die Praxis-Realität. Was ist machbar ohne externe Berater? Was sollte man delegieren? Was muss die Arztin oder der Arzt verstehen, um gute Entscheidungen zu treffen?

4.5. Checkliste: Grundlagen der Praxis-Infrastruktur

- ☐ Ich habe einen Überblick über alle Komponenten meiner Praxis-IT (Server, Router, Backup-Systeme, eHBA, etc.).
- ☐ Ich weiß, wer welche Komponente betreut oder administriert.
- ☐ Es gibt eine einfache Dokumentation der Praxis-IT – wo diese liegt, weiß mindestens noch eine weitere Person.
- ☐ Alle Mitarbeiter wissen, dass Patientendaten sensibel sind und unter Datenschutz stehen.
- ☐ Ich oder mein IT-Dienstleister haben einen Plan für den Fall eines IT-Ausfalls.
- ☐ Das Backup wurde zuletzt getestet – nicht nur ein Dateien-Restore, sondern auch die Wiederherstellungszeit geprüft.

4.6. Passwörter & Zwei-Faktor-Authentifizierung in der Arztpraxis

4.6.1. Das Passwort-Dilemma: Wer arbeitet an welchem Gerät?

Eine typische Szene: Die Praxis-Rezeption sitzt an zwei PCs. Der erste PC ist für die Terminverwaltung zuständig. Der zweite für Abrechnung und Dokumentation. Morgens kommt Petra an, mittags kommt Simone. Beide brauchen Zugriff auf die Patientenakten, aber auf unterschiedliche Funktionen der Software.

Wenn Sie beide Arzthelferinnen mit dem gleichen Passwort ausstatten, können Sie später nicht mehr nachvollziehen, wer welche Änderung vorgenommen hat. Das ist ein Dokumentations- und Kontrollproblem – aber auch aus datenschutzrechtlicher Sicht problematisch, denn die DSGVO verlangt, dass Zugriffe auf Patientendaten protokollierbar sind.

Die Lösung heißt: **Jede Person hat ihren eigenen Login.** Das ist nicht optional, sondern Pflicht. Das bedeutet:

Jede Arzthelferin, jede Ärztin, jeder Arzt hat einen eigenen Benutzer-Account im Betriebssystem. Sie sperren den PC nach sich ab oder nutzen eine automatische Sperrung nach fünf bis zehn Minuten Inaktivität. Wenn die nächste Person den PC nutzen möchte, meldet sie sich mit ihren eigenen Anmeldedaten an.

Das klingt aufwändig. In der Praxis funktioniert es, wenn es zur Routine wird – und es ist unverzichtbar, weil es die einzige Möglichkeit ist, zu dokumentieren, wer wann auf welche Patientendaten zugegriffen hat.

> **Wichtig:** Ein Praxis-PC, der öffentlich zugänglich ist, muss durch eine automatische Sperrung nach kurzer Inaktivität geschützt werden. Sonst liest jeder Patient mit, der nach dem Arzt im Wartezimmer sitzt.

4.6.2. Der eHBA und seine PIN – die medizinische Identität

Der eHBA (elektronischer Heilberufsausweis) ist kein gewöhnlicher USB-Stick. Er ist das digitale Äquivalent Ihres Arztstempels. Mit dem eHBA signieren Sie digitale Rezepte, greifen auf die TI zu, und bei manchen Systemen auch auf kritische Patientenfunktionen.

Die PIN des eHBA ist das Passwort zu dieser Identität. Eine schwache PIN ist gleichbedeutend damit, dass jemand, der die PIN kennt, in Ihrem Namen handeln kann – Rezepte ausstellen, Befunde ansehen, oder technische Operationen durchführen.

Das Problem ist klassisch: Die PIN wird aufgeschrieben. Und wo wird sie aufgeschrieben? Oft auf dem Post-it, das am Monitor über dem eHBA-Leser klebt. Das ist auch pragmatisch verständlich – niemand kann sich mehrere verschiedene PINs merken. Aber es ist nicht sicher.

Die beste Lösung: Ein Passwort-Manager. Dieser speichert die eHBA-PIN verschlüsselt und ermöglicht es Ihnen, die PIN zu nutzen, ohne sie zu merken. Welche Passwort-Manager für die Praxis infrage kommen, klären wir gleich.

Alternativ – und das ist kein Ersatz für einen Manager, sondern nur als Notfall-Backup – die PIN an einem sicheren Ort aufbewahren, der nicht am Monitor klebt. Ein verschlossener Tresor, ein Schlüsselsafe, getrennt vom eHBA.

> **Merksatz:** Ein eHBA ohne Passwort-Manager ist wie ein Rezeptpad ohne Schloss. Schreiben Sie Ihre PIN nicht auf Post-its auf.

4.6.3. Die Praxisverwaltungssoftware (PVS) – Richtlinien des Herstellers nutzen

Die meisten Praxen setzen eine spezialisierte Praxisverwaltungssoftware ein – Titanium, MEDI, MEDISTAR, oder eine andere Lösung. Diese Software hat fast immer ein eingebautes Benutzer- und Recht-Management-System. Die PVS kann festlegen, welche Benutzerin welche Funktionen nutzen darf. Die Arzthelferin kann die Abrechnung vielleicht nicht einsehen, während der Arzt Zugang zu allen Funktionen hat.

Nutzen Sie diese Möglichkeiten – aber verlassen Sie sich nicht allein darauf.

Warum die PVS allein nicht reicht: In vielen Praxen liegen Daten nicht nur in der PVS. Es gibt Netzlaufwerke, auf denen Briefe, Befunde, Laborergebnisse oder eingescannte Dokumente abgelegt werden – am PVS vorbei. Außerdem sind viele PVS-Systeme so aufgebaut, dass ihre Datenbanken und Dateien auf Betriebssystemebene erreichbar sind. Wer Zugang zum Windows-Explorer oder zum Dateiserver hat, kann unter Umständen direkt auf die PVS-Datenbank zugreifen – ganz ohne PVS-Login.

Das bedeutet: **Sie brauchen mehrere Verteidigungsebenen.** Die PVS-Zugriffskontrolle ist eine davon. Aber genauso wichtig sind die Absicherung auf Betriebssystemebene (eigene Benutzerkonten, Dateiberechtigungen auf Netzlaufwerken) und auf Netzwerkebene (wer darf auf welche Freigaben zugreifen). Erst wenn alle drei Ebenen zusammenspielen, ist der Zugriff auf Patientendaten wirklich kontrolliert.

Konkret heißt das:

1. Jede Person in der Praxis hat einen eigenen Benutzer-Account in der PVS – mit einem starken Passwort, das nur diese Person kennt.
2. Das Passwort wird in einem Passwort-Manager gespeichert. Der Passwort-Manager läuft auf dem Praxis-Netzwerk (mehr dazu unten).
3. Die Passwort-Richtlinien der PVS sind aktiviert: mindestens 12 Zeichen, Großbuchstaben, Kleinbuchstaben, Zahlen, Sonderzeichen. Passwort-Wiederverwendung ist nicht erlaubt. Passwörter werden regelmäßig geändert (mindestens alle 90 Tage, besser alle 30 Tage).
4. Die Admin-Konten werden besonders behandelt: Der Admin-Account der PVS hat ein besonders starkes Passwort, das nur eine Person (meistens der IT-Dienstleister) kennt. Im Notfall kann der Arzt oder die Arztin dieses Passwort vom IT-Dienstleister anfordern, es wird aber danach sofort geändert.

Welche weiteren Passwort-Einstellungen die PVS hat, hängt vom Hersteller ab. Ihr IT-Dienstleister sollte ein Dokument haben, das diese Einstellungen dokumentiert.

4.6.4. Passwort-Manager für die Praxis – Sicherheit und Komfort

Das Kernproblem: Sie können sich nicht für jeden Account ein einzigartiges, starkes Passwort merken. Ein Passwort-Manager macht dieses Problem lösbar.

Für eine Arztpraxis gelten aber spezielle Anforderungen:

Erstens: Der Manager muss datenschutzkonform sein. Das bedeutet konkret: Das Master-Passwort ist lokal verschlüsselt, bevor es in irgendeine Cloud geht. Nur so haben Sie

volle Kontrolle über die Daten. Cloud-Synchronisierung kann optional sein (praktisch für mehrere Geräte), aber nicht erzwungen.

Zweitens: Mehrere Praxis-Mitarbeiter brauchen Zugriff – aber nicht auf alle Passwörter. Ein Passwort-Manager braucht ein Team-Feature, mit dem Sie Passwörter oder Passwort-Kategorien für bestimmte Personen freigeben können.

Drittens: Der Manager muss selbst gut dokumentiert sein. Wer kümmert sich um den Master-Passwort des Managers? Wer hat diese Verwaltungs-Rechte? Im Notfall – wenn der Passwort-Manager-Admin nicht erreichbar ist – muss ein zweiter Weg existieren, die kritischen Passwörter abzurufen.

Empfehlenswerte Passwort-Manager für Praxen:

Bitwarden – Open Source, kostenlose Version reicht oft, es gibt auch Enterprise-Versionen. Bitwarden kann selbst gehostet werden (das stellt mancher IT-Dienstleister zur Verfügung, was vollständige Kontrolle über die Daten gibt). Mit Team-Features können Sie Passwörter zwischen Mitarbeitern teilen. Dezentral, gut für Praxen, die maximale Kontrolle wünschen.

heylogin – Deutsches Unternehmen, passwortlos: Anmeldungen werden nicht mit Passwörtern bestätigt, sondern über Biometrie auf einem gekoppelten Smartphone. Das ist aus Sicherheitssicht sehr stark (kein Passwort kann gestohlen werden). Für Teams geeignet, da die Verwaltung zentralisiert ist. Kostet etwas, ist aber für Praxen eine saubere Lösung.

KeePassXC – Lokal, kein Cloud-Zwang. Die Passwort-Datei liegt auf der Praxis-Festplatte oder auf dem NAS und wird lokal mit einem Master-Passwort geschützt. Sie müssen sich um Updates und Sicherung selbst kümmern, haben aber maximale Kontrolle. Für Praxen mit IT-Unterstützung eine Option.

1Password – Kommerziell, sehr bedienungsfreundlich, kostenpflichtig. Für Praxen mit mehreren Mitarbeitern gibt es Business-Pläne. Gut, wenn Sie sich um die Technik nicht kümmern wollen und jemand das für Sie übernimmt.

Welchen Manager Sie wählen, ist weniger wichtig als das, dass Sie überhaupt einen nutzen. Sprechen Sie mit Ihrem IT-Dienstleister – er kennt wahrscheinlich schon die beste Lösung für Ihre Situation.

4.6.5. Zwei-Faktor-Authentifizierung – Besonders für KIM und Admin-Zugänge

Zwei-Faktor-Authentifizierung (2FA) bedeutet: Ein Passwort allein reicht nicht. Sie brauchen zusätzlich einen zweiten Faktor – typischerweise einen Code, den eine App oder ein Hardware-Schlüssel erzeugt.

Für eine Arztpraxis ist 2FA nicht überall nötig. Aber es gibt **kritische Bereiche**, wo 2FA Pflicht sein sollte:

KIM (Kommunikation im Medizinwesen). Der KIM-Zugang ist Ihre sichere E-Mail über die TI. Mit KIM können Sie vertrauliche Patienten-Mitteilungen austauschen. Der KIM-Account sollte 2FA haben – entweder TOTP (Time-based One-Time Password) oder – noch besser – über den eHBA selbst.

Administrations-Zugänge. Wer Admin-Rechte auf der PVS, dem Server oder dem Router hat, sollte 2FA nutzen.

E-Mail-Konto der Praxis. Das E-Mail-Konto ist oft der Schlüssel zu allem anderen – über E-Mail lassen sich andere Passwörter zurücksetzen. 2FA hier ist wichtig.

Praxis-Cloud-Dienste. Falls Sie Terminkalender, Buchhaltung oder andere Dienste in einer Cloud laufen haben, sollten diese 2FA haben – besonders wenn mehrere Mitarbeiter darauf zugreifen.

2FA funktioniert typischerweise über eine App auf dem Smartphone – Google Authenticator, Authy, oder integriert in einen Passwort-Manager. Alle 30 Sekunden erzeugt diese App einen neuen sechsstelligen Code. Bei der Anmeldung geben Sie das Passwort ein und dann noch den Code aus der App.

Das Problem: Was passiert, wenn das Smartphone weg ist? Hier kommt wieder die Frage nach Backup-Codes: Fast jeder Dienst, der 2FA anbietet, erzeugt beim Einrichten eine Liste mit Notfall-Codes. Diese müssen sicher aufbewahrt werden – nicht im selben Smartphone, das die 2FA-App hat.

Eine pragmatische Lösung für Praxen: Die Backup-Codes werden ausgedruckt, in einem verschlossenen Umschlag aufbewahrt und dem Tresor der Praxis vertraut. Wenn jemand sein Smartphone verliert und nicht mehr in seinen Account kommt, gibt es einen Weg, sich selbst wieder herein zu lassen.

4.6.6. Passwort-Hygiene im Alltag – praktische Regeln

Mehrere Menschen, mehrere Systeme, mehrere Passwörter. Wie bringt man Struktur rein?

Regel 1: Kein doppeltes Passwort. Jedes System hat ein eigenes Passwort. Besonders wichtig: Das Passwort der PVS ist nicht das gleiche wie das des Praxis-PCs, das nicht das gleiche wie das des Passwort-Managers.

Regel 2: Admin-Passwörter sind anders gelagert. Das Admin-Passwort der PVS, des Servers, des Praxis-Routers – diese kennt idealerweise nur der IT-Dienstleister. Wenn die Arztin es wissen muss: gespeichert im Passwort-Manager, nicht aufgeschrieben.

Regel 3: Passwort-Änderungen protokollieren. Wenn ein Passwort gewechselt wird, wird der neue Passwort-Manager aktualisiert. Alte Passwörter werden nicht wiederverwendet – zumindest nicht in absehbarer Zeit.

Regel 4: Beim Arbeitsumsatz (Urlaub, Kündigung) sofort handeln. Wenn eine Arzthelferin in den Urlaub geht, wird ihr Account deaktiviert (nicht gelöscht!). Wenn jemand die Praxis verlässt, werden alle ihre Zugänge entfernt.

> **Merksatz:** Ein Passwort-Manager ist die Basis. Zwei-Faktor-Authentifizierung ist ein Plus. Aber beide funktionieren nur, wenn die Passwörter selbst regelmäßig aktualisiert und systematisch verwaltet werden.

4.6.7. Checkliste: Passwörter & 2FA in der Arztpraxis

- ☐ Jede Person in der Praxis hat ihren eigenen Benutzer-Account auf den Praxis-PCs – nicht geteilt, nicht mit Standard-Passwort.
- ☐ Die automatische Sperrung nach Inaktivität ist aktiviert (5–10 Minuten).
- ☐ Ein Passwort-Manager ist installiert und wird für kritische Passwörter genutzt.
- ☐ Die eHBA-PIN ist im Passwort-Manager gespeichert – nicht auf einem Post-it am Monitor.
- ☐ Die PVS hat eigene Benutzer-Konten pro Person mit individuellen Passwörtern.
- ☐ Die Passwort-Richtlinien der PVS sind aktiviert (Mindestlänge, Komplexität, Ablauf).
- ☐ Der Admin-Account der PVS hat ein besonders starkes Passwort, das nicht leichtfertig weitergegeben wird.
- ☐ 2FA ist mindestens für KIM, Admin-Zugänge und das Praxis-E-Mail-Konto aktiviert.
- ☐ Für alle 2FA-Konten existieren Backup-Codes, die sicher aufbewahrt sind.
- ☐ Es gibt eine Offboarding-Checkliste für Mitarbeiter, die die Praxis verlassen – Passwörter werden geändert, Zugänge entzogen.
- ☐ Mindestens eine weitere Person in der Praxis kennt den Master-Passwort des Passwort-Managers (für Notfallzugriff).
- ☐ Regelmäßig (alle 90 Tage) werden kritische Passwörter geändert, besonders Admin-Passwörter.

4.7. Backups & Datensicherung in der Arztpraxis

4.7.1. Das Backup-Szenario: Wenn der Notfall eintritt

Es ist Montag morgens, 8 Uhr. Eine Ihrer Arzthelferinnen macht den Praxis-PC an – und bemerkt sofort etwas Seltsames. Der PC braucht länger zum Booten. Als er endlich oben ist, sehen die Dateien anders aus. Alle Dateinamen haben plötzlich eine neue Endung: .locked. Sie können kein PDF mehr öffnen, keine Bilddatei ansehen. Ein schwarzer Bildschirm erscheint mit einer Nachricht: „Ihre Daten wurden verschlüsselt. Um sie wiederherzustellen, überweisen Sie 50.000 Euro…"

Ransomware. Sie haben gerade Minuten, um zu entscheiden, was Sie tun. Der erste Instinkt ist oft, die Praxis-IT auszuschalten – was richtig ist. Aber jetzt brauchen Sie die Patientenakten. Ohne Backup sind sie weg. Mit Backup – aber nur, wenn es getestet und erreichbar ist – können Sie den Betrieb in wenigen Stunden wieder aufnehmen.

Das ist keine hypothetische Szene. Viele Arztpraxen müssen durch diese Situation gehen. Und ob sie danach noch Daten haben oder nicht, hängt fast vollständig davon ab, wie gut die Backups waren.

4.7.2. Die 3-2-1-Regel – auch für Arztpraxen

Ein bewährtes Backup-Prinzip lautet 3-2-1:

- **3 Kopien** Ihrer Daten (Original plus zwei Backups)
- **2 verschiedene Speichermedien** (z. B. lokale Festplatte und Cloud, oder Festplatte und NAS)

- **1 Kopie außerhalb der Praxis** (Offsite-Backup)

Für eine Arztpraxis konkret könnte das aussehen:

- Kopie 1: Die live-Daten auf dem Praxis-Server oder in der Cloud-PVS
- Kopie 2: Ein tägliches Backup auf ein NAS im Büro
- Kopie 3: Ein wöchentliches Backup auf eine externe Festplatte, die in einem Safe eines Bankschließfaches oder bei einem IT-Dienstleister aufbewahrt wird

Das klingt nach Aufwand. In der Praxis läuft das nach der Einrichtung größtenteils automatisch – der Server sichert sich selbst über Nacht, das NAS macht täglich ein Backup, die externe Festplatte wird jede Woche von der IT-Servicefirma getauscht.

> **Merksatz:** Wenn Sie nur an einem Ort ein Backup haben und dieser Ort (Ihre Praxis) abbrennt, haben Sie kein Backup mehr. Mindestens eine Kopie muss physisch woanders sein.

4.7.3. Was muss alles gesichert werden?

Bevor man eine Backup-Strategie aufsetzt, braucht man eine klare Antwort auf die Frage: Was sind die kritischen Daten meiner Praxis? Die Antwort ist immer spezifischer als man denkt.

Patientendaten. Alles, was der Betrieb der Praxis unmittelbar braucht: die PVS-Datenbank, Bilddaten (DICOM), Laborrückläufer und externe Befunde. Das ist das Herzstück – wenn diese Daten weg sind, ist die Praxis auf Papier zurückgeworfen. Was genau gesichert werden muss, hängt von der eingesetzten Praxissoftware und der Infrastruktur ab – dazu mehr in Teil 5.

Infrastruktur-Konfiguration. Router-Einstellungen, Passwort-Manager-Dateien, VPN-Konfigurationen, Firewall-Regeln, TI-Konnektor-Einstellungen. Diese werden oft vergessen – aber ihre Wiederherstellung dauert im Notfall länger als das Einspielen der eigentlichen Daten.

Buchführung und Finanzen. Rechnungseingang, Laborabrechnungen, Gehaltsabrechnung – oft in der PVS integriert, manchmal separat geführt.

Was **nicht** systematisch gesichert werden muss: Handbücher, Schulungsmaterialien, Software-Installationspakete. Diese sind nice-to-have, nicht kritisch.

4.7.4. Gesetzliche Aufbewahrungsfristen – ein Backup ist nicht genug

Hier kommt eine wichtige rechtliche Komponente: Patientenakten müssen aufbewahrt werden. Wie lange?

Nach § 630f BGB (Bürgerliches Gesetzbuch): **10 Jahre nach Behandlungsende.**

Das bedeutet: Ein Backup, das Sie nach zwei Jahren löschen, ist nicht ausreichend. Ihre Backup-Strategie muss sicherstellen, dass Patientenakten mindestens 10 Jahre erhalten bleiben – nicht nur die aktuellen, sondern auch die alten.

Ein Hinweis für Praxen, die Kinder und Jugendliche behandeln: Die 10-Jahres-Frist läuft ab Behandlungsende – nicht ab Volljährigkeit. Bei früh abgeschlossenen Behandlungen

können die Unterlagen also noch während der Minderjährigkeit aufbewahrungspflichtig ablaufen. Manche Ärztekammern empfehlen hier aus Vorsicht eine längere Aufbewahrung. Klären Sie das im Zweifel mit Ihrer Ärztekammer oder einem auf Medizinrecht spezialisierten Anwalt.

Praktisch heißt das:

Alte Backups werden nicht einfach überschrieben. Sie werden langfristig archiviert – entweder auf separaten Speichermedien, die verschlüsselt in einem Archiv aufbewahrt werden, oder in einer Cloud mit entsprechend langer Aufbewahrung. Manche Praxen nutzen dafür ein separates WORM-Speichersystem (Write Once, Read Many) – ein Speicher, auf den man nur einmal schreiben kann und der danach unveränderlich bleibt.

Ihr IT-Dienstleister sollte ein Konzept für diese Langzeitarchivierung haben. Falls nicht, müssen Sie das klären.

4.7.5. Backup-Häufigkeit und Restore-Test

Wie oft sollte eine Arztpraxis Backups machen?

Mindestens täglich. Für eine Praxis, in der täglich Patientenakten angelegt und aktualisiert werden, ist ein tägliches Backup das Minimum. Ein Ransomware-Angriff, der nachts passiert, darf nicht zwei Tage alte Daten kosten.

Stündlich, wenn möglich. Größere oder technisch gut ausgestattete Praxen machen stündliche inkrementelle Backups (die nur die Änderungen seit dem letzten Backup speichern). Das reduziert den Datenverlust auf maximal eine Stunde.

Aber – und das ist wichtig – ein Backup, das nie getestet wurde, ist kein Backup. Es ist eine Hoffnung.

Restore-Test: Mindestens alle drei Monate sollten Sie eine Datei aus dem Backup zurück einspielen und überprüfen, ob sie intakt und vollständig ist. Einmal im Jahr sollte ein vollständiger Restore-Test stattfinden: Kann das gesamte System aus dem Backup wiederhergestellt werden? Wie lange dauert das? Sind alle Daten vollständig?

Diese Tests müssen dokumentiert werden. Datum, Uhrzeit, Ergebnis, eventuelle Probleme. Im Notfall ist dieses Dokument der Beweis dafür, dass die Backups funktionieren.

> **Merksatz:** Ein Backup, das Sie nie getestet haben, ist wie Feuer auf einem Rettungsboot – es sieht gut aus, bis es passiert.

4.7.6. Ransomware-Resilienz: Offline und Air-Gapped Backups

Ransomware ist das größte Bedrohungsszenario für Arztpraxen. Die Schadsoftware durchsucht beim Befall aktiv alle erreichbaren Laufwerke und verschlüsselt sie. Eine externe Festplatte, die dauerhaft am Praxis-Server hängt, wird genauso verschlüsselt wie die Original-Daten.

Das bedeutet: Ein Backup, das erreichbar ist, ist kein Schutz vor Ransomware.

Die Lösung ist **Offline-Backup** oder **Air-Gapped Backup**:

Offline-Backup. Das Backup-Laufwerk ist nur während des Backup-Prozesses angeschlossen – danach wird es physisch getrennt und eingelagert. Was nicht erreichbar ist, kann nicht verschlüsselt werden. Das ist die einfachste Lösung für kleine bis mittlere Praxen.

Air-Gapped Backup. Das Backup-System läuft in einer Netzwerk-Umgebung, die vom Praxis-Netzwerk vollständig isoliert ist. Idealerweise mit eingenetem Admin-Account und Firewall-Regeln, die verhindert, dass das System von außen erreichbar ist. Technisch aufwendiger, aber für größere Praxen sinnvoll.

Immutable Backups in der Cloud. Manche Cloud-Backup-Anbieter (z. B. Backblaze, Wasabi) unterstützen Object Lock – eine Funktion, die gespeicherte Backups für einen definierten Zeitraum vor Löschung schützt. Selbst ein Angreifer mit Admin-Zugriff kann diese Backups nicht löschen. Für Praxen, die Cloud-Backups nutzen, ist das eine saubere Lösung.

Eine pragmatische Kombination für viele Praxen: Tägliches lokales Backup (schnell, einfach zu restore), wöchentliches Offline-Backup auf externe Festplatte (Ransomware-Schutz), monatliches Cloud-Backup für die absolute Notfallsicherung.

4.7.7. Backup-Verschlüsselung

Backups sind Kopien von Patientendaten. Eine unverschlüsselte Backup-Festplatte, die gestohlen wird oder verloren geht, ist ein Datenschutzverstoß – und meldepflichtig nach der DSGVO.

Alle Backups sollten verschlüsselt sein, besonders wenn sie außerhalb der Praxis aufbewahrt werden:

- Externe Festplatten: BitLocker (Windows) oder FileVault (Mac)
- NAS-Laufwerk: Verschlüsselung auf Ordner- oder Volume-Ebene (Synology, QNAP)
- Cloud-Backups: Verschlüsselung durch den Backup-Provider (Backblaze, Arq)

Der Verschlüsselungsschlüssel muss separat aufbewahrt werden – nicht auf der gleichen Festplatte. Ein Passwort-Manager ist auch hier die beste Lösung.

4.7.8. Backup-Verantwortung – wer macht's?

Das ist oft unklar in Praxen. Wer ist verantwortlich für das Backup?

- Der Praxis-Inhaber trägt die rechtliche Verantwortung.
- Der IT-Dienstleister trägt die technische Verantwortung.
- Es sollte schriftlich fixiert sein, wer was macht und wie oft.

Eine gute Vereinbarung mit dem IT-Dienstleister deckt folgende Punkte ab:

- Backup-Häufigkeit (täglich, stündlich?)
- Backup-Ort (lokal, Offsite, Cloud?)
- Restore-Test-Häufigkeit (quartalsweise, jährlich?)
- Verschlüsselung (ja, mit welcher Methode?)
- Archivierung alter Daten (wie lange, wo?)
- Notfall-Kontakt (wer ist erreichbar bei Datenverlust?)

- Kosten und SLA (Service Level Agreement)

Falls Sie keinen IT-Dienstleister haben, sollten Sie sich einen holen – zumindest für die Backup-Strategie.

4.7.9. Checkliste: Backups & Datensicherung

- ☐ Ich habe mindestens drei Kopien meiner kritischen Daten – Original plus zwei Backups.
- ☐ Meine Backups liegen auf mindestens zwei verschiedenen Medien oder Typen (z. B. NAS + externe Festplatte + Cloud).
- ☐ Mindestens eine Backup-Kopie befindet sich außerhalb der Praxis.
- ☐ Ich sag klar: Welche Daten müssen gesichert werden? (PVS, DICOM-Bilder, Labordaten, TI-Konfiguration, etc.)
- ☐ Die Backup-Häufigkeit ist festgelegt – täglich ist das Minimum, stündlich ist besser.
- ☐ Ich führe regelmäßig Restore-Tests durch (mindestens quartalsweise einzelne Dateien, jährlich vollständig).
- ☐ Die Restore-Test-Ergebnisse sind dokumentiert.
- ☐ Meine Backups sind verschlüsselt – besonders externe Festplatten und Cloud-Backups.
- ☐ Der Verschlüsselungsschlüssel ist separat und sicher aufbewahrt.
- ☐ Für Ransomware-Schutz: mindestens ein Backup ist offline oder air-gapped (nicht dauerhaft angeschlossen).
- ☐ Ich beachte die Aufbewahrungsfrist für Patientenakten (10 Jahre nach Behandlungsende) – alte Backups werden archiviert, nicht überschrieben.
- ☐ Mit meinem IT-Dienstleister ist schriftlich geklärt, wer für das Backup verantwortlich ist und wie oft es getestet wird.
- ☐ Im Notfall kenne ich die Restore-Zeit – wie lange dauert es, den Betrieb wieder hochzufahren?

4.8. Endgeräte absichern

4.8.1. Der offene Praxis-PC – eine ständige Gefahr

Stellen Sie sich folgende Situation vor: Nach einer Sprechstunde sitzt ein Patient noch im Wartezimmer. Die Arzthelferin hat sich gerade angemeldet und die Patientenakte des nächsten Patienten aufgerufen – voller sensibler Informationen. Sie dreht sich um, um etwas zu kopieren. Der Patient, der noch sitzt, kann in diese Zeit hinein direkt auf den Monitor schauen. Er sieht Namen, Diagnosen, Befunde des nächsten Patienten.

Das ist nicht nur ein Datenschutzproblem – es ist auch eine Frage von Menschenwürde und Vertrauen. Patienten wollen nicht, dass andere ihre Akte sehen.

Die einfachste Lösung ist eine **automatische Sperrung nach kurzer Inaktivität.** Nach fünf bis zehn Minuten ohne Tastatur- oder Maus-Bewegung sperrt sich der Monitor – und wer weitermachen will, muss sich neu anmelden.

Das funktioniert, wenn es zur Standard-Einstellung wird und nicht überstimmt. Am besten: Der IT-Dienstleister konfiguriert das per Gruppen-Richtlinie (Group Policy in Windows), sodass Nutzer es nicht einfach deaktivieren können.

> **Wichtig:** Automatische Sperrung ist nicht optional für eine Arztpraxis. Sie ist Datenschutz-Pflicht.

4.8.2. Updates und Patch-Management – eine geteilte Verantwortung

Software-Updates sind langweilig und unterbrechen die Arbeit. Sie sind aber die erste Verteidigungslinie gegen bekannte Sicherheitslücken. Ein Praxis-PC, der Monate ohne Updates läuft, ist nicht nur unmodern – er ist ein bekanntes Angriffsziel.

In einer Arztpraxis entsteht oft Verwirrung: Wer ist für Updates zuständig? Der Arzt selbst? Die Arzthelferin? Der IT-Dienstleister?

Die Antwort: Das muss schriftlich geklärt sein.

Automatische Updates (Best Practice):

Das Betriebssystem sollte automatisch Updates einspielen – Windows und macOS unterstützen das. Der Update-Prozess sollte nachts laufen oder so geplant sein, dass die Praxis-Arbeit nicht unterbrochen wird. Nach einem Update kann ein Neustart erforderlich sein – auch das sollte zeitlich geplant sein (Freitag nachts, nicht Montag morgens vor der Sprechstunde).

Browser und Browser-Plugins:

Browser aktualisieren sich meist automatisch, aber nur, wenn sie regelmäßig beendet werden. Ein Browser, der Wochen lang offen läuft, bekommt Updates erst beim nächsten Neustart. Für kritische Browser (besonders wenn sie zur Authentifizierung oder zum Zugriff auf die PVS genutzt werden) sollte monatlich ein Neustart zur Routine werden.

Browser-Plugins sind eine separate Baustelle – oft werden sie vergessen. Ein veraltetes Flash-Plugin oder ein Adobe-Reader ohne Updates sind bekannte Angriffsvektoren. Regel: Nur die Plugins installieren, die wirklich nötig sind. Alles andere deinstallieren.

Praxisverwaltungssoftware (PVS):

Die PVS hat oft keine automatischen Updates. Sie müssen manuell geprüft werden – monatlich, mindestens quartalsweise. Der Hersteller gibt Sicherheits-Patches heraus, oft mit deutlichen Hinweisen auf ihre Wichtigkeit. Der IT-Dienstleister oder der PVS-Hersteller sollte dafür verantwortlich sein. Es sollte aber auch dokumentiert sein, wann das letzte Update war.

Medizinische Spezial-Software (PACS für Bilddaten, Labor-Schnittstellen, etc.): Auch diese brauchen regelmäßige Updates. Ein PACS-System, das zwei Versionen veraltet ist, kann Sicherheitslücken haben, die aktiv ausgenutzt werden.

Router-Firmware:

Wer denkt an den Router? Meist wird der einmal installiert und danach ignoriert. Die Router-Firmware sollte mindestens einmal jährlich geprüft werden – bei der Fritz!Box unter `fritz.box` → System → Update.

NAS-Firmware (falls vorhanden):

Ähnlich wie der Router – das NAS-Betriebssystem und installierte Apps müssen aktuell sein. Synology und QNAP machen regelmäßig Sicherheits-Updates.

Eine gute Vereinbarung mit dem IT-Dienstleister regelt, wer wann Updates macht. Eine Checkliste, die dokumentiert, wann Updates durchgeführt wurden, ist die Basis für die Kontrolle.

4.8.3. Shared Workstations – mehrere Nutzer, sichere Logs

Es ist typisch für Arztpraxen: Mehrere Arzthelferinnen arbeiten an den gleichen PCs – nacheinander oder parallel (wenn es mehrere Geräte gibt). Jede braucht Zugriff auf die PVS, aber jede darf nur ihre eigenen Funktionen nutzen.

Das ist kein IT-Problem allein – es ist auch ein Praxis-Management-Problem. Aber die technische Lösung ist klar:

Separate Windows-Benutzer-Accounts für jede Person. Keine gemeinsamen Accounts. Das ist nicht nur für die Sicherheit wichtig, sondern auch für die Dokumentation – später muss klar sein, wer wann was gemacht hat.

Die PVS-Software selbst hat dann noch eine zweite Ebene von Nutzerverwaltung. Das ist gut so – Double-Check sorgt für Sicherheit.

Ablauf im Alltag:

1. Petra kommt morgens an, meldet sich mit ihrem Windows-Account an
2. Sie arbeitet in der PVS (die hat auch einen Petra-Account mit ihren Rechten)
3. Sie geht zur Mittagspause – sie sperrt den PC (Windows-Taste + L)
4. Simone kommt zurück, meldet sich mit ihrem Windows-Account an
5. Sie arbeitet in der PVS mit ihren Rechten
6. Am Abend werden beide User loggt aus und der PC gesperrt

Das funktioniert, wenn es zur Routine wird. Der IT-Dienstleister kann auf dem PC auch eine Gast-Session einrichten – für den Fall, dass eine externe Person schnell etwas prüfen muss, ohne einen eigenen Account zu haben.

4.8.4. Mobile Geräte für Hausbesuche – Tablets und Notebooks

Immer mehr Praxen nutzen Tablets oder Notebooks für Hausbesuche – um direkt beim Patienten die Akte zu sehen, Befunde zu dokumentieren oder auch nur zur Kommunikation mit der Praxis.

Das ist praktisch. Es bringt aber auch Risiken:

Was darf auf einem mobilen Gerät sein?

- Ja: Die Praxisverwaltungssoftware (wenn der Provider das unterstützt)
- Ja: Ein sicherer Remote-Zugang zur Praxis-Datenbank (VPN + Passwort-geschützte Anwendung)
- Nein: Unkindierte Kopien von Patientendaten
- Nein: Passwörter in Notizen oder E-Mails

- Nein: Unverschlüsselte Backup-Dateien

Ein Tablet, das auf Hausbesuchen mitgenommen wird und verloren geht, darf nicht unverschlüsselt Patientenakten enthalten. Das ist ein datenschutzrechtlicher Notfall.

Praktische Regeln für mobile Geräte:

- Vollständige Geräteverschlüsselung ist Pflicht
- Starke Authentifizierung – mindestens 6-stelliger PIN, besser biometrisch
- VPN, wenn der Zugriff auf die Praxis-Datenbank remote passiert
- Regelmäßige Updates – mobile Geräte sind nicht von Sicherheitslücken ausgenommen
- Fernlösch-Funktion aktiviert – im Fall des Verlusts können Sie das Gerät aus der Ferne löschen
- Keine automatische Synchronisierung von Patientendaten in die private Cloud des Tablets

4.8.5. BYOD – Bring Your Own Device. Warum es problematisch ist

Die Versuchung ist groß: Eine Arzthelferin fragt, ob sie ihren privaten Laptop mitbringen darf, um in der Praxis-Cloud zu arbeiten. Oder ein Arzt möchte sein iPhone nutzen, um KIM zu überprüfen.

Kurze Antwort: Das ist problematisch und sollte minimalisiert werden.

BYOD bedeutet, dass private Geräte auf Praxis-Daten zugreifen. Das bringt folgende Probleme mit sich:

Datenschutz. Ein privates Gerät ist privat versichert, private gesichert, privat administriert. Die Kontrolle über Patientendaten ist nicht gewährleistet. Das ist ein DSGVO-Problem.

Sicherheit. Das private Gerät hat möglicherweise andere Antivirus-Software, andere Update-Prozesse, möglicherweise auch private Daten gemischt mit Praxis-Daten. Die Praxis hat keine Kontrolle.

Rechtshaftung. Wenn der Laptop der Arzthelferin gehackt wird und Patientendaten kompromittiert werden, wer haftet? Unklar.

Besser: Praxis-Geräte für Praxis-Daten. Die Praxis stellt Notebooks, Tablets oder sogar Smartphones zur Verfügung, wenn mobiler Zugriff nötig ist. Diese werden wie Praxis-PCs behandelt – regelmäßig aktualisiert, verschlüsselt, überwacht.

Falls die Nutzung von privaten Geräten ausnahmsweise erlaubt ist (z. B. zum Abrufen von KIM auf dem privaten iPhone), dann sollte es klare Grenzen geben: nur Lesen, keine Download, Zwei-Faktor-Authentifizierung, und die Praxis-App wird nach Gebrauch gelöscht.

> **Merksatz:** Private Geräte für private Daten, Praxis-Geräte für Patientendaten. Eine Vermischung ist ein Datenschutz- und Sicherheitsrisiko.

4.8.6. Altgeräte: Sichere Entsorgung

Ein alter Praxis-PC wird ausgemustert. Was passiert mit ihm?

Viele Menschen denken: Ein einfaches Löschen der Festplatte reicht. Das ist falsch. Gelöschte Dateien können mit speziellen Tools wiederhergestellt werden – selbst nach dem Formatieren.

Sichere Entsorgung bedeutet:

- **Festplatte schreddern** – Physische Vernichtung. Die Festplatte wird in einem zertifizierten Shredder-Service zerlegt. Das ist sicher, und es gibt Entsorgungsbetriebe, die das für wenig Geld machen.
- **Sichere Löschung (Disk Wiping)** – Software, die die Festplatte mehrfach mit Zufallsdaten überschreibt – nach dem Standard NIST SP 800-88 oder besser. Tools wie DBAN (Darik's Boot and Nuke) tun das. Es braucht aber Zeit und Sorgfalt.
- **Ganzsystem-Neuinstallation** – Der PC wird komplett neu aufgesetzt, mit neuer Lizenz. Aber das ist weniger sicher als Schreddern – Überreste könnten bleiben.

Für eine Arztpraxis mit sensibler Patientenakten ist **Festplattenschreddern die sicherste Variante.** Es kostet meist zwischen 50 und 100 Euro pro Gerät. Danach haben Sie ein Zertifikat über die sichere Entsorgung – was auch dokumentarisch wichtig ist, falls es später Fragen gibt.

Der IT-Dienstleister sollte sich um die Entsorgung kümmern. Falls nicht, müssen Sie einen spezialierten Entsorgungsbetrieb kontaktieren.

4.8.7. Checkliste: Endgeräte

- ☐ Automatische Sperrung ist auf allen Praxis-PCs aktiviert (nach 5–10 Minuten Inaktivität).
- ☐ Das Betriebssystem hat automatische Updates aktiviert.
- ☐ Der Browser wird regelmäßig neugestartet – mindestens monatlich – um Updates einzuspielen.
- ☐ Browser-Plugins sind auf das Nötigste reduziert; veraltete werden regelmäßig überprüft.
- ☐ Die PVS-Software wird mindestens quartalsweise auf Updates geprüft.
- ☐ Andere medizinische Software (PACS, Labor-Schnittstellen) wird regelmäßig aktualisiert.
- ☐ Router-Firmware wird mindestens jährlich geprüft und bei Verfügbarkeit aktualisiert.
- ☐ NAS-Firmware und Pakete werden regelmäßig aktualisiert (falls NAS vorhanden).
- ☐ Jede Person in der Praxis hat ihren eigenen Windows-Benutzer-Account – keine gemeinsamen Accounts.
- ☐ Mit dem IT-Dienstleister ist schriftlich geklärt, wer für Updates zuständig ist.
- ☐ Mobile Geräte (Tablets, Notebooks) für Hausbesuche sind vollständig verschlüsselt.
- ☐ Mobile Geräte haben die Fernlösch-Funktion aktiviert.
- ☐ BYOD ist minimalisiert – nur in Ausnahmefällen und mit klaren Grenzen erlaubt.
- ☐ Ausgemusterte Geräte werden sicher entsorgt – Festplattenschreddern ist dokumentiert.

- ☐ Es existiert eine Übersicht aller Praxis-Geräte (Alter, Betriebssystem, Wartungsstatus).

4.9. Verschlüsselung – Das letzte Sicherheitsnetz

4.9.1. Warum Verschlüsselung für Arztpraxen nicht optional ist

Das Szenario ist einfach und real: Ein Laptop wird aus einer Praxis gestohlen. Oder eine externe Backup-Festplatte geht im Umzug verloren. Oder ein Tablet mit Patientendaten wird im Taxi vergessen.

Ohne Verschlüsselung sind diese Daten für jeden lesbar, der das Gerät öffnet. Mit Verschlüsselung sind sie wertlos – ohne den richtigen Schlüssel.

Aus rechtlicher Perspektive ist das nicht nur gut für die Sicherheit, sondern auch eine Pflicht. Das Strafgesetzbuch (§ 203 StGB) schützt das Berufsgeheimnis von Ärzten. Die Datenschutzgrundverordnung (DSGVO) verlangt eine „Verarbeitung personenbezogener Daten mit angemessenen Mitteln". Für Gesundheitsdaten ist Verschlüsselung eine dieser Mittel.

Und praktisch: Ein unverschlüsselter USB-Stick mit Patientendaten ist nicht nur ein Sicherheitsrisiko – es ist im schlimmsten Fall eine Straftat.

> **Merksatz:** In einer Arztpraxis ist Verschlüsselung nicht die höchste Sicherheitsstufe – sie ist die Mindestanforderung.

4.9.2. Festplattenverschlüsselung – Standard auf allen Praxis-PCs

Das Erste und Wichtigste: die Festplatte des Computers, auf dem täglich gearbeitet wird.

Moderne Betriebssysteme haben eingebaute Verschlüsselungsfunktionen, die einfach zu nutzen sind:

Windows – BitLocker:

Windows 10 und 11 Pro/Enterprise haben BitLocker. Die Aktivierung passiert unter Systemsteuerung → BitLocker-Laufwerkverschlüsselung. Alternativ: Windows Home nutzt eine vereinfachte Geräteverschlüsselung, die automatisch aktiv ist, sobald Sie sich mit einem Microsoft-Konto anmelden.

Wichtig: Microsoft speichert den BitLocker-Wiederherstellungsschlüssel standardmäßig im Online-Konto (Microsoft Cloud). Das ist praktisch – wenn Sie den Key verlieren, können Sie ihn wiederherstellen. Es ist aber auch ein Sicherheitsrisiko – Microsoft hat theoretisch Zugang zu Ihrem Verschlüsselungsschlüssel.

Sicherere Alternative: Deaktivieren Sie die Online-Speicherung des Keys und bewahren Sie den Key lokal auf – ausgedruckt oder im Passwort-Manager. Das ist aufwendiger (wer den Key verliert, verliert auch die Daten), ist aber sicherer: Nur Sie haben Zugang zu Ihren Daten.

macOS – FileVault:

Auf Apple-Computern heißt die Festplattenverschlüsselung FileVault. Sie finden sie unter Systemeinstellungen → Datenschutz & Sicherheit → FileVault. Auf Macs mit Apple Silicon ist FileVault aktiv, sobald Sie ein Benutzerpasswort gesetzt haben.

Den Wiederherstellungsschlüssel müssen Sie speichern – im Passwort-Manager oder ausgedruckt. Falls Sie den Key verlieren und Ihr Passwort vergessen, sind die Daten unwiederbringlich weg.

Linux – LUKS:

Wer Linux nutzt, hat LUKS (Linux Unified Key Setup) – typischerweise bei der Installation konfiguriert.

4.9.3. Smartphones und Tablets

Ein Smartphone ist eine vollwertiges Arbeitsgerät für Ärzte und Arzthelferinnen. Es speichert Passwörter, KIM-Zugang, möglicherweise auch Notizkarten mit Patienten-Informationen.

Das gute: Moderne iPhones und Android-Geräte verschlüsseln ihre Speicher standardmäßig, sobald eine Bildschirmsperre (PIN, biometrische Authentifizierung) eingerichtet ist.
Was Sie prüfen müssen:

- ☐ Ist eine starke Bildschirmsperre aktiviert? (mindestens 6 Ziffern, besser biometrisch)
- ☐ Das Gerät verschlüsselt dann automatisch

Bei älteren Geräten können Sie die Verschlüsselung auch manuell aktivieren – typischerweise in den Sicherheitseinstellungen unter „Geräteverschlüsselung" (Android) oder „Code" (iPhone).

4.9.4. USB-Sticks und externe Festplatten

Hier passiert oft Leichtsinn. Ein USB-Stick wird zur Datensicherung oder zum Transport von Patientendaten zwischen Geräten verwendet – und niemand verschlüsselt ihn.

Ein unverschlüsselter USB-Stick mit Patientendaten ist:

1. Ein Datenschutzrisiko
2. Ein Straftatrisiko (unverschlüsselte Patientendaten im öffentlichen Raum)
3. Ein Vertrauensproblem – falls verloren oder gestohlen

Lösungen:

Festplattenverschlüsselung mit BitLocker To Go (Windows): Externe USB-Laufwerke können mit BitLocker verschlüsselt werden. Wenn Sie den Stick an einen anderen Computer anschließen, wird Ihnen ein Passwort abgefragt.

FileVault für externe Laufwerke (macOS): Ähnlich – externe Festplatten können mit FileVault verschlüsselt werden.

VeraCrypt: Ein plattformübergreifendes Verschlüsselungstool, das auf Windows, macOS und Linux funktioniert. Sie erstellen ein verschlüsseltes Volumen auf dem USB-Stick. Aus Anwendersicht sieht es aus wie einen externen Ordner, der gelöst werden muss.

Hardware-verschlüsselte USB-Sticks: Es gibt USB-Sticks mit eingebautem Verschlüsselungs-Chip (z. B. IronKey). Diese sind praktisch, kosten aber mehr.

Regel für die Praxis: Kein USB-Stick mit Patientendaten ohne Verschlüsselung. Und der Passwort sollte sich vom eHBA-Passwort unterscheiden.

4.9.5. NAS-Verschlüsselung

Falls Ihre Praxis ein NAS-System hat (Synology, QNAP, oder ähnlich) – auch dort sollten sensible Daten verschlüsselt sein.

Beide Hersteller bieten Verschlüsselung auf Ordner- oder Volume-Ebene an. Das funktioniert transparent – Nutzer sehen keinen Unterschied, aber die Daten sind geschützt.

Praktische Frage: Soll ich alles verschlüsseln?

Nicht unbedingt. Ein NAS, das nur mit Praxis-Daten befüllt ist, kann selektiv verschlüsselt werden – zumindest die Ordner mit Patientendaten sollten geschützt sein. Ordner mit unkritischen Daten (Verwaltungsdokumente, IT-Dokumentation) können unverschlüsselt bleiben, um die Performance nicht zu belasten.

Der Verschlüsselungsschlüssel muss sicher aufbewahrt sein – im Passwort-Manager, nicht auf einem Post-it.

4.9.6. Cloud-Verschlüsselung – nicht blind vertrauen

Alle großen Cloud-Anbieter (Microsoft OneDrive, Google Drive, Dropbox) verschlüsseln Ihre Daten. Das ist richtig und wichtig. Aber es ist **Anbieter-seitige** Verschlüsselung – der Anbieter hat den Schlüssel, nicht Sie.

Das bedeutet: Der Anbieter kann Ihre Daten lesen. Behörden mit Gerichtsbeschluss können Zugang verlangen. Ein Hack auf die Anbieter-Server könnte zu Schlüssel-Kompromittierung führen.

Für besonders sensible Daten – Patientenakten in der Cloud – ist **clientseitige Verschlüsselung** die bessere Lösung. Das bedeutet: Sie verschlüsseln die Daten auf Ihrem Gerät, bevor sie in die Cloud gehen. Der Anbieter sieht nur unlesbares Datenmüll.

Praktische Tools für clientseitige Verschlüsselung:

Cryptomator: Open Source und kostenlos. Es erstellt einen verschlüsselten Tresor in Ihrem Cloud-Ordner. Dateien werden lokal verschlüsselt, bevor sie hochgeladen werden. Funktioniert mit Dropbox, OneDrive, Google Drive.

Boxcryptor / Nordlocker: Kommerzielle Alternativen mit zusätzlichen Features wie Team-Unterstützung.

Hinweis für Arztpraxen: Falls die PVS in der Cloud läuft und der Anbieter keine clientseitige Verschlüsselung anbietet, muss das mit dem PVS-Anbieter geklärt sein. Viele große PVS-Anbieter (z. B. Agfa, CGM, Medistar) betreiben Cloud-Infrastruktur, die DSGVO-konform ist – das sollte ausreichen.

4.9.7. Wiederherstellungsschlüssel – die oft vergessene Achillesferse

Alle Verschlüsselungssysteme haben ein Problem: Wenn Sie den Verschlüsselungsschlüssel vergessen oder verlieren, sind die Daten weg.

Deshalb generieren fast alle Systeme beim Aktivieren der Verschlüsselung einen **Wiederherstellungsschlüssel** – eine lange Zeichenfolge, mit der Sie Zugang wiederherstellen können, falls Sie den Hauptschlüssel verlieren.

Diese Schlüssel MÜSSEN sicher aufbewahrt werden:

- Ausgedruckt und in einem Tresor aufbewahrt (physisch, nicht digital)
- Im Passwort-Manager gespeichert
- Getrennt vom verschlüsselten Gerät aufbewahrt (nicht auf der gleichen Festplatte)

Eine gute Praxis-Dokumentation listet auf: Welche Geräte sind verschlüsselt, wo liegt der Wiederherstellungsschlüssel, wer hat Zugang?

4.9.8. Checkliste: Verschlüsselung

- ☐ Auf allen Praxis-PCs (Windows/macOS) ist Festplattenverschlüsselung aktiviert (BitLocker / FileVault).
- ☐ Die Wiederherstellungsschlüssel sind sicher aufbewahrt – getrennt von den Geräten.
- ☐ Bei BitLocker: Ich habe bewusst entschieden, ob der Schlüssel online oder lokal gespeichert wird.
- ☐ Alle Smartphones und Tablets haben eine starke Bildschirmsperre (mindestens 6 Ziffern).
- ☐ USB-Sticks mit Patientendaten sind verschlüsselt (BitLocker, VeraCrypt, oder Hardware-Verschlüsselung).
- ☐ Externe Backup-Festplatten sind verschlüsselt.
- ☐ Das NAS verschlüsselt mindestens die Ordner mit Patientendaten.
- ☐ Der NAS-Verschlüsselungsschlüssel ist im Passwort-Manager gespeichert.
- ☐ Falls Cloud-Services genutzt werden: Ich weiß, wie diese verschlüsselt sind (Anbieterseitig oder clientseitig).
- ☐ Für besonders sensible Cloud-Daten nutze ich clientseitige Verschlüsselung (z. B. Cryptomator).
- ☐ Alle Verschlüsselungsschlüssel sind dokumentiert – wo liegen sie, wer hat Zugang?
- ☐ Im Notfall (Schlüssel verloren) kenne ich den Wiederherstellungsprozess.

4.10. Internetzugang absichern

4.10.1. Der kritische Kanal – vom WLAN bis zur Telematik-Infrastruktur

Der Internetzugang einer Arztpraxis ist nicht nur eine Verbindung zum Surfen. Er ist der Kanal zu:

- Der TI (Telematik-Infrastruktur) – für E-Rezepte, KIM, Notfalldaten
- Der PVS-Cloud (falls die Software in der Cloud läuft)
- Der Laborschnittstelle

- Der E-Mail
- Der Videokonferenz (Telemedizin, Sprechstunde)

Ein Internetzugang-Ausfall paralysiert eine Praxis. Das passiert häufiger, als man denkt: Ein Baggerunfall trifft das Glasfaserkabel. Der Router wird defekt. Der Provider führt Wartungsarbeiten durch. Die DSL-Leitung wird instabil.

Auf all das haben Sie keinen Einfluss. Auf Vorbereitung haben Sie sehr wohl Einfluss.

4.10.2. Die Grundlage: Router-Sicherheit

Ein Router ist nicht nur ein Gerät – er ist ein konfiguriertes System. Und wie jedes System braucht auch ein Router Sicherheit und Wartung.

Router-Admin-Zugang:

Der Standard-Admin-Zugang (oft Admin/12345 oder ähnlich) ist ein Sicherheitsproblem. Der erste Schritt ist: **Passwort ändern** unter `fritz.box` → System → Fritz!Box-Benutzer (bei AVM Fritz!Box). Ein starkes, einzigartiges Passwort, gespeichert im Passwort-Manager.

Danach: Der Router sollte nur aus dem eigenen Netz administrierbar sein. Fernzugriff (von außen) ist standardmäßig deaktiviert – und sollte es bleiben, solange Sie ihn nicht bewusst aktivieren.

Firmware aktualisieren:

Die Router-Firmware sollte mindestens jährlich geprüft werden. Sicherheitslücken in Router-Software werden aktiv ausgenutzt. Bei Fritz!Box unter `fritz.box` → System → Update. Falls ein Update verfügbar ist, einspielen – am besten nachts, wenn die Praxis nicht arbeitet.

WLAN-Sicherheit:

Das WLAN sollte WPA3 (oder mindestens WPA2) nutzen – nicht WEP oder offenes WLAN. Das WLAN-Passwort sollte starker sein als typische Patient-Passwörter – mindestens 16 Zeichen, Großbuchstaben, Kleinbuchstaben, Zahlen.

Wichtig: Die Standard-SSID (der Name des WLANs) sollte geändert werden – nicht einfach „FRITZ!Box 7590" nennen, sondern etwas Generisches wie „Praxis_WLAN" oder ähnlich.

4.10.3. Praxisnetz Patientennetz – WLAN-Trennung ist Pflicht

Eine Arztpraxis hat oft ein WLAN für Mitarbeiter und ein WLAN für Patienten. Das ist kein Luxus – das ist eine Sicherheitsnotwendigkeit.

Ein Patient, der im WLAN sitzt, sollte nicht in der Lage sein, auf die Patientenakten aller anderen Patienten zuzugreifen. Dafür braucht es eine **WLAN-Trennung** – entweder durch zwei separate WLANs (von zwei verschiedenen Access Points) oder durch eine Gäste-WLAN-Funktion des Routers.

Praktisch:

- **Praxis-WLAN (intern):** Zugriffsschutz, starkes Passwort, Zugang zu Praxis-Servern, zu Cloud-Services, zur TI. Nur Mitarbeiter kennen das Passwort.
- **Gäste-WLAN (extern):** Offenes oder schwach gesichertes WLAN, nur Internetzugang, keine Verbindung zu Praxis-Systemen. Patienten können das nutzen, wenn sie möchten.

Die Fritz!Box hat eine Gäste-WLAN-Funktion unter System → Gäste-WLAN. Das ist ausreichend für viele Praxen. Größere Praxen können zwei separate Geräte einsetzen.

> **Wichtig:** Ein Patient im Gäste-WLAN sollte nicht in der Lage sein, auf Systeme im Praxis-Netz zuzugreifen. Das ist ein Netzwerk-Segmentierungs-Problem, das ein IT-Dienstleister konfigurieren muss.

4.10.4. TI-Verbindung – stabil und mit Fallback

Der TI-Konnektor ist das Gerät, das Ihre Praxis mit der Telematik-Infrastruktur verbindet. Ein Ausfall des Internets bedeutet kein Zugriff auf E-Rezepte, KIM oder Notfalldaten.

Die Anforderung: Eine stabile, durchgehende Internetverbindung.

Die Realität: Das Internet fällt manchmal aus.

Die Lösung: Ein Fallback – eine Backup-Verbindung, wenn die Hauptverbindung weg ist.

Praktische Optionen:

Zwei verschiedene Internet-Anschlüsse. DSL von Anbieter A und Glasfaser von Anbieter B. Falls der DSL ausfällt, läuft die TI noch über Glasfaser. Das ist teuer und nicht immer verfügbar, aber am sichersten.

Mobiler Internet-Router als Fallback. Ein 5G/LTE-Router (auch MiFi genannt) mit eigener SIM-Karte als Backup. Falls die Hauptverbindung ausfällt, schaltet man schnell um. Diese Router kosten 100–200 Euro und eine SIM-Karte mit wenig Datenvolumen kostet 10–20 Euro monatlich.

Smartphone-Hotspot als Not-Notfall. Das ist nicht ideal (begrenzte Bandbreite, Akku wird schnell leer), funktioniert aber für E-Mail und KIM kurzfristig.

Welche Variante sinnvoll ist, hängt von Ihrer Praxis-Situation ab. Ein IT-Dienstleister kann das einschätzen.

4.10.5. WLAN-Internetzugang absichern – die Fritz!Box-Härtung

Eine gut konfigurierte Fritz!Box ist bereits ein guter Schutz. Einige zusätzliche Maßnahmen reduzieren das Risiko weiter:

UPnP deaktivieren: Universal Plug and Play erlaubt Geräten, selbstständig Portfreigaben einzurichten – ohne Ihre Zustimmung. Schadsoftware kann das nutzen. Deaktivieren unter fritz.box → Heimnetz → Netzwerk → Heimnetzfreigaben (je nach Firmware).

Netzwerkfilter aktivieren: - NetBIOS-Filter schützt vor älteren Windows-Netzwerk-Anfragen (fritz.box → Internet → Filter) - DNS-Rebinding-Schutz verhindert Misdirect-Attacken - IPv6-Firewall sollte aktiv sein (fritz.box → Internet → Zugangsdaten → IPv6)

Portfreigaben überprüfen: Jede aktive Portfreigabe (fritz.box → Internet → Freigaben) ist ein potentieller Eingangskanal für Angreifer. Alles, was nicht aktiv gebraucht wird, sollte entfernt werden.

4.10.6. Fernzugriff – wenn überhaupt, dann sicher

Es gibt Szenarien, in denen ein Arzt von außerhalb auf die Praxis-Systeme zugreifen muss – Notfall nachts, Frage zum Patienten im Urlaub, oder generell mobiles Arbeiten.

Unsicher: Ein direkter Zugriff auf die Administrationsoberfläche des Routers oder auf Praxis-Systeme aus dem Internet.

Sicherer: Ein **VPN (Virtual Private Network)**, das Ihren externen Zugriff verschlüsselt.

Die Fritz!Box hat VPN-Funktionen (WireGuard, IPSec). Ein VPN-Zugang funktioniert so: Sie bauen von außen eine verschlüsselte Verbindung in Ihr Praxis-Netz auf – danach sind Sie im Netz, als würden Sie am Router selbst sitzen.

Zwei-Faktor-Authentifizierung für VPN ist wichtig – das Passwort allein ist nicht genug.

4.10.7. Öffentliche WLANs im mobilen Arbeitsalltag

Ärzte und Arzthelfer arbeiten nicht nur in der Praxis. Sie sind in Kliniken, im Homeoffice, im Cafe – überall mit WLAN.

Öffentliche WLANs sind das unsicherste Netzwerk, in dem Sie regulär arbeiten. Ein Angreifer im gleichen WLAN kann den Datenverkehr anderer Geräte mitlesen – besonders kritisch bei sensiblen Daten wie Patientenakten oder Passwörtern.

Schutz: Ein **VPN auf dem mobilen Gerät**, das den gesamten Internetverkehr verschlüsselt. Empfehlenswerte VPN-Anbieter: Mullvad (5 Euro monatlich), ProtonVPN (auch kostenlose Basis-Version), oder ein WireGuard-VPN, das Sie selbst betreiben.

Nicht nutzen: Kostenlose VPN-Anbieter von fragwürdiger Herkunft – viele davon finanzieren sich durch Weiterverkauf von Nutzerdaten.

Regel für die Praxis: Wenn Sie sich mit Patientendaten in einem öffentlichen WLAN anmelden müssen, nutzen Sie ein VPN. Besser noch: Nutzen Sie für sensible Arbeit den mobilen Hotspot des Praxis-Smartphones – das ist ein Netzwerk, das nur Sie kontrollieren.

4.10.8. Zugangsdaten und Router-Backup – für den Notfall

Wenn der Router kaputt geht, brauchen Sie schnell einen Ersatz. Das Problem: Wie richtet man den neuen Router ein, ohne die Zugangsdaten zu kennen?

Was Sie dokumentieren sollten:

- Zugangsdaten des Internetanschlusses (DSL/Glasfaser) – Benutzername und Passwort
- Das aktuelle Router-Backup (Export unter fritz.box → System → Sicherung)
- Das WLAN-Passwort (backup)
- Die Telefonnummer des Providers

Diese Daten gehören in Ihr Notfalldokument – an einem sicheren Ort, nicht im Router selbst.

Ein Router-Backup ist wertvoll, weil Sie damit auf einem neuen Gerät die gleiche Konfiguration einspielen können – WLAN-Einstellungen, Portfreigaben, VPN-Konfiguration, alles ist wiederhergestellt.

> **Merksatz:** Der Internetzugang ist so kritisch wie der Strom. Planen Sie für Ausfälle. Ein Fallback und dokumentierte Zugangsdaten kosten wenig und sparen im Notfall Stunden.

4.10.9. Checkliste: Internetzugang

- ☐ Das Router-Admin-Passwort ist nicht das Standard-Passwort – es ist stark und im Passwort-Manager gespeichert.
- ☐ Die Router-Firmware wird mindestens jährlich auf Updates geprüft und eingespielt.
- ☐ Das Praxis-WLAN und das Gäste-WLAN sind getrennt.
- ☐ Das Gäste-WLAN hat keinen Zugriff auf Praxis-Systeme (Netzwerk-Segmentierung).
- ☐ Die WLAN-Sicherheit ist WPA2 oder WPA3 – nicht WEP oder offen.
- ☐ Die Router-SSID wurde vom Standard-Namen geändert.
- ☐ UPnP ist deaktiviert.
- ☐ NetBIOS-Filter und DNS-Rebinding-Schutz sind aktiviert.
- ☐ IPv6-Firewall ist aktiv.
- ☐ Portfreigaben wurden überprüft – nur die nötigsten sind aktiv.
- ☐ Ein Internet-Fallback ist geplant oder vorhanden (zweiter Anschluss, mobiler Router, Hotspot).
- ☐ Falls Fernzugriff benötigt wird: VPN ist eingerichtet, nicht direkter Internet-Zugriff.
- ☐ Zwei-Faktor-Authentifizierung ist für VPN-Zugang aktiviert.
- ☐ Zugangsdaten des Internet-Anschlusses sind dokumentiert und im Notfalldokument.
- ☐ Ein Router-Backup ist gespeichert und getestet.
- ☐ Im mobilen Arbeitsalltag wird in öffentlichen WLANs ein VPN genutzt – besonders für sensible Daten.

4.11. Cloud-Dienste in der Arztpraxis

4.11.1. Das Missverständnis: Es geht nicht um Herkunft, sondern um Zertifizierung

Ein verbreitetes Missverständnis lautet: „US-Cloud ist verboten, europäische Cloud ist erlaubt." Das ist so nicht richtig.

Seit dem 10. Juli 2023 ist der **EU-US Data Privacy Framework** in Kraft – ein Angemessenheitsbeschluss der EU-Kommission, der den Datentransfer in die USA auf eine rechtlich anerkannte Grundlage stellt. Das Schrems-II-Urteil von 2020, das diese Grundlage damals aufgehoben hatte, ist durch diesen neuen Rahmen ersetzt worden. Das Europäische Gericht hat den Beschluss im September 2025 in einer Klage bestätigt. Er ist damit zum Stand März 2026 gültig – wenngleich politisch weiterhin nicht völlig stabil.

Für Arztpraxen ist die entscheidende Frage daher nicht: *Wo hat der Anbieter seinen Sitz?* Die entscheidende Frage ist: *Erfüllt der Cloud-Dienst die Anforderungen des § 393 SGB V?*

4.11.2. Was § 393 SGB V verlangt

Seit dem 1. Juli 2024 gilt für alle Cloud-Computing-Dienste, die Gesundheits- oder Sozialdaten im deutschen Gesundheitswesen verarbeiten, § 393 SGB V. Die Norm gilt unmittelbar für Cloud-Anbieter – aber als Arztpraxis tragen Sie die Verantwortung, nur zertifizierte Dienste einzusetzen.

Die Kernanforderungen:

C5-Typ-2-Testat des BSI. Cloud-Dienste, die Patientendaten verarbeiten, müssen seit dem 1. Juli 2025 ein gültiges C5-Typ-2-Testat des Bundesamtes für Sicherheit in der Informationstechnik (BSI) vorweisen. Das C5-Testat prüft anhand von 125 Kriterien in 17 Themenbereichen, ob ein Cloud-Dienst definierte Mindeststandards erfüllt – und beim Typ-2-Testat zusätzlich, ob diese Maßnahmen auch über einen längeren Zeitraum (typisch 6–12 Monate) wirksam waren. Das gilt für alle Anbieter – europäische wie amerikanische.

Datenspeicherort und Rechtsgrundlage für den Datentransfer. Hier kommt eine zweite Dimension ins Spiel, die vom C5-Testat unabhängig ist:

- *Daten werden in EU/EWR gespeichert:* Kein Problem – weder für europäische noch für US-Anbieter, die europäische Rechenzentren betreiben.
- *Daten werden in den USA verarbeitet oder gespeichert:* Dann braucht es zusätzlich zum C5-Testat eine rechtliche Grundlage für den Datentransfer. Der einfachste Weg: Der Anbieter ist nach dem **EU-US Data Privacy Framework (TADPF)** beim US-Handelsministerium zertifiziert. Alternativ sind EU-Standardvertragsklauseln (SCC) möglich – aber nur zusammen mit einer Transfer-Folgenabschätzung (Transfer Impact Assessment, TIA) und gegebenenfalls weiteren technischen Schutzmaßnahmen. Das ist deutlich aufwendiger.

Kundenseitige Anforderungen. Das C5-Testat prüft den Cloud-Anbieter – aber der Testat-Bericht enthält auch sogenannte „korrespondierende Kundenkriterien": Anforderungen, die der Anbieter prinzipiell nicht für Sie erfüllen kann, weil sie davon abhängen, wie Sie den Dienst nutzen. Das BSI dokumentiert diese im Testat-Bericht. Konkret geht es um:

- *Berechtigungsmanagement:* Wer in Ihrer Praxis hat Zugang zu welchen Daten? Das legt nicht der Anbieter fest, sondern Sie.
- *Protokollierung:* Viele Cloud-Dienste bieten Zugriffs-Logs an – diese müssen aktiviert und aufbewahrt werden.
- *Schlüsselverwaltung:* Falls der Dienst Ihnen Verschlüsselungsschlüssel aushändigt, liegt deren sichere Aufbewahrung bei Ihnen.
- *Eigene Risikoeinschätzung:* Das Testat ist generisch – Sie müssen prüfen, ob das geprüfte Sicherheitsniveau für Ihren konkreten Einsatzzweck ausreicht.

Ihr IT-Dienstleister sollte diese Punkte kennen und umsetzen.

> **Merksatz:** C5-Typ-2 ist für alle Anbieter Pflicht. Bei US-Anbietern, die Daten außerhalb der EU verarbeiten, kommt zusätzlich die TADPF-Zertifizierung dazu – oder der deutlich aufwendigere Weg über SCC und TIA. Ein europäischer Anbieter ohne C5-Testat ist genauso ungeeignet wie ein US-Anbieter ohne TADPF.

4.11.3. Die Übergangsregelung: Gleichwertige Zertifizierungen

Nicht alle Cloud-Anbieter haben bereits ein C5-Typ-2-Testat. Für diesen Fall hat das Bundesgesundheitsministerium die **C5-Gleichwertigkeitsverordnung** (C5GleichwV) erlassen – rückwirkend zum 1. Juli 2024 in Kraft.

Diese Verordnung erlaubt übergangsweise den Einsatz von Cloud-Diensten, die (noch) kein C5-Testat haben, aber eine gleichwertige Zertifizierung vorweisen können. Anerkannt sind:

- ISO/IEC 27001 (ggf. auf Basis BSI IT-Grundschutz)
- Cloud Controls Matrix (CCM) Version 4.0

Die Bedingung: Es reicht nicht, einfach ein ISO-27001-Zertifikat vorzulegen. Der Anbieter muss zusätzlich eine **GAP-Analyse** vorlegen, die dokumentiert, welche C5-Anforderungen durch das bestehende Zertifikat noch nicht abgedeckt sind – und einen verbindlichen Maßnahmenplan, wie diese Lücken geschlossen werden.

Die Fristen für den Übergang:

- Innerhalb von 12 Monaten: Schließung der identifizierten Lücken
- Innerhalb von 18 Monaten: Erlangung des C5-Typ-1-Testats
- Innerhalb von 24 Monaten: Erlangung des C5-Typ-2-Testats

Das bedeutet: Die Übergangsregelung ist keine Dauerlösung, sondern ein zeitlich begrenzter Weg zum vollständigen C5-Testat.

4.11.4. Was das für die Praxis bedeutet

Als Arztpraxis müssen Sie selbst kein C5-Testat haben. Sie müssen aber sicherstellen, dass die Cloud-Dienste, die Sie für Patientendaten einsetzen, die Anforderungen erfüllen. In der Praxis heißt das:

Fragen Sie Ihren IT-Dienstleister und Ihre Cloud-Anbieter konkret: Haben Sie ein aktuelles C5-Typ-2-Testat? Falls nicht: Haben Sie eine gleichwertige Zertifizierung plus GAP-Analyse und Maßnahmenplan nach der C5-Gleichwertigkeitsverordnung?

Bei US-Anbietern, die Daten außerhalb der EU verarbeiten: Zusätzlich fragen, ob der Anbieter nach dem EU-US Data Privacy Framework (TADPF) beim US-Handelsministerium zertifiziert ist. Diese Zertifizierung ist öffentlich überprüfbar unter dataprivacyframework.gov.

Prüfen Sie den Auftragsverarbeitungsvertrag (AVV). Für jeden Cloud-Dienst, der Patientendaten verarbeitet, brauchen Sie einen AVV. Das ist unabhängig von § 393 SGB V eine DSGVO-Anforderung.

Unterscheiden Sie, was wo verarbeitet wird. Nicht alle Daten in der Praxis sind Patientendaten. Buchführung ohne Patientenbezug, interne Dokumente, Terminkalender ohne Namen – das unterliegt anderen Anforderungen.

4.11.5. Was ist wo erlaubt?

Patientendaten (Diagnosen, Befunde, Behandlungsunterlagen, Laborwerte, Bilddaten): → Nur in Cloud-Diensten mit C5-Typ-2-Testat oder anerkannter Übergangsregelung nach C5GleichwV, plus AVV, plus Datenspeicherung in zugelassenen Regionen.

Praxis-Infrastrukturdaten (Router-Konfigurationen, Passwort-Manager, interne Dokumente ohne Patientenbezug): → Keine spezifischen SGB-V-Anforderungen, aber DSGVO und sorgfältige Auswahl gelten weiterhin.

Terminverwaltung (sofern keine Patientendaten im engeren Sinne enthalten sind): → Dienste wie Doctolib, die einen AVV anbieten und DSGVO-konform sind, sind möglich. Ob C5 hier greift, hängt davon ab, ob die verarbeiteten Daten als Gesundheitsdaten einzustufen sind.

Cloud-Buchhaltung, E-Mail-Archivierung, Video-Konferenzen (ohne Patientendaten): → Keine C5-Pflicht, aber AVV und DSGVO-Konformität des Anbieters prüfen.

4.11.6. Ein unterschätztes Risiko: Cloud-Kontosperrung

Unabhängig von Zertifizierungsfragen gibt es ein praktisches Risiko, das oft übersehen wird: Was passiert, wenn ein Cloud-Anbieter Ihren Account sperrt?

Große Anbieter können Accounts automatisch sperren – bei verdächtigen Aktivitäten, bei fehlgeschlagenen Zahlungen, nach einer Beschwerde. Support ist dann schwer erreichbar, Wiederherstellung dauert Tage oder Wochen.

