

Die elektronische Gesundheitskarte und Sicherheitsaspekte: Ein Vorschlag zur entwicklungsbegleitenden Sicherheitsevaluation aus Anwendersicht

Ali Sunyaev, Jan Marco Leimeister, Andreas Schweiger, Helmut Krcmar

Lehrstuhl für Wirtschaftsinformatik
Technische Universität München
Boltzmannstraße 3
85748 Garching bei München
{sunyaev, leimeister, schweiga, krcmar}@in.tum.de

Abstract: Dieser Beitrag schlägt ein Vorgehen für eine frühzeitige Sicherheitsevaluation der elektronischen Gesundheitskarte aus technischer, organisatorischer und ökonomischer Perspektive zur Begleitung der Feldtests vor. Dadurch sollen mögliche Fehler und Schwachstellen in den Prozessen rund um die eGK rechtzeitig identifiziert und behoben werden. Das in diesem Beitrag vorgeschlagene Vorgehen wird in der Testregion Ingolstadt erprobt werden.

1 Einführung

Die elektronische Gesundheitskarte (eGK), der Heilberufsausweis (HBA) und die dafür geschaffene Telematik-Infrastruktur in Deutschland können wesentliche Mehrwerte [BP97, S. 24] für alle Beteiligten im Gesundheitswesen – Patienten, Leistungserbringer und Kostenträger – schaffen. Hierdurch sollen sowohl Qualitätssteigerungen bei der medizinischen Leistungserbringung als auch Senkungen der Behandlungskosten erreicht werden und somit das deutsche Gesundheitswesen insgesamt wirtschaftlicher gestaltet werden.

Dieser durch neue Informations- und Kommunikationstechnologie (IKT) hervorgerufene organisatorische Wandel betrifft vor allem die Alltagsprozesse der beteiligten Akteure [Sc04, S. 54]. Um diese, durch die flächendeckende Einführung der eGK induzierte sektor- und institutionsübergreifende Nutzung der vernetzten Informationstechnologien sicher und zuverlässig bereitstellen zu können und eine breite Akzeptanz durch die Patienten zu unterstützen, muss gewährleistet werden, dass Integrität, Verfügbarkeit und Vertraulichkeit der sensiblen medizinischen Daten in der Telematik-Infrastruktur gegeben sind. Darüber hinaus kann aus der Nutzung der Telematik-Infrastruktur, der dafür vorgesehenen Karten (eGK/HBA) und der Verwendungsprozesse um diese Techniklösungen eine Vielzahl an Sicherheitsbedrohungen mit unterschiedlichsten Gefahrenpotenzialen resultieren. Solche Bedrohungen können dabei auch direkt das menschliche Leben betreffen [He06]. Die Gewährleistung des Schutzes der personenbezogenen Gesundheitsinformationen sowie der Gesundheitsinformationssysteme spielt damit eine zentrale Rolle. Weiterhin ist es rechtlich erforderlich, aktuelle Datenschutz- und Datensicherheitsdienste zu berücksichtigen [BP05].

2 Problemstellung

Die Einführung der neuen elektronischen Gesundheitskarte erfolgt, aufgrund der Komplexität und des Umfangs des weltweit größten Telematik-Projektes, in mehreren Schritten [GE05]. Nach den gesetzlich vorgeschriebenen und angesetzten Labortests wird die Einführung der elektronischen Gesundheitskarte in ausgewählten Testregionen¹ erprobt. Anschließend soll die eGK schrittweise flächendeckend eingeführt werden.

