Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Die IT-Sicherheitsrichtlinie

nach § 75b SGB V

Hinweise des BSI für Anwenderinnen und Anwender

Einleitung

Die IT-Sicherheitsrichtlinie nach § 75b SGB V regelt die Anforderungen an das IT-Sicherheitsniveau in den Praxen der Ärztinnen und Ärzte, Zahnärztinnen und Zahnärzte und Psychotherapeutinnen und Psychotherapeuten in der gesetzlichen Versorgung.

01

Alle Anforderungen dieser IT-Sicherheitsrichtlinie dienen der Sicherstellung des Schutzes der Patientendaten. Insoweit handelt es sich bei der IT-Sicherheitsrichtlinie um eine Konkretisierung der technisch-organisatorischen Maßnahmen, die die Rechte und Freiheiten der Patienten und Patientinnen sicherstellen sollen. Vielen Anwenderinnen und Anwendern dürften sie grundsätzlich schon aus den direkten Vorgaben des Datenschutzes für Praxen geläufig sein. Idealerweise ergänzen sich die Anforderungen des Datenschutzes und der IT-Sicherheit.

Durch die fortschreitende Digitalisierung werden erhöhte Anforderungen an die IT-Sicherheit erzeugt. Dabei stellt eine Praxis eine eigene Repräsentanz und Sicherheitszone dar, die gegen vielfältige Gefährdungen zu schützen ist. Die Anforderungen zur IT-Sicherheit sind in diesem Kontext als erweiterte Anforderungen zu den betrieblichen Anforderungen an Arbeitsstätten und Anforderungen an die Geschäftsprozesse zu sehen. Der Gesetzgeber hat den Ärztinnen und Ärzten, Zahnärztinnen und Zahnärzten und Psychotherapeutinnen und Psychotherapeuten dabei aufgegeben, die Anforderungen zur IT-Sicherheit verbindlich umzusetzen und damit auch den Patientinnen und Patienten ein Versprechen zum Vertrauensschutz in die Informationssicherheit der Praxen gegeben.

Praxisnetze und vernetzte Geräte lassen sich heute in der Regel kaum mehr ohne direkte Verbindungen ins Internet betreiben, sei es zum regelmäßigen Update der Systeme oder um Patientinnen und Patienten digitale Service- oder Dienstleistungen anzubieten. Diese fortschreitende Vernetzung macht die Systeme auch grundsätzlich für Angriffe, beispielweise von Kriminellen, erreichbar, die sich durch Erpressung finanziell bereichern wollen. Schäden werden u.a. verursacht durch das Mitlesen und Kopieren von Patientendaten und der Drohung, diese zu veröffentlichen oder durch Verschlüsselung zentraler Systeme deren Verfügbarkeit zu entziehen und gegen Lösegeldzahlungen deren Freigabe zu versprechen. Generell rät das BSI davon ab, auf Forderungen von Erpresserinnen und Erpressern einzugehen, da es sehr unsicher ist, ob diese ihren Zusagen der Rückgabe nachkommen. Wenn Kriminelle ihr Wort halten, bedeutet es nicht, dass alle betroffenen Systeme sich wieder sicher betreiben lassen.

Die Beseitigung von angriffsbedingten Schäden verursacht in der Regel erhebliche Aufwände und Kosten – vor allem bei Servern und sonstigen Prozessen, die nicht direkt von den Betreiberinnen und Betreibern gewartet werden.

Durch die steigende Vernetzung und Komplexität der Prozesse wird in Zukunft auch der Schutz der vernetzten Medizintechnik in den Praxen und deren Abschottung gegen die Praxisnetze, insbesondere zum Schutz sensibler Großgeräte, noch an Bedeutung gewinnen – allein schon, um damit die Werte zu schützen. Auch mit der Einführung des E-Rezeptes ist damit zu rechnen, dass Begehrlichkeiten von Wirtschaftskriminellen entstehen, da die Praxen als Angriffsziele attraktiver werden.

Aus diesen Gründen erscheint die Ausführung der Anforderungen der IT-Sicherheitsrichtlinie in jeder Praxis angeraten. Ein erfolgreicher IT-Angriff kann jede Praxis an die Grenze der wirtschaftlichen Tragbarkeit und zusätzlich zu einem Verlust des Ansehens führen.

Betreiberinnen und Betreiber, Heilberuflerinnen und Heilberufler sollten sich bewusst sein, dass sie die **Verantwortung für die IT-Sicherheit ihrer Systeme und Prozesse** tragen, auch wenn sie die Umsetzung von Maßnahmen in fachkundige Hände abgeben oder Verträge mit entsprechenden Dienstleistern zur Sicherstellung eines bestimmten Schutzniveaus geschlossen haben.

