EXTERN

KVB
Kassenärztliche
Vereinigung
Bayerns

KVB 80684 München

An alle
Zugelassene Ärzte/Psychotherapeuten/
Ermächtigte Ärzte/Einrichtungen/Kliniken/
Institute/Labore/BSD-/NAD-Ärzte

Geschäftsführung

Ihr Ansprechpartner:
KVB eTec-Support
Telefon: 089 57093-40040
Unser Zeichen: GT-DIG

27.02.2025

Telematikinfrastruktur (TI): Hinweise zur Sicherheit Ihrer Praxis-IT

Das Wichtigste auf einen Blick:

Zum Hintergrund

Die vom Chaos Computer Club (CCC) Ende letzten Jahres vorgestellten Angriffsszenarien zur neuen elektronischen Patientenakte („ePA für alle“) haben verdeutlicht**, dass Sicherheitsvorkehrungen in den Praxen unerlässlich sind.**

Wir empfehlen

Ergreifen Sie in Ihrer Praxis ausreichende Maßnahmen zum Schutz Ihrer IT-Systeme und -Komponenten sowie zur Verhinderung von Missbrauch sensibler Behandlungs- und Abrechnungsdaten.

Sehr geehrte Damen und Herren,

vor dem Hintergrund der vom CCC im Dezember 2024 aufgezeigten Schwachstellen möchten wir Ihr Bewusstsein dafür schärfen, wachsam zu sein in Bezug auf die Komponenten, die den Zugang zur Telematikinfrastruktur (TI) ermöglichen, und technische sowie organisatorische Maßnahmen zu ergreifen, um Ihre Praxis-IT ausreichend zu schützen und Patientendaten sicher zu verwalten.

KVB Kassenärztliche Vereinigung Bayerns

Komponenten für den Zugang zur TI

Die primären Komponenten für den Zugang zur TI umfassen **den Konnektor, das E-Health Kartenterminal und den Praxisausweis (sogenannte SMC-B Karte).** Insbesondere der **Praxisausweis,** welcher im Kartenterminal steckt, darf nicht wie ein gewöhnlicher, veräußerbarer Teil der Praxisausstattung behandelt werden. Er ist der **Schlüssel,** der Ihre Praxis für die **Zugriffsberechtigung** auf die TI-Dienste eindeutig identifiziert. Zusammen mit der elektronischen Gesundheitskarte **(eGK)** des Patienten gewährt er Zugang zu den in der TI liegenden medizinischen Daten, die beispielsweise in der „ePA für alle“ liegen.

Empfehlung:
Daher ist der Praxisausweis ebenso sensibel zu handhaben wie der elektronische **Heilberufsausweis (HBA).** Die zugehörige PIN und PUK darf niemals leichtfertig an Dritte herausgegeben werden.

Müssen Konnektor oder Kartenterminal ausgetauscht werden, beachten Sie die Empfehlungen der gematik zum sachgerechten Austausch und zur Entsorgung von Altgeräten. So muss der Konnektor abgemeldet und auf Werkseinstellungen zurückgestellt werden, wenn dieser dauerhaft außer Betrieb genommen wird.

Achtung:
Bei der Außerbetriebnahme eines Kartenterminals muss der **Praxisausweis unbedingt aus dem Lesegerät entnommen werden.** Ist dieser noch gültig, kann er in einem anderen Kartenterminal weiterverwendet werden. Eine Weiterverwendung des Praxisausweises darf nur erfolgen, sofern sich die BSNR nicht ändert. Andernfalls ist es notwendig, ihn vor der Entsorgung zu sperren.

Bitte beachten Sie, dass es sich bei diesen Komponenten um **Elektrogeräte** handelt und diese **nicht im Hausmüll** entsorgt werden dürfen.

Phishing-Kampagnen und Schadprogramme

Fast unbemerkt können Viren, Trojaner und andere Schadprogramme auf Ihre Rechner gelangen. Mit besonderer Vorsicht und passender Software kann der Praxis-Computer und andere digitale Geräte besser vor Infektionen geschützt werden.

Kriminelle versuchen häufig aus der Ferne Zugriff auf die Praxis-IT zu erlangen. Eine häufige Methode sind **Phishing-Kampagnen**, bei denen die Opfer **meist per E-Mail** aufgefordert werden, vertrauenswürdige Daten preiszugeben.

Eine weitere Methode sind **Trojaner als eine Art von Schadprogrammen,** die sich oft als legitime Software tarnen, um unbefugten Zugriff auf das System eines Benutzers zu erlangen.

Besondere Vorsicht gilt deshalb bei Downloads und E-Mail-Anhängen. Letztere sollten bei jedem Zweifel, insbesondere wenn die Absender unbekannt sind, gelöscht werden. Außerdem sollten die IT-Systeme regelmäßig auf Anomalien sowie auf Aktualität überprüft werden. **Unverzichtbare Schutzmaßnahmen sind ein aktueller Virenscanner und eine Firewall.**

Externe IT-Dienstleister mit falschen Identitäten

Für Ärzte und Psychotherapeuten kann es ratsam sein, sich externe Unterstützung zu holen, wenn es um die Sicherheit der Praxis-IT geht. Hierbei ist jedoch eine besondere Sensibilität gegenüber externen IT-Dienstleistern geboten. Denn zunehmend geben sich Kriminelle mit falschen Identitäten und Dokumenten als IT-Fachkräfte aus, um an Daten heranzukommen. Deshalb sollten Sie und Ihre Mitarbeitenden sorgfältig verifizieren, ob beispielsweise ein Anrufer tatsächlich die Person ist, die sie vorgibt zu sein. Sie können beispielsweise die Ihnen bekannte Support-Nummer Ihres IT-Dienstleisters wählen und dort nachfragen.

Haben Sie Fragen?

Ausführliche Informationen zur **IT-Sicherheitsrichtlinie der Kassenärztlichen Bundesvereinigung (KBV)** in der Mindestmaßnahmen zum Schutz Ihrer Praxis-IT aufgeführt werden, finden Sie auf der Themenseite "IT-Sicherheitsrichtlinie" auf unserer Homepage.

Unser KVB eTec-Support hilft Ihnen unter der Telefonnummer **089 57093-400 40** oder unter **technik@kvb.de** gerne weiter.

Freundliche Grüße

gez.
Stephan Spring
Geschäftsführer