Opt-out reicht nicht: Die ePA ist ein Sicherheitsrisiko für alle

Die Präsentation von Bianca Kastl und Martin Tschirsich auf dem Kongress des Chaos Computer Clubs offenbarte erhebliche Sicherheits- und Vertrauensprobleme bei der Einführung der elektronischen Patientenakte (ePA). Während das Ziel einer flächendeckenden Digitalisierung des Gesundheitswesens grundsätzlich begrüßenswert ist, zeigt die Analyse, dass die Umsetzung in ihrer aktuellen Form zahlreiche Schwächen und Risiken birgt.

Hier ein Überblick über die zentralen Punkte:

Die ePA 3.0 soll künftig (ab 15.2.2025) für alle gesetzlich Versicherten automatisch eingerichtet werden, es sei denn, man widerspricht aktiv (Opt-out-Verfahren). Ziel ist es, medizinische Daten wie E-Rezepte, Arztbriefe und Befunde zentral verfügbar zu machen und den Zugang zu Gesundheitsinformationen für Patient:innen sowie Leistungserbringer zu erleichtern.

Sicherheitsmängel und Schwachstellen

1. Komplexität und mangelnde Kontrolle

Das System ist enorm komplex, mit hunderten Beteiligten, darunter Krankenkassen, Leistungserbringer und technologische Dienstleister. Diese Vielzahl an Akteuren erschwert eine klare Sicherheitsüberwachung. Selbst spezialisierte Gutachter wie Fraunhofer SIT kommen laut den Vortragenden an Grenzen, wenn es um die vollständige Erfassung und Bewertung der Infrastruktur geht.

2. Historische Sicherheitsprobleme

Schon bei der Einführung der ersten ePA-Versionen wurden Sicherheitslücken aufgezeigt, darunter einfache Angriffe auf Praxis- und Patientenidentitäten. Die Vortragenden schilderten, wie mit minimalem Aufwand und grundlegenden Kenntnissen Zugänge zu Patientenakten erschlichen werden konnten. Bemerkenswert ist, dass einige dieser Schwächen seit über einem Jahrzehnt

bekannt sind und dennoch nicht vollständig behoben wurden.

3. Zentrale Schwachstellen in der aktuellen ePA

- Versichertenstammdaten: Die für den Zugriff genutzten Identifikationsnummern sind weder hinreichend geschützt noch kryptografisch abgesichert, was Angriffe erleichtert.
- Opt-out-System: Die Zwangseinführung bei allen gesetzlich Versicherten schafft ein potenziell hohes Schadensausmaß. Die Wahrscheinlichkeit eines massenhaften Datenabflusses wächst mit der Anzahl der betroffenen Personen.
- Kartenbasierte Authentifizierung: Gesundheitskarten mit minimalen Sicherheitsanforderungen ermöglichen unbeabsichtigten oder missbräuchlichen Zugriff. Die Notwendigkeit zusätzlicher Sicherheitsmechanismen wie PINs wurde vielfach umgangen.

Gesellschaftliche und politische Implikationen

1. Vertrauen in die Digitalisierung

Die wiederholte Darstellung von Sicherheitsproblemen führt zu einem massiven Vertrauensverlust in die Digitalisierung des Gesundheitswesens. Insbesondere vulnerable Gruppen, die besonders von der ePA profitieren könnten (z. B. Menschen mit chronischen oder sensiblen Diagnosen), könnten sich gezwungen sehen, die Nutzung zu verweigern.

2. Fehlende Transparenz

Die Vortragenden kritisierten, dass die Kommunikation der Risiken intransparent und verharmlosend erfolgt. Aussagen wie „Die ePA ist die sicherste in Europa“ werden als irreführend empfunden, da offensichtliche Schwächen unberücksichtigt bleiben. Eine ehrliche Risikokommunikation würde es den Bürger:innen ermöglichen, informierte Entscheidungen zu treffen.

Fazit

„Ich muss gestehen, dass ich als chronisch Kranker bis letzte Woche die ePA als eine für mich mehr als sinnvolle Sache gehalten habe. Natürlich war mir klar, dass wohl alle Leistungserbringer Zugriff auf meine Daten haben. Doch die Vorteile überwogen für mich. „Daher war es selbstverständlich, dass ich hier nicht widersprechen werde“ berichtet Karl-Eugen Siegel, doch nach den Meldungen und heute nach dem Mitschnitt des Vortrages von Bianca Kastl und Martin Tschirsich war es klar: „Ich werde diesem stümperhaften System des ePA widersprechen!“ resümiert Siegel und gibt zu bedenken: „Die Sicherheitslücken, organisatorische Schwächen und eine unzureichende Kommunikation gefährden nicht nur den Erfolg des Projekts, sondern vor allem das Vertrauen in die Digitalisierung des Gesundheitswesens insgesamt. Ohne grundlegende Änderungen an Prozessen und Strukturen bleibt die ePA eine ambitionierte, aber mangelhafte Vision. Ein transparentes und sicherheitsorientiertes Vorgehen ist dringend notwendig, um die digitale Zukunft des Gesundheitswesens nachhaltig zu gestalten.“

Weitere Informationen unter:

Video mit Bianca Kastl und Martin Tschirsich

CCC fordert Ende der ePA-Experimente am lebenden Bürger

Dr. Stefan Streit: Elektronische Patientenakte (ePA) Made in Germany