MedWiss.Online

Zukunftsfähige Sicherheitsarchitektur für die Kommunikation im Gesundheitswesen

Über die Telematikinfrastruktur (TI) sollen Akteure des Gesundheitswesens Patientendaten sicher, schnell und ortsunabhängig austauschen können. Die Plattform für Gesundheitsanwendungen in Deutschland soll dafür nun eine neue Sicherheitsarchitektur erhalten. Der Datenaustausch zwischen allen Akteuren und der Zugang zu Fachdiensten soll erleichtert werden. Gemeinsam mit der Bundesdruckerei, CompuGroup Medical Deutschland AG, D-Trust GmbH und genua GmbH hat das Fraunhofer AISEC im Auftrag der gematik GmbH die Grundlagen dafür gelegt: Neben einem auf Zero-Trust-Prinzipien basierenden Architekturkonzept wurde ein Demonstrator für die Sicherheitsarchitektur der nächsten Generation entwickelt.

Ob elektronische Patientenakte, digitaler Medikationsplan oder E-Rezept – diese Anwendungen sind zentrale Elemente der Telematikinfrastruktur (TI). Die Plattform strebt eine einfache und zugleich sichere Kommunikation zwischen Arztpraxen, Krankenhäusern und weiteren Akteuren im Gesundheitswesen an. Medizinische Informationen, die für die Behandlung von Patientinnen und Patienten benötigt werden, wären dann ortsunabhängig verfügbar. Verantwortlich für die TI ist die gematik GmbH, die nationale Agentur für digitale Medizin, der neben dem Bundesministerium für Gesundheit (BMG) die Ärztekammern, Apotheken, Krankenhaus- und Versicherungsverbände als Gesellschafter angehören.

Die weiterentwickelte TI soll nun eine neue Sicherheitsarchitektur 2.0 erhalten. Die TI 1.0 ist bislang ein durch VPN abgesichertes, isoliertes Netzwerk, das Akteure mittels Smartcards identifiziert und teilnehmen lässt. Mit dem starken Wachstum an TI-Nutzenden und der weiteren Digitalisierung gehen jedoch neue Anforderungen in puncto Skalierbarkeit, Verfügbarkeit, nutzerfreundliche Sicherheit und mobile Nutzung einher, die die aktuelle Sicherheitsarchitektur nicht mehr erfüllen kann.

Zero-Trust-Prinzipien überprüfen jeden Zugriff

Die neue TI-Sicherheitsarchitektur soll auf Zero-Trust-Prinzipien basieren. »Zero Trust« bedeutet, dass Akteure in einem System einander grundsätzlich erst einmal nicht vertrauen, sondern die Vertrauenswürdigkeit kontinuierlich überprüft wird. So wird das Vertrauen bei jedem Zugriff auf die Ressourcen eines Dienstes neu aufgebaut und geht nach diesem Zugriff wieder verloren. Hierfür müssen für die Kommunikation zwischen den Akteuren stets verlässliche Nachweise erbracht werden, welche dieses Vertrauen begründen. Eine Zugriffskontrolle nach Zero-Trust-Prinzipien ist damit ein datengetriebener, fein-granularer Ansatz der Informationssicherheit, der nicht nur externe Bedrohungen, sondern auch interne Gefahrenpotentiale adressiert. Der Zero-Trust-Ansatz hebt sich insofern von klassischen Sicherheitskonzepten ab, die sich in der Regel auf die Sicherung der Unternehmensgrenzen konzentrieren.

Gleichberechtigte Integration aller Akteure

»Unser Vorschlag für eine TI-Sicherheitsarchitektur 2.0 ermöglicht den Zero-Trust-Ansatz, ohne dass proprietäre Komponenten eingesetzt werden müssen. Stattdessen setzt die

Sicherheitsarchitektur auf die Endgeräte, die bei den Nutzenden der Gesundheitsdienste bereits vorhanden sind und berücksichtigt deren Sicherheitsfunktionen bei der Autorisierung einzelner Zugriffe auf einen Dienst. Dabei haben wir Optionen für verschiedene Szenarien wie zum Beispiel den Zugriff durch Versicherte, Arztpraxen oder Krankenhäuser berücksichtigt«, erläutert Martin Seiffert, Senior Scientist der Abteilung Secure System Engineering am Standort des Fraunhofer AISEC in Berlin.