Für die Anwendung dieser IT-Sicherheitsrichtlinie ist sowohl ein Mindestmaß an **Kenntnissen über die Umsetzung der informationstechnischen Prozesse** in der konkreten Praxis, als auch ein Mindestmaß an **Verständnis für die Begrifflichkeiten der IT-Sicherheit** Voraussetzung. Medizinisches Fachpersonal, welches die IT-Sicherheitsrichtlinie selbst anwenden möchte, kann **kompetente Unterstützung durch fachkundige Dienstleister** erhalten, die auf Basis einer eigenen Richtlinie zertifiziert wurden. Die Kassenärztliche Bundesvereinigung bietet auf ihrer Webseite eine Übersicht dieser zertifizierten Dienstleister an.

Aktualität und Wachsamkeit schützt Ihre Systeme

Wer aktuelle Systeme auf dem Stand der Technik betreibt, schützt sich und die Daten seiner Patientinnen und Patienten in einem angemessenen Umfang.

Ein hundertprozentiger Schutz ist dennoch nicht möglich, weil es in der Natur der Technik liegt, dass immer wieder Schwachstellen zu Systemen aufgedeckt werden oder durch menschliche Fehlleistungen unbeabsichtigte Risiken entstehen.

Das BSI ist bereits seit Anfang der 2000er-Jahre mit Beratungsleistungen zur Einführung komplexer elektronischer Verfahren in das deutsche Gesundheitswesen mit einbezogen. Dazu zählen zahlreiche technische Richtlinien, die u.a. Vorgaben für die Verschlüsselung von Daten enthalten, das technische Design der ersten elektronischen Gesundheitskarte oder des elektronischen Heilberufsausweises (z.B. Arztausweis, eZahnarztausweis) betroffen haben.

Heute liegt ein Schwerpunkt des BSI bei der Beratung der gematik GmbH bei der Konzeption neuer vernetzter Verfahren mit sicheren Architekturen. Die folgenden Hinweise des BSI sollen deshalb allen Ärztinnen und Ärzten, Zahnärztinnen und Zahnärzten und Psychotherapeutinnen und Psychotherapeuten helfen, sich der für die Praxislandschaft eher neuen Dimension der IT-Sicherheit zu nähern und Interesse für das Thema zu erzeugen. Es werden in zeitlichen Abständen weitere Veröffentlichungen des BSI folgen, die dann auch mehr auf technische Einzelheiten eingehen.

Falls es doch einmal zu einem IT-Notfall kommt, sollten Sie sofort fachkundige Hilfe zu Rate ziehen und ggf. auch das BSI darüber informieren.

§ 75b SGB V

Die Kassenärztlichen Bundesvereinigungen regeln die Inhalte, welche Anforderungen alle Praxisinhaberinnen und Praxisinhaber in ihren Praxen erfüllen müssen. Die Kassenärztliche Bundesvereinigung (KBV) und die Kassenzahnärztliche Bundesvereinigung (KZBV) haben hierfür zwei Richtlinien veröffentlicht, die sich inhaltlich nur marginal unterscheiden.

02

Anforderung bedeutet, dass zu einer Kategorie, z.B. „Netzwerksicherheit“, ein bestimmtes Ziel definiert wird, z.B. „Grundlegende Authentisierung für den Netzmanagement-Zugriff“. Weiterhin wird eine Vorgabe für die Umsetzung festgelegt , z.B. „Für den Management-Zugriff auf Netzkomponenten und auf Managementinformationen muss eine geeignete Authentisierung verwendet werden.“

Es gibt Anforderungen, die für alle Praxen gelten, und basierend auf der Praxisgröße auch solche Anforderungen, die nur mittlere oder große Praxen erfüllen müssen. Das heißt, dass Sie auch eine ganze Reihe Anforderungen umsetzen müssen, wenn Sie nur als einzige Person eine Praxis betreiben.

Jede Anforderung gilt ab einem bestimmten Zeitpunkt. Es gibt z.B. Anforderungen, die ab dem 01.07.2021 zu erfüllen waren und z.B. Anforderungen, die erst ab 01.07.2022 zu erfüllen sind.

Deshalb – und da die Anforderungen der IT-Sicherheitsrichtlinie nach der Vorgabe des Gesetzestextes § 75b SGB V verbindlich umzusetzen sind – erscheint es ratsam, die Erfüllung der Anforderungen in der eigenen Praxis zu dokumentieren. Der Gesetzgeber hat zur Dokumentation und ihrer Form keine Vorgabe gemacht und auch die Richtlinie trifft hierzu keine Regelung. Es ist keine Regulierung dazu vorgesehen. Das heißt, es gibt keine Instanz, die die Umsetzung der Anforderungen prüfen oder kontrollieren muss. Um Haftungsfragen begegnen zu können, empfiehlt es sich, dennoch eine schriftliche Dokumentation zu führen, um sich im Falle von juristischen Klärungen entlasten zu können.

