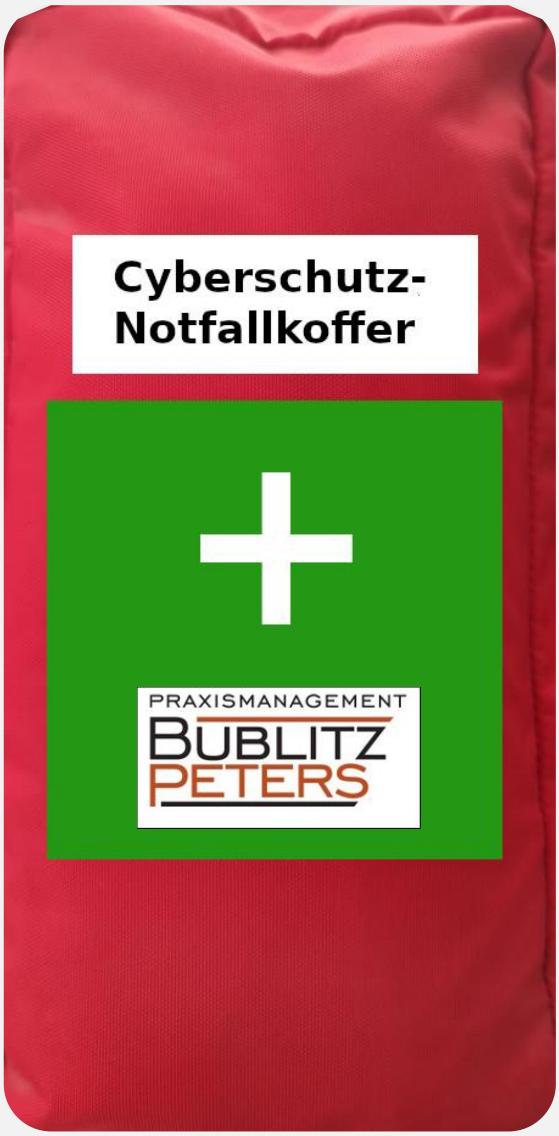
ITe@sy Praxismanagement

Was tun im IT-Notfall?

