Alles Gute.

KVBW

Kassenärztliche Vereinigung Baden-Württemberg

IT-Notfallmanagement

Strukturierte Vorgehensweise im IT-Notfall (z. B. Cyber-Angriff)

Ruhe bewahren!

Praxisteam bzw. verantwortliche Person über die Situation informieren

Arbeit am IT-System sofort einstellen und relevante Rechner bzw. Server umgehend ausschalten (Netzwerkstecker ziehen)

Notfallkontakte informieren

IT-Dienstleister: Tel.

Datenschutzbeauftragter der Praxis: Tel.

Cybercrime (ZAC) beim Landeskriminalamt Baden-Württemberg: Tel. 0711 5401-2444

Cyberwehr – Erstkontakt bei Cyberangriffen: Tel. 0800 292379347

alle mit dem IT-Notfall im Zusammenhang stehende Sachverhalte dokumentieren

Wichtige Hinweise

- Anweisungen der Notfallkontakte umsetzen
- ggf. Kassenärztliche Vereinigung bezüglich Abrechnung informieren
- Meldepflicht beim Landesdatenschutzbeauftragten (Frist innerhalb 72 Stunden)!

Präventionsmaßnahmen für die Cybersicherheit in Ihrer Praxis

Die Präventionsmaßnahmen sind jeweils nicht abschließend, sondern decken nur einen Teil der wichtigsten Bereiche der präventiven IT-Sicherheit ab:

- Aufklärung bzw. Schulung des Praxisteams
- Vorhandensein eines gut strukturierten und aktuellen Netzplans
- regelmäßige Durchführung von Backups, diese separieren und testen
- Informationsaustausch mit IT-Dienstleister und Meldekette im Notfall abstimmen
- Passwortrichtlinie inkl. Passwortlänge
- Notfall-Konzept
- aktuelle Software und Updates einspielen

Diese und weitere Maßnahmen finden Sie in der IT-Sicherheitsrichtlinie, die Sie in Ihrer Praxis umsetzen sollten: *https://hub.kbv.de/display/itsrl*

Tipps:

- Meldepflicht bei Datenschutzverstößen beim Landesdatenschutzbeauftragten unter: *https://www.baden-wuerttemberg.datenschutz.de/datenpanne-melden/*
- KBV-Praxischeck Datenschutz und Informationssicherheit: *https://praxischeck.kbv.de/mpc/courses/list.xhtml*