Datenschutz im Gesundheitswesen

Sensible Patientendaten: Woran Sie eine sichere Praxissoftware erkennen können

München, 25. August 2022

Die Nachricht über eine datenschutzrelevante Sicherheitslücke in einer bekannten deutschen Praxissoftware löst aktuell große Beunruhigung unter Heilberuflern aus. Einer IT-Aktivistengruppe war es offenbar ohne größeren Aufwand gelungen, sensible Patientendaten innerhalb kürzester Zeit aus dem entsprechenden medizinischen Verwaltungssystem auszulesen. Dabei lagen die Daten offenbar unverschlüsselt auf einem Server – ein Zustand, der im Gesundheitswesen leider viel zu häufig vorkommt. Es zeigt sich erneut: Die Verwahrung der Patientendaten in den Praxen selbst bietet nur eine trügerische Scheinsicherheit. Ergo: Nur eine echte Ende-zu-Ende Verschlüsselung aller medizinischen Daten – wie bei der cloudbasierten Praxissoftware RED medical – kann den Zugriff durch unbefugte Dritten wirksam verhindern. Ein wichtiges (und oftmals unterschätztes) Kriterium: Auch der Hersteller selbst darf zu keiner Zeit Zugriff auf die Klartext-Daten haben. Ob diese Anforderung auch auf die eigene Praxissoftware zutrifft, können Leistungserbringer mit einem einfachen Trick selbst herausfinden.

Hintergrund der aktuellen und branchenweiten Datenschutz-Diskussion ist, dass die auf IT-Sicherheit spezialisierte Aktivistengruppe *Zerforschung* mehrere gravierende Datenschutzlücken innerhalb einer bekannten deutschen Praxissoftware entdeckt hat. Laut einem Medienbericht von *NDR* und *WDR* soll es der Gruppe unter anderem gelungen sein, jegliche E-Mail-Kommunikation zwischen Arzt und Patienten innerhalb der Software einzusehen. Außerdem erlangten die Experten offenbar Zugang zu hochsensiblen Dokumenten wie Diagnosen, Laborbefunden, Blutwerten oder Attesten. Insgesamt seien von dieser IT-Lücke laut dem Berliner Datenschutzbeauftragten “mehr als 60.000 Patient:innen

von mehr als 270 Praxen betroffen" – ein Umstand, der nun verständlicherweise einen großen öffentlichen Aufschrei nach sich zieht.

Möglich war das Ganze offenbar nur, weil die Daten auf den Servern der Arztpraxen nicht verschlüsselt wurden, sondern im Klartext vorlagen – sie waren damit leichte Beute für die Aktivistengruppe, die die sensiblen Patienteninformationen anscheinend mühelos auslesen konnte. Laut *NDR* und *WDR* standen den Daten-Aktivisten mehr als eine Million Datensätze offen. Im folgenden Schaubild wird das Problem deutlich.

Nur Ende-zu-Ende verschlüsselte Patientendaten sind sicher

Das Kernproblem: Patientendaten, die im Klartext auf einem Server gespeichert werden, sind keine Seltenheit im Gesundheitswesen – und zwar unabhängig davon, ob es sich um einen Cloud-Dienst oder eine herkömmliche Software mit einem lokalen Server in der Praxis handelt. Sobald sich Cyberkriminelle erst einmal Zugang zum Inneren der Anwendung verschafft haben, haben beide Modelle dasselbe Problem: Die Daten können innerhalb kürzester Zeit aus dem medizinischen Verwaltungssystem ausgelesen werden. Auf diesen veritablen Missstand innerhalb der Branche möchte RED in aller Deutlichkeit hinweisen.

Außerdem wird an diesem Punkt bereits klar, dass datenschutztechnisch die Trennlinie nicht zwischen cloudbasierten Diensten und herkömmlichen On-Premise-Praxissystemen verläuft, sondern zwischen verschlüsselter und nicht verschlüsselter Datenspeicherung. Auch sogenannte Hybridsysteme - wie im vorliegenden Fall - ändern an dieser Tatsache nichts. Statt – wie gerne behauptet – das Beste aus zwei Welten miteinander zu verbinden, wird tatsächlich das Risiko nur noch vergrößert: unverschlüsselt lokal gespeicherte Patientendaten mit einem

zentralen Zugriff durch den Systemanbieter. Weiter öffnen kann man das Scheunentor wohl kaum.

Eine vergleichbare Sicherheitslücke ist bei einer Software, die alle Patientendaten bereits in der Praxis kryptografisch verschlüsselt, gar nicht erst denkbar. Dies möchten wir anhand der cloudbasierten und Ende-zu-Ende verschlüsselten Praxissoftware RED medical im Folgenden näher erläutern.

Cloud ist nicht gleich Cloud: Das Sicherheitskonzept von RED

Die Sicherheitsarchitektur von RED sieht vor, dass alle Patientendaten bereits in der Praxis verschlüsselt werden, bevor sie das Praxisnetzwerk verlassen und in einem deutschen Rechenzentrum gespeichert werden. Die dort befindlichen Patientendaten können ausschließlich von den Kunden (sprich: Heilberuflern) gelesen werden, denn nur sie sind softwareseitig mit der Möglichkeit ausgestattet, die verschlüsselten Daten wieder zu entschlüsseln (siehe Schaubild).

