# Informationssicherheit im Krankenhaus – eine prozessorientierte Analyse der Patientendaten

Roland Gabriel[1], Alexander Wagner,[2] Thomas Lux[3]

[1]Lehrstuhl für Wirtschaftsinformatik, Ruhr-Universität Bochum, 44801 Bochum
[2,3]Competence Center eHealth Ruhr, Universitätsstr. 150, 44801 Bochum
[1]rgabriel@winf.rub.de
[2]awagner@winf.rub.de, [3]thomas.lux@rub.de

**Abstract:** Mit zunehmender Digitalisierung und Vernetzung im Gesundheitswesen und insbesondere im Krankenhaus rückt die Frage der Informationssicherheit der Daten, und damit insbesondere der Patientendaten, immer mehr in den Vordergrund. Dabei fehlen in diesem Bereich geeignete Konzepte, IT-sicherheitsorientierte Anforderungen in eine prozessorientierten (Daten)Sicht zu integrieren. Im Rahmen eines Projektes wurde aufgezeigt, wie die geschäftsprozessorientierte Risikoidentifikation als ein Teil des Risikomanagementprozesses in die Ablauforganisation zu integrieren ist. Die bereits vorhandenen Prozessmodelle konnten um Informationen zur Datensicherheit und zum Datenschutz der verarbeiteten Informationen erweitert werden, um daraus geeignete IT-Sicherheitsmaßnahmen bzw. Schutzklassen abzuleiten.

## 1 Informationssicherheit im Gesundheitswesen

Die Notwendigkeit, Informationswerte vor Bedrohungen und Schwachstellen zu schützen, wird mit dem wachsenden Grad der Vernetzung und Digitalisierung in und außerhalb von Organisationen immer dringender. Gesundheitsorganisationen bleiben von dieser Entwicklung nicht verschont, sondern werden aufgrund der hier verarbeiteten Daten bzw. Informationen die Folgen dieser Veränderungen sogar noch stärker zu spüren bekommen als Unternehmen oder Behörden. Zum einen sind Gesundheitsorganisationen starken finanziellen Zwängen ausgesetzt, was die Durchführung angemessener Maßnahmen im Hinblick auf Informationssicherheit zumindest erschwert, zum anderen arbeiten Gesundheitsorganisationen in einer Umgebung, die einen vollständigen Ausschluss der Öffentlichkeit unmöglich macht [OV03]. Weiterhin nimmt die Notwendigkeit zur elektronischen Verarbeitung und Analyse der Daten immer mehr zu, sowohl für die Unterstützung der Prozesse (klinische Behandlungspfade), als auch als Steuerungswerkzeug für das Management. Daher ist die Berücksichtigung der Datensicherheit sowie des Datenschutzes und insbesondere der speziellen Regelungen für den Gesundheitsbereich zwingend erforderlich. Aktuelle Erhebungen zeigen, dass insbesondere im Krankenhausbereich die Informationssicherheit nur unzureichende Berücksichtigung findet und nicht an die technologischen Änderungen angepasst wird [LW10].

Die Vielfältigkeit der Formen – z. B. Papier, elektronische Dokumente, Filme, Röntgenbilder – in denen Informationen im Gesundheitsbereich vorhanden sind und die Vielzahl von Übertragungswegen – z. B. Post, elektronische Übertragung, Gespräche – erhöhen ebenfalls die Anzahl der möglichen Bedrohungen und Schwachstellen und erschweren somit einen angemessenen Schutz von Informationen. [OV02] Wesentliche grundlegende Norm der Informationssicherheit im Gesundheitswesen bilden die ISO/IEC 27000er Reihe. Ein besonderes Augenmerk gilt dabei der ISO 27799 Norm. Diese seit kurzem für die medizinische Informatik eingeführte Norm konkretisiert den Leitfaden für das Informationssicherheits-Management der ISO/IEC 27002 Norm in Bezug auf die Anforderungen im Gesundheitswesen.

