Chaos-Computer-Club

Sicherheitsstandard der ePA „ein Trauerspiel“

Wer gehofft hat, die Gematik arbeitet mit Hochdruck an den vom Chaos-Computer-Club (CCC) entdeckten Sicherheitslücken der ePA, wird nach Kenntnis des IT-Fachmanns Martin Tschirsich enttäuscht. „Keine unserer Forderung wurde bislang nach meiner Kenntnis überhaupt reflektiert“, sagte er am Samstag.

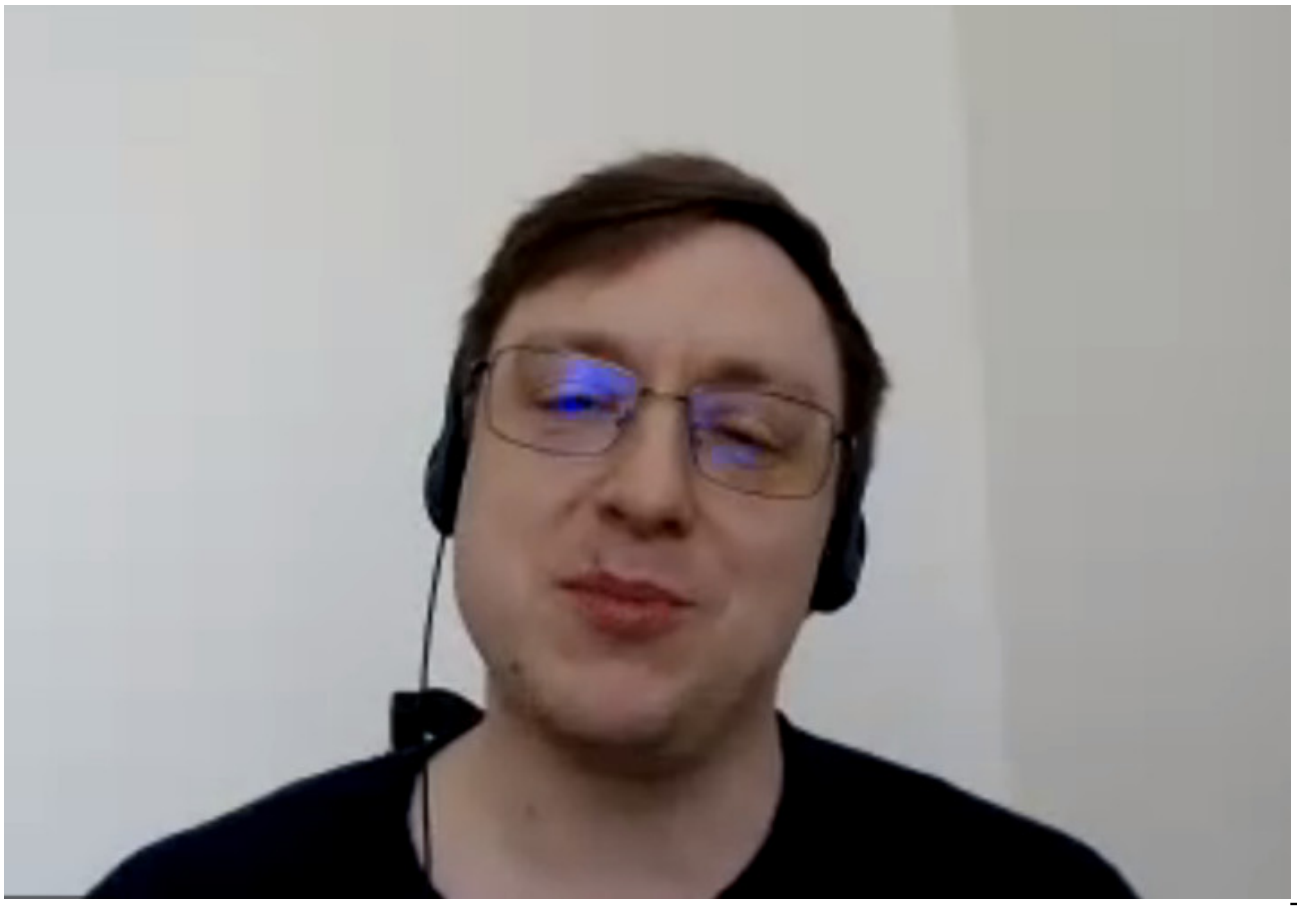
©Pakin/stock.adobe.com Hacker, die sich Zugriff auf ePAs verschaffen wollen, haben aus Sicht von Martin Tschirsich vom CCC leichtes Spiel.