Die Umsetzung dieser gesetzlichen Vorgaben findet in Bayern in der Test- und Modellregion Ingolstadt statt. Die in dieser Testregion realisierten Sicherheitsmaßnahmen gilt es nun zu überprüfen. Dadurch soll mehr Transparenz für die Anwender geschaffen werden. Weiterhin sollen sicherheitstechnische Fragen und Unsicherheiten von Seiten der Nutzer (sowohl Patienten als auch Leistungserbringer) beantwortet werden. Unter Berücksichtigung der spezifischen Situation im Testgebiet gilt es außerdem festzustellen, inwiefern die in den bisherigen Spezifikationen festgelegten Sicherheitsanforderungen ausreichend und praktisch umsetzbar sind. Folgende Kernfragestellungen sind dementsprechend mit diesem Sicherheitsevaluationsvorhaben zu adressieren:

- Welche Eigenschaften der zentralen technischen, organisatorischen und ökonomischen Kriterien können für eine derartige Sicherheitsanalyse identifiziert werden?
- Wie können Sicherheitsanforderungen des Telematikpilotprojektes erkannt und in der Modellregion Ingolstadt nutzergruppenspezifisch (Patienten, Leistungserbringer, Kostenträger) systematisiert werden?
- Wie können die definierten Sicherheitsanforderungen in der Testregion Ingolstadt umgesetzt werden? Wie ist die dafür notwendige Prozessreorganisation in der Modellregion zu gestalten?
- Wie kann die Verteilung der analysierten Sicherheitsanforderungen auf die verschiedenen Teilkomponenten der Gesundheitstelematikinfrastruktur im Raum Ingolstadt definiert werden? Wie wird die soziotechnische und ökonomische Vorteilhaftigkeit von Sicherheitskonzepten abgeschätzt?

In den bisherigen gematik²-Spezifikationen wurde das Thema „Sicherheit rund um die eGK“ praktisch nur aus technischer Umsetzungssicht betrachtet. Eine Sicherheitsanalyse der durch die Einführung der eGK erzwungenen Prozessreorganisation wäre jedoch notwendig, um die aufgeworfenen und offenen Fragestellungen beantworten zu können und somit mögliche Schwachstellen bereits während der Testphase aufzudecken.

¹ Flensburg, Bochum-Essen, Trier, Heilbronn, Wolfsburg, Löbau-Zittau, Ingolstadt.

² Die Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH wurde von der Bundesregierung mit der Organisation und Umsetzung der Einführung der eGK in Deutschland beauftragt.

Die möglichen Sicherheitslücken könnten dadurch vor der flächendeckenden Einführung der eGK wissenschaftlich abgeschätzt und evtl. gegebene Behebungsvorschläge würden rechtzeitig deutlich gemacht werden.

3 Vorschlag für eine entwicklungsbegleitende formative Sicherheitsevaluation

Die Sicherheitsevaluation des Telematikpilotprojektes zur elektronischen Gesundheitskarte im Raum Ingolstadt wird vom Munich Competence Center eHealth (MCCeH³) begleitet.

