Entwurf und Beschreibung wesentlicher Komponenten einer Sicherheitsarchitektur für medizinische Forschungsnetze

Dissertation

zur Erlangung des mathematisch-naturwissenschaftlichen Doktorgrades
„Doctor rerum naturalium“
der Georg-August-Universität Göttingen

vorgelegt von
Michael Grenz
aus Ust-Kamenogorsk, Kasachstan

Göttingen im August 2012

D7
Referent: Prof. Dr. Ulrich Sax
Korreferent: Prof. Dr. Klaus Pommerening
Tag der mündlichen Prüfung: 20.06.2012

Zusammenfassung

Die Durchführung einer qualifizierten medizinischen Forschung erfordert die Speicherung und die Auswertung einer großen Menge von forschungsrelevanten Patientendaten. Daraus ergeben sich hohe Anforderungen an Datenschutz und Datensicherheit.
In der hier vorliegenden Arbeit werden die mit der Handhabung dieser Daten verbundenen Risiken im Hinblick auf ihr Gefahrenpotenzial analysiert und die Strategien der Risikobewältigung vorgestellt. Es erfolgt eine kritische Auseinandersetzung mit den bisherigen Arbeiten über die Sicherheitsaspekte in der medizinischen Forschung. Bei den unterbreiteten Ergänzungs- und Verbesserungsvorschlägen steht die praktische Umsetzbarkeit stets im Vordergrund.
Die Arbeit zeigt auf, wie der Einsatz verfügbarer Ressourcen durch Standardisierung, Synergien sowie eine gezielte Risikopolitik optimiert werden kann. Zur Unterstützung für die Durchführung einer gezielten Risikopolitik wird ein im Rahmen dieser Arbeit entwickeltes Konzept des dynamischen Sicherheits- und Risikomanagements vorgeschlagen. Die vorliegende Arbeit ist als ein erweiterungsfähiges Rahmenwerk der Forschungsnetzsicherheit zu verstehen.

Abstract

The ability to successfully execute medical research requires the storage and interpretation of a large amount of research relevant patient information. This requires a strict adherence to stringent standards of data security and data protection.
In the present doctoral thesis, the risk potential of handling such data is analyzed and strategies for risk reduction are described. The thesis performs a critical examination of already existing work on the security aspects of the medical research networks. The practical feasibility of the recommendations provided was considered foremost.
The thesis shows how the usage of the available resources can be optimized through standardization, synergy and a determined policy toward managing risks. As part of this thesis a concept of dynamic risk management is developed. The proposed risk portfolio evaluation method enables goal oriented efficient risk handling. This thesis should be understood as an extendable security framework for medical research networks.

Danksagung

Mein Dank gilt allen, die mich bei der Erstellung meiner Doktorarbeit unterstützt haben. Herzlich bedanke ich mich bei Herrn Prof. Dr. Klaus Pommerening für die Überlassung dieses spannenden Themas und für seinen beispielhaften fachlichen und persönlichen Beistand während meines Promotionsvorhabens. Meinem Doktorvater Herrn Prof. Dr. Ulrich Sax möchte ich meinen tiefen Dank für seine vorbildliche Leitung und die Freiheiten, die er mir bei der Entwicklung der Arbeit ließ, aussprechen.

Bei Herrn Prof. Dr. Otto Rienhoff bedanke ich mich für sein hervorragendes Engagement, seine aufbauenden, lehrreichen Gespräche und die Möglichkeit, in seiner Abteilung Medizinische Informatik der Universitätsmedizin Göttingen intensiv an meiner Dissertation arbeiten zu dürfen. Zu großem Dank bin ich Herrn Prof. Dr. Dieter Hogrefe für seine Unterstützung bei der Aufnahme in das GAUSS-Promotionsprogramm sowie seine konstruktiven und hervorragenden Vorschläge verpflichtet. Des Weiteren gilt mein Dank Herrn Prof. Carsten Damm und Herrn Prof. Dr. Jens Grabowski für ihre Unterstützung beim Abschluss meiner Promotion.

Für die umfangreiche Hilfe, die ausgezeichneten Materialien und die vielen spannenden Diskussionen möchte ich mich bei den Mitgliedern der TMF-Arbeitsgruppe Datenschutz und insbesondere bei Herrn Dr. Johannes Drepper bedanken. Herrn Prof. Dr. Sebastian Iwanowski und Herrn Prof. Dr. Uwe Schmidt danke ich dafür, dass sie mich zur Aufnahme der Promotion ermuntert haben.

Meinen Kommilitonen und den Mitarbeitern der Abteilung Medizinische Informatik der Universitätsmedizin Göttingen danke ich für die kurzweiligen Stunden und lebhaften Diskussionen: Mein Dank gilt vor allem Sabine Rey, Frank Dickmann, Krister Helbing und Dr. Ghislain Kouematchoua. Dankbar bin ich auch Frau Gabriele Staupe für ihre Anregungen und ihre Engelsgeduld.

Zu großem Dank bin ich meinen Eltern, Anatol und Natalie Grenz, sowie meiner Schwester Anna verpflichtet, die mir immer zur Seite gestanden haben. Sie haben mich unermüdlich bei der Erstellung der Dissertation unterstützt. Meiner lieben Partnerin Tatjana danke ich von ganzem Herzen für ihre Liebe und ihr Verständnis.

Inhaltsverzeichnis

1. Einleitung

Die Gesundheit ist ein transzendentales Gut und stellt die Basisvoraussetzung für die Zielverwirklichung eines Individuums und somit für die Chancengleichheit in der Gesellschaft dar (vgl. [Mar08, S. 888]). Die immanente Ungleichheit der Gesundheit lässt sich nur teilweise durch das Gesundheitsverhalten eines Einzelnen erklären und beeinflussen. Vielmehr wird angenommen, dass etwa die Hälfte der gesundheitlichen Ungleichheit durch die sozio-ökologischen Faktoren wie beispielsweise Arbeits- und Wohnverhältnisse bedingt ist, die ein Individuum kaum verändern kann (vgl. [Mie10, S. 237]). Gesundheitsinformationen erlauben somit nicht nur Rückschlüsse über den Gesundheitszustand, sondern auch über die soziale Umgebung eines Individuums. Die Verfügbarkeit der Gesundheitsdaten breiter Bevölkerungsschichten birgt erhebliche Potenziale an gesellschaftlicher Steuerung und Kontrolle in sich (vgl. [Wel03, S. 80]).
Die Gesundheitsdaten gehören daher zu den höchst sensiblen persönlichen Informationen und müssen sorgfältig gemäß den Regeln der Ethik sowie nationalen und internationalen Datenschutzbestimmungen gehandhabt werden (vgl. [PSM+08, S. 7]). Die Befolgung dieser Regeln sorgt für die Sicherung der Grundrechte und erfordert den konsequenten Einsatz starker Maßnahmen wie beispielsweise sichere technische Lösungen und auch vertrauenswürdige Organisationen (vgl. [PSM+09, S. 1745]). Mit dem Oberbegriff „medizinisches Forschungsnetz“ oder dem Synonymbegriff „medizinischer Forschungsverbund“ bezeichnet man eine vernetzte Organisation mit der Zielsetzung, medizinische Daten oder Proben zu sammeln, langfristig aufzubewahren und diese für diverse wissenschaftliche Fragestellungen auszuwerten. Der Begriff umfasst die Kompetenznetze in der Medizin, Biomaterialdatenbanken, Koordinierungszentren für klinische Studien sowie weitere, i. d. R. krankheitsspezifische Netze und Register (vgl. [tmf10]).

1.1. Problemstellung und Motivation

Ein medizinisches Forschungsnetz ist bestrebt, eine qualifizierte Forschung durch die Speicherung und die Auswertung forschungsrelevanter Patientendaten zu betreiben. Aus diesem Grund versuchen die Forschungsverbünde die Behandlungsdaten ihrer Patienten zusammenzuführen, um die für die Forschung notwendigen Datenvolumina zu erreichen (vgl. [RDSP06, S. 2]). Die meisten Forschungsnetze weisen ähnliche Strukturen auf wie die universitären Einrichtungen. Dies ist für die Erfüllung der hohen Anforderungen an den Datenschutz und die Datensicherheit nicht einfach, da die Strukturen i. d. R. nicht für

die hohen Sicherheitsanforderungen ausgerichtet sind. In den meisten Fällen befinden sich die Qualitätssicherungsprozesse im Entwicklungsstadium und halten den z. T. komplexen Abläufen nicht stand. Erschwert wird die Situation durch teilweise fehlende Erfahrungen im Bereich Informationssicherheit, einem permanenten Mangel an Finanzmitteln und an Personal.

1.2. Ziele der Arbeit

Die Arbeit an der vorliegenden Dissertationsschrift wurde mit der Zielsetzung aufgenommen, die wesentlichen Bestandteile einer Sicherheitsarchitektur für die Bewältigung von sicherheitstechnischen und datenschutzrechtlichen Herausforderungen zu entwerfen und zu beschreiben, die die medizinischen Forschungsnetze mit sich bringen. Unter Sicherheitsarchitektur wird dabei die Gesamtheit der Informationssicherheitskonzepte und der daraus abgeleiteten Sicherheitsmaßnahmen verstanden (vgl. [kes12]). Die grundlegende Zielsetzung besteht in der Entwicklung von praktisch implementierbaren Konzepten. Die maßgeblichen gesetzlichen Vorschriften sowie die bereits vorhandenen Strukturen, Entwicklungen und Arbeiten, die den Sicherheitsbereich innerhalb der medizinischen Forschung betreffen, waren zu berücksichtigen.
Die Vielzahl relevanter Datenschutz- und Datensicherheitsvorschriften kann eine ungünstige Ausrichtung der Sicherheitsarchitektur auf die punktuelle Erfüllung einzelner Mindestanforderungen begünstigen. Untersuchungen zum IT-Portfoliomanagement belegen die aus der Einzelbetrachtung der Risiken resultierenden Gefahren. Sie unterstreichen die Notwendigkeit einer korrekten Integration und Aggregation einzelner Bewertungsgegenstände (vgl. [Zim08]). Um die einseitige Ausrichtung der Sicherheitsmaßnahmen zu vermeiden, gilt es, die für die Forschungsnetze relevanten Schadensszenarien zu ermitteln und die vorgestellten Sicherheitskonzepte an solchen Schadensszenarien zu orientieren. Die einzelnen Sicherheitskonzepte als Bestandteile der Sicherheitsarchitektur sollen sich harmonisch ergänzen und einen wirksamen Schutz gegen die Schadensszenarien bieten. Durch diese Ausrichtung soll der Einsatz verfügbarer knapper Ressourcen medizinischer Forschungsnetze optimiert werden. Das übergeordnete Ziel dieser Arbeit ist es, ein erweiterungsfähiges Rahmenwerk für die Gestaltung der Sicherheitsarchitektur zu erstellen, das generisch auf eine Reihe von Forschungsnetzen anwendbar ist.

1.3. Thematische Abgrenzung

Im Mittelpunkt der vorliegenden Arbeit steht die Beschreibung wesentlicher Sicherheitsarchitekturkomponenten für die medizinischen Forschungsnetze in Deutschland. Die in dieser Arbeit verwendete Definition für ein medizinisches Forschungsnetz bzw. Forschungsverbund wurde aus der Satzung der TMF übernommen, die sich als Dachverband für medizinische

Forschungsverbünde in Deutschland begreift. In der Satzung wird ein medizinisches Forschungsnetz als eine vernetzte Organisation verstanden, die den Zweck verfolgt, Daten oder Proben für die medizinische Forschung zu sammeln, langfristig aufzubewahren und für verschiedene, oft noch nicht feststehende wissenschaftliche Fragestellungen auszuwerten. Der Begriff „medizinische Forschungsnetze“ bzw. „medizinische Forschungsverbünde“ umfasst medizinische Kompetenznetze, Koordinierungszentren für klinische Studien, Biomaterialbanken und andere, meist krankheitsspezifische Forschungsnetze und Register (vgl. [tmf10], s. a. die Begriffsdefinition im Glossar). Auch die neu entstehenden nationalen Zentren für spezifische Krankheitsgruppen (Herzerkrankungen, Diabetes, Krebs, neurodegenerative Erkrankungen etc.) kann man dazu rechnen.
Diese Definition ist recht weit gefasst und schließt auch lose Kooperationen von öffentlich rechtlichen oder privatrechtlichen Organisationen mit einer Vielzahl möglicher Ausprägungen der Kooperationsformen ein. Aus diesem Grunde ist der untersuchte Themenbereich einzugrenzen. Die Beschreibung der in dieser Arbeit vorgestellten Sicherheitsarchitekturkomponenten basiert auf den Datenschutz- und Datensicherheitskonzepten, die im Rahmen der TMF entwickelt wurden. Folglich können die Ausführungen vor allem auf solche Forschungsnetze angewendet werden, die die TMF-Vorlagen im Hinblick auf die Verfahrensweisen als Grundlage haben. Als gemeinsame Werkzeuge kommen dabei die Anonymisierung bzw. Einwilligungserklärung, die Pseudonymisierung, das Identitätsmanagement sowie die informationelle Gewalteneinteilung zum Einsatz (vgl. [Pom11a]). Es müssen gemeinsame Verfahren und Module vorhanden sein, um eine Dynamisierung der Sicherheits- und Risikoportfolio-Bewertung mithilfe des in der vorliegenden Arbeit entwickelten Konzeptes „dynSRM“ erfolgreich zu realisieren.
Im Rahmen dieser Arbeit werden die gestellten Anforderungen an die Forschungsnetze in Bezug auf die Sicherheitsmaßnahmen untersucht. Zudem wird aufgezeigt, welche Anforderungen in den Netzen bezüglich der Gestaltung dieser Maßnahmen bestehen. Vor allem stehen dabei die Verbesserungsmöglichkeiten bei der Auswahl und der Umsetzung von Sicherheitsmaßnahmen im Fokus. Ziel dieser Sicherheitsmaßnahmen ist es, ein möglichst hohes Niveau an Sicherheit mit den verfügbaren Mitteln zu gewährleisten. Es werden Vorschläge entwickelt, wie das Sicherheitsniveau der bestehenden und zukünftigen medizinischen Forschungsnetze erhöht werden kann.

1.4. Aufbau der Arbeit

Nach diesem Einleitungskapitel folgt die Beschreibung des angewendeten methodischen Forschungsansatzes im Kapitel 2, das mit einer kurzen Aufzählung der bei der Erstellung der Dissertation verwendeten Werkzeuge und Vereinbarungen schließt. Mit den Anforderungen an die Sicherheitsdienste im Bereich der medizinischen Forschung befasst sich das Kapitel 3 „Bestandteile der Sicherheitsarchitektur für medizinische Forschungsnetze“. Nach einer generellen Einführung in den Themenbereich der Absicherung von medizinischen Forschungsnetzen und der Gestaltung von Sicherheitsrichtlinien als Be-

standteile einer Sicherheitsarchitektur werden in den drei Hauptabschnitten (3.3, 3.4 und 3.5) organisatorische, administrative und technische Aspekte der Sicherheitsmaßnahmen beschrieben. Die Möglichkeiten einer effizienten Gestaltung von Sicherheitsmaßnahmen werden im Rahmen der Analyse aktueller Sicherheits- und Risikomanagementansätze in den ersten beiden Abschnitten des vierten Kapitels (4.1 und 4.2) untersucht. Einer qualitativen Analyse der Gefährdungssituation im Bereich der medizinischen Forschung, die mithilfe der schutzbedarfs- und gefährdungsorientierten Ansätze durchgeführt wird (Abschnitt 4.3 „Qualitative Bewertung der Bedrohungs- und Risikosituation“), folgt die Herleitung eines quantitativen dynamischen Sicherheits- und Risikobewertungskonzeptes im Abschnitt 4.4. Das Basiskonzept wird durch die Kombination mit den BSI IT-Grundschutz-Katalogen weiterentwickelt und seine praktische Umsetzbarkeit wird anschließend mithilfe einer prototypischen Implementierung verifiziert.
Im fünften Kapitel erfolgt eine kritische Auseinandersetzung mit den Ergebnissen der Arbeit im Hinblick auf die im Rahmen der Arbeit unterbreiteten Empfehlungen für die Ausgestaltung von Sicherheitsmaßnahmen und dem entwickelten Konzept zur Bewertung und Steuerung des Sicherheitsmaßnahmenportfolios. Am Ende des Kapitels wird die Bedeutung der Arbeit im Hinblick auf den aktuellen Stand der Forschung eingeordnet. Zudem wird aufgezeigt, dass weitere Untersuchungen im Bereich der Sicherheit von medizinischen Forschungsnetzen notwendig sind. Im abschließenden sechsten Kapitel erfolgt eine kurze Zusammenfassung der wichtigsten Bestandteile dieser Arbeit. Ein Ausblick auf weiteren Forschungsbedarf rundet die vorliegende Arbeit ab.

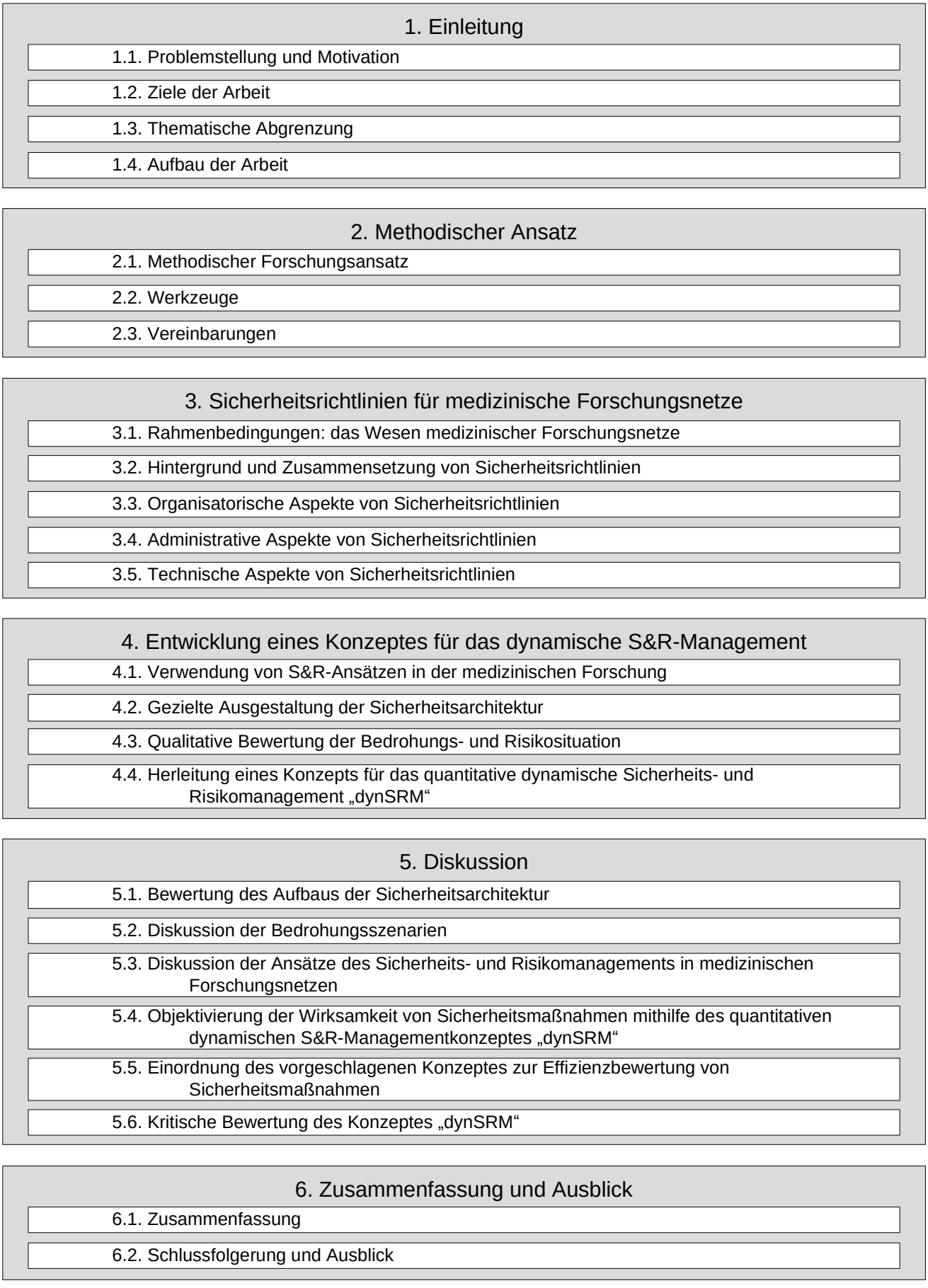

Abbildung 1.: Aufbau der Arbeit: Beschreibung der Sicherheitsarchitektur und Entwicklung eines Konzeptes zur effizienten Steuerung des Sicherheits- und Risikoportfolios stehen im Mittelpunkt dieser Arbeit.

2. Methodischer Ansatz

In diesem Kapitel werden die in dieser Arbeit eingesetzten Untersuchungsmethoden, die forschungsleitenden Fragen und das Forschungsdesign vorgestellt und erläutert.

2.1. Methodischer Forschungsansatz

Bisherige Datenschutz- und Datensicherheitskonzepte, die im Rahmen der Technologie- und Methodenplattform für die vernetzte medizinische Forschung (TMF) [tmf12] erstellt wurden, dienten dieser Arbeit als Basis. Insbesondere sind an dieser Stelle die generischen Datenschutzkonzepte der TMF [RDSP06], [SPR+06] und diverse Arbeiten zu der Weiterentwicklung und Ergänzung dieser Konzepte zu nennen. Es galt dieses und viel zusätzliches Material zu sichten und zu interpretieren. Konzepte und Empfehlungen der dieser Arbeit zugrunde liegenden Werke wurden zu keinem Zeitpunkt als Axiome angesehen und stets kritisch begutachtet und hinterfragt. In Fällen der Nichtübereinstimmung der Meinung des Autors mit diesen Konzepten wurden Änderungsvorschläge unterbreitet und durch die Abwägung ihrer Vor- und Nachteile begründet.
Bei den in der Arbeit unterbreiteten Vorschlägen wurde stets großer Wert auf ihre praktische Implementierbarkeit gelegt: Alle vorgeschlagenen Konzepte können mithilfe der heute verfügbaren Technologie mit einem vertretbaren Aufwand realisiert werden.

2.1.1. Organisation der Vorgehensweise

2.1.1.1. Forschungsleitende Fragen

Forschungsleitende Fragen legen die grobe Zielrichtung des wissenschaftlichen Interesses fest und dienen als Vorstufe des Forschungsdesigns (vgl. [Töp09, S. 128 f.]). Bei der Konzeption dieser Arbeit wurden drei forschungsleitende Fragen formuliert:

F1: Welche Anforderungen werden in Bezug auf die organisatorischen, technischen und administrativen Sicherheitsmaßnahmen an die medizinischen Forschungsnetze gestellt, und welche Anforderungen bestehen in Bezug auf die Sicherheitsmaßnahmen in den medizinischen Forschungsnetzen?

F2: Wie können die Sicherheitsmaßnahmen in den medizinischen Forschungsnetzen effizient gestaltet werden?

F3: Wie kann die Wirksamkeit von Sicherheitsmaßnahmen in den medizinischen Forschungsnetzen objektiv bewertet werden?

2.1.1.2. Thesenbildung

Neben den genannten forschungsleitenden Fragen wurden zwei Thesen formuliert, um die Konzeptualisierung und Operationalisierung des Forschungsprojektes zu stärken. Die Thesen bilden die substanziellen inhaltlichen Schussfolgerungen der Ausführungen und werden in der Arbeit auf der Basis der Darstellung der relevanten Sachverhalte und des bisherigen Forschungsstandes entwickelt und vorgestellt (vgl. [Töp09, S. 143 f.]). Folgende zwei Thesen werden in dieser Arbeit aufgestellt:

T1: Eine ganzheitliche Ausrichtung der Sicherheitsmaßnahmen ist notwendig, um einen umfassenden Schutz eines medizinischen Forschungsnetzes durch die Kombination von organisatorischen, technischen und administrativen Maßnahmen zu erreichen.

T2: Das Konzept des dynamischen Sicherheits- und Risikomanagements ermöglicht eine Verbesserung der Bewertung der Wirksamkeit von Sicherheitsmaßnahmen in einem medizinischen Forschungsnetz.

2.1.1.3. Forschungsdesign und Entstehung der Arbeit

Die wesentlichen Komponenten des Forschungsdesigns einer Arbeit sind die Aussagenart und das Untersuchungsziel (vgl. [Töp09, S. 123 f.]). Unter der Verwendung der erweiterten zweidimensionalen Klassifikation nach Fritz (vgl. [Fri95, S. 59 f.]) kann das Forschungsdesign der vorliegenden Arbeit als „exploratorisch-instrumentell“ eingeordnet werden. Das in der Abbildung 2 visualisierte Forschungsdesign kombiniert die erkenntnisorientierten und handlungsorientierten Elemente, die sich auf die kontingenztheoretische bzw. situative Analyse stützen (vgl. [Töp09, S. 136 f.]). Auf der Einflussebene sind die maßgeblichen Faktoren aufgeführt, die in einer Strategie zur Elimination bzw. Reduktion von Risiken resultieren. Auf der Gestaltungsebene ergibt sich eine zentralisierte Steuerung der Sicherheitsmaßnahmen ab, die ihrerseits durch die bestehenden Risiken und Wirksamkeit von Sicherheitsmaßnahmen bestimmt wird. Aus den einzelnen Effekten wird auf der Wirkungsebene eine Optimierung des Sicherheits- und Risikoportfolios abgeleitet.
Der für die Beantwortung der ersten forschungsleitenden Frage (F1) untersuchte Themenkomplex „Datenschutz und Datensicherheit“ in der medizinischen Forschung wurde in der jüngsten Zeit diversen gravierenden Veränderungen unterworfen. Auch wenn die grundlegenden Problembereiche dieses Themenkomplexes sich kaum verändert haben, erfuhren die zu berücksichtigenden Rahmenbedingungen in Form der Gesetzgebung und der technisch-organisatorischen Entwicklung einen starken Wandel. Seit der ersten Sichtung des verfügbaren Materials für diese Arbeit im Frühjahr 2006 und dem Zeitpunkt der Fertigstellung des letzten Kapitels am Anfang des Jahres 2012 verzeichnete der gesamte Themenbereich einen enormen Entwicklungsfortschritt. Die ursprünglich noch als Rohfassungen verfügbaren Konzepte entwickelten sich zu beachtlichen Werken, die die Rollen der beteiligten Parteien und des rechtlichen Rahmens aufzeigen und erläutern. Die mit der Veröffentlichung der generischen Datenschutzkonzepte im Jahr 2006 begonnene

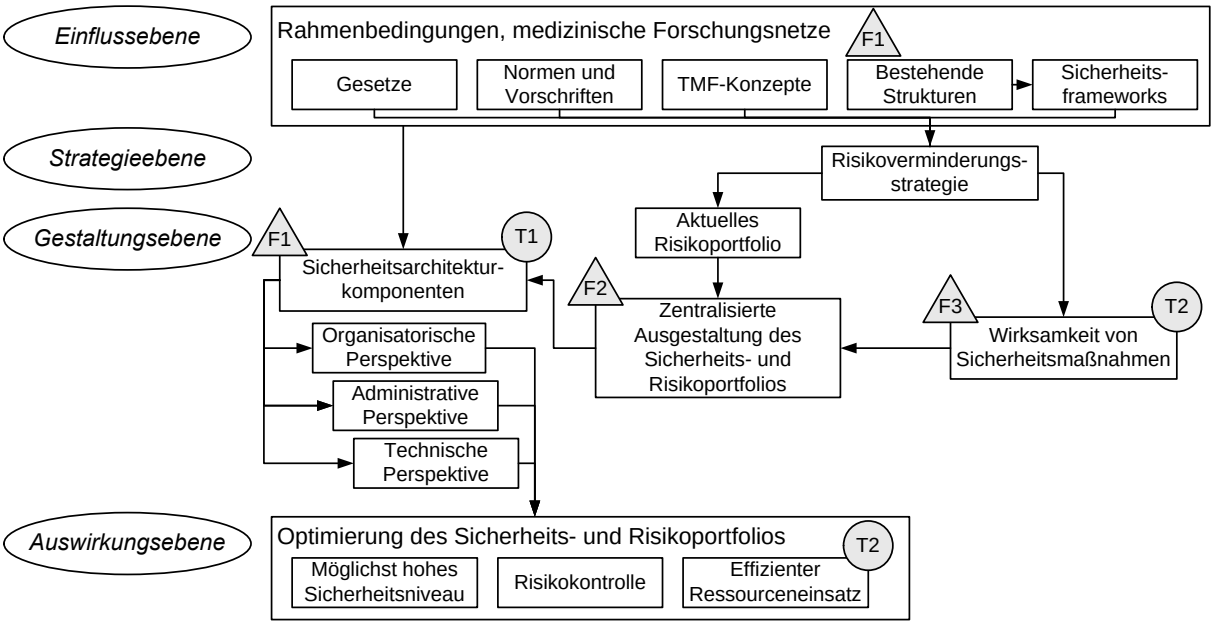

Abbildung 2.: Kennzeichnung der Thesen und forschungsleitenden Fragen im Forschungsdesign: Auf der Einflussebene sind die maßgeblichen Faktoren aufgeführt, die in einer Strategie zur Elimination bzw. Reduktion von Risiken resultieren. Auf der Gestaltungsebene leitet sich eine zentralisierte Steuerung der Sicherheitsmaßnahmen ab, die ihrerseits durch die bestehenden Risiken und Wirksamkeit von Sicherheitsmaßnahmen bestimmt wird. Aus den einzelnen Effekten wird auf der Wirkungsebene eine Optimierung des Sicherheits- und Risikoportfolios abgeleitet.

TMF-Schriftenreihe zählt inzwischen neun Bände[1] und leistet einen unschätzbaren Beitrag zur Gestaltung und Weiterentwicklung der vernetzten medizinischen Forschungsvorhaben.

2.1.1.4. Systematische Literaturrecherche

Die Arbeitsgruppe Datenschutz der TMF e. V. [tmf12] berät in ihrer Koordinierungsfunktion medizinische Forschungsprojekte und -einrichtungen in Datenschutz- und Datensicherheitsfragen. Die von der Arbeitsgruppe durchgeführten und in Auftrag gegebenen Arbeiten und Gutachten zu Fragen des Datenschutzes und der Verbundforschung sind für die Ausgestaltung der Datenschutz- und Datensicherheitskonzepte in Deutschland maßgebend. Die von der Arbeitsgruppe im Jahr 2003 entwickelten generischen Datenschutzkonzepte erleichtern den Forschungsverbünden die Erstellung spezifischer Datenschutzkonzepte und deren Abstimmung mit den Datenschützern. Im August 2012 bestand das Mitgliedernetzwerk der TMF aus 82 Forschungsverbünden. Dies spricht für die immense nationale Bedeutung der aufgebauten Strukturen und Lösungen.
Für die Untersuchung der zweiten forschungsleitenden Frage (F2) nach den Ansätzen für die effiziente Gestaltung von Sicherheitsmaßnahmen in den medizinischen Forschungsnetzen wurden die verfügbaren TMF-Materialien analysiert. Für die Zurverfügungstellung der Materialien und die geleistete Unterstützung möchte der Autor sich erneut bei der Geschäftsstelle der TMF e. V. und insbesondere bei den Mitgliedern der Arbeitsgruppe

[1] Stand: August 2012.

Datenschutz bedanken. Im Mittelpunkt der Untersuchung stand die Fragestellung, welche Normen, Standards und Frameworks im Bereich der Informationssicherheit derzeit von den medizinischen Forschungsnetzen eingesetzt werden, und der Einsatz welcher Normen, Standards und Frameworks grundsätzlich als möglich bzw. empfehlenswert diskutiert wird.[2] Die dadurch als relevant ermittelten Informationssicherheits-Frameworks wurden auf ihre Eigenschaften im Hinblick auf die Bewertung der Sicherheitsmaßnahmeneffizienz und folglich ihrer Potenziale für die effiziente Gestaltung der Sicherheitsarchitektur untersucht. Im ersten Schritt wurden alle mit der Arbeitsgruppe Datenschutz der TMF abgestimmten Datenschutzkonzepte der medizinischen Forschungsnetze[3] einer Analyse unterzogen. Auch weitere TMF-Materialien wurden studiert, um ein möglichst vollständiges Bild über die aktuell verwendeten oder geplanten Ansätze des Sicherheits- und Risikomanagements zu erhalten. Insbesondere die Unterlagen des Workshops „V016-01 Sicherheitskonzepte“ und des Projektes „V071-01 IT Service Management“ der TMF enthielten für die untersuchte Fragestellung relevante Informationen. Die in den analysierten Konzepten referenzierten Werke[4] wurden im Rahmen der sogenannten Schneeballsuche ebenfalls in die Untersuchung miteinbezogen.

Die durchgeführte Analyse verdeutlichte die unterschiedliche Handhabung der Fragestellung im Hinblick auf die Notwendigkeit und die Steuerung von Sicherheitsinvestitionen in den untersuchten Frameworks. Da die Normen und Standards nicht den aktuellen Stand der Forschung auf dem Gebiet der Informationssicherheit widerspiegeln, wurde die dritte forschungsleitende Frage (F3) im Rahmen einer systematischen Literaturrecherche erforscht. Dafür wurden während der oben beschriebenen Analyse der TMF-Materialien und der in ihnen referenzierten Frameworks die Bestandteile des Themas in Fachtermini übertragen, systematisch gesammelt und zusammen mit den häufig verwendeten Ausdrücken in tabellarischer Form festgehalten. Die Tabelle 17 im Anhang B fasst die zusammengetragenen Suchbegriffe zusammen. Die Relevanz (Ranking) der Suchbegriffe für das Thema „Messbarkeit von Informationssicherheit bzw. Sicherheitsmaßnahmen“ wurde vermerkt. Anschließend wurden die mit dem Rankingwert 0 gekennzeichneten Suchbegriffe für die primäre Suche verwendet:

```
De: Sicherheit AND
(Metrik* OR Messen OR Messung* OR Kennzahl* OR Messbarkeit)
En: Security AND
(metric* OR measure* OR measurement* OR measuring OR measurability)
```

[2] Aus Vereinfachungsgründen wird im Folgenden lediglich von (Informationssicherheits-)Frameworks gesprochen, wobei damit auch die Normen und die Standards für die Informationssicherheit gemeint sind. Die Definition und Abgrenzung der genannten Begriffe befindet sich im Glossar.

[3] [ABC+11], [DC06], [EW06], [GK10], [GM08], [Han11], [HHH06], [HHM+05], [HV08], [HWE05], [Ill02a], [Ill02b], [klr10a], [KP10], [Law06], [Lut07], [MM03], [NB04], [Spe04], [Spi07], [Min08], [Wöh08], [Wie03].

[4] Zum Beispiel Normen der ISO-Reihe, COBIT, ITIL Information Security-Management, BSI IT-Grundschutz-Kataloge etc.

Die Primärsuche wurde in insgesamt zehn Literaturdatenbanken[5] durchgeführt und lieferte 3.275 Treffer. Die Tabelle 18 im Anhang B dokumentiert folgende Aspekte der durchgeführten Recherche:

- Angaben zur Literaturdatenbank,
- Datum der Suche,
- verwendete Suchbegriffe und Suchstrategie,
- verwendete Kriterien für die Verfeinerung der Suche,
- Anzahl der Suchtreffer.

Die Präzisierung der Suche in Form der Relevanz der Suchtreffer erfolgte mithilfe der Suchbegriffe mit dem Rankingwert 1:

```
De: Bewerten, Bewertung, Effektivität, Effizienz, Kennzahlen,
Kennzahlensystem(e), Kosten-Nutzen-Analyse, KNA, Sicherheitsinvesti-
tion(en), Sicherheitsmaßnahme(n), Wirksamkeit, Framework(s), Rahmen,
Rahmenwerk(e).
En: assess, assessment, efficiency, effectiveness, performance, figure(s),
ratio(s), ratio system(s), cost benefit analysis, CBA, security invest(s)
OR investment(s), safety or security measure(s), framework(s).
```

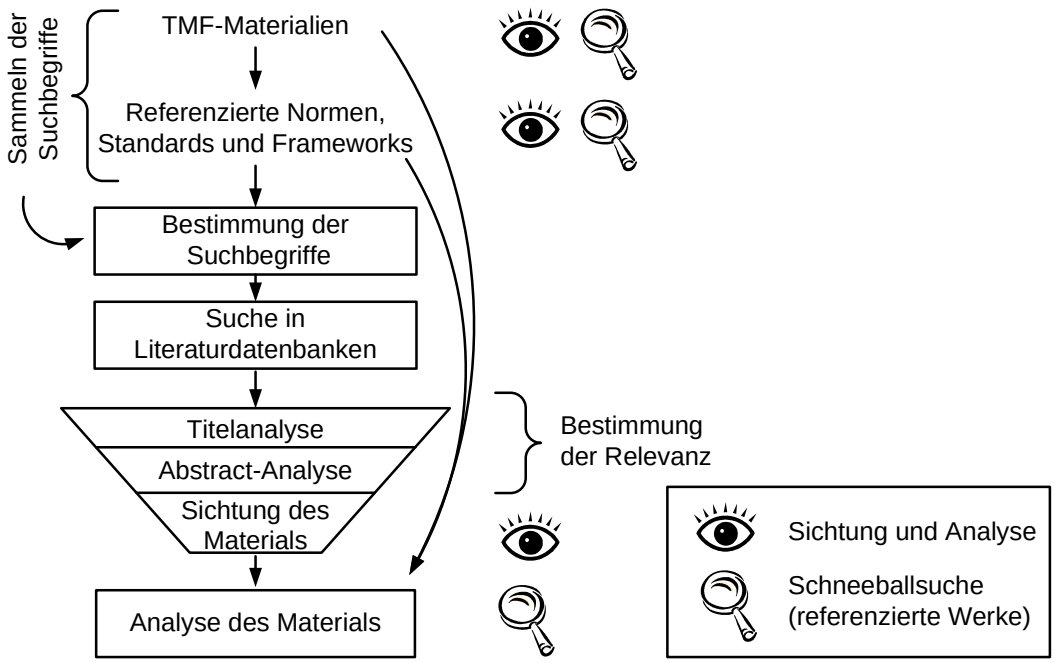

Abbildung 3.: Methodische Vorgehensweise bei der Durchführung der Literaturrecherche: Um die Literaturrecherche möglichst vollständig zu gestalten, wurde eine mehrstufige Vorgehensweise nach dem Trichter-Modell gewählt (vgl. [Töp09, S. 314 f.]).

[5]Unter anderem wurden KVK, MEDLINE, ISI Web of Science, ACM Digital Library, IEEE Digital Library und Google Scholar für die Suche verwendet.

Nach der Präzisierung der Suchbegriffe, Eliminierung von Dubletten und der sekundären Filterung anhand der Suchbegriffe mit dem Rankingwert 2 wurden 754 Werke als potenziell relevant identifiziert. Im nächsten Schritt wurden diese einer Abstract-Analyse unterzogen; die als relevant identifizierten Quellen wurden anschließend beschafft und untersucht. Während der Materialanalyse wurde stets die Schneeballsuche der referenzierten Werke angewendet (vgl. [Töp09, S. 312 ff.]). Die Abbildung 3 stellt die verwendete Vorgehensweise grafisch dar. Die wichtigsten für die untersuchte Problemstellung relevanten Werke sind mit der Angabe zum verwendeten bzw. empfohlenen Ansatz im Abschnitt B.2 aufgelistet.

2.1.2. Vorgehensweise zur Entwicklung des Konzeptes für das dynamische Sicherheits- und Risikomanagement „dynSRM“

Die im vorhergehenden Abschnitt beschriebene Analyse der Informationssicherheits-Frameworks verdeutlichte die Nachteile der untersuchten Ansätze. Es entstand die Überlegung, ein für die Bedürfnisse der Forschungsnetze speziell zugeschnittenes Sicherheits-Framework, zusammenzustellen. Die zwei bestehenden und etablierten Konzepte – die Risikomatrix und der Risikodreiklang nach [Mül11] – wurden kombiniert und weiterentwickelt. Auf dieser Basis wurde ein Konzept für das quantitative dynamische Sicherheits- und Risikomanagement, abgekürzt „dynSRM“, ausgearbeitet. Im nächsten Schritt erfolgte die Anwendung des Basiskonzeptes auf der Grundlage der BSI IT-Grundschutz-Kataloge [bsi11d]. Um die Implementierbarkeit des Konzeptes zu beweisen, erfolgte anschließend eine prototypische Implementierung. Die aus der Analyse des aktuellen Forschungsstandes zu der Wirksamkeitsbewertung von Sicherheitsmaßnahmen gewonnenen Erkenntnisse wurden verwendet, um das entwickelte Konzept im Hinblick auf die aktuelle Forschung einzuordnen und den Nachweis für die Erfüllung maßgeblicher Qualitätskriterien zu erbringen.

2.2. Werkzeuge

Bei der Literaturverwaltung und den Zitaten fand die Norm DIN 1505-2 in der erweiterten Form des BibTeX-Styles `ALPHADIN.BST` ihre Anwendung [Lor06]. Die in der Arbeit vorhandenen UML-Diagramme orientieren sich am UML-Standard 2.1.2 [obj12]. Die erstellten SecureUML-Diagramme entsprechen den in [Lod03] vorgestellten Konventionen. Beide Diagrammtypen wurden mithilfe von IBM Rational Software Architect 8.0.4 [ibm12] und NClass [tih12] angefertigt.

2.3. Vereinbarungen

Um die Lesbarkeit dieser Arbeit zu erhöhen, erfolgt am Ende eines jeden Kapitels eine Zusammenfassung der Kapitelinhalte. Die Quellcode-Auszüge werden durch `Schreibmaschinenschrift` hervorgehoben. Einige Stichwörter und Aufzählungspunkte werden im Text durch **fette** bzw. *kursive* Schrift gekennzeichnet.

Die Definitionen der meisten im Glossar aufgeführten Begriffe entstammen dem Glossarium der Arbeitsgruppe „Datenschutz“ der Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V. [tmf12] sowie dem zum Zeitpunkt der Erstellung dieser Arbeit noch nicht veröffentlichten Glossar für die Revisionsfassung des generischen Datenschutzkonzeptes der TMF. Einige zumeist technische Begriffsdefinitionen wurden aus dem Lexikon Datenschutz-Praxis [wek12], dem ARCHmatic-Glossar und -Lexikon [Oeb12], dem <kes>-Lexikon der Informationssicherheit [kes12] sowie der freien Enzyklopädie Wikipedia [wik12] übernommen. Auf die explizite Kennzeichnung der Urheberschaft einzelner Glossarbegriffe wird im Folgenden verzichtet.

3. Bestandteile der Sicherheitsarchitektur für medizinische Forschungsnetze

Im vorliegenden Kapitel werden die Anforderungen an die Sicherheitsarchitektur im Zusammenhang mit der medizinischen Forschung untersucht. Es wird sowohl geprüft, welche Anforderungen an die Forschungsnetze in Bezug auf die Sicherheitsmaßnahmen gestellt werden als auch welche Anforderungen in den Netzen an die Gestaltung der Sicherheitsarchitektur bestehen.