Wenn Ihre Praxis-IT darauf aufgebaut ist, können Sie in dieser Zeit nicht arbeiten.

Schutz dagegen: Lokale Backups aller Cloud-Daten (keine vollständige Abhängigkeit vom Cloud-Zugang), alternative Wiederherstellungs-Kontakte bei einem anderen E-Mail-Anbieter, und ein Notfallkonzept für den Fall, dass kritische Cloud-Dienste nicht erreichbar sind. Dazu mehr in Teil 10.

4.11.7. Checkliste: Cloud-Dienste

- ☐ Ich weiß, welche Cloud-Dienste ich nutze – und welche davon Patientendaten verarbeiten.
- ☐ Für alle Cloud-Dienste mit Patientendaten: C5-Typ-2-Testat vorhanden oder Übergangsregelung (ISO 27001 + GAP-Analyse nach C5GleichwV) dokumentiert?
- ☐ Für alle Cloud-Dienste mit Patientendaten: Auftragsverarbeitungsvertrag (AVV) geschlossen?
- ☐ Datenspeicherort geprüft: Daten in EU/EWR – oder, falls in den USA, TADPF-Zertifizierung des Anbieters verifiziert (dataprivacyframework.gov)?
- ☐ Bei US-Anbietern ohne TADPF: Standardvertragsklauseln (SCC) + Transfer Impact Assessment (TIA) vorhanden – ggf. rechtliche Beratung eingeholt?
- ☐ Kundenseitige Anforderungen aus dem C5-Testat-Bericht umgesetzt?
- ☐ Terminverwaltungs-Dienste (Doctolib etc.): DSGVO-Konformität und AVV geprüft?
- ☐ Lokale Backups kritischer Cloud-Daten vorhanden (keine vollständige Abhängigkeit).
- ☐ Wiederherstellungs-Kontakt für Cloud-Accounts liegt bei einem anderen Anbieter.

Rechtlicher Hinweis: Die Anforderungen aus § 393 SGB V und der C5-Gleichwertigkeitsverordnung sind komplex und entwickeln sich weiter. Die hier dargestellten Grundzüge ersetzen keine individuelle rechtliche oder technische Beratung. Klären Sie die konkrete Umsetzung mit Ihrem IT-Dienstleister und – bei Unsicherheit – mit einem auf IT-Recht oder Medizinrecht spezialisierten Anwalt.

4.12. Zugänge für Dritte – sicher teilen, sauber trennen

4.12.1. Das versteckte Sicherheitsrisiko

Eine Arzthelferin bleibt für zwei Wochen im Urlaub. Der IT-Dienstleister braucht schnell Zugang zum Server, um ein Problem zu beheben. Er bekommen das Admin-Passwort per

WhatsApp. Er loggt sich ein, macht die Arbeit, und das Passwort wird nicht geändert.

Das Labor sendet täglich Befunde elektronisch in die Praxis. Das Login für diese Schnittstelle ist ein generisches Konto – „labor" / „labor2024". Der Labortechniker kennt es (weil der IT-Dienstleister es ihm gesagt hat) und technisch ununterscheidbar von den Praxis-Mitarbeitern.

Ein Subunternehmer bearbeitet ein Projekt und braucht Zugang zur Praxis-Cloud. Die Arzt-Helferin schickt ihm die Anmeldedaten für ihr Konto. Nach drei Monaten endet das Projekt – aber der Subunternehmer hat immer noch die gleichen Zugangsdaten und loggt sich manchmal noch ein.

All das ist normal. Und all das ist ein Sicherheitsproblem.

> **Merksatz:** Jeder geteilte Zugang ist eine potenzielle Hintertür. Die Frage ist nicht, ob Sie jemandem vertrauen – sondern ob Sie wissen, wer gerade Zugang hat und ob dieser Zugang noch nötig ist.

4.12.2. Grundprinzip: Getrennte Zugänge statt geteilter Passwörter

Das oberste Gebot beim Zugang für Dritte: **Geben Sie niemals Ihre eigenen Zugangsdaten weiter.**

Wenn Sie einem IT-Dienstleister Ihr Admin-Passwort geben, ist er aus Sicht des Systems nicht mehr vom Admin zu unterscheiden. Wer hat was gemacht? Nachvollziehen unmöglich. Können Sie den Zugang entziehen, ohne selbst das Passwort zu ändern? Nein – das können Sie nur, wenn Sie das Admin-Passwort selbst ändern, und dann kennt der Dienstleister das neue Passwort auch nicht mehr.

Die Lösung: Der IT-Dienstleister hat seinen eigenen Account.

Praktisch heißt das:

In der PVS: Der Dienstleister bekommt einen Tech-Support-Account mit Admin-Rechten – sein Login, sein Passwort. Nur er kennt sein Passwort. Nach der Arbeit wird der Account deaktiviert (nicht gelöscht).

Auf dem Server/NAS: Ein separates Konto für den IT-Dienstleister, mit den Rechten, die er braucht. Nicht das Root-Passwort.

Im Router: Ein separates Benutzer-Konto, wenn möglich.

4.12.3. Das Prinzip der minimalen Rechte

Das gleiche Prinzip wie bei Mitarbeitern: Wer Zugang bekommt, sollte nur die Rechte haben, die er für seine konkrete Aufgabe braucht.

Praktische Fragen:

- Der Steuerberater prüft Belege – braucht er Schreibrecht in der Buchhaltungssoftware? Nein, Lesezugriff reicht.
- Der Lab-Techniker sendet Befunde – braucht er einen manuellen Login? Nein, ein automatisierter Schnittstellen-Account ohne manuellen Zugang ist besser.

- Der Webdesigner aktualisiert die Praxis-Website – braucht er Zugang zum E-Mail-System? Nein.
- Der IT-Dienstleister macht Wartung am Router – braucht er auch Zugang zur PVS? Nein.

Jeder erhält nur das Minimum. Das ist nicht bürokratisch – es ist eine Sicherheits-Grundregel.

4.12.4. Temporäre Zugänge und Ablaufdaten

Manche Zugänge sind dauerhaft (Steuerberater, Labor-Schnittstelle). Andere sind zeitlich begrenzt (Subunternehmer für ein Projekt, IT-Konsultant für eine einmalige Aufgabe).

Für temporäre Zugänge: **Legen Sie beim Einrichten fest, wann der Zugang endet.** Idealerweise hat das System eine Ablauf-Funktion (Gastlinks mit Ablaufdatum, temporäre Einladungen). Wenn nicht, tragen Sie sich im Kalender ein: Am X. Tag wird dieser Zugang wieder entfernt.

Das ist wichtig: Warten Sie nicht auf den anderen. Wenn ein Projekt endet oder eine Zusammenarbeit ausläuft, entziehen Sie den Zugang **aktiv am Tag der Beendigung** – nicht irgendwann. Die meisten Zugänge werden nicht bösartig missbraucht – aber wenn das Konto des anderen später kompromittiert wird, haben Sie das Risiko ausgeschlossen.

4.12.5. Fernwartung – sicher und kontrolliert

Wenn ein IT-Dienstleister Wartungsarbeiten durchführt, braucht er manchmal Fernzugriff auf den Praxis-Computer oder den Server. Das ist normal.

Unsicher: Der Dienstleister bekommt das Admin-Passwort und loggt sich direkt ein. Sie sehen nicht, was er tut.

Sicherer: Verwendung einer **Fernzugriffs-Software mit Sitzungs-ID**.

Tools wie TeamViewer, AnyDesk, oder Windows Remote Assistance funktionieren so: 1. Sie starten das Tool auf Ihrem Praxis-PC 2. Das Tool generiert eine Sitzungs-ID (z. B. 12345-678-90) 3. Sie teilen diese ID dem Dienstleister mit 4. Er verbindet sich über die ID 5. Sie sehen auf Ihrem Monitor, was er tut (idealer Fall: Vier-Augen-Prinzip) 6. Nach der Sitzung wird die ID ungültig – der Dienstleister kann sich nicht mehr verbinden

Das ist transparent und zeitlich begrenzt. Und die Verbindung wird protokolliert – später können Sie sehen, wann der Dienstleister Zugriff hatte.

Am sichersten: Ein separates Admin-Konto für den Dienstleister, das nur aktiviert wird, wenn Wartung ansteht. Danach wird es deaktiviert.

4.12.6. Labore und externe Dienstleister – Datenvertrag und Hilfspersonenvereinbarung

Ein Labor sendet täglich Befunde in die Praxis – über eine Schnittstelle, per E-Mail, oder über einen Web-Login. Das Labor hat technisch Zugriff auf die Praxis-Datenbank (zumindest zum Einspielen von Befunden).

Aus datenschutzrechtlicher Perspektive ist das eine **Auftragsverarbeitung.** Das Labor verarbeitet Patientendaten (Befunde, möglicherweise Untersuchungsergebnisse) im Auftrag der Praxis.

Das muss vertraglich geregelt sein – mit einem **Auftragsverarbeitungsvertrag (AVV).** Dieser Vertrag verpflichtet das Labor:

- Patientendaten nur nach Anweisung der Praxis zu verarbeiten
- Daten nicht an Dritte weiterzugeben
- Angemessene Sicherheitsmaßnahmen zu treffen
- Die Praxis über Verletzungen zu benachrichtigen

Viele große Labore haben Standard-AVVs. Der IT-Dienstleister oder die Praxis selbst sollte das einfordern.

Zusätzlich kann es sinnvoll sein, eine **Hilfspersonenvereinbarung** (auch Geheimhaltungsvereinbarung genannt) zwischen Praxis und Labor zu treffen – dass das Labor die ärztliche Schweigepflicht einhält und Daten nicht leichtfertig weitergeben.

Das klingt formell – ist aber die rechtliche Grundlage dafür, dass externe Zugriffe auf Patientendaten überhaupt zulässig sind.

4.12.7. Der Steuerberater-Sonderfall

Der Steuerberater braucht regelmäßig Zugang zu Finanzdaten – Belege, Buchungen, möglicherweise direkt in der Buchhaltungssoftware. Das ist völlig normal.

Sicher organisiert:

Nutzen Sie die **Freigabe-Funktion der Buchhaltungssoftware.** Moderne Programme wie Lexoffice, sevDesk oder FastBill haben Steuerberater-Zugänge eingebaut. Der Steuerberater loggt sich ein, sieht nur die Daten, die Sie freigeben – keine Praxis-Geheimnisse außer der Finanzseite.

Das ist besser als: Dateien per E-Mail zu schicken (E-Mails sind nicht verschlüsselt und bleiben in der Historie). Der Zugriff ist dokumentiert, es gibt eine Audit-Log, und Sie können den Zugriff jederzeit entziehen.

Standard-Lösung in vielen Praxen: DATEV-Unternehmen-Online. Das ist ein Dienst, über den Praxis und Steuerkanzlei standardisiert Finanzdaten austauschen. Es gibt einen AVV, es ist rechtssicher, und Steuerkanzleien kennen das System.

4.12.8. Offboarding – der vergessene Schritt

Das Onboarding ist selbstverständlich: Neue Person kommt, Sie richten den Zugang ein. Das Offboarding passiert oft gar nicht oder zu spät.

Offboarding-Checkliste bei Beendigung einer Zusammenarbeit:

1. Alle Zugänge entziehen (PVS, Server, Cloud-Dienste, VPN)
2. Geteilte Passwörter sofort ändern (falls doch welche geteilt wurden)
3. Zugangslinks und Einladungen widerrufen
4. Cloud-Freigaben entfernen, nicht nur die Nachricht löschen
5. Dokumentieren: Wann wurde der Zugang entzogen, von wem, welche Systeme?

Falls Sie mehrere externe Partner haben, hilft eine einfache Liste: Wer hat aktuell Zugang zu was? Das sind fünf Minuten Arbeit, die im Ernstfall Stunden spart.

4.12.9. Checkliste: Zugänge für Dritte

- ☐ Ich gebe keine eigenen Zugangsdaten an Dritte weiter – stattdessen richte ich separate Konten ein.
- ☐ Der IT-Dienstleister hat seinen eigenen Admin-Account, nicht das generische Admin-Passwort.
- ☐ Dritte erhalten nur die Rechte, die sie für ihre konkrete Aufgabe brauchen.
- ☐ Ich führe eine einfache Liste: Wer hat aktuell Zugang zu was?
- ☐ Zeitlich begrenzte Zugänge haben ein Ablaufdatum oder einen Kalendereintrag zum Widerrufen.
- ☐ Bei Beendigung einer Zusammenarbeit entziehe ich den Zugang aktiv am selben Tag.
- ☐ Geteilte Passwörter werden nach Beendigung der Zusammenarbeit geändert.
- ☐ Für Fernwartung wird eine Fernzugriffs-Software mit Sitzungs-ID genutzt, nicht direkter Admin-Zugang.
- ☐ Labore und externe Dienstleister mit Datenzugriff haben einen AVV (Auftragsverarbeitungsvertrag).
- ☐ Der Steuerberater-Zugang ist über die Freigabefunktion der Buchhaltungssoftware geregelt – nicht über E-Mail-Anhänge.
- ☐ Ich weiß, wem ich Zugriff gegeben habe und warum.
- ☐ Ich entziehe Zugänge proaktiv, nicht weil der andere es vergessen hat.

4.13. Firewall – Der Wächter im Netz

4.13.1. Was eine Firewall eigentlich tut

Das Wort „Firewall" klingt nach einem großen, teuren Gerät für große Unternehmen. Das ist teilweise richtig – aber auch Arztpraxen brauchen einen Firewall-Schutz, und dieser kann sehr verschieden aussehen.

Eine **Firewall kontrolliert den Netzwerkverkehr in beide Richtungen**: Was hereinkommt aus dem Internet, und was hinausgeht in den Internet.

Der Eingangsschutz ist offensichtlich: Verbindungsversuche von außen, die nicht erlaubt sind, werden blockiert. Kein unbefugter Zugriff auf Praxis-Systeme.

Der Ausgangsschutz ist unterschätzt – und oft wichtiger. Eine Firewall kann festlegen, welche Programme und Dienste überhaupt Verbindungen nach außen aufbauen dürfen. Das klingt weniger spektakulär, hat aber große Auswirkungen:

Schadsoftware kommuniziert nach Hause. Ransomware, Spyware, Trojaner – all das muss nach einer erfolgreichen Infektion nach außen telefonieren, um Anweisungen zu empfangen oder Daten abzuziehen. Eine Firewall, die ausgehenden Traffic kontrolliert, kann genau das blockieren.

Datenabfluss wird erkannt. Wenn ein Gerät plötzlich große Mengen Daten an eine unbekannte IP-Adresse überträgt, ist das ein Warnsignal – und ohne Ausgangs-Kontrolle bemerkt man das nie.

Programme können isoliert werden. Nicht jedes Programm braucht das Internet. Eine Firewall kann einzelnen Anwendungen die externe Kommunikation verbieten.

4.13.2. Die Fritz!Box – praktisch, aber nicht „Firewall"

Die AVM Fritz!Box ist ein hervorragendes Gerät. Zuverlässig, benutzerfreundlich, gut in Deutschland verankert. Für viele kleine Praxen ist sie ausreichend.

Aber: **Es ist kein echte Firewall – und das ist wichtig zu verstehen.**

Was die Fritz!Box kann:

Die Fritz!Box betreibt NAT (Network Address Translation). Alle Geräte in Ihrer Praxis-Netzwerk teilen sich eine einzige öffentliche IP-Adresse nach außen. Verbindungsanfragen aus dem Internet, die niemand initiiert hat, landen am Router und werden verworfen – nicht weil der Router sie aktiv erkennt, sondern weil er schlicht nicht weiß, an welches Gerät er sie weiterleiten soll. Das bietet einen passiven Schutz gegen viele einfache Angriffe.

Zusätzlich hat die Fritz!Box einfache Firewall-Features: Gäste-WLAN, UPnP-Deaktivierung, Netzwerkfilter. Das sind nützliche Zusätze.

Was die Fritz!Box NICHT kann:

- **Ausgehenden Traffic kontrollieren.** Alles, was Ihre Geräte nach außen senden wollen, lässt die Fritz!Box durch. Egal ob Browser, Betriebssystem oder Schadsoftware – ausgehende Verbindungen werden nicht überprüft.
- **Anwendungen erkennen.** Die Fritz!Box sieht, dass Daten über Port 443 (HTTPS) übertragen werden. Sie erkennt aber nicht, ob dahinter ein Browser, ein Cloud-Sync, oder ein Trojaner steckt. Diese Fähigkeit – „Deep Packet Inspection" – haben echte Firewalls.
- **Verhaltensanomalien erkennen.** Wenn ein Gerät im Netz plötzlich ungewöhnlich viel Traffic produziert, mit bekannten Schadsoftware-Servern kommuniziert, oder Port-Scans macht – die Fritz!Box bemerkt das nicht.
- **Interne Zonen trennen.** Ein Gäste-WLAN ist gut. Aber eine echte Netzwerk-Segmentierung – zum Beispiel medizinische Geräte in einer eigenen Zone, getrennt von den Praxis-Computern – ist damit nicht möglich.

Das ist keine Kritik an AVM. Die Fritz!Box ist für ihren Zweck gebaut: Heimrouter für Privatanwender und kleine Büros. Dieser Zweck umfasst keinen unternehmenstauglichen Netzwerkschutz.

> **Merksatz:** Die Fritz!Box schützt Ihr Netz vor ungebetenen Gästen von außen – aber nicht davor, dass etwas von innen unbemerkt nach außen kommuniziert.

4.13.3. Wann reicht die Fritz!Box – und wann nicht?

Sie reicht aus, wenn Sie: - Eine Einzelpraxis oder kleine Gemeinschaftspraxis sind - Keine besonders sensiblen Kundendaten verarbeiten (okay, das ist bei einer Arztpraxis fraglich – aber prinzipiell) - Aktuelle Endgeräte-Sicherheit haben (regelmäßige Updates, Antivirus) - Die anderen Sicherheits-Maßnahmen aus diesen Kapiteln umgesetzt haben (Passwörter, Verschlüsselung, Backups)

Sie reicht NICHT aus, wenn Sie: - Mit besonders schützenswerten Daten arbeiten (und das tun Sie – Patientendaten) - Mitarbeiter haben, die sich im selben Netz bewegen - Ein Büro oder eine Gemeinschaftsfläche betreiben - Regulatorisch verpflichtet sind, ein bestimmtes Sicherheitsniveau nachzuweisen - Kritische medizinische Geräte im Netz haben (PACS, Labor-Interface)

Ehrlich gesagt: Für eine Arztpraxis ist die Fritz!Box als einziger Netzwerk-Schutz knapp. Sie sollten zumindest eine Upgrade-Path haben – eine Möglichkeit, schnell auf eine bessere Firewall zu wechseln, wenn die Anforderungen steigen.

4.13.4. Der TI-Konnektor – und warum die interne Sicherheit trotzdem wichtig ist

Der TI-Konnektor ist ein spezielles Sicherheitsgerät, das die Verbindung zur Telematik-Infrastruktur absichert. Es hat eine eigene Firewall, eine eigene Verschlüsselung, und es läuft nach besonderen Sicherheits-Standards.

Das ist gut. Aber es gibt Ihnen **nicht** die volle Sicherheit des internen Netzes.

Ein Praxis-PC, der von Ransomware befallen ist, kann nicht auf die TI zugreifen (der TI-Konnektor blockiert das). Aber er kann trotzdem: - Andere Praxis-PCs im Netzwerk angegriffen - Patientendaten auf gemeinsame Netzwerk-Ordner verschlüsseln - Nach außen Daten abfließen lassen (wenn die Fritz!Box das nicht blockiert)

Der TI-Konnektor ist also ein zusätzlicher Schutz – aber nicht der einzige Schutz, den Sie brauchen.

4.13.5. Wenn Sie upgraden müssen – dedizierte Firewall und Segmentierung

Für mittlere und größere Praxen lohnt sich eine dedizierte Firewall. Das sind Geräte wie:

Sophos SG series, Palo Alto Networks, Fortinet FortiGate: Enterprise-Firewalls mit vollem Feature-Set. Zu groß und zu teuer für die meisten Praxen.

Ubiquiti UniFi Dream Machine, Firewalla Gold: Erschwinglichere Alternativen mit guten Funktionen. Kosten 300–800 Euro, haben aber nur noch lokale Verwaltung ohne Cloud-Abhängigkeit.

Synology SRM (mit Router-Hardware): Ein NAS, das auch als Router und Firewall fungiert. Praktisch für Praxen, die bereits ein NAS haben.

Was diese Geräte bringen:

Traffic-Inspection: Erkennung von verdächtigem Datenverkehr.

Intrusion Detection: Warnung bei Angriffsmustern.

Netzwerk-Segmentierung: Trennung von Geräten in verschiedenen Zonen – medizinische Geräte, Patientennetzwerk, Admin-Netzwerk.

VPN und sichere Fernzugriffe: Eingebaute VPN-Funktionen, nicht nur Router-VPN.

Protokollierung: Wer hat wann von wo zugegriffen? Alles dokumentiert.

Das klingt komplex. Ein erfahrener IT-Dienstleister kann das in wenigen Stunden einrichten und danach läuft es jahrelang zuverlässig.

4.13.6. Netzwerk-Segmentierung – das Prinzip dahinter

Die Idee: Nicht alles sitzt im gleichen Netzwerk. Stattdessen gibt es Zonen:

- **Admin-Zone:** Nur Admins und IT-Dienstleister, mit besonderen Sicherheitsanforderungen
- **Mitarbeiter-Zone:** Arzte, Arzthelfer, mit Zugang zur PVS und lokalen Ressourcen
- **Medizinische-Geräte-Zone:** Verbunden, aber isoliert von Arbeitsnetzwerk
- **Gäste-Zone:** Patienten-WLAN, kein Zugriff auf Praxis-Systeme

Das verringert das Risiko deutlich: Falls ein Gerät in einer Zone kompromittiert wird, kann ein Angreifer nicht einfach zum nächsten Gerät springen.

Das zu implementieren brauchts Sie aber eine richtige Firewall und jemanden, der das versteht.

4.13.7. Wer konfiguriert und wartet die Firewall?

Das ist eine wichtige Frage: Brauchen Sie einen IT-Dienstleister für eine Firewall-Installation?

Kurze Antwort: Ja.

Eine Firewall, die falsch konfiguriert ist, ist entweder nutzlos oder blockiert wichtigen Traffic (z. B. zur TI). Die Erstinstallation sollte ein Profi übernehmen. Danach können Patches und Updates oft automatisiert werden.

Der IT-Dienstleister sollte auch ein SLA (Service Level Agreement) haben – was passiert, wenn die Firewall ausfällt? Wie schnell wird das behoben? Wie oft wird sie geprüft und aktualisiert?

4.13.8. Checkliste: Firewall und Netzwerk

- ☐ Ich weiß, welches Gerät bei mir als Netzwerk-Schutz fungiert (Fritz!Box, dedizierte Firewall, oder beides).
- ☐ Ich verstehe, was dieses Gerät kann – und was nicht.
- ☐ Das Admin-Passwort ist nicht das Standard-Passwort – es ist stark und im Passwort-Manager gespeichert.
- ☐ Die Firmware ist aktuell – automatische Updates sind idealerweise aktiviert.
- ☐ UPnP ist deaktiviert.
- ☐ NetBIOS-Filter und DNS-Rebinding-Schutz sind aktiviert.
- ☐ IPv6-Firewall ist aktiv.
- ☐ Portfreigaben wurden überprüft – nur die nötigsten sind aktiv.
- ☐ Praxis-WLAN und Gäste-WLAN sind getrennt.
- ☐ Patienten im Gäste-WLAN haben keinen Zugriff auf Praxis-Systeme.
- ☐ Falls Fernzugriff aktiviert: Es läuft über VPN, nicht über direkte Port-Freigabe.
- ☐ Zwei-Faktor-Authentifizierung ist für Fernzugriff aktiviert.
- ☐ Ich habe überprüft: Arbeite ich mit sensiblen Daten, die über eine Fritz!Box hinausgehen?
- ☐ Falls ja: Ich habe geprüft, ob eine dedizierte Firewall sinnvoll wäre.
- ☐ Falls dedizierte Firewall vorhanden: Ein IT-Dienstleister ist verantwortlich für Installation und Wartung.
- ☐ Es existiert ein SLA mit dem IT-Dienstleister – Verfügbarkeit, Update-Häufigkeit, Notfall-Support.

5. Telematikinfrastruktur (TI): Der sichere Weg in die digitale Patientenversorgung

Es ist Montagmorgen, 7:45 Uhr. Sie schalten die Praxisklingel an und sehen es sofort: Der Konnektor neben dem Empfangstresen leuchtet rot. Nicht grün. Nicht wie sonst.

5.1. Was ist die Telematikinfrastruktur?

Die Telematikinfrastruktur, kurz TI, ist das sichere Netzwerk, über das deutsche Vertragsärzte mit den digitalen Systemen des Gesundheitswesens kommunizieren. Die TI ist nicht optional. Sie ist für Vertragsärzte Pflicht.

Wozu dient sie? Die TI ist der Schlüssel zu den modernen Leistungen des deutschen Gesundheitssystems:

- **eRezept:** Sie schreiben Rezepte elektronisch auf. Der Patient lädt sie sich herunter oder lässt sie direkt in die Apotheke übertragen.
- **eAU (elektronische Arbeitsunfähigkeitsbescheinigung):** Krankschreibungen gehen direkt an die Krankenkasse – ohne Papier.
- **KIM (Kommunikation im Medizinwesen):** Sie mailen mit anderen Ärzten und Institutionen, TI-basiert und verschlüsselt.
- **ePA (elektronische Patientenakte):** Ihre Patientendokumente werden zentral digital gespeichert (Opt-out seit 2025).

Wer betreibt die TI? Das ist wichtig zu verstehen: Die **gematik GmbH** (Gesellschaft für Telematik) ist der Betreiber und Regelsetzer. Die **KV (Kassenärztliche Vereinigung)** ist Ihr Ansprechpartner bei Fragen und Problemen. Ein **TI-Dienstleister** (wie Koconet oder secunet) ist der technische Umsetzer vor Ort.

> **Merksatz:** Die TI ist nicht nur Technik – sie ist Infrastruktur mit rechtlichen Anforderungen. Und sie funktioniert nur, wenn alles korrekt zusammenspielt: Konnektor, Zertifikate, Zugangsdaten, Netzwerkverbindung.

5.2. Die wichtigsten Komponenten der TI

Der Konnektor. Das ist eine kleine Hardware-Box, die an Ihrem Netzwerk hängt. Sie ist das Tor zur TI. Der Konnektor ist der einzige sichere Zugang. Alles andere – ePA-Zugriff, eRezept, eAU – läuft über ihn.

eHBA (elektronischer Heilberufsausweis). Das ist Ihr persönliches digitales Zertifikat. Mit Ihrem eHBA und einer PIN beweisen Sie, dass Sie derjenige sind, der Sie behaupten zu sein. Der eHBA ist eine Chipkarte oder eine USB-Smartcard. Darin ist ein privater Schlüssel, der nie nach außen darf.

SMC-B (Praxisausweis). Das ist der digitale Ausweis für Ihre gesamte Praxis. Mit dem SMC-B identifiziert sich die Praxis als juristische Einheit gegenüber der TI. Auch eine Chipkarte, auch mit PIN-Schutz.

KIM. Das ist Ihre TI-basierte E-Mail. Nicht unsicheres Webmail, sondern TI-verschlüsselt. Sie brauchen einen KIM-Account und eine KIM-Software (CGM, Arvato).

5.3. Das Szenario: Der rote Konnektor

Zurück zu Ihrem Montagmorgen. Der Konnektor leuchtet rot. Was kann das bedeuten?

1. **Der Konnektor ist nicht mit der TI verbunden.** Netzwerkproblem? Router-Konfiguration? Oder das TI-Netz ist gerade offline?
2. **Das Zertifikat des Konnektors ist abgelaufen.** Der Konnektor hat zeitlich begrenzte Zertifikate, die vom TI-Dienstleister aktualisiert werden müssen.
3. **Firmware-Update erforderlich.** Der Konnektor muss aktualisiert werden.
4. **Hardware-Fehler.** Der Konnektor selbst ist defekt.

Ihr erster Schritt: Den TI-Dienstleister anrufen. Das ist seine Aufgabe. Aber Sie sollten wissen, was zu prüfen ist: Ist das Netzwerk verbunden? Ist das TI-Passwort noch gültig? Wann war das letzte Zertifikats-Update?

> **Merksatz:** Sie sind nicht allein mit der TI-Verwaltung – aber Sie sind verantwortlich dafür, dass alles läuft. Das ist eine geteilte Verantwortung zwischen Ihnen und dem TI-Dienstleister.

5.4. Die restlichen Teile dieses Kapitels

Dieses Kapitel ist das Fundament. Die nächsten Abschnitte gehen tief:

- **Teil 4.1: TI-Grundlagen** – Wie die TI funktioniert, wer für was zuständig ist, Ihre Verantwortung
- **Teil 4.2: Der Konnektor** – Hardware, Updates, Sicherheit, was Sie prüfen können

- **Teil 4.3: eHBA und SMC-B** – Digitale Ausweise, PIN-Sicherheit, Verlängerung
- **Teil 4.4: KIM** – E-Mail auf Rezept, warum es Fax und unsicheres Webmail ersetzt
- **Teil 4.5: ePA, eRezept, eAU** – Die großen Anwendungen der TI im Praxisalltag
- **Teil 4.6: TI-Ausfall und Notbetrieb** – Was Sie tun, wenn es rot leuchtet

---

5.5. Checkliste: Telematikinfrastruktur – Die Basics

- ☐ Ich weiß, dass die TI für Vertragsärzte Pflicht ist – keine Option.
- ☐ Ich verstehe die vier Hauptanwendungen: eRezept, eAU, KIM, ePA.
- ☐ Ich kenne die Rollen: gematik (Betreiber), KV (Ansprechpartner), TI-Dienstleister (Techniker).
- ☐ Ich habe einen TI-Dienstleister benannt und seine Kontaktdaten gespeichert.
- ☐ Ich weiß, wo mein Konnektor ist und kann die Status-LEDs interpretieren.
- ☐ Ich habe meinen eHBA (Heilberufsausweis) an einem sicheren Ort aufbewahrt.
- ☐ Ich kenne die PIN für meinen eHBA und für die SMC-B.
- ☐ Ich habe einen Notfallplan, falls der Konnektor rot leuchtet.
- ☐ Ich weiß, dass die nächsten Teile tiefer in die Technik gehen – und ich lese sie gründlich.

5.6. TI-Grundlagen: Infrastruktur, Verantwortung und Rollen

Sie haben gerade von der KV eine Nachricht bekommen: „Der Konnektor muss bis Ende Monat erneuert werden." Sie fragen Ihren IT-Dienstleister. Der sagt: „Liegt bei der gematik." Die gematik-Hotline sagt: „Das ist Ihre KV-Aufgabe." Wer ist denn nun zuständig?

5.6.1. Wie die TI technisch funktioniert

Die Telematikinfrastruktur ist ein dezentrales Netzwerk. Im Gegensatz zu einer zentralen Cloud können Sie sich die TI als ein sicheres Postnetz vorstellen, bei dem jede Arztpraxis über einen **Konnektor** Zugang hat.

Der Konnektor ist das Herzstück. Er sitzt in Ihrer Praxis und ist die einzige autorisierte Schnittstelle zur TI. Alle elektronischen Dienste – eRezept, eAU, KIM – laufen durch den Konnektor. Der Konnektor ist nicht einfach ein WLAN-Router. Er ist ein zertifiziertes Gerät mit Verschlüsselung, Authentifizierung und Protokollierung.

Wie sieht der Zugriff aus? Sie wollen ein eRezept ausstellen. Ihr PVS (Praxisverwaltungssystem) sendet die Rezeptdaten zum Konnektor. Der Konnektor prüft Ihre Identität (eHBA + PIN). Er verschlüsselt die Daten. Er verbindet sich mit einem Zentral-Server der gematik. Das Rezept wird hochgeladen. Der Patient bekommt einen QR-Code. Das war's.

Die Kommunikation ist durchgehend verschlüsselt (TLS 1.2 oder höher) und jede Aktion wird protokolliert.

> **Merksatz:** Der Konnektor ist nicht nur Hardware – er ist Ihr Sicherheitsperimeter. Alles, was Sie digital mit der TI machen, läuft durch ihn.

5.6.2. Die Rollen: Wer ist wofür zuständig?

Das ist der kritische Punkt, an dem viele Praxen verwirrt sind. Es gibt mehrere Akteure, und es ist wichtig zu verstehen, wer für was verantwortlich ist.

Die gematik GmbH (Gesellschaft für Telematik). Die gematik ist der Betreiber der TI. Sie setzt die Standards, zertifiziert Konnektor-Hersteller, betreibt die zentralen Dienste (eRezept-Server, ePA-Server, etc.). Sie ist nicht Ihr direkter Ansprechpartner. Sie sind für die Betreiber-Hotline nicht erreichbar. Aber ihre Vorgaben durchziehen die ganze TI.

Die KV (Kassenärztliche Vereinigung). Die KV ist Ihr Ansprechpartner. Die KV koordiniert die TI-Bereitstellung in Ihrer Region. Sie kümmert sich um: - Konnektor-Bereitstellung und Austausch - Zertifikatsverwaltung und Renewal - Support und Störmeldungen - Schulung und Dokumentation

Die KV hat eine Telefon-Hotline. Wenn der Konnektor ausfällt, rufen Sie die KV an, nicht die gematik. Die KV vermittelt zum TI-Dienstleister.

Der TI-Dienstleister (z. B. Koconet, secunet, CompuGroup Medical). Der TI-Dienstleister ist der technische Umsetzer vor Ort. Er: - Liefert und installiert den Konnektor - Kümmert sich um Firmware-Updates - Repariert oder tauscht fehlerhafte Konnektoren aus - Verwaltet die Zertifikate (in Abstimmung mit der KV) - Ist Ihre erste Telefonnummer im Servicefall

Der Konnektor-Hersteller (Kocobox, secunet, RISE, etc.). Der Hersteller stellt die Konnektor-Hardware her und zertifiziert sie. Als Praxisinhaber bekommen Sie davon wenig mit – Ihr TI-Dienstleister kümmert sich darum.

Sie als Praxisinhaber. Ihre Rolle ist zentral, auch wenn Sie nicht selbst Hand anlegen: - Sie sind der Vertragspartner mit der KV - Sie sind der Vertragspartner mit dem TI-Dienstleister - Sie tragen die **Verantwortung** dafür, dass die TI läuft - Sie müssen sicherstellen, dass die Konnektor-Sicherheit nicht gefährdet wird (physischer Zugang, Passwortschutz) - Sie müssen Updates zeitnah durchführen lassen - Sie müssen dokumentieren, dass alles funktioniert

---

5.6.3. Die wichtigsten Regelungen und Verpflichtungen

Die „Anlage 10 der Verträge nach KVV-AV" ist die technische Grundlage. Darin stehen die Anforderungen für die TI-Beteiligung. Das ist rechtlich bindend. Sie müssen sie erfüllen, um als Vertragsarzt die Honorare zu erhalten.

Was ist die wichtigste Anforderung? Ein funktionierender Konnektor. Die Zertifizierungen dürfen nicht abgelaufen sein. Die Netzwerkverbindung muss gesichert sein.

Die Geldstrafe bei Nichterfüllung. Wenn Sie die TI-Anforderungen nicht erfüllen, kann die KV Honorarabzüge vornehmen – bis zu 2 % der Ausgaben. Das ist nicht unerheblich. Aber genauer gesagt: Sie müssen nachweisen, dass Sie sich bemüht haben. Ein defekter Konnektor, bei dem Sie sofort den TI-Dienstleister angerufen haben, ist keine Verletzung. Ignorieren ist ein Problem.

5.6.4. Die Konnektor-Sicherheit: Ihre persönliche Verantwortung

Hier wird es ernst: Der Konnektor ist nicht einfach ein Gerät, das Sie aufstellen und vergessen. Es ist ein Sicherheitsgerät, das Sie schützen müssen.

Physischer Schutz. Der Konnektor darf nicht für Unbefugte zugänglich sein. Er sollte nicht in einem offenen Patientenwartezimmer stehen, wo jemand einfach den Stecker ziehen könnte oder die Tastatur betätigt. Ein gesperrtes Büro oder ein Netzwerk-Schrank ist angemessen.

Passwortschutz. Der Konnektor hat ein Admin-Passwort. Dieses Passwort darf nicht auf einem Klebezettel neben dem Monitor kleben. Es sollte in einem sicheren Passwort-Manager gespeichert sein. Wer hat Zugriff? Nur Sie und der TI-Dienstleister im Servicefall.

Netzwerk-Sicherheit. Der Konnektor kommuniziert mit der TI über eine sichere Verbindung (VPN-ähnlich). Die Netzwerk-Architektur sollte sein: Der Konnektor sitzt in einem separaten Netzwerk-Segment, nicht gemischt mit Patientenpcs. Ein lokaler IT-Sicherheitsaudit kann hier helfen.

Firmware-Updates. Der TI-Dienstleister wird Sie kontaktieren, wenn Updates anstehen. Sie sollten diese schnell durchführen lassen (in der Regel über Nacht). Ein veralteter Konnektor mit bekannten Sicherheitslücken ist fahrlässig.

5.6.5. Checkliste: TI-Grundlagen und Verantwortung

- ☐ Ich verstehe, dass der Konnektor die zentrale Schnittstelle zur TI ist.
- ☐ Ich weiß, dass die gematik die Standards setzt, die KV mein Ansprechpartner ist, und der TI-Dienstleister der Techniker.
- ☐ Ich habe die Kontaktdaten meiner KV gespeichert.
- ☐ Ich habe einen Vertrag mit meinem TI-Dienstleister, der regelmäßige Updates und Support festlegt.
- ☐ Der Konnektor steht an einem gesicherten Ort (nicht öffentlich zugänglich).
- ☐ Das Admin-Passwort des Konnektors ist in einem Passwort-Manager gespeichert, nicht aufgeschrieben.
- ☐ Nur autorisierte Personen haben Zugriff auf den Konnektor.
- ☐ Ich habe einen Plan: Wer wird benachrichtigt, wenn der Konnektor ausfällt?
- ☐ Ich verstehe, dass Updates und Zertifikatsverlängerung regelmäßig anfallen – das ist normal.
- ☐ Ich dokumentiere, dass die TI funktioniert (z. B. monatlich einen Test-Rezeptabruf).

5.7. Der Konnektor: Die Hardware-Box der TI

Sie erhalten einen Brief von Ihrem TI-Dienstleister: „Ihr Konnektor geht in drei Monaten vom Netz. Neue Box kommt nächste Woche." Sie schauen auf die kleine Hardware-Box neben Ihrem Router. Ein unauffälliges Gerät, aber es ist kritisch.

5.7.1. Was ist ein Konnektor technisch?

Der Konnektor ist eine spezialisierte Hardware-Box, nicht größer als ein Standard-Router. Das Gerät ist zertifiziert nach den Anforderungen der gematik. Das bedeutet: Die Hardware, die Firmware, die Verschlüsselung – alles muss von der gematik genehmigt sein.

Was macht der Konnektor? Er ist ein Netzwerk-Gateway mit eingebauten Sicherheitsfunktionen:

- **Authentifizierung:** Er prüft, dass Sie es sind (über eHBA und PIN), bevor er eine Aktion freigibt.
- **Verschlüsselung:** Alle Daten zur TI werden verschlüsselt übertragen.
- **Protokollierung:** Jede Aktion wird geloggt (wer hat wann was gemacht).
- **Netzwerk-Isolation:** Der Konnektor isoliert die TI-Verbindung vom restlichen Praxis-Netzwerk.
- **Zertifikatsverwaltung:** Im Konnektor liegen die digitalen Zertifikate, die Ihre Praxis identifizieren.

Der Konnektor ist also nicht austauschbar mit einem normalen Router. Er ist speicherprogrammierte Sicherheit.

> **Merksatz:** Der Konnektor ist nicht nur Hardware – er ist eine Vertrauens-Instanz. Alle kryptografischen Operationen laufen hier ab.

5.7.2. Marktgängige Konnektor-Modelle

Es gibt mehrere zugelassene Konnektor-Hersteller. Die wichtigsten:

Kocobox (von Koconet). Das ist das meistverbreitete Modell. Kompakt, zuverlässig, mittlerer Preis. Die Bedienoberfläche ist übersichtlich. Updates laufen automatisch nachts.

secunet Products. Höherwertiges Produkt, robuster, längere Wartungszyklen, etwas teurer. Beliebt bei größeren Praxen.

RISE (von Arvato). Eine weitere Variante, Cloud-gestützter als die anderen. Integration mit anderen Arvato-Services.

Die Unterschiede sind gering – alle erfüllen die gematik-Anforderungen. Der Konnektor, den Sie haben, wird vom TI-Dienstleister geliefert. Das wichtigste ist nicht die Marke, sondern dass er aktuell zertifiziert ist.

5.7.3. Hardware-Konnektor oder gehosteter Konnektor? Eine Grundsatzfrage

Seit 2023 gibt es neben dem klassischen Hardware-Konnektor eine Alternative: das **TI-Gateway**, auch gehosteter Konnektor genannt. Die gematik hat diesen zweiten Zugangsweg zur TI zugelassen und zertifiziert. Welche Option für eine Praxis besser ist, hängt von Größe, IT-Infrastruktur und Risikoabwägung ab.

5.7.3.1. Wie der gehostete Konnektor funktioniert

Beim TI-Gateway entfällt die physische Hardware-Box in der Praxis. Die Konnektor-Funktionen – Authentifizierung, Verschlüsselung, Zertifikatsverwaltung, Protokollierung – laufen nicht mehr lokal, sondern in einem zertifizierten Hochsicherheits-Rechenzentrum in Deutschland. Die Praxis verbindet sich über eine verschlüsselte VPN-Verbindung mit diesem Rechenzentrum. Die Verbindung ist doppelt verschlüsselt (VPN plus TLS). Kartenterminals bleiben weiterhin vor Ort – die eHBA-Karte muss nach wie vor lokal gesteckt und die PIN lokal eingegeben werden.

Der Rechenzentrumsbetreiber ist durch die gematik und das BSI zertifiziert. Technisch kann er die verarbeiteten Daten nicht einsehen – die Verschlüsselung verhindert das.

5.7.3.2. Vorteile des gehosteten Konnektors

Kein Hardware-Austausch mehr. Der 5-Jahres-Zyklus, in dem Hardware-Konnektoren getauscht werden müssen, entfällt. Kein Brief vom TI-Dienstleister, keine Terminkoordination, keine Ausfallzeit beim Tausch.

Wartung liegt beim Anbieter. Updates, Zertifikatsverlängerungen und Fehlerbehebung werden zentral vom Anbieter durchgeführt. Die Praxis muss sich nicht darum kümmern.

Höhere Verfügbarkeit. Professionelle Rechenzentren betreiben georedundante Infrastruktur – das heißt, die Konnektor-Funktion läuft auf mehreren Standorten parallel. Ein einzelner Hardware-Ausfall in der Praxis ist damit kein Problem mehr.

Einfachere Verwaltung bei mehreren Standorten. Für MVZ oder Praxen mit Zweigstellen ist ein gehosteter Konnektor deutlich einfacher zu verwalten als mehrere Hardware-Boxen an verschiedenen Standorten.

5.7.3.3. Nachteile und Risiken des gehosteten Konnektors

Vollständige Abhängigkeit vom Internet. Der Hardware-Konnektor funktioniert im lokalen Netzwerk auch dann, wenn das Internet kurzzeitig ausfällt. Beim TI-Gateway gilt: Kein Internet, kein TI-Zugang. Für Praxen ohne zuverlässige Internetanbindung ist das ein relevantes Risiko.

Zentraler Ausfall trifft viele gleichzeitig. Wenn beim Anbieter etwas schiefgeht, sind alle angeschlossenen Praxen gleichzeitig betroffen. Ein lokaler Hardware-Konnektor fällt immer nur für eine Praxis aus. Das ist ein anderes Risikomuster.

Laufende Kosten statt einmaliger Hardware. Hardware-Konnektoren werden einmalig angeschafft und laufen dann jahrelang. TI-Gateways kosten monatliche Gebühren. Je nach Vertrag und Praxisgröße kann das auf Sicht teurer sein – oder günstiger, wenn man IT-Betreuungskosten für die Hardware einrechnet.

Weniger direkte Kontrolle. Mit einem Hardware-Konnektor haben Sie das Gerät physisch in der Praxis. Mit einem TI-Gateway vertrauen Sie darauf, dass der Anbieter verfügbar, sicher und zuverlässig bleibt. Anbieterwechsel sind möglich, aber aufwendig.

5.7.3.4. Für wen ist welche Variante besser?

Der **Hardware-Konnektor on premises** ist nach wie vor die Standardlösung – besonders für Praxen, die bereits eine funktionierende TI-Infrastruktur haben, keine zuverlässige Breitbandanbindung besitzen, oder Wert auf maximale lokale Kontrolle legen.

Der **gehostete Konnektor** ist interessant für Praxen, die gerade neu einsteigen und keine Hardware kaufen möchten, für MVZ und Praxen mit mehreren Standorten, sowie für Praxen, die ihren IT-Betreuungsaufwand dauerhaft minimieren wollen.

> **Merksatz:** Beide Varianten sind gematik-zertifiziert und gleichwertig in puncto Sicherheitsstandard. Die Wahl ist eine Frage von Betriebsmodell, Internetabhängigkeit und Kostenstruktur – nicht von Sicherheitsniveau.

5.7.4. Sicherheitsaspekte des Konnektors

Physischer Schutz. Der Konnektor sollte nicht in einem Patientenwartezimmer hängen. Er sollte auch nicht an einem Ort stehen, wo eine Arzthelferin versehentlich den Stecker ziehen kann. Ein Netzwerk-Schrank, ein Büroraum, oder eine gesperrte Nische ist angemessen. Niemand sollte die Tastatur oder den Monitor des Konnektors bedienen können.

Zugangsschutz. Der Konnektor hat ein Web-Interface (zur Konfiguration und zur Prüfung des Status). Dieses Interface ist nur aus dem lokalen Netzwerk erreichbar – nicht aus dem Internet. Das ist richtig so. Aber: Wer in Ihrer Praxis kann auf das Konnektor-Interface zugreifen? Idealerweise nur Sie und der TI-Dienstleister im Servicefall. Ein Passwort-Manager sollte die Zugangsdaten speichern.

Fernwartung. Der TI-Dienstleister muss manchmal remote auf den Konnektor zugreifen. Das ist normal. Aber es sollte protokolliert sein: Wann, von wem, für wie lange, zu welchem Zweck. Das Protokoll sollte in einem Wartungsvertrag dokumentiert sein.

Firmware-Sicherheit. Der Konnektor erhält regelmäßig Firmware-Updates (mehrmals pro Jahr). Diese Updates beheben Sicherheitslücken und aktualisieren Zertifikate. Sie sollten schnell eingespielt werden – idealerweise nachts, wenn die Praxis nicht läuft.

5.7.5. Zertifikate und ihre Verlängerung

Der Konnektor benutzt digitale Zertifikate, um sich gegenüber der TI auszuweisen. Diese Zertifikate sind zeitlich begrenzt – normalerweise gültig für 2-3 Jahre.

Was passiert, wenn ein Zertifikat abläuft? Der Konnektor kann sich nicht mehr mit der TI verbinden. Das rote Licht zeigt an: Zertifikat abgelaufen. Sie können keinen eRezept-Abruf mehr machen, kein eAU mehr ausstellen.

Wer verlängert das Zertifikat? Das ist eine geteilte Aufgabe: - Die KV und die gematik koordinieren die Zertifikatsverlängerung - Der TI-Dienstleister führt die technische Verlängerung durch - Sie bekommen eine Nachricht (von der KV oder dem TI-Dienstleister) und müssen zeitnah reagieren

Das Problem: Die Verlängerung passiert nicht automatisch. Wenn Sie nicht reagieren und niemand in Ihrer Praxis die Nachricht ernst nimmt, läuft das Zertifikat ab. Das ist vermeidbar – aber nur, wenn jemand die Aufgabe verfolgt.

Praktischer Tipp: Notieren Sie sich den Ablaufdatum des aktuellen Zertifikats (es steht in der Konnektor-Verwaltung). Sechs Monate vorher sollten Sie den TI-Dienstleister kontaktieren: „Das Zertifikat läuft am [Datum] ab. Wann müssen wir die Verlängerung einleiten?"

5.7.6. Konnektor-Laufzeiten und Ausfallsicherheit

Ein Konnektor sollte **24/7 laufen** – also rund um die Uhr, 7 Tage die Woche. Das ist die Erwartung.

In der Praxis: Manche Praxen fahren den Konnektor nachts runter (um Strom zu sparen). Das ist nicht empfohlen – der Konnektor braucht wenig Strom, und ständiges Hochfahren und Herunterfahren belastet die Hardware. Ideal: Der Konnektor läuft immer, nur die Praxis-Pcs werden abgeschaltet.

Was ist eine akzeptable Ausfallzeit? Wenn der Konnektor tagsüber ausfällt (z. B. Stromausfall, Netzwerk-Fehler), sollte er schnell wieder hochkommen. Das sind Minuten. Wenn der Konnektor Stunden ausfällt, ist das problematisch. Es gibt Fallback-Szenarien (siehe Teil 4.6), aber die sind nicht ideal.

Warum passiert der Ausfall? Die häufigsten Gründe: - Stromausfall in der Praxis - Netzwerk-Router geht weg (an den gleichen Stromkreis angeschlossen) - Hardware-Fehler im Konnektor selbst - Firmware-Update, bei dem der Konnektor neu bootet

---

5.7.7. Was Sie selbst prüfen können

Sie müssen nicht Techniker sein, um den Konnektor zu überwachen. Einige einfache Checks sind wertvoll:

Die Status-LEDs. Der Konnektor hat Lichter vorne. Grün bedeutet: OK. Rot bedeutet: Problem. Gelb bedeutet: Update läuft. Schauen Sie regelmäßig hin – mindestens morgens beim Eintreffen.

Das Web-Interface. Sie können sich ins Konnektor-Interface einloggen (lokal aus dem Praxis-Netzwerk). Dort sehen Sie: - Ist die Verbindung zur TI aktiv? - Wann war die letzte erfolgreiche Kommunikation? - Welche Zertifikate sind gespeichert? Wann laufen sie ab?

Ein regelmäßiger Test. Einmal die Woche (z. B. freitags) können Sie einen eRezept-Test machen: Ein einfaches Rezept schreiben, zum Konnektor senden, prüfen, ob der QR-Code generiert wurde. Das ist ein Indikator, dass die TI funktioniert.

Dokumentation. Führen Sie ein einfaches Wartungsprotokoll. Datum, Status der LEDs, eventuelle Fehlermeldungen, welcher TI-Dienstleister kontaktiert wurde, was gemacht wurde. Das ist wertvoll, wenn Probleme auftauchen.

> **Merksatz:** Der Konnektor ist zuverlässig, aber er braucht Aufmerksamkeit. Einmal die Woche hinschauen und einen Test machen ist nicht zu viel verlangt.

5.7.8. Checkliste: Der Konnektor

- ☐ Ich habe entschieden, ob ein Hardware-Konnektor on premises oder ein TI-Gateway für meine Praxis besser geeignet ist.
- ☐ Bei TI-Gateway: Anbieter ist gematik-zertifiziert, Vertrag regelt Verfügbarkeits-SLA und Notfallverfahren.
- ☐ Ich kenne die Marke und das Modell meines Konnektors.
- ☐ Der Konnektor steht an einem sicheren, geschlossenen Ort (nicht öffentlich).
- ☐ Ich kenne die Status-LED-Bedeutungen und schaue regelmäßig hin.
- ☐ Das Admin-Passwort für das Konnektor-Interface ist in einem Passwort-Manager gespeichert.
- ☐ Ich prüfe das Web-Interface mindestens monatlich.
- ☐ Ich kenne das Ablaufdatum der aktuellen Zertifikate.
- ☐ Sechs Monate vor dem Ablauf erinnere ich den TI-Dienstleister an die Zertifikatsverlängerung.
- ☐ Der Konnektor läuft 24/7 (nicht abgeschaltet in der Nacht).
- ☐ Ich führe ein einfaches Wartungsprotokoll (Datum, Status, eventuelle Störungen).
- ☐ Mit meinem TI-Dienstleister ist geklärt: Wer kümmert sich um Updates? Wann ist der beste Zeitpunkt?
- ☐ Ich weiß, wie ich den TI-Dienstleister oder die KV erreiche, wenn der Konnektor rot leuchtet.
- ☐ Ich mache wöchentlich einen Test (z. B. eRezept-Abruf), um sicherzustellen, dass die TI funktioniert.

5.8. eHBA und SMC-B: Die digitalen Ausweise

Sie bemerken am Montag, dass Ihr eHBA weg ist. Sie wissen nicht, wann Sie ihn zuletzt gesehen haben. Jetzt können Sie kein eRezept mehr ausstellen, keine eAU mehr senden. Der Patient sitzt im Zimmer und wartet.

5.8.1. Was ist der eHBA (elektronischer Heilberufsausweis)?

Der eHBA ist Ihr persönliches digitales Zertifikat. Es ist eine Chipkarte oder eine USB-Smartcard, ungefähr so groß wie eine EC-Karte oder kleiner. Darauf ist Ihr Name, Ihre Approbationsnummer und vor allem: ein kryptografischer Schlüssel, der Sie eindeutig identifiziert.

Wozu dient der eHBA? Er ist Ihre digitale Unterschrift. Wenn Sie mit dem eHBA und Ihrer PIN agieren, beweisen Sie: - Ich bin Dr. Meyer - Ich bin ein berechtigter Arzt - Ich habe diese Aktion autorisiert

Der eHBA wird benötigt für: - **eRezept:** Sie signieren das Rezept mit Ihrem eHBA. - **eAU:** Die elektronische Arbeitsunfähigkeitsbescheinigung wird mit Ihrem eHBA signiert. - **KIM:** Der KIM-Account ist an den eHBA gebunden. - **ePA-Zugriff:** Um auf die Patientenakte zuzugreifen, brauchen Sie den eHBA.

Der eHBA ist also nicht optional – das ist Ihre berufliche digitale Identität.

5.8.2. Was ist die SMC-B (Sicherheitsmodul-Chipkarte für Betriebe)?

Die SMC-B ist der digitale Ausweis der Praxis. Wenn der eHBA Sie persönlich identifiziert, identifiziert die SMC-B Ihre Praxis als Institution.

Die SMC-B ist ebenfalls eine Chipkarte. Darauf ist: - Der Name der Praxis - Die BSNR (Betriebsstättennummer) - Ein Zertifikat der Praxis

Wozu wird die SMC-B benutzt? - **KIM:** Der KIM-Account der Praxis ist an die SMC-B gebunden. - **Praxis-Administration:** Verwaltungstätigkeiten in der TI (Benutzerverwaltung, Konfiguration) laufen über die SMC-B. - **Signatur:** Manche Dokumente (z. B. organisatorische Anweisungen) werden mit der SMC-B signiert.

Die SMC-B ist üblicherweise bei der Verwaltungsangestellten oder der Praxisleiterin aufbewahrt, weil sie administrative Aufgaben repräsentiert. Der eHBA ist bei Ihnen (dem Arzt).

5.8.3. PIN-Sicherheit: Das Entscheidende

Hier kommt der kritische Punkt: Sowohl der eHBA als auch die SMC-B haben PINs. Eine 6- bis 8-stellige numerische PIN.

Die PIN ist Ihre letzte Verteidigungslinie. Wenn jemand Ihren eHBA findet, kann er ohne PIN nicht viel machen. Mit PIN kann er sich als Sie ausgeben und Rezepte in Ihrem Namen schreiben.

Das bedeutet konkret:

Regel 1: Die PIN wird niemals aufgeschrieben. Nicht auf einem Klebezettel unter der Tastatur. Nicht in einem Notizbuch. Nicht in einer E-Mail. Das ist ein absolutes No-Go. Eine PIN muss sich eine Person merken.

Regel 2: Die PIN wird nicht weitergegeben. Nicht an die Arzthelferin, nicht an den IT-Dienstleister, nicht an den TI-Dienstleister. Wenn jemand eine Aktion mit dem eHBA braucht (z. B. eRezept signieren), macht das nur der berechtigte Arzt persönlich mit seiner PIN.

Regel 3: Die PIN wird nicht in einem Passwort-Manager gespeichert. Ein Passwort-Manager ist für Passwörter gut (für Web-Zugänge, E-Mail, etc.). Aber eine PIN ist etwas anderes – es ist ein physisches Geheimnis, das nur im Kopf leben sollte.

Regel 4: Wenn Sie die PIN vergessen, muss sie zurückgesetzt werden. Das geht über die Landesärztekammer (die den eHBA ausgestellt hat). Das kostet Zeit (1-2 Wochen) und eventuell Geld. Das ist unangenehm, aber notwendig.

> **Merksatz:** Die PIN ist nicht optional. Kein eHBA ohne PIN. Und die PIN ist nur ein effektiver Schutz, wenn sie wirklich geheim ist.

5.8.4. Wer stellt eHBA und SMC-B aus?

Die Landesärztekammer. Die Ärztekammer Ihres Bundeslandes ist der Aussteller. Sie haben sich dort registriert, bekommen den eHBA per Post mit einer PIN (versiegelt).

Das bedeutet: Wenn Sie die PIN vergessen, kontaktieren Sie die Ärztekammer (nicht die KV, nicht die gematik). Die Ärztekammer kann die PIN zurücksetzen.

Der Antrag auf eHBA wird normalerweise bei der Approbation gestellt. Bei einer neuen Praxis müssen Sie den Antrag aktiv stellen.

5.8.5. Laufzeiten und Verlängerung

Der eHBA ist zeitlich begrenzt – normalerweise 5 Jahre gültig. Nach 5 Jahren muss er verlängert oder neu ausgestellt werden.

Das Problem: Die Verlängerung geschieht nicht automatisch. Sechs Monate vorher sollten Sie die Landesärztekammer kontaktieren: „Mein eHBA läuft in 6 Monaten ab. Was muss ich tun?"

Die Ärztekammer schickt Ihnen dann einen neuen eHBA per Post (wieder mit versiegelter PIN). Der alte eHBA wird dann ungültig.

Zwischendrin: Was ist, wenn der alte eHBA noch gültig ist, aber Sie einen neuen brauchen? Das kann passieren, wenn die PIN vergessen ist oder die Karte beschädigt wurde. Sie können einen neuen beantragen – das ist kein Problem, aber es kostet etwas Zeit.

Die SMC-B hat eine ähnliche Laufzeit (3-5 Jahre, je nach Aussteller). Die KV oder die Ärztekammer informieren Sie vorher.

5.8.6. Verlust, Beschädigung und Sperren

Szenario: Ihr eHBA ist weg.

Schritt 1: Rufen Sie sofort die Landesärztekammer an und melden Sie den Verlust. Der eHBA kann dann in den Systemen gesperrt werden (damit niemand Ihre Identität missbrauchen kann).

Schritt 2: Beantragen Sie einen neuen eHBA. Das dauert 1-2 Wochen per Post.

Schritt 3: Fallback in der Zwischenzeit: Sie können Rezepte noch auf Papier (Muster-16) ausstellen. eAU geht nicht – das ist elektronisch. Hier müssen Sie mit Ihrer Kollegin oder auf dem Papierweg arbeiten.

Szenario: Der eHBA ist beschädigt (z. B. Kontakte korrodiert, Chip nicht lesbar).

Das ist seltener, aber möglich. Die Ärztekammer kann einen neuen ausstellen (nicht so schlimm wie Verlust, weil Sie den alten zurück schicken können und es nicht als Sicherheitsrisiko gilt).

Szenario: Die PIN ist vergessen.

Kontaktieren Sie die Ärztekammer. Sie können die PIN zurücksetzen oder einen neuen eHBA mit neuer PIN ausstellen. Das dauert etwa 1 Woche.

5.8.7. Lagerung und Zugriff

Wo sollte der eHBA aufbewahrt werden?

- Nicht in Ihrem Hosentasche (zu leicht verloren zu gehen)
- Nicht auf dem Schreibtisch (Diebstahl)
- Am besten in einem kleinen Safe oder einer gesperrten Schublade im Praxisbüro
- Oder: Tragen Sie den eHBA in einem verschlossenen Etui bei sich (wenn Sie viel unterwegs sind)

Wer hat Zugriff? Nur Sie (der Arzt). Niemand sonst braucht den eHBA in der Hand. Wenn die Verwaltung ein eRezept oder eAU braucht, geben Sie der Verwaltung das Signal, und Sie selbst machen es mit dem eHBA.

Notfall-Regelung: Falls Sie im Urlaub sind, kann eine vertretungsberechtigte Kollegin mit ihrem eHBA handeln. Der eHBA wird nicht weitergegeben – jeder nutzt seinen eigenen.

5.8.8. Checkliste: eHBA und SMC-B

- ☐ Ich habe einen gültigen eHBA und weiß, wo er ist.
- ☐ Ich habe einen gültigen SMC-B (oder habe das geklärt, wenn mehrere MFAs die SMC-B teilen).
- ☐ Ich kenne die PIN für meinen eHBA und habe sie nicht aufgeschrieben.
- ☐ Meine PIN ist geheim – auch die MFAs und der IT-Dienstleister kennen sie nicht.
- ☐ Der eHBA wird sicher aufbewahrt (Safe, gesperrte Schublade, oder Etui bei mir).
- ☐ Nur ich nutze meinen eHBA – niemand sonst hat ihn in der Hand.
- ☐ Ich kenne das Ablaufdatum meines eHBA.
- ☐ Sechs Monate vor Ablauf kontaktiere ich die Landesärztekammer für die Verlängerung.
- ☐ Ich weiß, wie ich die Landesärztekammer erreiche, falls der eHBA verloren geht.
- ☐ Falls der eHBA beschädigt ist, kann ich einen neuen beantragen – bei der Ärztekammer.
- ☐ Falls die PIN vergessen ist, weiß ich, dass die Ärztekammer helfen kann (kostet Zeit und evtl. Geld).
- ☐ Ich habe einen Notfall-Plan: Was läuft, wenn mein eHBA ausfällt (eRezept → Muster-16, eAU → Papierform oder Vertretung)?

5.9. KIM: Sichere Ärzte-Kommunikation

Ein Facharzt ruft an: „Könnten Sie mir die AU des Patienten mailen?" Sie öffnen Ihr Webmail. Das ist unsicher – jeder könnte mitlesen. Dann fällt Ihnen ein: Ich sollte KIM benutzen. Aber wo ist KIM?

5.9.1. Was ist KIM?

KIM steht für „Kommunikation im Medizinwesen". Es ist die offizielle, sichere E-Mail für Ärzte, Zahnärzte und andere Heilpraktiker im deutschen Gesundheitswesen. KIM ist nicht eine kommerzielle E-Mail wie Gmail oder Outlook. Es ist eine TI-basierte, verschlüsselte Kommunikationsplattform.

Warum gibt es KIM? Die traditionelle E-Mail (SMTP/POP3) ist unsicher. Der Text kann mitlesen. KIM verschlüsselt alles Ende-zu-Ende: Die Nachricht wird beim Sender verschlüsselt, wird verschlüsselt übertragen, und nur der Empfänger kann sie entschlüsseln.

Das ist nicht optional, sondern Pflicht: Vertragsärzte müssen KIM nutzen – insbesondere für sensible Kommunikation wie AU-Bescheinigungen, Arztbriefe und Überweisungen.

> **Merksatz:** KIM ist nicht ein Privacy-Nice-to-have. Es ist die Infrastruktur für sichere ärztliche Kommunikation. Fax und unsichere E-Mail gehören der Vergangenheit an.

5.9.2. KIM im Praxisalltag: Konkrete Anwendungsfälle

Arbeitsunfähigkeitsbescheinigung per KIM. Sie stellen eine AU aus und können sie direkt per KIM an die Krankenkasse senden. Die KIM-Adresse der Krankenkasse ist standardisiert. Keine Papier, keine Faxe.

Arztbrief an den Hausarzt. Ein Patient war bei Ihnen (dem Facharzt) zur Untersuchung. Sie schreiben einen Arztbrief. Mit KIM können Sie ihn direkt an den Hausarzt senden, verschlüsselt. Der Hausarzt empfängt die Nachricht in seinem KIM-Postfach.

Überweisungsunterlagen. Ein Patient braucht eine Überweisung zu einem Spezialisten. Sie können die Unterlagen per KIM direkt zum Spezialisten schicken (wenn dieser KIM hat). Die Unterlagen sind verschlüsselt.

Kommunikation mit Behörden. Krankenversicherungen, Berufsgenossenschaften und Unfallkassen haben KIM-Adressen. Sie können offiziellen Schriftverkehr sicher per KIM abwickeln.

Das ändert den Praxisalltag: Kein Fax-Modem mehr, kein Faxpapier, keine Sorge, dass die Faxleitung besetzt ist. Alles läuft asynchron und verschlüsselt.

5.9.3. KIM-Anbieter und Optionen

Es gibt mehrere KIM-Anbieter. Die beiden großen sind:

CGM (CompuGroup Medical) / CGM KIM. Das größte System. Viele Praxen nutzen CGM. Das KIM-System läuft über die CGM-Infrastruktur. Sie brauchen einen CGM-Account.

Arvato / RISE / Postbox KIM. Alternativer Anbieter, teilweise über bestehende Verträge integriert.

Die Unterschiede sind minimal – alle erfüllen die gematik-Standards. Der Anbieter, den Sie wählen, ist oft eine Geschäftsentscheidung. Viele Praxen gehen mit ihrem PVS-Hersteller: Wenn Sie Turbomed oder Medistar nutzen, haben Sie oft schon KIM integriert.

Das Wichtigste: Sie brauchen nur einen KIM-Account. Eine Praxis, mehrere Ärzte – alle können auf den gleichen Account Zugriff haben (getrennte Login), oder Sie haben separate Accounts. Das ist flexibel.

5.9.4. KIM-Technik: Wie funktioniert es?

Technisch läuft KIM über:

- **TI-Konnektor:** Ihr Konnektor authentifiziert Ihre Identität (eHBA oder SMC-B).
- **TLS-Verschlüsselung:** Die Verbindung zur KIM-Infrastruktur ist verschlüsselt.
- **Ende-zu-Ende-Verschlüsselung:** Der KIM-Anbieter speichert Ihre Nachrichten verschlüsselt (nicht lesbar ohne Ihren Schlüssel).

Praktisch: Sie nutzen eine KIM-Software (z. B. ein KIM-Client auf Ihrem PC oder im Web) und schreiben eine Nachricht. Die Software verschlüsselt die Nachricht, sendet sie zum KIM-Anbieter, dieser speichert sie, und der Empfänger empfängt sie verschlüsselt. So funktioniert es.

Das ist aufwendiger als normales Webmail, aber es ist das, was Sicherheit kostet.

> **Merksatz:** KIM braucht den Konnektor. Wenn der Konnektor ausfällt, fällt auch KIM aus. Das ist ein weiterer Grund, den Konnektor zuverlässig zu halten.

5.9.5. KIM in der Praxis: Integration ins PVS

Das Ideal ist die Integration ins PVS. Ihr Praxisverwaltungssystem (z. B. Turbomed, Medistar, Tomedo) sollte KIM eingebaut haben. Das bedeutet:

- Sie schreiben einen AU, klicken „Senden via KIM", und das System kümmert sich um Verschlüsselung und Versand.
- Eingehende KIM-Nachrichten landen direkt im PVS (z. B. Arztbriefe von anderen Ärzten).

- Keine separate KIM-Software nötig – es läuft im Hintergrund.

Das ist komfortabel. Falls Ihr PVS keine KIM-Integration hat, müssen Sie einen separaten KIM-Client nutzen (z. B. eine Web-Anwendung). Das ist machbar, aber aufwendiger.

5.9.6. Was KIM nicht ist (Wichtige Unterscheidung)

KIM ist nicht die E-Mail für Patientenkommunikation. Sie können nicht mit KIM auf eine Patientenfrage per E-Mail antworten. KIM ist Arzt-zu-Arzt, Arzt-zu-Institution. Wenn ein Patient Ihnen eine E-Mail schreibt, brauchen Sie einen anderen Kanal (z. B. Online-Terminvergabe, Patientenportal, oder traditionelle E-Mail – aber dann mit Datenschutzhinweis).

KIM ersetzt nicht die Sprechstunde. KIM ist für geschäftliche Kommunikation (AU, Arztbriefe, Überweisungen). Medizinische Beratung per KIM ist nicht vorgesehen. Das bleibt der Sprechstunde vorbehalten.

KIM ist kein Ersatz für Dokumentation in der PVS. Die Arztbriefe, die Sie per KIM empfangen, müssen Sie in die PVS importieren und dokumentieren. KIM ist ein Kanal, nicht das Archiv.

5.9.7. KIM einrichten: Die praktischen Schritte

1. **Auswahl des Anbieters:** Sprechen Sie mit Ihrem PVS-Hersteller. Meist ist KIM schon integriert oder es gibt eine Empfehlung.
2. **Registrierung:** Sie registrieren sich bei CGM oder Arvato (je nach Wahl). Sie brauchen Ihre BSNR (Betriebsstättennummer) und eine Authentifizierung (eHBA oder SMC-B).
3. **Konfiguration:** Der KIM-Anbieter stellt Sie bereit. Ihre KIM-Adresse wird vergeben (Format: vorname.nachname@ki-dr.de oder ähnlich).
4. **Integration ins PVS:** Falls integriert, muss die Verbindung hergestellt werden (Zugangsdaten, Token-Austausch).
5. **Test:** Senden Sie eine Test-KIM an die Krankenkasse oder einen Kollegen, um sicherzustellen, dass es funktioniert.

Das dauert insgesamt 1-2 Wochen. Danach läuft KIM im Hintergrund.

5.9.8. KIM und der Notbetrieb

Was passiert, wenn Ihr Konnektor ausfällt? Dann funktioniert KIM nicht – weil KIM an den Konnektor gekoppelt ist.

Im Notbetrieb müssen Sie auf Papier ausweichen: AU auf Papier, Arztbriefe per Fax, Überweisungen auf Papier. Das ist zulässig, solange der Konnektor ausfällt. Aber es ist langsamer und unsicherer.

Das ist ein weiterer Grund, warum die Konnektor-Zuverlässigkeit so wichtig ist.

5.9.9. Checkliste: KIM

- ☐ Ich verstehe, dass KIM für Vertragsärzte Pflicht ist.
- ☐ Ich habe einen KIM-Account bei CGM oder Arvato.
- ☐ Meine KIM-Adresse ist bekannt und ich habe sie an Kollegen und Institutionen weitergegeben.
- ☐ Das KIM ist ins PVS integriert (oder ich nutze einen separaten KIM-Client).
- ☐ Ich habe einen Test gemacht: eine AU oder einen Brief per KIM versandt.
- ☐ Ich weiß, dass KIM den Konnektor braucht – bei Konnektor-Ausfall funktioniert KIM nicht.
- ☐ Meine Zugangsdaten für KIM sind sicher gespeichert (im PVS oder in einem Passwort-Manager).
- ☐ Ich nutze KIM für AU, Arztbriefe und institutionelle Kommunikation – nicht für Patientenkommunikation.
- ☐ Empfangene KIM-Nachrichten werden ins PVS importiert und dokumentiert.
- ☐ Ich kenne meinen KIM-Anbieter und seine Support-Telefonnummer.

5.10. ePA, eRezept und eAU: Die drei zentralen TI-Dienste

Ein Patient fragt: „Kann ich meine Unterlagen in die ePA importieren?" Ein anderer: „Warum kriege ich das eRezept per QR-Code?" Eine Arzthelferin: „Wo sehe ich, ob die eAU angekommen ist?" Drei Systeme, drei Fragen. Hier die Antworten.

5.10.1. Die ePA (elektronische Patientenakte)

5.10.1.1. Was ist die ePA?

Die ePA ist eine zentrale, digitale Gesundheitsakte für jeden Patienten. Sie wird von der gematik betrieben. Der Patient kann darin Dokumente speichern und verwalten – Arztbriefe, Laborbefunde, Röntgenbilder, Impfpass, sogar Medikamentenlisten.

Der Patient entscheidet, wer Zugriff hat: „Darf dieser Arzt meine Akte sehen?" Ja oder nein.

5.10.1.2. ePA ab 2025: Opt-Out statt Opt-In

Seit Januar 2025 hat sich das Regelwerk geändert. **Alle Patienten erhalten automatisch eine ePA** – es sei denn, sie widersprechen (Opt-Out). Das ist ein großer Wechsel vom früheren Opt-In (Patient musste aktiv zustimmen).

