FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

Exemplarische Sicherheitsanalyse und Sicherheitsanforderungen an eine Arztpraxis in Deutschland

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur/in

im Rahmen des Studiums

Wirtschaftsinformatik

eingereicht von

Markus Freudenthaler
Matrikelnummer 0525525

an der
Fakultät für Informatik der Technischen Universität Wien

Betreuung
Betreuer/in: Thomas Grechenig

Wien, 21. Dezember 2010 _____ _____
(Unterschrift Verfasser/in) (Unterschrift Betreuer/in)

Forschungsgruppe Industrial Software
Institut für Rechnergestützte Automation
der Fakultät für Informatik
der Technischen Universität Wien

Diplomarbeit

Exemplarische Sicherheitsanalyse und Sicherheitsanforderungen an eine Arztpraxis in Deutschland

Autor:
Markus Freudenthaler, BSc.
Neubaugasse 17-19/2/5 1070 Wien

Betreuer:
Thomas Grechenig

Wien, 21. Dezember 2010

Eidesstattliche Erklärung

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Wien, 21. Dezember 2010

Inhaltsverzeichnis

Abkürzungsverzeichnis

BS	Betriebssystem
BSI	Bundesamt für Sicherheit in der Informationstechnik
eGK	Elektronische Gesundheitskarte
EHIC	Europäische Gesundheitskarte
GS-Tool	Grundschutz-Tool
GSHB	Grundschutzhandbuch
HBA	Heilberufsausweis
HCA	Gesundheitsanwendung
IT	Informationstechnologie
KVK	Krankenversicherungskarte
MBO	Muster Berufsordnung für die deutschen Ärztinnen und Ärzte
OCR	Optische Zeichenerkennung
PKI	Public Key Infrastruktur
PVS	Praxisverwaltungssystem
RVO	Röntgenverordnung
TI	Telematikinfrastruktur
TSP	Vertrauenswürdiger Zertifizierungsdiensteanbieter
VDE	Verband für Elektrotechnik, Elektronik und Informationstechnik
VSD	Versicherungsstammdaten
ZKA	Zentraler Kreditausschuss

Zusammenfassung

Im Jahre 2003 hat die Deutsche Bundesregierung den Entschluss zur Einführung einer bundesweiten elektronischen Gesundheitskarte getätigt. Diese ist eine Chipkarte, die als Nachfolger für die bis dato übliche Krankenversicherungskarte geplant war. Neben ihrer Eigenschaft als elektronischer Ausweis bietet die eGK noch weitere Funktionalitäten an. Eine beispielhafte Funktionalität ist jene, dass auf freiwilliger Basis sensible Gesundheitsdaten, wie etwa Allergien, Arzneimittelunverträglichkeiten und chronische Vorerkrankungen, auf dem Chip gespeichert werden können. So werden einerseits Vorteile und neue Möglichkeiten für den Patienten geschaffen, andererseits gilt es auch Risiken des unberechtigten Zugriffs auf diese Daten zu minimieren und dem Datenschutz wird somit eine besondere Bedeutung zugewiesen.

Diese Diplomarbeit hat das Ziel, geeignete Sicherheitsanforderungen an eine Arztpraxis auf der Basis der eGK Architektur zu ermitteln. Zu Beginn werden die nötigen Grundlagen erläutert. Schwerpunkte bilden hier zum einen die einzelnen Komponenten der Telematikinfrastruktur und zum anderen die IT-Sicherheit im Allgemeinen. Anschließend wird eine Musterpraxis im Umfeld der eGK definiert und mögliche Sicherheitsbedrohungen erläutert. Anhand dieser Bedrohungen erfolgt die Ermittlung der einzelnen Sicherheitsanforderungen und der resultierenden technischen und organisatorischen Lösungen.

Abstract

In the year 2003, the German Federal Government made the decision to establish a nationwide electronic health card. This chip card was planed to be the successor of the health insurance card used until then. Aside from her characteristic as an electronic identification card, the eGK offers a lot more functionalities. An example can be the functionallity to store sensitive health data on a voluntary basis, such as allergy, drug intolerance and chronic pre-existing conditions, on the chip. On one side, advantages and new possibilities for the patients are created, on the other side, it is important to minimize the risks of unauthorised access to this data. That way, the data protection becomes especially important.

This diploma thesis aspires to develop appropriate safety requirements for a medical practice based on the architecture of the eGK. At the beginning, the necessary basic principles are defined. On one hand, the main points are the particular components of electronic data transmission infrastructure and on the other hand, it is important not to forged about IT-security in general. Afterwards, an example for a medical practice in the environment of the eGK will be defined as well as possible safety risks will be explained. With the help of the definition of these risks, the particular safety requirements and the resulting technical and organizational solutions will be determined.

Danksagung

Zuerst gilt mein Dank all jenen Personen, die diese Diplomarbeit ermöglicht haben. Besonders möchte ich hierbei bei meinem Betreuerteam: Univ.Prof. DI Dr. Thomas Grechenig und Dipl.-Ing. Florian Fankhauser, für ihre Unterstützung und Betreuung danken.

Eine weitere Stütze während meines gesamten Studiums war meine Familie. Durch ihre Unterstützung ist es möglich gewesen, dieses Studium zu absolvieren. Auch gaben sie mir in den letzten Jahren immer wieder Motivation, das Studium zu Ende zu bringen. Vielen Dank.

Zuletzt gilt mein Dank meinen Studienkollegen. Während des gesamten Studiums haben wir uns immer gegenseitig zu Höchstleistungen motivieren können. Gemeinsam war das Studium eine lehrreiche und vor allem sehr schöne Zeit an der Universität. Besonders hervorzuheben möchte ich hierbei die Studienkollegen und mittlerweile Freunde, Michael Krieber, Daniel Teuffenbach und Roland Ladengruber. Vielen Dank.

Kapitel 1

Einleitung

Informations- und Kommunikationstechnologien verbreiten sich gerade im medizinischen Bereich immer mehr. Hochsensible Daten werden elektronisch erfasst und weiterverarbeitet. Durch diese Maßnahmen kann das Gesundheitswesen effizienter und somit zufriedenstellender für die Patienten arbeiten.

Durch immer wiederkehrende Nachrichten über Datendiebstähle bei anerkannten Unternehmen (Beispielsweise Deutsche Telekom [Spi]) wird den Bürgern immer deutlicher bewusst, welche Daten die Unternehmen über sie sammeln und auswerten. Die Zahl jener, die sich über ihre eigene Privatsphäre Sorgen machen, steigt, wobei dies auch eine Generationsfrage ist: Die jüngeren Generationen wachsen in einer offenen Umgebung auf und sind daran gewöhnt, keine Privatsphäre zu erwarten. Somit schwinden die Erwartungen immer mehr. [Sch10]

Trotz dieser Tatsache ist es im medizinischen Umfeld, wo höchst sensible, personenbezogene Daten verarbeitet und gespeichert werden, wichtig, dass das Vertrauen der Menschen in die Datensicherheit gewährleistet ist.[EMC] Der Schutz dieser Daten umfasst Sicherheitsmaßnahmen, die sicherstellen sollen, dass Informationen

- nicht verloren gehen
- nicht ausspioniert werden
- nicht verfälscht werden
- in einer entsprechenden Qualität verfügbar sind

Der Gesetzgeber hat zum Schutze dieser Daten geeignete Bestimmungen erlassen und in verschiedene Gesetzbücher niedergeschrieben. Zentrale Rollen spielen hierbei besonders das Strafgesetzbuch und das Bundesdatenschutzgesetz. Zudem unterliegen viele Handlungen der beruflichen bzw. der ärztlichen Schweigepflicht (Patientengeheimnis[1]), soweit die Verarbei-

[1] STGB § 203 Abs. 1 [Bune]

tung bei den Leistungserbringern erfolgt. Weiters handelt es sich dabei um eine *besondere Art personenbezogener Daten*[2], deren Verarbeitung strengen rechtlichen Anforderungen unterliegt[3]. [Wei04] Eine nähere Begutachtung der rechtlichen Aspekte erfolgt gesondert im Kapitel 3.8.

Für die Telematikinfrastruktur (TI) ist in Deutschland die gematik verantwortlich. Die gematik hat unter anderem die Aufgabe die Telematikinfrastruktur zu planen und geeignete Sicherheitsmaßnahmen zu spezifizieren, dass der IT-Sicherheit genüge geleistet wird. [DMHB07]

Bei dieser Konzeption sind vielfältige Aspekte zu berücksichtigen. Hauptschwierigkeit stellt hierbei die sehr große Komplexität des Systems dar, in dem alle Informationen zur rechten Zeit, schnell und unkompliziert am richtigen Ort abrufbar sein sollen und sicherheitsrelevante Aspekte dabei nicht vernachlässigt werden dürfen. Diese Konzeption und Integration in bestehende Systeme ist dementsprechend sehr ressourcen- und zeitaufwendig. Aufgrund dieser Faktoren ist es zudem sehr schwierig ein standardisiertes Datenschutzkonzept zu entwickeln und bis dato hat sich deswegen auch noch keines etabliert. Trotz dieser Tatsache erarbeiten einzelne Hersteller, Verbände und Organisationen eigene Standards. Beispielsweise hat der Verband für Elektrotechnik, Elektronik und Informationstechnik (VDE) ein Sicherheits- und Qualitätsmanagement-System für die Telemedizin erarbeitet. Das VDE Prüf- und Zertifizierungsinstitut zeichnet damit Telemedizin-Zentren nach den harmonisierten Normen ISO/IEC 9001 aus. [Hei08]

Diese Diplomarbeit beschäftigt sich primär mit Sicherheitsanforderungen, die an eine Arztpraxis in Deutschland gestellt werden, wobei zwei unterschiedliche Sichtweisen speziell behandelt werden. Einerseits werden alle einschlägigen Komponenten im Umfeld der Arztpraxis näher erläutert und sicherheitskritische Aspekte aufgezeigt. Andererseits wird das praxisnahe Umfeld in einer Arztpraxis analysiert und erläutert, welche exemplarische Schutzmaßnahmen in einer Arztpraxis umgesetzt werden können, um den Schutz von hochsensiblen Daten sicherzustellen.

1.1 Zielsetzung

Fachliches Ziel dieser Arbeit ist es, eine gute Basisliteratur bezüglich möglicher Sicherheitsbedrohungen im Umfeld einer Arztpraxis in Deutschland aufzuzeigen und gleichzeitig, exemplarische Sicherheitslösungen zu beschreiben. Anhand dieser soll die Möglichkeit geschaffen werden, die sicherheitsrelevanten Aspekte objektiv und fachlich zu verstehen. Konkret soll in dieser Diplomarbeit die Frage beantwortet werden, wie eine Arztpraxis dabei helfen kann, die Sicherheit der Patientendaten zu gewährleisten oder ggf. zu

[2]BDSG § 3 Abs. 9 [Bunb]
[3]BDSG § 28 Abs. 6-9 [Bunb]

erhöhen. Für diesen Zweck werden exemplarisch organisatorische und technische Lösungen beschrieben.

1.2 Aufbau der Arbeit

Diese Diplomarbeit ist in sieben Kapitel unterteilt. In den ersten zwei Kapiteln erhält der Leser einen Gesamtüberblick über die Arbeit und im folgenden wird die Deutsche- Elektronische Gesundheitskarte erläutert. Das dritte Kapitel widmet sich den fachlichen Grundlagen. Speziell gilt es im diesem Kapitel, fachliches Wissen aufzubauen und beispielsweise die Grundlagen eines Telematiksystems darzulegen. Im Zuge dessen wird aber auch die IT-Sicherheit im Allgemeinen und der rechtliche Rahmen behandelt. Ab den vierten bis sechsten Kapitel wird das praxisnahe Umfeld einer Arztpraxis analysiert, dessen Charakteristika, Sicherheitsbedrohungen und -anforderungen exemplarisch erläutert und näher beschrieben. Im letzten Kapitel folgt eine Zusammenfassung der wichtigsten Punkte, wobei hier besonders auf wichtige Erkenntnisse hingewiesen wird.

Kapitel 2

Die Deutsche- Elektronische Gesundheitskarte

Die elektronische Gesundheitskarte ist das derzeit mit Abstand größte E-Ausweisprojekt in Deutschland. Mittelpunkt und Namensgeber dieses Vorhabens ist eine Smartcard, die an alle Krankenversicherten Deutschlands ausgegeben werden soll [Sch09]

Ausweise im Gesundheitswesen sind durchaus üblich. Seit dem 19. Jahrhundert werden Ausweise im Gesundheitswesen eingesetzt, aber im Gegensatz zu heute waren diese nur für das medizinische Personal vorgesehen. [Goe07] In Deutschland begann das Zeitalter der elektronischen Ausweise im Jahre 1994. Der Verband der deutschen Krankenversicherungen einigte sich damals auf eine Karte, die den Namen Krankenversicherungskarte (KVK) trug. Das Ziel der KVK war, den damals üblichen Krankenschein abzulösen. [Sch09] International gesehen nimmt ist die europäische Gesundheitskarte (EHIC) eine bedeutende Rolle im europäischen Raum ein. Sie ist im Gesundheitswesen eine der wenigen international gültigen Dokumente. Seit dem 1. Juni 2004 ist es mit dieser möglich, medizinische Leistungen während des Urlaubes im europäischen Wirtschaftsraum in Anspruch zu nehmen. Die EHIC ist im Grunde genommen kein elektronischer Ausweis, da sie sich nicht zur Identifizierung von Personen nutzen lässt. Sie dient rein als Beleg, dass der Inhaber eine Krankenversicherung abgeschlossen hat und auch für die Kosten aufkommt. Deswegen nutzen viele Staaten die Rückseite ihrer Ausweise, um die EHIC aufzubringen. [WRCB06] Ende der neunziger Jahre kamen in Deutschland erstmals konkrete Pläne auf, die Krankenversichertenkarte durch einen leistungsfähigen elektronischen Ausweis zu ersetzen. 2003 startete das Bundesgesundheitsministerium ein Projekt, das dieses Vorhaben in die Praxis umsetzen sollte. Die neue Karte wurde elektronische Gesundheitskarte (eGK) getauft und sollte innerhalb einiger Jahre an die Stelle der Krankenversichertenkarte treten. Anders als bei der Krankenver-

sichertenkarte beteiligen sich an der elektronischen Gesundheitskarte auch die privaten Krankenversicherungen, weshalb auch deren Kunden eine Karte erhalten werden. [Sch09] Der breiten Öffentlichkeit wurde die eGK erstmals, von der damaligen Bundesgesundheitsministerin Ulla Schmidt, im Rahmen der CeBit im Jahre 2004 vorgestellt. Das erklärte Ziel der eGK war die Behandlungsqualität entscheidend zu verbessern und gleichzeitig die Kosten für die Behandlung zu senken. [KLK06]

Oberflächlich gesehen ist das Gesundheitssystem in Deutschland technologisch hoch entwickelt. Für Diagnostik, Behandlungen und Therapien stehen modernste Einrichtungen und Geräte zur Verfügung, welche durch moderne Datenverarbeitungsprogramme in ihrer Qualität und Effektivität unterstützt und in ihrer Leistungsfähigkeit erweitert werden. Defizite gibt es im Bereich der Kommunikation und Informationsverarbeitung. Dieser Bereich liegt derzeit weit hinter den modernen technischen Möglichkeiten zurück. Das Gesundheitswesen ist in Deutschland bislang noch überwiegend geprägt durch das Arbeiten mit Papier. Beispielsweise nehme man nur Rezepte, Rechnungen, Arztbriefe oder Patientenakten. Dieser Umstand verursacht an vielen Stellen Doppelarbeiten, Fehler und Kosten. Zwar gibt es auch moderne Kommunikations- und Datenverarbeitungsverfahren, doch werden diese nur selten Einrichtungsübergreifend genutzt, da die dafür notwendige Kompatibilität fehlt. [Del08] Daraus folgt, dass die informationstechnische Grenze regelmäßig dort beginnt, wo die eigene Einrichtung Betriebswirtschaftlich aufhört. [BDHM07]

Ein weitere Aspekt für die Einführung der elektronischen Gesundheitskarte ist jener, dass durch den Einsatz moderner Telematik die Behandlungsqualität deutlich verbessert werden kann. Die Qualität der Versorgung ist hierzulande nicht mehr allein abhängig von dem Können des behandelnden Arztes oder von den technischen Möglichkeiten, sondern hängt auch entscheidend davon ab, wie schnell, zuverlässig und sicher geeignete Informationen vorliegen und zwischen unterschiedlichsten Akteuren ausgetauscht werden kann. [Del08] In der Bundesrepublik Deutschland besteht deswegen zu Recht die weit verbreitete Überzeugung, dass Telematik die Qualität und Wirtschaftlichkeit der medizinischen Versorgung und Gesundheitsverwaltung steigern kann. [Han08]

Wenn man den internationalen Vergleich nicht scheut, ist die Senkung der Bahandlungskosten auch dringend notwendig. Die folgende Abbildung 2.1 zeigt einen internationalen Vergleich der Ausgaben für Gesundheitssysteme pro Kopf in den Mitgliedstaaten der OECD[1].

[1] Organisation für wirtschaftliche Zusammenarbeit und Entwicklung

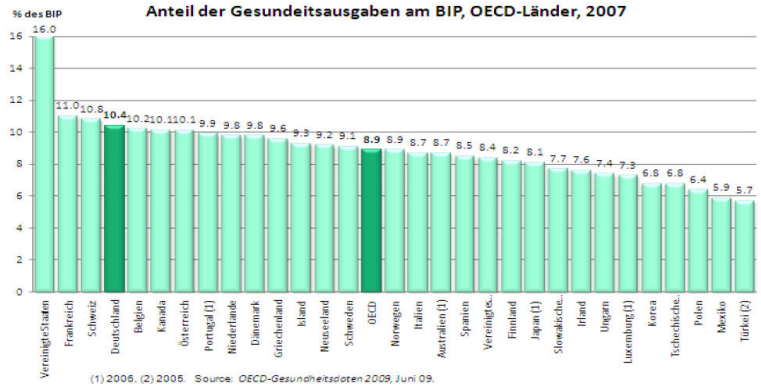

Abbildung 2.1: Vergleich der Ausgaben für Gesundheitssysteme pro Kopf in den Mitgliedstaaten der OECD [Org]

Nach der Abbildung 2.1 gab Deutschland im Jahre 2009 10,4 % des Bruttoinlandsproduktes für Gesundheitsausgaben aus. Dies ist um 1,5 % mehr als der Durchnitt der OECD Länder. [KLK06]

Im Jahre 2003 ermittelte das Bundesgesundheitsministerium im Rahmen einer Ausschreibung eine Reihe von Anbieter, die für die Umsetzung der elektronischen Gesundheitskarte verantwortlich sein sollten. Diese Firmen schlossen sich im Konsortium bIT4health (better IT for better health) zusammen. Im Jahr 2005 wurde zudem die Firma gematik gegründet, die die Koordination des Projekts übernahm. Die Gesellschafter der Gematik sind die Spitzenverbände des deutschen Gesundheitswesens, wobei sowohl die Leistungserbringer (Ärzte, Apotheker, Krankenhäuser usw...) als auch die Kostenträger (gesetzliche und private Krankenversicherungen) vertreten sind. [Sch09] Die gematik hat unter anderem die Aufgabe die Telematikinfrastruktur zu planen und geeignete Sicherheitsmaßnahmen zu spezifizieren, dass der IT-Sicherheit genüge geleistet wird. Im Zuge dessen hat diese Spezifikationen für Komponenten der Telematikinfrastruktur publiziert, die die Beteiligten der TI zwingend zum Betrieb einsetzen müssen. [DMHB07] Eine nähere Beschreibung erfolgt dazu im Abschnitt 3.3.1

Äußerlich ähnelt die elektronische Gesundheitskarte der Krankenversichertenkarte. Auf der Rückseite ist die europäische Krankenversicherungskarte (EHIC) abgebildet. Im Gegensatz zur Krankenversichertenkarte ist auf der elektronischen Gesundheitskarte ein Passfoto aufgedruckt, was den Missbrauch erschweren soll. Technisch speichert die elektronische Gesundheitskarte zwar wichtige Daten in einem eigenen Chip, jedoch der wichtigere Anwendungsbereich ist der Zugriff auf Online-Angebote, für die Ärzte und Patienten ihre Karten nutzen können. [Sch09] Das Gesetz[2] unterscheidet

[2]SGB V § 291a [Bund]

hinsichtlich der Funktionen der neuen eGK zwischen Pflichtanwendungen und freiwilligen Anwendungen. [Ron] Die folgende Tabelle 2.1 gibt einen Überblick über die einzelnen Anwendungen.

Anwendung	Typ	Beschreibung
Datenverwaltung	P	Verarbeitung administrativer Daten (insbesondere Name, Geburtsdatum, Anschrift, Versicherungsstatus, Krankenkasse, Krankenversicherungsnummer)
Berechtigungsnachweis	P	Berechtigungsnachweise zur Inanspruchnahme von Leistungen im europäischen Ausland.
Elektronisches Rezept	P	Elektronisches Rezept (vom Arzt an Stelle des Papierrezeptes zur Verfügung gestelltes elektronisches Rezept, auf das der Apotheker mit seinem Heilberufsausweis und der eGK zugreifen kann)
Arzneimittel-dokumentation	F	Dokumentation der ärztlich verordneten Medikamente und der rezeptfrei in der Apotheke erworbenen Medikamente für die Durchführung einer Therapiesicherheitsprüfung beim Arzt oder bei der Ausgabe eines Medikaments durch den Apotheker des Papierrezeptes zur Verfügung gestelltes
Notfalldaten	F	Speicherung von Notfalldaten wie: Allergien, individuelle Risiken, Arzneimittelunverträglichkeiten, chronische Vorerkrankungen etc.
Elektronischer Arztbrief	F	Dient zur elektronischen Übermittlung von Überweisungen im ambulanten Bereich und ist eine Information für den Arzt der die Behandlung übernimmt.
Elektronische Patientenakte	F	Dient zur elektronischen Speicherung der Patientenakte in der Telematikinfrastruktur
Patientenfach	F	Vom Versicherten eingerichtetes Patientenfach, das vom Versicherten in eigener Verantwortung genutzt werden kann.
Elektronische Patientenquittung	F	Elektronische Patientenquittung zur Information des Versicherten über die abgerechneten Leistungen und deren vorläufige Kosten.

Tabelle 2.1: eGK Anwendungen nach [Ron]

Wie in der Tabelle 2.1 ersichtlich werden neun unterschiedliche Anwendungen im Rahmen der eGK unterschieden. Die Unterscheidung ob es sich hierbei um eine Pflichtanwendung oder um eine freiwillige Anwendung handelt erfolgt in der Der Spalte „Typ“ ´. („P“ Pflichtanwendungen, „F“ Freiwillige Anwendungen) Insgesamt werden laut Gesetzt[3] nur drei verpflichtende Anwendungen vorgeschrieben. Die restlichen Anwendungen sind alle freiwillig und können je nach Bedarf genutzt werden. [Ron] Der Erfolg oder Misserfolg der eGK lässt sich somit ableiten, in wie weit die freiwilligen Anwendungen auch benutzt werden. Ausschlaggebend wird sein, in wie fern eine Akzeptanz des Einsatzes von Informationstechnologie im Gesundheitswesen existiert. [Sch]

Hinter der Einführung der eGK stehen also der Gedanke und das Ziel, eine elektronische Vernetzung der im Gesundheitswesen beteiligten Personen und Organisationen zu schaffen. Sie ist somit das wichtigste Projekt zur Modernisierung des deutschen Gesundheitswesens. Mit ihrer Hilfe sollen Kosten auf administrativen Seite verringert, der Missbrauch von Versichertendaten unterbunden, bzw. die Behandlungsqualität verbessert werden. Darüber hinaus soll den Versicherten bzw. Patienten zukünftig die Möglichkeit geboten werden, stärker als bislang in das Behandlungsgeschehen einbezogen zu werden. [Del08]

Im folgenden Kapitel wird nun gezielt auf die IT-Sicherheit eingegangen und die Komponenten der Telematikinfrastruktur beschrieben bzw. analysiert.

[3]SGB V § 291a [Bund]

Kapitel 3

Grundlagen der IT - Sicherheit im Umfeld einer Arztpraxis

Das fachliche Ziel dieses Kapitels besteht darin, dem Leser ein grundlegendes Wissen und Verständnis für die Materie Informationstechnologie (IT) zu geben und die Grundlage für ein Verständnis von Zusammenhängen der einzelnen Komponenten in der Telematikinfrastruktur zu schaffen. Dabei gilt es anfangs, einige Begriffe zu definieren und genauer zu erläutern. In den darauf folgenden Abschnitten werden die grundlegenden Komponenten der Telematikinfrastruktur der eGK näher untersucht und jeweils genau definiert, ebenso werden Schwachstellen oder Probleme aufgezeigt. Speziell werden folgende Komponenten des Systems näher erläutert:

- Telematikinfrastruktur
- Primärsystem
- Konnektor
- Kartenterminal
- Smartcard
- eGK

Im letzten Punkt des Kapitels wird der rechtliche Rahmen in Deutschland begutachtet und die vom Staat gegebenen Möglichkeiten und Rahmenbedingungen dargestellt. Von besonderem Interesse werden personenbezoge- und medizinisch relevante Daten sein.

3.1 IT - Sicherheit

Das mobile Büro ist aus der Wirtschaftswelt nicht mehr wegzudenken und auch im privaten Bereich wollen immer mehr Personen jederzeit auf ihre Dateien zugreifen können. Basis dessen sind immer IT-Systeme, die die gespeicherten Daten verwalten und deren Verfügbarkeit sicherstellen. Ein funktionierendes IT-Sicherheitssystem muss hierbei eine zentrale Rolle einnehmen. Doch so gut dieses auch ist, stellen die eigenen Mitarbeiter eine nicht zu unterschätzende Gefahr dar.[Uns07] Beispielsweise zeigt eine vom Institut Insight Express durchgeführte Studie auf, dass rund 22 Prozent der Telearbeiter von Unternehmen die bereitgestellte IT-Infrastruktur unbekannten Personen zur Verfügung stellen. [Len06]
Aus diesem Beispiel ist schön ersichtlich, dass die IT-Sicherheit nicht alleine einem Produkt- oder Serviceproblem zuzuordnen ist. Stattdessen ist hierbei besonders das Management gefordert, eine unternehmensweite IT-Sicherheitsstrategie zu entwickeln und diese den eigenen Mitarbeitern zu vermitteln. Zusätzlich ist es von Nöten die eigenen Mitarbeiter bei Bedarf zu schulen, strategische Partner auszuwählen und eine geeignete IT-Sicherheitspolitik im Unternehmen einzuführen. Geeignete Messinstrumente müssen dauerhaft die Wirksamkeit der eingesetzten Lösungen überwachen und frühzeitig mögliche Schwachstellen im IT-System ausfindig machen. [Opp07]

Auch muss das mögliche IT-Sicherheitsrisiko eingestuft werden. Unter einem IT-Sicherheitsrisiko versteht man die Unfähigkeit, anforderungsgerechte IT-Leistungen effektiv und effizient mit zugrundeliegenden, korrekten Daten erbringen zu können. IT-Leistungen sind dabei der Betrieb und die Entwicklung von Systemlösungen, das Projektmanagement sowie das Management dieser Leistungen und die Beratung der Geschäftsbereiche für deren Geschäftstätigkeit. [Sei06] Bei wirtschaftlichen Aktivitäten werden die meisten Entscheidungen mit einen gewissen Restrisiko getroffen, da sie stets zukunftsorientiert, geprägt von Unsicherheit, Unbestimmtheit und Unvollständigkeit und nicht eindeutig vorhersehbar sind. Genau das trifft auch auf die IT zu. Die erste Aufgabe besteht darin, Werte im IT-System festzustellen. Der international am häufigsten eingesetzte Standard zur IT-Sicherheit ISO/IEC 17799, definiert einen Wert als „anything that has a value to the organization“. [Hei07] Sind nun die Werte in einem IT-System definiert, gilt es, mögliche Gefahren für diese Werte zu eruieren. Laut [HP03] wird grundsätzlich zwischen zwei Gefährdungen unterschieden.