3.1. Rahmenbedingungen: das Wesen medizinischer Forschungsnetze

Mithilfe von medizinischen Forschungsnetzen erfolgt die Bündelung von Kompetenzen zur Weiterentwicklung des medizinischen Wissens, die grob in die klinische, epidemiologische Forschung und die Grundlagenforschung eingeteilt werden können. Im Rahmen der klinischen Forschung werden Studien direkt an Patienten beispielsweise zur Prüfung neuer Therapieverfahren durchgeführt. Die epidemiologische Forschung untersucht die Langzeiteffekte von Krankheiten sowie deren Ursachen und Trends im Bevölkerungsbezug. Im Rahmen der Grundlagenforschung werden die Daten zu wissenschaftlichen Zwecken prozessiert. Die Grundlagenforschung ist heute zum großen Teil genetisch orientiert und arbeitet zunehmend mit Biomaterialien und genetischen Informationen (vgl. [Pom11a]).
Allen drei Forschungsarten ist gemeinsam, dass für ihre Durchführung viele qualitativ hochwertige medizinische Datensätze in kürzester Zeit untersucht und ausgewertet werden müssen. Die teilnehmenden Parteien[1] eines Forschungsnetzes befinden sich in einem permanenten Interessenkonflikt. So wünschen sich beispielsweise Patienten eine optimale Behandlung und eine möglichst geringe Beeinträchtigung durch die Aufnahme ihrer Daten in eine Forschungsdatenbank. Sponsoren und Wissenschaftler streben eine möglichst detaillierte Speicherung und unkomplizierte Auswertung von Forschungsnetzdaten an. Um die Regeln der Handhabung der hoch sensiblen medizinischen Daten und Proben

[1] Ärzte, Patienten, Wissenschaftler, Sponsoren etc.

nach den maßgeblichen ethischen Regelungen sowie nationalen und internationales Datenschutzbestimmungen zu vereinheitlichen, wurden im Rahmen der Technologie- und Methodenplattform für die vernetzte medizinische Forschung (TMF e. V.) generische Schemenbeschreibung für die Prozessierung von medizinischen Daten entwickelt (vgl. [RDSP06], [Pom07]). Die generischen Konzepte, deren wichtigsten Aspekte die informationelle Gewaltenteilung, Pseudonymisierungskonzepte sowie Vorlagen für die Patienteneinwilligung, Policies und Verträge sind, dienen als Grundlage für die Entwicklung der spezifischen Konzepte konkreter Forschungsnetze und vereinfachen somit die Abstimmung mit den zuständigen Datenschutzverantwortlichen (vgl. [PSM+08], [HDR+10]).
Die Patienteneinwilligung stellt die Grundlage für die Datenverarbeitung dar. Das grundsätzliche Recht eines jeden Patienten, seine Einwilligung zu widerrufen, kann eingeschränkt werden, z. B. durch Anonymisierung der Daten oder durch gesetzliche Bestimmungen (vgl. [HIB+06], [SPR+06], [Ron04]). Die Einwilligung wird vom behandelnden Arzt eingeholt und ist die notwendige Voraussetzung für die folgende Datenverarbeitung. Der Patient wird dabei über seine Rechte, den Umfang der erhobenen Daten und deren Verwendungszweck aufgeklärt. Der Patient kann zu jedem Zeitpunkt seine Einwilligung zurückziehen, woraufhin seine Daten gelöscht oder anonymisiert werden müssen. Die Gültigkeit einer Einwilligungserklärung muss stets im Verwendungskontext betrachtet werden und ist abhängig von der Qualität der personenbezogenen Daten, dem Verwendungszweck, der Verarbeitungsdauer und der datenverarbeitenden Stelle (vgl. [RHJ08, S. 18, 27]).
Vertrauliche Behandlung von Patientendaten und eine möglichst geringe Beeinträchtigung der Privatsphäre des Patienten spielen im in der medizinischen Forschung die mit Abstand wichtigste Rolle (vgl. [SBH+07], [SS00], [BRR99], [BC96]). Im Falle eines Bruchs im Vertrauensverhältnis zwischen den Patienten und dem Forschungsnetz könnten die Patienten ihre Mitarbeit verweigern. Dies würde dem Forschungsnetz seine Existenzgrundlage rauben (vgl. [RDSP06, S. 3], [KC08]).
Die Hauptschwierigkeit bei der Erstellung des Sicherheitskonzeptes für medizinische Forschungsnetze besteht in ihrer offenen Struktur. Die an einem Forschungsnetz beteiligten Ressourcen können räumlich weit verstreut sein. Es ist unmöglich, das komplette Forschungsnetz lediglich durch restriktive administrative Maßnahmen zu sichern.[2] Vor allem ist eine einheitliche Hard- und Softwareausstattung der Netzteilnehmer in den meisten Fällen nicht durchsetzbar.[3] Sicherheitskonzepte vieler Unternehmen basieren auf den sogenannten Corporate Security Policies bzw. Corporate Standards. Diese gelten sowohl

[2]Diese Art von Sicherheitsmaßnahmen wird im Abschnitt 3.4 „Administrative Aspekte von Sicherheitsrichtlinien“ ausführlich erläutert.

[3]Eine fest reglementierte Soft- und Hardwareausstattung ist ein wichtiger Aspekt bei der Konzeption von Sicherheitsmaßnahmen. Sicherheitskonzepte vieler großer Unternehmen setzen eine homogene Infrastruktur voraus, die in Rahmen von sogenannten Lockdown-Projekten definiert und umgesetzt wird. Lockdown bedeutet, dass dem Benutzer u. a. administrative Rechte genommen werden, sodass er nicht in der Lage ist, die Hard- oder Softwarekonfiguration seines Arbeitsplatzes zu verändern bzw. zu manipulieren, was die Aufgabe vereinfacht, Systemkonformität zu einem bestimmten Unternehmensstandard zu gewährleisten.

für die Dienstanbieter als auch für diejenigen, die diese Dienste in Anspruch nehmen. Einem Client, der die festgelegten Voraussetzungen[4] nicht erfüllt, wird der Zugriff auf bestimmte Ressourcen verweigert. In einem medizinischen Forschungsnetz ist es unmöglich, solch restriktive Vorschriften für die Client-Umgebung durchzusetzen. Die Teilnehmer des Forschungsnetzes würden die Einschränkung auf ein bestimmtes Betriebssystem und einen Satz von als „sicher“ eingestuften Anwendungen genauso wenig akzeptieren, wie das Verbot, Software zu installieren, die sie möglicherweise für ihre tägliche Arbeit benötigen. Die Hinzunahme zusätzlicher Softwareprodukte in das Softwareangebot bei einem Systemumfeld, in dem noch nicht einmal das verwendete Betriebssystem eine gemeinsame Komponente darstellt, ist eine kaum zu kontrollierende Aufgabe. Viele Sicherheitslücken einer Anwendung werden erst im Zusammenspiel mit anderen Softwareprodukten aktiviert (vgl. [Sch04]). Dies bedeutet, dass die geringste Erweiterung des Softwareangebots oder gar unvermeidbare Einspielung von Updates, die Durchführung diverser komplexer Tests und Neu-Zertifizierung des Gesamtpakets erfordert. Ein TCSEC (Orange Book)-ähnlicher Ansatz, bei dem man vordefinierte Konfigurationen von Systemen mit Sicherheitseinstufung versieht und abhängig davon den Zugriff auf bestimmte Dienste gewährt oder nicht, ist für medizinische Forschungsnetze nicht praktikabel. Die bereits erwähnte offene Struktur medizinischer Forschungsnetze erfordert einen Ansatz, der eine breite Teilnehmerbasis ansprechen kann und gleichzeitig das notwendige Sicherheitsniveau bietet (vgl. [RDSP06], [SPR+06]).

3.2. Hintergrund und Zusammensetzung von Sicherheitsrichtlinien als Komponenten einer Sicherheitsarchitektur

Vorbeugen ist einfacher als Heilen: Es ist schwieriger, ein wirksames Sicherheitskonzept für eine bereits bestehende Infrastruktur zu erstellen, als noch in der Planungsphase ihre kritischen Aspekte zu analysieren und diese bei der Erstellung des Sicherheitskonzeptes zu berücksichtigen. Viele für die medizinischen Forschungsnetze geltenden datenschutzrelevanten Fragestellungen werden in den generischen Datenschutzkonzepten der TMF [RDSP06] untersucht und beantwortet: Es wird u. a. hinterfragt, ob die einzelnen Teilziele des Forschungsnetzes auch ohne die Verarbeitung personenbezogener Daten erreicht werden können, ob der Umfang der personenbezogenen Daten reduziert werden kann, ob der Personenbezug über den gesamten Verarbeitungsablauf erhalten bleiben muss, zu welchen Zeitpunkten Anonymisierung und Pseudonymisierung erfolgen müssen etc. Die im Folgenden als Ausgangsbasis für die Ausführungen in diesem Ka-

[4] Dies können z. B. bestimmte Betriebssystemstände, installierte Sicherheitspatches, unternehmenseigene Compliance-Software etc. sein.

pitel verwendeten generischen Datenschutzkonzepte der TMF wurden von anerkannten Sicherheitsexperten ausgearbeitet und auf ihre Schwächen und Weiterentwicklungsbedarf analysiert (vgl. [HDR+10], [PSM+09], [Pom09]), sodass es an dieser Stelle nicht sinnvoll erscheint, die für ein medizinisches Forschungsnetz relevanten Aspekte der generischen Konzepte erneut aufzulisten. Vielmehr werden die Ergebnisse der o. g. Untersuchungen als Grundbausteine eines Forschungsnetzes vorausgesetzt, auf denen die Ausführungen dieses Abschnittes basieren.

In der ursprünglichen Version dieses Abschnitts wurde die in [RDSP06] vorgesehene Aufteilung in klinisch und wissenschaftlich fokussierte Forschungsnetze (Typ A und Typ B) berücksichtigt. Die beiden Netztypen haben unterschiedliche Anforderungen an die Sicherheitsarchitekturkomponenten, da sie sich in der Art der Datenspeicherung, des Zugriffs und des Pseudonymisierungs- bzw. Anonymisierungsprozesses unterscheiden. Im Vergleich zu den wissenschaftlich orientierten Netzen, deren Prozesse keinen unmittelbaren Einfluss auf die klinische Prozesse aufwiesen, stellten die klinisch fokussierten Forschungsnetze aufgrund der Besonderheiten ihrer Datenprozessierung eine besondere Herausforderung dar (vgl. [RDSP06, S. 20 ff.]):

- Für die Behandlung ist eine eindeutige Identifikation des Patienten auf dem Bildschirm des behandelnden Arztes zwecks Dateneingabe bzw. -abfrage notwendig.
- Eine automatische Zusammenführung von *IDAT* und *MDAT* erfolgt auf dem Rechner des behandelnden Arztes:[5]
  - Die identifizierenden Patientendaten werden auf dem Rechner des Arztes im Klartext eingegeben.
  - Die Übertragung der *IDAT* an die Patientenliste erfolgt durch die Verschlüsselung auf dem Transportweg (SSL).
  - Die Speicherung der *IDAT*- und *MDAT*- Daten erfolgt zentral auf zwei räumlich und administrativ verteilten Datenbanken in verschlüsselter Form.
  - Die Datenspeicherung erfolgt in den sogenannten Industrie-Standard-Datenbanken.
  - Ein restriktives rollenbasiertes Zugriffsberechtigungskonzept mit zeitlich limitierten Accounts sorgt dafür, dass die Datenzusammenführung nur durch den behandelnden Arzt durchgeführt werden kann.
  - Die Datenzusammenführung beim behandelnden Arzt erfolgt über eine *TempID*, sodass der *PID* nie die *IDAT*- respektive *MDAT*-Datenbank verlässt.
- Derzeit ist keine geeignete serverbasierte Schlüsselinfrastruktur vorhanden (und bezahlbar), die die im generischen Datenschutzkonzept beschriebenen Verfahren

[5] In den klinisch fokussierten Forschungsnetzen ist die Umgehung der zentralen *IDAT*-Speicherung vorstellbar, sodass die *IDAT*-Daten auf dem Rechner des behandelnden Arztes abgelegt werden könnten. Eine solche Art der Datenzusammenführung würde allerdings bedeuten, dass die Sicherheit der dezentral abgelegten Daten durch die Sicherheitsmaßnahmen des Forschungsnetzes kaum garantiert werden kann. Bei einer dezentralen Datenspeicherung ist außerdem die Einbindung der Laborärzte kaum durchführbar (vgl. [RDSP06, S. 40]).

tragen könnte. Diese wird möglicherweise erst durch die öffentliche Infrastruktur der HPCs und der Gesundheitskarte geschaffen.[6]

- Die Beschränkung der *IDAT* und *MDAT* auf notwendige und klar definierte Mindestinhalte entspricht dem Prinzip der Datensparsamkeit (vgl. [RDSP06, S. 39 f.]).

Die praktischen Erfahrungen mit der Ableitung von spezifischen Datenschutzkonzepten aus den beiden generischen Modellen machten diese Aufteilung obsolet, da viele Projekte eine Kombination der beiden Netztypen erfordern.[7] Die generischen Datenschutzkonzepte befinden sich derzeit in einem Revisionsprozess und sehen durch einen modularen Ansatz die Koexistenz von Datenbanken für den Behandlungs- und den Forschungskontext vor (vgl. [PSM+09, S. 1751]). Abbildung 4 stellt das Referenzmodell des künftigen revidierten Datenschutzkonzeptes der TMF dar, das die Aufteilung in die Versorgungs-, Studien-, Forschungs-, Bild- und Biobankmodule vorsieht. Die Patientenliste und der Pseudonymisierungsdienst übernehmen die Rolle des zentralen Identitätsmanagements (vgl. [PSM+09, S. 1754], [Pom11b], [Pom09, S. 10], [Pom10b]).

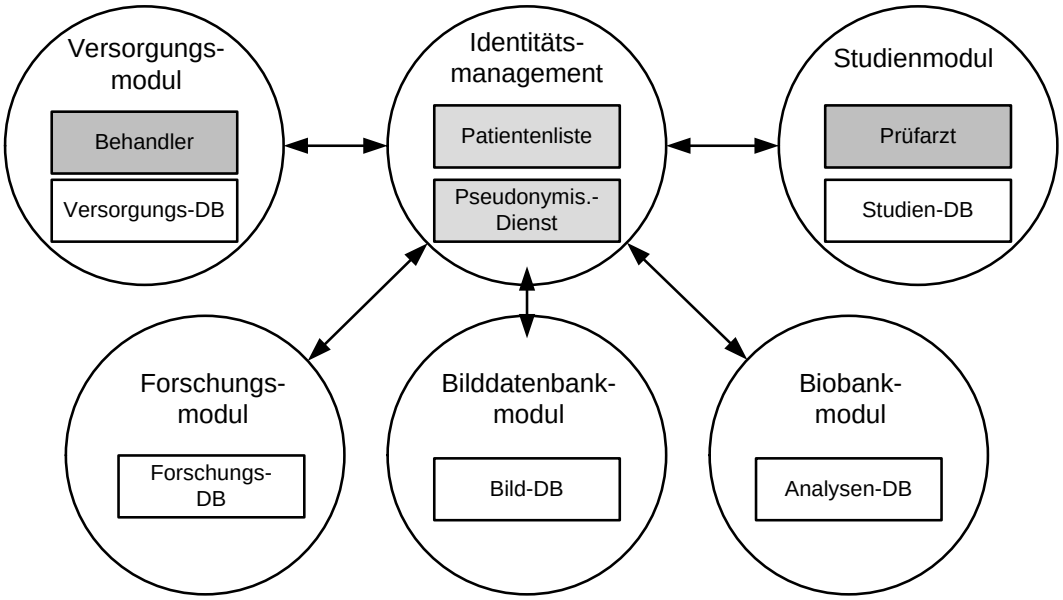

Abbildung 4.: Referenzmodell im künftigen revidierten Datenschutzkonzept der TMF: Die Patientenliste und der Pseudonymisierungsdienst übernehmen die Rolle des zentralen Identitätsmanagements. Der einheitliche modulare Aufbau sieht die Aufteilung in das Versorgungs-, Studien-, Forschungs- und Biobankmodul vor.

Die in den folgenden Abschnitten dieses Kapitels vorgestellten Sicherheitsrichtlinien sind ressourcen-, plattform- und produktunabhängig. Man kann in diesem Zusammenhang von sogenannten generischen Sicherheitskonzepten sprechen. Durch die Unabhängigkeit

[6]Nach der aktuellen Rechtsauffassung kann die vor der bundesweiten Einführung stehende elektronische Gesundheitskarte zwar für die Identifizierung eines Patienten, nicht jedoch zu Forschungszwecken verwendet werden (vgl. [RHJ08, S. 50]). Einen guten Überblick über die geschichtliche Entwicklung des Projektes „Elektronische Gesundheitskarte“ bietet [Bor08].

[7]Beispielsweise für die Begleitung chronisch kranker Patienten (Typ A) und für den Aufbau von Langzeitdatenpools (Typ B).

von einer konkreten Implementierung sind diese Konzepte relativ selten Veränderungen unterworfen; sie übernehmen die Rolle von systemübergreifenden Vorgaben. Generische Sicherheitskonzepte werden auch oft als Policies bezeichnet. In einem Unternehmen regeln solche Policies die meisten Organisationsbereiche. Im Konzept der Sicherheits- und Risikomanagementpyramide (S&R-Pyramide) nach Klaus-Rainer Müller [Mül11] bilden die Policies die letzte abstrakte Ebene und dienen als Basis für die Entwicklung systemspezifischer Sicherheitskonzepte und ihre Umsetzung – die Sicherheitsmaßnahmen.[8] Aufgrund des hohen Abstraktionsgrades weisen die Policies unterschiedlicher Organisationen viele Gemeinsamkeiten auf. Einige Sicherheitsrichtlinien ohne besondere Forschungsnetzspezifika, die für einen sicheren Forschungsnetzbetrieb jedoch unabdingbar sind, werden im Abschnitt C.6 „Beispiele für die Richtliniengestaltung“ vorgestellt.

Da innerhalb des Forschungsnetzes personenbezogene Daten erhoben und verarbeitet werden, müssen die im § 9 BDSG[9] definierten Anforderungen erfüllt werden:

- Zutrittskontrolle (kein unbefugter Zutritt zu den Datenverarbeitungsanlagen (DV-Anlagen)),
- Zugangskontrolle (kein unbefugter Zugang zu DV-Anlagen und Systemen),[10]
- Zugriffskontrolle (Zugriff nur auf die der Zugriffsberechtigung unterliegenden Daten),
- Weitergabekontrolle (Aufzeichnung der Datenübermittlung sowie kein Lesen, Verändern, Löschen oder Kopieren der Daten während der Datenübermittlung),
- Eingabekontrolle (nachträgliche Überprüfung der Eingaben),[11]
- Auftragskontrolle (Verarbeitung nur entsprechend den Weisungen des Auftraggebers),
- Verfügbarkeitskontrolle (Schutz gegen zufällige Zerstörung und Verlust),
- die zweckgebundene Verarbeitung (getrennte Verarbeitung von für unterschiedliche Zwecke erhobenen Daten).

Um diese Anforderungen des BDSG zu erfüllen, bedarf es Schutzmaßnahmen, die grob in

[8] Das Konzept der S&R-Pyramide nach [Mül11] wird im Abschnitt C.5 „RiSiKo-(Management-)Pyramide: ein generischer S&R-Ansatz“ vorgestellt.

[9] Ein Auszug aus dem BDSG befindet sich im Anhang E „Auszüge aus BDSG und StGB“.

[10] Im Rahmen der Zutrittskontrolle wird der Zutritt zu Räumen oder Gebäuden bzw. Gebäudeteilen geregelt. Eine der einfachsten Formen der Zutrittskontrolle ist die Schlüsselvergabe; kompliziertere Formen der Zutrittskontrolle können mehrstufige Benutzerauthentifizierung beinhalten. In [bsi11d] befindet sich eine ausführliche Anleitung zur Konzeption eines sicheren Zutrittkontrollsystems, die sich aus baulichen, organisatorischen, personellen und technischen Maßnahmen zusammensetzt. Dazu zählen u. a. Einschränkung des zutrittsberechtigten Personenkreises, ausführliche Dokumentation erteilter Zutrittsberechtigungen, sichtbar getragene Zutrittsausweise, Begleitung von Besuchern etc. Im Gegensatz zu der Zutrittskontrolle regelt die Zugangskontrolle den unmittelbaren Zugang zum System. Die Zugangskontrolle beschränkt sich meistens auf die technischen Maßnahmen (z. B. eine SmartCard-basierte Authentifizierung).

[11] Im Rahmen der Eingabekontrolle muss im Nachhinein überprüft werden können, wer welche Daten zu welchem Zeitpunkt eingegeben bzw. verändert hat. Grundlage dafür sind technische und organisatorische Maßnahmen. Organisatorische Maßnahmen bestehen in einer möglichst lückenlosen Erfassung und Aufbewahrung der Erfassungsdokumente sowie einer klaren Dokumentation der Eingabeprozeduren. Die technischen Maßnahmen beinhalten Protokollierung bzw. Monitoring der Vorgänge, die ausführlich im Abschnitt 3.5.12 „Monitoring und Protokollierung“ dargestellt werden.

drei Kategorien eingeteilt werden können: organisatorische, administrative und technische Maßnahmen (vgl. [Eck07, S. 37 f.]). Die zentrale in diesem Kapitel untersuchte Fragestellung wird in Form der ersten forschungsleitenden Frage zusammengefasst:

> F1: Welche Anforderungen werden in Bezug auf die organisatorischen, technischen und administrativen Sicherheitsmaßnahmen an die medizinischen Forschungsnetze gestellt, und welche Anforderungen bestehen in Bezug auf die Sicherheitsmaßnahmen in den medizinischen Forschungsnetzen?

Diese Fragestellung berücksichtigt die folgenden Sichtweisen: Die externe Sicht der Anforderungen bezieht sich auf die Voraussetzungen und die geltenden Rahmenbedingungen der Sicherheitsmaßnahmen. Die interne Sicht der Anforderungen befasst sich mit der möglichen Beschaffenheit des Sicherheitsmaßnahmenportfolios. Diese beiden Sichtweisen, die sich im Hinblick auf die medizinischen Forschungsnetze ergeben, werden in den folgenden Abschnitten 3.3, 3.4 und 3.5 untersucht und erörtert.

3.3. Organisatorische Aspekte von Sicherheitsrichtlinien

Unter organisatorischen Sicherheitsmaßnahmen versteht man planerische Vorkehrungen, deren Ziel in der Sicherstellung des angestrebten Sicherheitsniveaus besteht. Organisatorische Sicherheitsmaßnahmen für ein medizinisches Forschungsnetz beinhalten eine ständige Anpassung der Sicherheitsstrategie und Erweiterung der Sicherheitsrichtlinie. Außerdem müssen die Informationssicherheitsanforderungen angepasst und die zu treffenden Schutzmaßnahmen priorisiert werden (vgl. [PB06]).

Die für ein Forschungsnetz gültigen Richtlinien und Standards werden von einer zentralen Stelle innerhalb des Forschungsnetzes[12] entwickelt und müssen von allen Beteiligten eingehalten werden. Selbstverständlich können auch kleinere Organisationseinheiten ihre eigenen Standards entwickeln; diese dürfen die Anforderungen der bereichsübergreifenden Richtlinien nicht unterschreiten und bedürfen einer Genehmigung des zentralen Gremiums. Alle in Verbindung mit der Einhaltung der Richtlinien stehenden Aktivitäten müssen auditfähig sein. In den durch die Richtlinien nicht abgedeckten Fällen muss eine angemessene Dokumentierung der Vorgänge erfolgen. In den folgenden Abschnitten erfolgt eine Untersuchung für eine Auswahl von organisatorischen Sicherheitsmaßnahmen: rechtliche und finanzielle Absicherung, personale Aspekte, Notfallvorsorgemaßnahmen, Wiederaufnahme des Betriebs sowie Benefit Denial.

[12] Empfehlenswert ist die Einrichtung einer Organisationseinheit, die beispielsweise dem Ausschuss Datenschutz unterstellt ist.

3.3.1. Rechtliche und finanzielle Absicherung von Forschungsnetzen

Ein medizinisches Forschungsnetz kann als ein Dienstleister gesehen werden, der bestimmte Daten einem Kreis von Forschern und Organisationen zur Verfügung stellt, wobei das primäre Ziel eines medizinischen Forschungsnetzes nicht in der Erzielung des maximalen Gewinns, sondern in der Kommunikationsoptimierung zwischen Wissenschaftlern, behandelnden Ärzten und Patienten besteht. Trotzdem ist ein Forschungsnetz auf finanzielle Mittel zwecks Aufrechterhaltung und Erweiterung seines Betriebs angewiesen. Kritische Presseberichte können den Ruf des Forschungsnetzes negativ beeinträchtigen und das Vertrauen der Teilnehmer bzw. Patienten senken, sodass diese ihre Zusammenarbeit mit dem Forschungsnetz verweigern, was sich auf die Förderung des Netzes auswirken würde. Es kann nicht ausgeschlossen werden, dass während des Bestehens des Forschungsnetzes ein Sicherheitsvorfall auftritt, und das Netz mit dem Rückgang der Teilnehmerzahl und der finanziellen Mitteln konfrontiert wird. In einem solchen Fall gibt es grundsätzlich folgende Alternativen: Man erklärt das Konzept dieses bestimmten Forschungsnetzes für gescheitert, um etwas später eine neue Initiative zu gründen, oder man untersucht den Vorfall, lernt aus den Fehlern, verbessert die bestehende Sicherheitsinfrastruktur und stellt das für das Fortbestehen des Netzes notwendige Vertrauen der Forschungsnetzteilnehmer wieder her. Für die zweite Option bedarf es finanzieller Mittel. Da ein Forschungsnetz – als eine i. d. R. zum größten Teil durch öffentliche Gelder finanzierte Organisation – kaum in der Lage wäre, die zur Deckung möglicher Risiken notwendigen Rücklagen selbstständig zu bilden und zu verwalten,[13] kommen die Bildung eines Risiko-Pools bzw. ein Abschluss von Versicherungsverträgen als eine Form der Absicherung in Frage. Zusätzlich müsste geprüft werden, inwiefern die zu versichernden Risiken bereits von den das Forschungsnetz i. d. R. betreibenden Kliniken oder öffentlichen Institutionen abgedeckt sind. Risikopools könnten bei schwer oder nur zu ungünstigen Konditionen zu versichernden Risiken in Frage kommen; die praktische Umsetzung würde jedoch wahrscheinlich aus den gleichen Gründen wie bei der bereits erwähnten Rücklagenbildung scheitern. Risikotransfer zeichnet sich durch die Verlagerung des Risikos auf einen anderen Träger aus und kann z. B. durch den Abschluss von Versicherungsverträgen erfolgen. Versicherer prüfen, ob eine Haftung aufgrund von gesetzlichen Bestimmungen besteht und ob die Höhe der gestellten Ansprüche gerechtfertigt ist. Ansprüche, die in ihrer Art und/oder Höhe unberechtigt sind, werden (ggf. vor Gericht) abgewehrt. Die auf gerechtfertigten Ansprüchen basierenden Verpflichtungen werden vom Versicherer (i. d. R. ohne einen finanziellen Nachteil für das Forschungsnetz) übernommen.

Einer Reihe von rechtlichen und finanziellen Risiken kann zuverlässig durch den Abschluss von Versicherungsverträgen begegnet werden. Eine ausführliche Auseinandersetzung mit diesem organisatorischen Sicherheitsinstrument erfolgt im Abschnitt C.1 „Versicherungsschutz als organisatorisches Sicherheitsinstrument“.

[13] Die Rechtmäßigkeit der Rücklagenbildung bei e. V. der öffentlichen Förderung bedarf weiterer rechtlicher Klärung (vgl. § 58 Nr. 6, 7 AO).

3.3.2. Personale Aspekte für den Betrieb von Forschungsnetzen

Personalwesen ist eines der empfindlichsten Bereiche einer jeden Organisation. Der Personalmanagementprozess umfasst Personalbedarfsplanung, Personalbeschaffung, -einarbeitung, -betreuung und -freistellung (vgl. [bsi11d, M 3]). Im Folgenden werden die sicherheitskritischen Aspekte des Personalwesens vorgestellt. In diesem Zusammenhang wird die Beschaffung des qualifizierten Personals, dessen Integration und Motivation sowie die Fluktuationskontrolle thematisiert.

3.3.2.1. Einstellungspolitik

Der Einstellung von Personal steht eine Planungs- und Akquisitionsphase zuvor. Die Planungsphase soll in diesem Zusammenhang nicht näher erläutert werden.[14] Nach der Genehmigung von Stellen folgt eine Akquisitionsphase. Diese ermöglicht die Erhöhung des Sicherheitsstandes eines Forschungsnetzes mit vertretbaren Investitionen. Die während der Personalbeschaffung zugelassenen Fehler können später nur mit einem hohen Aufwand behoben werden. So sollte man z. B. während der Personalbeschaffung bestrebt sein, Konflikte zu vermeiden, die durch verwandtschaftliche Beziehungen zwischen den Neueinstellungen und dem Mitarbeiterstamm entstehen können. Die Qualität des Personals und seine Loyalität dem Arbeitgeber gegenüber ist maßgeblich für die Höhe und das Ausmaß der Angriffe auf eine Organisation. Auch weitere Faktoren wie Mitarbeiterzufriedenheit haben Auswirkungen auf die Sicherheitssituation. Ein Beispiel dafür ist das oft verschwiegene Thema „Insiderangriff“.

Viele Unternehmen versuchen Diskussionen über die Insiderangriffe zu umgehen, indem sie einseitig ihre internen Kontrollen und die Strafenkataloge verschärfen. Doch die Durchführung von übertriebenen Kontrollmaßnahmen ist i. d. R. kostspielig und liefert des Öfteren nicht wünschenswerte Ergebnisse. So senken die übertriebene Kontrolle und die ständigen Androhungen von personellen Konsequenzen die Arbeitsmoral und Produktivität der Belegschaft und erreichen somit den gegenseitigen Effekt. Beweise hierfür sind allgegenwärtig. So wurden – trotz den erwähnten Maßnahmen – der im Jahr 2004 von KPMG durchgeführten Betrugsstudie zufolge fast 80 Prozent der Betrugsfälle von Insidern durchgeführt (vgl. [kpm04]). Dabei können die Insiderangriffe durch eine vernünftige Einstellungs- und eine arbeitnehmerfreundliche Beschäftigungspolitik reduziert werden.

In der heutigen Arbeitswelt wachsen permanent die Anzahl von befristeten Arbeitsverhältnissen sowie die Abhängigkeit von zeitlich begrenzten Managementressourcen. Diese beiden Faktoren erhöhen das Risiko eines Insiderangriffs. Für das Forschungsnetz ist aus diesem Grunde ein arbeitnehmerfreundliches Verhalten empfehlenswert, das sich u. a. in längerfristigen Arbeitsverhältnissen ausdrücken sollte. Diese Forderung ist im akademischen Bereich nicht leicht zu erfüllen, denn die meisten Einstellungen sind an die befristeten

[14] Die Einflussmöglichkeiten eines Forschungsnetzes auf die Personal(bedarfs)planung sind i. d. R. eingeschränkt und hängen oft von der Höhe der Fördermittel ab.

Forschungsprojekte gebunden, und die Vergütungen liegen oft unter den Vergütungen der „freien Wirtschaft“ (vgl. [WB09]).[15] Aus diesem Grund gilt es, bereits bei der Einstellung die Bewerber auf ihre Eignung und die zu erwartende Loyalität besonders aufmerksam zu prüfen. Im Rahmen des Auswahlverfahrens kann das Risikopotenzial von Bewerbern anhand von objektiven Kriterien gemessen werden. Dazu gehört beispielsweise das Einholen von Auskünften über die Vermögensverhältnisse der einzustellenden Kandidaten.[16] Bei Neueinstellungen kann das polizeiliche Führungszeugnis des Bewerbers angefordert und dessen Vergangenheit auf einschlägige Vorstrafen untersucht werden. Dies kann aufgrund der zu erbringenden Arbeitsleistung[17] von Bedeutung und zulässig sein. Als empfehlenswert erweist sich außerdem das Einholen von Referenzen beim ehemaligen Arbeitgeber (vgl. [bsi11d, M 3.31-M 3.33]).

3.3.2.2. Funktionstrennung

Bei der Erstellung von Tätigkeitsbeschreibungen und Zuweisung von Verantwortlichkeitsbereichen an die Forschungsnetzmitarbeiter ist das Prinzip der Funktionstrennung zu beachten. Dieses Prinzip stellt sicher, dass eine Person keine sich gegenseitig ausschließenden Funktionen ausführen kann. So darf z. B. ein Mitarbeiter nicht seine eigene Tätigkeit oder die Tätigkeit seines Vorgesetzten im Rahmen einer Revision kontrollieren. Genauso wenig ist es sinnvoll, ausschließlich Entwickler für die Prüfung des von ihnen selbst erstellten Produktes einzusetzen. Grundsätzlich empfiehlt sich eine generelle Trennung der Bereiche Entwicklung, Test, Produktion und Auditing. Sollte ein Mitarbeiter in mehr als einem dieser Bereiche am gleichen Produkt oder Dienst eingesetzt werden, muss dies begründet werden (vgl. [bsi11d, M 2.5]).

3.3.2.3. Personalentwicklung

Viele Angriffe aus dem Inneren einer Organisation sind nicht beabsichtigt, sondern erfolgen aufgrund der fehlenden Kenntnisse bzw. des fehlenden Sicherheitsbewusstseins. Es ist aus diesem Grund nicht nur notwendig, das Bewusstsein für sicherheitskritische Situationen bei den Forschungsnetzmitarbeitern zu wecken, sondern es gilt, die Mitarbeiter zu einem verantwortungsvollen Handeln zu bewegen. Für diesen Zweck eignen sich Schulungen, die folgende Themenbereiche behandeln (vgl. [bsi11d, M 3], [Zie06]):

---

[15] Selbstverständlich gibt es auch diverse Ausnahmen zu dieser Regel. So ist z. B. die feste Anstellung des Administrationspersonals üblich. Die Kombination einer marktüblichen Vergütung mit einer hohen Arbeitsplatzsicherheit resultiert i. d. R. in einem loyalen Arbeitnehmerverhältnis.

[16] Dies ist zulässig, da in diesem Fall ein berechtigtes Informationsinteresse des Forschungsnetzes aufgrund der Eigenart und des besonderen Verstrauensbedürfnisses der zu besetzenden Stelle besteht.

[17] Zum Beispiel vertrauliche Behandlung von Patienten- bzw. Probandendaten, an deren Veröffentlichung, Kauf, Reidentifizierung etc. mehrere Wirtschaftsorganisationen interessiert sein könnten (s. a. Abschnitt 4.3.2 „Bedrohungsorientierte Analyse“).

- Forschungsnetzmitarbeiter sind über die *Gründe der Sicherheitsmaßnahmen* aufzuklären. Der Mitarbeiter muss den Zweck von Sicherheitsüberprüfungen verstehen, die rechtlichen Rahmenbedingungen des Forschungsnetzbetriebs kennen, sicherheitsrelevante Veränderungen wahrnehmen und bewerten können.
- Dem Mitarbeiter müssen die *Gefahren am Arbeitsplatz*, die durch Unwissenheit oder Bequemlichkeit der Benutzer auftreten können, bekannt sein. Der Mitarbeiter muss über korrektes Verhalten während der Arbeit bzw. beim Verlassen des Arbeitsplatzes aufgeklärt werden. Er muss die von den Besuchern ausgehenden Gefahren einschätzen und die häufigsten Anzeichen für Hard- oder Softwaremanipulationen erkennen lernen. Beim Verlassen seines Arbeitsbereichs muss er das Prinzip des aufgeräumten Arbeitsplatzes beachten. Ein unbefugter Dritter darf bei Abwesenheit des Mitarbeiters nicht auf die Datenträger, Unterlagen oder gar aktive Systemanmeldungen zugreifen können.
- Der Mitarbeiter sollte die *Spionagegefahren* erkennen können. Er muss die Risikosituationen bemerken, diese vermeiden und ggf. auf Spionageversuche korrekt reagieren können.
- Dem Mitarbeiter muss ein richtiger *Umgang mit Internetinhalten* vermittelt werden. Der Anwender muss die Gefahrenpotenziale einschätzen können und wissen, welche Auswirkungen ein Malware-Befall auf ein System haben kann.[18]
- *Zerstörung und Diebstahl* des Forschungsnetzeigentums können mehrere Ursachen haben und zur Verletzung der Integrität oder Vertraulichkeit von Patientendaten führen. Forschungsnetzmitarbeiter müssen über diese Gefahren aufgeklärt werden und potenzielle Risikosituationen erkennen und vermeiden können.
- Ein sorgfältiger *Umgang mit Arbeitsmitteln* reduziert die Wahrscheinlichkeit für den Datenverlust bzw. Datendiebstahl. Forschungsnetzmitarbeiter müssen lernen, wie geeignete Datenträger ausgewählt werden und welche Vorbeugemaßnahmen (Verschlüsselung der Inhalte, sorgfältige Auswahl von Informationen etc.) den Schaden des Datenträgerverlusts reduzieren können.

3.3.2.4. Personalfreistellung

Die Trennung vom Personal ist ein weiterer kritischer Punkt im Personalmanagementprozess: Ein fest definierter Übergabeprozess muss eingehalten werden, um die Weitergabe des Know-hows sicherzustellen und die Bekanntgabe von vertraulichen Daten zu vermeiden. Eine rechtzeitige Deaktivierung von Benutzerzugriffsrechten, die Übergabe von Dateien, Datenträgern, Weiterleitung von E-Mails, Rückgabe von Geräten etc. sind im Rahmen des Personalfreistellungsprozesses zu berücksichtigen (vgl. [bsi11d, M 3.6]).

[18] Diese Forderung ist jedoch angesichts der sich ständig ändernder Angriffsszenarien nur schwer zu erfüllen.

3.3.3. Organisation und Gestaltung von Notfallvorsorgemaßnahmen

Fehlerfreie Systeme existieren nicht (vgl. [AMR07]).[19] Gibt es Anreize für einen Angriff, so muss mit Kompromittierungsversuchen gerechnet werden. In einem medizinischen Forschungsnetz werden Daten verarbeitet, die nicht nur für Freizeithacker interessant sind. Banken, Versicherungen, Werbewirtschaft, pharmazeutische Industrie etc. könnten an den Daten des Netzes interessiert sein.[20] Trotz strikter Einhaltung diverser Sicherheitsmaßnahmen kann es erfolgreiche Angriffe geben.

Eine frühzeitige Vorbereitung auf den Ernstfall ist ein Teil der organisatorischen Sicherheitsmaßnahmen eines Forschungsnetzes. Sie verringert den Wiederherstellungsaufwand in einem Schadensfall oder ermöglicht erst die Problembehebung. Die Notfallvorbereitungen können als Teil eines sogenannten Service-Continuity-Managements (SCM) angesehen werden, dessen Ziel nach ITIL in der Unterstützung des Business-Continuity-Managements besteht, im dessen Rahmen sichergestellt wird, dass die notwendigen Dienste innerhalb von erforderlichen und abgestimmten Zeiträumen verfügbar gemacht werden. Eine Reihe von sogenannten kritischen Erfolgsfaktoren wie beispielsweise die Unterstützung des Managements, die Praktikabilität der Reportingprozesse, eine organisationsweite Einbeziehung und Abstimmung mit den ITSCM- und Kapazitätsmanagementprozessen etc. ist für den SCM-Erfolg unabdingbar (vgl. [LR07, S. 214 ff.]).

Bei der Erstellung eines Notfallkonzeptes spielen sowohl die externen[21] als auch die forschungsnetzinternen Vorgaben eine Rolle. Im Rahmen der Notfallvorsorge werden die potenziellen Notfallszenarien für die wichtigsten Dienste und Geschäftsprozesse ermittelt, Zusammensetzung der Krisenstabs, Stellvertreterregelungen und Eskalationswege werden festgelegt; Notbetriebpläne und der Übergang zum Normalbetrieb werden geplant. Um die Adäquatheit der Vorsorgemaßnahmen zu garantieren, müssen die möglichen Schadensszenarien im Rahmen der Risikoeinschätzung (s. a. Abschnitt 4.3 „Qualitative Bewertung der Bedrohungs- und Risikosituation“) ermittelt werden. Diese lassen sich in Systemfehler (Hard- oder Softwarefehler), menschliche Fehler bzw. gezielte Angriffe gegen Infrastrukturbestandteile aufteilen.

Hard- und Software: Die Vorsorge gegen den größten Teil der Hardwareprobleme ist vergleichbar einfach. Trotz der stetig sinkenden Hardwarepreise empfiehlt sich eine Vorratshaltung von Ersatzgeräten kaum. Die notwendige Verfügbarkeit von Ersatzgeräten kann man durch den Abschluss von Wartungsverträgen mit Hardwareherstellern für for-

[19] Auch wenn Anhänger der funktionalen Programmierung an dieser Stelle gerne einen Einspruch einlegen würden. Sobald Nebeneffekte ins Spiel kommen (und das ist z. B. bei Benutzereingaben der Fall), kann die Fehlerfreiheit eines komplexeren (funktionalen) Systems nicht mehr garantiert werden.

[20] Struktur und Motive der Angreifer werden im Abschnitt 4.3.2 „Bedrohungsorientierte Analyse“ ausführlich untersucht.

[21] Zum Beispiel gesetzliche und normative Vorgaben.

schungsnetzeigene Systeme und von entsprechenden SLAs mit den Dienstleistern meist effizienter und kostengünstiger erreichen. Alternativ kann die Hardwareausfallsicherheit durch den Einsatz von Failover-Systemen und eine entsprechende Infrastrukturkonzeption erfolgen (s. a. Abschnitt 3.5.10 „Firewalling und Proxying“).
Softwareausfälle können i. d. R. schwieriger vermieden werden, denn diese können unterschiedlichste Ursachen haben: Einspielen von Patches, Konfigurationsänderungen aber auch die bereits erwähnten Hardwareprobleme können dafür verantwortlich sein. Dafür müssen die kritischen Systeme[22] erst ermittelt werden. Alle relevanten Konfigurationsänderungen an solchen Systemen sind zu protokollieren; eine Dokumentation für das Vorgehen in Notfällen muss erstellt werden. Diese Dokumentation darf nicht nur in digitaler Form an einer zentralen Stelle vorliegen; die wichtigsten Teile müssen in Form eines Handbuchs, das nach dem „Kochbuch-Prinzip“ schrittweise die für die Wiederherstellung notwendigen Schritte beschreibt, vorhanden sein. Da technische Beschreibungen dieser Art regelmäßig aktualisiert werden müssen, können nur die wichtigsten (statischen) Bestandteile ausgedruckt werden. Die häufig aktualisierten Dokumentationsbestandteile können auch auf tragbaren Speichermedien[23] dezentral gesichert werden; die Dokumentation muss folgende Punkte berücksichtigen:

- Wer und in welcher Reihenfolge kontaktiert bzw. über den Vorfall informiert werden muss (Administratoren, Hardwarelieferanten, Ansprechpartner für die Wartungsverträge etc.).
- Konfigurationsbeschreibung (Hardware, Berechtigungsstruktur etc.).
- Update- und Release-Informationen.
- Schritte zum Starten/Beenden von Diensten.
- Performance- und Diagnosedetails.