Das bedeutet für die Praxis: Viele neue Patienten haben plötzlich eine ePA. Sie sollten frühzeitig fragen: „Können wir Ihre Unterlagen in die ePA hochladen?"

5.10.1.3. Im Praxisalltag

Sie stellen eine Diagnose, schreiben einen Brief. Sie können diesen Brief mit dem eHBA digital signieren und direkt in die ePA des Patienten hochladen (mit seiner Zustimmung). Der Patient hat ihn sofort online.

Das erspart: Papier ausdrucken, patient mitnehmen, Patient muss es archivieren. Die ePA ist zentralisiert.

5.10.1.4. Der Sicherheitsaspekt: Zugriffsprotokollierung

Wichtig: Die ePA protokolliert jeden Zugriff. Der Patient kann sehen: „Am 15.3. um 14:30 hat Dr. Meyer meine Akte angesehen." Das ist ein Feature – keine Komplikation. Der Patient vertraut, dass nur Befugte zugreifen.

Sie sollten also keine ePA-Zugriffe machen, die nicht dokumentiert werden dürfen. Immer mit ärztlicher Indikation arbeiten.

5.10.1.5. Ihr Zugriff auf die ePA

Sie nutzen Ihren eHBA und den Konnektor, um auf die ePA zuzugreifen. Das PVS kann integriert sein – Sie sehen eine Schaltfläche „ePA abrufen", und das System holt die Unterlagen.

Falls Sie keine ePA-Integration haben, müssen Sie einen ePA-Client nutzen (eine separate Software). Das ist aufwendiger.

5.10.2. Das eRezept

5.10.2.1. Was ist das eRezept?

Das eRezept ist die elektronische Variante des klassischen rosa Rezepts (Muster 16). Sie schreiben das Rezept im PVS, signieren es mit Ihrem eHBA, und das System erzeugt einen QR-Code.

Der Patient bekommt diesen QR-Code (per Papier, per E-Mail, oder per Handy-App). Mit dem QR-Code kann der Patient in jede Apotheke gehen und sagt: „Hier ist mein eRezept." Die Apotheke scannt den Code, und das Medikament wird dispensiert.

5.10.2.2. Das eRezept ist Pflicht

Seit 2024 ist das eRezept für alle Ärzte verpflichtend – mit wenigen Ausnahmen (z. B. im Notbetrieb, wenn der Konnektor ausfällt).

Das heißt: Papierrezepte sind jetzt die Ausnahme, nicht die Regel. Das ist ein großer Change für viele Praxen, besonders traditionelle.

5.10.2.3. Im Praxisalltag

Sie schreiben ein Rezept. Das PVS fragt: „eRezept oder Papier?" Sie klicken „eRezept". Das System verbindet sich mit Ihrem Konnektor, signiert das Rezept mit Ihrem eHBA (Sie geben die PIN ein), und generiert den QR-Code.

Der Vorgang dauert wenige Sekunden – aber er braucht den funktionierenden Konnektor. Wenn der Konnektor rot leuchtet, müssen Sie auf Papierrezepte ausweichen.

5.10.2.4. Der gematik-Server

Die eRezepte werden auf einem zentralen Server der gematik gespeichert. Der QR-Code ist ein Verweis auf diesen Server. Das bedeutet: Selbst wenn der Patient den QR-Code verliert, kann er die Apotheke anrufen und die gematik direkt fragen: „Welche eRezepte für mich gespeichert?" Das ist ein Sicherheitsfeature.

Wichtig: Sie müssen auf diesem Server ein Konto haben und Ihre eRezepte hochladen können. Das regelt der TI-Dienstleister oder das PVS.

5.10.2.5. Besonderheit: Betäubungsmittel (BtM-eRezepte)

Für Betäubungsmittel (z. B. Opioid-Analgetika) gibt es spezielle eRezepte. Die Regel ist strenger – höhere Sicherheit, mehr Dokumentation. Das PVS sollte das automatisch handhaben.

5.10.3. Die eAU (elektronische Arbeitsunfähigkeitsbescheinigung)

5.10.3.1. Was ist die eAU?

Die eAU ist die elektronische Arbeitsunfähigkeitsbescheinigung – der Ersatz für den papiernen Krankschein.

Wenn Sie einen Patienten krankmelden, erstellen Sie die eAU im PVS. Das System verbindet sich mit der Krankenkasse des Patienten und übermittelt die Daten direkt. Der Patient bekommt eine Bescheinigung (meist digital oder per Post), und sein Arbeitgeber wird informiert.

Das ist komfortabel: Der Patient muss die Bescheinigung nicht zum Arbeitgeber tragen oder per Fax schicken. Es funktioniert automatisch.

5.10.3.2. eAU-Übermittlung

Die eAU wird direkt an die Krankenkasse übermittelt – das ist der Standardweg. Das PVS sollte das tun, sobald Sie die AU signieren.

Das heißt konkret: Sie brauchen beim Ausstellen der eAU die Krankenversicherungsdaten des Patienten (Krankenkasse, Versichertennummer). Das PVS hat das meist schon im Patientenstamm gespeichert.

5.10.3.3. Was Sie dokumentieren müssen

In der eAU speichern Sie: - Diagnose (ggf. verschlüsselt nach ICD-10) - Beginn und Ende der Arbeitsunfähigkeit - Besonderheiten (z. B. Hausbesuch nötig, psychische Erkrankung)

Die eAU ersetzt den Papier-Krankschein vollständig. Der Patient braucht keine Kopie mehr mitzunehmen – die Krankenkasse hat die Original-Daten.

5.10.3.4. Im Notbetrieb (Konnektor weg)

Wenn der Konnektor ausfällt, können Sie keine eAU ausstellen. Sie müssen auf Papierform ausweichen (Muster 1 oder Muster 4). Das ist zulässig, aber Sie müssen es dokumentieren: Grund für den Papier-AU (z. B. „Konnektor-Ausfall 15.3.–17.3.").

5.10.4. Vergleich: ePA, eRezept, eAU

Merkmal	ePA	eRezept	eAU
Was ist es?	Patientenakte	Rezept	Arbeitsunfähigkeit
Pflicht?	Opt-Out seit 2025	Ja (ab 2024)	Ja
Wer speichert?	gematik-Server	gematik-Server	Krankenkasse
Patient hat Kontrolle?	Ja (Zugriff freigeben)	Teilweise (QR-Code teilen)	Nein (direkte Übermittlung)
Braucht Konnektor?	Ja	Ja	Ja
Fallback?	Papierausdrucke	Papierrezept Muster-16	Papier-AU Muster 1/4

5.10.5. Checkliste: ePA, eRezept und eAU

- ☐ Ich verstehe, dass alle drei Dienste Pflicht für Vertragsärzte sind.
- ☐ Mein PVS unterstützt eRezepte – und ich habe einen Test gemacht.
- ☐ Ich weiß, wie ich die PIN für die eHBA-Signatur eingebe.
- ☐ Ich stelle eAUs elektronisch aus – und kenne den Papier-Fallback.
- ☐ Ich bin angemeldet beim gematik-eRezept-Server (oder mein PVS regelt das).
- ☐ Meine Patienten verstehen, was der eRezept-QR-Code ist.
- ☐ Ich dokumentiere die Diagnose in der eAU korrekt (ICD-10).
- ☐ Falls der Konnektor ausfällt, weiß ich, auf welche Papierform ich ausweiche.
- ☐ Für die ePA frage ich meine Patienten aktiv: „Darf ich Ihre Unterlagen hochladen?"
- ☐ Ich verstehe, dass die ePA-Zugriffe protokolliert werden – nur mit ärztlicher Indikation arbeiten.
- ☐ Mein PVS ist für alle drei Dienste konfiguriert.
- ☐ Ich kenne die Besonderheiten: BtM-eRezepte, eAU-Verschlüsselung, ePA-Consent.

5.11. TI-Ausfall und Notbetrieb: Wenn die Infrastruktur ausfällt

Es ist Mittwoch, 9 Uhr. Der Konnektor leuchtet rot. Sie versuchen, ein eRezept zu schreiben – es funktioniert nicht. Der erste Patient sitzt im Zimmer und wartet. Was tun Sie jetzt?

5.11.1. Was passiert bei einem TI-Ausfall?

Ein TI-Ausfall kann mehrere Formen annehmen:

1. **Konnektor-Ausfall bei Ihnen vor Ort.** Der Konnektor ist defekt, offline oder hat ein Zertifikatsproblem. Das ist der häufigste Fall.
2. **TI-Netzwerk-Ausfall.** Die zentrale TI ist offline (sehr selten, aber möglich).
3. **Teilweiser Ausfall.** KIM funktioniert, eRezept nicht. Oder umgekehrt.

Im Fall 1 sind Sie lokal betroffen. Im Fall 2 sind alle Ärzte betroffen. Im Fall 3 müssen Sie je nach Service fallback.

Die erste Frage ist immer: Ist der Konnektor das Problem oder die TI?

- Schauen Sie auf die Status-LEDs des Konnektors. Rot = wahrscheinlich Konnektor-Problem.
- Rufen Sie Ihren TI-Dienstleister an. Der kann prüfen, ob die TI online ist.
- Prüfen Sie das Konnektor-Web-Interface (lokal, aus dem Netzwerk): Steht da eine Fehlermeldung?

5.11.2. Die rechtliche Regelung: Honorarabzug und Nachweis

Das ist wichtig zu verstehen: **Bei Konnektor-Ausfall darf die KV Ihnen keinen Honorar abziehen.** Das ist seit 2021 explizit geregelt.

Aber: Es gibt Bedingungen.

Sie müssen nachweisen, dass Sie nicht schuld sind. Wenn Sie den Konnektor einfach ignoriert haben, ihn nicht gepflegt haben, und plötzlich ist er offline – das zählt als Schuld. Dann kann die KV Abzüge vornehmen.

Aber wenn Sie sofort gehandelt haben (den TI-Dienstleister angerufen, den Fehler dokumentiert), dann schuldlos. Da gibt es Kulanz.

Sie müssen der KV Meldung geben. Wenn der Konnektor länger als 24 Stunden ausfällt, sollten Sie die KV informieren. Das geschieht über ein standardisiertes Formular. Die KV dokumentiert die Ausfallzeit. Das ist Ihr Beweis.

> **Merksatz:** TI-Ausfall ohne Verschulden = Keine Honorarkürzung. Aber nur, wenn Sie sofort reagiert haben und die KV informiert haben.

5.11.3. Fallback-Szenario 1: eRezept → Muster-16 (Papier)

Was tun Sie, wenn der Konnektor ausfällt und Sie können keine eRezepte ausstellen?

Sie wechseln auf das Papierrezept – Muster 16.

Das Muster 16 ist das klassische rosa Rezept. Es ist immer noch gültig, auch wenn eRezepte Pflicht sind. Im Notfall dürfen Sie Muster-16 nutzen.

Praktisch: Sie haben Papier-Rezeptblöcke im Schrank. Falls der Konnektor ausfällt, greifen Sie darauf zurück. Sie schreiben das Rezept wie gehabt, unterschreiben es von Hand, und der Patient geht damit in die Apotheke.

Das ist langsamer (Sie müssen selbst schreiben statt zu tippen), aber es funktioniert.

Dokumentation: Sie sollten kurz notieren: „Muster-16 ausgestellt aufgrund TI-Ausfall, 15.3.2026, 9:15–10:30 Uhr."

5.11.4. Fallback-Szenario 2: eAU → Papierform

Die eAU braucht den Konnektor. Wenn der Konnektor ausfällt, können Sie keine eAU ausstellen.

Fallback: Sie nutzen die Papierform – **Muster 1** (normale Arbeitsunfähigkeit) oder **Muster 4** (Arbeitsunfähigkeit mit Diagnoseangabe).

Diese Formulare erhalten Sie von der KV. Sie sind gelb oder orange (je nach Form). Sie schreiben sie von Hand aus, unterschreiben, und der Patient nimmt das Original mit. Die Arbeitgeber- und Krankenkassenkopie gehen an die angegebenen Stellen.

Das ist das alte, papiergestützte Verfahren. Nicht elegant, aber zulässig im Notbetrieb.

Dokumentation: Auch hier sollten Sie notieren: „Papier-AU Muster 1 aufgrund TI-Ausfall, 15.3.2026."

5.11.5. Fallback-Szenario 3: ePA → Kein Zugriff

Die ePA braucht den Konnektor. Wenn der ausfällt, können Sie nicht auf die ePA zugreifen und keine neuen Unterlagen hochladen.

Was tun Sie? Sie dokumentieren alles lokal im PVS wie gehabt. Sobald der Konnektor wieder läuft, spielen Sie die Unterlagen nach – oder Sie warten, bis der nächste geplante Upload.

Der Patient wird nicht benachteiligt – seine Behandlung läuft normal. Die ePA ist eine Ergänzung, nicht essentiell für die Versorgung.

Das Wichtigste: Die Therapie läuft weiter. Die ePA-Synchronisation kann warten.

5.11.6. Fallback-Szenario 4: KIM → Papier, Fax oder Phone

KIM braucht den Konnektor. Wenn der ausfällt, funktioniert KIM nicht.

Was tun Sie, wenn Sie dringend einen Brief an einen Kollegen schreiben müssen?

1. **Fax:** Noch immer zulässig. Ein Faxgerät oder ein Fax-Service kann helfen.
2. **Post:** Ein Arztbrief per Post dauert länger, aber es ist zuverlässig.
3. **Telefon:** Für Notfälle können Sie anrufen und mündlich abstimmen.
4. **Klinik-Intercom:** Falls Sie mit einer Klinik arbeiten, kann der interne Botenverkehr Unterlagen transportieren.

Das ist langsamer, aber es funktioniert. Manche Praxen haben immer noch ein Faxgerät für Notfälle – das ist nicht dumm.

5.11.7. Notfall-Checkliste: Was tun beim TI-Ausfall?

Wenn der Konnektor rot leuchtet:

1. **Ruhig bleiben.** Das ist nicht das Ende der Welt. Es gibt Fallbacks.
2. **Status prüfen.** LEDs kontrollieren, Konnektor-Interface prüfen.
3. **TI-Dienstleister anrufen.** Das ist Ihre erste Telefonnummer. Nicht die gematik, nicht die KV – der TI-Dienstleister.
4. **KV Bescheid geben.** Wenn der Ausfall länger als 24 Stunden dauert.
5. **Fallback aktivieren.** Papierrezepte, Papier-AU, lokale Dokumentation im PVS.
6. **Dokumentieren.** Zeit des Ausfalls, Ursache (wenn bekannt), was Sie getan haben.

5.11.8. Die Notfall-Telefonummern sollten Sie kennen

- **TI-Dienstleister:** Im Vertrag festgehalten. Speichern Sie die Nummer prominent ab.
- **KV-Servicenummer:** Die KV Ihres Bundeslandes hat eine Hotline. Speichern Sie diese ebenfalls.
- **gematik-Hotline (nur für großflächige TI-Ausfälle):** Nicht Ihre erste Anlaufstelle, aber für die Info, ob die TI selbst offline ist.

5.11.9. Wie lange darf die TI weg sein?

Theoretisch: Keine zeitliche Begrenzung – Sie dürfen im Notbetrieb so lange arbeiten, wie nötig.

Praktisch: Ein paar Stunden ist okay. Ein paar Tage ist nervös. Eine Woche ist ein Problem – dann brauchen Sie eventuell technische Hilfe von außen.

Die meisten Konnektor-Probleme sind innerhalb von 24 Stunden behoben. Ein Firmware-Update braucht 1-2 Stunden. Ein Zertifikatswechsel braucht ein paar Stunden. Nur bei Hardware-Ausfall (Konnektor selbst defekt) dauert es länger – bis zum Austausch durch den TI-Dienstleister (1-2 Tage Lieferzeit).

5.11.10. Langfristige Planung: Redundanz und Vorbereitung

Falls Sie in einer großen Praxis sind oder mehrere Standorte haben, können Sie überlegen:

- **Redundanter Konnektor:** Zwei Konnektoren, im Notfall schaltet man zum zweiten um. (Aufwendig, aber für große Praxen erwägenswert.)
- **Backup-Internet:** Zwei Internet-Provider, damit nicht ein Ausfallfall isoliert.
- **Papier-Bestände:** Immer ein Vorrat an Muster-16, Muster-1 und Muster-4 Formularen im Schrank.

Für kleine Praxen: Nicht notwendig. Aber Sie sollten wenigstens ein paar Papierrezepte und Papier-AU-Formulare im Schrank haben.

5.11.11. Checkliste: TI-Ausfall und Notbetrieb

- ☐ Ich kenne die Telefonnummer meines TI-Dienstleisters und habe sie gespeichert.
- ☐ Ich kenne die Telefonnummer meiner KV und habe sie gespeichert.
- ☐ Ich weiß, dass ich im Notbetrieb Muster-16, Muster-1 und Muster-4 nutzen darf.
- ☐ Ich habe einen kleinen Vorrat dieser Formulare im Schrank.
- ☐ Ich verstehe, dass die KV mir keinen Honorarabzug geben darf bei schuldlosem Ausfall.
- ☐ Ich weiß, dass ich die KV bei Ausfällen länger als 24 Stunden informieren muss.
- ☐ Ich habe einen Plan: Wer wird kontaktiert, wenn der Konnektor rot leuchtet?
- ☐ Ich dokumentiere Ausfallzeiten und was ich unternommen habe.
- ☐ Ich prüfe monatlich, dass die Fallback-Formulare verfügbar sind.
- ☐ Mein PVS kann mit Offline-Betrieb umgehen (lokale Speicherung).
- ☐ Falls länger Ausfall droht, habe ich einen IT-Support in der Nähe, der helfen kann.

6. Praxisverwaltungssystem (PVS): Das Herz der Praxis

Es ist 8:45 Uhr, Sprechstundenstart in 15 Minuten. Sie machen den Praxis-PC an – und sehen auf dem Monitor einen roten Fehler: „Datenbankfehler 3007". Das PVS lädt nicht. Die ersten Patienten stehen an der Rezeption und wollen angemeldet werden.

6.1. Was ist ein PVS?

Das Praxisverwaltungssystem (PVS) ist die zentrale Software einer jeden Arztpraxis. Es ist kein Programm, das Sie nebenbei nutzen. Es ist der Kern des Praxisbetriebs.

Was speichert das PVS?

- **Patientenstammdaten:** Name, Geburtsdatum, Kontaktdaten, Versicherungsdaten.
- **Anamneseblätter:** Die medizinische Vorgeschichte jedes Patienten.
- **Behandlungsunterlagen:** Was wurde wann gemacht, welche Diagnosen, welche Medikationen.
- **Labordaten:** Laborergebnisse, Werte, Trends.
- **Bilddaten:** Röntgenaufnahmen, Ultraschallbilder (falls digital gespeichert).
- **Abrechnungsdaten:** Alle medizinischen Leistungen für die KV-Abrechnung.
- **Termindaten:** Wer kommt wann zur Sprechstunde.

Das PVS ist die Datenbank der Praxis. Wenn es nicht läuft, ist die Praxis funktionsmäßig erledigt.

> **Merksatz:** Das PVS ist nicht austauschbar wie eine Browser-App. Es ist die Infrastruktur. Ausfallzeit beim PVS ist Ausfallzeit der Praxis.

6.2. Bekannte PVS-Systeme (ohne Wertung)

Es gibt mehrere etablierte PVS-Produkte am Markt:

Turbomed (von Turbomed GmbH). Eines der verbreitetsten Systeme im deutschsprachigen Raum. Stabil, gute Integration mit TI, großes Netzwerk von Supportern.

Medistar (von Medistar). Auch weit verbreitet, ähnlich etabliert wie Turbomed. Guter KIM-Support, gute Anbindung an Labore.

Tomedo (von Tomedo GmbH). Cloud-basiertes System. Etwas jünger, modernes Interface, Integration mit ePA.

CGM M1 (von CompuGroup Medical). Ein großes System, viele Funktionen, oft in größeren Praxen.

x.isynet (von xitos). Ein weiteres etabliertes System, speziell für Fachärzte.

Dampsoft. Kleineres, eher in speziellen Fachgruppen verbreitet.

Alle diese Systeme erfüllen die KBV-Zertifizierung und unterstützen die TI. Der Unterschied liegt in Details: Benutzerfreundlichkeit, Supportqualität, Preis, spezielle Features.

Das Wichtigste: Welches System Sie haben, ist weniger kritisch als dass es zertifiziert ist und regelmäßig Updates bekommt.

6.3. Warum ist der PVS-Ausfall so dramatisch?

Ein Ausfall des PVS bedeutet:

- Sie können keine Patienten anmelden (die Termin-/Patientenliste ist im PVS).
- Sie können nicht auf Patientenakten zugreifen.
- Sie können keine Rezepte schreiben (zumindest nicht elektronisch).
- Sie können keine Abrechnungsdaten erfassen.
- Sie können keine AU ausstellen.
- Sie wissen nicht, welche Laborwerte vorliegen.

Im Notfall können Sie Papier nutzen – aber das ist langsam, fehleranfällig und belastet die Praxis massiv.

Das ist der Grund, warum die PVS-Auswahl, -Wartung und -Sicherung so kritisch sind.

6.4. Die restlichen Teile dieses Kapitels

Die nächsten Abschnitte behandeln:

- **Teil 5.1: PVS-Auswahl und Zertifizierung** – Worauf achten bei der Auswahl oder dem Austausch eines PVS
- **Teil 5.2: PVS-Sicherheit im Betrieb** – Zugriffsrechte, Protokollierung, Netzwerksicherheit
- **Teil 5.3: PVS-Backup** – Datensicherung, Aufbewahrungsfristen, Restore-Tests

---

6.5. Checkliste: PVS – Grundverständnis

- ☐ Ich weiß, welches PVS-System wir nutzen (Turbomed, Medistar, Tomedo, etc.).
- ☐ Ich verstehe, dass das PVS die zentrale Datenbank der Praxis ist.
- ☐ Ich weiß, dass das PVS zertifiziert sein muss (KBV-Zertifizierung).
- ☐ Ich verstehe, dass ein PVS-Ausfall die ganze Praxis lahmlegt.
- ☐ Ich kenne meinen PVS-Support (Telefonnummer, Ansprechpartner).
- ☐ Ich habe einen Plan für einen PVS-Ausfall (Papierform-Fallback).
- ☐ Das PVS wird regelmäßig aktualisiert (mindestens monatlich).
- ☐ Ich weiß, dass die Sicherheit des PVS genauso wichtig ist wie die Verfügbarkeit.
- ☐ Die letzten drei Teile sind für die Praxis-Resilience essentiell.

6.6. PVS-Auswahl und Zertifizierung: Das richtige System wählen

Sie planen einen PVS-Austausch. Ein Anbieter verspricht: „Wir haben die beste Benutzeroberfläche, niedrigere Kosten und einen persönlichen Support vor Ort." Ein anderer: „Wir sind seit 20 Jahren am Markt und Cloud-basiert." Welches System wählen Sie?

6.6.1. Die KBV-Zertifizierung als Pflicht

Das ist die erste und wichtigste Anforderung: **Das PVS muss von der KBV (Kassenärztliche Bundesvereinigung) zertifiziert sein.**

Was bedeutet das? Die KBV hat Anforderungen für die Funktionalität, Sicherheit und Zuverlässigkeit von PVS-Systemen. Ein zertifiziertes System erfüllt diese Standards. Es kann medizinische Daten korrekt speichern, die TI-Anbindung funktioniert, Sicherheitsstandards werden eingehalten.

Wenn Sie ein nicht-zertifiziertes System nutzen, riskieren Sie:

- Honorarforderungen der KV (weil die Abrechnung fehlerhaft sein könnte)
- Vertragsprobleme (Sie erfüllen die Anforderung von Vertragsarzt nicht)
- Datenschutz-Probleme (Ohne Zertifizierung können Standards verletzt sein)

Das Mittel zum Schutz: Bevor Sie ein PVS auswählen oder austauschen, prüfen Sie die KBV-Zertifizierung. Es gibt eine offizielle Liste auf der KBV-Website. Nur Systeme dieser Liste sind akzeptiert.

> **Merksatz:** Keine KBV-Zertifizierung = Nicht verhandlungsfähig. Das ist nicht optional.

6.6.2. Worauf Sie bei der Auswahl achten sollten

1. TI-Kompatibilität und Aktualität.

Das PVS muss die Telematikinfrastruktur unterstützen – eRezept, eAU, KIM, ePA. Es muss nicht nur heute unterstützen, sondern auch in den nächsten 5 Jahren. Fragen Sie den Anbieter:

- "Welche TI-Dienste unterstützen Sie aktuell?"
- "Welche sind in Entwicklung?"
- "Was ist Ihre Roadmap für die nächsten 3 Jahre?"

Ein PVS, das nur eRezept unterstützt, aber eAU noch per Papier erfordert, ist veraltet. Ein PVS, das KIM noch nicht integriert hat, ist nicht zukunftsfähig.

2. Update-Versprechen und Frequenz.

Fragen Sie: "Wie oft werden Updates eingespielt?" Ideal ist monatlich oder quartalsweise. Ein PVS, das nur alle 6-12 Monate ein Update bekommt, ist langsam in der Innovation und Sicherheit.

Auch wichtig: "Wie lange ist eine alte PVS-Version noch supported?" Manche Anbieter stoppen Support nach 2 Jahren. Das kann problematisch sein, wenn Sie ein Update verpassen.

3. Vertragslaufzeit und Exit-Strategie.

Vorsicht vor Langzeitverträgen (5+ Jahre ohne Kündigungsmöglichkeit). Besser sind kurze Verträge (1-3 Jahre) mit jährlicher Verlängerung. Das gibt Ihnen Flexibilität.

Wichtig: **Was passiert, wenn Sie kündigen wollen?**

- Können Sie Ihre Daten exportieren?
- In welchem Format? (XML, Standard-Datenbank oder proprietär?)
- Wie lange dauert der Export?
- Kostet der Export extra?

Das ist der "Vendor Lock-in" Problem: Manche Anbieter machen es schwer, Ihre Daten zu nehmen und zu einem anderen System zu gehen. Das sollten Sie verhindern.

4. Datenexport und Dateneigentum.

Ihre Patientendaten gehören Ihnen, nicht dem Software-Anbieter. Das ist rechtlich klar. Aber vertraglich sollte das auch stehen.

Fragen Sie: "Kann ich meine gesamte Datenbank jederzeit in einem Standard-Format exportieren?" Die Antwort sollte "Ja, natürlich" sein. Wenn der Anbieter das ablehnt oder erschwert, ist das ein rotes Licht.

5. Wartungsvertrag und Service Level Agreement (SLA).

Ein SLA definiert, wie schnell der Support reagiert und wie verfügbar das System sein soll. Typisch:

- "Support-Anruf wird innerhalb 4 Stunden beantwortet."
- "Systemverfügbarkeit von mindestens 99,5% pro Monat."
- "Bei kritischen Bugs: Hotfix innerhalb 24 Stunden."

Überprüfen Sie, dass das SLA Ihre Anforderungen erfüllt. Für eine Praxis mit 5 Ärzten ist ein 99,5%-SLA oft ausreichend. Für eine größere Praxis könnte 99,9% notwendig sein.

6. Hosted vs. On-Premise – Die kritische Entscheidung.

On-Premise: Das PVS läuft auf Ihrem Server in der Praxis. Sie haben Kontrolle, Sie speichern die Daten lokal. Der Vorteil: Maximale Kontrolle. Der Nachteil: Sie sind verantwortlich für Sicherung, Updates, Hardware.

Hosted / Cloud: Das PVS läuft auf den Servern des Anbieters. Die Daten sind in einer Remote-Cloud. Der Vorteil: Der Anbieter kümmert sich um Backups und Updates. Der Nachteil: Sie sind abhängig von der Internet-Verbindung und vom Anbieter.

Für kleine Praxen ist Hosted oft praktischer (weniger Verwaltungsaufwand). Für größere Praxen ist On-Premise oft besser (mehr Kontrolle). Aber das ist eine Geschäftsentscheidung.

Wichtig: Falls Sie sich für Hosted entscheiden, prüfen Sie: - Wo sind die Server? (Deutschland ist besser für Datenschutz.) - Wie gut ist die Internet-Verbindung? - Was ist der Fallback, wenn das Internet weg ist?

> **Merksatz:** On-Premise = Ihre Kontrolle, Ihre Verantwortung. Hosted = Anbieter-Kontrolle, Internet-Abhängigkeit.

6.6.3. Die Transition: Wechsel von einem System zum anderen

Wenn Sie das PVS wechseln, ist das ein großes Projekt. Plan im Voraus:

1. **Parallelbetrieb:** Einige Zeit (oft 1-2 Wochen) laufen beide Systeme parallel. Im alten System dokumentieren Sie noch, das neue System wird befüllt und getestet.
2. **Datenmigration:** Die Altdaten werden aus dem alten System exportiert und in das neue importiert.
3. **Test-Phase:** Intensives Testen, ob alle Daten korrekt übertragen sind, ob die Termindaten passen.
4. **Stichtag:** An einem Freitag wechselt man zum neuen System. Ab Montag läuft alles nur noch im neuen System.
5. **Nachbetreuung:** Die erste Woche nach dem Wechsel sind die kritischen Tage. Der Support des neuen Anbieters sollte vor Ort oder per Hotline verfügbar sein.

Das kostet Zeit und oft auch Geld. Aber es ist notwendig, um einen sauberen Übergang zu schaffen.

6.6.4. Checkliste: PVS-Auswahl und Zertifizierung

- ☐ Das neue/aktuelle PVS ist KBV-zertifiziert – ich habe das auf der KBV-Website überprüft.
- ☐ Das PVS unterstützt alle aktuellen TI-Dienste (eRezept, eAU, KIM, ePA).
- ☐ Der Anbieter hat eine klare Roadmap für zukünftige TI-Updates.
- ☐ Updates werden mindestens vierteljährlich eingespielt.
- ☐ Der Vertrag hat eine kurze Laufzeit (1-3 Jahre) mit jährlicher Verlängerungsoption.
- ☐ Ich kann meine Daten jederzeit in einem Standard-Format exportieren.
- ☐ Das Service Level Agreement (SLA) erfüllt meine Anforderungen (Verfügbarkeit, Support-Zeiten).
- ☐ Falls Cloud-basiert: Die Server stehen in Deutschland oder der EU.
- ☐ Falls Cloud-basiert: Es gibt einen Fallback, wenn das Internet ausfällt.
- ☐ Falls On-Premise: Ich bin verantwortlich für Backups, Updates, Hardware – und habe einen Plan dafür.
- ☐ Der PVS-Anbieter bietet Schulung für die Mitarbeiter an.
- ☐ Ich habe einen Wechsel-Plan, falls ich später das System austauschen muss.

6.7. PVS-Sicherheit im Betrieb: Wer darf was tun?

Eine Arzthelferin sitzt am Praxis-PC und lädt sich eine E-Mail herunter. Das Passwort des PVS klebt auf einem Klebezettel unter der Tastatur. Der Facharzt nutzt den gleichen Account wie die Verwaltung. Niemand dokumentiert, wer wann was im PVS getan hat.

6.7.1. Das Kernprinzip: Getrennte Benutzerkonten und Rollen

Das ist nicht optional, sondern ein Standard des Datenschutzes und der Patientensicherheit: **Jeder Nutzer des PVS braucht einen eigenen Benutzeraccount.**

Warum? Mehrere Gründe:

1. **Haftung:** Wenn etwas schief geht (falsche Diagnose in der Akte, unbefugter Zugriff), muss klar sein, wer es getan hat. Mit einem gemeinsamen Account ist das unmöglich.
2. **Sicherheit:** Ein gemeinsamer Account mit einfachem Passwort ist ein Sicherheitsrisiko. Ein eigener Account mit komplexem Passwort ist besser zu schützen.
3. **Zugriffskontrolle:** Ein Arzt braucht andere Rechte als eine Arzthelferin. Die Buchhaltung braucht andere Rechte als die Annahme. Das PVS sollte diese Unterschiede durchsetzen.
4. **Audit-Trail:** Die Protokollierung zeigt, wer wann was getan hat. Das ist für Datenschutz und Fehleranalyse essentiell.

Die Rollen im PVS sollten typischerweise so aussehen:

- **Arzt:** Voller Zugriff auf Patientenakten, Diagnosen, Rezepte, eAU, ePA. Darf alle klinischen Entscheidungen treffen.

- **MFA (Medizinische Fachangestellte):** Zugriff auf Patientenverwaltung, Termin-Erfassung, Labordaten-Eingabe. Darf keine Diagnosen ändern.
- **Abrechnung:** Zugriff auf Abrechnungsdaten, aber nicht auf sensible Diagnosen. Darf Abrechnung verwalten, keine Ärztliche Tätigkeit.
- **Admin (IT):** Technischer Zugang für Wartung, aber keinen klinischen Zugriff. Oder ein separater Admin, der Benutzer verwaltet.

Das PVS sollte diese Rollen durchsetzen. Es sollte verhindern, dass eine Arzthelferin eine Diagnose ändert. Das sollte technisch unmöglich sein, nicht nur ein "Bitte nicht tun".

6.7.2. PIN und Passwort-Sicherheit

Hier kommt der praktische Teil: **Jeder Account braucht ein starkes Passwort.**

Was ist stark? Mindestens 12 Zeichen, Mix aus Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen. Ein Passwort-Manager (z. B. Bitwarden, 1Password, KeePass) sollte diese Passwörter speichern.

Das klassische Szenario – "Das Passwort ist zu komplex, also schreibe ich es auf einen Klebezettel" – ist ein absolutes No-Go. Das macht die ganze Zugriffsschutz zunichte.

PIN-Login beim Start: Manche PVS-Systeme erfordern zusätzlich eine PIN beim Hochfahren der Workstation oder beim Login. Das ist sinnvoll – es verhindert, dass jemand eine Arzthelferin-PC nutzt und damit im PVS handelt.

Automatischer Logout: Das PVS sollte automatisch ausloggen, wenn der Nutzer eine Weile inaktiv ist (z. B. 15 Minuten). Das verhindert, dass jemand einen verlassenen PC nutzt.

6.7.3. Protokollierung und Audit-Trail

Das PVS sollte alles protokollieren:

- **Wer hat sich angemeldet?** Zeitstempel.
- **Was wurde getan?** Welche Akte wurde geöffnet, welche Diagnose wurde eingegeben, welches Rezept wurde geschrieben.
- **Wann wurde es getan?** Sekunden-Genauigkeit.
- **Was wurde geändert?** Der alte Wert, der neue Wert.

Diese Protokolle sollten mindestens 1-2 Jahre aufbewahrt werden. Im Notfall (z. B. bei einem Datenschutz-Vorfall) können Sie nachvollziehen: "Am 15.3. um 14:30 hat Arzthelferin Sandra die Akte des Patienten Meyer geöffnet und die Diagnose gelesen. Das war korrekt, es war zur Terminverwaltung nötig."

Diese Protokollierung ist nicht optional – sie ist eine Anforderung nach dem Datenschutz (DSGVO) und der ärztlichen Schweigepflicht.

> **Merksatz:** Protokollierung ist nicht Misstrauen, sondern Transparenz und Nachvollziehbarkeit. Im Notfall ist es Ihr Beweis, dass alles korrekt gelaufen ist.

6.7.4. Das Betriebssystem unter dem PVS: Alte Windows-Versionen sind eine Falle

Hier ist ein großes Sicherheits-Problem: **Das PVS läuft auf einem Betriebssystem – oft Windows 10 oder älter.**

Das ist problematisch. Windows 10 ist veraltet. Windows-Versionen erhalten etwa 10 Jahre Support. Danach gibt es keine Security-Updates mehr. Ein PC mit Windows 7 (Release 2009, Support-Ende 2020) ist heute ein Sicherheitsrisiko – ohne Patches für neue Sicherheitslücken.

Was sollten Sie tun?

1. **Überprüfen Sie, welche Windows-Version auf den PVS-Workstations läuft.** (Windows Settings → About)
2. **Wenn es älter als Windows 10 ist, planen Sie ein Upgrade.** Windows 11 ist die aktuelle Version.
3. **Sprechen Sie mit dem PVS-Anbieter:** Unterstützt das PVS auch Windows 11? Gibt es Kompatibilitätsprobleme?
4. **Update-Plan:** Das Windows-Betriebssystem sollte regelmäßig (mindestens monatlich) aktualisiert werden. Das sollte geplant und getestet sein.

Eine vernünftige PVS-Infrastruktur hat ein modernes Windows-Betriebssystem mit regelmäßigen Security-Updates. Alles andere ist fahrlässig.

6.7.5. Netzwerksicherheit: Der PVS-Server gehört nicht ins Internet

Das ist kritisch: **Der PVS-Server (falls On-Premise) sollte nicht direkt aus dem Internet erreichbar sein.**

Was bedeutet das konkret? Der PVS-Server läuft im lokalen Netzwerk der Praxis. Administratoren können sich von außen per VPN einloggen (mit Authentifizierung), aber nicht direkt per Internet-Verbindung ohne VPN.

Ein gängiges Szenario: - PVS-Server: Im lokalen Netzwerk, Adresse 192.168.1.10. - Firewall: Blockiert alle direkten Internet-Zugriffe auf den Server. - Fernwartung: Der IT-Dienstleister verbindet sich per VPN, nicht per direkte Internet-Verbindung.

Das ist deutlich sicherer als: “Der PVS läuft mit Port 3389 (Remote Desktop) offen im Internet – jeder kann versuchen, sich einzuloggen.”

Netzwerk-Architektur für große Praxen:

- **Separate Netzwerk-Segmente:** Der PVS-Server sitzt in einem separaten Netzwerk-Segment, getrennt von Patientenpcs und Internet-Nutzung.
- **Firewall-Regeln:** Nur autorisierte Geräte können auf den PVS zugreifen.
- **Monitoring:** Ein System überwacht, wer auf den PVS zugreift und von wo.

Für kleine Praxen: Ein solides Passwort, ein Firewall und ein Update-Plan reichen oft aus.

6.7.6. Fernwartung: Nur mit Protokoll und Genehmigung

Der IT-Dienstleister oder der PVS-Anbieter braucht manchmal Fernzugriff auf den PVS, um Updates zu spielen oder Fehler zu beheben. Das ist normal, aber es sollte protokolliert sein.

Regeln für Fernwartung:

1. **Genehmigung:** Vor der Fernwartung sollte eine Genehmigung vorliegen. Im Idealfall: Der Praxisinhaber stimmt zu.
2. **Zeitfenster:** Die Fernwartung sollte zu einer vereinbarten Zeit stattfinden, z. B. nachts nach der Sprechstunde, nicht mittendrin.
3. **Dokumentation:** Wer hat remote zugegriffen? Wann? Für wie lange? Zu welchem Zweck? Was wurde gemacht?
4. **Zugangsschutz:** Der Fernzugriff sollte mit Authentifizierung (z. B. VPN + Passwort) geschützt sein, nicht einfach offen.

Das ist ein feines Gleichgewicht: Fernwartung ist oft notwendig, aber sie muss kontrolliert und dokumentiert sein.

6.7.7. Checkliste: PVS-Sicherheit im Betrieb

- ☐ Jeder Nutzer des PVS hat einen eigenen Benutzeraccount – keine gemeinsamen Accounts.
- ☐ Die Zugriffsrechte sind nach Rollen aufgeteilt (Arzt, MFA, Abrechnung, Admin).
- ☐ Das PVS verhindert technisch, dass MFAs Diagnosen ändern können.
- ☐ Alle Passwörter sind stark (mindestens 12 Zeichen, gemischt) und werden in einem Passwort-Manager gespeichert.
- ☐ Keine Passwörter auf Zetteln unter der Tastatur.
- ☐ Das PVS protokolliert, wer wann was getan hat.
- ☐ Die Audit-Logs werden mindestens 1-2 Jahre aufbewahrt.
- ☐ Das Betriebssystem der PVS-Workstations ist aktuell (Windows 10 oder 11).
- ☐ Security-Updates für Windows werden mindestens monatlich eingespielt.
- ☐ Der PVS-Server ist nicht direkt aus dem Internet erreichbar.
- ☐ Fernwartung erfordert Genehmigung und wird dokumentiert.
- ☐ Es gibt eine Firewall oder Netzwerk-Segmentierung, die den PVS schützt.
- ☐ Nach längerer Inaktivität erfolgt ein automatischer Logout.

6.8. Backup im PVS-Kontext: Was konkret gesichert werden muss

Die Grundprinzipien einer soliden Backup-Strategie – 3-2-1-Regel, Backup-Häufigkeit, Ransomware-Resilienz, Verschlüsselung, Verantwortungsregelung mit dem IT-Dienstleister – sind in Teil 3 erklärt. Dieses Kapitel setzt diese Prinzipien konkret auf die PVS-Situation an: Was genau muss gesichert werden? Worauf kommt es beim Restore-Test an? Und welche Fehler passieren in der Praxis immer wieder?

6.8.1. Das vollständige PVS-Backup: Mehr als nur die Datenbank

Ein häufiger Irrtum: "Wir sichern das PVS" – und damit ist nur die Datenbank gemeint. Das PVS-Backup ist aber ein Gesamtpaket.

1. Die PVS-Datenbank. Patientenstammdaten, Behandlungsunterlagen, Diagnosen, Medikationen, Abrechnungsdaten. Das Herzstück. Die meisten Backup-Lösungen decken das ab – aber prüfen Sie es explizit.

2. DICOM-Bilddaten. Röntgenaufnahmen, CT-Bilder, Ultraschallbilder sind oft nicht in der PVS-Datenbank gespeichert, sondern auf einem separaten PACS-Server oder Bildarchiv. Eine Backup-Lösung, die nur die Datenbank sichert, lässt diese Daten außen vor. Das fällt erst im Notfall auf.

3. Labordaten und externe Befunde. Laborrückläufer von externen Laboren, EKG-Dateien, Befunde von Fachkollegen – je nach PVS-Konfiguration in der Datenbank importiert oder separat im Dateisystem abgelegt. Lassen Sie von Ihrem IT-Dienstleister klären, wo diese Dateien liegen und ob sie gesichert werden.

4. TI-Konfiguration. Konnektor-Konfiguration, eHBA/SMC-B-Verwaltung, KIM-Einstellungen. Diese sind nicht in der PVS-Datenbank enthalten, aber im Notfall (z. B. Konnektor-Austausch) dringend notwendig. Mindestens als dokumentierte Sicherung anlegen.

5. Praxis-Infrastruktur. Router-Einstellungen, VPN-Konfigurationen, Firewall-Regeln, Passwort-Manager-Dateien. Dazu mehr in Teil 3 – hier der Hinweis: Diese werden oft vergessen und kosten im Notfall mehr Zeit als der eigentliche Daten-Restore.

> **Merksatz:** Ein Backup, das nur die Datenbank sichert, aber nicht die Bilddaten oder Labordaten, ist unvollständig. Im Notfall fehlen genau diese Dokumente – und sie sind nicht wiederherstellbar.

6.8.2. Backup-Schema: Vollbackup und inkrementell

Neben der 3-2-1-Strategie (Teil 3) lohnt es sich, das Backup-Schema zu optimieren:

Vollbackup einmal pro Woche (z. B. Sonntagsnacht): Alle Daten werden komplett gesichert. Langsamerer Prozess, braucht mehr Speicherplatz – aber einfacher im Restore.

Inkrementelle Backups täglich oder stündlich: Nur die Änderungen seit dem letzten Backup werden gespeichert. Schnell, kompakt – aber im Restore-Fall müssen Vollbackup und alle Inkremente zusammengespielt werden.

Eine pragmatische Kombination für die meisten Praxen: Wöchentliches Vollbackup + tägliche inkrementelle Backups. Im Notfall ist der Datenverlust auf maximal einen Tag begrenzt, der Speicherbedarf bleibt überschaubar.

6.8.3. Der PVS-spezifische Restore-Test

In Teil 3 ist der Restore-Test als Grundprinzip erklärt. Im PVS-Kontext gibt es eine zusätzliche Anforderung: **Funktioniert das PVS nach dem Restore?**

Eine Datenbank lässt sich technisch korrekt wiederherstellen – aber die Praxissoftware läuft danach trotzdem nicht, weil Lizenzdaten fehlen, Konfigurationseinstellungen verloren gegangen sind oder die Software-Version nicht mehr mit der gesicherten Datenbank kompatibel ist.

Der jährliche Vollständige Restore-Test sollte daher folgende Punkte abdecken:

- Datenbank wiederhergestellt – vollständig und ohne Fehler?
- PVS startet und ist voll funktionsfähig?
- Patientenakten sind lesbar und korrekt?
- DICOM-Bilder und externe Befunde sind vorhanden?
- Abrechnungsdaten der letzten Quartale sind korrekt?

Dieser Test sollte dokumentiert werden: Datum, Ergebnis, etwaige Probleme und wie sie gelöst wurden. Im Streitfall ist das Ihr Nachweis, dass ein zuverlässiges Backup-System existiert.

6.8.4. Typische Fehler: Was in der Praxis schiefgeht

Diese Fehler tauchen in Arztpraxen immer wieder auf:

Fehler 1: Backup auf dem gleichen Server wie die Daten. Die Datenbank wird auf einer zweiten Festplatte gesichert – aber beide Festplatten stecken im gleichen Server-Gehäuse. Wenn der Server brennt oder gestohlen wird, sind beide weg. Das ist kein Backup, das ist ein Spiegel.

Fehler 2: Backup nie getestet. Das Backup läuft automatisch jede Nacht. Die Praxis hat es seit zwei Jahren nicht getestet. Im Notfall funktioniert es nicht – die Backup-Software war fehlkonfiguriert, oder die Dateien wurden beschädigt gespeichert. Das fällt erst auf, wenn man es braucht.

Fehler 3: Alte Backups werden gelöscht. Nach zwei Jahren werden alle Backups überschrieben – "weil Speicherplatz kostet". Ein Patient kommt fünf Jahre später zur Kontrolle und braucht Unterlagen aus seiner damaligen Behandlung. Die Akte ist weg. Das ist nicht nur ein praktisches Problem, sondern ein Verstoß gegen die Aufbewahrungspflicht nach § 630f BGB.

Fehler 4: Backup-Schlüssel verloren. Die Backups sind verschlüsselt, aber der Schlüssel liegt auf dem Laptop des IT-Dienstleisters. Der Dienstleister wechselt, der Laptop ist weg, der Schlüssel ist weg. Die Backups sind nicht mehr lesbar.

Fehler 5: Nur die Datenbank gesichert, nicht die Bilddaten. Die PVS-Datenbank wird täglich gesichert. Die DICOM-Bilder liegen auf einem separaten Server – der nie in die Backup-Strategie einbezogen wurde. Im Notfall fehlen alle Röntgenbilder und CT-Aufnahmen.

6.8.5. Monatlicher Backup-Report vom IT-Dienstleister

Eine gute Vereinbarung mit dem IT-Dienstleister enthält nicht nur die Backup-Parameter (Häufigkeit, Ort, Verschlüsselung) – sie enthält auch einen **monatlichen Nachweis**, dass die Backups tatsächlich funktionieren.

Das kann ein einfacher Bericht sein: "Backup vom [Datum] erfolgreich, Größe X GB, Restore-Test durchgeführt am [Datum], Ergebnis: vollständig." Wenn Sie diesen Bericht nicht bekommen, fragen Sie danach. Wer das Backup verantwortet, muss auch belegen können, dass es funktioniert.

6.8.6. Checkliste: Backup im PVS-Kontext

- ☐ Das Backup umfasst nicht nur die PVS-Datenbank, sondern auch DICOM-Bilder, Labordaten und Infrastruktur-Konfiguration.
- ☐ Ich weiß, wo DICOM-Bilddaten physisch gespeichert sind – und sie sind in der Backup-Strategie erfasst.
- ☐ Labordaten und externe Befunde sind im Backup enthalten (auch wenn sie nicht in der Datenbank sind).
- ☐ Die TI-Konfiguration (Konnektor, KIM) ist dokumentiert und als Backup verfügbar.
- ☐ Das Backup-Schema ist definiert: wöchentliches Vollbackup plus tägliche Inkremente.
- ☐ Der jährliche Restore-Test prüft explizit, ob das PVS nach dem Restore funktionsfähig ist.
- ☐ Alter Backups werden archiviert, nicht überschrieben – Aufbewahrungspflicht 10 Jahre (§ 630f BGB).

- ☐ Ich erhalte monatlich einen Backup-Report vom IT-Dienstleister.
- ☐ Der Backup-Schlüssel ist sicher und an mindestens zwei Orten aufbewahrt – unabhängig vom IT-Dienstleister.
- ☐ Die Vereinbarung mit dem IT-Dienstleister deckt alle Backup-Parameter schriftlich ab.

7. Teil 6: Medizinische Geräte am Netz

Vernetzte medizinische Geräte sind ein Sicherheitsparadoxon: Ohne sie läuft eine moderne Praxis nicht. Aber genau diese Geräte sind oft die größten Schwachstellen.

7.1. Das Paradoxon der vernetzten Medizintechnik

Stellen Sie sich eine typische Arztpraxis vor. Ein modernes Röntgengerät steht im Nebenraum, an das Praxisnetzwerk angeschlossen, damit die Bilder direkt ins PVS gehen. Ein EKG-Gerät ist mit der Workstation des Arztes verbunden. Das Labor sendet Ergebnisse automatisch in die Patientenakte. Das Ultraschallgerät speichert seine Aufnahmen in einem DICOM-Server. Alles vernetzt, alles modern, alles effizient.

Dann die Kehrseite: Das Röntgengerät läuft auf Windows XP – aus dem Jahr 2001. Der Hersteller sagt: Ein Update würde die CE-Zertifizierung aufheben, die Garantie verfallen, die regulatorischen Freigaben entfallen. Also bleibt es wie es ist. Das WLAN-Passwort für das EKG-Gerät steht auf der Rückseite. Das Labor-Interface wurde vor fünfzehn Jahren programmiert und funktioniert nur mit einer ganz bestimmten – und heute unsicheren – Verschlüsselungsmethode. Der DICOM-Server läuft in einem Schrank im Patientenzimmer, ohne Firewall-Schutz, direkt ans Internet angeschlossen.

Dies ist kein erfundenes Szenario. Dies ist die Realität in vielen Praxen. Und genau hier liegt das Problem: Medizinische Geräte sind oft die letzten Bastionen von veralteter, unsicherer Technik in Betrieben, die ansonsten professionell aufgestellt sind.

7.2. Warum medizinische Geräte ein besonderes Risiko sind

Es gibt mehrere Gründe, warum vernetzte Medizintechnik ein besonderes Sicherheitsrisiko darstellt – Gründe, die es bei fast keinem anderen Gerät gibt.

Lange Betriebsdauer: Ein Röntgengerät wird nicht nach fünf Jahren ausgetauscht wie ein Computer. Es wird zwanzig, dreißig Jahre lang betrieben. Der Hersteller unterstützt es vielleicht für zehn Jahre – dann nicht mehr. Sicherheitsupdates gibt es möglicherweise schon lange nicht mehr. Das Betriebssystem, auf dem es läuft, ist längst out of support.

Zulassungsrecht und CE-Zertifizierung: In Europa unterliegen medizinische Geräte der Medizinprodukte-Verordnung (MDR). Eine Änderung am Gerät – auch nur ein Software-Update – erfordert formale Überprüfung und neue Zertifizierung. Das ist teuer, zeitaufwendig und oft wirtschaftlich nicht mehr sinnvoll für alte Geräte. Der Hersteller sagt nicht “das können wir nicht”, sondern “das dürfen wir nicht”. Und damit ist die Sache erledigt.

Keine Alternativen: Es gibt oft keine einfache Lösung. Sie können das Röntgengerät nicht einfach durch ein anderes ersetzen – Platzmangel, Kosten, Umbauten, neue Schulung. Also bleibt das alte Gerät im Betrieb. Und da es weiterhin Patienten untersucht, erleichtern Sie sich nicht einfach davon.

Vernetztheit: Die Geräte sind nicht isoliert. Sie sind ans Praxisnetzwerk angeschlossen, um Daten direkt ins PVS zu senken, um Patienteninformationen zu empfangen, um Befunde zu versenden. Das Netzwerk dieser Geräte ist damit auch das Netzwerk aller anderen IT-Systeme der Praxis.

Unkomplizierte physische Zugänglichkeit: Ein Röntgengerät steht offen herum. Das WLAN-Passwort klebt hinten dran. Der DICOM-Server läuft in einem Patientenzimmer ohne Netzwerksegmentierung. Ein Eindringling – oder schlicht ein neugieriger Patient – kann sich Zugang verschaffen, ohne dass es jemandem auffällt.

7.3. Das zentrale Problem: Ein Windows-XP-PC mit Netzanschluss ist ein Einfallstor

Das Röntgengerät von 2001, das auf Windows XP läuft – wäre es ein Einzelfall, könnte man sich entspannen. Es ist aber einer der häufigsten Fälle. Und genau hier liegt das zentrale Risiko:

Ein Windows-XP-PC mit Netzwerkverbindung ist heute ein offenes Einfallstor für jeden halbwegs kompetenten Angreifer. Es gibt tausende bekannte Sicherheitslücken in Windows XP, die niemand mehr patcht. Angreifer-Werkzeuge, die auf diese Lücken zielen, sind online frei verfügbar. Ein Gerät mit dieser Konfiguration ist eine wandelnde Beute für jeden Ransomware-Worm, der das Netzwerk passiert.

Das Szenario könnte so aussehen: Ein Mitarbeiter der Praxis öffnet eine Phishing-E-Mail, klickt auf einen Link, und infiziert seinen Laptop mit Malware. Die Malware breitet sich übers Netzwerk aus – und findet das Röntgengerät. Dieses läuft auf einem ungepatchen System mit bekannten Schwachstellen. Der Angreifer hat leichte Beute. Plötzlich ist nicht nur das Röntgengerät infiziert, sondern über die Netzwerkverbindung auch das PVS, die Praxisserver, alles.

Das ist nicht Paranoia. Das ist IT-Realität für Arztpraxen, die Medizingeräte nutzen.

7.4. Welche Geräte besonders betroffen sind

Nicht alle medizinischen Geräte sind gleich riskant. Manche sind isoliert, manche sind vernetzt. Manche laufen auf modernen Systemen, manche auf veralteten.

Besonders kritisch: - **Röntgen- und DICOM-Geräte:** Diese werden oft über Netzwerk angesprochen, speichern Daten zentral, sind mit dem PVS verbunden. Viele ältere Röntgengeräte laufen auf veralteten Windows-Versionen. - **Labor-Systeme:** Automatisierte Labore sind oft hochgradig vernetzt – und kommunizieren mit älteren, proprietären Protokollen, die nie für Sicherheit entworfen wurden. - **EKG- und Kardio-Geräte:** Viele ältere Modelle haben WLAN oder USB-Konnektivität ohne moderne Sicherheitsstandards.

- **DICOM-Viewer und Workstations:** Dedizierte Bildbetrachtungssysteme speichern oft Patientendaten lokal und haben keine regelmäßigen Updates.

Moderat kritisch: - **Ultraschall-Geräte:** Viele neuere Modelle haben bessere Sicherheitsstandards als ältere Röntgen- oder Labor-Systeme. Ältere Geräte können aber problematisch sein, besonders wenn sie älter als zehn Jahre sind. - **Zahnärztliche Röntgen-Intraoralsysteme:** Diese sind oft weniger kritisch, weil sie weniger mit dem Netzwerk integriert sind. Aber auch hier gilt: Alter = Risiko.

Weniger kritisch (aber nicht unbedenklich): - **Patientenmonitore, Blutdruck-Messgeräte, einfache Thermometer:** Diese stellen oft ein geringeres Netzwerk-Risiko dar, weil sie weniger automatisiert vernetzt sind. Sie können aber trotzdem Vektor für Sicherheitsprobleme sein, wenn sie zentral verwaltet werden.

7.5. Die Frage, die Sie sich stellen müssen

Vor allem: Wissen Sie eigentlich, welche Geräte in Ihrer Praxis vernetzt sind? Und wie?

Das ist die Schlüsselfrage. Viele Praxisinhaber können das gar nicht verlässlich beantworten. Das Röntgengerät wurde vor fünfzehn Jahren installiert, und seitdem kümmert sich der Hersteller-Techniker darum. Wer genau weiß, welches Betriebssystem draufläuft, welche Ports offen sind, wie es mit dem Netzwerk verbunden ist? Oft: niemand.

Genau das ist das Problem. Und genau damit müssen Sie beginnen – mit einer ehrlichen Bestandsaufnahme. Die kommenden Kapitel zeigen Ihnen, wie.

7.6. Checkliste: Grundlagen zu Medizingeräten

- ☐ Ich kenne alle medizinischen Geräte in meiner Praxis, die ans Netzwerk angeschlossen sind.
- ☐ Ich weiß, welches Betriebssystem auf jedem dieser Geräte läuft (Windows XP/7/10, Linux, proprietär?).
- ☐ Ich weiß, wann diese Geräte das letzte Update bekommen haben.
- ☐ Ich kenne die Herstellerangaben zur CE-Zertifizierung und zur Update-Unterstützung.
- ☐ Ich habe die Hersteller kontaktiert und explizit nach Sicherheitsupdates und deren Verfügbarkeit gefragt.
- ☐ Mein IT-Dienstleister kennt alle vernetzten Geräte und deren Spezifikationen.

7.7. Vernetzte Geräte und ihre Risiken

7.7.1. Das Dilemma: Funktionalität versus Sicherheit

Das grundlegende Problem ist schnell erklärt, aber fast unlösbar: Medizinische Geräte werden für Jahrzehnte betrieben. Während dieser Zeit laufen ihre Betriebssysteme und

Software-Komponenten völlig aus dem Support. Der Hersteller liefert keine Sicherheitsupdates mehr. Neue Sicherheitslücken werden entdeckt – aber nicht für diese Geräte gepatcht. Trotzdem müssen die Geräte funktionieren. Und nicht nur funktionieren – sie müssen mit modernen Systemen wie dem PVS vernetzt sein.

Das ist das Dilemma. Die Lösung scheint offensichtlich: "Einfach updaten!" Aber hier kommt die regulatorische Komponente ins Spiel.

7.7.2. Das Zulassungsrecht: Warum Updates oft verboten sind

In Europa unterliegen medizinische Geräte der Medizinprodukte-Verordnung (MDR). Diese Verordnung ist nicht einfach eine Richtlinie – sie ist Gesetz. Sie regelt, wie medizinische Geräte entwickelt, geprüft, zertifiziert und vermarktet werden.

Ein Röntgengerät ist nicht einfach ein Computer mit Röntgen-Software. Es ist ein zertifiziertes medizinisches Gerät. Diese Zertifizierung – die CE-Kennzeichnung – basiert auf einer Prüfung des exakten Zustandes, in dem sich das Gerät befindet. Hersteller, Herstellungsprozess, Software-Version, Kalibrierung – alles wurde überprüft und genehmigt.

Wenn Sie jetzt ein Update installieren oder etwas am Gerät ändern, ist diese Zertifizierung potenziell ungültig. Der Hersteller müsste das Gerät in seinem neuen Zustand erneut überprüfen, genehmigen, zertifizieren lassen. Das kostet mehrere hunderttausend Euro und dauert Monate.

Aus ökonomischer Perspektive ist das für alte Geräte unmöglich. Der Hersteller verdient nichts mehr damit. Also sagt er nicht "das können wir nicht technisch machen", sondern "das dürfen wir nicht rechtlich machen – ohne massive Kosten". Viele Hersteller verbieten Updates explizit im Warranty-Dokument: "Jedes Update macht die Zertifizierung ungültig."

Das ist die legale Erklärung dafür, warum Ihr Röntgengerät von 2001 auf Windows XP läuft und wahrscheinlich nie aktualisiert werden wird.

7.7.3. Welche Geräte besonders betroffen sind

Röntgengeräte und DICOM-Systeme sind das häufigste Problem. Diese Geräte sind oft: - 10-20 Jahre alt - Tief ins Netzwerk integriert (Bilduebertragung, DICOM-Abfragen, PVS-Integration) - Mit proprietärer oder uralt-aktualisierter Software bestückt - Nicht standardisiert – jeder Hersteller hat sein eigenes System

Labor-Analysegeräte sind ebenfalls kritisch. Automatisierte Labore kommunizieren über Schnittstellen, die teilweise zwanzig Jahre alt sind und unsichere Protokolle nutzen. Ein einzelnes Labor-Interface kann das ganze Praxisnetzwerk durchdrungen haben.

EKG- und Kardio-Systeme sind oft älter als Sie denken. Viele Kardiographen, die heute noch in Praxen laufen, stammen aus den 2000er Jahren. Einige haben WLAN-Module, die ohne jegliche moderne Verschlüsselung arbeiten – WEP-Verschlüsselung, die 2001 bereits unsicher war, oder ganz ohne Verschlüsselung.

DICOM-Viewer und Workstations sind dedizierte Bildbetrachtungssysteme. Sie speichern manchmal Patientendaten lokal und haben eine ältere Betriebssystem-Installation, die regelmäßig vergessen wird zu patchen.

7.7.4. Die praktischen Konsequenzen

Was bedeutet das alles konkret für Ihre Praxis?

Ein Röntgengerät auf Windows XP mit Netzwerkverbindung ist ein direktes Einfallstor. Die bekannten Schwachstellen von Windows XP sind dokumentiert, Exploit-Tools sind online verfügbar. Wenn ein Angreifer ins Netzwerk kommt – durch Phishing, Brute-Force, oder wenn er den Netzwerk-Zugang physisch nutzt – kann er das Röntgengerät compromittieren. Von dort aus kann er sich lateral ins PVS oder zu anderen Systemen ausbreiten.

Ein unsicheres Labor-Interface bedeutet, dass jemand mit Netzwerk-Zugang die Laborergebnisse manipulieren könnte, oder dass Patientendaten auf dem Lab-Interface offengelegt werden. Die proprietären Protokolle bieten keine modernen Sicherheitsstandards.

Ein WLAN-fähiges EKG-Gerät mit WEP-Verschlüsselung oder ohne Verschlüsselung bedeutet, dass jemand mit einfachen Werkzeugen den Datenverkehr abhören und manipulieren kann.

Das sind keine theoretischen Risiken. Das sind reale, bekannte Angriffsvektoren, die Cyberkriminelle aktiv nutzen.

7.7.5. Was Sie trotzdem tun können

Sie können nicht einfach das Gerät updaten. Aber Sie können mehreres tun, um das Risiko zu minimieren:

1. Das Gerät vom Rest des Netzes isolieren

Ein Gerät, das nicht mit anderen Systemen kommuniziert, kann das Praxisnetzwerk nicht infizieren. Wenn die Architektur es zulässt, können vernetzte Medizingeräte in einem separaten Netzwerk-Segment laufen – getrennt vom PVS-Netzwerk durch eine Firewall. Die Datenübertragung zum PVS findet dann über ein gut gesichertes Gateway statt, das die Kommunikation überwacht und filtert.

Das ist nicht immer möglich – manche Geräte sind direkt mit dem PVS integriert und brauchen direkten Zugang. Aber wo es geht, sollte es gemacht werden.

2. Kein Internetzugang für Medizingeräte

Ein Medizingerät braucht normalerweise kein Internet. Es braucht Netzwerk-Zugang zum PVS und zu lokal-vernetzten Systemen, aber nicht zum Internet. Wenn das Gerät keinen Internet-Zugang hat, reduziert das die Angriffsfläche erheblich. Eine Firewall-Regel, die dem Medizin-Netzwerk-Segment den Internetzugang verbietet, ist eine simple, aber wirksame Schutzmaßnahme.

3. DICOM-Daten nur über gesicherte Netze übertragen

Wenn das Röntgengerät Bilder ins PVS sendet, sollte diese Übertragung nicht über offene Netzwerke laufen. Ein VPN-Tunnel zwischen dem Gerät und dem PVS-Server, oder zumindest eine sichere, verschlüsselte Verbindung mit Authentifizierung ist das Minimum.

4. Regelmäßige Schnittstellenupdates und Firmware-Updates wo möglich

Viele Hersteller können die Firmware des Gerätes nicht updaten, ohne die Zertifizierung zu gefährden – aber sie können spezifische Sicherheits-Patches für Schnittstellenmodule

liefern. Der HL7-Schnittstellen-Stack kann manchmal separat aktualisiert werden, ohne die Radiologie-Software anzutasten. Hersteller-Support gezielt fragen: “Welche Komponenten können ohne Neuzertifizierung aktualisiert werden?”

5. Physische und Netzwerk-Kontrolle

Das Gerät sollte in einem Bereich sein, zu dem nicht jeder physischen Zugang hat. WLAN-Passwörter sollten nicht auf der Rückseite kleben. Netzwerk-Verbindungen sollten überwacht sein – Bewegungen in der Log-Datei sollten auffallen.

6. Notwendigkeit neu bewerten

Bei Praxis-Renovierungen oder großeren IT-Projekten sollte die Notwendigkeit des vernetzten Betriebs neu bewertet werden: Kann das Röntgengerät isoliert laufen und Bilder manuell (oder mit sicherer automatisierter Schnittstelle) ins PVS gelangen? Kostet die Neuanschaffung eines modernen, sicheren Gerätes nicht weniger als die jährliche IT-Sicherheits-Aufrüstung für das alte System?

7.7.6. Die Rolle des IT-Dienstleisters

Ihr IT-Dienstleister sollte eine klare Inventur aller vernetzten Medizingeräte haben – mit Informationen zu: - Hersteller, Modell, Alter - Betriebssystem und aktuelle Versions-Nummer - Supportstatus beim Hersteller - Netzwerk-Integration: Wie ist das Gerät angebunden? - Bekannte Schwachstellen für diesen Geräte-Typ

Auf Basis dieser Inventur sollte für jedes kritische Gerät ein Maßnahmen-Plan erstellt werden. Dieser Plan kann die oben erwähnten Schritte (Isolierung, Firewall-Regeln, Firmware-Updates) konkret umsetzen.

7.7.7. Checkliste: Vernetzte Geräte und ihre Risiken

- ☐ Ich habe eine vollständige Inventur aller vernetzten medizinischen Geräte mit Alter, Betriebssystem und Hersteller.
- ☐ Für jedes Gerät habe ich beim Hersteller geklärt: Welche Updates sind verfügbar, und welche würden die Zertifizierung gefährden?
- ☐ Mein IT-Dienstleister hat einen Isolierungs- oder Segmentierungs-Plan für kritische Geräte erstellt.
- ☐ Medizingeräte haben keinen direkten Internetzugang – nur Zugang zum Praxis-Intra-Netz.
- ☐ DICOM- und Labordaten werden verschlüsselt übertragen.
- ☐ Ich habe eine Übersicht, welche Schnittstellenkomponenten updatebar sind und wann sie zuletzt aktualisiert wurden.
- ☐ Physischer Zugang zu Geräten und Netzwerk-Steckdosen ist kontrolliert.
- ☐ Das Thema ist mit meinem IT-Dienstleister geklärt und ein Eskalations-Plan existiert.

7.8. Netzsegmentierung als Lösung

7.8.1. Was Netzsegmentierung bedeutet

Stellen Sie sich Ihr Praxisnetzwerk momentan wie einen großen Raum vor: Alle Geräte sind darin, alle können miteinander kommunizieren. Der Röntgen-PC kann aufs PVS zugreifen, das PVS auf den Print-Server, der Print-Server auf das Röntgen-Gerät. Das klingt praktisch – ist aber unsicher. Wenn ein Gerät kompromittiert ist, können Angreifer von dort aus zu allen anderen Geräten lateral-bewegen.

Netzsegmentierung bedeutet: aus diesem großen Raum werden mehrere kleinere Räume. Jeder Raum ist durch eine Tür (Firewall) vom anderen getrennt. Geräte in Raum A können mit Raum B kommunizieren – aber nur über diese kontrollierte Tür. Geräte in Raum C sind komplett isoliert und können überhaupt nicht mit A oder B sprechen, es sei denn, das ist explizit erlaubt.

In praktischen Begriffen heißt das: Sie verwenden sogenannte VLANs (Virtual Local Area Networks). Ein VLAN ist eine logische Trennung – nicht physisch neue Kabel, sondern eine Konfiguration auf dem Switch. Der Switch kennt mehrere VLANs und weiß, dass Traffic zwischen ihnen blockiert ist, bis eine Firewall das erlaubt.

7.8.2. Warum das für Arztpraxen wichtig ist

Für eine Arztpraxis mit vernetzten Medizingeräten ist Netzsegmentierung nicht optional – es ist das Minimum einer sicheren Infrastruktur.

Szenario: Das Röntgengerät läuft auf Windows XP. Ein Angreifer kommt ins Praxisnetzwerk (durch Phishing eines Mitarbeiters). Er findet das Röntgengerät, kompromittiert es. Jetzt sitzt er auf einem Gerät, das mit dem gleichen Netzwerk verbunden ist wie das PVS, die Patientenakten, die Abrechnungsdaten. Von hier aus kann er lateral zum PVS gehen und Patientendaten stehlen.

Mit Segmentierung: Das Röntgengerät läuft auf einem separaten VLAN. Der Angreifer kompromittiert es. Jetzt versucht er, von diesem VLAN aufs PVS-VLAN zuzugreifen – und scheitert. Die Firewall blockiert den Zugriff. Der Schaden ist begrenzt auf das Röntgengerät. Das PVS und alle Patientendaten sind sicher.

Das ist die zentrale Logik von Segmentierung: Der Schadensradius jedes kompromittierten Gerätes wird begrenzt.

7.8.3. Wie man das umsetzt: Die praktische Architektur

Eine typische Netzsegmentierung für eine Arztpraxis könnte so aussehen:

VLAN 1 – Medizingeräte-Netz: Röntgen, EKG, Labor, DICOM-Viewer, Ultraschall. Alle diese Geräte laufen auf diesem Netz. Sie können untereinander kommunizieren, aber nicht ins PVS-Netz oder ins Internet.

VLAN 2 – PVS-Netz: Der PVS-Server, die Workstations der Mitarbeiter, die darauf zugreifen. Dieses Netz hat Zugang zum Internet (für TI, Updates, E-Mail) und zu den Medizingeräten (begrenzt, nur für Datenaustausch).

VLAN 3 – TI-Netz: Der TI-Konnektor und die Systeme, die damit kommunizieren (elektronische Gesundheitskarte, Rezepte). Getrennt vom Rest, um zu verhindern, dass ein kompromittiertes Praxis-Gerät die TI-Sicherheit gefährdet.

VLAN 4 – Gast-WLAN: Separate WLAN für Patienten und Besucher. Völlig isoliert vom restlichen Netz.

Management-Vlan: Optional: Ein separates Netz nur für die Verwaltung der Netzwerk-Hardware selbst.

Die Firewall dazwischen regelt, welche VLANs miteinander kommunizieren dürfen. Ein sauberes Regelwerk könnte zum Beispiel so aussehen: - Medizin-VLAN darf zum PVS-VLAN kommunizieren (nur Port 443, 80 für Datenaustausch) - Medizin-VLAN darf nicht ins Internet - PVS-VLAN darf mit Internet und TI-VLAN kommunizieren - Gast-WLAN darf ins Internet, aber nicht zu PVS oder Medizin - TI-VLAN nur zu PVS-VLAN für notwendige Funktionen

7.8.4. Was das technisch braucht

Um Netzsegmentierung umzusetzen, brauchen Sie drei Komponenten:

1. VLAN-fähiger Switch

Ihr aktueller Netzwerk-Switch muss VLANs unterstützen. Das ist bei modernen Manageable Switches Standard – aber bei älteren, einfachen Switches oft nicht der Fall. Der Hersteller kann das schnell sagen. Kosten: Ein VLAN-fähiger 24-Port Switch kostet zwischen 300-1000 Euro, je nach Qualität und Features.

2. Router/Firewall mit Firewall-Regeln

Zwischen den VLANs sitzt eine Firewall, die Regeln durchsetzt. Das ist oft nicht ein separates Gerät, sondern eine Funktion im Router. Moderne Router (Fritzbox, Ubiquiti, Mikrotik) können alle VLANs verwalten und Firewall-Regeln definieren. Eine dedizierte Appliance wie Palo Alto oder Fortigate ist für Arztpraxen meist Overkill.

3. Konfiguration und Administration

Der Switch muss konfiguriert werden: welche Ports gehören zu welchem VLAN? Die Firewall muss programmiert werden: welche Regeln erlaubt/blockiert? Das ist nicht schwierig, aber es braucht jemanden, der das versteht. Ihr IT-Dienstleister sollte das können.

