c't magazin für computer technik

c't deckt auf: Sicherheitslücke in elektronischer Patientenakte

| 31.12.2021 06:00 Uhr Hartmut Gieselmann, Detlef Borchers, Hajo Schulz

2022 bekommt jeder Kassenpatient eine elektronische Patientenakte. Darin gespeicherte Dateien könnten Viren enthalten und Arztpraxen und Kliniken infizieren.

Dateisysteme, die etwas mit Gesundheitsdaten zu tun haben, sind besonders gut gesichert, sollte man meinen. Ausgerechnet die elektronische Patientenakte (ePA) ist es nicht. In ihr speichern Ärzte Befunde für gewöhnlich als Dokumente und Bilder ab. Um zumindest einen formalen Schutz gegen Viren und Trojaner zu gewährleisten, dürfen nur bestimmte Dateitypen in die ePA geladen werden.

[1]

Erlaubt sind nach der Spezifikation der Gematik (**PDF [2]**) die Dateitypen PDF, JPEG, PNG, TIFF, text/plain und text/rtf, XML, HL7-V3, PKCS7-mime und FHIR+XML. Zip-Container sind verboten, da sie nicht nur beliebige Dateien mit Schadcode, sondern auch sogenannte Dekompressionsbomben enthalten könnten. Die schreiben beim Auspacken die gesamte Festplatte voll und legen den Rechner lahm.

Derzeit existieren in Deutschland drei Server-Backends der ePA, die von Bitmarck/Rise, IBM und ITSG betrieben werden. Ärzte können dort Befunde über ihre Praxisverwaltungssoftware einstellen und herunterladen. Patienten haben Zugriff über Apps ihrer Krankenkassen und können darüber ebenfalls Dateien hoch- und herunterladen – sowie **mit Start der neuen ePA 2.0 [3]** auch Zugriffe von Ärzten erlauben oder blockieren.

TK-App erkennt Zip-Dateien nicht zuverlässig

Zu den populärsten ePA-Apps gehört derzeit "Die TK-App" für Android- und iOS-Smartphones von der Techniker Krankenkasse. Ende November bekamen wir einen anonymen Tipp, dass die Android-Version 3.15.0 (Produktversion 3.1.0.13) der TK-App es über ihre Funktion TK-Safe erlauben würde, eigentlich verbotene Zip-Container in die ePA zu laden. Bei der anschließenden Prüfung gelang es uns tatsächlich, eine Zip-Datei in die ePA hoch- und wieder herunterzuladen.

Eigentlich sollte die App einen solchen Upload durch eine Typ-Prüfung der Datei verhindern. Dazu kontrolliert sie aber offenbar nur dessen MIME-Typ in den Metadaten. Um dies zu umgehen, konstruierten wir einen Zip-Container "Röntgenbilder.zip", fügten die zusätzliche Endung ".txt" an und luden sie auf Google Drive hoch. Dieses stufte die Datei anhand der Dateinamensendung als MIME-Typ "text/plain" ein. Anschließend entfernten wir die .txt-Endung wieder aus dem Namen und konnten "Röntgenbilder.zip" vom Google Drive über TK-Safe als "Dokument ohne besondere Form" in die ePA hochladen.

Lücke in Version 4.1 geschlossen

Wir informierten Anfang Dezember Gematik und die Techniker Krankenkasse, die die Lücke bestätigte. Demnach übernahm die TK-App den vom Google Drive beim ersten Hochladen identifizierten MIME-Typ "text/plain", den Google Drive bei der Namensänderung beibehielt. Am 15. Dezember teilte uns die Techniker Krankenkasse mit, dass die Lücke in der TK-App Version 4.1 (Produktversion 4.0.0.1) geschlossen sei.