Notuser-Verfahren: Das nur in Notfällen zu verwendende Notuser-Verfahren muss eingerichtet werden. Einem Missbrauch der Notuser-Kennung in Nicht-Notfällen zwecks Berechtigungserweiterung muss durch die Aufbewahrung von Zugriffsdaten im einbruchssicheren Safe in versiegelten Umschlägen bzw. Behältern vorgebeugt werden. In Folge der Untersuchung von Mehrfaktor-Authentifizierungsverfahren im Abschnitt 3.5.3 „Authentifizierung von Forschungsnetzteilnehmern“ wird die Verwendung von einer Kombination aus SmartCard und PIN-Nummer für die Teilnehmerauthentifikation empfohlen. Zusätzliche Sicherheit der Notuser-Kennung kann durch die getrennte Aufbewahrung der Karten und der PINs erreicht werden. Alle PINs für die Notuser-Kennung müssen Einmal-PINs sein. Die PIN-Liste kann zusätzlich in mehrere unabhängige Teillisten[24] aufgeteilt werden.

[22] Dazu zählen z. B. Firewalls, Router, Datenbankserver, Applikationsserver, IDS-Komponenten etc.

[23] USB-Sticks, DVDs etc.

[24] Es könnte sogar sinnvoll sein, jede einzige PIN in einem separaten (durchnummerierten) versiegelten Umschlag aufzubewahren.

Bei der Verwendung des Notuser-Verfahrens ist festzuhalten, wer, weshalb und wann die Kennung verwendete. Außerdem müssen die mit der Notuser-Kennung durchgeführten Aktionen zwecks einer späteren Auswertung dokumentiert und archiviert werden.

Notfallsimulation: Der wohl wichtigste Punkt bei einem Notfallkonzept ist dessen Erprobung. So müssen in regelmäßigen Zeitabständen (z. B. halbjährlich) Wiederherstellungsversuche für einige Systeme im Rahmen der Notfallsimulation gestartet werden. Die Ergebnisse der Notfallsimulation sind aufzuzeichnen und nach jedem Versuch auszuwerten (vgl. [bsi11d, M 6, B 1.3]).

3.3.4. Wiederaufnahme des Betriebs

Die Dienste eines Forschungsnetzes müssen nach einem Sicherheitsvorfall oder einer Katastrophe innerhalb eines angemessenen Zeitrahmens wieder verfügbar gemacht werden können. Voraussetzung dafür sind die für unterschiedliche Notfallszenarien entwickelten Pläne zur Notfall- und Katastrophenvorsorge[25]. Das Ziel dieser Pläne ist die Beschreibung einer geordneten Vorgehensweise zur Wiederherstellung der wichtigsten Forschungsnetzdienste.
Die im Rahmen der Business-Continuity-Planung (BCP) vorbereiteten Maßnahmen hängen von der finanziellen Ausstattung der Organisation und dem Sicherheitsbewusstsein der beteiligten Personen ab. Eine kleine Organisation kann BCP in Form eines außerhalb des Unternehmensgebäudes aufbewahrten Ordners umsetzen, in dem die Adressliste der Mitarbeiter sowie der wichtigsten Geschäftspartner, Kopien der Versicherungsverträge und Bankdaten abgeheftet sind.[26]
Die Entwicklung der BC-Pläne kann man in Phasen einteilen: Analyse-, Design-, Implementierungs- und Erprobungs- sowie Pflegephase. Im Rahmen der Vorbereitung auf den Ernstfall wird den Beteiligten ein formales Dokument ausgehändigt, in dem die Maßnahmen vor, während und nach dem Auftreten einer existenzbedrohenden Störung beschrieben werden.
In der *Analysephase* werden die Risiken auf ihre Existenzbedrohlichkeit geprüft und die entsprechenden Schadensszenarien entwickelt. Anschließend wird der Einfluss von möglichen Schadensereignissen auf die kritischen Forschungsnetzdienste untersucht, wobei die Einstufung sowohl die internen Bedürfnisse als auch die Bedürfnisse der Kunden/Geschäftspartner bzw. gesetzliche Anforderungen berücksichtigen muss.
In der *Designphase* werden die Vorgehensszenarien für die in der Analysephase als kritisch

[25] Auch als „Business-Continuity-Pläne“(BCP) bekannt.

[26] Die Business-Continuity-Vorbereitungen eines weltweit agierenden Konzerns können beliebig kompliziert werden und die Benutzung eines Ausweichrechenzentrums und Ausweichbüroräume, Anleitungen zur Wiederherstellung der wichtigsten Systeme, Richtlinien für die Weitergabe von Informationen an die Presse etc. beinhalten.

bewerteten Risiken erarbeitet, denn für viele Schadensereignisse unterscheiden sich die Maßnahmenkataloge beträchtlich.[27] Der Aufwand für die Planerstellung kann erheblich verringert werden, indem mehrere Risikoszenarien mit ähnlichen Schadensauswirkungen zusammengefasst werden. So können z. B. ein Flugzeugabsturz auf das Gebäude des Rechenzentrums und eine Explosion bzw. Brand als Verlust des Rechenzentrums aufgefasst werden. In der Designphase werden die effizienten Wege ermittelt, um die kritischen Dienste innerhalb eines angemessenen Zeitrahmens wieder in Betrieb zu nehmen.
In der *Implementierungs- und Erprobungsphase* werden die Erkenntnisse der beiden vorhergehenden Phasen zusammengefasst, die erforderlichen Vorbereitungsmaßnahmen werden getroffen und auf ihre Praktikabilität hin getestet. Die Testsergebnisse offenbaren Planungslücken und dienen als Übung für das Personal.
Der Zweck der *Pflegephase* besteht in der kontinuierlichen Aktualisierung der entwickelten Maßnahmen. Die Informationen in den Notfallkatalogen (Telefon-, Adresslisten etc.) werden stets auf dem aktuellen Stand gehalten. Auch die technischen und organisatorischen Maßnahmen werden in regelmäßigen Zeitabständen auf ihre Aktualität geprüft. Für ein Forschungsnetz ist die Durchführung von jährlichen Notfallübungen sinnvoll, wobei aus Kostengründen nicht stets alle Notfallplan-Szenarien geprüft werden müssen. Die während der Tests gewonnenen Erkenntnisse liefern Verbesserungsansätze für die Design- und Implementierungsphase. Übungen können sowohl angekündigt als auch unangekündigt erfolgen. Es erscheint sinnvoll, die BCP-Entwicklungsphasen in regelmäßigen Zeitabständen oder auch bei Änderung der Bedrohungs- und Risikosituation zu wiederholen, um die Aktualität der Notfallpläne zu gewährleisten (vgl. [Mül11], [TK03]).

Forschungsnetzspezifische Business-Continuity-Pläne: Das größte Hindernis bei der Entwicklung von Business-Continuity-Plänen für ein Forschungsnetz bereiten die verfügbaren finanziellen Mittel (s. a. Abschnitt 3.3.1 „Rechtliche und finanzielle Absicherung von Forschungsnetzen“). In der medizinischen Forschung ist die Regel, dass bereits kurz nach der Förderung während der Gründungsphase, kaum Gelder in ein Forschungsprojekt mehr fließen. Kaum ein Forschungsnetz wird also in der Lage sein, selbstständig ein Ausweichrechenzentrum und entsprechende Büroräume für den Ernstfall aufzubauen, wenn diese nicht bereits zu Beginn des Projektes vorhanden waren, oder die Forschungsnetzbetreiber solche Einrichtungen besitzen. Trotzdem ist es möglich, auch mit geringen finanziellen Mitteln, eine sinnvolle Notfallvorsorge zu treffen. Der Schwerpunkt der Business-Continuity-Planung eines Forschungsnetzes muss deshalb in den kostengünstigen administrativen und organisatorischen Maßnahmen liegen.

[27] Die Wiederaufnahme des Betriebs im Falle eines Flugzeugabsturzes auf das Gebäude des Rechenzentrums, einer Epidemie oder Veröffentlichung der Patientendatenbank in der lokalen Zeitung erfordert jeweils unterschiedliche Maßnahmenkataloge. Eine Reihe von möglichen Schadensszenarien wird in den Abschnitten 4.3.1 und 4.3.2 untersucht.

In Bezug auf die Bewältigung von Notfällen besteht der große Vorteil eines Forschungsnetzes gegenüber einem Unternehmen in der Tatsache, dass ein Unternehmen auf eine kontinuierliche Leistungserbringung zur Deckung seiner laufenden Kosten angewiesen ist, während ein Forschungsnetz insbesondere im wissenschaftlichen Zusammenhang die Verfügbarkeit seiner Dienste auch für einen längeren Zeitraum einschränken kann. Im Ernstfall ist erstrangig die Vertraulichkeit von Forschungsnetzdaten zu gewährleisten. Zweitrangig ist dagegen der Zeitraum, in dem die Daten externen Forschern wieder verfügbar gemacht werden. Lediglich Dienste, die im Behandlungszusammenhang für die Patientenversorgung unabdingbar sind, müssen innerhalb kürzester Zeit wieder verfügbar sein. Der Betrieb eines Forschungsnetzes bedarf auch keines großen Mitarbeiterstamms, wie es z. B. im produzierenden Gewerbe der Fall ist. In vielen Fällen ist deswegen die Bereithaltung von Ausweichbüros für die Forschungsnetzmitarbeiter nicht notwendig, zumal viele der Administrationsaufgaben von beliebigen Standorten aus erledigt werden können. Für die wenigen notwendigen festen Arbeitsplätze sollte bei der Auswahl der Räumlichkeiten ihre längerfristige Verfügbarkeit für einen Mindestzeitraum von drei Jahren angestrebt werden. Die Ausweichstandorte sollen die Installation der für die Sprach- und Datenübertragung notwendigen Infrastruktur erlauben. Die Räumlichkeiten müssen eine ausreichende Stromversorgung und im Falle der Notwendigkeit eines Serverbetriebs die dafür notwendige Klimatisierung aufweisen. Dem Personal muss eine zumutbare Arbeitsumgebung zur Verfügung stehen. Die ausgewählten Räume müssen angemessene Sicherheit bezüglich Zutrittskotrolle, Brandschutzmaßnahmen, Notfallstromversorgung und des Abstands zu gefährlichen Industrieanlagen[28] etc. aufweisen (vgl. [bsi11d, B 1.3, M 6]).

Mehrere Anbieter spezialisieren sich auf der Vermarktung von Ausweichräumen und Notfallinfrastrukturen. Durch optimiertes Risikomanagement und Risikoverteilung[29] zwischen mehreren Kunden werden kostengünstige Notfalllösungen angeboten. Auch die Vorratshaltung von entsprechender Hardware wird günstiger, wenn die Hardwarekosten zwischen mehreren Kunden geteilt werden. Die eigenständige Bereithaltung vergleichbarer Kapazitäten würde das Mehrfache an finanziellen Mitteln erfordern.

Wenn die finanziellen Mittel eines Forschungsnetzes die Inanspruchnahme solcher Dienstleistungen nicht erlauben, können alternativ Vereinbarungen unter den Forschungseinrichtungen bzw. Kliniken selbst getroffen werden. Diese könnten z. B. eine zeitlich befristete Überlassung von Räumlichkeiten und Equipment in Notsituationen vorsehen. Die sogenannten Übereinkünfte auf Gegenseitigkeit sind jedoch rechtlich nicht durchsetzbar. Aus diesem Grund wird der Abschluss eines Vertrags über einen Ausweichstandort[30] empfohlen. Auf das gegenseitige Abkommen mit den anderen Forschungseinrichtungen kann

[28] Chemische Industrie, Müllverbrennungsanlagen, Feuerwerkskörper-Fabriken etc.

[29] So vermeidet man beispielsweise die gemeinsame Nutzung von Ausweichbüros zwischen räumlich nahe zueinander liegenden Unternehmen.

[30] Als Hot-, Warm- oder Coldsite.

bei Nichtverfügbarkeit des Ausweichstandorts im Ernstfall zurückgegriffen werden. Beim Abschluss des Vertrages auf Gegenseitigkeit müssen folgende Punkte berücksichtigt werden (vgl. [MH07]):

- Schutzniveau der Ausweichstandortes,
- zeitliche Verfügbarkeit der Ausweichumgebung,
- Unterstützung des Personals der kooperierenden Einrichtung bei der Integration des Forschungsnetzes,
- Ressourcenanteil (Räumlichkeiten, Systeme und Personal die dem Forschungsnetz zur Verfügung gestellt werden),
- Eskalationswege bei Interessenkonflikten,
- Abwicklung des Konfigurationsmanagements,
- zulässige Häufigkeit der Notfallübungen.

Im Rahmen der Erstellung von Business-Continuity-Plänen ist der Abschluss zusätzlicher Sachversicherungsverträge empfehlenswert. In einem Ernstfall sorgt dies für die zur Einleitung von Sicherheitsmaßnahmen notwendigen finanziellen Mittel.[31] Die in den Versicherungsverträgen vereinbarte Entschädigungsleistung darf sich nicht am Zeitwert der versicherten Gegenstände orientieren; der Neubeschaffungspreis muss als Richtwert für die Höhe der Entschädigung dienen (vgl. [bsi11d, M 6.16], s. a. Abschnitt C.1).

3.3.5. Verringerung der Lukrativität eines Angriffs (Benefit Denial)

Unter dem Begriff „Benefit Denial“ werden Maßnahmen zusammengefasst, die die Straftat für die Angreifer unrentabel machen sollen. In den Neunzigerjahren begannen einige Kaufhäuser ihre Waren mit Farbbehältern zu versehen. Diese konnten nur mit dem Spezialwerkzeug an der Kasse entfernt werden. Beim gewaltsamen Entfernungsversuch durch den Ladendieb brachen die Behälter und machten die Kleidung durch die darin enthaltene Farbe unbrauchbar. In vielen Juweliergeschäften existieren ähnliche Anti-Diebstahlsicherungen, deren unsachgemäße Entfernung die gestohlenen Gegenstände beschädigt. Zunehmend werden Fahrzeuge mit Sendern bestückt, die die genaue Position des gestohlenen Fahrzeugs übermitteln und so tief in die Steuerungselektronik des Autos integriert sind, dass es praktisch unmöglich ist, diese zu entfernen, ohne das Fahrzeug in einen „unbeweglichen Eisenhaufen“ zu verwandeln. Die o. g. Sicherungen senken die Lukrativität eines gesetzeswidrigen Gegenstanderwerbs und fallen damit unter den Begriff „Benefit Denial“ (vgl. [SC08, S. 111 ff.], [DC96], [Hay93]).

Forschungsnetzdaten lassen sich nicht ohne Weiteres mit Sicherungen ausstatten. Die einem Teilnehmer zur Verfügung gestellten Daten müssen in einer Form vorliegen, die ihm eine Weiterverarbeitung bzw. Auswertung der Daten erlaubt, was wiederum die unerwünschte Weitergabe von Daten an Dritte erleichtert. Die „Benefit Denial“-Maßnahmen

[31] Anmietung der Räume, Fortzahlung der Gehälter, Bestellung der Ersatzhardware etc.

des Forschungsnetzes reduzieren sich somit auf die Maßnahmen, die die Ermittlung der die Informationen verbreitenden Stelle ermöglichen. Dazu zählen die im Abschnitt 3.5.12 „Monitoring und Protokollierung“ beschriebenen Maßnahmen wie das Versehen von Bildern mit robusten Wasserzeichen und detaillierte Aufzeichnungen über die weitergegebenen/abgerufenen Daten. Die Verwendbarkeit der Daten zu nicht forschungsrelevanten Zwecken kann außerdem durch die strikte Einhaltung des Minimalprinzips und Pseudonymisierung bzw. Anonymisierung bei der Datenweitergabe verringert werden (vgl. [RDSP06]).
Zusätzlich zu den bereits erwähnten Maßnahmen sind weitere Vorkehrungen vorstellbar, die einen Angriff auf Forschungsnetzdaten weniger lukrativ machen. So ist bei einigen Erkrankungen bereits die Information über die Zugehörigkeit eines Patienten zu einem bestimmten Forschungsnetz schutzrelevant.[32] Die ausgespähte *IDAT*-Datenbank eines bestimmten Forschungsnetzes erlaubt Rückschlüsse über die Zugehörigkeit eines Patienten zu einer vom Forschungsnetz untersuchten Risikogruppe. Aus diesem Grund erscheint es logisch, die *IDAT*-Datenbanken mehrerer Forschungsnetze im Rahmen einer gemeinsamen Initiative zusammenzuführen. Für die Erzeugung, Verschlüsselung und Speicherung der *IDAT*-Datensätze müsste in diesem Fall ein einheitlicher Standard vereinbart werden. Durch die einheitliche *PID*-Erzeugung wäre eine Aussage über die Zugehörigkeit eines Patienten zu einem bestimmten Forschungsnetz nicht möglich (vgl. [Sch04]). Man könnte allerdings annehmen, dass diese Praxis im Widerspruch zu der Forderung einiger Datenschützer steht. [Sok99, S. 64]: *„Die Wahrscheinlichkeit, dass Patientendaten in unzulässiger Weise offenbart werden, hängt von ihrem Wert und von der Anzahl der Personen ab, die Zugang zu ihnen haben. Das Aggregieren von Patientendaten erhöht beide Risikofaktoren zugleich.“* Auch in den „Generischen Lösungen der TMF zum Datenschutz für die Forschungsnetze in der Medizin“ wird mit dem Verweis auf die gleiche Quelle festgestellt: *„Darüber hinaus wurde klargestellt, dass es keinen einheitlichen Patienten-Identifikator in verschiedenen Netzen geben darf...“* [RDSP06, S. XIV]. Die Warnung von [Sok99] bezieht sich jedoch auf die aggregierte Speicherung und Verarbeitung von Patientendaten allgemein. Es wäre falsch, aus dieser Aussage über die Gefahrenpotenziale einer aggregierten Datenspeicherung ein grundsätzliches Verbot für die Zusammenlegung der *IDAT*-Datenbanken herauszulesen. Die Zusammenlegung wäre folglich kein Widerspruch zu der Aussage der Datenschutz-Expertin. Jedoch ist die Warnung durchaus nachvollziehbar, denn die Wahrscheinlichkeit des Wiederfindens eines Personeneintrags in der Datenbank steigt mit der Anzahl der darin enthaltenen Datensätze. Die zusammengeführte *IDAT*-Datenbank aller Forschungsnetze würde einen großen Teil der Bevölkerung der Bundesrepublik Deutschland abbilden, was das Interesse am Ausspähen dieser Datenquelle und somit die Gefährdung erhöhen würde. Ein Kompromiss könnte im Zusammenschluss einiger weniger *IDAT*-Datenbanken bestehen, wobei die die gesellschaftlich tabuisierten

[32] Dies ist nicht nur bei gesellschaftlich tabuisierten Erkrankungen (z. B. AIDS) der Fall, sondern auch bei Krankheiten mit einem unmittelbaren Einfluss auf die Lebenserwartung bzw. Lebensqualität des Patienten.

Krankheiten untersuchenden Netze mit den sich mit „Volkskrankheiten“ befassenden Netzen zusammenschließen könnten. Die Größe eines Forschungsnetzes könnte ebenfalls als ein Zusammenschlusskriterium dienen (s. a. Abschnitt 5.1.1.4).

Organisatorische Aspekte von Sicherheitsrichtlinien, Zusammenfassung: In den vorhergehenden Abschnitten wurden einige organisatorische Aspekte der Sicherheitsarchitektur für medizinische Forschungsnetze untersucht: rechtliche und finanzielle Absicherung, personale Aspekte, Notfallvorsorgemaßnahmen, Wiederaufnahme des Betriebs sowie Benefit Denial. Als Nächstes erfolgt die Untersuchung administrativer Aspekte der Sicherheitsarchitektur.

3.4. Administrative Aspekte von Sicherheitsrichtlinien

Unter administrativen Schutzmaßnahmen versteht man Aktionen, die kontinuierlich den Betrieb begleiten. Zu den technisch-administrativen Schutzmaßnahmen zählen Systempflege, Reaktion auf Sicherheitsvorfälle sowie ihre Dokumentation und Infrastrukturvorkehrungen. Im Folgenden werden einige infrastrukturelle administrative Sicherheitsrichtlinien vorgestellt, wobei lediglich die für medizinische Forschungsnetze relevanten Aspekte beleuchtet werden und die Untersuchung nicht abschließend ist. Administrative Aspekte von Informationssicherheitsmaßnahmen werden ausführlich in den BSI IT-Grundschutz-Katalogen [bsi11d] erörtert. Auf die für die untersuchten Inhalte relevanten Bausteine und Module der Grundschutz-Kataloge wird bei der Erörterung der administrativen Aspekte der Sicherheitsrichtlinien im Rahmen dieses Abschnitts verwiesen.

Administrative Trennung von medizinischen und identifizierenden Daten: $IDAT$ und $MDAT^W$ werden konform zu § 40 Abs. 2 S. 2 BDSG (Verarbeitung und Nutzung personenbezogener Daten durch Forschungseinrichtungen) auf zwei unterschiedlichen Servern aufbewahrt. Die beiden Server sind physikalisch getrennt und werden von zwei unterschiedlichen Administratoren(-Teams) betreut. Es ist darauf zu achten, dass auch die wechselseitige Unabhängigkeit ihrer weisungsbefugten Vorgesetzten gegeben ist (vgl. [PB06], [RDSP06]). Als zusätzliche Sicherheitsmaßnahme dient die Zugriffseinschränkung für Wissenschaftler auf pseudonymisierte $MDAT^W$. So hat ein Angreifer, der die Identität eines Wissenschaftlers angenommen hat, Zugriff auf lediglich einen fest definierbaren Teil der medizinischen Daten ($MDAT^S$) mit einem geringen Reidentifizierungsrisiko (vgl. [RDSP06], [PRDS05]). Er ist somit nicht in der Lage, beliebige Abfragen gegen die Behandlungsdatenbank durchzuführen.

Aufzeichnung von Zutritten zu den kritischen Forschungsnetzbereichen: Sämtliche Forschungsnetzserver, die Patientendaten enthalten, sind in speziell abgesicherten Serverräumen aufzustellen. Den Zugang zu den Räumen soll nur für Administrationspersonal

durch die Authentifizierung mithilfe einer SmartCard nach der PIN-Eingabe möglich sein. Zugang zu den Räumen soll für institutsfremde Personen nach Möglichkeit vermieden werden und darf nur in Begleitung eines befugten Forschungsnetzmitarbeiters oder -dienstleisters beim Vorliegen einer Genehmigung des zentralen Benutzerservices erfolgen. Name der institutsfremden Person, Zeitpunkt, Grund und Dauer des Besuches sind in einer Protokollliste festzuhalten (vgl. [bsi11d, M 2.16-2.17]).

Unterbrechungsfreie Stromversorgung: Alle kritischen Infrastrukturbestandteile sind an eine USV-Anlage anzuschließen. USV kann nicht nur Stromausfälle für eine kurze Zeit überbrücken, sondern schützt die Forschungsnetzanlagen vor Über- und Unterspannung, Frequenzänderungen und Oberschwingungen. Eine Überbrückungszeit für Stromausfälle von 10 bis 15 Minuten gilt als angemessen. Für das geordnete Herunterfahren von Systemen empfiehlt BSI eine Stützzeit von 30 bis 60 Minuten, die sich aus der Wartezeit (ca. 10 Minuten) und der doppelten Shutdown-Zeit zusammensetzt (vgl. [bsi11d, M 1.25, M 1.28, M 1.70]).

Kontrolle der kritischen Bereiche: Innerhalb der kritischen Forschungsnetzbereiche[33] dürfen keine Broadcast-Komponenten[34] verwendet werden. In kritischen Forschungsnetzsegmenten dürfen nur Switches installiert werden, die lediglich dedizierte Verbindungen zulassen. Die nicht verwendeten SPAN-Ports[35] müssen deaktiviert werden. Wireless-Technologie (WLAN, Bluetooth etc.) soll im administrativen Bereich des Forschungsnetzes nicht eingesetzt werden. Die kritischen Bereiche müssen regelmäßig auf die unerlaubt installierte Wireless Access-Points untersucht und von diesen gesäubert werden (vgl. [bsi11d, M 2.277, M 4.298, G 2.117]).

Dokumentation der Sicherheitsvorfälle: Sämtliche Sicherheitsvorfälle müssen sauber dokumentiert werden. Dazu zählen Malware-Vorfälle, Datenverlust, Sicherheitswarnungen der Systeme etc. Die Dokumentation soll in digitaler Form an einer zentralen Stelle erfolgen. Nur berechtigte Personen (Administratoren, Auditors etc.) dürfen Zugang zu dieser Dokumentation haben (vgl. [bsi11d, M 6.134]).

Veränderungen der Sicherheitsinfrastruktur: Sämtliche Veränderungen an der Sicherheitsinfrastruktur (z. B. Änderungen der Router-Konfiguration, Firewallanpassung, Änderung der IDS-Konfiguration etc.) dürfen nur nach dem Vier-Augen-Prinzip erfolgen und müssen einheitlich und ausführlich dokumentiert werden (vgl. [bsi11d, M 2.221]).

[33] Dazu zählen beispielsweise Netzsegmente, in denen sich Administrationsarbeitsplätze, Datenspeicherungs- und Datenarchivierungseinrichtungen, DMZ-Systeme etc. befinden.

[34] Zum Beispiel Netzwerk-Hubs.

[35] Monitoring Ports.

Zugriffsrechtevergabe: Die Vergabe und Änderung von Zugriffsrechten erfolgt nur bei der Zustimmung von mindestens zwei dazu befähigten Personen nach dem „Need-to-know-Prinzip“ bzw. „Need-to-Access-Prinzip“.[36] Sämtliche Transaktionen dieser Art sind zu dokumentieren und regelmäßig (mindestens zwei Mal im Jahr) zu verifizieren. Zusätzlich ist die Integration eines IAM-Systems (Identity- and Access-Management) empfehlenswert. Die Eigenschaften eines IAM-Systems werden im Abschnitt 3.5.9 „Antimalware-Einrichtungen“ ausführlich erläutert (s. a. Abschnitt 3.5.4).

Datensicherung: Eine Datensicherung ist täglich durchzuführen. Mindestens ein Mal in der Woche muss ein Full-Backup sämtlicher Daten erfolgen. Die täglich anfallenden Backups dürfen nicht am Ort der Sicherung aufbewahrt werden. Es ist notwendig, ein unabhängiges, auf der Aufbewahrung von Datenbackups spezialisiertes Unternehmen mit der Aufbewahrung der Sicherungsbänder zu beauftragen. Die Datensicherung darf nur in verschlüsselter Form erfolgen, wobei eine symmetrische Verschlüsselung angewendet werden soll. Empfehlenswert ist der Einsatz von AES mit einer Schlüssellänge von 256 Bit. Die Anforderung von Backup-Tapes (z. B. zwecks Datenwiederherstellung) darf nur vom fest definierten Personenkreis nach Vier-Augen-Prinzip initiiert werden (vgl. [bsi11d, B. 1.4]).

Getrennte Datenhaltung: Im Abschnitt 4.3.2 „Bedrohungsorientierte Analyse“ wird die Gefahr eines Sniffing-Angriffs beschrieben. Eine der Ausprägungen des Sniffing-Angriffs wäre das Sammeln von *IDAT* möglichst vieler Patienten. Dieser Angriff kann durch die Verwendung von *TempIDs* vermieden werden.[37] $MDAT^W$ und *IDAT* befinden sich in keinem System zum gleichen Zeitpunkt außerhalb des Rechners des behandelnden Arztes. Der Angreifer könnte versuchen, die Schutzmechanismen der *IDAT*- und $MDAT^W$- Datenbanken auszuhebeln. Würde es ihm gelingen, die beiden Datenbanken auszuspähen, könnte er die darin enthaltenen Datenbestände zusammenführen. Die Tatsache, dass die beiden Datenbanken physikalisch voneinander getrennt sind und von unabhängigen Administratoren verwaltet werden, verkleinert jedoch das damit verbundene Risiko. Es ist sinnvoll, nicht nur unterschiedliche DBMS zu verwenden, sondern auch die Server unter unterschiedlichen Betriebssystemen zu betreiben (s. a. Abschnitt 3.5.8 „Datenbanksicherheit“). Die Verwendung von Systemen unterschiedlicher Hersteller ist in vielen anderen Situationen (z. B. zwecks Erreichung einer qualitativ hochwertigen Redundanz) empfehlenswert. Wenn das Ersatz- oder Ausfallsystem die gleiche Konfiguration wie das primäre System aufweist, kann

[36] Die Rechte sollen Zugriffe nur auf Informationen ermöglichen, die für den jeweiligen Behandlungs- oder Forschungskontex notwendig sind.

[37] Der behandelnde Arzt fragt bei der Patientenliste nach, ob ein bestimmter Patienteneintrag bereits existiert. Wenn dies der Fall ist, wird eine temporäre ID (*TempID*) erzeugt, die sowohl dem Arzt als auch der Behandlungsdatenbank übermittelt wird. Die Behandlungsdatenbank wird angewiesen, die *TempID* für die Dauer der Abfrage dem entsprechenden Patientendatensatz zuzuordnen. Diese wird nach einer erfolgreichen Abfrage gelöscht. Die Kommunikation (Übermittlung der *TempID*) zwischen der Patientendatenbank und der Behandlungsdatenbank erfolgt über eine sichere Verbindung (vgl. [RDSP06]).

davon ausgegangen werden, dass es prinzipiell die gleichen Schwächen, Sicherheitslücken etc. besitzt. So ist es z. B. nicht sinnvoll bei der Kompromittierung eines Webservers ein Ausweichsystem mit der gleichen Konfiguration wie das erfolgreich angegriffene in Betrieb zu nehmen.

PIN- und SmartCard-Verteilung: Zu den administrativen Schutzmaßnamen gehört auch die Verteilung von SmartCards und PINs an die Teilnehmer. Karten und PIN-Briefe (mehrere PINs sind notwendig z. B. für elektronische Signatur, Authentifizierung und Entschlüsselung, Entsperren und Ändern der PINs etc.) werden getrennt an die dezentralen Teilnehmerservices verschickt. Diese können von Teilnehmern persönlich gegen eine Unterschrift bei der Vorlage eines Lichtbildausweises abgeholt werden. Sowohl die Karten als auch die Briefe sollten so gestaltet sein, dass das Lesen der PIN in einem ungeöffneten Zustand nicht möglich ist. Außerdem soll das Öffnen der Briefe stets nachweisbar sein (vgl. [sch03, S. 12 ff.], s. a. Abschnitt 3.5.3).

Sperrung der Zugriffe: Sollte ein Forschungsnetzteilnehmer die SmartCard verlieren oder Verdacht auf eine Ausspähung des SmartCard-Schlüssels, der PIN etc. bestehen, ist das Zertifikat sofort sperren zu lassen (vgl. [sch03, S. 16], s. a. Abschnitt 3.5.6). Es ist sicherzustellen, dass der Nutzer beim Verlassen seines Arbeitsplatzes die SmartCard nicht unbeaufsichtigt lässt. Nach einer längeren Zeit ohne Benutzeraktion (z. B. sieben Minuten) ist die Forschungsnetzanwendung zu sperren. Die Entsperrung kann nur durch eine erneute Benutzerauthentifizierung (über SmartCard und PIN) erfolgen.

Informationspolitik: Die im Falle von bekannt gewordenen Sicherheitslücken zu treffenden Maßnahmen sind ein weiteres wichtiges Thema. Mitarbeiter und Teilnehmer des Forschungsnetzes müssen aufgefordert werden, die ihnen bekannt gewordenen Sicherheitslücken unverzüglich zu melden. Es soll ihnen untersagt werden, selbstständig die Öffentlichkeit über das Vorhandensein von Sicherheitslücken zu informieren,[38] Exploits, die diese Lücke ausnutzen, anzufertigen oder Pressestellungnahmen ohne vorherige Genehmigung zu beziehen. Der gemeldete Vorfall ist vom der dafür zuständigen Stelle[39] zu untersuchen; die erforderlichen Problembehebungsmaßnahmen sind zu treffen. Nach dem Beheben der Sicherheitslücke dürfen die Details des Vorfalls dem relevanten Personenkreis[40] bekannt gegeben werden. Die Entdecker der Sicherheitslücken sollten nach Möglichkeit honoriert werden, wobei selbstverständlich nicht nur finanzielle Leistungen

[38] Zum Beispiel durch Verfassen von Meldungen in einschlägigen Newsgroups.

[39] Zum Beispiel Ausschuss Datenschutz oder ein anderes, dem Ausschuss Datenschutz unterstelltes Gremium.

[40] Internes Administrationspersonal, Entwickler etc. Das Ziel soll sein, ähnliche Fehler in Zukunft zu vermeiden.

in Frage kommen (vgl. [bsi11d, M. 6.58, M. 2.1, M 3.55, M 3.77], s. a. Abschnitte 3.3.2, 3.3.4).
Die vorgeschlagene Vorgehensweise mag dem Full-Disclosure-Prinzip widersprechen, ist jedoch angesichts der hohen Schutzwürdigkeit der Patientendaten sinnvoll.[41]

Beschlagnahmesicherheit: Strafverfolgungsbehörden könnten (z. B. im Rahmen von staatsanwaltlichen Ermittlungen) ihr Interesse an den Forschungsnetzdaten bekunden. Die Herausgabe der für die Ermittlung relevanten Daten liegt nicht immer im Interesse des Forschungsnetzes, kann jedoch im Rahmen der Zusammenarbeit mit den Behörden akzeptabel sein. Es sollte jedoch der Fall vermieden werden, dass die Datenbestände des Forschungsnetzes beschlagnahmt werden. Gesetzliche Grundlage für die Beschlagnahme der Daten bilden § 94 Abs. 1 und Abs. 2 StPO.[42] Das für die Nichtherausgabe von Forschungsnetzdaten (Beschlagnahmesicherheit) maßgebliche „Schlupfloch“ weisen § 97 Abs. 1 Satz 3 StPO[43] und

[41] Das Full-Disclosure-Prinzip basiert auf der Tatsache, dass eine Schwachstelle unabhängig davon, ob sie jemand kennt oder nicht, existiert. Die Veröffentlichung der Schwachstellen mag zwar die Wahrscheinlichkeit eines Angriffs erhöhen, hat jedoch keinen Einfluss auf die Schwere der Schwachstelle. Die Veröffentlichung einer Sicherheitslücke ist außerdem die Voraussetzung dafür, dass man sich mit den für die Beseitigung dieser Schwachstelle erforderlichen Maßnahmen beschäftigen kann. Eine Schwachstelle kann vom Angreifer nicht ausgenutzt werden, wenn er diese nicht kennt. Im Umkehrschluss kann sich ein Forschungsnetz gegen einen Angriff nicht schützen, der nicht bekannt ist. Die grundsätzliche Gültigkeit des Full-Disclosure-Prinzips für das Forschungsnetz ist mehr als fraglich. Full-Disclosure berücksichtigt nämlich nicht die für das Forschungsnetz gültigen Rahmenbedingungen: Geschlossene Infrastruktur mit einem überschaubaren externen Benutzerkreis, der außerdem in seinem Handeln an die Sicherheitsleitlinie des Forschungsnetzes gebunden ist. Der Full-Disclosure-Ansatz entstand ursprünglich aufgrund der langsamen Reaktion von Softwareherstellern auf gemeldete Sicherheitsprobleme. Durch die Veröffentlichung von Sicherheitslücken versprach man sich ein schnelleres Erstellen von Patches. Innerhalb der Full-Disclosure-Gemeinde existieren unterschiedliche Anschauungen, an wen, wann und welche Informationen weitergegeben werden dürfen. So melden viele Full-Disclosure-Anhänger den Vorfall erst an den Softwarehersteller und veröffentlichen die Details nach dem Ablauf einer bestimmten Frist, was dem Hersteller die Möglichkeit gibt, die Sicherheitslücke zu beheben.

Unabhängig von der Anwendbarkeit des Full-Disclosure-Prinzips im geschilderten Zusammenhang ist von dem „security through obscurity“-Prinzip – der Hoffnung, eine Sicherheitslücke würde durch den relativ kleinen Bekanntheitsgrad und z. T. nicht vorhandenen Know-how der Teilnehmer nicht bemerkt und nicht ausgenutzt – abzuraten. Auf Dauer würde solche Praxis der Sicherheit des Forschungsnetzes schädigen. Um das Beheben von gefundenen Sicherheitslücken zu beschleunigen, kann – alternativ zum in Falle eines Forschungsnetzes kaum anwendbaren Full-Disclosure-Ansatz – die interne priorisierte Behandlung von Sicherheitsvorfällen eingesetzt werden. Dies kann z. B. durch entsprechende Vereinbarungen in den SLAs bei externen Produkten/Dienstleistungen oder dem Code-Freeze für interne Produktweiterentwicklungen bis zur Fehlerbehebung sein. In vielen Fällen kann man sogar das Abschalten von Diensten bis zu einer endgültigen Fehlerbehebung bzw. Klärung der Situation in Erwägung ziehen (s. a. Abschnitt 4.3.2 „Bedrohungsorientierte Analyse“).

[42] „(1) Gegenstände, die als Beweismittel für die Untersuchung von Bedeutung sein können, sind in Verwahrung zu nehmen oder in anderer Weise sicherzustellen. (2) Befinden sich die Gegenstände in dem Gewahrsam einer Person und werden sie nicht freiwillig herausgegeben, so bedarf es der Beschlagnahme.“

[43] „Der Beschlagnahme unterliegen nicht (...) andere Gegenstände einschließlich der ärztlichen Untersuchungsbefunde, auf die sich das Zeugnisverweigerungsrecht der in § 53 Abs. 1 Satz 1 Nr. 1 bis 3b Genannten erstreckt.“

§ 97 Abs. 2 Satz 3 StPO[44] auf. In [RDSP06] wird vorgeschlagen, die Forschungsnetzdaten zwecks Beschlagnahmesicherheit unter die Aufsicht von Rechenzentren von Universitäts- bzw. Großkliniken zu stellen, denn obwohl ein Forschungsnetz mit Patientendaten arbeitet, genießen diese nicht die Beschlagnahmefreiheit.[45] Die Beschlagnahmesicherheit der bei den Kliniken untergebrachten und im Behandlungszusammenhang verwendeten Forschungsdaten resultiert aus der ärztlichen Schweigepflicht. Die direkte Beauftragung eines Dienstleisters zur Verarbeitung von Forschungsnetzdaten würde eine Beschlagnahme somit nicht verhindern können. Wenn aber eine Krankenanstalt einen Dienstleister mit der Verarbeitung von Forschungsnetzdaten beauftragen und dem Forschungsnetz die Nutzung dieser Daten erlauben würde, wären diese Daten vor Beschlagnahme sicher. Für die Bewertung der Beschlagnahmesicherheit ist auch die Betrachtung des Forschungsnetzes als ein Gehilfe des Arztes interessant, der im Auftrag einer oder mehrerer Krankenanstalten (datenerhebende Stellen) Daten verwaltet. Die Beschlagnahmesicherheit der Daten würde aus der ärztlichen Schweigepflicht bzw. aus dem verfassungsrechtlich verankerten Recht des Patienten auf Selbstbestimmung resultieren[46] und sich auf das Forschungsnetz analog zum § 203 Abs. 3 StGB anwenden lassen (vgl. [SPR+06], s. a. Anhang E „Auszüge aus BDSG und StGB“). Die ärztliche Schweigepflicht findet jedoch mit höchster Wahrscheinlichkeit keine Anwendung, wenn die Daten dem Arzt (bzw. einer medizinischen Einrichtung) im Rahmen eines Forschungsvorhabens und nicht einer medizinischen Behandlung übertragen werden.

Eine weitere Möglichkeit, die Beschlagnahmesicherheit von Forschungsdaten zu erreichen, könnte darin bestehen, die Forschungsnetzdaten bei einer „beschlagnahmefesten“ Personengruppe (Geistliche, Abgeordnete, Schwangerschaftsberater, Mitarbeiter von Presse und Rundfunk, Rechtsanwälte, Steuerberater etc.) unterzubringen. Nach der aktuellen Rechtsauffassung bietet jedoch noch nicht einmal die die größten Erfolgsaussichten in Bezug auf die Beschlagnahmesicherheit bei der Datenunterbringung aufweisende Berufsgruppe der Notare einen Schutz vor Beschlagnahme: Bei einem als *Datentreuhänder* agierenden Notar kann der Bezug zwischen den Forschungsdaten und der Berufsausübung nicht immer als ge-

[44] „Diese Beschränkungen gelten nur, wenn die Gegenstände im Gewahrsam der zur Verweigerung des Zeugnisses Berechtigten sind ... Der Beschlagnahme unterliegen auch nicht Gegenstände, auf die sich das Zeugnisverweigerungsrecht der Ärzte, Zahnärzte, Psychologischen Psychotherapeuten, Kinder- und Jugendlichenpsychotherapeuten, Apotheker und Hebammen erstreckt, wenn sie im Gewahrsam einer Krankenanstalt oder eines Dienstleisters, der für die Genannten personenbezogene Daten erhebt, verarbeitet oder nutzt, sind, sowie Gegenstände, auf die sich das Zeugnisverweigerungsrecht der in § 53 Abs. 1 Satz 1 Nr. 3a und 3b genannten Personen erstreckt, wenn sie im Gewahrsam der in dieser Vorschrift bezeichneten Beratungsstelle sind. Die Beschränkungen der Beschlagnahme gelten nicht, wenn die zur Verweigerung des Zeugnisses Berechtigten einer Teilnahme oder einer Begünstigung, Strafvereitelung oder Hehlerei verdächtig sind oder wenn es sich um Gegenstände handelt, die durch eine Straftat hervorgebracht oder zur Begehung einer Straftat gebraucht oder bestimmt sind oder die aus einer Straftat herrühren.“

[45] Von Relevanz ist die Feststellung zur Beschlagnahmesicherheit aus dem von TMF vergebenen Rechtsgutachten zu den Biobanken [BGH+06].