- Angriff
- Störung

Im Falle Störung wird im Gegensatz zu einem Angriff davon ausgegan-

gen, dass diese nicht unter Vorsatz ausgeübt wird. Dieser groben Gruppierung folgend, wurde in weitere Kategorien untergegliedert. Die Abbildung 3.1 zeigt die vollständige Kategorisierung:

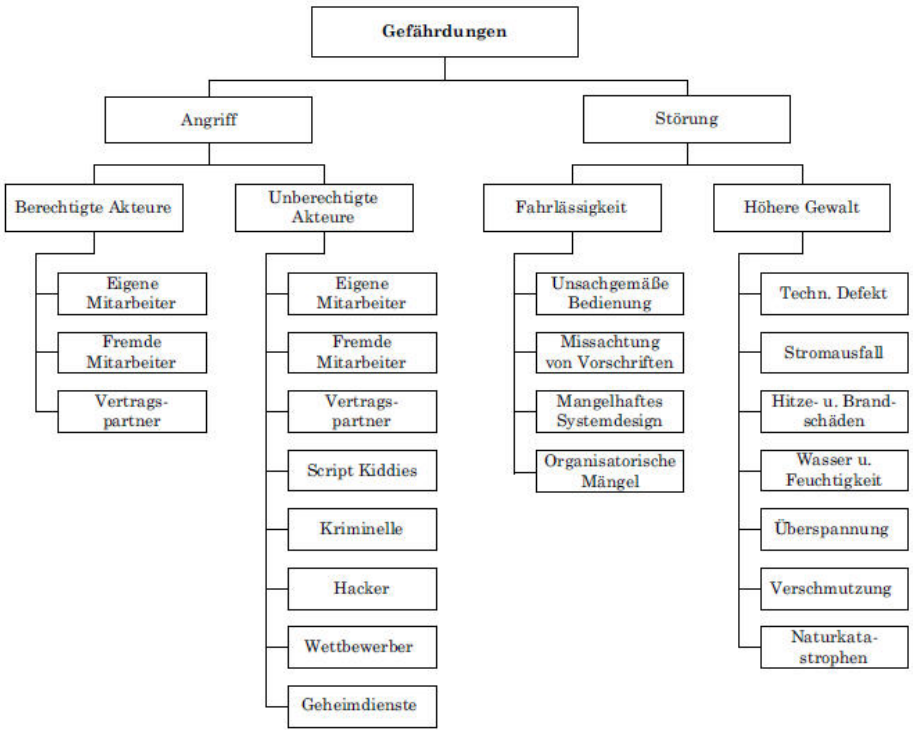

Abbildung 3.1: Überblick über potenzielle Gefährdungen [HP03]

Wie in Abbildung 3.1 ersichtlich, wird bei einem Angriff weiter unterschieden, ob es sich dabei um berechtigte oder um nichtberechtigte Akteure gehandelt hat. Weiters gilt zu beachten, dass das Gefahrenpotenzial von Gruppe zu Gruppe stark variiert. Beispielsweise stellen Script Kiddies im Vergleich zu versierten Hackern eine viel kleinere Bedrohung dar, da sie vorgefertigte Software, z.B. Rootkits, Viren, Trojaner, etc., nutzen oder nach im Internet verfügbaren Anleitungen für Angriffe vorgehen und über keine herausragenden Programmierfähigkeiten oder Netzwerkkenntnisse verfügen. [Hei07] Im Gegensatz dazu können versierte Hacker selbst in gesicherte Netzwerke eindringen und so eine tatsächliche Bedrohung darstellen. Geheimdienste sind durch ihre sehr großen technischen, finanziellen wie auch materiellen Ressourcen eine große Bedrohung. [Hei07]
Bei einer Störung wird währenddessen zwischen einer fahrlässigen und einer durch höhere Gewalt verursachten Störung unterschieden. Als höhere Gewalt werden Ereignisse bezeichnet, die nicht im eigenen Einflussbereich stehen. Zu diesen gehören beispielsweise Naturkatastrophen oder Stromausfälle, unter

Fahrlässigkeiten werden Ereignisse eingeordnet, die durch die eigenen Nutzer des Systems ausgelöst werden und die zugleich eine schadhafte Auswirkung auf das IT-System darstellen.

Ist man sich über die potentiellen Gefahren und Risiken im Klaren, kann mit der Planung eines IT-Systems begonnen werden. Ein funktionierendes IT-System stellt die Grundlage vieler wirtschaftlicher Unternehmungen dar. Beispielsweise im Finanzwesen hätte ein Tag ohne ein funktionierendes oder oder mit einem fehlerhaften IT-System sehr ernste wirtschaftliche Konsequenzen. Beispielsweise können geringe geringe Zeitvorsprünge darüber entscheiden, ob man Millionen verliert oder gewinnt. Folgende Abbildung 3.2 veranschaulicht, welche Kosten Unternehmen entstehen, wenn alleine die IT für eine Stunde ausfällt.

Brokerage operations	$6,450,000
Credit card authorization	$2,600,000
Ebay	$225,000
Amazon.com	$180,000
Package shipping services	$150,000
Home shopping channel	$113,000
Catalog sales center	$90,000
Airline reservation center	$89,000
Cellular service activation	$41,000
On-line network fees	$25,000
ATM service fees	$14,000

Abbildung 3.2: Kosten eine Stunde IT Ausfall [Pat02]

Die Abbildung 3.2 veranschaulicht sehr deutlich, wie wertvoll eine funktionierende IT für ein Unternehmen ist. Je nachdem, wie stark das zu Grunde liegende Geschäftsmodell auf der IT basiert, fallen die Kosten höher oder niedriger aus.

In besonders sicherheitskritischen Bereichen, wie z.B. in der Medizin, stellen Patientendaten einen großen Wert dar. Hinsichtlich dieses Wertes müssen diese auch entsprechend gesetzlicher Bestimmungen beschützt und gespeichert werden. Die gespeicherten Daten werden hierbei von zwei unterschiedlichen Sichtweisen beschützt: [Wit08]

- Schutz der (gespeicherten) Daten und ihrer Verarbeitung
  vor unerwünschtem Zugriff (vor allem im Sinne von zweckwidrigem Missbrauch) oder Verlust oder

- Schutz des Bürgers vor unerwünschten Folgen (insbesondere durch

zweckwidrigen Missbrauch) aufgrund des Zugriffs auf (gespeicherte) Daten bzw. des ungewollten Datenverlusts.

Wobei die erste Sichtweise, Daten sind vorhanden und werden gespeichert, zwingend für die zweite Betrachtungsweise erforderlich ist. Diese ist auch jene, die die meisten Personen in unmittelbaren Zusammenhang mit Datensicherheit bringen.[Wit08] Zusätzlich müssen die Daten gemäß der geltenden Ziele der Daten- und Informationssicherheit geschützt werden. Als Ziele der Daten- und Informationssicherheit gelten folgende: [Bun08]

- Vertraulichkeit
- Integrität
- Verfügbarkeit

Diese frei Ziele wurden vom Bundesamt für Sicherheit in der Informationstechnik (BSI) definiert und gelten als allgemeine Ziele der Daten- und Informationssicherheit. Je nach Anwendungsfall macht es aber durchaus Sinn, diese Ziele zu erweitern. Im Rahmen der Telematikinfrastruktur wurden deswegen diese durch die Ziele *Authentizität* und *Nichtabstreitbarkeit* ergänzt. Aus fachlicher Sicht besteht darüber hinaus ein Anspruch auf die Validität der verarbeiteten Daten. Die *Validität* erhobener beziehungsweise verarbeiteter Daten muss aber im Gegensatz zu den restlichen Zielen im Rahmen der Fachanwendungen bearbeitet werden und stellt keinen sicherheitstechnischen Aspekt dar. [gem08b]

Nachfolgend werden die einzelnen Punkte speziell beschrieben und gleichzeitig auch auf die Auswirkungen auf das IT-System der eGK eingegangen. Folgend wird auch jedes Ziel in Schutzbedarfsklassen eingeteilt. Diese bestimmt, welcher Schutz für die Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist. Da der Schutzbedarf meist nicht genau quantifizierbar ist, hat sich eine Unterteilung in vier Schutzbedarfskategorien bewährt. [Hae04]

- Niedrig:
  Schadensauswirkungen sind nicht zu erwarten.
- Normal:
  Schadensauswirkungen sind überschaubar und begrenzt.
- Hoch:
  Schadensauswirkungen können ein beträchtliches Ausmaß erreichen.
- Sehr Hoch:
  Schadensauswirkungen können ein katastrophales und existentiell bedrohliches Ausmaß annehmen.

Im Rahmen der Schutzbedarfsfeststellung nach BSI wird dieser Schutzbedarf zuerst je Anwendung und in weiterer Folge pro IT-System festgestellt. Der Schutzbedarf der einzelnen Anwendungen vererbt sich auf den Schutzbedarf des IT-Systems. Da diesen meist mehrere Anwendungen beeinflussen unterscheidet man folgende Fälle: [Bun08]

- Maximumprinzip:
  Der höchste Schutzbedarf einer einzelnen Anwendung wird übernommen.

- Kumulationseffekt:
  Der Schutzbedarf kann höher ausfallen als jene der einzelnen Anwendungen. Dies ist beispielsweise bei einem Server der Fall, wenn auf ihm mehrere Anwendungen mit niedrigerem Schutzbedarf in Betrieb sind.

- Verteilungseffekt:
  Wenn die einzelnen Anwendungen auf verschiedene IT-Systeme verteilt sind, kann der Gesamtschutzbedarf niedriger sein als der Schutzbedarf der einzelnen Anwendungen.

Je nach Anwendungsfall muss das richtige Verfahren angewendet werden, um den Schutzbedarf des IT-Systems zu bestimmen. Weiters wird in weiterer Folge für die Qualität der Verarbeitungsprozesse der Begriff Prozessqualität verwendet. Dieser ist informelle Festlegung eines Qualitätsmerkmales des Verarbeitungsprozesses. [gem08c]

Unter *Vertraulichkeit* versteht man jenen Zustand eines Systems, wenn dieses keine unautorisierte Informationsgewinnung ermöglicht. Gerade im medizinischen Bereich ist es notwendig, dass Patientendaten, Rezepte und ähnlich hoch sensible Daten vor unautorisiertem Zugriff geschützt sind. Um genau eben diese Vertraulichkeit in einem IT-System zu gewährleisten, sind genaue Festlegungen von Zugriffsberechtigungen erforderlich. Das Ziel dieser Maßnahme besteht darin, dass nur berechtigte Personen auf die Daten Zugriff erhalten. Ein weiteres Problem stellt in diesem Zusammenhang die Interferenz-Kontrolle dar. Unter diesem Begriff wird die Möglichkeit verstanden, dass man aus der Kenntnis von Einzelinformationen weitere Informationen ableitet. Das Problem in dieser technischen Lösung besteht nun darin, dass unter Umständen die abgeleitete Informationen aufgrund von Zugriffsbeschränkungen gar nicht verfügbar sein dürfen und so mit den festgelegten Zugriffsberechtigungen kollidieren. Charakterisierend für diese Problemkomponente sind jegliche Datenbankabfragen, die besonders im Business Intelligence Bereich häufig eingesetzt werden. [Eck04]
Folgende Tabelle 3.1 gibt einen Überblick über die einzelnen Schutzbedarfsklassen des Schutzziels Vertraulichkeit und deren Anforderung auf die Prozessqualität im System der Gesundheitstelematik. Daten jeglicher Art werden folgend als „Informationsobjekte“ bezeichnet.

Schutzbedarf	Prozessqualität
Niedrig	Der Zugriff ist durch einfache, zweckmäßige Verfahren eingeschränkt.
Mittel	Informationsobjekte dieser Schutzbedarfskategorie sind vor unberechtigtem Zugriff durch Verschlüsselungsverfahren geschützt. Der Zugriff auf ein Informationsobjekt dieser Schutzbedarfskategorie ist nur nach einer Autorisierung entsprechend eines Verfahrens der Prozessqualität „Benutzername und Passwort“ möglich.
Hoch	Informationsobjekte dieser Schutzbedarfskategorie sind vor unberechtigtem Zugriff durch Verschlüsselungsverfahren geschützt. Der Zugriff auf ein Informationsobjekt dieser Schutzbedarfskategorie ist nur nach einer Autorisierung entsprechend eines Verfahrens der Prozessqualität wie z. B. „Zertifikat und Passwort“ möglich. Der Besitzer der Daten muss den Zugriff auf diese Daten durch explizite Zustimmung freigeben.
Sehr Hoch	Informationsobjekte dieser Schutzbedarfskategorie sind vor unberechtigtem Zugriff durch starke Verschlüsselungsverfahren geschützt. Der Zugriff auf ein Informationsobjekt dieser Schutzbedarfskategorie ist nur nach einer Autorisierung entsprechend eines Verfahrens der Prozessqualität „Zertifikat und Passwort“ möglich. Der Besitzer der Daten muss den Zugriff durch explizite Zustimmung freigeben.

Tabelle 3.1: Schutzbedarsklassen: Vertraulichkeit [gem08b]

Unter *Integrität* versteht man jenen Zustand eines Systems, wenn dieses Subjekten nicht ermöglicht, die zu schützenden Daten unautorisiert und unbemerkt zu manipulieren. Die Datenintegrität beschäftigt sich nun mit Maßnahmen, damit existierende Daten nicht durch unberechtigten Zugriff manipuliert werden. [Eck04]
Bezug nehmend auf die Telematikinfrastruktur verlangt das Sicherheitskonzept für die TI, dass die Integrität der erhobenen, verarbeiteten, transportierten und gespeicherten Daten gewährleistet sein muss. Die Daten dürfen nicht unbemerkt manipuliert werden. Ihre Korrektheit, Echtheit und Vollständigkeit ist für den Behandlungserfolg außerordentlich wichtig. [gem08a]
Im Bezug auf medikamentöse Verschreibungen und Dosierungshinweise ist hier im medizinischen Bereich besondere Vorsicht geboten.
Folgende Tabelle 3.2 gibt einen Überblick über die einzelnen Schutzbedarfs-

klassen des Schutzziels Integrität und deren Anforderung auf die Prozessqualität im System der Gesundheitstelematik.

Schutzbedarf	Prozessqualität
Niedrig	Integritätsprüfung erfolgt nach Ermessen, Integritätsverletzungen können nicht eindeutig und zweifelsfrei erkannt werden.
Mittel	Integritätsprüfung erfolgt nach Ermessen, Integritätsverletzung ist erkennbar, deren Verursacher sind nicht ermittelbar.
Hoch	Integritätsprüfung erfolgt an allen relevanten Prozessschritten, Integritätsverletzung ist erkennbar, deren Verursacher ist nicht immer ermittelbar.
Sehr Hoch	Integritätsprüfung erfolgt an allen relevanten Prozessschritten, Integritätsverletzung ist erkennbar, deren Verursacher ist immer ermittelbar.

Tabelle 3.2: Schutzbedarsklassen: Integrität [gem08b]

Unter *Verfügbarkeit* versteht man jenen Zustand eines Systems, wenn dieses gewährleistet, dass authentifizierte und autorisierte Subjekte in der Wahrnehmung ihrer Berechtigungen nicht beeinträchtigt werden können. Besonders im praktischen Einsatz kann es vielerorts zu solchen Problemen kommen, speziell, wenn mehrere Prozesse oder Personen auf dieselbe Ressource zugreifen möchten. Demzufolge zählt die Datenverfügbarkeit auch zu den Zielen der Daten- und Informationssicherheit. Zur Prävention werden meist technische Hilfsmittel verwendet. Besonders wird hierzu auf Maßnahmen zurückgegriffen, die die Nutzung von Systemressourcen wie beispielsweise CPU-Zeit oder Speicher reglementieren. [Eck04]
Bezug nehmend auf die Telematikinfrastruktur verlangt das Sicherheitskonzept der TI, dass die Daten eines Versicherten immer zeitnah zur Verfügung stehen müssen. [gem08a] Bei der elektronischen Verordnung ist zudem gefordert, dass die Daten auch offline zur Verfügung stehen müssen. [gem09b] Nicht oder nicht rechtzeitig zur Verfügung stehende Daten können zur Handlungsunfähigkeit bzw. zu einem zu späten Handeln oder Behandlungsfehlern des Mediziners führen und u.U. lebensbedrohende Folgen für den Patienten haben. [BWB+02]
Folgende Tabelle 3.3 gibt einen Überblick über die einzelnen Schutzbedarfsklassen des Schutzziels Verfügbarkeit und deren Anforderung auf die Prozessqualität im System der Gesundheitstelematik für die zentralen Komponenten. Der Wiederherstellungszeitraum beschreibt dabei die maximale Dauer der Unterbrechung der Verfügbarkeit aufgrund einer dedizierten Ursache. Die geforderte Verfügbarkeit wird prozentuell im Verhältnis zur konkreten zeitlichen Verfügbarkeit innerhalb der Servicezeiten und Betriebszei-

ten angegeben und ist in der folgenden Tabelle 3.3 als Zuverlässigkeit zu finden. [gem08b]

Schutzbedarf	Wiederherstellungszeitraum	Zuverlässigkeit
Niedrig	<6 Stunden	>75%
Mittel	<1 Stunde	>95,83%
Hoch	<10 min	>99,3%
Sehr Hoch	<1 min	>99,93%

Tabelle 3.3: Schutzbedarsklassen: Verfügbarkeit für zentrale Komponenten der TI [gem08b]

Die in der Tabelle 3.3 angegebenen Wiederherstellungszeiten und Zuverlässigkeitsangaben gelten im Rahmen der TI nur für die zentralen Komponenten der TI. (Beschreibung Abschnitt 3.3.1) Für die dezentralen Komponenten gelten die folgenden Wiederherstellungszeiten. (Tabelle 3.4)

Schutzbedarf	Wiederherstellungszeitraum
Niedrig	<2 Wochen (14 Tage)
Mittel	<1 Woche (7 Tage)
Hoch	<3 Tage (72 Stunden)
Sehr Hoch	<1 Tag (24 Stunden)

Tabelle 3.4: Schutzbedarsklassen: Verfügbarkeit für dezentrale Komponenten der TI [gem08b]

Unter *Authentizität* versteht man jenen Zustand eines Systems, wenn dieses gewährleistet, dass die gespeicherten Daten immer glaubwürdig und in der notwendigen Echtheit verfügbar sind. Das hat zur Folge, dass der Autor bzw. der Verantwortliche von patientenbezogenen Daten sowie der Auslöser eines Verarbeitungsganges jederzeit eindeutig feststellbar sein muss. Im Rahmen der eGK ist es zudem unerheblich ob es sich dabei um eine natürliche Person, eine Organisation oder eine technische Komponente handelt. Zudem ist es von Nöten, die Herkunft der im Rahmen der Personalisierung auf eine Karte´aufgebrachten Daten aus der Sicht der personalisierenden Stelle eindeutig bestimmbar und prüfbar sind. [gem08c] Können medizinische Vorgänge nicht eindeutig bestimmt werden, entstehen dadurch unter Umständen nicht vorhersehbare Folgeschäden für den Patienten, da das Prinzip der Authentizität verletzt wurde. [Eck04]
Folgende Tabelle 3.5 gibt einen Überblick über die einzelnen Schutzbedarfsklassen des Schutzziels Authentizität und deren Anforderung auf die Prozessqualität im System der Gesundheitstelematik.

Schutzbedarf	Prozessqualität
Niedrig	Handlungen sind nicht eindeutig einer bestimmten Gruppe oder bestimmten natürlichen Person zuordenbar
Mittel	Handlungen sind auf eine eindeutig bestimmbare Gruppe rückführbar.
Hoch	Handlungen sind eineindeutig auf eine natürliche Person rückführbar.
Sehr Hoch	Handlungen sind eineindeutig und nachweisbar auf eine natürliche Person rückführbar.

Tabelle 3.5: Schutzbedarsklassen: Authentizität [gem08b]

Unter *Nichtabstreitbarkeit* versteht man jenen Zustand eines Systems, wenn dieses gewährleistet, dass einerseits der Sender eines patientenbezogenen Dokuments sicher sein kann, dass das Dokument seinen Empfänger erreicht hat, und er darf nicht abstreiten können, genau dieses Dokument an genau den Empfänger gesendet zu haben. Andererseits muss der Empfänger eines patientenbezogenen Dokuments sicher sein können, genau dieses Dokument von einem bestimmten Sender empfangen zu haben, und er darf nicht abstreiten können, genau das Dokument von einem bestimmten Sender empfangen zu haben. [gem09a] Diese Nichtabstreitbarkeit muss sowohl für den Vorgang der Datenübertragung wie auch für die Information der Übertragung gewährleistet sein. [gem08c]
Folgende Tabelle 3.6 gibt einen Überblick über die einzelnen Schutzbedarfsklassen des Schutzziels Nichtabstreitbarkeit und deren Anforderung auf die Prozessqualität im System der Gesundheitstelematik.

Schutzbedarf	Prozessqualität
Niedrig	Handlungen sind nicht eindeutig einer bestimmten Gruppe oder bestimmten natürlichen Person zuordenbar.
Mittel	Handlungen sind auf eine eindeutig bestimmbare Gruppe oder technische Einheit rückführbar. Handlung kann vom Ausübenden bestritten werden. Nachweispflicht der Handlung liegt beim Kläger.
Hoch	Handlungen sind eineindeutig auf eine natürliche Person rückführbar. Handlung kann vom Ausübenden nur schwer bestritten werden. Nachweispflicht der Handlung liegt beim Kläger.
Sehr Hoch	Handlungen sind eineindeutig und nachweisbar auf eine natürliche Person rückführbar. Nachweispflicht der Nicht-Handlung liegt beim Handelnden. Die Nichtabstreitbarkeit hat Beweiskraft vor Gericht.

Tabelle 3.6: Schutzbedarsklassen: Nichtabstreitbarkeit [gem08b]

Das Ziel ist nun, dass jedes einzelne System in der Systemarchitektur die Ziele der Daten- und Informationssicherheit erfüllt. Steht man vor der Aufgabe, bestehende Systeme sicher zu gestalten, hat man es zum Teil mit gewachsenen Systemen oder Teilsystemen zu tun, die von ihrer Architektur her nicht nicht für Sicherheitsaspekte ausgelegt sind. Zugleich muss jede Einzelkomponente separat analysiert und schlussendlich das Gesamtsystem nochmals überprüft werden. Hilfestellung für eine solche Aufgabe erhält man vom Grundschutzhandbuch (GSHB), dass vom BSI herausgegeben und regelmäßig aktualisiert wird. Die vom GBSHB empfohlenen Maßnahmen reichen jedoch nur bis zu einem Schutzbedarf von „mittel“ und sind somit nicht für Sicherheitsanforderungen medizinischen Daten, Schutzbedarf „hoch“, geeignet. [Bun08] (Näheres siehe Kapitel 5) Auf Grund der geringen Komplexität der IT in der Arztpraxis (Abschnitt 3.1), im Vergleich zur IT in großen Konzernen sowie Krankenhäusern und der Tatsache, dass es sich bei den IT-Systemen um Standardsysteme handelt, ist eine Modellierung nach dem Grundschutzhandbuch ausreichend. nach [SBJK08]

Die Besonderheit des GSHB besteht im modularen Aufbau. Dabei steht es dem Anwender frei, wie nach dem Baukastenprinzip, nur jene Module zu nutzen, die er für sein System benötigt. Somit erhält man ein schlankes Sicherheitskonzept, das nur jene Bestandteile besitzt, die für das jeweilige IT-System relevant sind. Dadurch ist es zwingend erforderlich, dass man vor der Erstellung eines Sicherheitskonzeptes eine exakte Strukturanalyse durchführt und somit alle Komponenten des Systems identifiziert. Ist dies geschehen, so wählt man frei die passenden Bausteine des GSHB aus, prüft

diese und vergleicht somit den derzeitigen Ist- mit dem wünschenswerten Sollzustand. Entstehen bei dieser Gegenüberstellung Differenzen, müssen die Bausteine entsprechend ergänzt werden. Eine weitere Besonderheit des GSHB ist auch, dass es in allen relevanten Bereichen Maßnahmen vorgibt. Diese sind breit gestreut und reichen von z.B. Client-Server-Netzen, baulichen Einrichtungen bis z.B. zu Kommunikations- und Applikationskomponenten. [KT05]
Eine weitere Besonderheit des GSHB besteht darin, dass es sich bei den vorgeschlagenen Aktionen um Standardmaßnahmen der IT handelt, die zudem ökonomisch vertretbar und somit attraktiv für Unternehmen sind. Zudem wird Einsteigern dank detaillierten Beschreibungen und Anleitungen der Beginn erleichtert. Hat man die vorgeschlagen Sicherheitskomponenten erfolgreich in sein IT-System integriert, ist es in weiterer Folge notwendig, diese zu warten und wenn notwendig weitere Verbesserungsmaßnahmen einzuleiten. Um jederzeit einen Überblick über den aktuellen Stand der realisierten Schutzmaßnahmen zu haben und deren Kosten und Nutzen jederzeit analysieren zu können, steht das Grundschutz-Tool (GS-Tool), jedem Anwender frei zur Verfügung. Alle Aufgabe und Daten rund um das Sicherheitskonzept lassen sich damit bequem und übersichtlich verwalten. Besonders unterstützt werden dabei folgende Bereiche: [Bun08]

- IT-Systemerfassung
- Anwendungserfassung
- Schutzbedarfsfeststellung
- Modellierung nach IT-Grundschutz
- Realisierungsplanung
- Kostenauswertung
- Berichterstellung
- Revisionsunterstützung
- Basis-Sicherheitscheck
- IT-Grundschutz-Zertifikat

Bei der Modellierung nach IT-Grundschutz muss das betrachtete Informationsverbund mit Hilfe der vorhandenen Bausteine nachgebildet werden. Für diese Modellierung ist es von Nöten zuerst das betrachtete IT-System abzugrenzen und zu erfassen. Dies geschieht in der IT-Systemerfassung. Diese Erfassung beginnt Untersuchung des vorhandenen beziehungsweise geplanten IT-Verbundes und Endet bei der Erfassung von Softwareanwendungen und der eingesetzten Hardware. Ziel ist die Schaffung einer soliden Grundlage, in der alle sicherheitsrelevanten Parameter beschrieben

sind. Weiters muss eine Schutzbedarfsfeststellung erstellt werden. Ziel dieser ist es zu bestimmen, wie viel Schutz die Informationstechnik und deren unterstützten Anwendungen benötigen. Sind diese beiden Dokumente erstellt kann mit der Modellierung nach dem IT-Grundschutz begonnen werden. Auf Basis der Systemerfassung und der Schutzbedarfsfeststellung wird nun ein Modell des betrachteten Informationsverbundes erstellt. Dieses Modell besteht aus verschiedenen, gegebenenfalls auch mehrfach verwendete IT-Grundschutz-Bausteinen und ist somit eine Abbildung der sicherheitsrelevanten Aspekten des Informationsverbunds. Gilt es nun viele Sicherheitsmaßnahmen umzusetzen ist es empfehlenswert, eine Realisierungsplanung zu erstellen. Diese hilft somit dabei, die gefundenen Sicherheitsmaßnahmen erfolgreich umzusetzen. Die Kostenauswertung, Berichterstellung und Revisionsunterstützung sind Funktionen des GS-Tools und somit Unterstützungswerkzeuge. Sie helfen beispielsweise bei der systematische Überprüfung vorgegebener Richtlinien oder um die laufenden Kosten einzelner Richtlinien auszuwerten.
Der Basis-Sicherheitscheck hat den Sinn, einen schnellen Überblick über das vorhandene IT-Sicherheitsniveau zu bieten. Mithilfe von Interviews wird der aktuelle Status des bestehenden IT-Verbundes in Bezug auf den Umsetzungsgrad von Sicherheitsmaßnahmen des IT-Grundschutzhandbuchs ermittelt. Das Ergebnis ist ein Katalog von Maßnahmen, in dem für jede Maßnahme der aktuelle Umsetzungsstatus erfasst ist. Anhand dessen werden Verbesserungsmöglichkeiten für die Sicherheit des IT-Verbunds aufgezeigt. Das IT-Grundschutz-Zertifikat bietet Unternehmen die Möglichkeit, ihre Bemühungen um IT-Sicherheit transparent darzustellen. Somit signalisiert man Außenstehenden sofort, dass die eigene IT auf einem gewissen Schutz-Level basiert, ebenso wird das Vertrauen zwischen Unternehmen und Kunden gefördert. Dabei kann frei nach Wünschen und Anforderungen zwischen einer Vielzahl von Zertifikaten gewählt werden. Die Spanne reicht von einer Selbsterklärung bis hin zu einer Zertifizierung durch das BSI. [KT05] [Bun08]

In den folgenden Abschnitten wird nun speziell auf die Kernkomponenten der Gesundheitstelematik eingegangen. Als erste zentrale Komponente wird die Chipkarte analysiert, deren Technologie untersucht und mögliche Angriffsmöglichkeiten aufgezeigt.

