Praxistipps zur Stärkung der Cybersicherheit

Diese 13 Praxistipps sollen dazu beitragen, die Cybersicherheit in Ihrer Praxis zu stärken und sensible Patientendaten zu schützen:

1 Sicherheitsschulung für Mitarbeiter

Schulen Sie das gesamte Praxispersonal in Bezug auf sichere Online-Verhaltensweisen und Sensibilisierung für Phishing-Angriffe.

2 Regelmäßige Software-Updates

Halten Sie Betriebssysteme, Anwendungen und Antivirensoftware auf dem neuesten Stand, um Sicherheitslücken zu schließen.

3 Starke Passwörter und Zwei-Faktor-Authentifizierung

Ermutigen Sie Mitarbeiter dazu, starke, einzigartige Passwörter zu verwenden und aktivieren Sie die Zwei-Faktor-Authentifizierung für kritische Systeme.

4 Netzwerksegmentierung

Teilen Sie Ihr Netzwerk in verschiedene Segmente auf, um den Zugriff auf sensible Daten zu beschränken.

5 Regelmäßige Datensicherung

Führen Sie regelmäßige Backups Ihrer Patientendaten durch und speichern Sie diese an einem sicheren Ort.

6 Sicherheitsrichtlinien und -verfahren

Entwickeln und dokumentieren Sie klare Sicherheitsrichtlinien und Verfahren, die von allen Mitarbeitern befolgt werden müssen.

7 Sicherheitssoftware einsetzen

Installieren Sie Firewalls, Intrusion Detection-Systeme und Antivirensoftware, um Angriffe zu erkennen und abzuwehren.

8 Physische Sicherheit

Schützen Sie Serverräume und Hardware vor unbefugtem Zugriff.

9 Notfallplan für Sicherheitsvorfälle

Entwickeln Sie einen Notfallplan, um auf Sicherheitsvorfälle angemessen zu reagieren und den Geschäftsbetrieb aufrechtzuerhalten.

10 Externe Sicherheitsbewertungen

Lassen Sie regelmäßige Sicherheitsbewertungen von unabhängigen Experten durchführen, um Schwachstellen zu identifizieren.

11 Datenschutz und Compliance

Achten Sie auf die Einhaltung der Datenschutzbestimmungen (z.B. DSGVO) und anderer gesetzlicher Vorschriften.

12 Sichere mobile Geräte:

Implementieren Sie Richtlinien für die sichere Nutzung von Mobilgeräten, die in der Praxis verwendet werden.

13 Regelmäßige Überwachung und Audit:

Überwachen Sie das Netzwerk kontinuierlich auf verdächtige Aktivitäten und führen Sie regelmäßige Sicherheitsaudits durch.