[46] Die ärztliche Schweigepflicht ist auch als Berufspflicht im § 9 MBO-Ä festgelegt.

geben angenommen werden, wodurch auch der Beschlagnahmeschutz der Forschungsdaten durch die Tätigkeit als Notar fragwürdig erscheint. Nach der aktuellen Rechtsauslegung macht das Bedürfnis nach der Aufrechterhaltung des Vertrauensverhältnisses zwischen dem Arzt und dem Patient den forschenden Arzt bzw. die entsprechende medizinische Einrichtung zeugnisverweigerungsberechtigt. Somit können die im Rahmen von Studien erhobenen Daten dem Beschlagnahmeschutz unterliegen, wenn der Verbleib der Daten in der Einrichtung gegeben ist. Auch die beschlagnahmesichere Aufbewahrung der erhobenen Daten bei einem Dienstleister scheint gegeben zu sein, wenn ein direkter Auftrag des behandelnden Arztes an den Dienstleister zwecks Datenaufbewahrung vorliegt. Hier muss jedoch zwischen den personenbezogenen Daten des Patienten und den medizinischer Dokumentation des Arztes unterschieden werden. Dem Beschlagnahmeschutz unterliegt nämlich die ärztliche Dokumentation und nicht die sich in der Datenhoheit des Patienten befindenden Daten (vgl. [RHJ08, S. 56 f.]).
Ein Datentreuhänder als eine selbstständige, Daten besitzende Stelle übernimmt die Rolle eines vertrauenswürdigen Dritten zwischen den Patienten, Forschern und der Daten haltenden Stelle. Die Unabhängigkeit des Datentreuhänders wird durch eine klare räumliche und organisatorische Trennung von den Forschern und den Daten haltenden Stellen zum Ausdruck gebracht. Ein Treuhänder muss weisungsunabhängig sein und sich auf ein Beschlagnahmeverbot berufen können. Der Datentreuhänder muss außerdem an eine Schweigepflicht gebunden sein und ein Aussageverweigerungsrecht besitzen (vgl. [RDSP06], [MW02]). Der Beschlagnahmeschutz gilt jedoch nur dann, wenn ein unmittelbarer Bezug zur Berufsausübung besteht, was u. U. im nicht gegebenen Beschlagnahmeschutz der Forschungsdaten resultieren kann. Diese Auffassung wird durch Rechtsgutachten bestätigt, sodass eine Datenunterbringung z. B. bei einem Notar als Datentreuhänder, keine Vorteile im Bezug auf den Beschlagnahmeschutz im Vergleich zum Klinikrechenzentrum bietet. (vgl. [RHJ08, S. 56 f.], [PSM+09, S. 1757]).
Zu den administrativen Komponenten einer Sicherheitsarchitektur gehört auch die Vergabe von Serviceaufträgen und eine geordnete Reaktion auf die Sicherheitsvorfälle. Diese beiden Aspekte der administrativen Maßnahmen werden im Abschnitt C.2 „Merkmale von administrativen Sicherheitsrichtlinien“ des Anhangs C erläutert.

Zusammenfassung: Im Abschnitt 3.4 wurden u. a. die administrativen Aspekte der Sicherheitsrichtlinien für medizinische Forschungsnetze untersucht. Im nächsten Abschnitt erfolgt die Analyse technischer Sicherheitsrichtlinien als Bestandteil der Sicherheitsarchitektur eines medizinischen Forschungsnetzes.

3.5. Technische Aspekte von Sicherheitsrichtlinien

Technische Aspekte der Informationssicherheitsarchitektur umfassen die Beschreibung der Soft- und Hardwarekomponenten mit dem Ziel, die Vertraulichkeit, die Integrität und die Verfügbarkeit von Forschungsnetzdiensten und -daten zu gewährleisten. In den folgenden Unterabschnitten werden die wichtigsten technischen Komponenten einer Sicherheitsarchitektur für medizinische Forschungsnetze untersucht. Die in diesem Abschnitt beschriebenen Zugriffskontroll-, Verbindlichkeits- und Bridging-Komponenten gewährleisten eine sichere Arbeitsumgebung, eine sichere Zusammenführung von Patientendaten, Authentifikationsverfahren, Vergabe von Zugriffsberechtigungen, Verzeichnisdienste sowie die Datenbanksicherheit. Der Abschnitt schließt mit der Darstellung eines Beispielszenarios für das Zusammenspiel dieser einzelnen Komponenten. Um den Umfang dieses Abschnitts nicht zu sprengen, wurde die Darstellung der Technologiegrundlagen und einiger Aspekte der technischen Sicherheitsarchitektur in den Anhang C platziert. Die jeweiligen Verweise werden im Text gekennzeichnet.

3.5.1. Sichere Arbeitsumgebung

Das Problem einer sicheren Arbeitsumgebung beschäftigt Sicherheitsexperten seit geraumer Zeit, sodass entsprechend viele Konzepte für diesen Problembereich bereits entwickelt wurden. Die meisten dieser Lösungsansätze entstammen entweder dem Militär oder der Rechteindustrie.[47] Eine der bekanntesten Initiativen in dieser Richtung ist der TCPA-Nachfolger TCG. Die meisten bisher entwickelten Konzepte widersprechen den Grundsätzen einer offenen Arbeitsumgebung, und basieren auf einer obligatorischen Einführung eines Hardwaremoduls.[48]

Trotz der Abneigung Vieler gegen die o. g. Technologie eignet sich diese, um eine für die Sicherheit des Forschungsnetzes kritische vertrauenswürdige Laufzeitumgebung zu schaffen. Es ist wichtig sicherzustellen, dass insbesondere Forschungsnetzteilnehmer, die mit personenbeziehbaren oder -bezogenen Daten arbeiten, mit sicheren malwarefreien Systemen an den angebotenen Diensten partizipieren; dies setzt jedoch eine standardisierte Hardwarebasis voraus. Die flächendeckende Standardisierung der sicheren Hardwareumgebung ist in der absehbaren Zukunft nicht durchsetzbar, obwohl IBM bereits seit 2003 die Notebooks mit der Technologie ausstattet, und auch Intels eigene Lösung[49] seit 2007 mit

[47] Die Entstehung des Konzeptes für das sichere Booten ist in den Entwicklungen der Rechtenindustrie eher als Nebenprodukt zu sehen.

[48] So setzt beispielsweise TCG auf das sogenannte Trusted Platform Module (TPM) und eine BIOS-Erweiterung namens „Core Root of Trust Measurement“ (CRTM). Eine aus der Sicht des Autors lesenswerte Auseinandersetzung mit den Perspektiven und Gefahren der TCG-Technologie ist im Buch von Norbert Pohlmann und Helmut Reimer *„Trusted Computing : Ein Weg zu neuen IT-Sicherheitsarchitekturen“* [HH07] zu finden.

[49] Trusted Execution Technology ehemals LaGrande Technology.

der Einführung der Chipsätze Q33 und Q35 auf dem Markt verfügbar ist. Auch wenn die Festlegung auf eine bestimmte Hardwareausstattung[50] für das Administrationspersonal denkbar ist, würde es den Grundsätzen eines Forschungsnetzes widersprechen, Benutzer mit einer dem Forschungsnetz nicht konformen Hardwareausstattung von den Diensten auszuschließen (s. a. Abschnitt 3.1).

Die Schaffung einer sicheren Hardwareumgebung für die Administrationskräfte des Netzes setzt den Einsatz einer TCG-konformen Hardware voraus. Diese besteht aus einem in das System fest integrierten Trusted Platform Module (TPM); einem Chip, der von der BIOS-Erweiterung des Systems unterstützt wird. Dieser Chip kann zwar den Bootvorgang des PCs nicht beeinflussen, ist jedoch in der Lage, die verwendeten PC-Komponenten zu identifizieren. Selbstverständlich ist es möglich,[51] die unverschlüsselte Kommunikation zwischen dem sogenannten Fritz-Chip[52] und der CPU abzuhören. Ein solcher Angriff ist allerdings aufwendig und wird noch schwieriger, wenn TPM im Hauptprozessor untergebracht wird. Die für die Sicherheit des Forschungsnetzes maßgeblichen TPM-Eigenschaften sind:

- Hardwareschutz für die im TPM gespeicherten Schlüssel und Signaturen,
- Verifizierung der Systemkonfiguration und des Systemstatus mithilfe von Hashwerten,
- Daten- und Dateischutz durch einen Hardware-Zufallszahlengenerator für die Erzeugung von starken Schlüsseln (vgl. [tcg09b], [And03]).

Trotz ihrer grundsätzlichen Zuverlässigkeit bieten die hardwarebasierten Sicherheitsmaßnahmen keinen hundertprozentigen Schutz, wenn die Hardware sich im Besitz des Angreifers befindet.[53] Der Aufwand für einen Hardwareangriff ist jedoch i. d. R. höher als im Falle eines Softwareangriffs. Bei einem ausreichend hohen Aufwand lohnt sich der Angriff nicht mehr; ob die getroffenen Sicherheitsmaßnahmen hard- oder softwarebasiert sind, ist zweitrangig. Die Frage, ob es möglich ist, innerhalb einer unsicheren Hardwareumgebung, eine sichere Softwareumgebung einzurichten, kann mit einem eindeutigen Nein beantwortet werden. Nun stellt sich die Frage, wie man mit einem vertretbaren Aufwand, ohne die Benutzer in ihrer Arbeitsweise besonders einzuschränken, eine geschützte Plattform mit Softwaremitteln erzeugen kann, wobei diese Umgebung vom Angreifer nur mit einem enorm hohen Aufwand kompromittiert werden kann. Im Abschnitt C.3.1 wird ein solcher

[50] Dies würde die Einrichtung einer sicheren Umgebung möglich machen.

[51] Das Vorhandensein nicht unerheblicher finanzieller Mittel vorausgesetzt.

[52] Diese Bezeichnung wurde zu Ehren von Fritz Hollings vergeben – eines ehemaligen US-Senators, der sich besonders stark für die globale Einführung von TC eingesetzt hat. TCG streitet die Ähnlichkeiten ihrer Technologie mit dem Fritz-Chip ab und weist darauf hin, dass der Fritzchip mit dem DRM-Hintergrund entwickelt wurde (vgl. [CFF+04]).

[53] Ein Beispiel dafür, dass noch nicht einmal die Chipsätze vor physikalischen Angriffen geschützt sind, ist in [CNO08] dokumentiert. Durch das Abschleifen und das Abfotografieren der Schichten des MiFare-Chipsatzes mithilfe eines elektronischen Mikroskops konnten die Schwächen der in den Chipsätzen verwendeten Verschlüsselung „Crypto-1“ nachgewiesen werden.

softwarebasierter Ansatz vorgestellt, mit dem sich ein erfolgreicher Angriff auf die Arbeitsumgebung zwar nicht vollständig vermeiden, dessen Wahrscheinlichkeit sich jedoch auf ein akzeptables Maß reduzieren lässt. Bei der Auswahl eines Konzeptes für eine sichere Arbeitsumgebung müssen mehrere Faktoren berücksichtigt werden, um ein erforderliches Niveau an Sicherheit zu gewährleisten. Im Abschnitt C.3.1 werden einige Aspekte des Einsatzes von softwaregeschützten Arbeitsumgebungen inklusive Überlegungen zum Einsatz von Remote-Desktop- und TPM-Technologien sowie Konzepte zur Sicherstellung der Ausfallsicherheit von Arbeitsumgebungen näher untersucht.

3.5.2. Zusammenführung von Patientendaten

Im vorhergehenden Abschnitt erfolgte die Beschreibung der technischen Alternativen für die Gewährleistung einer sicheren Arbeitsumgebung. Die Sicherheit der Arbeitsumgebung ist insbesondere für die vertrauliche Zusammenführung von Patientendaten *IDAT* und *MDAT* im Behandlungszusammenhang von Bedeutung. Die technischen Aspekte der während der Erstellung dieser Arbeit aufgetretenen Fragestellung nach der Zusammenführung der Daten im Clienten werden in diesem Abschnitt untersucht. Die Zielsetzung ist der Vergleich von Ajax, Java und der Terminal Server-Technologie in Bezug auf ihre Eignung, die Anforderungen der Datenprozessierung in den klinisch fokussierten medizinischen Forschungsnetzen zu erfüllen. Der Vergleich bezieht sich auf die Einsatzpotenziale der o. g. Technologien und bewertet nicht die tatsächliche Sicherheit einer möglichen konkreten Umsetzung. Mit der gleichen Technologie sind viele besser oder schlechter geeignete Konfigurationen denkbar; auch die Entwicklungs-, Implementierungs- und Einsatzaspekte der Anwendung müssen berücksichtigt werden. Schließlich werden nicht die drei Technologien nach dem „Stiftung Warentest-Prinzip“ bewertet, um die „ultimative“ Siegertechnologie zu ermitteln. Vielmehr werden die potenziellen Kombinationsmöglichkeiten dieser Technologien untersucht, denn diese können sich im Rahmen einer Lösung sinnvoll ergänzen, um eine sichere Zusammenführung von *IDAT* und *MDAT* zu gewährleisten.

3.5.2.1. Sicherheit von Ajax

In den letzten Jahren ersetzt zunehmend die Ajax-Technologie die klassischen Desktop-Anwendungen. Dabei realisiert man mithilfe der Webtechnologie Desktop-ähnliche Applikationen. Als Grundlage für Ajax dienen HTML/XHTML, DOM, JavaScript und XMLHttpRequest.
Die Basis für die Sicherheit von Ajax bilden die asynchrone Datenübertragung und das zugrunde liegende JavaScript. Ajax-Anwendungen bestehen aus der Client- und Serverseite sowie dem Transportweg und gehören somit zu den verteilten Systemen. Die Ajax-Skripte werden in einer Sandbox-ähnlichen Umgebung im Browser des Nutzers ausgeführt, die den Aufbau von Verbindungen zu den anderen Skripten via XMLHttpRequest und die Manipulation der lokalen Benutzer-Ressourcen verhindern soll.

Bei unzureichender Validierung von GET- und POST-Parametern kann eine solche Anwendung gegenüber von Cross-Site Scripting-Angriffen (XSS) anfällig sein. Die Zusammenführung der Patientendaten auf dem Client-Rechner setzt jedoch die Freischaltung dieser unsicheren Technologie voraus, was die Vertrauenswürdigkeit des gesamten Ansatzes negativ beeinträchtigt.
Die in der letzten Zeit stattgefundene starke Verbreitung der XSS-Angriffe führte zu der Aufrüstung auf der Seite der Sicherheitsexperten. Moderne Browser erkennen viele XSS-Angriffe zuverlässig, sodass es wahrscheinlich ist, dass die Operation der Datenzusammenführung auf dem Client mithilfe von XSS als Angriff erkannt wird. Es ist denkbar, dass der gleichzeitige Datenabruf von zwei Servern in einer Websitzung von den Sicherheitsmechanismen des Browsers als ein Angriff gewertet und nicht zugelassen wird. Dies kann die Umsetzbarkeit der Ajax-Lösungen in der Praxis und ihre Verbreitung zwecks Datenzusammenführung im Clienten nach dem Vorschlag des generischen Datenschutzkonzeptes einschränken.
Bei einer Kompromittierung des Systems erleichtert Ajax die Durchführung weiterer Angriffe, da der Datenaustausch via XMLHttpRequest für den Benutzer transparent im Hintergrund erfolgt. Diese potenzielle Sicherheitslücke ist jedoch keine Besonderheit der Ajax-Anwendungen und kann auch auf JavaScript-Applikationen zutreffen. Für die untersuchte Fragestellung ist es wichtig, zu analysieren, auf welche Art und Weise die o. g. Komponenten einer Ajax-Anwendung angegriffen werden können. Die Untersuchungsergebnisse der möglichen Angriffsszenarien auf die Ajax-basierte Datenzusammenführung sind im Abschnitt C.3.3.1 zusammengefasst.
Eine Erhöhung der Sicherheit einer Ajax-Anwendung kann durch die Verwendung von Ajax-Frameworks[54] erreicht werden. Die Vorteile von solchen Frameworks bestehen in den von professionellen Entwicklern aufbereiteten Funktionen. Es liegt im Interesse der Entwickler, die populären Frameworks im Hinblick auf die Sicherheitsaspekte zu prüfen. Ein Beispiel dafür, dass die Ajax-Frameworks auf ihre Sicherheit systematisch untersucht werden, ist das OWASP AJAX Security-Projekt.[55] Das Projekt wurde mit dem Ziel gegründet, die gängigen Ajax-Frameworks auf ihre Sicherheitsaspekte zu untersuchen. Auf der Basis der OWASP Top Zehn-Liste können Sicherheitsmetriken entwickelt werden (vgl. [owa12], [NP07]). Die Verwendung von Frameworks kann jedoch auch zu einem Sicherheitsproblem werden, wenn das Framework Sicherheitslücken aufweist. Die auf diesem Framework aufsetzenden Implementierungen erben die Sicherheitslücken des Frameworks, was die Attraktivität der Suche nach den Framework-Exploits erhöht; denn ein Angreifer kann durch die Ausnutzung

[54]Zum Beispiel ASP.NET Ajax Framework, XAJAX, SAJAX etc. In diesem Abschnitt steht der Framework-Begriff für ein Programmiergerüst, das als Rahmen für die Softwareentwicklung verwendet wird und dem Entwickler bestimmte Bausteine zur Designstruktur zur Verfügung stellt bzw. die Erstellung diverser Applikationen ermöglicht. Eine abweichende Framework-Definition in Verbindung mit dem Sicherheits- und Risikomanagement befindet sich im Glossar.

[55]OWASP: Open Web Application Security Project.

einer Sicherheitslücke in der Framework-Implementierung eine Vielzahl von den auf dem betroffenen Framework basierenden Anwendungen kompromittieren.
Um die Sicherheit der Ajax-basierten Applikationen zu prüfen, könnten Penetrations-Tests durchgeführt werden. Da die einer Ajax-Applikation zugrunde liegenden Strukturen denen einer gewöhnlichen Webanwendung ähneln, gelten hier grundsätzlich dieselben Prüfroutinen bzw. -punkte. So ist z. B. auf die Verwendung einer möglichst aktuellen Browser-Version bzw. potenzielle Fehler in der JavaScript-Implementierung des Browsers zu achten.

3.5.2.2. Sicherheit von Java

Die Bezeichnung „Java“ ist vielschichtig, sodass es falsch wäre, allgemein von der Java-Sicherheit zu schreiben. Die Sicherheit eines Java-Applets kann kaum mit der Sicherheit einer Java-Servlet-Anwendung verglichen werden, die ihrerseits nicht mit der Sicherheit eines Standalone-Java-Programms gleichgestellt werden kann. Um die Java-Sicherheit im Kontext der Datenzusammenführung bewerten zu können, muss daher eine Eingrenzung der für die Fragestellung relevanten Java-Technologie erfolgen. Diese vorgenommene Eingrenzung darf jedoch nicht zu einem konkreten Implementierungskonzept werden, da sonst die Sicherheit einer bestimmten Konfiguration und nicht die allgemeine Sicherheit der Java-Plattform im Zusammenhang mit der Zusammenführung von Patientendaten bewertet wäre.
Die Basissicherheitsfunktionen der Java-Technologie werden im Abschnitt C.3.3.2 „Nutzung der Java-Sicherheitsfunktionen für die Datenzusammenführung“ erörtert. Im gleichen Abschnitt wird beispielhaft das Szenario einer Java-basierten Datenzusammenführung aufgezeigt.
Für den dargestellten Aufbau und den Ablauf der Datenzusammenführung gelten die gleichen Angriffe wie in Falle der Ajax-Technologie: Die Angriffe können auf dem Client, dem Server oder dem Transportweg erfolgen. Die grundlegenden Angriffsszenarien werden im Zusammenhang mit der Ajax-Sicherheit im Abschnitt C.3.3.1 beschrieben, sodass an dieser Stelle keine explizite Analyse der Angriffsarten erfolgt.

3.5.2.3. Sicherheit der Terminalserver-Technologie

Beim Einsatz der Terminal Services-Technologie für die Datenzusammenführung soll zuerst die Frage beantwortet werden, ob die Daten nun auf dem Client oder doch zentral zusammengeführt werden. Für die clientseitige Datenzusammenführung spricht die Tatsache, dass die Logik der Datenzusammenführung auf den Clients abgebildet ist, die durchaus unterschiedliche Beschaffenheit haben können. Für die Klassifizierung als einen zentralisierten Ansatz spricht dagegen, dass die kritischen Anwendungen an einer zentralen Stelle einfacher kontrolliert und geschützt werden können.

Die Sicherheit der Terminalserver-Technik wird im Abschnitt 3.5.1 „Sichere Arbeitsumgebung“ erörtert. Kennzeichnend für das zu untersuchende Anwendungsfeld ist die Tatsache, dass die Patientendaten an einer zentralen Stelle – dem Terminal Server zusammengeführt werden. Dies gewährleistet einerseits eine höhere Sicherheit, da die zentralen Dienste i. d. R. einfacher abzusichern sind, als die inhomogenen verteilten Client-Ressourcen. Gleichzeitig stellt die Zentralisierung besondere Anforderungen an die Sicherheitsvorkehrungen, da die zentralen Dienste lukrativere Angriffsziele darstellen. Die Kompromittierung des zentralen Terminal Service-Dienstes wäre vermutlich schwerwiegender als die Kompromittierung eines einzelnen Clients.
Um die Sicherheitseigenschaften der Terminal Services-Technologie zusammenzufassen, bleibt festzuhalten, dass die Beschaffenheit der Clients und der Laufzeitumgebungen zwar unterschiedlich sein könnte, man sich jedoch aus administrativen Gründen wahrscheinlich für eine gemeinsame Zielplattform entscheiden würde. Ein Angreifer, der den Terminal Server übernimmt, hätte Zugriff auf die Sessions mehrerer Clients, sodass hier die Aufteilung der Daten aus der sicherheitstechnischen Perspektive nicht so vorteilhaft wäre wie im Falle des „echten“ clientbasierten Ansatzes.
Sowohl aktive als auch passive Angriffe wären auch bei diesem Einsatzszenario denkbar. Durch die Verwendung eines Standard-Pakets als Terminal-Services ergeben sich einerseits die Vorteile durch den Hersteller-Support und eine (hoffentlich) schnelle Fehlerbehebung. Andererseits könnten die Terminal-Lösungen ebenfalls eine Reihe von Sicherheitslücken aufweisen, die ein Angreifer dann ausnutzen könnte. Zu berücksichtigen ist auch, dass zwischen den Clients und dem Terminal Server nicht die Patientendaten, sondern die Daten der Terminal-Sessions übertragen werden. Da die gängigen Produkte bereits in der Standardkonfiguration Verschlüsselung einsetzen, bleibt die Wahrscheinlichkeit für einen erfolgreichen Angriff auf dem Transportweg relativ gering.

3.5.2.4. Kombination der Technologien

Am Anfang des Abschnitts 3.5.2 wurde erwähnt, dass die drei beschriebenen Technologien nicht als Konkurrenz zueinander verstanden werden müssen. Vielmehr existieren Szenarien, in denen die Vorteile der Technologien miteinander kombiniert werden. Ein Beispiel für eine solche Symbiose ist der parallele serverseitige Einsatz von Terminal-Services und Java. Die Abbildung 5 veranschaulicht den Einsatz von Terminal-Services, um dem Nutzer eine abgesicherte vertrauenswürdige Umgebung mit einem eingeschränkten Umfang an Applikationen zur Verfügung zu stellen. Dies kann z. B. nur ein bestimmter Browser sein, mit dessen Hilfe man auf den dahinter platzierten Webserver zugreifen kann, oder die vom medizinischen Personal verwendete Client-Applikation. Der Vorteil eines solchen Aufbaus liegt darin, dass die zentralisierte Integrität der Terminal Server-Umgebung einfacher und zuverlässiger erreicht werden kann als die Integrität der sich in der „Benutzer-Gewalt“ befindenden Systeme. Die vom Terminal-Server aus auf dem Webserver erfolgenden Zugriffe

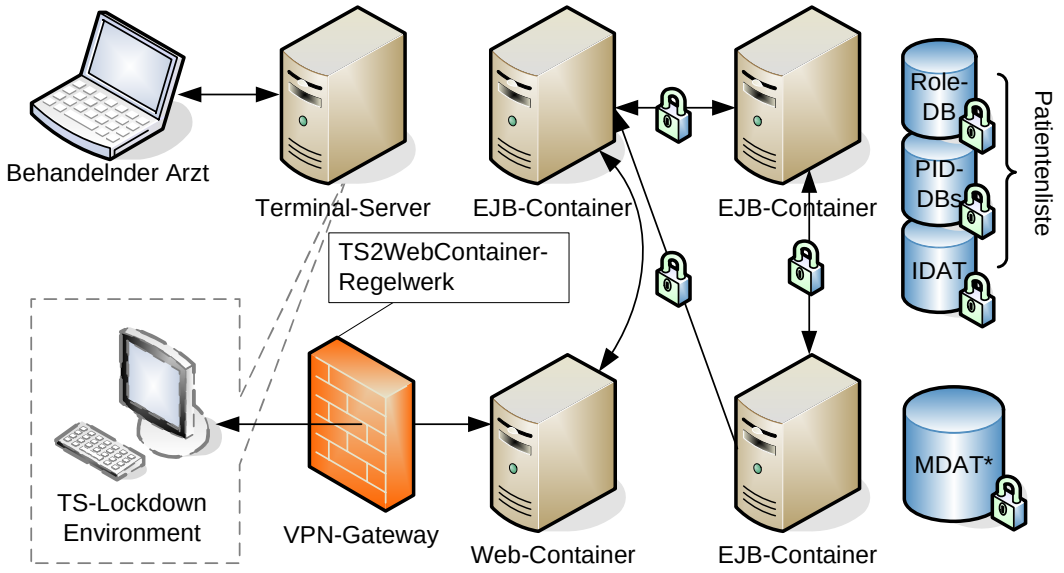

Abbildung 5.: Kombination aus Terminal-Services und Java-Technologie: Die Client-Zugriffe erfolgen aus einer kontrollierten – auf Terminal-Services basierenden – Umgebung.

können auf einen mindest notwendigen Maß reduziert werden.[56] Zusätzlich kann die Einhaltung des aufgestellten Sicherheitsregelwerks vor dem Zugriff auf den Webserver kontrolliert werden. Dadurch wird sichergestellt, dass gegen den Webserver keine direkten Angriffe von den Clients aus erfolgen können. Als ein – beim reinen clientseitigen Webserver-Zugriff nicht existierender – Nachteil der Zusammenlegung beider Technologien gilt das bereits bei den Terminal-Services erwähnte Argument, dass die Fehler in der Terminal-Software dem Angreifer Einblick in die Sessions anderer Benutzer offenbaren können.

3.5.3. Authentifizierung von Forschungsnetzteilnehmern

Es existieren mehrere Ansätze zur Überprüfung der Teilnehmeridentität. Häufig authentisiert sich ein Teilnehmer, indem er seine ID in Verbindung mit einem Passwort eingibt, wobei die Benutzer-ID i. d. R. nicht geheim ist. Diese sogenannte passwortbasierte Authentifikation hat diverse Nachteile: Gewöhnlich hat ein Benutzer eine Vielzahl von ID/Passwortkombinationen für mehrere Systeme. Die Menge an Passwörtern[57] zwingt den Benutzer zur Verwendung von gleichen oder leicht zu erratenden Passwörtern für mehrere Systeme und zum Einsatz von trivialen Passwortmodifikationsverfahren.[58] Dies macht die Passwörter anfällig für Wörterbuch- und Brute-Force-Angriffe. Ein durch Phishing-Angriff bekannt gewordenes Passwort vom privaten E-Mail-Account öffnet dem Angreifer häufig Zugriff zum Firmenlogin, Onlinebanking-System und diversen weiteren Diensten. Durch

[56] Zum Beispiel durch die Einschränkung der IP-Adressbereiche, Ports und Protokolle.

[57] Diese müssen zudem noch in regelmäßigen Abständen geändert werden.

[58] Ein typisches Beispiel ist die Benutzung von sequenziellen Zahlenfolgen (Passwort1, Passwort2, Passwort3 etc.) oder von Zeitangaben (PasswortDez, PasswortJan, PasswortFeb etc.).

Sensibilisierung der Benutzer hinsichtlich dieser Problematik, durch Hinweise auf die mit der Verwendung von schwachen Passwörtern verbundenen Gefahren und durch konsequente regelmäßige Passwortänderung kann die Sicherheit passwortbasierter Authentifikation deutlich erhöht werden (s. a. Abschnitt 3.3.2). Einige interessante Ansätze zur Erzeugung von sicheren und gleichzeitig leicht zu merkenden Passwörtern beschreibt z. B. Mark Burnett in seinem Buch „Perfect Passwords“ [Bur05].
Gleichzeitig beteuern einige Sicherheitsexperten, dass die Passwörter keine sichere Authentifizierung mehr ermöglichen. Die heutige Technik ist inzwischen so weit fortgeschritten, dass auch lange komplexe Passwörter mit einem vertretbaren Aufwand erraten werden können. So betont Bruce Schneier in seinem Blog: *„For anything that requires reasonable security, the era of passwords is over“* [Sch05b] und verlangt nach dem Einsatz von Mehrfaktor-Authentifizierungsverfahren. Einer dieser Authentifizierungsansätze besteht darin, für die Identifikation ein zusätzliches „Besitzmerkmal“ zu verwenden. Das können sowohl biometrische Merkmale[59] der Person als auch bestimmte Gegenstände sein, die sich im Besitz der Person befinden. Identifizierung allein aufgrund von biometrischen Merkmalen ist derzeit noch recht unsicher. Denn sobald ein Angreifer ein biometrisches Merkmal „stiehlt“,[60] kann dieses nicht mehr verwendet werden. Und schließlich ist die Anzahl der möglichen zu verwendenden biometrischen Merkmale nicht unendlich groß (vgl. [Sch04]). Wesentlich zuverlässiger ist die Kombination der beiden Ansätze: Man muss etwas besitzen und etwas wissen, um sich am System anmelden zu können. Für eine solche Form von Authentifizierung existieren mehrere Konzepte. Folgende Zwei-Wege-Authentifikationskonzepte und insbesondere deren Anwendbarkeit im Bereich der medizinischen Forschungsnetze werden im Abschnitt C.3.4 „Aspekte des Einsatzes von Zwei-Wege-Authentifizierungskonzepten“ untersucht:

- PIN-Code + Passwort auf SmartCard/Token (Abschnitt C.3.4.1),
- Biometrisches Merkmal + Passwort/Zertifikat auf SmartCard (Abschnitt C.3.4.2),
- PIN-Code + Zertifikat auf SmartCard/Token (Abschnitt C.3.4.3),
- PIN-Code + One-Time-Passwort am Token (Abschnitt C.3.4.4).

Die Ergebnisse dieser Analyse zeigen eine gute Eignung von PIN-Code-geschützten Zertifikaten auf SmartCards für die Authentifizierung von Forschungsnetzteilnehmern.

3.5.4. Rollenbasierte Rechtevergabe (RBAC)

Zugriffskontrolle erfüllt die Aufgabe der Überwachung des Zugriffs auf bestimmte Ressourcen mit dem Ziel, die Integrität, Vertraulichkeit und Verfügbarkeit von Informationen

[59] Fingerabdruck, Iris-Muster etc.

[60] Biometrische Systeme verwenden zur Authentifizierung die Hashwerte von bestimmten digitalisierten Körpermerkmalen. Unter der Voraussetzung, dass man die für die Hash-Errechnung verwendeten Verfahren kennt und über das passende Gerät zur Übermittlung der Daten an das authentifizierende System verfügt, kann man mit einem vertretbaren Aufwand die Identität einer anderen Person vortäuschen („stehlen“).

sicherzustellen. Ein Zugriffskontrollsystem übernimmt die Aufgaben der Zugriffskotrolle und entscheidet auf der Basis eines Regelwerks, ob der Zugang auf bestimmte Dienste und Ressourcen gewährt oder verwehrt wird. Für den Einsatz im Bereich der medizinischen Forschung muss ein Zugriffskontrollsystem mehrere Anforderungen erfüllen (vgl. [bsi11d, M 2.8, M 2.80]):

- Die Zugriffsentscheidungen dürfen nicht manipulierbar sein (Integrität der Zugriffsentscheidungen).
- Das System muss fehlertolerant sein. Bei Systemausfällen und -störungen muss das Zugriffskontrollsystem in geeigneter Weise reagieren, ohne die Funktionalität/Sicherheit der gesamten Infrastruktur zu gefährden.
- Das Zugriffskontrollsystem muss leicht wartbar sein, da die Änderungen der Zugriffsumgebung (z. B. bei Personaländerungen) eine schnelle/einfache Anpassung erfordern.
- Um die Unterschiede der Forschungsnetzteilnehmer in Bezug auf die Sicherheit der Verbindung bzw. der Arbeitsumgebung zu berücksichtigen, muss das Zugriffskontrollsystem eine Parametrisierung der Zugriffe unterstützen.
- Das System muss eine ausführliche Protokollierung ermöglichen, da im Forschungsnetz mit vertraulichen Patientendaten gearbeitet wird.
- Insbesondere im Behandlungszusammenhang muss das System eine hohe Verfügbarkeit aufweisen, damit kontrollierte Zugriffe stattfinden können.[61]

Jedes Zugriffskontrollsystem basiert auf einem Zugriffskonzept, dessen primäres Ziel in der Überprüfung der Zulässigkeit von Datenzugriffen besteht. Eine ausführliche Auflistung und Bewertung der möglichen Zugriffskonzepte würde den Rahmen dieses Abschnitts sprengen, sodass an dieser Stelle auf die weiterführende Literatur verwiesen wird.[62] IT-Sicherheitsexperten sind sich darüber einig, dass die Berechtigungen einer Person von den durch diese Person zu verrichtenden Tätigkeiten bestimmt werden sollen, wobei manche Autoren zusätzlich zwischen den Organisations- und Rollenmodellen unterscheiden. Die Unterscheidung wird dadurch begründet, dass im Organisationsmodell der Organisations-

[61] In [Ser01] wird zwischen drei Verfügbarkeitsstufen unterschieden. Danach müssen höchstverfügbare Systeme innerhalb von wenigen Sekunden auf eine Anfrage reagieren, die Wartezeit bei einem hochverfügbaren System darf maximal einige Minuten betragen, geringe Verfügbarkeit bedeutet, dass ein System auch für längere Zeit ausfallen darf. Als Beispiel für ein System mit geringer Verfügbarkeit wird das Rollenvergabemodul als Bestandteil des Zugriffkontrollsystems genannt. Da dieses Modul für die Vergabe und Zurücknahme von Berechtigungen zuständig ist, liegt es nahe, seine Verfügbarkeitseinstufung als „hoch“ zu deklarieren. In Fällen des Datenmissbrauchs oder bei Verletzung der Sicherheitsleitlinie müssen den betroffenen Accounts ihre Zugriffsprivilegien schnell wieder entzogen werden können. Im Forschungskontext kann eine sogenannte Rückfallposition definiert werden: Beispielsweise wird dem nicht administrativen Personal beim Ausfall des Moduls oder dessen Fehlfunktion der Zugriff auf Daten verweigert. Im Behandlungskontext wäre diese Lösung inakzeptabel, da das Leben und die Gesundheit eines Patienten höhere Priorität als die Geheimhaltung der Patientendaten vor dem Krankenhauspersonal haben würden.

[62] Umfassende Beschreibungen der Sicherheitsmodelle sind beispielsweise in [Eck07], [Mos02] und [Sch99] zu finden.

aufbau mithilfe von Benutzergruppen abgebildet wird; beim rollenbasierten Modell stehen die ausgeführten Aufgaben im Vordergrund (vgl. [PE06]). In der Praxis wird man eine Mischform der beiden Modelle vorfinden, wobei der Schwerpunkt im Folgenden auf den rollenbasierten Zugriffskonzepten liegen wird, zumal wissenschaftliche Untersuchungen die grundsätzliche Eignung rollenbasierter Zugriffskonzepte für den Einsatz im medizinischen Bereich beweisen (vgl. [PBB+96]). Für die bessere Eignung dieses Zugriffsmodell spricht auch die Tatsache, dass externe Forschungsnetzteilnehmer nicht zu der Organisation des Forschungsnetzes im engeren Sinne gehören.

Das Verfahren zur Vergabe von rollenbasierten Berechtigungen in Mehrbenutzersystemen oder Rechnernetzen wird auch als „Role Based Access Control“ (RBAC) bezeichnet (vgl. [ans04], [FSG+01]). RBAC entstand aus Forschungsprojekten des US-Verteidigungsministeriums (Department of Defense) mit dem Ziel, ein Verfahren zur Zugriffseinschränkung auf vertrauliche Informationen zu entwerfen. Die damals entwickelten Methoden der Zugriffskontrolle: Discretionary Access Control (DAC) und Mandatory Access Control (MAC) erwiesen eine viel zu hohe Komplexität bei der Konzeptumsetzung.[63] RBAC als Weiterentwicklung der Konzepte stellt eine alternative Technik dar. Bei RBAC erfolgt die Einteilung der Benutzer in Gruppen, wobei ein Benutzer (Person) seinerseits mehreren Gruppen angehören kann. Je nach Gruppenzugehörigkeit werden ihm dann die Zugriffsrechte auf Ressourcen erteilt oder verwehrt. Eine Gruppe trägt bei RBAC die Bezeichnung „Role“ (Rolle) und impliziert in der Regel die auszuführende(n) Aufgabe(n) (z. B. Manager, Administrator, Arzt etc.). Durch die Aufteilung in Benutzer und Rollen ist es möglich, Zugriffsrechte auf Gruppenebene (für mehrere Benutzer gleichzeitig) zu vergeben oder zu ändern, was die Administration von Benutzerberechtigungen deutlich erleichtert (vgl. [San96], [SCFY96], [FK92]).

Um zu vermeiden, dass ein Benutzer mehr Berechtigungen erhält, als er für die Ausführung seiner Aufgabe benötigt, muss seine Tätigkeit vor der (rollenbasierten) Berechtigungsvergabe genau beschrieben werden. Ein Benutzer erhält dabei nur die für die Ausführung seiner Tätigkeit notwendigen Privilegien (Minimalanforderung), deren Bestimmung nicht immer trivial ist. Oft finden die dieselben Zugriffsrechte in mehreren Rollen wieder; daher bedient man sich der Hierarchien zwecks Vermeidung der Redundanzen in Rollendefinitionen. So kann die Rolle eines behandelnden Arztes sämtliche Berechtigungen an einer Patientenakte beinhalten, die auch ein nicht behandelnder Arzt an der Akte besitzt.

---

[63] DAC basiert auf der Vergabe von Zugriffsberechtigungen auf Daten, die als Eigentum von Benutzern angesehen werden, was im Falle von Organisationen (und auch im Forschungsnetz) meistens nicht zutrifft. Die MAC-basierten Zugriffsberechtigungen werden auf Basis der Datenvertraulichkeitseinstufung und der Berechtigung eines Subjektes, auf die Daten bestimmter Vertraulichkeitsstufe zuzugreifen, vergeben. [FK95]: *„(...). A means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i.e. clearance) of subjects to access information of such sensitivity. (...)“*. Obwohl DAC und MAC in einigen Zugriffsmodellen wieder zu finden sind, sind sie für die Abbildung von komplexen Berechtigungsmodellen in der Wirklichkeit nur bedingt geeignet. Der Abgleich der Zugriffsrechte eines Individuums mit der Vertraulichkeitsstufe des entsprechenden Dokuments ist in der realen Welt nicht praktikabel (vgl. [FK92]).

Eine Rolle kann parametrisiert werden: Zugriffsberechtigungen können aufgrund von Parametern bestimmt werden. Dies ist z. B. bei der Definition der Rolle „behandelnder Arzt“ der Fall. Ein behandelnder Arzt unterscheidet sich von einem nicht behandelnden Arzt lediglich durch den Behandlungszusammenhang-Parameter in Bezug auf einen Patienten. Formal wird die Zugriffskontrolle (ZK) als eine Relation zwischen den Benutzern und den Zugriffsberechtigungen definiert: $ZK \subseteq Benutzer \times Zugriffsberechtigungen$. Ein Benutzer b erhält Zugriffsberechtigung z nur dann, wenn $(b, z) \in ZK$. RBAC teilt diese Relation in Benutzer- (BZ) und Berechtigungszuweisung (RZ) auf:
$BZ \subseteq Benutzer \times Rollen, RZ \subseteq Rollen \times Zugriffsberechtigungen; ZK := BZ \circ RZ$.
Somit kann die Zugriffskontrolle auch definiert werden als:
$\exists rolle \in Rollen : (b, rolle) \in ZK \wedge (rolle, z) \in RZ$.
Diese Basisdefinition von RBAC berücksichtigt allerdings keine dynamischen Zugriffseinschränkungen[64] und eignet sich somit weniger gut für die Abbildung der Zugriffskontrollstrukturen für das Forschungsnetz. Aus diesem Grund wird für die Beschreibung der Zugriffsszenarien in dieser Arbeit eine erweiterte Definition der RBAC nach Torsten Lodderstedt [Lod03] verwendet, die in der Abbildung 6 dargestellt ist.

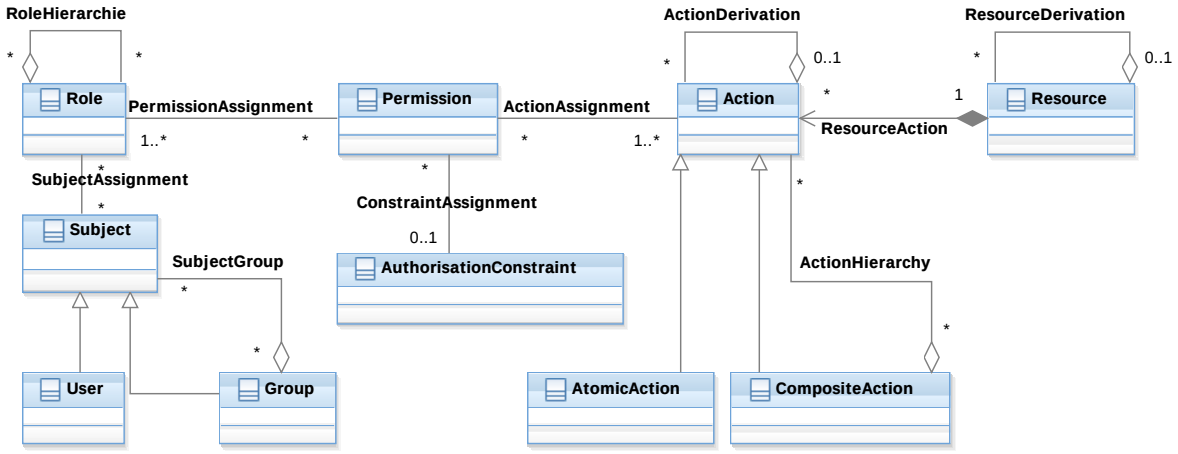

Abbildung 6.: Erweiterung des RBAC-Modells nach Torsten Lodderstedt [Lod03]: Die erweiterte RBAC-Definition erlaubt die Abbildung von solchen dynamischen Zugriffseinschränkungen wie Art der Verbindung, zeitliche Komponente etc. Dies erfolgt durch die Verwendung von sogenannten Constraints.

Nach der erweiterten RBAC-Definition in [Lod03] werden Benutzer, Prozesse und Benutzergruppen zum Basistyp „Subjekt“ zusammengefasst. Den Rollen werden Berechtigungen zugeordnet, wobei die Berechtigungen aus Aktionen auf Objekten bestehen. Die o. g. dynamischen Abhängigkeiten werden mithilfe von Constraints abgebildet. Constraints versehen die Berechtigungen mit Einschränkungen. So kann man beispielsweise die maximale Anzahl der erfolglosen Anmeldeversuche eines Forschungsnetzteilnehmers auf drei beschränken, um die Wörterbuch- oder Brute-Force-Angriffe vorzubeugen. Die Möglichkeiten für die Nutzung dieser erweiterten RBAC-Definition für die Berechtigungsvergabe für die Szenari-

[64] Standort des Systems, Art der Verbindung, zeitliche Komponente etc.

en in den medizinischen Forschungsnetzen werden im Abschnitt C.3.5 „Beschreibung eines RBAC-Konzeptes mithilfe von SecureUML“ erörtert.

