Fahrplan für die Niedergelassenen

Falls Sie unser Rundschreiben zur IT-Sicherheitsrichtlinie vom 8. April 2021 umgesetzt haben und die Titelfrage: „Sind Sie sicher?“ beherzt mit „Ja“ beantworten können, können Sie diesen Beitrag überspringen. Falls nicht, zeigen wir Ihnen hier den Einstieg, der nicht schwer ist.

Sie war keine leichte Geburt, die Richtlinie zur IT-Sicherheit nach § 75b SGB V. Seit 23. Januar 2021 in Kraft, beschreibt sie ein Mindestmaß von Maßnahmen zur Gewährleistung einer sicheren Praxis-IT. Diese gelten verbindlich für alle Vertragsärzte und Psychotherapeuten. Die Richtlinie hat einen Zwilling, die Richtlinie zur Zertifizierung von IT-Service-Dienstleistern. Über Letztere können sich IT-Praxisberater (freiwillig) zertifizieren lassen, sodass an einem unübersichtlichen Beratungsmarkt künftig ein Nachweis über die Fachkunde zu diesen sicherheitskritischen Themen vorhanden ist.

Eine Änderung aus dem Digitale-Versorgung-Gesetz vom Dezember 2019 hat die KBV gesetzlich verpflichtet, die IT-Sicherheitsanforderungen für Arztpraxen in einer speziellen Richtlinie verbindlich festzulegen. Über den Inhalt galt es, Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) herzustellen. Dieses übernimmt gemäß Selbstbeschreibung auf der Homepage „als zentrales Kompetenzzentrum für Informationssicherheit in Deutschland [...] Verantwortung als Gestalter einer sicheren Digitalisierung“ in der Gesundheitsversorgung. Das BSI ist zudem Aufsichtsbehörde für Betreiber Kritischer Infrastruktur, wie beispielsweise Kliniken oder Pharmahersteller ab einer bestimmten Größe. Der ambulante Versorgungssektor zählt ausdrücklich nicht dazu, sondern Praxen behandelt das BSI wie Unternehmen. Für diese veröffentlicht das

Bundesamt regelmäßig das sogenannte IT-Grundschutzkompendium, mit aktuell 810 Seiten Umfang eine Art IT-Sicherheits-Enzyklopädie. Das sollte nach Auffassung des BSI auch Maßstab für die Arztpraxen werden. Der Annäherungsprozess von BSI, KBV und KVen sowie BMG muss hier nicht aufgerollt werden, das Ergebnis zählt – und das ist sinnvoll und machbar.

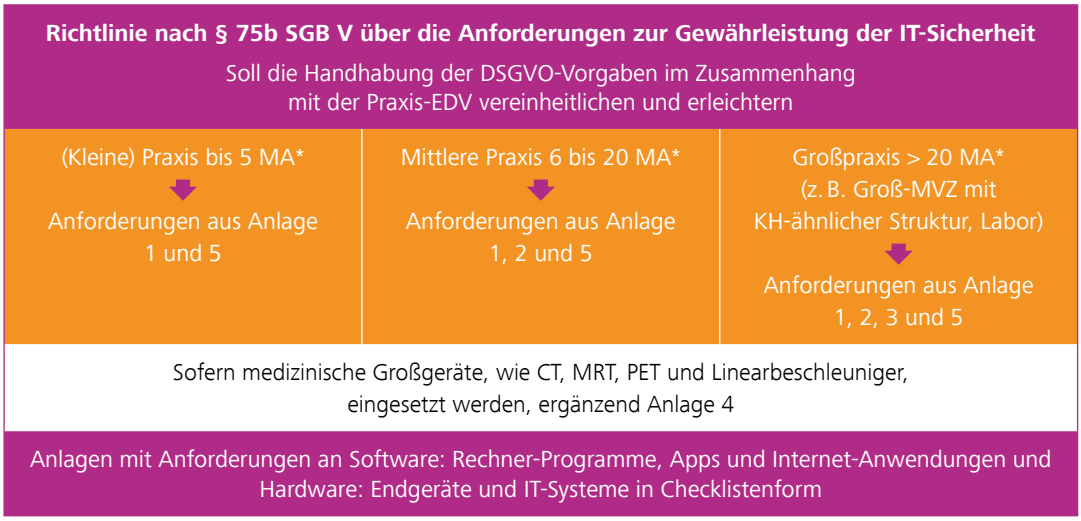
Die IT-Sicherheitsrichtlinie soll das Sicherheitsniveau in Arztpraxen anheben, quasi ein regelmäßiger Fitnesstest angesichts der Digitalisierung, Vernetzung und schwer greifbarer Cyberrisiken. Jährliche Updates werden folgen, weil die Anforderungen dem jeweiligen Stand der Technik entsprechen müssen und an das Gefährdungspotenzial anzupassen sind.