3.2 Chipkarten

Elektronische Ausweisdokumente nehmen immer öfters Einzug in unser Leben. Ein Ausweis ist in diesem Zusammenhang eine amtliche oder private Urkunde, die die Identität ihres Inhabers mit dem Anspruch auf Verbindlichkeit darstellt. Die Verbreitung nimmt immer mehr zu und auch die eGK wird ein zentraler Bestandteil digitaler Ausweisdokumente in Deutschland

sein. Allgemein spricht man von einem elektronischen Ausweisdokument, wenn ein Mikrochip in einen Ausweis integriert wird. [Sch09]
Der Nutzen des integrierten Mikrochips ist vielfältig und reicht von der Abspeicherung von persönlichen Daten bis hin zur Erhöhung der Fälschungssicherheit. [Sch09]

Bei näherer Begutachtung der vielfältigen Vorteile, verwundert es kaum jemanden, dass sich elektronische Ausweisdokumente immer mehr verbreiten. Allein im deutschsprachigen Raum gibt es derzeit über 10 Großprojekte, die als zentralen Bestandteil einen elektronischen Ausweis zum Inhalt haben. [Sch09]

3.2.1 Funktionsweise

Um Daten auf einer Plastikkarte zu speichern und anschließend maschinell auszulesen bedient man sich verschiedenster Techniken. Die geläufigsten sind:[Sch09]

- Hochprägung
- Maschinenlesbare Schrift
- Strichcodes und 2D-Codes
- Magnetstreifen
- Optischer Speicherstreifen
- Speicherchips
- Mikrochips

Bei einer Hochprägung handelt es sich um die einfachste Technik der Datenspeicherung. Bei dieser werden die Informationen mittels eines erhabenen Aufdruckes auf die Karte geschrieben. Diese Information ist dadurch sehr gut sichtbar und einfach zu fühlen. Diese Technik ist besonders bei Unternehmen der Finanzbranche beliebt. Viele Bankinstitute nutzen diese Technik, um Informationen wie den Namen und die Kontonummer auf ihren Kundenkarten aufzubringen. Die Bedeutung dieser Technik hat in den letzten Jahren sehr an Bedeutung verloren. Trotzdem ist es nicht abzusehen, dass diese Technik in naher Zukunft verschwindet. Besonders Bankinstitute setzen noch immer darauf, da sie so ihren Kundenkarten ein edleres Aussehen verleihen können. [Sch09]

Bei einer Informationsaufbringung durch maschinenlesbare Schrift bedient man sich des Umstandes, dass moderne Computer in der Lage sind, optische Zeichenketten zu erkennen und sich die aufgebrachte Information so

automatisiert verarbeiten lässt. Fachlich spricht man bei dieser Technik von optischer Zeichenerkennung (OCR). Dank des technischen Fortschritts stellt eine Erkennung von unterschiedlichen Schriftarten, sogar von Handschrift, kein Problem mehr dar. Das bekannteste Einsatzgebiet dieser Technik ist sicherlich der standardisierte Reisepass. [Sch09]

Strichcodes oder 2D-Codes sind ein weit verbreitetes Mittel zur Informationsaufbringung. Die Idee hinter Strichcodes ist, dass sich der Kontrast zwischen weißer und schwarzer Farbe am einfachsten mittels handelsüblicher Scanner ermitteln lässt und daraus leicht Information gewonnen werden können. Strichcodes sind nicht standardisiert und es gibt sie in mehreren Formen. Alle basieren aber auf schwarzen Strichen mit weißen Lücken dazwischen. Alles in allem lässt sich diese Form der Information leicht und kostengünstig auf einer Plastikkarte auftragen. Dennoch wird diese Methode nur sehr selten verwendet, da die Information nicht von Menschen lesbar ist. [Sch09]

Der Magnetstreifen ist wohl die bekannteste Methode, um Informationen auf einer Plastikkarte unterzubringen. Dieser ist seit Jahrzehnten zentraler Bestandteil von Bankkarten. Der Magnetstreifen ist etwa 1 cm dick und mit magnetischem Metalloxid überzogen. Magnetstreifen, die nach der Norm ISO/IEC 7810 gefertigt wurden, beinhalten drei Datenbereiche mit einer Gesamtspeicherkapazität von 1.024 Bit. Elektronische Ausweise basierend auf dieser Technik spielen nur begrenzt eine Rolle, da sich die gespeicherte Information leicht verändern lässt. [Sch09]

Ein optischer Speicherstreifen ist eine weitere Möglichkeit, um Informationen auf einer Plastikkarte unterzubringen. Diese Technik ist vergleichbar mit jener, die bei einer CD-ROM angewendet wird, sie wurde von der Firma Lasercard entwickelt. Dabei wird ein Speicherstreifen auf die Rückseite der Karte aufgetragen. Die maximale Speicherkapazität beträgt dabei 1 MByte. [TMTN03] Ein optischer Speicherstreifen ist zudem nur für dauerhaftes Auslesen konzipiert und lässt somit nur einen einmaligen Schreibvorgang zu. Hersteller von elektronischen Ausweisen nutzen diese technische Möglichkeit, um Fälschungen ihrer Ausweise zu erschweren. [Sch09]

Eine weitere, sehr interessante Möglichkeit, um Daten auf einer Plastikkarte unterzubringen ist der Speicherchip. Dabei handelt sich um eine Spezialform des Mikrochips. Allgemein kann ein Speicherchip nur einmalig beschrieben werden und anschließend werden nur mehr Leseoperationen darauf durchgeführt. Auch spricht man von einem Speicherchip, wenn auf diesem leichte Rechenoperationen durchgeführt werden können, die zu Grunde liegende Logik muss aber im Gegensatz zum Mikrochip fest verdrahtet sein und kann so nicht umprogrammiert werden. Die Speicherkapazität ei-

nes Speicherchips kann bis zu mehreren GB betragen. In der Praxis liegt diese bei elektronischen Ausweisen nur bei mehreren KB, da hier ein gutes Preis-Leistungsverhältnis realisiert werden kann. [Sch09]

Die weitaus interessantere Möglichkeit, um Information auf eine Plastikkarte aufzubringen, ist der Mikrochip. Diesen gibt es in mehreren Ausführungen und generell unterscheidet man zwischen kontaktlosen und kontaktbehafteten Versionen. Bei der kontaktbehafteten Version muss bei der Datenübertragung eine galvanische Verbindung vorhanden sein. Die Verbindung besteht aus sechs oder acht vergoldeten Kontakten, deren Anordnung und Größe auf der Karte wird durch die Norm ISO/IEC 7816-2 aus dem Jahre 1988 festgelegt. [Hor98]

3.2.2 Angriffsmöglichkeiten

Chipkarten weisen in verschiedenen Lebenszyklen unterschiedliche Schwachstellen auf und diese können gezielt ausgenutzt werden, um später auf die gespeicherte Information Zugriff zu erlangen. Laut [Ran08] werden drei unterschiedliche Lebenszyklen unterschieden:

- Angriffe während der Chipentwicklung
- Angriffe während der Chipproduktion
- Angriffe während der Chipkartenbenutzung

Folgend wird detailliert auf den letzten Lebenszyklus, d.h. während der Chipkartenbenutzung, eingegangen, da nur dieser im Rahmen einer Arztpraxis beeinflusst werden kann. Die ersten beiden Lebenszyklen betreffen den Entwicklungs- und Produktionsprozess und sind somit nicht für diese Arbeit relevant. Eine genaue Beschreibung für diese beiden Lebenszyklen befindet sich in [Ran08].

Folgend werden Angriffsmethoden im Lebenszyklus der Chipkartenbenutzung beschrieben. Da diese oft sehr komplex und kompliziert sind, entspricht die nähere Begutachtung nicht mehr dem Fokus dieser Arbeit und so werden sie in Folge nur oberflächlich behandelt. Eine genauere Beschreibung der einzelnen Methoden befinden sich in folgender Literatur: [RE03], [PKS07], [GR05], [JLG09], [HCH07], [KLC09] und [SCL09]

Vonseiten der Chipkartenhersteller sehr viel Aufwand betrieben, um ihre Produkte sicher zu gestallten und somit das nicht befugte Auslesen der gespeicherten Informationen unmöglich zu gestalten. Trotz aller Anstrengung existieren technische Möglichkeiten, um dies zu bewerkstelligen. Die

folgende Tabelle 3.7 gibt einen Überblick über die verschiedenen Techniken: [GR05]

Angriffsart	Angriffstechnik
invasiv	Re-Engineering Probing
nicht-invasiv	Software attacks Side-channel attacks Fault Attacks

Tabelle 3.7: Angriffsmöglichkeiten auf Chipkarten [GR05]

Grundlegend wird unter einem *invasiven* und einem *nicht-invasiven* Angriff unterschieden. [Par00] Der grundsätzliche Unterschied liegt in der Tatsache, dass bei einem *nicht-invasiven Angriff* der Chip nicht zerstört wird. Bei einem *invasiven* Angriff wird der Chipkarte zerstört und kann in Folge nicht wieder benutzt werden.

Durch Zerstörung und anschließender Analyse der Innenkomponenten wird bei der *re-engineering*-Methode versucht, die innere Struktur zu analysieren und so auf die gespeicherten Informationen Zugriff zu erlangen. Wenn es dem Angreifer gelingt, die interne Struktur, beispielsweise die Anschlüsse zum ROM-Speicher zu rekonstruieren, kann er die gespeicherte Information auslesen. Der Speicherchip wird bei dieser Angriffsmethode vollständig zerstört. [GR05]
Bei der Angriffstechnik *probing* wird der zu untersuchende Chip geöffnet und anschließend mit speziellen Nadeln bestückt. Durch diese Nadeln ist man in der Lage, die anliegenden Potentiale zu messen und zu manipulieren. Durch Messung eines einzigen Kontakts ist es beispielsweise schon gelungen, einzelne Sicherheitsalgorithmen zu knacken und so Zugriff auf die gespeicherte Information zu erlangen.[GR05] Zusätzlich kann diese Angriffstechnik dazu verwendet werden, um die elektrisch anliegenden Potentiale zu beeinflussen und so Sicherheitslücken auszunutzen. Durch die moderne und immer kleiner werdende Fertigungstechnik ist diese Art des Angriffs nur mehr mit sehr großen Aufwand möglich.[GR05]

Bei *nicht-invasiven* Angriffsmethoden wird versucht, durch Analyse verschiedenster Daten, Zugriff auf den Speicherbaustein zu erlangen. Dazu werden verschiedenste Informationen ausgewertet, die nachstehend beschrieben werden. [GR05]
Die simpelste Möglichkeit, um eine Chipkarte anzugreifen, ist jene, die Kommunikation zwischen der Chipkarte und dem Terminal auszuwerten. Auf nicht verschlüsselte Daten kann mit dieser Angriffsmethode sofort zugegriffen werden. Bei verschlüsselten Daten wird zuerst der geheime Schlüssel rekonstruiert und anschließend auf die übertragende Information zugegriffen.

Diese Angriffsmethode fällt unter die Gruppe der *software attacks*. [PKS07] In der Gruppe der *side-channel attacks* werden Angriffsmethoden zusammengefasst die messbare Seiteninformation auswerten. [KLC09] Folgende Seiteninformationen werden üblicherweise für diesen Angriff verwendet:

1. Stromverbrauch
2. Zeitspanne
3. das elektro-magnetische Feld

Bedingt durch die verwendeten Bauteile der Chipkarten verbrauchen sie je nach Operation unterschiedlich viel Strom, brauchen dafür unterschiedlich viel Zeit und erzeugen dadurch ein unterschiedliches elektrisches Feld. Durch Analyse dieser physikalischen Größen lassen sich durch mathematische Modelle Rückschlüsse auf den geheimen Schlüssel, der im EEPROM der Karte gespeichert ist, ziehen. [JLG09]

Bei der letzten Angriffsmethode versucht man, durch gezieltes Senden von Falschinformation über den geplanten Ablauf einen Zustand des BS herzustellen, der es erlaubt, Zugriff auf den geschützten Speicher zu erhalten oder Befehle abzusetzen, für die er eigentlich keine Rechte besitzt. Eine besondere Schwierigkeit besteht bei dieser Methode in der Tatsache, dass sich der Angreifer nicht immer sicher sein kann, wann und ob er einen Fehler verursacht hat.[SCL09]
Aktuelle Chipkarten sind gegen diese Form des Angriffs weitestgehend geschützt. Durch optimierte Software-Designs wird von Seiten der Hersteller streng darauf geachtet, dass physikalische Eigenschaften, wie Beispielsweise Stromverbrauch und Ausführungszeiten nicht von den im Algorithmus verwendeten Operanden abhängen.[Phi09]

Die verwendeten Chipkarten in der Telematikinfrastruktur müssen laut der Spezifikation gegen alle beschriebenen Angriffsmethoden resistent sein. Im Sicherheitskonzept der Telematikinfrastruktur sind die einzelnen Sicherheitsanforderungen an die Chipkarte genau spezifiziert. Beispielsweise muss diese folgende Sicherheitsanforderungen erfüllen:[gem08a]

- Die Smartcard muss Schutz gegen Sidechannel Attacks bieten.
- Die Smartcard muss Schutz gegen nicht-invasive Angriffe bieten.
- Es muss eine feste Verbindung der Bausteine mit der Schutzschicht geben, bei deren Entfernung das Bauelement zerstört werden muss.
- Die Smartcard muss mit Temperatur-, Frequenz- und Spannungssensoren ausgestattet sein.

In den Sicherheitskonzept befinden sich noch eine Vielzahl dieser Sicherheitsanforderungen. Eine Spezifikation, wie diese Sicherheitsanforderungen erreicht werden können, findet aber nicht statt. Der Hersteller der Smartcard ist hier in der Pflicht geeignete Maßnahmen zu treffen.[gem08a]

3.3 Telematikinfrastruktur

Unter dem Begriff Telematikinfrastruktur (TI) werden alle Komponenten zusammengefasst, die für die Einführung und Anwendung der elektronischen Gesundheitskarte erforderlichen interoperablen und kompatiblen Informations-, Kommunikations- und Sicherheitsinfrastrukturen notwendig sind.[gem09a] Folgend dieser Definition werden folgende Komponenten als Teil der Telematikinfrastruktur gesehen:

- Smartcard
- Kartenterminal, mobiles Kartenterminal
- Konnektor
- Zentrale Infrastrukturdienste
- Fachdienste
- Mehrwertfachdienste
- Komponenten/Dienste/Systeme zum Betrieb der TI

Im folgenden Abschnitt werden nun die einzelnen Komponenten näher erläutert und die Architektur der TI erklärt.

3.3.1 Überblick

In der Telematikinfrastruktur stellen zentrale und dezentrale Komponenten die Kernstücke dar. Zu den dezentralen Komponenten zählen alle Systeme, die bei den einzelnen Leistungserbringern in Betrieb sind. Die restlichen Komponenten werden folgend als zentrale Komponenten bezeichnet.[gem09a] Die folgende Abbildung 3.3 zeigt die einzelnen Komponenten der TI plus dem Primärsystem. Dieses wird zum besseren Verständnis abgebildet.

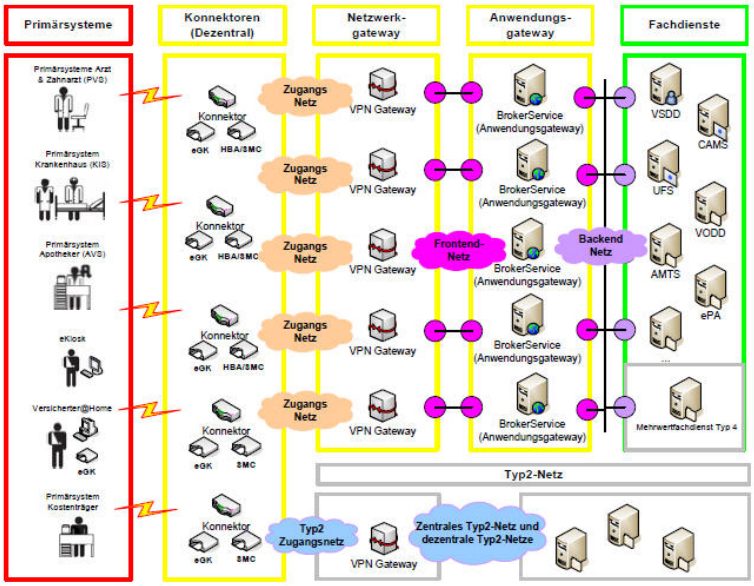

Abbildung 3.3: Die Telematikinfrastruktur der eGK [gem09a]

Wie aus Abbildung 3.3 ersichtlich, besteht die TI aus mehreren einzelnen Komponenten. Die umrandete Farbe kennzeichnet zusätzlich die Systemgrenze. (Gelb = Dezentrale Komponente + Netzwerk-Anwendungsgateway, Grün = Fachdienste, Grau = Mehrwertfachdienste, Rot = Primärsysteme) [gem09a]

In der gelben Systemgrenze befinden sich die dezentralen Komponenten der TI, der Netzwerk- und Anwendungsgateway. Zu den dezentralen Komponenten gehören der Konnektor, das Kartenterminal und die Smartcard. Mittels Konnektoren erfolgt der Zugriff der einzelnen Primärsysteme auf das Telematiknetzwerk. Zusätzlich erfolgt durch den Konnektor der Zugriff auf das Kartenterminal und sogleich auf die Smartcard. Dazu besitzt er Schnittstellen zum Primärsystem, zu den angebundenen Kartenterminals und zum Telematiknetzwerk. Der Zugang zum Telematiknetzwerk wird durch Netzwerk-Gateways geschützt. Diese VPN-Gateways stellen sicher, dass nur zugelassene Konnektoren Zugang zum Telematiknetzwerk erhalten. Der Zugang zu serverbasierten Anwendungsservices wird über Anwendungs-Gateways, Broker-Services, gesteuert und geschützt. Broker-Services bieten vor allem eine Sicherheits- und Datenschutzfunktion, indem sie Zugriffe auf ausgewählte Services anonymisieren. Zudem stellen diese sicher, dass alle Datenzugriffe oder Versuche von Datenzugriffen aufgezeichnet werden. In der grünen Systemgrenze befinden sich die einzelnen Fachdienste. Unter Fachdienste werden die einzelnen Anwendungen der eGK verstanden, die wiederum in Pflicht- und in freiwillige Anwendungen unterteilt werden. (siehe Kapitel 2) Die letzte, graue Systemgrenze der TI ist jene der Mehr-

wertfachdienste. Unter Mehrwertfachdienste fallen Anwendungen, die nicht gesetzlich vorgeschrieben sind, jedoch von der TI angeboten werden. Sie ist somit eine Anwendung, die zwingend für mindestens eine Benutzergruppe einen Nutzwert darstellt und Teile der TI anwendet. [gem09a]

In den folgenden zwei Abschnitten wird gezielt auf den Konnektor und das Primärsystem eingegangen. Diese zusätzliche Betrachtungsweise erfolgt einerseits aufgrund der Bedeutung der beiden Komponenten für die TI und der Gesamtarchitektur und andererseits aufgrund der bis jetzt noch mangelnden Beschreibung der beiden Komponenten. Im Abschnitt 3.1 wird auf Probleme innerhalb der TI eingegangen und diese erläutert.

3.3.2 Konnektor

Der Konnektor ist eine von drei dezentralen Komponenten der Telematikinfrastruktur. Dazu gehören des Weiteren noch die Chipkarten und das Kartenterminal. Zu diesem Zweck besitzt der Konnektor zwei Netzwerkschnittstellen und verbindet so über seine LAN-Schnittstelle das Primärsystem mit dem Kartenterminal. Über die WAN-Schnittstelle stellt er eine Verbindung mit der Telematikinfrastruktur her und stellt so Dienste und Anwendungen der TI zur Verfügung. Seine Hauptaufgabe ist somit die sichere Ankopplung der dezentralen Systeme an die Telematikinfrastruktur und das Bereitstellen einer lokalen, sicheren Umgebung, in der Dienste mit hohem Schutzbedarf ausgeführt werden können. [gem08e] Die sichere Ankopplung an die Telematikinfrastruktur erfolgt über ein IPSec-basiertes VPN. Zusätzlich muss der Konnektor gegen einwirkende Bedrohungen gesichert sein. Beispielsweise besteht seine Aufgabe darin, Angriffe aus dem Transportnetz abzuwehren und so die zentrale Telematikinfrastruktur zu schützen. Da so der Konnektor eine entscheidende Rolle im Sicherheitskonzept der TI einnimmt, muss dieser von einer gesonderten Stelle sicherheitstechnisch geprüft und zertifiziert werden. Bei dieser Zertifizierung muss der Hersteller ein Sicherheitskonzept und ein Sicherheitsgutachten vorlegen, dass seine Eignung für den Einsatz in der Telematikinfrastruktur bescheinigt. Ein zentraler Punkt der Zertifizierung ist die Sicherstellung, dass der private Schlüssel und die elektronische Signatur, die im Konnektor aufbewahrt werden, nicht veränderbar in einem Sicherheitsmodul gespeichert sind. [gem08k]

Elektronische Signaturen stellen ein Teilgebiet der Kryptografie dar und dienen zur eindeutigen Feststellung der Identität des Signators. Mithilfe von Signaturen wird sichergestellt, dass ein Dokument nach einer elektronischen Signatur nicht verändert wurde. [Fäs08] Diese Prozedur ist notwendig, wenn man die Integrität eines Dokumentes sicherstellen will. Im Rahmen der eGK muss aber zudem die Authentizität des Absenders sichergestellt werden. Um dies zu gewährleisten, benötigt man eine Public Key Infrastruktur (PKI).

Unter einer PKI werden alle Instanzen zusammengefasst, die für den Einsatz asymmetrischer Kryptographie in offenen Systemen erforderlich sind. Die wichtigste Aufgabe einer PKI ist die Registrierung der Nutzer sowie das Ausstellen und Verwalten von Zertifikaten. [PR06] Auch in der Telematikinfrastruktur wird eine PKI eingesetzt. In einer PKI-Infrastruktur stellen kryptographische Verfahren eine essentielle Rolle dar. Es gibt grundlegend zwei unterschiedliche Verfahren der Ver- und Entschlüsselung:

- Symmetrische Kryptoalgorithmen:
  Bei symmetrischen Kryptoalgorithmen wird das Dokument mit demselben Schlüssel verschlüsselt und anschließend wieder entschlüsselt. Viele Algorithmen basieren auf diesem Verfahren, der bekannteste ist der DES-Algorithmus.

Abbildung 3.4: Das Prinzip symmetrischer Kryptoalgorithmen [Ran08]

  Wie aus Abbildung 3.4 ersichtlich, wird der Klartext zunächst mit dem geheimen Schlüssel verschlüsselt und anschließend zum Empfänger übertragen. Dieser kann anschließend den verschlüsselten Text mithilfe des gleichen geheimen Schlüssel entschlüsseln.[Fäs08]

- Asymmetrische Kryptoalgorithmen:
  Asymmetrische Kryptoalgorithmen basieren auf zwei unterschiedlichen Schlüsseln. Einer wird als geheimer und der andere als öffentlicher Schlüssel bezeichnet. Der öffentlicher Schlüssel dient zum Verschlüsseln, der geheime zum Entschlüsseln.