Um entscheiden zu können, ob eine bestimmte Anforderung erfüllt ist, ist eine gewisse Kompetenz notwendig. Deshalb hat der Gesetzgeber eine zusätzliche Richtlinie vorgesehen, mit der fachliche Dienstleister ihre Kompetenz zur Erfüllung der Anforderungen der Richtlinie nachweisen können. Die Kassenärztliche Bundesvereinigung hat dazu in Absprache mit der Kassenzahnärztlichen Bundesvereinigung eine Prüfungsordnung aufgestellt, bei

der Dienstleister sowohl ihre Kompetenz in Sachen IT-Sicherheit, als auch ihre technischen Fertigkeiten mit einer Prüfung nachweisen müssen. Dies hat für Sie den Vorteil, wenn Sie sich für die Inanspruchnahme eines IT-Dienstleisters entscheiden, dass Sie aufgrund der Zertifizierung sicher sein können, dass er mit den Anforderungen der IT-Sicherheitsrichtlinie in medizinischen Praxen vertraut ist. Leistungserbringende, die die Anforderungen selbst erfüllen möchten, müssen keine Prüfung ablegen oder ihre Kompetenz nachweisen.

Bestimmte Praxen haben aufgrund anderer datenschutzrechtlicher Vorgaben die Pflicht, eine Datenschutzfolgeabschätzung zu erstellen. In diesem Fall empfiehlt sich eine abgestimmte Vorgehensweise zur Erfüllung der technisch-organisatorischen Maßnahmen des Datenschutzes und der Erfüllung der Anforderungen nach der IT-Sicherheitsrichtlinie, da es inhaltliche Überschneidungen gibt.

Umsetzung der IT-Sicherheitsrichtlinie in der Praxis projektieren

Es empfiehlt sich, die Umsetzung der Richtlinie in einer Praxis vorab zu planen und zu projektieren.

Dies kann selbst in einer kleinen Praxis von Vorteil sein, um den Überblick zu behalten und den Fortschritt des Umsetzungsprozesses transparent und aktuell darzustellen.

03

Erster und wichtigster Punkt ist, die Frage der Verantwortung zu klären. Selbst wenn man den eigentlichen Umsetzungsprozess extern fachlich an einen Dienstleister delegiert, sollte ein Mindestmaß an Überblickswissen auch in der eigenen Praxis vorhanden sein. Es ist verständlich, dass der Fokus Ihrer Praxis auf der Versorgung und individuellen Betreuung Ihrer Patientinnen und Patienten liegt und dadurch bedingt alle Ärztinnen und Ärzte, Zahnärztinnen und Zahnärzte und Psychotherapeutinnen und Psychotherapeuten einen anderen Grundstock an Kenntnissen im Umgang mit der IT-Sicherheit mitbringen.

Um die Fachbegriffe der IT-Sicherheit und die fachlich-technischen Zusammenhänge grundsätzlich verstehen zu können, ist eine Basis-Schulung zur IT-Sicherheit sicher hilfreich. Entsprechende Angebote mit einer Dauer von ein bis zwei Tagen sind vielfältig am Markt verfügbar. Einen Einstieg in die prozessorientierte IT-Sicherheit in der Praxis finden Sie in der Regel über entsprechende Websites der Hersteller Ihres Praxis-Verwaltungssystems. Es ist denkbar, dass über die Bedienung der Praxisverwaltungssysteme hinaus die Themen IT und IT-Sicherheit in der Ausbildung der Gesundheitsberufe nicht so präsent sein könnten, dass darüber die Umsetzung der IT-Sicherheitsrichtlinie ohne weitere Fortbildung möglich wäre.

Bei der Festlegung der Verantwortung sollte insbesondere in mittleren und großen Praxen der Umfang und die Komplexität der IT-Landschaft und deren Vernetzung berücksichtigt werden. Nach der derzeit gültigen IT-Sicherheitsrichtlinie gelten Praxen mit bis zu fünf Beschäftigten, die ständig mit Aufgaben der Datenverarbeitung betraut sind, als kleine Praxen, sechs bis 20 Beschäftigte als mittlere Größe und über 20 Beschäftigte als große Praxen.

Gegebenenfalls ist die Verantwortung entsprechend aufzuteilen, z.B. in Geräteverwaltung, Software-Administration, Betrieb der Praxis-IT. Soweit die Praxis Dienstleistungen, wie den eigenen Online-Auftritt oder das Terminmanagement, an Dienstleister vergeben hat, sollten auch diese Bestandteile bei der Umsetzung der IT-Sicherheitsrichtlinie berücksichtigt werden, da auch in diesem Fall die Verantwortung bei den Praxisbetreibenden bleibt.

Dies gilt insbesondere auch für den Fall, dass ein praxisübergreifendes IT-Sicherheitskonzept über die Anforderung der Umsetzung der IT-Sicherheitsrichtlinie hinaus geplant ist. Für diesen Fall wären auch die Komponenten zu berücksichtigen, die von der derzeitigen IT-Sicherheitsrichtlinie nicht direkt erfasst werden, wie z.B. alle kaufmännischen und buchhalterischen Prozesse, Beschaffung, administrativen Aktivitäten, sonstige vernetzte Medizintechnik oder sekundäre Laborbereiche.