7.8.5. Was das konkret kostet und wann es sich lohnt

Investition: - VLAN-fähiger Switch: 500-1000 Euro (ggf. schon vorhanden) - Router-Upgrade (falls notwendig): 300-800 Euro - Konfiguration und Installation durch IT-Dienstleister: 4-8 Stunden à 100-150 Euro/Std = 400-1200 Euro - **Gesamt: ca. 1200-3000 Euro**

Wann es sich lohnt: - Sie haben medizinische Großgeräte (Röntgen, CT, MRT, Labor-Automaten) - Die Geräte älter als 10 Jahre sind (und damit unsicherer) - Die Geräte an eurem Praxisnetzwerk angebunden sind - Sie hatten bereits Sicherheitsvorfälle oder machen sich Sorgen um die Sicherheit

Wann es optional ist: - Sie haben nur sehr neue Medizingeräte (unter 5 Jahren) mit modernen Sicherheitsstandards - Die Geräte sind völlig isoliert und nicht mit dem PVS verbunden - Ihre Praxis ist sehr klein (1-2 Mitarbeiter) mit minimaler Netzwerk-Komplexität

Für die meisten Praxen mit echten Medizingeräten ist Netzsegmentierung eine gute Investition. Sie kostet weniger als ein Ransomware-Schaden – und die KBV verlangt das auch implizit in ihrer IT-Sicherheitsrichtlinie.

7.8.6. Was Sie Ihrem IT-Dienstleister beauftragen sollten

Ein klares Arbeitspaket für die Netzsegmentierung könnte so aussehen:

1. **Audit:** Alle Geräte im Netz erfassen, dokumentieren, die Kommunikations-Anforderungen klären.
2. **Netzwerk-Design:** Ein Diagramm erstellen mit den oben beschriebenen VLANs und Firewall-Regeln.
3. **Hardware-Empfehlung:** Welcher Switch, welcher Router ist nötig?
4. **Implementierung:** Hardware installieren, VLANs konfigurieren, Firewall programmieren.
5. **Dokumentation:** Ein Netzwerk-Diagramm (zur Aufbewahrung in Ihrem Notfalldokument) und eine Übersicht der Firewall-Regeln.
6. **Testing:** Sicherstellen, dass Kommunikation funktioniert, wo sie soll – und blockiert, wo sie blockiert sein soll.

7.8.7. Checkliste: Netzsegmentierung

- ☐ Ich habe eine Übersicht aller Geräte und ihrer Kommunikations-Anforderungen erstellt.
- ☐ Mein IT-Dienstleister hat ein Netzwerk-Design-Konzept mit VLANs erstellt.
- ☐ Mein aktueller Switch ist VLAN-fähig (oder wird ausgetauscht).
- ☐ Meine Firewall kann Regeln zwischen VLANs durchsetzen.
- ☐ Medizingeräte haben ein separates VLAN.
- ☐ Gast-WLAN ist vom restlichen Netz isoliert.
- ☐ Ein Netzwerk-Diagramm existiert und ist aktuell.
- ☐ Firewall-Regeln sind dokumentiert und werden jährlich überprüft.
- ☐ Ich habe mit meinem IT-Dienstleister geklärt, wer die Regeln wartet und bei Problemen Anpassungen macht.

8. Teil 7: KBV IT-Sicherheitsrichtlinie

Die KBV IT-Sicherheitsrichtlinie ist nicht optional. Sie ist eine gesetzliche Anforderung mit Bußgeld-Konsequenzen. Aber sie ist auch praxisnah und machbar.

8.1. Was ist die KBV IT-Sicherheitsrichtlinie?

Die "Richtlinie zur Sicherheit und zum Datenschutz sowie zum Schutz des Verbrauchervermögens in Arztpraxen, Zahnarztpraxen und Psychotherapie-Praxen" – so der offizielle Name – ist eine Regelwerk der Kassenärztlichen Vereinigung (KBV), das IT-Sicherheit für niedergelassene Ärzte, Zahnärzte und Psychotherapeuten vorschreibt.

Rechtsgrundlage: § 390 SGB V (Sozialgesetzbuch). Diese Norm beauftragt die KBV, Richtlinien zu erlassen, die die Sicherheit und den Datenschutz in Vertragsarztpraxen regeln.

Gelber im April 2025 überarbeitet, ab Oktober 2025 vollständig verpflichtend: Die KBV hat die Richtlinie 2025 grundlegend überarbeitet. Die neue Fassung tritt Oktober 2025 in Kraft. Danach müssen alle Vertragsärzte und -zahnärzte die neuen Anforderungen erfüllen. Die Übergangsfrist von sechs Monaten erlaubt, bestehende Systeme anzupassen – aber nicht, die Anforderungen zu ignorieren.

8.2. Für wen gilt die Richtlinie?

Gilt für: - Alle niedergelassenen Vertragsärzte (Allgemeinmedizin, Fachärzte) - Alle Vertragszahnärzte - Alle Vertragstherapeuten (Psychotherapeuten, Verhaltenstherapeuten) - Alle Praxen, die mit den Krankenkassen abrechnen

Gilt nicht für: - Privatärzte (die nicht mit Krankenkassen abrechnen) – aber: Die KBV-Richtlinie ist ein guter Referenzrahmen auch für sie - Kliniken und Krankenhäuser (die haben andere Regelwerke)

Besonderheit: Zahnärzte und Psychotherapeuten unterliegen zusätzlich ihren eigenen Kammer-Regelungen, die aber inhaltlich ähnlich sind.

Wenn Sie als Arzt oder Zahnarzt eine Praxis betreiben und mit Krankenkassen abrechnen, gilt diese Richtlinie für Sie.

8.3. Staffelung nach Praxisgröße

Die KBV stellt Anforderungen nicht als "one size fits all". Die Richtlinie unterscheidet drei Kategorien nach Praxisgröße und Infrastruktur:

Kleine Praxen (bis 5 Personen): - Grundanforderungen zu Passwort-Verwaltung, Datensicherung, Zugriffskontrolle - Vereinfachte Anforderungen, aber nicht weniger wichtig - Typischerweise: Ein Arzt mit 1-4 Mitarbeitern, einfache Netzwerk-Infrastruktur

Mittlere Praxen (6-20 Personen): - Alle Anforderungen der kleinen Praxis plus zusätzliche Anforderungen - Netzwerk-Segmentierung (Trennung von Medizingeräten, TI, Praxis-IT) - Schriftliche IT-Sicherheitsrichtlinie (eigene Policy-Dokumente) - Formale Protokollierung von Zugriffen - Typischerweise: Ein Arzt mit 5-20 Mitarbeitern, eventuell mehrere Ärzte in einer Gemeinschaftspraxis

Große Praxen (über 20 Personen oder medizinische Großgeräte): - Alle Anforderungen der mittleren Praxis plus: - Dedizierter IT-Sicherheitsbeauftragter (intern oder extern) - Regelmäßige Penetrationstests (externe Sicherheitsprüfungen) - Formales ISMS (Information Security Management System) - Typischerweise: Mehrere Ärzte, Gemeinschaftspraxen, oder Praxen mit CT/MRT/Labor-Automation

8.4. Sanktionen bei Nichterfüllung

Die KBV Richtlinie ist nicht optional. Das wird durch Sanktionen unterstrichen:

Bußgelder: Bis zu 100.000 Euro bei Verstößen gegen die Richtlinie **Honorarkürzungen:** Die KBV kann Honorare kürzen oder aussetzen **Ausschluss:** Im schlimmsten Fall kann eine Praxis aus dem Netzwerk der Vertragsärzte ausgeschlossen werden

Diese Konsequenzen sind nicht theoretisch. Die KBV überprüft Compliance immer stärker. Digitalisierung in Gesundheitsberufen wird kontrolliert. Wenn ein Sicherheitsvorfall bekannt wird – Ransomware, Datenverlust, Datenpanne – überprüft die KBV, ob die Richtlinien-Anforderungen erfüllt waren. Waren sie nicht, folgen Konsequenzen.

Wichtig: Auch die Datenschutzbehörde prüft – unabhängig von der KBV. Ein Verstoß gegen die IT-Sicherheitsrichtlinie ist oft auch ein Verstoß gegen DSGVO-Anforderungen (Sicherheitsmaßnahmen nach Art. 32 DSGVO). Das kann zu zusätzlichen Bußgeldern der Datenschutzbehörde führen – bis zu 20 Millionen Euro oder 4% des Umsatzes.

8.5. Das Wichtigste: KBV stellt Unterstützung bereit

Die gute Nachricht: Die KBV bietet Unterstützung. Es sind nicht einfach abstrakte Anforderungen, sondern es gibt konkrete Hilfsmittel:

- **Checklisten** für kleine, mittlere und große Praxen
- **Musterdokumente** für Verpflichtungserklärungen, Policies, Verarbeitungsverzeichnisse
- **Schulungs-Materialien** für Mitarbeiter
- **Beratungs-Kontakte** zu IT-Sicherheitsexperten

Diese Materialien sind kostenlos und finden sich auf der KBV-Website. Sie sind ein solider Startpunkt.

8.6. Checkliste: Die KBV-Richtlinie verstehen

- ☐ Ich kenne die Anforderungen, die für meine Praxisgröße gelten.
- ☐ Ich habe die Muster-Dokumente der KBV heruntergeladen (Checklisten, Verpflichtungserklärungen, Policies).
- ☐ Mein IT-Dienstleister kennt die KBV-Anforderungen.
- ☐ Ich weiß, welche Sanktionen bei Nichterfüllung drohen.
- ☐ Ich habe einen Plan, bis Oktober 2025 die neuen Anforderungen umzusetzen.

8.7. KBV-Anforderungen für kleine Praxen

8.7.1. Das Mindest-Set für Praxen bis 5 Personen

Eine kleine Arztpraxis – ein Arzt oder eine Ärztin, vielleicht ein bis zwei Medizinische Fachangestellte – braucht nicht weniger Sicherheit als eine große Praxis. Sie braucht nur weniger komplexe Infrastruktur. Die KBV-Anforderungen für kleine Praxen sind daher reduziert, aber nicht minimal.

Alle folgenden Anforderungen stammen aus Anlage 1 der KBV IT-Sicherheitsrichtlinie. Sie sind nicht optional. Sie sind konkrete, überprüfbare Maßnahmen, die bis Oktober 2025 implementiert sein müssen.

8.7.2. 1. Einarbeitung neuer Mitarbeiter

Anforderung: Jeder neue Mitarbeiter muss zur Einhaltung von Datenschutz und Schweigepflicht verpflichtet werden – bevor er oder sie Zugang zu Patientendaten erhält.

Was konkret zu tun ist: - Eine schriftliche **Verpflichtungserklärung nach Art. 32 Abs. 4 DSGVO** aufbewahren. Sie muss enthalten: welche personenbezogenen Daten wird diese Person verarbeiten, was darf damit nicht getan werden, wie lange bleibt die Verpflichtung nach Kündigung bestehen? - Für medizinische Berufe zusätzlich: Eine **förmliche Verpflichtung nach § 203 Abs. 4 StGB** (Schweigepflicht). Diese muss vor dem ersten Zugang zu geschützten Daten unterschrieben sein. - Die Unterschriften aufbewahren – in der Personalakte oder einem separaten Datenschutz-Ordner.

Praktisch: Ein einseitiges Dokument (“Verpflichtung zur Vertraulichkeit und Einhaltung der Schweigepflicht”) unterschreiben lassen – fertig. Das kostet 10 Minuten. Die KBV bietet Muster.

8.7.3. 2. Austrittsverfahren

Anforderung: Wenn ein Mitarbeiter die Praxis verlässt, müssen seine Zugänge sofort gesperrt werden – nicht irgendwann, sondern am letzten Arbeitstag.

Was konkret zu tun ist: - Am letzten Tag oder sofort danach: - [ ] PVS-Zugang deaktivieren - [ ] E-Mail-Konto sperren oder weiterleiten - [ ] WLAN-Passwort ändern - [ ] Gegebenenenfalls eHBA oder andere Authentifizierungs-Token einsammeln - [ ] Firmeneigene Geräte (Laptop, Smartphone, Schlüssel) zurückfordern - Dokumentieren: Wann war der letzte Arbeitstag? Wann wurden Zugänge gesperrt?

Besonderheit für Ärzte: Der eHBA (elektronischer Heilberufsausweis) bleibt beim Arzt. Aber ein Praxis-Mitarbeiter, der geht, darf ihn nicht mitnehmen. Klären Sie, wer den eHBA verwaltet.

Praktisch: Eine Ein-Seiten-Checkliste “Offboarding” ausdrucken und beim Austritt abarbeiten.

8.7.4. 3. Fremdpersonal-Regelung

Anforderung: Wenn externe IT-Dienstleister, Reparateure oder andere externe Personen Zugang zur Praxis-IT erhalten, muss das geregelt sein.

Was konkret zu tun ist: - Einen **Auftragsverarbeitungsvertrag (AVV)** mit Ihrem IT-Dienstleister haben – schriftlich, unterzeichnet - Der AVV regelt: welche Daten darf der IT-Dienstleister verarbeiten, wie behandelt er diese, welche Sicherheitsmaßnahmen trifft er? - Für andere externe Personen (Geräte-Reparateure): Eine einfache Verpflichtung auf Vertraulichkeit ist ausreichend - Dokumentieren: Wer hatte wann Zugang? Welche IT-Dienstleister sind im Einsatz?

Praktisch: Mit Ihrem IT-Dienstleister klären, ob ein AVV bereits existiert. Falls nicht, einen aufsetzen oder von der KBV ein Muster-AVV verwenden.

8.7.5. 4. IT-Sicherheitsschulungen (Neu ab Oktober 2025)

Anforderung: Alle Mitarbeiter müssen mindestens einmal jährlich zu IT-Sicherheitsthemen geschult oder unterwiesen werden.

Was konkret zu tun ist: - Mindestens einmal jährlich ein Gespräch (30 Minuten) oder eine Schulung durchführen zu: - Phishing und verdächtige E-Mails - Passwort-Sicherheit - Umgang mit Patientendaten - Was tun bei Verdacht auf einen Sicherheitsvorfall? - Die Teilnahme dokumentieren (mit Unterschriften)

Praktisch: Im Januar ein kurzes Treffen mit allen Mitarbeitern. Der Arzt oder die Ärztin führt durch ein Gespräch über die wichtigsten Punkte. Teilnehmerliste unterschreiben. Fertig.

Alternativ: KBV stellt Online-Schulungs-Module zur Verfügung – zum Selbststudium.

8.7.6. 5. Datensicherung (Backup)

Anforderung: Alle Patientendaten müssen regelmäßig gesichert werden – und die Sicherung muss funktionieren (getestet sein).

Was konkret zu tun ist: - Ein **automatisiertes Backup-System** einrichten für: - Das PVS (Patientendatenbank) - Alle lokal gespeicherten Patientendaten (Briefe, Befunde, Scans) - Alle anderen geschäftskritischen Dateien - Das Backup muss mindestens täglich erfolgen – besser mehrmals täglich - Das Backup muss außerhalb der Praxis aufbewahrt werden (Cloud oder externe Festplatte an anderem Ort) - Einmal im Quartal testen: Kann ich Daten aus dem Backup zurückspielen? Funktioniert es? - Dokumentieren: Welches Backup-System? Welcher Rhythmus? Wann wurde zuletzt getestet?

Praktisch: Mit dem IT-Dienstleister klären: Ist ein Backup eingerichtet? Wenn ja, Restore-Test machen. Wenn nein, eines einrichten (kostet typischerweise 100-200 Euro Initial, dann 20-50 Euro/Monat).

8.7.7. 6. Virenschutz und Firewall

Anforderung: Alle Computer und Netzwerk-Geräte müssen durch Antivirus und Firewall geschützt sein.

Was konkret zu tun ist: - Auf jeden Praxis-Computer: **Antivirus-Software** installiert und aktiv. Das kann Windows Defender (kostenlos, bei Windows 10+ integriert) oder ein Drittanbieter sein. - Eine **Firewall** auf dem Router oder dem Netzwerk (bei modernen Routern integriert) - Alles sollte automatisch aktualisiert werden

Praktisch: Das ist meist schon vorhanden. Mit IT-Dienstleister klären: Ist Antivirus auf allen Computern aktiv? Ist die Firewall aktiviert?

8.7.8. 7. Zugriffsschutz – Passwörter und Gerätesperren

Anforderung: Nur Berechtigte dürfen auf Patientendaten zugreifen. Das wird durch Passwörter und Gerätesperren durchgesetzt.

Was konkret zu tun ist: - **Im PVS:** Jeder Mitarbeiter hat einen eigenen Benutzer mit Passwort. Keine geteilten Accounts. - **Starke Passwörter:** Mindestens 8 Zeichen, gemischte Klein-/Großbuchstaben, Zahlen, Sonderzeichen. Oder: Passwort-Manager verwenden (Bitwarden, 1Password). - **Windows-Anmeldung:** Jeder Praxis-Computer braucht eine Benutzer-Anmeldung mit Passwort – kein Auto-Logon - **Bildschirmsperre:** Nach 15 Minuten Inaktivität sperrt sich der Bildschirm automatisch – Passwort erforderlich zum Entsperren - **Keine Post-its:** Passwörter nicht aufschreiben und ins Netzwerk hängen

Praktisch: Im Windows einmalig einrichten, dann ist es Standard. Im PVS mit dem Hersteller klären.

8.7.9. 8. Mobile Geräte

Anforderung: Wenn Mitarbeiter auf mobilen Geräten (Laptops, Tablets, Smartphones) auf Praxis-Daten zugreifen, muss das sicher sein.

Was konkret zu tun ist: - Mobile Geräte müssen **verschlüsselt** sein (BitLocker auf Windows, FileVault auf Mac, Standard auf modernen Smartphones) - Wenn das Gerät verloren geht, muss es **ferngelöscht** werden können (Find My iPhone, Find My Device für Android) - Bildschirmsperre und Passwort müssen aktiv sein - WLAN nur über WPA2/WPA3, nicht über WEP oder offen

Praktisch: Moderne Geräte haben das meist schon integriert. Mit IT-Dienstleister klären: Sind die Verschlüsselung und Fern-Lösch-Funktionen aktiviert?

8.7.10. Praktische Umsetzungs-Schritte für kleine Praxen

1. **Inventur (1 Tag):** Was haben wir bereits? Welche Anforderungen sind erfüllt, welche nicht?
2. **Dokumentation (2 Tage):** Verpflichtungserklärungen für alle Mitarbeiter ausfüllen und unterschreiben lassen
3. **Backup-Test (1 Stunde):** Mit IT-Dienstleister klären und ggf. einrichten
4. **Schulung (2 Stunden):** Ein erstes Schulungs-Gespräch mit dem Team
5. **Jährliche Nachpflege (2 Stunden/Jahr):** Einmal im Jahr überprüfen und Schulung wiederholen

Kosten: Meist zwischen 0-1000 Euro (für externe Beratung oder Backup-Service). Die Anforderungen sind mit bestehenden Mitteln erfüllbar.

8.7.11. Checkliste: KBV-Anforderungen kleine Praxen

- ☐ Verpflichtungserklärungen nach Art. 32 Abs. 4 DSGVO liegen für alle Mitarbeiter vor und sind unterschrieben.
- ☐ Förmliche Verpflichtung nach § 203 Abs. 4 StGB liegt vor (Schweigepflicht).
- ☐ Eine Offboarding-Checkliste existiert und wird bei jedem Mitarbeiterabgang abgearbeitet.
- ☐ Ein Auftragsverarbeitungsvertrag (AVV) mit dem IT-Dienstleister liegt vor.
- ☐ Externe Personen werden bei längeren Zugriffen verpflichtet.
- ☐ Eine Schulung zu IT-Sicherheit hat mindestens einmal stattgefunden (dokumentiert).
- ☐ Ein Backup-System ist eingerichtet und wird mindestens täglich durchgeführt.
- ☐ Das Backup wurde in den letzten 3 Monaten getestet.
- ☐ Antivirus und Firewall sind auf allen Geräten aktiv.
- ☐ Jeder Mitarbeiter hat einen eigenen PVS-Benutzer mit starkem Passwort.
- ☐ Bildschirmsperre ist nach 15 Minuten Inaktivität eingestellt.
- ☐ Mobile Geräte sind verschlüsselt und können ferngelöscht werden.
- ☐ WLAN nutzt WPA2 oder WPA3-Verschlüsselung mit starkem Passwort.

8.8. KBV-Anforderungen für mittlere Praxen

8.8.1. Was sich für mittlere Praxen ändert

Eine mittlere Praxis mit 6-20 Mitarbeitern hat eine komplexere Infrastruktur. Sie hat vielleicht mehrere Ärzte, spezialisierte Funktionen (Abrechnung, Verwaltung, Empfang), möglicherweise vernetzte Medizingeräte. Dies erfordert zusätzliche Kontrollen.

Alle Anforderungen der kleinen Praxis gelten weiterhin – plus folgende zusätzliche Anforderungen:

8.8.2. 1. Netzwerk-Segmentierung

Anforderung: Das Praxis-Netzwerk muss in logische Bereiche aufgeteilt sein – Medizingeräte-Netz, Praxis-IT-Netz, möglicherweise Gast-WLAN.

Was konkret zu tun ist: - Das Netzwerk physisch oder logisch aufteilen in: - Medizingeräte-Netz (Röntgen, Labor, etc.) - PVS-Netz (Patientenverwaltung und -daten) - Gast-WLAN (getrennt vom Praxis-Netz) - TI-Konnektor-Netz (optional aber sauberer) - Eine Firewall regelt die Kommunikation zwischen den Netzen - Dokumentation: Netzwerk-Diagramm mit VLAN-Aufteilung

Praktisch: Das ist ein Projekt für einen IT-Dienstleister. Der Aufwand liegt bei 1-2 Tagen, die Kosten bei 1500-3000 Euro. Siehe auch Kapitel “Netzsegmentierung” in Teil 6.

8.8.3. 2. Formale IT-Sicherheitsrichtlinie (schriftlich)

Anforderung: Die Praxis muss eine schriftliche, eigene IT-Sicherheitsrichtlinie haben – nicht nur die KBV-Richtlinie, sondern eine praxis-spezifische Policy.

Was konkret zu tun ist: - Ein Dokument “IT-Sicherheitsrichtlinie der Praxis” erstellen, das enthält: - Grundsätze des Umgangs mit Patientendaten - Passwort-Policy (wie lang, wie oft wechseln, etc.) - Umgang mit mobilen Geräten (BYOD) - Verschlüsselung von Daten - Incident Response (was tun bei einem Sicherheitsvorfall?) - Verantwortlichkeiten (wer ist IT-Verantwortlicher?) - Das Dokument muss unterschrieben sein (vom Praxisinhaber oder Geschäftsführer) - Alle Mitarbeiter müssen es lesen und bestätigen

Praktisch: Die KBV stellt Muster zur Verfügung. Eine Praxis-spezifische Policy ist keine Raketenwissenschaft – es ist eine 3-5 seitige Zusammenfassung der Regeln. 1 Tag Arbeit mit externer Unterstützung.

8.8.4. 3. Erweiterte Zugriffskontrollen

Anforderung: Nicht alle Mitarbeiter dürfen alles sehen. Zugriffe müssen rollenbasiert sein und dokumentiert.

Was konkret zu tun ist: - **Im PVS:** Rollen definieren und Zugriffsrechte danach zuweisen - Ärzte: voller Zugriff auf Patientenakten - MFA: Zugriff auf Terminverwaltung, begrenzte Patienten-Einsicht - Abrechnungsbeauftragte: Zugriff nur auf Abrechnung, kein

klinischer Zugriff - **Audit-Logs:** Das PVS muss dokumentieren, wer wann auf welche Patientenakte zugegriffen hat - **Überprüfung:** Mindestens jährlich überprüfen: Hat jeder noch die Rechte, die er braucht?

Praktisch: Die meisten PVS-Systeme können das. Mit dem PVS-Hersteller klären: Wie richten wir Rollen ein? Wie exportieren wir Audit-Logs?

8.8.5. 4. Protokollierung von Zugriffen

Anforderung: Es muss protokolliert werden, wer auf Patientendaten zugegriffen hat und wann.

Was konkret zu tun ist: - Das PVS muss Zugriffsgrupen speichern (Audit-Log) - Mindestens folgende Informationen: Wer (Benutzer), Was (welche Patientenakte), Wann (Datum/Uhrzeit) - Diese Logs müssen mindestens für 30 Tage aufbewahrt werden - Ungewöhnliche Zugriffe sollten überprüft werden (z.B. warum hat die MFA Zugriff auf eine Patientenakte, die nicht in ihrem Terminplan war?)

Praktisch: Das ist meist eine integrierte Funktion des PVS. Mit dem Hersteller klären, wo die Logs sind und wie oft sie überprüft werden.

8.8.6. Was sich konkret ändert gegenüber kleine Praxen

Klein: Eine Praxis, ein Arzt, alles auf einem Netz **Mittel:** Mehrere Ärzte/Mitarbeiter, spezialisierte Funktionen, Medizingeräte – braucht Struktur

Die praktischen Unterschiede:

Anforderung	Kleine Praxis	Mittlere Praxis
Netzwerk-Struktur	Einfach, alles auf einem Netz	Segmentiert (VLANs)
Benutzer-Rollen	Einfach (Arzt, MFA, Verwaltung)	Detailliert (verschiedene Rollen für verschiedene Funktionen)
Zugriffsprotokollierung	Minimal	Regelmaßig überprüft
Dokumentation	Basis-Anforderungen	Formale Richtlinien
IT-Governance	Ad-hoc	Strukturiert mit Verantwortlichkeiten

8.8.7. Praktische Umsetzungs-Schritte

1. **Audit (2 Tage):** Mit IT-Dienstleister: Wo stehen wir? Was fehlt?
2. **Netzwerk-Design (1 Tag):** Segmentierung planen
3. **Policies schreiben (1-2 Tage):** Mit externem Berater oder Muster-Dokumente anpassen
4. **Netzwerk-Umbau (2-5 Tage):** Hardware, VLANs, Firewall-Regeln

5. **Konfiguration PVS (2 Tage):** Rollen, Zugriffsrechte, Audit-Logs
6. **Schulung (4 Stunden):** Alle Mitarbeiter einweisen
7. **Jährliche Überprüfung (1 Tag/Jahr):** Audit-Logs überprüfen, Rollen validieren

Kosten: 3000-8000 Euro (abhängig von externem Dienstleister und Hardware-Bedarf)

8.8.8. Checkliste: KBV-Anforderungen mittlere Praxen

- ☐ Alle Anforderungen der kleinen Praxis sind erfüllt.
- ☐ Das Netzwerk ist segmentiert (Medizin, PVS, Gast-WLAN, ggf. TI).
- ☐ Ein Netzwerk-Diagramm mit VLAN-Aufteilung liegt vor.
- ☐ Eine formale IT-Sicherheitsrichtlinie (schriftlich, unterschrieben) liegt vor.
- ☐ Alle Mitarbeiter haben die Richtlinie gelesen und bestätigt.
- ☐ Benutzer-Rollen sind im PVS konfiguriert und dokumentiert.
- ☐ Nicht alle Mitarbeiter haben Zugriff auf alle Patientenakten.
- ☐ Das PVS speichert Audit-Logs (Wer, Was, Wann).
- ☐ Audit-Logs werden mindestens monatlich überprüft.
- ☐ Es gibt einen IT-Sicherheitsverantwortlichen (oder dedizierter Kontakt zum IT-Dienstleister).

8.9. KBV-Anforderungen für große Praxen

8.9.1. Das Thema: Enterprise-Security im Arztpraxis-Kontext

Große Praxen – über 20 Mitarbeiter, oder Praxen mit medizinischen Großgeräten – haben ein Sicherheits-Anforderungsprofil, das über die bisherigen Kapitel hinausgeht. Es geht nicht mehr nur um Grundschutz, sondern um kontinuierliche Überwachung, systematische Sicherheitsverbesserung und formalisiertes Management.

Die KBV nennt das “erweiterte Anforderungen für große Praxen”. In praktischen Worten bedeutet das: Sicherheit als kontinuierliche Aufgabe, nicht als einmalige Konfiguration.

8.9.2. 1. Dedizierter IT-Sicherheitsbeauftragter

Anforderung: Es gibt eine Person, die IT-Sicherheit verantwortlich trägt.

Was konkret zu tun ist: - **Option A – Intern:** Ein Mitarbeiter wird als IT-Sicherheitsbeauftragter benannt. Das kann sein: - Ein Arzt mit IT-Verständnis - Ein technischer Mitarbeiter mit Sicherheits-Schwerpunkt - Die person hat die Verantwortung für die Sicherheits-Agenda und rapportiert an die Praxisleitung - **Option B – Extern:** Ein externer IT-Sicherheits-Berater oder -Consultant wird beauftragt. Er oder sie kommt regelmäßig (z.B. monatlich oder quartalsweise) in die Praxis, überprüft die Sicherheitslage, macht Empfehlungen. - **Dokumentation:** Eine Stellenbeschreibung oder ein Vertrag mit klaren Verantwortlichkeiten

Was der Sicherheitsbeauftragte tut: - Überprüft regelmäßig die IT-Sicherheit (monatlich oder quartalsweise) - Führt Audit-Logs-Analysen durch - Plant Sicherheits-Schulungen - Identifiziert und eskaliertrisiken - Berichtet an die Praxisleitung

Praktisch: Für viele große Praxen ist die externe Option günstiger und bessser. Ein externer Consultant kostet ca. 100-200 Euro/Stunde. Ein Quartal mit einer Stunde pro Monat = 400-800 Euro/Quartal = 1600-3200 Euro/Jahr. Das ist für eine große Praxis verkraftbar.

8.9.3. 2. Penetrationstests

Anforderung: Mindestens einmal jährlich sollte die IT-Sicherheit durch ein externes "Penetrations-Test" überprüft werden – ein autoritativer Sicherheits-Check, bei dem Experten versuchen, Schwachstellen zu finden.

Was konkret zu tun ist: - Einen Penetrations-Test-Dienstleister beauftragen (z.B. spezialisierte IT-Sicherheits-Agenturen) - Der Tester versucht, von außen und von innen Schwachstellen zu finden: - Phishing-E-Mails an Mitarbeiter - Schwache Passwörter - Ungepatche Systeme - Netzwerk-Zugang von außen - Physischer Zugang (kann ich einfach einen USB-Stick einstecken?) - Ein Bericht wird erstellt mit Findings und Recommendations - Die Praxis behebt die Schwachstellen

Kosten: Typischerweise 2000-5000 Euro pro Jahr (abhängig von Praxisgröße und Scope)

Wichtig: Das ist nicht nur eine Kontrolle – es ist auch eine gute Übung. Mitarbeiter lernen, wenn Phishing-Tests durchgeführt werden. Das Sicherheits-Bewusstsein steigt.

8.9.4. 3. Formales ISMS (Information Security Management System)

Anforderung: Eine dokumentierte, kontinuierliche Sicherheits-Management-Struktur.

Was konkret zu tun ist: - Ein "ISMS" ist für kleine Organisationen nicht das volle ISO 27001, sondern eine vereinfachte Version - Es enthält: - **Sicherheits-Policy** (bereits vorhanden in mittleren Praxen) - **Asset-Inventar:** Was haben wir? (Hardware, Software, Daten) - **Risikoanalyse:** Was sind unsere größten Risiken? - **Kontroll-Katalog:** Welche Sicherheits-Maßnahmen haben wir? - **Incident Response Plan:** Was tun wir im Notfall? - **Schulungs-Plan:** Wer wird trainiert, wann? - **Review-Prozess:** Mindestens jährlich überprüfen und anpassen

Praktisch: Das klingt aufwendig – aber es ist strukturiertes Nachdenken. Mit externer Unterstützung kann man das in 5-10 Tagen aufsetzen. Danach ist es hauptsächlich eine Wartungsaufgabe.

Kosten: 2000-5000 Euro für die initiale Erstellung mit externe Unterstützung. Danach 500-1000 Euro/Jahr für die jährliche Überprüfung.

8.9.5. Besonderheit: Medizinische Großgeräte

Wenn eine Praxis CT, MRT, Labor-Automation oder ähnliche Großgeräte betreibt, wird sie in die "Große Praxis"-Kategorie eingeteilt – unabhängig von der Mitarbeiterzahl.

Diese Geräte erfordern zusätzliche Sicherheits-Aufmerksamkeit: - Regelmäßige Firmware-Updates (oder Begründung, warum nicht) - Hersteller-Sicherheitsmitteilungen überwachen - Zusätzliche Netzwerk-Segmentierung - Regelmäßige Penetrationstests im Medizingeräte-Netzwerk

Das ist ein Grund, warum die KBV große Praxen stärker reguliert – die Geräte sind komplexer und riskanter.

8.9.6. Praktische Umsetzungs-Schritte für große Praxen

1. **IT-Sicherheitsbeauftragter benennen (1 Tag):** Intern oder extern beauftragen
2. **ISMS-Erstellung (5-10 Tage mit Unterstützung):** Asset-Inventar, Risikoanalyse, Kontroll-Katalog
3. **Erster Penetrationtest (2 Tage):** Durchführung und Reporting
4. **Behebung von Findings (2-10 Wochen):** Abhängig von Befunden
5. **Laufender Betrieb:**
    - Monatlich: Sicherheitsbeauftragter überprüft Audit-Logs
    - Quartalsweise: Sicherheitsbesprechung mit Praxisleitung
    - Jährlich: Penetrationtest, ISMS-Überprüfung, Schulungen

Kosten (jährlich): - IT-Sicherheitsbeauftragter (extern): 2000-3500 Euro/Jahr - Penetrationtest: 2000-5000 Euro/Jahr - ISMS-Wartung: 500-1000 Euro/Jahr - **Summe: ca. 4500-9500 Euro/Jahr**

Das ist für eine große Praxis ein akzeptabler Kostenpunkt – und deutlich günstiger als ein Sicherheitsvorfall.

8.9.7. Checkliste: KBV-Anforderungen große Praxen

☐ Alle Anforderungen der mittleren Praxis sind erfüllt.
☐ Ein IT-Sicherheitsbeauftragter (intern oder extern) ist benannt.
☐ Der Sicherheitsbeauftragte hat eine klare Stellenbeschreibung/Vertrag.
☐ Regelmäßige Überprüfungen (monatlich oder quartalsweise) sind geplant.
☐ Ein formales ISMS-Dokument liegt vor mit:
  – Asset-Inventar
  – Risikoanalyse
  – Kontroll-Katalog
  – Incident Response Plan
  – Schulungs-Plan

- ☐ Mindestens einmal jährlich wird ein Penetrationtest durchgeführt.
- ☐ Findings aus Penetrationstests werden behoben.
- ☐ Praxisleitung und Sicherheitsbeauftragter treffen sich regelmäßig.
- ☐ Bei Großgeräten: Zusätzliche Netzwerk-Segmentierung existiert.
- ☐ Sicherheits-Schulungen finden mindestens jährlich statt.

9. Teil 8: KI in der Arztpraxis

KI ist ein mächtiges Werkzeug. Aber KI und Patientendaten sind eine gefährliche Kombination – wenn man nicht weiß, was man tut.

9.1. Das Szenario: Arztbrief im ChatGPT

Stellen Sie sich einen typischen Arztpraxis-Alltag vor. Ein Arzt dictiert schnell einen Arztbrief in sein Smartphone:

> "Patient Müller, 67 Jahre, Diabetes Typ 2, Hypertonus. Heute Besuch wegen persistierender Kopfschmerzen seit zwei Wochen. In Computertomografie Hinweis auf kleine zerebrale Ischämie temporal-links. Diagnose: Leichte zerebrale Durchblutungsstörung. Plan: Blutdruckeinstellung intensivieren, ASS 100 mg täglich starten…"

Dann, statt mit Papier zu arbeiten, gibt der Arzt den Text in ChatGPT ein: "Bitte formuliere das als formalen Arztbrief mit ICD-Codes und gib mir ein Schreiben für die Überweitung zum Neurologen."

ChatGPT liefert in zehn Sekunden einen perfekt strukturierten Arztbrief. Alle wichtigen Informationen sind drin, die Ton ist professionell, die Formatierung ist korrekt. Der Arzt kopiert den Text ins PVS, und der Brief ist fertig.

Das ist effizient. Das ist auch illegal.

Was ist passiert? Ein öffentliches KI-System (ChatGPT) hat erhalten: - Den Namen eines Patienten - Sein Alter - Sensitive Diagnosen - Bildgebungs-Befunde - Behandlungspläne

Alles – absolut alles – sind personenbezogene Gesundheitsdaten. Sie sind jetzt in den Training-Daten von OpenAI landetet, möglicherweise für immer. Der Patient hat nicht zugestimmt. Die DSGVO wurde verletzt. Die ärztliche Schweigepflicht nach § 203 StGB wurde verletzt.

Das ist nicht nur eine rechtliche Grenzüberschreitung. Es ist auch ein Sicherheitsrisiko: Der Arzt hat keine Kontrolle darüber, was OpenAI mit den Daten tut. OpenAI kann die Daten speichern, für Training nutzen, an Dritte weitergeben – ganz nach ihren Datenschutzbestimmungen.

Das ist das zentrale Problem dieses Kapitels: KI-Tools sind hilfreich, aber sie sind nicht automatisch sicher für Patientendaten.

9.2. Was KI in der Arztpraxis leisten kann

KI kann echten Nutzen bringen – wenn sie richtig eingesetzt wird.

Arztbriefe strukturieren und formulieren (mit anonymisierten Daten): "Hier ist ein Beispiel-Fall: 67-jähriger Patient mit Diabetes und Hypertonie, neu diagnostizierte zerebrale Ischämie. Formuliere einen Arztbrief." Das funktioniert, weil keine echten Patientendaten drin sind.

Befund-Strukturierung: Sonographie-Befunde, EKG-Interpretationen – können durch KI strukturiert und zusammengefasst werden, um Zeit zu sparen.

ICD- und OPS-Codierung: KI kann Ärzte bei der Codierung unterstützen – "Dieser Patient hat Diagnose X, Y und Z. Schlag mir passende ICD-Codes vor." Die Ärzte prüfen und wählen dann.

Administrative Aufgaben: Terminplanung, Recall-Management (Patien

ten an Vorsorgetermine erinnern), Rechnungsvorbereitung – solche Aufgaben enthalten oft keine sensitiven Daten und sind daher für KI geeignet.

KI-gestützte Diagnoseunterstützung: Das ist ein separates Thema. Spezial-Software (z.B. Radiologie-KI, Pathologie-KI) ist speziell für medizinische Zwecke entwickelt, DSGVO-konform und in den medizinischen Betrieb integriert. Das ist etwas anderes als ChatGPT – und es ist in vielen Praxen bereits im Einsatz.

9.3. Was KI nicht kann und nicht darf

KI kann nicht entscheiden. KI kann Vorschläge machen, aber Ärzte treffen Entscheidungen. Eine KI-Diagnose-Empfehlung muss immer von einem Arzt überprüft und bestätigt werden.

KI darf nicht mit echten Patientendaten gefüttert werden, wenn das System nicht DSGVO-konform ist. Das ist nicht verhandelbar.

KI darf nicht die Schweigepflicht gefährden. Wenn Sie Patient-Namen, Diagnosen, oder andere identifizierende Informationen in ein öffentliches KI-Tool eingeben, verletzen Sie § 203 StGB.

9.4. Die Kernfrage: Ist mein KI-Tool erlaubt?

Die Antwort hängt von zwei Dingen ab:

1. **Sind echte Patientendaten im Input?** (Ja = Problem)
2. **Hat der Anbieter einen DSGVO-konformen Vertrag mit der Praxis?** (Nein = Problem)

Wenn beides mit "Nein" beantwort wird – also: keine Patientendaten, und es gibt einen Vertrag – kann das KI-Tool in Betracht kommen.

Die praktische Formel ist einfach: **Keine echten Patientendaten in öffentliche KI-Tools.** Punkt. Das ist das Minimum.

9.5. Checkliste: KI in der Arztpraxis

- ☐ Ich verstehe, dass öffentliche KI-Tools (ChatGPT, Gemini, Copilot) keine DSGVO-Auftragsverarbeiter sind.
- ☐ Ich gebe keine echten Patientendaten in öffentliche KI-Tools ein.
- ☐ Wenn meine Praxis KI-Tools einsetzt, gibt es einen Auftragsverarbeitungsvertrag.
- ☐ Meine Mitarbeiter sind geschult, welche Daten sie in KI-Tools geben dürfen und welche nicht.
- ☐ Spezialisierte medizinische KI-Systeme (Diagnoseunterstützung) sind in den PVS integriert und DSGVO-konform.

9.6. Was KI in der Arztpraxis leisten kann

9.6.1. Realistisch bewerten: Der Unterschied zwischen Hype und Nutzen

KI-Enthusiasten versprechen, dass KI Ärzte in fünf Jahren überflüssig macht. KI-Skeptiker sagen, dass KI in der Medizin nie funktionieren wird. Die Wahrheit liegt in der Mitte: KI kann spezifische, begrenzte Aufgaben in der Arztpraxis sehr gut unterstützen – aber sie ersetzt keine ärztliche Entscheidung und keine menschliche Diagnose.

Was KI in der Arztpraxis konkret leisten kann:

9.6.2. 1. Arztbriefe und Befunde formulieren

Eine KI kann helfen, Zeit beim Schreiben von Arztbriefen und Befunden zu sparen – aber nur mit anonymisierten Daten.

Beispiel – Falsches Vorgehen: Arzt diktiert in ChatGPT: “Patient Schmidt, 45 Jahre, Bluthochdruck, heute Besuch wegen Kopfschmerzen. Bitte schreib einen Arztbrief.”

Beispiel – Richtiges Vorgehen: Arzt diktiert in ChatGPT: “Ein 45-jähriger Patient mit bekanntem Bluthochdruck stellt sich mit Kopfschmerzen vor. Es wird ein ausführlicher körperlicher Befund erhoben, Blutdruck ist erhöht. Verdacht auf hypertensive Entgleisung. Bitte schreib einen formalen medizinischen Befundbericht mit dem typischen Aufbau.”

ChatGPT generiert einen strukturierten Text, den der Arzt mit seinen echten Patientendaten ergänzt. Die KI hat keinen Patientenbezug erhalten – nur eine Aufgabenbeschreibung.

Das spart echte Zeit. Ein Arzt, der normalerweise 15 Minuten an einem Brief schreibt, hat jetzt einen Rohtext in 2 Minuten.

9.6.3. 2. Befund-Strukturierung und Interpretation

Beispiel: Ein Arzt hat einen Sonographie-Befund geschrieben: “Leber nicht vergrößert, Konturen glatt, echogenität normal. Niere B 10,5 cm, normal. Keine Steine. Vena cava inferior kollabierbar. Keine Peritoneale Flüssigkeit.”

Der KI sagt man: “Fasse diese Sonographie-Befunde zusammen und ordne sie systematisch nach Organen mit einer kurzen klinischen Einschätzung.”

KI antwortet: “Sonografische Befunde: Leber: regelrechte Größe und Echogenität, keine fokalen Läsionen. Nieren: bds. altersentsprechend, bis 10,5 cm, keine Nephrolitiasis. Gefäße: Vena cava inferior komprimierbar. Peritoneal: keine freie Flüssigkeit. Gesamteindruck: Unauffällige abdominale Sonographie.”

Das ist sofort passend für den Report.

9.6.4. 3. Diagnose-Codierung (ICD/OPS) unterstützen

Ein Arzt dokumentiert: “Patient mit neu diagnostiziertem Diabetes Typ 2, BMI 32, metabolisches Syndrom, Hyperlipoproteinämie. Heute Ernährungsberatung durchgeführt.”

Der Arzt fragt ChatGPT: “Gib mir mögliche ICD-10-Codes für diese Diagnosen.”

ChatGPT antwortet: “Wahrscheinliche ICD-10-Codes: E11 (Typ-2-Diabetes), E66.9 (Adipositas, Grad nicht näher bezeichnet), E88.81 (metabolisches Syndrom), E78.2 (gemischte Hyperlipidämie). Prozedur OPS: 9-4XX (Beratung und Edukation).”

Der Arzt überprüft diese Codes, validiert sie gegen die echte Dokumentation und wählt aus. Die KI hat keine Patientendaten erhalten – nur Diagnose-Begriffe.

Das spart dem Arzt die Recherche im ICD-Katalog.

9.6.5. 4. Administrative Aufgaben

Beispiel – Terminplanung: Eine Arztpraxis möchte Patienten mit chronischen Erkrankungen erinnern, ihre jährlichen Vorsorgeuntersuchungen zu machen. Eine KI kann (ohne Patientendaten zu speichern) automatisiert Reminder-E-Mails generieren:

KI-Input: “Generiere eine Erinnerungs-E-Mail für einen Patienten, dem die letzte Blutdruck-Kontrolle 12 Monate zurückliegt.”

KI-Output: “Liebe Patientin, lieber Patient, Sie haben sich zur regelmäßigen Kontrolle Ihres Blutdrucks angemeldet. Die letzte Kontrolle liegt nun über einem Jahr zurück. Bitte vereinbaren Sie einen Termin für eine neue Messung. [Kontakt-Info]”

Die E-Mail wird dann mit echten Patientendaten personalisiert. Die KI hatte keinen Zugriff auf echte Daten.

Beispiel – Rechnungsvorbereitung: Eine KI kann Abrechnungsassistenten helfen, Rechnungen vorzubereiten: “Dieser Patient hatte einen Hausbesuch von 30 Minuten mit EKG. Welche Gebührenposition passt?” Die KI schlägt vor, der Mitarbeiter prüft und gibt ein.

9.6.6. 5. Spezialisierte medizinische KI-Systeme (Diagnoseunterstützung)

Das ist eine andere Kategorie als ChatGPT. Es gibt spezialisierte KI-Systeme, die in der Radiologie, Pathologie und anderen medizinischen Bereichen eingesetzt werden.

Beispiele: - Radiologie-KI erkennt in Röntgenbildern verdächtige Strukturen - Pathologie-KI unterstützt bei der Diagnose von Gewebeproben - EKG-KI erkennt Rhythmusstörungen

Diese Systeme sind speziell für medizinische Zwecke entwickelt, haben DSGVO-Verträge mit den Praxen und sind in den medizinischen Betrieb integriert. Ein Arzt nutzt solche Systeme täglich und weiß, dass die Diagnose-Empfehlung immer validiert werden muss.

Diese Systeme sind sicher – weil sie speziell dafür gemacht wurden.

9.6.7. 6. Was KI nicht leisten kann

KI kann nicht allein entscheiden. Der Arzt entscheidet. KI unterstützt.

KI kann nicht mit echten Patientendaten spielen. Das ist nicht optional.

KI kann nicht Ärzte ersetzen. Sie kann spezifische Aufgaben unterstützen, aber nicht den ärztlichen Urteilsvermögen.

KI kann nicht in allen Kontexten eingesetzt werden. Kritische Diagnosen erfordern volle ärztliche Aufmerksamkeit, nicht KI-Unterstützung.

9.6.8. Die praktische Realität: KI als Produktivitäts-Werkzeug, nicht als Ratgeber

Für Arztpraxen ist KI realistische sinnvoll als Produktivitäts-Werkzeug: etwas, das Ärzte bei zeitaufwendigen, repetitiven Aufgaben hilft – Schreiben, Strukturieren, Zusammenfassen, Codierung – während der Arzt die medizinische Entscheidung bleibt.

Das ist nicht revolutionär. Es ist Evolution: ein Werkzeug, das den Arzt schneller macht, ohne die ärztliche Verantwortung zu ändern.

9.6.9. Checkliste: KI-Chancen in der Arztpraxis

- ☐ Ich habe ein klares Verständnis, was KI leisten kann und was nicht.
- ☐ Wenn meine Praxis KI einsetzt, ist es für Aufgaben ohne Patientendaten.
- ☐ Spezialisierte medizinische KI-Systeme sind bekannt und haben DSGVO-Verträge.
- ☐ KI-Output wird immer von einem Arzt überprüft und validiert.
- ☐ Mitarbeiter sind geschult, KI produktiv aber sicher zu nutzen.
- ☐ Es gibt eine klare Policy, welche Aufgaben mit KI unterstützt werden dürfen.

9.7. Datenschutz und Schweigepflicht beim KI-Einsatz

9.7.1. Das zentrale Problem: Öffentliche KI-Dienste sind keine Auftragsverarbeiter

Das ist der entscheidende Punkt. Lesen Sie das noch einmal:

Öffentliche KI-Dienste wie ChatGPT, Google Gemini, Microsoft Copilot sind NICHT DSGVO-konforme Auftragsverarbeiter für Gesundheitsdaten.

Das bedeutet: Sie dürfen echte Patientendaten nicht in diese Tools eingeben. Punkt.

Warum? Weil diese Dienste – per Datenschutzbestimmung – Ihre Eingaben speichern, zum Training nutzen und möglicherweise an Dritte weitergeben können. Der Betreiber (OpenAI, Google, Microsoft) wird dadurch selbst ein Datenverarbeiter ohne rechtliche Grundlage. Die DSGVO wird verletzt.

Konkret: Wenn Sie einen Patientennamen, eine Diagnose oder eine identifizierende Information eingeben, können Sie nicht kontrollieren, was damit passiert. OpenAI könnte die Daten speichern, an andere Kunden weitergeben, oder in Training-Daten integrieren.

Das ist nicht paranoia – das ist Tatsache.

Zusätzlich: Für Ärzte existiert § 203 StGB – die Schweigepflicht. Diese Pflicht schützt nicht nur den Namen eines Patienten, sondern alle Informationen, die ihn oder sie erkennbar machen könnten. Wenn Sie diese Informationen einem öffentlichen KI-Service geben, verletzen Sie diese Pflicht.

Konzentrat: Keine Patientendaten in ChatGPT. Nicht „nur ein bisschen anonymisiert", nicht „nur kurz", nicht „in der kostenlosen Version ist es sicher". Nein – nie.

9.7.2. Was Anonymisierung bedeutet (und warum Pseudonymisierung nicht ausreicht)

Es gibt zwei ähnlich klingende Konzepte, die in der Datenschutz-Diskussion verwechselt werden: Anonymisierung und Pseudonymisierung.

Pseudonymisierung bedeutet: Sie ersetzen den Namen durch ein Pseudonym. "Patient Schmidt" wird zu "Patient A". Die Daten sind nicht mehr direkt identifizierbar – aber der Bezug zum echten Patienten bleibt erhalten (über eine Schlüsseltabelle).

Anonymisierung bedeutet: Die Daten sind für die KI wirklich anonym. Es gibt keine Möglichkeit, sie einem Patienten zuzuordnen – auch nicht über einen Schlüssel.

Die DSGVO erlaubt Pseudonymisierung unter bestimmten Bedingungen. Aber **Pseudonymisierung schützt nicht vor Datenschutzverletzungen in die öffentliche KI.** Warum? Weil die DSGVO immer noch anwendbar ist, wenn ein Bezug zum Patienten bestehen könnte.

Beispiel: Sie sagen der KI "Patient A, 45 Jahre, Witwer, arbeitet als Lehrer in München, Diabetes Typ 2, letzte HbA1c 6,8…". Ein geschickter Angreifer könnte jemanden mit dieser Kombination von Details identifizieren. Die Pseudonymisierung ist leicht zu durchbrechen. Das ist nicht anonym – das ist unzureichend anonymisiert.

Echte Anonymisierung für KI-Input würde bedeuten: "Ein Patient mittleren Alters mit Diabetes und HbA1c-Wert im Bereich 6,5-7,5". Keine Altersangaben, die zu spezifisch sind, keine beruflichen Details, keine Ortsangaben. Nur generische, stark abstrahierte Informationen.

Mit dieser Stufe von Anonymisierung können Sie ein KI-Tool bedenkenlos nutzen – aber es ist dann auch kaum spezifisch genug, um praktisch nützlich zu sein.

9.7.3. DSGVO-konforme Alternativen

Wenn Sie KI in Ihrer Praxis nutzen möchten – egal ob für Arztbriefe, Codierung oder andere Aufgaben – gibt es sichere Wege:

9.7.3.1. 1. Lokale KI-Modelle (Ollama, LocalLLM)

Das ist die datenschutz-sicherste Option. Sie betreiben ein KI-Modell auf Ihrem eigenen Server oder Computer. Die Daten verlassen nie die Praxis.

Wie es funktioniert: - Sie installieren eine Open-Source KI-Software (z.B. Ollama) auf Ihrem Praxis-Server - Sie laden ein KI-Modell herunter (z.B. Llama 2, ein quelloffen Modell) - Sie nutzen die KI lokal – alles bleibt in Ihrer Praxis

Vorteile: - Vollständige Datenkontrolle - Keine Daten-Uploads - DSGVO-konform per Design - Kostengünstig (einmalige Software-Lizenz, dann Betriebskosten)

Nachteile: - Die Qualität ist derzeit unter ChatGPT (aber verbessert sich schnell) - Braucht technisches Know-how zur Einrichtung - Braucht lokale Rechenleistung

Für Arztpraxen: Das ist für viele Aufgaben (Strukturierung, einfache Textentwürfe) gut genug. Für spezialisierte medizinische Aufgaben vielleicht nicht.

9.7.3.2. 2. DSGVO-konforme Enterprise-Dienste mit AVV

Einige KI-Anbieter bieten Enterprise-Versionen an, die DSGVO-konform sind. Sie schließen einen Auftragsverarbeitungsvertrag (AVV) ab, und der Anbieter garantiert: - Daten werden nicht zum Training genutzt - Daten werden in der EU gespeichert (oder wo Sie es wollen) - Daten werden sicher gelöscht nach Vereinbarung - Regelmäßige Sicherheits-Audits

Beispiele: - OpenAI bietet ChatGPT Business/Enterprise mit AVV-Option - Microsoft bietet Copilot Pro für Unternehmen mit AVV - Spezialisierte Med-Tech Anbieter haben native DSGVO-Integration

Kosten: Typischerweise 20-50 Euro pro Benutzer pro Monat für Enterprise-Versionen.

Für Arztpraxen: Das ist sicher und legal – aber teurer als kostenlose Versionen.

9.7.3.3. 3. Strikte Anonymisierung + Richtlinien

Wenn Sie ChatGPT in der kostenlosen Version nutzen wollen, geht das – aber nur unter strengen Bedingungen: - Keine echten Patientendaten - Keine Ortsangaben, keine identifizierenden Details - Nur generische Beschreibungen oder fiktive Szenarien - Klare Policy für Mitarbeiter, was sie nicht eingeben dürfen

Beispiel – Erlaubt: "Ein 45-jähriger Patient mit unkontrolliertem Bluthochdruck kommt mit Kopfschmerzen. Schreib einen Arztbrief-Entwurf."

Beispiel – Nicht erlaubt: "Mein Patient Hans Müller, geb. 15.7.1978, wohnhaft Hauptstr. 5, 10115 Berlin, hat unkontrolliertem Bluthochdruck…"

Mit dieser Regel können Sie ChatGPT nutzen – aber es braucht ständige Vigilanz von Mitarbeitern. Der Fehler ist eine Daten-Panne.

9.7.3.4. 4. Spezialisierte medizinische KI-Systeme

Es gibt KI-Systeme, die speziell für medizinische Zwecke entwickelt wurden und native DSGVO-Integration haben: - Dragon Medical One (Spracherkennung mit medizinischem Vokabular) - Nabla (ärztliche Dokumentation) - Nuance DAX (medizinische KI-Suite)

Diese Systeme sind für Ärzte entwickelt, verstehen Medizin, und haben legale Auftragsverarbeitungsverträge.

Kosten: Typischerweise 50-100 Euro pro Benutzer pro Monat.

Für Arztpraxen: Das ist oft die beste Lösung – spezialisiert, sicher, bezahlt sich durch Zeiteinsparung.

9.7.4. § 203 StGB-Aspekt: KI als „Hilfsperson"

Eine letzte rechtliche Spitzfindigkeit: Der ärztliche Schweigepflicht nach § 203 StGB schließt die Weitergabe an "Hilfspersonen" ein. Ein KI-System könnte theoretisch als Hilfsperson ausgelegt werden – wenn es DSGVO-konform ist und der Arzt die volle Kontrolle hat.

Das ist die rechtliche Grundlage dafür, dass lokale KI-Modelle oder DSGVO-konforme Enterprise-KI ohne zusätzliche Bedenken genutzt werden kann. Die KI wird zur "Hilfsperson" in der Praxis.

Eine öffentliche ChatGPT-Instanz ist das nicht – sie ist ein unabhängiger Dritter ohne rechtliche Beziehung zur Praxis.

9.7.5. Checkliste: Datenschutz und KI

- ☐ Ich nutze keine öffentlichen KI-Tools (ChatGPT kostenlos, Gemini, Copilot) mit echten Patientendaten.
- ☐ Wenn meine Praxis ChatGPT oder ähnliche Tools einsetzt, nur mit strikter Anonymisierung.
- ☐ Es gibt eine klare schriftliche Policy, welche Daten Mitarbeiter nicht eingeben dürfen.
- ☐ Mitarbeiter sind geschult, was Anonymisierung bedeutet und wie man sie praktiziert.
- ☐ Für häufig eingesetzte KI-Aufgaben nutzen wir entweder lokale Modelle oder DSGVO-konforme Enterprise-Dienste.
- ☐ Es existiert ein AVV mit jedem KI-Anbieter, mit dem wir arbeiten.
- ☐ Spezialisierte medizinische KI-Systeme sind in Betracht gezogen.

9.8. KI-Tools im Überblick – Wofür sind sie geeignet?

9.8.1. Die Kategorien

Es gibt mehrere Kategorien von KI-Tools, die für Arztpraxen relevant sind. Sie haben unterschiedliche Datenschutz-Profile und unterschiedliche Eignung:

9.8.1.1. Kategorie 1: Transkriptions-Tools (Diktaphone-Ersatz)

Diese Tools wandeln Sprache in Text um – und sind speziell für medizinische Nutzung optimiert.

Beispiele: - **Dragon Medical One** (Nuance, jetzt Microsoft): Medizinische Spracherkennung mit medizinischem Vokabular. Der Arzt diktiert, und das System schreibt automatisch Arztbriefe. - **Nabla Copilot** (Nabla): Spezialisiert auf ärztliche Dokumentation. Ärzte diktieren, die KI strukturiert den Text. - **Nuance DAX** (Microsoft): Suite aus Spracherkennung + medizinischer KI für Dokumentation.

Warum relevant für Arztpraxen: - Spart massive Zeit (ein Arztbrief, den der Arzt 15 Minuten schreiben würde, wird in 2-3 Minuten diktiert) - Spezialisiert auf Medizin – versteht medizinisches Vokabular, Nomenklatur, Strukturen - Haben native Auftragsverarbeitungsverträge – DSGVO-konform - Integrieren oft direkt mit dem PVS

Datenschutz: - Diese Tools haben explizite AVV mit den Arztpraxen - Daten werden nicht zum Training genutzt (im Gegensatz zu ChatGPT) - Medizinische Daten sind explizit als “besondere Kategorien” im Vertrag geschützt

Kosten: - Typischerweise 50-100 Euro pro Benutzer pro Monat - Oft Volumen-Rabatte für Praxen

Für Arztpraxen: Das ist oft die beste Lösung. Spezialisiert, sicher, zahlt sich durch Zeiteinsparung aus.

9.8.1.2. Kategorie 2: Text-Hilfe für administrative Aufgaben

Diese sind allgemeine KI-Tools, die für nicht-sensitive Aufgaben in Praxen genutzt werden können.

Beispiele: - ChatGPT (OpenAI) – mit Enterprise AVV - Google Gemini for Business - Microsoft Copilot Pro

Wofür geeignet in Arztpraxen: - Termin-Reminder-E-Mails schreiben (ohne Patientendaten) - Verwaltungs-Schreiben formulieren - Allgemeine Praxis-Kommunikation - Schulungs-Materialien für Patienten (generisch)

Wofür NICHT geeignet: - Arztbriefe (verwenden Sie spezialisierte Transkription-Tools) - Befund-Formulierung (dito) - Anything mit echten Patientendaten

Datenschutz: - **Kostenlose Versionen:** Unsicher. Daten werden zum Training genutzt. NICHT für Praxis-Daten. - **Enterprise-Versionen:** Sicher mit AVV.

Kosten: - Kostenlos (aber unsicher) - Enterprise: 20-50 Euro pro Nutzer/Monat

Für Archtspraxen: Die kostenlose Version ist ein Risiko. Enterprise ist sicher, aber für administrative Aufgaben braucht es Disziplin (keine Patientendaten).

9.8.1.3. Kategorie 3: KI-gestützte Codierung (ICD, OPS)

Spezialisierte Tools, die Ärzte bei der Diagnose- und Prozeduren-Codierung unterstützen.

Beispiele: - **Optum Impact ProCoder** (Optum): KI-basierte Codierungs-Empfehlung - **3M CodeCompass** (3M): Codierungs-Unterstützung mit KI - **Verschiedene PVS-Hersteller** bieten native Codierungs-KI an

Warum relevant: - ICD/OPS-Codierung ist zeitaufwendig - Die KI kann aus Freitexten automatisch Codes vorschlagen - Der Arzt überprüft und bestätigt

Datenschutz: - Diese Tools haben AVV-Verträge - Sie sind speziell für den medizinischen Betrieb entwickelt

Für Arztpraxen: Spezialisiert und sicher. Lohnt sich, wenn die Praxis viel codiert.

9.8.1.4. Kategorie 4: KI-gestützte Diagnoseunterstützung

Das ist etwas anderes als allgemeine KI. Das sind spezialisierte Systeme für spezifische medizinische Aufgaben:

Beispiele: - **Radiologie-KI:** Erkennung verdächtiger Strukturen in Röntgen-, CT-, MRT-Bildern - **Pathologie-KI:** Unterstützung bei Gewebediagnosen - **EKG-KI:** Automatische EKG-Interpretation - **Labor-KI:** Anomalie-Erkennung in Labordaten

Warum relevant: - Diese Systeme sind speziell für medizinische Diagnose trainiert - Sie haben in klinischen Studien bewiesene Genauigkeit - Sie sind in den Behandlungsprozess integriert

Datenschutz: - Diese Systeme haben AVV und sind DSGVO-konform - Medizinische Daten sind geschützt

Für Archtspraxen: Wenn Sie Radiologie machen oder Labor-Automation haben, sind diese Systeme sinnvoll.

9.8.2. Die praktische Regel: Wer braucht einen AVV?

Die Faustregel ist einfach:

> **Wer einen AVV mit dem KI-Anbieter abschließen kann und wer Gesundheitsdaten als "besondere Kategorie" im Vertrag abdeckt, kann den Dienst in Betracht ziehen. Wer das nicht kann (z.B. kostenlose ChatGPT-Version), darf keine Patientendaten eingeben.**

Das bedeutet konkret:

Mit AVV möglich: - Dragon Medical One - ChatGPT Business/Enterprise (wenn der Arzt einen AVV abschließt) - Nabla - 3M CodeCompass - Radiologie-KI-Systeme

Ohne AVV nicht möglich: - ChatGPT kostenlos - Google Gemini kostenlos - Microsoft Copilot kostenlos

Workaround (mit Vorsicht): - Kostenlose Tools KÖNNEN genutzt werden, wenn strikte Anonymisierung durchgesetzt wird - Aber das braucht ständige Vigilanz und ist fehleranfällig

---

9.8.3. Praktische Empfehlung für Arztpraxen

Basierend auf Kosten, Nutzen und Datenschutz:

1. **Für Transkription/Arztbriefe:** Dragon Medical One oder Nabla. Spezialisiert, sicher, zahlt sich aus.
2. **Für administrative Texte:** Wenn überhaupt, Enterprise-Version eines großen Anbieters mit AVV. Oder lokale KI-Modelle.
3. **Für Codierung:** Spezialisierte Codierungs-KI oder PVS-integrierte Lösung.
4. **Für Diagnoseunterstützung:** Spezialisierte medizinische KI-Systeme, wenn relevant für Ihre Praxis.

Das Minimum: - Keine echten Patientendaten in kostenlose KI-Tools - Spezialisierte medizinische Tools für spezialisierte medizinische Aufgaben

---

9.8.4. Checkliste: KI-Tools für Arztpraxen

- ☐ Ich kenne die verfügbaren KI-Tools und ihre Datenschutz-Profile.
- ☐ Für jeden genutzten KI-Tool gibt es einen Auftragsverarbeitungsvertrag.
- ☐ Meine Mitarbeiter wissen, welche Tools für welche Aufgaben geeignet sind.
- ☐ Spezialisierte medizinische KI-Tools sind in Betracht gezogen (Transkription, Diagnoseunterstützung).
- ☐ Es gibt eine klare Policy: Welche Tools darf die Praxis nutzen, und wofür?
- ☐ Mitarbeiter sind geschult, diese Policy zu befolgen.
- ☐ Risiko-Tools (kostenlose ChatGPT) sind entweder gesperrt oder unter strikten Richtlinien.

10. Teil 9: Personal & Zugänge

Eine Medizinische Fachangestellte verlässt die Praxis – ihre Zugangsdaten funktionieren noch drei Monate später. Das ist nicht Sicherheit, das ist Fahrlässigkeit.

10.1. Das zentrale Prinzip: Need-to-Know

Jeder Mitarbeiter bekommt Zugang nur zu dem, was er oder sie für ihre konkrete Arbeit braucht – und nicht mehr. Das ist nicht Misstrauen – das ist Schutz.

Wenn ein Mitarbeiterkonto kompromittiert wird, richtet ein Konto mit minimalen Rechten weit weniger Schaden an als ein Administratorkonto mit Vollzugriff auf alles.

Der praktische Gedanke: Wenn eine MFA versehentlich eine Patientenakte löscht, die sie nie hätte sehen sollen – wer haftet? Wenn ein ehemaliger Mitarbeiter Kundendaten mitnimmt – wie war das möglich? Das alles lässt sich durch minimale Rechte verhindern.

10.2. Berechtigungen und Rollen in der Praxis

Die typische Rollen-Struktur in einer Arztpraxis:

- **Arzt/Ärztin:** Voller Zugriff auf PVS, eHBA (elektronischer Heilberufsausweis), alle Patientenakten, Abrechnung
- **MFA (Medizinische Fachangestellte):** Zugriff auf Terminverwaltung, Patientendaten für Terminübersicht, aber nicht auf sensitive Befunde oder Laborwerte ohne Grund
- **Abrechnungsbeauftragte:** Zugang zu Abrechnung und Kostenträgerdaten, aber kein Zugriff auf klinische Patientenakten
- **Verwaltung:** Terminen, Patientenkontakt, aber keine Patientendaten
- **Ggf. Arzt-Vertreter:** Zugang wie Arzt, aber zeitlich begrenzt

Das sind Rollen – keine Personen. Der Punkt ist, dass Sie nicht ein “Büro-Login” für alle teilen, sondern dass jeder Mensch sein oder ihr eigenes Konto mit seinen oder ihren Rollen hat.

Warum Shared Accounts verboten sind: - Du weißt nicht, wer was getan hat - Du kannst den Zugang nicht gezielt entziehen - Es ist unmöglich, Zwei-Faktor-Authentifizierung einzurichten - Die KBV verbietet es explizit

10.3. Onboarding – Der erste Tag ist entscheidend

10.3.1. 1. Eigene Konten einrichten

Der erste Tag: Der neue Mitarbeiter bekommt eigene Zugangsdaten für alle Systeme, die er nutzt. Im PVS wird ein eigenes Benutzerkonto angelegt – nicht "allgemeines Büro-Login", sondern die Person als Individuum.

Für externe Dienste (E-Mail, Cloud, etc.) bekommt er oder sie eine Einladung mit eigener E-Mail-Adresse.

10.3.2. 2. Rechte dokumentieren

Bevor Zugänge eingerichtet werden, ist dokumentiert:

System	Zugriffsumfang	Zielgruppe
PVS	MFA-Rolle (Terminverwaltung + Basispatientendaten)	Alle MFAs
E-Mail	Voll	Alle
Labor-Interface	Read-only	MFA, Arzt
Abrechnung	Admin	Abrechnungsbeauftragte nur

Das kostet 10 Minuten, spart aber beim Offboarding Stunden.

10.3.3. 3. Verpflichtung auf Vertraulichkeit

Vor dem ersten Datenzugriff unterschreibt der Mitarbeiter: - **Art. 32 Abs. 4 DSGVO:** Verpflichtung auf Vertraulichkeit bei der Verarbeitung personenbezogener Daten - **§ 203 Abs. 4 StGB:** Förmliche Verpflichtung auf Schweigepflicht (speziell für ärztliche Praxen)

Die KBV stellt Muster bereit. Eine Seite, Unterschrift – fertig. Aber: vor dem ersten Zugang, nicht danach.

10.3.4. 4. Sicherheits-Einweisung

Ein kurzes Gespräch (30 Minuten) über: - Passwort-Sicherheit - Phishing-Erkennung - Umgang mit Patientendaten - Was tun bei verdächtigem Vorfall? - Meldepflicht

Unterschrift unter eine "Sicherheits-Regeln"-Seite. Dokumentation in Personalakte.

10.4. Offboarding – Der kritischste Moment

Das ist das Sicherheits-Problem, das fast alle übersehen: Ein Mitarbeiter, der vor sechs Monaten die Praxis verlassen hat und theoretisch noch Zugang zur Kundendatenbank hat.

Die Offboarding-Checkliste – am letzten Arbeitstag:

Sofort (vor der Person Praxis verlässt, im Idealen Fall): - [ ] PVS-Konto sperren - [ ] E-Mail-Konto sperren oder auf Nachfolger weiterleiten - [ ] WLAN-Passwort ändern - [ ] Alle mobilen Device-Zugriffe deaktivieren - [ ] eHBA oder andere Authentifizierungs-Token zurückfordern

Innerhalb 24 Stunden: - [ ] Alle geteilten Passwörter ändern (auch die "nur kurz genutzten") - [ ] Cloud-Zugang deaktivieren - [ ] VPN-Zugang sperren - [ ] Fernlöschung von ausgegebenen Geräten prüfen

Für Berufsgeheimnisträger zusätzlich: - [ ] Schriftliche Erinnerung an fortbestehende Schweigepflicht (§ 203 StGB) – unterschreiben lassen! - [ ] Alle Unterlagen und Datenträger mit geschützten Daten zurückfordern - [ ] Löschnachweis für personenbezogene Daten auf ausgegebenen Geräten

Das muss ein standardisierter Prozess sein – ausgeführt am selben Tag, nicht irgendwann später.

10.5. Zugriffsprotokollierung im PVS

Ein Punkt, den viele vergessen: Das PVS muss protokollieren, wer auf welche Patientenakte zugegriffen hat und wann.

- Mindestens 30 Tage protokollieren
- Monatlich oder quartalsweise überprüfen: Wer hat Zugriff auf Patienten, die nicht in seinem Terminplan sind?
- Ungewöhnliche Zugriffe eskalieren

Das ist kein Misstrauen – es ist Sicherheit. Es schützt Patienten und Mitarbeiter.

10.6. Checkliste: Personal und Zugänge

☐ Jeder Mitarbeiter hat eigene Zugangsdaten – keine Shared Accounts.
☐ Rollen sind definiert (Arzt, MFA, Abrechnung, etc.) und dokumentiert.
☐ Verpflichtungserklärungen (Art. 32 Abs. 4 DSGVO + § 203 StGB) sind unterschrieben und in der Personalakte.
☐ Eine Zugangsliste existiert: Wer hat Zugang zu was, seit wann?
☐ Onboarding-Checkliste wird bei jedem neuen Mitarbeiter durchlaufen.

- ☐ Offboarding-Checkliste wird am letzten Arbeitstag durchlaufen – nicht später.
- ☐ PVS-Audit-Logs werden mindestens monatlich überprüft.
- ☐ Ungewöhnliche Zugriffe werden dokumentiert und eskaliert.
- ☐ Mitarbeiter sind in Sicherheits-Regeln eingewiesen und haben dies bestätigt.

10.7. Berechtigungen und Rollen in der Praxis

10.7.1. Das Fundament: Rollen statt Personen

Das PVS muss Rollen unterstützen. Das heißt: Der Administrator legt fest, was eine "MFA-Rolle" darf und was nicht. Wenn dann Maria als MFA angestellt wird, bekommt sie diese Rolle. Die Berechtigung ist nicht an Maria gebunden, sondern an die Rolle.

Vorteil: Wenn Maria die Praxis verlässt und Klaus kommt, der auch MFA ist, braucht Klaus die gleiche Rolle. Leicht zu machen. Keine individuellen Rechte-Salad.

