LPPKJP HESSEN

Hinweise zum Datenschutz in der Praxis

Die Gefahr eines Angriffs durch Schadsoftware besteht auch für den Praxiscomputer und sollte nicht unterschätzt werden. Wir haben einige Empfehlungen zusammengestellt, um zu gewährleisten, dass sensible Patientendaten gut geschützt sind.

Dies sind nur einige, keineswegs vollständige Hinweise zur Datensicherheit. Informieren Sie sich regelmäßig über aktuelle Sicherheitsgefährdungen und entsprechende Gegenmaßnahmen, z. B. in regelmäßig erscheinenden Periodika und bei IT-Fachleuten.

Maximale Sicherheit:

- Nutzen Sie zwei voneinander getrennte Computer für die Patientendaten und zur Nutzung Ihres Email-Accounts bzw. des Internets: Der Praxiscomputer mit den Patientenakten sollte nicht an das Internet angeschlossen werden!
- Sind Kontakte mit dem Internet unvermeidbar, beispielsweise für Softwareupdates, beachten Sie bitte die entsprechenden Sicherheitsmaßnahmen im folgenden Abschnitt.

Mögliche Gefährdung auch bei Beachtung folgender Sicherheitsmaßnahmen:

- Patientenakten müssen passwortgeschützt gespeichert werden.
- Befunddaten niemals unverschlüsselt über das Internet versenden.
- Achten Sie auf ein sicher verschlüsseltes WLAN.
- Sorgen Sie für einen immer aktuellen Virenscanner und eine funktionsstarke Firewall-Lösung.
- Keine unbekannten USB-Sticks verwenden wegen der Gefahr der Übertragung von Computerviren auf den Computer. Vor jeder Datenübertragung von einem externen Speichermedium auf einen Praxisrechner sollten die zu übertragenden Daten mit einer entsprechenden Software auf eine potentielle Gefährdung geprüft werden. Zur sicheren Umgehung von Bootsektormalware kann der zu übertragende Inhalt auch auf eine DropBox hoch- und von dort heruntergeladen werden.
- Öffnen Sie Anhänge von Emails nur, wenn Ihnen der Absender bekannt ist. Da auch Ihnen bekannte Emailkonten zu Angriffszwecken benutzt werden können, öffnen Sie nie Anhänge mit aktiven Inhalten wie .zip- oder.exe-Dateien. Im Zweifel beim Absender nachfragen! Evt. E-Mail-Anhänge mit geeigneten Virenscannern (z. B. Virus Total) checken.
- Makros nach Möglichkeit deaktivieren.
- Installieren Sie keine Software, deren Quelle Sie nicht sicher kennen.

- Sorgen Sie für eine funktionsfähige Back-Up-Lösung Ihrer Systemdaten mit einer täglichen Sicherung Ihrer Dokumente und Patientendatenbank auf einer externen Festplatte. Das Sicherungssystem vom Internet und vom PC getrennt verwahren! Monatlich prüfen, ob die Sicherungen funktionsfähig sind. Möglichst eine zweite, zumindest einmal monatlich aktualisierte Sicherungs-Festplatte außerhalb der Praxis in einem Banksafe verwahren.

- USB-Festplatte nur für die Zeit der Sicherung mit dem PC verbinden, anschließend wieder trennen.
- Spielen Sie nie eine Sicherung ein, wenn Sie nicht 100% sicher sind, dass das System sauber ist.

Sollten Sie feststellen, dass Ihr System befallen wurde:

- Isolieren Sie sofort den befallenen Computer vom Netzwerk und schalten Sie ihn aus. Ist das Gesamtsystem betroffen, setzen Sie es außer Betrieb bspw. durch das Herunterfahren aller Server und organisieren Sie sich professionelle Hilfe.
- Noch ein Wort zu Ransomangriffen: Werden Sie aufgefordert, zur Deaktivierung eines Angriffes auf Ihre Daten Geld zu zahlen, erstatten Sie sofort Anzeige bei der Polizei. Eine Wiederherstellung von durch solche Schadsoftware verschlüsselten und z. T. veränderten Daten ist meistens nicht möglich. Selbst der vom Angreifer versprochene Schlüssel zum Rückgängigmachen der Verschlüsselung ist oft eine Täuschung und wird zerstörte Daten nicht wiederherstellen können. Die Polizei wird Ihnen in der Regel raten, nicht zu zahlen.