INHALT UND AUFBAU DER RICHTLINIE

Die Maßnahmen der Richtlinie zielen auf Datensicherheit als zentrale Voraussetzung für einen effektiven Datenschutz. Sie schlägt dadurch eine Brücke zwischen den Anforderungen der DSGVO und der technisch-organisatorischen Umsetzung in der Praxis.

Die Richtlinie selbst umfasst schlanke zwei Seiten und verweist hinsichtlich der eigentlichen Sicherheitsmaßnahmen auf die Anlagen. In insgesamt fünf Anlagen sind die Anforderungen an die Hard- und Software als Checklisten mit Erläuterungen und Fristen formuliert. Diese bauen aufeinander auf. Anlage 1 enthält grundlegende Anforderungen, gültig für alle Praxen und die Anlagen 2 und 3 jeweils zusätzliche Anforderungen in Abhängigkeit von der Praxisgröße. Anlage 4 gilt nur für Nutzer medizinischer Großgeräte. Anlage 5 beschreibt schließlich Anforderungen an die sichere Installation und den Betrieb von Komponenten und Diensten der Telematikinfrastruktur (TI).

Die Größe der Praxis bestimmt den Umfang der zu erfüllenden Anforderungen (siehe Grafik).



* Anzahl der ständig mit Datenverarbeitung betrauten Personen (i.d.R. alle Mitglieder eines Praxisteams inkl. Labor und Praxisinhaber, die mit dem PVS arbeiten, aber etwa auch mit der (Lohn-)Buchhaltung beschäftigt sind, unabhängig vom ausgeübten Tätigkeitsumfang).

KLEINES EINMALEINS GEGEN STÖRUNGEN

Grundsätzlich gilt, dass Anforderungen nur für die IT-Komponenten umzusetzen sind, die im Praxisbetrieb vorhanden sind. Gibt es beispielsweise kein dienstlich genutztes Tablet, entfallen die entsprechenden Positionen ersatzlos. Der für alle Praxisgrößen gültige Grundkatalog in Anlage 1 adressiert neun Komponenten in 34 Punkten. Die Maßnahmen sind mit Umsetzungsfristen hinterlegt, die bis Juli 2022 reichen. Vieles davon sollte ein verantwortungsbewusster EDV-Nutzer im eigenen Interesse berücksichtigen. Einiges dürfte auch in Ihrer Praxis schon angewendet werden.

CHECKLISTE
SO KÖNNEN SIE VORGEHEN

Sie wollen prüfen, ob Sie die Anforderungen der IT-Sicherheitsrichtlinie erfüllen oder welche Maßnahmen Sie zusätzlich ergreifen müssen, um vertrauliche Daten noch besser vor unberechtigten Zugriffen zu schützen? Doch womit fangen Sie am besten an? Die Checkliste soll Ihnen helfen, einen Einstieg zu finden.

1 PRAXISTYP FESTLEGEN

Welcher Praxistyp sind wir?
Je nach Praxistyp müssen die Anforderungen nach den entsprechenden Anlagen erfüllt werden:

Praxis mit 1 bis 5 Personen*
Anlage 1, 5 (und 4 bei medizinischen Großgeräten)

Mittlere Praxis mit 6 bis 20 Personen*
Anlage 1, 2, 5 (und 4 bei medizinischen Großgeräten)

Große Praxis mit mehr als 21 Personen* oder sehr vielen Daten
Anlage 1, 2, 3, 5 (und 4 bei medizinischen Großgeräten)

* ständig mit der Datenverarbeitung betraute Personen

2 IT-KOMPONENTEN FINDEN

Welche IT-Komponenten nutzen wir in unserer Praxis?
Erstellen Sie eine Liste der IT-Komponenten. Nur wenn eine IT-Komponente vorhanden ist, müssen Sie die Anforderungen erfüllen und Sicherungsmaßnahmen umsetzen.