## 2 Informationssicherheits-Managementsystem (ISMS) im Krankenhaus

Das Informationssicherheits-Managementsystem (ISMS) basiert auf der ISO/IEC 27001 und ist „Teil des gesamten Managementsystems, der auf der Basis eines Geschäftsrisikoansatzes die Entwicklung, Implementierung, Durchführung, Überwachung, Überprüfung, Instandhaltung und Verbesserung der Informationssicherheit abdeckt. Das Managementsystem enthält die Struktur, Grundsätze, Planungsaktivitäten, Verantwortung, Praktiken, Verfahren, Prozesse und Ressourcen der Organisation.“ [OV01].

Im Laufe der Zeit können sich die Sicherheitsanforderungen, die Geschäftsprozesse[1] sowie die Größe und Struktur einer Organisation ändern. Aus diesem Grund darf das ISMS nicht als eine bloße (statische) Abarbeitung einer Checkliste verstanden werden, wie es leider oftmals der Fall ist. Damit eine ständige Kontrolle und Verbesserung möglich ist, muss auf alle Prozesse eines ISMS ein Zyklus angewandt werden. Einen solchen Zyklus beschreibt das „Plan-Do-Check-Act“ (PDCA) – Modell, dessen Darstellung in Form eines Zyklus möglich ist, entsprechend den Darstellungen in den Normen ISO 27799 und ISO/IEC 27001 [KRS03]. Dabei werden die Anforderungen und Erwartungen an die Informationssicherheit durch die vier Phasen „Planen“, „Ausführen“, „Überprüfen“ und „Handeln“ in die verwaltete Informationssicherheit transformiert. Dabei eignet sich die prozessorientierte Perspektive, ausgehend von den verarbeiteten Daten, z.B. entlang des Behandlungsprozesses eines Patienten.

[1] In der Praxis beschränkt sich die Auseinandersetzung mit Informationssicherheit oft auf die einmalige Absicherung von IT-Komponenten gegen Bedrohungen. Die Geschäftsprozesse werden oft gar nicht oder nur unzureichend in die Analyse der Informationssicherheit einbezogen. Der vorgeschlagene Ansatz stellt daher die Geschäftsprozesse einer Gesundheitsorganisation in den Vordergrund und lässt auch die Auswirkungen von Sicherheitsvorfällen auf die Geschäftsprozesse nicht außer Acht.

# 3 Prozessorientierte Analyse der Informationssicherheit im Krankenhaus

Für die Analyse und Darstellung von (Geschäfts-) Prozessen in der Unternehmung steht eine Menge unterschiedlicher Notationen und auch Modellierungswerkzeuge zur Verfügung. Als Quasi-Standard, welcher sowohl die Vorgehensweise als auch das Software-Werkzeug miteinander verbindet, konnte sich das ARIS-Toolset der IDS Scheer etablieren. Insbesondere das Konzept der Ereignisgesteuerten Prozesskette (EPK) ist eine sehr verbreitete Notation zur Darstellung von Unternehmensabläufen. Aber auch andere Modelltypen wie z. B. Wertschöpfungskettendiagramme oder Leistungsbäume können hier zur Darstellung von Prozessen genutzt werden. Nachfolgende Abbildung visualisiert exemplarisch am Beispiel eines Medikationsprozesses im Krankenhaus die Notation einer EPK.

