2020/02 Inland

https://jungle.world/artikel/2020/02/datenklau-fuer-laien

Hacker zeigen, wie schlecht die Daten der elektronischen Gesundheitsakte geschützt sind

Datenklau für Laien

Von **Enno Park**

Ab dem kommenden Jahr sollen Gesundheitsdaten in einer elektronischen Patientenakte zusammengeführt werden können. Hacker des Chaos Computer Club zeigten kürzlich, wie leicht die Daten sich stehlen lassen – ganz ohne IT-Kenntnisse.

Eigentlich wollten die IT-Sicherheitsexperten Martin Tschirsich und André Zilch sowie Christian Brodowski, Arzt und Mitglied im Chaos Computer Club (CCC), die elektronische Patientenakte und die Telematikinfrastruktur des Gesundheitssystems hacken, um Sicherheitslücken aufzudecken. Tatsächlich fanden sie Sicherheitslücken, die Angreiferinnen und Angreifern vollen Zugriff auf die Gesundheitsdaten von Patientinnen und Patienten ermöglichen. Doch Hacken war dafür gar nicht nötig, wie Tschirsich, Zilch und Brodowski am vorvergangenen Freitag auf dem jährlich stattfindenden Chaos Communication Congress des CCC darlegten.

> Wenn Krankheitsdaten in falsche Hände gelangen und missbraucht werden, ist das ein Schaden, der nicht rückgängig gemacht und kaum finanziell kompensiert werden kann.

Die elektronische Patientenakte soll zum 1. Januar 2021 eingeführt werden. An sich handelt es sich um eine sinnvolle Idee. Sämtliche Krankheitsdaten wie Allergien, Blutwerte, Impfungen, Medikamente, Röntgenbilder, Vorbehandlungen und Arztberichte sollen auf Servern der halbstaatlichen Gematik GmbH – zu den Gesellschaftern des Unternehmens gehört unter anderem das Bundesgesundheitsministerium – verschlüsselt gespeichert werden. Ärztinnen und Apotheker sowie andere Heilberuflerinnen sollen diese Daten abrufen können, allerdings nur wenn der betroffene Patient dies im Einzelfall erlaubt. Der Patient soll auch darüber entscheiden, ob überhaupt eine elektronische Patientenakte angelegt wird. Indem die Krankheitsdaten digital verfügbar gemacht werden, soll vermieden werden, dass unnötige Mehrfachuntersuchungen stattfinden, Patientinnen von verschiedenen Ärzten miteinander unverträgliche Medikamente erhalten oder Krankheiten nicht erkannt werden, weil den Behandelnden nicht die gesamte Krankengeschichte vorliegt.

Um die Sicherheit des Systems zu gewährleisten, wurde eine komplexe IT-Infrastrukur mit aufwendiger Verschlüsselung geschaffen, die auf der Website der Gematik GmbH eingesehen werden kann. Das Sicherheitskonzept sieht vor, dass Arztpraxen einen sogenannten Connector

besitzen, eine Art Internet-Router, mit dem sie sich mit der geschützten Telematikinfrastruktur verbinden können. Heilberufler, die Daten abrufen wollen, müssen sich darüber hinaus mit einem Arzt- oder Heilberufeausweis in Form einer Chipkarte identifizieren. Entschlüsselt werden können die Daten außerdem nur, wenn die Patienten den Datenzugriff mit einer Chipkarte freigeben. Das klingt recht sicher, aber auch wie eine Einladung an Hackerinnen und Hacker, sich auf die Suche nach Sicherheitslücken zu machen.

Allerdings lässt sich das System auch ohne Hackingkenntnisse sehr einfach überlisten. Den Connector, der eigentlich nur an autorisierte Arztpraxen ausgegeben werden soll, konnten Tschirsich, Zilch und Brodowski im Internet bestellen. Geringfügig schwieriger war es, an einen Praxisausweis zu gelangen. Dieser muss online unter Angabe von Betriebsstättennummer, Geburtsdatum, Arztnummer, Nachname und Profession bestellt werden. Abgesehen vom Geburtsdatum finden sich diese Daten üblicherweise auf jedem Rezept oder Überweisungsschein. Der Angreifer muss also nur noch herausfinden, wann der betreffende Arzt geboren wurde. Praktischerweise kann auch eine von der Arztpraxis abweichende Lieferanschrift angegeben werden.