Abbildung 3.5: Das Prinzip asymmetrische Kryptoalgorithmen [Ran08]

  Wie aus Abbildung 3.5 ersichtlich, werden nun bei einem Ver- und Entschlüsselungsvorgang zwei unterschiedliche Schlüssel benutzt. Einer der bekanntesten Algorithmen, basierend auf diesem Kryptoalgorithmus, ist der RSA-Algorithmus. Der RSA-Algorithmus basiert auf dem Prinzip der Arithmekrik großer Ganzzahlen. Basis des Schlüsselpaares

bilden zwei große Primzahlen. Die Sicherheit liegt dabei im Faktorisierungsproblem großer Zahlen. Es gibt bis heute noch keinen effektiven Algorithmus, um den Modulus zweier Primzahlen wieder in seine Primzahlen zu zerlegen. [Fäs08]

Innerhalb der Telematikinfrastruktur ist eine PKI unerlässlich, da an mehreren Stellen digitale Zertifikate mit privaten und geheimen Schlüsselpaaren verwendet werden. Unter einem digitalen Zertifikat werden strukturierte Daten verstanden, mit denen sich der Eigentümer des Zertifikats und dessen öffentlicher Schlüssel bestätigen. Im Rahmen der eGK werden verschiedenste Zertifikate unterschieden, die wichtigsten sind: [Sch09] [gem08f]

- Netz-Zertifikate werden zur sicheren Verbindung zwischen dem Konnektor und der Telematikinfrastruktur benötigt.
- Dienst-Zertifikate dienen zur eindeutigen Identifikation der einzelnen Dienste in der TI
- eGK-Zertifikate gehören zum fixen Bestandteil der elektronischen Gesundheitskarte. Diese werden zum Authentifizieren und Verschlüsseln der Daten benutzt.
- CV-Zertifikate dienen der Kommunikation der einzelnen eingesetzten Smartcards untereinander. Beispielsweise werden sie benötigt, wenn der Arzt mit seinem Heilberufsausweis (HBA) auf die eGK zugreift.
- HBA-SMC-Zertifikate sind Zertifikate des HBA und der Sicherheitsmodulkarte.
- Geräte-Zertifikate dienen zur eindeutigen Identifikation von Geräten innerhalb der Telematikinfrastruktur.

Jedes Zertifikat wird von einem Trust Service Provider (TSP) ausgegeben. Weiters hat die TSP die Aufgabe, die Echtheit der erstellten Zertifikate zu garantieren. Für die Überprüfung der einzelnen Zertifikate muss davon ausgegangen werden, dass dem TSP uneingeschränkt vertraut werden kann. In der Telematikinfrastruktur ist es deswegen unerlässlich, dass alle Zertifizierungsstellen einheitliche Sicherheitsstandards erfüllen und auch diese regelmäßig von unabhängigen Instanzen überprüft werden.[NFS08] Sollte dennoch ein Sicherheitsproblem seitens einer Zertifizierungsstelle auftauchen, so besteht die Möglichkeit, einzeln ausgestellte Zertifikate wieder sperren zu lassen. Im Rahmen der eGK wird dafür das „Online Certificate Status Protocol“ verwendet.[gem08c] Dieses Protokoll bietet die Möglichkeit, den Status von Zertifikaten bei einem Validierungsdienst abzufragen.[Ran08]

3.3.3 Primärsystem

Unter einem Primärsystem versteht man unterschiedliche Anwendungsprogramme für die Nutzer der TI. Die einzelnen Primärsysteme können anhand der direkt beteiligten Personen in drei unterschiedliche Gruppen eingeteilt werden. Man unterscheidet: [gem09a]

- Primärsysteme für Leistungserbringer:
  In dieser Gruppe werden alle Praxisverwaltungssysteme bei den einzelnen Ärzten und Zahnärzten, Krankenhausinformationssysteme in den Krankenhäusern und die unterschiedlichen Apothekenverwaltungssysteme der Apotheker zusammengefasst.

- Primärsysteme für Kostenträger:
  Primärsysteme der Kostenträger sind Anwendungsprogramme in den einzelnen Versicherungen und Beratungsstellen. Diese dienen in erster Linie zur Aktualisierung der Versichertenstammdaten bei den Versicherungen und zur persönlichen Beratung bei den einzelnen Beratungsstellen.

- Primärsysteme für Versicherte:
  In dieser Gruppe sind nur zwei Anwendungen von Bedeutung. Zum einen die Anwendung eKiosk und zum anderen die Anwendung Versicherter@Home. Sie erlauben den einzelnen Versicherten die Einsicht in die gespeicherten Daten. Weiters stellen diese Applikationen Funktionen bereit, um:

  – bestimmte Daten zu verbergen/sichtbar zu machen
  – einzelne Datensätze zu löschen
  – die Verwaltung der Berechtigungen für die Nutzung der gespeicherten Daten zu steuern.

  Die einzelnen Funktionen sind aber allesamt noch nicht genau spezifiziert und deswegen kann noch keine genaue Aussage getroffen werden, welche Funktionen schlussendlich zur Verfügung stehen. [gem09a]

3.3.4 Probleme

Im Rahmen des ersten Feldtests konnte erstmals die TI unter annähernd realistischen Bedingungen getestet werden. Während dieses ersten Test wurden zahlreiche Probleme festgestellt. In der folgenden Abbildung 3.6 sind die aufgetretenen Fehler den zugehörigen Komponenten der TI zugeordnet: [gem08i]

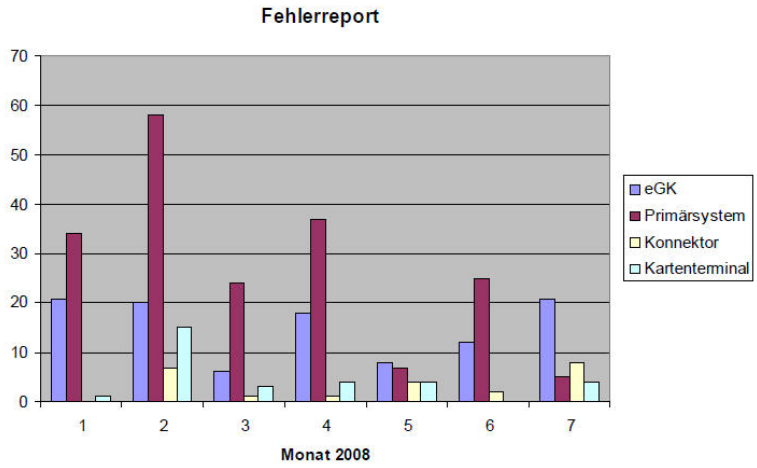

Abbildung 3.6: Fehlerreport im Rahmen des ersten Feldtests [gem08i]

Wie in der Abbildung 3.6 ersichtlich betraf den Großteil der Fehler, die Primärsysteme. Die Ursache dafür, scheint in der Komplexität der Systeme und der heterogenen Abbildung der Geschäftsprozesse zu liegen.
Speziell wurden folgende Probleme mit dem Primärsystem festgestellt:[gem08i]

- Unterschiedliches Verständnis der Prozessabläufe zwischen Leistungserbringer und Primärsystemhersteller.
- Bedienungsfehler, die zum Teil durch Schulungsmaßnahmen reduziert werden konnten.
- Programmtechnische Umsetzungsfehler, die durch die PS-Hersteller behoben werden mussten.

Größere Probleme anderer Komponenten der TI, beispielsweise des Konnektors, des Kartenterminals und der eGK konnten nicht festgestellt werden. Vereinzelt musste ein Kartenterminal aufgrund eines technischen Defektes ausgetauscht werden. Die Anzahl der getauschten Terminals beläuft sich im einstelligen Zahlenbereich. Probleme mit den Konnektor betrafen meist Softwarefehler, die schnell mit einen Update der Firmware behoben werden konnten. Probleme mit der eGK resultieren weitestgehend aus Fehlern im Rahmen des Personalisierungsprozesses.[gem08i]

Ein weiteres Problem wurde mit den vorgegebenen Arbeitsschritten der Primärsysteme festgestellt. Aufgrund mangelhafter Implementierung wurden viele Anwendungen der eGK im Rahmen des Tests nur geringfügig verwendet. Dies betraf besonders die eVerordnung. Hintergrund hierfür ist die fehlende Möglichkeit zur Remote-PIN-Eingabe, so dass der HBA ständig in das jeweilige Kartenterminal umgesteckt und der PIN mehrfach eingegeben werden muss.[gem08i]

3.4 Sicherheitsaspekte Kartenterminal

In diesem Kapitel erfolgt eine genauere Betrachtung des Kartenterminals. Ein Kartenterminal ist eine Peripheriekomponente, die die Verbindung der Chipkarte mit der äußeren Umgebung herstellt. Folglich müssen sich Terminals in die bestehende IT-Infrastruktur einbinden und je nachdem geeignete Schnittstellen nach außen bereitstellen können. Im folgenden Unterkapitel erfolgt eine genauere Definition und die unterschiedlichen Unterscheidungsmerkmale werden analysiert. Weiters werden spezifische Angriffsmöglichkeiten auf ein Kartenterminal aufgezeigt.

3.4.1 Definition

Üblicherweise bieten Chipkarten nur eine serielle Schnittstelle für die Kommunikation nach außen an. Es besteht keine andere Möglichkeit, mit der Karte zu kommunizieren, als über diese Schnittstelle. Ein Kartenterminal ist somit eine Komponente, die die Aufgabe hat, die Chipkarte elektrisch zu versorgen und einen Kommunikationskanal zwischen der Chipkarte und der angeschlossenen Peripherie herzustellen. [Ran08] Kartenterminals unterliegen je nach Ausstattung einer gewissen Klassifizierung. Die folgende Abbildung 3.7 zeigt eine solche nach [Ran08].

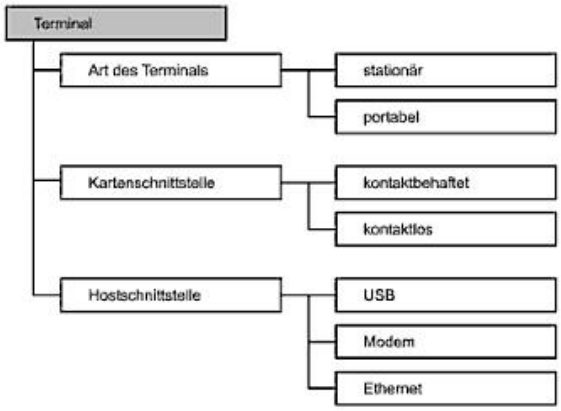

Abbildung 3.7: Klassifizierungsbaum von Terminals für Chipkarten [Ran08]

Folglich werden Kartenterminals nach drei unterschiedlichen Gesichtspunkten bewertet. Die erste Unterscheidung erfolgt nach der Art des Terminals. Man unterscheidet zwischen einem stationären und einem portablen Terminal. Stationäre Terminals sind dafür konzipiert, fix an einem Standpunkt betrieben zu werden. Sie besitzen meist eine fixe Verkabelung und eine Anbindung an ein Hostsystem. Portable Kartenterminals können hingegeben frei nach Wahl aufgestellt und wieder abgebaut werden. Die Datenübertragung erfolgt meist per Funk und sie besitzen eine autonome Ener-

giequelle. [RE03] Die zweite Unterscheidung betrifft die Schnittstelle zur Chipkarte. Analog zu den Chipkarten wird folglich auch bei den Terminal zwischen kontaktbehafteten und kontaktlosen Terminals unterschieden. Je nach Schnittstelle kann diese auch nur mit der analogen Chipkarte kommunizieren. Folglich braucht eine kontaktlose Chipkarte zwingend ein Terminal mit einer kontaktlosen Schnittstelle und umgekehrt. [RE03] Die letzte Unterscheidung betrifft die Hostschnittstelle. Dies ist jene, die das Terminal bereitstellt, um eine Kommunikationmit weiteren Peripheriekomponenten zu ermöglichen. Wie in der Abbildung 3.7 ersichtlich, ist entweder eine USB-, eine Modem- oder eine Ethernet-Schnittstelle an einen Terminal angebracht. [RE03]

Eine zusätzliche Einteilung von Kartenterminals erfolgt durch den zentralen Kreditausschuss (ZKA). Dieser teilt Kartenterminals nach deren Funktionselementen in in vier unterschiedliche Gruppen, auch Klasse genannt, ein. In der folgende Tabelle 3.8 werden die unterschiedlichen Klassen dargestellt.

Klasse	Funktionselemente
Klasse 1	Kontakteinheit, Schnittstelle zu anderen Systemen
Klasse 2	Klasse 1 Funktionselemente mit Display
Klasse 3	Klasse 2 Funktionselemente mit Tastatur
Klasse 4	Klasse 3 Funktionselemente mit Sicherheitsmodul

Tabelle 3.8: Einteilung der Kartenterminals nach ZKA [Ran08]

Die beschriebene Klassifizierung unterscheidet die einzelnen Kartenterminals nach ihren Elementen. Ein Klasse 1 Kartenterminal besteht im Wesentlichen aus einer Kontakteinheit mit der Chipkarte und einer Schnittstelle, die die Verbindung zu anderen Systemen bereitstellt. Klasse 2 Terminals besitzen alle Funktionselemente der Klasse 1 und zusätzlich ein Display. Auf diesen können unterschiedlichste Informationen dargestellt werden. Klasse 3 Kartenterminals erweitern deren Funktionsumfang zusätzlich um eine Tastatur. Klasse 4 Terminals sind zugleich die höchste Klasseneinheit und stellen die aufwändigste Klasse mit allen Funktionselementen der unterliegenden Klassen dar. Sie besitzt den vollen Funktionsumfang der Klassen 1 bis 3 und erweitert diesen um ein Sicherheitsmodul. [Ran08]

Im Rahmen der eGK werden Kartenterminals zusätzlich unterschieden: [gem08h]

- Netzwerkfähige Kartenterminals
- Virtuelle Kartenterminals

Unter netzwerkfähigen Kartenterminals werden jene zusammengefasst, die einen Ethernetanschluss als Hostschnittstelle (Abbildung 3.7) aufweisen und alle Sicherheitsvorgaben der gematik unterstützen. Diese Schnittstelle wird gebraucht, um eine sichere Verbindung zum Konnektor (Kapitel 3.5) herzustellen. Virtuelle Kartenterminals besitzen weder Display, Tastatur noch Sicherheitsmodul. Die Smartcard wird hierbei von einen Kartenlesegerät ausgelesen und jegliche Interaktion seitens des Benutzers läuft über eine Software, die beispielsweise an einem PC installiert ist.[gem08h]

Im folgenden Abschnitt wird speziell auf potenzielle Schwachstellen und Angriffsmöglichkeiten bei Kartenterminals eingegangen.

3.4.2 Angriffsmöglichkeiten

Kartenterminals besitzen je nach dem dafür vorgesehenen Kartentyp und Anwendungsgebiet unterschiedliche Sicherheitsvorkehrungen und Angriffsmöglichkeiten. Sind keine speziellen Sicherheitsmerkmale auf der Karte vorhanden weist das Terminal keinerlei Sicherheitseinrichtungen auf, da die Karte einen sehr einfachen Aufbau besitzt und sich darauf keine Sicherheitsmerkmale befinden, die überprüft werden müssen. Anders fällt es aus, wenn das Terminal zeitweise oder ganz im Offline-Betrieb arbeitet. In einen solchen Fall muss ein Hauptschlüssel, der für die einzelnen Verschlüsselungsmethoden gebraucht wird, entweder im Terminal oder in angrenzenden Komponenten gespeichert werden. Diese Hauptschlüssel stellen sicherheitstechnisch ein großes Problem dar, da die gesamte Sicherheit im System auf diese aufgebaut ist. Angreifer kennen ihre Wichtigkeit und versuchen mit allen Mitteln, diese zu entschlüsseln. Ist der Hauptschlüssel im Terminal aufbewahrt, wird dieser Schlüssel auch nicht direkt im Terminal gespeichert, sondern in einem speziellen Sicherheitsmodul. Dies ist meist in Epoxidharz gegossen und so gegen äußere Eingriffe geschützt. Eine Kommunikation kann nur über eine spezielle Schnittstelle zwischen dem Sicherheitsmodul und dem Terminalcomputer erfolgen. Moderne Ausführungen besitzen eine sehr sensible Sensorik zur Detektion von Angriffen. Auch bei abgeklemmter Betriebsspannung kann die Elektronik somit Angriffe erkennen und alle gespeicherten Schlüssel unwiderruflich löschen. Kartenterminals, wie sie im Rahmen der eGK eingesetzt werden, besitzen kein solches Modul. Hierbei erfolgt die Schlüsselberechnung in der NPU der Smartcard. [Ran08]

Eine weitere Angriffsart ist jene, die Kommunikation zwischen den Kontakten der Chipkarte und des Terminals abzuhören. Typisch werden Drähte von der Chipkarten nach außen abgeführt und so die Kommunikation abgehört. Unverschlüsselte Datenströme können mit dieser Angriffsart einfach abgehört werden. Abhilfe schaffen Shutter. Ein Shutter ist eine mechanische Sicherheitseinrichtung, die alle abführenden Kontakte im Terminal mit einer Schere abschneidet. Sind die Drähte zu dick oder können sie aufgrund

ihrer materiellen Eigenschaften nicht unterbrochen werden, so wird mit einer weiteren Einrichtung das Einrasten der Karte verhindert und so die Kommunikation nicht gestartet. Probleme stellt hier die Wartung und die Fehleranfälligkeit dar. Shutter sind sehr fehleranfällig und müssen in regelmäßigen Abständen gewartet werden. Deswegen verzichten die meisten Hersteller auf eine solche Einrichtung. [Ran08]

Die im Rahmen der eGK eingesetzten Kartenterminals besitzen zwingend eine numerische Tastatur. Über diese muss der Besitzer später seinen persönlichen PIN eingeben und so das auslesen der Daten freigeben. Dieser Umstand kann auch ein Sicherheitsrisiko darstellen, da Angreifer versuchen, könnten den PIN mitzulesen. Aus diesen Grund muss die numerische Tastatur speziell gegen Eingriffe aller Art geschützt sein. Eine solche geschützte Tastatur wird auch Encrypting PIN Pad genannt. Dieses schützt die Übertragung zum Terminalcomputer und das Tastenfeld besitzt Vorkehrungen, die eine Manipulation nur mit sehr großen Aufwand ermöglicht. [MPRNS08] [RE03]

Die verwendeten Kartenterminals in der Telematikinfrastruktur müssen laut der Spezifikation gegen alle beschriebenen Angriffsmethoden resistent sein. Im Sicherheitskonzept der Telematikinfrastruktur sind die einzelnen Sicherheitsanforderungen an das Kartenterminal genau spezifiziert. Beispielsweise muss diese folgende Sicherheitsanforderungen erfüllen:[gem08a]

- Manipulationsversuche müssen zuverlässig erkennbar sein
- Zur Erkennbarkeit von Hardware-Manipulationen müssen geeignete Methoden (z. B. Versiegelung mit fälschungssicherem Sicherheitsaufkleber, welcher sich bei Entfernung zerstört und damit nur einmal verwendbar ist) verwendet werden.
- Das eHealth-Kartenterminal muss technische Funktionen zur Anwenderauthentifizierung (z. B. KeyPad) bieten.
- Die Manipulation von Daten, die im eHealth-Kartenterminal (temporär) abgelegt sind, darf nicht möglich sein.

In den Sicherheitskonzept befinden sich noch eine Vielzahl dieser Sicherheitsanforderungen. Eine Spezifikation, wie diese Sicherheitsanforderungen erreicht werden können, findet aber nicht statt. Der Hersteller des Kartenterminals ist hier in der Pflicht geeignete Maßnahmen zu treffen.[gem08a]

3.5 Sicherheitsaspekte Konnektor

In diesem Abschnitt erfolgt eine genauere Betrachtung des Konnektors. Dieser stellt eine zentrale Komponente in der eGK Telematikinfrastruktur dar

und verbindet das Kartenterminal mit der Telematikinfrastruktur. Der Konnektor stellt ein zentrales Bindeglied dar, da er die internen Rechnersysteme und das Kartenterminal verbindet und zugleich eine Verbindung mit der Telematikinfrastruktur herstellt. [gem08j]

3.5.1 Definition

Der Konnektor wird innerhalb der Spezifikation als Black-Box-Lösung beschrieben. Die Umsetzung der geforderten Anforderungen, seitens der Gematik, unterliegt vollkommen den Hersteller.[gem06]
Allgemein bietet der Konnektor im Rahmen der eGK drei unterschiedliche Schnittstellen um mit anderen Komponenten der TI zu kommunizieren.[gem09a]

- Schnittstelle zum Telematiknetzwerk:
  Über die WAN-Schnittstelle des Konnektors kann dieser auf serverbasierte Fachdienste zugreifen. Teil dieser Verbindung bildet der Virtual Private Network-Client. Dieser stellt seinen sichereren Kommunikationskanal mit dem VPN-Konzentrator in der Middleware her. [gem09a]

- Schnittstelle zu den Kartenterminals:
  Über die Karten- und Kartenterminal-Services ist der Konnektor in der Lage, auf die eGK zuzugreifen. [gem09a]

- Schnittstelle zu den Primärsystemen:
  Mithilfe der LAN-Schnittstelle des Konnektors ist dieser in der Lage, mit dem Primärsystem zu kommunizieren. Er kappselt die konkreten Abläufe zum Zugriff auf die Karten- und serverbasierten Fachdienste. [gem09a]

Der Konnektor dient somit als Verbindungsglied zwischen den Komponenten und Funktionen der Telematik und der bestehenden Infrastruktur der Leistungserbringer. Durch diese Konstruktion bildet dieser eine gekapselte Einheit, die eine Entkoppelung zwischen den zentralen Diensten der Telematik und den Primärsystemen sicherstellt.[gem06]

3.5.2 Angriffsmöglichkeiten

Ein Konnektor bietet aufgrund seiner Konzeption und Bauform nur eingeschränkte Angriffsmöglichkeiten. Konnektoren werden innerhalb der Spezifikation der gematik als Black-Box-Lösung angesehen und dem Hersteller ist die technische Ausführung freigestellt. Grundbedingung für diesen technischen Freiraum ist jene, dass alle Konnektoren die spezifizierten Leistungs- und Sicherheitsanforderungen sicherstellen. Daraus folgend lassen sich die möglichen Angriffe in folgende Kategorien einteilen:

- Mechanischer Angriff

- Software-Angriff
- Schnittstellen-Angriff

Bei einem mechanischen Angriff wird versucht, durch Zerstörung des Gehäuses Zugriff auf die im Konnektor befindlichen Bauteile zu erhalten. Durch Manipulation der eingebauten Bauteile kann anschließend das Verhalten des Konnektors beeinflusst werden. Dadurch können beispielsweise die von Seiten des Herstellers implementierten Sicherheitsvorkehrungen außer Kraft gesetzt werden.

Bei einem Software-Angriff wird versucht die Software der betreffenden Komponente zu verändern oder Schwachstellen gezielt auszunutzen. Dabei werden beispielsweise Fehler in der Software oder Features, wie beispielsweise die Updatefähigkeit, ausgenutzt um die Software zu manipulieren oder unberechtigt Zugriff auf Dateien zu erlangen. Beispielsweise muss ein Update der Software des Konnektors jederzeit im Online- als auch im Offline-Betrieb möglich sein und stellt somit ein mögliches Sicherheitsrisiko dar. Gelingt es dem Angreifer, die modifizierte Firmware mit dem geheimen Schlüssel des Herstellers zu signieren, kann er seine Software ungehindert einspielen. Eine zusätzliche Überprüfung durch die gematik ist zwar zwingend vorgesehen, jedoch keine zusätzliche Signatur durch diese. [gem08e]

Bei der dritten und zugleich letzten Angriffsmöglichkeit wird die Kommunikation der angebotenen Schnittstellen des Konnektors abgehört. Beispielsweise kann durch Abhören der WAN-Schnittstelle des Konnektors jegliche Kommunikation mit der Telematikinfrastruktur gespeichert werden. Die Verbindung erfolgt mittels einer IPSec-basierten VPN-Verbindung. Diese Art der Verbindung ist unter speziellen Voraussetzungen durchwegs angreifbar. Wenn beispielsweise der „initialization vector“ in Klartext gesendet wird ist man mittels eines IV-Angriffs (Initialization Vector Attacks) in der Lage, die IPSec-Verschlüsselung zu bezwingen. [MSS00]

Die verwendeten Konnektoren in der Telematikinfrastruktur müssen laut der Spezifikation gegen alle beschriebenen Angriffsmethoden resistent sein. Im Sicherheitskonzept der Telematikinfrastruktur sind die einzelnen Sicherheitsanforderungen an die Konnektoren genau spezifiziert. Beispielsweise muss diese folgende Sicherheitsanforderungen erfüllen:[gem08a]

- Der Konnektor soll Manipulationsversuche zuverlässig erkennen. (z.B Manipulation der installierten Software)
- Das Auslesen von privaten und geheimen Schlüsseln aus dem Konnektor darf nicht möglich sein.
- Unautorisiertes Einbringen einer Software in den Konnektor darf nicht möglich sein.

- Die Hardware des Konnektors muss gegen Entwendung gesichert werden.
- Erfolgreicher Einsatz von Konnektor-Klonen darf nicht möglich sein.
- Man-in-the-Middle Attacken bei verschlüsselten Verbindungen zum Konnektor dürfen nicht möglich sein.

In den Sicherheitskonzept befinden sich noch eine Vielzahl dieser Sicherheitsanforderungen. Eine Spezifikation, wie diese Sicherheitsanforderungen erreicht werden können, findet aber nicht statt. Der Hersteller des Konnektors ist hier in der Pflicht geeignete Maßnahmen zu treffen.[gem08a]

3.6 Sicherheitsaspekte Primärsystem

Da das Primärsystem schon im Abschnitt 3.3.3 erläutert wurde, erfolgt in diesem Abschnitt 3.6 ein Fokus auf die möglichen Angriffsmöglichkeiten auf die Primärsysteme.

3.6.1 Definition

Unter einen Primärsystem werden Anwendungsprogramme für Leistungserbringer, Kostenträger und Versicherte im Rahmen der TI bezeichnet. Sie dienen beipsielsweise für die Aktualisierung der Versicherungsstammdaten oder stellen Funktionen zur Verwaltung der eigenen Daten zur Verfügung. (Näheres Abschnitt 3.3.3)

3.6.2 Angriffsmöglichkeiten

Da es sich bei Primärsysteme und Anwendungsprogramme handelt, wird folgend unter folgenden unterschiedliche Formen des Angriffs unterschieden:

- Angriff auf das Anwendungsprogramm:
  Bei dieser Art des Angriffs versucht man, die Anwendungssoftware so zu manipulieren, sodass sie ein für den Angreifer nützlicheres Verhalten aufweist. Beispielsweise könnte der Angreifer durch Manipulation der Software erreichen, dass integrierte Schutzmaßnahmen ausgeschaltet sind und er so unbegrenzten Zugang auf die Daten und Funktionen des Programms erhält. [GC06]
- Angriff auf die zu Grunde liegende Peripherie:
  Bei einem Angriff auf die zu Grunde liegende Peripherie versucht man, Zugriff auf den lokalen Rechner zu erlangen. Der Zugriff wird hierbei durch vorhandene Sicherheitslücken des BS oder installierte Schadsoftware ermöglicht, beispielsweise wird die Manipulation des BS durch

Trojaner erreicht. Trojaner sind Programme, die ohne Wissen des Anwenders bestimmte Tätigkeiten am System ausführen. [Kra04]

3.7 Sicherheitsaspekte elektronische Gesundheitskarte

In Deutschland gibt es seit den Zeiten von Otto von Bismarck (ab 1883) eine gesetzliche Krankenversicherung. Diese gesetzliche Krankenversicherung galt für den Großteil der Bevölkerung, war somit verpflichtend. Für die Bescheinigung, dass der Versicherte über eine gesetzliche Krankenversicherung verfügt, vergaben die einzelnen Krankenversicherungen Krankenscheine. Mit diesen konnte der Versicherte zum Arzt gehen und so Leistungen beziehen. Ende der 70iger Jahre kam die Überlegung auf, den bis dato üblichen Krankenschein mit einen amtlichen Ausweis auszustatten. Im Jahr 1977 wurde der Öffentlichkeit ein Prototyp im ID-1-Format vorgestellt. Die amtlichen Daten waren damals per Hochprägung angebracht. Das Zeitalter der Chipkarten erreichte Deutschland im Jahre 1994. Seit diesem Jahr erhalten alle Krankenversicherten in Deutschland eine Krankenversicherungskarte. Die KVK war eine Chipkarte im ID-1-Format Der integrierte Chip war ein Speicherchip mit einen maximalen Speicherplatz von 256 Byte. Auf diesen wurden bei der Ausgabe die personenbezogenen Daten gespeichert. Hier waren die personenbezogenen Daten aber nicht geschützt und konnten mit einfachsten Mitteln ausgelesen, geändert oder beschrieben werden. [Sch09] In den neunziger Jahren kam erstmals der Wunsch auf, die KVK durch einen elektronischen Ausweis zu ersetzen und im Jahre 2003 wurde anschließend mit dem Projekt der eGK begonnen. Ähnlich der KVK ist die eGK auch eine Chipkarte im ID-1-Format und rein äußerlich ähneln sich die beiden sehr. Der größte Unterschied liegt im integrierten Chip. Bei der eGK wird im Gegensatz zur KVK eine Smartcard eingesetzt. [Sch09]
Im folgenden Unterkapitel erfolgt eine genauere Betrachtung der technischen Grundlagen der eGK.

