Die neue elektronische Patientenakte (ePA) ab 2025: IT-Sicherheit als Grundvoraussetzung in den Praxen

In den vergangenen Wochen sind mehrere mögliche Angriffsszenarien auf die Telematik-Infrastruktur (TI) bekannt geworden. Der Chaos Computer Club (CCC) hat kurz vor dem Jahreswechsel schwerwiegende Sicherheitsmängel bei der elektronischen Patientenakte aufgedeckt.

Einige dieser möglichen Angriffsszenarien betreffen die technischen Systeme außerhalb der Praxen oder den technischen Umgang mit den Versicherteninformationen auf der elektronische Gesundheitskarte (eGK). Für diese möglichen Angriffsszenarien werden derzeit Lösungen entwickelt und Updates durch die jeweiligen Hersteller bereitgestellt.

Andere Angriffsszenarien betreffen jedoch einen möglichen Missbrauch der in den Praxen genutzten Komponenten wie Konnektor und Kartenterminals sowie den darin genutzten Karten, insbesondere den Praxisausweisen (SMC-B). Aus diesem Anlass möchten wir nochmal für das Thema IT-Sicherheit in den Praxen und den Umgang mit den Komponenten und Identitäten informieren und sensibilisieren.

Geben Sie niemals Zugangsdaten oder Ausweiskarten und PIN/PUK weiter!
Mittels der Praxisausweise (SMC-B) und Zugangsdaten identifiziert sich die Praxis oder mit dem elektronischen Heilberufsausweis (eHBA) der Leistungserbringer eindeutig gegenüber der TI. Diese Karten und Zugangsdaten dürfen in keinem Fall an Dritte weitergegeben werden!
Potenzielle Angreifer auf die TI können mit diesen Karten und den entsprechenden Geräten Zugang zur TI erhalten und weisen sich darin dann als die jeweilige Praxis oder Arzt/Psychotherapeut aus und würden Zugriff auf die Daten der Praxis und der Patienten in der TI erhalten.

Umgang mit defekten oder nicht mehr benötigten Komponenten
Sollten Konnektoren oder Lesegeräte weitergegeben werden, müssen vorher die Ausweiskarten (SMC-B und eHBA) entfernt und diese Geräte auf den Werkszustand zurückgesetzt werden. Die Karten müssen unmittelbar über das Kundenportal des Kartenherstellers (D-Trust, medisign oder T-Systems) gesperrt werden. Sollte eine Sperrung durch die Praxis nicht möglich sein, kann das Arztregister der Kassenärztlichen Vereinigung Sachsen-Anhalt (KVSA) die Sperrung beim Kartenhersteller durchführen. Persönliche Zugangsdaten und PIN/PUK für die Ausweiskarten dürfen keinesfalls weitergegeben werden. Diese Informationen sollten datenschutzkonform vernichtet werden, wenn sie nicht mehr benötigt werden. Ob die Geräte veräußert werden dürfen, entnehmen Praxen den Bedingungen des Kauf- oder Mietvertrags mit dem Lieferanten.

Defekte Geräte sollten dagegen sicher bei einem zertifizierten Entsorger entsorgt, das heißt vernichtet werden. Diese Geräte könnten noch sensible Daten enthalten, wenn sie nicht mehr ordnungsgemäß zurückgesetzt werden können. Konnektoren können in der Regel auch an den Lieferanten zurückgegeben werden.

IT-Sicherheit als Grundvoraussetzung in den Praxen
Der Gesetzgeber hat die Kassenärztliche Bundesvereinigung (KBV) beauftragt, eine IT-Sicherheitsrichtlinie für alle Praxen zu entwickeln (nach § 390 SGB V). Diese Richtlinie beschreibt das Mindestmaß der zu ergreifenden Maßnahmen, um die IT-Sicherheit in den Praxen zu gewährleisten. Die Vorgaben an die IT-Sicherheit richten sich nach der Größe der Praxis. Dabei finden sich in der Richtlinie Anforderungen, die von allen Praxen erfüllt werden müssen, um die Sicherheit der verwendeten Hard- und Software zu gewährleisten.

Um den Umgang mit der Richtlinie praxisgerecht zu gestalten, hat die KVSA die Anforderungen nach der jeweiligen Praxisgröße zusammengefasst und in die Form von Checklisten gestaltet, mit der die Praxen die durchgeführten Maßnahmen einfach dokumentieren können. Die betreffenden Checklisten finden Praxen mit Aufruf des am Ende des Artikels aufgeführten Link.

Praxen, die bereits ein aktuelles Virenschutzprogramm verwenden, verschlüsselte Internetanwendungen nutzen und keine vertraulichen Daten über Apps oder per E-Mail versenden, erfüllen bereits einen kleinen Teil der Vorgaben, die durch die IT-Sicherheitsrichtlinie gelten. Darüber hinaus gibt es eine Reihe weiterer wichtiger Anforderungen, die in jeder Praxis Grundvoraussetzung sein muss.

Die wichtigsten Basisanforderungen für alle Praxisgrößen

Sicherer Umgang mit Zugangsdaten
- Verwendung sicherer Kennwörter: Kennwörter sollten mindestens den aktuellen Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik entsprechen: mindestens zwölf Zeichen, Nutzung von Groß- und Kleinbuchstaben, Ziffern sowie Sonderzeichen. Für mobile Geräte sollten möglichst komplexe Entsperrcodes verwendet werden.
- Verwendung von Multi-Faktor-Authentisierung: Bei allen Diensten und Geräten, die dies unterstützen, sollte die Multi-Faktor-Authentisierung eingerichtet werden. Beispiele für zusätzliche Faktoren sind Hardware-Token, wie z. B. der Yubikey, Authenticator-Apps oder Biometrie.

