Informationsoffensive zur IT-Sicherheit in Praxen

Mit zahlreichen Informations- und Schulungsangeboten will die Kassenärztliche Bundesvereinigung (KBV) die Praxen beim Schutz vor Cyberkriminalität unterstützen. Es geht darum, geeignete Sicherheitsmaßnahmen zu ergreifen und potenzielle Risiken zu vermeiden.

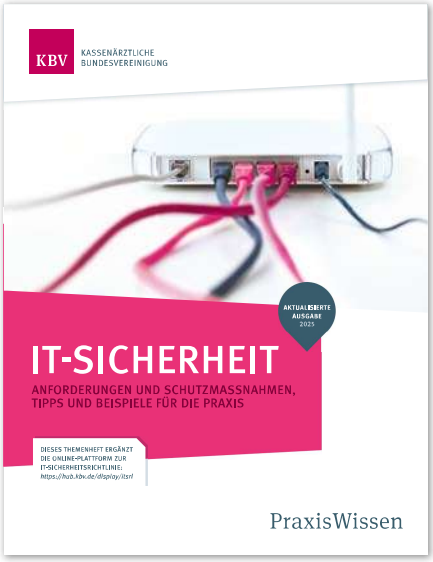
„Die Bedrohung der IT-Sicherheit wächst weltweit. Auch die ärztlichen und psychotherapeutischen Praxen sind davon betroffen und müssen ihre IT vor unberechtigten Zugriffen schützen“, sagte KBV-Vorstandsmitglied Dr. Sibylle Steiner.

Aus diesem Grund hat die KBV erst jüngst die IT-Sicherheitsrichtlinie aktualisiert. „Wir sind gesetzlich verpflichtet, Anforderungen zur Gewährleistung der IT-Sicherheit in Praxen in einer Richtlinie festzulegen und diese regelmäßig anzupassen“, sagte Steiner. Dies erfolge im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI).

Mit der Aktualisierung wurde die Richtlinie hauptsächlich um Maßnahmen ergänzt, die das Sicherheitsbewusstsein des Praxispersonals betreffen. Die Mitarbeiter sollen nach einer Empfehlung des BSI stärker sensibilisiert und geschult werden, um potenzielle Sicherheitsrisiken zu erkennen und zu vermeiden.

Die KBV bietet den Praxen hierfür Informationsmaterialien sowie Schulungen an. Teil der Informationsoffensive ist eine monatliche Serie in den Praxis-Nachrichten, die Tipps und Hinweise zur Cybersicherheit gibt. Das Themenspektrum reicht vom Umgang mit Spam bei E-Mails über sichere Passwörter, Virenschutz, Software-Updates und das Nutzen einer Cloud bis hin zum Basisschutz der Praxis-IT oder was bei einem Sicherheitsvorfall zu tun ist.

Einen kompakten Einstieg in das Thema gewährt das Serviceheft „IT-Sicherheit“ aus der Reihe PraxisWissen. Es wurde neu aufgelegt und berücksichtigt nun auch das Praxispersonal, das spätestens ab Oktober 2025 regelmäßig für Informationssicherheit sensibilisiert und geschult werden muss. Dies sieht die aktualisierte IT-Sicherheitsrichtlinie vor.



Das 16-seitige Heft ist 2021 erstmals erschienen. Es enthält neben Informationen zu den Sicherheitsanforderungen auch eine Checkliste, Tipps sowie Beispiele für die Umsetzung von Schutzmaßnahmen in der Praxis.

Fortbildung und Schulungen für das Praxispersonal

Speziell für Medizinische Fachangestellte (MFA) bietet die KBV zwei Online-Schulungen zur IT-Sicherheit an. Es gibt eine Basis-Schulung und eine Schulung zum Thema Phishing für MFA. Praxisinhaberinnen und Praxisinhaber können die Angebote nutzen, um ihre Angestellten in Fragen der IT-Sicherheit zu schulen.

Beide Schulungen stehen im Fortbildungsportal der KBV bereit. Dort wird es demnächst auch eine Fortbildung zur IT-Sicherheit für Ärzte und Psychotherapeuten geben, die mit CME-Punkten zertifiziert ist.

Online-Plattform bündelt alle Informationen

Mehr Informationen zu Fortbildungen für das Praxispersonal finden Interessierte im Hub zur IT-Sicherheit, einer Online-Plattform. Dort bietet die KBV auch Musterdokumente an, zum Beispiel eine Verschwiegenheitserklärung für Mitarbeiter und für externes Personal, das in der Praxis beispielsweise Technik installiert.

Praxisinhaber können die Musterdokumente nutzen und für ihre Gegebenheiten anpassen. Im Hub sind zudem alle Anforderungen an die IT-Sicherheit übersichtlich aufgelistet und mit Hinweisen versehen. Außerdem stehen dort Fragen und Antworten bereit.

„Es geht um sensible Gesundheitsdaten, die besonders geschützt werden müssen“, sagte KBV-Vorstandsmitglied Steiner. Praxisinhaber trügen hierfür eine große Verantwortung. Sowohl die IT-Sicherheitsrichtlinie als auch die Informationsmaßnahmen der KBV sollen sie unterstützen, notwendige Vorkehrungen zu treffen.

KBV-Praxisnachrichten vom 19. Juni 2025

Telematik-Infrastruktur: Technische Neuerungen bis Ende 2025

Bis zum Jahresende kommen nach derzeitigem Kenntnisstand auf Praxen im Bereich der Telematik-Infrastruktur (TI) noch technische Änderungen zu. Lesen Sie hier im Überblick, worum es sich handelt und was zu beachten ist.

