ELGA

Ärztekammer warnt vor Datenklau

Eine im Auftrag der Wiener Ärztekammer durchgeführte Analyse des Systems und der Funktionalitäten der Elektronischen Gesundheitsakte deckt gefährliche Schwachstellen in der Gesamtarchitektur auf. Demnach kann man davon ausgehen, dass ELGA im Besonderen in den nächsten Jahren Ziel von Angriffen sein wird – oder schon ist.

Die Wiener Ärztekammer steht dem Einsatz moderner Informationstechnologien im österreichischen Gesundheitssystem positiv gegenüber – sofern gewisse Bedingungen erfüllt werden. Dazu gehört an erster Stelle die Sicherheit der sensiblen Patientendaten. Doch durch die Elektronische Gesundheitsakte (ELGA) haben sich die Angriffsfläche und die Auswirkungsbreite von Cyberattacken auf unsere Gesundheitsdaten stark erhöht. Mit einem erfolgreichen Angriff können nunmehr großflächig die Gesundheitsdaten aller ELGA-Teilnehmer kompromittiert werden – und das mit fatalen Folgen. Denn der medizinische Identitätsdiebstahl ist doppelt gefährlich, weil neben dem finanziellen Schaden auch die Krankengeschichte des Opfers durch den „falschen Patienten" verfälscht wird.

„Das kann gefährlich werden", verdeutlicht Ärztekammerpräsident Thomas Szekeres. „Die Folgen reichen von Rufschädigung und finanziellen Schäden bis hin zu einer deutlichen Gefahr für Leib und Leben, wenn etwa falsche Befunde in der Patientenakte zu Behandlungsfehlern führen oder Plätze auf Wartelisten für Operationen gelöscht werden."

Die Ärztekammer stützt sich bei ihren Erkenntnissen auf eine Studie, die von der renommierten K-Advisors Consulting und Beteiligungsmanagement GmbH durch den IT- und Sicherheitsfachmann Cornelius Granig und den Cybersecurity-Experten und Geschäftsführer von TS Management Consulting, Thomas Stubbings, erstellt wurde. Und dass die Bedrohungslage evident ist, zeigen auch die Vorfälle der nahen Vergangenheit.

Lukratives Geschäft

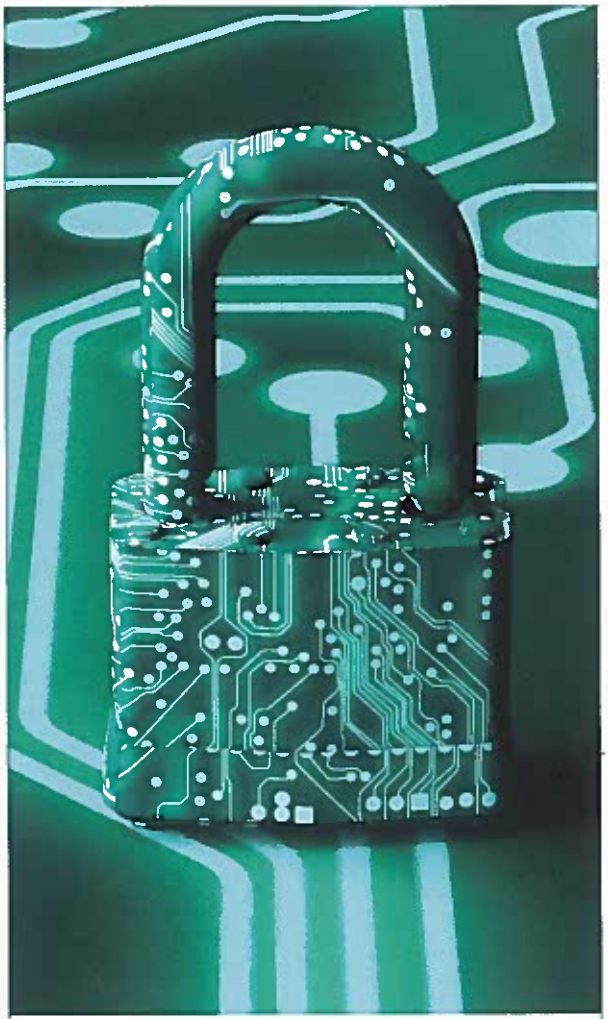
Im Oktober 2013 wurde ein Datenleck bei der österreichischen Sozialversicherung bekannt, bei dem sensible Daten wie Adressen, Konto- und Telefonnummern, Angaben über Arbeitgeber sowie Informationen über Kinder und Sozialversicherungsnummern der Versicherten aus der Zentralen Partnerverwaltung (ZPV) der Sozialversicherung betroffen waren. Die genauen Umstände sind nach wie vor nicht öffentlich bekannt, das Aktivistenkollektiv Anonymous Austria reklamiert jedenfalls diesen erfolgreichen Hack für sich.

