DSGVO-Zwickmühle

c’t deckt auf: Datenschutzverstöße bei TI-Konnektoren in der Medizin

Konnektoren des Herstellers Secunet zeichnen in Logs personenbezogene Daten auf und missachten damit die Spezifikationen der Gematik. Der Bundesdatenschützer sieht erstaunlicherweise Ärzte statt Hersteller in der Verantwortung für die DSGVO-Verstöße.

Von Thomas Maus

Kassenpatienten stecken beim Arztbesuch ihre elektronische Gesundheitskarte (eGK) in ein Kartenterminal. Das Terminal ist über einen Konnektor mit der Telematischen Infrastruktur (TI) verbunden und tauscht darüber unter anderem mit den gesetzlichen Krankenkassen Stammdaten der Versicherten (VSDM) aus.

Patientendaten gehen nur den Arzt und die Versicherung etwas an. Deshalb haben diese Daten in Logs des Konnektors nichts zu suchen. Die Spezifikationen der für die TI verantwortlichen Gematik (gemSpec_Kon_V4.11.1.doc und gemSpec_Kon_V5.8.0.docx) verlangen daher gleichlautend: „Personenbezogene Daten DÜRFEN NICHT in Protokolleinträgen gespeichert werden.“

Deshalb staunten wir nicht schlecht, als wir bei unseren Untersuchungen zu Ausfällen der TI (siehe c’t 4/2022, S. 44) in den Log-Dateien von Konnektoren auf personenbezogene Daten stießen. Wir fanden sie im Zeitraum von Oktober 2018 bis Dezember 2020 in den Protokollen des Konnektors von T-Systems. Dieser wurde 2020 bundesweit gegen den Einboxkonnektor von Secunet ausgetauscht. Bei Secunet fanden wir personenbezogene Daten von Mai 2020 bis zum Ende unseres Testzeitraums im Juli 2021.

Die System- und Sicherheits-Logs speicherten bei jedem VSDM-Fehler die Seriennummer des Krypto-Zertifikats der eGK. In den VSDM-Logs der Konnektoren kam noch die ICCSN (Integrated Circuit Card Serial Number) der eGK hinzu. Über diese Nummern lassen sich Versicherte zumindest indirekt zuordnen. Sie zählen deshalb laut der genannten Spezifikationen zu den personenbezogenen Daten: „Die ICCSN darf nicht mit (dem) Sicherheitsprotokoll gespeichert werden“, heißt es dort unter Punkt TIP1-A_4710. Die Protokolle identifizieren zudem die Praxis eindeutig. Zugriff auf die Logs sollen laut Gematik nur „Leistungserbringer-Institutionen und von ihnen beauftragte Dienstleister“ haben, nicht jedoch die Trust Service Provider (TSP), die die Krypto-Zertifikate der eGKs ausstellen.

Wenn man die Log-Daten illegalerweise mit denen der Kartenhersteller oder TSP zusammenführt, ließe sich nämlich feststellen, welcher Patient wann welchen Arzt aufgesucht hat. Man bekäme heraus, wann Herr Meier beim Psychiater war und in welchem Zeitraum Frau Müller in einer Suchtklinik behandelt wurde.

Wir meldeten dies Mitte Januar dem Bundesbeauftragen für Datenschutz und Informationsfreiheit (BfDI). Dieser stellte am 14. Februar „eine Datenschutzverletzung nach Art. 33 Abs. 1 DSGVO“ fest. Laut Christof Stein, Sprecher des BfDI, habe die Gematik den Hersteller Secunet informiert. Demnach protokolliere der Secunet-Konnektor selbst mit der aktuellen Firmware 4.10.1 noch immer personenbezogene Daten und verstoße damit gegen die DSGVO. Secunet wolle dies in einem kommenden Update des Konnektors beheben. Anfragen von c’t wollte Secunet nicht beantworten.

Bild: Medatixx

In den Protokollen des Konnektors von Secunet fand c’t personenbezogene Daten von Patienten.

Schwarzer Peter

Auf die Frage, wer für den DSGVO-Verstoß verantwortlich sei, antwortete der BfDI: „Datenschutzrechtlich verantwortlich für die Konnektoren sind diejenigen, die diese für die Zwecke der Authentifizierung und elektronischen Signatur sowie zur Verschlüsselung, Entschlüsselung und sicheren Verarbeitung von Daten in der zentralen Infrastruktur nutzen, soweit sie über die Mittel der Datenverarbeitung mitentscheiden.“ Auf Nachfrage erklärte der BfDI, dies seien „Ärzte und Leistungserbringer“ – und nicht etwa die für den Betrieb der TI verantwortliche Gematik, die die fehlerhaften Konnektoren zugelassen hat. Warum sie die Spezifikationsverletzung bei den Zulassungstests nicht entdeckt hatte, erklärte die Gematik nicht. Dies ist umso unverständlicher, weil der gleiche Fehler bereits 2018 bei den KoCo-Box-Konnektoren auftrat und behoben werden musste.

Ärzte und Leistungserbringer wurden jedoch unter der Androhung von Honorarkürzungen gesetzlich verpflichtet, sich über einen von der Gematik zugelassenen Konnektor mit der TI zu verbinden. Sie haben keinerlei Möglichkeiten, die Protokollierung der personenbezogenen Daten abzustellen – außer sie schalten den Konnektor aus. Bei Redaktionsschluss tauschte sich der BfDI noch mit der Gematik aus, ob Ärzte etwa die gegen die DSGVO verstoßenden Secunet-Konnektoren abschalten müssen und wie betroffene Patienten informiert werden sollen. Ebenso ungeklärt blieben Fragen von c’t zu eventuellen Bußgeldern und Schadenersatzforderungen. Der verzwickte Fall dürfte Juristen noch lange beschäftigen. *(hag@ct.de)* c't