# Ist Ihre IT-Sicherheit up to date?

## Datenschutz und IT-Sicherheit in der Zahnarztpraxis

Der gemeinsame Leitfaden „Datenschutz und IT-Sicherheit“ der KZBV und BZÄK wurde aktualisiert und um Aspekte der neuen IT-Sicherheitsrichtlinie erweitert. Der Beitrag greift aus der Fülle der in der 84-seitigen Broschüre angesprochenen Themen einige beispielhaft und gestrafft heraus, um zu zeigen, dass der Leitfaden eine praxisorientierte Orientierungshilfe zum Thema IT-Sicherheit bietet.

### PCs, Mobilgeräte und Tablets – das müssen Sie beachten

Die Anforderungen an Hard- und Software hängen maßgeblich von der Größe der Praxis ab. Sind mehrere Rechnerarbeitsplätze vorhanden, kann ein zentraler Rechner (Server) installiert werden, der sämtliche Daten vorhält. Keinesfalls sollte der Server gleichzeitig als Arbeitsplatz genutzt werden.

Für jeden einzelnen Arbeitsplatz gilt: Mikrofon und Kamera am Rechner generell abschalten und nur bei Bedarf temporär direkt am Gerät aktivieren, um eine unautorisierte Nutzung zu verhindern. Nach Ende der Anwendung ist der Zugang zum Gerät immer zu sperren, sodass es nur über die erneute Eingabe des Kennworts wieder gestartet werden kann. Die Synchronisierung von Nutzerdaten mit Cloud-Diensten sollte vollständig deaktiviert werden, da die Betriebssysteme diese Daten sammeln und häufig unbemerkt an den Hersteller weitergeben.

### Schwachstelle Kennwort

Wirksamen Schutz vor unberechtigtem Zugriff bieten Kennwörter nur, wenn sie bestimmte Kriterien erfüllen und regelmäßig gewechselt werden. Zudem darf ein Kennwort nur für jeweils einen Zweck genutzt werden. Verlässt ein Mitarbeiter die Praxis (beispielsweise wegen Kündigung), sind dessen Berechtigungen und die persönlichen Zugänge bzw. Accounts sofort zu löschen oder zu ändern.

Sinnvoll ist es, neben dem Konto des Administrators zusätzliche Benutzerkonten einzurichten. So können jedem Mitarbeiter genau die – eingeschränkten – Rechte zugewiesen werden, die dieser für seine tägliche Arbeit benötigt.

Foto: Sikov - stock.adobe.com

## NACHSCHLAGEWERK ZUM DOWNLOAD

Umfangreiche Informationen zum Thema Datenschutz und IT-Sicherheit bietet der aktualisierte Leitfaden von KZBV und BZÄK:

bzaek.de/fileadmin/PDFs/za/datenschutzleitfaden.pdf


### Regelmäßige Updates und Backups

Unverzichtbar ist der Schutz der PCs durch ein stets aktuelles Virenschutzprogramm, das regelmäßig die gesamte Festplatte sowie den Datenbestand überprüft. Das Programm läuft üblicherweise im Hintergrund und beeinträchtigt die Nutzung der Geräte nicht oder nur minimal.

Daten-Backups schützen im Falle eines Diebstahls oder Elementarschadens vor Datenverlust. Transportable Speichermedien (zum Beispiel Bänder, externe Festplatten, Flash-Speicher) können möglicherweise auch in einem Datentresor außerhalb der Praxis aufbewahrt werden.

Wie die Rechner selbst muss auch das Speichermedium durch Verschlüsselung vor dem Zugriff Unbefugter geschützt werden. Wenn möglich wird ein Mitarbeiter benannt, der die Sicherheits-Updates ausführt und regelmäßig überprüft.

### Auch Software hat ein Verfallsdatum

Betriebssystem und PC-Software haben in der Regel eine begrenzte Lebensdauer. Nach Ablauf können die Systeme zwar ohne Weiteres weiterverwendet werden, sie werden jedoch nicht mehr mit aktuellen Sicherheits-Updates versorgt. Schnell kann sich hier unbemerkt eine Sicherheitslücke auftun, das Risiko eines Hackerangriffs auf das „veraltete System“ steigt.

### Besondere Vorsicht bei Smartphone und Tablet

Mobilgeräte wie Smartphones und Tablets gehören heute zur Standard-Ausstattung. Um das erforderliche Schutzniveau für die verarbeiteten Daten sicherzustellen, sollten hier jedoch stets die strengsten bzw. sichersten Einstellungen gewählt werden.

Bevor eine Praxis Smartphones oder Tablets einsetzt, empfiehlt es sich, Nutzung und Kontrolle der Geräte generell festzulegen, ebenso die Frage, welche Daten übertragen werden dürfen. Auch bei Mobilgeräten lassen sich Zugriffsrechte durch Berechtigungen individuell je nach Aufgabengebiet regeln.

Die Geräte selbst müssen mit einem komplexen Gerätesperrcode und die eingesetzten SIM-Karten durch PIN geschützt werden. Der Zugriff auf den Super-PIN wie auch auf den PUK darf nur durch Verantwortliche erfolgen.

### Klare Regeln für Apps

Generell sollten Apps nur aus den offiziellen Stores heruntergeladen werden. Der für Datensicherheit Verantwortliche prüft die Apps und gibt den Download frei. Wichtige Kriterien: Werden die Dokumente verschlüsselt? Erfolgt die Speicherung der Daten ausschließlich lokal? Vertraulichen Daten sollten über Apps prinzipiell nicht versendet werden.

Updates des Betriebssystems und der eingesetzten Apps müssen auch auf mobilen Geräten stets zeitnah installiert werden, um Schwachstellen zu vermeiden. Zum Schutz vor Phishing und Schadprogrammen im Browser gibt es ebenfalls Schutzprogramme. Apps, die nicht mehr verwendet werden, gilt es restlos zu löschen.

**Redaktion BLZK**