IT-Sicherheit in der Ordination

Schutz personenbezogener Daten in der täglichen Praxis.

ganyMED Kutschera
DIE IT-KOMPLETTLÖSUNG FÜR IHRE ARZTPRAXIS

Horst Kögler

Graz, 16.1.2020

ganyMED
DIE LÖSUNG FÜR IHRE ARZTPRAXIS.

Umgang mit PCs und Daten

- **Aktuellste Software** verwenden (Windows 7 ist nicht mehr erlaubt)
- **Clear Desk Policy** (Ausdrucke, Kennwörter usw. nicht sichtbar für andere am Arbeitsplatz…)
- Schriftstücke und Datenträger **richtig entsorgen**
- **Wechselmedien und mobile Geräte** besonders schützen (Verschlüsselung, nicht im Fahrzeug liegen lassen…)
- **Social Engineering** verhindern (Herauslocken von Informationen über Telefon, Sichtschutz auf Monitor, PC beim Verlassen mit „Win + L“ sperren…)

gany MED
DIE LÖSUNG FÜR IHRE ARZTPRAXIS.

Passwörter

- **Sichere Passwörter** verwenden
- **Mindestens 10 Zeichen,** mit Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen
- **Niemals** Namen, Vornamen, Geburtsdatum, Wörter aus dem Wörterbuch usw.
- **Tipp:** Passwort aus Wortanfängen und Satzzeichen eines Merksatzes, z.B. „Ein langes Passwort ist auf jeden Fall immer sicher!“ = „1lPiajFis!“

Nutzung von Internet

- Internet-Surfen mit **Hausverstand** (Ist das ein angesehener Anbieter? Vorsicht beim Herunterladen von Programmen!)
- Nur **verschlüsselte Seiten** nutzen („https:“ vor dem www!)
- **Besondere Vorsicht bei sozialen Netzwerken** (Ist Facebook, Instagram etc. am Ordi-PC erlaubt? Auch Schadprogramme werden dort oft verbreitet.)

E-Mails und Spam

- 2/3 der weltweiten E-Mails sind unerwünschte Nachrichten (**Spam**) mit mehr oder weniger gefährlichem Inhalt!
- Die **meisten Schadensfälle** entstehen durch Klicks in gefälschten E-Mails (Cryptolocker, Ransomware)!
- E-Mails vor dem Öffnen von Beilagen oder Klick auf Links **immer auf Echtheit prüfen**!!! (Hausverstand einschalten, nicht übereilt handeln!)
- **Im Zweifel** löschen oder IT-Betreuer kontakieren.

Die Datensicherung

- **Datensicherungskonzept** muss vorhanden sein
- **Tägliche/Laufende** Datensicherung
- **Mehrere Datenträger** abwechselnd benutzen
- **Sicherungsprotokoll** prüfen (Checkliste mit Unterschrift)
- Mind. 1 Sicherung immer **extern lagern**
- Datenträger **verschlüsseln**
- Sie sind **gesetzlich verantwortlich**, dass die Daten nicht verloren gehen (Hardwaredefekt usw.)