- **Zum Stand der Digitalisierung im Gesundheitswesen [4]**

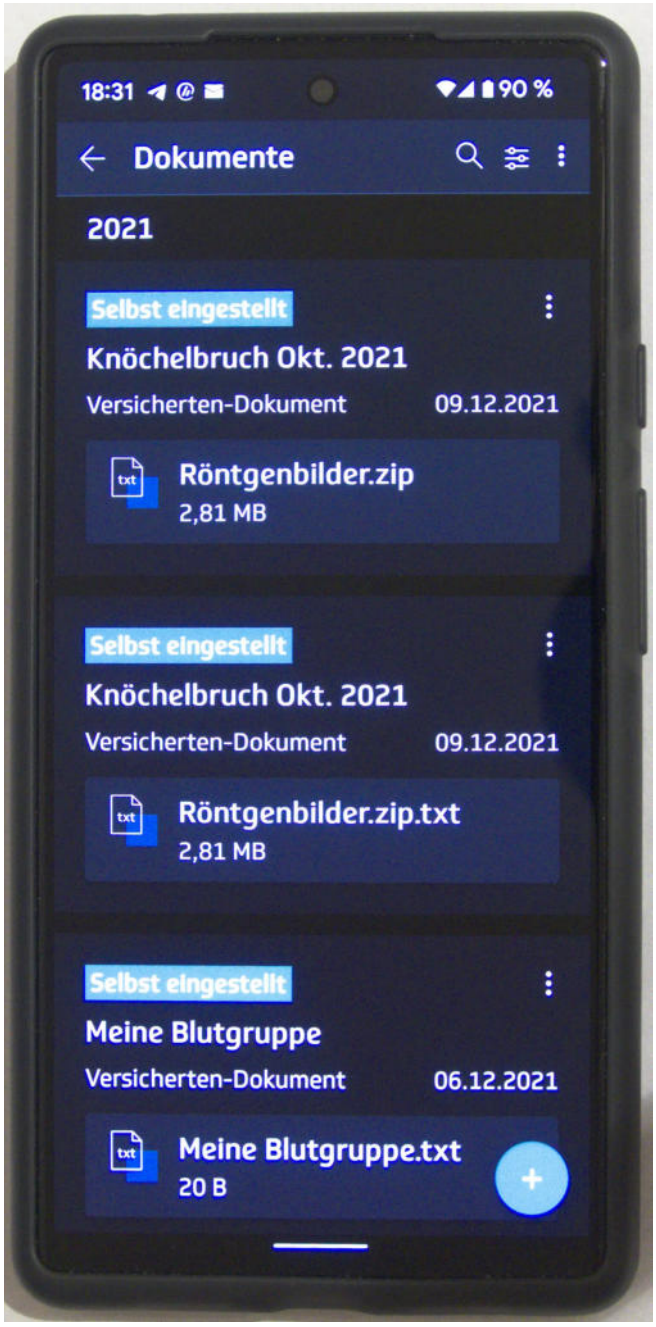
Prüfung erst beim Download

Hersteller einer ePA-App müssen diese von der Gematik zertifizieren lassen. Allerdings gilt das nicht für "Aktualisierungen mit unwesentlichen Änderungen". Demnach hatte die Gematik lediglich die Produktversion 3.1.0 der TK-App zertifiziert und die von uns beschriebene Lücke darin nicht gefunden.

Die Techniker Krankenkasse erklärte jedoch, dass die Sicherheit der Praxen durch einen möglichen Upload von Zip-Dateien in die ePA nicht gefährdet gewesen sei. Weil alle Dateien in der ePA Ende-zu-Ende-verschlüsselt übertragen werden, müssen sie im Frontend geprüft werden. Und da die TK-App nur eine Möglichkeit von vielen sei, die ePA zu befüllen, müssten Ärzte die ePA-Dateien unbedingt beim Download auf möglichen Schadcode prüfen.

Eine entsprechende Vorschrift findet man im Implementierungsleitfaden der ePA (**gemILF_PS_ePA_V2.0.0.pdf, PDF [5]**) von der Gematik. Dort heißt es unter dem neu aufgenommenen Punkt A_17769: "Das PS soll Maßnahmen zur Absicherung gegen mögliche Schadsoftware in heruntergeladenen Dokumenten ergreifen, falls das Format oder der Inhalt des heruntergeladenen Dokumentes nicht mit dem angegebenen Dokumententyp in den Metadaten übereinstimmen." PS steht dabei für Primärsystem und bedeutet Praxisverwaltungs- oder Krankenhausinformationssysteme.

Laut Auskunft der Techniker Krankenkasse soll es eine "Plausibilitätsprüfung durchführen und geeignete Maßnahmen ergreifen". Anwendungen wie die TK-App, mit denen die Versicherten eigenständig Dateien in die ePA hoch- und herunterladen können, zählen allerdings nicht zu den Primärsystemen.



Aufgrund einer Sicherheitslücke in der Android-App „Die TK-App“ gelang es uns, eine verbotene Zip-Datei in die ePA hochzuladen.