10.7.2. Typische Rolle in Arztpraxen

Arzt/Ärztin: - Voller Zugriff auf alle Patientenakten - Abrechnung einsehen und bearbeiten - eHBA-Zugang - Verordnungen ausstellen - Befunde und Labor-Ergebnisse einsehen - Audit-Logs für die eigene Praxis einsehen

MFA (Medizinische Fachangestellte): - Terminverwaltung (anlegen, ändern, löschen) - Patientendaten für Terminmanagement (Name, Kontakt, Grunddaten) - Labor-Anforderungen einrichten - Rechnung-Vorbereitung (nicht Abrechnung selbst) - **NICHT:** Befunde lesen, sensitive Diagnosen einsehen, Patientenakten nach Belieben öffnen

Abrechnungsbeauftragte: - Abrechnung einsehen und bearbeiten - Kostenträger-Kommunikation - Rechnungs-Statistiken - **NICHT:** Klinische Patientendaten, Befunde, Diagnosen

Verwaltung: - Terminverwaltung (read-only oder modify) - Patientenkontakt-Daten - **NICHT:** Medizinische Daten

10.7.3. Windows-Benutzerkonten: Admin ist nicht für den täglichen Betrieb

Ein häufiger Fehler: Der Rechner, auf dem das PVS läuft, wird mit Admin-Rechten genutzt. Das bedeutet, jeder, der sich am Rechner anmeldet, hat Admin-Rechte für den gesamten Computer.

Das ist ein Sicherheits-Desaster. Wenn ein Mitarbeiter versehentlich ein verdächtiges Programm klickt oder die MFA-erin ein Phishing-Link öffnet, kann der Angreifer Admin-Rechte bekommen.

Die Lösung ist einfach: - Der tägliche Benutzer hat Standard-Rechte (kein Admin) - Nur für spezifische Aufgaben (Updates, neue Software) wird kurzzeitig auf Admin erhöht - Der Admin-Account wird selten genutzt und hat ein starkes Passwort

Das ist bei modernen Windows-Versionen Standard und braucht nur im Setup beachtet zu werden.

10.7.4. Zugriffsprotokollierung – Audit Logs

Das PVS sollte protokollieren, wer auf welche Patientenakte zugegriffen hat.

Was protokolliert werden sollte: - Benutzer (wer) - Patientenakte (welche) - Zeit (wann) - Aktion (was – Öffnen, Ändern, Löschen)

Was Sie damit tun: - Monatlich die Logs exportieren - Nach Anomalien suchen: Hat eine MFA auf eine Patientenakte zugegriffen, die nicht in ihrem Terminplan ist? - Hat jemand einen Patienten 10x aufgerufen, obwohl er nicht in der Praxis war? - Solche Anomalien dokumentieren und mit dem Mitarbeiter klären

Das ist nicht Misstrauen – es ist eine Art Interner Audit. Es schützt sowohl die Patienten (vor Missbrauch) als auch die Mitarbeiter (vor falschen Verdächtigungen).

10.7.5. Zwei-Faktor-Authentifizierung (2FA) im PVS

Viele moderne PVS-Systeme unterstützen 2FA. Das heißt: Nach der Passwort-Eingabe wird ein zweiter Faktor abgefragt (typischerweise ein Code aus einer App oder per SMS).

Das macht Phishing viel schwerer: Selbst wenn ein Angreifer das Passwort hat, braucht er den zweiten Faktor – und den hat er nicht (es sei denn, er hat auch das Handy).

Empfehlung: 2FA im PVS aktivieren, besonders für Ärzte und Verwaltung. Für alle ist ideal – wenn die Systeme nicht zu viel Reibung erzeugen.

10.7.6. Checkliste: Berechtigungen und Rollen

- ☐ Das PVS unterstützt Rollen (nicht nur einzelne Berechtigungen).
- ☐ Rollen sind definiert und mit dem PVS-Hersteller konfiguriert.
- ☐ Jeder Mitarbeiter hat eine Rolle – nicht eine Ad-hoc-Sammlung von Rechten.
- ☐ MFAs können ihre Aufgaben erfüllen – aber nicht mehr als das.
- ☐ Abrechnungsbeauftragte sehen keine medizinischen Daten.
- ☐ Windows-Benutzer verwenden Standard-Rechte für den täglichen Betrieb, nicht Admin.
- ☐ PVS-Audit-Logs sind aktiviert und werden mindestens monatlich überprüft.
- ☐ Anomalien in den Logs (unerwartete Zugriffe) werden dokumentiert und eskaliert.
- ☐ 2FA ist im PVS aktiviert (zumindest für Ärzte und sensible Rollen).

10.8. Onboarding und Offboarding

10.8.1. Onboarding: Der erste Tag entscheidet

Onboarding ist nicht nur HR – es ist IT-Sicherheit. Was am ersten Tag eingerichtet wird, bestimmt die Sicherheit der nächsten Jahre.

10.8.1.1. Onboarding-Checkliste (Am ersten Arbeitstag durchführen)

Vor dem ersten Arbeitstag: - [ ] Nächster Arzt oder Senior-Mitarbeiter wird als "Pate" für Einweisung benannt - [ ] Alle Verpflichtungserklärungen sind vorbereitet (ausgedruckt)

Am ersten Arbeitstag – Computer und Zugang: - [ ] Benutzer im PVS anlegen - [ ] Name korrekt eingeben (nicht "Mitarbeiter 5") - [ ] Rolle zuweisen (MFA, Verwaltung, etc.) - [ ] Startes Passwort vergeben (lang, komplex, zu ändern beim ersten Login) - [ ] 2FA einrichten (wenn verfügbar) - [ ] Windows-Benutzerkonto anlegen (Standard-Rechte, nicht Admin) - [ ] E-Mail-Konto erstellen oder aktivieren - [ ] WLAN-Zugang erklären und geben - [ ] Telefon-Zugang erklären

Am ersten Arbeitstag – Verpflichtungen: - [ ] Verpflichtungserklärung nach Art. 32 Abs. 4 DSGVO unterschreiben lassen - [ ] Förmliche Verpflichtung nach § 203 StGB unterschreiben lassen (Schweigepflicht) - [ ] Datenschutz-Informationsblatt nach Art. 13 DSGVO geben und unterschreiben lassen - [ ] Beide Dokumente in der Personalakte hinterlegen

Am ersten Arbeitstag – Sicherheits-Einweisung: - [ ] Kurzes Gespräch (30 Min) über Sicherheits-Regeln - [ ] Passwort-Sicherheit - [ ] Phishing-Erkennung (verdächtige E-Mails) - [ ] Umgang mit Patientendaten - [ ] Meldepflicht bei verdächtigem Vorfall - [ ] Sicherheits-Regeln-Seite unterschreiben lassen

In der ersten Woche: - [ ] Praxis-Tour + IT-Infrastruktur zeigen (wo sind die Server, Backup-Geräte, etc.) - [ ] PVS-Schulung (mit Hersteller oder erfahrenem Kollegen) - [ ] Fachliche Einarbeitung beginnen

Dokumentation: Alle Unterschriften und Bestätigungen sollten in einer Ordner "Onboarding" in der Personalakte gespeichert werden oder analog.

10.8.2. Offboarding: Der kritischste Moment

Offboarding passiert oft gar nicht. Das ist das eigentliche Sicherheits-Problem. Ein Mitarbeiter, der vor sechs Monaten gegangen ist und noch Zugang hat – das ist der normale Fall.

10.8.2.1. Offboarding-Checkliste (Am LETZTEN Arbeitstag durchführen)

Im Gespräch oder direkt vorher mit dem Mitarbeiter: - [ ] Klären, dass Schweigepflicht und Vertraulichkeit nach Kündigung weitergilt - [ ] Alle firmeneigenen Geräte zurückfordern - [ ] Laptop - [ ] Smartphone - [ ] eHBA oder Schlüsselkarten - [ ] Schlüssel (Praxis, Schränke) - [ ] Cloud-Synchronisierungen auf Privatgeräten beenden/erklären - [ ] Rückgabe aller Unterlagen

SOFORT (noch am gleichen Tag oder am nächsten Morgen, bevor der Mitarbeiter Praxis betreten kann): - [ ] PVS-Konto sperren - [ ] Windows-Benutzerkonto

deaktivieren - [ ] E-Mail-Konto sperren oder auf Nachfolger umleiten - [ ] Alle Geräte-Zugriffe deaktivieren (Laptop, Smartphone, Zugangskontrollen) - [ ] WLAN-Passwort ändern (falls Mitarbeiter es kannte) - [ ] Fernlöschung von ausgegebenen Geräten initiieren (wenn möglich)

Im Laufe des Tages: - [ ] Alle benutzerdefinierten Passwörter, die der Mitarbeiter kannte, ändern - [ ] Zugriffsberechtigungen für Cloud-Dienste entziehen - [ ] VPN-Zugang deaktivieren (falls vorhanden) - [ ] Telefon-Weiterleitung deaktivieren oder neu einrichten

In der Woche danach: - [ ] Ausgegebene Geräte überprüfen (Daten löschen, wenn nötig) - [ ] Audit-Logs checken, ob der Mitarbeiter noch irgendwo Zugriff hatte, den wir nicht kennten - [ ] Customers informieren, falls der Mitarbeiter direkter Ansprechpartner war

Besonderheit für Berufsgeheimnisträger: - [ ] Schriftliche Erinnerung an fortbestehende Schweigepflicht (§ 203 StGB) – unterschreiben oder empfangen (Einschreiben) - [ ] Alle Unterlagen und Datenträger mit geschützten Informationen sind zurückgefordert und dokumentiert - [ ] Löschnachweis für persönliche Daten auf privaten Geräten des Mitarbeiters (wenn möglich)

Dokumentation: Alle Offboarding-Schritte sollten auf einer Checkliste dokumentiert werden. Datum, Uhrzeit, wer hat es getan. Diese Dokumentation schützt die Praxis, falls später Fragen auftauchen.

10.8.3. Der Notfall: Fristlose Kündigung

Wenn ein Mitarbeiter fristlos gekündigt wird oder plötzlich geht, müssen Sie schneller handeln. Im Idealfall wird die Sperrung noch während des Kündigungsgesprächs durchgeführt – oder sofort danach, bevor der Mitarbeiter den Ort verlässt.

Plan im Kopf haben: - Wer sperrt Zugänge? (IT-Dienstleister oder technischer Mitarbeiter) - Welche Systeme sind am kritischsten? (PVS, E-Mail, Finanzen) - Wie wird internen kommuniziert? (Wer informiert die Kunden?)

So etwas kann im Streitfall eskalieren – Vorbereitung ist wichtig.

10.8.4. Checkliste: Onboarding & Offboarding

Onboarding: - [ ] Verpflichtungserklärungen sind vorbereitet. - [ ] Alle Onboarding-Schritte werden am ersten Tag durchgeführt. - [ ] PVS-Konto mit Rolle und starkem Passwort. - [ ] Verpflichtungen unterschrieben, in Personalakte. - [ ] Sicherheits-Einweisung dokumentiert.

Offboarding: - [ ] Offboarding-Checkliste existiert und wird bei jedem Abgang durchlaufen. - [ ] Alle Zugänge werden am letzten Arbeitstag gesperrt. - [ ] Geräte werden zurückgefordert und überprüft. - [ ] Firmen-Passwörter werden geändert (auch “nur kurz benutzte”). - [ ] Schweigepflicht-Erinnerung wird dokumentiert. - [ ] Audit-Logs werden überprüft auf unerwartete Zugriffe.

11. Teil 10: Notfall & Resilienz

Eine Ransomware-Attacke auf eine Arztpraxis ist nicht abstrakt. Sie passiert. Die Frage ist nicht "ob", sondern "wann" – und ob die Praxis darauf vorbereitet ist.

11.1. Das Szenario: Ein Morgen im März

Ein Arzt kommt in die Praxis, schaltet seinen Computer ein. Statt des PVS-Fensters sieht er einen roten Bildschirm. Text: "Ihre Dateien sind verschlüsselt. Um sie freizugeben, überweisen Sie 5000 Euro auf diese Bitcoins-Adresse…"

Das ist Ransomware. Ein Angreifer hat die Praxis-Systeme verschlüsselt und fordert Lösegeld. Der Arzt kann seine Patientendaten nicht öffnen. Die Praxis läuft nicht.

Was macht er jetzt? Das ist genau der Moment, in dem Panick die schlechtesten Entscheidungen treibt. "Sollen wir zahlen?" "Sollen wir die Polizei anrufen?" "Sollen wir das PVS wieder starten?"

Die Antwort ist ein Plan. Ein Notfallplan, der vor der Krise aufgestellt wurde, und den der Arzt im Notfall Schritt für Schritt abarbeiten kann.

11.2. Warum Arztpraxen besonders attraktiv für Angreifer sind

Arztpraxen sind für Cyberkriminelle sehr attraktive Ziele:

1. **Patientendaten sind Geld:** Gesundheitsdaten auf dem Schwarzmarkt kosten ein Vielfaches von Kreditkartendaten. Ein Name + Diagnose + Krankenkassen-Nummer bringt Tausende Euro.
2. **Erpressungs-Potenzial:** Eine Praxis, bei der Patientendaten zugegriffen werden, ist erpressbar. Nicht nur Lösegeld für die Entschlüsselung, sondern auch Schweigegeld, um zu verhindern, dass Patientendaten veröffentlicht werden.
3. **Leicht zu durchdringen:** Viele Praxen haben einfache IT-Sicherheit. Ein Phishing-Angriff auf eine MFA, und der Angreifer sitzt im Netz.
4. **Bereitschaft zu zahlen:** Praxen sind oft desperat, ihre Daten wiederherzustellen, und zahlen eher Lösegeld als größere Unternehmen.

Das heißt nicht, dass Sie paranoid sein sollten. Aber Sie sollten vorbereitet sein.

11.3. Was Sie in den nächsten Kapiteln lernen

Kapitel 10-01 – Social Engineering und Phishing in der Arztpraxis: Wie Angreifer in die Praxis kommen. Typische Szenarien: Fake-E-Mail vom "KBV-Sicherheitsdienst", Anruf vom "TI-Dienstleister", Phishing-Mail die wie eine KIM-Nachricht aussieht.

Kapitel 10-02 – Krisenszenarien und Handlungsanweisungen: Konkrete Szenarien und was man tut: Ransomware, Datenpanne, TI-Totalausfall, Gerätediebstahl, Praxisbrand. Für jedes Szenario: konkrete Schritte, Meldepflichten, Dokumentation.

Kapitel 10-03 – Der Praxis-Notfallplan: Was ein Notfallplan ist, warum er fertig sein muss, bevor man ihn braucht, und wie man ihn aufbaut. Ein praktisches Template.

Kapitel 10-04 – Digitaler Nachlass: Was mit Patientenakten passiert, wenn der Arzt stirbt oder berufsunfähig wird? Aufbewahrungspflichten, Praxisübergabe, Notfallzugänge. Ein unangenehmes, aber notwendiges Thema.

11.4. Checkliste: Notfall & Resilienz

- ☐ Ich habe einen Notfallplan (oder habe vor, einen zu erstellen).
- ☐ Mein IT-Dienstleister kennt die wichtigsten Krisen-Szenarien.
- ☐ Ich weiß, wie Ransomware-Attacken funktionieren und warum Lösegeld zahlen keine gute Idee ist.
- ☐ Backup-Systeme sind aktiv und werden regelmäßig getestet.
- ☐ Ich kenne die Meldepflichten bei Datenpannen (72 Stunden DSGVO).
- ☐ Eine Vertrauensperson weiß, dass es einen Notfallplan gibt und wo dieser aufbewahrt ist.

11.5. Social Engineering und Phishing in der Arztpraxis

11.5.1. Das zentrale Risiko: Phishing ist das Einfallstor

Die meisten erfolgreichen Angriffe auf Arztpraxen beginnen nicht mit technischem Hacking. Sie beginnen mit einer E-Mail.

Ein Mitarbeiter erhält eine E-Mail, die aussieht, als käme sie vom KBV-Sicherheitsdienst. Darin wird behauptet, dass die Praxis eine Sicherheits-Überprüfung durchlaufen muss. Dafür werden PVS-Zugangsdaten abgefordert. Der Mitarbeiter – vielleicht überfordert mit Sicherheits-Anforderungen – gibt die Daten ein.

Jetzt hat der Angreifer Zugang zum PVS. Von dort aus kann er: - Patientendaten stehlen - Ransomware einschleusen - Sich lateral zu anderen Systemen ausbreiten

Das war kein technischer Hack. Das war Social Engineering – Manipulation eines Menschen.

11.5.2. Typische Phishing-Szenarien für Arztpraxen

11.5.2.1. Szenario 1: Fake E-Mail vom "KBV-Sicherheitsdienst"

Die E-Mail kommt angeblich vom KBV. Betreff: "Sicherheits-Überprüfung erforderlich - Ihre Praxis"

Inhalt: "Aufgrund neuer IT-Sicherheitsanforderungen müssen alle Praxen ihre Sicherheit überprüfen lassen. Klicken Sie auf den Link, um sich mit Ihren PVS-Zugangsdaten anzumelden. Bitte tun Sie dies bis zum nächsten Freitag, sonst wird Ihre Zulassung gefährdet."

Das ist Phishing. Der KBV fordert niemals Zugangsdaten per E-Mail an. Der Link führt zu einer gefälschten Website, die wie das KBV-Portal aussieht, aber nicht ist. Wer die Daten eingibt, gibt sie einem Angreifer.

Erkennungsmerkmale: - Dringlichkeit ("bis Freitag") - Forderung nach Zugangsdaten per E-Mail - Drohung ("Zulassung gefährdet") - Der Link sieht aus wie der KBV-Link, ist es aber nicht

Was ein Mitarbeiter tun sollte: - Nicht auf den Link klicken - Stattdessen das KBV-Portal direkt öffnen und dort überprüfen, ob ein solches Überprüfungs-Verfahren läuft - Im Zweifelsfall die KBV anrufen

11.5.2.2. Szenario 2: Anruf vom "TI-Dienstleister"

Das Telefon klingelt. Eine Person stellt sich vor als Techniker vom TI-Dienstleister oder als "Sicherheits-Consultant". Sie sagt: "Wir haben bei Ihnen ein Sicherheits-Problem erkannt. Können Sie mir kurz Fernzugriff auf Ihren Computer geben, damit ich das überprüfen kann?"

Das ist Social Engineering. Der Anrufer hat wahrscheinlich kein Sicherheits-Problem erkannt, sondern möchte Fernzugriff, um Malware einzuschleusen.

Erkennungsmerkmale: - Sie kennen diese Person nicht - Sie hat die Praxis nie kontaktiert - Sie fordert sofort Fernzugriff an - Es ist ein allgemeines "Sicherheits-Problem", nicht etwas Spezifisches

Was zu tun ist: - Höflich sagen: "Das geht zu schnell. Ich rufe meinen IT-Dienstleister zurück und kläre das." - Auflegen - Den IT-Dienstleister anrufen (die Nummer aus Ihrem Netzwerk-Vertrag, nicht aus der E-Mail) - Fragen, ob jemand anrufen sollte - Sehr wahrscheinlich: Nein, das war ein Angreifer

11.5.2.3. Szenario 3: Phishing-Mail, die wie eine KIM-Nachricht aussieht

KIM (Kommunikation im Medizinwesen) ist der sichere Kommunikations-Standard für Ärzte. Eine E-Mail, die aussieht wie eine KIM-Nachricht, wird möglicherweise als sicherer wahrgenommen.

Aber die E-Mail kommt nicht vom KIM-System, sondern von einem Angreifer, der die KIM-Nachricht nachahmt. Darin wird ein "wichtiges Dokument" angehängt – das in Wirklichkeit Malware ist.

Erkennungsmerkmale: - Die E-Mail sieht aus wie KIM, ist es aber nicht (andere E-Mail-Adresse, seltsamer Absender) - Ein “wichtiger” oder “dringender” Anhang - Druck, den Anhang zu öffnen

Was zu tun ist: - Nicht auf den Anhang klicken - Über das KIM-System überprüfen, ob die Nachricht legitim ist - Im Zweifelsfall beim Absender anrufen

11.5.3. Was tun, wenn Sie auf Phishing hereingefallen sind?

Falls Sie oder Ihr Mitarbeiter versehentlich Zugangsdaten in ein Phishing-Fenster eingegeben oder einen verdächtigen Anhang geöffnet haben, ist schnelles Handeln entscheidend.

Sofort (erste 15 Minuten): 1. Das betroffene Passwort ändern – von einem anderen Gerät aus, wenn möglich 2. Alle aktiven Sitzungen beenden (im betroffenen Dienst: “Alle Geräte abmelden”) 3. Überprüfen, ob neue Benutzer angelegt, E-Mail-Weiterleitungen eingerichtet oder Wiederherstellungsadressen geändert wurden 4. Den IT-Dienstleister informieren – sofort, nicht später

In den nächsten Stunden: 5. Überprüfen, ob der Anhang Malware hatte (IT-Dienstleister Scan) 6. Überprüfen der PVS-Logs: Wurden von diesem Konto ungewöhnliche Zugriffe gemacht? 7. Die Datenschutzbehörde informieren, falls Patientendaten betroffen sind (Frist 72 Stunden)

Wichtig: Nicht mit sich selbst hadern. Phishing-Attacken sind professionell gemacht und täuschen auch erfahrene Nutzer. Schnelles und vollständiges Reagieren ist wichtiger als Schuldzuweisung.

11.5.4. Schulung und Prävention

Die beste Verteidigung gegen Phishing ist geschulte Mitarbeiter.

Einmal jährlich (minimum) sollte ein Schulungs-Gespräch stattfinden: - Wie erkenne ich verdächtige E-Mails? - Wenn ich unsicher bin: nicht klicken, sondern nachfragen - Phishing-Beispiele durchgehen - Die “Rückruf-Regel”: Wenn eine E-Mail von der Bank/KBV/Hersteller kommt, rufe ich selbst an – nicht auf Links in der E-Mail

Simulation – Optional aber wertvoll: Manche IT-Dienstleister können Phishing-E-Mails simulieren und sehen, wer darauf hereinfällt. Das ist keine Strafe – das ist Training. Die Praxis lernt, und der Arzt weiß, wer noch mehr Schulung braucht.

11.5.5. Checkliste: Social Engineering & Phishing

- ☐ Mitarbeiter verstehen die typischen Phishing-Szenarien.
- ☐ Es gibt eine "Rückruf-Regel": Verdächtige Anfragen werden nicht beantwortet, sondern nachgefragt.
- ☐ Der IT-Dienstleister wird informiert, wenn etwas verdächtig ist.
- ☐ Passwort-Manager wird genutzt – damit werden automatisch schwache Passwörter verhindert.
- ☐ Alle aktiven Sitzungen beenden ist bekannt und dokumentiert.
- ☐ Praxis-Mitarbeiter haben jährlich ein Schulungs-Gespräch zu diesem Thema.
- ☐ Es gibt einen Plan, was zu tun ist, wenn jemand auf Phishing hereinfällt (Meldung, Passwort-Änderung, Logs).

11.6. Krisenszenarien und Handlungsanweisungen

11.6.1. Szenario 1: Ransomware-Angriff

Das PVS ist verschlüsselt. Alle Patientendaten sind nicht zugänglich. Der Bildschirm zeigt eine Nachricht mit einer Erpresser-Adresse.

Sofortmaßnahmen (Erste 30 Minuten):

1. **Gerät sofort vom Netzwerk trennen**
   - Netzwerkkabel ziehen (nicht nur WLAN deaktivieren, sondern physisch trennen)
   - Das verhindert die Ausbreitung auf andere Geräte
2. **Externe Festplatten und USB-Geräte trennen**
   - Falls noch nicht verschlüsselt, schnell entfernen
3. **Gerät ausschalten – nicht neu starten**
   - Starten Sie nicht neu und versuchen Sie nicht zu beheben
4. **Backup-Status prüfen**
   - Liegt ein sauberes Backup vor, das VOR dem Angriff erstellt wurde?
   - Das ist Ihre Rettung
5. **IT-Fachmann hinzuziehen – sofort**
   - Ransomware-Entfernung braucht Expertise
   - Kontakt aus dem Notfalldokument

In den nächsten Stunden:

6. **Einfallstor identifizieren**
   - Wie kam die Ransomware rein?
   - Phishing-Mail? Unsicherer RDP-Zugang? Ungepatche Software?
   - Das muss gefixt werden, sonst kommt der nächste Angriff

7. **Alle Passwörter ändern**
    - Ransomware klaut oft auch Zugangsdaten
    - Alle Dienste, die sensibel sind (PVS, E-Mail, Banking)
8. **Anzeige erstatten**
    - Ransomware ist eine Straftat
    - Polizei anrufen, Anzeige aufgeben
    - Aktenzeichen notieren
9. **Datenschutzbehörde informieren**
    - Wenn das betroffene Gerät NICHT verschlüsselt war: 72-Stunden-Meldepflicht nach DSGVO Art. 33
    - Kontakt aus dem Notfalldokument
10. **Versicherung informieren**
    - Cyber-Versicherung überprüfen
    - Manche decken Wiederherstellungskosten ab

Wiederherstellung:

11. **Gerät von Grund auf neu aufsetzen**
    - Formatieren und Betriebssystem neu installieren
    - Niemals versuchen, Ransomware zu "bereinigen"
12. **Backup wiederherstellen**
    - NUR von einem Backup, das eindeutig VOR dem Angriff liegt
    - Schrittweise testen, ob Daten korrekt sind

Wichtig: Zahlen Sie nicht Die häufigste Frage ist: "Sollen wir Lösegeld zahlen?" Die Antwort ist nein. - Die Zahlung garantiert keine Entschlüsselung - Sie machen sich zum wiederholten Ziel - Sie finanzieren Kriminelle - Die Polizei rät davon ab

Ihre beste Hoffnung ist ein gutes Backup – nicht die Zahlung.

11.6.2. Szenario 2: Datenpanne – Patientendaten versehentlich weitergegeben

Eine E-Mail mit Patientendaten wurde versehentlich an die falsche Person gesendet. Oder: Ein USB-Stick mit Patientenakten wurde gefunden.

Das ist eine Datenpanne. Sie haben eine Meldepflicht.

Sofortmaßnahmen (Erste 24 Stunden):

1. **Umfang klären**
    - Welche Daten waren betroffen? (Names, Diagnose, Versichertennummern?)
    - Wie viele Patienten betroffen?

- Ist das Risiko “hoch” oder “niedrig”?

2. **Betroffene Daten zurückfordern**
   - Bei E-Mail: Die Empfängerin anrufen und um Löschung bitten
   - Bei USB-Stick: Mit Polizei arbeiten, Stick sichern
3. **Datenschutzbehörde informieren**
   - Frist: 72 Stunden ab Kenntnis
   - Meldepflicht nach DSGVO Art. 33
   - Kontakt im Notfalldokument
   - Was melden: Umfang der Panne, betroffene Daten, Maßnahmen
4. **Betroffene Patienten benachrichtigen** – WENN hohes Risiko
   - Wenn es wahrscheinlich ist, dass Daten missbracht werden
   - Information sollte Datenschützer-freundlich sein und was Patienten tun können
5. **Interne Untersuchung**
   - Wie ist das passiert?
   - Fehler des Mitarbeiters? Mangelnde Kontrolle? Zu permissive Berechtigungen?
   - Was muss sich ändern?

11.6.3. Szenario 3: TI-Totalausfall

Der Konnektor ist nicht erreichbar. Die TI funktioniert nicht. Die Praxis kann keine Rezepte ausstellen, keine KIM-Nachrichten empfangen, keine eHBA-Funktionen nutzen.

Sofortmaßnahmen:

1. **KV-Hotline anrufen**
   - Kontakt im Notfalldokument
   - Klären, ob es ein allgemeiner Ausfall ist oder nur bei der Praxis
2. **Praxis auf Offline-Betrieb wechseln**
   - Können Sie Rezepte auf Papier ausstellen? (Ja, das ist erlaubt)
   - Können Sie Patienten über die Ausfalls informieren? (Telefonanrufe)
   - Was kann die Praxis OHNE TI noch tun?
3. **Fallback-Verfahren anwenden**
   - Manuelle Dokumentation von Rezepten
   - Kommunikation über Alternative (Telefon, Fax – wenn nötig)
   - Informieren Sie Patienten ehrlich: “Die TI fällt aus, aber wir können Sie behandeln”
4. **IT-Dienstleister: Hardware überprüfen**
   - Ist der Konnektor selbst defekt?
   - Ist es ein Netzwerk-Problem?

- Ist es ein Dienst-Ausfall bei der Telematik-Infrastruktur?

Trost: TI-Ausfälle passieren. Das ist eine bekannte Situation. Sie ist unangenehn, aber managebar. Mit einem Fallback-Plan ist die Praxis nicht völlig lahm.

11.6.4. Szenario 4: Gerätediebstahl – Laptop mit Patientendaten

Ein Mitarbeiter verlässt die Praxis, und der Laptop ist weg. Der Laptop war nicht verschlüsselt, und die Festplatte enthält gecachte Patientendaten.

Sofortmaßnahmen (Erste 2 Stunden):

1. **Polizei anrufen und Diebstahl anzeigen**
   - Aktenzeichen notieren
2. **Gerät remote löschen** (wenn möglich)
   - Findmeapp, Microsoft-Account-Geräte-Verwaltung
   - Das ist nur möglich, wenn es aktiviert war
3. **PVS-Zugang des Mitarbeiters sperren**
   - Falls der Laptop mit gespeicherten Zugangsdaten hatte
4. **Backup überprüfen**
   - Wurden Daten lokal kopiert? (Das sollte nicht sein)
5. **Umfang klären**
   - Welche Patientendaten waren auf dem Laptop?
   - Sind sie verschlüsselt? (Wenn ja: geringeres Risiko)
   - Sind sie identifizierbar? (Name + Diagnose = hoch Risiko)
6. **Datenschutzbehörde informieren** – WENN hohes Risiko
   - 72-Stunden-Meldepflicht
   - Aber: Wenn der Laptop verschlüsselt war, ist das Risiko gering – Meldung kann entfallen
7. **Versicherung informieren**
   - Hausrat oder Cyber-Versicherung

Lektion: Laptops sollten verschlüsselt sein (BitLocker, FileVault). Das macht solche Vorfälle viel weniger kritisch.

11.6.5. Szenario 5: Praxisbrand oder Wasserschaden

Physische IT-Katastrophe. Server, Netzwerk-Infrastruktur, Geräte sind zerstört.

Sofortmaßnahmen:

1. **Sicherheit zuerst** – Evakuieren, Feuerwehr, Rettung
2. **Versicherung anrufen** – Dokumentiere alles fotografisch
3. **Backup-Zugriff überprüfen** – Ist das Backup physisch an einem anderen Ort?
4. **IT-Dienstleister: Recovery-Plan starten**
   - Notfall-Hardware beschaffen
   - Backups spielen auf neuen Systemen ein
5. **Fallback-Betrieb einrichten** – Extern, im Homeoffice, bei Kolleg*innen

Das ist die schlimmste Krise – aber mit cloudgestütztem Backup und einem guten Recovery-Plan ist die Wiederherstellung möglich.

11.6.6. Checkliste: Krisenszenarien

- ☐ Ich kenne die wichtigsten Szenarien und ihre Sofortmaßnahmen.
- ☐ Ein Notfalldokument mit Kontakten (IT-Dienstleister, Polizei, Datenschutzbehörde, KV) existiert.
- ☐ Alle Mitarbeiter wissen, dass Ransomware ein Gerät sofort vom Netz trennt – nicht neu startet.
- ☐ Backup-Tests sind dokumentiert und zeigen, dass Daten wiederhergestellt werden können.
- ☐ Es gibt einen Fallback-Plan für den Fall, dass die TI ausfällt.
- ☐ Versicherungen (Cyber, Betriebsunterbrechung) sind überprüft.

11.7. Der Praxis-Notfallplan für IT

11.7.1. Warum ein Plan, den Sie nie brauchen, trotzdem unverzichtbar ist

Ein Notfallplan ist wie eine Versicherung: Sie hoffen, ihn nie zu brauchen. Wenn Sie ihn brauchen, sind Sie froh, dass er existiert. Der Unterschied zu einer echten Versicherung: Ein Notfallplan kostet Sie einmal einen Nachmittag Arbeit – und spart Ihnen möglicherweise eine Krise.

Die wichtigste Regel: Der Plan muss FERTIG sein, BEVOR Sie ihn brauchen. Sie können den Plan nicht unter Stress schreiben. Er muss eine Checkliste sein, die Sie um 23 Uhr nach einem Schock Schritt für Schritt abarbeiten können.

11.7.2. Die Struktur eines IT-Notfallplans

Ein guter Notfallplan besteht aus drei Teilen:

11.7.2.1. Teil A: Das Notfalldokument

Ein physisch vorhandenes Dokument (gedruckt, nicht nur digital), das folgende Informationen enthält:

Kontaktliste – Die ersten Menschen, die angerufen werden: - IT-Dienstleister (Telefon, E-Mail, eventuell Notfall-Hotline) - PVS-Support/Hersteller (Telefon) - KV-Servicenummer (für TI-Probleme) - Datenschutzbehörde (Bundesland-spezifisch, Telefon + E-Mail) - BSI-Hotline (für Sicherheitsvorfälle) - Polizei (naja, 110, aber trotzdem) - Eigene Versicherung (Cyber, falls vorhanden) - Ein vertrauenswürdiger Freund oder Kollege (jemand außerhalb der Praxis, der im Notfall Rat geben kann)

Passwort-Tresor-Standort - Wo liegt der Passwort-Manager und wie kann man ihn öffnen? - Wer hat den Master-Passwort? (Sollte nicht nur der Arzt sein) - Fallback: Wo sind die wichtigsten Passwörter gedruckt aufbewahrt? (Analog, verschlossen, aber erreichbar im Notfall)

Backup-Standort und Restore-Prozess - Wo wird das Backup aufbewahrt? (Cloud-Anbieter, externer Server, externe Festplatte?) - Wie wird es wiederhergestellt? - Wer hat Zugang? Wie lange dauert ein Restore? - Test-Dokumentation: Wann wurde zuletzt erfolgreich restauriert?

Fallback-Verfahren bei TI-Ausfall - Wie funktioniert die Praxis ohne TI? - Können Rezepte auf Papier ausgestellt werden? - Wer informiert Patienten? - Welche Funktionen funktionieren offline?

Hardware-Ersatz-Plan - Wo kann die Praxis kurzfristig Ersatz-Hardware kaufen oder leihen? - Lieferant, Kontakt, Kosten?

11.7.2.2. Teil B: Szenario-Checklisten

Für die häufigsten Krisen jeweils eine konkrete Schritt-für-Schritt-Liste. Diese Listen sollten so konkret sein, dass Sie sie ohne Nachdenken abarbeiten können – auch unter Stress.

Szenario 1: Ransomware - [ ] Gerät vom Netzwerk trennen - [ ] Andere Geräte prüfen auf Infektion - [ ] IT-Dienstleister anrufen - [ ] Backup-Status prüfen - [ ] Anzeige bei Polizei - [ ] Datenschutzbehörde informieren (wenn nötig) - (… und so weiter, wie in Kapitel 10-02 detailliert)

Szenario 2: Datenpanne - [ ] Umfang klären - [ ] Betroffene Daten zurückfordern - [ ] Datenschutzbehörde informieren (72 Stunden) - (… und so weiter)

Szenario 3: TI-Ausfall - [ ] KV-Hotline anrufen - [ ] Fallback-Betrieb aktivieren - (… und so weiter)

Szenario 4-X: ... (weitere relevante Szenarien)

11.7.2.3. Teil C: Kontaktliste (separate, schnelle Übersicht)

Eine kurze Liste, die nur Nummern und Namen enthält – zum schnellen Nachschlagen im Notfall.

11.7.3. Aufbau und Pflege des Notfallplans

Initiale Erstellung: 2-4 Stunden 1. Alle Kontakte zusammentragen (IT-Dienstleister, Datenschutz, BSI, etc.) 2. Passwort-Manager / Backup-System überprüfen 3. Fallback-Verfahren mit IT-Dienstleister klären 4. Szenario-Checklisten schreiben (basierend auf diesem Ratgeber) 5. Alles ausdrucken und abheften

Jährliche Aktualisierung: - Kontakte überprüfen: Sind alle Nummern noch aktuell? - Hardware/Software-Änderungen: Hat sich die Infrastruktur verändert? - Backup-Test: Funktioniert das Backup noch? - Aktualität überprüfen: Gibt es neue Szenarien, die relevant sind?

Tragen Sie einen Termin ein: "Notfallplan überprüfen" – jedes Jahr am 1. Januar oder an Ihrem Geburtstag. Das kostet 2 Stunden und kann ein Leben retten.

11.7.4. Die kritischen Fragen zum Notfallplan

Bevor Sie den Plan für "fertig" erklären, stellen Sie sich folgende Fragen:

1. **Könnte ich mit diesem Plan im Notfall arbeiten?** (Oder ist es zu vage/zu technisch?)
2. **Sind alle Kontakte aktuell und erreichbar?** (Rufen Sie den IT-Dienstleister an und überprüfen Sie die Nummer)
3. **Wo wird der Plan aufbewahrt?** (Analog, nicht nur digital!)
4. **Wer außer mir kennt den Plan?** (Ein Vertrauensperson sollte wissen, dass es ihn gibt und wo)
5. **Wurde das Backup zuletzt erfolgreich getestet?** (Ein Plan ist wertlos, wenn Backups nicht funktionieren)

11.7.5. Checkliste: Der Praxis-Notfallplan

- ☐ Der Notfallplan ist gedruckt und liegt in Papierform vor (nicht nur digital).
- ☐ Der Notfallplan liegt an einem sicheren Ort: zu Hause, im Safe, oder bei der Vertrauensperson.
- ☐ Alle Kontakte sind aktuell und überprüft.
- ☐ Der Passwort-Tresor-Standort ist dokumentiert.
- ☐ Backup-System und Restore-Prozess sind dokumentiert.
- ☐ Fallback-Verfahren für TI-Ausfall sind klar.
- ☐ Szenario-Checklisten existieren für die wichtigsten Krisen.
- ☐ Eine Vertrauensperson weiß, dass der Notfallplan existiert und wo er liegt.
- ☐ Der Notfallplan wird jährlich überprüft und aktualisiert.
- ☐ Backup-Tests sind dokumentiert und zeigen Funktionalität.

11.8. Digitaler Nachlass in der Archtpraxis

11.8.1. Das unangenehme Thema: Was passiert mit der Praxis, wenn Sie ausfallen?

Das ist ein Gespräch, das kein Arzt gerne führt. Aber es ist notwendig: Was passiert mit den Patientenakten, den Praxis-Daten, der Praxis-IT, wenn Sie morgen für Wochen ausfallen? Oder im schlimmsten Fall: wenn Sie sterben?

Für angestellte Ärzte ist das ein Problem der Klinik. Für niedergelassene Ärzte und Zahnärzte ist es ihre Verantwortung.

11.8.2. Die rechtlichen Anforderungen: Aufbewahrungspflichten bleiben bestehen

Patientenakten müssen 10 Jahre aufbewahrt werden – das steht im Gesetz. Das gilt unabhängig davon, ob Sie noch praktizieren oder nicht. Wenn Sie sterben, müssen Ihre Akten immer noch 10 Jahre aufbewahrt werden – von irgendwem.

Das bedeutet: Im Todesfall gibt es keine "einfach löschen"-Lösung. Es braucht jemanden, der sich um die Akten kümmert – digital und analog.

Zusätzlich: Wenn Sie die Praxis an einen Nachfolger übergeben, muss die IT-Infrastruktur übergeben werden – zusammen mit allen Zugängen und Dokumentationen.

11.8.3. Die praktischen Probleme

Problem 1: Der eHBA bleibt beim Arzt Der eHBA (elektronischer Heilberufsausweis) ist persönlich und bleib bei dem Arzt. Was passiert damit, wenn dieser stirbt? Wer kann damit noch arbeiten?

Problem 2: PVS-Zugang und Passwörter Wer hat Zugang zum PVS? Nur der Arzt? Dann ist die Praxis im Notfall lahm. Wie und wann wird ein Nachfolger Zugang bekommen?

Problem 3: Patientendaten und -geheimnis Auch nach dem Tod bleibt die Schweigepflicht bestehen. Die Person, die mit den Patientendaten umgehen muss (zur Sicherung und Übergabe), muss ebenfalls zur Schweigepflicht verpflichtet sein.

Problem 4: Krankenkassen-Kommunikation Wer nimmt Abrechnung vor? Wer bearbeitet Anträge? Im Notfall kann das Wochen oder Monate sein.

11.8.4. Was zu tun ist: Der digitale Nachlass-Plan

11.8.4.1. 1. Eine Vertrauensperson benennen

Eine Person, die im Notfall (Ausfallz, Berufsunfähigkeit, Tod) Zugriff auf die digitale Infrastruktur bekommt und weiß, was zu tun ist. Das kann sein: - Ein Familienmitglied mit IT-Verständnis - Ein befreundeter Kollege - Ein externer Sicherheitsbeauftragter (formaler, aber distanziert)

Diese Person muss: - Wissen, dass sie diese Rolle hat - Die Rolle schriftlich verstehen (was ist zu tun?) - Zur Schweigepflicht verpflichtet sein

11.8.4.2. 2. Das Notfalldokument erweitern

Das besteht bereits für IT-Krisenszenarien. Jetzt wird ein neuer Abschnitt hinzugefügt: “Im Notfall meines Ausfalls oder Todes”

Dieser Abschnitt sollte enthalten: - **Wichtige Kontakte:** Wen informieren? Familienmitglieder? Ärzte-Kammer? KV? - **Laufende Patienten:** Gibt es besonders vulnerable Patienten, die vor Unterbrechung schützen müssen? - **eHBA und Zugangsdaten:** Wo liegen sie? Wer bekommt Zugriff? - **PVS-Zugang:** Wer wird ein Notfall-Admin? Wie wird dieser informiert? - **Patientenakten-Aufbewahrung:** Wer kümmert sich um die 10-Jahres-Aufbewahrung? Ein Nachfolger? Archiv? - **Praxisübergabe:** Soll die Praxis übernommen werden? Von wem? Mit welchen Schritten? - **Domains, Verträge, Versicherungen:** Wer kündigt, wer verzichtet?

11.8.4.3. 3. Eine Vollmacht ausstellen

Eine schriftliche Vollmacht, die einer Vertrauensperson erlaubt, im Notfall in Ihrem Namen zu handeln – gegenüber: - IT-Anbietern (um Zugänge zu entsperren) - Der Ärztekammer (zur Notifikation) - Banken (für Praxis-Konten) - Krankenkassen und KV (zur Abrechung)

Das ist ein rechtliches Dokument. Besprechen Sie es mit Ihrem Anwalt.

11.8.4.4. 4. Testament und digitaler Nachlass

In Ihrem Testament können Sie festlegen: - Wer erbt die Praxis? (Falls relevant) - Wer kümmert sich um die Patientenakten? - Wie werden sensible Daten nach der Aufbewahrungspflicht gelöscht?

Manche Cloud-Anbieter (Google, Microsoft) haben spezielle “Nachlassverwalter”-Tools, wo Sie zentral festlegen können, wer im Todesfall Zugriff bekommt.

11.8.4.5. 5. Ein Übergabe-Szenario durchdenken

Wenn Sie berufsunfähig werden oder retire gehen, soll die Praxis übergeben werden. Das braucht IT-seitig: - Ein formales "Handover"-Dokument: Alle Zugänge, Passwörter, Verträge, Hardware - Ein Training für den Nachfolger: "So funktioniert die IT dieser Praxis" - Eine Übergangszeit (3-6 Monate?), in der die alte und neue IT parallel laufen

---

11.8.5. Die minimale Lösung – und sie reicht für den Anfang

Sie brauchen nicht sofort ein perfektes System. Die Minimalversion ist diese:

1. **Es gibt eine Vertrauensperson, die weiß, dass sie diese Rolle hat.** (Das allein ist schon ein Riesen-Schritt)
2. **Diese Person weiß, wo das Notfalldokument liegt – und wie sie darauf zugreifen kann.** (Zuhause? Beim Anwalt? Beim Safe-Vermieter?)
3. **Das Notfalldokument enthält genug Information, um die kritischsten Dinge zu tun:** Wichtige Kunden informieren, laufende Geräte-Verträge stilllegen, Daten sichern.

Das ist nicht perfekt. Aber es ist unendlich besser als nichts.

11.8.6. Spezialfall: Ärztekammer und regulatorische Anforderungen

Die Ärztekammer Ihres Bundeslandes hat möglicherweise Regelungen zur Praxis-Abwicklung im Todesfall oder bei Berufsunfähigkeit. Informieren Sie sich: - Aufbewahrungspflicht für Patientenakten - Wer kann die Praxis übernehmen? - Wer kümmert sich um die Fortführung?

Das ist regional unterschiedlich – es lohnt sich, die Kammer zu fragen.

11.8.7. Checkliste: Digitaler Nachlass

- ☐ Es gibt eine Vertrauensperson, die im Notfall handeln kann und weiß, dass sie diese Rolle hat.
- ☐ Diese Person weiß, wo das Notfalldokument liegt – und wie sie darauf zugreifen kann.
- ☐ Das Notfalldokument enthält einen Abschnitt "Im Notfall meines Ausfalls oder Todes".
- ☐ Eine schriftliche Vollmacht ist vorbereitet oder zumindest geplant.
- ☐ Das Thema ist in meinem Testament oder meiner Nachlassplanung erwähnt.
- ☐ Ich habe die Ärztekammer kontaktiert und kenne die regionalen Anforderungen zur Praxis-Abwicklung.
- ☐ Der eHBA und wichtige Passwörter sind dokumentiert (wo, nicht in Text).
- ☐ Ein Nachfolge-Szenario ist zumindest im Kopf durchdacht.

12. Glossar

Begriff Definition des Begriffs.
Weiterer Begriff Definition des weiteren Begriffs.

13. Quellenverzeichnis

Dieses Verzeichnis enthält die Quellen, auf die sich dieser Ratgeber stützt. Es erhebt keinen Anspruch auf Vollständigkeit und ersetzt keine individuelle Rechts- oder Fachberatung. Gesetze und Verordnungen werden in der jeweils geltenden Fassung zitiert.

13.1. Gesetze und Verordnungen

§ 203 StGB – Verletzung von Privatgeheimnissen Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322). https://www.gesetze-im-internet.de/stgb/___203.html

§ 393 SGB V – Cloud-Einsatz im Gesundheitswesen; Verordnungsermächtigung Sozialgesetzbuch Fünftes Buch, eingefügt durch das Gesundheitsdatennutzungsgesetz (GDNG), in Kraft seit 1. Juli 2024. https://www.gesetze-im-internet.de/sgb_5/___393.html

§ 630f BGB – Dokumentation der Behandlung Bürgerliches Gesetzbuch. https://www.gesetze-im-internet.de/bgb/___630f.html

C5GleichwV – Verordnung über gleichwertige Sicherheitsnachweise zum C5-Standard für Cloud-Computing-Dienste im Gesundheitswesen Bundesministerium für Gesundheit, rückwirkend in Kraft getreten zum 1. Juli 2024. https://www.gesetze-im-internet.de/c5gleichwv/BJNR05B0A0025.html

DSGVO – Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates (Datenschutz-Grundverordnung) https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016R0679

KBV-IT-Sicherheitsrichtlinie – Richtlinie nach § 75b SGB V zur IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung Kassenärztliche Bundesvereinigung (KBV), aktuelle Fassung. https://www.kbv.de/html/it-sicherheit.php

---

13.2. Behörden und Institutionen

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2024): C5-Kriterienkatalog – FAQ. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/C5-FAQ/kriterienkatalog-c5-faq_node.html

Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) (2023): Angemessenheitsbeschluss zum EU-U.S. Data Privacy Framework in Kraft getreten. https://www.bfdi.bund.de/SharedDocs/Kurzmeldungen/DE/2023/17_Angemessenheitsbeschluss-EU-US-DPF.html

---

13.3. Rechtlicher Rahmen: EU-US Datentransfer

2b Advice (2025): EGC confirms EU-US Data Privacy Framework: What companies must now consider. Bericht zum EuG-Urteil T-553/23 vom 3. September 2025. https://2b-advice.com/en/2025/09/04/eug-confirms-eu-us-data-privacy-framework-what-companies-need-to-consider-now/

activemind.legal (2024): EU-US Data Privacy Framework – Leitfaden. https://www.activemind.legal/de/guides/eu-us-data-privacy-framework/

13.4. Cloud-Nutzung im Gesundheitswesen: § 393 SGB V und C5-Testat

BVMed – Bundesverband Medizintechnologie (2024): Infoseite C5-Testat / § 393 SGB V – Cloud-Einsatz im Gesundheitswesen. https://www.bvmed.de/themen/recht/infoseite-c5-testat-393-sgb-v-cloud-einsatz-im-gesundheitswesen

curacon GmbH (2025): C5-Gleichwertigkeitsverordnung rückwirkend in Kraft getreten. https://www.curacon.de/neuigkeiten/neuigkeit/c5-gleichwertigkeitsverordnung-rueckwirkend-in-kraft-getreten

Rödl & Partner (2024): Die C5-Testatpflicht nach § 393 SGB V – Wen trifft es denn nun wirklich? https://www.roedl.com/insights/c5-testatpflicht-nach-paragraph-393-sgb-v/

SRD Rechtsanwälte (2024): Cloud im Gesundheitswesen: § 393 SGB V und C5-Testat. https://www.srd-rechtsanwaelte.de/blog/cloud-nutzung-im-gesundheitswesen-393-sgb-v-und-c5-testat

telekonnekt (2024): C5-Testat – Verarbeitung von Gesundheitsdaten in der Cloud. https://www.telekonnekt.de/artikel/c5-testat

audit professionals (2025): BSI C5 Testierung 2025 – Übergangslösung im Gesundheitswesen. https://audit-professionals.de/bsi-c5-testierung-2025-uebergangsloesung/

13.5. Telematikinfrastruktur: TI-Gateway und gehosteter Konnektor

gematik GmbH (2024): TI-Zugang – TI-Gateway. https://www.gematik.de/telematikinfrastruktur/ti-zugang/ti-gateway

KV Sachsen (2024): TI-Gateway bietet neuen Weg in die Telematikinfrastruktur. https://www.kvsachsen.de/fuer-praxen/aktuelle-informationen/praxis-news/ti-gateway-bietet-neuen-weg-in-die-telematikinfrastruktur

telekonnekt (2024): TI-Gateway – Sichere Anbindung an die Telematikinfrastruktur. https://www.telekonnekt.de/artikel/ti-gateway

13.6. Aufbewahrungsfristen für Patientenunterlagen

Virchowbund (o. J.): So lange müssen Sie Patientenunterlagen wirklich aufbewahren. https://www.virchowbund.de/praxisaerzte-blog/so-lange-muessen-sie-patientenunterlagen-wirklich-aufbewahren

A. IT-Sicherheit: Vertiefungen

Die Hauptkapitel geben das notwendige Handlungswissen – hier finden Sie das Verständnis dahinter. Dieser Anhang richtet sich an alle, die tiefer einsteigen möchten: wie Backup-Strategien wirklich funktionieren, was in einem Passwort-Manager intern passiert, wie Sie Ihr Praxisnetzwerk systematisch absichern – und wie Sie sich mit einer Cyberversicherung gegen die Restrisiken absichern, die trotz guter Vorbereitung bleiben.

Was Sie in diesem Anhang erwartet:

A1 – Backup-Strategie für Fortgeschrittene: Über die 3-2-1-Regel hinaus. Wie eine wirklich robuste Backup-Strategie aussieht, was Versioning und Retention bedeuten, wie Sie einen Restore-Test durchführen, der tatsächlich etwas beweist – und was Immutable Backups von gewöhnlichen Cloud-Backups unterscheidet. Mit spezieller Berücksichtigung von Patientendatenbanken und PVS-Systemen.

A2 – Passwort-Manager im Detail: Wie Passwort-Manager intern funktionieren, was die Architekturunterschiede zwischen cloudbasierten und lokalen Lösungen bedeuten, was bei Verlust des Master-Passworts passiert – und warum Passkeys langfristig die Passwort-Frage neu stellen werden. Relevant für den Zugriff auf PVS, TI-Konnektor und eHBA-Management.

A3 – Netzwerksicherheit in der Praxisumgebung: Was in Ihrem Praxisnetzwerk wirklich passiert, wer Zugang hat, welche Angriffsflächen durch schlecht konfigurierte Router und unsichere WLAN-Einstellungen entstehen – und wie Sie sie schließen. Mit Fokus auf TI-Konnektor-Netzwerk, medizinische Geräte und Patientendaten-WLAN.

A4 – Cyberversicherung: Was eine Cyberversicherung leistet und was nicht, wie die Kostenstruktur eines Angriffs aussieht, welche Klauseln im Kleingedruckten zum Problem werden können – und wie Sie den richtigen Tarif für Ihre Praxissituation finden. Mit Schwerpunkt auf branchenspezifische Anforderungen für Arztpraxen und MVZ.

A.1. Backup-Strategie für Fortgeschrittene

Das Hauptkapitel hat die Grundlagen gelegt: 3-2-1-Regel, Backup-Software, erster Restore-Test. Dieser Deep Dive geht einen Schritt weiter – für alle, die verstehen wollen, wie eine wirklich robuste Backup-Strategie aussieht, was im Ernstfall zählt und wie man einen Restore-Test so durchführt, dass er tatsächlich etwas beweist. Speziell für Arztpraxen, MVZ und Praxisnetzwerke.

A.1.1. Backup-Typen: Voll, inkrementell, differenziell

Nicht jedes Backup ist gleich aufgebaut. Die meisten modernen Backup-Programme kombinieren verschiedene Backup-Typen automatisch – aber wer versteht, was dahintersteckt, kann seine Software besser konfigurieren und im Ernstfall schneller handeln.

Vollbackup (Full Backup) Ein Vollbackup sichert alle ausgewählten Daten vollständig – unabhängig davon, was sich seit dem letzten Backup geändert hat. Es ist die einfachste und robusteste Form: Zur Wiederherstellung brauchen Sie genau eine Sicherungskopie. Der Nachteil ist der Speicherbedarf und die Zeit – ein tägliches Vollbackup von 500 GB ist für die meisten Arztpraxen unpraktisch.

Inkrementelles Backup Ein inkrementelles Backup sichert nur die Dateien, die sich seit dem letzten Backup – egal ob Voll- oder inkrementell – geändert haben. Das spart Speicherplatz und Zeit erheblich. Der Nachteil: Zur Wiederherstellung brauchen Sie das letzte Vollbackup plus alle seither erstellten inkrementellen Backups in der richtigen Reihenfolge. Fehlt auch nur eines, ist die Wiederherstellung unvollständig.

Differenzielles Backup Ein differenzielles Backup sichert alle Dateien, die sich seit dem letzten **Vollbackup** geändert haben – unabhängig von zwischenzeitlichen differenziellen Backups. Das ist ein Kompromiss: größer als inkrementell, aber zur Wiederherstellung brauchen Sie nur das letzte Vollbackup und das letzte differenzielle Backup.

Was in der Praxis empfehlenswert ist: Die meisten modernen Backup-Programme (Time Machine, Arq, Duplicati) arbeiten intern mit inkrementellen Backups, präsentieren dem Nutzer aber eine einfache Oberfläche mit Zeitstempeln. Das ist der beste Ansatz für Arztpraxen: automatisch, platzsparend, und die Komplexität der Typen ist intern gelöst.

> **Merksatz:** Verstehen Sie, wie Ihre Backup-Software intern arbeitet – insbesondere wie eine Wiederherstellung abläuft. Was Sie nicht kennen, können Sie im Ernstfall nicht bedienen.

A.1.2. Versionierung: Wie viele Versionen brauchen Sie wirklich?

Das Hauptkapitel empfiehlt mindestens 30, besser 90 Tage Versionshistorie. Hier ist die Begründung, warum das so wichtig ist – und wie Sie die richtige Tiefe für Ihre Praxis bestimmen.

Das Problem der stillen Datenbeschädigung Nicht jeder Datenverlust ist sofort sichtbar. Eine Patientendatenbank in Ihrem PVS kann korrumpiert sein, ohne dass Sie es sofort merken. Eine Ransomware-Infektion kann Dateien verschlüsseln, die Sie erst Wochen später öffnen. Ein Bearbeitungsfehler in einer Patientenakte kann unbemerkt gespeichert werden. Wenn Ihr Backup nur die letzten sieben Tage kennt, sind all diese Szenarien nicht abgedeckt.

Faustregel für die Versionstiefe: - **Arbeitsdateien und PVS-Daten** (Patientenakten, Praxisverwaltung): mindestens 90 Tage - **Systemdaten und Konfigurationen** (inkl. TI-Konnektor, eHBA): mindestens 30 Tage - **E-Mail-Archive und Patientenkommunikation** (KIM): mindestens 1 Jahr - **Steuerrelevante Daten und Abrechnungsdaten**: mindestens 10 Jahre (gesetzliche Aufbewahrungspflicht nach § 10 GOZ und

Abrechnungsrichtlinien der KBV) - **Patientendaten**: mindestens 10 Jahre nach letzte Behandlung oder länger, je nach Landesrecht und Patientenschutz

Speicherbedarf ist kein Argument mehr Cloud-Backup ist erschwinglich geworden – aber in Deutschland und Europa sieht die Anbieterlandschaft anders aus als in den USA, und DSGVO-Konformität ist ein eigenständiges Auswahlkriterium. Für Arztpraxen kommt hinzu: Patientendaten müssen nach deutschem und europäischem Recht behandelt werden.

Für Arztpraxen in Deutschland bieten sich vor allem folgende Optionen an:

- **IONOS HiDrive / STRATO HiDrive:** Deutsche Rechenzentren, DSGVO-konform, ISO 27001-zertifiziert. Reiner Cloud-Speicher, der als Backup-Ziel mit Software wie Duplicati oder Arq genutzt werden kann. Preislich liegen beide im einstelligen Euro-Bereich pro Monat für typische Datenmengen – aktuelle Preise auf den jeweiligen Websites vergleichen, da sich Tarife regelmäßig ändern.
- **IONOS Cloud Backup (powered by Acronis):** Vollständige Backup-Lösung mit deutschem Rechenzentrum, clientseitiger Verschlüsselung, Versionshistorie und Wiederherstellungsfunktionen. Eher für Nutzer geeignet, die eine schlüsselfertige Lösung suchen.
- **Backblaze Personal Backup:** US-amerikanischer Anbieter mit einem Rechenzentrum in Amsterdam. Günstig und unbegrenzt, aber kein europäischer Anbieter. Für Arztpraxen mit Patientendaten ist ein europäischer Anbieter vorzuziehen.
- **Duplicati + selbst gewählter Speicher:** Open-Source-Backup-Software, die mit nahezu jedem Cloud-Speicher (HiDrive, Backblaze B2, Wasabi, S3-kompatible Dienste) zusammenarbeitet. Volle Kontrolle, clientseitige Verschlüsselung, kostenlos.

  Empfehlung: Wer die Wahl hat, bevorzugt einen Anbieter mit deutschen oder europäischen Rechenzentren und einem unterzeichneten AVV (Auftragsverarbeitungsvertrag). Das vereinfacht die DSGVO-Compliance erheblich und vermeidet Fragen zu Drittlandtransfers. Für Arztpraxen ist dies nicht optional, sondern gesetzlich erforderlich. Aktuelle Preise direkt beim Anbieter prüfen – der Markt ist in Bewegung.

A.1.3. Verschlüsselung von Backups – kein optionales Extra

Ein Backup enthält alle Ihre sensiblen Daten: Patientenakten, Abrechnungsinformationen, ärztliche Anamnesedaten, Diagnosen, Fotos. Ein unverschlüsseltes Backup, das in die falschen Hände gerät, ist nicht nur eine Datenverletzung im Sinne von Art. 33 DSGVO – es ist ein Verstoß gegen den ärztlichen Berufscode und § 203 StGB (Verletzung der Berufsgeheimnis-Schweigepflicht).

Lokale Backups: Externe Festplatten sollten verschlüsselt sein – entweder durch die Backup-Software selbst oder durch Verschlüsselung des gesamten Laufwerks (BitLocker To Go unter Windows, FileVault-kompatible Verschlüsselung unter macOS). Eine externe Festplatte, die unverschlüsselt im Praxisbüro liegt, ist bei einem Einbruch ein vollständiger Datenverlust mit Haftungskonsequenzen.

Cloud-Backups: Nie ein Cloud-Backup ohne clientseitige Verschlüsselung einrichten. Das bedeutet: Die Verschlüsselung findet auf Ihrem Gerät statt, bevor die Daten den Cloud-Anbieter erreichen. Der Anbieter sieht nur verschlüsselte Datenpakete – er kann nicht auf Ihre Daten zugreifen, auch wenn er dazu aufgefordert wird.

Arq Backup, Duplicati und Restic unterstützen clientseitige Verschlüsselung standardmäßig. Backblaze Personal Backup verschlüsselt ebenfalls clientseitig mit einem optionalen privaten Schlüssel – aktivieren Sie diese Option, da andernfalls Backblaze technisch Zugang zu Ihren Daten hat.

> **Warnung:** Wer den Verschlüsselungsschlüssel verliert, verliert sein Backup unwiederbringlich. Bewahren Sie den Schlüssel bzw. das Passwort an einem sicheren, vom Backup getrennten Ort auf – zum Beispiel im Notfalldokument oder in einem Passwort-Manager.

A.1.4. Die 3-2-1-Regel erweitern: 3-2-1-1-0

Die klassische 3-2-1-Regel ist ein guter Ausgangspunkt. Für höhere Sicherheitsanforderungen gibt es eine Erweiterung, die in der professionellen IT zunehmend als Standard gilt: **3-2-1-1-0**.

- **3** Kopien der Daten
- **2** verschiedene Medientypen
- **1** Offsite-Kopie
- **1** Offline- oder Air-Gap-Kopie (physisch getrennt, nicht erreichbar)
- **0** Fehler bei der Wiederherstellung – verifiziert durch regelmäßige Restore-Tests

Die entscheidende Ergänzung ist die **Offline-Kopie**: ein Backup, das nicht dauerhaft mit dem Netz oder dem Computer verbunden ist. Das kann eine externe Festplatte sein, die nach dem Backup-Lauf physisch abgezogen wird, oder ein Cloud-Backup mit aktiviertem Object Lock (unveränderliche Aufbewahrung für einen definierten Zeitraum).

Die **0 Fehler** sind der häufig übersehene Teil: Ein Backup-System ist erst dann vollständig, wenn regelmäßig bewiesen wurde, dass die Wiederherstellung funktioniert.

A.1.5. Der Restore-Test: So machen Sie ihn richtig

Ein Backup, das nie getestet wurde, ist eine Hoffnung. Ein getestetes Backup ist eine Garantie.

Was viele falsch machen: Sie öffnen die Backup-Software, sehen grüne Häkchen, und nennen das einen Test. Das ist keiner. Ein echter Test bedeutet: Daten aus dem Backup tatsächlich wiederherstellen und prüfen, ob sie vollständig und korrekt sind.

A.1.5.1. Stufe 1: Datei-Restore (monatlich, 10 Minuten)

1. Wählen Sie eine zufällige Datei aus Ihrem Backup – am besten eine, die Sie regelmäßig verwenden.
2. Stellen Sie sie an einem anderen Speicherort wieder her (nicht am Originalort – Sie wollen das Original nicht überschreiben).
3. Öffnen Sie die Datei und prüfen Sie, ob sie vollständig und korrekt ist.
4. Prüfen Sie das Datum der wiederhergestellten Version – kommt sie wirklich aus dem Backup und nicht aus dem Cache?
5. Dokumentieren Sie: Datum, wiederhergestellte Datei, Ergebnis.

A.1.5.2. Stufe 2: Ordner-Restore (vierteljährlich, 30 Minuten)

1. Wählen Sie einen ganzen Ordner – zum Beispiel Ihre Patientenakten des letzten Monats oder einen Dateiordner des PVS.
2. Stellen Sie ihn vollständig an einem temporären Speicherort wieder her.
3. Prüfen Sie Dateianzahl und Gesamtgröße gegen das Original.
4. Öffnen Sie mehrere Dateien aus verschiedenen Unterordnern stichprobenartig.
5. Löschen Sie den temporären Ordner anschließend wieder.

A.1.5.3. Stufe 3: Vollständiger System-Restore (jährlich, mehrere Stunden)

Das ist der Test, der tatsächlich beweist, dass Sie im Katastrophenfall wiederhergestellt werden können. Er erfordert Vorbereitung:

1. **Vorbereitung:** Stellen Sie sicher, dass Sie einen bootfähigen Wiederherstellungsdatenträger haben (macOS: Recovery-Partition oder externer Datenträger mit macOS; Windows: Wiederherstellungslaufwerk oder Windows-Installationsmedium).
2. **Testumgebung:** Idealerweise verwenden Sie einen zweiten Rechner oder eine virtuelle Maschine – so riskieren Sie nichts am Produktivsystem. Alternativ: Stellen Sie auf einem leeren externen Datenträger wieder her.
3. **Restore durchführen:** Booten Sie vom Wiederherstellungsmedium, verbinden Sie sich mit dem Backup und starten Sie den Restore-Prozess.
4. **Prüfen:** Startet das System? Sind alle wichtigen Programme vorhanden? Sind die Daten vollständig? Ist das PVS-System oder TI-Konnektor korrekt konfiguriert?
5. **Zeit messen:** Wie lange hat der Restore gedauert? Das ist Ihre reale Recovery Time – wichtig für die Planung und Notfallmanagement.

> **Wichtig:** Wenn Sie noch nie einen vollständigen Restore durchgeführt haben, wissen Sie nicht, ob Ihr Backup funktioniert. Planen Sie diesen Test einmal jährlich bewusst ein – am besten zu einem ruhigen Zeitpunkt, nicht wenn der Ernstfall eingetreten ist.

A.1.6. Backup-Monitoring: Wissen, dass es läuft

Ein automatisches Backup, das still und heimlich seit Wochen fehlschlägt, schützt nicht. Die meisten Backup-Programme zeigen Fehler nur an, wenn man aktiv nachschaut – oder senden E-Mail-Benachrichtigungen, die im Spam landen.

Mindestanforderungen ans Monitoring:

- **Benachrichtigung bei Fehler:** Konfigurieren Sie Ihre Backup-Software so, dass sie Sie aktiv benachrichtigt, wenn ein Backup fehlschlägt – per E-Mail oder Push-Benachrichtigung.
- **Wöchentliche Sichtprüfung:** Schauen Sie einmal pro Woche kurz in die Backup-Software und prüfen Sie, ob das letzte Backup erfolgreich war und wann es stattgefunden hat.
- **Kalender-Erinnerung für Tests:** Tragen Sie die Restore-Tests direkt als Kalendertermine ein. Was nicht im Kalender steht, wird nicht gemacht.

Healthchecks.io ist ein kostenloser Dienst, der für technisch affine Nutzer eine elegante Lösung bietet: Ihre Backup-Software sendet nach jedem erfolgreichen Backup einen HTTP-Ping an einen individuellen URL. Bleibt der Ping aus – etwa weil das Backup fehlgeschlagen ist oder der Rechner nicht lief – sendet Healthchecks.io eine Benachrichtigung. Das ist ein einfaches, aber zuverlässiges Dead-Man's-Switch-Prinzip.

A.1.7. Sonderfall: NAS als Backup-Ziel in der Praxisumgebung

Ein NAS (Network Attached Storage) im Praxisnetzwerk ist ein beliebtes Backup-Ziel – praktisch, immer verfügbar, große Kapazität. Es hat aber eine kritische Schwäche: Es ist dauerhaft mit dem Netzwerk verbunden, in dem auch PVS, TI-Konnektor und andere kritische Systeme arbeiten.

Wenn Ransomware Ihren Praxis-Rechner befällt und das NAS als Netzlaufwerk eingebunden ist, kann die Ransomware auch das NAS verschlüsseln. Ein NAS als einziges Backup-Ziel ist deshalb kein ausreichender Schutz – besonders in einer Praxisumgebung, wo der Datenverlust nicht nur finanzielle, sondern auch medizinische und rechtliche Konsequenzen hat.

Empfehlung für NAS-Nutzer:

- Nutzen Sie das NAS als **erste Backup-Ebene** (schnell, lokal, komfortabel).
- Ergänzen Sie es durch ein **Cloud-Backup mit clientseitiger Verschlüsselung** als zweite, unabhängige Ebene.
- Aktivieren Sie auf dem NAS **Snapshot-Funktionen** (verfügbar bei Synology und QNAP): Snapshots erstellen schreibgeschützte Momentaufnahmen des Dateisystems zu definierten Zeitpunkten. Ransomware kann bestehende Snapshots in der Regel nicht löschen, wenn die Snapshot-Funktion korrekt konfiguriert ist.
- Aktivieren Sie wenn möglich **Object Lock oder WORM** auf dem NAS – neuere Synology- und QNAP-Modelle unterstützen dies.
- Isolieren Sie das NAS im Praxisnetzwerk durch ein VLAN, um das Infektionsrisiko zu minimieren.

Merksatz: Ein NAS ist ein hervorragendes erstes Backup-Ziel – aber kein Ersatz für ein vom Netz getrenntes oder cloud-basiertes Offsite-Backup.

A.1.8. Checkliste: Backup-Strategie für Fortgeschrittene

- ☐ Ich kenne den Backup-Typ meiner Software (inkrementell/differenziell/voll) und weiß, was ich zur Wiederherstellung brauche.
- ☐ Meine Versionshistorie beträgt mindestens 90 Tage für Patientendaten und PVS-Daten.
- ☐ Abrechnungs- und Steuerdaten werden mindestens 10 Jahre aufbewahrt.
- ☐ Patientendaten werden mindestens 10 Jahre nach letzter Behandlung aufbewahrt oder länger (landesspezifisch).
- ☐ Alle Backups – lokal und in der Cloud – sind verschlüsselt.
- ☐ Bei Cloud-Backups ist clientseitige Verschlüsselung aktiv – der Anbieter hat keinen Zugang zu meinen Patientendaten.
- ☐ Der Verschlüsselungsschlüssel ist sicher und getrennt vom Backup aufbewahrt.
- ☐ Der Cloud-Anbieter ist in Deutschland oder der EU ansässig und hat einen unterzeichneten AVV.
- ☐ Mindestens eine Backup-Kopie ist offline oder per Object Lock geschützt (3-2-1-1-0).
- ☐ Ich erhalte aktive Benachrichtigungen, wenn ein Backup fehlschlägt.
- ☐ Ich führe monatlich einen Datei-Restore-Test durch und dokumentiere das Ergebnis.
- ☐ Ich führe vierteljährlich einen Ordner-Restore-Test durch.
- ☐ Ich habe mindestens einmal einen vollständigen System-Restore-Test durchgeführt und weiß, wie lange er dauert.
- ☐ Falls ich ein NAS nutze: Snapshots sind aktiviert, es gibt ein zusätzliches Offsite- oder Cloud-Backup, und das NAS ist im Praxisnetzwerk isoliert.

A.2. Passwort-Manager im Detail

Das Hauptkapitel hat die Grundlage gelegt: Passwort-Manager sind die Lösung für das Passwort-Problem, und die Empfehlung lautet Bitwarden, 1Password oder KeePassXC. Dieser Deep Dive erklärt, wie Passwort-Manager intern funktionieren, was die Architekturunterschiede bedeuten, was bei Verlust des Master-Passworts passiert – und was Passkeys sind und warum sie langfristig die Passwort-Frage neu stellen. Mit Bezug zu Arztpraxen und TI-Konnektor-Authentifizierung.

A.2.1. Wie ein Passwort-Manager funktioniert – das Zero-Knowledge-Prinzip

Das Vertrauensproblem beim Passwort-Manager ist offensichtlich: Sie geben alle Ihre Zugangsdaten in eine einzige Anwendung – und vertrauen darauf, dass diese Anwendung sicher ist. Was passiert, wenn der Anbieter gehackt wird?

Die Antwort liegt im Zero-Knowledge-Prinzip: Ein gut designter Passwort-Manager verschlüsselt Ihren Tresor ausschließlich auf Ihrem Gerät, bevor irgendetwas den Anbieter erreicht. Der Anbieter speichert nur verschlüsselte Datenpakete – er kennt weder Ihr Master-Passwort noch den Inhalt Ihres Tresors. Selbst wenn die Server des Anbieters kompromittiert werden, haben Angreifer nur wertlosen Chiffretext.

Wie das technisch funktioniert:

1. Sie geben Ihr Master-Passwort ein.
2. Aus dem Master-Passwort wird lokal auf Ihrem Gerät ein kryptografischer Schlüssel abgeleitet – durch eine rechenintensive Hashfunktion (z. B. PBKDF2 oder Argon2). Diese Funktion ist bewusst langsam, um Brute-Force-Angriffe zu erschweren.
3. Mit diesem Schlüssel wird Ihr Tresor lokal entschlüsselt.
4. Wenn Sie Änderungen speichern, wird der Tresor lokal neu verschlüsselt und der verschlüsselte Tresor an den Server übertragen.