Die Ursache ist dafür umso offensichtlicher: „Mangelndes Sicherheitsbewusstsein der Verantwortlichen, unausgereifte Sicherheitskonzepte sowie fehlende Investitionen in die IT-Sicherheit werden den Angreifern auch bei ELGA ein leichtes Spiel machen", ist Johannes Steinhart, Obmann der Kurie niedergelassene Ärzte und Vizepräsident der Ärztekammer für Wien, überzeugt.

Dass Funktionalität und Sicherheit des Systems nicht gewährleistet sind, zeigen auch die aktuellen Erfahrungen in Deutschlandsberg. Das E-Medikations-Pilotprojekt musste dort wegen des technisch nicht ausgereiften Systems von den teilnehmenden Ärzten im Spätsommer 2016 abgebrochen werden.

Die Gefährdungslage bei ELGA sieht auch Studienautor Stubbings: „Man kann und muss davon ausgehen, dass ELGA im Besonderen in den nächsten Jahren Ziel von Angriffen sein wird – oder sogar schon ist." Ein Hacker könnte Zugriff und so zum Beispiel Zugang zu allen Daten über die Patienten und deren Behandlung erlangen: „Das ist eine neue Form des Identitätsdiebstahls und ein lukratives Geschäft. Laut FBI zahlten Unbekannte im Frühjahr 2014 für eine einzige gestohlene digitale Krankenakte 50 Dollar."

Neben dem Identitätsdiebstahl ist auch der Einsatz von Schadsoftware eine reale Bedrohung. Die Funktionsweise ist einfach: Die Daten werden durch die



Die fünf Forderungen der Ärztekammer zur Sicherheit von ELGA

- Einführung einer zentralen Benutzerverwaltung für alle ELGA-berechtigten Anwender
- Einführung einer verpflichtenden separaten Authentifizierung beim Einstieg in ELGA durch jeden ELGA-User
- Verwendung einer starken Zweifaktor-Authentifizierung
- Einführung einer flächendeckenden digitalen Signatur von Gesundheitsdokumenten
- Regelmäßige Informationen an Patienten über deren gespeicherte Daten und Abrufe, zum Beispiel über E-Mail oder SMS („Push Service")

Schadsoftware verschlüsselt, und nur gegen Zahlung von Lösegeld erhält man den elektronischen Schlüssel und damit wieder Zugang zu den Patientendaten. „Wenn dieser Zugang zu den Patientendaten nicht garantiert werden kann, so kann ein solcher Angriff durchaus lebensbedrohliche Folgen nach sich ziehen", unterstreicht Stubbings.

Cyberangriffe auf Gesundheitsanbieter sind längst auch in Österreich keine Ausnahme mehr. So wurde etwa die Homepage eines österreichischen Krankenhauses bei einem Hackerangriff mit einer Kinderpornografie-Seite verlinkt. Im Jahr 2009 wurden in Kärnten in drei Spitälern ungefähr 3000 Krankenhaus-PCs mit dem Computer-Wurm „Conficker" befallen und mussten komplett neu aufgesetzt werden.

„Das mag – abgesehen vom Reputationsschaden – noch nicht gefährlich sein, zeigt aber, wie schnell die Bedrohungsszenarien real werden können", betont Steinhart. „Das sollte auch der Hauptverband der österreichischen Sozialversicherungsträger wissen und, bevor er einen flächendeckenden Roll-out von ELGA und E-Medikation unvorbereitet in ganz Österreich durchpeitscht, lieber seine Sicherheitsarchitektur verbessern."

Denn die Kosten nach einer solchen Cyberattacke sind enorm: In den USA gilt die Regel, dass die Kosten pro gehacktem Datensatz bis zu 200 Dollar betragen können. Diese Kosten betreffen insbesondere Berichterstattung, Berichtigungen, Verwaltung und Cyberuntersuchungen.

Anfällig für Missbrauch

ELGA setzt auf ein dezentrales föderales Identitätsmanagement und Berechtigungskonzept. Jeder Zugang in einem Krankenhaus oder in einer anderen Einrichtung mit Schwachstellen in der IT-Security kann dazu missbraucht werden, potenziell sämtliche ELGA-Gesundheitsdaten aller Österreicher einzusehen, die kein Opt-out verfügt haben. „Das Auftreten von Schwachstellen und in weiterer Folge das fahrlässig oder vorsätzlich herbeigeführte Auftreten von Sicherheitsvorfällen ist bei ELGA wahrscheinlicher als bei einer zentral gemanagten Architektur mit einheitlichen Sicherheitsstandards und einer konsequenten Security Governance", erklärt Stubbings.