Zu einer Projektierung der Umsetzung gehören auf jedem Fall:

- Die Festlegung der **Verantwortlichkeiten**
- Die Klärung, ob ein **externer Dienstleister** zur Unterstützung beauftragt werden soll
- Die **zeitliche Planung** unter Berücksichtigung des Praxisbetriebs
- Die konkrete Zuweisung der **Umsetzungstätigkeiten** und **Ressourcenplanung** (Zeit + Budget)
- Die Klärung, ob zur Umsetzung **Hilfsmittel** beschafft werden müssen
- Die Absprache mit **externen Ansprechpartnerinnen und Ansprechpartnern**, die Aufgaben im IT-Bereich wahrnehmen (z.B. die Wartung der Praxis-IT oder der Praxisverwaltungssysteme)

Aus Sicht des BSI bietet es sich auch an, bei der Projektierung bestehende Policies (Richtlinien) für den Praxisbetrieb zu berücksichtigen und zu hinterfragen, z.B. ob und wie private IT (z.B. Smartphones oder Tablets) im Bereich des Praxisnetzes betrieben wird sowie ob und wie private IT der Patientinnen und Patienten in der Praxis eine Rolle spielt oder sogar in die Praxisprozesse integriert ist.

Bereits zu einem frühen Zeitpunkt sollten sich die Praxisbetreiberinnen und Praxisbetreiber darüber informieren, was sie als IT-Notfall betrachten und welche Abläufe in diesen Fällen besonders wichtig sind. Ein IT-Notfall kann zum Beispiel vorliegen, wenn im Falle eines erfolgreichen Angriffs kein Zugriff auf die Patientendaten mehr möglich ist, weil alle Daten verschlüsselt wurden. Aus Sicht des BSI ist es wichtig, dass Praxisinhabende einschätzen können, wann bei einem Ausfall der IT ein wirtschaftlicher Totalschaden eintritt und wie sie auch ohne die vorhandene IT den Minimalbetrieb sichern können.

Da in diesen schwierigen Situationen konkrete Notfallplanungen länger dauern, ist es in jedem Fall hilfreich immer für den Notfall vorgesorgt zu haben. Ohne Notfallplanungen sind längere Ausfallzeiten sehr wahrscheinlich.

Bestandsaufnahme

Die Umsetzung der IT-Sicherheitsrichtlinie kann zu einer Bestandsaufnahme genutzt werden.

04

Je genauer die vorhandenen IT-Komponenten erfasst und dokumentiert sind, desto einfacher ist es, im Schadens- oder Notfall geeignete Maßnahmen zu ergreifen.

Wenn beispielsweise ein Smartphone nicht mehr vorhanden ist, fehlen möglicherweise wichtige Informationen, um es sperren zu lassen, damit sich mit dem Gerät bzw. dessen SIM-Karte kein Missbrauch betreiben lässt. Vor Ort und schnell verfügbar sollten auch alle Administrations-Passwörter sein, die die kritischen Prozesse garantieren. Zugangsdaten für IT-Systeme, beispielsweise für das PVS-System, vernetzte Medizintechnik oder mobile Endgeräte sollten in jeder Praxis geschützt verfügbar sein und nicht nur bei einem externen Dienstleister, damit Sie z.B. bei dringenden Reparaturen oder Ersatzbeschaffungen nicht auf Ihren Dienstleister angewiesen sind.

Genauso sollten mindestens die Prozesse dokumentiert werden, die wichtig sind und jeden Tag genutzt werden, damit auch Dienstleister, die von den Abläufen in der Praxis keine näheren Kenntnisse haben, im Notfall wissen, welche Geräte und Programme wie zusammenarbeiten und wo die Daten gespeichert oder archiviert werden.

Eine Bestandsaufnahme wird nicht von der IT-Sicherheitsrichtlinie gefordert, aber der zusätzliche Aufwand hilft bei der Identifizierung der abzusichernden IT-Komponenten und könnte sich im Schadens- oder Notfall durch einen Zeitvorteil für die Wiederherstellungsdauer auszahlen.

Ebenfalls hilfreich ist es, die Verträge, die Sie mit externen Dienstleistern geschlossen haben, inklusive der dazugehörigen Ansprechpartnerinnen und Ansprechpartner verfügbar zu halten.

Es ist heute üblich, dass Sie in einem Rollen-, Rechtekonzept und Berechtigungskonzept transparent verfügbar haben, welche Personen aktuell auf welche Komponenten Zugriff haben, um gegebenenfalls schnell Rechte widerrufen, entziehen oder duplizieren zu können.

Beispiel Rollen- und Rechtekonzept

Für die Nutzung von IT-Systemen und der darauf befindlichen IT-Anwendungen, beispielsweise ein PVS, sollte idealerweise vorab identifiziert werden, welche Person oder welche Personengruppe auf eben diese Komponenten und mit welchen Befugnissen zugreifen dürfen. Analog zu Zugangsberechtigungen für Medikamente oder physische Akten von Patientinnen und Patienten, sind entsprechende Berechtigungen für die Verwendung von Systemen und auch physischer Zutritt zu diesen Systemen und Komponenten notwendig. Nicht jede Person, die in einer Praxis vor einem Rechner sitzt, sollte direkten Zugang zu dem System haben und keinesfalls unautorisiert die Berechtigung erlangen, Einstellungen des Systems zu ändern.