Der Anbieter sieht zu keinem Zeitpunkt den Schlüssel oder die entschlüsselten Inhalte. Das ist Zero-Knowledge.

Die Konsequenz: Wenn Sie Ihr Master-Passwort vergessen, kann Ihnen der Anbieter nicht helfen. Es gibt keine „Passwort vergessen"-Funktion, die Ihre Daten zurückbringt. Der Anbieter kann Ihren Account löschen, aber er kann den Tresor nicht entschlüsseln. Das ist eine Stärke – und zugleich eine Verantwortung.

A.2.2. Architekturunterschiede: Cloud, lokal, selbst gehostet

Die drei empfohlenen Passwort-Manager verfolgen unterschiedliche Architekturansätze – mit unterschiedlichen Stärken und Schwächen.

A.2.2.1. Bitwarden – Cloud mit Open-Source-Kern

Bitwarden ist Open Source: Der gesamte Quellcode ist öffentlich einsehbar und wird regelmäßig von unabhängigen Sicherheitsforschern geprüft. Das ist ein erheblicher Vertrauensvorteil gegenüber proprietären Lösungen – Sie müssen dem Anbieter nicht blind vertrauen, weil Sie (oder jemand mit technischem Know-how) den Code selbst prüfen können.

Der Standardbetrieb ist cloudbasiert: Bitwarden synchronisiert Ihren verschlüsselten Tresor über die eigenen Server. Zero-Knowledge ist implementiert.

Selbst-Hosting: Bitwarden kann vollständig auf einem eigenen Server betrieben werden – entweder auf einem VPS oder auf einem Praxis-Heimserver. Das gibt maximale Kontrolle, erfordert aber technisches Know-how und regelmäßige Wartung. Für die meisten Arztpraxen ist der Cloud-Betrieb die pragmatischere Wahl.

Kostenmodell: Die kostenlose Version deckt alle wesentlichen Funktionen ab. Der Premium-Plan (wenige Euro pro Jahr) ergänzt TOTP-Generierung im Manager, verschlüsselte Dateianhänge und erweiterte 2FA-Optionen – relevant, wenn Sie eHBA-Zugangsdaten speichern.

A.2.2.2. 1Password – Cloud mit starkem Team- und Praxisfokus

1Password ist proprietär – der Quellcode ist nicht öffentlich. Das ist ein prinzipieller Nachteil gegenüber Bitwarden, der aber durch umfangreiche externe Sicherheitsaudits und eine langjährige positive Sicherheitsbilanz teilweise ausgeglichen wird.

1Password implementiert eine technische Besonderheit: den **Secret Key**. Neben dem Master-Passwort gibt es einen zusätzlichen, zufällig generierten Schlüssel, der lokal gespeichert wird. Der Tresor wird mit der Kombination aus Master-Passwort und Secret Key verschlüsselt. Ein Angreifer, der Ihr Master-Passwort kennt, aber nicht Ihren Secret Key hat, kann Ihren Tresor nicht entschlüsseln.

Der Nachteil: Der Secret Key muss beim Einrichten auf neuen Geräten eingegeben werden. Wer ihn verliert und sich gleichzeitig von allen Geräten aussperrt, verliert den Zugang zum Tresor unwiederbringlich. Der Secret Key muss deshalb sicher aufbewahrt werden – 1Password stellt dafür ein druckbares „Emergency Kit" bereit.

Kostenmodell: 1Password ist ausschließlich kostenpflichtig – es gibt keinen dauerhaften kostenlosen Plan, nur eine Testphase. Für Praxen mit mehreren Mitarbeitern gibt es Team-Pläne.

A.2.2.3. KeePassXC – lokal, kein Cloud-Zwang

KeePassXC speichert den Tresor als verschlüsselte Datei lokal auf Ihrem Gerät. Es gibt keinen Anbieter, keinen Server, keine Synchronisierung – es sei denn, Sie richten sie selbst ein.

Das ist der maximale Kontrollansatz: Ihre Daten verlassen niemals Ihr Gerät, es sei denn, Sie entscheiden sich aktiv dafür. Für alle, die aus Gründen des ärztlichen Berufsgeheimnisses grundsätzlich keine Daten in Drittanbieter-Clouds geben wollen, ist KeePassXC die konsequente Wahl.

Der Preis der Kontrolle: Sie sind selbst für die Synchronisierung zwischen Geräten verantwortlich. Eine verbreitete Lösung ist, die KeePass-Datenbankdatei in einem selbst kontrollierten Speicher (verschlüsselter USB-Stick, lokales NAS, eigener Server) abzulegen und manuell oder über ein Sync-Tool zwischen Geräten abzugleichen. Das ist fehleranfälliger als eine automatische Cloud-Synchronisierung.

KeePassXC ist Open Source, kostenlos und hat keine laufenden Kosten.

A.2.3. Was passiert, wenn das Master-Passwort verloren geht?

Das ist die existenzielle Frage beim Passwort-Manager – und die Antwort ist unbequem: **Wer das Master-Passwort verliert und keinen Wiederherstellungsweg eingerichtet hat, verliert seinen Tresor unwiederbringlich.**

Kein seriöser Passwort-Manager bietet eine „Passwort vergessen"-Funktion, die Ihren Tresor zurückbringt. Das wäre nur möglich, wenn der Anbieter Zugang zu Ihren entschlüsselten Daten hätte – was das Zero-Knowledge-Prinzip aufheben würde.

Was Sie jetzt einrichten sollten:

Option 1: Notfallzugang (Bitwarden, 1Password) Bitwarden bietet einen „Emergency Access": Sie können einer Vertrauensperson (z. B. Praxispartner, Praxismanager) Zugang zu Ihrem Tresor gewähren. Die Person muss den Zugang anfragen; Sie haben eine konfigurierbare Wartezeit (z. B. 7 Tage), um den Zugang abzulehnen. Läuft die Frist ab, erhält die Vertrauensperson Zugang. Das schützt gegen unberechtigten Zugang und sichert gleichzeitig den Notfallzugang.

1Password's Emergency Kit erfüllt eine ähnliche Funktion: Das ausgedruckte Dokument mit Master-Passwort und Secret Key wird sicher verwahrt – z. B. im Bankschließfach oder beim Notar.

Option 2: Aufbewahrung im Notfalldokument Das Master-Passwort (und ggf. der Secret Key bei 1Password) gehören ins Notfalldokument – physisch ausgedruckt, sicher aufbewahrt, nicht digital gespeichert. Das Notfalldokument selbst ist verschlossen aufzubewahren.

Option 3: KeePass-Datenbankdatei sichern Bei KeePassXC ist die Datenbankdatei das Backup. Eine verschlüsselte Kopie der Datenbankdatei – zusammen mit dem Master-Passwort an einem getrennten, sicheren Ort – ist der Wiederherstellungsweg.

> **Merksatz:** Das Master-Passwort ist der Generalschlüssel zu allem. Wer es verliert und keinen Notfallweg eingerichtet hat, steht vor verschlossenen Türen – ohne Schlüsseldienst.

A.2.4. Den Tresor selbst sichern – Backup-Strategien für den Passwort-Manager

Der vorherige Abschnitt behandelt den Zugang zum Tresor – was passiert, wenn das Master-Passwort verloren geht. Davon zu trennen ist eine andere Frage: Was passiert, wenn der Dienst selbst nicht mehr verfügbar ist? Ein Anbieter kann ausfallen, ein Konto gesperrt werden, ein Abo unbemerkt ablaufen. Auch der Tresor selbst braucht daher eine Backup-Strategie.

Die folgenden Ansätze lassen sich kombinieren – und sollten es auch. Ein einzelner Wiederherstellungsweg ist ein Single Point of Failure.

Strategie 1: Zweiter Passwort-Manager als paralleler Tresor

Ein zweiter, unabhängiger Passwort-Manager wird regelmäßig mit einem Export aus dem Primärsystem befüllt. Im Notfall – Dienst nicht erreichbar, Konto gesperrt, Abo abgelaufen – ist der zweite Tresor sofort nutzbar.

Diese Strategie ist in der Praxis eine der zuverlässigsten, weil sie keine manuelle Entschlüsselung oder technische Expertise im Notfall erfordert. Voraussetzung ist, dass der zweite Dienst wirklich unabhängig ist: anderer Anbieter, andere Infrastruktur, idealerweise andere Authentifizierungsmethode. Ein zweiter Bitwarden-Account hilft wenig, wenn Bitwarden selbst ausfällt.

Geeignete Kombinationen: 1Password als Primärsystem + Bitwarden (kostenlos) als Backup-Tresor, oder umgekehrt. Wer maximale Unabhängigkeit will, nutzt KeePassXC als Offline-Backup – keine Cloud, kein Dienst, der ausfallen kann.

Eine interessante Variante ist der Einsatz eines konzeptionell anders aufgebauten Dienstes als Backup-Tresor – etwa heylogin. Im Unterschied zu klassischen Passwort-Managern arbeitet heylogin hardwaregebunden: Die Authentifizierung erfolgt über ein physisches Gerät (Smartphone oder Hardware-Token), ohne klassisches Master-Passwort. Wer 1Password oder Bitwarden als Primärsystem nutzt und seine Zugangsdaten regelmäßig per Export nach heylogin importiert, hat damit einen Backup-Tresor mit völlig anderer Architektur – was die Unabhängigkeit erhöht. Ein Angriff oder Systemfehler, der den einen Ansatz trifft, trifft den anderen in der Regel nicht.

Der kritische Punkt: Die Exportdatei, die zwischen den Systemen wandert, enthält alle Passwörter im Klartext oder in leicht entschlüsselbarem Format. Sie darf niemals unverschlüsselt auf der Festplatte liegen. Importieren Sie sie direkt und löschen Sie die Exportdatei anschließend sicher. Legen Sie sie niemals in einem unverschlüsselten Cloud-Ordner ab.

Strategie 2: Verschlüsselter Offline-Export

Regelmäßiger Export aus dem Passwort-Manager als CSV oder JSON, sofortige Verschlüsselung der Exportdatei (z. B. in einem VeraCrypt-Container oder einem 7-Zip-Archiv mit AES-256-Verschlüsselung und starkem Passwort), anschließende Ablage auf einem verschlüsselten USB-Stick oder einer externen Festplatte, die offline und sicher aufbewahrt wird.

Vorteil gegenüber Strategie 1: kein zweiter laufender Dienst nötig, keine laufenden Kosten, vollständige Offline-Verfügbarkeit. Nachteil: rein manueller Prozess, der konsequent und regelmäßig durchgeführt werden muss. Wer den Export-Rhythmus nicht in seine Routine integriert, hat schnell einen veralteten Stand.

Empfehlenswert für Arztpraxen, die Notfalldokumente mit sensiblen Zugangsdaten führen: Dieser Export ersetzt oder ergänzt das physische Notfalldokument.

Empfehlenswerter Rhythmus: monatlich, nach jeder größeren Änderungsphase (z. B. nach dem Migrieren vieler eHBA-bezogener Passwörter) und immer vor einem geplanten Gerätewechsel.

Strategie 3: Physisches Notfalldokument für kritische Konten

Nicht alle Passwörter, aber die wirklich existenzkritischen – E-Mail-Konto, Domain-Registrar, Banking, Zugang zu eHBA und TI-Konnektor, der Passwort-Manager selbst – werden ausgedruckt und physisch sicher aufbewahrt. Ein Bankschließfach, ein Tresor oder die Aufbewahrung beim Notar sind geeignete Orte.

Das physische Dokument hat einen unschlagbaren Vorteil: Es ist vollständig unabhängig von Technik, Strom und Internet. Es hat aber auch eine klare Schwäche: Es veraltet. Wer ein Passwort ändert, muss das Dokument aktualisieren – was in der Praxis leicht vergessen wird. Deshalb eignet sich diese Strategie nicht als einzige Maßnahme, sondern als letztes Sicherheitsnetz für die absolute Kerngruppe kritischer Zugänge.

Strategie 4: Bitwarden Emergency Access / 1Password Emergency Kit

Diese in einem früheren Abschnitt bereits beschriebenen Mechanismen sichern primär den Zugang, nicht den Tresor als Datei. Sie sind eine sinnvolle Ergänzung – aber kein Ersatz für ein inhaltliches Backup, denn sie helfen nur, wenn der Dienst selbst noch funktioniert.

Empfehlung: Mindestens zwei Strategien kombinieren

Keine dieser Strategien ist für sich allein ausreichend. Die pragmatischste Kombination für Arztpraxen:

- Strategie 1 (zweiter Tresor) als Haupt-Backup – immer erreichbar, kein technischer Aufwand im Notfall
- Strategie 3 (physisches Dokument) für die 5–10 kritischsten Zugänge – als letztes Netz, das auch ohne Strom und Internet funktioniert

Wer höhere Anforderungen hat oder Berufsgeheimnisträger ist, ergänzt mit Strategie 2 (verschlüsselter Offline-Export) für eine vollständige, unabhängige Kopie des gesamten Tresors.

> **Merksatz:** Ihr Passwort-Manager ist selbst ein kritisches System – und kritische Systeme brauchen ein Backup. Die Frage ist nicht ob Sie eine Backup-Strategie brauchen, sondern welche Kombination zu Ihrer Arbeitsweise passt.

A.2.5. Passwort-Manager und 2FA – das optimale Zusammenspiel

Ein häufiger Fehler: TOTP-Codes für Dienste im selben Passwort-Manager speichern wie die Passwörter für diese Dienste. Das ist praktisch – aber es untergräbt den Sinn von Zwei-Faktor-Authentifizierung.

Der zweite Faktor soll sicherstellen, dass ein Angreifer, der Ihr Passwort kennt, trotzdem keinen Zugang hat. Wenn Passwort und TOTP-Code aus derselben Quelle kommen – dem kompromittierten Passwort-Manager – ist der zweite Faktor wirkungslos.

Empfehlung: TOTP-Codes für kritische Dienste (E-Mail, Domain-Registrar, Banking, eHBA-Zugang, TI-Konnektor, der Passwort-Manager selbst) in einer separaten 2FA-App aufbewahren – zum Beispiel Aegis (Android, Open Source), Raivo (iOS) oder einem Hardware-Token wie YubiKey. Für weniger kritische Dienste ist die Speicherung im Passwort-Manager ein akzeptabler Kompromiss zwischen Sicherheit und Komfort.

A.2.6. Passkeys – die Zukunft ohne Passwörter

Passkeys sind eine neue Authentifizierungstechnologie, die Passwörter langfristig ersetzen soll. Sie werden von den großen Plattformanbietern (Apple, Google, Microsoft) und zunehmend von vielen Websites unterstützt. Es lohnt sich, das Konzept zu verstehen – auch wenn Passkeys heute noch nicht überall verfügbar sind.

Wie Passkeys funktionieren:

Ein Passkey ist ein kryptografisches Schlüsselpaar: ein privater Schlüssel, der auf Ihrem Gerät gespeichert bleibt, und ein öffentlicher Schlüssel, den der Dienst kennt. Beim Login beweist Ihr Gerät durch eine kryptografische Signatur, dass es den privaten Schlüssel besitzt – ohne den Schlüssel selbst zu übertragen. Die Authentifizierung erfolgt durch Biometrie (Fingerabdruck, Face ID) oder PIN auf Ihrem Gerät.

Was das bedeutet: - Es gibt kein Passwort, das gestohlen werden kann. - Es gibt kein Passwort, das bei einem Datenleck des Anbieters kompromittiert wird. - Phishing-Angriffe funktionieren nicht: Ein Passkey ist an die exakte Domain des Dienstes gebunden – eine gefälschte Website kann den Passkey nicht nutzen.

Der aktuelle Stand: Passkeys werden von Google, Apple, Microsoft, GitHub, PayPal und vielen anderen Diensten unterstützt. Die Verbreitung wächst schnell. Moderne Passwort-Manager (Bitwarden, 1Password) können Passkeys bereits speichern und synchronisieren.

Was Sie heute tun sollten: Aktivieren Sie Passkeys für Dienste, die sie anbieten – insbesondere für Google-Konto, Apple ID und Microsoft-Konto. Behalten Sie aber vorerst Passwort und 2FA als Fallback, bis Passkeys flächendeckend etabliert sind.

> **Merksatz:** Passkeys machen Phishing auf kompatiblen Diensten praktisch unmöglich. Sie sind keine Zukunftsmusik mehr – aber noch kein vollständiger Ersatz für Passwörter.

A.2.7. Die Grenzen des Passwort-Managers

Ein Passwort-Manager ist ein mächtiges Werkzeug – aber kein Allheilmittel. Die wichtigsten Grenzen:

Das Master-Passwort ist der schwächste Punkt. Wenn das Master-Passwort schwach ist, bricht die gesamte Sicherheitskette zusammen. Das Master-Passwort muss lang sein (mindestens 16 Zeichen, besser 20+), einzigartig und niemals anderswo verwendet werden. Eine Passphrase aus mehreren zufälligen Wörtern – zum Beispiel vier oder fünf unzusammenhängende Wörter – ist sowohl sicher als auch merkbar.

Malware auf dem Gerät hebt die Sicherheit auf. Wenn Ihr Gerät mit einem Keylogger oder Infostealer infiziert ist, kann Malware das Master-Passwort abfangen, während Sie es eingeben, oder den entschlüsselten Tresor aus dem Arbeitsspeicher auslesen. Der Passwort-Manager schützt gegen Angriffe auf Server und Netzwerk – nicht gegen Angriffe auf das Endgerät selbst. Deshalb sind Gerätesicherheit und aktuelle Software unverzichtbar.

Browser-Erweiterungen sind eine Angriffsfläche. Die meisten Passwort-Manager bieten Browser-Erweiterungen für automatisches Ausfüllen. Diese Erweiterungen sind praktisch – aber sie erweitern auch die Angriffsfläche. Böswillige Websites können versuchen, die automatische Ausfüllfunktion auszunutzen. Konfigurieren Sie die Erweiterung so, dass sie nur auf Anfrage ausfüllt, nicht automatisch beim Laden der Seite.

Geteilte Passwörter sind ein Sonderfall. Wenn Sie Zugangsdaten mit Mitarbeitern oder Praxispartnern teilen, gelten besondere Anforderungen. Bitwarden und 1Password

unterstützen geteilte Tresore oder Organisationen. Teilen Sie niemals das Master-Passwort selbst – sondern nutzen Sie die dafür vorgesehenen Freigabefunktionen.

A.2.8. Checkliste: Passwort-Manager im Detail

- ☐ Ich nutze einen Passwort-Manager mit Zero-Knowledge-Verschlüsselung.
- ☐ Mein Master-Passwort ist lang (mindestens 16 Zeichen), einzigartig und wird nirgendwo sonst verwendet.
- ☐ Das Master-Passwort (und ggf. Secret Key / Emergency Kit) ist sicher aufbewahrt – physisch, getrennt vom Gerät.
- ☐ Ich habe einen Notfallzugang eingerichtet (Emergency Access bei Bitwarden, Emergency Kit bei 1Password, Datenbankdatei-Backup bei KeePassXC).
- ☐ Ich habe mindestens zwei Backup-Strategien für den Tresor selbst: z. B. zweiter Passwort-Manager + physisches Notfalldokument für kritische Konten.
- ☐ Exportdateien aus dem Passwort-Manager werden sofort verschlüsselt und nach dem Import gelöscht – sie liegen nie unverschlüsselt auf der Festplatte oder in der Cloud.
- ☐ Der verschlüsselte Offline-Export (falls genutzt) wird regelmäßig aktualisiert – mindestens monatlich.
- ☐ TOTP-Codes für kritische Dienste (eHBA, TI-Konnektor, E-Mail, Banking) liegen in einer separaten 2FA-App, nicht im Passwort-Manager.
- ☐ Die Browser-Erweiterung ist so konfiguriert, dass sie nur auf Anfrage ausfüllt.
- ☐ Ich habe geprüft, welche meiner wichtigen Dienste Passkeys unterstützen, und aktiviere sie schrittweise.
- ☐ Mein Gerät ist aktuell und frei von Malware – die Sicherheit des Passwort-Managers steht und fällt mit der Gerätesicherheit.

A.3. Netzwerksicherheit in der Praxisumgebung

Das Hauptkapitel hat den Internetzugang als Grundvoraussetzung behandelt – Zugangsdaten, Router-Backup, Fallback-Lösungen. Dieser Deep Dive geht einen Schritt weiter: Was passiert in Ihrem Praxisnetzwerk? Wer hat Zugang? Welche Angriffsflächen entstehen durch schlecht konfigurierte Router, unsichere WLAN-Einstellungen oder ungeschützte Geräte – und wie schließen Sie sie? Mit spezieller Berücksichtigung des TI-Konnektors, medizinischer Geräte und des Patienten-WLAN.

A.3.1. Der Router: Das Tor zu allem

Der Router ist das wichtigste Sicherheitsgerät in Ihrem Netz – und gleichzeitig das am häufigsten vernachlässigte. Er ist rund um die Uhr eingeschaltet, direkt mit dem Internet verbunden und kontrolliert den gesamten Datenverkehr zwischen Ihren Geräten und der Außenwelt.

Ein schlecht konfigurierter Router ist ein offenes Tor. Die häufigsten Schwachstellen:

Standard-Zugangsdaten für das Router-Interface Viele Router werden mit voreingestellten Passwörtern für die Administrationsoberfläche ausgeliefert – oder mit einem Passwort, das auf dem Gerät aufgedruckt ist und das jeder kennt, der das Gerät in der Hand hatte. Wer Zugang zum Router-Interface hat, kann das gesamte Praxisnetzwerk kontrollieren: WLAN-Passwörter auslesen, Portweiterleitungen einrichten, den DNS-Server umleiten. Ändern Sie das Admin-Passwort des Routers – auf ein starkes, einzigartiges Passwort, das Sie im Passwort-Manager speichern.

Fernzugriff von außen deaktivieren Viele Router bieten die Möglichkeit, das Admin-Interface aus dem Internet erreichbar zu machen. Das ist eine erhebliche Angriffsfläche. Deaktivieren Sie den Fernzugriff auf das Router-Interface vollständig, sofern Sie ihn nicht aktiv benötigen. Bei einer Fritz!Box: `fritz.box` → System → Fritz!Box-Benutzer → Zugang aus dem Internet erlauben → deaktivieren.

Firmware-Updates Router-Firmware enthält wie jede Software Sicherheitslücken. Hersteller wie AVM (Fritz!Box) liefern regelmäßig Updates, die bekannte Lücken schließen. Aktivieren Sie automatische Firmware-Updates oder prüfen Sie regelmäßig manuell auf neue Versionen. Ein Router, der seit Jahren nicht aktualisiert wurde, ist ein bekanntes Angriffsziel.

UPnP deaktivieren Universal Plug and Play (UPnP) erlaubt Geräten in Ihrem Netz, automatisch Portweiterleitungen im Router einzurichten – ohne dass Sie das bestätigen. Das klingt praktisch, ist aber ein Sicherheitsrisiko: Schadsoftware kann UPnP nutzen, um sich selbst nach außen erreichbar zu machen. Deaktivieren Sie UPnP, sofern Sie keine spezifische Anwendung kennen, die es benötigt.

A.3.2. WLAN-Sicherheit: WPA3, Passwörter und versteckte Netzwerke

Verschlüsselungsstandard Das WLAN sollte mit WPA3 verschlüsselt sein – dem aktuellen Standard, der erheblich sicherer ist als das veraltete WPA2. WPA2 ist noch weit verbreitet und für die meisten Praxisanwendungen ausreichend, wenn das Passwort stark ist – aber WPA3 ist vorzuziehen, wenn Router und Endgeräte es unterstützen. WEP und WPA (ohne Versionsnummer) sind veraltet und unsicher; kein modernes Netz sollte sie noch verwenden.

WLAN-Passwort Das WLAN-Passwort sollte lang und zufällig sein – mindestens 16 Zeichen. Da es in der Regel nur einmalig pro Gerät eingegeben wird, spielt Merkbarkeit keine Rolle; nutzen Sie einen Passwort-Generator. Das Passwort gehört in den Passwort-Manager.

Versteckte SSIDs sind kein Schutz Ein verbreiteter Irrtum: Wer den WLAN-Namen (SSID) versteckt, glaubt damit unsichtbar zu sein. In der Praxis ist ein verstecktes WLAN für Tools, die den Funkverkehr abhören, leicht sichtbar – und verursacht zusätzliche Verbindungsprobleme auf Endgeräten. Versteckte SSIDs sind kein Sicherheitsmerkmal, sondern eine Illusion.

A.3.3. Netzwerksegmentierung in der Praxis: Gäste-WLAN, Patienten-WLAN und medizinische Geräte

Eines der wirkungsvollsten Sicherheitsprinzipien im Praxisnetzwerk ist die Trennung: Nicht alle Geräte sollen miteinander kommunizieren können. Die meisten modernen Router – auch einfache Fritz!Box-Modelle – unterstützen die Einrichtung mehrerer WLAN-Netzwerke.

Gäste-WLAN Richten Sie ein separates WLAN für Gäste ein. Wer sich ins Gäste-WLAN einloggt, hat Internetzugang – aber keinen Zugriff auf Ihre Arbeitsgeräte, Ihren NAS, Ihre PVS-Systeme oder medizinischen Geräte. Das schützt Sie vor versehentlicher oder absichtlicher Kompromittierung durch ein Gerät, das ein Besucher mitbringt. Die Einrichtung dauert wenige Minuten.

Patienten-WLAN (optional) Wenn Sie Patienten in Ihrer Praxis WLAN zur Verfügung stellen, nutzen Sie ein eigenes, vom medizinischen Netzwerk völlig getrenntes Patienten-WLAN. Dies hat dieselben Isolationseigenschaften wie das Gäste-WLAN.

Netzwerk für medizinische Geräte Smart-Home-Geräte, Netzwerkkameras, smarte Lautsprecher, Fernseher mit Internetanschluss, aber auch medizinische Geräte wie Blutdruckmessgeräte mit Netzwerkverbindung – all das sind potenzielle Schwachstellen. Viele IoT- und Medizingeräte werden jahrelang nicht mit Firmware-Updates versorgt, haben schwache Standardpasswörter und kommunizieren mit externen Servern, über die Sie keine Kontrolle haben. Isolieren Sie diese Geräte in einem eigenen WLAN-Segment, das keinen Zugriff auf Ihr Medizin-Netzwerk (PVS, TI-Konnektor, eHBA) hat.

TI-Konnektor-Netzwerk Der TI-Konnektor und die damit verbundenen eHBA-Systeme sollten in einem eigenen, besonders gesicherten Netzwerksegment betrieben werden – getrennt von allgemeinen Arbeitsgeräten und auf keinen Fall mit Gäste- oder Patienten-WLAN verbunden. Die KBV-Richtlinien und die Telematikinfrastruktur-Sicherheitsrichtlinien verlangen diese Segmentierung.

Bei einer Fritz!Box lässt sich das über separate Gastnetzwerke oder – für technisch Versiertere – über VLANs umsetzen. Das Prinzip ist einfach: Was nicht kommunizieren muss, soll nicht kommunizieren können.

> **Merksatz:** Ihre medizinischen Geräte und der TI-Konnektor dürfen keinen Zugang zu Patientenwifi oder Gastnetzwerken haben. Trennen Sie die Netzwerke physisch und logisch.

A.3.4. DNS-Sicherheit: Wer beantwortet Ihre Anfragen?

Jedes Mal, wenn Sie eine Website aufrufen, stellt Ihr Gerät eine DNS-Anfrage: „Welche IP-Adresse hat diese Domain?" Die Antwort kommt in der Regel vom DNS-Server Ihres Internetproviders.

Das hat zwei Schwachstellen: Erstens sind herkömmliche DNS-Anfragen unverschlüsselt – ein Angreifer im Netz kann mitlesen, welche Domains Sie aufrufen. Zweitens kann ein kompromittierter oder manipulierter DNS-Server Sie auf eine gefälschte Website umleiten – auch wenn die URL in Ihrem Browser korrekt ist (DNS-Spoofing).

DNS-over-HTTPS (DoH) und DNS-over-TLS (DoT) Diese Protokolle verschlüsseln DNS-Anfragen, sodass sie für Dritte nicht lesbar sind. Viele moderne Browser (Firefox, Chrome) unterstützen DoH nativ. Alternativ können Sie auf Router-Ebene einen verschlüsselten DNS-Dienst eintragen:

- **Cloudflare (1.1.1.1):** Schnell, datenschutzfreundliche Richtlinien, keine Protokollierung von Nutzer-IPs nach kurzer Zeit.
- **Quad9 (9.9.9.9):** Gemeinnütziger Betreiber, Sitz in der Schweiz, blockt bekannte Schadsoftware-Domains automatisch.

DNS-Filtering als kostenloser Schutz Quad9 und ähnliche Dienste blocken automatisch DNS-Anfragen an bekannte Malware- und Phishing-Domains. Das ist ein einfacher, wartungsfreier Schutzlayer, der auf Router-Ebene für das gesamte Netz gilt – ohne Software auf jedem Gerät installieren zu müssen. Besonders für Praxen mit älteren oder verwalteten Geräten sinnvoll.

A.3.5. VPN: Schutz im fremden Netz und Zugriff auf Praxissysteme

Ein VPN (Virtual Private Network) verschlüsselt den gesamten Internetverkehr Ihres Geräts und leitet ihn über einen Zwischenserver. Das schützt Sie vor Abhören im lokalen Netz – besonders wichtig in öffentlichen WLANs (Cafés, Hotels, Coworking-Spaces).

Wann ein VPN sinnvoll ist: - Bei Arbeit in öffentlichen WLAN-Netzen - Beim Zugriff auf sensible Systeme (PVS, TI-Konnektor-Daten, Patientendaten) außerhalb des eigenen Praxisnetzes - Bei Nutzung von Hotspot-Verbindungen über fremde Netzwerke - Für Ärzte, die mobil oder an mehreren Standorten arbeiten

Wann ein VPN im Praxisnetzwerk weniger relevant ist: Im eigenen, gut gesicherten Praxisnetzwerk bringt ein kommerzieller VPN-Dienst wenig zusätzliche Sicherheit – der Verkehr ist bereits durch HTTPS verschlüsselt, und der VPN-Anbieter selbst ist eine neue Vertrauensstelle. Im Praxisnetzwerk ist die direkte Verbindung zum Provider in der Regel vertrauenswürdiger als die Weiterleitung über einen VPN-Anbieter.

VPN für den Zugriff auf das eigene Praxisnetz Eine andere VPN-Nutzung ist der verschlüsselte Fernzugriff auf das eigene Praxisnetzwerk – zum Beispiel auf den NAS, interne Systeme oder PVS-Daten von zu Hause. Hier betreiben Sie Ihren eigenen VPN-Server auf dem Router oder NAS (Fritz!Box unterstützt WireGuard, viele NAS-Systeme ebenfalls). Das ist sicherer als der Direktzugriff über offene Ports.

Kommerzielle VPN-Anbieter Wer einen kommerziellen VPN-Dienst nutzen möchte, sollte auf Anbieter mit nachgewiesener No-Log-Politik, transparenten Eigentümerstrukturen und unabhängigen Audits achten. Mullvad VPN (schwedischer Betreiber) und ProtonVPN (Schweiz, Betreiber von ProtonMail) gehören zu den in der Datenschutz-Community angesehenen Optionen. Viele günstige oder kostenlose VPN-Anbieter finanzieren sich durch den Verkauf von Nutzerdaten – das ist das Gegenteil von Schutz.

A.3.6. Portfreigaben und Angriffsfläche reduzieren

Jede offene Portweiterleitung im Router ist ein potenzieller Eintrittspunkt für Angreifer. Prüfen Sie regelmäßig, welche Portweiterleitungen in Ihrem Router eingerichtet sind, und entfernen Sie alle, die Sie nicht aktiv benötigen.

Bei einer Fritz!Box: `fritz.box` → Internet → Freigaben → Portfreigaben. Jeder Eintrag dort bedeutet: Anfragen aus dem Internet an diesem Port werden an ein Gerät in Ihrem Praxisnetz weitergeleitet. Wenn Sie nicht wissen, wozu eine Freigabe dient, ist das ein Zeichen, dass sie möglicherweise nicht mehr benötigt wird.

Besonders kritisch: Direkter RDP-Zugriff (Windows Remote Desktop) über das Internet ist eine der meistmissbrauchten Angriffsflächen. Wenn Sie Remote-Zugriff auf einen PVS-Rechner oder andere Praxiscomputer benötigen, nutzen Sie stattdessen einen VPN-Tunnel – und stellen RDP nur innerhalb des VPN zur Verfügung, nicht direkt aus dem Internet.

TI-Konnektor-Ports: Überprüfen Sie besonders sorgfältig, ob Ports für TI-Konnektor-Systeme weitergeleitet sind. Diese sollten unter keinen Umständen direkt aus dem Internet erreichbar sein.

A.3.7. Netzwerk-Inventar: Wissen Sie, was in Ihrem Netz ist?

Ein unterschätztes Sicherheitsproblem: Geräte, die im Netz aktiv sind, obwohl niemand mehr weiß, dass sie dort sind. Ein alter Drucker mit veralteter Firmware, ein Smart-TV, der seit Jahren keine Updates mehr bekommt, eine vergessene NAS-Box, ein altes PVS-Terminal.

Die meisten Router zeigen eine Liste aller verbundenen Geräte – bei der Fritz!Box unter `fritz.box` → Heimnetz → Netzwerk. Schauen Sie sich diese Liste einmal an: Erkennen Sie alle Geräte? Geräte, die Sie nicht kennen oder nicht mehr benötigen, sollten vom Netz genommen oder zumindest in das isolierte IoT-Segment verschoben werden.

Für Praxen mit PVS und medizinischen Geräten: Führen Sie ein Inventar aller Netzwerkgeräte und dokumentieren Sie, welche kritisch sind. Dies ist oft auch eine Anforderung von Praxis-Management-Systemen oder Datenschutz-Audits.

A.3.8. Checkliste: Netzwerksicherheit in der Praxisumgebung

- ☐ Das Admin-Passwort meines Routers ist geändert – kein Standardpasswort, kein aufgedrucktes Passwort.
- ☐ Der Fernzugriff auf das Router-Interface aus dem Internet ist deaktiviert.
- ☐ Die Router-Firmware ist aktuell – automatische Updates sind aktiviert oder ich prüfe regelmäßig manuell.
- ☐ UPnP ist deaktiviert.
- ☐ Mein WLAN nutzt WPA2 oder WPA3 mit einem starken, zufälligen Passwort.

- ☐ Es gibt ein separates Gäste-WLAN – Gäste und Patienten kommen nicht ins Arbeitsnetz.
- ☐ Es gibt ein separates WLAN für medizinische Geräte und IoT-Geräte, isoliert vom TI-Konnektor-Netzwerk.
- ☐ Der TI-Konnektor und eHBA-Systeme sind in einem separaten, besonders gesicherten Netzwerksegment.
- ☐ Ich nutze einen verschlüsselten DNS-Dienst (z. B. Quad9) auf Router- oder Browser-Ebene.
- ☐ Ich habe die Portfreigaben meines Routers geprüft und nicht benötigte entfernt.
- ☐ Kein direkter RDP-Zugriff aus dem Internet – nur über VPN.
- ☐ TI-Konnektor-Ports sind nicht direkt aus dem Internet erreichbar.
- ☐ Ich kenne alle Geräte in meinem Praxisnetzwerk und habe unbekannte Geräte entfernt oder isoliert.
- ☐ Ich führe ein Inventar aller kritischen Netzwerkgeräte (PVS, TI-Konnektor, Drucker, Kameras).
- ☐ Für die Arbeit in öffentlichen WLANs nutze ich ein VPN.
- ☐ Für den Remotezugriff auf Praxissysteme verwende ich einen VPN-Tunnel, nicht direkte Portweiterleitungen.

A.4. Cyberversicherung – Schutz, Fallstricke und was für Arztpraxen wirklich zählt

Die Cyberversicherung wird im Guide an mehreren Stellen als hilfreiche Ressource im Krisenfall erwähnt. Aber was ist das eigentlich genau, lohnt sie sich für Arztpraxen und MVZ, was leistet sie wirklich – und was steht im Kleingedruckten, das im Schadensfall zum Problem wird? Dieser Deep Dive beantwortet diese Fragen.

A.4.1. Was ein Sicherheitsvorfall wirklich kostet

Bevor wir zur Versicherung kommen, lohnt sich ein nüchterner Blick auf das, was sie abdecken soll. Die Frage „Was kostet mich ein Cyberangriff?" klingt einfach. Die Antwort ist es nicht.

Studien zu Angriffskosten zeigen ein realistisches Bild: Für kleine Arztpraxen und MVZ entstehen Schäden bei Cyberattacken, die deutlich über das hinausgehen, was viele unterschätzen.

A.4.1.1. Die Kostenstruktur: Drei Wellen

Ein Sicherheitsvorfall erzeugt Kosten in drei Wellen, die zeitlich versetzt einschlagen.

Welle 1: Sofortkosten (Tage bis Wochen)

IT-Forensik und Incident Response kosten zwischen 150 und 300 Euro pro Stunde; eine grundlegende Forensik dauert selten weniger als ein bis zwei Tage – also 1.200 bis 5.000

Euro, eher mehr. Dazu kommen Systemwiederherstellung, Notfallhardware (ein Ersatzlaptop oder Praxis-Terminal: 800 bis 1.500 Euro) und externe Rechts- und Datenschutzberatung. Der GDV (Gesamtverband der Deutschen Versicherungswirtschaft) hat für ein Ransomware-Szenario einer kleinen Arztpraxis direkte Sofortkosten von rund **18.500 Euro** errechnet; für ein Datenklau-Szenario derselben Praxis rund **37.000 Euro** – allein die Informationspflichten gegenüber Patienten schlugen mit 4.000 Euro zu Buche.[1]

Welle 2: Betriebsunterbrechungskosten (Tage bis Monate)

Das ist oft der größte Posten – und derjenige, der Arztpraxen am härtesten trifft. Eine Praxis mit einem Jahresumsatz von 200.000 Euro erzielt täglich rund 800 Euro. Eine Ausfallzeit von zehn Tagen entspricht 8.000 Euro Umsatzverlust – die laufenden Fixkosten nicht eingerechnet. Hinzu kommt: Während ein Ransomware-Angriff läuft, können Sie keine Patienten behandeln, können Notfälle entstehen und Patientensicherheit kann gefährdet sein – was zusätzliche Haftungsrisiken schafft.

Welle 3: Folgekosten (Monate bis Jahre)

DSGVO-Bußgelder können sich auch bei kleinen Betrieben schnell im fünfstelligen Bereich bewegen – Art. 83 DSGVO sieht bis zu 4 Prozent des Vorjahresumsatzes vor. Schadensersatzforderungen betroffener Patienten kommen hinzu – und diese können bei Gesundheitsdaten substantiell sein. Auch dauerhafte Reputationsschäden und höhere Versicherungsprämien nach einem Vorfall entstehen.

Fasst man die Wellen zusammen, ergibt sich für einen mittelgravierenden Vorfall bei einer kleinen Praxis oder einem MVZ ein realistisches Schadensband von **15.000 bis 150.000 Euro** – je nach Branche, Datenmenge, Reaktionsgeschwindigkeit und ob ein funktionierendes Backup vorhanden war.

A.4.1.2. Besondere Risiken für Arztpraxen und MVZ

Arztpraxen und Heilberufe: Gesundheitsdaten sind auf dem Schwarzmarkt besonders wertvoll. Patientendaten können zu Identity Theft, Versicherungsbetrug und emotionalen Schäden führen. Laut einer BSI-Studie von 2024 war jede zehnte befragte Arztpraxis mindestens einmal von einem IT-Sicherheitsvorfall betroffen – und zwei Drittel erfüllten die gesetzlich vorgeschriebenen Schutzmaßnahmen nicht vollständig.[2]

Moderne Ransomware nutzt die „Double-Extortion"-Methode – Daten werden erst kopiert, dann verschlüsselt. Selbst ein funktionierendes Backup schützt nicht vor der Erpressung mit gestohlenen Patientendaten. Die Drohung, sensible medizinische Informationen zu veröffentlichen, erzeugt enormen Druck.

MVZ-Betreiber: MVZ (Medizinische Versorgungszentren) verwalten potenziell noch größere Datenmengen und mehrere Standorte, was die Angriffsfläche und die Komplexität erhöht.

Die Kalkulation, die fast niemand macht

[1] Diese Funktionalität wird als „Egress Filtering" bezeichnet. Im Heimnetz-Bereich ist sie selten aktiviert, weil Standard-Router sie nicht bieten. In Unternehmensnetzen gehört sie zur Grundkonfiguration. Referenz: NIST SP 800-41 Rev. 1, „Guidelines on Firewalls and Firewall Policy".

[2] BSI, *Evaluierung der IT-Sicherheitsrichtlinie in Arztpraxen (SiRiPrax 2024)*, März 2024.

Die Kosten grundlegender IT-Sicherheitsmaßnahmen für Arztpraxen sind überschaubar: Ein Passwort-Manager kostet 2 bis 5 Euro pro Monat, eine saubere Backup-Lösung 10 bis 30 Euro, eine Cyberversicherung ab etwa 30 bis 100 Euro für kleine Praxen. Die Gesamtkosten einer soliden Basisabsicherung liegen also bei etwa **500 bis 1.500 Euro pro Jahr** – einem möglichen Schaden von 15.000 bis 150.000 Euro gegenübergestellt, ist das eine eindeutige Kalkulation.

A.4.2. Lohnt sich eine Cyberversicherung für Arztpraxen?

Die kurze Antwort: **Ja, definitiv** – besonders wenn Sie von Ihrer IT abhängig sind, Patientendaten verarbeiten und einen Ausfall nicht einfach aussitzen können. Bei einer Arztpraxis ist der Ausfall nicht nur finanziell relevant, sondern auch eine medizinische Notfall-Situation.

Eine Cyberversicherung ist keine Alternative zu guter IT-Sicherheit. Wer kein Backup hat, keine Geräteverschlüsselung nutzt und auf jedem Dienst dasselbe Passwort verwendet, ist für viele Versicherer gar nicht oder nur zu sehr hohen Prämien versicherbar. Die Versicherung setzt voraus, dass Sie Grundmaßnahmen ergreifen – sie federt die Restrisiken ab, die trotz dieser Maßnahmen bleiben.

Was für eine Cyberversicherung spricht:

Der wichtigste Vorteil ist oft nicht das Geld, sondern die Infrastruktur im Krisenfall. Gute Cyberversicherungen bieten eine 24/7-Hotline, über die Sie sofort IT-Forensiker, Rechtsanwälte und Krisenberater erreichst – Menschen, die wissen, wie man mit Ransomware-Forderungen umgeht, wie Patientenbenachrichtigungen ablaufen und wie Sie die Behördenkonformität nach einem Vorfall gewährleisten. Als Praxisinhaber haben Sie im Ernstfall niemanden, der Ihnen sagt, was als nächstes zu tun ist – eine Cyber-Police kauft Ihnen dieses Netzwerk ein.

Was gegen eine Cyberversicherung sprechen könnte:

Eine Cyberversicherung ist kein Freifahrtschein. Wer grundlegende Sicherheitsmaßnahmen vernachlässigt, verliert den Versicherungsschutz – ganz oder teilweise. Und wer glaubt, die Versicherung erledige schon alles, wird im Schadensfall enttäuscht sein, wenn Obliegenheitsverletzungen oder Ausschlussklauseln greifen.

Grobe Kostenorientierung:

Für Arztpraxen mit einem Jahresumsatz unter 200.000 € und einer Deckungssumme von 250.000 € beginnen seriöse Tarife ab etwa 400–800 € jährlich, je nach Größe, Branche, Risikoeinschätzung und gewünschten Leistungsbausteinen.[3] IT-nahe Praxen oder solche mit zusätzlichen Diensten zahlen mehr. Praxen mit besonderen Anforderungen (MVZ mit mehreren Standorten, telemedizinische Angebote) zahlen ebenfalls mehr.

---

[3] Diese Preisspanne basiert auf öffentlich verfügbaren Vergleichsrechnern und Anbieterinformationen (Stand: 2026). Prämien variieren erheblich je nach Branche, Deckungsumfang und individueller Risikolage. Für verbindliche Angaben: finanzchef24.de oder exali.de nutzen bzw. einen spezialisierten Versicherungsmakler befragen.

A.4.3. Was eine Cyberversicherung leistet – und was nicht

A.4.3.1. Eigenschäden (eigene Kosten nach einem Angriff)

Das ist der Kernbereich. Gute Tarife decken:

IT-Forensik und Systemwiederherstellung: Die Kosten für die Analyse des Angriffs, die Bereinigung oder Neuinstallation des Systems und die Wiederherstellung von Daten. Das ist oft der größte Posten – mehrere tausend Euro für Spezialisten sind keine Seltenheit. Für Arztpraxen kommt hinzu: Wiederherstellung des PVS-Systems, Wiederherstellung von Patientenakten, Validierung der Datenbankintegrität.

Betriebsunterbrechung: Wenn Sie durch den Angriff nicht arbeiten können, zahlt die Versicherung ein Tagegeld oder ersetzt den entgangenen Umsatz für die Dauer des Ausfalls – bis zu einem vertraglich festgelegten Maximum. Für Arztpraxen ist dieser Baustein besonders wichtig, weil kein Betrieb = keine Patientenversorgung und keine Einkünfte.

Krisenmanagement und PR: Kosten für Krisenberater, die Ihnen helfen, den Vorfall zu managen und die Kommunikation zu gestalten – intern wie extern. Für Arztpraxen: Umgang mit Patientenbenachrichtigungen, Pressestatements, Vertrauenswiederherstellung.

Rechtsberatung und DSGVO-Kosten: Anwaltskosten für die Erfüllung der Informationspflichten nach Art. 33 und 34 DSGVO, Kosten für die Kommunikation mit der Datenschutzbehörde, und – in manchen Tarifen – DSGVO-Bußgelder. Wichtig: Nicht alle Versicherer decken Bußgelder ab; in Deutschland ist die Versicherbarkeit von Bußgeldern rechtlich nicht abschließend geklärt. Lies hier den Tarif sehr genau.

Erpressung/Ransomware: Manche Tarife übernehmen Kosten im Zusammenhang mit Ransomware-Erpressungen – darunter Verhandlungsführung durch Spezialisten und in manchen Fällen das Lösegeld selbst. Aber: Behörden (BSI, BKA) raten von Lösegeldzahlungen ab, und viele Versicherer erstatten das Lösegeld nur, wenn eine Zahlung ausdrücklich mit ihnen abgestimmt wurde. Eigenmächtige Zahlungen können den Anspruch vernichten.

A.4.3.2. Drittschäden (Schäden bei anderen durch Ihren Vorfall)

Wenn durch einen Angriff auf Ihr System Patienten oder Geschäftspartner geschädigt werden – etwa weil Sie versehentlich Schadsoftware weitergeleitet haben oder weil gestohlene Patientendaten zu Schäden bei Dritten geführt haben –, übernimmt die Versicherung begründete Schadensersatzforderungen und wehrt unbegründete ab (Abwehrschutz).

Dieser Baustein ist für Arztpraxen besonders relevant, da Sie Patientendaten verarbeiten und haftbar sein können.

A.4.3.3. Was typischerweise nicht versichert ist

- **Vorsätzliche Handlungen:** Selbst verursachte Schäden durch bewusstes Fehlverhalten.
- **Bekannte Sicherheitslücken:** Wenn der Angriff über eine Schwachstelle lief, die Sie kannten oder hättest kennen müssen und nicht behoben haben.

- **Hardwareschäden:** Eine Cyberversicherung deckt keine physischen Geräteschäden durch Feuer, Wasser oder Sturz – das ist Aufgabe der Geschäftsinhaltsversicherung.
- **Rein finanzieller Betrug:** CEO-Fraud oder Phishing, bei dem Sie selbst Geld überwiesen haben, weil Sie eine gefälschte E-Mail für echt gehalten haben – dieser Bereich ist in vielen Tarifen ausgeschlossen oder nur als Zusatzbaustein versicherbar.
- **Krieg und staatliche Angriffe:** Nach den jüngsten Diskussionen in der Branche haben viele Versicherer Kriegsausschlüsse für Cyberangriffe verschärft. Achten Sie auf die Formulierung in den Bedingungen.

A.4.4. Die Fußangeln – was im Schadensfall schiefgehen kann

Das ist der wichtigste Abschnitt dieses Kapitels. Viele Versicherte erleben die böse Überraschung erst, wenn sie den Versicherungsschutz in Anspruch nehmen wollen.

A.4.4.1. Obliegenheitsverletzungen: Der häufigste Ablehnungsgrund

Eine Obliegenheit ist eine Pflicht, die Sie als Versicherungsnehmer einhalten müssen – nicht als gesetzliche Pflicht, aber als vertragliche Voraussetzung für den Versicherungsschutz. Die häufigsten Obliegenheiten in Cyberpolicen:

Mindest-Sicherheitsmaßnahmen: Fast alle Cyberversicherungen verlangen als Voraussetzung, dass Sie grundlegende Sicherheitsmaßnahmen einhalten – aktueller Virenschutz, aktuelle Updates, regelmäßige Backups, starke Passwörter und 2FA für kritische Zugänge, separate Backups die nicht dauerhaft mit dem Hauptsystem verbunden sind. Für Arztpraxen kommen hinzu: Einhaltung von KBV-Richtlinien, Sicherung des TI-Konnektors, regelmäßige Sicherheits-Schulungen für Mitarbeiter.

Der Teufel steckt im Detail: Wenn Sie beim Antragsformular angeben, dass Sie all das macht, und beim Schadensfall stellt sich heraus, dass Ihr Betriebssystem seit einem Jahr nicht aktualisiert wurde, kann der Versicherer die Leistung kürzen oder verweigern. Das ist einer der häufigsten Ablehnungsgründe.

Sofortige Schadenmeldung: Die meisten Policen verlangen eine Meldung binnen 24 bis 72 Stunden nach Entdeckung. Merksatz: Versicherung melden ist Priorität 1B, direkt nach dem Netzwerkkabel ziehen.

Kein eigenmächtiges Handeln: Viele Versicherer verlangen, dass Sie vor größeren Schritten – insbesondere der Einleitung von Wiederherstellungsmaßnahmen oder einer Lösegeldzahlung – ihre Zustimmung einholen. Wer eigenständig teure Forensiker beauftragt, ohne die Versicherung einzubinden, kann auf den Kosten sitzen bleiben.

A.4.4.2. Vorvertragliche Anzeigepflicht

Beim Abschluss müssen Sie alle gefahrrelevanten Umstände wahrheitsgemäß angeben – frühere Vorfälle, eingesetzte Sicherheitsmaßnahmen, Branche und Datenarten. Für Arztpraxen: Anzahl der Patienten, Datenvolumen, verwendete Systeme (PVS, TI-Konnektor). Wer hier unvollständige oder falsche Angaben macht – auch unabsichtlich –, riskiert, dass die Versicherung im Schadensfall vom Vertrag zurücktritt.

A.4.4.3. Die Deckungssumme ist oft zu niedrig angesetzt

Viele Arztpraxen wählen aus Kostengründen eine Deckungssumme von 50.000 oder 100.000 Euro. Das klingt viel – aber ein ernsthafter Vorfall mit DSGVO-Bußgeldern, IT-Forensik, Anwaltskosten, Betriebsunterbrechung und Drittschadensersatz kann diese Summe überschreiten. Mindestens 250.000 bis 500.000 Euro sind für die meisten Arztpraxen sinnvoller als Orientierung – je nach Größe und Datenvolumen auch mehr.

A.4.4.4. Kriegsausschlüsse und Ransomware

Nach dem NotPetya-Angriff 2017 haben viele Versicherer ihre Bedingungen verschärft. Achten Sie auf Formulierungen wie „staatlich gelenkte Cyberangriffe" oder „Cyberwar" – in der Praxis ist die Abgrenzung oft unklar, aber Sie sollten wissen, ob dieser Ausschluss in Ihrer Police steht.

A.4.5. Welche Leistungen für Arztpraxen wirklich wichtig sind

Nicht jeder Baustein ist gleich wichtig. Eine Priorisierung speziell für Arztpraxen:

Unverzichtbar: - IT-Forensik und Systemwiederherstellung (insbesondere für PVS und TI-Konnektor) - 24/7-Notfallhotline mit Vermittlung von IT-Spezialisten - Betriebsunterbrechung (medizinische Praxen können keine Patienten versorgen) - Rechtsberatung und DSGVO-Kosten (einschließlich Patientenbenachrichtigung)

Sehr sinnvoll: - Drittschadenshaftpflicht (Patientendaten-Schäden) - Ransomware/Erpressung inklusive Krisenverhandlungsführung - Krisen-PR und Reputationsmanagement

Je nach Situation: - CEO-Fraud/Social Engineering (bei Überweisungen an externe Dienstleister) - Spezialschutz für TI-Konnektor und eHBA

A.4.6. Wie komme ich zu einer guten Cyberversicherung?

Online-Vergleichsportale und Direktabschluss: Anbieter wie finanzchef24.de, hiscox.de oder exali.de (letzterer speziell für Freelancer und IT-Berufe) bieten Online-Rechner und Direktabschlüsse. Das ist schnell und günstig – aber Sie treffen die Entscheidung ohne Beratung. Für Standardsituationen kann das funktionieren; für Arztpraxen mit besonderen Anforderungen ist es riskant.

Unabhängiger Versicherungsmakler: Ein Makler, der auf Gewerbepolicen spezialisiert ist und Erfahrung mit Arztpraxen hat, kann den Markt für Sie sondieren, Bedingungen vergleichen und Sie im Schadensfall unterstützen. Empfehlenswert für alle Praxen über 50.000 Euro Jahresumsatz oder mit besonderen Risiken (Telemedizin, Laborleistungen, enge Kundeneinbindung).

Vor dem Abschluss – was Sie prüfen sollten: - Leistungsauslöser (greift die Versicherung nur bei externen Angriffen oder auch bei menschlichem Versagen?) - Obliegenheiten (welche Sicherheitsmaßnahmen sind Pflicht, können Sie sie nachweisen?) - Schadensmeldungsfrist - Selbstbeteiligung - Deckungssumme pro Schadenfall und pro Jahr - Rückwärtsdeckung (Retroaktivität) - Kriegsausschluss-Formulierung - Absicherung für Home-Office und Subunternehmer - Speziellausschlüsse für medizinische Praxen

Den Fragebogen ernst nehmen: Das ist keine Formalität – es ist die Grundlage des Vertrags. Wenn Sie unsicher sind, ob Sie eine Frage mit „Ja" beantworten können: Holen Sie sich zuerst die Maßnahme nach, dann schließen Sie die Versicherung ab.

A.4.7. Die wichtigsten Verhaltenspflichten nach Abschluss

Eine Cyberversicherung ist kein einmaliger Kauf, der dann im Schrank liegt. Sie haben laufende Pflichten: Sicherheitsmaßnahmen aufrechterhalten; wesentliche Änderungen des Risikos melden (neues Geschäftsfeld, gestiegener Umsatz, neue Datenarten, neue Standorte bei MVZ); im Schadensfall sofort melden – nicht nach einer Woche; keine unnötigen Kosten verursachen, ohne die Versicherung einzubinden.

A.4.8. Checkliste: Cyberversicherung

A.4.8.1. Vor dem Abschluss

- ☐ Ich habe die grundlegenden Sicherheitsmaßnahmen umgesetzt, die als Obliegenheit verlangt werden (Antivirus, Updates, Backup, 2FA, KBV-Richtlinien).
- ☐ Ich habe den Fragebogen vollständig und wahrheitsgemäß ausgefüllt.
- ☐ Ich habe die Obliegenheiten im Vertrag gelesen und verstanden.
- ☐ Ich habe die Deckungssumme realistisch gewählt (mindestens 250.000 € – 500.000 € als Orientierung für Arztpraxen).
- ☐ Ich habe die Selbstbeteiligung und ihre Auswirkungen verstanden.
- ☐ Ich weiß, was der Kriegsausschluss in meiner Police besagt.
- ☐ Ich weiß, ob CEO-Fraud/Social Engineering mitversichert ist.
- ☐ Ich habe überprüft, ob spezielle Anforderungen für TI-Konnektor und eHBA abgedeckt sind.
- ☐ Ich habe die Notfall-Hotline-Nummer der Versicherung im Notfalldokument eingetragen.

A.4.8.2. Im laufenden Betrieb

- ☐ Ich halte die vertraglich zugesicherten Sicherheitsmaßnahmen aufrecht.
- ☐ Ich melde wesentliche Änderungen meines Risikoprofils an den Versicherer.
- ☐ Ich überprüfe meinen Versicherungsschutz jährlich – deckt er noch meine aktuelle Praxis ab?
- ☐ Ich führe regelmäßige Sicherheits-Schulungen für Mitarbeiter durch.

A.4.8.3. Im Schadensfall

- ☐ Versicherung sofort nach Entdeckung informiert (Frist beachten).
- ☐ Keine eigenmächtigen Kosten oder Entscheidungen ohne Rücksprache mit Versicherung.
- ☐ Alle Maßnahmen und Kommunikation dokumentiert.
- ☐ Notfall-Hotline angerufen, um Unterstützung durch Forensiker, Anwälte und Krisenmanager zu aktivieren.

A.5. Firewalls und Netzwerksegmentierung – Deep Dive

Das Hauptkapitel hat erklärt, was eine Firewall ist, und warum eine Fritz!Box diese Anforderungen nicht erfüllt. Dieser Deep Dive geht einen Schritt weiter: Welche Arten von Firewalls gibt es? Gegen welche Angriffe schützen sie – und gegen welche nicht? Wie baut man ein sinnvoll segmentiertes Praxisnetz auf? Und was braucht man dafür an Hardware?

A.5.1. Firewall-Typen: Vom einfachen Filter zur intelligenten Analyse

Nicht jede Firewall ist gleich. Die Bezeichnung umfasst ein breites Spektrum von Technologien mit sehr unterschiedlichen Fähigkeiten.

Paketfilter (Stateless Firewall)

Die einfachste Form. Ein Paketfilter prüft jeden einzelnen Netzwerkpakete anhand fester Regeln: Erlaubt sind Pakete von dieser IP-Adresse, an diesen Port, über dieses Protokoll. Alle anderen werden verworfen. Der Paketfilter hat kein Gedächtnis – er weiß nicht, ob ein eingehendes Paket zu einer Verbindung gehört, die ein internes Gerät initiiert hat, oder ob es ein ungebetener Angriff ist.

Paketfilter sind schnell und ressourcenschonend, aber eingeschränkt. Sie sind heute meist als erstes Element in komplexeren Systemen eingebaut, nicht mehr als eigenständige Lösung.

Stateful Inspection Firewall

Der aktuelle Standard für die meisten Einsatzbereiche. Diese Firewalls verwalten eine Verbindungstabelle: Sie merken sich, welche Verbindungen interne Geräte nach außen aufgebaut haben, und erlauben eingehende Antwortpakete nur dann, wenn sie zu einer bestehenden Verbindung gehören. Pakete ohne passenden Eintrag in der Tabelle werden verworfen.

Das klingt nach dem, was die Fritz!Box auch tut – und tatsächlich ist NAT eine vereinfachte Form dieses Prinzips. Der Unterschied liegt in der Konfigurierbarkeit, den Logging-Möglichkeiten, der Unterstützung für ausgehende Regeln und der Möglichkeit, das Verhalten gezielt zu steuern.

Application Layer Firewall / Next-Generation Firewall (NGFW)

Diese Systeme analysieren nicht nur, wohin Daten gehen, sondern was sie enthalten. Sie erkennen Protokolle unabhängig vom Port (also auch dann, wenn jemand Schadsoftware-Kommunikation über Port 443 versteckt), identifizieren Anwendungen und können Regeln auf Anwendungsebene durchsetzen.

Moderne NGFWs kombinieren diese Fähigkeit mit Intrusion Detection and Prevention (IDS/IPS), SSL-Inspektion (Entschlüsselung und Analyse von HTTPS-Verkehr), DNS-Filtering und teils auch Antivirusscan des Datenverkehrs. Diese Systeme waren lange nur für Unternehmen erschwinglich – heute gibt es Software-Lösungen, die auf handelsüblicher Hardware betrieben werden können.

A.5.2. Gegen welche Angriffe schützt eine Firewall?

Eine Firewall ist kein Allheilmittel. Was sie kann und was nicht, lässt sich klarer einordnen, wenn man konkrete Angriffsszenarien betrachtet.

Was eine Firewall verhindert:

Port-Scans und ungebetene eingehende Verbindungen. Angreifer scannen das Internet systematisch nach erreichbaren Diensten – offene Ports auf Routern, Servern oder Geräten. Eine korrekt konfigurierte Firewall zeigt nach außen keine offenen Ports, die nicht bewusst freigegeben sind. Was nicht erreichbar ist, kann nicht angegriffen werden. Das schützt Ihre PVS-Systeme und TI-Konnektor-Infrastruktur vor unautorisierten Zugriffsversuchen.

Zugriff auf interne Dienste. Ein NAS, ein interner Server, eine PVS-Instanz, ein TI-Konnektor – all das soll nicht aus dem Internet erreichbar sein. Die Firewall sorgt dafür, dass diese Dienste intern verfügbar sind, aber von außen unsichtbar bleiben.

Command-and-Control-Kommunikation nach Infektion. Schadsoftware, die sich auf einem Gerät eingenistet hat, muss in der Regel nach außen kommunizieren – um Daten abzuziehen, Befehle zu empfangen oder Ransomware-Schlüssel zu übertragen. Eine Firewall mit ausgehenden Regeln kann diese Kommunikation blockieren oder zumindest sichtbar machen, wenn plötzlich ungewöhnlicher ausgehender Traffic auftritt.[4]

Lateral Movement – Ausbreitung im Netz. Hat ein Angreifer oder eine Schadsoftware ein Gerät kompromittiert, versucht sie in der Regel, sich von dort auf weitere Geräte im Netz auszubreiten. In einem flachen Netz – alle Geräte im selben Segment – ist das einfach. Durch Segmentierung (dazu unten mehr) und Firewall-Regeln zwischen den Segmenten lässt sich diese Ausbreitung erheblich erschweren. Das ist in einer Praxisumgebung besonders wichtig, da ein kompromittiertes Gerät nicht auf den TI-Konnektor oder auf Patientendaten-Speicher zugreifen sollte.

Was eine Firewall nicht verhindert:

Angriffe über erlaubte Verbindungen. Eine Firewall erlaubt in der Regel ausgehenden HTTPS-Verkehr. Phishing-Seiten, manipulierte Downloads und bösartige Inhalte kommen

[4] Diese Funktionalität wird als „Egress Filtering" bezeichnet. Im Heimnetz-Bereich ist sie selten aktiviert, weil Standard-Router sie nicht bieten. In Unternehmensnetzen gehört sie zur Grundkonfiguration. Referenz: NIST SP 800-41 Rev. 1, „Guidelines on Firewalls and Firewall Policy".

genau über diesen Kanal. Die Firewall sieht, dass eine Verbindung zu einer Website aufgebaut wird – aber nicht, ob die Seite schädlich ist. Dafür braucht es zusätzliche Maßnahmen: DNS-Filtering, Browser-Schutz, Antivirussoftware auf dem Gerät.

Fehler des Benutzers. Wenn jemand auf einen Phishing-Link klickt, ein manipuliertes Dokument öffnet oder einem Social-Engineering-Angriff erliegt, hilft die Firewall nur begrenzt weiter.

Verschlüsselte bösartige Inhalte. HTTPS verschlüsselt den Inhalt der Kommunikation – auch wenn die Kommunikation von Schadsoftware stammt. Eine Application Layer Firewall mit SSL-Inspektion kann das analysieren, aber diese Konfiguration ist komplex und für kleine Setups oft unverhältnismäßig.

A.5.3. VLANs und Netzwerksegmentierung: Sicherheit durch Trennung

Die wirkungsvollste Maßnahme gegen die Ausbreitung von Angriffen im eigenen Netz ist die Segmentierung: Das Netz wird in logische Zonen aufgeteilt, die nur über definierte, kontrollierte Wege miteinander kommunizieren können.

Das Konzept dahinter ist das Prinzip minimaler Rechte: Jedes Gerät darf nur mit den Systemen kommunizieren, mit denen es das auch wirklich muss.

Was ist ein VLAN?

Ein VLAN – Virtual Local Area Network – ist eine logische Netzwerktrennung, die auf einem Switch implementiert wird. Obwohl alle Geräte physisch am selben Switch hängen, sehen sie jeweils nur die Geräte in ihrem eigenen VLAN. Aus ihrer Perspektive befinden sie sich in einem getrennten Netz.

Die Trennung ist vollständig: Ein Gerät im VLAN „IoT" kann nicht direkt mit einem Gerät im VLAN „Medizin" kommunizieren – es sei denn, der Datenverkehr wird explizit über eine Firewall geleitet, die diese Kommunikation prüft und gegebenenfalls erlaubt.

Eine sinnvolle Netzwerkstruktur für Arztpraxen

Für eine kleine Praxis oder ein MVZ mit erhöhten Sicherheitsanforderungen reichen mehrere dedizierte Zonen aus:

Zone 1 – Medizin/Klinische Systeme: Laptops der Ärzte, PVS-Terminals, TI-Konnektor, eHBA-Lesegeräte, NAS mit Patientendaten. Vollständiger Internetzugang für berufliche Zwecke (Updates, Online-Konferenzen, KBV-Zugang). Keine Kommunikation mit IoT, Gästen oder Patient*innen-WLAN.

Zone 2 – Verwaltung/Büro: Praxisverwaltungs-PCs, Abrechnungssysteme, Personalcomputer. Moderat restriktiver Internetzugang. Kein direkter Zugriff auf klinische Daten.

Zone 3 – IoT/Medizinische Geräte: Smart-Home-Geräte, Drucker, IP-Kameras, smarte Waagen oder Blutdruckmessgeräte mit Netzanbindung. Internetzugang für Firmware-Updates und Cloud-Dienste (falls notwendig). Kein Zugriff auf Medizin-, Verwaltungs- oder Patientennetzwerk.

*Zone 4 – Gäste/Patient*innen:* WLAN für Besucher und Patienten. Nur Internetzugang. Kein Zugriff auf Arbeitsnetz, medizinische Systeme oder IoT.

Die Firewall sitzt zwischen diesen Zonen und dem Internet sowie zwischen den Zonen untereinander. Sie entscheidet, welcher Traffic zwischen den Zonen und nach außen erlaubt ist. Ein IoT-Gerät, das versucht, mit einem Gerät im Medizin-Netzwerk zu kommunizieren, wird von der Firewall blockiert – selbst wenn es kompromittiert ist.

```
Internet

 [Firewall]
  /   \ \
Med Verw IoT Gäste
```

Diese Struktur bedeutet: Ein kompromittiertes Smart-Home-Gerät kommt nicht ans medizinische Netzwerk. Ein Patient mit einem infizierten Laptop bedroht nur sich selbst. Schadsoftware im Verwaltungsnetzwerk kann nicht unbemerkt auf medizinische Systeme übergreifen.

A.5.4. Consumer-Switch vs. Managed Switch – der Unterschied, der alles ausmacht

VLANs klingen nach einer guten Idee – und sind auch technisch nicht besonders kompliziert. Warum nutzen sie so wenige?

Der häufigste Grund ist Hardware: Ein Standard-Netzwerkswitch aus dem Elektronikmarkt unterstützt keine VLANs.

Consumer-Switches (Unmanaged Switches)

Ein unmanaged Switch macht genau eine Sache: Er verbindet alle Geräte, die an ihm hängen, miteinander – ohne jede Konfigurationsmöglichkeit. Kein Web-Interface, keine VLANs, keine Portpriorisierung. Plug and Play in seiner ursprünglichsten Form. Das ist für einfache Setups vollkommen ausreichend – aber für Netzwerksegmentierung unbrauchbar.

Diese Geräte kosten oft unter 20 Euro und sind in Haushalten weit verbreitet. Das macht sie nicht schlecht, nur begrenzt.

Managed Switches

Ein managed Switch lässt sich konfigurieren: über ein Web-Interface, eine App oder eine Kommandozeile. Er unterstützt VLANs, kann Ports verschiedenen logischen Netzen zuordnen und ermöglicht eine feingranulare Kontrolle über den Datenverkehr zwischen seinen Ports.

Managed Switches sind teurer – einfache Modelle für Praxen und kleine Büros beginnen aber bereits bei 50 bis 80 Euro. Hersteller wie Netgear (Smart Managed Switches der Plus-Linie), TP-Link (TL-SG108E und ähnliche), oder Ubiquiti (UniFi-Linie) bieten Einsteigerlösungen, die für kleine Setups völlig ausreichen.

Wichtig zu wissen: Einen managed Switch richtig zu konfigurieren ist keine Hexerei – aber es ist auch keine Aufgabe, die man ohne Vorbereitung oder Erfahrung mal eben erledigt. Die Konfiguration muss zur Firewall passen, die VLANs müssen korrekt definiert sein, und ein Fehler kann bedeuten, dass plötzlich alle Geräte in derselben Zone landen oder gar kein Zugriff mehr möglich ist.

A.5.5. Die häufigsten Fehler im Umgang mit Firewalls

Selbst wer eine Firewall betreibt, kann sie falsch betreiben. Die häufigsten Fehler in der Praxis:

Ausgehenden Traffic pauschal erlauben. Die Default-Konfiguration vieler Firewalls erlaubt allen ausgehenden Traffic ohne Einschränkung. Das ist bequem – aber verzichtet auf einen erheblichen Schutzmechanismus. Eine sinnvolle Grundregel wäre: Nur bekannte, benötigte ausgehende Verbindungen werden erlaubt. Alles andere wird geloggt und blockiert.

Keine Logs, oder Logs die niemand liest. Eine Firewall erzeugt wertvolle Daten – aber nur, wenn Logging aktiviert ist und jemand hin und wieder hinschaut. Firewall-Logs zeigen Verbindungsversuche, geblockte Pakete, ungewöhnliche Traffic-Muster. Wer seine Logs nie liest, bemerkt Angriffe und Anomalien erst, wenn es zu spät ist.

Veraltete Firmware. Firewalls sind Software – und Software hat Sicherheitslücken. Ein Firewall-System, das seit zwei Jahren kein Update bekommen hat, schützt möglicherweise gegen bekannte Bedrohungen von vor zwei Jahren. Aktuell halten gilt für Firewalls genauso wie für Betriebssysteme und Antivirussoftware.

„Set and forget" – einmal einrichten, nie wieder anfassen. Ein Netz verändert sich: Neue Geräte kommen hinzu, alte werden abgeklemmt, Dienste ändern sich. Firewall-Regeln, die für eine bestimmte Konfiguration erstellt wurden, passen vielleicht nach einem Jahr nicht mehr. Regelmäßige Überprüfung – mindestens einmal jährlich – ist Pflicht.

Zu viele Ausnahmen. Firewall-Regeln werden gelegentlich „schnell mal aufgemacht" – für einen Test, für eine neue Anwendung, für einen Dienst, der plötzlich blockiert wird. Diese temporären Ausnahmen werden selten wieder geschlossen. Mit der Zeit entstehen so Regelsätze mit Dutzenden von Ausnahmen, die niemand mehr überblickt. Jede unnötige Ausnahme ist eine potenzielle Angriffsfläche.

Nur Perimeter-Schutz, keine interne Segmentierung. Viele setzen eine Firewall ans Gateway – zwischen dem eigenen Netz und dem Internet. Das ist wichtig, aber nicht ausreichend. Wer ins Netz gelangt (etwa durch ein kompromittiertes Gerät), findet sich in einem flachen Netz mit direktem Zugriff auf alle anderen Geräte. Interne Segmentierung schränkt den Schaden ein, den ein Angreifer anrichten kann, der es einmal durch das Gateway geschafft hat. In einer Praxisumgebung könnte das bedeuten: Ein kompromittierter Admin-PC könnte sonst auf alle Patientendaten zugreifen – mit Segmentierung nur auf Verwaltungssysteme.

A.5.6. Praktische Empfehlungen für Arztpraxen

Hier sind drei Szenarien, abgestuft nach Aufwand und Schutzwirkung:

Einstieg: OPNsense auf einem Mini-PC

OPNsense ist eine quelloffene Firewall-Software, die kostenlos verfügbar ist und auf günstiger Mini-PC-Hardware läuft. Anbieter wie Protectli, Topton oder Minisforum verkaufen speziell dafür ausgelegte Geräte mit zwei Netzwerkports – ab etwa 150 bis 200 Euro. Die Fritz!Box bleibt als Modem und WLAN-Zugangspunkt erhalten; OPNsense übernimmt den Firewall-Job.