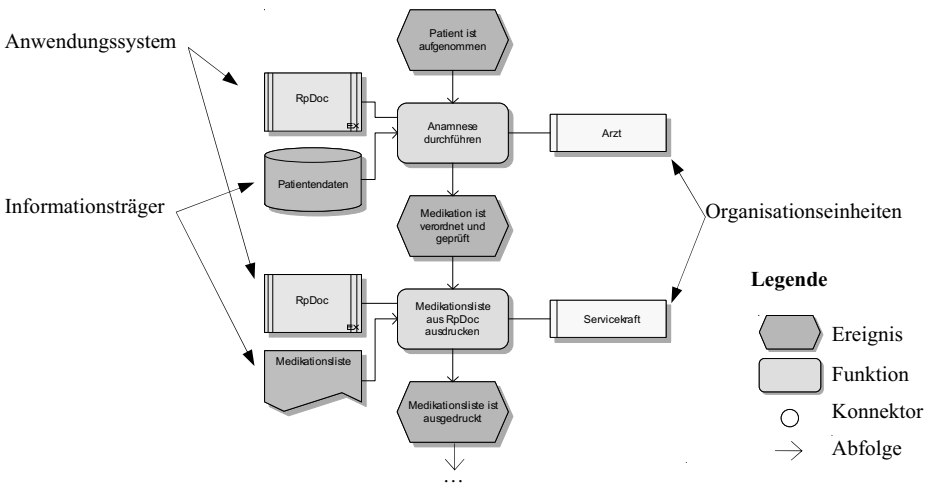


Abbildung 1: Darstellung einer Ereignisgesteuerten Prozesskette am Beispiel eines Medikationsprozesses in einem analysierten Krankenhaus

Wie Abbildung 1 verdeutlicht, besteht das grundlegende Ziel der prozessorientierten Darstellung darin, den sachlich-logischen Ablauf sowie die notwendigen Ressourcen und auch Informationen bzw. Daten darzustellen.

Die Beziehung zwischen Informationssicherheit und Geschäftsprozessorientierung kann auf unterschiedlichen Ebenen dargestellt werden. So kann das **Sicherheitsmanagement** selbst als Geschäftsprozess betrachtet werden, mit allen notwendigen Tätigkeiten und Aufgaben wie strategisches Sicherheitsmanagement, Risikomanagement und Entwicklung bzw. Einsatz von Sicherheitsmaßnahmen. Das Sicherheitsmanagement ist damit selbst Betrachtungsgegenstand der prozessorientierten Perspektive. [Ko01]

Weiterhin kann die prozessorientierte Analyse und Gestaltung um **sicherheitsorientierte Analyse- und Betr achtungsbereiche** erweitert werden. Damit erfolgt eine Ergänzung der prozessorientierten Sichtweise um Sicherheitsziele. Diese sind dann sowohl bei der Analyse als auch bei der Gestaltung von Geschäftsprozessen zu berücksichtigen. [Ko01]

Über die reine Analyse und Gestaltung hinaus besteht die Möglichkeit, Risiken der Informationsverarbeitung im Rahmen der **Geschäftsprozessmodellierung** zu identifizieren. Dazu erfolgt zunächst die Identifikation der Informationswerte[2]. Dazu ist die Betrachtung aller im Prozessablauf verarbeiteten Informationen notwendig sowie die Feststellung des **Wertes** bzw. des **Schutzbedarfes** der Informationen. [SN02] Anschließend sind mögliche **Bedrohungen** bzw. **Schwachstellen** für die Sicherheit dieser Informationen zu identifizieren und zu dokumentieren[3]. [KRS03]

Die nachfolgende Abbildung zeigt auf, wie aus Sicht der Informationssicherheit die Betrachtung des bereits in Abbildung 1 dargestellten Geschäftsprozesses möglich ist.