3.7.1 Grundlagen

Die eGK ist als kontaktbehaftete Smartcard ausgeführt und besitzt eine maximale Speicherkapazität von 32 KByte. Aufbauend auf der KVK ist auch die eGK im ID-1-Format ausgeführt. Die genauen Maße sind in der ISO/IEC 7810 und ISO/IEC 7816 spezifiziert. Die Vorderseite der eGK ist genau festgelegt und besteht aus sechs voneinander unabhängigen Feldern. Die Gliederung auf der Karte wird in der folgenden Abbildung 3.8 dargestellt: [gem08d]

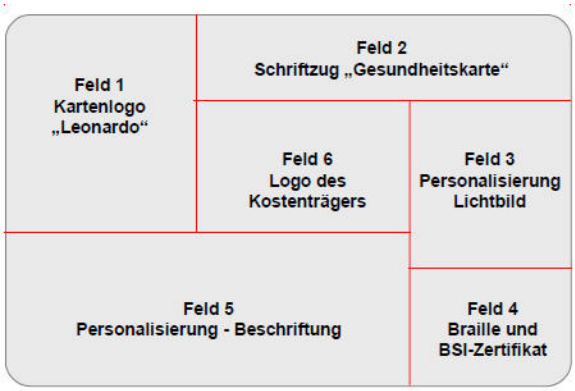

Abbildung 3.8: Felder der Kartenvorderseite der eGK [gem08d]

Wie in der Abbildung 3.8 ersichtlich, kann die eGK in sechs unterschiedlichen Feldern eingeteilt werden. Die nachfolgende Aufzählung beschreibt kurz die Inhalte dieser.

- Feld 1:
  In diesem ist das einheitliche Logo der eGK platziert.
- Feld 2:
  Dieses Feld enthält die einheitliche Kartenbezeichnung "Gesundheitskarte".
- Feld 3:
  In diesem wird das Lichtbild des Karteninhabers platziert.
- Feld 4:
  In diesem Feld werden die Buchstaben ëgkïn Blindenschrift platziert, es enthält auch optional eine Bildmarke für das vom BSI erteilte Zertifikat.
- Feld 5:
  Enthält alle personenbezogenen Daten des Karteninhabers.
- Feld 6:
  In diesen wird das Logo des Kostenträgers platziert und ggf. unternehmensspezifische Angaben

Die Felder 1, 2, 3 und 5 bilden zusammen ein einheitliches Erkennungszeichen und sind in Größe und Lage genau spezifiziert. [gem08d]

3.7.2 Funktionen

Neben der grundlegenden Funktion als elektronischer Ausweis hat die eGK zwei Hauptaufgaben zu erledigen. Diese sind:

- eGK dient als Authentifizierungswerkzeug:
  Dabei wird bei der erstmaligen Verwendung ein vom Karteninhaber gewählter, individueller PIN festgelegt und verschlüsselt auf dem Chip gespeichert. Erfolgt anschließend ein Zugriffsversuch, ohne sich mit dem korrekten PIN vorher zu authentifizieren, blockiert die Chipkarte jeglichen Zugriffsversuch und ein Zugriff auf die gespeicherten Daten ist somit nicht möglich. Zur Sicherheit werden die letzten 50 Zugriffe auf der Smartcard gespeichert. [gem08j]

- Durchführung der kryptografischen Verschlüsselungen:
  Die eGK ist mit mehreren Kryptografiefunktionen ausgestattet um eine sichere Kommunikation und Verschlüsselung der Daten zu gewährleisten. Um dies effektiv durchführen zu können, besitzt die eGK insgesamt sieben verschiedene private Schlüssel und die dazugehörigen Zertifikate. Die eGK muss nun in der Lage sein Datenpakete mit den jeweiligen privaten Schlüssel zu signieren und so die Echtheit der Daten zu garantieren. Die eGK verwendet bei der Verschlüsselung eine hybride Verschlüsselungstechnik. Dabei werden die Gesundheitsdaten zunächst zum Konnektor verschickt und symmetrisch mit einer Zufallszahl verschlüsselt. Dieser geheime Schlüssel wird anschließend mit dem öffentlichen Schlüssel des Empfängers verschlüsselt. [gem08j] Diese Art der Verschlüsselung hat den entscheidenden Vorteil, dass die rechenintensive Verschlüsselung nicht in der Smartcard, sondern im davor optimierten Konnektor stattfinden kann. [Sch09] [gem09b]

Im folgenden Kapitel erfolgt eine Übersicht der gespeicherten Informationen auf der eGK.

3.7.3 Gespeicherte Informationen

Auf der eGK werden eine Reihe von Informationen gespeichert. Der gesamte verfügbare Speicherplatz beträgt 32 KByte. Viele der gespeicherten Dateien sind Betriebssystemabhängig und werden folgend nur beispielhaft angeführt. Neben den Dateien für das BS werden auf der eGK Daten für eine Reihe von obligatorischen Anwendungen gespeichert. Die Daten für die eGK befinden sich dabei in der Health Care Anwendung (HCA). Die folgende Abbildung 3.9 zeigt die Struktur des Dateibaumes der HCA:

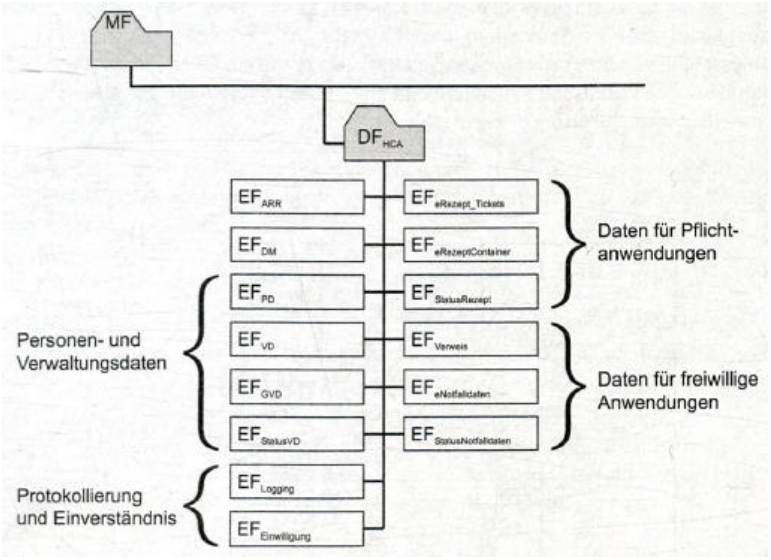

Abbildung 3.9: Dateibaum der Anwendung HCA auf der eGK [Ran08]

Wie in der Abbildung 3.9 ersichtlich, kann der bestehende Dateibaum in vier verschiedene Datenblöcke eingeteilt werden. Diese sind:

- Daten für freiwillige Anwendungen:
  In diesem Datenblock werden alle Daten für die freiwilligen Anwendungen gespeichert. Eine Besonderheit stellen jene Daten dar, die für die Notfalldaten gespeichert sind. Die Authentifizierung erfolgt hierbei mittels der Card-to-Card-Authentifizierung. Somit ist gewährleistet, dass nur Inhaber eines HBA, SMC-B oder HB Ausweises die Notfalldaten der eGK auslesen können. Dies ist besonders bei einem Unfall von Bedeutung, wenn der Versicherte nicht mehr in der Lage ist, den PIN einzugeben. [gem09a]

- Daten für Pflichtanwendungen:
  In den Datenblock für Pflichtanwendungen fällt das elektronische Rezept. Dieses ist eine Pflichtanwendung auf der eGK und soll den bis jetzt üblichen Medienbruch ablösen. Der Medienbruch kommt dadurch zustande, dass der Arzt dem Patienten das Rezept in Papierform übergibt und dieses in der Apotheke wieder aufwändig elektronisch erfasst werden muss. Zukünftig wird, beispielsweise wenn die TI nicht erreichbar ist, in diesen Datenblock das Rezept hinterlegt und mit der Signatur des Arztes versehen. Um wieder auf die Daten Zugriff zu erlangen, bedarf es wiederum eines HBA. Mit dem HBA des Apothekers ist er anschließend in der Lage, die Daten entweder von der Karte oder von einem Server herunterzuladen. [gem08g]

- Protokollierung und Einverständnis:

In diesen Datenblock werden zwei unterschiedliche Arten von Daten gespeichert. Im $EF_{Logging}$ ist die Protokolldatei über die letzten 50 Zugriffe gespeichert. Diese Daten werden automatisch durch die CPU der Smartcard gespeichert. [gem08j]
Im $EF_{Einwilligung}$ werden Informationen über die Nutzung freiwilliger Angaben gespeichert. Die Anzahl der freiwilligen Angaben ist seitens der eGK nicht beschränkt. Laut der derzeit gültigen Spezifikation [gem08g] sind derzeit aber nur drei unterschiedliche freiwillige Angaben spezifiziert:

- Die Notfalldaten:
  Im Gegensatz zu den auf der eGK gespeicherten Notfalldaten kann hier viel mehr Information zur Verfügung gestellt werden, da hier die Daten nicht auf der Smartcard, sondern auf einem zentralen Server gespeichert werden. Die Möglichkeiten der zu speichernden Daten sind fast unbegrenzt und reichen von Notfallnummern, die im Notfall kontaktiert werden sollen, bis hin zu operativen Eingriffe.
- Arzneimitteldokumentation:
  In dieser können alle Medikamte gespeichert werden, die der Karteninhaber derzeit einnimmt bzw. jeweils eingenommen hat. Auch die Dosierung und die Art des Arzneimittels (Rezeptpflichtig oder frei erhältlich) werden gespeichert. Der Arzt kann aufgrund der vorliegenden Daten wichtige Rückschlüsse auf die derzeitige Erkrankung schließen und so Doppelverordnungen vermeiden.
- Die elektronische Patientenakte:
  In der elektronischen Patientenakte werden Informationen über den Krankheitsverlauf des Karteninhabers gespeichert. Dies war auch bisher der Fall, jedoch hat diese neue Form den Vorteil, dass die Patientenakte auf Wunsch orts- und zeitunabhängig abgerufen werden kann. Der große Vorteil liegt daran, dass der Karteninhaber, egal zu welchem Arzt er geht, immer sicher sein kann, dass der Arzt den aktuellen Krankheitsverlauf kennt. Gleichzeitig fördert es auch die Kommunikation zwischen den Ärzten und die Therapiesicherheit, da so die Ärzte untereinander Rücksprache halten können.

- Personen und Verwaltungsdaten:
  In der Gruppe der Personen und Verwaltungsdaten werden vier Dateien auf der eGK gepflegt. In den Dateien EF_{PD} und EF_{VD} werden die für die Verwaltung wichtigen Personenstammdaten und Versicherungsdaten gespeichert. In der EF_{GVD} Datei werden Versicherungsdaten (VSD) gespeichert, die besonders schützenswert sind. Diese können erst nach einer erfolgreichen Authentisierung gelesen werden. [Ran08]

Die Datei $EF_{StatusVD}$ dient dazu, das Datum der letzten Aktualisierung, die Version und den Status der einzelnen Dateien zu sichern. Dies wird benötigt, da garantiert sein muss, dass die einzelnen Versicherungsstammdaten untereinander konsistent sind. [gem09b]
Aufgrund in der bis dato befindlichen Übergangsphase können abweichende Inhalte in den einzelnen VSD vorkommen. [gem09b]

In der Daten EF_{ARR} werden Zugriffsregeln für die restlichen Dateien und in der EF_{DM} wird eine Nachricht gespeichert, die nach einer erfolgreichen Authentisierung am Display des Kartenterminals angezeigt werden kann. Diese Nachricht wird benötigt, damit der Karteninhaber die sichere Kommunikation zwischen dem Kartenterminal und dem Primärsystem feststellen kann. [Ran08]

3.8 Rechtliche Aspekte

In diesem Abschnitt werden die rechtlichen Rahmenbedingungen der eGK erläutert. Neben der Definition von medizinischen und persönlichen Daten werden auch die gesetzlichen Grundlagen der eGK aufgezeigt.

3.8.1 Grundlagen für die eGK

Für die Umsetzung der eGK mussten zunächst einmal rechtliche Rahmenbedingungen geschaffen werden, in denen sich jede Aktivität abspielt. Diese Bedingungen wurden im Sozialgesetzbuch und im Bundesdatenschutzgesetz festgeschrieben.[Wei04]

- Sozialgesetzbuch V: (SGB V) [Bund]
  Im Sozialgesetzbuch § 291a wurde die eGK „zur Verbesserung von Wirtschaftlichkeit, Qualität und Transparenz der Behandlung“ mit Wirkung per 1.1.2006 eingeführt. Gleichzeitig wurde auch eine Verpflichtung zu Funktionalitäten, „die eine Übermittlung ärztlicher Verordnungen in elektronischer und maschinell verwertbarer Form“ ermöglichen, festgelegt.
  Liegt die Einwilligung seitens des Versicherten vor, muss die eGK folgende Anwendungen der Datenverarbeitung unterstützen:
  - Notfalldatensatz
  - elektronischer Arztbrief
  - Arzneimitteldokumentation
  - elektronische Patientenakte
  - die in Anspruch genommenen Leistungen und deren Kosten

Nach § 291a Abs. 3 ist die Krankenkasse zudem verpflichtet, den Versicherten spätestens bei der Aussendung der eGK über deren Anwendung „allgemein und verständlich“ zu informieren. Diese Einwilligung seitens des Versicherten muss auf der Karte gespeichert werden und gilt bis auf Widerruf.
Nach § 291a Abs. 4 wird der Zugriff auf das Erforderliche „zur Versorgung“ beschränkt. Als Konsequenz wird der Zugriff auf folgende Berufsgruppen beschränkt:

  - Versicherte
  - Ärzte und Zahnärzte
  - Apotheker
  - pharmazeutisches Personal
  - sonstige Erbringer ärztlich verordneter Leistungen

  Nach § 291a Abs. 6 müssen die gespeicherten Daten nach Aufforderung des Versicherten unwiderruflich gelöscht werden.
  § 291a Abs. 6 sieht zudem noch vor, dass die letzten 50 Zugriffe auf der Karte mitprotokolliert werden müssen.

- Bundesdatenschutzgesetz: (BDSG) [Bunb]
  Im BDSG § 3a ist festgelegt, dass die Grundsätze der „Datensparsamkeit und Datenvermeidung“ zwingend einzuhalten sind. Nach § 19 und § 34 schreibt der Gesetzgeber zwingend ein Auskunftsrecht über den Inhalt der gespeicherten Daten und ihre Herkunft vor.

3.8.2 Medizinische Daten

Medizinische Daten werden im Zuge des BDSG § 6c zu den besonders schützenswerten personenbezogenen Daten gezählt. Aufbauend auf diese Bestimmung müssen für diese Daten folgende Anforderungen gegeben sein: [Cau06]

- Die Zuordnung zwischen der Person und den dazugehörigen Daten darf nur autorisierten Nutzern möglich sein.
- Datenspuren, die im Zuge der Datenverarbeitung entstehen und so Rückschlüsse auf Dateninhalte erlauben, sind zwingend zu vermeiden.
- Medizinische Daten dürfen nicht in einem zentral zugänglichen Verzeichnis aller Versicherten gespeichert werden. Dies soll die Verknüpfung mit anderen Datenbeständen erschweren.

3.8.3 Persönliche Daten

Auf der eGK werden folgende persönliche Daten erfasst: [gem08d]

- Lichtbild des Versicherten
- vollständiger Name und eventuell vorhandener Titel
- Versicherungsnummer

Diese Daten werden sowohl in der Smartcard zur elektronischen Datenverarbeitung gespeichert als auch öffentlich auf der eGK aufgedruckt. Aufgrund dessen sind sie für jedermann einsehbar und unterliegen keinerlei speziellen Datenschutzbestimmungen. [Cau06]

Aufbauend dieser Grundlagen wird im nächsten Kapitel das Gesamtsystem einer Arztpraxis charakterisiert. Für diesen Zweck wird eine Musterpraxis mit den typisch eingesetzten IT-Komponenten erläutert und die räumliche Aufteilung der Arztpraxis näher besprochen.

Kapitel 4

Charakteristika des Gesamtsystems Arztpraxis

Dieses Kapitel dient dazu, einen kompakten Überblick über die typischen Charakteristika einer Arztpraxis zu bekommen. Hierbei wird gezielt auf organisatorische und informationstechnische Eigenheiten eingegangen und näher erläutert. In einem weiteren Schwerpunkt dieses Kapitels werden bestimmte Kennzahlen der Berufsgruppe „Ärzte“ erläutert. Zuletzt wird die typische Arztpraxis beschrieben. Zentrale Bestandteile bilden hierbei Kennzahlen einer deutschen Arztpraxis und typische Eigenheiten, wie beispielsweise die räumliche Organisation. All diese Punkte werden in den folgenden zwei Abschnitten behandelt. Den Anfang bilden die Charakteristika und Kennzahlen einer Arztpraxis.

4.1 Charakteristika und Kennzahlen einer Arztpraxis

Um einen Einblick in die finanziellen Möglichkeiten einer deutschen Arztpraxis, zur Behebung der IT-Sicherheitsbedrohungen durch technische oder organisatorische Lösungen, zu bekommen wird folgend die finanzielle Situation einer deutschen Arztpraxis erläutert. Die Einkommenssituation der Ärzte und Ärztinnen in Deutschland ist von verschiedenen Aspekten abhängig. Gerade regionale Unterschiede und oder eine Spezialisierung, beispielsweise in Form eines Zahnarztes, machen eine Vereinheitlichung schwierig. Generell gilt, dass nur dann eine Aussage über die Einkommenssituation getroffen werden kann, wenn die Kosten der Praxen in die Betrachtung mit einbezogen werden. Entsprechende Angaben werden regelmäßig durch das Zentralinstitut für die kassenärztliche Versorgung in der Bundesrepublik Deutschland (ZI) ermittelt und veröffentlicht. Demnach liegt das bundesdurchschnittliche

Jahreseinkommen vor Steuern im Jahre 2007 bei 206.247 Euro. Das ergibt einen Jahresüberschuss von rund 91.780 Euro im Jahr. Regional können hierbei aber große Unterschiede auftreten. Am schlechtesten verdienen Ärzte im Bundesland Hessen. Dort liegt das durchschnittliche Jahreseinkommen vor Steuern bei 183.758 Euro. Spitzenreiter ist Nord-Württemberg mit 238.563 Euro Jahreseinkommen. Bei einem Vergleich zwischen „neuen“ und „alten“ Bundesländern kann so ein großer Unterschied nicht festgestellt werden. In der folgenden Tabelle 4.1 wird das bundesdurchschnittliche Jahreseinkommen im Vergleich mit den „alten“ und „neuen“ Bundesländern dargestellt. [BNF09]

Region	Umsatz	Überschuss
Bund	206.247	91.780
Neue Länder	207.568	92.368
Alte Länder	206.026	91.682

Tabelle 4.1: Durchschnittseinkommen je Arzt im Vergleich [BNF09]

In der Tabelle 4.1 ist das bundesweite Durchschnittseinkommen der Ärzte im Vergleich mit den „alten“ und „neuen“ Bundesländern dargestellt. Der Wert bezieht sich allein aus den Einnahmen der gesetzlichen Krankenversicherung und beinhaltet somit keinerlei private Einnahmen. Der Vergleich zeigt deutlich, dass nur minimale Unterschiede der einzelnen Regionen im Vergleich zum Bund vorhanden sind. Zusätzlich zu diesen Einkommen erzielen Ärzte Einnahmen aus Sonderverträgen mit Krankenkassen sowie aus privater Tätigkeit. Erst bei Berücksichtigung dieser Einnahmen sind Aussagen zur tatsächlichen Einkommenssituation der Ärzte möglich. Zur Höhe dieser Einnahmen liegen jedoch anders als zu den GKV-Umsätzen keine flächendeckenden Daten vor. Im Vergleich zum durchschnittlichen Bruttoverdienst der Arbeitnehmer, das im Jahr 2007 bei rund 28.000 Euro im Jahr lag, ergibt es ein überdurchschnittlich hohes Einkommen. Auch der Arbeitsmarkt sieht für Ärzte und Ärztinnen in Deutschland sehr gut aus. Arbeitslosigkeit kommt kaum vor. Im Jahr 2007 waren 3.686 Ärzte arbeitslos gemeldet. Bei rund 315.000 berufstätigen Ärzten entspricht dies einer Arbeitslosenquote von 1,1 Prozent. Auf dem Arbeitsmarkt für Ärzte herrscht damit Vollbeschäftigung. [BNF09]

In einer deutschen Praxis werden durchschnittlich 31,4 Patienten pro Tag behandelt. In der Woche ergeben sich so insgesamt im Durchschnitt 243 Patientenkontakte. Für jeden einzelnen Patient hat der Arzt nur 7,8 Minuten Zeit, oft muss der Arzt pro Patient aber mehrere Krankheiten gleichzeitig untersuchen. 89 Prozent der deutschen Ärzte gaben an, dass sie häufig Patienten mit mehreren chronischen Erkrankungen behandeln. [KGS07] Diese Kennzahlen verdeutlichen, dass eine Praxis gut organisiert sein muss, um

die hohe Anzahl von kranken Personen in der zur Verfügung stehenden Zeit behandeln zu können. [BNF09]

Räumlich muss eine Arztpraxis so aufgestellt sein, dass diese auch den Wünschen und Bedürfnissen der Patienten entspricht. Ganz besonders großes Augenmerk muss hier auf die Wahrung des Patientengeheimnisses und des Datenschutzes gelegt werden. Dies ist besonders von Bedeutung, wenn medizinische Sachverhalte oder persönliche Angaben der Patienten von Unbeteiligten oder Unbefugten mitgehört werden können. Aus diesem Grund ist eine räumliche Trennung der einzelnen Bereiche einer Praxis unvermeidbar. Eine Arztpraxis ist somit in folgende Bereiche unterteilt: [HN08]

- Empfangsbereich
- Wartebereich
- Behandlungsbereich

In einer klassischen Praxis stellt der Empfangsbereich den ersten räumlichen Teil dar, den die Patienten betreten und somit sehen. Dieser ist typischerweise mit einem Tresen ausgestattet und durch Türen räumlich von den anderen Bereichen getrennt. Diese räumliche Trennung ist notwendig, um das Patientengeheimnis zu wahren. Der Empfangsbereich ist so gestaltet, dass der Patient sein Anliegen schildern kann, ohne dass unbeteiligte Personen dabei mithören können. Dies ist besonders problematisch, wenn sich mehrere Personen im Empfangsbereich befinden und ihre Anliegen darlegen wollen. Ist dies der Fall, muss unbedingt eine Diskretionszone geschaffen werden. Ähnlich wie in einer Bank kann dies beispielsweise durch Spannen eines Seiles geschehen. [HN08] Der Tresen ist so gestaltet, dass er keine Barriere für die Patienten darstellt. Er gehört ganz und gar den Patienten und sollte genügend Platz zur Verfügung stellen. Idealerweise hat der Patient direkte Sicht auf den PC der Arzthelferin, denn so kann er direkt verfolgen, welche seiner Daten verwaltet und/oder gespeichert werden. [SD06] Neben dem Empfangsbereich unterscheidet man noch den Warte- und den Behandlungsbereich. In modernen Praxen ist der Wartebereich in den Empfangsbereich integriert und beide sind beispielsweise nur durch eine Glaswand voneinander getrennt. Der Behandlungsbereich hingegen ist immer von den anderen Räumen getrennt. Dies ist vor allem notwendig, um für die zuvor schon angesprochene Diskretion zu sorgen. [HN08]

4.2 IT-Infrastruktur einer Arztpraxis

Die IT-Infrastruktur einer Arztpraxis unterscheidet sich auf die verschiedenste Art und Weise wesentlich von Ähnlichem und kann somit nicht standardisiert werden. Oft gibt es keine Vernetzung der PCs untereinander oder

man ist beispielsweise ohne Sicherheitsgateway mit dem Internet verbunden. Mit der Einführung der eGK ist aber davon auszugehen, dass eine Arztpraxis mindestens der Praxis in der Abbildung 4.1 entspricht. Diese Praxis wird im Rahmen dieser Arbeit weiter als Musterpraxis bezeichnet. Die folgende Abbildung 4.1 zeigt den beispielhaften Netzplan einer Arztpraxis im Rahmen der eGK: [SKD09] [SBJK08]

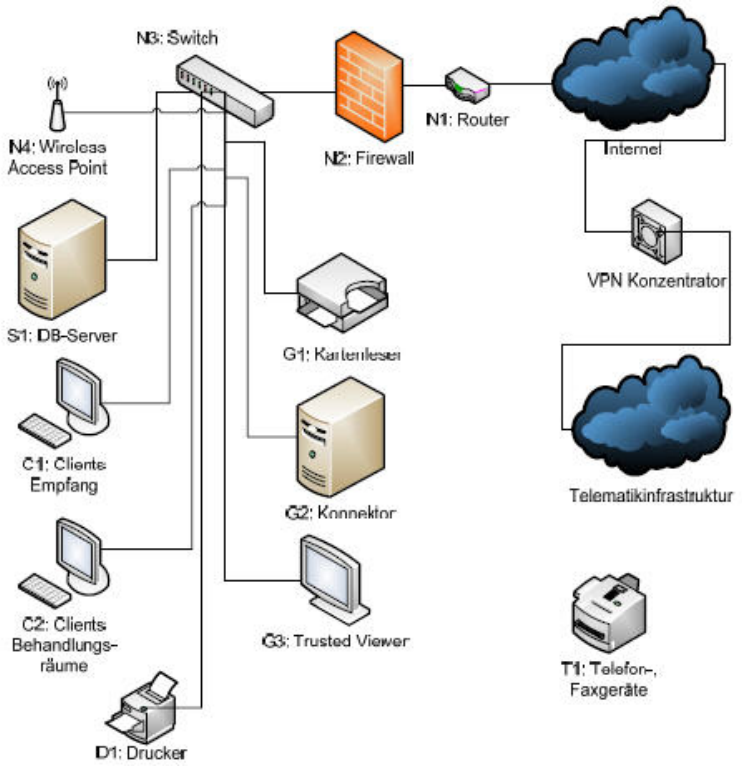

Abbildung 4.1: Netzplan einer Arztpraxis im Rahmen der eGK [SBJK08]