Notwendigkeit für die Vervollständigung rollenbasierter Zugriffsberechtigungskonzepte durch administrative und organisatorische Vorkehrungen: Unsere Welt besteht aus Ausnahmen und ein Zugriffskonzept ist ein Beispiel dafür. In medizinischen Einrichtungen steht die Gesundheit bzw. das Leben der Patienten im Vordergrund – Situationen in denen man die beschriebenen Sicherheitsvorkehrungen umgehen können muss. In Notsituationen hat nicht die Informationssicherheit oder der Datenschutz die höchste Priorität, sondern die Erhaltung des menschlichen Lebens. Eine umfangreiche Protokollierung der Zugriffe soll Missbrauch des Notfallkonzeptes minimieren bzw. bei der späteren Untersuchung des Vorfalls unterstützen.
Die Schwachstelle eines jeden Zugriffsberechtigungskonzeptes besteht in der Tatsache, dass es auf einem Modell[65] basiert. Schwer zu quantifizierende Elemente wie beispielsweise zwischenmenschliche Beziehungen können i. d. R. nicht berücksichtigt werden. So kann eine unbefugte Kooperation zwischen den Forschungsnetzteilnehmern durch das rollenbasierte Konzept kaum vermieden werden. Die in den Abschnitten 3.3 und 3.4 beschriebenen organisatorischen und administrativen Maßnahmen vervollständigen die rollenbasierten Berechtigungskonzepte und können beispielsweise die Umgehung der bei der Vergabe der Zugriffsberechtigungen einzuhaltenden Vier-Augen-Prinzips verhindern.

3.5.5. Zugangsszenarien von Netzteilnehmern zu den Forschungsnetzdiensten

Für den Zugriff von Nutzern auf das Forschungsnetz gelten diverse Einschränkungen, die das Risiko des Datenmissbrauchs minimieren. So werden einem Forscher nicht beliebige Daten zur Verfügung gestellt, sondern nur krankheitsspezifische, klar definierte für sein Forschungsvorhaben relevante Inhalte. Ein restriktives Zugriffsberechtigungskonzept, die Zweiteilung der Daten in *IDAT* und *MDAT*, technische Sicherheit der Datenbankserver, ausgefeilte Anonymisierungs- und Pseudonymisierungsverfahren und viele weitere Maßnahmen sorgen für ein geringes Reidentifizierungspotenzial (vgl. [RDSP06]). Trotz der erwähnten Sicherheitsmaßnahmen ist es nicht empfehlenswert, die Forschungsdatenbank zu veröffentlichen bzw. jedem Interessenten Zugriff auf diese Datenbank pauschal zu gewähren. Einer der Gründe, die gegen die pauschale Datenfreigabe sprechen, ist die bedingte Anonymisierbarkeit von Patientendaten bzw. die Relativität des Personenbezugs der Daten (vgl. [RHJ08, S. 27 ff.]). Insbesondere lässt sich der Personenbezug bei biologischen Proben und den daraus gewonnenen Daten nur schwer bis gar nicht eliminieren

[65] Das Modell ist ein Abbild, das nicht alle Details der realen Welt erfasst (s. a. Begriffsdefinition im Glossar).

(vgl. [Pom11a]). Die Reidentifizierung von Patientendaten aufgrund von Alleinstellungsmerkmalen ist ebenfalls möglich.[66] Außerdem können Fehler im Anonymisierungs- bzw. Pseudonymisierungsverfahren entdeckt werden, die eine vereinfachte Reidentifizierung ermöglichen. Diese Risikofaktoren in Verbindung mit einer stetig wachsenden Anzahl von Personendatensätze enthaltenden (Referenz-)Datenbanken machen die Freischaltung der Forschungsdatenbank nur für einen auserwählten vertrauenswürdigen Benutzerkreis notwendig (vgl. [Pom10a], [Kre06]). Mit einer ähnlichen Aufgabenstellung wird ein Unternehmen bei der Anbindung von Außendienstmitarbeitern oder der Einrichtung von Home-Arbeitsplätzen konfrontiert – also dann, wenn ein Gerät des Unternehmens die sichere LAN-Umgebung verlässt (vgl. [AE08], [RDSP06], [SPR+06]).

Das Rezept für die Sicherung eines kleineren Unternehmensnetzes ist relativ einfach: Man ermittle die Grenzen eines Netzwerkes sowie dessen Anbindungspunkte an die Außenwelt und sichere diese mithilfe des Firewallings und des Routings ab. Eventuell erhalten die Systeme innerhalb des Netzes zusätzliche Immunisierung in Form von Antivirensoftware, Personal Firewalls, Sicherheitspatches und werden regelmäßig mithilfe von Compliance-Software auf die Einhaltung von Sicherheitsstandards untersucht. Für ein größeres Unternehmen ist diese Aufgabe nicht mehr so einfach zu lösen: Das Unternehmensnetz besteht in der Regel aus mehreren räumlich verteilten Segmenten. In der Unternehmenswelt neigt man dazu, diese Segmente über dedizierte Leitungen miteinander zu verknüpfen und die Teilnehmersysteme an bestimmte Standards zu binden. Man spricht auch von einer harten Schale, die solche Einrichtungen um ein Netz bilden. Das Innere eines Netzes bleibt dagegen leicht angreifbar. Eine Malware, die die sichere äußere Schutzschicht überwindet, kann innerhalb der meist homogenen Struktur immense Schäden anrichten, da die Systeme weitestgehend gleiche Konfiguration aufweisen[67] und was noch wichtiger ist, nach dem Prinzip des gegenseitigen Vertrauens funktionieren. Aus diesem Grund wird der „Defense in Depth"-Ansatz zunehmend populär. Dieser Ansatz sieht vor, dass Infrastrukturbestandteile durch diverse Maßnahmen (Personal Firewalls, HIDS, Weiterleitung von sicherheitsrelevanten Informationen an auswertende Systeme etc.) gegen Angriffe immunisiert werden. Dies führt dazu, dass ein Angriff auch dann erkannt und gestoppt werden kann, wenn die äußere Verteidigungslinie versagt.[68]

Ein Firmennetz ist i. d. R. so aufgebaut, dass jeder Mitarbeiter Zugang zu fast allen Informationen hat. Nur die wenigen kritischen Bereiche, wie Gehaltslisten, Business-Continuity-Pläne, Finanzbereich etc. bleiben dem größten Teil der Belegschaft vorenthalten. In der Versicherungsbranche ist es beispielsweise üblich, komplette Kunden- und Maklerkarteien

[66] Die *MDAT* enthält nicht nur Befunde und Diagnosen, sondern auch die sogenannten soziodemografischen Daten (u. a. Alter, Bildung, Lifestylefaktoren, Umweltdaten) und sonstige Begleitdaten (Archivierungsort, Daten des behandelnden Arztes etc.), die die unerwünschte Reidentifizierung ermöglichen bzw. vereinfachen könnten (s. a. Glossar).

[67] Und folglich gegenüber gleichen Angriffen anfällig sind.

[68] So kann z. B. die Kompromittierung eines Systems von einem Anti-Rootkit erkannt werden, obwohl das Antivirenprogramm die Malware nicht bemerkt.

pauschal für alle Mitarbeiter freizugeben, da viele Geschäftsprozesse auf der Verfügbarkeit dieser Informationen aufbauen.
Ein Forschungsnetz ist mit einem üblichen Unternehmensnetzwerk kaum vergleichbar. Streng genommen existiert überhaupt kein dediziertes klar abgegrenztes Netz.[69] Die Teilnehmer des Forschungsnetzes gehören unterschiedlichen Organisationen an und können unterschiedliche Ziele verfolgen. Die grundsätzliche Freigabe aller Ressourcen und die Sperrung lediglich kritischer Bereiche (nach dem Vorbild eines üblichen Unternehmensnetzes) sind auf ein Forschungsnetz nicht anwendbar. Aus diesem Grund kann die Freigabe von Ressourcen in einem medizinischen Forschungsnetz nur nach dem „Need-to-know-Prinzip“ erfolgen.
Anders als bei einem Unternehmensnetz, in welchem es durch organisatorische und administrative Maßnahmen möglich ist, die Infrastruktur einheitlich zu halten, ist es bei allen Teilnehmern des Forschungsnetzes nicht realistisch, von einer sicheren Umgebung auszugehen. Die Hard- und Softwareausstattung der Teilnehmer ist unterschiedlich. Restriktive Maßnahmen, die auf die Homogenisierung der Systemlandschaft abzielen, würden lediglich zu einer verringerten Teilnehmerakzeptanz führen. Heterogene Umgebung erlaubt keine Sicherheitskonzepte, die auf der Integrität teilnehmender Systeme aufbauen: Ein versierter Angreifer mit einem physikalischen Zugang zu einem solchen System wäre trotzdem in der Lage, es zu manipulieren, um beispielsweise Patienten- oder Arztdaten auszuspähen (s. a. Abschnitt 3.5.1).
Es wäre somit nicht ratsam, dem Client eine Menge von Daten zur Verfügung zu stellen und zu hoffen, dass die lokal auf dem Teilnehmersystem installierte Software die Filterungsfunktion zuverlässig ausführt und dem Teilnehmer – basierend auf dem Zugriffsberechtigungskonzept – nur die Daten liefert, in die er Einsicht nehmen darf. Auf der Client-Seite dürfen nur die Daten ankommen, deren Zulässigkeit für den Benutzer in der sicheren Serverumgebung überprüft ist.[70] Eine webbasierte Lösung ist für ein solches Einsatzszenario prädestiniert. Doch auch eine webbasierte Lösung befreit nicht von der Notwendigkeit, die Authentizität der Teilnehmer und die Integrität der verwendeten Client-Software zu überprüfen. Die Zurverfügungstellung von Forschungsnetzdiensten in Form des für alle Internetteilnehmer verfügbaren Webangebots wird nicht empfohlen. Es wurde bereits erläutert, wieso keine pauschale Annahme der absoluten Anonymität von medizinischen Daten erfolgen kann, sodass man sich nicht nur auf die Anonymisierungs- bzw. Pseudonymisierungsmaßnahmen verlassen darf. Im Abschnitt 3.5.1 „Sichere Arbeitsumgebung“ wird die Verwendung einer virtualisierten Arbeitsumgebung vorgeschlagen. Beim Zugriff auf die webbasierten Forschungsnetzdienste werden Daten zwischen der in der

[69] Abgesehen von einem relativ kleinen Administrationskern bzw. zentralen Diensten (s. a. Abschnitte 3.1 und 3.2).

[70] Desktop-Datenbanken, die zuerst die Tabelleninhalte in den Speicher laden und erst nachträglich die relevanten Einträge ausfiltern, wären in diesem Zusammenhang nicht empfehlenswert.

virtualisierten Umgebung laufenden Anwendung[71] und dem Forschungsnetzserver ausgetauscht. Da die Datenübertragung i. d. R. über ein öffentliches Netz stattfindet, muss diese verschlüsselt werden. Im Abschnitt C.3.2 werden einige Anbindungsmöglichkeiten für die externen Forschungsnetzteilnehmer auf ihre Praxistauglichkeit untersucht. Dabei werden Aspekte des Einsatzes von virtuellen privaten Netzen (VPN) und standleitungsbasierten Anbindungen betrachtet; auch die Möglichkeiten der Verwendung von PKI sowie die gängigen Standards und ihre Alternativen werden erörtert. Für die Authentifizierung der Benutzer können die im nächsten Abschnitt behandelten X.509v3-Zertifikate verwendet werden. Die Identität eines Forschungsnetzteilnehmers kann dabei an ein Schlüsselpaar gebunden und durch eine CA beglaubigt werden. Die Authentifizierung von Forschungsnetzteilnehmern wird im Abschnitt 3.5.3 erörtert.

3.5.6. Verzeichnisdienste (LDAP, OCSP)

Aufgrund der i. d. R. weiten räumlichen Verteilung der Forschungsnetzteilnehmer bzw. -systeme ist der manuelle Austausch von öffentlichen Schlüsseln zwischen den Teilnehmern (sogenannte manuelle Public-Key-Verteilung) nicht praktikabel. Um die Zugehörigkeit eines öffentlichen Schlüssels zu einer Person festzustellen, verwendet man digitale Zertifikate, denn ein digitales Zertifikat bindet einen öffentlichen Schlüssel an den Schlüsselinhaber. Dafür unterzeichnet eine anerkannte Beglaubigungsinstanz (Certification Authority (CA)) eine aus den identifizierenden Informationen des Schlüsselinhabers und dem öffentlichen Schlüssel bestehende Nachricht. Es existieren mehrere Zertifikatformate; am verbreitetsten ist X.509v3 (vgl. [HPFS02]). Ausführliche Informationen zum Aufbau des X.509v3-Zertifikats befinden sich in [BP01]. X.509v3-Zertifikate sind flexibel bezüglich der Namensformate und ermöglichen Identifizierung des Zertifikatsinhabers anhand von E-Mail-Adresse, Domainnamen, X.500-Verzeichnisnamen, IP-Adresse etc. Mehrere Parteien sind in eine PKI-Infrastruktur involviert:

- Die *Certification Authority (CA)* (Zertifizierungsstelle) ist für die Authentizität der Teilnehmer verantwortlich. CA überprüft die Identität der Teilnehmer, vergibt, verwaltet und widerruft die Zertifikate. Dafür verteilt eine CA ihren eigenen öffentlichen Schlüssel in Form eines Zertifikats. Das Zertifikat wird entweder von einer anderen CA oder von der CA selbst unterschrieben. In solchen Fällen spricht man von sogenannten self-signed Zertifikaten. Man unterscheidet zwischen zwei Formen von CAs: öffentliche und private. Öffentliche CAs bedienen einen breiten Benutzerkreis; die privaten betreuen nur die Benutzer der eigenen Gemeinschaft. Eine CA umfasst nicht nur die Dienste, sondern auch Hard- und Softwarekomponenten sowie Personal, operative Prozeduren und Richtlinien.
- Die *Registration Authority (RA)* übernimmt die verwaltungstechnischen Aufgaben einer CA. RAs werden eingerichtet, um die administrative Last einer CA zu überneh-

[71] Zum Beispiel Webbrowser.

men. So nehmen die RAs Registrierungsinformationen von Neuanmeldungen entgegen, generieren Schlüssel für Benutzer, verwalten und autorisieren Zertifikatswiderrufe und organisieren Verteilung und Zurücknahme von SmartCards. Außerdem erfüllen die RAs durch die Übernahme der CA-Aufgaben eine Schutzfunktion, da sie lokal betrieben werden, und die CA dafür in einer besonders sicheren Offline-Umgebung arbeiten kann.

- Der *Zertifizierungsserver* ist für die Herausgabe der Zertifikate zuständig. Der Zertifizierungsserver kombiniert den öffentlichen Schlüssel des Teilnehmers mit seinen identifizierenden Informationen und signiert die dadurch entstehende Zertifikatsstruktur mit dem privaten CA-Schlüssel.

- Das *Zertifikatsverzeichnis* ist eine zentrale Zertifikatverwaltungs- und -verteilungsstelle. Verzeichnisse werden i. d. R. eingesetzt, um persönliche Attributsinformationen samt Zertifikaten zu speichern. Dadurch werden Benutzerinformationen in eine übersichtliche Form gebracht. Clients können auf die Zertifikatsverzeichnis-Inhalte mithilfe von Verzeichnisprotokollen (z. B. X.500 oder LDAP) zugreifen.

- Der *Schlüsselwiedergewinnungsserver bzw. Schlüsselsicherungs- und -wiederherstellungsserver* sichert die Schlüssel bei der Erzeugung und hilft später, die verlorenen Schlüssel wiederherzustellen. Der Schlüsselwiedergewinnungsserver ist notwendig angesichts der großen Teilnehmerzahl eines Forschungsnetzes und dem Bedürfnis, auf die Daten trotz des Verlusts der SmartCard oder der PIN zugreifen zu können. Schlüssel-Wiedergewinnung ähnelt der Schlüssel-Hinterlegung bei einem Treuhänder. Der maßgebliche Unterschied besteht darin, dass die Schlüsselwiedergewinnung intern erfolgt und bei der Schlüsselhinterlegung eine dritte Partei den Schlüssel zur Aufbewahrung erhält.

- Die *Verwaltungsprotokolle* (z. B. Certificate Management Protocol (CMP)) werden für die PKI-interne Kommunikation eingesetzt. Sie unterstützen Registrierung von Benutzern, helfen bei der Zertifizierung und Initialisierung. Die Verwaltungsprotokolle werden bei der Schlüsselwiedergewinnung, -aktualisierung und -widerruf verwendet und unterstützen die Kreuzzertifizierung.

- Die *operationalen Protokolle* (z. B. HTTP, FTP, LDAP etc.) dienen der Zertifikatverteilung und dem Austausch von Informationen über den Widerrufstatus (vgl. [BP01]).

- Der *Zeitserver* ermöglicht die Erstellung und Überprüfung eines Zeitstempels. Ein Zeitstempel wird bei der Erzeugung signiert, was die Überprüfung der Zeitquelle erlaubt. Die dadurch entstehende zuverlässige Zeitangabe ist notwendig für Revisionsprotokolle, Eingangsbestätigungssysteme, Workflow- und Dokumentmana-

gementsysteme. Aspekte des Einsatzes von Zeitstempeldiensten in medizinischen Forschungsnetzen werden im Abschnitt C.3.12 untersucht und erörtert.

Folgende Aspekte des Einsatzes von Verzeichnisdiensten in den medizinischen Forschungsnetzen werden im Abschnitt C.3.6 untersucht:

- Benutzerregistrierung bei einer Zertifizierungsstelle,
- Widerruf von Zertifikaten,
- Verwendung von Zertifikaten für die Authentifizierung und Autorisierung,
- PKI-Vertrauensmodelle,
- gemeinsame Benutzung von Verzeichnisdiensten von mehreren Forschungsnetzen.

3.5.7. Ticketing, Single Sign-On (SSO)

Ein medizinisches Forschungsnetz bietet seinen Teilnehmern Dienste an, die durch eine Vielzahl von Anwendungen repräsentiert werden und folglich eigene unterschiedliche Authentifizierungsfunktionen anbieten können. Meistens hat ein Benutzer mehrere Chipkarten, Benutzerkennungen und Passwörter, wobei die Bildungsregeln und Änderungsintervalle für Passwörter unterschiedlich ausfallen können. Dies hat zwei Folgen: Häufige Anrufe beim Helpdesk wegen gesperrter Benutzerkennungen und ein insgesamt negativer Einfluss auf die Infrastruktursicherheit, weil die Benutzer eine ihrer Sicherheitskarten/Tokens verlieren, gleiche leicht zu erratende Passwörter für mehrere Applikationen (auch privat) verwenden oder ihre Passwörter/PINs an leicht zugänglichen Stellen aufbewahren (z. B. Beschriftung der SmartCard-Rückseite mit der PIN. S. a. Abschnitt 3.5.3 „Authentifizierung von Forschungsnetzteilnehmern“).
Als Single Sign-On (SSO) bezeichnet man eine Technologie, die lediglich eine einmalige Anmeldung notwendig macht. Die im Abschnitt 3.5.3 „Authentifizierung von Forschungsnetzteilnehmern“ unterbreitete Empfehlung sieht eine Zwei-Faktor-Authentifikation mithilfe einer SmartCard und einer PIN-Nummer bzw. eines Passworts vor. In Verbindung mit SSO würde das bedeuten, dass ein Forschungsnetzteilnehmer nur diese beiden Faktoren benötigt, um alle für ihn verfügbaren Dienste benutzen zu können. Diese Erleichterung erkauft man allerdings durch ein Vertrauen in das SSO-System, dessen Verfügbarkeit und Vertraulichkeit die aller anderen Systeme des Forschungsnetzes übersteigen muss.
Nach der Vorstellung einer Taxonomie von Single Sign-On-Ansätzen werden im Abschnitt C.3.7 „Aspekte des Einsatzes von Single Sign-On in medizinischen Forschungsnetzen“ die Anforderungen an den Einsatz dieser Technologie in der medizinischen Forschung untersucht. Nach einer Analyse der Ticketing-Verfahren schließt der Abschnitt mit einer Übersicht der SSO-Technologie.
Die Frage, ob der Einsatz eines Single Sign-On-Systems einen positiven oder einen eher negativen Einfluss auf die Sicherheit eines medizinischen Forschungsnetzes mit sich bringt, kann nicht pauschal beantwortet werden. Die Annahme, dass die Eingabe von unterschiedlichen Passwörtern für unterschiedliche Systeme die Sicherheit einer Infrastruktur erhöht

und informationelle Gewaltenteilung fördert, ist nicht unbegründet. Gelingt es einem Angreifer, die Zugangsdaten für eine Anwendung auszuspähen, hat er bei mehreren unterschiedlichen Anmeldungen keinen Zugriff auf das nächste System. Beim Single Sign-On existieren solche Barrieren nicht. Diese Überlegung funktioniert recht gut in der Theorie, hat jedoch in der Praxis eine eingeschränkte Gültigkeit: Die pauschale Annahme eines Benutzers, der sichere ungleiche Passwörter für unterschiedliche Systeme verwendet, diese nicht in seinem Terminkalender aufschreibt und nicht weitergibt, ist wirklichkeitsfremd. Applikationen laufen auf mehreren – oft miteinander inkompatiblen – Plattformen, unterschiedliche Protokolle und Authentifikationsverfahren werden eingesetzt. Benutzer haben Dutzende in unterschiedlichen Zeitintervallen zu ändernde Passwörter. Häufig kann der Angreifer durch das Ausspähen eines Logins weitere Zugangsdaten erspähen, indem er beispielsweise auf einem kompromittierten Client-System einen Keylogger installiert und die Benutzereingaben mitloggt.

Die Kompromittierung eines Systems kann also Kompromittierung weiterer Systeme nach sich ziehen, auch wenn man unterschiedliche Logins verwendet. Auch beim Ausspähen eines der Logins kann somit die aufwendige Änderung aller anderen Zugangsdaten des Benutzers notwendig sein, die zusätzlich mit der Gefahr verbunden ist, einen der Logins zu übersehen. Beim Single Sign-On reicht dagegen die einfacher zu kontrollierende Änderung einer einzelnen Anmeldung.

Auch wenn die Standards strikt befolgt werden, ist deren natürliche „Alterung“ unumgänglich. Die heute noch aktuellen Technologien werden in einem Jahrzehnt durch neue abgelöst; eine sture Befolgung veralteter Standards ist in der schnelllebigen IT-Welt wenig sinnvoll. Ein Forschungsnetz ist in dieser Beziehung keine Ausnahme, da es auf Systemen der Betreiber, den vorhandenen Sicherheitsmodulen und den Applikationen aufbaut, die z. T. bereits seit Jahrzehnten bestehen. Gleichzeitig ist es unrealistisch anzunehmen, dass die alten Applikationen ausnahmslos auf die neue Technologie migriert werden können, sodass eine Infrastruktur bei der Hinzuziehung des zeitlichen Faktors zwangsläufig inhomogen ist. Es wird unmöglich sein, einen gleich hohen Sicherheitsstandard für eine Vielzahl von Applikationen aufrechtzuerhalten. Ein zu den Sicherheitsrichtlinien des Forschungsnetzes konformes SSO-System kann somit das Sicherheitsniveau erhöhen. Die Überwindung eines sicheren auf der Mehrfaktorauthentifizierung basierenden SSO-Systems (s. a. Abschnitt 3.5.3 „Authentifizierung von Forschungsnetzteilnehmern“) gestaltet sich für den Angreifer wesentlich aufwendiger als die Kompromittierung mehrerer Systeme mit schwächerer Benutzerauthentifizierung.

Die Einführung eines SSO-Systems erleichtert die Einhaltung eines gemeinsamen Sicherheitsstandards, verringert die Anzahl der vom Benutzer durchzuführenden Anmeldungen und entlastet das Administrationspersonal.[72] Außerdem erleichtert ein Single Sign-On-

[72]Passwortänderungen und Reaktivierung von Accounts, die aufgrund von falsch eingegebenen Passwörtern gesperrt wurden, bilden mehr als fünf Prozent aller Helpdesk-Anfragen (vgl. [TK03]).

System die Durchsetzung und die Überwachung der im Abschnitt 3.5.4 „Rollenbasierte Rechtevergabe (RBAC)“ beschriebenen rollenbasierten Zugriffskonzepte.

3.5.8. Datenbanksicherheit

In mehreren für die Forschungsnetze entwickelten Datenschutz- und Datensicherheitskonzepten beschränkt man sich beim Thema der Datenbanksicherheit auf die Einsatzempfehlung für die Datenbanksysteme. Beispielsweise [RDSP06, S. 40]: *„Es dürfen ausschließlich Industrie-Standard-Datenbanken ... zum Einsatz kommen, deren Eindring-Sicherheit in das System durch einen technischen Angriff Unberechtigter ‚von außen‘ sehr hoch ist.“* Dabei werden die wichtigsten Daten des Forschungsnetzes in den Datenbanken gespeichert; die Datenbanken gehören daher zu den schutzwürdigsten Bestandteilen des Forschungsnetzes und die Sicherheitsmaßnahmen für die Datenbanken demzufolge zu den wichtigsten Komponenten der Sicherheitsarchitektur. Es ist daher empfehlenswert, den technischen Aspekten der Datenbanksicherheit eine größere Beachtung zu schenken. Wesentliche Aspekte der Datenbanksicherheit für den Forschungsnetzeinsatz werden im Abschnitt C.3.9 „Aspekte der Datenbanksicherheit“ untersucht und erörtert.
Insgesamt muss festgehalten werden, dass die Datenbanksicherheit kein triviales Thema ist, denn der Sicherheitsstand eines Systems ändert sich häufig[73] und ist von der Systemkonfiguration abhängig. Die im Abschnitt C.3.9 unterbreiteten Konfigurationsempfehlungen sollen daher nicht als endgültig angesehen werden. Vielmehr ist es empfehlenswert, unmittelbar kurz vor der Systemimplementierung die Entscheidung für eine Systemkonfiguration zu treffen, wobei solche Faktoren wie Know-how der Mitarbeiter, finanzielle Situation des (kommerziellen) Softwareanbieters, Presseberichte etc. in die Entscheidung einfließen sollen. Als der o. g. Abschnitt verfasst wurde, erschien beispielsweise der Einsatz von OpenBSD in Verbindung mit PostgreSQL-, Firebird- oder Ingres®-DBMS als empfehlenswert.

3.5.9. Antimalware-Einrichtungen

Viele Angriffe werden erst aufgrund des menschlichen Versagens bzw. durch Konfigurationsfehler möglich. Bei einer Integration mehrerer – möglicherweise inhomogener – Infrastrukturen zu einem Forschungsnetz ist die Erreichung eines gewissen Komplexitätsgrades bei der Administration unumgänglich. Derzeit versucht die Industrie die Komplexität der Konfigurationen durch die Integration von Sicherheitsmechanismen und Verzeichnisdienstkomponenten für Benutzer- und Rechteverwaltung zu reduzieren. Diese Entwicklung ist auch als Unified Threat Management (UTM) bzw. Identity- and Access-Management (IAM)[74]

[73] Zum Beispiel durch das Bekanntwerden von Exploits, Einbringung von neuen Releases, Patch-Managementpolitik etc.

[74] Diverse IAM-Lösungen werden derzeit von einer Reihe von Herstellern angeboten: Siemens Communications, CA, Evidian, IBM, BMC, Novell, HP etc.

bekannt und besteht aus mehreren Modulen für die zentrale Benutzeradministration, das Rechte- und Rollenmanagement, SmartCards, SSO etc. Eine UTM-Lösung vereint mehrere Sicherheitskomponenten (Antivirenscanner, Firewall, E-Mail- und Content-Filter, VPN, IDS etc.) unter einer einheitlichen Oberfläche, was Konfigurations- und Bedienungsrisiken erheblich reduziert. Außerdem erspart IAM kostspielige und fehleranfällige Mehrfacherfassung in vielen Einzelsystemen (vgl. [Sti05]). Die Speicherung aller Benutzerzugriffsrechte innerhalb des IAM-Systems steht zum Teil im Widerspruch zu den in [RDSP06] unterbreiteten Empfehlungen. So wird in [RDSP06] eine direkte Ablage von Zugriffsberechtigungen der Ärzte in der Patientenliste empfohlen. In der vorliegenden Arbeit wird die Auffassung vertreten, dass die speziell für diesen Funktionsbereich optimierte IAM-Technologie für diese Aufgabe besser geeignet ist. Ein IAM-System ermöglicht eine saubere Aufgabentrennung zwischen den Arzt- und Patientendaten und den Berechtigungsinformationen.
In seinem Vortrag „Identity Life Cycle Management“ [Wie05] auf dem SIT-Sicherheitsforum 2005 stellte Hans Wieser die Behauptung auf, dass im Durchschnitt 40 Prozent der Nutzer mehr Rechte besäßen, als sie eigentlich brauchen würden, und verwies in diesem Zusammenhang auf das wohl bekannte Azubi-Phänomen.[75] Im „Information Risk in the Professional Services“-Report [SST+07] wird sogar von 50 bis 90 Prozent der Mitarbeiter berichtet, die den Zugriff auf Ressourcen besitzen, die sie nicht mehr für die Ausübung ihrer neuen Funktion im Unternehmen benötigen; die alten Zugriffsberechtigungen wurden bei Änderung der Funktion nicht entzogen. Ein integriertes IAM-System kann helfen, den Überblick über die Berechtigungen der Benutzer auch beim häufigen Rollenwechsel zu behalten (vgl. [DBN10]).
Ein weiteres bekanntes Problem bilden die nur temporär gültigen Zugriffsrechte. Besonders deutlich wird die Problematik bei Vertretungsregelungen. Die meisten Organisationen umgehen die Vertretungsproblematik durch die Mehrfachbesetzung für bestimmte Aufgaben: Mehrere Mitarbeiter haben gleiche Zugriffsrechte, obwohl eine Aufgabe meistens von einer einzigen Person ausgeführt wird, und die anderen für diese Person nur in Ausnahmefällen[76] einspringen. Ein IAM-System bietet die Möglichkeit, zeitlich begrenzte Berechtigungen an die Teilnehmer des Forschungsnetzes zu vergeben. Dies ist z. B. im Rahmen der Vertretungsregelung wichtig und entspricht dem „Need-to-know-Prinzip“.[77] Ein IAM-System als ein wichtiger Bestandteil der technischen Sicherheitsarchitektur eines medizinischen Forschungsnetzes kann die konsequente Schließung der Einstiegslöcher für einen Angreifer unterstützen.

[75] Im Laufe der Ausbildung durchläuft ein Auszubildender mehrere Abteilungen des Unternehmens, wobei seine alten Berechtigungen i. d. R. nicht gelöscht werden, was dazu führen kann, dass er am Ende seiner Ausbildung mehr Zugriffsrechte hat als die meisten langjährigen Mitarbeiter.

[76] Beispielsweise bei längerer Abwesenheit.

[77] Ein Forschungsnetzteilnehmer erhält nur diejenigen Zugriffsrechte, die er zu diesem Zeitpunkt tatsächlich benötigt.

3.5.10. Firewalling und Proxying

Um den Rahmen dieses Abschnitts nicht zu sprengen wurde die Beschreibung der Grundlagen der Firewall-Technologie in den Anhang (Abschnitte C.3.10 und C.6.6) ausgegliedert. Im Abschnitt C.6.6 „Netzabsicherung“ werden u. a. die Vorteile des mehrstufigen Firewall-Aufbaus beschrieben. Der mehrstufige Aufbau reduziert das von einem kompromittierten Bereich/System ausgehende Risiko. Die redundante Auslegung der Firewalls ermöglicht eine unproblematische Abschaltung von Teilen der Infrastruktur z. B. für die Dauer der Wartungsarbeiten, ohne dass die Forschungsnetzdienste dadurch unsicher oder unerreichbar blieben. Dieselbe Redundanz sollte auch bei der Anbindung des Forschungsnetzes an das Internet angestrebt werden.[78] Mehrere physikalische unabhängige Leitungen garantieren zuverlässige Erreichbarkeit der Dienste.

Die Abbildung 7 zeigt eine mehrstufige, redundant ausgelegte Firewall-Infrastruktur. Die Redundanz erhöht nicht nur die Verfügbarkeit der Forschungsnetzdienste, sondern vereinfacht auch ihre Wartung und Absicherung. So können z. B. die Regelwerke der redundant ausgelegten Firewalls zwischen dem Internet und der DMZ1 ohne Unterbrechung des Betriebs angepasst werden. Zusätzliche Sicherheit kann durch unterschiedliche Konfiguration (Hard- und Software) der auf der gleichen Ebene eingesetzten Firewalls erzwungen werden: Bei Kompromittierung einer der beiden Firewalls könnte diese ohne Unterbrechung des Betriebs heruntergefahren werden. Das ermöglicht eine gründliche Fehleranalyse und -behebung ohne übermäßigen Zeitdruck. Ebenfalls wichtig ist die Trennung der Server nach ihrem Bedrohungspotenzial in unterschiedliche Netzsegmente. In der Abbildung 7 sind zwei DMZ-Segmente dargestellt. Prinzipiell könnte man DMZ1 und DMZ2 so lange aufteilen, bis sich jeder Server in einem separaten DMZ-Bereich befindet. Die Sinnhaftigkeit dieser Vorgehensweise müsste jedoch hinterfragt werden, da dies den Aufbau verkompliziert, was wiederum die Wahrscheinlichkeit einer Fehlkonfiguration erhöht. Die Auslastung der Firewalls könnte dadurch ebenfalls nachteilig beeinflusst werden.

In der DMZ1 positioniert man i. d. R. Server, die eine hohe Kompromittierungswahrscheinlichkeit aufweisen, da sie mit der Außenwelt i. d. R. intensiver kommunizieren als die Systeme in den nachgelagerten Netzsegmenten. In der DMZ2 können Forschungsnetzserver aufgestellt werden, die ihre Dienste einem engen Benutzerkreis anbieten und mit den Systemen im internen Netzbereich kommunizieren müssen (Antivirus-, Applikationsserver etc.). Es kann u. U. sinnvoll sein, DMZ2 vom internen Netz durch eine weitere Firewall-Stufe abzugrenzen. Diese Trennung reduziert das von den DMZ2-Systemen ausgehende Kompromittierungsrisiko für die internen Systeme.

Der Begriff DMZ wird oft in Verbindung mit einer extrem hohen Sicherheit gebracht. Tatsächlich handelt es sich bei einer DMZ um einen geschützten Bereich für ein oder mehrere

[78] In einem solchen Fall spricht man auch von der sogenannten aktiven Redundanz. Zusätzlich unterscheidet man zwischen einer semiaktiven und einer passiven Redundanz. Im Falle der semiaktiven Redundanz ist ein überschaubarer Zeitraum erforderlich, um die Ausweichlösung zu aktivieren. Im Falle der passiven Redundanz ist der Zeitraum für die Aktivierung der Ausweichlösung wesentlich größer.

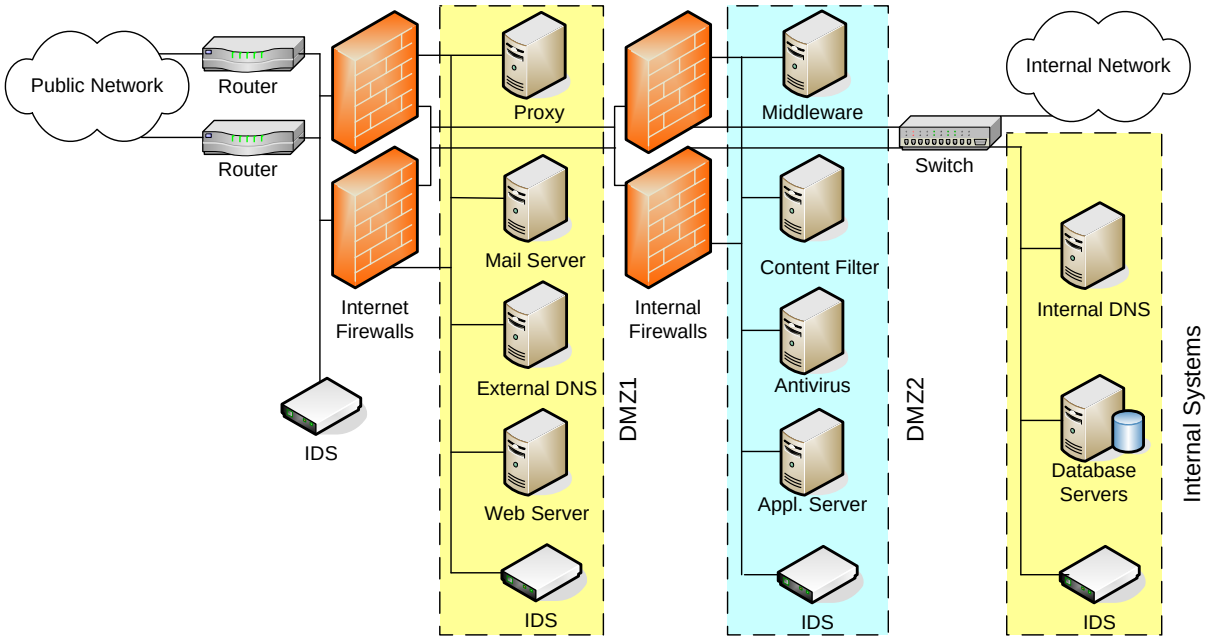

Abbildung 7.: Empfehlung für den Aufbau der Firewall-Infrastruktur in einem Forschungsnetz: Eine redundante mehrstufige Auslegung der Firewall-Infrastruktur erhöht u. a. die Verfügbarkeit der Lösung und erleichtert die Wartung und Fehleranalyse.

Systeme, die zwischen zwei Computernetzen platziert sind. Dieser Bereich wird meist durch eine Firewall (außen) und eine Firewall (innen) gegen die Außenwelt abgeschirmt. Durch diese Trennung besteht die Möglichkeit, den Zugriff auf öffentliche Dienste über die sogenannten Bastion Hosts anzubieten und zugleich das interne Netz (LAN) vor unberechtigten Zugriffen zu schützen. Daher ist der Datenbankserver im DMZ-Bereich per Definition schlechter geschützt als im Falle seiner Platzierung im internen Netzwerk (siehe Abbildung 7). Die im TMF-Gutachten für Biobanken [BGH+06, S. 144] ausgesprochene Empfehlung, die Datenbank-Server im DMZ-Bereich zu platzieren, kann ein erhöhtes Risiko für die Server bedeuten. Für die Unterbringung der Datenbankserver sind die speziell abgesicherten Bereiche innerhalb des internen Netzes besser geeignet.[79] Das Thema Proxying sowie einige Aspekte der Platzierung von IDS-Sensoren und VPN-Endpunkten in Verbindung mit Firewalling werden im Abschnitt C.3.10 untersucht und erörtert.

3.5.11. Intrusion Detection Systeme (IDS)

Firewalls können mit einem Türschloss verglichen werden, denn sie ermöglichen eine Überwachung des Datenverkehrs an einem bestimmten Punkt (vgl. [Wal02]). Sollte ein Angreifer dieses Schloss überwunden oder sich auf eine andere Weise den Zugang zu einer Infrastruktur verschafft haben, nutzen die Firewall-Lösungen wenig. Intrusion Detection-Systeme werden auch als „second line of defense“ bezeichnet und können in solchen Fällen hilfreich sein. Das Ziel eines Intrusion Detection-Systems besteht darin, die sich gegen eine

[79] Dieses Thema wird auch im Abschnitt 3.5.13 „Übersicht der technischen Komponenten der Sicherheitsarchitektur“ erörtert.

Infrastruktur richtenden Angriffe zu erkennen und auf diese adäquat zu reagieren. Die Überwachung wird durch ein deterministisches System oder einen Verbund solcher Systeme vollzogen.[80] Für die Feststellung eines Angriffs existieren mehrere Techniken; die wichtigsten davon sind Signaturerkennung, Analyse auf Protokollebene und Anomalienanalyse. Eine Beschreibung der IDS-Technologie sowie die Darstellung eines möglichen IDS-Einsatzszenarios in einem medizinischen Forschungsnetz befindet sich im Abschnitt C.3.11 „IDS-Technologie und -Einsatzszenario in einem medizinischen Forschungsnetz".
Als Ergebnis dieser Betrachtung lässt sich feststellen, dass die Intrusion Detection-Systeme lediglich ein Bestandteil der technischen Schutzmaßnahmen einer Infrastruktur sind (vgl. [Gre03]). Die Einführung eines Intrusion Detection-Systems alleine wird die Sicherheit des Forschungsnetzes nicht wesentlich erhöhen können. Erst das Zusammenspiel mehrerer Faktoren, wie adäquate Reaktion des entsprechend geschulten Personals, gut durchdachte Konzepte der Datenverteilung, ein wohl definiertes Konzept der Berechtigungsvergabe und -kontrolle, Zusammenspiel der IDS mit anderen Infrastrukturbestandteilen etc. sorgen in Verbindung mit weiteren organisatorischen und administrativen Maßnahmen für den optimalen Schutz (s. a. Abschnitte 3.3.2, 3.4, 3.5.9 und 3.5.10).

3.5.12. Monitoring und Protokollierung

Protokollierung und Monitoring stehen für manuelle oder automatische Erfassung von Zuständen, Beobachtung und Überwachung von Vorgängen oder Prozessen, wobei Monitoring die aktive Form der Überwachung ist, da es Eingriffe in die Prozessabläufe ermöglicht. Durch die Auswertung der erfassten Informationen muss sich feststellen lassen, wer wann auf welche Ressourcen zugegriffen hat bzw. zugreifen kann.
So unterscheidet man zwischen der Verfahrens- und der Systemüberwachung. Die wichtigsten Aspekte der Überwachung dieser beiden Aktionsarten werden im Abschnitt C.3.12 „Aspekte der Protokollierung und des Monitorings in medizinischen Forschungsnetzen" ausführlich dargestellt. Im gleichen Abschnitt erfolgt eine Untersuchung der für die Protokolldaten geltenden Aufbewahrungsfristen sowie der bei der Protokollierung einzuhaltenden Rahmenbedingungen. Am Ende des Abschnitts werden die Einsatzpotenziale für die Watermarking- und die Zeitstempeldiensttechnologie in den medizinischen Forschungsnetzen analysiert.

