04.03.2016 BDC|News

Locky und Co: So können sich Praxen vor Computerviren schützen

Kassenärztliche Bundesvereinigung

Aktuell verbreiten sich sogenannte Verschlüsselungstrojaner wie Locky oder TeslaCrypt mit rasanter Geschwindigkeit im Internet und machen auch vor Krankenhäusern und Arztpraxen nicht Halt. Cyberkriminelle verschlüsseln die Dateien ihrer Opfer und fordern Lösegeld für die Entschlüsselung. Praxen können Vorkehrungen treffen, um sich vor solchen Angriffen zu schützen.

Die aktuell grassierenden Verschlüsselungstrojaner sind so gut programmiert, dass die einmal verschlüsselten Daten verloren scheinen. Trotzdem empfiehlt zum Beispiel das Bundesamt für Sicherheit in der Informationstechnik (BSI), das geforderte Lösegeld nicht zu zahlen. Die Erfahrungen der letzten Wochen zeigen, dass die von den Cyberkriminellen versprochene Entschlüsselung oftmals trotz einer Lösegeldzahlung ausbleibt.

Es ist daher sehr empfehlenswert, einige wichtige Grundsätze beim Surfen im Internet und beim Öffnen von E-Mails zu beachten und alle Praxismitarbeiter für dieses Thema zu sensibilisieren.

Updates installieren und aktuelle Antiviren-Software nutzen

Auch bei Computern ist der beste Schutz die Vorsorge: Schadsoftware sollte erst gar nicht auf den Praxisrechner gelangen können. Dabei hilft ein regelmäßiges Update des Betriebssystems, des Browsers und sämtlicher genutzter Software – in Kombination mit einer aktuellen Antiviren-Software. Ein Virus kann ansonsten schon allein durch den Besuch einer entsprechend präparierten Webseite den Praxisrechner infizieren.

Auf den E-Mail-Absender achten

Cyberkriminelle versuchen auch, ihre Schadsoftware per E-Mail mit Dateianhang oder über Verlinkungen zu verteilen. Derzeit fügen sie ihren E-Mails zum Beispiel eine Word-Datei bei, die dann durch eine sogenannte Makro-Funktion für die eigentliche Infektion sorgt. Daher gilt es, beim Öffnen von E-Mails und insbesondere den Dateianhängen und mitgeschickten Links größte Vorsicht walten zu lassen.

Der E-Mail-Empfänger sollte stets die Identität des Absenders prüfen – E-Mail-Adressen lassen sich durch Cyberkriminelle leicht fälschen. Handelt es sich wirklich um die bekannte E-Mail-Adresse oder wird beispielsweise nur der Name des Absenders angezeigt und es ist eine unbekannte Adresse hinterlegt? Im Zweifelsfall sollten Dateianhänge beziehungsweise Links nicht geöffnet werden.

Backup für den Ernstfall: Daten regelmäßig sichern

Eine wirkungsvolle Absicherung für den Ernstfall bieten Datensicherungen – sogenannte Backups. Sollte ein Praxisrechner von einem Virus betroffen sein, können die verlorenen Daten darüber wiederhergestellt werden. Moderne Verschlüsselungstrojaner sind allerdings mittlerweile in der Lage, auch die Daten in angeschlossenen Netzlaufwerken und auf externen Festplatten mit zu verschlüsseln.

Ein Backup, das zum Beispiel auf einer externen, aber weiterhin angeschlossenen Festplatte abgelegt wird, wäre dadurch ebenfalls verloren und somit wertlos. Daher ist es wichtig, Backups auf Speichermedien abzulegen, die nicht dauerhaft mit dem potentiell betroffenen Praxisrechner verbunden sind.

Weiterführende Informationen
Tipps und Informationen des BSI zu Backups
KBV Praxis-IT
Broschüre "Sicheres Surfen im Internet - So schützen Sie sich!"

Quelle: Kassenärztliche Bundesvereinigung, Herbert-Lewin-Platz 2, 10623 Berlin, http://www.kbv.de