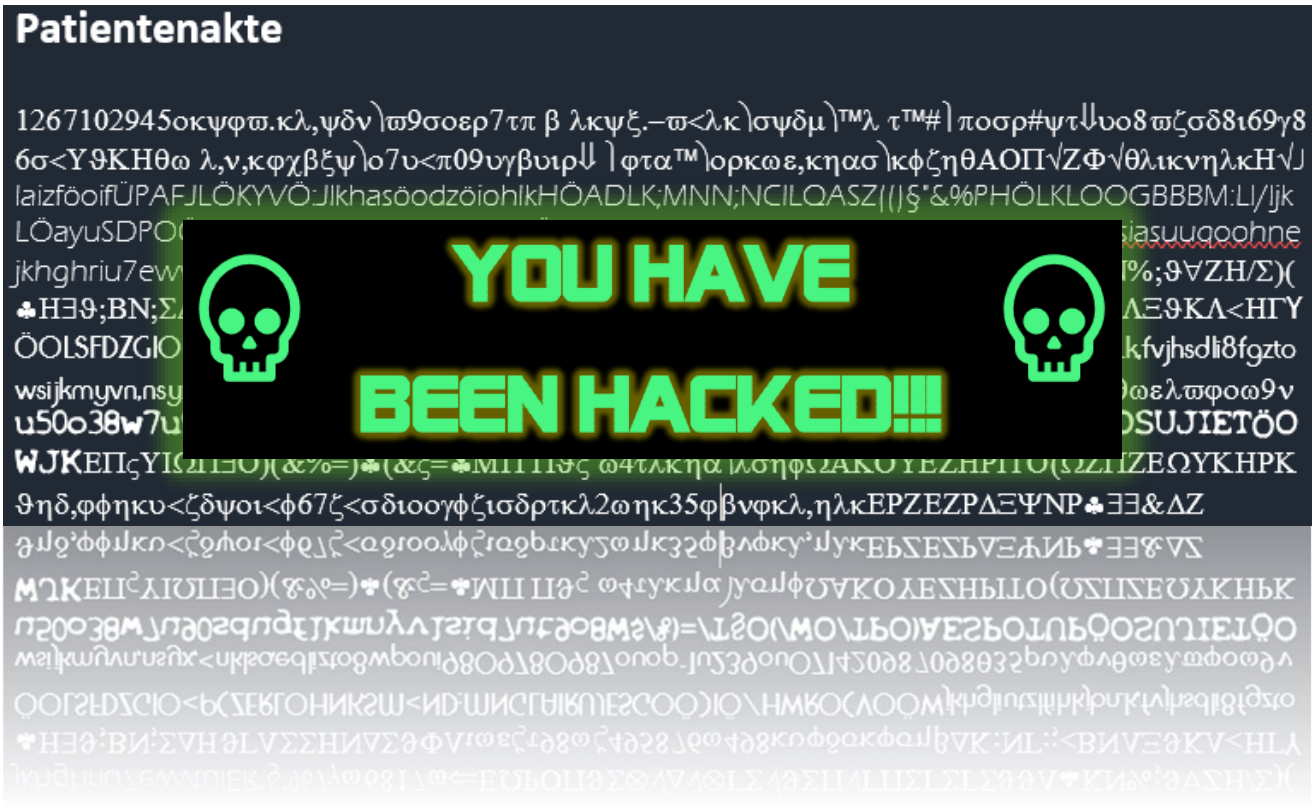


IT-Sicherheit

Was tun im Notfall?

Was tun im IT-Notfall?

Vorbeugen



Risiko

Durch die unzureichende Absicherung Ihres Netzwerks können sich Kriminelle unerlaubt Zugang zu Ihren sensiblen Daten verschaffen und diese verschlüsseln.

Die Ausgangssituation

Die reinste Horrorvorstellung! Es ist Montagmorgen, die Patientinnen und Patienten stehen bereits in einer langen Schlange vor Ihrer Praxis und es geht: NICHTS!!! Cyberkriminelle haben sich Zugriff zu Ihrer Praxisverwaltungssoftware verschafft, die Daten verschlüsselt und drohen nun damit, diese unwiederbringlich zu zerstören, wenn Sie nicht bereit sind, ein hohes Lösegeld zu zahlen. Da ist guter Rat teuer!

Soweit muss es aber nicht kommen! In diesem ITe@sy erfahren Sie, wie Sie sich vor einem Cyberangriff schützen, und wie Sie sich, sollte ES trotz aller Vorsichtsmaßnahmen doch passieren, gezielt darauf vorbereiten können.

Übung macht den Meister!

Vorbeugen

Gut zu wissen: Sie sind Angriffen auf Ihr Praxis-Netzwerk nicht schutzlos ausgeliefert. Im Vorfeld können Sie eine ganze Menge tun, um sich vor Schäden zu schützen.

Am Anfang steht zunächst eine Bestandsaufnahme: Wie ist das vorhandene EDV-Netzwerk aufgebaut? Welchen möglichen Gefahren sind Ihre sensiblen Daten ausgesetzt? Denken Sie dabei nicht nur an Schäden durch Cyberkriminalität, sondern auch an Gefahren durch Wasserschäden, Vandalismus etc.

Diese Gefahrenquellen sollten Sie clustern und in einem nächsten Schritt eine Liste erstellen mit technisch-organisatorischen Maßnahmen, die Sie ergreifen können und sollten, um alle in der Praxis vorhandenen Daten zukünftig besser schützen zu können.

Der erste Schritt: Verschaffen Sie sich zunächst einen Überblick. Daran anschließend stellen Sie Maßnahmen zusammen, die Sie Schritt für Schritt umsetzen können.

Wo finde ich Unterstützung?

Natürlich können Sie nicht über das Fachwissen verfügen, um Ihr EDV-System ausreichend vor Gefahren abzusichern. Sprechen Sie deshalb mit Ihrem IT-Dienstleister, nehmen Sie gegebenenfalls Kontakt zu Ihrem Vermieter auf und klären Sie, welche baulichen Veränderungen Sie vornehmen dürfen, um die Praxis vor Einbrechern zu schützen. Und natürlich steht auch Praxismanagement Bublitz-Peters an Ihrer Seite und unterstützt Sie im gesamten Prozess.

Auf der folgenden Seite erhalten Sie eine Liste mit technisch-organisatorischen Maßnahmen (TOM), die Sie in Ihrer Praxis umsetzen sollten. Hierbei handelt es sich um Maßnahmen, die nach Artikel 32 der Datenschutz-Grundverordnung vorgeschrieben sind, um die Sicherheit personenbezogener Daten zu gewährleisten.

Wichtig ist, zunächst Verantwortlichkeiten für die einzelnen Aufgaben festzulegen. Die grundsätzliche Verantwortung liegt jedoch beim Praxisinhaber.

Die aufgeführten Maßnahmen sind grob gegliedert nach Maßnahmen zum Schutz des Netzwerks und nach baulichen Gegebenheiten, die Sie beachten sollten. Aus diesen TOMs lässt sich dann ein Notfallplan ableiten.

Auch wenn sich diese Liste natürlich noch beliebig erweitern lässt, so bilden die dargestellten Maßnahmen eine erste solide Basis.

Die getroffenen Maßnahmen sollten Sie in Zukunft dann regelmäßig auf ihre Aktualität und Effektivität hin überprüfen (mindestens ein Mal pro Jahr) und - wenn nötig - anpassen.