Datensicherheit von elektronischen Gesundheitsakten

Der IT-Security Analyst des Schweizer IT-Sicherheitsunternehmens modzero, Martin Tschirsich, im Gespräch mit Sabine Schmitt vom DFZ.

© LeoWolfert/Shutterstock.com

■ Die elektronische Patientenakte kommt. Spätestens 2021 soll sie flächendeckend für jeden verfügbar sein. Die ePA soll sozusagen zum Herzstück der „vernetzten Gesundheitsversorgung“ werden und über Telematikinfrastruktur laufen.

Sabine Schmitt: Herr Tschirsich, Sie haben ja schon so ziemlich alle derzeit verfügbaren IT-Systeme geknackt. Ist die TI denn sicher vor Hackerangriffen und irgendwelchen Leaks?

Martin Tschirsich: Die auf dem Chaos Communication Congress in Leipzig betrachteten elektronischen Gesundheitsakten sind Vorläufer der kommenden elektronischen Patientenakte (ePA). Sie sind nicht Teil der Telematikinfrastruktur (TI), also nicht von der gematik spezifiziert. Dennoch sind auch diese Gesundheitsakten in Teilen bereits an die TI angebunden und sollen, so die Intension, schrittweise in die ePA übergehen. Die Entwickler der künftigen ePA werden also zum Teil die gleichen sein, die für die jetzigen Anwendungen verantwortlich zeichnen.

Nun kann man optimistischerweise erwarten, dass die in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) entstandene Spezifikation der ePA viele der zurzeit vorgefundenen konzeptionellen Sicherheitsmängel von vornherein ausschließen wird. Risiken bestehen dann noch in einer fehlerhaften Umsetzung der Spezifikation als auch in grundlegenden Schwächen der Spezifikation selber, welche sich beispielsweise aus der geforderten zentralen Datenhaltung und der Verarbeitung von unverschlüsselten Metadaten beim Cloud-Anbieter ergeben könnten.

Grundsätzlich aber ist zu erwarten, dass Daten an den Schnittstellen des Systems abfließen, also beispielsweise beim Übergang von der TI in das Patientenaktensystem eines großen Krankenhauses.

Bundesgesundheitsminister Spahn möchte gern die ePA für den Patienten auf dessen Smartphone nutzbar machen. Die Sicherheitsstandards müssten dafür ja nicht so hoch wie für den Arzt sein, für den die ePA seiner Patienten ja fremde Daten sind, für die er haftet. Und schnell müsse das gehen, weil die Patienten es so wollten. Außerdem stünden Google & Co. ja schon vor der Tür, um die Gesundheitsdaten gern zu verwalten (und zu nutzen natürlich). Also muss eine Patientenakte fürs Handy her. Warum sollte das schlecht sein?

Die Forderung nach einer Patientenakte für das Smartphone ist eng verbunden mit einer zweiten Forderung nach einem einfacheren Zugang zur ePA unter Verzicht der Gesundheitskarte (eGK). Bislang sieht die Spezifikation eine sichere Authentifizierung des Versicherten über seine eGK vor. Typischerweise wird die eGK über ein Kartenlesegerät mit PIN-Eingabepad ausgelesen. Die wenigsten Versicherten besitzen ein solches Lesegerät für ihr Smartphone, und die ausgegebenen eGKs sind bislang auch nicht NFC-fähig. Der geplante Zugang ohne eGK wird dagegen ohne Zusatz-Hardware auskommen und damit komfortabler sein, aber eben auch weniger sicher.

Ein weiteres Risiko ergibt sich aus den vielen im Umlauf befindlichen Smartphones mit veralteter Software. Soll die ePA einem großen Nutzerkreis zur Verfügung stehen, dann müssen Abstriche bei den Sicherheitsanforderungen an die mobile Plattform gemacht werden.

Viele Leute wollen ihre Daten schnell und leicht verfügbar haben. Bei Bankgeschäften dachte man früher auch: Oje, niemals kann das sicher sein übers Netz. Heute ist es für jeden unter 60 völlig normal, seine Bankgeschäfte online zu erledigen. Sind Gesundheitsdaten da noch sensibler?

Wir haben uns im Onlinebanking daran gewöhnt, dass die Banken den Kunden das Geld im Betrugsfall meist aus Kulanz erstatten. Tatsächlich aber steigen die Verluste durch Betrug im Onlinebanking regelmäßig an, wie zuletzt Statistiken aus England belegen.

Doch während ein finanzieller Schaden einfach ausgeglichen werden kann, sieht dies bei Gesundheitsdaten anders aus. Nicht umsonst sind Gesundheitsdaten nach Artikel 9 DSGVO besonders geschützt. Das liegt auch daran, dass Gesundheitsdaten sehr langlebig sind und ein Leben lang sicher verwahrt werden müssen – ein bisher ungelöstes Problem.