Wie aus Abbildung 4.1 ersichtlich, besteht die IT-Infrastruktur der Musterpraxis aus mehreren einzelnen IT-Komponenten. Der vorangestellte Buchstabe kennzeichnet den Typ der IT-Komponente: (S = Server, D = Dienstkomponente, C = Client, N = Netzkomponente, G = eGK Komponente T = Telekommunikationskomponente) [SBJK08]
In der Gruppe C werden die eingesetzten Clients zusammengefasst. In dieser werden weiter zwei unterschiedliche Clients, die in den Behandlungsräumen und die am Empfang, eingesetzt. Weiters ist ein zentraler Server an das IT-System angeschlossen. Aufgrund der Kompatibilität zu den gängigen Praxisverwaltungssystemen (PVS) handelt es sich dabei um einen Windows-Server. [SBJK08]
Alle Komponenten, die für den erfolgreichen Betrieb der eGK notwendig sind, werden in Gruppe G zusammengefasst. Diese enthält die schon bekann-

ten Komponenten (Kartenleser, Konnektor) und den Trusted Viewer. Der Trusted Viewer ist eine Anzeigekomponente für die Erstellung und Prüfung einer qualifizierten elektronischen Signatur. Dieser ist im § 17 Abs. 2 des Signaturgesetzes zwingend vorgeschrieben und dient bei einem Signiervorgang dazu, dem Benutzer das zugehörige Dokument und das verwendete Zertifikat zu zeigen. Bei einer Signaturprüfung werden dem Benutzer das zugrundeliegende Dokument, das verwendete Zertifikat und das Ergebnis der Signaturprüfung angezeigt. [gem06] [Bunc] Netzwerkkomponenten wie Switch, Wireless Access Point, Router und Firewall befinden sich in der Gruppe der Netzkomponenten (Gruppe N). Diese ermöglichen eine erfolgreiche Kommunikation der eingesetzten IT-Komponenten untereinander. Telefone und Faxgeräte werden in der letzten Gruppe der Telekommunikationskomponenten zusammengefasst. [SBJK08]

Welche Art von Praxissoftware in einer Praxis eingesetzt wird, unterliegt keinen Einschränkungen. Der Arzt kann sich frei nach seinen Wünschen das beste Produkt am Markt aussuchen und in seiner Praxis einsetzen. Der Markt ist sehr groß und in Deutschland ist eine Vielzahl unterschiedlichster Praxissoftware im Einsatz. Laut einer Statistik der Kassenärztlichen Bundesvereinigung werden in Deutschland rund 164 unterschiedliche Installationen von Praxissoftware eingesetzt. Die TOP 5 wichtigsten Anbieter und deren Marktanteil sind in der folgenden Tabelle 4.2 dargestellt. [Kas10a]

Rang	Anbieter	% Anteil
1	Compugroup Holding AG	24,45 %
2	medatiXX Medizinische Informationssysteme GmbH & Co.KG	18,03 %
3	TurboMed EDV GmbH	11,31 %
4	Psyprax GmbH	7,12 %
5	HASOMED GmbH	4,09 %

Tabelle 4.2: TOP 5 Anbieter von Praxissoftware in Deutschland [Kas10b]

Wie in der Tabelle 4.2 ersichtlich teilen sich die TOP 5 wichtigsten Anbieter von Praxissoftware den deutschen Markt. Mit einem Gesamtmarktanteil von 65 % rüsten sie fast zwei Drittel aller Arztpraxen mit Software aus. [Kas10b]

Egal welche Praxissoftware schlussendlich eingesetzt wird, so unterscheidet sich der Einsatz von EDV in der Arztpraxis essentiell von der für privaten Gebrauch erfolgten Nutzung von Computern. Im beruflichen Einsatz in der Arztpraxis sind aus strafrechtlichen und haftungsrechtlichen Gründen besondere Schutzvorkehrungen erforderlich. Besonders hervorzuheben ist hierbei die ärztliche Schweigepflicht.

Die ärztliche Schweigepflicht ist im Strafgesetzbuch[1] und in der Berufsordnung für die deutschen Ärztinnen und Ärzte[2] (MBO) geregelt. Nach § 203 Abs. 1 StGB macht sich strafbar, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis offenbart, das ihm als Arzt anvertraut worden oder sonst bekannt geworden ist. Nach § 9 MBO haben Ärzte über das, was ihnen in ihrer Eigenschaft als Arzt anvertraut oder bekannt geworden ist, zu schweigen. Kombiniert mit der Verpflichtung zur ärztlichen Dokumentation muss der Arzt Maßnahmen treffen, dass die anvertrauten Daten nicht von Unbefugten gelesen werden können. Die ärztliche Dokumentationspflicht besagt, dass Ärzte über die in Ausübung ihres Berufs gemachten Feststellungen und getroffenen Maßnahmen entsprechende Aufzeichnungen anfertigen müssen. Diese Dokumentationspflicht ist unter anderem in der MBO[3] verpflichtend vorgeschrieben.
Ärztliche Aufzeichnungen sind für die Dauer von zehn Jahren nach Abschluss der Behandlung aufzubewahren, soweit nicht nach gesetzlichen Vorschriften eine längere Aufbewahrungspflicht besteht. Längere Aufbewahrungsfristen ergeben sich beispielsweise für Aufzeichnungen über Röntgenbehandlung gemäß Röntgenverordnung[4] (RVO). Zu beachten ist aber auch die zivilrechtliche Verjährungsfrist, die für Ansprüche eines Patienten gegen seinen Arzt nach dem Bürgerlichen Gesetzbuch (BGB) gilt. Zwar beläuft sich die Verjährungsfrist grundsätzlich auf drei Jahre, gemäß Bürgerlichen Gesetzbuch[5], diese Frist beginnt jedoch erst mit dem Ende des Jahres, in dem der Anspruch entstanden ist und der Patient von den den Anspruch begründenden Umständen und der Person des Schädigers Kenntnis erlangt oder ohne grobe Fahrlässigkeit hätte erlangen müssen. Dies kann im Einzelfall bis zu 30 Jahre nach Abschluss der Behandlung der Fall sein. Daher sollte der Arzt seine Aufzeichnungen über die jeweils vorgeschriebene Aufbewahrungsfrist hinaus solange aufbewahren, bis aus medizinischer Sicht keine Schadenersatzansprüche mehr zu erwarten sind. [Kas08]
Neben diesen Aspekten ist beim Umgang mit Patientendaten in der Arztpraxis das informationelle Selbstbestimmungsrecht des Patienten zu beachten. Diesem Gedanken muss der Arzt dadurch Rechnung tragen, dass er sowohl bei konventionellen Patientenakten als auch beim Einsatz von Datenverarbeitungstechniken gewährleistet, dass sowohl im Empfangsbereich als auch in den Behandlungsräumen unbefugte Dritte keinen Zugriff in die Patientendaten erhalten. So dürfen Patientenakten in keinem Fall so bereitgelegt werden, dass etwa Patienten Daten anderer Patienten zur Kenntnis nehmen können. Dementsprechend sind Bildschirme so aufzustellen, dass sie nur vom Arzt und dem Praxispersonal eingesehen werden können. [Kas08]

[1] StGB § 203 [Bund]
[2] MBO § 9 [Bung]
[3] MBO §10 Abs. 1 [Bung]
[4] RVO § 28 Abs. 3 Satz 1 [Bunf]
[5] BGB § 195 [Buna]

Bei all diesen Anforderungen ist es nur verständlich, dass der gesetzeskonforme Betrieb einer IT- Landschaft in einer Arztpraxis besonderes Wissen erfordert. Dieses hat nur in den seltensten Fällen der Arzt selbst. Besonders das Personal in Arztpraxen ist nicht geschult im Umgang mit IT. Mediziner eignen sich ihr Wissen selbst an und Arzthelfer lernen allenfalls den Umgang mit der Software. Bei Problemen mit der Praxissoftware wird meist die Hotline der Praxissoftware kontaktiert. [Sch04] Auch für die ständige Wartung und Erweiterung der eigenen IT-Landschaft muss meist, da das Wissen des Praxisleiters oder des Personals nicht ausreicht, ein externer Dienstleister beauftragt werden. [SBJK08]

In diesem Kapitel wurde nun eine Arztpraxis für den Zweck dieser Arbeit vollständig charakterisiert. Im nächsten Kapitel werden nun aufbauend auf diesen Erkenntnissen mögliche IT-Sicherheitsbedrohungen gesucht.

Kapitel 5

IT-Sicherheitsbedrohungen in einer Arztpraxis

Dieses Kapitel dient dazu, mögliche Sicherheitsbedrohungen in einer Arztpraxis aufzudecken und zu erläutern. Diese Bedrohungen stellen jedoch nur einen Ausschnitt aller möglichen Bedrohungen dar. Anhand der aufgezeigten Methodik können viele weitere spezifiziert werden. Wie im Kapitel 4 (Abbildung 4.1) bereits dargestellt, besitzt eine Arztpraxis zahlreiche IT-Komponenten, die sie für die tägliche Arbeit braucht und den Patienten teilweise als Serviceleistung zur Verfügung stellt. Jede diese einzelnen Komponenten kann aufgrund falscher Konfiguration oder beispielsweise aus Unkenntnis der vorhandenen Möglichkeiten zu einer Schwachstelle im IT-System führen. [Kas08] Diese Schwachstellen aufzuzeigen, ist das Ziel dieses Kapitels.

Für die Ermittlung der einzelnen Sicherheitsbedrohungen ist es für die weitere Analyse von Bedeutung, in der Folge drei unterschiedliche Szenarien zu unterscheiden:

1. Bedrohungen für die IT-Systeme
2. Bedrohungen für die Kommunikationsverbindungen
3. Bedrohungen für die Räume

Aufgrund dieser Unterscheidung werden nachfolgend für jedes Szenario unterschiedliche Sicherheitsbedrohungen eruiert.

5.1 IT-Sicherheitsbedrohungen für die IT-Systeme

Basierend auf der Musterpraxis (Abbildung 4.1), werden nun die eingesetzten IT-Komponenten beschrieben und anschließend Anwendungsszenarien

erstellt. Diese dienen dazu, den einzelnen Schutzbedarf jeder IT-Komponente festzustellen und anschließend mögliche Sicherheitsbedrohungen zu erkennen. Die dazugehörigen Maßnahmen werden anschließend gesondert im Kapitel 6 erläutert.

Als ersten Schritt gilt es, die vorhandenen IT-Systeme der Musterpraxis darzulegen. Bei dieser Aufstellung gilt zu beachten, dass IT-Komponenten, die mehrfach vorhanden sind, in eine Gruppe zusammengefasst wurden. Dies betrifft vor allem die Einzelplatzcomputer, die in unterschiedlichster Anzahl in einer Praxis vorhanden sind. Eine Unterscheidung wird hier aufgrund ihres Anwendungsgebietes getroffen. Die folgende Tabelle 5.1 bietet eine Übersicht über die vorhandenen IT-Komponenten in der Musterpraxis (nach Abbildung 4.1):

Bezeichnung	Beschreibung	Standort
S1	DB-Server	Serverraum
C1	Client Empfang	Empfang
C2	Client Behandlungsräume	Behandlungsräume
D1	Drucker	Empfang, Behandlungsräume
T1	Telefon- Faxgeräte	Empfang, Behandlungsräume
G1	Kartenleser	Empfang, Behandlungsräume
G2	Konnektor	Serverraum
G3	Trusted Viewer	Empfang, Behandlungsräume
N1	Router	Serverraum
N2	Firewall	Serverraum
N3	Switch	Serverraum
N4	Wireless Access Point	Je nach Abdeckung in allen Räumen verfügbar

Tabelle 5.1: IT-Komponenten und Systeme in der Musterpraxis [SBJK08]

In der Tabelle 5.1 wurden alle IT-Komponenten der Musterpraxis übersichtlich dargestellt. Notwendige Infrastrukturkomponenten, wie beispielsweise Strom und Netzwerkanschlüsse werden aufgrund der Vereinheitlichung mit der Abbildung 4.1 nicht extra angeführt. Jede Komponente ist einer eindeutigen Bezeichnung zugeordnet. In weiterer Folge wird hier nur mehr diese verwendet. Die Zuordnung einen Standortes wurde deswegen vorgenommen, da die einzelnen Standorte unterschiedlichen Bedrohungen ausgesetzt sind und sich somit unterschiedliche Sicherheitsanforderungen ergeben.
Als nächstes werden den einzelnen Komponenten die typischen Anwendungen in einer Arztpraxis zugeordnet. Diese Zuordnung ist notwendig, um anschließend jeder einzelnen Anwendung den Schutzbedarf nach BSI zuzuordnen. Aufgrund der besseren Übersicht werden diese Zuordnungen folgend in zwei unterschiedlichen Tabellen dargestellt. In der ersten Tabelle 5.2 er-

folgt eine Zuordnung dessen, welche Anwendungen mit welchem Rechner in der Arztpraxis interagieren. In der zweiten 5.3 Tabelle werden anschließend die einzelnen Anwendungen den involvierten Telekommunikations- und Netzkomponenten zugeordnet.
Die folgende Tabelle 5.2 zeigt, welche Anwendungen in einer Arztpraxis durchgeführt werden und welche Rechner damit in Berührung kommen:

Nr	Beschreibung	Patientendaten	S1	C1	C2
A1	Internetrecherche	Ggf.		X	X
A2	Email	Ggf.		X	X
A3	BS-Benutzerauthentifikation	Indirekt	X	X	X
A4	Terminverwaltung	Ja	X	X	X
A5	Patientenverwaltung	Ja	X	X	X
A6	Abrechnung	Ggf.	X	X	X
A7	Drucken	Ja		X	X
A8	Faxen	Ggf.			
A9	Datensicherung	Ja	X		

Tabelle 5.2: Zuordnung der Anwendungen zu den involvierten Rechnern nach [SBJK08]

Da Patientendaten das höchste zu schützende Gut einer Arztpraxis darstellen, wurde in der Zuordnung auch immer angeführt, ob in der betreffenden Anwendung Patientendaten involviert sind. Diese Zuordnung wird später bei der Feststellung des Schutzbedarfes benötigt. [SBJK08]
Die folgende Tabelle 5.3 zeigt die gleichen Anwendungen, jedoch erfolgt jetzt die Zuteilung zu den involvierten Telekommunikations- und Netzkomponenten. Ob Patientendaten involviert sind oder nicht, wird im Folgenden nicht extra gekennzeichnet. Diese Zuordnungen sind aus nachstehender Tabelle 5.2 ersichtlich:

Nr	Beschreibung	T1	G1	G2	G3	N1	N2	N3	N4
A1	Internetrecherche					X	X	X	X
A2	Email					X	X	X	X
A3	BS-Benutzerauthentifikation		X	X				X	X
A4	Terminverwaltung							X	X
A5	Patientenverwaltung		X	X	X			X	X
A6	Abrechnung		X			X	X	X	X
A7	Drucken							(X)	(X)
A8	Faxen	X							
A9	Datensicherung								

Tabelle 5.3: Zuordnung der Anwendungen zu den involvierten IT-Komponenten nach [SBJK08]

Beim Anwendungsfall des Druckens kann nicht genau bestimmt werden, welche Netzkomponenten involviert sind. Je nach Anwendungsfall und von welchen Ort aus gedruckt wird, können verschiedene Komponenten in die Kommunikation eingebunden sein. Aufgrund dieser Unsicherheit erfolgte die Kennzeichnung in Klammern.
Anhand dieser beiden Zuordnungstabellen ist man nun in der Lage, den Schutzbedarf jeder Komponente zu bestimmen. Dies erfolgt durch Analyse der einzelnen Anwendungen. Bei dieser wird für jede Anwendung der Schutzbedarf nach BSI ermittelt.

In der folgenden Tabelle 5.4 werden nun die Ziele der Daten- und Informationssicherheit zu den einzelnen Anwendungen bestimmt. Diese dient als Grundlage für die Bestimmung des Schutzbedarfes der einzelnen IT-Komponenten der Musterpraxis.

Nr	Ziel	Schutzbedarf	Begründung
A1	Vertraulichkeit	Niedrig	Kein wichtiger Bestandteil der Arbeit. Daten sind öffentlich verfügbar.
	Integrität	Normal	Falsche Informationen fallen leicht auf.
	Verfügbarkeit	Niedrig	Für ärztliche Grundversorgung kein Internet zwingend notwendig.
A2	Vertraulichkeit	Niedrig / Sehr Hoch	Abhängig davon, ob Patientendaten übermittelt werden.
	Integrität	Niedrig / Sehr Hoch	Abhängig davon, ob Patientendaten übermittelt werden.
	Verfügbarkeit	Niedrig	Alternativen (Telefon, Fax) verfügbar.
A3	Vertraulichkeit	Hoch	Zugang zum System wird ermöglicht.
	Integrität	Normal	Fehler rasch erkennbar.
	Verfügbarkeit	Normal	Praxisbetrieb nur gering beeinflusst.
A4	Vertraulichkeit	Hoch	Personenbezogene Daten sind betroffen.
	Integrität	Normal	Fehler rasch erkennbar.
	Verfügbarkeit	Normal	Führt zu Unstimmigkeiten. Alternativen verfügbar. (Papier)
A5	Vertraulichkeit	Sehr Hoch	Medizinische Daten sind betroffen.
	Integrität	Hoch	Kann zu Fehlbehandlungen führen.
	Verfügbarkeit	Normal	Betrifft nur ambulante Versorgung.
A6	Vertraulichkeit	Hoch	Rückschlüsse auf Patienten möglich.
	Integrität	Hoch	Kann zu Zahlungsausfällen führen.
	Verfügbarkeit	Normal	Daten können nachgetragen werden.
A7	Vertraulichkeit	Hoch	Personenbezogene Daten sind betroffen.
	Integrität	Niedrig	Fehler werden rasch erkannt.
	Verfügbarkeit	Normal	Alternativen (Handschrift) verfügbar
A8	Vertraulichkeit	Sehr Hoch	Medizinischen Daten sind betroffen.
	Integrität	Niedrig	Fehler werden rasch erkannt.
	Verfügbarkeit	Niedrig	Alternativen (Email, Post) verfügbar
A9	Vertraulichkeit	Sehr Hoch	Medizinische personenbezogene Daten betroffen.
	Integrität	Hoch	Kann zu Fehlbehandlungen führen.
	Verfügbarkeit	Hoch	30jährige Aufbehaltung gesetzlich vorgeschrieben.

Tabelle 5.4: Eintelung des Schutzbedarfes je Anwendung nach [SBJK08]

Mithilfe der Zuordnung der einzelnen Anwendungen zum jeweiligen speziellen Schutzbedarf (Tabelle 5.4) ist es nun möglich, den Schutzbedarf einer einzelnen IT-Komponente der Musterpraxis zu bestimmen. Dies erfolgt durch Zuordnung der einzelnen Anwendungen zu den betreffenden Komponenten. (Tabelle 5.2 & Tabelle 5.3) In der folgenden Tabelle 5.5 wird nun

der Schutzbedarf für die eingesetzten IT-Komponenten ermittelt:

Nr	Ziel	Schutzbedarf	Begründung
S1	Vertraulichkeit	Sehr Hoch	Maximumprinzip (Anwendung A9)
	Integrität	Hoch	Maximumprinzip (Anwendungen A5,A6,A9)
	Verfügbarkeit	Hoch	Maximumprinzip (Anwendung A9)
C1	Vertraulichkeit	Sehr Hoch	Maximumprinzip (Anwendung A2)
	Integrität	Sehr Hoch	Maximumprinzip (Anwendung A2)
	Verfügbarkeit	Normal	Maximumprinzip (Anwendungen A3-A7)
C2	Vertraulichkeit	Sehr Hoch	Maximumprinzip (Anwendung A2)
	Integrität	Sehr Hoch	Maximumprinzip (Anwendung A2)
	Verfügbarkeit	Normal	Maximumprinzip (Anwendungen A3-A7)
D1	Vertraulichkeit	Hoch	Anwendung A7
	Integrität	Niedrig	Anwendung A7
	Verfügbarkeit	Normal	Anwendung A7
T1	Vertraulichkeit	Sehr Hoch	Anwendung A8
	Integrität	Niedrig	Anwendung A8
	Verfügbarkeit	Niedrig	Anwendung A8
G1	Vertraulichkeit	Sehr Hoch	Anwendung A5
	Integrität	Hoch	Maximumprinzip (Anwendungen A3,A5)
	Verfügbarkeit	Normal	Maximumprinzip (Anwendungen A3,A5,A6)
G2	Vertraulichkeit	Sehr Hoch	Anwendung A5
	Integrität	Hoch	Maximumprinzip (Anwendungen A3,A5)
	Verfügbarkeit	Normal	Maximumprinzip (Anwendungen A3,A5)
G3	Vertraulichkeit	Sehr Hoch	Anwendung A5
	Integrität	Hoch	Maximumprinzip (Anwendungen A3,A5)
	Verfügbarkeit	Normal	Maximumprinzip (Anwendungen A3,A5)

Tabelle 5.5: Eintelung des Schutzbedarfes je IT-Komponente nach [SBJK08]

Die Tabelle 5.5 zeigt die einzelnen Schutzziele jeder IT-Komponente der Musterpraxis. Sind einer Komponente mehrere Anwendungen zugeordnet, wurde durchgehend das Maximumprinzip angewandt, da es für den Einsatzzweck im medizinischen Umfeld am besten geeignet ist. Die ausschlaggebenden Anwendungen werden in der Tabelle 5.5 in der Spalte Begründung angeführt. Aufgrund dieser Beurteilung kann mit dem Eruieren möglicher Sicherheitsbedrohungen begonnen werden. Die folgende Tabelle 5.6 veranschaulicht die jeweiligen Sicherheitsbedrohungen der einzelnen IT-Komponenten der Musterpraxis:

Nr	Ziel	Sicherheitsbedrohung
S1,C1,C2	Vertraulichkeit, Integrität Verfügbarkeit	Physischer Zugriff auf die Komponenten Zugriff auf das System Mutwillige Zerstörung, Hardwareausfall
D1	Vertraulichkeit Integrität Verfügbarkeit	Ausspähen der Ausdrucke Physischer Zugriff auf die Komponente Mutwillige Zerstörung, Hardwareausfall
T1	Vertraulichkeit Integrität Verfügbarkeit	Ausspähen der übermittelten Daten beziehungsweise Mithören Physischer Zugriff auf die Komponenten Mutwillige Zerstörung, Hardwareausfall
G1,G2,G3	Vertraulichkeit Integrität Verfügbarkeit	Ausspähen der übermittelten Daten Physischer Zugriff auf die Komponenten Zugriff auf das System Physischer Zugriff auf die Komponenten Physische Zerstörung, Hardwareausfall

Tabelle 5.6: Sicherheitsbedrohungen je IT-Komponente nach [SBJK08]

5.2 IT-Sicherheitsbedrohungen für die Kommunikationsverbindungen

Aufbauend der IT-Sicherheitsanalyse für die IT-Komponenten werden nun die Bedrohungen für die Kommunikationsverbindungen eruiert. Die Basis bildet hierfür wieder die Musterpraxis mit ihren IT-Komponenten (Abbildung 4.1). Die folgende Abbildung 5.1 zeigt die kritischen Verbindungen in der Praxis:

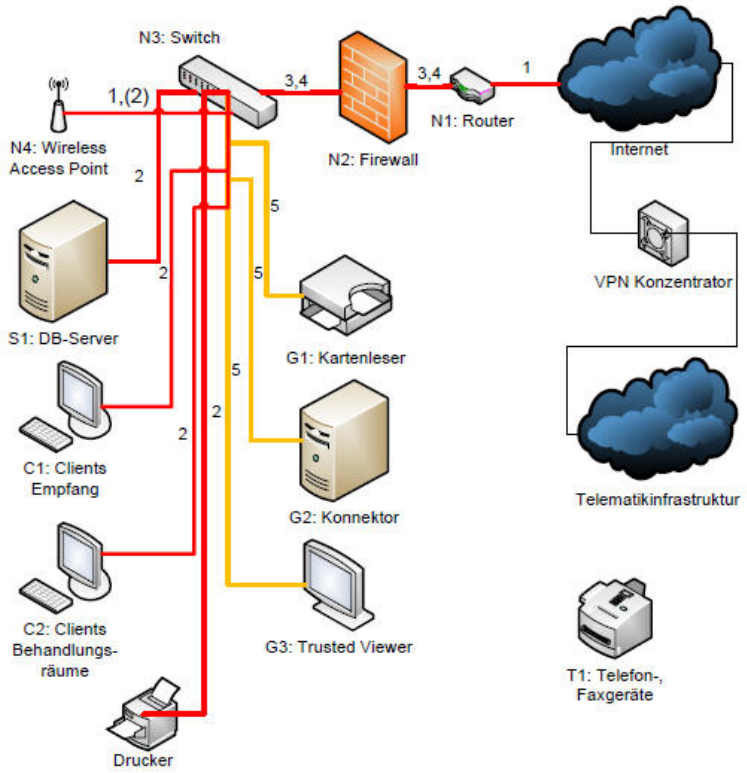

Abbildung 5.1: Kritische Verbindungen des Netzes der Musterpraxis [SBJK08]

In der Abbildung 5.1 werden alle kritischen Verbindungen des Netzes der Musterpraxis abgebildet. Die Nummer neben jeder Kommunikationsverbindung zeigt den Grund, warum eine Verbindung als kritisch eingestuft wurde. Die Ziffern haben folgende Bedeutung: nach [SBJK08]

1. Kritisch aufgrund einer Außenverbindung
2. Kritisch aufgrund von vertraulichen Daten die übertragen werden
3. Kritisch aufgrund hohen Verfügbarkeitsanforderungen durch den Konnektor
   Für den Konnektor ist eine erhöhte Verfügbarkeit zu den Sprech-, Öffnungszeiten gefordert [gem06]
4. Es dürfen nur verschlüsselte, vertrauliche Daten übertragen werden
5. Verbindung der eGK Komponenten

Aufgrund dieser Einstufung ergeben sich folgende Sicherheitsbedrohungen für Kommunikationsverbindungen:

1. Physische Zerstörung
2. Manipulation der Kommunikationsverbindungen
3. Abhören des Datenverkehrs

5.3 IT-Sicherheitsbedrohungen für die Praxisräume

Aufbauend auf den bereits gefundenen Sicherheitsbedrohungen werden nun jene für die Räume der Arztpraxis evaluiert. Zu diesem Zweck muss zuerst bestimmt werden, in welchen Räumen die verschiedensten IT-Komponenten einer Arztpraxis zu erwarten sind. Basierend auf der Zuordnungstabelle 5.1 werden folgende Räume unterschieden:

- Empfang
- Behandlungsräume
- Serverraum

Unter dem Empfang ist jener Raum zu verstehen, wo die Patienten begrüßt werden und sie die Möglichkeit haben, ihr Anliegen zu schildern. In den Behandlungsräumen praktiziert der behandelnde Arzt und im Serverraum wiederum werden alle wichtigen Daten und Unterlagen untergebracht. [SBJK08]
Die folgende Tabelle 5.7 erfasst für jeden Raum den Schutzbedarf nach BSI mit den Zielen der Daten- und Informationssicherheit:

Raum	Ziel	Schutzbedarf
Serverraum	Vertraulichkeit	Hoch
	Integrität	Hoch
	Verfügbarkeit	Hoch
Empfang	Vertraulichkeit	Hoch
	Integrität	Hoch
	Verfügbarkeit	Normal
Behandlungsräume	Vertraulichkeit	Hoch
	Integrität	Hoch
	Verfügbarkeit	Normal

Tabelle 5.7: Schutzbedarf der Räumlichkeiten [SBJK08]

Der in der Tabelle 5.7 festgelegte Schutzbedarf richtet sich dabei vor allem an den jeweiligen Schutzbedarf der IT-Systeme, die sich in den einzelnen Räumen befinden. Befinden sich mehrere IT-Komponenten in einem betrachteten Raum, so kann der Schutzbedarf höher sein als der einzelne

Schutzbedarf der jeweiligen IT-Komponente.
Aufbauend auf dieser Analyse ergeben sich nun beispielhaft die folgenden Sicherheitsbedrohungen für die Räumlichkeiten einer Arztpraxis:

- Überlastete Stromleitungen
- Brand
- Wasserschäden
- Einbruch

Mit dieser letzten Schutzbedarfsanalyse wurden beispielhafte Bedrohungen für das Gesamtsystem Arztpraxis definiert. Die folgende Tabelle 5.8 fasst noch einmal alle Bedrohungen zusammen. Zusätzlich wird dabei jeder Bedrohung eine eindeutige Nummer zugeordnet. Diese wird im folgenden Kapitel 6 zur leichteren Zuordnung benötigt.