Der Ärzteverbund MEDI GENO hatte für diesen Samstag zu einer Informationsveranstaltung über die elektronische Patientenakte (ePA) eingeladen. Einer der Referenten: IT-Fachmann Martin Tschirsisch, der im Dezember gemeinsam mit der IT-Fachfrau Bianca Kastl öffentlich über von ihnen gefundene Sicherheitslücken in der und um die Akte aufdeckte.

Was ist seither passiert? „Keine unserer Forderung wurde bislang nach meiner Kenntnis überhaupt reflektiert“, so Tschirsich. Der CCC hatte der Gematik bereits im August 2024 seine Erkenntnisse sowie Forderungen mitgeteilt. Eine war, eine unabhängige und belastbare Bewertung der Sicherheitsrisiken zu erstellen. Denn es bestehe noch ein großes Dunkelfeld, schließlich hätten Kastl und er nicht in alle Bereiche der ePA hineingeschaut. „Es kann ja nicht sein, dass zwei Leute in ihrer Freizeit Sicherheitsmängel finden, die dazu führen, dass der Rollout um drei Monate verschoben werden musste.“

„Bewusst eingegangenes Risiko“

Doch die Gematik scheint das anders zu sehen: Dem IT-Fachmann zufolge sagte sie praktisch, „wir akzeptieren das Risiko“. Tschirsich hält das für fahrlässig, für „ein bewusst eingegangenes Risiko“. Diese Vorgehensweise könne er nicht verstehen. Außerdem ist die Gematik seiner Meinung gar nicht zu dieser Aussage autorisiert. Schließlich gehe nicht sie, sondern die Versicherten die Risiken ein – und eigentlich sei es an ihnen, die Risiken zu akzeptieren. Tatsächlich gebe es eine Bewertung der Sicherheit vom Fraunhofer Institut, die Tschirsich allerdings nicht für belastbar hält, weil sie einerseits direkt von der Gematik in Auftrag gegeben worden sei und andererseits eine „stark eingeschränkte Zielsetzung“ gehabt habe.



©änd-Screenshot Martin Tschirsich referierte über die Sicherheitslücken der ePA.

Eine weitere Forderung sei nicht erfüllt worden, und zwar die nach mehr Transparenz durch die Gematik: „Die schotten sich weiter ab.“ Krankenkassen hätten sogar beim CCC nachgefragt, ob neue Vorgaben der Gematik die Sicherheitsmängel beheben würden. Die Kommunikation sei sehr vage geblieben.

Tatsächlich hatte die Bundestagsfraktion der Linken im Februar die Bundesregierung nach der Sicherheit der ePA und geplanten Maßnahmen infolge der CCC-Erkenntnisse gefragt. In der Antwort der Bundesregierung heißt es, dass einige Schwachstellen der Gematik bereits bekannt gewesen seien, die Ausnutzung allerdings als „unwahrscheinlich“ eingestuft wurde. Die konkreten Maßnahmen jedoch hält Tschirsich für unzureichend. „Ich kann nur hoffen, dass das nicht alles ist.“

Gerade vor dem Hintergrund der Ankündigung der Abteilungsleiterin für Digitalisierung im Bundesgesundheitsministerium, Dr. Susanne Ozegowski, die ePA werde die sicherste in Deutschland sein, ist die ePA-Sicherheitsinfrastruktur aus Sicht von Tschirsich nicht gut genug. „Das ist ein Trauerspiel, ein Trümmefeld.“ Er könne sich nicht vorstellen, dass das BDI sein Einverständnis für das Rollout gebe. MEDI-GENO-Vorsitzender Dr. Norbert Smetak zeigte sich ob dieses Berichtes ernüchtert. „Es hinterlässt uns frustriert, dass nichts passiert.“

Der Chaos-Computer-Club hatte im Dezember beispielsweise gezeigt, dass die Vielzahl der Beteiligten im System, von Krankenkassen und Gesundheitsinstitutionen bis hin zu technischen Dienstleistern, kritisch zu sehen sei, weil sie alle Zugriffsmöglichkeiten auf unterschiedliche Ebenen der ePA hätten. Wenn einzelne Fehler machten, schlage sich das im gesamten Konstrukt nieder. Außerdem sei schon fraglich, dass die Kartenherausgeberportale, die SMBC-Karten herausgeben, selbst keinen strengen Sicherheitsrichtlinien unterliegen würden. Es sei zudem zu einfach, mit wenigen Daten an eine Gesundheitskarte einer anderen Person zu gelangen.