Notwendig für die Erarbeitung eines Rollen- und Rechtekonzeptes, ist die Identifikation berechtigter Personen und Personengruppen durch entsprechende Fragestellungen:

- → Welche Aufgabe soll mein Mitarbeiter/meine Mitarbeiterin erfüllen?
- → Welche Werkzeuge/Systeme sind hierfür erforderlich?
- → Mit welchen Berechtigungen muss eine Person auf das Werkzeug/System zugreifen können?
- → Reicht die Einsicht in Dokumente?
- → Muss ebenfalls das Eintragen neuer Informationen ermöglicht werden?
- → Dürfen bestehende Einträge auch geändert werden?
- → Dürfen bestehende Einträge gelöscht werden?

Hieran schließt sich die grundsätzliche Frage an, welche Systeme und Anwendungen derzeit im Arbeitsalltag verwendet werden. Die Beantwortung der Frage kann auch zu der Einschätzung führen, dass bisherige Anwendungen ggf. für den weiteren Betrieb nicht notwendig sind.

Zur Dokumentation der Rollen und Rechte der Mitarbeitenden dient eine Tabelle, wie im Folgenden beispielhaft skizziert:

Funktion/Personengruppe	Alle Mitarbeitenden	Spezialisierte Mitarbeitende *(bspw. Empfang oder Sekretariat)*	Administrator
Patientinnen und Patienten empfangen	×	×	
Rezepte & Überweisungen ausstellen	×	×	
Digitale Kommunikation mit anderen medizinischen Fachrkäften		×	
Verwaltung der IT			×

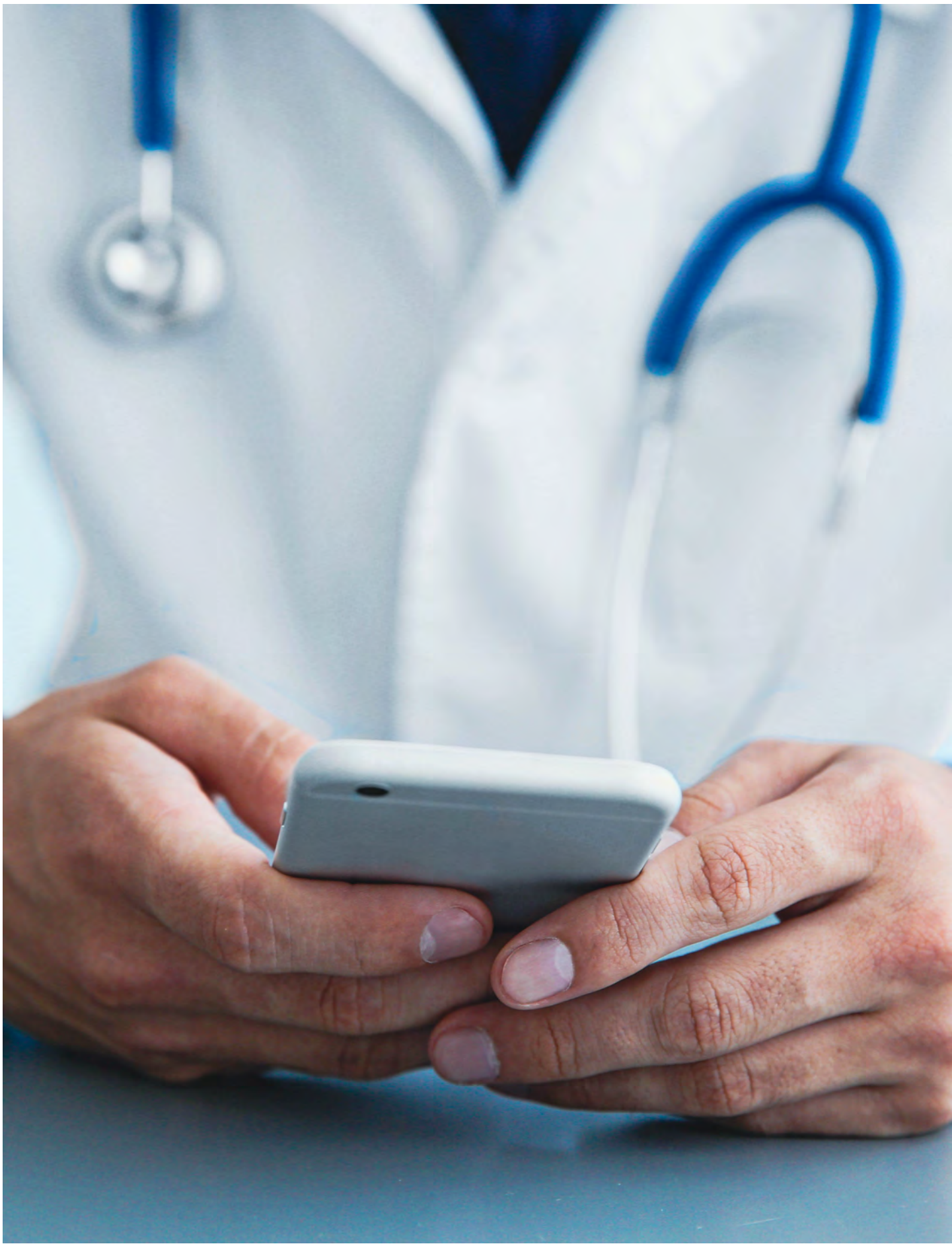
Die Granularität eines Rechte- und Rollenkonzeptes kann unterschiedlich und aufeinander aufbauend verfolgt werden. So lassen sich in einer ersten Betrachtung lediglich die Aufgaben fokussieren, in einer folgenden die hierfür benötigten Anwendungen/Systeme und weitergehend die dafür zu beachtenden Rechte der Personengruppe. Ein solches Konzept kann auch direkt einzelne Beschäftigte identifizieren. Die Granularität der identifizierten Personengruppen lässt sich unterschiedlich wählen.

