Georgios Raptis
Dr. med.

Vertraulichkeit von medizinischen Daten in der Telematik-Infrastruktur – Sicherheitsanalyse unter Berücksichtigung von Aspekten der langfristigen Sicherheit

Geboren am 7.11.1972 in Larisa / Griechenland
Staatsexamen am 30.10.1997 an der Universität Leipzig

Promotionsfach: Medizinische Biometrie u. Informatik
Doktorvater: Herr Prof. Dr. rer. nat. Thomas Wetter

Medizinische Daten unterliegen der ärztlichen Schweigepflicht. Deren Vertraulichkeit muss geschützt werden.

In Deutschland wurde durch den Gesetzgeber im §291a SGB V eine Telematik-Infrastruktur im Gesundheitswesen definiert und Anwendungen beschrieben. Zielsetzung dieser Telematik-Infrastruktur ist die „Verbesserung von Wirtschaftlichkeit, Qualität und Transparenz der Behandlung“ (SGB V § 291a Abs. 1). Die mit dem Gesetz definierte elektronische Gesundheitskarte sowie die Anwendungen der Telematik-Infrastruktur werden durch die gematik GmbH, eine Gesellschaft aus Vertretern der Selbstverwaltung des Gesundheitswesens, konzipiert und teilweise auch entwickelt und implementiert. Dabei steuert die Regierung über eine 2005 erlassene Rechtsverordnung wesentlich das Projekt.

In der vorliegenden Arbeit wird die Sicherheit der Gesamtarchitektur für die Anwendungen der Telematik-Infrastruktur beleuchtet und in Hinblick auf den Schutz, speziell auf die Vertraulichkeit von medizinischen Daten analysiert und bewertet.

Ziel der Arbeit ist also zu untersuchen, ob die Vertraulichkeit der medizinischen Daten auf Basis der bereits vorliegenden Spezifikationen gewährleistet wird. Methodisch wird eine semi-formale Sicherheitsanalyse in Anlehnung an die Methodologie der Common Criteria durchgeführt, eines für Sicherheitsevaluierungen komplexer Systeme anerkannten Rahmenwerks, der den Rang eines ISO-Standards hat und internationale Akzeptanz findet. Insbesondere wird dabei beachtet, ob die für den sehr hohen Schutzbedarf der Daten erforderliche Mechanismenstärke der spezifizierten Sicherheitsfunktionen erreicht wird und ob die Sicherheitsanalyse im Sinne der Anforderungen der Common Criteria vollständig ist. Für fehlende Anwendungen werden die übergreifenden generischen Sicherheitsanforderungen aus der Gesamtarchitektur und dem Sicherheitskonzept der Telematik-Infrastruktur herangezogen.

Die Ergebnisse der Sicherheitsanalyse zeigen, dass das Gesamtsystem der Telematik-Infrastruktur repräsentiert durch die bisher (Stand 12.12.2007) veröffentlichten Spezifikationen und Dokumente grundsätzlich ein hohes Sicherheitsniveau in Bezug auf die Vertraulichkeit medizinischer Daten aufweist. Insbesondere können dabei die konsequente Verschlüsselung der Dateninhalte schon in der Arztpraxis / im Krankenhaus, der Einsatz sicherheitszertifizierter Schlüsselspeicher (Chipkarten), die Anforderungen an die organisatorische Sicherheit, die Definition von nach dem Stand der Wissenschaft als sicher geltenden kryptographischen Algorithmen und Schlüssellängen, ein nach dem Stand der Technik gutes Netzwerk-Sicherheitskonzept und das kryptographisch abgesicherte Rechtemanagement-System hervorgehoben werden.

Es gibt jedoch noch einige offene Punkte, die noch angegangen werden müssen, um eine hohe Vertraulichkeit der Daten zu gewährleisten. Dazu gehören die kritische Stellung des Brokers und des Audit-Dienstes, der Schutz von Meta-Daten, welche Rückschlüsse auf Arzt-Patient-Beziehungen erlauben können, das noch nicht spezifizierte sicherheitskritische Datenerhalt-Konzept, die nicht spezifizierte Sicherheit der Mehrwertdienste sowie nicht erforderliche Sicherheitszertifizierungen für zentrale Komponenten und für den Betrieb. Da medizinische Daten sehr langlebig sein können, wird auch das Problem der langfristigen Vertraulichkeit in Bezug auf die Sicherheitsleistung der Verschlüsselung kritisch betrachtet.

In diesem Rahmen werden Vorschläge in Form von Konzepten, insbesondere für die langfristige kryptographische Sicherheit verschlüsselter Daten und für den sicheren Datenerhalt dargelegt. Außerdem wird das Restrisiko einer Online-Speicherung abgewogen und als mögliche Maßnahme die optionale dezentrale Speicherung von medizinischen Daten im Ermessen des Patienten vorgeschlagen. Die mangelnde öffentliche Darstellung und wissenschaftliche Bewertung der Sicherheit des Gesamtprojektes der Telematik-Infrastruktur wird in Bezug auf seine Akzeptanz kritisiert.