3.5.13. Übersicht der technischen Komponenten der Sicherheitsarchitektur

In den vorhergehenden Abschnitten wurden die technischen Aspekte der Sicherheit eines medizinischen Forschungsnetzes sowie die Vor- und Nachteile einiger möglicher Konfigura-

[80] Die von IDS verwendeten auf statistischen und logischen Ansätzen sowie neuronalen Netzen basierenden Angriffserkennungsmethoden werden in [Hoe01] ausführlich vorgestellt.

tionen der Sicherheitsarchitekturkomponenten untersucht und erörtert. Dieser Abschnitt führt die Ergebnisse der Vorgängerabschnitte zusammen, indem ein generischer Aufbau für das Zusammenspiel der untersuchten Komponenten der Sicherheitsarchitektur vorgestellt wird. Die Entscheidung für eine bestimmte Kombination der Komponenten hängt von vielen Faktoren ab: Einsatzzweck, bereits vorhandene Infrastruktur, Know-how der Mitarbeiter, Sicherheits- und Risikopolitik, gesetzliche Anforderungen und nicht zuletzt die Verhältnismäßigkeit[81]. Es wäre utopisch zu glauben, jede erdenkliche Konfiguration bzw. Ausprägung der Forschungsnetzinfrastruktur beschreiben zu können; trotzdem ist es möglich, eine generische Empfehlung zu erzeugen, die als Vorlage bei der Konzeption der technischen Sicherheitsarchitektur eines Forschungsnetzes dienen kann. In der Abbildung 8 ist eine der möglichen Varianten für einen solchen generischen Aufbau dargestellt, wobei die in vorhergehenden Abschnitten empfohlenen Redundanzen[82] aus Vereinfachungsgründen nicht abgebildet werden.

Zusammenfassung des Infrastrukturaufbaus: In der vorliegenden generischen Empfehlung sind die *IDAT*- und *MDAT*-Datenbanken physikalisch und organisatorisch voneinander getrennt. Der Zugriff auf die *IDAT*-Datenbank wird durch einen dreistufigen Aufbau (FW3, ALG1, FW5) abgesichert (s. a. Abschnitt 3.5.10 „Firewalling und Proxying“). Die Entschlüsselung ankommender Anfragen erfolgt auf dem Application Level Gateway (ALG1), die dann unverschlüsselt an die Applikationsserver (SRVIDAT) weitergeleitet werden. SRVIDAT ermitteln ihrerseits die Abfragedaten von den dahinter platzierten Datenbankservern. Die Kommunikation zwischen den Datenbank- und den Applikationsservern wird gefiltert, wobei der Filterausbau mehrstufig sein kann. Die Verschlüsselung dieser Daten ist optional; die Komponenten sollten sich mithilfe von Zertifikaten identifizieren können. Ein in etwa gleicher dreistufiger Aufbau ist auch der *MDAT**-Datenbank in Form von FW1, FW2 und FW4 davor geschaltet.
Sowohl die Daten in *IDAT* als auch in *MDAT** sind in verschlüsselter Form abgespeichert; auch die Datenübertragung findet verschlüsselt statt.[83] Die Datenbanken sollen zusätzlich durch eine Reihe weiterer im Abschnitt 3.5.8 „Datenbanksicherheit“ aufgeführter Sicherheitsmaßnahmen geschützt werden.
Externe Forschungsnetzteilnehmer greifen auf die Dienste der Applikationsserver nicht direkt zu; eine Lockdown-Umgebung und ein SSO-System stellen sicher, dass auf medizinische Daten nicht aus einer kompromittierten Umgebung bzw. von einer unbefugten Person zugegriffen wird (s. a. Abschnitte 3.5.1 „Sichere Arbeitsumgebung“, 3.5.3 „Authentifizie-

[81]Erforderlichkeit im Sinne des begründeten Verzichts auf einige Redundanzen oder der Implementierung von „einfacheren“ Sicherheitsvorkehrungen. Mangelnde Ressourcen gelten nicht als ein Verhältnismäßigkeitskriterium (vgl. [Pom11b]).

[82]Beispielsweise der mehrstufige Firewall-Aufbau.

[83]S. a. Abschnitt C.3.8 „Verschlüsselung und Signaturen“.

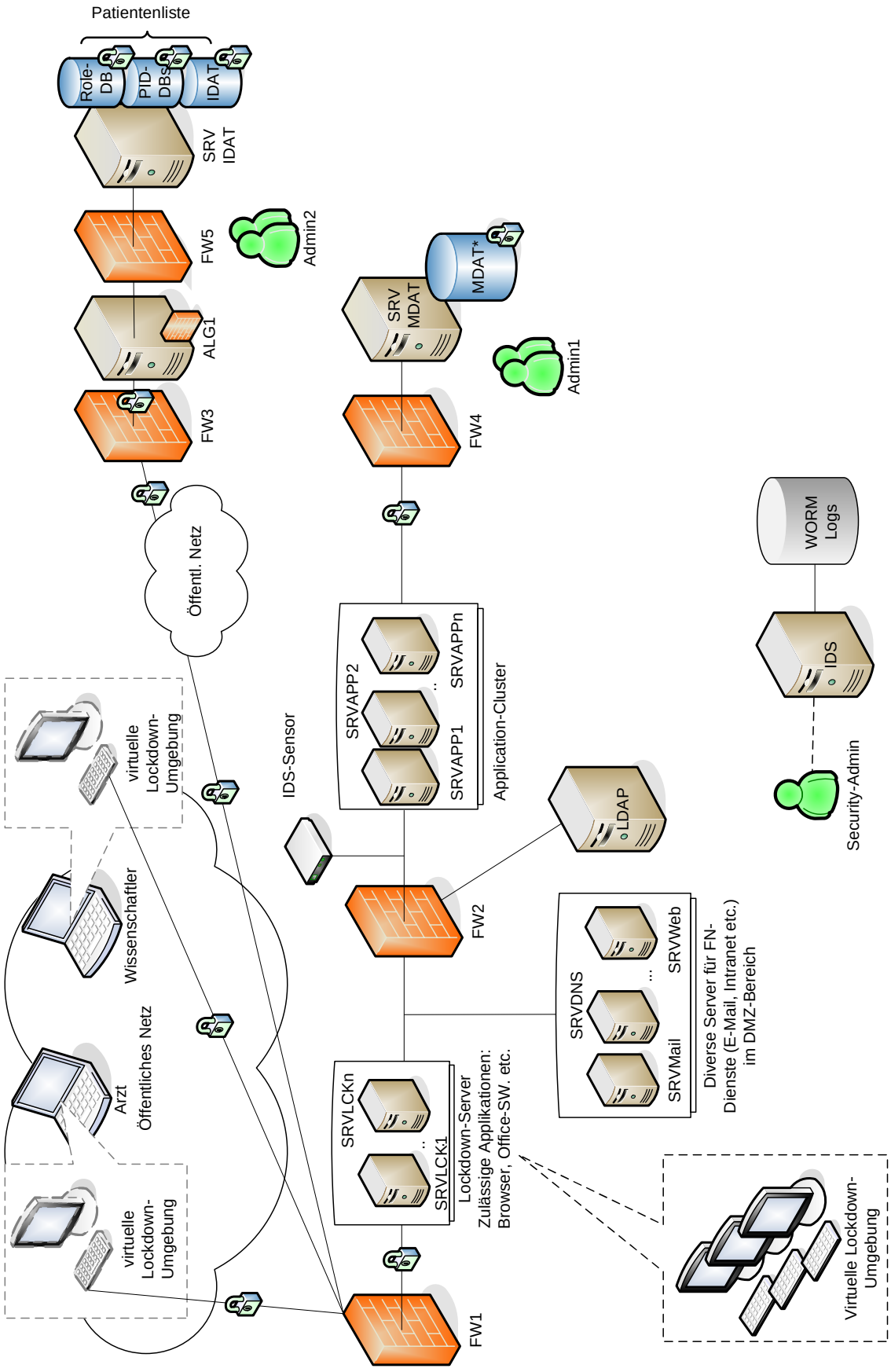

Abbildung 8.: Generische Empfehlung für den Infrastrukturaufbau: Die abgebildete Aufbaumöglichkeit berücksichtigt die Trennung der $IDAT$- und $MDAT$-Datenbanken. Der Client-Zugriff auf die Applikationsserver erfolgt ausschließlich aus einer kontrollierbaren Umgebung (Lockdown). Die Platzierung der VPN-Endpunkte und IDS-Sensoren berücksichtigt die zu kontrollierende Datenmenge und Datenverschlüsselung. IDS-Daten werden über ein dediziertes Netzsegment übertragen.

rung von Forschungsnetzteilnehmern“ und 3.5.5 „Zugangsszenarien von Netzteilnehmern zu den Forschungsnetzdiensten“). Die Zulässigkeit von Benutzertransaktionen wird anhand der Benutzerberechtigungen (rollenbasiert) und der Vertraulichkeit der Arbeitsumgebung überprüft (s. a. Abschnitte 3.5.4 „Rollenbasierte Rechtevergabe (RBAC)“ und 3.5.6 „Verzeichnisdienste (LDAP, OCSP)“).
Diverse Anti-Malware-Einrichtungen garantieren die Systemsicherheit (s. a. Abschnitt 3.5.9 „Antimalware-Einrichtungen“). Das von einem Security-Administratorenteam bediente Intrusion Detection-System wertet Daten aus, die von den an mehreren Standorten installierten Sensoren übermittelt werden (s. a. Abschnitt 3.5.11 „Intrusion Detection Systeme (IDS)“). Sicherheitsrelevante Transaktionen und Vorgänge werden überwacht und protokolliert (s. a. Abschnitt 3.5.12 „Monitoring und Protokollierung“).
Die gleichzeitige Einhaltung aller in den vorhergehenden Abschnitten beschriebenen Sicherheitsrichtlinien in ihrer Funktion als Bestandteile einer Sicherheitsarchitektur ist oft nicht möglich. Die Gründe dafür können vielfältig sein, liegen jedoch meistens in der finanziellen Ausstattung und den für die Umsetzung verfügbaren Ressourcen. Die Nichteinhaltung von Sicherheitsrichtlinien kann in der Erhöhung des Gefahrenpotenzials für das Forschungsnetz resultieren. Aus diesem Grund muss jede Abweichung von den Regeln begründet sein. Eine abweichende Regelung kann beispielsweise getroffen werden, wenn nachgewiesen wird, dass alle forschungsnetzkonformen Lösungsmöglichkeiten berücksichtigt wurden, diese jedoch aus Gründen der technischen Machbarkeit oder der Verhältnismäßigkeit nicht umgesetzt werden.[84]

3.6. Zusammenfassung des Kapitels

In diesem Kapitel wurden die generischen Sicherheitsrichtlinien als Bestandteile der Sicherheitsarchitektur eines medizinischen Forschungsnetzes vorgestellt. Im Vordergrund stand die Aufteilung der Sicherheitsarchitektur und entsprechend der Sicherheitsmaßnahmen in die Bereiche Organisation, Administration und Technik. Bei der Ausarbeitung von Einsatzempfehlungen einzelner Maßnahmenarten wurden die Bedeutung und die Notwendigkeit einer ausgewogenen Kombination und der gegenseitigen Ergänzung dieser Maßnahmenkategorien deutlich. Die Erkenntnis der Notwendigkeit einer ausgewogenen Maßnahmenkombination sowie der Unzulänglichkeit des Schutzes eines medizinischen Forschungsnetzes bei unzureichender Berücksichtigung einer der drei Maßnahmenkategorien führt zu der als folgende These zusammengefassten Schlussfolgerung:

T1: Eine ganzheitliche Ausrichtung der Sicherheitsmaßnahmen ist notwendig, um einen umfassenden Schutz eines medizinischen Forschungsnetzes durch die Kombination von organisatorischen, technischen und administrativen Maßnahmen zu erreichen.

[84] Eine Untersuchung der Bedeutung der Einhaltung von Sicherheitsrichtlinien sowie der Möglichkeiten des Einsatzes von Schutzprofilen als ein Sicherheitsinstrument in der medizinischen Forschung erfolgt im Abschnitt C.4 „Die Bedeutung der Einhaltung von Sicherheitsrichtlinien“.

Die Gestaltung eines sinnvollen Zusammenspiels zwischen den Komponenten einer Sicherheitsarchitektur und insbesondere die Möglichkeiten der Bewertung des Sicherheitsniveaus eines Forschungsnetzes werden im nächsten Kapitel untersucht.

4. Entwicklung eines Konzeptes für das dynamische S&R-Management

Das Hauptziel der vorliegenden Arbeit ist die Beschreibung der Vorgehensweise, wie die Forschungsnetzdienste vor Ausfällen, kriminellen Handlungen, höherer Gewalt und menschlichem Versagen geschützt werden können. Die Forschungsnetzdienste sind auf Ressourcen angewiesen, die ihre Verfügbarkeit und Schutz garantieren. Zu solchen Ressourcen zählen u. a. Räumlichkeiten, IT-Systeme, und natürlich die Mitarbeiter mit ihrem Know-how. Sicherheits- und Risikomanagement ist ein Verfahren zur Analyse und zur Bewertung von Sicherheitsrisiken sowie zur Definition und Identifizierung geeigneter Schutz- und Kontrollmechanismen, die die Erreichung eines spezifizierten Sicherheitsniveaus gewährleisten (vgl. [wek12]). In diesem Kapitel wird der Sicherheits- und Risikomanagementprozess (S&R-Prozess) als ein Vorgang zum Aufbau, zur Steuerung und zur Entwicklung eines sicheren Forschungsnetzbetriebs detailliert untersucht. Im Vordergrund der Prozessgestaltung stehen die Ermittlung des erforderlichen Sicherheitsniveaus und die effiziente Verwendung verfügbarer Ressourcen, um dieses Niveau zu erreichen. Die Effizienz ergibt sich aus dem Verhältnis zwischen einem definierten Nutzen (Sicherheitsniveau) und dem Aufwand (Sicherheitsmaßnahmen), der zu dessen Erreichung notwendig ist.

4.1. Verwendung von S&R-Ansätzen in der medizinischen Forschung

Die zweite in dieser Arbeit definierte und im Folgenden untersuchte forschungsleitende Frage lautet (s. a. Abschnitt 2.1.1):

> F2: Wie können die Sicherheitsmaßnahmen in den medizinischen Forschungsnetzen effizient gestaltet werden?

Für die Ermittlung der in der medizinischen Forschung verwendeten Sicherheits- und Risikomanagementansätze (S&R-Ansätze) wurden im Rahmen dieser Arbeit die mit der Arbeitsgruppe Datenschutz der TMF abgestimmten Datenschutzkonzepte medizinischer Forschungsnetze analysiert. Diese für die Beantwortung der zweiten Forschungsfrage durchgeführte Untersuchung ergab, dass in den einzelnen Forschungsnetzen folgende gesetzliche und normative Bestimmungen, Normen, Standards und Frameworks für die

Konzeption und Umsetzung von Sicherheitsmaßnahmen angewendet werden:

- Die generischen Datenschutzkonzepte der TMF bzw. bereits bestehende und als sicher eingestufte Sicherheitskonzepte anderer Netze (z. B. [RDSP06]).
- Bundes- und Landesdatenschutzgesetze[1] sowie Vorschläge der Bundes- und Landesdatenschutzbeauftragten (beispielsweise [Wir08], [Der07])[2] sowie die Regelungen der GCP, MBO, AMG, MPG, StrlSchV, StGB, Regulierungen der FDA etc. bestimmten die in den Datenschutzkonzepten beschriebenen Sicherheitsmaßnahmen in Bezug auf die Aufbewahrungsfristen, die Datenweitergabe und die Qualitätssicherung.[3]
- Vertragliche Vereinbarungen, SOPs und Verwendung bestehender Sicherheitsstrukturen der dateneingebenden, -speichernden, und -verarbeitenden Stellen.[4]
- Circle of Security[5].
- BSI-Empfehlungen, BSI-Grundschutz bzw. Grundschutzzertifizierungen.[6]

Einige der untersuchten Datenschutzkonzepte enthalten detaillierte Beschreibungen der einzelnen Phasen des S&R-Prozesses und der zu erfüllenden Sicherheitsanforderungen. Die im Datenschutzkonzept des Brain-Net [NB04] aufgeführten Sicherheitsmaßnahmen basieren beispielsweise auf dem „Circle of Security“-Ansatz (vgl. [Nor00]). Im Datenschutzkonzept des Brain-Net wird außerdem das Thema der Wirksamkeitsbewertung von Sicherheitsmaßnahmen thematisiert. Die aufgezeigte Möglichkeit zur kontinuierlichen Überprüfung der Wirksamkeit von Sicherheitsmaßnahmen besteht im Datenvergleich vor und hinter einem Sicherheitssystem (vgl. [NB04, S. 37]).
Einige Konzepte enthalten detaillierte Bedrohungsanalysen sowie Bewertungen der Risiken und der Schutzbedürftigkeit einzelner Systeme oder Prozesse (z. B. [Spi07], [HV08], [HWE05]). Die Analysen basieren auf den Hinweisen zur Risikoanalyse und Vorabkontrolle nach dem Hamburgischen Datenschutzgesetz [Wir08] bzw. BSI-Standards zu Risikoanalyse auf der Basis von IT-Grundschutz [bsi08c].

---

[1] Beispielsweise Anlage zu § 9 Satz 1 BDSG, §§ 5,6,35 BDSG, §§ 3,5,19 BlnDSG, § 9 LDSG B-W, §§ 9,10 LDSG NRW etc.

[2] Zum Beispiel in [HHH06], [Spi07], [GM08], [GK10], [MM03], [Han11], [Ill02a], [Law06], [HV08], [Wöh08], [ABC+11], [Spe04], [HHM+05], [Lut07], [KP10], [EW06], [HWE05].

[3] Zum Beispiel in [MM03], [HV08], [Spe04], [Lut07, S. 33], [KP10, S. 22], [EW06].

[4] Zum Beispiel in [HHH06], [GM08], [GK10], [MM03], [MM03], [Wöh08], [ABC+11], [Han11] [Spe04], [Lut07], [KP10], [EW06].

[5] Zum Beispiel in [NB04]

[6] Zum Beispiel in [HHH06], [Spi07], [Spe04], [HHM+05], [HWE05], [Han11].

Die Untersuchung einer Reihe weiterer TMF-Materialien ergab eine besondere Relevanz des TMF-Workshops „Sicherheitskonzepte in der vernetzten medizinischen Forschung“[7] vom 11. Dezember 2006. Die Workshop-Unterlagen beschreiben die Anforderungen an das Sicherheitsniveau sowie den Umsetzungsstand der Konzepte in den Forschungsverbünden und enthalten Expertenberichte aus den Bereichen Industrie und universitären Klinikrechenzentren über die verwendeten S&R-Ansätze. Als für die Untersuchung relevant erwiesen sich außerdem die Unterlagen zum TMF-Projekt „V071-01 IT Service Management“.
Neben den bereits bei der Analyse der TMF-Datenschutzkonzepte erwähnten Sicherheits-Frameworks, IT-Grundschutz und gesetzlichen Regelungen wurden im Rahmen des TMF-Projektes V016-01 folgende Frameworks und ihre potenzielle Eignung diskutiert: CobiT, BS 7799 und ISO/IEC 17799, ISO 27001, BSI 100-2, 100-3 (vgl. [Pup06, S. 5, 16], [Spe06, S. 9 f.]). Auch die Potenziale der Kombination unterschiedlicher Frameworks bzw. das Zusammenspiel von Standards wurden berücksichtigt: z. B. ISO 27799 mit ISO 17799 (vgl. [Pup06, S. 7], [Spe06, S. 16 f.]).
Neben den bereits genannten Frameworks wurde das modifizierte Sicherheitsmodell nach [TBC00] vorgestellt (vgl. [BS06]). Dieses Sicherheitsmodell berücksichtigt neben den managementbezogenen die inhaltlichen, kommunikationsbezogenen und zugangssicherheitstechnischen Aspekte.[8] Im Zusammenhang mit der Sicherheit im GRID-Bereich wurde das Globus-Toolkit [the12][9] genannt (vgl. [MST06]). Zusätzlich zu den bereits erwähnten gesetzlichen und normativen Anforderungen wurden die Sicherheitsanforderungen aus 21CFR11 der FDA [Foo97] als relevant identifiziert (vgl. [Ver06]). Der Abschlussbericht des Workshops betont die Komplexität und Aufwendigkeit einer dauerhaften Umsetzung von Sicherheitskonzepten (vgl. [SD07, S. 6.]).
Im Abschnitt A.1 „Untersuchung der Wirksamkeitsbewertung von Sicherheitsmaßnahmen mithilfe von etablierten S&R-Frameworks“ wird detailliert untersucht, wie die Bewertung der Wirksamkeit und Effizienz bzw. Verhältnismäßigkeit von Sicherheitsmaßnahmen in den hier aufgeführten und weiteren etablierten Sicherheits- und Risikoframeworks erfolgt. Die Analyse berücksichtigt folgende Frameworks:

- ISO-Normenreihe (ISO 2700X) (Abschnitt A.1.1),
- COBIT 4.1 (Abschnitt A.1.2),
- ITIL V.3 (Abschnitt A.1.3),

[7] Durchgeführt im Rahmen des TMF-Projektes „V016-01 Sicherheitskonzepte“.

[8] Sicherheitsmanagement (Policies), Content Security (Integrität), Zugangssicherheit (Nichtabstreitbarkeit und Authentizität), Kommunikationssicherheit im Sinne von Vertraulichkeit.

[9] Die Sicherheitsinfrastruktur von Globus Toolkit berücksichtigt die Sicherheitsmaßnahmen auf der Message- und Transport-Ebene: Die Standards SAML, WS-Security, SOAP, X.509 und TLS kommen zum Einsatz (vgl. [SW05], [Wel05], s. a. Abschnitt 3.5 „Technische Aspekte von Sicherheitsrichtlinien“). Die gesichtete Dokumentation enthält keine Hinweise im Hinblick auf die verwendeten Risikomanagementansätze und insbesondere im Hinblick auf die Messung der Effizienz von Sicherheitsmaßnahmenportfolios, sodass die Globus-Sicherheitsinfrastruktur im Rahmen der folgenden Analyse von Sicherheits- und Risikomanagementansätzen nicht näher untersucht wird.

- NIST 800-X (Special Publications) (Abschnitt A.1.4),
- BSI IT-Grundschutz (Abschnitt A.1.5),
- Open Source Security Testing Methodology Manual (Abschnitt A.1.6.1),
- Operationally Critical Threat Asset and Vulnerability Evaluation (OCTAVE) (Abschnitt A.1.6.2),
- CCTA Risk Analysis and Management Method (CRAMM) (Abschnitt A.1.6.3),
- SIEM-Systeme (Abschnitt A.1.6.4),
- SAS-Systeme (Abschnitt A.1.6.5),
- HIPAA Security Series (Abschnitt A.1.6.6),
- Circle of Security (Abschnitt A.1.6.7) und
- SSE-CMM, ISSEA (Abschnitt A.1.6.8).

Eine vergleichende Bewertung der Sicherheitsstände einzelner Forschungsnetze mit dem Ziel, die notwendigen Sicherheitsvorkehrungen zu ermitteln und einzuleiten, erfordert einen Ansatz, der mit möglichst wenig zusätzlichem Aufwand und ohne umfangreiche Änderung bestehender Strukturen auskommt und dabei die Sicherheitsanforderungen dieser Strukturen berücksichtigt. Die beschriebene Bandbreite der in den Forschungsnetzen eingesetzten S&R-Frameworks ist groß. Die Ansätze unterscheiden sich in der gewählten Betrachtungsweise der Informationssicherheit, der Handhabung der Fragestellung nach der Notwendigkeit und der Steuerung von Sicherheitsinvestitionen. Auch wenn die betrachteten Frameworks teilweise gegenseitig die Methoden anderer Ansätze nutzen,[10] so kann ihre gegenseitige Kompatibilität nicht als gegeben gelten. Gäbe es eine theoretische Kompatibilität von verwendeten spezifischen Frameworks, und könnte eines der untersuchten Frameworks die Sicherheitsbedürfnisse aller berücksichtigten Forschungsnetze abdecken, dürfte der immense Konsolidierungsaufwand der praktischen Vereinheitlichung entgegenstehen (vgl. [Tou05]).

4.2. Gezielte Ausgestaltung der Sicherheitsarchitektur für die medizinischen Forschungsnetze

Die Menge und die Art der umzusetzenden Sicherheitsmaßnahmen ist per Definition durch die Höhe der verfügbaren finanziellen Mittel und Ressourcen eingeschränkt, die es möglichst effektiv einzusetzen gilt. Die Möglichkeiten und Empfehlungen zur Effektivitätsmessung von Sicherheitsmaßnahmen durch die etablierten S&R-Ansätze wurden im vorhergehenden Abschnitt untersucht. Dass die Sicherheitsinvestitionen nicht nach dem Gießkannenprinzip, sondern gezielt eingesetzt werden sollen, bestätigen die aktuellen Erkenntnisse auf dem Gebiet der Sicherheitsforschung. So wird in der NIST-Publikation

[10] Zum Beispiel ISO 2700X in ITIL, OCTAVE, CRAMM und BSI-IT-Grundschutz, NIST in HIPAA Security Series, SSE-CMM und Circle of Security.

800-55[11] explizit darauf hingewiesen, dass die Verteilung der Sicherheitsinvestitionen im Zusammenhang mit einem umfangreichen Risikomanagementprogramm erfolgen soll. Die Verwendung von Sicherheitsmetriken soll dabei eine quantifizierbare und dadurch objektive Entscheidungsgrundlage liefern. Dadurch wird eine Optimierung des Ressourceneinsatzes angestrebt. [CSS+08, S. 11]: *„By using measures to target security investments, these measures can aid organizations in obtaining the best value from available resources.“* Dies legitimiert die Notwendigkeit eines ganzheitlichen S&R-Managements.

4.2.1. Bedeutung und Struktur einer Sicherheitsleitlinie

Die Sicherheitspolitik eines Forschungsnetzes wird durch seine Struktur/Aufgabe bestimmt. Die Sicherheitspolitik legt die Bedeutung des Themas Sicherheit für ein Forschungsnetz fest und beschreibt dessen Risikostrategie. Die Entscheidung für die Ausrichtung der Sicherheitspolitik sollte bereits bei der Gründung eines Forschungsnetzes erfolgen. Diese Ausrichtung ist jedoch nicht frei und wird durch diverse Gesetze, Vorschriften, Verordnungen und Standards bestimmt. Bei der Festlegung der Richtung der Sicherheits- und Risikopolitik sind diverse gesetzliche Anforderungen, Normen sowie datenschutzrechtliche Bestimmungen[12] die treibenden Kräfte (vgl. [dat11], [Gua09], [Moh07, S. 71], [MW02], [RLV+01], [ich96]). Zu berücksichtigen ist, dass die Sicherheit eines Forschungsnetzes nicht die Rolle eines „Verkaufsarguments“ besitzt. Ein Sicherheitsstand, der höher als gesetzlich und vertraglich notwendig ist, erhöht nicht den Erfolg eines Forschungsnetzes. Eine ausführliche Übersicht der die Sicherheitspolitik eines Forschungsnetzes bestimmenden Randbedingungen ist in [RDSP06] und [SPR+06] erläutert.

Die Sicherheitspolitik eines Forschungsnetzes ist die oberste richtungweisende, für die Gestaltung der Sicherheitsarchitektur maßgebliche Ebene. Sie hilft bei der Konsolidierung von Bemühungen mehrerer Verantwortlicher und vermeidet die Festlegung von individuellen, mit der Informationssicherheitsstrategie des Forschungsnetzes nicht kompatiblen Sicherheitszielen.[13] Es ist empfehlenswert, die Leitaussagen zur Sicherheitsstrategie im Rahmen einer sogenannten Sicherheitsleitlinie zusammenzufassen (vgl. [bsi11d, M 2.192]). Auch wenn für jedes Forschungsnetz eine individuelle Sicherheitsleitlinie entwickelt werden muss, kann auf der Grundlage des für ein jedes Forschungsnetz geltenden Grundsatzes – Vorantreiben der medizinischen Forschung unter der Berücksichtigung der maßgeblichen gesetzlichen Rahmenbedingungen – eine allgemeine Sicherheitsleitlinie als Ausgangsbasis entwickelt werden. Eine gesetzeskonforme Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit der Forschungsnetzdaten gilt als eine wichtige Rahmenbedingung eines jeden Forschungsnetzes. Ein Vorschlag für die Gestaltung der Sicherheitsleitlinie wird im

[11] „Performance Measurement Guide for Information Security“ [CSS+08].

[12] GG, EG-Datenschutz-Richtlinie (z. B. 95/46/EG, 2002/58/EG, 2001/20/EG, 2005/28/EG), BDSG, LDSG, GenDG, StGB, SigG, BOÄ etc.

[13] Ein anschauliches Beispiel für die Bedeutung der Sicherheits- und Risikopolitik aus der Verarbeitung von medizinischen Daten präsentiert Michael Ronellenfitsch in seinem Tätigkeitsbericht [Ron05].

Abschnitt A.2 unterbreitet. Die einzelnen Aussagen dieser generischen Sicherheitsleitlinie müssen von einem konkreten Forschungsnetz auf ihre Gültigkeit und Relevanz überprüft werden.

4.2.2. Sicherstellung der Gültigkeit der Sicherheitsleitlinie

Einige Autoren empfehlen eine regelmäßige Überprüfung der Sicherheitsleitlinie im Hinblick auf ihre Aktualität (vgl. [PB06]). Es wird außerdem empfohlen, die Leitlinie von jedem Teilnehmer unterschreiben zu lassen, um dadurch das Einverständnis der Teilnehmer mit dem Inhalt der Leitlinie festzuhalten, denn die unterschriebene Einverständniserklärung des Teilnehmers kann im Falle eines Rechtsstreits verwendet werden. Durch die ausreichend allgemeine Formulierung der Sicherheitsleitlinie ist ein lediglich geringer zukünftiger Aktualisierungsaufwand zu erwarten. Bei der Vertragsgestaltung sind Elemente der Sicherheitsleitlinie zu berücksichtigen.[14]

4.3. Qualitative Bewertung der Bedrohungs- und Risikosituation

Ordnet man die Sicherheitsleitlinie in das im Abschnitt C.5 vorgestellte generische S&R-Modell der RiSiKo-Pyramide ein, wird deutlich, dass die Sicherheitsleitlinie in die oberste Ebene der Sicherheitspolitik gehört. Zwischen der Ebene der Sicherheitspolitik, den daraus abgeleiteten Sicherheitszielen und der Entscheidung zugunsten einer konkreten Sicherheitsmaßnahmenkombination besteht i. d. R. nur ein mittelbarer Zusammenhang. Vor der Quantifizierung der Bedrohungen und der daraus abgeleiteten Entscheidung für die Maßnahmenumsetzung ist eine qualitative Einschätzung der Gefährdungslage hilfreich. Grundsätzlich kann eine solche Einschätzung durch die Betrachtung der geltenden Risiken bzw. Motive für einen Angriff oder aber durch die Auseinandersetzung mit den angebotenen Diensten und ihren Sicherheitsanforderungen erfolgen. In diesem Abschnitt werden diese beiden Ansätze zur Einschätzung der Bedrohungs- und Risikosituation vorgestellt. Der schutzbedarfsorientierte Ansatz basiert auf der Bewertung der Risikopotenziale für die vom Forschungsnetz angebotenen Dienste und den daran beteiligten Ressourcen. Der bedrohungsorientierte Ansatz setzt sich mit den potenziellen Angreifern und ihren Motivationen auseinander. Durch die unterschiedlichen Herangehensweisen der beiden Ansätze an die qualitative Gefährdungsbewertung können vielfältige Aspekte der Gefährdungslage ermittelt werden.

[14] Zum Beispiel Vertrag mit dem behandelnden Arzt zur Qualitätssicherung, mit den Wissenschaftlern zur vorschriftsmäßigen Datenverwendung und mit den Rechenzentren und Systembetreuern zur Sicherung der regelmäßigen Administration der Datenbanken und deren Schutz (vgl. [HWE05]).

4.3.1. Schutzbedarfsorientierte Analyse

Beim schutzbedarfsorientierten Ansatz werden die Forschungsnetzdienste und die daran beteiligten Ressourcen auf ihre Bedeutung für den Forschungsnetzbetrieb analysiert (vgl. [HV08, S. 20 f.], [Spi07, S. 24 f.], [HWE05, S. 18 f.]). Dabei wird jeder Dienst auf die Einhaltung von den Sicherheitskriterien Authentizität, Integrität, Konformität, Robustheit, Verbindlichkeit, Verfügbarkeit und Vertraulichkeit geprüft, und die Folgen der Sicherheitsverletzungen[15] werden ermittelt (vgl. [Mül11, S. 162 f.]). Als besonders relevant für die schutzbedarfsorientierte Analyse wurden folgende Forschungsnetzdienste identifiziert:

- zentrale Patientenliste,
- PID-Dienst,
- Rückmeldung von Forschungsergebnissen,
- Pseudonymisierung von Patientendaten,
- Anonymisierung von Patientendaten,
- Public Key-Infrastruktur,
- Teilnehmerservice zur Beantragung und Verteilung von Chipkarten und Softwarezertifikaten,
- Qualitätssicherungsservice,
- Datenexport und Datenabruf,
- Verwaltung von Zugriffsrechten,
- Handhabung von Biomaterialien und den daraus gewonnenen Daten.

Die aus der Schutzbedarfsanalyse gewonnenen Erkenntnisse bilden die Basis für die Sicherheitsanforderungen an die Forschungsnetzdienste. Die Ergebnisse der qualitativen Schutzbedarfsuntersuchung für die Forschungsnetzdienste sind im Abschnitt A.3 zusammengefasst.

Vor der Schutzbedarfsuntersuchung für die o. g. Dienste erfolgt jeweils eine kurze Beschreibung der gemachten Annahmen und der Funktionsweise des Dienstes. Die Beschreibungen lehnen sich hauptsächlich an die Ausführungen in [RDSP06], [SPR+06], [SSS06] und [DC06]. Die Bedeutungen von Verletzungen einzelner Sicherheitskriterien für die genannten Dienste werden beschrieben und anschließend mit Noten zwischen 1 (keine schwerwiegenden Folgen) und 5 (potenziell hoher Schaden) bewertet. Die Bedeutung einzelner Schutzbedarfsklassen wird im Anhang D „Qualifizierung von Sicherheitskriterien“ erläutert.

4.3.2. Bedrohungsorientierte Analyse

Eine praxisnahe Einschätzung des bestehenden Bedrohungspotenzials kann durch die Beantwortung folgender Frage erfolgen: Auf welche Art könnte ein Angreifer die Dienste des Forschungsnetzes missbrauchen? Bruce Schneier empfiehlt für diesen Zweck die Aufstellung

[15] Zum Beispiel Manipulation und Verfälschung beim Sicherheitskriterium *„Integrität“*, Systemausfall beim Kriterium *„Verfügbarkeit“* etc.

eines sogenannten Angriffsbaumes für eine Infrastruktur (vgl. [Sch04]). Ein möglichst vollständiger Angriffsbaum ist die Grundlage für die Ermittlung von Bedrohungspotenzialen und berücksichtigt die Angriffsszenarien, auf deren Basis die Gegenmaßnahmen ausgearbeitet werden können.
Neben der schutzbedarfsorientierten Betrachtung ist die bedrohungsorientierte Analyse eine wirkungsvolle Methode zur Erkennung der Schwächen einer Sicherheitsarchitektur. Mithilfe der Bedrohungsanalyse können die für ein Forschungsnetz geltende Bedrohungssituation erforscht und die Wirkungspotenziale der Risiken auf den Forschungsnetzbetrieb besser verstanden werden. Eine qualitative Untersuchung der für ein medizinisches Forschungsnetz geltenden Angreiferstruktur sowie der von diesen Angreifern ausgehenden Bedrohungsszenarien erfolgt im Abschnitt A.4. Diese Untersuchung verdeutlicht die möglichen Überschneidungen zwischen den Motiven mehrerer Angreifer und zeigt auf, dass in den meisten Fällen ein Angreifer auf das Interesse einer Drittpartei[16] an den Forschungsnetzdaten angewiesen ist.

Zusammenfassung: Die finanziellen und die ressourcenseitigen Einschränkungen sind dafür maßgeblich, dass nicht alle möglichen Sicherheitsmaßnahmen gleichzeitig umgesetzt werden können, sodass eine Auswahl der durchzuführenden Maßnahmen im Hinblick auf ihre Relevanz, Dringlichkeit oder Effizienz erfolgen muss. Im Zusammenhang mit der Begründung der Notwendigkeit von Sicherheitsmaßnahmen ist die Betrachtung ihrer Verhältnismäßigkeit von Bedeutung (vgl. [PSM+09], [Pom11b]). Manche Autoren fordern gar die Erstellung betriebswirtschaftlicher Kosten-Nutzen-Analysen für die Sicherheitsinvestitionen (vgl. [SGF02, S. 37 f.]). Die in diesem Abschnitt erörterten qualitativen schutzbedarfs- und bedrohungsorientierten Analysen erlauben Aufschlüsse über die möglichen Schwachstellen und die Notwendigkeit der Implementierung von Sicherheitsmaßnahmen. Die Frage, ob die Sicherheitsmaßnahme „X“ der Maßnahme „Y“ vorzuziehen ist, und welche weiteren Sicherheitsinvestitionen notwendig sind, um das erforderliche Sicherheitsniveau zu erreichen, kann mithilfe der beiden Ansätze jedoch nicht beantwortet werden. Um die Verhältnismäßigkeit von Sicherheitsmaßnahmen und die optimale Gestaltung einer Sicherheitsarchitektur bestimmen zu können bedarf man eines quantitativen Messansatzes für die Auswirkungen der Sicherheitsmaßnahmen auf das Sicherheits- und Risikoportfolio.

[16] Zum Beispiel Wirtschaft, Presse etc.

4.4. Herleitung eines Konzeptes für das quantitative dynamische Sicherheits- und Risikomanagement

Im Zusammenhang mit der Wirksamkeitsbewertung von Sicherheitsmaßnahmen wird häufig eine, Lord Kelvin[17] zugeschriebene, Aussage zitiert: *„If you can not measure it, you can not improve it“* (Lord Kelvin (1883)).
Die Suche nach einem objektiven Bewertungsverfahren für die Wirksamkeit von Sicherheitsmaßnahmen für die darauf aufbauende Steuerung des Sicherheits- und Risikoportfolios wurde im Rahmen der Beantwortung der dritten forschungsleitenden Frage durchgeführt:

F3: Wie kann die Wirksamkeit von Sicherheitsmaßnahmen in den medizinischen Forschungsnetzen objektiv bewertet werden?

Die für die Recherche in den Literaturdatenbanken verwendete Vorgehensweise ist ausführlich im Abschnitt 2.1.1.4 beschrieben. Die wichtigsten für die untersuchte Problemstellung als relevant ermittelten Ansätze sind im Abschnitt B.2 aufgelistet und erörtert. Die im Rahmen der systematischen Literaturrecherche untersuchten etablierten S&R-Frameworks (s. a. Abschnitt 4.1) sowie aktuelle Publikationen zur Wirksamkeitsbewertung von Sicherheitsmaßnahmen (s. a. Abschnitte A.1, B.2, 2.1.1) enttäuschten durch die Unvollkommenheit der Metrikvorschläge sowie den für ein einzelnes Forschungsnetz kaum zu bewältigenden Umsetzungs- und Wartungsaufwand. Es entstand die Idee, eine leichtere, zentralisierte auf die Bedürfnisse und Möglichkeiten der Forschungsnetze zugeschnittene Lösung zu entwickeln.
Als eines der Ergebnisse dieser Arbeit wurde das in diesem Abschnitt vorgestellte Konzept für das dynamische Sicherheits- und Risikomanagement „dynSRM“ entwickelt, mit dessen Hilfe eine insgesamt objektivere Bewertung der Wirksamkeit und Notwendigkeit von Sicherheitsmaßnahmen ermöglicht wird.

4.4.1. Das Basiskonzept des dynamischen Sicherheits- und Risikomanagements „dynSRM“

Eine besonders häufig eingesetzte Methode der Risikobewertung ist die sogenannte Risikomatrix („Risk-Level Matrix“) (vgl. [LR07, S. 226], [LM07, S. 251], [CS07, S. 198], [SGF02, S. 24 f.], [AD01, Vol. 9a S. I7-5 ff.]). Die Risikomatrix stellt die Wahrscheinlichkeit des Schadenseintritts der potenziellen Schadenshöhe gegenüber. Die Methode ist nicht zuletzt wegen der einfach verständlichen übersichtlichen Darstellungsform beliebt und ist eher für die Bewertung von sogenannten operationalen Risiken als für die Berücksichtigung einzelner Schadensereignisse geeignet. Die Nachteile der Risikomatrix-Vorgehensweise liegen im Schätzproblem, das im Hinblick auf die Komponenten Eintrittswahrscheinlichkeit

[17] William Thomson, 1. Baron Kelvin, auch oft als Kelvin of Largs bezeichnet.

und Schadenshöhe besteht. Außerdem ist das Schadensausmaß bei vielen Schadensarten keine feste Größe und unterliegt den Wahrscheinlichkeitsverteilungen, was durch eine Risikomatrix kaum berücksichtigt wird (vgl. [VV10], [CD09, S. 91. ff.], [BN08]). Die aus der Risikomatrix abgeleitete und in der Tabelle 1 abgebildete Tragbarkeit eines Risikos hängt von zwei Faktoren ab: der Schadenshöhe und der Eintrittswahrscheinlichkeit.[18]

Tragbarkeit des Risikos		**Höhe des Schadens**					**Höhe des Schadens**				
		1	**2**	**3**	**4**	**5**	**1**	**2**	**3**	**4**	**5**
Eintritts-wahrschein-lichkeit	**1**	ja	ja	ja	ja	nein	1	2	3	4	5
	2	ja	ja	ja	nein	nein	2	4	6	8	10
	3	ja	ja	nein	nein	nein	3	6	9	12	15
	4	ja	nein	nein	nein	nein	4	8	12	16	20
	5	nein	nein	nein	nein	nein	5	10	15	20	25

Tabelle 1.: Tragbarkeit eines Risikos: Die aus dem Konzept der Risikomatrix abgeleitete Tragbarkeit eines Risikos hängt von der Schadenshöhe und deren Eintrittswahrscheinlichkeit ab. Die rechts abgebildete Beispielbelegung mit Zahlenwerten (Ordinalskala) zeigt auf, dass das mathematische Produkt der beiden Größen nicht immer mit dem Ergebnis über die Tragbarkeit eines Risikos übereinstimmt und somit nicht das alleinige Entscheidungskriterium für oder gegen die Tragbarkeit des Risikos ist.

Die sich aus der Risikomatrix ergebende Risikodefinition lautet: $R_t = H_t \times P_t$ (R – Risiko, H – Höhe des Schadens, P – Eintrittswahrscheinlichkeit, t – zeitliche Komponente). Liegt R_t unterhalb einer bestimmten Grenze (R_{max}), gilt das Risiko als tragbar; liegt sein Wert oberhalb dieser Grenze, ist das Risiko nicht mehr tragbar. Diese Aussage gilt jedoch mit Einschränkungen: Nach dem oben beschriebenen Ansatz würde man ein Risiko R_1 nicht behalten, wenn $R_1 \geq R_2$ und $R_2 > R_{max}$ wäre.

