Vertrauen entzogen

Warum 80.000 Arztpraxen ihre Verbindung zur Telematik-Infrastruktur verloren

Seit Ende Mai können tausende Arztpraxen keine Stammdaten von Patienten mehr zur Telematik-Infrastruktur übertragen. Die Ursachenanalyse offenbart gravierende Mängel in der Sicherheitsarchitektur, die bis zur Einführung der elektronischen Patientenakte und des e-Rezeptes dringend behoben werden müssen.

Von Hartmut Gieselmann, Thomas Maus und Markus Montz

Es gibt zwar Stimmen, die aufgrund der nicht abreißenden Pannenserie der Telematik-Infrastruktur (TI) deren Abschaltung fordern. Dass die für die TI verantwortliche Gematik dem aber so schnell – wenn auch unfreiwillig – nachkommt, hatten selbst die schärfsten Kritiker nicht erwartet.

Bislang nutzen in Deutschland etwa 130.000 angeschlossene Arztpraxen und Kliniken die TI, um die Stammdaten ihrer Patienten mit den Krankenkassen abzugleichen. Dazu sind sie über spezielle Sicherheits-Router – Konnektoren genannt – mit den Servern der TI verbunden. Vier große Hersteller teilen sich den Markt der Konnektoren auf: die Telekom-Tochter T-Systems, RISE, Secunet sowie CGM mit der „KoCoBox Med+“. Ende Mai konnten jedoch rund 80.000 Praxen mit Konnektoren der drei erstgenannten Anbieter bestimmte Dienste der TI nicht mehr erreichen. Von Praxen mit der KoCobox waren laut Hersteller nur ein Prozent betroffen.

Rund eine Woche später hatte die Gematik die Ursache gefunden. Schuld war demnach ein falscher Eintrag in der Trust-Service Status List (TSL). Sie enthält die notwendigen Zertifikate, mit denen die Konnektoren vertrauenswürdige Verbindungen zu den Servern der TI aufbauen. Die Gematik stellte Anfang Juni eine korrigierte TSL-Datei zum Download bereit.

Doch behoben ist der Fehler damit noch lange nicht. Denn die betroffenen Konnektoren sind ja offline und können somit auch die neue TSL-Datei nicht automatisch nachladen. Aufspielen müssen das Update die sogenannten Dienstleiter vor Ort (DvO), die die Konnektoren in den Praxen administrieren. Da die TI ein Netzwerk „höchster Sicherheitsansprüche“ darstellt, ist in vielen Fällen selbst eine Fernwartung der Konnektoren nicht freigegeben. Also müssen die DvO Termine mit den Ärzten abstimmen – und das dauert bei 80.000 Anschlüssen. Mitte Juni war laut Gematik noch immer der Stammdatenabgleich von über 40.000 mit der TI verbundenen Praxen gestört.

Bild: CGM

Rund 50.000 Konnektoren vom Typ „KoCoBox med+“ sind vom Ausfall nicht betroffen, weil sie auf eine Absicherung per DNSSEC verzichten.

Fehlerhaftes Zertifikat

Um zu verstehen, wie es zu dem Ausfall kam, haben wir die neue Datei „TSL.xml“ mit einer älteren Version verglichen. Die TSL-Datei ist ein zentrales Element des Sicherheitskonzepts der TI und definiert, welche Dienste mit welchen kryptografischen Schlüsseln authentisiert werden. Sie stellt im Prinzip eine signierte Liste vertrauenswürdiger Root-Zertifikate dar, die die Konnektoren über den TI-Anschluss normalerweise täglich oder spätestens bei jedem Neustart vollautomatisch aktualisieren.

Diese automatische Aktualisierung funktioniert nicht mehr, wenn beispielsweise die VPN-Zertifikate auslaufen würden. Das war hier jedoch nicht der Fall, da die Ablaufdaten der Zertifikate weit in der Zukunft liegen.

Zur manipulationssicheren Namensauflösung der IP-Adressen innerhalb der TI nutzen viele Konnektoren zudem DNSSEC. Die TSL-Datei führt sämtliche Kenndaten des zur Prüfung nötigen DNS-Root-Anchor auf. Das Zertifikat für den DNS-Root-Anchor ist im Block der von der Arvato Systems GmbH kontrollierten Zertifikate gelistet.

