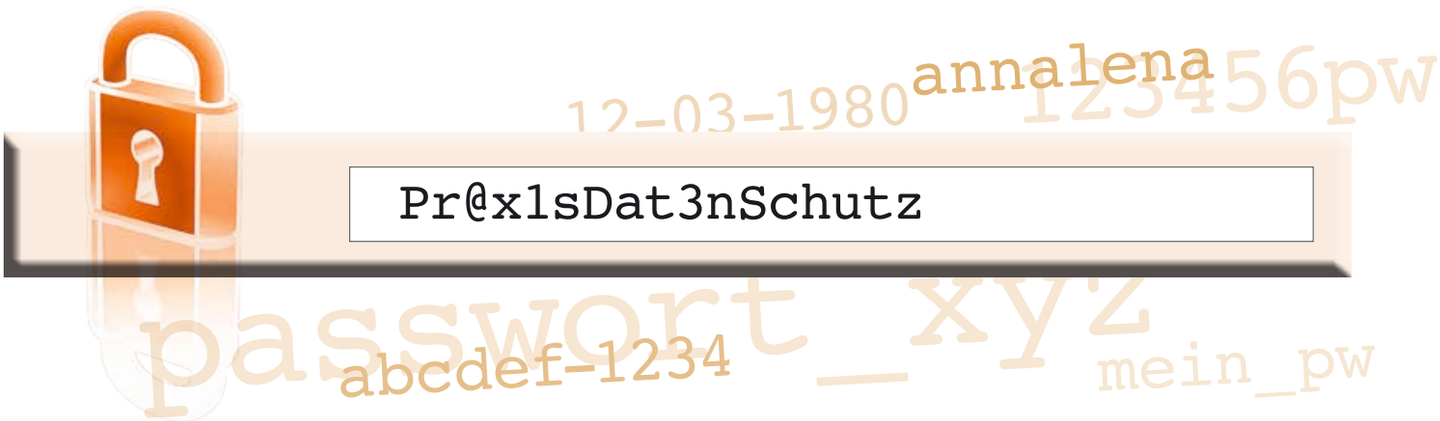
Gut geschützt mit Passwörtern

Nina Richard, M. Sc.



Jeder Arbeitsplatz, egal ob er mit dem Internet verbunden ist, Zugriff auf die Patientendaten per Patienteninformationssystem ermöglicht oder die Buchhaltung beinhaltet, sollte durch ein Kennwort geschützt sein. Kennwörter dienen in Kombination mit dem Benutzernamen der Authentifizierung von Personen am jeweiligen Arbeitsplatz. Damit wird sicher gestellt, dass nur die Informationen zur Verfügung gestellt werden, die für die tägliche Arbeit relevant sind. So gilt es, hierarchische Strukturen, Zuständigkeiten und Kompetenzen bei der Zuteilung von Berechtigungen zu berücksichtigen. Die Praxismanagerin benötigt beispielsweise im Vergleich zu der Auszubildenden einen erweiterten Zugriff auf die Praxissysteme. Zum anderen schützen Passwörter Praxis- und Patientendaten.

Im oftmals hektischen Arbeitsalltag oder außerhalb der Sprechzeiten ist es nicht immer möglich, alle Arbeitsplätze in der Praxis im Auge zu behalten: Sie sind unbeaufsichtigt und, im Falle eines Einbruchs, eine gern genommene Möglichkeit, ohne Probleme an wertvolle Daten zu gelangen.

Passwörter richtig einsetzen

Passwörter sind schön und gut, aber nur, wenn Sie richtig eingesetzt werden. Vermeiden Sie deshalb:

- Zettel am Monitor, auf der Schreibtischunterlage oder unter der Tastatur, auf denen Sie Ihr Passwort notieren.
- Nutzen Sie keine Sammelaccounts. Erfahrungsgemäß führen solche Accounts zu einem Sinken des Datenschutzniveaus, da für jeden merkbare Kennwörter wie „Praxis1234“ genutzt werden.
- Verraten Sie Ihr Kennwort niemandem. Jeder Mitarbeiter sollte einen eigenen Zugang mit den entsprechenden Zugriffsrechten erhalten.
- Nutzen Sie keine Passwörter, die ihr Geburtsdatum, die Namen der Kinder oder simple Tastaturreihenfolgen wie „wertzuiop“ oder „123456“ sind.

All dies erleichtert den unerwünschten Zugriff auf schützenswerte Daten.

So geht's richtig

Grundsätzlich gilt: Je komplexer ein Kennwort, desto sicherer ist es. Das heißt, es sollte aus mindestens acht Zeichen, Groß- und Kleinschreibung und Sonderzeichen bestehen, um diese Komplexität zu gewährleisten.

Beispiel: Pr@x1sDat3nSchutz

Da solche Passwörter nur schwer zu merken sind, kann eine gleichwertige Komplexität ebenfalls durch eine entsprechende Länge des Passworts erreicht werden. Passwörter wie „Datenschutz-InUnseremGesundheitswesen" oder „SicherePasswoerterSindWichtig!" sind ggf. deutlich leichter im Gedächtnis zu behalten – und für einen Angreifer schwer zu knacken.

Sollten Passwörter regelmäßig gewechselt werden?

Grundsätzlich sind regelmäßige Passwortwechsel sinnvoll. Dabei sollte jedoch bedacht werden, dass Nutzer, die komplexe Passwörter oft tauschen, dazu neigen, diese immer weniger komplex zu gestalten. Im schlimmsten Fall führt dies dazu, dass der Endbenutzer sein Passwort auf einem Zettel notiert und diesen am Bildschirm festklebt. Ein Zustand, den es definitiv zu vermeiden gilt.

In Umgebungen, in denen hochsensible Daten verarbeitet werden, ist ein Passwortwechsel alle drei Monate angezeigt. In allen anderen Situationen genügt ein jährlicher Passwortwechsel.

Maßnahmen:

- Jeder Account ist mit einem Passwort geschützt.
- Passwörter verfügen über eine ausreichende Komplexität, z. B. mindestens 8 Zeichen lang.
- Passwörter enthalten Groß- und Kleinschreibung, mindestens eine Zahl oder ein Sonderzeichen.
- Passwörter sind maximal ein Jahr gültig
- Passwörter werden lediglich verschlüsselt als Hashes abgespeichert und niemals im Klartext.
- Nach 15 fehlerhaften Logins wird der Account für mindestens 30 Minuten gesperrt, um einem unbemerkten Durchprobieren von Passwörtern entgegenzuwirken.

Nina Richard, M. Sc.

Nina Richard, M. Sc. ist Leiterin Marketing und Kommunikation bei DATATREE AG/ISDSG, Institut für Sicherheit und Datenschutz im Gesundheitswesen. Zudem betreut Sie die Fort- und Weiterbildungsangebote wie den zertifizierten Datenschutzbeauftragten (IOM) und die Angebote der DATATREE-Akademie.