OPNsense bietet stateful Inspection, ausgehende Regeln, VLAN-Unterstützung, DNS-Filtering über pfBlockerNG und detailliertes Logging. Die Einrichtung erfordert etwas Zeit und Einarbeitungsaufwand – oder einen IT-Dienstleister, der das übernimmt. Für kleine Arztpraxen kann das eine wirtschaftliche Lösung sein.

Mittleres Setup: Ubiquiti UniFi

Ubiquiti bietet mit der UniFi-Produktlinie ein integriertes Ökosystem aus Router, Access Points und Switches. Die Dream Machine Pro oder die kleineren Dream Router-Modelle kombinieren Firewall, VLAN-Management und WLAN-Controller in einem Gerät. Managed Switches aus der UniFi-Linie ermöglichen saubere Netzwerksegmentierung.

Das System ist deutlich aufwändiger in der Ersteinrichtung als eine Fritz!Box, aber danach über eine zentrale Web-Oberfläche gut verwaltbar. Kosten für ein kleines Setup: ab 300 bis 400 Euro für Router und einen Switch. Für Praxen mit mehreren Standorten oder MVZ ist das eine skalierbare Lösung.

Pragmatischer Ansatz: Holen Sie sich Hilfe

Das muss kein IT-Großunternehmen sein. Viele lokale IT-Dienstleister und Systemhäuser richten genau solche Setups für kleine Büros und Arztpraxen ein – und zwar zu realistischen Preisen. Einmalige Einrichtungskosten von ein paar Hundert Euro (Hardware plus Arbeitszeit) stehen einem deutlich besserem Sicherheitsniveau gegenüber, das danach weitgehend wartungsfrei läuft.

Ein sauberes Netz einzurichten ist handwerkliches IT-Wissen, das viele lokale Dienstleister beherrschen. Es ist keine Raketenwissenschaft – aber es ist auch kein Job für einen Nachmittag ohne Erfahrung. Wer sagt „Das ist mir zu kompliziert", trifft eine völlig vernünftige Entscheidung, wenn die nächste Handlung ist: jemanden fragen, der das kann.

> **Merksatz:** Eine Firewall ist kein einmaliges Produkt, das man kauft und vergisst – sie ist eine Konfiguration, die gepflegt werden will. Mit der richtigen Unterstützung ist das handhabbar.

A.5.7. Checkliste: Firewalls und Netzwerksegmentierung

- ☐ Ich weiß, welchen Firewall-Typ ich betreibe und was er kann – und was nicht.
- ☐ Ausgehender Traffic wird eingeschränkt oder zumindest geloggt.
- ☐ Firewall-Logs sind aktiviert und werden regelmäßig gesichtet.
- ☐ Firmware und Software der Firewall werden regelmäßig aktualisiert.
- ☐ Firewall-Regeln werden mindestens einmal jährlich überprüft und bereinigt.
- ☐ Mein Netz ist in sinnvolle Zonen segmentiert (mindestens: Medizin, Verwaltung, IoT, Gäste).
- ☐ Der TI-Konnektor und medizinische Systeme sind in einem separaten, stark geschützten Segment isoliert.
- ☐ Ich habe einen managed Switch, wenn ich VLANs betreibe – und keinen unmanaged Consumer-Switch.
- ☐ Die Kommunikation zwischen den Zonen ist explizit konfiguriert – nicht alles ist pauschal erlaubt.
- ☐ Ich habe bei Bedarf professionelle Hilfe für die Einrichtung in Anspruch genommen oder plane das.
- ☐ Patient*innen-WLAN und Gäste-WLAN sind vollständig vom medizinischen Netzwerk getrennt.

B. Technische Grundlagen

Sie müssen die Technik hinter Ihren IT-Maßnahmen nicht kennen, um sie umzusetzen. Aber wer verstehen will, warum bestimmte Dinge so funktionieren wie sie funktionieren – und wer im Fehlerfall nicht blind vor einem Problem steht – findet hier die Antworten. Dieser Anhang erklärt die technischen Konzepte, auf denen viele der im Guide empfohlenen Maßnahmen aufbauen.

Was Sie in diesem Anhang erwartet:

B1 – DNS & Domains – wie es wirklich funktioniert: Was passiert, wenn jemand Ihre Domain eingibt? Wie funktioniert das DNS-System intern, was bedeuten TTL und Propagation wirklich, welche Eintragstypen gibt es – und wie nutzen Sie dieses Wissen, um im Notfall schnell und richtig zu handeln?

B2 – E-Mail-Authentifizierung – SPF, DKIM und DMARC im Detail: Wie die drei Mechanismen zusammenarbeiten, wie Sie sie korrekt konfigurieren, wie Sie Fehler erkennen – und was passiert, wenn DMARC auf „reject" steht und plötzlich Ihre eigenen Mails verschwinden.

B3 – Verschlüsselung – was sie leistet und wo ihre Grenzen sind: Was bei einer Verschlüsselung technisch passiert, was „sicher" wirklich bedeutet, welche Verschlüsselung wogegen schützt – und wo der Schutz aufhört und menschliches Verhalten übernehmen muss.

B.1. DNS & Domains – wie es wirklich funktioniert

Das Hauptkapitel hat die wichtigsten Domain-Fallen und DNS-Grundbegriffe erklärt. Dieser Deep Dive geht tiefer: Wie funktioniert das DNS-System intern, was passiert bei einer Anfrage, was bedeuten TTL und Propagation wirklich – und wie nutzen Sie dieses Wissen, um im Notfall schnell und richtig zu handeln?

B.1.1. Wie eine DNS-Anfrage wirklich funktioniert

Wenn Sie `www.ihrpraxis.de` in den Browser eingeben, passiert folgendes – in Millisekunden:

1. **Lokaler Cache:** Ihr Gerät prüft zuerst seinen eigenen DNS-Cache. Hat es diese Adresse kürzlich schon nachgeschlagen, verwendet es die gespeicherte Antwort direkt.
2. **Recursive Resolver:** Ist keine gespeicherte Antwort vorhanden, fragt Ihr Gerät einen sogenannten Recursive Resolver – in der Regel den DNS-Server Ihres Internetproviders oder einen konfigurierten Dienst wie Quad9 oder Cloudflare. Dieser Resolver übernimmt die eigentliche Arbeit der Auflösung.
3. **Root-Server:** Der Resolver fragt einen der 13 Root-Nameserver weltweit: „Wer ist zuständig für `.de`-Domains?" Die Root-Server kennen nicht die konkreten Adressen, aber sie wissen, welche Server für jede Top-Level-Domain (`.de`, `.com`, `.org` usw.) zuständig sind.
4. **TLD-Nameserver:** Der Resolver fragt den für `.de` zuständigen Nameserver der DENIC: „Wer ist zuständig für `ihrpraxis.de`?" Dieser antwortet mit den Nameservern Ihres Registrars oder DNS-Anbieters.
5. **Autoritativer Nameserver:** Der Resolver fragt Ihren autoritativen Nameserver (den DNS-Server, der Ihre Einträge verwaltet): „Was ist die IP-Adresse von `www.ihrpraxis.de`?" Dieser antwortet mit dem konkreten A-Record.
6. **Antwort zurück:** Der Resolver gibt die IP-Adresse an Ihr Gerät zurück. Ihr Browser baut eine Verbindung zu dieser IP auf.

Warum ist das wichtig? Weil Sie verstehen, wo Sie eingreifen können – und wo nicht. Sie kontrollieren Ihren autoritativen Nameserver (über Ihren Registrar oder DNS-Anbieter). Sie können A-Records, MX-Records und TXT-Records ändern. Aber Sie haben keine Kontrolle über Caches bei Endbenutzern, über andere Resolver oder über Root-Server.

B.1.2. TTL – der Hebel für schnelle Änderungen

Jeder DNS-Eintrag hat einen TTL-Wert (Time to Live) – gemessen in Sekunden. Er gibt an, wie lange ein Resolver oder ein Endgerät die Antwort cachen darf, bevor er erneut nachfragen muss.

Ein typischer TTL-Wert ist 3600 Sekunden (1 Stunde) oder 86400 Sekunden (24 Stunden). Das bedeutet: Wenn Sie einen A-Record ändern, kann es bis zu TTL Sekunden dauern, bis alle Nutzer die neue Adresse sehen – weil alte Antworten noch in Caches stecken.

Der praktische Tipp für geplante Migrationen:

Wenn Sie wissen, dass Sie in einer Woche Ihren Hoster wechseln werden, senken Sie bereits jetzt den TTL-Wert des betroffenen Eintrags auf 300 Sekunden (5 Minuten). Wenn Sie dann tatsächlich umschalten, verbreitet sich die Änderung innerhalb von Minuten – statt Stunden. Nach dem Wechsel können Sie den TTL-Wert wieder auf den Normalwert erhöhen.

Merksatz: TTL ist Ihr Hebel für schnelle Propagation. Senken Sie ihn im Voraus, wenn Sie eine Migration planen.

B.1.3. DNS-Einträge im Detail

Das Hauptkapitel hat die wichtigsten Record-Typen benannt. Hier die vollständige Übersicht für Arztpraxen:

A-Record Verknüpft einen Hostnamen mit einer IPv4-Adresse. `ihrpraxis.de → 203.0.113.10`. Das ist der Eintrag, der Ihre Website erreichbar macht.

AAAA-Record Wie der A-Record, aber für IPv6-Adressen. Viele moderne Hoster unterstützen IPv6 – wenn Ihr Hoster Ihnen eine IPv6-Adresse gibt, tragen Sie sie ein.

CNAME-Record Ein Alias. `www.ihrpraxis.de → ihrpraxis.de`. Statt einer IP-Adresse zeigt der CNAME auf einen anderen Hostnamen. Der Resolver löst dann diesen Hostnamen weiter auf. Wichtig: Ein CNAME darf nicht für die Apex-Domain (die Domain ohne Präfix, also `ihrpraxis.de`) verwendet werden – nur für Subdomains.

MX-Record Steuert die E-Mail-Zustellung. Er hat zwei Felder: Priorität und Ziel-Hostname. Beispiel: `10 mail.ihrpraxis.de`. Mehrere MX-Records mit unterschiedlichen Prioritäten sind möglich – E-Mails werden zuerst an den Server mit der niedrigsten Prioritätszahl gesendet; fällt dieser aus, an den nächsten.

TXT-Record Freitext-Feld, das für verschiedene Zwecke genutzt wird: SPF, DKIM, DMARC, Domain-Verifikation bei Google/Microsoft und mehr. Eine Domain kann mehrere TXT-Records haben.

NS-Record Gibt die autoritativen Nameserver für die Domain an. Diese Einträge werden beim Registrar gesetzt und bestimmen, welcher DNS-Anbieter Ihre Einträge verwaltet. Wenn Sie Ihren DNS-Anbieter wechseln, ändern Sie diese Einträge.

SOA-Record Start of Authority – technischer Verwaltungseintrag, der automatisch gesetzt wird. Enthält u. a. den primären Nameserver und die E-Mail-Adresse des Zone-Administrators. Wird in der Regel nicht manuell bearbeitet.

B.1.4. Registrar vs. DNS-Anbieter vs. Hoster – drei verschiedene Rollen

Ein häufiger Irrtum: Viele glauben, Registrar und DNS-Anbieter sind dasselbe. Das müssen sie nicht sein.

Registrar: Das Unternehmen, bei dem Sie Ihre Domain registriert haben und das die Inhaberschaft verwaltet. IONOS, Strato, united-domains, Hetzner, Namecheap. Der Registrar ist für die NS-Records zuständig – er bestimmt, welche Nameserver für Ihre Domain autoritativ sind.

DNS-Anbieter: Das Unternehmen, dessen Nameserver Ihre DNS-Einträge (A, MX, TXT usw.) verwalten. Oft ist das der Registrar – aber es kann auch ein separater Dienst sein,

zum Beispiel Cloudflare DNS, die eine schnelle und zuverlässige DNS-Infrastruktur als kostenlose Ergänzung anbieten.

Hoster: Das Unternehmen, auf dessen Servern Ihre Website liegt. Der A-Record zeigt auf die IP-Adresse des Hosters.

Warum die Trennung sinnvoll ist: Wenn Ihr Hoster ausfällt oder Sie ihn wechseln, ändern Sie nur den A-Record beim DNS-Anbieter. Ihre Domain bleibt wo sie ist. Wenn Ihr DNS-Anbieter Probleme hat, können Sie die Nameserver beim Registrar auf einen anderen Anbieter umstellen. Jede Ebene ist unabhängig austauschbar.

B.1.5. DNSSEC – Schutz vor gefälschten DNS-Antworten

DNSSEC (DNS Security Extensions) ist ein Sicherheitsmechanismus, der DNS-Antworten mit digitalen Signaturen versieht. Er schützt vor DNS-Spoofing: einem Angriff, bei dem ein Angreifer gefälschte DNS-Antworten in den Cache eines Resolvers einschleust und Nutzer so auf gefälschte Websites umleitet.

Ohne DNSSEC hat ein Resolver keine Möglichkeit zu verifizieren, ob eine DNS-Antwort echt ist oder von einem Angreifer gefälscht wurde. Mit DNSSEC wird jede Antwort mit einem kryptografischen Schlüssel signiert, und der Resolver kann die Signatur verifizieren.

Für Arztpraxen: DNSSEC wird von vielen Registraren angeboten – bei IONOS, Strato und anderen kann es mit wenigen Klicks aktiviert werden. Der Nutzen ist real: DNS-Spoofing wird erheblich erschwert.

Allerdings ist DNSSEC nicht immer kostenlos. Einige Registrare – darunter IONOS – berechnen für DNSSEC einen Aufpreis pro Domain. Das ist kein Grund, DNSSEC grundsätzlich abzulehnen, aber es lohnt sich, Kosten und Nutzen abzuwägen: Für eine Domain, über die Sie Patientenkommunikation und geschäftskritische Dienste abwickeln, ist der Aufpreis gut investiert. Für eine rein informative Nebendomain mit wenig Traffic ist die Entscheidung weniger eindeutig. Prüfen Sie die aktuellen Konditionen Ihres Registrars und entscheiden Sie bewusst.

> **Hinweis:** DNSSEC muss auf beiden Seiten konsistent sein – beim Registrar (der das DS-Record einträgt) und beim DNS-Anbieter (der die Zone signiert). Wenn Sie DNS-Anbieter wechseln, muss DNSSEC neu eingerichtet werden; ein inkonsistenter Zustand macht Ihre Domain unerreichbar.

B.1.6. Domain-Hijacking: Wie Domains gestohlen werden

Domain-Hijacking ist der Diebstahl einer Domain – entweder durch Übernahme des Registrar-Kontos oder durch betrügerischen Transfer. Es ist selten, aber wenn es passiert, hat es sofortige und weitreichende Konsequenzen: Website weg, E-Mail weg, digitale Identität weg.

Die häufigsten Angriffswege:

Kompromittiertes Registrar-Konto: Der Angreifer gelangt über Phishing oder ein schwaches Passwort in Ihr Registrar-Konto und ändert die Nameserver oder initiiert einen Transfer.

Social Engineering beim Registrar: Angreifer geben sich gegenüber dem Support des Registrars als Kontoinhaber aus und überzeugen ihn, Zugang zu gewähren oder einen Transfer zu genehmigen.

Ablauf der Domain: Eine vergessene Domain läuft ab, wird sofort von Domain-Squattern registriert.

Schutzmaßnahmen: - Starkes, einzigartiges Passwort und 2FA für das Registrar-Konto – das ist der wichtigste Schutz. - **Transfer-Lock aktivieren:** Die meisten Registrare bieten einen Transfer-Lock, der verhindert, dass die Domain ohne explizite Freigabe zu einem anderen Registrar transferiert werden kann. Aktivieren Sie ihn. - **WHOIS Privacy:** Viele Registrare bieten an, Ihre persönlichen Kontaktdaten im WHOIS-Eintrag zu verbergen. Das verhindert zwar keinen Angriff, reduziert aber die für Social Engineering verfügbaren Informationen.

B.1.7. Checkliste: DNS & Domains im Detail

- ☐ Ich verstehe den Unterschied zwischen Registrar, DNS-Anbieter und Hoster – und weiß, welche Rolle bei meiner Praxis wer übernimmt.
- ☐ Der Transfer-Lock ist für meine Domain aktiviert.
- ☐ Mein Registrar-Konto ist mit 2FA gesichert.
- ☐ Ich kenne den TTL-Wert meiner wichtigsten DNS-Einträge und weiß, wie ich ihn vor einer geplanten Migration senken kann.
- ☐ Ich habe alle aktuellen DNS-Einträge dokumentiert (Screenshot oder Export).
- ☐ DNSSEC ist aktiviert, sofern Registrar und DNS-Anbieter es unterstützen.
- ☐ WHOIS Privacy ist aktiviert.
- ☐ Ich weiß, wie ich im Notfall Nameserver, A-Record und MX-Record meiner Domain ändern kann.

B.2. E-Mail-Authentifizierung – SPF, DKIM und DMARC im Detail

Das Hauptkapitel hat SPF, DKIM und DMARC als Schutz vor Missbrauch eingeführt. Dieser Deep Dive erklärt, wie die drei Mechanismen intern zusammenarbeiten, wie Sie sie korrekt konfigurieren, wie Sie Fehler erkennen – und was passiert, wenn DMARC auf „reject" steht.

B.2.1. Das Problem: Warum E-Mail-Absender gefälscht werden können

Das E-Mail-Protokoll (SMTP) wurde in den 1970er Jahren entworfen – zu einer Zeit, als Vertrauen im Netz noch als selbstverständlich galt. Das Protokoll sieht keine eingebaute Authentifizierung vor: Jeder Server kann eine E-Mail mit einer beliebigen Absenderadresse versenden. `info@ihrpraxis.de` als Absender bedeutet technisch nichts – es ist nur ein Textfeld.

Das ist die Grundlage für E-Mail-Spoofing: Angreifer versenden E-Mails mit Ihrer Absenderadresse, ohne Zugang zu Ihrem Konto zu haben. Ihre Patienten erhalten dann gefälschte Rechnungen oder Phishing-Mails, scheinbar von Ihrer Praxis – und Sie wissen davon nichts.

SPF, DKIM und DMARC sind drei unabhängige, aber zusammenwirkende Mechanismen, die dieses Problem adressieren. Sie wurden nachträglich ins DNS-System eingebaut und sind heute der Standard.

B.2.2. SPF – wer darf in meinem Namen senden?

Sender Policy Framework (SPF) ist ein DNS-TXT-Record, der festlegt, welche Server berechtigt sind, E-Mails für Ihre Domain zu versenden.

Aufbau eines SPF-Records:

```
v=spf1 include:_spf.google.com include:_spf.mimecast.com ~all
```

- `v=spf1` – Kennzeichnung als SPF-Record
- `include:` – Erlaubt alle Server, die im SPF-Record des angegebenen Dienstes aufgeführt sind (hier: Google Workspace und Mimecast)
- `ip4:` / `ip6:` – Erlaubt eine konkrete IP-Adresse oder einen IP-Bereich
- `a` – Erlaubt den Server, auf den der A-Record der Domain zeigt
- `mx` – Erlaubt die Server, die als MX-Records eingetragen sind
- `~all` – Soft Fail: E-Mails von nicht autorisierten Servern werden als verdächtig markiert, aber nicht abgelehnt
- `-all` – Hard Fail: E-Mails von nicht autorisierten Servern werden abgelehnt

Praktischer Hinweis: Viele E-Mail-Anbieter (Google Workspace, Microsoft 365, Fastmail) liefern den exakten SPF-Record, den Sie eintragen müssen. Kopieren Sie ihn genau – und passen Sie ihn an, wenn Sie mehrere Dienste nutzen, die E-Mails in Ihrem Namen senden (z. B. ein Buchungssystem für Patienten oder ein CRM-System).

Häufiger Fehler: Für eine Domain darf es nur **einen** SPF-Record geben. Wenn Sie mehrere TXT-Records mit `v=spf1` haben, ist der SPF-Record ungültig. Mehrere Dienste werden durch mehrere `include:`-Direktiven in einem einzigen Record kombiniert.

Prüfen: `mxtoolbox.com/spf.aspx` zeigt Ihnen, ob Ihr SPF-Record korrekt ist und welche IP-Adressen er autorisiert.

B.2.3. DKIM – eine Unterschrift unter jeder E-Mail

DomainKeys Identified Mail (DKIM) ergänzt SPF um eine kryptografische Signatur: Jede ausgehende E-Mail wird vom sendenden Server mit einem privaten Schlüssel signiert. Der empfangende Server kann die Signatur mit dem öffentlichen Schlüssel verifizieren, der im DNS Ihrer Absenderdomain hinterlegt ist.

Was DKIM leistet: - Beweist, dass die E-Mail tatsächlich von einem Server Ihrer Domain gesendet wurde (und nicht von einem gefälschten Absender). - Beweist, dass der Inhalt der E-Mail auf dem Transportweg nicht verändert wurde.

Wie DKIM im DNS aussieht:

DKIM-Einträge sind TXT-Records an einer spezifischen Subdomain nach dem Schema `selector._domainkey.ihrpraxis.de`. Der „Selector" ist ein frei wählbarer Name, der es ermöglicht, mehrere DKIM-Schlüssel gleichzeitig zu betreiben.

```
google._domainkey.ihrpraxis.de  TXT  "v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb..."
```

Der lange String nach `p=` ist der öffentliche Schlüssel.

Was Sie tun müssen: Die meisten E-Mail-Anbieter generieren das Schlüsselpaar automatisch und zeigen Ihnen den genauen TXT-Record, der eingetragen werden muss. Sie tragen ihn bei Ihrem DNS-Anbieter ein – fertig. Den privaten Schlüssel verwahrt der E-Mail-Anbieter; Sie müssen ihn nicht kennen.

Mehrere Dienste: Wenn Sie neben Ihrem Hauptpostfach auch ein Buchungssystem oder Laborergebnis-System nutzen (die E-Mails versenden), hat dieses seinen eigenen DKIM-Selector und eigenen TXT-Record. Beide können gleichzeitig existieren, da sie unterschiedliche Subdomains nutzen.

Prüfen: `mxtoolbox.com/dkim.aspx` – geben Sie Domain und Selector ein, um die Konfiguration zu prüfen.

B.2.4. DMARC – die Policy, die alles zusammenbringt

Domain-based Message Authentication, Reporting & Conformance (DMARC) ist der Dirigent: Er legt fest, was mit E-Mails passiert, die SPF oder DKIM nicht bestehen – und sorgt dafür, dass Sie über Verstöße informiert werden.

DMARC führt das Konzept des „Alignment" ein: Es reicht nicht, dass SPF oder DKIM irgendwie passt – der geprüfte Absender muss mit dem im `From:`-Header sichtbaren Absender übereinstimmen. Das schließt eine Angriffstechnik, bei der Angreifer einen anderen, legitimen Absender für SPF/DKIM verwenden, aber im `From:`-Header Ihre Domain anzeigen.

Aufbau eines DMARC-Records:

```
_dmarc.ihrpraxis.de  TXT  "v=DMARC1; p=quarantine; rua=mailto:dmarc@ihrpraxis.de; pct=100
```

- `v=DMARC1` – Kennzeichnung
- `p=` – Die Policy: `none` (nur beobachten), `quarantine` (in Spam verschieben), `reject` (ablehnen)
- `rua=` – Adresse, an die Aggregate-Reports geschickt werden (tägliche Zusammenfassung)
- `ruf=` – Adresse für Forensic-Reports (detaillierte Berichte über einzelne Verstöße) – optional
- `pct=` – Prozentsatz der E-Mails, auf die die Policy angewendet wird (100 = alle)

Die drei Policy-Stufen – und warum Sie nicht sofort auf „reject" gehen sollten:

`p=none` – Monitoring-Modus. Keine E-Mail wird abgelehnt, aber Sie erhalten Reports über alle E-Mails, die in Ihrem Namen versendet werden – legitime und illegitime. Das ist der richtige Einstieg: Sie beobachten zuerst, welche Dienste E-Mails in Ihrem Namen senden, und stellen sicher, dass alle in SPF und DKIM konfiguriert sind.

`p=quarantine` – E-Mails, die SPF/DKIM nicht bestehen, landen beim Empfänger im Spam-Ordner. Ein guter Zwischenschritt.

`p=reject` – E-Mails, die SPF/DKIM nicht bestehen, werden vom empfangenden Server vollständig abgelehnt. Das ist die stärkste Schutzmaßnahme – aber wenn ein legitimer Dienst (z. B. ein Buchungssystem für Patiententermine oder ein Laborverbindungsdienst) nicht korrekt in SPF/DKIM konfiguriert ist, werden dessen E-Mails ebenfalls abgelehnt.

Empfohlene Vorgehensweise: 1. Starten Sie mit `p=none` und einer `rua=`-Adresse. 2. Werten Sie die Reports aus – entweder manuell oder mit einem kostenlosen Tool wie `dmarcian.com` oder `dmarc.postmarkapp.com`. 3. Stellen Sie sicher, dass alle legitimen Absender in SPF und DKIM konfiguriert sind. 4. Wechseln Sie zu `p=quarantine`, beobachten Sie weiter. 5. Wechseln Sie zu `p=reject`, wenn Sie sicher sind, dass alle legitimen Dienste korrekt konfiguriert sind.

B.2.5. DMARC-Reports lesen

Die täglichen Aggregate-Reports kommen als XML-Datei per E-Mail. Sie sind nicht für direkte Lektüre gedacht – ein Tool wie `dmarc.postmarkapp.com` (kostenlos, ohne Registrierung) oder `dmarcian.com` (kostenloser Einstieg) visualisiert sie lesbar.

Was Sie in den Reports sehen: - Welche IP-Adressen E-Mails in Ihrem Namen gesendet haben - Ob SPF und DKIM bestanden wurden - Wie viele E-Mails von welchem Dienst kamen

Das ist wertvoll: Sie sehen nicht nur Angriffe, sondern auch legitime Dienste, die Sie vielleicht vergessen haben zu konfigurieren – zum Beispiel ein Buchungssystem, das Bestätigungsmails in Ihrem Namen sendet.

B.2.6. Zusammenspiel der drei Mechanismen

SPF, DKIM und DMARC ergänzen sich – keiner ersetzt den anderen:

Mechanismus	Was er prüft	Was er nicht abdeckt
SPF	Ob der sendende Server autorisiert ist	Ob der Inhalt verändert wurde; Weiterleitungen
DKIM	Ob Inhalt und Absender authentisch sind	Ob der Server überhaupt senden darf
DMARC	Policy-Durchsetzung und Alignment	Nichts – er koordiniert SPF und DKIM

Warum SPF alleine nicht reicht: Bei E-Mail-Weiterleitungen (z. B. wenn ein Patient seine E-Mail weiterleitet) schlägt SPF oft fehl, weil der weiterleitende Server nicht im SPF-Record steht. DKIM überlebt Weiterleitungen in der Regel, weil die Signatur am Inhalt hängt.

Warum DKIM alleine nicht reicht: DKIM prüft nicht, ob der sendende Server legitim E-Mails für die Domain senden darf. Ein Angreifer könnte seinen eigenen DKIM-Schlüssel für eine andere Domain nutzen.

Erst zusammen sind sie stark: DMARC mit `p=reject` und korrektem SPF + DKIM macht E-Mail-Spoofing Ihrer Domain praktisch unmöglich.

B.2.7. Checkliste: E-Mail-Authentifizierung

- ☐ SPF-Record ist eingetragen und korrekt – geprüft mit mxtoolbox.com.
- ☐ Alle Dienste, die E-Mails in meinem Namen versenden (E-Mail-Anbieter, Buchungssystem, Laborverbindung), sind im SPF-Record aufgeführt.
- ☐ Es gibt nur einen SPF-Record für meine Domain.
- ☐ DKIM ist für alle sendenden Dienste eingerichtet und die TXT-Records sind eingetragen.
- ☐ DMARC ist eingerichtet – mindestens mit `p=none` und einer `rua=`-Adresse.
- ☐ Ich werte DMARC-Reports aus – entweder direkt oder mit einem Visualisierungstool.
- ☐ Ich habe einen Plan, schrittweise zu `p=quarantine` und `p=reject` zu wechseln.

B.3. Verschlüsselung – was sie leistet und wo ihre Grenzen sind

Das Hauptkapitel hat erklärt, wie Sie Geräte, NAS und Cloud-Speicher verschlüsseln. Dieser Deep Dive geht tiefer: Was passiert bei einer Verschlüsselung technisch, was bedeutet „sicher" wirklich, wo hört der Schutz auf – und welche Verschlüsselung schützt wogegen?

B.3.1. Was Verschlüsselung tut – und was nicht

Verschlüsselung macht Daten für jeden unlesbar, der nicht im Besitz des richtigen Schlüssels ist. Eine verschlüsselte Datei, die in fremde Hände gerät, ist wertloser Datenmüll – ohne den Schlüssel nicht zu entschlüsseln, auch nicht mit erheblichem Rechenaufwand, wenn die Verschlüsselung korrekt implementiert ist.

Das ist eine mächtige Eigenschaft. Aber Verschlüsselung hat klare Grenzen:

Was Verschlüsselung schützt: - Daten auf einem gestohlenen oder verlorenen Gerät (Festplattenverschlüsselung) - Daten auf einem verlorenen USB-Stick oder einer externen Festplatte - Daten beim Transport über das Internet (TLS/HTTPS) - Daten in der Cloud vor Zugriff durch den Anbieter (clientseitige Verschlüsselung)

Was Verschlüsselung nicht schützt: - Daten auf einem entsperrten, eingeschalteten Gerät – ist das Gerät entsperrt, ist der Schlüssel aktiv, und wer Zugang zum Gerät hat, hat Zugang zu den Daten - Daten vor Malware auf demselben Gerät – Schadsoftware kann entschlüsselte Daten im laufenden Betrieb abgreifen - Daten vor einem schwachen oder kompromittierten Passwort - Metadaten – Verschlüsselung verbirgt den Inhalt, aber nicht unbedingt, dass zwei Parteien kommunizieren

> **Merksatz:** Verschlüsselung schützt Daten im Ruhezustand und auf dem Transportweg – nicht im aktiven Betrieb. Ein entsperrtes Gerät ist ein entschlüsseltes Gerät.

B.3.2. Symmetrische vs. asymmetrische Verschlüsselung

Es gibt zwei grundlegende Typen von Verschlüsselung, die in der Praxis oft kombiniert werden.

Symmetrische Verschlüsselung Sender und Empfänger nutzen denselben Schlüssel – zum Ver- und Entschlüsseln. Der wichtigste Standard ist AES (Advanced Encryption Standard), in der Variante AES-256 (256-Bit-Schlüssel). AES-256 gilt als praktisch unknackbar – mit heutiger Technik würde ein Brute-Force-Angriff Milliarden von Jahren dauern.

Symmetrische Verschlüsselung ist schnell und effizient – ideal für große Datenmengen. Das Problem: Wie übergeben Sie den gemeinsamen Schlüssel sicher an den Empfänger, ohne dass ein Angreifer ihn abfängt?

Asymmetrische Verschlüsselung Hier gibt es zwei Schlüssel: einen öffentlichen Schlüssel (den jeder kennen darf) und einen privaten Schlüssel (der geheim bleibt). Was mit dem öffentlichen Schlüssel verschlüsselt wird, kann nur mit dem privaten Schlüssel entschlüsselt werden – und umgekehrt.

Das löst das Schlüsselaustausch-Problem: Sie veröffentlichen Ihren öffentlichen Schlüssel. Jeder kann Ihnen damit verschlüsselte Nachrichten senden. Nur Sie können sie mit Ihrem privaten Schlüssel lesen.

Asymmetrische Verschlüsselung ist rechenintensiv – deshalb wird sie in der Praxis meist nur für den sicheren Austausch eines symmetrischen Schlüssels genutzt (Hybridverschlüsselung). Das ist genau, was TLS/HTTPS macht: Asymmetrische Verschlüsselung für den

Schlüsselaustausch, dann symmetrische Verschlüsselung für den eigentlichen Datentransport.

B.3.3. Festplattenverschlüsselung: Was BitLocker, FileVault und LUKS wirklich tun

BitLocker (Windows), FileVault (macOS) und LUKS (Linux) sind Vollverschlüsselungslösungen für Festplatten. Sie verschlüsseln den gesamten Inhalt eines Laufwerks – Betriebssystem, Programme, Daten.

Wie es funktioniert: Beim Einschalten fragt das System nach dem Entsperrfaktor – einem Passwort, einer PIN, oder einem Hardware-Token (TPM). Erst dann wird der Verschlüsselungsschlüssel im Arbeitsspeicher bereitgestellt und das System kann starten. Solange das Laufwerk gesperrt ist, sind alle Daten darauf unlesbar – auch wenn jemand die Festplatte ausbaut und in einen anderen Computer einbaut.

Der TPM-Chip und seine Tücken BitLocker nutzt standardmäßig den TPM-Chip (Trusted Platform Module) des Computers – ein kleiner Sicherheitschip auf dem Mainboard, der den Verschlüsselungsschlüssel sicher verwahrt. Das hat einen praktischen Vorteil: Der Computer startet ohne Passwortabfrage, der TPM gibt den Schlüssel automatisch frei, wenn er erkennt, dass die Hardware unverändert ist.

Das hat aber auch eine Schwäche: Wer das entsperrte Gerät in Händen hält, hat Zugang zu allen Daten – ohne jede Hürde. Für ein Gerät, das in der Praxis bleibt, ist das akzeptabel. Für ein Laptop, das regelmäßig mitgenommen wird, sollte zusätzlich eine **Pre-Boot-PIN** konfiguriert werden: BitLocker fragt dann beim Start nach einer PIN, bevor es den TPM-Chip aktiviert.

Der BitLocker-Wiederherstellungsschlüssel Bei der Aktivierung von BitLocker wird ein 48-stelliger Wiederherstellungsschlüssel generiert. Dieser Schlüssel ist die einzige Möglichkeit, das Laufwerk zu entsperren, wenn das Passwort vergessen wurde, der TPM-Chip defekt ist oder das Gerät getauscht wird.

Standardmäßig lädt Windows diesen Schlüssel in das mit dem Windows-Konto verknüpfte Microsoft-Konto hoch – also in die Microsoft-Cloud. Das ist praktisch, bedeutet aber: Microsoft hat technisch Zugang zu Ihrem Verschlüsselungsschlüssel. Für Berufsgeheimnisträger und sensible Patientendaten ist das kritisch.

Empfehlung: Exportieren Sie den Wiederherstellungsschlüssel und speichern Sie ihn sicher – in Ihrem Passwort-Manager, im Notfalldokument oder auf einem verschlüsselten USB-Stick. Entfernen Sie ihn anschließend aus dem Microsoft-Konto, wenn Sie das Risiko des Cloud-Uploads vermeiden wollen.

B.3.4. Ende-zu-Ende-Verschlüsselung (E2EE)

Ende-zu-Ende-Verschlüsselung bedeutet, dass Daten bereits beim Sender verschlüsselt werden und erst beim Empfänger entschlüsselt werden. Kein Server, kein Anbieter, kein Dritter dazwischen kann die Inhalte lesen.

Messenger: Signal, WhatsApp (für Inhalte, nicht für Metadaten) und iMessage nutzen E2EE standardmäßig. Telegram verschlüsselt nur in „Secret Chats" Ende-zu-Ende – normale Chats liegen auf Telegrams Servern unverschlüsselt.

E-Mail: Standard-E-Mail ist nicht Ende-zu-Ende-verschlüsselt. TLS schützt den Transport zwischen Servern – aber der E-Mail-Anbieter kann auf Ihre Mails zugreifen. Echte E2EE für E-Mail erfordert PGP (Pretty Good Privacy) oder S/MIME – beide sind in der Praxis umständlich und setzen voraus, dass beide Seiten die Technologie nutzen.

Cloud-Speicher: Die meisten Cloud-Dienste verschlüsseln Daten in Ruhe und auf dem Transport – aber mit Schlüsseln, die der Anbieter kontrolliert. Das schützt gegen externe Angreifer, aber nicht gegen den Anbieter selbst oder gegen behördlichen Zugriff. Clientseitige Verschlüsselung (Cryptomator, Boxcryptor-Nachfolger, Backup-Software wie Arq oder Duplicati) verschlüsselt die Daten auf Ihrem Gerät, bevor sie die Cloud erreichen – der Anbieter sieht nur verschlüsselte Pakete.

B.3.5. TLS/HTTPS – Verschlüsselung im Web

Wenn Sie eine Website mit `https://` aufrufen, ist die Verbindung durch TLS (Transport Layer Security) verschlüsselt. Das schützt die übertragenen Daten vor Abhören im Netz.

Was das grüne Schloss bedeutet – und was nicht: Das Schloss-Symbol im Browser bedeutet, dass die Verbindung verschlüsselt ist. Es bedeutet **nicht**, dass die Website vertrauenswürdig ist oder keine Malware enthält. Auch Phishing-Websites können HTTPS nutzen – und tun es zunehmend.

HSTS (HTTP Strict Transport Security): Wenn Ihre Website vorhanden ist, stellen Sie sicher, dass HTTPS erzwungen wird – durch eine 301-Weiterleitung von HTTP auf HTTPS und einen HSTS-Header. Das verhindert Downgrade-Angriffe, bei denen ein Angreifer versucht, die Verbindung auf unverschlüsseltes HTTP zurückzustufen.

Zertifikate: HTTPS-Zertifikate werden von Zertifizierungsstellen (CAs) ausgestellt. Let's Encrypt stellt kostenlose Zertifikate aus, die von allen Browsern anerkannt werden. Die meisten modernen Hoster aktivieren Let's Encrypt-Zertifikate automatisch.

B.3.6. Quantencomputer und die Zukunft der Verschlüsselung

Ein Thema, das in IT-Sicherheitskreisen zunehmend diskutiert wird: Quantencomputer könnten in Zukunft bestimmte Verschlüsselungsverfahren brechen – insbesondere asymmetrische Verfahren wie RSA und ECC, die auf mathematischen Problemen basieren, die Quantencomputer effizient lösen könnten.

Was das für Sie heute bedeutet: Noch nichts. Praktisch einsatzfähige Quantencomputer, die aktuelle Verschlüsselung brechen können, gibt es nicht – und werden es auf absehbare Zeit nicht geben. Die Branche arbeitet bereits an quantensicheren Algorithmen (Post-Quantum Cryptography), die NIST hat 2024 erste Standards verabschiedet.

Das relevanteste Risiko für heute ist das sogenannte „Harvest now, decrypt later"-Szenario: Angreifer sammeln heute verschlüsselte Daten und hoffen, sie in zehn oder zwanzig Jahren mit Quantencomputern entschlüsseln zu können. Für die meisten Arztpraxen ist das kein realistisches Bedrohungsszenario.

B.3.7. Checkliste: Verschlüsselung – technisches Verständnis

- ☐ Alle meine Geräte sind vollverschlüsselt (BitLocker, FileVault, LUKS).
- ☐ Mein Laptop hat eine Pre-Boot-PIN konfiguriert, wenn es regelmäßig außer Haus mitgenommen wird.
- ☐ Der BitLocker-Wiederherstellungsschlüssel ist sicher gespeichert – nicht nur in der Microsoft-Cloud.
- ☐ Cloud-Backups nutzen clientseitige Verschlüsselung – der Anbieter hat keinen Zugang zu meinen Daten.
- ☐ Meine Website nutzt HTTPS mit einem gültigen Zertifikat und erzwingt HTTPS via Weiterleitung.
- ☐ Für sensible Kommunikation nutze ich Messenger mit Ende-zu-Ende-Verschlüsselung (Signal, iMessage).
- ☐ Ich verstehe, dass Verschlüsselung nur im Ruhezustand und Transport schützt – nicht gegen Malware oder auf entsperrten Geräten.

C. Vorlagen & Muster

Wissen ist gut – fertige Ausgangspunkte sind besser. Dieser Anhang enthält Musterbefüllungen und Vorlagen, die Sie direkt für Ihre eigene Praxissituation anpassen können. Sie sind als Arbeitsmaterial gedacht, nicht als fertige Lösung: Prüfen Sie jeden Abschnitt auf Vollständigkeit und Richtigkeit für Ihre konkrete Situation, und lassen Sie kritische Dokumente im Zweifelsfall von einem auf Medizinrecht spezialisierten Anwalt gegenlesen.

Was Sie in diesem Anhang erwartet:

C1 – VVT-Musterbefüllungen für typische Verarbeitungstätigkeiten in Arztpraxen: Konkrete Beispieleinträge für das Verzeichnis von Verarbeitungstätigkeiten (VVT) nach Art. 30 DSGVO – für fünf typische Verarbeitungsbereiche in Arztpraxen und MVZ: Patientenbehandlung & Dokumentation, Abrechnung, Kommunikation, Praxis-Website und Personalverwaltung. Jedes Muster enthält Verarbeitungszweck, Rechtsgrundlage, betroffene Personengruppen, Datenkategorien, Löschfristen und Hinweise auf typische Auftragsverarbeiter. Besondere Beachtung der Gesundheitsdaten nach Art. 9 DSGVO, der §§ 630f BGB und § 203 StGB.

C.1. VVT-Musterbefüllungen für Arztpraxen und MVZ

Das Hauptkapitel hat erklärt, was ein Verzeichnis von Verarbeitungstätigkeiten (VVT) ist, warum es Pflicht ist und wie man es aufbaut. Dieser Anhang liefert konkrete Musterbefüllungen für fünf typische Verarbeitungsbereiche in Arztpraxen und MVZ: Patientenbehandlung & Dokumentation, Abrechnung, Kommunikation, Praxis-Website und Personalverwaltung.

Alle Muster sind Ausgangspunkte – keine fertigen Dokumente. Prüfen Sie jeden Eintrag auf Ihre konkrete Situation: Welche PVS-Systeme nutzen Sie tatsächlich? Welche Laborpartner, Kliniken oder Ärzte sind Empfänger? Welche Auftragsverarbeiter sind eingebunden? Welche Rechtsgrundlage passt wirklich? Ergänzen Sie, was fehlt, und streichen Sie, was nicht zutrifft.

Für alle Muster gilt: Die technischen und organisatorischen Maßnahmen (TOMs) werden als Verweis auf ein separates TOM-Dokument behandelt – was dort stehen sollte, ergibt sich aus den Maßnahmen in den Teilen 2 und 6 dieses Guides. Alle Muster berücksichtigen Art. 9 DSGVO (Gesundheitsdaten), § 630f BGB (10-jährige Aufbewahrungspflicht) und § 203 StGB (Berufsgeheimnis).

C.1.1. Muster 1: Patientenbehandlung & Dokumentation

Verantwortliche/r: [Name Praxis/MVZ, Adresse, E-Mail] **Stand:** [Datum]

Verarbeitungstätigkeit 1: Patientenverwaltung und Behandlungsdokumentation

Pflichtangabe	Inhalt
Zweck	Anbahnung und Durchführung von Patientenbehandlungen; Dokumentation von Anamnese, Diagnose, Therapie und Befunden gemäß ärztlicher Dokumentationspflicht; Erinnerungshilfe für Folgebehandlungen; Sicherung der Behandlungsqualität
Rechtsgrundlage	Art. 9 Abs. 2 lit. h DSGVO (Gesundheitsversorgung) i.V.m. Art. 6 Abs. 1 lit. c DSGVO (rechtliche Verpflichtung durch § 630f BGB und ärztliche Dokumentationspflicht); § 203 StGB (Berufsgeheimnis)
Betroffene Personen	Patienten (natürliche Personen)
Datenkategorien	Name, Vorname, Geburtsdatum, Geschlecht, Adresse, Kontaktdaten (Telefon, E-Mail); Versicherungsdaten; Medizinische Anamnese, Beschwerden, Diagnosen, Befunde, Diagnose-Codes (ICD-10); Behandlungsnotizen, durchgeführte Maßnahmen, Medikationen, Allergien, Unverträglichkeiten; Laborergebnisse, Bildgebung, Befundbriefe (als Gesundheitsdaten nach Art. 9 DSGVO); Patienteneinwilligungen
Empfänger	PVS-Software (Anbieter: _____) als Auftragsverarbeiter; überweisende/übernehmende Ärzte und Fachkliniken (mit Schweigepflichtentbindung); Labore und Radiologien (mit Schweigepflichtentbindung); behandelnde Psychotherapeuten oder Fachärzte (mit Schweigepflichtentbindung); ggf. Krankenhaus zur Aufnahme (mit Schweigepflichtentbindung)

Pflichtangabe	Inhalt
Drittland	Nein – PVS-Daten müssen auf deutschen/europäischen Servern gespeichert sein. US-Anbieter für Gesundheitsdaten sind datenschutzrechtlich nicht zulässig (kein angemessenes Schutzniveau nach Art. 45 DSGVO). EU-US Data Privacy Framework ist für Gesundheitsdaten nicht ausreichend.
Speicherdauer	Mindestens 10 Jahre nach Abschluss der Behandlung (§ 630f BGB) oder nach Tod des Patienten; Abrechnungsunterlagen: 10 Jahre (§ 147 AO); archivierte Unterlagen: nach Ablauf der Aufbewahrungsfrist dem Patienten zurück geben oder sicher vernichten
TOMs	Siehe TOM-Dokument – besonderer Hinweis: Verschlüsselung der Patientenakte ist bei Gesundheitsdaten zwingend, nicht optional (Art. 32 DSGVO, KBV-Sicherheitsrichtlinie); Zugang nur für berechtigtes Personal auf Need-to-know-Basis; Anmeldung mit individuellem Passwort und Zwei-Faktor-Authentifizierung; Audit-Logging aller Zugriffe

---

Verarbeitungstätigkeit 2: Terminverwaltung und Terminbuchung

Pflichtangabe	Inhalt
Zweck	Verwaltung und Koordination von Patiententerminen; Online-Terminbuchung (wenn vorhanden)
Rechtsgrundlage	Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung – Anbahnung der Behandlung); ggf. Art. 9 Abs. 2 lit. h DSGVO, wenn Terminbuchungssystem Behandlungsgrund enthält (Gesundheitsdaten)
Betroffene Personen	Patienten; bei Terminbuchungsportalen auch Besucher der Website

Pflichtangabe	Inhalt
Datenkategorien	Name, Kontaktdaten, Terminzeit; ggf. Behandlungsgrund oder -art (dann: Gesundheitsdaten nach Art. 9 DSGVO); IP-Adressen und Browser-Daten von Website-Besuchern
Empfänger	Online-Terminbuchungssystem / PVS-Modul (Anbieter: _____) – bei Gesundheitsdaten: AVV zwingend, Anbieter muss auf deutschen/europäischen Servern operieren und angemessenes Datenschutzniveau nachweisen; ggf. Praxis-Personal zur Bestätigung
Drittland	Kritisch bei Online-Buchungssystemen: US-Anbieter (Calendly, Acuity Scheduling) für Gesundheitsdaten nicht zulässig. Deutsche/europäische Alternativen bevorzugen (z. B. Doctolib mit deutschem Datenschutz, appointmed, PVS-integrierte Lösungen). Prüfung des Datenstandorts ist obligatorisch.
Speicherdauer	Reine Terminhistorie ohne Behandlungsdokumentation: 1 Jahr nach Termin; mit Behandlungsbezug: wie Behandlungsdokumentation (10 Jahre nach Abschluss der Behandlung)
TOMs	Siehe TOM-Dokument; bei Online-Terminbuchung: sichere Übertragung (HTTPS mit hochwertigem Zertifikat), Validierung der Eingaben, kein Speichern sensitiver Daten in Cookies

---

C.1.2. Muster 2: Abrechnung

Verantwortliche/r: [Name Praxis/MVZ, Adresse, E-Mail] **Stand:** [Datum]

Verarbeitungstätigkeit 1: Kassenabrechnung und Abrechnungsvorbereitung

Pflichtangabe	Inhalt
Zweck	Erstellung, Prüfung und Übermittlung von Abrechnungsdaten an Krankenkassen und Kassenärztliche Vereinigung (KV); Dokumentation von erbrachten Leistungen; Abrechnung erbrachter Leistungen nach EBM oder GOÄ
Rechtsgrundlage	Art. 6 Abs. 1 lit. c DSGVO (rechtliche Verpflichtung: §§ 295ff SGB V für Kassenärzte, Abrechnungsrichtlinien der KBV, § 147 AO); Art. 9 Abs. 2 lit. h DSGVO (Gesundheitsversorgung – Diagnosen und Leistungen sind Gesundheitsdaten)
Betroffene Personen	Patienten
Datenkategorien	Patientenstammdaten (Name, Geburtsdatum, Versichertennummer, Krankenkasse); ICD-10-Diagnose-Codes; KODI-Kodes (Leistungs-Codes nach EBM oder GOÄ); Behandlungstage und -dauer; überweisende Ärzte; durchgeführte Untersuchungen und Leistungen; ggf. Laborergebnisse (als Gesundheitsdaten)
Empfänger	KV (Kassenärztliche Vereinigung) des Bundeslandes als Auftragsverarbeiter/Empfänger; Krankenkassen (für Kostenerstattung); PVS-Software (Anbieter: _____) als Auftragsverarbeiter; ggf. Abrechnungsdienstleister (Anbieter: _____, AVV vorhanden: ja/nein); Steuerberater/in (nur anonymisierte/aggregierte Abrechnungsdaten, kein Zugriff auf Patientenakten)
Drittland	Nein – KV-Übermittlung läuft über deutsche Systeme; PVS-Software muss auf deutschen/europäischen Servern laufen.
Speicherdauer	Abrechnungsunterlagen und Belege: 10 Jahre (§ 147 AO, § 257 HGB); Kassenabrechnung: wie Abrechnungsrichtlinien der KBV vorgeben (regelmäßig Quartal + 2 Jahre Nachlagefrist)

Pflichtangabe	Inhalt
TOMs	Siehe TOM-Dokument; besondere Anforderung: Verschlüsselung bei Übermittlung an KV; Prüfung der Abrechnungsdaten auf Vollständigkeit und Korrektheit vor Übermittlung; Audit-Trail aller Abrechnungsvorgänge

---

Verarbeitungstätigkeit 2: Privatpatienten-Abrechnung und Gebührenabrechnung

Pflichtangabe	Inhalt
Zweck	Erstellung und Versand von Rechnungen für Privatpatienten und private Leistungen nach GOÄ; Verfolgung von Zahlungseingängen; Mahnverfahren bei Nicht-Zahlung
Rechtsgrundlage	Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung – private Behandlungsvereinbarung); Art. 6 Abs. 1 lit. c DSGVO (steuerliche Aufbewahrung: § 147 AO, § 257 HGB); Art. 9 Abs. 2 lit. h DSGVO (Diagnosen und durchgeführte Leistungen)
Betroffene Personen	Privatpatienten; Kostenträger (Privatversicherungen, Beihilfestellen)
Datenkategorien	Patientenstammdaten (Name, Adresse); ICD-10-Diagnose-Codes; GOÄ-Leistungs-Codes; Betrag der Leistung; Privatabrechnung; Rechnungsdaten; ggf. Bankverbindung oder Zahlungsdaten (bei Kartenzahlung)
Empfänger	PVS-Software (Anbieter: _____) als Auftragsverarbeiter; Rechnungs- und Buchhaltungssoftware (Anbieter: _____); Steuerberater/in; ggf. Zahlungsdienstleister (für Kartenzahlungen: Anbieter: _____, PCI-DSS-konform); ggf. Inkassounternehmen (mit Vertrag und Schweigepflicht nach § 203 Abs. 4 StGB)
Drittland	PVS und Buchhaltungssoftware: europäische Server bevorzugt; Zahlungsdienstleister: PCI-DSS-Konformität prüfen

Pflichtangabe	Inhalt
Speicherdauer	Rechnungen und Abrechnungsbelege: 10 Jahre (§ 147 AO); Zahlungsdaten: nach Begleichung + Gewährleistungszeit + Verjährung (regelmäßig 3-4 Jahre); Bankverbindungen: nach Ende der Geschäftsbeziehung löschen
TOMs	Siehe TOM-Dokument; besondere Anforderung: Zahlungsdaten dürfen nicht in der PVS gespeichert sein (PCI-DSS); Rechnungen müssen verschlüsselt versendet werden; Kassendatenträger (GDPdU-Anforderungen für Finanzamt) müssen sicher verwahrt sein

---

C.1.3. Muster 3: Kommunikation

Verantwortliche/r: [Name Praxis/MVZ, Adresse, E-Mail] **Stand:** [Datum]

Verarbeitungstätigkeit 1: E-Mail-Kommunikation mit Patienten und Partnern

Pflichtangabe	Inhalt
Zweck	Geschäftliche und medizinische Kommunikation mit Patienten, überweisenden Ärzten, Fachkliniken und anderen medizinischen Partnern; Terminabsprachen; Befundmitteilungen; Behandlungskoordination
Rechtsgrundlage	Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung – Behandlung); Art. 9 Abs. 2 lit. h DSGVO (wenn Befunde oder Diagnosen mitgeteilt werden); § 203 StGB (Berufsgeheimnis)
Betroffene Personen	Patienten, überweisende Ärzte, Fachärzte, Klinikpersonal, Praxis-Partner
Datenkategorien	Name, E-Mail-Adresse, Kommunikationsinhalte (ggf. Befunde, Diagnosen, Behandlungshinweise als Gesundheitsdaten)

Pflichtangabe	Inhalt
Empfänger	E-Mail-Anbieter mit eigenem Server (Anbieter: _____) – muss sicheres IMAP/POP3 oder proprietäres System mit Verschlüsselung haben; nur europäische Provider empfohlen; als Auftragsverarbeiter
Drittland	Nein – US-Anbieter (Gmail, Outlook, Office 365) für ärztliche Kommunikation datenschutzrechtlich problematisch. EU-US DPF reicht für Gesundheitsdaten nicht. Deutsche Alternative bevorzugt (z. B. Posteo, mailbox.org mit deutschem Datenschutz und DSGVO-Zertifizierung).
Speicherdauer	Geschäftliche Korrespondenz mit medizinischem Inhalt: 10 Jahre (analog § 630f BGB); reine Terminabsprachen: 2 Jahre nach Termin; gelöschte E-Mails: permanent löschen, nicht in Papierkorb hinterlassen
TOMs	Siehe TOM-Dokument; besonderheiten: Verschlüsselung end-to-end bei sensiblen Inhalten (z. B. Befunde); Versand von Diagnosen oder Befunden nur über verschlüsselten Kanal; S/MIME oder PGP für medizinische Inhalte; Passwortschutz bei Cloud-Mailboxen; Anmeldedaten sicher gespeichert (Passwort-Manager)

Verarbeitungstätigkeit 2: KIM (Kommunikation im Medizinwesen)

Pflichtangabe	Inhalt
Zweck	Sichere Kommunikation mit anderen Ärzten, Kliniken, Apotheken und medizinischen Fachpersonen über das KIM-System (Kommunikation im Medizinwesen der gematik)
Rechtsgrundlage	Art. 9 Abs. 2 lit. h DSGVO (Gesundheitsversorgung); § 203 StGB (Berufsgeheimnis); ggf. KIM-Betreiber-Anforderungen der gematik
Betroffene Personen	Patienten (Empfänger von Befunden/Terminen), andere medizinische Fachpersonen (Empfänger von Arztbriefen)

Pflichtangabe	Inhalt
Datenkategorien	Name, KIM-Adresse, Befunde, Diagnose-Codes, Befundbriefe, Arztbriefe, Termineinladungen
Empfänger	KIM-Anbieter (Anbieter: _____) als Auftragsverarbeiter; Empfänger-Ärzte, -Kliniken, -Apotheken; ggf. TI-Betreiber
Drittland	Nein – KIM läuft über deutsche Telekommunikations-Infrastruktur
Speicherdauer	Wie Arztbriefe und medizinische Kommunikation: 10 Jahre
TOMs	Siehe TOM-Dokument; KIM nutzt gematik-Standard mit Ende-zu-Ende-Verschlüsselung; Authentifizierung über eHBA (elektronischer Heilberufsausweis) oder Nutzer-Zertifikat; Audit-Logging über gematik; Transport über verschlüsselte TI-Verbindung

---

Verarbeitungstätigkeit 3: Telefon und Telemedizin

Pflichtangabe	Inhalt
Zweck	Telefonische Patientenberatung, Terminabsprache, Befundmitteilung; Video-Sprechstunde (Telemedizin)
Rechtsgrundlage	Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung – Behandlung); Art. 9 Abs. 2 lit. h DSGVO (bei medizinischen Inhalten)
Betroffene Personen	Patienten
Datenkategorien	Name, Telefonnummer, Gesprächsinhalte (bei Videokonferenz: Bild, Ton, ggf. Bildschirm-Sharing); Befunde, Diagnosen (Gesundheitsdaten); Terminabsprachen
Empfänger	Telefon-Provider (Anbieter: _____); Videokonferenz-Anbieter (falls Telemedizin: Anbieter: _____, muss ärztliche Standards erfüllen – z. B. HIPAA-ähnliche Zertifizierung oder gematik-zugelassen); Praxis-Personal mit Telefon-Zugang

Pflichtangabe	Inhalt
Drittland	Telemedizin-Plattformen: nur europäische Anbieter oder Anbieter mit angemessenem Datenschutzniveau (z. B. Jitsi, BigBlueButton auf eigenem Server, gematik-zugelassene Anbieter). US-Plattformen (Zoom, Microsoft Teams) für ärztliche Videokonferenzen nur mit zusätzlichen Sicherheitsmaßnahmen (Verschlüsselung, Datenstandort-Prüfung).
Speicherdauer	Gesprächsnotizen mit medizinischem Inhalt: 10 Jahre (wie Behandlungsdokumentation); Aufzeichnungen von Videokonferenzen: nur mit expliziter Patienteneinwilligung, dann wie Behandlungsdokumentation (10 Jahre); reine Terminabsprachen: 1 Jahr
TOMs	Siehe TOM-Dokument; Videokonferenzen: nur auf sicheren, verschlüsselten Plattformen; Aufzeichnungen benötigen gesonderte Einwilligung und müssen verschlüsselt gespeichert sein; Telemedizin-Software muss ärztliche Anforderungen erfüllen (z. B. gematik-Zulassung, HIPAA, ISO 27001)

C.1.4. Muster 4: Praxis-Website und Terminbuchung

Verantwortliche/r: [Name Praxis/MVZ, Adresse, E-Mail] **Stand:** [Datum]

Verarbeitungstätigkeit 1: Website, Kontaktformular und allgemeine Online-Präsenz

Pflichtangabe	Inhalt
Zweck	Informationsbereitstellung über die Praxis (Öffnungszeiten, Leistungen, Ausstattung); Bearbeitung von Kontaktanfragen und Terminanfragen über Kontaktformular

Pflichtangabe	Inhalt
Rechtsgrundlage	Kontaktformular: Art. 6 Abs. 1 lit. b DSGVO (vorvertragliche Maßnahmen) / Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse: Beantwortung von Anfragen). Webhosting/technisch notwendige Daten: Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse: sicherer Betrieb der Website)
Betroffene Personen	Website-Besucher, Personen, die das Kontaktformular nutzen
Datenkategorien	IP-Adressen (Serverlog); Name, E-Mail, Telefon (optional, aus Kontaktformular); Nachrichteninhalt; ggf. User-Agent und Browser-Informationen; Cookies (falls vorhanden)
Empfänger	Webhoster (Anbieter: _____) als Auftragsverarbeiter; Formular-Plugin-Anbieter (falls nicht integriert: Anbieter: _____, AVV vorhanden: ja/nein); Praxis-Personal (zur Bearbeitung der Anfragen)
Drittland	Nur europäische Webhoster verwenden. US-Hoster (GoDaddy, AWS, Google Cloud) sind ohne EU-Äquivalenzsicherung datenschutzrechtlich problematisch. Deutsche/schweizer Hoster bevorzugen (z. B. Hetzner, netcup, Alfahosting).
Speicherdauer	Serverlog: max. 7 Tage (statistische/sicherheitliche Analyse); Kontaktanfragen: bis Bearbeitung abgeschlossen, danach wie E-Mail-Kommunikation (2 Jahre, falls keine medizinische Relevanz)
TOMs	Siehe TOM-Dokument; Website muss HTTPS mit aktuellen Zertifikaten nutzen (mindestens TLS 1.2); Kontaktformular muss geschützt sein (CAPTCHA oder ähnlich gegen Spam-Bots); kein Speichern von Zahlungsdaten im Formular; Cookies dürfen nur mit Einwilligung (Consent-Banner) gesetzt werden

---

C.1.5. Muster 5: Personalverwaltung (MVZ und größere Praxen mit Mitarbeitern)

Verantwortliche/r: [Name Praxis/MVZ, Adresse, E-Mail] **Stand:** [Datum]

Verarbeitungstätigkeit 1: Personalverwaltung und Mitarbeiterdaten

Pflichtangabe	Inhalt
Zweck	Verwaltung von Mitarbeiterstammdaten; Abrechnung von Gehalt und Lohn; Sozialversicherungs- und Steuermeldungen (Lohnsteuer, Beitragsnachweise); Einhaltung arbeitsrechtlicher Verpflichtungen; Schulungs- und Fortbildungsmanagement
Rechtsgrundlage	Art. 6 Abs. 1 lit. b DSGVO (Arbeitsvertrag); Art. 6 Abs. 1 lit. c DSGVO (rechtliche Verpflichtungen: Lohnsteuer, Sozialversicherung § 108 SGB IV, Arbeitszeitgesetz); Art. 9 Abs. 2 lit. b DSGVO (falls erforderlich für Arbeitnehmervergünstigungen oder Schutzmaßnahmen: z. B. Schwerbehindertenausweis)
Betroffene Personen	Mitarbeiter (Ärzte, Arzthelferin/Arzhelfer, MTA, sonstiges Personal)
Datenkategorien	Name, Geburtsdatum, Geschlecht, Adresse, Kontaktdaten; Sozialversicherungsnummer, Steuernummer; Bankverbindung (für Gehalt); Arbeitsvertrag und Zusatzvereinbarungen; Arbeitszeit und Urlaub; Krankmeldungen; Qualifikationen, Approbation, Fachzertifikate; Schulungs- und Fortbildungsnachweise; ggf. Arzt-/Zahnarzt-Registrierung in KZV/KV
Empfänger	Lohn- und Finanzbuchhaltungssoftware (Anbieter: _____); Steuerberater/in oder Lohnabrechner (mit Verschwiegenheitsverpflichtung nach § 203 Abs. 4 StGB); Finanzamt (für Lohnsteuer-Anmeldung); Krankenkasse und Rentenversicherung (für Beitragsnachweise); Berufsgenossenschaft (für Unfallversicherung)
Drittland	Nein – Lohnabrechnung darf nicht auf US-Servern laufen. Europäischer Anbieter mit deutschem Datenschutz erforderlich.

Pflichtangabe	Inhalt
Speicherdauer	Personalstammdaten: Dauer der Betriebszugehörigkeit + 3 Jahre (Aufbewahrung nach BetrVG und Arbeitsrecht); Lohnabrechnungen und Beitragsnachweise: 6 Jahre (§ 257 HGB, § 147 AO); Arbeitsunfähigkeit und Krankmeldungen: 4 Jahre (Aufbewahrungspflicht unter Betriebsräte-Vereinbarungen)
TOMs	Siehe TOM-Dokument; besondere Anforderung: Personaldaten müssen streng vom Arztsystem getrennt sein – nicht in der PVS speichern; Zugriff nur für berechtigte Praxis-Leiter und HR-Personal; Verschlüsselung aller Personaldaten; Sichere Vernichtung nach Aufbewahrungsfrist

---

Verarbeitungstätigkeit 2: Dienstpläne und Urlaubsverwaltung

Pflichtangabe	Inhalt
Zweck	Erstellung und Verwaltung von Schicht- und Dienstplänen; Verwaltung von Urlaub und Abwesenheiten; Einhaltung von Arbeitszeitgesetzen
Rechtsgrundlage	Art. 6 Abs. 1 lit. b DSGVO (Arbeitsvertrag); Art. 6 Abs. 1 lit. c DSGVO (Arbeitszeitgesetz, Betriebsverfassungsgesetz)
Betroffene Personen	Mitarbeiter
Datenkategorien	Name, Arbeitszeit, Schicht-Zuordnung, Urlaub und Abwesenheits-Gründe; ggf. Notizen zu Langzeitkrankmeldungen
Empfänger	Dienstplan-Software (Anbieter: _____) oder PVS-Modul (wenn integriert); ggf. alle Mitarbeiter (zur Einsicht in den eigenen Dienstplan); Schichtleitung/Praxisleitung
Drittland	Deutsche/europäische Lösung bevorzugt
Speicherdauer	Gültige Dienstpläne für Betriebsdauer + 6 Monate (für Retrospektive); archivierte Pläne: 2 Jahre (Nachweis für Arbeitszeit-Audits)

Pflichtangabe	Inhalt
TOMs	Siehe TOM-Dokument; Dienstpläne sollten nicht in der PVS mit Patientendaten sichtbar sein; Zugriff nur für Planungs-Personal und betroffene Mitarbeiter

---

C.1.6. Hinweise zur Anpassung

Was Sie immer ergänzen müssen: - Konkrete Anbieter aller eingesetzten Dienste (PVS-Software, KIM-Anbieter, E-Mail, Videokonferenz, Personalmanagement) - Ob ein Auftragsverarbeitungsvertrag (AVV) mit diesen Anbietern besteht – und wenn nicht, ob einer benötigt wird - Konkrete Drittland-Situation bei Cloud-Diensten: Welche Garantie gilt? (EU-US DPF ist für Gesundheitsdaten NICHT ausreichend) - Deine spezifischen Löschfristen und ob Sie sie technisch umsetzen - Laborpartner, Überweisungspartner und Kliniken, an die Patientendaten übermittelt werden (mit/ohne Schweigepflichtentbindung)

Was Sie im Zweifelsfall rechtlich prüfen lassen sollten: - Rechtsgrundlage für ungewöhnliche Verarbeitungstätigkeiten - Verarbeitung besonderer Datenkategorien (Art. 9 DSGVO): Gesundheitsdaten sind immer besondere Kategorien - Drittlandübermittlungen und deren Garantien – besonders kritisch: US-Anbieter - Interaktion zwischen DSGVO und ärztlichen Berufsgeheimnissen (§ 203 StGB, § 630f BGB) - Anforderungen der KBV-Sicherheitsrichtlinie und Einhaltung der TI-Standards - Besonderheiten beim MVZ: kollektive Haftung, Daten-Zugriff zwischen Ärzten

Jährliche Pflege: Das VVT ist kein einmaliges Dokument. Jeder neue Dienst, jeder Anbieterwechsel, jede neue Verarbeitungstätigkeit muss eingetragen werden. Eine jährliche Überprüfung ist Pflicht – ein kurzer Kalendertermin reicht dafür. Besonders wichtig: Jährliche Prüfung der AVVs mit allen Auftragsverarbeitern.

D. Krisenmanagement: Deep Dives

Ein Notfallplan ist der erste Schritt. Was danach kommt – in den Stunden und Tagen nach einem ernsthaften Sicherheitsvorfall – ist komplexer, als die meisten erwarten. Dieser Anhang geht über die konkreten Handlungsanweisungen der Hauptkapitel hinaus und behandelt die strategischen und kommunikativen Dimensionen einer Krise in der Arztpraxis: Wie treffen Sie Entscheidungen unter Druck? Wie kommunizieren Sie professionell, ohne Haftungsrisiken einzugehen? Wie informieren Sie Ihre Patienten und die KV? Und wie stellen Sie sicher, dass Sie aus einem Vorfall gestärkt hervorgehen – statt ihn nur zu überstehen?

Was Sie in diesem Anhang erwartet:

D1 – Krisenmanagement – der vollständige Leitfaden für Arztpraxen: Von der Erstreaktion bis zur Nachbereitung. Wie Sie Patienten-Kommunikation professionell gestalten, wann und wie Sie Datenpannen melden (besonders an Datenschutzbehörde und ggf. Patienten), wie Sie die Kassenabrechnung während eines Ausfalls organisieren, wie Sie die TI-Verbindung bei Ausfall bewältigen, wie Sie Ihr PVS-System sicher wiederherstellen, wie Sie mit Ransomware-Erpressung und der Drohung mit Datenveröffentlichung umgehen – und wie Sie alternative Kommunikationskanäle schalten, wenn Ihre primären Kanäle kompromittiert sind.

Die Krisenszenarien in Teil 7 geben konkrete Handlungsanweisungen für die ersten Stunden nach einem Vorfall. Dieser Deep Dive geht tiefer: Welche Strategien gibt es für das Krisenmanagement insgesamt? Wie gestalten Sie die Kommunikation mit Patienten professionell? An wen wenden Sie sich zur Unterstützung? Wann und wie melden Sie Datenpannen? Wie informieren Sie die KV bei laufenden Kassenabrechnung? Wie schalten Sie alternative Kommunikationskanäle, wenn Ihre primären Kanäle ausgefallen oder kompromittiert sind? Wie stellen Sie Ihr PVS-System sicher wieder her, ohne erneut infiziert zu werden? Und: Wie gehen Sie mit Ransomware-Erpressung und der Drohung um, Patientendaten im Darknet zu veröffentlichen?

D.1. Krisenmanagement als Haltung – nicht als Checkliste

Der häufigste Fehler im Krisenmanagement ist nicht das Fehlen eines Plans – sondern das Fehlen der Haltung, die einen Plan überhaupt nutzbar macht. Wer unter Stress in Panik verfällt, trifft schlechte Entscheidungen, macht Fehler und kommuniziert unklar. Wer gelernt hat, eine Krise als Problem zu behandeln, das lösbar ist, bleibt handlungsfähig.

Zwei Grundprinzipien helfen dabei:

Erstens: Trennung von Erkennen und Handeln. Die ersten Minuten nach einem Vorfall sind für Diagnose, nicht für Aktionismus. Netzwerkkabel ziehen ist eine Ausnahme – das sollte sofort passieren. Alles andere: erst verstehen, was passiert ist, bevor Sie handeln. Wer überstürzt handelt, zerstört möglicherweise Beweise, verschlimmert die Situation oder rennt in die falsche Richtung.

Zweitens: Dokumentation von Beginn an. Halten Sie von der ersten Minute an fest, was Sie wann getan haben, was Sie vorgefunden haben und welche Entscheidungen Sie getroffen haben. Diese Dokumentation ist dreifach wertvoll: für die Datenschutzbehörde (72-Stunden-Meldepflicht), für die Polizei (Strafanzeige), und für Sie selbst (Wiederanlauf, Versicherung, Nachbereitung).

D.2. Strategien im Krisenmanagement

Es gibt kein universelles Krisenmanagement-Modell – aber es gibt bewährte Phasen, die sich auf fast jeden IT-Vorfall in der Arztpraxis anwenden lassen.

D.2.1. Phase 1: Eindämmung (Containment)

Das erste Ziel ist nicht Wiederherstellung – sondern Schadensbegrenzung. Was nicht kompromittiert ist, muss es auch nicht werden.

- Betroffenes Gerät/System sofort vom Netzwerk trennen (Ethernet-Kabel, WLAN, Bluetooth)
- NAS und externe Backup-Festplatten trennen, sofern noch nicht verschlüsselt oder kompromittiert
- Cloud-Synchronisation pausieren – damit lokal verschlüsselte Dateien nicht in die Cloud synchronisiert werden und dort die guten Versionen überschreiben
- Zugangsdaten zu Cloud-Diensten und PVS von einem sauberen Gerät aus sofort ändern
- TI-Konnektor: Physisch vom Netzwerk trennen (bei Bedarf mit IT-Dienstleister besprechen – kann Notfall-Auswirkungen haben)

Erst wenn die Ausbreitung gestoppt ist, beginnt die Analyse.

D.2.2. Phase 2: Analyse

Was ist passiert? Wie ist es passiert? Was ist betroffen?

- Welche Systeme sind betroffen? (Arbeitsstation, Server, NAS, Cloud-Speicher, PVS?)
- Welche Patientendaten lagen auf diesen Systemen – und sind darunter besonders sensible Daten (Befunde, Diagnosen, Medikationen)?

- Gibt es Anzeichen für Datenabfluss (Exfiltration) – nicht nur Verschlüsselung, sondern auch Diebstahl?
- Was ist das wahrscheinliche Einfallstor? (Phishing-Mail, unsichere RDP-Verbindung, veraltetes Plugin, infizierter USB-Stick, schwaches Passwort?)
- War der Zugriff über den TI-Konnektor, über VPN, oder lokal?