Funktion/Personengruppe	Alle Mitarbeitenden	Spezialisierte Mitarbeitende *(bspw. Empfang oder Sekretariat)*	Administrator
Einrichten/Konfigurieren (neuer) IT-Komponenten (z.B. Rechner, Router, Telefone)			X
Installation von Updates			X
Anlegen und Vergabe (neuer) Nutzeraccounts			X
Vergabe von Zugangsdaten			X
Sperrung von Zugängen			X
Zugriff auf E-Mailpostfächer		X	X
Zugriff auf Kalendereinträge	X *(lesend)*	X *(ohne Einschränkungen)*	

Ziel des Rechte- und Rollenkonzeptes ist eine einheitliche, stringente Vergabe notwendiger Berechtigungen und die Generierung einer Übersicht zur Identifikation zuständiger Ansprechpartner. Das dargelegte Beispiel soll einen Eindruck vermitteln, wie ein solches Konzept erarbeitet und dokumentiert werden kann. Für die individuellen Kontexte des Arbeitsalltages werden unterschiedliche Granularitäten und unterschiedliche Personengruppen berücksichtigt werden müssen. Eine allgemeingültige Vorlage kann aufgrund des individuellen Kontextes in jeder einzelnen Praxis nicht bereitgestellt werden

.Weitere Informationen zu einem solchen Konzept sind hier zu finden:

Umsetzungshinweise:
ORP.4. Identitäts- und Berechtigungsmanagement



Weiterführende Hinweise des BSI

05

5.1 Schwachstellen und der Faktor Mensch

Der Cyber-Raum, beziehungsweise das Internet ist für alle Nutzerinnen und Nutzer, sowie für Praxen, eine potentiell gefährliche Umgebung.

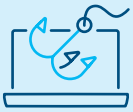
Es gibt Bedrohungen, die permanent vorhanden sind, wenn IT-Nutzerinnen und IT-Nutzer Dienste im Internet aufrufen. Beispielsweise bei der gezielten Suche nach Informationen, aber auch weitgehend unbemerkt, wenn Betriebssysteme oder andere Software im Hintergrund die neuesten Updates automatisch laden und installieren. Aus Sicht der IT-Sicherheit ist es sicherer, wenn Aktualisierungen nur kontrolliert und getestet eingespielt werden. Um dies zeitnah zur Bereitstellung durch die Hersteller sicherzustellen, ist allerdings ein erheblicher organisatorischer Aufwand notwendig. Diese Maßnahme bringt nur einen Zuwachs an Sicherheit, wenn sie immer zeitnah umgesetzt wird.

Es ist ein Trugschluss zu denken, dass es dann am einfachsten wäre, keine Dienste oder kein Internet in Anspruch zu nehmen. Leider ist es in vielen Fällen sehr aufwändig, isolierte Systeme auf einem aktuellen und sicheren Stand zu halten. Ein isoliertes System zeichnet sich dadurch aus, dass es keinerlei Kommunikation zu externen Komponenten aufnimmt und deshalb nicht über die sonst nötigen Verbindungen zu Routern, Konnektoren oder anderen Möglichkeiten, beispielsweise Bluetooth oder Mobilfunk verfügt.

Die permanenten Bedrohungen können durch Ausnutzung von Schwachstellen zu Gefährdungen werden und somit konkrete Risiken für Ihre IT-Umgebung verursachen.

Menschen, die IT-Systeme bedienen und über diese kommunizieren, sollten – im Gegensatz zur medizinischen Tätigkeit im Gesundheitssektor – bezüglich der vermeintlichen Kommunikationspartner und Kommunikationspartnerinnen ein gesundes Misstrauen an den Tag legen.

Dies sollte z.B. zur Folge haben, dass diese keine E-Mails öffnen, deren Absendeadressen sie nicht genau identifizieren können und im Internet ausschließlich Eingaben an Stellen machen, von denen sie sicher wissen, dass sie vertrauenswürdig sind.