Dezentrale Komponenten der TI, zum Beispiel Konnektor, Kartenlesegerät, Praxisausweis

Endgeräte, zum Beispiel Computer, Laptop, Notebook

Endgeräte mit Windows-Betriebssystem, zum Beispiel Computer, auf denen Windows läuft

Internet-Anwendungen, zum Beispiel praxisbetriebene Webpräsenz, selbst betriebene Onlineterminvergabe

Medizinische Großgeräte, zum Beispiel CT, MRT, PET

Mobile Anwendungen (Apps)

Mobile Device Management / MDM, zum Beispiel mobile Geräte wie Praxis-Laptops oder Praxis-Tablets werden zentralisiert überwacht/verwaltet

Mobiltelefone, die dienstlich genutzt werden

Netzwerksicherheit, zum Beispiel (W)LAN-Sicherheit

Office-Produkte, zum Beispiel Programme für Textverarbeitung, Tabellenkalkulation, Präsentationen

Smartphones und Tablets

Wechseldatenträger, Speichermedien, zum Beispiel USB-Sticks, Speicherkarten, externe Festplatten

↗ Die IT-Komponenten sind im Hub in den Anlagen unter „Zielobjekt" aufgeführt: ***https://hub.kbv.de/display/itsrl***

3 SICHERUNGSMASSNAHMEN FESTLEGEN

Mit welchen Maßnahmen schützen wir die IT-Zielobjekte unserer Praxis?
Prüfen Sie, mit welchen Maßnahmen Sie Ihre IT-Komponenten bereits schützen und welche weiteren Maßnahmen Sie ergreifen können.

↗ Weiterführende Informationen dazu finden Sie auf den Seiten 8 bis 9 im PraxisWissen-Themenheft „IT-Sicherheit": ***https://www.kbv.de/media/sp/PraxisWissen_IT-Sicherheit.pdf***
↗ Ausführlich können Sie sich im Hub informieren: ***https://hub.kbv.de/display/itsrl***

4 DIENSTLEISTER JA ODER NEIN?

Beauftragen wir einen IT-Dienstleister, der uns berät und unterstützt?
Die KBV veröffentlicht eine Liste der IT-Dienstleister, die speziell für die Umsetzung der Vorgaben aus der IT-Sicherheitsrichtlinie zertifiziert wurden. Dies ist ein optionales Angebot. Praxisinhaberinnen und -inhaber können sich auch für einen nicht zertifizierten Dienstleister entscheiden, wenn sie sich Hilfe holen möchten.

↗ Die Liste der IT-Dienstleister steht online zur Verfügung: ***www.kbv.de/media/sp/KBV_ISAP_Dienstleister_ZERT_P75b_SGBV.pdf***

5 UMSETZUNG STARTEN

Beginnen Sie mit der Umsetzung und tauschen Sie sich dazu gegebenenfalls mit Ihrem IT-Dienstleister aus.

- Verfügen Ihre Geräte über einen aktuellen Virenschutz?
- Laden Sie regelmäßig Updates und nutzen Sie die Möglichkeit zur automatischen Softwareaktualisierung?
- Nutzen Sie nur gesicherte Verbindungen (https://...) und sichere Authentisierungen wie die Zwei-Faktor-Authentisierung?
- Versenden Sie keine personenbezogenen Daten oder laden sie in eine Cloud?

Wenn Sie alle Fragen mit „Ja" beantworten können, dann sind zentrale Aspekte dieser Richtlinie schon erfüllt.

Mobile Anwendungen (Apps) sollten nur in den offiziellen Stores heruntergeladen werden, das heißt für iOS-Geräte im App Store und für Android über Google Play. Über die Sicherheitseinstellungen der Geräte können Apps aus externen Quellen blockiert werden. Zur Vermeidung von Schwachstellen sind Updates zeitnah zu installieren. Wichtig zur Verhinderung von Datenabfluss ist, keine vertraulichen Daten wie Diagnosen oder Befunde über Apps zu versenden, auch nicht auf Wunsch des Patienten. Vorsicht ist insbesondere bei den allgegenwärtigen Messenger- und Chatdiensten wie WhatsApp, Telegram oder Skype geboten. Perspektivisch sollten nur Apps zum Einsatz kommen, die Dokumente verschlüsselt und lokal abspeichern. Nicht mehr benötigte Apps sind restlos zu löschen.

Bei **Office-Produkten** wird von der Nutzung des integrierten Cloudspeichers zur Speicherung personenbezogener Informationen abgeraten. Auch OneDrive ist gegebenenfalls zu deaktivieren. Stattdessen sollte eine lokal installierte Office-Version zur Anwendung kommen. In Dokumenten und Musterschreiben sollte auf sensible Daten aus Vorversionen geachtet werden, auch in den „Eigenschaften". Für digitale Dokumente wird eine Speicherung und Weitergabe im PDF-Format empfohlen. Gehen Sie sparsam mit persönlichen Daten und der Vergabe von Rechten in der Benutzerkontensteuerung um.