Neues Verschlüsselungsverfahren – Austausch von TI-Komponenten bis Jahresende notwendig
Zahlreiche Komponenten der TI sollen bis Jahresende auf ein neues Verschlüsselungsverfahren umgestellt werden. Infolgedessen müssten zahlreiche Konnektoren, Heilberufs-, Praxisausweise sowie Gerätekarten ausgetauscht werden.

In der TI kommen Verschlüsselungsverfahren zum Einsatz, die in Abständen von jeweils fünf Jahren auf neue, zeitgemäße Verschlüsselungsverfahren aktualisiert werden müssen. Nach Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) und der Bundesnetzagentur darf der aktuell in Verwendung befindliche RSA-Algorithmus (Rivest–Shamir–Adleman) in Deutschland nur noch bis zum 31. Dezember 2025 verwendet werden. Ab 1. Januar 2026 muss das neue Verfahren Elliptic Curve Cryptography mit 256 Bit Schlüssellängen (ECC256) genutzt werden. Dieses gilt als sicherer und effizienter als RSA2048.

Betroffen sind bundesweit noch rund 35.000 TI-Konnektoren, 100.000 Heilberufsausweise (eHBA) und 30.000 Praxisausweise (SMC-B-Karten). Durch die hohe Anzahl der noch zu tauschenden Komponenten hält die Kassenärztliche Bundesvereinigung (KBV) eine sichere und reibungsfreie Umsetzung der neuen Verschlüsselungsanforderungen in der Kürze der Zeit für kaum realisierbar und drängt auf eine Fristverlängerung.
Es muss eine geordnete Umstellung ermöglicht werden, zumal andere Länder, wie z.B. Frankreich, weiterhin beide Verfahren zulassen und die Nutzung von RSA2048 dort noch bis Ende 2030 erlaubt ist. Die gematik hält dennoch an dem Zeitplan fest – mit einigen Ausnahmen: Gerätekarten für Kartenterminals dürfen in Abstimmung mit dem BSI vorübergehend auch nach der Frist am 31. Dezember weiter genutzt werden.

Von der Umstellung des Verschlüsselungsverfahrens sind nicht alle Praxen gleichermaßen betroffen. Es hängt davon ab, ob die eingesetzten Komponenten bereits ECC-fähig sind oder ausschließlich mit dem RSA-Verfahren arbeiten können.

Die individuelle Information darüber, welcher Verschlüsselungsalgorithmus aktuell in den TI-Komponenten der Praxis genutzt wird und ob daraus resultierend ein Austausch notwendig wird, erhalten Praxen von ihrem Praxisverwaltungssystem (PVS)-Anbieter bzw. IT-Dienstleister. In der Regel werden sich die PVS-Anbieter/IT-Dienstleister mit der Praxis in Verbindung setzen, wenn der Austausch erforderlich ist. Auch die Anbieter von Heilberufsausweisen und Praxisausweisen haben gegenüber der Kassenärztlichen Bundesvereinigung zugesagt, betroffene Praxen eigenständig auf auslaufende Ausweise hinzuweisen, ohne vorherige Kontaktaufnahme durch die Praxen.

Betroffene Praxen sollten die Vorlaufzeit nutzen und den Austausch mit ihrem PVS-Anbieter/IT-Dienstleister planen, um diesen fristgerecht realisieren zu können.

KV-Connect wird Ende Oktober abgeschaltet
Der Kommunikationsdienst KV-Connect wird am 20. Oktober 2025 abgeschaltet. Der Datenaustausch für die meisten Anwendungen läuft danach über den Kommunikationsdienst KIM (Kommunikation im Medizinwesen), der sich als Kommunikationsstandard im Gesundheitswesen über die Verfahren eRezept, eArztbrief oder eAU etabliert hat. Die Umstellung läuft im Hintergrund über die Softwarehersteller und die Datenannahmestellen.

Praxen, die KIM noch nicht nutzen, sollten den Kommunikationsdienst rechtzeitig bestellen. Erste Ansprechpartner sind der PVS-Hersteller oder IT-Dienstleister der Praxis. Die Kassenärztliche Bundesvereinigung bietet neben anderen Anbietern hierfür mit kv.dox einen eigenen KIM-Dienst an.

Die folgenden Anwendungen laufen künftig ausschließlich über KIM. Eine Übertragung von Daten mit KV-Connect ist nach dem 20. Oktober 2025 nicht mehr möglich:
- 1ClickAbrechnung
- eDMP
- eHKS
- eArztbrief
- eNachricht
- eDokumentation
- QSPB
- U-Teilnahme
- LDT-Auftrag / LDT-Befund
- DiMus

Auch die Anwendungen 116117 Terminservice „Vermittlungscode anfordern“ und 116117 Terminservice „Abrechnungsinformation abrufen“ sind von der Abschaltung von KV-Connect betroffen. Hier erfolgt eine Umstellung auf eine andere technische Schnittstelle (FHIR), die ebenfalls im Hintergrund durch die Softwarehersteller durchgeführt wird.

Weitere Informationen finden Sie unter www.kv.digital >> Medizinische Kommunikation >> KV-Connect

Zusätzlich hat die kv.digital ein Infoblatt mit allen wichtigen Informationen zusammengestellt.

Haben Sie Fragen oder wünschen Sie weitere Informationen? Gern können Sie sich an den IT-Service der KV Sachsen-Anhalt unter it-service@kvsa.de bzw. unter Telefon 0391 627-7000 wenden.

KVSA