Und hier findet sich die Antwort: Mit Wirkung vom 25.5.2020, 0:00 Uhr wurde ein neuer DNSSEC-Root-Trust-Anchor gesetzt. Zusammen mit einem gravierenden Administrationspatzer dürfte dies die Ursache und der Zeitpunkt des Störungsbeginns für die Ausfälle sein, die die Gematik zwei Tage später öffentlich machte.

Die Konnektoren von T-Systems, RISE und Secunet setzen DNSSEC offenbar flächendeckend ein. Nur bei der KoCoBox von CGM ist diese Absicherung optional und Zahlen des Herstellers zufolge bei 99 Prozent der Geräte nicht aktiviert. Wenn rund 50.000 KoCoBoxen kein DNSSEC nutzen, können sie zwar weiterhin Stammdaten mit der TI austauschen. So konfiguriert sind sie aber anfällig für Angriffsszenarien im Bereich des Routing und genügen kaum den „höchsten Sicherheitsstandards“, die für die TI gelten sollen.

Die Analyse der TSL-Datei offenbarte darüber hinaus weitere Gefahren: So kon-

trolliert die zur Bertelsmann-Gruppe gehörende Arvato Systems GmbH nicht nur das Zertifikat für den DNS-Root-Anchor, sondern auch das TSL-Signer-CA-Zertifikat, das die TSL über ein Signer-Zertifikat sichert. Dieses Zertifikat wacht über sämtliche Vertrauensverhältnisse der TI.

Die neu ausgespielte Reparatur-TSL nennt zwar die Gematik GmbH als TSL-Signer-Certificate-Authority, listet das zugehörige Zertifikat aber weiter im Block der von Arvato kontrollierten Schlüssel. Demnach kann eine einzelne Privatfirma mit beschränkter Haftung die komplette TI auf einen Schlag außer Gefecht setzen.

Das Bundesministerium für Gesundheit (BMG) wollte uns zum Ausfall keine Fragen beantworten und verwies an die Gematik. Aber auch hier gab es bis Redaktionsschluss keine Antworten. So ist weiter unklar, wer für den fehlerhaften Eintrag in der TSL verantwortlich ist und warum er vor der Ausspielung des Updates nicht auffiel. Transparente Aufklärung sieht anders aus.

Ohne Absicherung

Bei einer kritischen Infrastruktur wie der TI ist die Kontrolle der Schlüssel eine hoheitliche Aufgabe, die in staatliche Hand gehört. Schätzungen des Präsidenten der Bundesärztekammer, Dr. Klaus Reinhardt, zufolge könnte sich der Ausfall der TI über zehn Wochen hinziehen. Zu der langen Dauer trägt auch ein Streit der Gematik mit den IT-Dienstleistern bei: Normale Wartungsarbeiten der DvO gelten Ärzte mit einer Service-Pauschale von 248 Euro pro Quartal ab. Doch viele Dienstleister sind nicht bereit, einen Fehler zu reparieren, den sie nicht zu verantworten haben.

Auf Fragen, wie sich derartige Ausfälle künftig vermeiden ließen, gab die Gematik keine Antwort. Bei einem korrekten Change-Management hätte der Fehler eigentlich vorher auffallen müssen. Ebenso fehlt offenbar eine Rollback-Strategie, auf die die Konnektoren bei einer solchen Panne zurückgreifen können. Dr. Reinhardt forderte denn auch folgerichtig ein „Notstromaggregat“, das der TI bislang fehlt.

Ausbaupläne

Angesichts der fehlenden Sicherungen können Ärzte und Patienten nur froh sein, dass der Ausbau der Telematik-Infrastruktur dem Zeitplan weit hinterherhinkt. Denn wenn die TI bereits Patientenakten und Rezepte elektronisch kontrollieren würde, wären die Folgen des wochenlangen Ausfalls katastrophal gewesen – selbst ohne Corona.

