Sicherheitstipps fürs Praxisteam

Notebooks, Tablets & Smartphones in der Arztpraxis

Neben den Maßnahmen, die ein IT-Dienstleister z.B. auf Programmebene ergreift, um mobile Endgeräte gegen Datenverlust abzusichern, kann und muss das Praxisteam auch organisatorische Regelungen treffen.

Sichere Passwörter für mobile Geräte

- ☐ Mitarbeiter anweisen: Keine gemeinsamen Passwörter im Praxisteam, jeder Nutzer braucht für jede Anwendung ein eigenes Passwort.
  Außer: Das System verfügt über Single-Sign-On, dann kann das individuelle Passwort einmal für alle Anwendungen eingerichtet und auch immer wieder geändert werden.
- ☐ Mitarbeiter anweisen zur Passwortstärke. Empfohlen wird: mindestens acht Zeichen, bestehend aus Buchstaben, Sonderzeichen und Zahlen, mit Groß- und Kleinschreibung, benutzerbezogene Daten wie Geburtsdatum, Adresse usw. vermeiden. Tipp: Satz ausdenken (Ich habe 23 Tage ! vor Ostern Geburtstag) und Passwort aus Anfangsbuchstaben (Ih23T!vOG) bilden.
  Passworttest unter http://www.anonym-surfen.com/passwort-test
- ☐ Mitarbeiter anweisen: keine automatischen Logins erlauben (kein Passwort speichern in der Anwendung), stattdessen sichere Passwortspeicherung in der Praxis regeln (keine Zettelwirtschaft).
- ☐ Mitarbeiter anweisen: regelmäßigen Passwortwechsel (z.B. quartalsweise)
- ☐ Bei ausscheidenden Mitarbeitern Passwörter abfragen, diese sperren und neue anlegen.
  Ist das vergessen worden, aber ein automatischer Kennwortablauf eingerichtet, ist das Risiko von Missbrauch geringer.
- ☐ Mitarbeiter anweisen: Praktikanten oder Aushilfen keinen Zugang zu Passwörtern geben.
- ☐ Gute Alternativen: USB-Fingerprintlösungen oder Smartcard.

Physische Maßnahmen gegen Geräteverlust

- ☐ Notebooks anschließen, abhängig von der Situation auch bei Einsatz in den Praxisräumen.
- ☐ Notebookschloss vorsehen (Kensington Lock oder Kette).
- ☐ Aufbewahrungsort sichern, wenn das Gerät nur zeitweise im Einsatz ist.

Maßnahmen gegen Verlust / gegen Datendiebstahl bei Verlust des Gerätes

- ☐ Unbedingt Festplatte verschlüsseln!
- ☐ Remote Wipe (Fernlöschung der Daten) einrichten und aktivieren – UMTS nötig.
- ☐ Trackingmöglichkeit (Ortung) einrichten – GPS nötig.
  Achtung: Bei Nutzung durch Mitarbeiter kommt Datenschutz und gegebenenfalls Betriebsrat ins Spiel!
- ☐ Mitarbeiter informieren: Wer wird bei Verlust eines mobilen Gerätes bzw. USB-Sticks benachrichtigt?

Sicherer Einsatz von USB-Sticks

- ☐ USB-Sticks nur mit Passwortschutz und Verschlüsselung zulassen, fremde Datenträger über Erkennung der Seriennummer sperren.
- ☐ Automatische Malware-Scannung bei jedem Anschluss einrichten.
- ☐ Vorhandene USB-Sticks inventarisieren, um Verluste umgehend zu bemerken.

Mitarbeiterunterweisung

- ☐ Richtlinien aufstellen für die private Nutzung von mobilen Geräten.
- ☐ Richtlinien aufstellen für die Nutzung von Social Media auf Praxisgeräten (sollte in der Regel verboten sein bzw. kann technisch unterbunden werden).
- ☐ Regelmäßige Mitarbeiteraufklärung zur generellen Sicherheit bei mobilen Geräten als Teil der Schulungen bzw. Sensibilisierungen zum Thema Datenschutz.
- ☐ Unangekündigte Tests durchführen: z.B. Anruf eines angeblichen Technikers, der zu Durchführung einer Wartung die Passwörter abfragt (und sie oft auf diesem Weg erhält).