

Wie sicher sind die Daten der Versicherten im Gesundheitswesen?

von Martin Ortgies

Aktuelle Anwendungen wie die elektronische Gesundheitskarte markieren das gestiegene Niveau der Digitalisierung und Vernetzung im Gesundheitswesen. Untrennbar damit verbunden ist auch die gestiegene Gefährdung sensibler personenbezogener Patientendaten. Für die Krankenkassen als „Informationseigentümer“ wird der Datenschutz-Nachweis immer schwieriger, da die Verarbeitung sensibler Daten an eine Vielzahl externer IT-Dienstleister ausgelagert wird.

Die Geschäftsabläufe der Krankenkassen werden durch immer leistungsfähigere EDV-Anwendungen bestimmt. Höhere Effektivität und geringere Kosten sind das Ziel. Das Dilemma: Datenschutz und IT-Security bleiben hinter dem Tempo der Vernetzung zurück, die Maßnahmen sind nicht standardisiert und auf recht unterschiedlichem Niveau. Hier hat die ITSC GmbH in Hannover, das Servicerechenzentrum für 84 gesetzliche Krankenversicherungen, Neuland betreten. Als bisher einziger EDV-Dienstleister im Gesundheitswesen hat sich das ITSC offiziell vom Bundesamt für Sicherheit in der Informationstechnik (BSI) intensiv prüfen und die Sicherheit rund um den sensiblen IT-Verbund ISKV (Informationssystem Krankenversicherungen) nach IT-Grundschatz zertifizieren lassen. "IT-Grundschatz" des BSI ist die anerkannte nationale Ausgestaltung der internationalen Norm "ISO/IEC 27001". IT- Grundschatz beschreibt mit umfangreichen Leitfäden und detaillierten Step-by-Step Anleitungen, wie ein Informationssicherheits-Managementsystem (ISMS) nach den Anforderungen der ISO27001 im Unternehmen eingeführt werden kann.

Warum ist das ITSC diesen Weg gegangen? ITSC-Geschäftsführer Martin Behmann verweist darauf, dass sein Unternehmen auch vor der Einführung der neuen Sicherheitsphilosophie viel für das Thema IT-Security getan hat. „Wir waren aber überrascht, wie viele Lücken wir in den komplexen Abläufen noch erkannt und beseitigt haben“, so Behmann. Nach einem dreijährigen Prozess habe man jetzt von unabhängiger Seite den Nachweis, dass international anerkannte Sicherheitsprozesse und -technologien eingeführt sind und in der Praxis auch gelebt werden. Die eigentliche Einführung des neuen Informationssicherheits-Managementsystems sei im Wesentlichen eine Fleißarbeit und dauere gar nicht so lange. Vorher sei aber ein wichtiger Lernprozess notwendig gewesen. Der Geschäftsführer erzählt freimütig, dass die BSI-Zertifizierung zunächst aus Marketing-Gesichtspunkten betrieben worden sei. Behmann: "Ich gebe zu, das Thema Informationssicherheit unterschätzt zu haben. Wir sind durch den Einführungsprozess viel sensibler geworden und erkennen erst jetzt die Vorteile daraus."

Das Konzept der Informationssicherheit

Aus Sicht von Behmann macht der Aufwand für die zusätzliche Sicherheit vor allem deshalb Sinn, weil die Kunden, also die angeschlossenen Krankenkassen, davon profitieren. Mit dem neuen Konzept der Informationssicherheit sei als Best-Practice-Ansatz die Erfahrung tausender IT-Experten und Rechenzentren eingeflossen. Henning Kopp, lizenziertes IT-Security-Auditor von DS Data Systems: „Mit der Umsetzung der IT-Security-Normen hat ITSC den Schritt von der IT-Sicherheit hin zur Informationssicherheit gemacht.“ Das Wesentliche daran sei, dass neben der reinen Technologie jetzt eine ganzheitliche Sicherheitsbetrachtung der Geschäftsabläufe vollzogen und ein einheitliches Sicherheitsniveau etabliert werde. Der Vorteil für die Krankenkassen: Sie

erhalten überprüfbare Service Level Agreements, klare Schnittstellendefinitionen, transparente IT-Prozesse und ein funktionierendes IT-Risikomanagement – nachgewiesen durch den unabhängigen IT-Sicherheitsnachweis des BSI.

Der Zertifizierungsprozess

Nach einem Einführungsworkshop war bereits 2004 ein Team für die Einführung des IT-Sicherheitsmanagements gebildet worden. Die Komplexität des Themas wurde aber unterschätzt. Viele Prozesse waren zwar etabliert, jedoch nicht dokumentiert. Gleiches galt für übergreifende Konzepte, Richtlinien, Workflows, Antragswesen usw. Das Verständnis von der Thematik und von der Herangehensweise war unterschiedlich und die intern verfügbaren Ressourcen und Erfahrungen waren zu gering, um das Projekt erfolgreich zu stemmen. Der IT-Security-Spezialist DS Data Systems brachte schließlich die notwendige Hilfe. Ausgewählt aufgrund seiner Kompetenz und Erfahrung für das Thema, regte er zunächst „Sensibilisierungs-Veranstaltungen“ an, die tatsächlich den Durchbruch brachten. Wo vorher das Projekt als unnötig oder zu bürokratisch abgelehnt wurde, stieg die Akzeptanz. Andreas Rosenthal, Geschäftsbereichsleiter Technik bei ITSC: „Die Mitarbeiter identifizieren sich inzwischen mit dem Projekt und haben ganz praktisch erfahren, wie wichtig IT-Sicherheit ist.“ Die umfangreichen Maßnahmenbündel wurden von den technischen Fachbereichen jetzt in Rekordzeit umgesetzt. Workflows wurden etabliert, Arbeitsprozesse geregelt, Abläufe dokumentiert und Notfallvorsorgekonzepte verfeinert. Rosenthal: „Es gab ein gemeinsames Ziel, das Zertifikat zu erreichen. Die ganze Mannschaft betrachtete die Prozesse mit anderen Augen. Jeder musste sich um bestimmte Aufgaben kümmern, SLAs (Service Level Agreements) erfüllen und in laufenden Übungen nachweisen.“ Bei der abschließenden Prüfung durch einen unabhängigen BSI-lizenzierten Auditor wurde nicht nur begutachtet, ob ausreichende technische Einrichtungen (von der Firewall bis zum zutrittssicheren Rechenzentrum) vorhanden sind, sondern das Augenmerk lag vor allem auf durchgängige Sicherheitskonzepte in den IT-Prozessen.