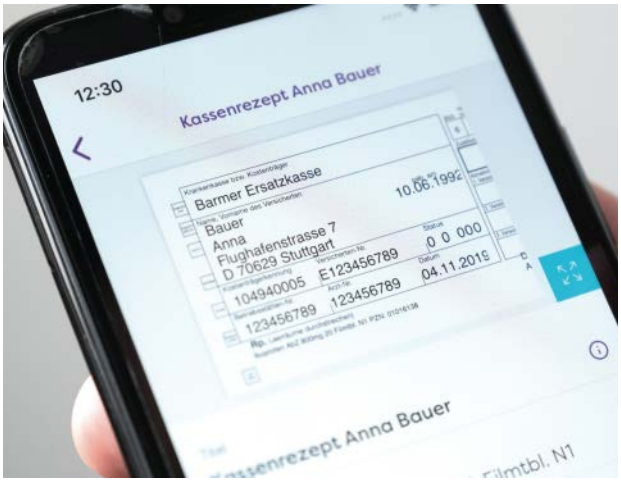

Bild: Bernd Weißbrod/dpa

Ab Januar 2022 sollen Patienten elektronische Rezepte per App empfangen. Papierrezepte sind künftig nur noch in Ausnahmefällen vorgesehen. Fällt die Telematik zwischen Arztbesuch und Rezepteinlösung aus, drohen Patienten weitere Laufwege und Wartezeiten, bis sie ihre Verschreibungen bekommen.

Doch das soll sich bald ändern: Ab dem kommenden Jahr haben Krankenversicherte einen Anspruch darauf, dass ihr Arzt ihre elektronische Patientenakte (ePA) mit Daten füllt. Dazu gehören Notfalldaten, Medikationspläne sowie Befunde und Arztberichte. Um dies zu regeln, hat der Bundestag just das Patientendaten-Schutz-Gesetz (PDSG) verabschiedet. Es soll im Herbst 2020 in Kraft treten.

Ob und welche Daten in der ePA landen, soll der Versicherte entscheiden. Er bestimmt auch über Zugriffsrechte und Löschungen. Zunächst können Versicherte ihren Ärzten allerdings nur Vollzugriff gewähren. Sie selbst können ihre Daten erst ab 2022 per Smartphone oder Tablet einsehen und bestimmen, welcher Arzt welche Dokumente sieht.

Der Landesdatenschützer von Baden-Württemberg, Dr. Stefan Brink, kritisiert dieses anfängliche „Alles-oder-nichts-Prinzip“ und fürchtet, dass es der Akzeptanz der Digitalisierung schadet. Ärzteverbände warnen hingegen vor haftungsrechtlichen Fragen, wenn Ärzte sich später nicht mehr darauf verlassen können, eine vollständige ePA mit allen für eine Behandlung relevanten Informationen zu erhalten.

Der Datenaustausch der ePA läuft über die Telematik. Darüber hinaus regelt der Gesetzgeber ab Januar 2022 eine eigene, an die TI angeschlossene App für E-Rezepte. Mit der App sollen Patienten digitale Rezepte von ihrem Arzt empfangen, die sie in einer Apotheke vor Ort oder online einlösen. Rezepte auf Papier sind laut den Erläuterungen zum PDSG künftig nur noch in Ausnahmefällen, etwa bei technischen Störungen der TI vorgesehen.

Strafen und Schadenersatz

Zu Forschungszwecken können Versicherte ab 2023 pseudonymisierte Daten aus ihrer ePA freiwillig spenden – ein besonders strittiger Punkt. Vor einer Freigabe müssen die Versicherten über den Einsatzzweck und die Zugriffsberechtigten informiert werden. Ein Widerruf der Freigabe betrifft nur künftige Forschungsvorhaben und ist bei bereits laufenden Projekten nicht mehr möglich.

Angesichts der aktuellen Probleme der TI fallen künftige Strafen für Verletzungen der Sicherheit und des Datenschutzes niedrig aus. Betreiber von Diensten und Komponenten innerhalb der TI müssen laut PDSG Störungen und Sicherheitsmängel unverzüglich der Gematik melden, andernfalls drohen Bußgelder bis 300.000 Euro. Der wirtschaftliche Schaden, den Krankenkassen, Ärzte und IT-Dienstleister durch eine Störung der TI erleiden, dürfte im aktuellen Fall jedoch um einige Größenordnungen höher liegen. Laut Handelsblatt drohen Schadenersatzforderungen in Millionenhöhe.

Die Gematik selbst ist dem PDSG zufolge verpflichtet, „unverzüglich die erforderlichen technischen und organisatorischen Maßnahmen zu treffen“, um Gefahren für die Sicherheit und Funktionstüchtigkeit der TI abzuwehren. Über Störungen muss sie das Bundesamt für Sicherheit in der Informationstechnik informieren und dessen Anweisungen befolgen. Ob die Gematik künftige Sicherheitsmängel der TI dann auch zeitnah abstellen können wird, darf angesichts der fortwährenden Probleme bezweifelt werden. *(hag@ct.de)* c't

Weitere Infos: ***ct.de/yv2d***