Ein weiterer Vorteil der neuen Sicherheitsarchitektur soll die Erweiterung des Kreises der Nutzenden sein. »In der bisherigen VPN-Infrastruktur ist ein direkter Zugriff auf Gesundheitsdienste nur für Leistungserbringer wie Arztpraxen mit einem festen Standort und über den VPN-Konnektor als proprietäre Komponente vorgesehen. Für Leistungserbringer ohne festen Standort oder Versicherte ist dieser Zugriffsweg nicht geeignet. Das Konzept für die TI 2.0 sieht hingegen einheitliche Zugriffsmechanismen für sämtliche Nutzergruppen und auch die Nutzung mobiler Endgeräte vor«, hebt Monika Kamhuber hervor, Wissenschaftlerin aus der Abteilung Secure Operating Systems am Fraunhofer AISEC in Garching.

Dynamisches, flexibel anpassbares Regelwerk

Eine weitere Stärke des Konzepts für die Sicherheitsarchitektur ist, dass bei der Regelung der Zugriffe nicht allein die Identität der Nutzenden ausschlaggebend ist, sondern auch Faktoren wie Ort und Zeitpunkt des Zugriffs sowie Sicherheitsanforderungen an die Endgeräte berücksichtigt werden können. Welche Daten konkret für die Autorisierung eines Zugriffs auf die Gesundheitsdaten erforderlich sind, wird dabei in einem dynamischen Regelwerk festgelegt, das mit dem Stand der Technik mitwächst: Das Regelwerk integriert zügig aktuelle Entwicklungen in der Informationssicherheit und Anpassungen hinsichtlich der Nutzung von Gesundheitsdiensten, ohne dafür jeden einzelnen Fachdienst einzeln aktualisieren zu müssen.

Die Zugriffsanforderungen können für die verschiedenen Nutzergruppen und Anwendungen je nach Risiko festgelegt und bei Bedarf wieder angepasst werden. So können beispielsweise für Ärztinnen und Ärzte höhere Sicherheitsvorgaben beim Zugriff auf Patientendaten nötig sein, wenn diese auf eine Vielzahl von Patientendaten zugreifen können, als für Versicherte, die nur ihre eigenen persönlichen Daten einsehen möchten.

Besonderer Schutz für sensible Patientendaten

Die sichere Verwaltung von Patientendaten und die Wahrung des Datenschutzes haben in einem so sensiblen Umfeld wie dem Gesundheitswesen oberste Priorität. Vor diesem Hintergrund versucht das Konzept des Fraunhofer AISEC und seiner Partner Allmachtstellungen zu vermeiden, indem es dafür sorgt, dass keine der Infrastrukturkomponenten alleine den Zugriff auf die Gesundheitsdienste ermöglichen kann. So kann für den Zugang zur TI 2.0 neben einem Identitätsnachweis auch das Vorhandensein eines einmalig registrierten Geräts geprüft werden, sodass ein entwendeter oder manipulierter Identitätsnachweis allein ebenso wenig für einen Zugriff ausreicht wie der Diebstahl eines registrierten Endgeräts.

»Da es sich bei der Telematikinfrastruktur um ein Netz handelt, in dem allen voran persönliche Gesundheitsdaten der Patienten verarbeitet werden, werden an die TI 2.0 sehr hohe Sicherheitsanforderungen gestellt. Unsere Architektur nutzt verschiedene, im Bereich des Identitäts- und Zugriffsmanagements standardisierte und im Rahmen von Zero Trust etablierte Komponenten und macht es so möglich, diesen Anforderungen gerecht zu werden«, so Seiffert.

Das Konzept für eine TI 2.0 auf Basis von Zero-Trust-Mechanismen des Fraunhofer AISEC und der Partner Bundesdruckerei, CompuGroup Medical, D-Trust und genua wurde von der gematik online

veröffentlicht.