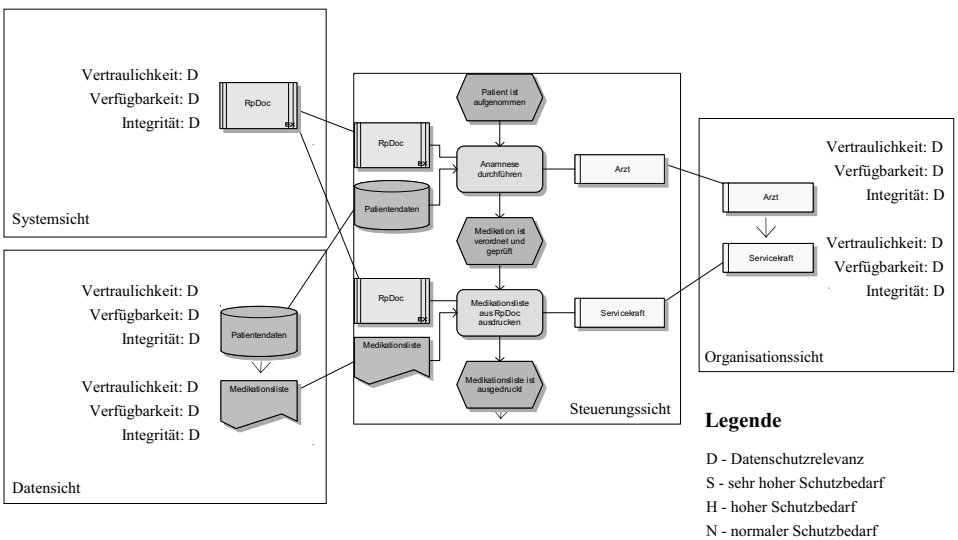


Abbildung 2: Sichten der Informationssicherheit auf den untersuchten Medikationsprozess – Darstellung der festgelegten Sicherheitsziele für die identifizierten Informationswerte

[2] Unter Informationswerten werden hierbei alle Werte verstanden die entweder selbst Informationen darstellen oder in irgendeiner Weise mit der Verarbeitung von Informationen zu tun haben. Es reicht hier also bei weitem nicht, nur die IT-Komponenten in den Analysebereich einzubeziehen.

[3] Die relevanten Bedrohungen und Schwachstellen müssen von einer Gesundheitsorganisation vorher in Form einer Liste erfasst werden. Hierbei ist es außerordentlich wichtig, dass diese Listen regelmäßig aktualisiert werden.

# 4 Analyse der Informationssicherheit des Medikationsprozesses

In der Steuerungssicht werden zunächst die Informationswerte identifiziert und den entsprechenden Sichten (z. B. Systemsicht, Datensicht, Organisationssicht) zugeordnet. In den einzelnen Sichten lassen sich anschließend die Abhängigkeiten zwischen den einzelnen Informationswerten modellieren.

Im nächsten Schritt erfolgt auf der strategischen Ebene die Festlegung der strategischen Sicherheitsziele unter Berücksichtigung der allgemeinen Organisationsziele. Zum Beispiel muss, ohne das Ziel der Kostensenkung aus den Augen zu verlieren, ein sehr hoher Schutz von personenbezogenen Daten und des Patienten gewährleistet sein. Wie in Abbildung 2 dargestellt, ist es mit Hilfe der strategischen Sicherheitsziele möglich, über die Geschäftsprozessebene, Sicherheitsziele für die einzelnen Informationswerte abzuleiten und zu konkretisieren [Ko01]. In dem dargestellten Ausschnitt eines real erfassten Medikationsprozesses werden ausschließlich personenbezogene Daten verarbeitet. Im Hinblick auf die Vorgaben der Geschäftsleitung des Krankenhauses bezüglich der strategischen Sicherheitsziele wurde in diesem Beispiel für alle Sicherheitsziele die Datenschutzrelevanz angenommen.

Sobald die Sicherheitsziele für jeden einzelnen Informationswert festgestellt wurden, erfolgt im nächsten Schritt die Analyse der Informationswerte im Hinblick auf die vorhandenen Schwachstellen und die darauf wirkenden Bedrohungen. Die identifizierten Schwachstellen und Bedrohungen werden in den – dafür bereitgestellten – Attributen der Informationswerte dokumentiert[4] (vgl. Abbildung 3).

Auf der Grundlage der Dokumentation bezüglich Sicherheitsziele, Schwachstellen und Bedrohungen ist es abschließend möglich, eine Einschätzung der möglichen Schäden hinsichtlich der Sicherheitsziele (z. B. Vertraulichkeit, Verfügbarkeit, Integrität) durchzuführen[5].


