Vorgehensweise bei einem Ransomware-Vorfall in der Arztpraxis

Sofortmaßnahmen

1. Bewahren Sie Ruhe und trennen Sie betroffene Computer oder Arbeitsplätze sofort vom Netzwerk, um die Ausbreitung der Ransomware zu verhindern. Schalten Sie WLAN, Netzwerkkabel und andere Verbindungen ab. Lassen Sie die Geräte eingeschaltet!
2. Notieren oder fotografieren Sie alle Warnungen oder Nachrichten, die auf dem Bildschirm angezeigt werden, und halten Sie fest, welche Computer oder Geräte betroffen sind (z. B. PC, Server).

Kommunikation

1. Informieren Sie alle Mitarbeitenden über den Vorfall.
2. Melden Sie den Vorfall umgehend an Ihren IT-Dienstleister, die Kassenärztliche Vereinigung und – falls Patientendaten betroffen sind – an die zuständige Datenschutzbehörde Ihres Bundeslandes.

Erste Schritte zur Eindämmung (in Zusammenarbeit mit Ihrem IT-Dienstleister)

1. Prüfen Sie die aktuellen Backups und stellen Sie sicher, dass sie intakt und nicht betroffen sind. Führen Sie keine Wiederherstellung durch, bevor Ursache und Umfang des Angriffs geklärt sind.
2. Erstellen Sie eine Kopie der verschlüsselten Daten, falls zukünftig ein Entschlüsselungstool verfügbar wird.
3. Dokumentieren Sie alle Feststellungen und machen Sie Screenshots der Ransomware-Nachrichten. Sichern Sie E-Mails, die auf den Angriff hindeuten.

CGM CompuGroup Medical

Technische Unterstützung

1. Kontaktieren Sie umgehend einen spezialisierten IT-Dienstleister für Cybersicherheit und besprechen Sie die Analyse und Bereinigung der Systeme.
2. Erkundigen Sie sich bei Bedarf bei Stellen wie LKA, BKA oder BSI nach Entschlüsselungstools und weiterer Unterstützung.

Nachbereitung und Prävention

1. Nach erfolgreicher Bereinigung spielen Sie die Daten aus den Backups zurück. Überprüfen Sie alle Systeme auf verbleibende Schwachstellen.
2. Schulen Sie Ihr Praxisteam in IT-Sicherheit und im Erkennen von Phishing-Angriffen. Entwickeln Sie klare Richtlinien zur Vorbeugung.
3. Implementieren Sie zusätzliche Sicherheitsmaßnahmen wie Schutzsoftware für alle Geräte, die Trennung von Netzwerken (Netzwerksegmentierung) und regelmäßige Sicherheitsupdates.

Wichtige Kontakte im Notfall

- IT-Dienstleister
- Kassenärztliche Vereinigung
- Gesetzliche Notrufnummern für Cybersecurity-Vorfälle

(Bitte halten Sie die entsprechenden Telefonnummern in Ihrer Praxis stets griffbereit.)

Weitere Informationen unter **cgm.com**/it-sicherheit

CompuGroup Medical Deutschland AG
Maria Trost 21, 56070 Koblenz
cgm.com/de