Samstag, 18. Januar 2025, Darmstadt / Wirtschaft

Zu leicht zu knacken

Bei der elektronischen Patientenakte steht der Datenaustausch über der Sicherheit / Von Thilo Weichert

In Frankreich gab es Datenlecks bei Kranken- und Sozialversicherungsdienstleistern, wovon 33 Millionen Menschen, betroffen waren. In den USA verursachte ein Cyberangriff auf eine Online-Gesundheitsplattform 1,6 Milliarden US-Dollar Kosten. Lösegelderpressungen betrafen in Australien 3,9 Millionen Krankenversicherte, in Finnland psychisch-Kranke, in Estland in einer Gendatenbank Gespeicherte. Die Liste mit gehackten Patientenakten ist lang.

Nun werden in Deutschland von allen gesetzlich Krankenversicherten, die nicht widersprochen haben, bei den Krankenkassen elektronische Patientenakten (ePA) angelegt und – für Zwecke der „Sekundärnutzung“ – in pseudonymisierter Form in einem Forschungsdatenzentrum gespeichert. Die Gründe hierfür sind ehrenwert: Es geht um die Verbesserung der Behandlung, das Einsparen von Kosten, die Nutzung der Daten für die Forschung und eine verbesserte Gesundheitsversorgung.

Gegen das Anlegen individueller digitaler Krankengeschichten für diese Zwecke wäre nichts einzuwenden, wenn das Patientengeheimnis, die Vertraulichkeit der Gesundheitsakten, gewahrt bliebe. Dies wird den Versicherten auch versprochen.

Die Realität orientiert sich aber nicht am politischen Wunschdenken. Bianca Kastl und Martin Tschirsich präsentierten auf dem Chaos Communication Congress Ende 2024, wie sie mit einfachen Mitteln „remote“, also von außen, als sicher gepriesene elektronische Patientenakten gehackt haben. Sie konnten in wenigen Minuten fremde Gesundheitskarten bestellen. Innerhalb weniger Stunden verschafften sie sich Zugang zu beliebig vielen ePA, wovon es in Bälde 73 Millionen geben wird. Die dafür benötigten Kartenterminals hatten sie sich über Kleinanzeigen beschafft. Es gelang ihnen auch, den digitalen Zugang zu Arztpraxen zu kompromittieren.

Pilotphase nicht starten

In Reaktion auf die Präsentation der vielfältigen Sicherheitsmängel erklärte Gesundheitsminister Karl Lauterbach (SPD): „Die ePA bringen wir erst

dann, wenn alle Hackerangriffe, auch des CCC, technisch unmöglich gemacht worden sind." Zugleich erklärte sein Ministerium, dass am Zeitplan des Rollouts der ePA, also am Start der Pilotphase am 15. Januar 2025, festgehalten werde. Die Bundesdatenschutzbeauftragte und das Bundesamt für die Sicherheit in der Informationstechnik zeigten sich indes weniger sicher bezüglich der Sicherheit. Es müssten „umgehend zusätzliche Schutzmaßnahmen entwickelt und deren Umsetzung veranlasst" werden.

Es gibt keine völlige Sicherheit vor internen und externen Angriffen bei einer digitalen Datenverarbeitung, die kann es nicht geben. Dies gilt erst Recht für ein komplexes System wie das der ePA mit tausenden Gesundheitseinrichtungen, knapp hundert Krankenkassen und mehr als hundert Softwaresystemen, die erst kurzfristig an die ePA-Spezifikationen angepasst werden konnten.

Qualität geht vor Geschwindigkeit. Vor Abschluss der zusätzlich zu installierenden Schutzmaßnahmen sollte selbst der Pilotbetrieb nicht starten. Auf jeden Fall muss den Betroffenen zur Datensicherheit reiner Wein eingeschenkt werden, damit sie eine bewusste Entscheidung treffen können, ob sie gegen die ePA Widerspruch einlegen wollen oder nicht.

Thilo Weichert (1955) ist Jurist und Politologe. Er ist Mitglied im Vorstand der Deutschen Vereinigung für Datenschutz e.V. und war bis 2015 Datenschutzbeauftragter des Landes Schleswig-Holstein.