IT+Technik

Kein **Zutritt!**

Die dunkle Jahreszeit ist Jahr für Jahr die Zeit der Einbrecher. Ein abgestuftes Zutrittskonzept hilft nicht nur gegen Langfinger, sondern legt auch die Grundlage für **effektiven Datenschutz**.

Im Bundesdatenschutzgesetz – und de facto analog im Sozialgesetzbuch – wird als erste Maßnahme für einen effektiven Datenschutz die Zutrittskontrolle aufgeführt. Dem Gesetz zufolge gilt es *„Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle)"* [Anlage 1 zu § 9, (1) BDSG]. Der **Zutrittsschutz** ist somit auf die physische Absicherung der Daten ausgelegt und soll den Zugang zu Daten(-verarbeitungsanlagen) unterbinden – angefangen bei Mauern, über Haus- und Kellereingänge bis hin zu den Bürotüren in der Praxis.

Christian Kierdorf
IT-Sicherheitsbeauftragter Deutscher Hausärzteverband

Da die Vorgaben für Hauswände und tragende Wände in der Regel ausreichend sind, sollte man bei der Gesamtbetrachtung der Zutrittssicherheit Fenstern und Türen erhöhte Beachtung schenken. So ist in diversen Normen verankert, welcher Widerstandsklasse der Einbruch- oder Feuerhemmung ein Fenster oder eine Tür zuzurechnen ist. Zur Beratung bei Neu- und Umbauten wenden Sie sich am besten an einen Fachmann vor Ort. Weiterhin sind die Schlösser zu berücksichtigen, auch hier gibt es unterschiedlichste Ausführungen der Sicherheitsstufen – selbstverständlich normiert – sowie Schließsysteme, bei denen Sie mittels Generalschlüssel überall Zutritt haben, nicht aber die Mitarbeiter, Reinigungskräfte oder ein IT-Dienstleister. Neben mechanischen Schlössern gibt es mittlerweile vermehrt elektronische Schließsysteme, die auch den zeitgesteuerten Zutritt erlauben – somit können Sie den Zutritt über Nacht oder am Wochenende nur für bestimmte Personen(-kreise) erlauben. Die obigen Überlegungen werden ebenfalls durch die Lage der Praxis beeinflusst, da in Industriegebieten andere Gefährdungen zu berücksichtigen sind als in belebten Innenstadtlagen oder einem Wohngebiet.

Wenn Sie die richtigen Voraussetzungen geschaffen habe, gilt es nur noch, die zentrale Fragestellung zu beantworten: **Wer darf wann wohin?** Hierfür gibt es keine Norm und eventuell ist die zeitliche Komponente vernachlässigbar, aber folgende Überlegungen sollten Sie anstellen:
Wer muss in den Rechnerraum? Und darf der IT-Fachmann auch ohne Anwesenheit von Praxismitarbeitern oder einem Arzt an die Systeme? Besser wohl nicht! Muss jeder Mitarbeiter ins Archiv oder gibt es sonstige Räumlichkeiten, die nur ausgewählten Mitarbeitern vorbehalten sind? Experten sprechen hier von der Festlegung von Sicherheitszonen. Bei allen Überlegungen sollten Sie Notfälle wie eine akute Erkrankung oder Ähnliches berücksichtigen und – vielleicht in einem versiegelten Umschlag oder einem per Zahlenschloss gesicherten Schlüsselkasten – einen Generalschlüssel vorhalten.

Grundsätzlich sollten Sie ein Inventar der Schlüssel pflegen, in dem per Schlüsselnummer dokumentiert wird, wann eine Schlüsselausgabe erfolgt ist und wann der Schlüssel zurückgegeben wurde. Mitarbeiter sollten dafür sensibilisiert werden, verloren gegangene oder gestohlene Schlüssel zu melden. Versicherungen gegen Schlüsselverlust minimieren im Bedarfsfall die Kosten für einen Austausch.

Foto: fotolia