Dies bedeutet in der Konsequenz, dass auch RED selbst zu keiner Zeit Zugriff auf die Klartext-Daten hat. Greift ein Hacker also die Server von RED an, kann er aufgrund der eingesetzten Sicherheitstechnologie weder Logindaten für die Netze der Praxen noch Klartext-Patienteninformationen erbeuten. Dies ist ein großer Unterschied zu Praxissystemen, bei denen sich die Hersteller die Möglichkeit offen halten, in Ausnahmefällen doch auf die Daten zuzugreifen oder die Zugangsdaten zu rekonstruieren.

Ist die Option “Passwort vergessen” gegeben?

Wie lässt sich nun also herausfinden, ob ein Hersteller tatsächlich eine vollständige Ende-zu-Ende-Verschlüsselung einsetzt, um Patientendaten zu schützen? Die einfachste Methode besteht darin, so zu tun, als habe man das Passwort vergessen und ein Zurücksetzen desselben zu beauftragen. Ist dies aus Gründen der Sicherheitsarchitektur nicht möglich, handelt es sich in der Tat um eine Ende-zu-Ende verschlüsselte Anwendung. Sollte ein Zurücksetzen durch den Anbieter jedoch möglich sein, könnte der Hersteller sich auch selbst ohne Zutun der Kunden Zugang zu den Daten verschaffen. Damit liegt keine echte Ende-zu-Ende-Verschlüsselung vor. Das System und die darin gespeicherten Daten sind unsicher.

Zusätzlicher Hinweis:

Im Rahmen der vorliegenden Nachrichtenlage hatte der Sprecher des Bundesdatenschutzbeauftragten erklärt, dass aufseiten der Softwarehersteller keine gesetzliche Verpflichtung besteht, das eigene Produkt “in irgendeiner Art und Weise datenschutzkonform auszugestalten”. Diese inhaltlich zutreffende Aussage macht in unseren Augen ein großes Problem im Gesundheitswesen deutlich, denn im Umkehrschluss bedeutet dies, dass Heilberufler die alleinige Verantwortung für die Datenschutzkonformität Ihrer Praxissoftware tragen müssen. Eine Situation, die wir bei RED für fatal halten. Aus diesem Grund übernehmen wir bei RED für alle unsere cloudbasierten Systeme die (sicherheits-)technische Verantwortung.

> *“Die unverschlüsselte Speicherung von Patientendaten - egal ob in der Cloud oder in einem herkömmlichen Praxisverwaltungssystem - ist immer risikobehaftet. Warum? Weil Cyberkriminelle leichtes Spiel haben und ohne weiteres Zutun alle Daten auslesen können, sobald sie sich Zugriff auf die Anwendung verschafft haben. Deshalb setzen wir bei allen unseren RED-Produkten auf konsequente Ende-zu-Ende-Verschlüsselung. Alle sensiblen Informationen sind damit wirksam vor dem Zugriff unbefugter Dritter geschützt.”*
>
> Jochen Brüggemann, Geschäftsführer RED

Weitere Informationen zur Sicherheitsarchitektur von RED finden Sie unter https://www.redmedical.de/zertifiziert-sicher/. Interviewanfragen an Jochen Brüggemann können Sie jederzeit unter presse@redmedical.de stellen.

Die RED Medical Systems GmbH entwickelt und vertreibt mit RED medical und RED pharma die jeweils erste und einzige webbasierte und Ende-zu-Ende verschlüsselte Praxis- bzw. Verordnungssoftware, die durch die Kassenärztliche Bundesvereinigung (KBV) zertifiziert ist. Darüber hinaus ist RED mit der zertifiziert sicheren RED connect Videosprechstunde auf Basis von über 60.000 registrierten Organisationen deutschlandweiter Marktführer. Mit RED telematik bietet das Unternehmen außerdem einen zuverlässigen Anschluss an die Telematikinfrastruktur, bei dem der Konnektor nicht vor Ort, sondern in einem Rechenzentrum steht. Das Produktportfolio wird abgerundet durch den parallelen TI-Zweitanschluss RED telematik safe, der im Störungsfall innerhalb eines Arbeitstages aktiviert werden kann, um größere Umsatzausfälle oder Betriebsunterbrechungen zu vermeiden.

RED wurde im Jahr 2013 von Jochen Brüggemann und Alexander Wilms gegründet, um mit web- und cloudbasierten Systemen die tägliche Arbeit aller Heilberufler zu erleichtern. In Deutschland arbeiten für das Unternehmen derzeit rund 60 hochmotivierte Mitarbeiter:innen, deren Zahl ständig steigt.

Kontakt & weitere Informationen:
RED Medical Systems GmbH, Lutzstraße 2, 80687 München,
Jochen Brüggemann, Tel. 089 / 9545755-31, info@redmedical.de
www.redmedical.de