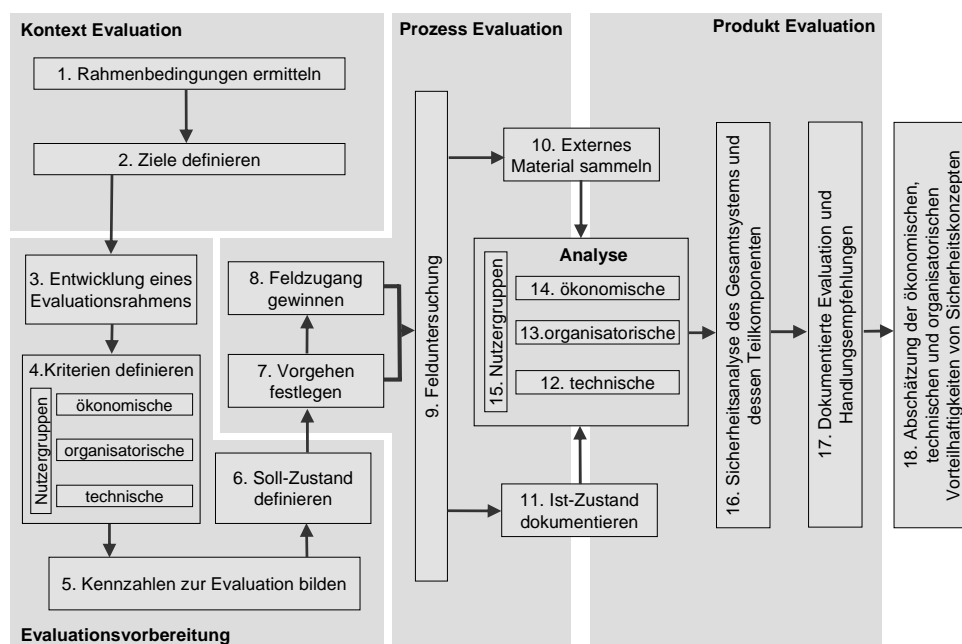


Abbildung 1: Vorgehensvorschlag zur formativen Sicherheitsevaluation

Um die in Abschnitt 2 genannten Kernfragen intersubjektiv nachvollziehbar beantworten zu können, bedarf es eines adäquaten Vorgehensmodells. Dieses wird im Folgenden beschrieben und ist in Abbildung 1 dargestellt. Das Vorgehen umfasst dabei die Definition und Entwicklung der technischen, organisatorischen und ökonomischen Kriterien. Durch eine nutzergruppenspezifische Aufteilung der vordefinierten Kriterien kann das Evaluationsvorgehen entwicklungsbegleitend durchgeführt und somit von Anfang an in der Testregion kommuniziert werden, um die Ergebnisse in die Weiterentwicklung der Lösung einfließen zu lassen.

³ <http://mccch.in.tum.de/home>

Das Evaluationsvorhaben gliedert sich in die vier Oberbereiche Kontext, Vorbereitung, Prozess und Produkt. Das entsprechende Vorgehensmodell ist sequentiell in dieser Reihenfolge aufgebaut. Die einzelnen Evaluationsschritte werden in den folgenden Abschnitten detailliert beschrieben.

3.1 Kontext

Um ein derartiges entwicklungsbegleitendes, formatives Sicherheitsevaluationsvorhaben durchführen zu können, bedarf es einer grundlegenden Einarbeitung in die Kontextproblematik. Dazu werden im ersten Schritt die für die Test- und Modellregion Ingolstadt spezifischen Rahmenbedingungen ermittelt. Diese beinhalten sowohl technische als auch organisatorische, wirtschaftliche und politische Fragestellungen wie z.B.: Probleme bei der Umsetzbarkeit der erforderlichen Maßnahmen, der finanzielle Rahmen und die entstehenden Kosten, Handhabbarkeit der Lösung, gesetzliche Bestimmungen, begrenzte Verfügbarkeit der relevanten Informationen. Aus diesen werden die Ziele für das Sicherheitsevaluationsvorhaben abgeleitet wie z. B.: technische, organisatorische und ökonomische Bewertung von Sicherheitsmaßnahmen in der Testregion, Bewertung der Nutzbarkeit und Bedienbarkeit der elektronischen Gesundheitskarte bzw. des Heilberufsausweises von Seiten aller Projektbeteiligten (Leistungsnehmer und Leistungserbringer), Analyse der Performanz der Prozesse rund um die Karten eGK/HBA. Die allgemeine Aufgabenstellung der Überprüfung der getroffenen Sicherheitsmaßnahmen aus Anwendersicht gliedert sich dabei in mehrere Unterziele mit unterschiedlichen Prioritäten und Aufwandvorgaben. Diese werden im Laufe der Evaluation verfeinert und den Gegebenheiten nach priorisiert.