Laut der in der Tabelle 1 abgebildeten Risikobewertung ist die absolute Risikohöhe als Produkt aus H und P nicht das einzige Entscheidungskriterium für die Tragbarkeit des Risikos. So wird z. B. $R_{1;5} = 5$ als nicht tragbar bewertet, obwohl $R_{2;3} = 6$ ($R_{2;3} > R_{1;5}$) als tragbar gilt. Somit werden Risiken mit einem höheren R-Wert gegenüber Risiken mit niedrigeren R-Werten bevorzugt. Der Grund liegt darin, dass man Risiken mit einem sehr hohen Schadenspotenzial trotz der niedrigen Eintrittswahrscheinlichkeit bzw. Risiken mit einem kleinen Schadenspotenzial und einer sehr hohen Eintrittswahrscheinlichkeit (bzw. Eintrittshäufigkeit) nicht eingehen möchte.

Wenn man die Inhalte der Tabelle 1 in ein Koordinatensystem überträgt, erhält man die Abbildung 9a. Abbildung 9b erhält man durch die Verfeinerung der Rasterung. Ein

[18]Die in der Tabelle 1 abgebildete Beispiel-Risikomatrix ist an die Risikobewertung in den Datenschutzkonzepten mehrerer Forschungsnetze angelehnt. Als Schäden mit hohem Potenzial werden beispielsweise in [HWE05] Systeminfiltration, vorsätzliche Beschädigung, menschliche Fehler und Fehlfunktionen der beiden Datenbanksysteme (hier *IDAT* und *MDAT*) eingestuft. Als ebenfalls kritisch wird die Tätigkeit der beiden Datenbankadministratoren angesehen, ein Thema, welches im Abschnitt 3.3.2 „Personale Aspekte für den Betrieb von Forschungsnetzen“ behandelt wird. Am gefährlichsten gelten dabei menschliche Fehler, da diese Einfluss auf Vertraulichkeit, Integrität und Verfügbarkeit haben können. Im Konzept selbst greift man auf die Hinweise zur Risikoanalyse des Hamburgischen Datenschutzbeauftragten und an die Risikoanalysenempfehlungen des BSI zurück. Die aktualisierten Hinweise zur Risikoanalyse und Vorabkontrolle des Hamburgischen Datenschutzbeauftragten Sebastian Wirth sind unter [Wir08] verfügbar, die aktuellen Risikoanalyseempfehlungen des BSI befinden sich unter [bsi08b].

Körper K symbolisiert dabei die Menge der als tragbar bewerteten Risiken ($R_{H;P} \in R_{tragbar}$ genau dann, wenn $R_{H;P} \in K$); H_{max} und P_{max} sind die Grenzen für die maximale als tragbar geltende Schadenshöhe bzw. höchste akzeptable Eintrittswahrscheinlichkeit für Schadensereignisse. Die beiden Limits werden durch die Linien a und b dargestellt, die parallel zu den jeweiligen Koordinatenachsen verlaufen. Risiken (Punkte der Ebene), die nahe an dem Koordinatenursprung liegen, zeichnen sich durch relativ geringe Schadenshöhe und niedrige Eintrittswahrscheinlichkeit aus; Risiken in der Nähe der Linien a, b und der Funktion $f(H;P)$ bergen dagegen größeres Risikopotenzial in sich. An dieser Stelle muss darauf hingewiesen werden, dass $f(H;P)$ keine lineare Funktion sein muss, tatsächlich muss es sich bei $f(H;P)$ nicht einmal um eine Funktion handeln. Auch die Annahme, dass sich die Menge tragbarer Risiken in Form eines einzigen Körpers darstellen lässt, ist nicht richtig. Tatsächlich kann es sich um mehrere disjunkte Körper handeln. Die gewählte Form einer Geraden ist eine Vereinfachung, die aufgrund des Aufbaus der Risikomatrix gewählt wurde. Realistischer an der Stelle wäre ein logarithmus- bzw. hyperbel- oder kreisförmiger Aufbau (vgl. [CD09, S. 92]).

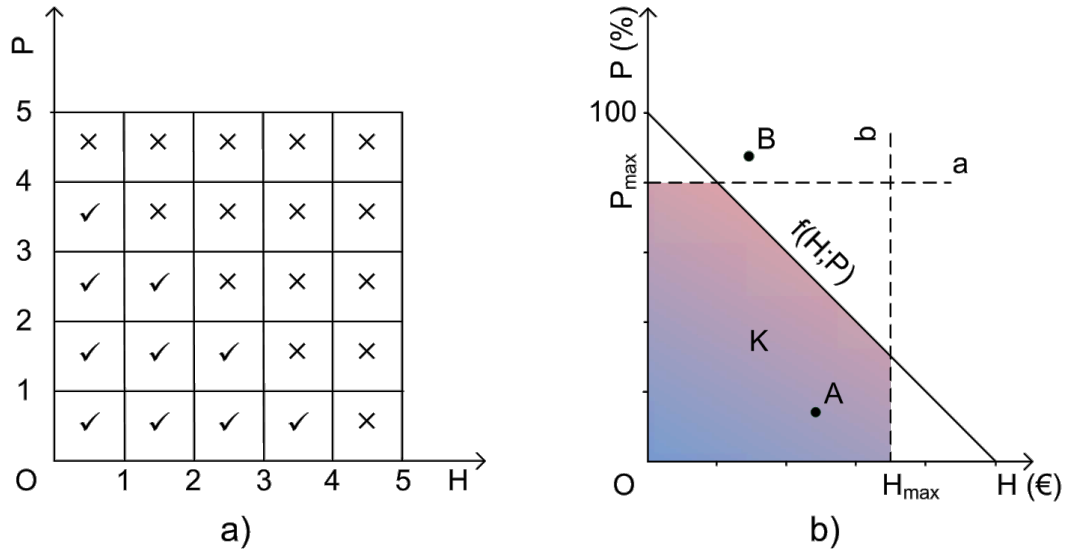

Abbildung 9.: Tragbarkeit eines Risikos: Abbildung 9a entsteht durch die Übertragung der Risikobewertungsmatrix in ein Koordinatensystem; Abbildung 9b kommt durch eine verfeinerte Rasterung zustande. Körper K symbolisiert die Menge aller tragbaren Risiken.

Der Risikobewertungsansatz $R_t = H_t \times P_t$ zeichnet sich aus durch seine bedingte Anpassungsfähigkeit an die Änderung der Bedrohungssituation. So kann die Höhe eines Schadens kaum aktiv beeinflusst werden. Die Wahrscheinlichkeit des Schadenseintritts ist eine i. d. R. empirisch ermittelte subjektive Größe. Eine solche Bewertung der Risikosituation hilft zwar bei der Einschätzung der Risikotragbarkeit, ist aber wenig hilfreich bei der Beurteilung, welche Maßnahmen sinnvoll sind, um die Risikostruktur eines Forschungsnetzes zu optimieren.

Der Begriff des „Nettorisikos“ erlaubt hierfür eine detailliertere Betrachtung. Unter dem

Nettorisiko versteht man das Produkt aus dem potenziellen Schaden eines Angriffs,[19] der empirisch ermittelten Wahrscheinlichkeit des Schadenseintritts und dem Schwachstellenpotenzial (vgl. [Mül11, S. 114 f.]). Das Schwachstellenpotenzial kann als Bewertung des Wirkungsgrades von Sicherheitsmaßnahmen verstanden werden. Die Definition des Risikos wird somit um eine zusätzliche Dimension ergänzt. Wenn man die in der Abbildung 9a visualisierte Risikobewertungsmatrix um eine Dimension erweitert, entsteht die Abbildung 10a. In der Ausgangsform ist die Größe S (Schwachstellenpotenzial) konstant und beträgt 100 Prozent. Überträgt man die zusätzliche Dimension auf die Abbildung 9b, erhält man ein dreidimensionales Gebilde (Abbildung 10b). Aus einem Punkt der Ebene $E_{H;P}$ (Risiko) wird ein Einheitsvektor, dessen Ursprung stets auf der Ebene $E_{H;P}$ liegt, und der parallel zu der S-Achse verläuft.[20] Die Länge eines solchen Vektors kann nun durch das Einleiten von sicherheitsrelevanten Maßnahmen ($m \in M$) reduziert werden ($|m(r_1\vec{r}_2)| \leq |r_1\vec{r}_2|$; $|r_1\vec{r}_2| \leq 100$). Die Tragbarkeit eines Risikos kann somit auf die Frage zurückgeführt werden, ob sämtliche Punkte des Risikovektors $r_1\vec{r}_2$ innerhalb des Körpers K liegen. Sollte ein Teil des Vektors $r_3\vec{r}_4$ außerhalb des Körpers K liegen, kann dies durch die Änderung des Parameters S korrigiert werden. Dadurch wird r_4 (das Ende des Vektors) entlang der S-Achse in Richtung des Vektoranfangs r_3 verschoben. Die Größe des Koeffizienten S gibt Aufschluss über die Höhe der Aufwände, die notwendig sind, um ein im Umfang geändertes Risiko wieder unter Kontrolle zu bringen.

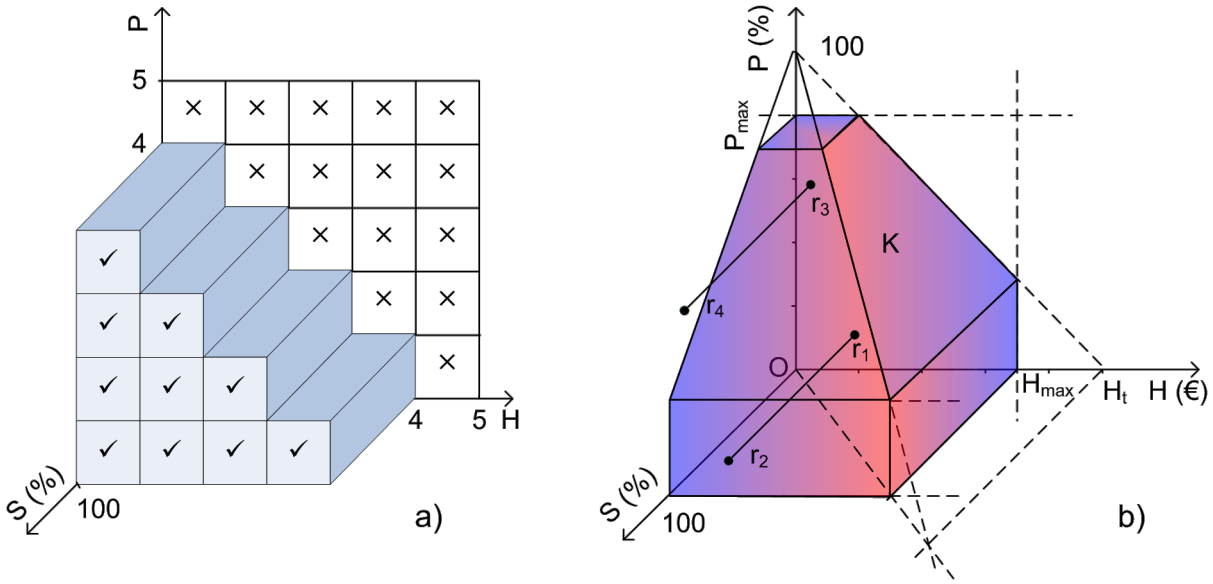

Abbildung 10.: Erweiterung des Risikobegriffs: Abbildung 10a entsteht durch die Ergänzung der Risikobewertungsmatrix aus der Abbildung 9a um eine weitere Dimension (Schwachstellenpotenzial). Das dreidimensionale Gebilde 10b entsteht durch die Übertragung dieser zusätzlichen Dimension auf die Abbildung 9b.

Die Herstellung eines monetären Zusammenhangs zwischen den risikospezifischen Koeffizienten S_r und den Investitionen in die Informationssicherheitsarchitektur könnte

[19] Dieser Wert wird ohne Berücksichtigung der Schutzmaßnahmen errechnet.

[20] Der Ursprung des Vektors hat die Form $(p_1, h_1, 0)$.

als Optimierungsansatz für das Sicherheitsportfolio eines Forschungsnetzes bei einem fixen Sicherheitsbudget dienen. So könnte man beispielsweise versuchen, die Summe der Abstände zwischen den Endpunkten der Risikovektoren und dem Koordinatenursprung (siehe Abbildung 11) zu minimieren: $\sum_{i=1}^{n} |O;\vec{r}_n|;\ n = 2 \times i, i \in \mathbb{N}\backslash\{0\}$. Eine solche Aufgabenstellung kann auf das bekannte Rucksackproblem zurückgeführt werden. Die Auswahl einer optimalen Kombination aus verfügbaren Sicherheitsmaßnahmen wird in der aktuellen Sicherheitsforschung aktiv untersucht. Neben dem eine hohe Berechnungskomplexität aufweisenden Brute-Force-Ansatz werden in diesem Zusammenhang beispielsweise dynamische Programmierung und evolutionäre Algorithmen angewendet (vgl. [KK11]).
Auch die Anwendung von anderen akzeptierten Bewertungs- und Prognosemodellen wird mit dem Ansatz möglich. In der Wirtschaft werden z. B. das DFA-Modell (Dynamic Financial Analysis bzw. Dynamische Finanzanalyse der Versicherungswirtschaft) und das VaR-Modell[21] (Value at Risk) zur Bewertung des Risikoportfolios eingesetzt (vgl. [GDH+10]). Eine vereinfachte Abwandlung eines dieser Modelle könnte für diesen Zweck adaptiert werden.

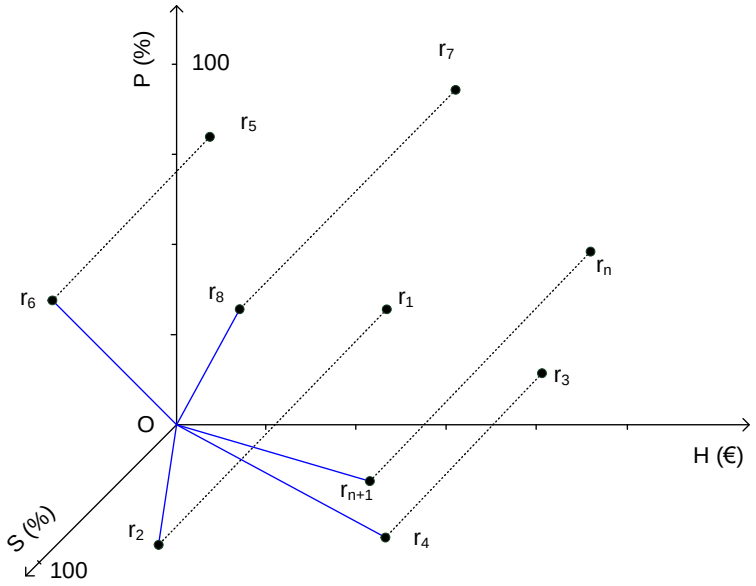

Abbildung 11.: Optimierung des Risikoportfolios: Ein möglicher Ansatz für die Optimierung des Risikoportfolios besteht in der Minimierung der Summe der Abstände zwischen den Endpunkten der Risikovektoren und dem Koordinatenursprung ($\sum_{i=1}^{n} |O;\vec{r}_n|;\ n = 2 \times i, i \in \mathbb{N}\backslash\{0\}$).

Besonders interessant wird das Konzept, wenn man auf eine gemeinsame unabhängige Bewertungsbasis für die Höhe der Schäden und deren Eintrittswahrscheinlichkeit zurückgreifen

[21] Die Eignung des VaR-Ansatzes für die Optimierung des Risikopotenzials müsste kritisch hinterfragt werden, denn die Risiken, die über einem bestimmten Konfidenzniveau liegen, blieben beim VaR-Ansatz unberücksichtigt. Die bereits erwähnten Risiken mit einem sehr hohen Schadenspotenzial und einer geringen Eintrittswahrscheinlichkeit würden in die Bewertung des Risikomanagements nicht einfließen.

kann.[22] Für diese Aufgabe können beispielsweise die zentral verwalteten Gefährdungen mit den im Abschnitt A.3 vorgenommenen Bewertungen der Bedeutung von Sicherheitskriterien einzelner Forschungsnetzdienste verknüpft werden. Dadurch kann jedes medizinische Forschungsnetz den Einfluss einzelner Maßnahmen auf die Einhaltung der Kriterien Authentizität, Integrität, Konformität, Robustheit, Verbindlichkeit, Verfügbarkeit und Vertraulichkeit durch die einzelnen Dienste und Komponenten prüfen. Ein standardisierter Bewertungsmaßstab der Wirksamkeit von Sicherheitsmaßnahmen für spezifische Risiken ($|m(r_n\vec{r_{n+1}})|$) würde die Objektivität der Bewertung verstärken. Um die Aussagekraft der Berechnungen zu gewährleisten, müssten die Ausgangsdaten auf ihre Konsistenz, Korrektheit, Genauigkeit und Relevanz getestet werden. Eine Reihe bereits existierender Risikokataloge zur Bewertung von IT-Bedrohungen kann für diesen Zweck angepasst und eingesetzt werden. Eine der zahlreichen Möglichkeiten dafür ist der offene Standard CVSS, der zur Meldung sowie Relevanz- und Risikoeinschätzung von Malware-Bedrohungen eingesetzt wird (vgl. [nis12]) oder beispielsweise CRAMM (s. a. Abschnitt A.1.6.3). Im nächsten Abschnitt werden die in Deutschland zu den Standardwerken der Informationssicherheit zählenden BSI IT-Grundschutz-Kataloge [bsi11d] mit dem Basiskonzept „dynSRM“ kombiniert und für die Bestimmung von Gefährdungs- und Schutzszenarien verwendet.

4.4.2. Anwendung des Basiskonzeptes „dynSRM“ auf der Grundlage von BSI IT-Grundschutz-Katalogen

Die BSI IT-Grundschutz-Kataloge sind in Bausteine gegliedert; am Ende eines Bausteines erfolgt eine Gegenüberstellung der Gefährdungen und der dagegen gültigen Sicherheitsmaßnahmen (s. a. Abschnitt A.1.5 „BSI IT-Grundschutz“). Die Tabelle 2 als ein Auszug aus dem BSI IT-Grundschutz-Baustein B 1.6 „Schutz vor Schadsoftware“ veranschaulicht eine solche Gegenüberstellung in Form einer Matrix. Die aufgezeigten Beispielgefährdungen setzen sich aus drei Kategorien zusammen: den organisatorischen Mängeln, dem technischen Versagen und den vorsätzlichen Handlungen. Für das abgebildete Beispiel wurden aus jeder dieser drei Kategorien jeweils zwei Gefährdungen[23] ausgesucht. Die zweite Dimension der Matrix belegen die Sicherheitsmaßnahmen, die sich im Beispiel auf die Maßnahmenkataloge M2 „Organisation“, M3 „Personal“, M4 „Hard- und Software“ und M6 „Notfallvorsorge“ verteilen. Die Tabelle veranschaulicht, dass die organisatorische Maßnahme M 2.154 „Erstellung eines Sicherheitskonzeptes gegen Schadprogramme„ für die Gefährdungen

[22] Zum Beispiel entsprechen 100 ausgespähte Datensätze von nicht prominenten Personen einem Schaden in Höhe von $X(EUR) \times f$, f – Risikofaktor eines Forschungsnetzes, der Datensensibilität etc. Als Grundlage für die Ermittlung der Werte können Ergebnisse der Studien zu den Kosten als Folge des Datenverlusts oder -diebstahls von Daten wie beispielsweise [pon11] verwendet werden. Auch eine Vergabe von Punktwerten in Abhängigkeit von der Art und der Anszahl gespeicherter Datensätze ist in diesem Zusammenhang möglich.

[23] G 2.4 bis G 5.71.

G 2.4 „Unzureichende Kontrolle der Sicherheitsmaßnahmen“ und G 2.8 „Unkontrollierter Einsatz von Betriebsmitteln“ wirksam ist. Die Personalmaßnahme M 3.69 „Einführung in die Bedrohung durch Schadprogramme“ ist dagegen bei keiner der im Beispiel aufgelisteten Bedrohungen wirksam.

Die Dynamik-Eigenschaft des Konzeptes „dynSRM“ kann mithilfe von BSI IT-Grundschutz-Katalogen wie folgt verdeutlicht werden: Da die Informationstechnik schnelllebig ist und sich permanent weiterentwickelt, werden die IT-Grundschutz-Kataloge ständig aktualisiert und um neue Themen erweitert. Im Rahmen der Aktualisierung werden beispielsweise die Gefährdungen und die Schutzmaßnahmen hinzugefügt, durch neue Informationen ergänzt oder aus den Katalogen entfernt. Auch die Informationen über die Wechselwirkungen von Maßnahmen und Gefährdungen werden auf den neuesten Stand gebracht. Die sich ständig aktualisierenden Angriffsmethoden erfordern eine Anpassung der Verteidigungsmaßnahmen; die neuen praktischen Erfahrungen über die Wirksamkeit des Schutzes gegen bestimmte Gefährdungen bedingen eine Neubewertung ihrer Effektivität. Dienen die BSI IT-Grundschutz-Kataloge als Ausgangsbasis für die Risikovektoren und die Sicherheitsmaßnahmen, bewirkt ihre Aktualisierung eine Änderung der Bewertung des individuellen Sicherheits- und Risikoportfolios.

B 1.6 Schutz vor Schadprogrammen		M 2 Organisation							M 3 Personal	M 4 HW und SW		M 6 Notfall-vorsorge		
		M 2.34	M 2.154	M 2.157	M 2.158	M 2.159	M 2.160	M 2.224	M 3.69	M 4.3	M 4.84	M 6.23	M 6.24	M 6.32
G 2 Organisatorische Mängel	G 2.4 Unzureichende Kontrolle der Sicherheitsmaßnahmen		x				x					x		
	G 2.8 Unkontrollierter Einsatz von Betriebsmitteln		x	x		x	x			x	x	x		x
G4 Technisches Versagen	G 4.13 Verlust gespeicherter Daten			x	x	x	x	x		x	x	x	x	x
	G 4.22 Software-Schwachstellen oder -Fehler													
G 5 Vorsätzliche Handlungen	G 5.2 Manipulation an Informationen oder Software			x		x		x						
	G 5.71 Vertraulichkeitsverlust schützenswerter Informationen			x	x	x	x	x		x	x	x		

M 2.34 Dokumentation der Veränderungen an einem bestehenden System	M 3.69 Einführung in die Bedrohung durch Schadprogramme
M 2.154 Erstellung eines Sicherheitskonzeptes gegen Schadprogramme	M 4.3 Einsatz von Viren-Schutzprogrammen
M 2.157 Auswahl eines geeigneten Viren-Schutzprogramms	M 4.84 Nutzung der BIOS-Sicherheitsmechanismen
M 2.158 Meldung von Schadprogramm-Infektionen	M 6.23 Verhaltensregeln bei Auftreten von Schadprogrammen
M 2.159 Aktualisierung der eingesetzten Viren-Schutzprogramme und Signaturen	M 6.24 Erstellen eines Notfall-Bootmediums
M 2.160 Regelungen zum Schutz vor Schadprogrammen	M 6.32 Regelmäßige Datensicherung
M 2.224 Vorbeugung gegen Schadprogramme	

Tabelle 2.: Auszug aus dem BSI IT-Grundschutz-Baustein B 1.6 „Schutz vor Schadprogrammen“: Die Gefährdungen und Sicherheitsmaßnahmen werden in den BSI-Bausteinen gegenübergestellt. Durch die Matrix-Form wird verdeutlicht, welchen Gefährdungen durch welche Sicherheitsmaßnahmen begegnet werden kann.

Um das Prinzip des dynamischen Risikomanagements mithilfe der BSI IT-Grundschutz-Kataloge zu veranschaulichen, werden im Folgenden einige Modellannahmen getroffen, die insbesondere die Ausgangssituation eines fiktiven Risikoportfolios, das aus den sechs aufgelisteten Gefährdungen besteht, und die Wirksamkeit der Sicherheitsmaßnahmen M 2.34 bis M 6.32 in Bezug auf die Gefährdungen betrifft:

$$\vec{r} \in R, R\text{- Risikoportfolio}$$
$$\vec{r} \Leftrightarrow \vec{AB},\ A(h,p,0),\ B(h,p,s),\ h,p,s \in \mathbb{R}^+,\ h \geq 0,\ 0 \leq p \leq 100,\ 0 \leq s \leq 100$$
$$\text{Ausgangslage: } \forall \vec{AB} \in R,\ A(h,p,0),\ B(h,p,100)$$
$$\text{Maßnahmen: } m \in M, M\text{-Maßnahmenkatalog}$$
$$m(\vec{AB}) \rightarrow (\vec{AB_1}),\ B_1(h,p,m(s)),\ m(s) = \frac{1}{2}s,\ \text{Kosten: } k,\ k(m) = 1,\ \forall m \in M$$
$$\text{Güte des Risikoportfolios: } G(R) : \sum_{1}^{n} \left|\vec{OB_n}\right|, n \in \mathbb{N}\backslash\{0\}$$
$$\text{Berechnungsformel: } \left|\vec{OB}\right| = \sqrt{h^2 + p^2 + s^2}$$

Tabelle 3 illustriert die Ausgangslage eines fiktiven Risikoportfolioszenarios, das im Folgenden mithilfe der Sicherheitsmaßnahmen modifiziert wird. Sechs Gefährdungen aus drei Gefährdungskategorien kann mithilfe der Sicherheitsmaßnahmen M 2.34 bis M 6.32 begegnet werden. Jede Sicherheitsmaßnahme kann höchstens ein einzelnes Mal angewendet werden. Aus Vereinfachungsgründen wird nicht zwischen der vollständigen und unvollständigen Implementierung von Sicherheitsmaßnahmen unterschieden; außerdem erfolgt keine Unterscheidung der Maßnahmenkosten. Das Ziel besteht in der Optimierung der Güte des Risikoportfolios für die Anwendung von zwei Sicherheitsmaßnahmen unter den gegebenen Modellannahmen.

	H	P (%)	S	$\|OB\|$
G 2.4	10	50	100	112
G 2.8	20	50	100	114
G 4.13	30	25	100	107
G 4.22	40	25	100	111
G 5.2	50	12,5	100	113
G 5.71	60	12,5	100	117
			G(R)	674

Tabelle 3.: Ausgangslage eines Risikoportfolioszenarios: Das fiktive Risikoportfolio berücksichtigt sechs Gefährdungsszenarien, die jeweils mit der Schadenshöhe H und der allgemeinen Eintrittswahrscheinlichkeit p geschätzt werden. Es wird angenommen, dass im Ausgangszustand keine Sicherheitsmaßnahmen implementiert sind, sodass das Schadenspotenzial S 100% beträgt. Der Abstand zwischen dem Ende eines Risikovektors und dem Koordinatenursprung wird als $|OB|$ gekennzeichnet.

Im Ausgangszustand beträgt die Güte des Risikoportfolios $G(R_0) = 674$. Die anschließende Anwendung der Maßnahme $M2.34$ auf $G(R_0)$ ($G(M2.34(R_0)) = G(R_0)$) bewirkt keine Änderung der Gefährdungslage, da die Maßnahme im Hinblick auf keine der Gefährdungen

Wirkung zeigt. Die Anwendung der Maßnahme $M2.154$ reduziert die Gefährdungslage auf einen Wert von 593: $G(M2.154(R_0)) = 593$. Die Auswirkung weiterer Maßnahmen auf die Güte des Risikoportfolios kann analog geprüft werden, um eine optimale Kombination von Sicherheitsmaßnahmen zu ermitteln. Die Abbildung 12 veranschaulicht das beschriebene Prinzip.

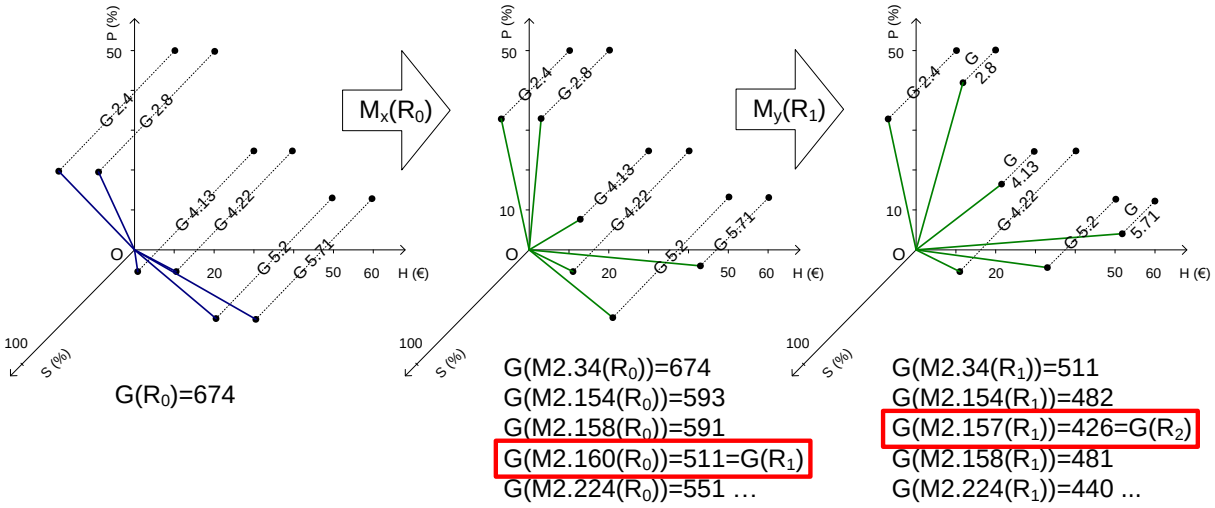

Abbildung 12.: Änderung der Güte des Risikoportfolios bei Anwendung von Sicherheitsmaßnahmen: In Abhängigkeit von der Auswahl angewendeter Sicherheitsmaßnahmen ändert sich der Zustand des Risikoportfolios. Im Ausgangszustand hat $G(R_0)$ einen Wert von 674. Die Anwendung der Sicherheitsmaßnahme M2.160 ($M2.160(R_0)$) verbessert den Wert auf 511. Die Anwendung der Maßnahme M2.157 bewirkt weitere Verbesserung des Risikoportfolios: $G(M2.157(M2.160(R_0))) = G(M2.157(R_1)) = G(R_2) = 426$.

4.4.3. Prototypische Implementierung einer quantitativen dynamischen Risikoportfolioberechnung mithilfe von dynSRM

Im Rahmen dieser Arbeit wurde auf der Basis des „dynSRM“-Konzeptes ein Prototyp entwickelt, mit dessen Hilfe ein Risikoportfolio und dessen Änderungen nach der Anwendung von Sicherheitsmaßnahmen bequem simuliert werden können. Die prototypische Implementierung erfolgte in der Programmiersprache Java; das UML-Klassendiagramm des Prototyps ist in der Abbildung 13 dargestellt.

Beim Aufruf der Main-Methode der Klasse PortfolioCalculator wird das beschriebene Modell, bestehend aus Risikovektoren und Sicherheitsmaßnahmen, initialisiert. Dies erfolgt durch das Einlesen von zwei XML-Dateien mit Informationen zu den Risiken und Sicherheitsmaßnahmen, die wie folgt aufgebaut sind:

```
<?xml version="1.0" encoding="UTF-8" ?>
 <RiskVectors>
  <RiskVector>
  <Risk_ID>G2.4</Risk_ID>
  <Risk_Name>Unzureichende Kontrolle der Sicherheitsmaßnahmen</Risk_Name>
  <Risk_H>10</Risk_H>
  <Risk_p>50</Risk_p>
```

```
  <Risk_S>100</Risk_S>
  </RiskVector>
  ...
 </RiskVectors>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<SecurityMeasures>
 <SecurityMeasure>
        <SecurityMeasure_ID>M2.154</SecurityMeasure_ID>
        <SecurityMeasure_Name>Erstellung eines Sicherheitskonzeptes
         gegen Schadprogramme</SecurityMeasure_Name>
        <lMitigatedRisks>G2.4;G2.8</lMitigatedRisks>
        <SecurityMeasure_Costs>1</SecurityMeasure_Costs>
        <SecurityMeasureApplied>false</SecurityMeasureApplied>
 </SecurityMeasure>
  ...
</SecurityMeasures>
```

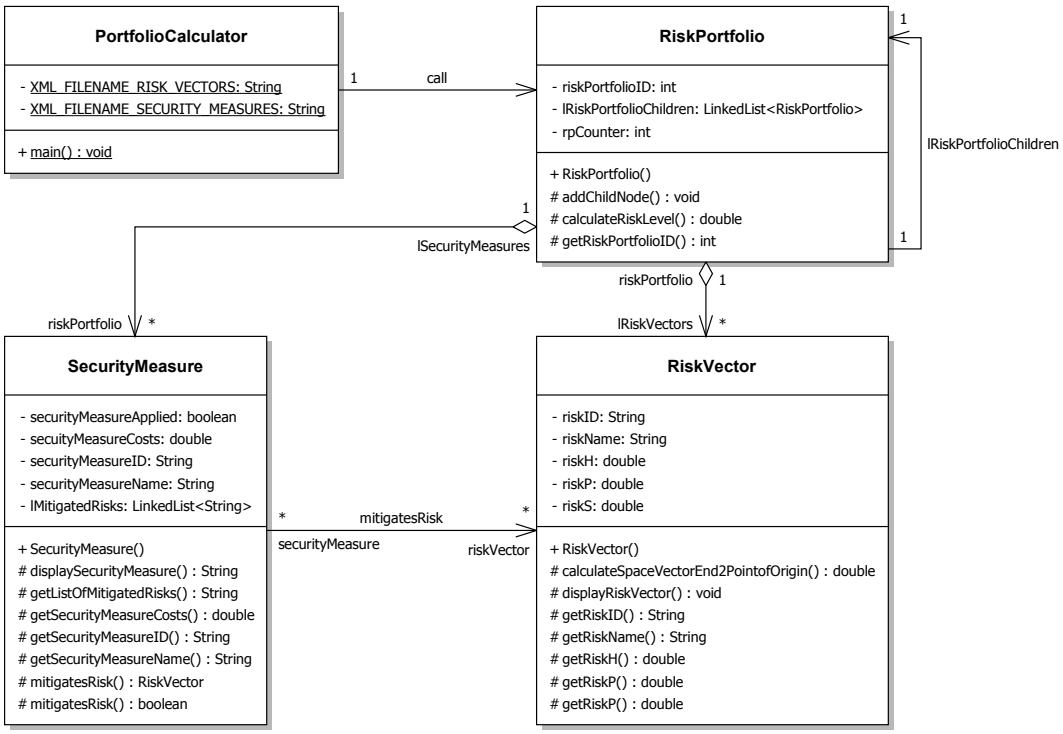

Abbildung 13.: Aufbau des Prototyps zur dynamischen Risikoportfolioberechnung als UML-Klassendiagramm: Die Veränderung des Risikoportfolios in Abhängigkeit von den angewendeten Sicherheitsmaßnahmen wird durch den rekursiven Konstruktor-Aufruf der Klasse RiskPortfolio in einer Baumstruktur festgehalten. Der dadurch entstandene Baum wird anschließend traversiert, um die Güte des Risikoportfolios für jeden Baumknoten zu berechnen.

Der Benutzer wird nun aufgefordert, die Anzahl der durchzuführenden Sicherheitsmaßnahmen einzugeben. Als maximal zulässige Eingabe gilt die Gesamtanzahl der möglichen Sicherheitsmaßnahmen minus eins. Nach der Eingabe gibt das Programm die möglichen Kombinationen der Maßnahmen aus und berechnet die erwartete Güte des Risikoportfolios als $G(R_x)$. Die Abbildung 14 zeigt einen Teilausschnitt der Ausgabe des Prototyps für die Auswahl von drei Sicherheitsmaßnahmen.

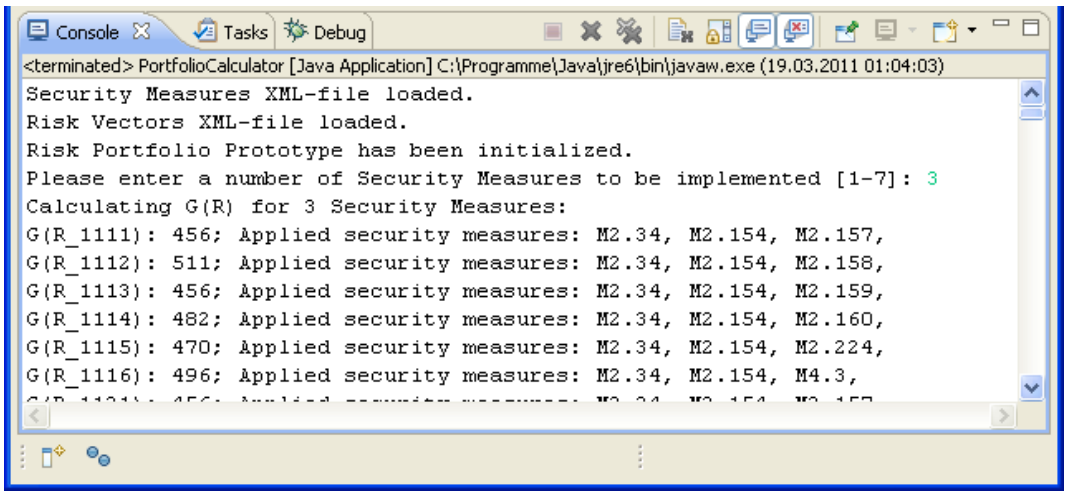

Abbildung 14.: Ausgabe des Prototyps zur Risikoportfolioberechnung: Der Prototyp initialisiert das Risikoportfolio, indem zwei XML-Dateien mit Risiken und Sicherheitsmaßnahmen eingelesen werden. Dadurch kann das Sicherheitsportfolio frei konfiguriert werden. Nachdem der Benutzer die Anzahl der Sicherheitsmaßnahmen eingegeben hat, erfolgt die Berechnung der Güte des Risikoportfolios $G(R_x)$ für unterschiedliche Maßnahmenkombinationen.

4.5. Zusammenfassung des Kapitels

In diesem Kapitel wurden die Themen Sicherheits- und Risikopolitik und Schutzbedarfsermittlung als Aspekte des Sicherheits- und Risikomanagements behandelt. Vor allem wurde die Bedeutung einer einheitlichen Risikopolitik dargelegt. Aufbauend auf der Sicherheits- und Risikopolitik wurde ein Vorschlag zur Ermittlung der kritischen Bereiche/Vorgänge in einer Forschungsnetzinfrastruktur unterbreitet, und die wichtigsten Forschungsnetzdienste wurden auf ihre Kritikalität untersucht. Anschließend erfolgte eine Auseinandersetzung mit der Struktur der Angreifer und ihren Motiven. Es wurde ein neuartiges Konzept des dynamischen Sicherheits- und Risikomanagements „dynSRM“ entwickelt, das die Objektivierung der Entscheidung für oder gegen eine Sicherheitsinvestition ermöglicht. Eine, auf dem BSI IT-Grundschutz-Katalogen basierende prototypische Implementierung untermauerte die praktische Umsetzbarkeit des Konzeptes.
Die Objektivität der Wirksamkeitsbewertung von Sicherheitsmaßnahmen wird erreicht durch die Berücksichtigung des Risikoportfolios, das sich aus organisationsneutralen und organisationsspezifischen Komponenten zusammensetzt und den Vergleich der potenziellen Auswirkungen der Sicherheitsmaßnahmen auf das Sicherheitsniveau eines Forschungsnetzes ermöglicht. Das Konzept des dynamischen Sicherheits- und Risikomanagements „dynSRM“ ermöglicht eine Verbesserung der Bewertung der Wirksamkeit von Sicherheitsmaßnahmen und dadurch eine gezielte Steuerung der Sicherheitsarchitektur eines medizinischen Forschungsnetzes.

T2: Das Konzept des dynamischen Sicherheits- und Risikomanagements ermöglicht eine Verbesserung der Bewertung der Wirksamkeit von Sicherheitsmaßnahmen in einem medizinischen Forschungsnetz.

5. Diskussion

In diesem Kapitel erfolgt eine differenzierte Auseinandersetzung mit den Ergebnissen der Arbeit, die im Kontext der aktuellen Forschung erörtert und kritisch bewertet werden.

5.1. Bewertung des Aufbaus der Sicherheitsarchitektur für die medizinischen Forschungsnetze

Um das für die medizinischen Forschungsnetze erforderliche Sicherheitsniveau zu gewährleisten, wird ein Sicherheitskonzept benötigt, das organisatorische, administrative und technische Schutzkomponenten berücksichtigt. Viele Angriffe[1] nutzen die erwünschte ordnungsgemäße Funktion von Systemen bzw. Prozessen aus, sodass nur eine Kombination der drei genannten Komponenten einen sinnvollen Schutz ergibt (vgl. [KS09], [bsi08b]). Diese Dreiteilung der Sicherheitsmaßnahmen wurde im Kapitel 3 „Bestandteile der Sicherheitsarchitektur für medizinische Forschungsnetze“ umgesetzt. Das angestrebte Ziel des Kapitels war die Erzeugung von generischen plattformunabhängigen Richtlinien, die auf eine Vielzahl von Forschungsnetzinfrastrukturen angewendet werden können.

5.1.1. Organisatorische Sicherheitsrichtlinien

5.1.1.1. Rechtliche und finanzielle Absicherung

Im Abschnitt 3.3 „Organisatorische Aspekte von Sicherheitsrichtlinien“ werden u. a. Vorkehrungen wie beispielsweise die rechtliche und finanzielle Absicherung des Forschungsnetzes vorgestellt. Vielfältige Risikoauslagerungsmöglichkeiten in Form von Versicherungsverträgen werden aufgezeigt. Einige Risiken müssen aufgrund von gesetzlichen und sonstigen Bestimmungen (wie z. B. Probandenversicherung bei der Durchführung von klinischen Studien nach dem Arzneimittel- und dem Medizinproduktgesetz) pflichtversichert werden. Bei vielen Versicherungsprodukten besteht jedoch keine Pflicht, es handelt sich also um eine für das Forschungsnetz fakultative Versicherung, bei der es die Kosten und den Nutzen eines Versicherungsvertrags gegenüberzustellen gilt. Mehrere Versicherungsgesellschaften bieten bereits jetzt die sogenannten Cyberinsurance-Verträge mit den Deckungssummen bis zu 50 Millionen USD an. Die momentan eher verhaltene Reaktion des Marktes auf das Angebot

[1] Insbesondere aus dem Bereich „Social-Engineering“.

kann sich schlagartig ändern, wenn der Abschluss der Cyberversicherungen als Pflicht gesetzlich verankert werden sollte (vgl. [BP07, S. 52. f.]). Die in den Abschnitten 4.3.1 und 4.3.2 durchgeführten Analysen können als eine Bewertungsbasis für die Optimierung des Risikoportfolios eines Forschungsnetzes bei der Entscheidung für oder gegen den Abschluss von Versicherungsverträgen dienen. Da die Versicherungen in erster Linie die Minimierung des eigenen Risikos anstreben, knüpfen sie ihre Deckungszusagen an die Implementierung möglichst vollständiger Sicherheitsmaßnahmenkataloge gegen alle erdenklichen Gefahren. Aus diesem Grund sind Versicherungen als Teil der Risikotransferstrategie nicht als das Allheilmittel, sondern als Ergänzung des Sicherheitsmaßnahmenportfolios zu verstehen (vgl. [Böh10]).