Sogar die ELGA GmbH geht in ihrer eigenen Risikoanalyse davon aus, dass Endgeräte mit Schadsoftware kompromittiert sind und dass dadurch in weiterer Folge Missbrauch stattfinden kann. Eine zentrale Überprüfung der IT-Sicherheit gibt es aber nicht. Der Identitätsmissbrauch wird damit durch ELGA vereinfacht. Der Benutzer meldet sich nur mit Username und Passwort an, eine weitere Authentifizierung ist nicht notwendig. ELGA nützt also „Single-Sign-On": Wer Zugang zum Passwort hat, hat alle Berechtigungen und kann zum Beispiel Gesundheitsdaten abrufen, speichern, kopieren, verschicken, verändern sowie neue Befunde schreiben. „Jeglicher Missbrauch ist hierbei möglich", zeigt Szekeres die Gefahren auf.

Denn anders als beim Online-Banking, wo eine starke Zweifaktor-Authentifizierung durch eine zusätzliche TAN-Eingabe oder einen Hardware-Token plus PIN notwendig ist und einen elektronischen Diebstahl damit unmöglich macht, erleichtert das ELGA-Authentifizierungsverfahren den Identitätsdiebstahl. Die Einsicht in die sensiblen Daten erfordert nicht einmal die Zustimmung und Anwesenheit des Patienten. „ELGA und E-Medikation sind anfällig für Missbrauch und müssen zurück in die Werkstatt, sonst sind sie eine enorme Gefahr für die Patientensicherheit", fasst Steinhart zusammen.

Für die Ärztekammer ist ein Neustart unumgänglich, um die Sicherheitsschwachstellen abzubauen. Steinhart: „Wir fordern eine umfassende Evaluierung sowie die Implementierung sicherheitsfördernder Maßnahmen, statt ELGA und E-Medikation in Österreich flächendeckend mit Gewalt durchzupeitschen".

„Die Ärztekammer ist nicht grundsätzlich gegen den Fortschritt, den eine elektronische Datenvernetzung mit sich bringen könnte", fasst Szekeres zusammen. Allerdings müsse bei der Nutzung die Sicherheit für Patienten und Ärztinnen und Ärzte gewährleistet werden, und die für eine elektronische Vernetzung notwendigen finanziellen Mittel müssten in einer vernünftigen Relation zum prognostizierten Nutzen stehen. „Erst dann stehen wir hinter diesem Projekt, denn in der jetzigen Form droht ELGA zum Spionage-Tool für Krankenakten zu werden", so Szekeres. □

Kammeramt der Wiener Ärztekammer ist ISO-zertifiziert

Um die Organisation für die Mitglieder der Ärztekammer bestmöglich darzustellen und auch nachzuweisen, dass die Prozesse zur Unterstützung der Ärzteschaft qualitätsgesichert ablaufen, hat die Wiener Ärztekammer bereits 2015 beschlossen, das Kammeramt nach ISO 9001 zu zertifizieren. Die diesbezüglichen Arbeiten nahmen eineinhalb Jahre in Anspruch; sie bedeuten eine umfassende Neuorientierung des prozessualen Denkens bei den Mitarbeitern der Ärztekammer.

Gemäß den ISO-Vorgaben wurden Dutzende Prozesse niedergeschrieben, eine umfassende Qualitätspolitik wurde entwickelt und das Kammeramt wurde einer eingehenden Prüfung unterzogen. Viele der von ISO geforderten Systeme waren schon etabliert, jedoch gab es kein Gesamtsystem, das eine umfassende Qualitätspolitik im Kammeramt sichergestellt hätte.

Übernahme der Zertifizierungsurkunde stellvertretend für alle Mitarbeiter: Ärztekammerpräsident Thomas Szekeres (li.) und Kammeramtsdirektor Thomas Holzgruber

Nach internen Audits und einem Voraudit fand das entscheidende zweitägige Audit durch Auditoren der Quality Austria am 14. und 15. Dezember 2016 in allen Abteilungen des Hauses statt und wurde erfolgreich bestanden.

Um das Audit erfolgreich bestehen zu können und auch nachhaltig die Qualitätspolitik im Kammeramt zu etablieren, wurde eine eigene Stabsstelle „Qualitätsmanagement und HR" geschaffen, die sich mit dem Thema weiter beschäftigen wird.

Die politischen Prozesse rund um die gewählten Organe (Präsidium, Vollversammlung, Vorstand et cetera) sowie aller Referate, Fachgruppen, Turnus- und Bezirksärztevertreter wurden bewusst aus der Zertifizierung ausgenommen, da politische Prozesse einer Zertifizierung nicht zugänglich sind.