"Grenze der Sicherheitsleistung"

Laut Gematik existiere bei der ePA kein erhöhtes Sicherheitsrisiko. Sie spricht lieber von einer "Grenze der Sicherheitsleistung" und schreibt dazu: "Die Kontrolle über diese Dateien liegt beim Versicherten

selbst, das heißt, dass auch nur der Versicherte selbst dies aushebeln und die Ärztin/den Arzt seines Vertrauens bewusst mit einer Datei schädigen kann. Dieses eher unrealistische Szenario betrifft nicht nur die Nutzung der ePA, sondern besteht bereits jetzt, beispielsweise bei der Übermittlung von Befunden (wie z. B. Röntgenbildern) auf einem Datenträger, die der Versicherte mit in die Praxis bringt."

Offensichtlich hat sich bis zur Gematik noch nicht herumgesprochen, dass Trojaner durchaus Dateien infizieren können, ohne deren Besitzern (Ärzte oder Patienten) dies mitzuteilen.

Damit stellt sich die Frage, wer die Verantwortung trägt, falls es doch ein Schadcode in die ePA schafft und sich an der "Plausibilitätsprüfung" sowie den "geeigneten Maßnahmen" vorbeimogelt. Weil bei der ePA stets nachgewiesen werden könne, wer eine Datei ins System einstellt, sei das System sicherer als etwa eine Übermittlung per E-Mail, argumentiert die Gematik. Deshalb gebe es auch keine Folgeabschätzungen, welcher Schaden durch Einspielen von Schadcode in die ePA entstehen könnte. Laut Gematik seien Ärzte nach § 75b SGB V verpflichtet, "Standardsicherheitsmaßnahmen gegen Malware" einzuhalten.

Ärzte und andere Leistungserbringer sollten daher aktualisierte Virenscanner und frisch gepatchte PDF-Reader auf ihren Systemen haben. Darüber hinaus ist es eine gute Idee, ePA-Daten sowie Mail-Anhänge in einer virtuellen Maschine zu öffnen, die eine Ausbreitung von möglichem Schadcode zumindest deutlich erschwert.

MEHR INFOS

Viele c't-Investigativ-Recherchen sind nur möglich dank anonymer Informationen von Hinweisgebern.

Wenn Sie Kenntnis von einem Missstand haben, von dem die Öffentlichkeit erfahren sollte, können Sie uns Hinweise und Material zukommen lassen. Nutzen Sie dafür bitte unseren anonymen und sicheren Briefkasten.

https://heise.de/investigativ [6]

Haftungsfragen

Aus Angst vor möglichen Haftungsfolgen wollen manche Ärzte die ePA aber gar nicht erst unterstützen. So schrieb uns ein Arzt: "Ein erster Schritt wäre, den Patienten per Unterschrift zur Kenntnis nehmen zu

lassen, dass man seine ePA nicht entgegennimmt, weil dem Arzt die juristischen und technischen Risiken zu hoch sind und der Patient insofern den Arzt von Haftungsfolgen durch Nichtkenntnisnahme seiner ePA befreit."

So einfach können es sich die Ärzte aber nicht machen. **Denn während die Nutzung einer ePA für Versicherte freiwillig ist (Opt-out) [7]**, hat der Arzt nach § 291a SGB V eine Mitwirkungspflicht, wenn jemand eine ePA mit Arztdaten befüllt hat oder befüllen will. Der behandelnde Arzt muss zudem nachweisen, dass er die Daten vollständig gesichtet hat. Andernfalls könnte man ihm einen Befunderhebungsfehler vorwerfen. Im Unterschied zum Vorwurf eines Diagnosefehlers kann es dabei zu einer Beweislastumkehr kommen: Der Arzt muss nachweisen, dass er tatsächlich alle Befunde einbezogen hat.

Rechtsanwalt Dirk Wachendorf bezeichnete die ePA deshalb auf dem jüngsten Kongress der Freien Ärzteschaft als "haftungstechnisch durch und durch vergiftetes Angebot". Den versammelten Ärzten empfahl er neben der Berufshaftpflicht-Police deshalb den Abschluss einer "Cyberrisk-Versicherung".

Eine solche Police stünde wahrscheinlich auch den Kassenversicherten gut zu Gesicht, um sich gegen mögliche Schadenersatzforderungen abzusichern, sollte doch einmal eine ihrer ePA-Dateien eine Praxis mit Schadcode lahmlegen. Wer die damit verbundenen Zusatzkosten nicht akzeptieren will, hat dann noch immer die Möglichkeit zum Opt-out bei der ePA.