Bleibt noch die elektronische Gesundheitskarte des Patienten, dessen Daten gestohlen werden sollen. Diese kann unter der Behauptung, der Patient sei umgezogen, ohne weiteres auf fremden Namen bei den Krankenkassen bestellt werden. Früher ging das mit einem einfachen Telefonanruf, mittlerweile geht es per E-Mail, Fax oder Brief. Zilch führt dies seit Jahren vor, das ZDF berichtete bereits 2015 darüber – bislang ohne Folgen.

Die Präsentation der Ergebnisse von Tschirsich, Zilch und Brodowski auf dem CCC-Kongress in Leipzig hatte Konsequenzen: Eines der Identifikationsverfahren für Ärzte, das besonders unsicher war, wurde abgeschaltet, und die Ausgabe neuer Praxisausweise wurde bis auf weiteres eingestellt. Streng genommen müssten alle bisher ausgegebenen Praxisausweise eingezogen werden, da niemand nachträglich feststellen kann, wie viele von ihnen womöglich erschlichen wurden. Ob es bis zur geplanten Einführung der Patientenakte im kommenden Jahr gelingen könnte, sämtliche Heilberufler in Deutschland neu zu identifizieren und mit gültigen Ausweisen zu versorgen, ist fraglich. Allerdings ist unklar, ob das überhaupt versucht werden soll. Gegenwärtig sind 115 000 Arztpraxen an die Telematikinfrastruktur angeschlossen. Bis Jahresende sollen die übrigen Praxen hinzukommen.

Dass elektronische Gesundheitskarten unbürokratisch verschickt werden, barg keine besonders großen Risiken solange die Versichertenkarten lediglich für Abrechnungszwecke dienten. Die durch einen etwaigen Abrechnungsbetrug verursachten Schäden ließen sich noch einigermaßen verschmerzen. Der Betrug wurde juristisch verfolgt, von einer Versicherung ausgeglichen oder schlicht finanziell einkalkuliert. Das Datenschutzproblem der elektronischen Patientenakte ist anders gelagert. Wenn Krankheitsdaten in falsche Hände gelangen und missbraucht werden, ist das ein Schaden, der nicht rückgängig gemacht und kaum finanziell kompensiert werden kann. Deshalb sollten für die elektronische Patientenakte wesentlich strengere Regeln gelten als für die elektronische Gesundheitskarte. Die Gematik GmbH weist immer wieder darauf hin, wie wichtig eine zweifelsfreie Identifikation von Patienten und Heilberuflern ist. Dennoch wurden die Schwachstellen des Systems bisher nicht behoben – nicht klar ist, wer für die Sicherheit des Systems verantwortlich ist: die Gematik GmbH, IT-Anbieter oder das Bundesgesundheitsministerium und die gesetzlichen Krankenkassen, die ebenfalls Gesellschafter der Gematik GmbH sind.

Zynische Menschen könnten sich fragen, wozu der ganze Sicherheitsaufwand bei der elektronischen Patientenakte überhaupt betrieben werden sollte. Schließlich sieht das bereits in Kraft getretene »Digitale-Versorgung-Gesetz« ohnehin die Einrichtung einer zentralen Gesundheitsdatenbank vor. Diese soll sämtliche Krankheitsdaten enthalten, die die gesetzlichen Krankenversicherungen über ihre Versicherten haben (**Jungle World 46/2019**). Diese Datenbank hat nichts mit der elektronischen Patientenakte zu tun. Sie enthält zwar weniger Details, legt aber die Krankengeschichten offen für Versicherungen, Forschungseinrichtungen, staatliche Stellen und private Anbieter etwa von Gesundheits-Apps – und diejenigen, die es schaffen, sich anderweitig Zugriff darauf zu verschaffen.