Datensicherheit und -schutz in der Zahnarztpraxis:

CRONIQ Ingenieurgesellschaft mbH
Dipl.-Ing. Tilo Schneider
zertifizierter IT-Sicherheitsbeauftragter
Geneststrasse 5 · 10829 Berlin
www.croniq.de info@croniq.de

CRONIQ

Tausend Finanz GmbH
Marcus Tausend
zertifizierter Berater Heilwesen (IHK)
Taubenstrasse 26 · 10117 Berlin
www.tausend-finanz.de
info@tausend-finanz.de

Tausend Finanz

Zuerst sollten Sie Ihre Datensicherung überprüfen. Wenn Sie Zweifel haben, ob eine Rücksicherung erfolgreich sein wird, sollten Sie die Wiederherstellung von Daten von Ihrem IT-Dienstleister testen lassen. Sorgen Sie außerdem dafür, dass Sie in regelmäßigen – bestenfalls täglichen – Abständen alle Daten auf externen Speichermedien sichern. Diese sollten Sie außerhalb Ihrer Praxis aufbewahren. Im Fall eines Brandes, eines Wassereinbruchs oder eines anderen Schaden-Ereignisses werden Sie verstehen, was dieser Tipp wert war.

Der nächste Blick sollte Ihrem Internetzugang gelten. Verwenden Sie einen handelsüblichen Router, besteht hier Handlungsbedarf. Diese Geräte sind aus einer Reihe von Gründen für den Heimgebrauch gut geeignet. Für den Einsatz in Ihrer Praxis sind sie ungeeignet. Ersetzen Sie Fritz!Box, Speedport und Co. gegen professionelle IT-Sicherheitssysteme.

Wenn die Daten in Sicherheit sind und Ihre Verbindung zum Internet ein Sicherheitsniveau aufweist, das Sie als Praxisinhaber erwarten, dann sollten Sie sich als nächstes um Ihr Computernetzwerk und Ihre digitalen Arbeitsplätze kümmern.

Ihr Computernetzwerk ist das zentrale Nervensystem, über das alle beteiligten Arbeitsplätze, Drucker und sonstige Systeme Informationen untereinander austauschen. Stellen Sie sicher, dass Ihnen alle, die in Ihrem Netzwerk agieren dürfen, bekannt sind.

Dokumentieren Sie akribisch alle PCs, Server, Router, Drucker, Kartenterminals usw. Sorgen Sie dafür, dass Sie zu allen Geräten detaillierte Informationen besitzen und in jedem Fall alle administrativen Passwörter zur Hand haben. Das ist z. B. dann der Fall, wenn Sie sich von Ihrem Administrator trennen oder ein Dritter Sie nach einem IT-Sicherheitsvorfall bei der Forensik unterstützen soll.

Verschaffen Sie sich einen Überblick, welche Personen Zugang und Zugriff auf Ihre IT-Systeme und damit auf Ihre Patientendaten haben. Das können Sie leicht durch den Einsatz eines zentralen Berechtigungs-Servers erledigen, der gleichzeitig dafür sorgt, dass Unberechtigte draußen bleiben.

Wenn nicht jetzt, wann dann?

Datensicherheit und -schutz sollte ein regelmäßiges Thema in Ihrer Praxis sein.

Und schon sind wir bei Ihrem wichtigsten Handlungsfeld: Ihre Mitarbeiter. Vermitteln Sie Ihren Mitarbeitern ein Gefühl dafür, was die in Ihrer Praxis genutzte Informationstechnologie für einen Stellenwert für die tägliche Arbeit aller Beteiligter hat.

Alle digital unterstützen Prozesse in Ihrer Praxis sind heute durch Gefahren aus dem Internet, durch Schadsoftware und bewusstes oder versehentliches Fehlverhalten Ihrer Mitarbeiter gefährdet.

Und zu guter Letzt der Hinweis, dass auch die erfahrensten IT- und Datenschutz-Experten keine 100%-ige Sicherheit für Ihre Patientendaten gewährleisten können. Selbst wenn Sie Ihren Internetzugang, die Datensicherung, die IT-Systeme und das Know-How Ihrer Mitarbeiter auf geforderten Standard gebracht haben, besteht immer noch eine Gefahr.

Mutwilliges oder versehentliches Löschen, Vervielfältigen oder Weitergeben der Patientenakten kann den Datenschutz-Supergau herbeiführen. Dann hilft Ihnen nur noch der Griff zum Telefonhörer, um den Vorfall mit Ihrer Cyberrisk- und Datenschutz-Versicherung zu besprechen, die dann alles Weitere veranlassen, damit Sie möglichst schnell wieder arbeiten können.

momius / Tausend Finanz GmbH