IT+Technik

Passwort – **Aber sicher**

Fast jeder Web-Dienst fordert eins, manche kann man nicht mal ändern und dann ist die gewählte Komplexität auch noch zu gering – Passwörter. Sie verfolgen uns im Alltag, sind aber doch (noch) unerlässlich. Nachfolgend ein paar **Hintergründe und Tipps** zum leichteren Umgang.

Dass nur die persönliche Kenntnis eines Geheimnisses den Zugriff auf ausgewählte Dienste und Informationen ermöglicht, kennen wir schon lange – die PIN einer EC-Karte ist de facto auch ein Passwort. Denn das Passwort – in Verbindung mit einem Benutzerkonto, einer E-Mail Adresse oder eben der EC-Karte – dient der Authentifizierung eines Benutzers und soll so die Vertraulichkeit von Informationen sicherstellen oder die Nutzung von Angeboten auf zahlende, zumindest aber bekannte Kunden einschränken.

Dies gilt auch in der Arztpraxis, wo sensible Patienteninformationen nur für festgelegte Mitarbeiter zugänglich sein dürfen und protokolliert werden kann, von wem eine Änderung im AIS durchgeführt wurde.

Unsichere, sogenannte „schwache" Passwörter stellen heutzutage keinen ausreichenden Schutz vor Missbrauch durch Dritte dar, denn mit entsprechenden Werkzeugen ausgestattet können schwache Passwörter in Sekunden (!) entschlüsselt werden. Es gibt zwei entscheidende Merkmale für die Stärke eines Passworts: die Länge sowie die Anzahl der verwendeten Zeichen.

Rein statistisch steigt der Aufwand zum Erraten eines Passworts immens, wenn Sie nicht nur (Groß- und Klein-) Buchstaben verwenden, sondern auch Sonderzeichen und Zahlen einbauen. Neben dem stumpfen Durchprobieren aller Möglichkeiten gibt es auch intelligentere Ansätze zum Knacken eines Passwortes: Bei sogenannten Wörterbuchangriffen werden bekannte Begriffe einer oder mehrerer Sprachen als gesamte Zeichenkette ausprobiert. Auch sinnvolle Zahlenkombinationen (bspw. Geburtsdaten) liegen als Quelle zur Durchführung eines Angriffs auf Passwörter vor.

Wie man sichere Passwörter generiert, die man sich auch noch merken kann, finden sie im Kasten.

Darüber hinaus empfehlen Sicherheitsexperten, Passwörter in regelmäßigen Abständen zu ändern, um der Gefahr des zufälligen Bekanntwerdens zu begegnen. In der Arztpraxis kann ein regelmäßiger Wechsel oftmals durch Richtlinien erzwungen werden und ist mindestens dann geboten, wenn der Dienstleister wechselt oder ein Mitarbeiter ausscheidet.

Und auch wenn es Konzepte gibt, die Passwörter zumindest theoretisch überflüssig machen könnten – begleiten werden sie uns noch sehr lange.

Sichere Passwörter

Für ein nach heutigem Maßstab ausreichend sicheres Passwort sollten Sie zumindest folgende Empfehlungen berücksichtigen:

- Länge: 10 Zeichen
- Verwendung von mindestens drei der vier Zeichensätze Kleinbuchstaben, Großbuchstaben, Ziffern, Sonderzeichen
- Keine Wörter oder Namen
- Sollte nicht den Benutzernamen oder größere Bestandteile dessen enthalten

Um sich solche Zeichenketten besser merken zu können, hilft in der Regel ein Merksatz. So wird aus den führenden Buchstaben des Satzes: „Für 2014 habe ich 3 gute Vorsätze!" das Kennwort „F2014hi3gV!".
Und wenn Sie nicht dasselbe Passwort für mehrere Konten verwenden wollen, kombinieren Sie ein sicheres Kennwort mit einer dienst-spezifischen Ergänzung, z. B. „Di1sPfm-mail" für Ihren E-Mail Account und „Di1sPfm-foto" für das digitale Fotoalbum.

Christian Kierdorf
IT-Sicherheitsbeauftragter Deutscher Hausärzteverband

Foto: fotolia