

Datenraub bei über 15 Mio. Patienten

Frankreichs Datenleck zeigt: Ende-zu-Ende-Verschlüsselung muss Standard für Praxissoftware werden

Die wichtigsten Punkte im Überblick:

- In Frankreich wurden nach einem Cyberangriff auf den Praxissoftware-Anbieter Cegedim Santé Daten von rund 15 Millionen Menschen entwendet.
- Der Vorfall verdeutlicht: Zentral gespeicherte Klartextdaten und Daten mit providerseitig zugänglichen Schlüsseln sind ein systemisches Risiko.
- RED ist überzeugt: Nur Ende-zu-Ende-verschlüsselte Cloud-Systeme, bei denen ausschließlich die Leistungserbringer die Daten entschlüsseln können, verhindern solche Leaks wirksam.

München, 6. März 2026

Eine massive Cyberattacke auf den französischen Praxissoftware-Anbieter Cegedim Santé hat gezeigt, wie schnell aus „Verwaltungsdaten“ ein existenzielles Vertrauensproblem werden kann: Berichten zufolge wurden bei dem Hackerangriff die Datensätze von rund 15 Millionen Patienten entwendet. In etwa 165.000 Fällen sind zusätzlich Freitext-Notizen vom Datenleck betroffen – darunter auch Informationen zu Spitzenpolitikern und Sicherheitsbeamten. Teilweise enthalten die Texte höchst sensible Angaben, etwa zu HIV-Status, sexueller Orientierung, Religion oder Suizidgedanken. Diese Datensätze sind nun im Darknet aufgetaucht. RED sieht darin einen Weckruf für das gesamte europäische

Gesundheitswesen und fordert, Ende-zu-Ende-Verschlüsselung als Sicherheitsstandard für Praxissoftware konsequent zu etablieren.

Ende-zu-Ende-Verschlüsselung im Gesundheitswesen bedeutet, dass Daten **bereits beim Leistungserbringer** verschlüsselt werden und **nur dort** wieder entschlüsselt werden können – mit einem Code, der nur dem Leistungserbringer bekannt ist. Bei einer vollständigen Ende-zu-Ende-Verschlüsselung kann also kein Dritter, auch nicht der Softwarehersteller selbst, die im PVS hinterlegten Daten lesbar machen. Im Ernstfall sind abgegriffene Datenbanken dann „wertlos“, weil Angreifer keinen Zugriff auf den Klartext haben.

Jochen Brüggemann, Geschäftsführer von RED, ordnet den Vorfall ein:

„Wenn handschriftliche Konsultationsnotizen im Netz auftauchen, ist das mehr als ein kleiner Datenschutzvorfall – es ist ein Bruch des zentralen Versprechens im Gesundheitswesen: Vertraulichkeit! Systeme müssen so gebaut sein, dass selbst ein erfolgreicher Hacker-Angriff nicht automatisch zu einem Klartext-Datenleak führt. Dafür braucht es Ende-zu-Ende-Verschlüsselung – nicht als Option, sondern als Standard.“

Was Leistungserbringer jetzt prüfen sollten

RED empfiehlt Praxen und Einrichtungen aller Fachrichtungen, ihre Praxissysteme mit Blick auf folgende Fragen zu bewerten:

- **Sind meine Daten konsequent verschlüsselt?** Werden alle Daten immer und überall verschlüsselt gespeichert und transportiert?
- **Wer besitzt die Schlüssel?** Liegt die Entschlüsselung ausschließlich bei mir selbst – oder kann mein Softwareanbieter serverseitig entschlüsseln? Ein Hinweis auf serverseitige Schlüssel (= Risiko) ist, wenn es eine “Passwort zurücksetzen”-Funktion gibt (siehe auch unten).
- **Sind Freitext-Felder geschützt?** Werden Notizen, Kommentare, Bilder und Dokumente technisch genauso streng abgesichert wie medizinische Daten?
- **Wie wird Zugriff abgesichert?** Ist meine Praxissoftware technisch in der Lage, Benutzerrollen und Zugriffsrechte zu vergeben?

Um herauszufinden, ob Datenbanken vollständig Ende-zu-Ende-verschlüsselt sind, reicht ein einfacher Test: Ist ein Servicepartner oder Softwareanbieter in der Lage, bei Passwortverlust auszuweichen, hat er Zugriff auf die Daten – denn wenn er ein neues Passwort erstellen kann, dann kann er dieses auch für sich selbst erstellen und die Datenbank damit auslesen. Und wenn der Anbieter das kann, kann ein Hacker das auch. Es handelt sich in so einem Fall also nicht um eine konsequente Ende-zu-Ende-Verschlüsselung (E2E). Leider haben Tests von RED ergeben, dass die meisten Praxisverwaltungssysteme keine echte E2E-Verschlüsselung vorweisen können.

Jochen Brüggemann weist auf die damit einhergehenden Gefahren hin:

“Viele Wettbewerber speichern Daten so, dass sie – wenn überhaupt – nur serverseitig verschlüsselt werden. Genau hier liegt die Achillesferse: Wird ein Anbieter kompromittiert, droht im schlimmsten Fall ein massenhafter Abfluss von auswertbaren Patientendaten.”

Für weitere Informationen zum wirksamen Schutz vor Hackerangriffen und zu sicherer Cloud-Praxissoftware lesen Sie [unseren Artikel zum Thema](#) oder kontaktieren Sie RED unter sales@redmedical.de.

Die RED Medical Systems GmbH wurde im Jahr 2013 von Jochen Brüggemann und Alexander Wilms mit der Vision gegründet, durch intelligente, sichere und cloudbasierte Systeme die tägliche Arbeit aller Heilberufler zu erleichtern und so das deutsche Gesundheitswesen in ein neues, digitales Zeitalter zu führen. Derzeit arbeiten für das Unternehmen rund 80 Mitarbeiter:innen an zwei Standorten (München, Bendorf). RED entwickelt und vertreibt folgende Produkte:

RED medical

- KBV-zertifizierte und Ende-zu-Ende-verschlüsselte Psychotherapie-Praxissoftware
- Vollständig cloudbasierte Lösung für mobiles, geräteunabhängiges Arbeiten
- Intelligente All-in-One-Lösung (Dokumentation, Abrechnung, Videotherapie & Praxisverwaltung)

RED medical classic

- Erste vollständig cloudbasierte Arztsoftware mit KBV-Zertifizierung
- Ende-zu-Ende-verschlüsseltes System ohne eigenen Praxis-Server
- Mobiles Arbeiten jederzeit möglich – unabhängig vom Endgerät

RED telematik

- Anschluss an die Telematikinfrastruktur
- Konnektor in mehrfach gesichertem Rechenzentrum ("TI as a Service")
- Automatische Updates und Sicherheitschecks sowie regelmäßige Fernwartungen

RED connect

- Zertifiziert sichere Videosprechstunde
- Deutschlandweiter Marktführer mit über 70.000 registrierten Anwendern
- Orts- und geräteunabhängig nutzbar

RED protect

- Firewall-Lösung speziell für kleine und mittelgroße Praxen
- Wirksamer Schutz vor unbefugtem externen Zugriff auf das Praxisnetzwerk
- Erfüllt die Firewall-Anforderung der IT-Sicherheitsrichtlinie der KBV

Kontakt & weitere Informationen:

RED Medical Systems GmbH, Lutzstraße 2, 80687 München

Annika Götz (Leiterin Vertrieb und Key-Account-Management)

sales@redmedical.de

www.redmedical.de