Auch wenn es bequem sein mag: Für alle **Internet-Anwendungen** gilt, dass automatische Zugriffe oder Speicherungen konsequent unterbunden werden sollten. Hinterlassen Sie möglichst wenige Spuren im Internet; dazu können Sie die Einstellungsmöglichkeiten im Browser nutzen. Bei Abfragen mit Voreinstellungen (zum Beispiel Cookies) ist der sichere Weg regelmäßig der unbequeme Weg, das heißt, ich muss die Schaltfläche aktiv wechseln oder deaktivieren. Dass Passwörter hinreichend komplex sein sollten, gehört inzwischen zu den Selbstverständlichkeiten. Halten wir uns konsequent daran? Hilfreich kann ein Passwortmanager sein, ein Programm zur Verwaltung von Benutzernamen und Passwörtern. Mittels Verschlüsselung und eines komplexen Masterpassworts (das man sich allerdings merken muss) verwahren Passwortmanager die Passwörter sicher.

Was **Endgeräte** anbelangt, so sollten diese nur bei aktiver Nutzung entsperrt und aktiviert (Kamera und Mikrofon) werden. Virenschutzprogramme schützen nur, wenn sie durch Updates aktuell gehalten werden. Die Bedeutung der täglichen Datensiche-

rung für Praxis- und Abrechnungsdaten kann gar nicht überschätzt werden. Ausnahmslos jede Praxis sollte über ein Datensicherungskonzept verfügen und das Funktionieren ab und an testen. Es spricht nichts gegen die Verwendung marktüblicher Backup-Software (siehe Vergleichstests, Preise ab ca. 30 €) auf transportablen Speichermedien. Apropos Speichermedien und Wechseldatenträger wie USB-Sticks, Speicherkarten, externe Festplatten, Kameras: vor Nutzung (automatisch) auf Schadsoftware scannen, eindeutig kennzeichnen und alte Daten vollständig und sicher löschen.

Bei mobilen Geräten wie **Smartphone, Tablet und Mobiltelefon** sollten generell die strengsten Einstellungen für das Gerät selbst und die Apps darauf gewählt werden. Geräte sollten immer nur bei aktiver Nutzung entsperrt werden. SIM-Karten sind per PIN zu schützen, die Super-PIN/PUK und der Kontakt des Anbieters zur Sperrung der SIM-Karte im Fall des Geräteverlustes gehören sicher zentral aufbewahrt.

Den letzten Punkt bildet die **Absicherung** des Praxis**netzwerks** durch eine Hardware-Firewall. Damit kann der Datenverkehr kontrolliert und unerlaubter Zugriff unterbunden werden. Das interne Netz inklusive eines Netzplans ist zu dokumentieren. Ein Muster steht auf dem KBV Hub zur Verfügung.

Für mittlere und große Praxen bestehen einige zusätzliche Anforderungen an die obigen Komponenten. Arbeitshilfen finden sich auf dem KBV Hub und im Heft PraxisWissen.

TI IN EIGENER ANLAGE

Die TI unterscheidet zentrale und dezentrale Komponenten. Zentrale Komponenten laufen in Rechenzentren im Auftrag der gematik, die dezentralen Komponenten betreiben Sie in Ihren Praxen. Bislang zählen dazu Konnektor, der Kartenleser, der Praxisausweis (SMB-C-Karte) und der eHeilberufsausweis. Laut Anlage 5 ist wesentlich, dass die Komponenten gemäß der gematik- beziehungsweise Herstellerempfehlung installiert und betrieben werden und in Ihrer Praxis vor unkontrolliertem Zugriff geschützt sind. Unterstützt Sie ein Dienstleister bei der Installation und dem Betrieb der TI-Komponenten, sollten Sie trotzdem Kenntnis über Authentisierungsmerkmale und Administrationsdaten haben und diese sicher aufbewahren.

Alles schon mal irgendwie gehört? Dann kann es losgehen. Dieser Artikel streift die meisten Punkte der IT-Sicherheitsrichtlinie, eine gezielte Beschäftigung mit den einzelnen Anforderungen kann er leider nicht ersetzen. ■

Jutta Linnenbürger

Sie finden die Richtlinie auf der Homepage der KBV:
https://bit.ly/3wu4fIJ

Zu Ihrer Unterstützung hat die KBV eine Reihe von Umsetzungshilfen zur Richtlinie erarbeitet:

- die Informationsseite **hub.kbv.de** mit hilfreichem Informationsmaterial zur Umsetzung der Richtlinie (u.a. Musterdokumente zum Download) und FAQs
- ein Serviceheft in der Reihe PraxisWissen: „IT-Sicherheit. Hinweise zur Richtlinie, Tipps zur Umsetzung, Beispiele für die Praxis“. Dieses Heft hat die KBV auf ihrer Homepage eingestellt: **https://bit.ly/2OqUZ6O**
- Kurz und bündig informieren Sie sich unter **www.kvhessen.de/publikationen/it-sicherheit**