In Deutschland trifft das Wort „Schlusslicht“ Politiker immer direkt ins Mark. Schlusslicht in der Digitalisierung im Gesundheitswesen gehört eindeutig dazu. Können Sie sich ein System vorstellen, das Gesundheitsdaten wirklich sicher macht – ohne eine Rückkehr zum Papierarchiv im feuerfesten Stahlschrank in der Arztpraxis und ohne blinden Aktionismus auf Kosten der Datensicherheit? Geht einfach, modern und sicher? Wenn ja, wie?

In Deutschland sind wir historisch bedingt besonders für die Gefahren sensibilisiert, die sich aus der Sammlung und Verarbeitung personenbezogener Merkmale und Daten ergeben. Wenn wir jetzt sehen, wie in anderen Ländern mit Vorreiterrolle in der Digitalisierung nach und nach die Gesundheitsdaten – darunter genetische Merkmale – der Bevölkerung abfließen, dann bekommt das Wort „Schlusslicht“ auf einmal eine positive Konnotation. Denn das verschafft uns Zeit, die nachteiligen Folgen der Digitalisierung zu verstehen und abzufangen. Wir können aus den Fehlern der anderen lernen.

In jedem Fall wissen wir, dass Forderungen nach absoluter oder wirklicher Sicherheit nicht ehrlich, da nicht erfüllbar sind. Auch die gematik sieht bei der ePA Restrisiken, die trotz Zulassung und Sicherheitsmonitoring nicht ausgeschlossen werden können.

Es gibt einige weiterführende Ideen zur ePA. Herr Lauterbach von der SPD möchte gern, dass Patienten ihre Daten (freiwillig) für von Krankenkassen zertifizierten Drittanbietern ihre Daten öffentlich machen, um dann passgenaue Angebote für ihre Krankheit bekommen zu können (zusätzlich zur ärztlichen Therapie). Das ist für ihn ein Schritt zum mündigen Patienten, der eigenverantwortlich entscheiden kann und über alle Angebote aufgeklärt ist. Herr Hecken, Chef des G-BA, hat in den Ring geworfen, dass man überlegen müsse, ob man Patienten nicht verpflichten könne, ihre Daten herzugeben (zum Beispiel zu Forschungszwecken). Solidarität könne keine Einbahnstraße sein. Was halten Sie von solchen Geschäften mit Gesundheitsdaten?

Die Spezifikation der gematik sieht bereits heute vor, dass Daten aus der ePA mit Zustimmung des Versicherten unter Nutzung von expliziten Opt-in-Lösungen weitergeleitet werden können. Eine Verpflichtung zur Offenlegung von Daten aus der ePA ist insbesondere mit Blick auf die schon bestehenden Vorbehalte und Akzeptanzschwierigkeiten nicht tragbar.

Was sind Ihrer Ansicht nach die Lehren, die man aus dem Hackerangriff eines 20-Jährigen aus Mittelhessen ziehen sollte, der ja mit recht wenig krimineller Energie schon für reichlich Wirbel gesorgt hat?

Viele der abgegriffenen Daten lagen ja bei Anbietern, die zusätzliche, sichere Zugangsmöglichkeiten anbieten. Nur wurden diese oft nicht genutzt, offensichtlich auch, weil die Risiken für den Einzelnen schwer einzuschätzen sind und somit der Komfortgewinn bei weniger Sicherheit überwiegt. Auch hinsichtlich der ePA hören wir ja das Argument, dass der Versicherte eben den weniger sicheren Zugang verlangt und die Anbieter darauf reagieren müssen. Angesichts des aktuellen Vorfalls sollten wir uns also fragen, ob wir dieser Forderung in Anbetracht der für den einzelnen schwer zu erfassenden Risiken tatsächlich nachgeben sollten.

Mal anders gedacht: Was spricht eigentlich dagegen, alle Daten öffentlich zu machen? In Schweden z. B. sind alle Steuerdaten, Einkommen etc. öffentlich. Das stört niemanden. Ist es nicht möglich, Gesundheitsdaten völlig uninteressant zu machen, wenn sie von allen für alle verfügbar sind? Gibt es dazu Ideen?

Selbst in den skandinavischen Ländern wie Schweden, wo bei Steuererklärungen und Einkommen auf maximale Transparenz gesetzt wird, gilt dies explizit nicht für Gesundheitsdaten. Und das hat seinen Grund eben in den eingangs genannten fundamentalen Unterschieden zwischen Gesundheitsdaten und Finanzdaten. Eine völlige Datentransparenz hinsichtlich unserer Körperlichkeit, unserer Gesundheit bewegt sich im Bereich der Utopie. Oder der Dystopie, je nach Auslegung.

Vielen Dank für das Interview. ◂◂

Quelle: Freier Verband Deutscher Zahnärzte e.V.