CCC fordert Ende der ePA-Experimente am lebenden Bürger

2024-12-27 16:05:22

Sicherheitsmängel begleiten die elektronische Patientenakte (ePA) seit ihrer Einführung im Jahr 2020. Mit der Umstellung von Opt-In auf Opt-Out kommt nun die Patientenakte „für alle": Gesundheitsdaten von über 70 Millionen Versicherten werden ohne deren Zutun über Praxis- und Krankenhausgrenzen hinweg in einer zentralen Datenbank zusammengeführt. Doch auch die „ePA für alle" kann ihre Sicherheitsversprechen nicht halten. Beim 38C3 wird demonstriert, wie unberechtigte Personen mit wenig Aufwand massenhaften Zugang zur ePA für alle erlangen können.

Der Chaos Computer Club (CCC) begleitet die Lösungen aus dem Hause Gematik seit Jahren mit einer morbiden Faszination. Von geplanter Obsoleszenz bei den Konnektoren [1] über das Ident-Verfahren [2] bis zu dem von Anfang an bescheinigten bedenklichen Kosten-Nutzen-Verhältnis [3] waren die Projekte um die ePA von Turbulenzen begleitet.

Eine erneute Analyse des aktuellen Stands [4] ergab nun wieder Bedenkliches:

Sicherheitsforscher zeigen unter anderem, wie sie sich mit wenig Aufwand und zum wiederholten Male gültige Heilberufs- und Praxisausweise sowie Gesundheitskarten Dritter beschaffen und damit auf Gesundheitsdaten zugreifen konnten. Ursächlich sind erneut Mängel in den Ausgabeprozessen, den Beantragungsportalen sowie im real existierenden Umgang mit den Karten im Feld. Diese wurden bereits auf dem 36C3 [5] demonstriert.

Zudem demonstrieren die Forscher, wie Mängel in der Spezifikation es ermöglichen, Zugriffstoken für Akten beliebiger Versicherter zu erstellen. Dies ist möglich, ohne dass die Gesundheitskarten präsentiert oder eingelesen werden müssen. Damit hätten Kriminelle auf einen Schlag Zugriff auf mehr als 70 Millionen Akten.

Wie schon bei der letzten Visite gelang der Fernzugriff auf Patientenakten über unsicher konfigurierte IT, sowohl in den Gesundheitseinrichtungen als auch über Dienstleister-Zugänge. Trotzdem soll nun im Rahmen der Initiative „ePA für alle" das Experiment auf fast alle Versicherten ausgedehnt werden.

Während die Sicherheitsforscher des CCC in der ePA wühlten, wurde am Fraunhofer-Institut das Sicherheitskonzept von einer KI gelesen und mit geringen Mängeln für „sicher" befunden. [6] Ein Vorgehen, das nur Stirnrunzeln hervorrufen kann. Die freudige Feststellung der Gematik: „Gutachten bestätigt:

ePA für alle ist sicher" [7] kann nun getrost endgültig als halluzinierte Fehldiagnose betrachtet werden.

Nur wenn die Sicherheit der „ePA für alle" ausreichend gewährleistet ist, werden Leistungserbringer und Versicherte die ePA akzeptieren und auch nutzen. Das dazu notwendige Vertrauen lässt sich eben nicht verordnen.

Es gilt weiterhin, eine ePA tatsächlich für alle zu bauen, die den individuellen Sicherheitsbedarf berücksichtigt. Die gemeinsamen Forderungen der Sicherheitsforscher und des CCC lauten:

- Unabhängige und belastbare Bewertung von Sicherheitsrisiken,
- transparente Kommunikation von Risiken gegenüber Betroffenen und
- ein offener Entwicklungsprozess über den gesamten Lebenszyklus.

Vertrauenswürdige digitale Infrastrukturen können nur entstehen, wenn der Entstehungsprozess selbst Vertrauen ermöglicht.

Links und weiterführende Informationen

- [1] https://www.ccc.de/updates/2022/konnektoren-400-millionen-geschenk
- [2] https://www.ccc.de/de/updates/2022/chaos-computer-club-hackt-video-ident
- [3] https://www.ccc.de/en/elektronische-gesundheitskarte
- [4] https://fahrplan.events.ccc.de/congress/2024/fahrplan/talk/SRXRMA/
- [5] https://media.ccc.de/v/36c3-10595-hacker_hin_oder_her_die_elektronische_patientenakte_kommt
- [6] https://www.sit.fraunhofer.de/de/presse/details/news-article/show/neues-epa-sicherheitskonzept-auf-dem-pruefstand/
- [7] https://www.gematik.de/newsroom/news-detail/gutachten-bestaetigt-epa-fuer-alle-ist-sicher

Über den Chaos Computer Club

Der Chaos Computer Club e. V. (CCC) ist die größte europäische Hackervereinigung und seit über vierzig Jahren Vermittler im Spannungsfeld technischer und sozialer Entwicklungen. Die Aktivitäten des Clubs reichen von technischer Forschung und Erkundung am Rande des Technologieuniversums über Kampagnen, Veranstaltungen, Politikberatung, Pressemitteilungen und Publikationen bis zum Betrieb von Anonymisierungsdiensten und Kommunikationsmitteln. Der Club besteht aus einer Reihe dezentraler lokaler Vereine und Gruppen. Diese organisieren regelmäßige Veranstaltungen und Treffen in vielen Städten des deutschsprachigen Raums.