Abbildung 3: Exemplarische Erfassung der Attribute der Attributtypgruppe „Sicherheitsziele“ für den Informationswert „Medikationsliste“

[4] Die für einen Informationswert relevanten Bedrohungs- und Schwachstellentypen werden den bereits erwähnten Listen entnommen.
[5] Die Schäden ergeben sich dabei als mögliche Kombinationen von bereits für einen Informationswert erfasste Bedrohungen und Schwachstellen.

Die Abbildung 3 veranschaulicht die mögliche Strukturierung der Attribute in den speziell für dieses Vorhaben erstellten Attributtypgruppen: Sicherheitsziele, Bedrohungstypen, Schwachstellentypen und Schäden.

## 5 Zusammenfassung und Ausblick

In dem vorliegenden Beitrag zeigt die Vorgehensweise im Rahmen eines Projektes zur Analyse der Informationssicherheit auf. Dabei wurde der Medikationsprozess im Krankenhausbereich betrachtet. Die Ausrichtung der Vorgehensweise an den Geschäftsprozessen und die systematische Anreicherung dieser mit Informationen über Sicherheitsziele, Bedrohungen und Schwachstellen lassen eine sorgfältige Identifikation von möglichen Schäden der Informationswerte zu und bilden eine solide Basis für die anschließende Risikobewertung. Insbesondere bietet der Ansatz den Vorteil, unterschiedliche Aspekte des gleichen Prozesses (z.B. Sachlogik des Prozessablaufes, Kosten, Zeit, Medikationssicherheit und Informationssicherheit) in einem Modell aufzuzeigen.

Weitergehender Forschungsbedarf in diesem Bereich besteht z.B. in der Fragestellung, wie die im Rahmen der Risikoidentifikation und der Risikoeinschätzung gewonnenen Informationen über mögliche Schäden der Informationswerte für die anschließende Risikobewertung (z. B. mit der CRAMM-Methode) aufbereitet werden müssen.

## Literaturverzeichnis


[Ko01] Konrad, Peter (1998): Geschäftsprozessorientierte Simulation der Informationssicherheit, Entwicklung und empirische Evaluierung eines Systems zur Unterstützung des Sicherheitsmanagements, Wirtschaftsinformatik, Bd. 20, Josef Eul Verlag, Lohmar/Köln 1998.

[KRS03] Kersten, Heinrich; Reuter, Jürgen; Schröder, Klaus-Werner (2008): IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz, Der Weg zur Zertifizierung, 1. Aufl., Vieweg, Wiesbaden 2008.

[LW10] Lux, Thomas; Wagner, Alexander: Informationssicherheit im Gesundheitswesen – Eine prozessorientierte Analyse, Competence Center eHealth Ruhr, Bochum 2010.

[OV01] DIN ISO/IEC 27001:2008-09: Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen, Deutsches Institut für Normung, Beuth, Berlin 2008.

[OV02] DIN ISO/IEC 27002:2008-09: Informationstechnik – IT-Sicherheitsverfahren – Leitfaden für das Informationssicherheits-Management, Deutsches Institut für Normung, Beuth, Berlin 2008.

[OV03] DIN EN ISO 27799:2008-10: Medizinische Informatik – Sicherheitsmanagement im Gesundheitswesen bei Verwendung der ISO/IEC 27002, Deutsches Institut für Normung, Beuth, Berlin 2008.

[SN02] Sitzberger, Sabrina; Nowey, Thomas (2006): Lernen vom Business Engineering – Ansätze für ein systematisches, modellgestütztes Vorgehensmodell zum Sicherheitsmanagement, http://www-sec.uni-regensburg.de/publ/2006/SN2006MKWI2006BE.pdf, 20.08.2009, abgerufen am 21.08.2009.