3.2 Vorbereitung

Die Evaluationsvorbereitung fokussiert die Bestimmung eines systematischen und intersubjektiv nachvollziehbaren Ablaufes der Evaluation. Nach der Entwicklung des Evaluationsrahmens (Abbildung 1) folgt die Ausarbeitung der Evaluationskriterien. Diese werden in zentrale technische, organisatorische und ökonomische Sicherheitsanforderungen unterteilt und der jeweiligen Nutzergruppensicht (Leistungsempfänger, Leistungserbringer, Kostenträger) zugeordnet. Die Ausformulierung dieser Kriterien (z. B. Verteilung der Sicherheitsanforderungen auf die Teilkomponenten des Systems, zuständige Verantwortlichkeit, Komplexität und die daraus resultierenden Problemstellungen, jeweilige Schutzziele der unterschiedlichen Funktionalitäten aus der Anwendersicht) bildet die Basis für die Überprüfung der Sicherheitsmaßnahmen rund um die eGK. Dieser Überprüfung liegen die Verifikation und Einhaltung der genannten Sicherheitsanforderungen zugrunde. Das Ausarbeiten der Evaluationskennzahlen (Mess- und Vergleichsgrößen) und die Definition sowie Modellierung des zukünftigen Soll-Zustandes (Prozess- und Ablauffestlegung hinsichtlich eGK/HBA-Handling durch alle Beteiligten) schließt die Evaluationsvorbereitung ab.

3.3 Evaluationsprozess

Zur Vorbereitung des Evaluationsprozesses wird ein Erhebungsplan zur Felddatensammlung für die anstehende Sicherheitsanalyse des Pilotprojektes erarbeitet. Die Ausarbeitung des Erhebungsplans findet erst während der Gewinnung des Feldzuganges statt und ist deswegen nicht in der Vorbereitungsphase platziert. So wird ein geeigneter Feldzugang bestimmt, um die teilnehmende Beobachtung in der Testregion und die Einarbeitung in die Organisationsstruktur des Telematikpilotprojektes ermöglichen zu können. Die Untersuchung der Sicherheitsmaßnahmen im Feld erfordert sowohl die Dokumentation der im Feld erhobenen Daten als auch das Sammeln des externen Materials (parallele und weiterführende Literaturrecherche -> flächendeckende Einführung der eGK in weiteren Testregionen). Das in Erfahrung gebrachte Wissen wird als Ist-Zustand betrachtet und mit dem zuvor erarbeiteten Soll-Zustand verglichen.

3.4 Evaluationsprodukt

Die Beschreibung der gewonnenen Sicherheitsanforderungen im Anwendungsfeld Ingolstadt aus technischer, ökonomischer und organisatorischer Sicht bildet ein Teilprodukt der Sicherheitsanalyse. Aus der Überprüfung der vordefinierten Kriterien und Sicherheitsanforderungen lässt sich die Verteilung dieser auf die verschiedenen Teilkomponenten des zu untersuchenden Telematikpilotprojektes ableiten. Damit soll auch die sozio-technische und ökonomische Vorteilhaftigkeit von Sicherheitskonzepten abgeschätzt werden, um für alle Beteiligten eine Transparenz der Sicherheitsthematiken zu erhalten. Diese und weitere Erkenntnisse (wie z.B. Nutzungspotenziale der Karten eGK/HBA) können offene Fragen beantworten und somit zur Akzeptanz der neuen Technologie bei den Anwendern beitragen.

4 Verwandte Arbeiten und die Vorteile der vorgestellten Lösung

Die Arbeit basiert auf einer durchgeführten Literaturrecherche (u.a. in folgenden Fachzeitschriften: Computers & Security, Information Management & Computer Security, Information Systems Security, International Journal of Medical Informatics, Information Systems Journal, European Journal of Information Systems, International Journal of Information Security, security & privacy, Journal of computer security, ACM Transaction on Information and Systems Security und ACM Computing Surveys). Die Vorstellung und Abgrenzung aller untersuchten Sicherheitsevaluationsmethoden (Sicherheitsanalyse- und -bewertung) würde den Rahmen dieser Arbeit sprengen. Deshalb wird auf die Arbeiten von [Si05; DB01, Ba93, ES00] verwiesen, die alle das Ziel einer Klassifikation von Methoden im Bereich der IT-Sicherheit verfolgen.

