praxisoptimierung.at

10

CYBER SECURITY

MASSNAHMEN

publiziert

04/2025

Ihr kompakter und praxisnaher Leitfaden für Arztpraxen mit den 10 wichtigsten Maßnahmen zur Vermeidung von Cyberkriminalität.

10 Cybersecurity-Maßnahmen

FÜR IHRE ARZTPRAXIS

STEP 01

Schulung des Praxisteams

Schulen Sie regelmäßig Ihr gesamtes Team zu Cyberrisiken wie Phishing-Mails, gefälschten Links oder verdächtigen Anhängen. Menschen sind oft das Einfallstor Nr. 1.

STEP 02

Vorsicht bei E-Mails oder falschen Webshops mit Sonderangeboten

Öffnen Sie keine Anhänge oder Links in E-Mails von unbekannten Absendern. Besonders bei Feiertagsangeboten oder ungewöhnlichen Rechnungen gilt: lieber doppelt prüfen als einmal zu viel klicken. Bestellen Sie Praxisbedarf nur über bekannte, seriöse Anbieter. Besonders zu Feiertagen tauchen vermehrt Fake-Shops mit Sonderangeboten auf.

STEP 03

Starke Passwörter und 2-Faktor-Authentifizierung

Verwenden Sie für alle Systeme starke, individuelle Passwörter. Aktivieren Sie wo möglich Zwei-Faktor-Authentifizierung, z. B. bei Cloud-Zugängen oder Mail-Accounts.

STEP 04

Regelmäßige Software-Updates

Stellen Sie sicher, dass Betriebssysteme, Virenschutz, Praxissoftware und Browser immer auf dem neuesten Stand sind. Viele Angriffe nutzen bekannte Sicherheitslücken aus.

STEP 05

Zugriff nur nach Bedarf

Nicht jede:r Mitarbeiter:in braucht Zugang zu allen Daten oder Funktionen. Arbeiten Sie mit Rollen- und Rechtemanagement, um den Zugriff gezielt zu steuern.

+43 664 600 22 605 praxisoptimierung.at office@praxisoptimierung.at

10 Cybersecurity-Maßnahmen

FÜR IHRE ARZTPRAXIS

STEP 06

Sicheres Backup-Konzept

Erstellen Sie regelmäßige, automatisierte Backups Ihrer Patientendaten und speichern Sie diese an einem vom Praxisnetzwerk getrennten Ort (z. B. extern oder verschlüsselt in der Cloud).

STEP 07

Keine privaten Geräte am Praxisnetz

Vermeiden Sie, dass Mitarbeiter:innen ihre privaten Handys, Laptops oder USB-Sticks mit dem Praxisnetzwerk verbinden – das kann Einfallstore öffnen.

STEP 08

Cyberversicherung

Eine Cyberversicherung kann den Schadensfall zwar nicht verhindern, schützt aber vor finanziellen Folgen durch verschiedenste Formen von Cyberattacken erkundigen Sie sich bei Ihrem Versicherungsberater

STEP 09

Zugriffe überwachen

Führen Sie ein Protokoll über Systemzugriffe und Aktivitäten. So können verdächtige Vorgänge frühzeitig erkannt und analysiert werden.

STEP 10

Notfallplan bereithalten

Was tun bei einem Cybervorfall? Legen Sie fest, wer kontaktiert wird (z. B. IT-Dienstleister, Datenschutzbeauftragte:r), welche Systeme wie abgeschottet werden und wie die Kommunikation erfolgt.

+43 664 600 22 605 praxisoptimierung.at office@praxisoptimierung.at

Sie suchen eine umfassende Sicherheitslösung für Ihre Praxis?

Gerne stellen wir den Kontakt zu einem Experten aus unserem Netzwerk her.

office@praxisoptimierung.at

+43 664 600 22 605