Erfahrungen mit der Lösung

Aus Sicht des ITSC-Geschäftsführers Martin Behmann ist das Sicherheitsniveau gravierend gestiegen. „Der Aufwand hat sich gelohnt. Wir haben einen großen Gewinn an Sicherheit und Zeit.“ Das zeige sich an vielen Beispielen. So habe er auch als Geschäftsführer nur noch eingeschränkten Zugang zu bestimmten Sicherheitszonen; Notebooks seien viel strenger abgesichert; es gebe Vorgaben für die Verschlüsselung von E-Mail-Anhängen und selbst die Papierentsorgung wurde neu geregelt. Weniger offensichtlich – aber nicht minder bedeutungsvoll sind die organisatorischen Veränderungen. Das Unternehmen hatte seine Organisation bisher pragmatisch und unbürokratisch geregelt. Das war aber nicht gleichzeitig effizient und sicher. Um die Informationssicherheit zu gewährleisten, wurden die Arbeitsabläufe mit beträchtlichem Aufwand sorgfältig dokumentiert – mit vielen Vorteilen, wie sich anschließend in der Praxis zeigte.

Im dynamisch wachsenden Unternehmen finden neue Mitarbeiter jetzt definierte Aufgaben und Abläufe. Das beschleunigt die Einarbeitung. Auch die Störungsbeseitigung ist dank vorhandener Dokumentationen schneller und die Fehlerhäufigkeit sinkt, da erkannte Fehler systematischer verfolgt und Workflows angepasst werden. Als Servicezentrum macht das ITSC mit den Krankenkassen Backup-Übungen. Im laufenden Betrieb wird der Ausfall des eigenen Rechenzentrums simuliert und die Umschaltung auf ein Backup-Rechenzentrum praktiziert. Im Ergebnis führen die kontinuierlichen Verbesserungen sowohl zu einem höheren Sicherheitsniveau als auch zu einer steigenden Produktivität. Diese Vorteile und der Schutz sensibler

Versichertendaten nach international anerkannten Standards kommen bei den Krankenkassen gut an.

Weitere Schritte sind bereits geplant: Die Regeln des BSI schreiben eine Rezertifizierung nach zwei Jahren vor. Darüber hinaus ist die Zertifizierung der kompletten ITSC geplant, um die Vorteile aus der einheitlichen Arbeitsweise und einheitlichen Sicherheitsstandard in allen Arbeitsprozessen nutzen zu können.

ITSC

Die ITSC GmbH ist das IT-Servicezentrum für 84 gesetzliche Krankenkassen. Das Unternehmen ist innerhalb von fünf Jahren von 30 auf 140 Mitarbeiter gewachsen und bietet ein umfangreiches Dienstleistungsportfolio (vom ASP-Providing der Kernanwendung ISKV - Informationssystem der gesetzlichen Krankenversicherungen – bis zu neuen Dienstleistungen im Umfeld der elektronischen Gesundheitskarte, VoIP-Angeboten oder einer CRM-Lösung für Krankenkassen). Das ITSC wurde 1997 in Hannover gegründet mit weiteren Servicebüros in Hamburg, Essen, Frankfurt und Stuttgart.

Informationssicherheits-Managementsystem (ISMS)

Mit der neuen internationalen Norm "ISO/IEC 27001" werden Anforderungen an ein Informationssicherheits-Managementsystem (ISMS) im Unternehmen definiert. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) liefert mit seinem "IT-Grundschutz Standard für Informationssicherheit" die nationale Ausgestaltung dieser Norm. Der IT-Grundschutzansatz bietet einer Institution eine strukturierte und praxisorientierte Vorgehensweise sowie konkrete, detailliert beschriebene Maßnahmen zur Umsetzung der ISO 27001. Diese Standards sind branchenunabhängig und skalierbar von kleinen Unternehmen bis zu großen Konzernen, und dabei anwendbar für normalen, hohen und auch sehr hohen Schutzbedarf. Sie bilden eine Sammlung von Best-Practice-Ansätzen, die sich über Jahre in der Wirtschaft entwickelt und internationale Anerkennung gefunden haben.

Ansprechpartner für Rückfragen

Dipl.-Ing. Henning Kopp

Leiter Information Security / Portal
Tel. 0531 / 237 31-45
hkopp@datasystems.de

DS DATA SYSTEMS GmbH

Christian-Pommer-Str. 15, 38112 Braunschweig
Tel.: +49 531-2 37 31-0, Fax: +49 531-2 37 31-11
Internet: www.datasystems.de

Christian Kunze

Key Account Manager
Tel. 0531 / 237 31-35
ckunze@datasystems.de