Cybercrime-Maßnahmen

Prävention

- Bewusstsein entwickeln: Es kann jede/n treffen
- Sich Basisinformationen aneignen
- Sich die Folgen eines IT-Ausfalls vor Augen führen: Was geht ohne IT alles nicht? Was sind die Folgewirkungen (medizinisch und wirtschaftlich)?
- Sicherheitsmanagement für die Praxis entwickeln und regelmäßig aktualisieren
- Regelmäßiges Training in der Praxis mit allen Mitarbeiterinnen und Mitarbeitern – Weiterbildung
- Umfassende technische IT-Schutzmaßnahmen setzen – mit Hilfe von Expertinnen und Experten
- Aufwändige, mehrstufige Backups müssen laufend stattfinden – auch Offline-Datensicherung – mit Hilfe von Expertinnen und Experten
- Sichere Passwörter – auch wenn sie unbequem sind – verwenden und regelmäßig ändern
- Individuelle Zugangsdaten für jede berechtigte Person
- Berechtigungen nach individueller Notwendigkeit vergeben (Installation von Software, Updates etc.)
- Verschlüsselung von Daten (soweit technisch möglich)
- Verwendung von vertrauenswürdigen Programmen (keine dubiose Gratis-Software)
- E-Mails eventuell getrennt vom sonstigen System führen (in Abstimmung mit den Expertinnen und Experten)

Vorbereitung für den Ernstfall

- Notfalltelefonnummern zur Hand haben – nicht nur im elektronischen Telefonbuch
- Telefonische Verfügbarkeit ohne IT-gestützte Telefonanlage sichern
- Sich auf eine gewisse Zeit ohne IT (ein Tag, vielleicht sogar mehrere) vorbereiten: Wie kann der Ordinationsbetrieb dennoch funktionieren? Notfallpaket (Informationsunterlagen, Formulare, Aushänge …) auf Papier verfügbar haben

Was tun im Ernstfall (wenn ein Angriff erkannt wurde)?

- IT vom Stromnetz nehmen – und zwar die *gesamte* (auch Netzwerkdrucker etc.)
- *Alle* Netzwerkverbindungen kappen (alle Geräte abstecken)
- Technikerin oder Techniker des Vertrauens alarmieren
- Patientinnen und Patienten informieren
- Ordination auf „Papierbetrieb“ umstellen (der vorbereitet sein muss – Drucker funktionieren nicht mehr)

Nach dem Ernstfall

- Unbedingt Anzeige erstatten (am einfachsten im nächsten Polizeiwachzimmer); je genauer Informationen, z. B. über ein Virus, sind, umso besser
- Meldestelle für Internetkriminalität im Bundeskriminalamt (E-Mail: against-cybercrime@bmi.gv.at) oder Single Point of Contact – SPOC (Tel: +43 1-24836 Dw. 985025, 985026 oder 985027; E-Mail: Bundeskriminalamt@bmi.gv.at) kontaktieren und informieren
- Bei Datendiebstahl Anzeige bei der Österreichischen Datenschutzbehörde (Tel. +43 1 52 152-0; E-Mail: dsb@dsb.gv.at)
- Versicherung informieren (falls vorhanden)

Hilfreiche Links (zur Verfügung gestellt von webquake)

https://www.youtube.com/watch?v=YueZ6kv8TSA (Schulungsvideo)
https://www.youtube.com/watch?v=au2lJT-ywwI (Schulungsvideo)
https://www.onlinesicherheit.gv.at/praevention/startseite.html
https://www.sicher-im-netz.de/
https://cybercheck.de/berufe/aerzte
https://www.wko.at/site/it-safe/mitarbeiter-handbuch.pdf
https://www.wko.at/site/it-safe/kmu-handbuch.pdf

Zusammengestellt auf Basis von Experten-Aussagen (Webquake, Computerhaus Welz, Büroteam Leibnitz, Sie&wir, Bogen & Partner, EDV-Referat der Ärztekammer Steiermark)