Von allen anderen Sicherheitsevaluationsansätzen unterscheidet sich der hier vorgestellte Ansatz vor allem in folgenden Punkten: Fokus (Domäne Gesundheitswesen; technische, organisatorische und ökonomische Bewertung der Sicherheitsanforderungen und deren Umsetzung), Vollständigkeit (Berücksichtigung aller früheren Arbeiten und Konsolidierung dieser), Aktualität (Einsetzung modernster Erkenntnisse aus dem Gebiet der sozio-technischen Sicherheit), regionale Bestimmungen (Standort Deutschland, politische und regionale Rahmenbedingungen).

5 Zusammenfassung und Ausblick

Die Komplexität des Projektes zur Einführung der elektronischen Gesundheitskarte erfordert besondere Maßnahmen zur Erfolgssicherung, um Investitionen zu schützen. Dabei besitzt insbesondere die Akzeptanz des Systems durch die Nutzer, d.h. das medizinische und pflegerische Personal sowie Patienten, eine wesentliche Rolle. Ein bedeutender Aspekt für diese Akzeptanz ist die Bewertung von Sicherheitsmaßnahmen. Um die geplanten Eigenschaften der Telematik-Infrastruktur bewerten und ggf. vor der flächendeckenden Einführung der eGK entsprechende Veränderungen vornehmen zu können, ist ein intersubjektiv nachvollziehbares Vorgehen zur Evaluation der Sicherheitseigenschaften erforderlich. Denn nur somit lassen sich mögliche Fehler frühzeitig erkennen und die Ergebnisse der Sicherheitsevaluation zu der Verbesserung der eGK-Prozesse rechtzeitig allen Beteiligten kommunizieren. Dazu wurde in dem vorliegenden Beitrag eine Methode entwickelt, die einen Vergleich des Ist-Zustandes in der Testregion Ingolstadt mit dem erhobenen Soll-Zustand erlaubt. Ergebnisse der Evaluation können bei ihrer Berücksichtigung in der flächendeckenden eGK-Einführung Investitionen schützen. Dieses Vorgehen wird nun in der Testregion Ingolstadt erprobt und weiterentwickelt. Wir hoffen, zum Zeitpunkt der Konferenz über erste Erfahrungswerte berichten zu können.

Literaturverzeichnis

- [Ba93] Baskerville, R.: Information Systems Security Design Methods: Implications for Information Systems Development. In: ACM Computing Surveys, Vol. 25 Nr. 4, 376-414, 1993.
- [BP97] Roland Berger & Partner GmbH – International Management Consultants. Telematik im Gesundheitswesen: Perspektiven der Telemedizin in Deutschland. München: Im Auftrag des Bundesministeriums für Bildung, Wissenschaft, Forschung und Technologie und in Zusammenarbeit mit dem Bundesministerium für Gesundheit, 1997
- [BP05] Blobel, B.; Pharow, P.: Datensicherheit in medizinischen Informationssystemen und Gesundheitsnetzen,. Handbuch der medizinischen Informatik, Hanser Fachbuchverlag, 2005.
- [DB01] Dhillon, G.; Backhouse, J.: Current directions in IS security research: towards socio-organizational perspectives. Information Systems Journal, 11, 127–153, 2001.
- [ES00] Eloff, M.M.; von Solms, S.H.: Information Security Management: A Hierarchical Framework for Various Approaches. In: Computers & Security, Vol. 19 Nr. 3, 243-256, 2000.
- [GE05] Gesetzentwurf der Fraktionen SPD und BÜNDNIS 90/DIE GRÜNEN. Entwurf eines Gesetzes zur Organisationsstruktur der Telematik im Gesundheitswesen (Drucksache 15/4924), 2005.
- [He06] Heeks, R.: Health information systems: Failure, success and improvisation. International Journal of Medical Informatics, 75, 125—137, 2006.
- [Sc04] Schneier, B.: Secrets and Lies - Digital Security in a Networked World, Wiley, 2004.
- [Si05] Siponen, M.T.: An analysis of the traditional IS security approaches: implications for research and practice. European Journal of Information Systems (14), 303-315, 1005.