Nr	Sicherheitsbedrohung
B1	Physischer Zugriff auf die Komponente
B2	Zugriff auf das System
B3	Physische Zerstörung, Hardwareausfall
B4	Ausspähen der Ausdrucke
B5	Ausspähen der übermittelten Daten, bzw. Mithören
B6	Manipulation der Kommunikationsverbindungen
B7	Abhören des Datenverkehrs
B8	Überlastete Stromleitungen
B9	Brand
B10	Wasserschäden
B11	Einbruch

Tabelle 5.8: Gesamtübersicht Sicherheitsbedrohungen nach [SBJK08]

In der Tabelle 5.8 wurden alle Sicherheitsbedrohungen der Musterpraxis übersichtlich dargestellt. Die Unterscheidung ob es sich dabei um eine Bedrohung der IT-Systeme, der Kommunikationsverbindungen oder der Räumlichkeiten einer Arztpraxis handelt ist in den weiteren Kapiteln irrelevant. Aus diesen Grund ist diese Unterscheidung auch nicht in der Tabelle 5.8 zu finden. Aufbauend auf dieser Auflistung kann nun im nächsten Kapitel 6 begonnen werden, passende Sicherheitsanforderungen zu den einzelnen Sicherheitsbedrohungen zu evaluieren.

Kapitel 6

Sicherheitsanforderungen in einer Arztpraxis

Aufbauend auf dem vorangegangenen Kapitel 5 werden nun beispielhaft geeignete Sicherheitsanforderungen zu den einzelnen Sicherheitsbedrohungen (Tabelle 5.8) beschrieben. Mithilfe dieser Anforderungen werden in den folgenden Abschnitten geeignete Lösungen diskutiert. Diese Lösungen werden grundlegend in zwei Kategorien unterteilt:

- Organisatorische Lösungen
- Technische Lösungen

Unter organisatorischen Lösungen werden Lösungen verstanden, die nicht technischer Natur sind und beispielsweise durch Veränderungen, Optimierung der Organisation in der Arztpraxis zu bewerkstelligen sind. Analog dazu betreffen technische Lösungen nur Veränderungen die mit der Hilfe der IT-Infrastruktur, wie beispielsweise die Verschlüsselung der Datenträger, zu bewerkstelligen sind.

Aufbauend auf der Tabelle 5.8 werden folgend passende Sicherheitsanforderungen beschrieben. Jede Sicherheitsanforderung muss dabei mindestens einer Sicherheitsbedrohung zugeordnet werden können. Diese Zuordnung erfolgt in nachstehender Tabelle 6.1:

Nr	Bedrohung	Sicherheitsanforderungen
A1	B1	IT-Komponenten müssen gegen unautorisierten, physischen Zugriff geschützt sein.
A2	B2	IT-Komponenten müssen gegen unautorisierten Zugriff geschützt sein.
A3	B3	IT-Komponenten müssen gegen Zerstörung dieser geschützt sein.
A4	B3	Es müssen geeignete Maßnahmen getroffen werden, um die Gefahr von Datenverlust zu minimieren.
A5	B4	Ausspähen von Daten und Ausdrucken darf nicht möglich sein.
A6	B5,B7	Das unautorisierte Ausspähen bzw. Mithören der übermittelten Daten muss durch geeignete Maßnahmen verhindert werden.
A7	B6	Kommunikationsverbindungen müssen gegen Manipulation geschützt sein.
A8	B8	Die Auslastung der einzelnen Stromkreise muss so konzipiert sein, dass es zu keiner Überlastung kommt.
A9	B9	IT-Komponenten müssen durch geeignete Maßnahmen gegen Brand geschützt werden.
A10	B10	IT-Komponenten müssen durch geeignete Maßnahmen gegen Wasserschäden geschützt werden.
A11	B11	IT-Komponenten müssen durch geeignete Maßnahmen gegen Diebstahl geschützt werden.

Tabelle 6.1: Gesamtübersicht Sicherheitsanforderungen nach [SBJK08]

In der Tabelle 6.1 sind die einzelnen Sicherheitsanforderungen entsprechend den Bedrohungen in der Musterpraxis angeführt. In der ersten Spalte (Nr) ist jede Anforderung mit einer eindeutigen Nummer versehen. Die Zuordnung der einzelnen Sicherheitsanforderung zu den dazugehörigen Sicherheitsbedrohungen erfolgt in der zweiten Spalte (Bedrohung). Eine detaillierte Beschreibung der einzelnen Bedrohungen ist in der Tabelle 5.8 ersichtlich. Für all diese Bedrohungen gibt es eine resultierende Ursache in der Praxis. Diese können Organisatorischer oder Technischer Natur sein und können dadurch durch geeignete Lösungen kompensiert werden.

Wie im Kapitel 4 erläutert verfügen Ärzte und Helferinnen nur über eingeschränktes IT- Wissen und verstoßen so eventuell unbewusst ohne Vorsatz gegen das Patientengeheimnis oder den Datenschutz. Viele Datenschutzverstöße im ärztlichen Bereich basieren auf Unkenntnis, Sorglosigkeit und

Nachlässigkeit. Dies liegt vor allem daran, dass Erfahrungen der Ärztekammern und deren praktische Erfahrungen mit der Anwendung der Normen zum Patientengeheimnis nirgendwo bedarfsgerecht und systematisch aufbereitet wurde. Dies ist aber nötig, damit diese in breitem Umfang in die Praxis Eingang finden können. Das bisherige Informationsdefizit dürfte einer der Gründe dafür sein, dass es kaum einen Sektor gibt, in dem derart offensichtlich und flächendeckend gegen den Datenschutz verstoßen wurde und wird wie im Medizinbereich. Berichte über Patientenakten in Müllcontainern, offenen Computerbildschirmen in Arztpraxen, Eröffnungen von Krebsdiagnosen im Beisein anderer Patientinnen und Patienten oder unzulässige Datenübermittlungen an Arbeitgeber oder Versicherungen zeigen, dass im Alltag immer wieder Pannen passieren, die manchmal nur peinliche Situationen für die Betroffenen heraufbeschwören, teilweise aber auch für diese existenzielle Konsequenzen haben. [Wei07] Aktiv den Datenschutz und das Patientengeheimnis zu verbessern kann oft mit sehr einfachen Mitteln erfolgen. Beispielsweise kann dieser durch den korrekt aufgestellte Monitore, sodass dritte unbefugt keinerlei Informationen ablesen können, verbessert werden. [Kas10a]
Aufgrund dieser speziellen Situation in den Arztpraxen ist es von Nöten, die unterschiedlichen potentiellen Tätergruppen zu beschreiben und folgend speziell für diese Lösungen für die aufgezeigten Bedrohungen zu eruieren (Tabelle 6.1) In der Arztpraxis werden folgende Tätergruppen unterschieden:

- Bedrohung durch Innentäter
  - Reinigungsdienst
  - IT-Dienstleister
  - Mitarbeiter
- Bedrohung durch externe Angreifer

In der Arztpraxis werden folgend zwei unterschiedliche Tätergruppen unterschieden. In der ersten Gruppe fallen Bedrohungen durch Innentäter. Nach einem aktuellen Lagebericht des BSI zur Lage der IT- Sicherheit in Deutschland werden die meisten Verstöße gegen den Datenschutz von Innentäter ausgeführt. Im Jahre 2009 war diese Tätergruppe für 24 Prozent aller Verstöße verantwortlich. [Bun10] Als Innentäter werden Personen verstanden, die in einer gesellschaftlichen Beziehung mit der Arztpraxis stehen und so ein Vertrauensverhältnis gegenüber diesen Personen besteht. In die Gruppe fallen zum Beispiel Mitarbeiter, Reinigungsdienst und IT-Dienstleister. Alle Personen in diesen Personenkreis können sich in der Praxis frei bewegen und können so unbefugt Daten Dritter ausspähen. Folgende Personenkreise innerhalb dieser Gruppe werden unterschieden: [Rit09]

1. Der Reinigungsdienst:
   Der Reinigungsdienst hat eigenständigen Zugang zu den Praxisräumen, damit die Reinigung außerhalb der Sprechzeiten durchgeführt werden kann und der Praxisablauf nicht gestört wird. Oft kann sich der Reinigungsdienst uneingeschränkt in der Praxis bewegen und hat so physikalischen Zugang zu Computern, Praxisnetz und gegebenenfalls nicht verschlossenen Dokumenten. [Rit09]

2. IT- Dienstleister:
   Wie im Kapitel 4 beschrieben verfügen Ärzte meist nicht das nötige Wissen um die eigene IT- Architektur gesetzeskonform zu betreuen. Aus diesen Grund ist es keine Seltenheit, wenn für diese Aufgabe ein IT- Dienstleister engagiert wird. [Sch04] Aufgrund seiner Tätigkeit muss diesen in der Regel uneingeschränkter Zugriff auf die Computersysteme gewährt werden. Zudem wird meist die Möglichkeit einer Fernwartung genutzt und ein Fernwartungszugang muss dafür eingerichtet werden. [Rit09]

3. Mitarbeiter der Praxis:
   Ärztliches Personal, Sprechstundenhilfen und Hilfskräfte stehen aufgrund ihrer beruflichen Tätigkeit in einem Naheverhältnis mit dem Patienten und erfahren somit schätzenswerte Informationen. Diese anvertrauten Informationen sind vom Patientengeheimnis abgedeckt und das Personal darf diese Informationen in keinster Weise Dritten übermitteln. Zusätzlich verfügen sie meist über einen unbeschränkten Zugriff zu allen Patientendaten im Praxisverwaltungssystem. Dabei wird oft mit generischen Zugangskennungen gearbeitet und eine spätere Analyse, beispielsweise: „Wer hat auf welche Daten zugegriffen?“, ist später nicht mehr möglich. [Rit09]

In die zweite Tätergruppe fallen externe Angreifer. Unter externen Angreifern werden Kriminelle verstanden, die über Datennetze in die Computer der Praxis einbrechen. [Rit09] Dabei ist es unerheblich ob sie ihren Angriff ausserhalb oder innerhalb der Praxis durchführen. Die beste Lösung zum Schutz von Patientendaten im Praxisnetz ist daher eine durchgehende Trennung von Internet und Praxisnetz. Mit dem Einsatz der eGK ist dies aber nicht mehr möglich, da hierbei zwingend mit der Telematikinfrastruktur kommuniziert werden muss. Aus diesen Grunde ist von Nöten, das eigene Praxisnetz entsprechend abzusichern und so unerwünschten Datenfluss auszuschließen. Dabei stehen verschiedene technische Werkzeuge, wie etwa der Einsatz von Firewalls, zur Verfügung. Für die sichere Kommunikation mit der TI steht der Arztpraxis der zwingend einzusetzende Konnektor zur Verfügung. Er beinhaltet unter Anderem eine Firewall und entsprechende VPN- Eigenschaften zum Schutz der sensiblen Patientendaten. [Rit09]

[Deb01]

Aufbauend auf die aufgezeigten Sicherheitsanforderungen, Bedrohungen und Analyse der typischen Tätergruppen in einer Arztpraxis werden in den folgenden Abschnitten passende Lösungen zu den einzelnen Sicherheitsanforderungen beschrieben. Im folgenden Abschnitt 6.1 erfolgt eine Beschreibung der organisatorischen Lösungen.

6.1 Organisatorische Lösungen

In diesen Abschnitt erfolgt eine Beschreibung aller organisatorischen Lösungen die zum sicheren Betrieb der Musterpraxis beitragen. Bei allen Maßnahmen besteht das Ziel, eine oder mehrere Sicherheitsanforderungen (Tabelle 6.1) zu erfüllen. Der erste Bereich betrifft dies IT- Sicherheitssensibilisierung und –schulung der Mitarbeiter in der Arztpraxis.

- **Titel:** IT- Sicherheitssensibilisierung und –schulung
- **Bereich Nr.:** O1
- **Sicherheitsanforderung:** A5,A6
- **Periodizität:** jährlich

Unter *IT- Sicherheitssensibilisierung und –schulung* fallen organisatorische Maßnahmen, die das IT-Wissen und Verständnis der Praxismitarbeiter fördern. Wie im Kapitel 6 kurz angeschnitten passieren viele Verstöße gegen den Datenschutz unbeabsichtigt und aus Unkenntnis. Deswegen ist es zwingend von Nöten diesen Missstand durch organisatorische Maßnahmen, wie etwa Schulungen, auszugleichen. Landesweit werden von verschiedensten Institutionen praxisgerechte Schulungen für Praxispersonal angeboten. Diese Schulungen basieren meist auf Information, Beratung und Überzeugung. Im Selbstcheck können die Ärztinnen und Ärzte feststellen: Reicht die Diskretionszone am Empfang? Kann ein wartender Patient vertrauliche Gespräche mithören? Sind die Behandlungstüren geschlossen? Befinden sich Patientenakten und Karteikarten stets unter Verschluss und nicht für jedermann einsehbar, etwa auf dem Tresen oder im Behandlungsraum? Diese gesammelten Erfahrungen können anschließend sofort praxisgerecht in der eigenen Praxis umgesetzt werden und helfen so aktiv den Datenschutz und die Wahrung des Patientengeheimnisses in der eigenen Praxis zu verbessern. [Wei07] [Sch04]

- **Titel:** Aufbau und Nutzung der IT

- **Bereich Nr.:** O2
- **Sicherheitsanforderung:** A1,A2,A3,A5,A11
- **Periodizität:** täglich

Der nächste Bereich beschäftigt sich mit dem *Aufbau und Nutzung der IT*. Darunter werden organisatorische Maßnahmen verstanden, die aktiv den Datenschutz und die Wahrung des Patientengeheimnisses in der Arztpraxis durch den Aufbau und Nutzung der IT verbessern. Durch falsch aufgestellte Monitore des Computers oder durch unachtsame Nutzung des Druckers können leicht Patientengeheimnisse an unbefugte dritte weitergegeben werden. Die folgenden Hinweise helfen dabei den Datenschutz in der eigenen Praxis zu erhöhen und das Patientengeheimnis zu wahren. [Kas10a]

- Beim Aufbau der technischen Infrastruktur in der Praxis sollte darauf geachtet werden, dass Monitore so aufgestellt werden, dass sie nicht von außen oder von Praxisbesuchern eingesehen werden können.
- Der Server sollte in einem abschließbaren Raum gesichert sein, da er patientenbezogene Daten enthält, die besonders geschützt sein müssen.
- Der Drucker sollte so aufgestellt werden, dass er für Praxisbesucher nicht zugänglich ist, damit ausgedruckte Formulare nicht gestohlen oder eingesehen werden können.
- Falls kein sicherer Raum zur Verfügung steht, so sollten die PC und Datenserver in der Arztpraxis durch andere geeignete Mechanismen gesichert werden. Hier stehen diverse Bügel- sowie Kabelbefestigungen und fest verschweißte Computer Cases zur Auswahl.

Wie in der Auflistung ersichtlich, kann durch Ausübung einfachen, organisatorischen Maßnahmen dazu beigetragen werden, dass der Datenschutz erhöht und das Patientengeheimnis in der Arztpraxis gewahrt bleibt. Die Erfüllung dieser Maßnahmen muss täglich kontrolliert und entsprechend umgesetzt werden. nach [Kas10a]

- **Titel:** Abwehr von Innentätern
- **Bereich Nr.:** O3
- **Sicherheitsanforderung:** A2,A4,A11
- **Periodizität:** täglich

Der nächste organisatorische Bereich beschäftigt sich mit der *Abwehr von Innentätern*. Darunter werden organisatorische Maßnahmen verstanden, die den Datenschutz und das Patientengeheimnis gegenüber Dritten wahren. Verschiedenen Studien nach ist der Informationsabfluss in Unternehmen durch Innentäter am häufigsten. Das BSI spricht in seinem aktuellen Lagebericht der IT-Sicherheit in Deutschland von der größten Tätergruppe mit einen Anteil von 24 Prozent. [Bun10] Diese Zahlen lassen sich zwar nicht direkt auf Arztpraxen abbilden, da sich Patientendaten nicht so gut verkaufen lassen wie Geschäftsgeheimnisse, trotzdem sollte das Risiko durch Innentäter auch in diesem Bereich nicht unterschätzt werden. Folgende Maßnahmen müssen in einer Praxis getroffen werden, um das Risiko von unautorisierten Zugriff auf personenbezogene Daten zu vermindern: [Rit09]

- Der Reinigungsdienst hat eigenständigen Zugang zu den Praxisräumen, damit die Reinigung außerhalb der Sprechzeiten durchgeführt werden kann und der Praxisablauf nicht gestört wird. Oft kann sich der Reinigungsdienst uneingeschränkt in der Praxis bewegen und hat so physikalischen Zugang zu Computern, Praxisnetz und gegebenenfalls nicht verschlossenen Dokumenten. [Rit09]
  - Mit dem Reinigungsdienst ist eine Vertraulichkeitsvereinbarung zu schließen. [Rit09]
  - Die Reinigung sensibler Bereiche muss gesondert geregelt werden. Beispielsweise darf der Serverraum nur zu Zeiten gereinigt werden, in denen verantwortliche Mitarbeiter der Praxis anwesend sind. [Rit09]
- Der IT-Dienstleister hat in der Regel uneingeschränkten Zugriff auf die Computersysteme der Arztpraxis und darüber hinaus besteht oft ein Fernwartungszugang besteht. Dadurch muss mit dem IT-Dienstleister und den jeweiligen Angestellten ebenfalls eine Vertraulichkeitsvereinbarung abgeschlossen werden. Um die Datensicherheit bei Fernwartungszugang zu gewährleisten empfiehlt die Kassenärztliche Bundesvereinigung folgende organisatorischen Voraussetzungen: [Rit09]
  - Die Fernwartung muss ausdrücklich von der Arztpraxis freigegeben werden. [Kas08]
  - Das vom IT-Dienstleister benutzte Passwort muss anschließend durch das Praxispersonal geändert werden. [Kas08]
  - Der Praixsinhaber oder das Personal überwacht die Fernwartung am Monitor in der Praxis. [Kas08]
- Mitarbeiter der Praxis stehen aufgrund ihrer beruflichen Tätigkeit in engen Kontakt mit den Patienten und erfahren so schätzenswerte,

persönliche Informationen. Gesetzlich sind all diese Informationen durch die ärztliche Schweigepflicht geschützt. Trotz diesen Umstandes kann es von Nutzen sein folgende organisatorische Maßnahme zu treffen. [Rit09]

  - Mit dem Mitarbeitern ist eine Vertraulichkeitsvereinbarung zu schließen. [Rit09]

Die einzelnen organisatorischen Maßnahmen sind unabhängig voneinander mit dem jeweiligen Personenkreis durchzuführen und deren Umsetzung täglich zu kontrollieren. nach [Rit09] [Kas08]

- **Titel:** Abwehr von externen Angreifern
- **Bereich Nr.:** O4
- **Sicherheitsanforderung:** A2,A5,A6,A7
- **Periodizität:** täglich

Der nächste organisatorische Bereich beschäftigt sich mit der Abwehr von *Bedrohungen durch externe Angreifer*. Wie eingangs erwähnt ist es deren Ziel in das Praxisnetz einzudringen und Daten Dritter zu entwenden. Dabei gilt es folgende zwei Szenarien zu unterscheiden und jeweils passende Lösungen zu erarbeiten.

- Angriff ausserhalb der Praxis
- Angriff innerhalb der Praxis

Im ersten Szenario versucht der Angreifer über die externe Schnittstelle der Praxis Zugang zum Praxisnetz zu erlangen. In der definierten Musterpraxis (Abbildung 4.1) gibt es zwei voneinander unabhängige Schnittstellen zur Außenwelt. (N4: Wireless Access Point, N1: Router) Beide Schnittstellen stellen bei unsachgemäßer Konfiguration eine Gefahr für das Praxisnetz dar. Bei Angriffen innerhalb der Praxis versucht der Angreifer innerhalb der Praxis Zugang zum Praxisnetz zu bekommen. Folgende organisatorische Maßnahmen sind daher zwingend zum Schutz des IT- Infrastruktur anzuwenden. nach [Rit09] [Bhe06]

- Der Einsatz von Wireless-Local-Area-Network (WLAN) in einer Praxis soll möglichst vermieden werden. Das WLAN- Netz darf dadurch nur bei Bedarf, zum Beispiel während der Praxiszeiten, aktiviert werden. nach [Kas08]

- Überflüssige Accessgeräte sind bei Nichtgebrauch vom Praxisnetz zu trennen. nach [Bhe06]
- Praxisrelevante E-Mailadressen nicht im Internet veröffentlichen und so jeden mitteilen. nach [Bhe06]
- Die einzelnen Clients nur bei Bedarf an das Praxisnetz anschließen. Dabei kann zentral die Stromversorgung des Switches (N3 Abbildung: 4.1) getrennt und bei Praxiszeiten wiededer angeschlossen werden. nach [Bhe06]
- Der Arzt muss sich täglich von den angeschlossenen Peripheriegeräten am Praxisnetz überzeugen und sich vergewissern, dass kein ihm unbekanntes Gerät angeschlossen ist. nach [Kas08]
- Alle nicht verwendeten Netzwerkanschlüsse sind physikalisch zu trennen. nach [Kas08]
- Auszumusternde Datenträger müssen unter Aufsicht des Arztes vernichtet werden. [Kas99]

Wie in der Auflistung ersichtlich, müssen zahlreiche organisatorische Maßnahmen getroffen werden um einen wirksamen Schutz gegen externe Angreifer zu bewerkstelligen. Diese Maßnahmen müssen täglich kontrolliert und umgesetzt werden.

- **Titel:** Abwehr von sonstigen Ereignissen
- **Bereich Nr.:** O5
- **Sicherheitsanforderung:** A8,A9,A10
- **Periodizität:** monatlich

Der nächste Bereich von organisatorischen Maßnahmen beschäftigt sich mit der Abwehrvon Schäden an der IT- Infrastruktur durch Einfluss von natürlichen Ereignissen wie Feuer, Wasser und Ähnliches. In diese Gruppe fallen Maßnahmen, die gravierende Schäden infolge physischer Einwirkung von Feuer, Wasser oder Strom. Viele Geräte dürfen zudem nur unter bestimmten Klimabedingungen betrieben werden. Aus diesen Grunde müssen besonders wichtige IT- Komponenten besonders geschützt werden. Folgende organisatorische Maßnahmen sind deshalb zwingend zum ordnungsgemäßen Betrieb der IT- Infrastruktur notwendig. nach [Kas08]

- Feuerlöscher sind so zu positionieren, dass sie leicht zugänglich sind.
- IT- Komponenten sind mindestens 0,5m über den Boden zu platzieren.

- Die Stromlast jeder einzelnen Leitung muss monatlich auf deren Auslastung überprüft werden um Spannungsspitzen und resultierende Hardwareschäden zu vermeiden.
- Befreiung des Serverraums von brennbaren Materialien um bei einen Feuer Hardwareschäden zu minimieren.

Die angeführten organisatorischen Maßnahmen tragen zum Schutze der IT-Infrastruktur bei sonstigen Ereignissen bei. Diese Maßnahmen gilt es monatlich zu kontrollieren und umzusetzen. nach [Kas08]

In diesem Abschnitt wurden alle organisatorischen Lösungen in der Musterpraxis definiert und beschrieben. Im folgenden Abschnitt 6.2 erfolgt nun analog dazu die Definition und Beschreibung technischer Lösungen.

6.2 Technische Lösungen

In diesen Abschnitt 6.2 erfolgt eine Beschreibung aller technischen Lösungen analog zum Abschnitt 6.1. Bei allen Maßnahmen besteht das Ziel, eine oder mehrere Sicherheitsanforderungen (Tabelle 6.1) zu erfüllen. Der erste Bereich betrifft den Aufbau und Nutzung der IT in der Arztpraxis.

- **Titel:** Aufbau und Nutzung der IT
- **Bereich Nr.:** T1
- **Sicherheitsanforderung:** A2,A4,A6
- **Periodizität:** täglich

In dem Bereich *Aufbau und Nutzung der IT* fallen technische Maßnahmen, die zum Schutze des Patientengeheimnisses und des Datenschutzes unter Berücksichtigung des Umgangs der IT- Infrastruktur beitragen. Durch falsche Nutzung der vorhandenen Infrastruktur können Dritte unbemerkt Einblick in persönliche Daten gewinnen und so den Datenschutz verletzen. Die folgenden technischen Maßnahmen helfen dabei das Risiko eines unerlaubten Zugriffs auf persönliche Daten zu minimieren. nach [Bhe06] [Kas08]

- Durch den richtigen Umgang mit Passwörtern wird die Sicherheit des IT-Systems erhöht. Dazu ist es erforderlich, technisch geeignete Qualitätsanforderungen für ein Passwort zu definieren. Ein verwendetes Passwort in der Arztpraxis sollte deswegen folgende Kriterien erfüllen: [Bhe06]

  - Das Passwort muß min. 6 Zeichen, und darf max. 16 Zeichen lang sein (ein Zeichen ist ein Buchstabe, eine Ziffer, ein Satz- oder Sonderzeichen).
  - Das Passwort muß aus min. 4 Buchstaben und min. 2 anderen Zeichen (Ziffern, Satzoder Sonderzeichen) bestehen.
  - Umlaute und Leerzeichen sind nicht zulässig.
  - Keine Namen weder Benutzernamen noch andere Namen (wie z.B. Vor- oder Nachname).
  - Keine Buchstabenfolgen von der Tastatur wie "qwertzöder ähnliches.
  - Das Passwort darf keinen Begriff bilden, der in irgendeinem Wörterbuch (auch nichtdeutsch) enthalten ist.
  - Empfehlung: Kombination von Groß- und Kleinschreibung.
  - Möglichst dass Passwort so wählen, dass eine Notiz nicht notwendig ist.