Kein Backup, kein Mitleid

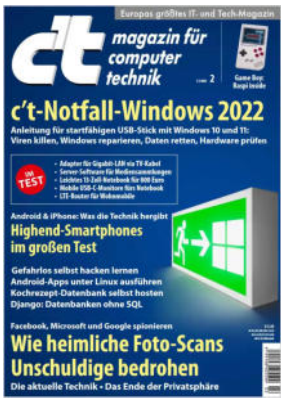
Wer die ePA hingegen künftig nutzen möchte, sollte stets auch ein Backup parat haben, falls die Server der ePA ausfallen. So geschehen etwa am 13. Dezember, als aufgrund der log4j-Lücke die gesamte Telematische Infrastruktur (TI) ausfiel, oder auch am 16. Dezember, als IBM sein Backend auf die ePA 2.0 umstellte und ein Drittel aller ePAs nicht erreichbar waren.

Weil auch andere Dienste der TI derzeit nicht gerade den Ansprüchen hochverfügbarer Systeme entsprechen, rebellierte Mitte Dezember die Kassenärztliche Bundesvereinigung (KBV) gegen die verpflichtende Einführung des E-Rezepts. Da es trotz des für Januar 2022 geplanten Starts in seinen Hintergrundprozessen noch nicht fehlerfrei arbeitet und auch nicht flächendeckend verfügbar ist, wollten die Ärztevertretungen die strengen Bestimmungen der Digitalisierung in fakultative Bestimmungen umwandeln. So hieß es etwa in der Mitteilung der KV Westfalen-Lippe: "Sofern die Apotheken in räumlicher Nähe zur Praxis nicht in der Lage oder nicht dazu bereit sind, E-Rezepte zu empfangen und einzulösen, können Sie dem Versicherten ein Papierrezept auf Muster 16 ausstellen."

Ebenso sollen bei der elektronischen Arbeitsunfähigkeitsbescheinigung (eAU) weiterhin alternative Papierausdrucke möglich bleiben. Damit ging die KBV auf direkten Konfrontationskurs zur Gematik und zum Bundesgesundheitsministerium (BMG). Das BMG zog daraufhin am 20. Dezember die Notbremse und stoppte die geplante bundesweite Einführung des E-Rezepts zum 1. Januar. Wegen "erheblicher

Bedenken" solle nun "der Test- und Pilotbetrieb schrittweise fortgesetzt und ausgeweitet werden", erklärte ein Sprecher des BMG – ohne einen neuen Einführungstermin zu nennen.

C'T AUSGABE 2/2022



In **c't 2/2022 [8]** haben wir für Sie das c't-Notfall-Windows 2022 zusammengestellt. Mit dem Bausatz für das vom USB-Stick laufendes System finden Sie Viren, retten Daten oder setzen Passörter zurück. Wir beleuchten, wie die EU Schlupflöcher der DSGVO für Content-Scanner nutzen will, wir haben Highend-Smartphones getestet, mobile USB-C-Monitore und Server-Software für die private Mediensammlung. Ausgabe 2/2022 finden Sie ab dem 31. Dezember im **Heise-Shop [9]** und am gut sortierten Zeitschriftenkiosk.

(**hag [10]**)

URL dieses Artikels:

https://www.heise.de/-6304671

Links in diesem Artikel:

[1] https://www.heise.de/ct/

[2] https://fachportal.gematik.de/fachportal-import/files/gemSpec_DM_ePA_V1.7.0.pdf

[3] https://www.heise.de/news/Elektronische-Patientenakte-76-Prozent-der-Deutschen-wollen-sie-benutzen-6287302.html

[4] https://www.heise.de/select/ct/2021/20/2121608552835744309

[5] https://fachportal.gematik.de/fileadmin/Fachportal/Downloadcenter/Implementierungsleitfaeden/gemILF_PS_ePA_V2.0.0.pdf

[6] https://heise.de/investigativ

[7] https://www.heise.de/news/Elektronische-Patientenakte-Krankenversicherer-hoffen-auf-hohe-Beteiligung-5000934.html

[8] https://www.heise.de/select/ct/2022/2

[9] https://shop.heise.de/ct-2-2022/PDF

[10] mailto:hag@ct.de