Diese Fragen müssen nicht sofort vollständig beantwortet werden – aber sie müssen gestellt werden. Die Antworten bestimmen die nächsten Schritte und ob eine Datenschutz-Meldepflicht entsteht.

D.2.3. Phase 3: Kommunikation

Parallel zur Eindämmung und Analyse beginnt die Kommunikation – intern (mit dem Praxis-Team, mit Ihrem IT-Dienstleister, mit Ihrer Cyber-Versicherung) und extern (Behörden, Patienten, KV). Mehr dazu in den folgenden Abschnitten.

D.2.4. Phase 4: Wiederherstellung

Wiederherstellung beginnt erst, wenn Eindämmung und Analyse abgeschlossen sind und das Einfallstor geschlossen ist. Überstürzter Wiederanlauf auf einem nicht bereinigten System ist eine der häufigsten Ursachen für Folgeinfektionen. Mehr dazu im Abschnitt *Sichere Wiederherstellung aus Backups*.

Besonderheit Arztpraxis: Klären Sie mit Ihrem IT-Dienstleister und mit der KV, welche Systeme Priorität haben (Notfall-Funktionen der PVS, TI-Verbindung für Kassenabrechnung).

D.2.5. Phase 5: Nachbereitung

Nach jeder Krise – auch einer kleineren – lohnt sich eine ehrliche Retrospektive: Was hat funktioniert? Was hat versagt? Was wäre fast schiefgelaufen? Welche Lücken im Notfallplan hat die Krise aufgedeckt? Diese Erkenntnisse fließen in eine Aktualisierung des Notfallplans ein.

D.3. Unterstützung von außen – wer hilft wann?

Als Arztpraxis haben Sie – anders als größere Krankenhäuser – keine IT-Abteilung und kein Incident-Response-Team. Das bedeutet nicht, dass Sie auf Unterstützung verzichten müssen. Es bedeutet, dass Sie wissen müssen, wen Sie rufst.

D.3.1. BSI – Bundesamt für Sicherheit in der Informationstechnik

Das BSI ist die zentrale Behörde für IT-Sicherheit in Deutschland. Es bietet kostenloses Informationsmaterial, Handlungsempfehlungen und im Fall größerer Vorfälle auch direkte Unterstützung.

Was das BSI für Sie tun kann: - Informationen und Handlungsempfehlungen zu aktuellen Bedrohungen (`bsi.bund.de`) - Der BSI-Leitfaden „IT-Grundschutz" – zwar primär für Behörden und Unternehmen konzipiert, enthält aber auch für Praxen nützliche Prüfrahmen - Bei Ransomware: `bsi.bund.de/ransomware` enthält aktuelle Hinweise und Verweise auf Entschlüsselungstools

Was das BSI nicht tut: Das BSI kommt nicht in Ihre Praxis und hilft Ihnen, Ihr System zu bereinigen. Für operative Unterstützung brauchen Sie einen IT-Dienstleister.

Tipp: Registrieren Sie sich für den BSI-Newsletter und die Warnmeldungen – so erfahren Sie zeitnah von aktuellen Bedrohungen und Sicherheitslücken, die auch Ihr PVS-System betreffen können.

D.3.2. Polizei / Landeskriminalamt (LKA)

Jeder IT-Sicherheitsvorfall, bei dem ein Angriff von außen stattgefunden hat, ist eine Straftat. Ransomware, Datendiebstahl, Account-Übernahme – das sind keine Pechfälle, sondern Verbrechen. Eine Strafanzeige ist sinnvoll, auch wenn die Täter selten gefasst werden.

Warum Anzeige trotzdem wichtig ist: - Voraussetzung für Versicherungsleistungen (Cyber-Versicherung verlangt in der Regel eine Strafanzeige) - Erzeugt eine Dokumentation des Vorfalls mit Aktenzeichen - Trägt zur Statistik bei, die für die Ressourcenplanung der Behörden genutzt wird - In seltenen Fällen werden Täter gefasst und Daten wiederhergestellt

Wohin: Zunächst zur nächsten Polizeidienststelle für die Anzeigenerstattung. Für Cyberkriminalität spezialisiert sind die Zentralen Ansprechstellen Cybercrime (ZAC) der Landeskriminalämter – jedes Bundesland hat eine eigene ZAC. Die Kontaktdaten findest du über die Website Ihres Landeskriminalamts.

Was mitbringen: Zeitpunkt der Entdeckung, betroffene Systeme, Screenshot oder Foto der Ransomware-Nachricht (falls vorhanden), alle technischen Hinweise auf das Einfallstor, betroffene Patientenzahl und Art der Daten.

D.3.3. KV – Kassenärztliche Vereinigung

Die KV muss bei längeren IT-Ausfällen informiert werden, die die Kassenabrechnung betreffen – insbesondere wenn die PVS nicht erreichbar ist.

Was die KV für Sie tun kann: - Information über Notfallproceduren bei PVS-Ausfall - Klärung von Abrechnung und Fristen bei längerer Ausfallzeit - Ggf. Genehmigung von Ausnahmeregelungen (z. B. handschriftliche Aufzeichnungen statt PVS)

Wann Sie die KV informieren sollten: - Ausfallzeit länger als 24 Stunden und Kassenabrechnung betroffen - Sicherheitsvorfall mit möglichem Datendiebstahl von Patientendaten - Notwendigkeit von Ausnahme-Abrechnungsregeln

D.3.4. Datenschutzbehörde (Landesdatenschutzbeauftragte)

Wenn personenbezogene Daten – also praktisch alle Patientendaten – von einem Vorfall betroffen sind, greift die Meldepflicht nach Art. 33 DSGVO. Mehr dazu im Abschnitt *Datenschutzmeldepflichten im Krisenfall*.

D.3.5. IT-Dienstleister / Incident-Response-Spezialisten

Für die operative Bereinigung und Wiederherstellung brauchen Sie einen IT-Fachmann oder -frau, der Erfahrung mit Sicherheitsvorfällen hat – besonders im Gesundheitswesen. Das ist nicht jeder IT-Dienstleister – ein normaler IT-Techniker, der Drucker einrichtet, ist für Ransomware-Bereinigung nicht ausgerüstet.

Worauf Sie achten sollten: - Erfahrung mit Incident Response, besonders bei PVS-Systemen - Vertrautheit mit TI-Infrastruktur und gematik-Standards - Referenzen von anderen Arztpraxen oder MVZ - Festpreis oder Stundensatz im Voraus klären - Im Krisenfall ist der Preisdruck groß – gute Entscheidungen brauchen ein ruhiges Gespräch

Idealfall: Sie haben einen IT-Dienstleister Ihres Vertrauens, bevor die Krise eintritt. Er kennt Ihre Infrastruktur und kann im Ernstfall schnell handeln.

D.3.6. Cyber-Versicherung

Falls Sie eine Cyber-Versicherung haben – informieren Sie sie sofort. Die meisten Cyber-Versicherungen bieten als Teil der Versicherungsleistung eine 24/7-Hotline und vermitteln Incident-Response-Dienstleister. Das ist einer der Hauptvorteile einer Cyber-Versicherung: nicht nur die finanzielle Absicherung, sondern der sofortige Zugang zu Experten.

D.4. Datenschutzmeldepflichten im Krisenfall

Eine vollständige Erklärung der DSGVO-Meldepflichten findet sich in Teil 4. Hier die praxisrelevante Kurzfassung für den Krisenfall.

Die zentrale Frage: Sind personenbezogene Daten – insbesondere Gesundheitsdaten – von dem Vorfall betroffen?

Wenn ja: Es ist eine Datenpanne im Sinne von Art. 33 DSGVO – unabhängig davon, ob die Daten gestohlen wurden oder „nur" verloren gegangen oder unzugänglich sind.

72-Stunden-Frist (Art. 33 DSGVO): Meldung an die zuständige Landesdatenschutzbehörde (der Bundesland, in dem sich Ihre Praxis befindet), wenn die Datenpanne voraussichtlich ein Risiko für betroffene Personen (Patienten) darstellt. Die Frist beginnt mit

dem Zeitpunkt, zu dem Sie von der Panne Kenntnis erlangt haben – nicht mit dem Zeitpunkt des Angriffs. Die Meldung kann stufenweise erfolgen, wenn nicht alle Informationen sofort vorliegen.

Was in die Meldung gehört: - Art des Vorfalls (Ransomware, Datendiebstahl, Hardwareausfalk, etc.) - Betroffene Datenkategorien (z. B. Diagnose-Codes, Medikationshistorie, Patientenstammdaten) und geschätzte Anzahl betroffener Patienten - Wahrscheinliche Folgen für die Patienten - Ergriffene und geplante Gegenmaßnahmen - Kontaktdaten des Verantwortlichen (Sie/Ihre Praxis) und ggf. des Datenschutzbeauftragten

Besonderheit für Gesundheitsdaten: Art. 9 DSGVO klassifiziert Gesundheitsdaten als besondere Kategorien. Eine Datenpanne mit Gesundheitsdaten wird behördenübergreifend ernster genommen.

Meldung an Betroffene (Art. 34 DSGVO): Wenn ein hohes Risiko für die betroffenen Patienten besteht – etwa weil unverschlüsselte Gesundheitsdaten, Bankverbindungen oder umfangreiche Patientendaten abgeflossen sind –, müssen Sie die Patienten direkt informieren. Formulierung: klar, verständlich, ohne Verharmlosung, mit konkreten Hinweisen, was die Patienten selbst tun können.

Wann entfällt die Meldepflicht an Betroffene: Wenn die kompromittierten Daten vollständig verschlüsselt waren und der Schlüssel nicht kompromittiert wurde. Das ist das konkrete Argument dafür, alle Daten zu verschlüsseln – es schützt nicht nur die Daten, sondern auch Sie vor einer aufwendigen Benachrichtigungspflicht.

Kontaktdaten der Behörden: Die zuständige Datenschutzbehörde richtet sich nach Ihrem Praxissitz. Eine Übersicht aller Landesdatenschutzbehörden findet sich unter `bfdi.bund.de`. Diese Kontaktdaten gehören in Ihr Notfalldokument – nicht erst im Krisenfall suchen.

D.5. Patienten-Kommunikation in der Krise

Schlechte Patienten-Kommunikation in einer Krise richtet oft mehr Schaden an als die Krise selbst. Patienten, die zu spät, zu vage oder gar nicht informiert werden, verlieren das Vertrauen dauerhaft. Patienten, die früh, ehrlich und klar informiert werden, reagieren in der Regel verständnisvoll.

D.5.1. Grundprinzipien

Proaktiv, nicht reaktiv. Informieren Sie Patienten, bevor Sie selbst merken, dass etwas nicht stimmt. Wer von einem Patienten angerufen wird, weil dessen Daten im Darknet auftauchen, hat die Initiative verloren.

Ehrlich, nicht verharmlosend. „Wir haben einen technischen Vorfall" ist keine ausreichende Information. Patienten verdienen zu wissen, was passiert ist, was das für sie bedeutet und was Sie dagegen tun.

Konkret, nicht allgemein. Welche Daten könnten betroffen sein? Welche nicht? Was sollen die Patienten konkret tun? Klare Antworten auf diese Fragen schaffen Vertrauen.

Schnell, nicht perfekt. Im Krisenfall ist eine schnelle, ehrliche Erstinformation besser als eine perfekt formulierte Nachricht, die zwei Tage zu spät kommt.

D.5.2. Was in die erste Patientenmitteilung gehört

1. **Was ist passiert** – sachlich und ohne übertriebene technische Details
2. **Welche Patientendaten könnten betroffen sein** – konkret benennen, was Sie wissen und was Sie (noch) nicht wissen
3. **Was Sie bereits unternommen haben** – welche Schritte Sie eingeleitet haben
4. **Was der Patient tun sollte** – falls seine eigene Handlung erforderlich ist (z. B. auf verdächtige Aktivitäten achten, verdächtige Zahlungen prüfen)
5. **Wie er sich informieren kann** – wo er Updates bekommt, wen er bei Fragen kontaktieren kann
6. **Wann Sie das nächste Update geben** – konkrete Zeitangabe, auch wenn Sie dann nur mitteilen können, dass die Situation noch andauert

D.5.3. Ton und Formulierung

Kein Juristendeutsch. Kein Kleinreden. Kein Abschieben von Verantwortung. Patienten spüren, ob jemand die Verantwortung übernimmt oder sich duckt. Ein klares „Ich übernehme die Verantwortung für diesen Vorfall und arbeite an der Lösung" wirkt besser als zehn Seiten mit Haftungsausschlüssen.

Wenn Patienten-Daten möglicherweise im Darknet gelandet sind: Sagen Sie das. Nicht mit Panik, aber klar. Informieren Sie die Patienten, was sie konkret tun können – Passwörter bei anderen Diensten ändern, falls sie dasselbe Passwort auch dort nutzen, Kontoauszüge auf unbekannte Transaktionen prüfen.

D.6. Ausfallmanagement – wenn Ihre PVS nicht erreichbar ist

Eines der gefährlichsten Szenarien für eine Arztpraxis: Ihre PVS ist nicht erreichbar – sei es durch Ransomware, durch Hardwareausfall, oder durch Netzwerkprobleme. Patienten stehen vor der Tür. Die Kassenabrechnung läuft. Sie müssen entscheiden: Wie läuft die Praxis weiter?

D.6.1. Notfall-Funktionen bewahren

Papiergebundene Workflows: Halten Sie im Krisenfall Papierformulare bereit: - Patientenstammdatenblatt (Name, Geburtsdatum, Versicherungsdaten) - Behandlungsnotizen-Vorlage (Datum, Symptome, Befunde, Diagnose, Therapie) - Rezept-Vorlagen (Muster 16 oder manuell ausgestellt) - Arbeitsunfähigkeits-Bescheinigung (Muster 1)

Notfall-Telefonnummern: Halten Sie Kontaktdaten bereit für: - Labore (für Anforderungen und Befundrückfragen) - Überweisungs-Partner und Fachkliniken - Apotheken (für Notfall-Verordnungen) - KV des Bundeslandes (für Abrechnung und Genehmigungen)

Offline-Patientenliste: Exportieren Sie regelmäßig eine Liste Ihrer regelmäßigen Patienten – Name, Geburtsdatum, Versicherungsdaten, Allergien, Dauermedikation. Speichern Sie diese Liste offline: ausgedruckt oder auf einem verschlüsselten USB-Stick, der nicht mit Ihrem Primärsystem verbunden ist. Im Krisenfall, wenn Ihre PVS nicht erreichbar ist, ist diese Liste Gold wert.

D.6.2. Kassenabrechnung bei Ausfall

Wenn Ihre PVS länger als 24 Stunden nicht erreichbar ist, müssen Sie die KV informieren:

- **Kontaktieren Sie die KV** – teilen Sie mit, dass Sie einen technischen Ausfall haben und voraussichtlich nicht rechtzeitig abrechnen können
- **Klären Sie mit der KV, wie Sie vorgehen:** Manche KVen akzeptieren handschriftliche Aufzeichnungen oder eine Verzögerung der Abrechnung
- **Dokumentieren Sie Ihre Leistungen analog:** Datum, Patientenstammdaten, Diagnose-Code (ICD-10), durchgeführte Leistungen (KODI), Behandlungsgrund. Diese Dokumentation ist notwendig für die spätere elektronische Abrechnung
- **Beachten Sie Abrechnungsfristen:** Kassenabrechnung muss regelmäßig erfolgen – eine längere Ausfallzeit kann zu Einnahmeausfällen führen

D.6.3. Notfall-Therapie

Für Patienten mit laufender Dauermedikation: - **Rezepte werden weiterhin ausgestellt** – notfalls handschriftlich (Muster 16) - **Dauermedikationen** weitergeben, wo möglich (unter Dokumentation für spätere Abrechnung) - **Absprache mit Apotheken:** Informieren Sie Ihre Apotheken-Partner, dass Sie eventuell vorübergehend manuell verschreiben

---

D.7. Alternative Kommunikationskanäle wenn die primären Kanäle ausgefallen sind

Eines der gefährlichsten Szenarien: Ihre E-Mail ist kompromittiert oder gesperrt. Ihre Website ist nicht erreichbar. Ihre PVS ist offline. Sie können Ihre Patienten nicht kontaktieren – und sie können Sie nicht erreichen.

D.7.1. Vorbereitungsmaßnahmen

Eine zweite E-Mail-Adresse bei einem anderen Anbieter. Sie kostet nichts (Posteo ab 1 €/Monat, oder eine kostenlose Adresse bei mailbox.org) und liegt bei einem vollständig anderen Anbieter. Im Krisenfall ist sie sofort verfügbar.

Eine Notfall-Telefonnummer auf Ihrer Website und in Ihren Aushängen. Wenn alles andere ausfällt, funktioniert das Telefon noch. Patienten, die Ihre Nummer haben, können Sie erreichen.

Offline-Patientenliste. Siehe oben.

Offline-Kontaktliste für Partner: Überweisungs-Ärzte, Labore, Kliniken – mit Telefonnummern und Ansprechpersonen. Im Krisenfall, wenn Ihre E-Mail nicht funktioniert, ist eine Telefonnummer Gold wert.

D.7.2. Im Krisenfall: Kanal-Alternativen

SMS oder Messenger. Wenn E-Mail nicht funktioniert, ist eine SMS oder eine Nachricht über Signal/WhatsApp der schnellste Weg. Patienten reagieren auf direkte Nachrichten schneller als auf E-Mails.

Telefonische Direktkommunikation. Für die wichtigsten Patienten und laufende Behandlungen: direkter Anruf. Unbequem, aber wirkungsvoll. Und er signalisiert Ernsthaftigkeit.

Temporäre Ersatz-Website. Wenn Ihre Hauptdomain ausgefallen ist, können Sie innerhalb von Minuten eine einfache statische Seite unter einer anderen Domain aufsetzen – bei Diensten wie GitHub Pages oder einem einfachen Hoster. Eine Seite mit Ihrer Notfall-E-Mail-Adresse, Ihrer Telefonnummer und einer kurzen Erklärung reicht. Die Adresse dieser Ersatzseite vorab kommunizieren – auf Ihrer normalen Website verlinken und in der E-Mail-Signatur erwähnen.

Praxis-Aushang. Ein Papier-Aushang vor der Praxis mit Ihrer Notfall-Telefonnummer kann vielen Patienten in der Sofort-Information helfen.

D.7.3. Sicherheit bei alternativen Kanälen

Ein wichtiger Aspekt: Kriminelle nutzen Krisen aus. Wenn bekannt wird, dass Sie Opfer eines Angriffs geworden sind, versuchen Angreifer manchmal, sich als Sie auszugeben und Ihre Patienten zu kontaktieren – mit gefälschten Zahlungsaufforderungen, mit der Bitte um Datenbestätigung, oder mit Schadsoftware-Links.

Informieren Sie Ihre Patienten deshalb ausdrücklich darüber, über welche Kanäle Sie sie kontaktieren – und dass sie misstrauisch sein sollen, wenn sie über andere Kanäle von jemandem kontaktiert werden, der vorgibt, Sie/Ihre Praxis zu sein.

D.8. Sichere Wiederherstellung aus Backups – ohne erneute Infektion

Das größte Risiko beim Zurückspielen von Backups: Sie spielen das Backup ein – und holen dabei die Schadsoftware gleich mit zurück.

D.8.1. Das Zeitfenster-Problem

Ransomware und andere Schadsoftware ist oft tagelang oder wochenlang auf einem System aktiv, bevor sie sich bemerkbar macht. Die Schadsoftware liegt still, erkundet das System, stiehlt Daten – und schlägt erst dann zu, wenn der Angriff strategisch optimal ist. Das bedeutet: Ein Backup vom Vortag kann bereits infiziert sein.

Wie weit zurückgehen? Als Faustregel: mindestens 2–4 Wochen vor dem ersten Anzeichen der Infektion. Falls Sie nicht wissen, wann die Infektion begann, müssen Sie das Einfallstor analysieren – Systemlogs, E-Mail-History – um den frühestmöglichen Infektionszeitpunkt einzuschätzen.

D.8.2. Der sichere Wiederherstellungsprozess

Schritt 1: Gerät/System vollständig neu aufsetzen Kein „Bereinigen" des infizierten Systems. Kein Antivirus-Scan, der die Schadsoftware „entfernt". Das einzige sichere Vorgehen ist: Festplatte formatieren, Betriebssystem neu installieren, alle Updates einspielen, bevor irgendwelche Daten zurückgespielt werden.

Schritt 2: PVS-System neu aufsetzen und aktualisieren Falls das PVS-System betroffen war: Vollständige Neuinstallation vom Hersteller (Backup der Installation vom bekannt-guten Stand). Alle Patches und Updates des PVS einspielen. Von Ihrem PVS-Anbieter bestätigen lassen, dass das System sauber ist.

Schritt 3: Backup vor dem Zurückspielen prüfen Bevor Backup-Daten auf das neu aufgesetzte System kopiert werden, prüfen Sie sie auf einem isolierten System oder mit einem aktuellen Virenscanner, der nicht Teil des kompromittierten Systems war. Ein Virenscanner auf einem infizierten System kann die Schadsoftware nicht zuverlässig erkennen – er könnte selbst kompromittiert sein.

Schritt 4: Daten schrittweise zurückspielen, nicht en bloc Spielen Sie zuerst die Daten zurück, die Sie dringend brauchen. Prüfen Sie das System nach jedem Schritt. Wenn Sie alles auf einmal zurückspielten und die Infektion erneut auftritt, wissen Sie nicht, welche Datei die Ursache war.

Schritt 5: Einfallstor schließen, bevor Sie online gehen Bevor das neu aufgesetzte System mit dem Internet verbunden wird: Das Einfallstor muss bekannt und geschlossen sein. Wenn der Angriff über veraltete Software kam – diese Software entweder aktualisieren oder nicht wieder installieren. Wenn der Angriff über kompromittierte Zugangsdaten kam – alle Passwörter ändern, bevor das System online geht.

Schritt 6: TI-Verbindung neu authentifizieren Falls Ihr System über die TI (Telematik-Infrastruktur) mit eHBA oder Konnektor verbunden war: Authentifizierung neu überprüfen und ggf. neu konfigurieren. Mit Ihrem IT-Dienstleister und mit dem TI-Betreiber absprechen.

Schritt 7: Passwörter auf einem anderen Gerät ändern Die Zugangsdaten, die auf dem infizierten System gespeichert waren, müssen als kompromittiert gelten – auch wenn Ransomware „nur" verschlüsselt hat und nicht sichtbar gestohlen hat. Moderne Ransomware exfiltriert in der Regel Daten, bevor sie verschlüsselt. Ändern Sie alle Passwörter von einem sauberen Gerät aus, bevor das wiederhergestellte System zum Einsatz kommt.

Schritt 8: Offline-Backup für die Wiederherstellung verwenden Backups, die mit dem kompromittierten System synchronisiert wurden, könnten ebenfalls Schadsoftware enthalten. Das ist der konkrete Grund für die 3-2-1-1-0-Regel mit einer Offline-Kopie: Ein Backup, das nie mit dem infizierten System verbunden war, ist das einzige, dem Sie im Wiederherstellungsfall wirklich vertrauen können.

D.9. Ransomware und Erpressung – die kritischen Entscheidungen

D.9.1. Zahlen oder nicht zahlen?

Die klare Empfehlung aller Behörden – BSI, BKA, Europol, FBI – lautet: **Nicht zahlen.**

Die Gründe: - Zahlung garantiert keine Entschlüsselung. Kriminelle sind nicht vertragsgebunden. - Zahlung macht Sie zum bekannten Zahler und damit zum wiederholten Ziel. - Zahlung finanziert weitere kriminelle Aktivitäten. - In manchen Fällen ist der Entschlüsselungsschlüssel ohnehin defekt – selbst nach Zahlung bleiben die Dateien unlesbar. - Manche Ransomware-Varianten haben kostenlose Entschlüsselungstools – prüfen Sie `nomoreransom.org`, bevor Sie irgendeine Entscheidung treffen.

Es gibt Ausnahmesituationen, in denen größere Einrichtungen zahlen – etwa wenn Menschenleben auf dem Spiel stehen (Krankenhäuser) oder wenn die Aufgabe die einzige Alternative wäre. Für eine Arztpraxis ist das in der Regel nicht der Fall, wenn Backups existieren.

D.9.2. Der Kontakt mit den Erpressern

Kommunizieren Sie nicht mit den Erpressern, ohne vorher rechtlichen Rat eingeholt zu haben. Jede Kommunikation kann Ihre rechtliche Position beeinflussen. Insbesondere: Keine Zahlungszusagen, keine Verhandlungen über die Lösegeldhöhe, keine Preisgabe von Informationen über Ihre Datenlage oder Versicherungssituation.

Falls Sie doch kommunizieren: Dokumentieren Sie jeden Austausch vollständig. Diese Dokumentation ist für Strafverfolgungsbehörden wertvoll.

D.9.3. Die Drohung mit Veröffentlichung im Darknet

Moderne Ransomware-Angriffe folgen oft einem doppelten Erpressungsschema (Double Extortion): Die Dateien werden verschlüsselt **und** gestohlen. Die Erpresser drohen dann, die gestohlenen Patientendaten im Darknet zu veröffentlichen, wenn nicht gezahlt wird. Das ist eine andere Qualität als reine Dateiverschlüsselung – weil sie nicht durch Backup-Wiederherstellung gelöst werden kann.

Was tun, wenn mit Darknet-Veröffentlichung gedroht wird:

Erstens: Die Drohung ernst nehmen, aber nicht in Panik verfallen. Nicht alle Drohungen werden umgesetzt – Erpresser haben ein Interesse daran, dass Sie zahlen, nicht daran, Ihre Daten zu veröffentlichen.

Zweitens: Sofort rechtlichen Rat einholen. Ein auf IT-Recht und Datenschutz spezialisierter Anwalt kann einschätzen, welche rechtlichen Optionen bestehen und wie die Kommunikation mit den Erpressern gestaltet werden sollte.

Drittens: Die Datenschutz-Meldepflicht auslösen. Wenn Patientendaten gestohlen wurden – und eine glaubhafte Drohung zur Veröffentlichung das nahelegt –, greift Art. 33 DSGVO. Die 72-Stunden-Frist läuft ab dem Zeitpunkt, zu dem Sie Kenntnis von der möglichen Datenpanne hatten.

Viertens: Betroffene Patienten informieren, wenn ein hohes Risiko besteht. Das ist rechtlich geboten (Art. 34 DSGVO) und auch im eigenen Interesse – Patienten, die durch eine Nachricht von Ihnen informiert werden, reagieren anders als Patienten, die ihre Daten selbst im Darknet entdecken.

Fünftens: Die Strafanzeige erstatten. Die ZAC der Landeskriminalämter hat Erfahrung mit Double-Extortion-Fällen. Eine Anzeige verhindert zwar nicht die Veröffentlichung, schafft aber eine offizielle Dokumentation und kann in manchen Fällen zu einer Festnahme der Täter führen.

Sechstens: Zahlung ist auch hier keine verlässliche Lösung. Es gibt keine Garantie, dass gestohlene Daten nach Zahlung tatsächlich gelöscht werden. Erpresser, die einmal zahlende Opfer gefunden haben, kommen erfahrungsgemäß zurück.

D.9.4. Darknet-Monitoring

Es gibt Dienste, die das Darknet nach gestohlenen Datensätzen durchsuchen und Alarm geben, wenn eigene Daten auftauchen. Für eine Arztpraxis ist das in der Regel kein regelmäßiges Monitoring wert – aber im Krisenfall, wenn ein Datendiebstahl vermutet wird, können spezialisierte Dienstleister einmalig prüfen, ob Daten bereits kursieren. Das BSI und die ZAC können entsprechende Hinweise geben.

D.10. Checkliste: Krisenmanagement für Arztpraxen

D.10.1. Vorbereitung (jetzt, nicht im Notfall)

- ☐ Kontaktdaten der zuständigen Landesdatenschutzbehörde sind im Notfalldokument.
- ☐ Kontaktdaten der ZAC meines Bundeslandes sind im Notfalldokument.
- ☐ Kontaktdaten der KV meines Bundeslandes sind im Notfalldokument.
- ☐ BSI-Warnmeldungen sind abonniert (`bsi.bund.de`).
- ☐ Ein IT-Dienstleister mit Incident-Response-Erfahrung und PVS-Kenntnissen ist identifiziert und seine Nummer im Notfalldokument.
- ☐ Ein auf Medizinrecht spezialisierter Anwalt ist identifiziert, falls Datenschutz-Fragen auftauchen.

- ☐ Eine zweite E-Mail-Adresse bei einem anderen Anbieter ist eingerichtet.
- ☐ Eine Offline-Patientenliste (Name, Geburtsdatum, Versicherungsdaten, Allergien, Dauermedikation) ist aktuell und offline verfügbar.
- ☐ Offline-Kontaktliste für Partner (Überweisungs-Ärzte, Labore, Kliniken) mit Telefonnummern ist vorhanden.
- ☐ Meine Praxis-Telefonnummer ist auf meiner Website und in Aushängen prominent platziert.
- ☐ Papierformulare für Notfallbetrieb (Patientenerfassung, Rezepte, Arbeitsunfähigkeit) sind vorgehalten.
- ☐ Mein aktuellstes Backup liegt offline – nicht synchronisiert mit dem Primärsystem.
- ☐ Cyber-Versicherung ist vorhanden; Notfall-Hotline ist im Notfalldokument eingetragen.

D.10.2. Im Krisenfall – Sofortmaßnahmen

- ☐ Betroffenes Gerät/System sofort vom Netz getrennt (Ethernet, WLAN, Bluetooth).
- ☐ Bei Bedarf TI-Konnektor vom Netzwerk trennen (mit IT-Dienstleister absprechen).
- ☐ Cloud-Synchronisation von anderen Geräten pausiert.
- ☐ Dokumentation des Vorfalls gestartet (was, wann, was getan).
- ☐ Analyse: Welche Patientendaten sind betroffen? (Diagnosen, Medikationen, Stammdaten?)
- ☐ IT-Dienstleister informiert.
- ☐ Datenschutzbehörde informiert, wenn Datenpanne vorliegt (72-Stunden-Frist, Art. 33 DSGVO).
- ☐ KV informiert, falls PVS betroffen oder Kassenabrechnung beeinträchtigt.
- ☐ Strafanzeige erstattet (Aktenzeichen notieren).
- ☐ Cyber-Versicherung informiert.
- ☐ Betroffene Patienten informiert – proaktiv, ehrlich, konkret.
- ☐ Passwörter von einem sauberen Gerät aus geändert.
- ☐ Notfallbetrieb mit Papierformularen gestartet.

D.10.3. Bei Ransomware zusätzlich

- ☐ `nomoreransom.org` geprüft – gibt es ein kostenloses Entschlüsselungstool?
- ☐ Nicht gezahlt ohne vorherigen rechtlichen Rat.
- ☐ Kommunikation mit Erpressern dokumentiert.
- ☐ Bei Double-Extortion-Drohung: Anwalt und ZAC kontaktiert.

D.10.4. Wiederherstellung

- ☐ Einfallstor identifiziert und geschlossen, bevor das System wieder online geht.
- ☐ System/PVS vollständig neu aufgesetzt – kein Bereinigen ohne Neuinstallation.
- ☐ PVS vom Hersteller bestätigt „sauber" und aktuell.
- ☐ Backup aus dem Zeitraum vor der Infektion verwendet (mindestens 2-4 Wochen zurück).
- ☐ Backup vor dem Zurückspielen auf Schadsoftware geprüft.
- ☐ TI-Authentifizierung (eHBA/Konnektor) neu überprüft und ggf. neu konfiguriert.

- ☐ Alle Passwörter geändert, bevor das System produktiv genutzt wird.
- ☐ Kassenpatienten und KV über Wiederaufnahme informiert.
- ☐ Verspätete Abrechnungsdaten mit KV klären.

E. Prüfliste

Theorie ist gut – aber am Ende zählt, was wirklich umgesetzt ist. Dieser Anhang enthält eine kompakte Prüfliste, mit der Sie den aktuellen Stand Ihrer IT-Sicherheit strukturiert erfassen können. Sie fasst die wichtigsten Maßnahmen aus allen Kapiteln in einem einzigen Dokument zusammen und eignet sich sowohl für die eigene Bestandsaufnahme als auch als Gesprächsgrundlage mit Ihrem IT-Dienstleister.

Gehen Sie die Liste einmal pro Jahr durch – oder immer dann, wenn sich etwas Wesentliches ändert: neuer IT-Dienstleister, neue Mitarbeiter, neue Cloud-Dienste, Umzug der Praxis.

Was Sie in diesem Anhang erwartet:

E1 – IT-Sicherheits-Prüfliste für Arztpraxen: Alle Checklisten des Guides in einem Dokument. Gegliedert nach den Themenbereichen des Guides: Infrastruktur & Zugänge, Backups, E-Mail & Kommunikation, Endgeräte, Telematik-Infrastruktur, KI-Nutzung, Recht & Datenschutz, Notfallplanung. Mit zusätzlichen Punkten speziell für Arztpraxen: PVS-Sicherheit, TI-Konnektor, medizinische Geräte am Netz, KBV-Richtlinie-Compliance, Berufsgeheimnis-Schutz. Nicht als einmalige Aufgabe gedacht, sondern als regelmäßiges Arbeitsinstrument.

E.1. IT-Sicherheits-Prüfliste für Arztpraxen und MVZ

Diese Prüfliste fasst alle Checklisten des Guides in einem Dokument zusammen. Sie ist kein Test – sie ist ein Arbeitsinstrument. Gehen Sie sie einmal pro Jahr durch, oder immer dann wenn sich etwas Wesentliches ändert: neuer IT-Dienstleister, neue Mitarbeiter, Umzug der Praxis, neue Cloud-Dienste, neue medizinische Geräte am Netz.

Nicht jeder Punkt ist für jede Praxis gleich relevant. Eine Einzelpraxis ohne Mitarbeiter überspringt die Abschnitte zu Mitarbeiterverwaltung. Ein MVZ mit mehreren Standorten hat erweiterte Anforderungen. Konzentrieren Sie sich auf das, was für Ihre konkrete Situation zutrifft.

Legende: Sie = Praxisinhaber/Verantwortliche/r · IT = IT-Dienstleister · G = Gemeinsam · PVS = Praxisverwaltungssystem

---

E.1.1. 1. Telematik-Infrastruktur (TI)

- ☐ TI-Konnektor ist installiert und aktuell – Firmware-Stand regelmäßig geprüft. *(IT)*
- ☐ eHBA (elektronischer Heilberufsausweis) ist vorhanden, aktuell und sicher verwahrt – nicht im Arbeitsbereich liegen lassen. *(Sie)*
- ☐ eHBA wird ausschließlich für berechtigte Zugriffe genutzt – nicht dauerhaft eingesteckt. *(Sie)*
- ☐ Primanota (Praxis-Konnektions-Verwaltung) ist richtig konfiguriert – nur notwendige Dienste aktiviert. *(IT)*
- ☐ VPN/Proxy zur TI ist aktiv und korrekt konfiguriert – keine direkten Ports zum Internet offengelegt. *(IT)*
- ☐ TI-Zertifikate sind aktuell und werden regelmäßig erneuert (vor Ablauf). *(IT)*
- ☐ TI-Verbindungen werden regelmäßig getestet – monatliches Audit am einfachsten über PVS-Logs. *(IT)*
- ☐ Notfallplan bei TI-Ausfall ist vorhanden: Wie läuft die Kassenabrechnung ohne TI? *(Sie / IT)*
- ☐ Fallback-Zugang zur KV ist dokumentiert (Telefon, E-Mail für Notfall-Kontakt). *(Sie)*

E.1.2. 2. Praxisverwaltungssystem (PVS)

- ☐ PVS läuft auf deutschen/europäischen Servern – nicht auf US-Infrastruktur. *(Sie)*
- ☐ PVS-Daten sind verschlüsselt in der Cloud oder vollständig lokal gespeichert. *(IT)*
- ☐ PVS-Software wird vom Hersteller regelmäßig aktualisiert – mindestens monatliche Updates. *(IT)*
- ☐ Sicherheits-Patches für die PVS werden innerhalb von 30 Tagen eingespielt. *(IT)*
- ☐ PVS-Zugang erfolgt nur über starke Authentifizierung: Benutzername + Passwort + Zwei-Faktor (falls möglich). *(IT)*
- ☐ Jeder Praxis-Mitarbeiter hat einen eigenen PVS-Zugang – keine gemeinsamen Accounts. *(You)*
- ☐ Standard-Passwörter der PVS wurden sofort nach Installation geändert. *(IT)*
- ☐ PVS-Backup wird täglich durchgeführt und regelmäßig getestet (mindestens monatlich). *(IT)*
- ☐ PVS-Backups sind verschlüsselt und liegen auf einem separaten, nicht ständig angeschlossenen System. *(IT)*
- ☐ PVS-Audit-Logs sind aktiviert – alle Datenzugriffe werden protokolliert. *(IT)*
- ☐ Audit-Logs werden regelmäßig überprüft (mindestens quartalsweise) auf verdächtige Zugriffe. *(G)*
- ☐ Archivfunktion in der PVS für alte Patienten ist aktiv – Datensätze nach Ablauf der Aufbewahrungsfrist werden archiviert/gelöscht. *(Sie / IT)*
- ☐ PVS-Herstellersupport ist aktiv – Sie erhalten Benachrichtigungen bei Sicherheitsproblemen. *(IT)*
- ☐ Notfall-Zugang zur PVS (z. B. Read-Only-Modus ohne Verschlüsselung) ist dokumentiert für den Fall eines Ausfalls. *(IT)*

E.1.3. 3. Medizinische Geräte am Netzwerk

- ☐ Bestandsliste aller medizinischen Geräte am Netzwerk ist vorhanden (EKG, Blutdruckmessgeräte, PACS-Systeme, etc.). *(Sie / IT)*
- ☐ Jedes Gerät hat eine Inventarnummer und einen Standort dokumentiert. *(Sie)*
- ☐ Firmware und Software aller Geräte werden regelmäßig aktualisiert (falls Updates verfügbar sind). *(IT)*
- ☐ Alte/EOL-Geräte (End-of-Life) ohne Hersteller-Support werden identifiziert und ggf. ausgebaut. *(Sie / IT)*
- ☐ Medizinische Geräte sind vom eigentlichen Arbeitsnetwork isoliert – oder nur über VPN erreichbar. *(IT)*
- ☐ Standardzugangsdaten (Admin-Passwörter) aller Geräte wurden geändert. *(IT)*
- ☐ Ein Geräte-Manager (Person oder IT-Dienstleister) ist benannt, der für Updates und Wartung zuständig ist. *(Sie)*
- ☐ Wenn Geräte das Internet brauchen (z. B. Cloud-Upload von Messwerten): Verbindung ist verschlüsselt und Datenschutzerklärung des Herstellers geprüft. *(IT)*

E.1.4. 4. Domain & DNS

- ☐ Sie sind der registrierte Inhaber Ihrer Domain – nicht Ihr Webdesigner oder Hoster. *(Sie)*
- ☐ Sie haben Zugang zum Konto bei Ihrem Registrar und kennen das Passwort. *(Sie)*
- ☐ Die automatische Verlängerung Ihrer Domain ist aktiviert und die Zahlungsmethode ist aktuell. *(Sie)*
- ☐ Das Ablaufdatum Ihrer Domain ist in Ihrem Kalender eingetragen (als Erinnerung 3 Monate vorher). *(Sie)*
- ☐ Sie haben eine Kopie Ihrer DNS-Einträge im Notfalldokument. *(Sie)*
- ☐ Sie wissen, wie Sie im Notfall den A-Record und den MX-Record Ihrer Domain ändern können. *(Sie)*
- ☐ DNSSEC ist aktiviert (wenn Registrar dies anbietet). *(IT)*

E.1.5. 5. E-Mail und Kommunikation

- ☐ Ihre geschäftliche E-Mail läuft über eine eigene Domain – nicht über @gmail.com, @web.de o. ä. *(Sie)*
- ☐ E-Mail-Provider läuft auf europäischen Servern – nicht auf US-Infrastruktur (Gmail/Outlook sind nicht geeignet). *(Sie)*
- ☐ SPF-Record ist eingetragen und korrekt – geprüft mit mxtoolbox.com. *(IT)*
- ☐ Alle Dienste, die E-Mails in Ihrem Namen versenden, sind im SPF-Record aufgeführt. *(IT)*
- ☐ DKIM ist für alle sendenden Dienste eingerichtet. *(IT)*
- ☐ DMARC ist eingerichtet – mindestens mit `p=none` und einer Reporting-Adresse. *(IT)*
- ☐ Spam-Filter ist aktiv und wird regelmäßig überprüft. *(IT)*

- ☐ E-Mail-Anhänge werden auf Viren geprüft. *(IT)*
- ☐ Ihre E-Mails werden lokal archiviert und sind Teil Ihres Backups – nicht nur Cloud. *(IT / Sie)*
- ☐ Sie haben eine alternative E-Mail-Adresse bei einem anderen Anbieter (für Notfall). *(Sie)*
- ☐ Ihre Patienten kennen mindestens eine weitere Möglichkeit, Sie zu erreichen (Telefon, SMS). *(Sie)*
- ☐ Sie wissen, wie Sie den MX-Record Ihrer Domain ändern können, wenn Sie den E-Mail-Anbieter wechseln müssen. *(Sie)*
- ☐ Mitarbeiter sind für Phishing und verdächtige E-Mails sensibilisiert – regelmäßig schulen. *(Sie)*
- ☐ Sie überprüfen regelmäßig (mindestens monatlich) die Authentifizierungs-Logs Ihres E-Mail-Anbieters auf verdächtige Zugriffe. *(Sie / IT)*

KIM (Kommunikation im Medizinwesen) – falls vorhanden:

- ☐ KIM-Adresse ist registriert und aktiv. *(Sie / IT)*
- ☐ KIM wird für Arztbriefe und Befunde genutzt – als sichere Alternative zu E-Mail. *(Sie)*
- ☐ KIM-Verbindung wird regelmäßig getestet (mindestens monatlich). *(IT)*

E.1.6. 6. Passwörter & Zwei-Faktor-Authentifizierung

- ☐ Sie nutzen einen Passwort-Manager für alle wichtigen Dienste (PVS, E-Mail, Cloud, KIM, etc.). *(Sie)*
- ☐ Passwort-Manager selbst ist geschützt: Starkes Master-Passwort, lokal gespeichert oder in Offline-Backup. *(Sie)*
- ☐ Jeder Dienst hat ein eigenes, starkes Passwort – kein Passwort wird mehrfach verwendet. *(Sie)*
- ☐ Passwort-Manager wird regelmäßig aktualisiert und die Datenbank wird gebackuppt. *(Sie / IT)*
- ☐ Sie haben Ihre E-Mail-Adresse auf `haveibeenpwned.com` geprüft. *(Sie)*
- ☐ Standard-/Werkspasswörter wurden bei allen Geräten und Diensten geändert. *(IT / Sie)*
- ☐ Keine Passwörter in unverschlüsselten Dateien oder auf Post-its. *(Sie)*
- ☐ 2FA ist für E-Mail-Konto aktiv. *(Sie)*
- ☐ 2FA ist für alle Cloud-Dienste aktiv (PVS-Cloud, Cloud-Speicher, etc.). *(Sie)*
- ☐ 2FA ist für VPN/Remote-Zugriff aktiv. *(IT)*
- ☐ Sie nutzen TOTP (App wie Authenticator oder Authy) statt SMS als zweiten Faktor, wo immer möglich. *(Sie)*
- ☐ Backup-Codes für alle 2FA-geschützten Dienste sind sicher aufbewahrt – nicht nur auf dem Smartphone. *(Sie)*
- ☐ Die wichtigsten Zugangsdaten sind im Notfalldokument dokumentiert (verschlüsselt oder offline). *(Sie)*
- ☐ Passwort-Policy für alle Mitarbeiter ist dokumentiert (Mindestlänge, Wechselfristen, Wiederverwenden-Verbot). *(Sie)*

E.1.7. 7. Endgeräte & Updates

- ☐ Automatische Updates sind für Betriebssystem auf allen Geräten aktiviert. *(IT / Sie)*
- ☐ Browser werden automatisch aktualisiert. *(IT)*
- ☐ Browser-Erweiterungen sind auf das Minimum reduziert und aktuell. *(Sie)*
- ☐ Praxismanagement-Software und Fachsoftware werden mindestens quartalsweise manuell auf Updates geprüft. *(Sie / IT)*
- ☐ Router-Firmware ist aktuell. *(IT / Sie)*
- ☐ NAS-Firmware und NAS-Pakete sind aktuell (falls NAS vorhanden). *(IT / Sie)*
- ☐ Sie haben geprüft, ob eingesetzte Software noch im Hersteller-Support ist (kein End-of-Life). *(IT / Sie)*
- ☐ Ein einfaches Software-Inventar mit Versionsständen ist angelegt. *(IT / Sie)*
- ☐ Alle Praxis-Smartphone haben eine starke Bildschirmsperre und aktuelle Software. *(Sie)*
- ☐ Die Fernlösch-Funktion ist auf Laptop und Smartphone eingerichtet und getestet. *(IT)*
- ☐ Sie wissen, was Sie in den ersten Stunden nach einem Gerätediebstahl tun müssen. *(Sie)*
- ☐ Kein lokaler Admin-Account wird für den Alltag genutzt – Arbeitsbenutzer ohne Admin-Rechte. *(IT)*
- ☐ Bildschirmsperre greift nach spätestens 5 Minuten Inaktivität. *(IT / Sie)*
- ☐ Keine unbekannten USB-Geräte werden angeschlossen (USB-Geräte sind deaktiviert oder per Policy blockiert). *(Sie)*
- ☐ Alte/EOL-Geräte (außer Garantie) werden aus dem Netzwerk entfernt oder neu aufgesetzt. *(IT)*

E.1.8. 8. Verschlüsselung

- ☐ Festplattenverschlüsselung ist auf allen Laptops aktiv (FileVault / BitLocker / LUKS). *(IT)*
- ☐ Bei BitLocker: Die Online-Speicherung des Schlüssels ist geprüft und eine bewusste Entscheidung getroffen. *(Sie)*
- ☐ Der Wiederherstellungsschlüssel ist sicher aufbewahrt – getrennt vom Gerät. *(Sie)*
- ☐ Praxis-Server/NAS: Festplatte ist verschlüsselt. *(IT)*
- ☐ Alle Smartphone haben eine Bildschirmsperre – damit ist die Geräteverschlüsselung aktiv. *(Sie)*
- ☐ Mein NAS verschlüsselt zumindest die Ordner mit sensiblen Daten (Patientenakten, Abrechnungen). *(IT / Sie)*
- ☐ Externe Festplatten und USB-Sticks mit Patientendaten sind verschlüsselt. *(IT / Sie)*
- ☐ Für besonders sensible Cloud-Daten wird clientseitige Verschlüsselung genutzt (z. B. mit Cryptomator). *(Sie / IT)*

- ☐ E-Mails mit Befunden oder Diagnosen werden verschlüsselt versendet (S/MIME oder PGP). *(Sie / IT)*

E.1.9. 9. Backups

- ☐ Sie haben mindestens zwei Backup-Kopien Ihrer Daten – zusätzlich zum Original (3-2-1-Regel). *(IT / Sie)*
- ☐ Ihre Backups liegen auf mindestens zwei verschiedenen Medien oder Diensten. *(IT / Sie)*
- ☐ Mindestens eine Backup-Kopie befindet sich außerhalb Ihrer Praxis oder an einem physisch getrennten Standort. *(IT / Sie)*
- ☐ Sie nutzen eine echte Backup-Lösung (z. B. Veeam, Duplicati) – keine reine Cloud-Synchronisierung wie OneDrive oder Dropbox. *(IT)*
- ☐ PVS-Backups werden täglich durchgeführt. *(IT)*
- ☐ Backups bewahren Versionen für mindestens 30 Tage auf (für Ransomware-Wiederherstellung). *(IT)*
- ☐ Ihre externe Backup-Festplatte ist nicht dauerhaft angeschlossen – oder Sie nutzen Object Lock/Immutable Backups. *(IT / Sie)*
- ☐ Alle Backups – lokal und in der Cloud – sind verschlüsselt. *(IT)*
- ☐ Bei Cloud-Backups ist clientseitige Verschlüsselung aktiv (Daten sind verschlüsselt, bevor sie in die Cloud gehen). *(IT)*
- ☐ Der Verschlüsselungsschlüssel ist sicher und getrennt vom Backup aufbewahrt. *(Sie)*
- ☐ Sie erhalten aktive Benachrichtigungen, wenn ein Backup fehlschlägt – und überprüfen diese täglichen Berichte. *(IT / Sie)*
- ☐ Sie haben Ihr Backup zuletzt getestet und die Wiederherstellung funktioniert (Restore-Test). *(IT / Sie)*
- ☐ Patientendaten und Abrechnungsdaten werden mindestens 10 Jahre aufbewahrt (nach § 630f BGB, § 147 AO). *(Sie)*

Falls NAS vorhanden:

- ☐ Sie wissen, dass RAID kein Backup ist – Sie haben ein separates Backup Ihres NAS. *(Sie)*
- ☐ Das NAS-Backup enthält eine physisch getrennte Kopie und eine Offsite-Kopie. *(IT / Sie)*
- ☐ Auf Ihrem NAS laufen nur Dienste, die Sie aktiv nutzen – alle anderen sind deaktiviert. *(IT)*
- ☐ Das NAS ist nicht direkt aus dem Internet erreichbar – oder der Zugang ist per VPN abgesichert. *(IT)*
- ☐ Standard-Passwort des NAS wurde geändert. *(IT)*

E.1.10. 10. Netzwerk & Internet

- ☐ Router-Modell und Firmware sind aktuell. *(IT / Sie)*
- ☐ Standard-Passwort des Routers wurde geändert. *(IT / Sie)*
- ☐ Gäste-WLAN ist vom Arbeitsnetz getrennt – Patienten/Besucher nutzen anderes WLAN. *(IT)*
- ☐ WLAN-Verschlüsselung ist WPA2 oder WPA3. *(IT / Sie)*
- ☐ WLAN-Passwort ist stark und wird regelmäßig geändert (mindestens jährlich). *(Sie / IT)*
- ☐ Fernzugriff (Remote) läuft über VPN, nicht über offene Ports wie RDP direkt aus dem Internet. *(IT)*
- ☐ VPN ist mit starker Authentifizierung geschützt (2FA oder Zertifikat). *(IT)*
- ☐ Ihre Zugangsdaten für den Internetanschluss sind notiert und im Notfalldokument. *(Sie)*
- ☐ Sie haben ein aktuelles Backup der Router-Konfiguration. *(IT)*
- ☐ Sie wissen, wie Sie Ihren Smartphone-Hotspot aktivieren – und haben ihn getestet. *(Sie)*
- ☐ Ihr Mobilfunktarif erlaubt Hotspot-Nutzung. *(Sie)*
- ☐ Die Störungs-Hotline Ihres Internet-Providers ist im Notfalldokument eingetragen. *(Sie)*
- ☐ In öffentlichen WLANs nutzen Sie eine VPN-Verbindung – nicht die offene WLAN. *(Sie)*
- ☐ Das automatische Verbinden mit bekannten WLANs ist auf Ihren Geräten deaktiviert (Sicherheitsrisiko). *(Sie / IT)*
- ☐ Netzwerk-Segmentierung ist vorhanden: Patientendaten-Netzwerk ist vom Gäste-Netzwerk getrennt. *(IT)*

E.1.11. 11. Cloud-Dienste & Online-Speicher

- ☐ Ihre wichtigsten Cloud-Daten sind Teil Ihres normalen Backups – nicht nur in der Cloud. *(IT / Sie)*
- ☐ Alle Cloud-Anbieter laufen auf europäischen Servern – US-Cloud (AWS, Google Cloud, Azure) ist für Patientendaten nicht geeignet. *(Sie / IT)*
- ☐ Als Wiederherstellungskontakt ist eine E-Mail-Adresse hinterlegt, die nicht beim selben Anbieter liegt. *(Sie)*
- ☐ Sie nutzen für kritische Funktionen nicht ausschließlich einen einzigen Cloud-Anbieter – Vendor-Lock-in vermeiden. *(Sie)*
- ☐ Sie wissen, wo Sie den Support Ihrer wichtigsten Cloud-Anbieter erreichen – Kontaktdaten sind notiert. *(Sie)*
- ☐ Ihre wichtigsten laufenden Daten sind auch lokal verfügbar – nicht nur in der Cloud. *(Sie / IT)*
- ☐ Datenstandort Ihrer Cloud-Dienste ist bekannt und DSGVO-konform (EU/EWR). *(Sie / IT)*
- ☐ Exit-Strategie ist vorhanden: Sie können Ihre Daten bei Bedarf jederzeit exportieren/migrieren. *(Sie / IT)*
- ☐ Auftragsverarbeitungsverträge (AVV) mit allen Cloud-Anbietern sind vorhanden und aktuell. *(Sie / IT)*

☐ Zwei-Faktor-Authentifizierung ist für alle Cloud-Konten aktiv. *(Sie)*

E.1.12. 12. Virenschutz & Schutz vor Schadsoftware

☐ Virenschutz-Software ist auf allen Geräten installiert und aktuell. *(IT / Sie)*
☐ Automatische Signatur-Updates sind aktiv. *(IT)*
☐ Ransomware-Schutz ist aktiviert. *(IT)*
☐ Web-Filter / DNS-Schutz für gefährliche/bösartige Websites ist aktiv. *(IT)*
☐ Browser und Browser-Plugins sind aktuell und auf das Minimum reduziert. *(IT / Sie)*
☐ Es werden keine raubkopierten oder nicht vertrauenswürdigen Softwarequellen genutzt. *(Sie)*
☐ Lizenzen des Virenschutzes sind aktuell und nicht abgelaufen. *(Sie / IT)*
☐ Geplante Scans sind aktiv (mindestens wöchentlich bei kritischen Systemen). *(IT)*

E.1.13. 13. Social Engineering & Phishing

☐ Sie prüfen die tatsächliche Absenderadresse bei verdächtigen E-Mails – nicht nur den Anzeigenamen. *(Sie)*
☐ Sie klicken nicht auf Links in E-Mails, die Sie nicht erwartet haben – Sie rufen die Website direkt auf. *(Sie)*
☐ Sie öffnen keine Anhänge aus unbekannten oder verdächtigen Quellen. *(Sie)*
☐ Geänderte Bankverbindungen werden immer telefonisch mit dem Absender bestätigt – niemals per E-Mail. *(Sie)*
☐ Sie wissen, was Sie tun müssen, wenn Sie auf eine Phishing-Mail hereingefallen sind (Session-Terminierung, Passwort-Änderung, ggf. Anzeige). *(Sie)*
☐ Sie wissen, wo Sie in Ihren wichtigsten Diensten (PVS, E-Mail, Cloud) alle aktiven Sitzungen beenden können. *(Sie)*
☐ Mitarbeiter sind für Phishing sensibilisiert – regelmäßig Schulung und Simulation. *(Sie)*
☐ Ihre Mitarbeiter kennen die Eskalationskette: An wen wenden Sie sich bei verdächtigen E-Mails? *(Sie)*

E.1.14. 14. KI-Tools sicher nutzen

☐ Sie wissen, welche KI-Tools Sie nutzen und wie diese Ihre Daten verarbeiten. *(Sie)*
☐ Sie geben keine personenbezogenen Patientendaten in öffentliche KI-Tools (ChatGPT, Copilot, Claude Free) ein. *(Sie)*
☐ Sie haben die Datenschutzeinstellungen Ihres KI-Tools geprüft – insbesondere ob Eingaben zum Training genutzt werden. *(Sie)*

- ☐ Sie nutzen ärztliche Schweigepflicht-Anforderungen nicht transparent um KI-Tools, die diese nicht erfüllen. *(Sie)*
- ☐ Sie prüfen KI-Output auf Fakten und Richtigkeit, bevor Sie diese an Patienten weitergeben (KI-Halluzinationen!). *(Sie)*
- ☐ Sie haben mit Patienten ggf. geklärt, ob der Einsatz von KI in ihrer Behandlung erlaubt ist. *(Sie)*
- ☐ Sie laden keine biometrischen Daten (Fotos von Patienten, Stimme, Videos) in KI-Tools hoch. *(Sie)*
- ☐ Auftragsverarbeitungsvertrag (AVV) mit KI-Anbieter ist vorhanden, wenn Sie personenbezogene Patientendaten verarbeiten. *(Sie / IT)*

E.1.15. 15. Datenschutz & DSGVO

- ☐ Sie führen ein Verzeichnis von Verarbeitungstätigkeiten (VVT) nach Art. 30 DSGVO. *(Sie)*
- ☐ Für jede Verarbeitungstätigkeit ist eine Rechtsgrundlage nach Art. 6 DSGVO benannt. *(Sie)*
- ☐ Art. 9 DSGVO (Gesundheitsdaten) ist in Ihrem VVT berücksichtigt. *(Sie)*
- ☐ Drittlandübermittlungen sind im VVT dokumentiert – mit der jeweiligen Garantie (SCCs, DPF o. ä.). *(Sie)*
- ☐ **Wichtig: EU-US Data Privacy Framework ist für Gesundheitsdaten NICHT ausreichend – meiden Sie US-Anbieter.** *(Sie)*
- ☐ Löschfristen sind für jede Datenkategorie festgelegt und werden eingehalten (insbesondere 10 Jahre für Patientenakten). *(Sie)*
- ☐ Die TOMs (Technische und Organisatorische Maßnahmen) sind im VVT dokumentiert – Verschlüsselung, Backup, Zugangsschutz. *(Sie)*
- ☐ Ihre Datenschutzerklärung auf der Website ist deckungsgleich mit dem VVT. *(Sie)*
- ☐ Datenschutzbeauftragter ist bestellt, falls erforderlich (meist: ja, für Arztpraxen ab 10 Personen oder bei automatisierter Datenverarbeitung). *(Sie)*
- ☐ Sie wissen, wie Sie auf Auskunfts- oder Löschanfragen von Patienten reagieren (Art. 15, 17 DSGVO). *(Sie)*
- ☐ Cookie-Banner (falls Website vorhanden) ermöglicht echte Ablehnung ohne Umwege. *(Sie)*
- ☐ Newsletter-Verteiler (falls vorhanden) basiert auf dokumentierten Double-Opt-in-Einwilligungen. *(Sie)*
- ☐ Kontaktdaten Ihrer zuständigen Landesdatenschutzbehörde sind im Notfalldokument. *(Sie)*
- ☐ Sie wissen, was im Falle einer Datenpanne zu tun ist – Meldung innerhalb von 72 Stunden (Art. 33 DSGVO). *(Sie)*

Auftragsverarbeitungsverträge (AVV):

- ☐ AVV mit IT-Dienstleister ist geschlossen und aktuell. *(Sie)*
- ☐ AVV mit PVS-Anbieter ist vorhanden. *(Sie)*
- ☐ AVV mit allen genutzten Cloud-Anbietern ist vorhanden. *(Sie)*
- ☐ AVV mit KIM-Anbieter ist vorhanden (falls KIM genutzt). *(Sie)*
- ☐ AVV mit Hosting-Provider / Website-Betreiber ist vorhanden. *(Sie)*

- ☐ AVV mit allen medizinischen Partnern (Labore, Radiologien, überweisende Ärzte) ist vorhanden. *(Sie)*
- ☐ Alle AVVs sind aktuell und vollständig – jährliche Prüfung. *(Sie)*
- ☐ Verschwiegenheitsverpflichtungen nach § 203 Abs. 4 StGB sind in alle Verträge mit Partnern aufgenommen. *(Sie)*

E.1.16. 16. Berufsgeheimnis & ärztliche Schweigepflicht (§ 203 StGB, § 630f BGB)

- ☐ Sie wissen, dass Sie als Arzt der Schweigepflicht unterliegen und § 203 StGB zum Schutz Ihrer Patientendaten. *(Sie)*
- ☐ Alle Endgeräte, auf denen geschützte Patientendaten gespeichert oder verarbeitet werden, sind verschlüsselt. *(IT)*
- ☐ Alle Mitarbeiter sind schriftlich zur Verschwiegenheit verpflichtet (idealerweise mit Verweis auf § 203 StGB). *(Sie)*
- ☐ Bei Ausscheiden von Mitarbeitern werden alle Zugangsdaten zum PVS geändert und Geräte zurückgegeben/gelöscht. *(Sie / IT)*
- ☐ Mit jedem externen Dienstleister (IT, Labore, Radiologie, überweisende Ärzte) liegt ein Auftragsverarbeitungsvertrag vor. *(Sie)*
- ☐ Dienstleisterverträge enthalten das Need-to-know-Prinzip: Der Partner erhält nur die Daten, die er konkret braucht. *(Sie)*
- ☐ Dienstleisterverträge regeln die Subunternehmerbeauftragung: Darf der Partner Unterstützer nutzen? *(Sie)*
- ☐ Sie halten sich an die Richtlinien Ihrer Kassenärztlichen Vereinigung oder der KBV. *(Sie)*
- ☐ Die KBV-Sicherheitsrichtlinie (IT-Sicherheitsrichtlinie nach § 390 SGB V) ist bekannt und Anforderungen sind umgesetzt. *(Sie / IT)*

E.1.17. 17. KBV-Sicherheitsrichtlinie Compliance (Kassenärzte)

- ☐ Sie kennen die KBV-Sicherheitsrichtlinie und deren Anforderungen. *(Sie)*
- ☐ Alle Anforderungen zu Passwörtern sind umgesetzt (Mindestlänge, Komplexität, Wechselfristen). *(IT)*
- ☐ Anforderungen zu Verschlüsselung (Festplatte, Transport) sind umgesetzt. *(IT)*
- ☐ Anforderungen zu Zugangsschutz und Rechteverwaltung sind umgesetzt. *(IT)*
- ☐ Anforderungen zu Dokumentation und Audit-Logging sind umgesetzt. *(IT)*
- ☐ Sicherheitsincidents werden dokumentiert und gemeldet (an KBV, wenn relevant). *(Sie / IT)*
- ☐ Regelmäßige Sicherheits-Schulungen für Mitarbeiter sind durchgeführt. *(Sie)*
- ☐ Ein Sicherheitsverantwortlicher (Person oder Rolle) ist benannt. *(Sie)*

E.1.18. 18. Website & Online-Präsenz

- ☐ Ihr Impressum enthält alle Pflichtangaben – E-Mail-Adresse und mindestens einen weiteren Kontaktweg. *(Sie)*
- ☐ Das Impressum ist über einen gut sichtbaren Link auf jeder Seite erreichbar. *(Sie)*
- ☐ Ihre Datenschutzerklärung ist vollständig und deckt alle Dienste ab, die Sie tatsächlich nutzen. *(Sie)*
- ☐ Sie überprüfen Impressum und Datenschutzerklärung mindestens jährlich. *(Sie)*
- ☐ Alle Bilder auf Ihrer Website stammen aus eigener Erstellung oder von lizenzierten Quellen. *(Sie)*
- ☐ Für alle Fotos mit erkennbaren Personen (Patienten, Mitarbeiter) haben Sie schriftliche Einwilligungen. *(Sie)*
- ☐ Alle eingesetzten Schriften (Fonts) sind für kommerzielle Nutzung lizenziert. *(Sie)*
- ☐ Ihre SSL-Konfiguration ist aktuell (mindestens TLS 1.2, idealerweise TLS 1.3). *(IT)*
- ☐ SSL-Zertifikat ist aktuell und wird vor Ablauf erneuert. *(IT)*
- ☐ Sie überprüfen die SSL-Bewertung Ihrer Website regelmäßig (https://www.ssllabs.com/). *(IT)*
- ☐ Sie nutzen einen automatischen Scanner, um die Website auf neue Tracker zu prüfen. *(Sie / IT)*
- ☐ Google Analytics und ähnliche Tracking-Tools sind datenschutzkonform konfiguriert (mit Anonymisierung). *(Sie)*
- ☐ Ihre Kontaktformulare nutzen HTTPS und haben einen CAPTCHA-Schutz gegen Bots. *(IT)*

E.1.19. 19. Notfallplanung & Krisenmanagement

Vorbereitung:

- ☐ Kontaktdaten der zuständigen Landesdatenschutzbehörde sind im Notfalldokument. *(Sie)*
- ☐ Kontaktdaten der ZAC (Zentrale Ansprechstelle Cybercrime) sind im Notfalldokument. *(Sie)*
- ☐ Kontaktdaten der KV Ihres Bundeslandes sind im Notfalldokument. *(Sie)*
- ☐ BSI-Warnmeldungen sind abonniert (bsi.bund.de). *(Sie)*
- ☐ Ein IT-Dienstleister mit Incident-Response-Erfahrung und PVS-Kenntnissen ist identifiziert. *(Sie)*
- ☐ Ein auf Medizinrecht spezialisierter Anwalt ist identifiziert (für Notfall-Fragen zu Datenschutz). *(Sie)*
- ☐ Eine zweite E-Mail-Adresse bei einem anderen Anbieter ist eingerichtet. *(Sie)*
- ☐ Eine Offline-Patientenliste (Name, Geburtsdatum, Versicherungsdaten, Allergien, Dauermedikation) ist aktuell. *(Sie)*
- ☐ Offline-Kontaktliste für Partner (Labore, Überweisungs-Ärzte, Kliniken, Apotheken) mit Telefonnummern. *(Sie)*
- ☐ Praxis-Telefonnummer und -Adresse sind auf Website und Aushängen prominent platziert. *(Sie)*
- ☐ Papierformulare für Notfallbetrieb sind vorgehalten (Patientenerfassung, Rezepte, Arbeitsunfähigkeit). *(Sie)*

- ☐ Ihr aktuellstes Backup liegt offline – nicht synchronisiert mit dem Primärsystem. *(IT)*
- ☐ Cyber-Versicherung ist vorhanden; Notfall-Hotline ist im Notfalldokument. *(Sie)*
- ☐ Notfall-Kontaktliste ist auch analog (auf Papier) verfügbar – nicht nur digital. *(Sie)*

Sofortmaßnahmen bei einem Vorfall:

- ☐ Betroffenes Gerät/System sofort vom Netz getrennt (Ethernet, WLAN, Bluetooth). *(Sie)*
- ☐ NAS/externe Festplatten vom Netz getrennt (falls vorhanden). *(Sie)*
- ☐ Cloud-Synchronisation von anderen Geräten pausiert. *(Sie)*
- ☐ Dokumentation des Vorfalls gestartet (was, wann, was getan – Timeline). *(Sie)*
- ☐ Analyse: Welche Patientendaten sind betroffen? (Diagnosen, Medikationen, Stammdaten?) *(Sie / IT)*
- ☐ IT-Dienstleister informiert. *(Sie)*
- ☐ Datenschutzbehörde informiert, wenn Datenpanne vorliegt (72-Stunden-Frist, Art. 33 DSGVO). *(Sie / IT)*
- ☐ KV informiert, falls PVS betroffen oder Kassenabrechnung beeinträchtigt. *(Sie)*
- ☐ Strafanzeige erstattet (Aktenzeichen notieren). *(Sie)*
- ☐ Cyber-Versicherung informiert. *(Sie)*
- ☐ Betroffene Patienten informiert – proaktiv, ehrlich, konkret (falls hohes Risiko). *(Sie)*
- ☐ Passwörter von einem sauberen Gerät aus geändert. *(Sie)*
- ☐ Notfallbetrieb mit Papierformularen gestartet. *(Sie)*

Bei Ransomware zusätzlich:

- ☐ `nomoreransom.org` geprüft – gibt es ein kostenloses Entschlüsselungstool? *(Sie / IT)*
- ☐ Nicht gezahlt ohne vorherigen rechtlichen Rat. *(Sie)*
- ☐ Kommunikation mit Erpressern dokumentiert (falls sie eine Nachricht hinterlassen haben). *(Sie)*
- ☐ Bei Double-Extortion-Drohung: Anwalt und ZAC kontaktiert. *(Sie)*

Wiederherstellung:

- ☐ Einfallstor identifiziert und geschlossen, bevor das System wieder online geht. *(IT)*
- ☐ System/PVS vollständig neu aufgesetzt – kein Bereinigen ohne Neuinstallation. *(IT)*
- ☐ PVS vom Hersteller bestätigt „sauber" und aktuell. *(IT)*
- ☐ Backup aus dem Zeitraum vor der Infektion verwendet (mindestens 2-4 Wochen zurück). *(IT)*
- ☐ Backup vor dem Zurückspielen auf Schadsoftware geprüft. *(IT)*
- ☐ TI-Authentifizierung (eHBA/Konnektor) neu überprüft und ggf. neu konfiguriert. *(IT)*
- ☐ Alle Passwörter geändert, bevor das System produktiv genutzt wird. *(Sie)*
- ☐ Kassenpatienten und KV über Wiederaufnahme des Betriebs informiert. *(Sie)*
- ☐ Verspätete Abrechnungsdaten mit KV klären. *(Sie)*

E.1.20. 20. Digitaler Nachlass & Notfallvollmacht

- ☐ Es gibt eine Vertrauensperson, die im Notfall handeln kann und weiß, dass sie diese Rolle hat. *(Sie)*
- ☐ Diese Person weiß, wo das Notfalldokument liegt – und wie sie darauf zugreifen kann. *(Sie)*
- ☐ Das Notfalldokument enthält klare Anweisungen für den Ausfall- oder Todesfall. *(Sie)*
- ☐ Sie haben eine schriftliche Vollmacht vorbereitet oder zumindest geprüft, ob Sie eine brauchen. *(Sie)*
- ☐ Das Thema ist in Ihrem Testament oder Ihrer Nachlassplanung berücksichtigt. *(Sie)*
- ☐ Praxisfortführung ist im Notfall geklärt: Wer übernimmt die Praxis? Wer hat Zugriff auf Patientendaten? *(Sie)*
- ☐ Patientendaten-Verwaltung nach Praxisschließung ist rechtlich geklärt (üblicherweise: an Nachfolger oder Archiv). *(Sie)*

E.1.21. 21. Regelmäßige Sicherheitsroutine

- ☐ Monatlicher Kalendertermin „IT-Kurzcheck" (15 Min.) ist eingerichtet. *(Sie)*
  - E-Mail-Log auf verdächtige Zugriffe prüfen
  - Backup-Status überprüfen (Erfolg/Fehler)
  - Neue Sicherheitswarnungen vom BSI checken
- ☐ Quartalsweiser Kalendertermin „IT-Wartung" (60 Min.) ist eingerichtet. *(Sie / IT)*
  - Router-Firmware überprüfen
  - Alle Passwörter auf Stärke überprüfen (ggf. erneuern)
  - Alle 2FA-Codes überprüfen
  - Backup-Test durchführen (Restore-Test)
- ☐ Jährlicher Kalendertermin „IT-Jahrescheck" (halber Tag) ist eingerichtet. *(Sie / IT)*
  - Gesamte Checkliste durchgehen
  - VVT aktualisieren (neue Dienste?)
  - AVVs überprüfen und aktualisieren
  - Mitarbeiter-Schulung durchführen
  - Notfalldokument aktualisieren
- ☐ Sie sind beim BSI-Newsletter angemeldet oder nutzen Have I Been Pwned für monatliche Leck-Prüfung. *(Sie)*
- ☐ Sie führen eine Liste der Zugänge für Dritte, die Sie monatlich überprüfen – wer hat noch Zugang? *(Sie)*
- ☐ Ihr Notfalldokument hat ein Datum der letzten Aktualisierung (sollte jährlich erneuert werden). *(Sie)*
- ☐ Passwörter für kritische Konten werden mindestens jährlich geändert. *(Sie)*
- ☐ Backup-Test wird mindestens halbjährlich durchgeführt. *(IT)*
- ☐ IT-Sicherheits-Schulung für Mitarbeiter wird mindestens jährlich durchgeführt. *(Sie)*

E.2. Zusammenfassung: Prioritäten für den Anfang

Falls Sie mit dieser Checkliste überfordert sind – machen Sie zuerst diese essentiellen Punkte:

1. **Backups:** Tägliche Backups mit 30-Tage-Versionierung, mindestens eine Kopie offline.
2. **Verschlüsselung:** Alle Festplatten verschlüsselt, PVS-Backups verschlüsselt.
3. **Passwörter:** Passwort-Manager, starke Passwörter, 2FA für E-Mail und Cloud.
4. **PVS-Sicherheit:** Auf europäischem Server, AVV vorhanden, regelmäßig aktualisiert.
5. **Datenschutz:** VVT vorhanden, Datenschutzerklärung, AVVs mit allen Partnern.
6. **Notfallplan:** Notfalldokument mit Kontakten, Offline-Patienten-/Partnerliste.

Diese sechs Punkte schützen Sie vor den meisten häufigen Angriffsszenarien. Alles andere ist Optimierung.