Phishing-Angriffe gehören zu den gängigsten Angriffsmethoden

Cyber-Kriminelle versuchen oftmals als scheinbar vertrauenswürdige Kommunikationspartnerinnen oder Kommunikationspartner mittels gefälschter E-Mail-Adressen oder Webseiten die Nutzerinnen und Nutzer zu Aktionen zu verleiten, welche die Integrität ihrer Systeme verletzt. Aktionen können z.B. im Öffnen schadbehafteter Anhänge bestehen oder in der Herausgabe von PIN oder Passwörtern. Zum Beispiel:

- Virenbehaftete Word-Dateien oder harmlos aussehende Katzenfotos mit deren Öffnen gleichzeitig Schadcode freigesetzt wird.
- Die Aufforderung die eigene Kontonummer und das Zugangspasswort zum Konto zu „verifizieren“, mit denen Kriminelle dann wirtschaftlichen Schaden verursachen.

Menschliche Fehler und Fehleinschätzungen sind nach wie vor eine der größten Gefahren für die Systemsicherheit.

Um den Versand von E-Mails abzusichern, sind diese zu verschlüsseln und zu signieren, sodass der Text oder sonstige Inhalte von unberechtigten Dritten nicht gelesen werden kann. Der Absender oder die Absenderin identifiziert sich durch ein individuelles Zertifikat einer sicheren Zertifizierungsstelle, bspw. der individuellen SMC-B oder des Heilberufsausweises. Dieses Verfahren wird von dem speziellen Dienst der TI zur Kommunikation im Medizinwesen (KIM) automatisch für die sichere Kommunikation im Gesundheitswesen verwendet.

Formulareinträge im Internet sollten nur vorgenommen werden, wenn eine verschlüsselte Verbindung vorliegt (https://, das „s“ wie secure macht den Unterschied), die Umsetzenden über den Prozess und seine Folgen informiert sind und die Adresse und den Inhalt der Abfrage kennen.

Aktuelle Gefährdungen sind gegeben, weil Kriminelle versuchen überall im Cyber-Raum Web-Server, die Dienste anbieten, zu hacken, damit sie danach eingeschleuste Schadsoftware auf Nutzerrechner (Rechner des Opfers, bspw. das Praxis-System) verteilen können oder durch die Ausnutzung von Schwachstellen versuchen, die Kontrolle über Nutzerrechner zu bekommen.

Die Basis für einen guten Schutz für Endsysteme wird erreicht, wenn Nutzerinnen und Nutzer alle Komponenten eines Systems aktuell halten, sie ein geschütztes Benutzerkonto ohne privilegierte Rechte fürs tägliche Arbeiten- sowie alle Sicherheitsfunktionen heutiger Standard-Systeme nutzen.

Falls Kriminelle ein System in einer Praxis manipulieren oder übernehmen können, besteht auch eine hohe Gefährdung für alle weiteren vernetzten Systeme in der Praxis. Deshalb sollten Nutzerinnen und Nutzer immer die mögliche Gefährdung durch Phishing-Attacken bedenken und auch schon beim geringsten Verdacht beim vermeintlichen Kommunikationspartner oder der Kommunikationspartnerin rückfragen, ob er oder sie tatsächlich die erstellende Person ist. Im Zweifel sollten Nutzerinnen und Nutzer auch in Betracht ziehen, die Klasse der gefährdetsten Rechner im Netz zu isolieren oder für die gefährdetsten Rechner ohne Praxisverwaltungssystem ein eigenes Netz und einen eigenen Internetzugang einzurichten, bspw. durch einen Rechner, der über den Gastzugang eines DSL-Routers angebunden ist. Grundsätzlich stellt jedes System mit Zugang ins Internet eine Gefahr dar. Deshalb sollten Praxisbetreiberinnen und -betreiber sorgfältig prüfen, ob ein Praxis-System wirklich Zugang zum Internet, bspw. über einen Browser, haben muss, oder ob sie den Zugriff aufs Internet nicht auf ein System beschränken können, auf dem keine medizinischen oder personenbezogenen Daten verarbeitet werden.

5.2 Aktualität der IT-Ausstattung

Ein besonders sensibles Thema ist immer die Auswahl des Betriebssystems für einen Rechner. Betriebssysteme haben im Grundsatz Zugriff auf alle Inhalte, die verarbeitet und gespeichert werden. In Abhängigkeit des Betriebssystems und dessen Konfiguration können Daten an Hersteller von Betriebssystemen oder Anwendungen übertragen werden. Viele Hersteller werten Nutzungsdaten und Systemzustände zur Weiterentwicklung des Systems beispielsweise zur Verbesserung der Systemstabilität aus. Zu diesem Zwecke werden Nutzerinnen und Nutzer darüber informiert, dass der Hersteller Daten sammelt. Gegebenenfalls erfordert es sehr hohe Aufwände, alle Möglichkeiten des Datensammelns zu verhindern.

Das BSI kann nicht zu einem bestimmten Betriebssystem raten oder abraten. Lediglich für den Fall, dass Sie personalisierte medizinische Daten durch Dritte verwalten, sei der Hinweis gegeben, dass neben dem Datenschutz auch der Schutz des Berufsgeheimnisses bei der Auftragsdatenverarbeitung zu berücksichtigen ist. Das heißt, dass die Person, welche die Daten im Auftrag verwaltet, dazu verpflichtet ist, sie auch entsprechend hoch zu schützen.