Absicherung von PC-Arbeitsplätzen
- Abmelden oder Sperren: Nach der Nutzung eines Gerätes sollte sich der Nutzer abmelden oder das Gerät

sperren. Geräte sollten so eingestellt sein, dass nach kurzer Zeit der Inaktivität eine automatische Sperrung stattfindet.
- Einsatz von Virenschutzprogrammen: In der Praxis werden aktuelle Virenschutzprogramme eingesetzt.

Schutz des Praxisnetzwerks vor unberechtigten Zugriffen
- Firewall benutzen: Das Praxisnetzwerk sollte durch eine Hardware-Firewall vor unberechtigten Zugriffen aus dem Internet geschützt sein.
- Netzwerk segmentieren: Das Netzwerk sollte in mehrere, voneinander getrennte Zonen eingeteilt sein, z. B. für den Internetzugang, für Praxis-PCs und für Medizintechnik. So kann das Risiko der Ausbreitung von Schadsoftware von Gerät zu Gerät reduziert werden.
- Internetzugang einschränken: Für den Zugang zum Internet sollten keine PCs mit Zugriff auf Patientendaten genutzt werden. Stattdessen empfiehlt sich ein separates Gerät (z. B. Laptop oder Tablet) in einem separaten Netzwerkbereich (z. B. Gäste-WLAN).

Fernwartungszugänge für Dienstleister
- Schriftliche Vereinbarungen treffen: Für alle Dienstleister, die Fernwartungszugänge nutzen sollen, müssen nach Artikel 28 der Datenschutz-Grundverordnung (DSGVO) Vereinbarungen zur Datenverarbeitung im Auftrag abgeschlossen werden. Darin muss geregelt sein, welche Daten verarbeitet werden, wie der Zugriff erfolgt und wer den Zugriff erhält.
- Ein Fernwartungszugriff ist immer von der Praxis aus aktiv freizugeben. Es dürfen keine Zugänge offen im Internet erreichbar sein und es sollten ausreichend sichere Zugangsdaten und Passwörter verwendet werden, keine Standardbenutzer oder Passwörter der Dienstleister.
- Keine Fernwartung ohne Aufsicht: Während der Fernwartung müssen die Dienstleister durch eine geeignete Person aus der Praxis beaufsichtigt werden, um sicherzustellen, dass es keine unberechtigten Zugriffe auf Daten gibt. Es muss jederzeit die Möglichkeit bestehen, seitens der Praxis die Verbindung zu trennen.

Datensicherung und -wiederherstellung
- Regelmäßige Datensicherung: Die Daten der Praxis sollten nach einem festgelegten Plan gesichert und regelmäßig überprüft werden, ob sich die gesicherten Daten wiederherstellen lassen. Wichtig ist auch, dass die gesicherten Daten verschlüsselt und an einem sicheren Ort aufbewahrt werden. Eine aktuelle Kopie der gesicherten Daten sollte möglichst außerhalb der Praxisräume an einem sicheren Ort aufbewahrt werden.

Installation von Updates bzw. Isolierung von Geräten
- Zeitnahes Installieren verfügbarer Aktualisierungen: Für alle Geräte in der Praxis sollten die vom Hersteller bereitgestellten Updates zeitnah installiert werden. Dies betrifft insbesondere Updates der Firewall sowie der Software auf Arbeitsplätzen.
- Isolierung von Geräten ohne Updates: Geräte, die vom Hersteller keine Updates mehr erhalten, sollten keine Verbindung zum Internet oder zu anderen Geräten mit Internetzugang erhalten. Sie sollten in einem separaten Netzwerkbereich untergebracht werden, der nur genau definierte Zugriffe auf andere Geräte erlaubt, z. B. zur Übertragung von Daten aus einem Medizinprodukt.

Dokumentation umgesetzter Sicherheitsmaßnahmen
- Sicheres Aufbewahren von Administrationsdaten: Für die dezentralen Komponenten der Telematik-Infrastruktur sind die Administrationsdaten sicher aufzubewahren.
- Dokumentation des Netzes: Praxen sollten, gegebenenfalls zusammen mit ihrem technischen Dienstleister, einen Plan ihres Netzwerks aufstellen. Dieser Plan sollte alle aktiven Netzwerkgeräte wie Router, Firewall, Switches, Konnektor, Kartenterminals, PCs, Drucker, Medizintechnik, usw. enthalten sowie die Verbindungen zwischen diesen Geräten darstellen.

Weitere Informationen zur Informationssicherheit in der Praxis
Zum Thema Informationssicherheit in der Praxis stellt die KVSA im Internet eine Reihe von Informationsmaterialien bereit, die Sie auf www.kvsa.de >> Praxis >> IT in der Praxis >> IT-Sicherheit finden können.

Darüber hinaus bietet die KVSA ihren Mitgliedern individuelle Beratung sowie die Möglichkeit, sich im Rahmen von Verstanstaltungen zur informieren.

Weitere Informationsmaterialien wie eine Checkliste, Beispiele und Praxis-Tipps bietet die KBV. Es ist ein Serviceangebot zur IT-Sicherheitsrichtlinie, das Praxen nutzen können und das als Unterstützung dienen soll:

- www.kbv.de >> Mediathek >> Publikationen >> Broschüren aus der Reihe Praxiswissen >> IT-Sicherheit

- www.kbv.de >> Service >> Service für die Praxis >> Digitale Praxis >> Datensicherheit

- www.kbv.de >> Service >> Service für die Praxis >> Digitale Praxis >> Datensicherheit >> IT-Sicherheitsrichtlinie

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.