- Der verwendete Client in der Praxis sollte bei Nichtgebrauch sofort gesperrt werden. In der Praxis hat sich die Verwendung eines Passwortes für den Bildschirmschoner als praktikabel erwiesen. Bei der Vergabe des Passwortes reicht ein einfaches Passwort. Untersuchungen haben gezeigt, dass bei komplexerer Passwortzusammensetzung, der Passwortschutz in diesem Fall gar nicht mehr aktiviert wird. Zusätzlich muss darauf geachtet werden, dass die Aktivierungszeit entsprechend gering eingestellt ist (1 - 2 Minuten) nach [Bhe06] [Kas08]

- Um IT-Systeme abzusichern, ist eine regelmäßige Informationsbeschaffung über neu aufgedeckte Schwachstellen und Hilfsmittel zu deren Beseitigung notwendig. In der Regel werden sicherheitsrelevante Schwachstellen vom Hersteller selbst beseitigt und mittels Updates ein Patch zur Verfügung gestellt. Deswegen ist es von höchster Priorität Sicherheits-Updates für eingesetzte Software einzuspielen. [Kas08]

- Ein Virenschutz ist auf jeden Arbeitsrechner zwingend einzusetzen. Über Datenträger oder Netze wie Internet und Intranet können Computerviren verbreitet werden. Der Einsatz von Virenschutzprogrammen ist auch für Rechner ohne Internetanschluss oder Netzanbindung verpflichtend. [Kas08]

Wie in der Auflistung ersichtlich, sind mehrere technische Maßnahmen für den reibungslosen Betrieb einer IT- Infrastruktur in der Arztpraxis unerlässlich. Die Erfüllung dieser Maßnahmen muss täglich kontrolliert und entsprechend umgesetzt werden. nach [Kas08]

- **Titel:** Abwehr von Innentätern
- **Bereich Nr.:** T2
- **Sicherheitsanforderung:** A1,A2,A3,A4
- **Periodizität:** täglich

Der nächste technische Bereich beschäftigt sich mit der *Abwehr von Innentätern*. Die nachfolgend beschriebenen technischen Maßnahmen helfen dabei den den Datenschutz und das Patientengeheimnis gegenüber Innentäter wahren. Analog zum Abschnitt 6.1 fallen Mitarbeiter, IT-Dienstleister und Reinigungsdienst unter die Personengruppe der Innentäter. [Rit09]

- Besonders wenn Computer beziehungsweise einzelne Festplatten repariert oder weggeworfen werden, können Unbefugte vertrauliche Daten einsehen oder rekonstruieren. Servicetechniker sollten daher nie allein (ohne Aufsicht) an IT-Systemen oder TK-Anlagen arbeiten. Wenn Datenträger das Haus verlassen, müssen vorher alle Daten sorgfältig gelöscht werden. [Kas08]
- Beim Einsatz der Fernwartung müssen grundlegende Sicherheitsvorkehrungen getroffen werden, um der Datensicherheit genüge zu tun. Folgende Maßnahmen müssen deshalb zwingend umgesetzt werden.
  - Der IT-Dienstleister muss sich mit einem, nur für die aktuelle Sitzung gültigen, Einmal- Passwort anmelden. [Kas08]
  - Die Zugriffsrechte des Technikers müssen auf ein Minimum gesetzt werden [Kas08]
  - Die Wartung einer EDV-Anlage oder jeglicher Fehlerbeseitigung vor Ort darf grundsätzlich nur mit Testdaten erfolgen. Im Notfall, z.B. bei Systemstillstand in einer spezifischen Patientendatenkonstellation, muss der Einblick Dritter in Originaldaten auf besondere Ausnahmefälle eingeschränkt bleiben. [Kas99]
  - Die Fernwartungsdaten zwischen dem Computer des Arztes und des Technikers dürfen nur verschlüsselt und über eine geschützte Verbindung übermittelt werden. [Kas08]
  - Alle Maßnahmen der Fernwartung müssen protokolliert werden. [Kas10a]
- Die Datenträger der in der Arztpraxis verwendeten Notebooks oder PDAs etc. mit Patientendaten, sind vollständig zu verschlüsseln, um bei Diebstahl einen Missbrauch sensibler Daten zu vermeiden. Des Weiteren können auch stationäre Rechner bei einem Einbruch gestohlen werden. Daher ist eine generelle Verschlüsselung, der auf einem

Datenträger befindlichen Patientendaten der Arztpraxis, ausdrücklich zu empfehlen. [Kas08]

Die einzelnen technischen Maßnahmen sind unabhängig voneinander mit dem jeweiligen Personenkreis durchzuführen und deren Umsetzung täglich zu kontrollieren. nach [Kas08] [Kas10a] [Kas99]

- **Titel:** Abwehr von externen Angreifern
- **Bereich Nr.:** T3
- **Sicherheitsanforderung:** A2,A7
- **Periodizität:** monatlich

In den Bereich der technischen Lösungen zum *Abwehr von externen Angreifern* fallen Maßnahmen, die die Sicherheit des IT- Netzes der Arztpraxis gewährleisten. Analog zum Abschnitt 6.1 versucht auch hier der Angreifer entweder von Außen oder von Innen in das Praxisnetz einzudringen. Folgende Maßnahmen sind deshalb zwingend zum Schutze des Praxisnetzwerkes umzusetzen. nach [Kas08]

- Ein Wireless-Local-Area-Network darf nur mit Verschlüsselung betrieben werden, die dem aktuellen Stand der Technik entspricht. Derzeit wird eine Absicherung des WLAN mit WPA2 empfohlen. nach [Kas08] [Kas10a]
- Die Einstellung von Standardpasswörtern in Accounts von Softwareprodukten und Administratorzugängen bei Hardwareprodukten ist allgemein bekannt. Bei Neuinstallation von Produktion muss daher zwingend das Handbuch nach voreingestellten Passwörtern gesichtet und diese umgehend geändert werden. [Kas08]

Die einzelnen technischen Maßnahmen schützen die IT- Infrastruktur von externen Angriffen. Diese Maßnahmen müssen unabhängig voneinander monatlich überprüft und wenn notwendig angewendet werden. nach [Kas08] [Kas10a]

- **Titel:** Abwehr von sonstigen Ereignissen
- **Bereich Nr.:** T4
- **Sicherheitsanforderung:** A9,A10,A11
- **Periodizität:** monatlich

Im letzten Bereich werden Maßnahmen zur Abwehr von Schäden an der IT- Infrastruktur durch Einfluss von natürlichen Ereignissen wie Feuer, Wasser und Ähnliches. Jegliche IT- Komponenten in der Arztpraxis müssen entsprechend geschützt sein und folgend sind die folgenden technischen Maßnahmen zwingend umzusetzen. nach [Kas08]

- Der Schutz der Backup-Medien ist für die Sicherheit der Patientendaten elementar. Am einfachsten gelangen Datendiebe über unzureichend abgesicherte Datensicherungen an sensitive Daten. Zumindest ein abschließbarer Schrank, besser ein Tresor, der auch Schutz vor Feuer bietet, sind erforderlich für die Aufbewahrung der Backup-Medien. [Kas08]
- Arztpraxen sind zwingend durch Türen und Fensterschutz und durch eine Alarmanlage, besonders gegen Einbruch, Sabotage und Diebstahl zu sichern. nach [Kas99]
- Nicht fix verankerte IT- Komponenten sind durch geeignete Diebstahlsicherungen gegen Diebstahl zu sichern.

Die angeführten technischen Maßnahmen tragen zum Schutze der IT- Infrastruktur bei allfälligen Ereignissen, wie Feuer oder Diebstahl, bei. Diese Maßnahmen gilt es monatlich zu kontrollieren und umzusetzen. nach [Kas08]

Kapitel 7

Zusammenfassung und Ausblick

Die eGK ist das derzeit mit Abstand größte E-Ausweisprojekt in Deutschland und hat zugleich einen enormen Stellenwert im Bemühen, das Gesundheitswesen in Deutschland zu modernisieren. Der Mittelpunkt dieses Vorhabens ist eine Smartcard, die an alle Krankenversicherten Deutschlands ausgegeben wird. Die eGK speichert zwar auch wenige Daten auf einen eigenen Chip, der wichtigste Anwendungsbereich ist jedoch der Zugriff auf Online-Angebote. Mit diesen Online-Services wird es beispielsweise möglich sein arztübergreifend auf die persönlichen Patientendaten zuzugreifen. Die Mehrheit zur Verfügung stehender Möglichkeiten sind nicht verpflichtend und können so vom Karteninhaber freiwillig genutzt werden. Der Erfolg oder Misserfolg der eGK lässt sich somit ableiten, in wie weit die freiwilligen Anwendungen auch benutzt werden. Ausschlaggebend wird sein, in wie fern eine Akzeptanz des Einsatzes von Informationstechnologie im Gesundheitswesen existiert. In dieser Diplomarbeit werden die Vorteile aber auch die Risiken des Einsatzes von IT im Gesundheitswesen thematisiert. Mithilfe einer Sicherheitsanalyse nach IT-Grundschutz werden beispielhafte IT-Sicherheitsbedrohungen in einer Arztpraxis aufgezeigt und zugleich passende Sicherheitsanforderungen festgelegt. Diese Anforderungen dienen dazu, passende technische und organisatorische Lösungen aufzuzeigen und so die IT-Sicherheitsanforderungen in einer Arztpraxis zu erfüllen.

Vom ursprüngliche Vorhaben, die eGK nach gesetzlichen Bestimmungen am 1. Januar 2006 einzuführen, ist man mittlerweile weit entfernt. Laut Bundesgesundheitsminister Philipp Rösler müsse die Industrie erst nachweisen, dass die gespeicherten Daten technisch sicher sind. Es ist dadurch unklar, wann die eGK nach der Pilotregion Nordrhein bundesweit eingeführt wird. [Ger09]

Tabellenverzeichnis

Abbildungsverzeichnis

Literaturverzeichnis

[BDHM07] Bales, Stefan ; Dierks, Christian ; Holland, Jana ; Müller, Jürgen: *Die elektronische Gesundheitskarte*. Müller (C.F.Jur.), 2007

[Bhe06] Bhend, Heinz: *IKT-Sicherheit in der Arztpraxis*. 2006

[BNF09] BNFI – Berufsverband Niedergelassener Fachärztlich Tätiger Internisten e.V.: *Einkommenssituation der Ärztinnen und Ärzte*. 2009

[Buna] Bundesministerium der Justiz: *Bürgerliches Gesetzbuch*. http://bundesrecht.juris.de/bgb/index.html. – zuletzt abgerufen am 21. Dezember 2010

[Bunb] Bundesministerium der Justiz: *Bundesdatenschutzgesetz*. http://bundesrecht.juris.de/bdsg_1990/index.html. – zuletzt abgerufen am 21. Dezember 2010

[Bunc] Bundesministerium der Justiz: *Signaturgesetz*. http://bundesrecht.juris.de/sigg_2001/index.html. – zuletzt abgerufen am 21. Dezember 2010

[Bund] Bundesministerium der Justiz: *Sozialgesetzbuch V*. http://bundesrecht.juris.de/sgb_5/index.html. – zuletzt abgerufen am 21. Dezember 2010

[Bune] Bundesministerium der Justiz: *Strafgesetzbuch*. http://bundesrecht.juris.de/stgb/index.html. – zuletzt abgerufen am 21. Dezember 2010

[Bunf] Bundesministerium der Justiz: *Verordnung über den Schutz vor Schäden durch Röntgenstrahlen*. http://bundesrecht.juris.de/r_v_1987/index.html. – zuletzt abgerufen am 21. Dezember 2010

[Bung] Bundesärztekammer: *Berufsordnung für die deutschen Ärztinnen und Ärzte*. http://www.bundesaerztekammer.de/

page.asp?his=1.100.1143. – zuletzt abgerufen am 21. Dezember 2010

[Bun08] Bundesamt für Sicherheit in der Informationstechnik: *IT Grundschutz Katalog 10. Ergänzungslieferung*, 2008

[Bun10] Bundesamt für Sicherheit in der Informationstechnik: *Die Lage der IT-Sicherheit in Deutschland 2009.* 2010

[BWB+02] Bultmann, Marion ; Wellbrock, Rita ; Biermann, Heinz ; Engels, Jürgen ; Ernestus, Walter ; Höhn, Udo ; Wehrmann, Rüdiger ; Schurig, Andreas: *Datenschutz und Telemedizin - Anforderungen an Medizinnetze.* 2002

[Cau06] Caumanns, Jörg: Der Patient bleibt Herr seiner Daten: Realisierung des eGK-Berechtigungskonzepts über ein ticketbasiertes, virtuelles Dateisystem. In: *Informatik-Spektrum* Band 29, Nummer 5 (2006), S. 323–331

[Deb01] Debold & Lux Beratungsgesellschaft für Informationssysteme und Organisation im Gesundheitswesen mbH Hamburg: *Kommunikationsplattform im Gesundheitswesen.* secunet Security Networks AG Essen, 2001

[Del08] Delvos, Andreas: *Die elektronische Gesundheitskarte - Einführung in das deutsche Gesundheitswesen.* GRIN Verlag, 2008

[DMHB07] Dierks, Christian ; Müller, Jürgen ; Holland, Jana ; Bales, Stefan: *Die elektronische Gesundheitskarte: Rechtskommentar, Standpunkte und Erläuterungen für die Praxis.* Müller (C.F.Jur.), 2007

[Eck04] Eckert, Claudia: *IT-Sicherheit Konzepte - Verfahren - Protokolle.* Oldenbourg Verlag München Wien, 2004

[EMC] EMC Corporation: *Elektronische Gesundheitskarte: Ein Schritt in die Selbstbestimmtheit.* http://germany.emc.com/leadership/business-view/interview-dak-asklepios.htm. – zuletzt abgerufen am 21. Dezember 2010

[Fäs08] Fässler, Lukas: *Elektronische Signatur: Unterschreiben & Verschlüsseln.* BPX Edition, 2008

[GC06] Goode, Sigi ; Cruise, Sam: What Motivates Software Crackers? In: *Journal of Business Ethics* Band 65, Nummer 2 (2006), S. 173–201

[gem06] gematik GmbH - Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH: *Konnektorspezifikation - Teil 1 Allgemeine Funktionen und Schnittstellen des Konnektors V0.6.0*, 2006

[gem08a] gematik GmbH - Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH: *Übergreifendes Sicherheitskonzept der Telematikinfrastruktur: Anhang B - Sicherheitsanforderungen V2.4.0*, 2008

[gem08b] gematik GmbH - Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH: *Übergreifendes Sicherheitskonzept der Telematikinfrastruktur: Anhang C - Schutzbedarfsanalyse V2.4.0*, 2008

[gem08c] gematik GmbH - Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH: *Übergreifendes Sicherheitskonzept der Telematikinfrastruktur V2.4.0*, 2008

[gem08d] gematik GmbH - Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH: *Die Spezifikation der elektronischen Gesundheitskarte - Äußere Gestaltung V2.2.0*, 2008

[gem08e] gematik GmbH - Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH: *Konnektorspezifikation V3.0.0*, 2008

[gem08f] gematik GmbH - Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH: *PKI für CV-Zertifikate Grobkonzept V1.5.0*, 2008

[gem08g] gematik GmbH - Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH: *Spezifikation der elektronischen Gesundheitskarte - Grundlegende Applikationen V2.2.1*, 2008

[gem08h] gematik GmbH - Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH: *Spezifikation eHealth-Kartenterminal V2.8.0*, 2008

[gem08i] gematik GmbH - Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH: *Testbericht Feldtest Release 1 V1.0.3*, 2008

[gem08j] gematik GmbH - Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH: *Whitepaper Sicherheit*, 2008

[gem08k] gematik GmbH - Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH: *Zulassungsverfahren für die Erstellung der kryptographischen Identität von Konnektoren V1.3.0*, 2008

[gem09a] gematik GmbH - Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH: *Gesamtarchitektur V1.7.0*, 2009

[gem09b] gematik GmbH - Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH: *Speicherstrukturen der eGK für Gesundheitsanwendungen V1.8.0*, 2009

[Ger09] Gerlof, Hauke: Ist die Gesundheitskarte ein Auslaufmodell, oder gibt es einen Neustart 2010? In: *Ärzte Zeitung* (2009)

[Goe07] Goetz, Christoph: Heilberufsausweise / Fraunhofer-Institut für Sichere Informationstechnologie. 2007. – Forschungsbericht

[GR05] Gammel, Berndt ; Rüping, Stefan: Smart cards inside. In: *Solid-State Device Research Conference, 2005. ESSDERC 2005. Proceedings of 35th European*, 2005, S. 69 – 74

[Hae04] Haeberlen, Thomas: *IT-Sicherheit - Grundschutz und Schutzbedarf.* Bundesamt für Sicherheit in der Informationstechnik, 2004

[Han08] Hanika, Heinrich: *Telematische Kooperationen für regionale Vernetzungen im Lichte des europäischen und deutschen Rechts.* Telemed 2008, 2008

[HCH07] Hamilton, Stephen ; Carlisle, Martin ; Hamilton, John: A Global Look at Authentication. In: *Information Assurance and Security Workshop, 2007. IAW '07. IEEE SMC*, 2007, S. 1–8

[Hei07] Heitmann, Marcus: *IT-Sicherheit in Unternehmungen.* DUV, 2007

[Hei08] Heike, Elisabeth: VDE-Standard für Datenschutz in der Telemedizin. In: *Ärzteblatt* Nummer 4 (2008), S. 2

[HN08] Höpken, Andreas ; Neumann, Helmut: *Datenschutz in der Arztpraxis. Ein Leitfaden für den Umgang mit Patientendaten.* Müller Heidelberg, 2008. – 440 S.

[Hor98] Horster, Patrick: *Chipkarten.* Vieweg & Teubner Verlag, 1998

[HP03] Hoppe, Gabriela ; Priess, Andreas: *Sicherheit von Informationssystemen*. NWB Verlag, 2003

[JLG09] Jin, Ji fang ; Lu, Er hong ; Gao, Xian wei: Resistance DPA of RSA on Smartcard. In: *Information Assurance and Security, 2009. IAS '09. Fifth International Conference on*, 2009, S. 406 –409

[Kas99] Kassenärztliche Vereinigung Bayerns: *Ärztliche Schweigepflicht - Datenschutz in der Arztpraxis - Sicherheit der Praxis-EDV*. 1999

[Kas08] Kassenärztliche Bundesvereinigung: *Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis*. Deutsches Ärzteblatt 105, Heft 19, 2008

[Kas10a] Kassenärztliche Bundesvereinigung: *Anforderungen an Hard- und Software in der Praxis*, 2010

[Kas10b] Kassenärztliche Bundesvereinigung: *Installationsstatistik - Anbieter*, 2010

[KGS07] Koch, Klaus ; Gehrmann, Ulrich ; Sawicki, Peter: Primärärztliche Versorgung in Deutschland im internationalen Vergleich: Ergebnisse einer strukturvalidierten Ärztebefragung. In: *Ärzteblatt* Band 104, Nummer 38 (2007), S. 84

[KLC09] Kang, Junki ; Lee, Deok-Gyu ; Choi, Dooho: Convolutive Noise Filtering in Power Analysis on Smartcards Using the Cepstrum. In: *Embedded and Multimedia Computing, 2009. EM-Com 2009. 4th International Conference on*, 2009, S. 1–4

[KLK06] Klapdor, Sebastian ; Leimeister, Marco ; Krcmar, Helmut: Die eGK und die Telematikinfrastruktur für das deutsche Gesundheitswesen / Technische Universität München, Lehrstuhl für Wirtschaftsinformatik. 2006. – Forschungsbericht

[Kra04] Krauss, Thomas: *Viren, Würmer und Trojaner*. Interest Verlag, 2004

[KT05] *Kapitel* Echtzeit-Business fordert Sicherheit, Vertrauen und Verfügbarkeit. In: Kuhlin, Bernd ; Thielmann, Heinz: *Real-Time Enterprise in der Praxis*. Springer Berlin Heidelberg, 2005, S. 307–317

[Len06] Lenssen, Klaus: IT-Sicherheitsbewusstsein von Telearbeitern steht im Gegensatz zu ihrem Verhalten / Cisco Systems GmbH. 2006. – Forschungsbericht

[MPRNS08] Martínez-Peláez, Rafael ; Rico-Novella, Francisco ; Satizábal, Cristina: Secure smart card reader design. In: *Consumer Electronics, 2008. ISCE 2008. IEEE International Symposium on*, 2008, S. 1–3

[MSS00] McCubbin, Christopher ; Selguk, Ali A. ; Sidhu, Deepinder: Initialization vector attacks on the IPsec protocol suite / University of Maryland Baltimore County Baltimore. 2000. – Forschungsbericht

[NFS08] Naujokat, Frédéric ; Fiedler, Arno ; Schwab, Wolfgang: Akzeptanz von Vertrauensräumen in IT-Infrastrukturen. In: *Datenschutz und Datensicherheit* Band 32, Nummer 9 (2008), S. 605–609

[Opp07] Oppliger, Rolf: IT security: in search of the Holy Grail. In: *Communications of the ACM* Band 50, Nummer 2 (2007), S. 96 – 98

[Org] Organisation für wirtschaftliche Zusammenarbeit und Entwicklung: *Gesundheitsdaten 2009*. `http://www.oecd.org/dataoecd/15/1/39001235.pdf`. – zuletzt abgerufen am 21. Dezember 2010

[Par00] Parag, Lala: *Self-Checking and Fault-Tolerant Digital Design*. Morgan Kaufmann, 2000

[Pat02] Patterson, David: A Simple Way to Estimate the Cost of Downtime / Computer Science Division, University of California at Berkeley. USENIX Association, 2002. – Forschungsbericht

[Phi09] Philipp, Stefan: Hardwaresicherheit von Smart Card ICs. In: *Elektrotechnik und Informationstechnik* Band 118, Nummer 10 (2009), S. 477–480

[PKS07] Partha, Dasgupta ; Karmvir, Chatha ; Sandeep, Gupta: Vulnerabilities of PKI based Smartcards. In: *Military Communications Conference, 2007. MILCOM 2007. IEEE*, 2007, S. 1–5

[PR06] Pomberger, Gustav ; Rechenberg, Peter: *Informatik Handbuch*. Hanser Fachbuchverlag, 2006

[Ran08] Rankl, Wolfgang: *Handbuch der Chipkarten*. Hanser Fachbuch, 2008

[RE03] Rankl, Wolfgang ; Effing, Wolfgang: *Smart Card Handbook*. John Wiley & Sons, Ltd, 2003

[Rit09] Rittmeier, Raffael: *Grundzüge eines Sicherheitskonzepts für Arztpraxen unter Berücksichtigung der Gesundheitstelematik*. 2009

[Ron] Ronellenfitsch, Michael: *Die elektronische Gesundheitskarte und die neue Telematikinfrastuktur*. `http://www.datenschutz.hessen.de/dg003.htm`. – zuletzt abgerufen am 21. Dezember 2010

[SBJK08] Sunyaev, Ali ; Beck, Johannes ; Jedamzik, Siegfried ; Krcmar, Helmut: *IT-Sicherheitsrichtlinien für eine sichere Arztpraxis*. Shaker, 2008

[Sch] Schaar, Peter: *Datenschutzrechtliche Rahmenbedingungen der elektronischen Gesundheitskarte*. `http://www.bfdi.bund.de/cln_029/nn_531010/DE/Oeffentlichkeitsarbeit/RedenUndInterviews/2005/RedeElektronischeGesundheitskarte.html`. – zuletzt abgerufen am 21. Dezember 2010

[Sch04] Schlegel, Verena: *IT in Arztpraxen – keine heile Welt*. Computer Reseller News, 2004

[Sch09] Schmeh, Klaus: *Elektronische Ausweisdokumente*. Hanser Fachbuch, 2009

[Sch10] Schneglberger, Gabriele: *Technische, organisatorische und gesellschaftliche Aspekte der Privatsphäre unter den Bedingungen der vernetzten Gesellschaft*, Technische Universität Wien, Fakultät für Informatik, Institut für Gestaltungs- und Wirkungsforschung, Diplomarbeit, 2010

[SCL09] Sere, Ahmadou ; Cartigny, Julien ; Lanet, Jean: Automatic detection of fault attack and countermeasures. In: *WESS '09: Proceedings of the 4th Workshop on Embedded Systems Security*, ACM, 2009, S. 1–7

[SD06] *Kapitel* Der Weg des Patienten durch die Praxis. In: Schüller, Anne ; Dumont, Monika: *Die erfolgreiche Arztpraxis*. Springer Berlin Heidelberg, 2006, S. 129–159

[Sei06] Seibold, Holger: *IT-Risikomanagement*. Oldenbourg, 2006

[SKD09] Schurr, Michael ; Kunhardt, Horst ; Dumont, Monika: *Unternehmen Arztpraxis—Ihr Erfolgsmanagement*. Springer Berlin Heidelberg, 2009

[Spi] Spiegel Online: *Skandal um Callcenter - Telekom meldet Datenklau.* `http://www.spiegel.de/wirtschaft/0,1518,572855,00.html`. – zuletzt abgerufen am 21. Dezember 2010

[TMTN03] Thorsten, Fischer ; Martin, Neebe ; Thorsten, Juchem ; Norbert, Hampp: Biomolecular optical data storage and data encryption. In: *NanoBioscience, IEEE Transactions on* Band 2, Nummer 1 (2003), S. 1–5

[Uns07] Unseld, Isabell: Mangelhafte Einweisung von Mitarbeitern birgt Gefahren für Unternehmen / McAfee GmbH. 2007. – Forschungsbericht

[Wei04] Weichert, Thilo: Die Elektronische Gesundheitskarte. In: *Datenschutz und Datensicherheit* Band 28, Nummer 7 (2004), S. 391–403

[Wei07] Weichert, Thilo: Aktion „Datenschutz in meiner Arztpraxis“. In: *Praktische Arbeitsmedizin* 8 (2007), S. 36–38

[Wit08] Witt, Bernhard: *Datenschutz kompakt und verständlich.* Friedrich Vieweg & Sohn Verlag, 2008

[WRCB06] Wagner, Hans ; Rowe, Gerard ; Choluj, Bozena ; Beichelt, Timm: *Europäische Sozialpolitik.* Vs Verlag, 2006