Sicherheitsrisiko Praxissoftware?

Bundesdatenschutzbeauftragter fordert Haftungspflicht der Hersteller

Das Nachrichtenmagazin „Focus" berichtete Ende Januar über Sicherheitsrisiken durch unzureichend geschützte Praxisverwaltungssysteme (PVS) in Arztpraxen. Der Bundesdatenschutzbeauftragte Ulrich Kelber plädiert deshalb für eine höhere Haftungspflicht der Hersteller. Doch dafür müsste wohl das Produkthaftungsgesetz geändert werden.

Die gesetzlich erzwungene Digitalisierung des Gesundheitswesens schafft auch neue Sicherheitsrisiken. So könnte ausgerechnet die Telematik-Infrastruktur (TI) zu einem „offenen Scheunentor" werden, wie es Kelber in einem Gastbeitrag für das Internetportal netzpolitik.org formulierte (siehe hierzu auch BZBplus 3/2023). Dass es keinen hundertprozentigen Schutz vor Hackerattacken gibt, unterstrich auch der Präsident des Bayerischen Landeskriminalamtes im BZB 5/2022. Patientendaten sind eine begehrte Ware. Betroffene sehen sich vielfach mit Lösegeldforderungen konfrontiert.

Neben der TI erleichtert aber offensichtlich auch so manche Praxissoftware Cyberkriminellen ihr Geschäft. Laut „Focus" weist die Arztpraxis-Software Medistar aus dem Hause CompuGroup Medical (CGM) deutliche Schwächen auf. Nach Einschätzung des IT-Experten Cedric Fischer sei Medistar sehr leicht zu hacken, da eben nicht nur in den jeweiligen Praxis-Netzwerken, sondern auch direkt bei der Software „eklatante Sicherheitsmängel" bestünden. Der Zugang zu Administratoren-Rechten laute bei Installation „admin", das Passwort „1234". Diese Daten seien „für alle Praxen einheitlich festgelegt", so Fischer. Würden sie vom Nutzer nicht geändert, so sei die Wahrscheinlichkeit, dass Unbefugte sich Zugriff auf Praxis- und Patientendaten verschaffen können, sehr hoch. „Ich konnte von meinem Rechner aus ohne Probleme Zugriff auf einen Praxisserver nehmen, auf dem Medistar lief. Damit hätte ich rund 30 000 Patientendaten einsehen können", zitiert der „Focus" den IT-Experten. Dafür seien nicht einmal besondere IT-Kenntnisse nötig gewesen. „Das hätte auch jeder andere machen können, der sich die IP-Adresse des Servers beispielsweise über die frei zugängliche Suchmaschine Shodan besorgt hätte." Der Fall liege zwar bereits einige Zeit zurück, könnte aber nach Fischers Einschätzung heute noch genauso auftreten. Auch enthielten die Datenbanken unverschlüsselte Patientendaten. Das Passwort im „Medistar"-Dokumentenmanagementsystem „Moviestar" könne „mit einem einfachen Tool sofort und in wenigen Millisekunden ausgelesen" werden.

Der Hersteller weist die Darstellung Fischers gegenüber dem „Focus" erwartungsgemäß zurück und sieht die Verantwortung beim Kunden, sprich bei den niedergelassenen Ärzten. Sie könnten und sollten die Zugangsdaten ändern. Die Umgebung, in der das Dokumentenmanagementsystem „Moviestar" betrieben werde, müsse klaren Sicherheits- und Konfigurationsvorgaben folgen. Dadurch sei der Zugang nur berechtigten Nutzern möglich. Generell müsse das Netzwerk, bevor die Praxis-Software installiert werde, unter anderem mit einer Firewall gesichert werden. Alle USB-Ports seien zu deaktivieren, der Server müsse in einem verschlossenen Raum stehen. „Aber ist das realistisch?", fragt sich wohl nicht nur der „Focus". So würden große Dateien nun einmal gerne auf USB-Sticks gespeichert. Ein eigener Serverraum könne für kleine Arztpraxen eine Herausforderung darstellen. Nicht nur Fischer, auch Michael Wiesner, ein renommierter Experte für