Verwenden Sie nur Geräte, Betriebssysteme und Programme, die noch vom Hersteller mit Sicherheitsupdates versorgt werden. Beispielsweise wird Windows 7 an vielen Stellen noch eingesetzt, obwohl der allgemeine Support am 14. Januar 2020 abgelaufen ist. Ohne spezielle Supportverträge mit Microsoft oder weitgehende Kapselung solcher Systeme im Netzwerk, rät das BSI dringend vom weiteren Einsatz ab. Praxisinhaberinnen und Praxisinhaber, die vom Hersteller nicht mehr gewartete IT-Komponenten einsetzen, werden sich im Schadensfall sicherlich dem Vorwurf der Fahrlässigkeit ausgesetzt sehen.

Mit Blick auf die oben erwähnten Datenübertragungen an den Hersteller empfehlen wir grundsätzlich aber auch in Bezug auf Windows 10, sich explizit mit diesen Eigenschaften der eingesetzten Betriebssysteme auseinanderzusetzen, bevor Sie Praxisverwaltungssysteme darauf betreiben. Soweit für Systeme ein hoher Schutzbedarf festgestellt wird, sollte bei allen derzeit am Markt verfügbaren Betriebssystemen eine fachkundige Bewertung möglicher Restrisiken erfolgen und ggf. ergänzende IT-Sicherheitsmaßnahmen umgesetzt werden.

Es ist möglich, mit bestimmten Vertragskonstellationen und unter Ausnutzung der betriebssystemseitigen Einstellmöglichkeiten auch ohne Expertise die Übertragung ungewollter Datenpakete an den Hersteller weitestgehend auszuschließen.

5.3 Vorfälle

Betreiberinnen und Betreiber von Praxen sollten folgende Abgrenzungen bedenken:

IT-Störungen:	Geringer Einfluss auf den Praxisbetrieb, in der Regel ausgelöst durch die eingeschränkte Verfügbarkeit von Hard- oder Software.
IT-Vorfälle:	Mittlerer Einfluss auf den Praxisbetrieb, Vorfälle sollten dokumentiert und ggf. gemeldet werden, z.B. Verdacht auf Schadprogramm.
IT-Notfälle:	Wesentliche Geschäftsprozesse sind nicht verfügbar. Falls keine Behebung des Notfalls möglich ist, droht ein hoher oder existentieller Schaden.

Aspekte, die man dabei berücksichtigen sollte, sind die Reaktionsgeschwindigkeiten. Beispielsweise, wie schnell der IT-Support auf Vorfälle reagieren soll und wie schnell Störungen beseitigt werden sollten und wann ein Zustand eintritt, in dem die Handlungsfähigkeit der Praxis so weit eingeschränkt ist, dass die Behandlung der Patientinnen und Patienten ohne Notfallmaßnahmen nicht mehr gewährleistet ist.

Ein für diese Fälle bewährtes Produkt ist die IT-Notfallkarte, welche Praxisbetreiberinnen und Praxisbetreiber an den Arbeitsplätzen der Praxis aufhängen können, damit die Beschäftigten alle, im Falle eines auftretenden IT-Problems, relevanten Telefonnummern oder Hilfsmittel auf einem Blick finden können. Durch die Steigerung der Abhängigkeit von der IT und fortschreitender Vernetzung sind entsprechende Maßnahmen in jedem Falle sinnvoll und angemessen.

Kassenzahnärztliche Bundesvereinigung:
Datenschutz und IT-Sicherheit in der Zahnarztpraxis

IT-Notfallkarte:
Verhalten bei IT-Notfällen

Impressum

Herausgeber:
Bundesamt für Sicherheit in der Informationstechnik (BSI)
53175 Bonn

Bezugsquelle:
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Referat DI24
Godesberger Allee 185–189
53175 Bonn
Telefon: +49 (0) 228 999582-0
E-Mail: bsi@bsi.bund.de
Internet: www.bsi.bund.de

Stand:
Dezember 2021

Texte und Redaktion:
Bundesamt für Sicherheit in der Informationstechnik (BSI);
FAKTOR 3 AG

Konzept und Gestaltung:
FAKTOR 3 AG
Kattunbleiche 35
22041 Hamburg
www.faktor3.de

Artikelnummer:
BSI-Bro21/06

Bildnachweise:
S. 3: AdobeStock © Halfpoint; S. 4-5: AdobeStock © Monet; S. 7: AdobeStock © cameravit;
S. 9: AdobeStock © insta_photos; S. 10-11: AdobeStock © takasu; S. 13: AdobeStock © green;
S. 15: AdobeStock © Rido; S. 17: AdobeStock © Africa Studio; S. 19: AdobeStock © mrmohock;
S. 20-21: AdobeStock © bongkarn; S. 22-23: AdobeStock © Syda Productions.