*Praxismanagement Bublitz-Peters*
*Unternehmensberatung im Gesundheitswesen*

PRAXISMANAGEMENT BUBLITZ PETERS

**Newsletter „Cyberschutz und Datensicherheit im Gesundheitswesen“ – Ausgabe 01/2021**

# Immer mehr Cyberattacken im Gesundheitswesen!

**Die Digitalisierung im Gesundheitswesen hat nicht nur wegen der aktuellen Corona-Pandemie deutlich an Fahrt aufgenommen. Damit einher geht jedoch auch eine zunehmende Zahl an Hackerangriffen auf sensible Patientendaten. Wir informieren darüber, wie Sie den Angriffen – und diese werden kommen – vorbeugen können und was zu tun ist, wenn Ihre Praxis angegriffen wurde.**

Immer mehr Arztpraxen, Pflegedienste, Kliniken und andere Akteure im Gesundheitswesen erleben folgendes Horrorszenario: Plötzlich ist der Zugriff auf die Daten verschlüsselt und Erpresser fordern ein hohes Lösegeld, damit sie die Daten wieder freigeben. Doch auch wenn Sie das Lösegeld zahlen, heißt das nicht, dass Sie dann wieder Zugriff auf Ihr System bekommen. Oftmals tauchen die Kriminellen mit dem Lösegeld einfach ab. Die Folgen für Sie sind verheerend: Die Daten sind für immer verloren, Sie haben viel Geld gezahlt und die Patient*innen haben das Vertrauen in Ihre Einrichtung verloren. Im schlimmsten Fall droht der Verlust der beruflichen Existenz.

## So beugen Sie vor

✓ Sensibilisieren Sie sich selbst und Ihre Angestellten

✓ Stellen Sie die Rechner so auf, dass kein schneller Zugriff auf USB-Anschlüsse möglich ist

✓ Ändern Sie regelmäßig die Passwörter (verwenden Sie Groß- und Kleinbuchstaben und Sonderzeichen, benutzen Sie keine Trivialnamen)

✓ Erstellen Sie regelmäßig (am besten täglich) Back-Ups Ihrer Daten und bewahren Sie die Datenträger an einem sicheren Ort außerhalb der Praxis auf

✓ Halten Sie das Betriebssystem, die Anti-Viren-Software, das Praxisverwaltungssystem, den TI-Konnektor und den Router immer auf aktuellem Stand (regelmäßiges Einspielen von Updates, Aktualisierung der Firmware etc.)

**Sollte es trotzdem zu einem Hackerangriff kommen, beachten Sie unbedingt die folgenden Punkte:**

## Notfallplan

⏩ Arbeit am IT-System **sofort** einstellen
⏩ Mit dem Hinweis auf eine „technische Störung“ schließen
⏩ Informieren Sie Ihre Cyberschutz-Versicherung
⏩ Beobachtungen dokumentieren
⏩ Weitere Maßnahmen am System **nur nach Anleitung durch Experten** ergreifen
⏩ **Strafanzeige** stellen
⏩ **Meldung der Datenschutzverletzung** innerhalb von 72 Stunden
⏩ IT-Dienstleister und die ZAC (Zentrale Ansprechstelle Cybercrime) informieren

Um in Zukunft für den Ernstfall gerüstet zu sein, sollten Sie sich oder Ihre Mitarbeiter/innen zur/zum

**Cyberschutz-Beauftragten (PBP) im Gesundheitswesen**

weiterbilden. Die **Heidelberger Health Care Academy** vermittelt in einem 3-teiligen Kompaktseminar sofort anwendbares Praxiswissen. Sie lernen Ihre Praxis oder Einrichtung effektiv und gemäß der neuen IT-Richtlinie der KBV vor Cyberrisiken zu schützen und bei einem Hackerangriff richtig zu reagieren.
So sorgen Sie für Datenschutz und Datensicherheit!

**Praxismanagement Bublitz-Peters GmbH & Co. KG**
Rohrbacher Str. 28
69115 Heidelberg
www.bublitzpeters.de
+49 (0) 62 21 - 43 85 00
info@bublitz-peters.de

**© Praxismanagement Bublitz-Peters 2021**

**Weitere Veranstaltungen:**