5.1.1.2. Personalmanagement

Im Abschnitt 3.3.2 „Personale Aspekte für den Betrieb von Forschungsnetzen“ erfolgt die Analyse der Sicherheitsmaßnahmen in einem der sicherheitstechnisch wichtigsten Bereiche einer Organisation: dem Personalmanagement. Die zu berücksichtigenden Merkmale der Personalplanung, -beschaffung, -einarbeitung, -weiterentwicklung und -trennung werden erläutert. Das Personalmanagement in medizinischen Einrichtungen und insbesondere im Forschungsbereich weist eine Reihe von Besonderheiten auf, die bei der Planung von Sicherheitsmaßnahmen berücksichtigt werden müssen. So muss der Personalbeschaffung aufgrund hoher Fluktuation, den befristeten Arbeitsverträgen und den ungenügenden finanziellen Mitteln für die Mitarbeiterschulungen eine besondere Bedeutung beigemessen werden (vgl. [WB09]).
Die in der Arbeit vorgestellten Aspekte des Personalmanagements müssen im Falle eines konkreten Forschungsnetzes wesentlich detaillierter untersucht werden. Vor allem die Konformität im Hinblick auf die geltende Gesetzgebung muss geprüft werden. So ist beispielsweise die für die Personalbeschaffung unterbreitete Empfehlung, die Auskünfte über die Vermögensverhältnisse des Bewerbers einzuholen, in vielen Fällen nicht rechtmäßig. Auch die Rechtmäßigkeit der Einholung eines Führungszeugnisses ist arbeitsrechtlich zu hinterfragen. Das vorgeschlagene Einholen von Referenzen beim aktuellen Arbeitgeber kann von einigen Bewerbern als negativ empfunden werden.
Trotz diverser noch zu klärender Fragen kann bereits die Einhaltung einiger weniger Grundregeln des Personalmanagementprozesses das Sicherheitsniveau deutlich erhöhen. Insbesondere die Personalsensibilisierung für die datenschutz- und die sicherheitsrelevanten Fragestellungen bedarf weiterer Untersuchungen. Erfahrungen zeigen, dass das Missachten bzw. Unterlassen von Sicherheitsmaßnahmen durch das Personal nicht allein durch die Schulungen in Verbindung mit technischen Unterstützungsmaßnahmen zu verhindern ist. Die Personalmanagementmaßnahmen müssen eine Reihe von intrinsischen und extrinsischen Faktoren berücksichtigen, um nicht nur das Sicherheitsbewusstsein des Personals zu wecken, sondern um auch die bewussten Sicherheitsfehlhandlungen effektiv zu verhindern (vgl. [WBS08]).

5.1.1.3. Notfallplanung

In den Abschnitten 3.3.3 „Organisation und Gestaltung von Notfallvorsorgemaßnahmen“ und 3.3.4 „Wiederaufnahme des Betriebs“ werden die als Vorbereitung auf den Ernstfall dienenden organisatorischen Maßnahmen vorgestellt. Durch diese Maßnahmen soll der Wiederherstellungsaufwand in einem Schadensszenario reduziert werden. Die vorgeschlagenen Maßnahmen beinhalten die Einrichtung eines Notuser-Verfahrens und die Durchführung von Notfallsimulationen. Auch den Soft- und Hardwareausfällen soll mit der Verfügbarkeit einer Notfalldokumentation sowie dem Abschluss von Verträgen mit Hardwareherstellern[2] vorgebeugt werden.
Die praktische Umsetzung der vorgeschlagenen Maßnahmen erfordert wie im Falle aller nicht wertschöpfenden Prozesse einen starken Rückhalt seitens der Forschungsnetzleitung. So zeigen die persönlichen Erfahrungen des Autors, dass alleine die wiederkehrende Vorbereitung einer Notfallsimulation mehrere Mannwochen an Aufwand erfordern kann und den Organisatoren einen hohen Kompetenzstand abverlangt. Angesichts der im Abschnitt 3.3.2 „Personale Aspekte für den Betrieb von Forschungsnetzen“ beschriebenen Probleme im Zusammenhang mit der Mitarbeiterfluktuation und dem permanenten Mangel an Personal erscheint eine konsequente Umsetzung dieser Maßnahmen im vollen Umfang als ein Wunschdenken. Synergien können für Abhilfe sorgen. So könnte beispielsweise die Verantwortung für die Planung und Durchführung von Notfallübungen von einem unabhängigen Träger übernommen werden oder in Form einer einrichtungsübergreifenden Kooperation erfolgen (vgl. [Sta09, S. 32]).
Die in den Kliniken angesiedelten Forschungsnetze können von den Notfallvorkehrungen der jeweiligen Einrichtungen profitieren. Es wäre erstrebenswert, wenn die Forschungsnetzkomponenten in den Plänen berücksichtigt würden. Die gravierendsten Probleme bestehen in der unzureichenden, nicht vorhandenen und oft nicht aktuellen Dokumentation. Für dieses Problem ist dem Autor auch keine wirksame Lösung bekannt.
Im Abschnitt 3.3.4 „Wiederaufnahme des Betriebs“ erfolgt die Auseinandersetzung mit den wichtigsten Voraussetzungen für die Wiederaufnahme des Betriebs nach einem Sicherheitsvorfall. Bei vielen Schadensszenarien ist dafür das Vorhandensein von finanziellen Mitteln notwendig. Dem steht jedoch der stark eingeschränkte finanzielle Spielraum eines Forschungsnetzes gegenüber. Insbesondere kurz nach einem Sicherheitsvorfall könnte ein Forschungsnetz in Liquiditätsprobleme geraten, die die Bewältigung des Vorfalls und eine schnelle Wiederaufnahme des Betriebs erschweren. Eine kreditbasierte Finanzierung würde mit höchster Wahrscheinlichkeit an der mangelnden Bonität des Forschungsnetzes scheitern. Auch die abgeschlossenen Versicherungsverträge beseitigen den Liquiditätsengpass nicht, denn die Zahlungen des Versicherers werden i. d. R. erst dann geleistet, wenn die Ursache und die Höhe des Schadens feststehen. Die erste Abschlagszahlung ist nicht früher als einen

[2] Die Vorratshaltung von Hardware empfiehlt sich nur in wenigen Fällen, z. B. dann, wenn die Infrastruktur mehrere gleichartige kritische Bestandteile aufweist.

Monat nach dem Melden des Vorfalls zu erwarten.[3] Die in der Wirtschaft oft anzutreffende Bildung von Rücklagen, um die erste Zeit zu überbrücken, ist bei einem Forschungsnetz kaum anwendbar. Eine mögliche Lösung bestünde in der Gründung eines Soforthilfe-Fonds, zu dem sich mehrere Forschungsnetze, Trägereinrichtungen, Sponsoren etc. zusammenschließen könnten. Alternativ können die Garantien von privaten oder öffentlichen Trägern in Erwägung gezogen werden. Dies sollte jedoch der Meinung des Autors nach zentralisiert für alle Forschungsnetze erfolgen, wofür es einer gesetzlichen bzw. politischen Initiative bedarf. Diese existiert jedoch dem Kenntnisstand des Autors nach nicht. Eine sorgfältige Prüfung der Notwendigkeit einer solchen Überbrückungsfinanzierung ist die Voraussetzung für die Planung und Gestaltung der vorgeschlagenen Notfallmaßnahmen.

5.1.1.4. Benefit Denial

Im Abschnitt 3.3.5 „Verringerung der Lukrativität eines Angriffs (Benefit Denial)“ werden einige Benefit-Denial-Maßnahmen diskutiert, deren Ziel in der Reduzierung der Lukrativität eines Angriffs besteht. Neben der konsequenten Anwendung des Minimalprinzips bei der Datensammlung und der Verwendung von robusten Watermarking-Verfahren bei Bilddaten werden auch die Vor- und Nachteile der Zusammenlegung von Daten mehrerer Forschungsnetze diskutiert.
Die geäußerten grundlegenden Bedenken der Datenschützer gegen eine gemeinsame Datenhaltung können mit der steigenden Lukrativität eines Angriffs erklärt werden (vgl. [Sok99]). Dabei muss die grundsätzliche Forderung nach der Sicherstellung des Nichtvorhandenseins von gemeinsamen Patientenindikatoren erfüllt werden (vgl. [RDSP06, S. XIV]). Die von der Datenzusammenlegung erhofften Vorteile bedürfen einer genaueren Überprüfung. Ein Vorteil der Datenzusammenlegung mehrerer Forschungsnetze könnte beispielsweise darin bestehen, dass auch beim Ausspähen der gemeinsamen *IDAT*-Datenbank die Zugehörigkeit eines Patienten zu einem Forschungsnetz und die daraus abgeleitete Bestimmung seiner Erkrankung nicht eindeutig feststellbar wären. Aus der heutigen Sicht wäre dabei nur ein eingeschränkter Nutzen zu erwarten, denn die notwendigen Voraussetzungen für eine nutzbringende Datenzusammenlegung wären in der Praxis kaum zu erfüllen.
So würde z. B. die Verschmelzung einer großen Forschungsdatenbank mit einer wesentlich kleineren die Wahrscheinlichkeit einer unerwünschten Reidentifizierung nur unwesentlich erhöhen. Doch so einfach und verlockend dieser Vorschlag in der Theorie erscheint, so problematisch kann die Auswahl der für die Datenzusammenführung sinnvollen „Kombinationsmöglichkeiten“ werden. Durch das Hinzuziehen von eventuell bekannten körperlichen

[3] Die meisten Versicherer integrieren ähnlich lautende Zahlungsklauseln in ihre Bedingungswerke: „Ist die Leistungspflicht des Versicherers dem Grunde und der Höhe nach festgestellt, hat die Auszahlung der Entschädigung binnen zwei Wochen zu erfolgen. Jedoch kann einen Monat nach Anzeige des Schadens als Abschlagszahlung der Betrag verlangt werden, der nach Lage der Sache mindestens zu zahlen ist.“

Merkmalen und weiteren Begleitinformationen[4] wären Rückschlüsse auf die Art der Erkrankung möglich (vgl. [PDKB08, S. 496]). In vielen Szenarien kann bereits das Bekanntwerden der Zugehörigkeit zu einem beliebigen Forschungsnetz durch eine unerwünschte Reidentifizierung für den Betroffenen negativ sein. So würde z. B. kaum ein Unternehmen in die Ausbildung einer jungen Führungskraft investieren, wenn die Geschäftsleitung über eine schwerwiegende Erkrankung des Mitarbeiters Bescheid wüsste. Praktisch alle durch die Forschungsnetze untersuchten Krankheiten wie Demenz, Parkinson, Schizophrenie, Depression, chronisch entzündliche Darmerkrankungen etc. wären in diesem Fall K.o.-Kriterien für weitere Investitionen in diesen Mitarbeiter. In dieser Hinsicht wäre die Datenzusammenlegung nur in begründeten Ausnahmefällen als eine sinnvolle Benefit-Denial-Maßnahme zu verstehen. In vielen Fällen wären die Auswirkungen auf das Sicherheitsniveau eher als negativ zu bewerten.

5.1.2. Administrative Sicherheitsrichtlinien

Administrative Schutzmaßnahmen begleiten kontinuierlich den Betrieb. Im Abschnitt 3.4 „Administrative Aspekte von Sicherheitsrichtlinien“ wurde u. a. die Forderung der Datenschützer nach einer strikten administrativen Trennung der *IDAT*- und *MDAT*-Datenbanken bekräftigt (vgl. [RDSP06], [PRDS05]). Zusätzlich wurden eine angemessene physikalische Absicherung der kritischen Infrastrukturbestandteile und die Durchführung von Konfigurationsveränderungen bei der strikten Einhaltung des Vier-Augen-Prinzips gefordert. Gleichzeitig wurde die Berechtigungsvergabe nach dem „Need-to-know-“ bzw. „Need-to-Access-Prinzip“ verlangt. Zusätzlich zu einer regelmäßigen Auswertung von Protokolldaten wurde außerdem die Durchführung von Querkontrollen vorgeschlagen. In sinnvollen Anwendungsfällen sollte grundsätzlich das „Vier-Augen-Prinzip“ seinen Einsatz finden.

Als ein wichtiger Bestandteil der administrativen Maßnahmen wurde das Verhalten der Netzteilnehmer beim Auftreten von Sicherheitslücken in den Bestandteilen der Forschungsnetzkonfiguration angesprochen. Dabei wurde festgestellt, dass statt einer kompromisslosen Befolgung des „Full-Disclosure“-oder des „Security through Obscurity“-Prinzips eine an die bestehenden Gegebenheiten angepasste Festlegung der internen Kommunikation sinnvoller wäre. Bei gravierenden Fehlern sollte die Abschaltung von Forschungsnetzdiensten bis zum endgültigen Abschluss der Fehleranalyse und Fehlerbehebung in Erwägung gezogen werden (vgl. [ATX08], [ANT06]).

Ein fest mit den organisatorischen Maßnahmen verbundenes Thema ist die Möglichkeit einer beschlagnahmefesten administrativen Datenunterbringung bei einem Datentreuhänder. Aufgrund der nur bedingt möglichen Aufteilung zwischen den organisatorischen und administrativen Maßnahmen in diesem Bereich wurde die Entscheidung getroffen, die

[4] Häufigkeit der Arztbesuche, auffällige körperliche Erscheinungsformen wie z. B. Zwergwuchs oder Haarausfall bei Chemotherapie etc.

Überlegungen zu diesem Themenkomplex mit den administrativen Maßnahmen zusammenzufassen.
Zum Zeitpunkt der Publikation der generischen Datenschutzkonzepte der TMF im Jahr 2006 war die Rechtmäßigkeit des Beschlagnahmeschutzes im Falle der Datenunterbringung bei einer mit der Schweigepflicht und dem Aussageverweigerungsrecht ausgestatteten Berufsgruppe nicht endgültig geklärt. Man hoffte, dass die Unterbringung der Forschungsnetzdaten z. B. bei einem Notar ausreichen würde, um diese vor Beschlagnahme zu schützen (vgl. [RDSP06], [MW02]). Man vermutete jedoch, dass der Beschlagnahmeschutz nur beim Vorliegen des Behandlungszusammenhangs Bestand habe. Im Folgenden ein Beispiel aus dem zweiten Band der TMF-Schriftenreihe „Biomaterialbanken – Rechtlichen Rahmenbedingungen“ [SPR+06, S. 3]: „ ... dass zwischen BMB und Spender nur dann ein Arzt-Patientenverhältnis besteht, wenn eine Probe zur Behandlung eines Leidens des Spenders bzw. zur Diagnosestellung entnommen wird (...) Liegt kein Behandlungszusammenhang vor und wird die Probe ausschließlich zu Forschungszwecken entnommen, so unterliegt im Wesentlichen nur die Probenentnahme als körperlicher Eingriff beim Spender dem ärztlichen Standesrecht ... die weitere Verwendung der Proben aber nicht (...) dass Zeugnisverweigerungsrechte und Beschlagnahmesicherheit *de lege lata* nur im Arzt-Patientenverhältnis bestehen ...“ Diese Rechtsauffassung bestätigt Alexander Roßnagel in seinem Rechtsgutachten zu den datenschutzrechtlichen Fragen der medizinischen Forschung (vgl. [RHJ08, S. 56 f.]). Die analoge Anwendung dieser Feststellung auf die sonstigen Datensammlungen zu Forschungszwecken würde bedeuten, dass die Forschungsnetzdaten nur solange Beschlagnahmesicherheit genießen, bis ein Behandlungszusammenhang besteht. Da bei anonymisierten Daten kein Behandlungszusammenhang bestehen kann, können diese beschlagnahmt werden. Dies würde wahrscheinlich auch für biologische Proben gelten, die trotz ihrer bedingten Anonymisierbarkeit nach dem Ablauf der Zeit, in der ein Behandlungszusammenhang vermutet werden kann, keinen Beschlagnahmeschutz genießen. Der Abschnitt schließt mit einer Beschreibung der administrativen Schritte im Falle einiger wahrscheinlicher Sicherheitsvorfälle ab. Der Schwerpunkt wird dabei auf die Reihenfolge der durchzuführenden Operationen gelegt, die für eine zügige Aufarbeitung der Vorfälle entscheidend ist. Die Liste der dargestellten Szenarien – die zwar denkbar, jedoch möglichst selten und hoffentlich nie im Forschungsnetzbetrieb auftreten werden – ist keineswegs abschließend. Die Beschreibung der empfohlenen Vorgehensweise soll dem zuständigen Personal im Rahmen der administrativen Schutzmaßnahmen bekannt gegeben werden. Die Maßnahmenkataloge sollten nach Möglichkeit kontinuierlich vervollständigt und aktualisiert werden.

5.1.3. Technische Sicherheitsrichtlinien

Im Abschnitt 3.5 „Technische Aspekte von Sicherheitsrichtlinien“ erfolgt eine Auseinandersetzung mit den Bestandteilen der Soft- und Hardwareinfrastruktur, deren sicherer

Aufbau eine unzulässige Nutzung von Forschungsnetzdiensten verhindern soll. Dieser Abschnitt bildet einen der Schwerpunkte der Arbeit. Um den Seitenumfang der Arbeit nicht zu sprengen, wurde die Darstellung der Technologiegrundlagen und einiger Aspekte der technischen Sicherheitsarchitektur in den Anhang C ausgegliedert. Es gilt zu beachten, dass die Wirksamkeit der technischen Maßnahmen sich erst durch ein Zusammenspiel mit den organisatorischen und administrativen Komponenten des Sicherheitskonzeptes entfalten kann.

5.1.3.1. Zugangsszenarien von Netzteilnehmern und sichere Arbeitsumgebung

Die Inhalte der Abschnitte 3.5.1 „Sichere Arbeitsumgebung“ und 3.5.5 „Zugangsszenarien von Netzteilnehmern zu den Forschungsnetzdiensten“ behandeln zwei unmittelbar zusammenhängende Themenbereiche. Im Mittelpunkt der untersuchten Aufgabenstellungen steht die Offenheit in Bezug auf die Erweiterung des Netzes und Sicherstellung einer vertraulichen Kommunikation bzw. einer integren Arbeitsumgebung. Eine Vielzahl einzelner Teillösungen zu diesem Themenkomplex wird präsentiert: von einer verschlüsselten VPN-Verbindung bis zu diversen Integritäts-Checkern und IDS-Modulen für die Gewährleistung eines sicheren Systemzustands. Die zu meisternde Herausforderung besteht darin, dass die Vertrauenswürdigkeit einer Arbeitsumgebung nur dann gegeben sein kann, wenn sämtliche Hard- und Softwarekomponenten eines Systems (inklusive Betriebssystem und Anwendungssoftware) eine vertrauenswürdige Kombination ergeben. Die Erfüllungskriterien für eine solche Vertrauenswürdigkeit sind jedoch nicht einheitlich und hängen von den Policies der teilnehmenden Parteien ab (vgl. [JP07]).
In der vorliegenden Arbeit wird daher die Verwendung von sogenannten Integrity Tested Network Connections bzw. Network Access Control (NAC) favorisiert. Es wird die Auffassung vertreten, dass die Entscheidung für den gewählten Ansatz der Integritätssicherstellung unter Berücksichtigung der Gegebenheiten einer Infrastruktur erfolgen muss, wobei eine softwarebasierte Standardlösung präferiert wird. Um die direkten Angriffe von den Clients auf die Applikationsserver zu vermeiden, wird außerdem der Aufbau einer Zwischenstufe in Form einer kontrollierten Lock-Down Umgebung vorgeschlagen. Die größte Herausforderung des NAC-Ansatzes besteht in der Sicherstellung der gegenseitigen Kompatibilität der einzelnen Teillösungen. Als positiv sind die Bemühungen der großen Hersteller zur Gewährleistung einer solchen Kompatibilität zu bewerten (vgl. [mic08], [cis06]).
Einer der größten Nachteile des – als eine potenzielle Lösung vorgestellten – NAC/NAP-Ansatzes besteht im erhöhten Administrationsaufwand. Insbesondere die geschilderten stark heterogenen Forschungsnetzstrukturen mit der Unmöglichkeit, die einzelnen Client-Rechner zu kontrollieren, stellen angesichts der Policies, die für alle erdenklichen Konfigurationen erstellt werden müssten, eine große Herausforderung dar. Bei einer Vielzahl solcher Policies ist davon auszugehen, dass es diverse Inkompatibilitäten geben kann. Auch die aus Kompatibilitätsgründen laufenden älteren Softwareversionen können zu Diskrepanzen

der Policies führen, was im Widerspruch zum Ziel des Ansatzes steht. Der Benutzer soll schließlich mit seinem System an einer Vielzahl von Infrastrukturen teilnehmen können und nicht für ein jedes Forschungsnetz ein separates Betriebssystem-Image bereithalten.
European Multilaterally Secure Computing Base (EMSCB) und Trusted Network Connect (TNC) sind weitere für das Forschungsnetz interessante Konzepte zur Gewährleistung einer sicheren Arbeitsumgebung. Mit EMSCB soll eine vertrauenswürdige, offene und faire Sicherheitsplattform geschaffen werden. EMSCB sieht eine virtuelle Hardwareschicht zwischen der Applikations- und der Hardwareebene vor, die als Kontrollinstanz zwischen dem Betriebssystem, sicherheitskritischen Anwendungen und der Hardware fungiert. EMSCB soll plattformunabhängig sein und die Funktionen der sogenannten Trusted Hardware verwenden können. Im Rahmen eines Open-Source-Projektes kann die für das Forschungsnetz notwendige günstige Virtualisierungsplattform entwickelt werden. Auch der die TPM-Plattform lediglich optional verwendende TNC-Ansatz soll die Endpoint-Integrität mithilfe einer offenen Architekturplattform sicherstellen können. Dabei kommen die hersteller-, plattform- und netzwerkunabhängigen Sicherheitspolicies zum Einsatz, um die Integritätsprüfung der Endsysteme zu gewährleisten (vgl. [ems12], [tcg12]).
Die in der Arbeit vorgestellten Ansätze zur Gewährleistung einer sicheren Arbeitsumgebung orientieren sich an die aktuellen Gegebenheiten der medizinischen Forschung in Deutschland. Die Konzepte berücksichtigen die förderzeitbedingte kurze Dauer von Projekten, das föderative System mit einer mangelhaften Verzahnung der klinischen Forschungsprojekte und den methodischen Zentren sowie die enorme Heterogenität der IT-Lösungen. Sie versuchen auf den kleinsten gemeinsamen Nenner zu kommen, um trotz der genannten Faktoren ein angemessenes Maß an Sicherheit zu gewährleisten (vgl. [DO05]). Eine grundlegend andere vorteilhaftere Vorgehensweise verwendet man im Rahmen des derzeit wohl weltweit größten Infrastrukturprojekts für vernetzte Krebsforschung caBIG des US National Cancer Institute (NCI). Das caBIG-Projekt fördert einen freien Zugriff auf die Forschungsressourcen, eine offene gemeinschaftliche Entwicklung und Verbesserung der vorhandenen Werkzeuge sowie einen durchgehenden Einsatz von Open Source. Die Kompatibilität der einzelnen Lösungen und die Durchgängigkeit der Begriffe in allen Modellkomponenten werden durch ein gemeinsames Informationsmodell und ein kontrolliertes Vokabular erreicht.
Für die Überlegungen der sicheren Teilnehmeranbindung sind die dabei entwickelten gemeinsamen quelloffenen APIs vom besonderen Interesse. Wäre eine solche forschungsnetzübergreifende Plattform in Deutschland vorhanden, ließe sich das Problem der Integrität der einzelnen Arbeitsumgebungen relativ einfach durch die signaturbasierte Integritätsprüfung der gemeinsam zu verwendenden Komponenten lösen. Im Gegensatz zu den eher nur die Symptome bekämpfenden Vorschlägen der Abschnitte 3.5.1 und 3.5.5 wäre dadurch die Sicherheitsprüfung von der – durch die Arbeitsumgebung aufgefangene – Betriebssystemebene auf die durch die Anwendungskomponenten gewährleistete Applikationsebene verlagert.

Die als erwünscht beschriebene Entwicklung ist nur mithilfe einer entsprechenden politischen Unterstützung möglich. Im Falle des caBIG-Projektes wird beispielsweise die Kompatibilität der neuen IT-Infrastrukturen im Hinblick auf die caBIG-Standards mit der politischen Entscheidung über die Förderungsrichtlinien im Bereich der Krebsforschung erreicht. Eine ähnliche Regelung würde in Deutschland ein derzeit fehlendes Anreizsystem zum Aufbau und Nutzung einer sicheren gemeinsamen technischen Infrastruktur begünstigen (vgl. [nci12], [OLH+08]).

5.1.3.2. Datenzusammenführung

Während der Erstellung des Abschnitts 3.5.2 „Zusammenführung von Patientendaten“ entfachte eine Diskussion über die Art und Weise, wie die Patientendaten *IDAT* und *MDAT* sicher zusammengeführt werden können. Als besonders empfehlenswert aus der Sicht der Datenschutzexperten wurde eine clientseitige Datenzusammenführung identifiziert. In der vorliegenden Arbeit werden die Möglichkeiten der Datenzusammenführung mithilfe der Ajax- und Java-Technologien untersucht. Zusätzlich erfolgt die Bewertung der Einsatzmöglichkeiten der im Abschnitt 3.5.1 „Sichere Arbeitsumgebung“ beschriebenen Terminal Services. Dabei werden zuerst die für den Vergleich verwendeten Annahmen aufgeführt, und anschließend die sicherheitsrelevanten Merkmale dieser Technologien im Hinblick auf ihre Vor- und Nachteile beim Einsatz für die Datenzusammenführung diskutiert. Schließlich erfolgt die Untersuchung, welche Vorteile durch eine Kombination dieser Technologien entstehen können.

Ajax: Einer der Vorteile des Einsatzes von Ajax ist die fehlende Notwendigkeit der zusätzlichen Software auf der Client-Seite in Form von z. B. Browser-Plugins. Aufgrund von JavaScript erlaubt Ajax außerdem einen plattformunabhängigen Einsatz. Eine Vielzahl fertiger Programmbibliotheken ermöglicht eine kostengünstige und gleichzeitig sichere Softwareentwicklung. Durch den Einsatz von Webforms- bzw. JSF-Technologien sind die den Desktop-Anwendungen ähnlichen Webapplikationen möglich. Für Ajax spricht außerdem die weite Verbreitung aufgrund der JavaScript-Unterstützung durch die meisten aktuellen Browser. Die beiden wichtigsten Nachteile des Ajax-Einsatzes sind das beschriebene Polling-Problem und die durch JavaScript bedingte geringere Sicherheit. Die Ermittlung der Eignung von Ajax in einem konkreten Einsatzszenario erfordert eine, vom Einsatzzweck abhängige, Prüfung. Zumindest scheint die grundlegende Verwendbarkeit von Ajax im Bereich der Datenzusammenführung gegeben zu sein. So bietet das vom nationalen US-Gesundheitsinstitut geförderte i2b2-Projekt den „Query and Analysis Tool“ u. a. als eine Ajax-Anwendung an (vgl. [ncb12]).

Java: Der Komplexität und Vielschichtigkeit der Java-Plattform geschuldet bietet der Abschnitt eine differenzierte Auseinandersetzung mit den bestehenden Gestaltungsmöglichkeiten einer Java-basierten Lösung zur Datenzusammenführung. Allgemein bleibt

festzuhalten, dass der Hauptvorteil von Java in ihrer – im Vergleich mit JavaScript/Ajax – ungleich höheren designbedingten Sicherheit liegt. Durch die große Verbreitung der Java-Laufzeitumgebungen für alle gängigen Plattformen steht Java dem JavaScript in der Support-Hinsicht in nichts nach.

Terminal Service-Technologie: Der Hauptvorteil für den Einsatz der Terminal Service-Technologie ist darin zu sehen, dass die Verwendung von Terminal Services nicht den gleichzeitigen Einsatz von Webtechnologie ausschließt. Dies sorgt für die notwendige Kompatibilität und für die mögliche Unterstützung der Legacy-Anwendungen. Ein weiterer Vorteil liegt in einer – im Vergleich zum „einfachen" Client – aufwendiger zu kompromittierenden Server-Umgebung, was die Wahrscheinlichkeit der von den Clients ausgehenden direkten anwendungsbasierten Angriffe reduziert. Der große Nachteil einer Terminal Service-Lösung besteht in der Notwendigkeit an einem Terminal Service-Client, dessen Verfügbarkeit je nach der getroffenen Plattformentscheidung nicht für alle Systeme gegeben sein kann. Außerdem stellt ein Terminal-Server einen sogenannten Single Point of Failure dar, was die Angriffe auf ihn als lukrativ erscheinen lässt.

5.1.3.3. Authentifizierung

Im Abschnitt 3.5.3 „Authentifizierung von Forschungsnetzteilnehmern" wird die Praxistauglichkeit und die Eignung der aktuell verfügbaren Lösungen zur Nutzerauthentifikation untersucht. Ein starkes Authentifikationsverfahren kann gegen viele Angriffe schützen und gleichzeitig bei einer Vielzahl anderer Angriffsarten versagen. So beschreibt Kevin Mitnick in seinem Buch „Die Kunst der Täuschung" einen einfachen und gleichzeitig erfolgreichen Social Engineering-Angriff, der eine teure Einmalpasswortlösung mit einem geringen Aufwand aushebeln konnte (vgl. [Mit03]). Eine kurze prägnante Analyse der in [Mit03] geschilderten Angriffsszenarien, gefolgt von einer Beschreibung der Angriffe auf der semantischen Ebene, ist im Buch *„Sichere Systeme: Konzepte, Architekturen und Frameworks"* von W. Kriha und R. Schmitz vorgestellt. Leider enthält auch dieses Werk außer der Forderung nach einem Benutzerschutz „auf einer höheren, semantischen Ebene" keine Patentlösung für das Problem einer sicheren Authentifikation bzw. eines sicheren Front-Ends (vgl. [KS09, S. 61 ff.]).
Da die aktuellen Authentifikationsmechanismen noch nicht so weit fortgeschritten sind, um die unterschwelligen Benutzerwünsche wahrnehmen zu können, soll die Durchführung einer Risikoanalyse bei der Einschätzung, ob eine Authentifizierungsmethode den Sicherheitsbedürfnissen des Forschungsnetzes entspricht, helfen (s. a. Kapitel 4 „Entwicklung eines Konzeptes für das dynamische S&R-Management"). Sinnvoller erscheint die Erkennung der relevanten Gefahren und die darauf basierende Auswahl einer passenden Teilnehmerauthentifizierungsplattform statt einer Installation der aktuell „sichersten", aufwendig zu implementierenden Authentifizierungslösung. Sollte nämlich eine solche Lösung imple-

mentiert werden können, würde sie nicht jeden erdenklichen Betrugsversuch verhindern können, sondern die Angreifer lediglich zur Änderung ihrer Angriffstaktiken zwingen.
Die im März 2011 bekannt gewordenen Ereignisse stellten erneut die Sicherheit von tokenbasierten Authentifizierungslösungen und insbesondere die Sicherheit der verwendeten Hardwarekomponenten unter Beweis. Als Folge eines ausgeklügelten Angriffs sollen dem Sicherheitsspezialisten RSA sowohl die für die SecurID-Tokens verwendeten Seeds als auch der SecurID-Quellecode gestohlen worden sein (vgl. [emc11]). Ein über diese Informationen verfügender Angreifer wäre in der Lage, die mithilfe der SecurID-Tokens generierten Einmalpasswörter zu reproduzieren. Die angebliche hohe Komplexität des durchgeführten Angriffs kann nur bedingt als Argument dafür dienen, dass ein vergleichbarer Angriff in Zukunft nicht mehr passieren wird bzw. wenig wahrscheinlich ist.
In seinem Blog vertritt Bruce Schneier die Meinung, dass die Benutzerauthentifizierung in der Vergangenheit ständig im Vordergrund gestanden habe, was dazu geführt hätte, dass es in diesem Bereich beträchtlich viele sichere Lösungen gäbe. Dem – seiner Ansicht nach – Hauptproblemfeld der unzureichend authentifizierten Transaktionen wird jedoch weiterhin zu wenig Beachtung geschenkt (vgl. [Sch05b]). Die Authentizität einer Transaktion ist unmittelbar mit der Identität des auszuführenden Benutzers verbunden. Selbstverständlich kann man die Authentizität einer jeden einzelnen Transaktion überprüfen,[5] doch würde dies die Benutzbarkeit und auch die Akzeptanz der Forschungsnetzdienste deutlich verringern. Die Anzahl von Transaktionen, die ein Teilnehmer durchführt, könnte außerdem den Überprüfungsaufwand unbezahlbar machen.
Die im Abschnitt 3.5.3 „Authentifizierung von Forschungsnetzteilnehmern“ vorgeschlagene Authentifizierungslösung der auf SmartCards gespeicherten und durch PIN-Code-geschützten Zertifikate erscheint in diesem Zusammenhang als ein sinnvoller Kompromiss, der einen erforderlichen Sicherheitsstand mit einem vertretbaren Implementierungs- und Betriebsaufwand kombiniert.

5.1.3.4. Rollenbasierte Zugriffsberechtigungen

Im Abschnitt 3.5.4 „Rollenbasierte Rechtevergabe (RBAC)“ wird ein möglicher Aufbau eines rollenbasierten Zugriffsberechtigungskonzeptes dargestellt. Dabei werden – basierend auf den „Beschreibungen der Sequenzgrafiken der AG Datenschutz“ [SSS06] – die relevanten Anwendungsfälle ermittelt und einige mithilfe der SecureUML-Syntax beschrieben. Es werden u. a. die Benutzerverwaltung, der Zugriff eines Wissenschaftlers auf die Forschungsdaten, die Durchführung eines Depseudonymisierungsvorgangs und die Sicherstellung der Datenqualität durch einen Monitor vorgestellt.
SecureUML ist eine UML-basierte Modellierungssprache, die es erlaubt, RBAC um dyna-

[5] Zum Beispiel nach dem Vorbild von einigen Banken könnte ein Forschungsnetzteilnehmer eine Bestätigungs-SMS für jede Transaktion erhalten, die dann zeitverzögert ausgeführt wird, wenn der Benutzer der erhaltenen Nachricht nicht widerspricht.

mische Komponenten in Form von sogenannten Autorisierungs-Constraints zu erweitern. Die dynamischen Einschränkungen können genutzt werden, um beispielsweise solche zugriffsrelevanten Komponenten wie Sicherheitszustand des Systems, Vertraulichkeit der Verbindung etc. abzubilden. Das SecureUML-Modell und die verwendete Syntax wurden aus der Dissertationsschrift von Torsten Lodderstedt „Model Driven Security from UML Models to Access Control Architectures“ [Lod03] übernommen.
Mehrere Untersuchungen belegen die grundsätzliche Eignung von rollenbasierten Zugriffskonzepten für den Einsatz im Gesundheitsbereich (vgl. [SM07], [GMNP02], [PBB+96]). Dies bedeutet allerdings nicht, dass der in dieser Arbeit unterbreitete Vorschlag automatisch das Optimum für jede Ausprägung eines medizinischen Forschungsnetzes beschreibt. Der vorgestellte Lösungsvorschlag erfüllt jedoch die maßgeblichen Sicherheitsanforderungen und kann als Ausgangspunkt für weitere Spezialisierung der konkreten Zugriffskonzepte dienen. Die Lösung berücksichtigt das Aufgabentrennungsprinzip und ermöglicht die Vergabe der sogenannten minimalen Rechte. Durch die Integration solcher dynamischen Komponenten wie die Zeit und die Zugriffsumgebung in das vorgestellte Modell können Funktionenänderungen der einzelnen Subjekte leicht abgebildet werden. Durch die Vererbung innerhalb des definierten Rollenmodells werden überflüssige Redundanzen in den Rollendefinitionen vermieden, was zu einer besseren Wartbarkeit des Modells beiträgt.
Obwohl das dem Modell zugrunde liegende RBAC derzeit noch als Standard für die Abbildung von Zugriffskontrollmodellen angesehen wird, zeigen die neueren Untersuchungen, dass die Anwendbarkeit eines RBAC-Systems in verteilten medizinischen Umgebungen eingeschränkt sein könnte. So wird beispielsweise eine ausführliche Begründung der bedingten Eignung des aktuell verbreiteten RBAC-Modells sowie ein Entwurf eines – aus der Spieltheorie entliehenen – Ansatzes für die Autorisierungskontrolle in den HealthGrid-Umgebungen G-UCON in der Dissertationsschrift „Data Protection and Data Security Concept for Medical Applications in a Grid Computing Environment“ [Moh08] von Yassene Mohammed vorgestellt. Weitere Untersuchungen belegen die potenzielle Schwäche des RBAC-Ansatzes für die Insider-Angriffe. Für besonders schützenswerte Patienteninformationen[6] gilt derzeit eine Kombination von RBAC-basierten Zugriffsberechtigungen mit dem auf der Basis von NIST Policy Machine [FGHK05] vergebenen temporären DAC-Zugriffsberechtigungen[7] als eine aussichtsreiche Lösung (vgl. [PFGG09]).

5.1.3.5. Verzeichnisdienste

Der Abschnitt 3.5.6 „Verzeichnisdienste (LDAP, OCSP)“ beginnt mit einer kurzen Beschreibung der Komponenten eines Verzeichnisdienstes. Bei den darauf folgenden Ausführungen wird von der Annahme ausgegangen, dass die Zertifikate der Forschungsnetzteilnehmer auf

[6] Zum Beispiel Personen des öffentlichen Interesses, gesellschaftlich tabuisierte Erkrankungen etc.

[7] Discretionary Access Control.

PIN-geschützten SmartCards verteilt werden. Leider widerspricht diese Annahme häufig der Wirklichkeit, denn aus Kostengründen werden oft Softwarezertifikate eingesetzt. Beim Einsatz von Softwarezertifikaten reduziert sich der Aufwand für die Ersetzung von alten Zertifikaten durch neue immens, sodass der im diskutierten Abschnitt unterbreitete Vorschlag, die Gültigkeitsdauer von Zertifikaten für nicht kritische Systeme bzw. Teilnehmer auf drei Jahre auszudehnen, in solchen Fällen als kaum angemessen erscheint.
Die Gültigkeitsverifikation von Zertifikaten ist ein weiteres Thema des Abschnitts. Aufgrund der geschilderten Nachteile der CRL- respektive ARL-basierten Gültigkeitsprüfung wird die Verwendung von OCSP bzw. SCVP vorgeschlagen, die sekundengenaue Sperrinformationen liefern können. Insbesondere für temporäre Sperrungen wäre die Verwendung der beiden Verfahren unbestritten vorteilhaft. Um die Entscheidung über das Vertrauen in die einzelnen Zertifikate nicht den Teilnehmern bzw. Systemen zu überlassen, wird die Verwendung von den durch die Vertrauensbasen verwalteten dynamischen Vertrauenslisten vorgeschlagen. Ein zusätzlicher Vorteil beim Einsatz der beiden Protokolle ist außerdem die Möglichkeit, zwischen den gesperrten und den gefälschten Zertifikaten zu unterscheiden, was jedoch eine entsprechende Konfiguration der Responder voraussetzt.
Auch die Nachteile von OCSP sollen nicht verschwiegen werden. So liefert das Protokoll zwar den Sperrstatus von Zertifikaten; ihre Gültigkeitsdauer, die Nutzungsbeschränkungen sowie die Korrektheit der Signaturen werden jedoch nicht überprüft. Die Konfiguration des OCSP-Responders ist ein weiterer kritischer Punkt, denn dieser kann auf den Sperrlisten basieren, was die Vorteile des OCSP-Einsatzes im Vergleich zu CLR/ARL einschränkt (vgl. [MAM+99]). Der zusätzlich zur Zertifikatsvalidierung die Generierung und die Validierung von Zertifikatspfaden unterstützende SCVP ist komplexer als OCSP. Die Spezifikation des Protokolls aus dem Dezember 2007 wird nur von wenigen Produkten unterstützt (vgl. [CSF+08], [FHM+07]).[8]
Forschungsnetze können Zertifikate in mehreren Bereichen einsetzen, in denen sie z. B. der Teilnehmer- oder der Komponentenidentifizierung dienen. Abhängig vom Einsatzzweck werden unterschiedliche Anforderungen an die Zertifikate gestellt. So wird beispielsweise ein Server-Zertifikat die IP-Adresse bzw. Namen des Servers enthalten, wobei das Zertifikat der im Abschnitt 3.5.1 „Sichere Arbeitsumgebung“ beschriebenen Virtualisierungslösung z. B. den Hashwert des Software-Pakets beinhalten kann.
In X.509 wird ein Mechanismus definiert, mit dessen Hilfe die Eignung eines Zertifikats für eine bestimmte Aufgabe festgehalten werden kann – die sogenannte Zertifizierungspolicy. Das Policy-Prinzip basiert auf den sogenannten Objekt-Identifikatoren (OID) – eine nach ISO/IEC 9834/1 normierte eindeutige Kennzeichnung für Objekte und Nachrichten.[9]

[8] Zum Vergleich: Die Veröffentlichungen der OCSP-Spezifikation erfolgte im Juni 1999.

[9] Zum Beispiel OID 1.2.276.0.76.4 ist die eindeutige Bezeichnung für die Instanz eines Objektes: ISO-Objekt (1), Mitglied (2), Deutschland (276), DIN-CERTCO (0), Gesundheitswesen (76), Identifizierungsmechanismen (4).

Mithilfe von OIDs könnten die Forschungsnetzkomponenten eindeutig identifiziert werden. Durch die Identifizierung wird die Eignung eines Zertifikats für eine bestimmte Aufgabe (des Objektes) verifiziert. Die OIDs werden im Zusammenhang mit den sogenannten Certificate Policies verwendet. Bei der Ausstellung eines Zertifikats kann eine Erweiterung als kritisch markiert werden, was bedeutet, dass das Zertifikat nur für die angegebenen Zwecke einzusetzen ist.[10] Das Forschungsnetz kann eigene Richtlinien-OIDs definieren und diese bei Bedarf registrieren. Insbesondere bei der gegenseitigen bzw. gemeinsamen Nutzung von Diensten durch mehrere Forschungsnetze kann dies garantieren, dass die ausgestellten Zertifikate nur für die bei der Ausstellung vorgesehenen Zwecke verwendet werden. Sollte die Verwendung registrierter OIDs bei einer gemeinsamen Nutzung von Diensten zwischen mehreren Forschungsnetzen nicht möglich sein, können die sogenannten Policy Mappings die Zuordnung zwischen den Richtlinienkennungen verschiedener Vertrauensdomänen übernehmen.[11] Die OIDs werden im Richtlinien-Kennungsfeld (Policy-Identifier) eingetragen. Zusätzlich können die Policy-Qualifiers die Eignung gefundener Pfade für die aktuelle Transaktion verifizieren. Die Suche nach einem gültigen Zertifizierungspfad gestaltet sich in einem hybriden Vertrauensmodell bzw. bei der Zusammenführung mehrerer Vertrauensdomänen als problematisch. Man unterteilt den Validierungsprozess in zwei Schritte: die Suche nach einem Pfad[12] und dessen Gültigkeitsprüfung. Während der Gültigkeitsprüfung werden u. a. folgende Kriterien verifiziert: Sperrstatus, kryptografische und zeitliche Gültigkeit der Signatur, Angaben zum Zertifikatsausteller und Zertifikatsinhaber, Zertifikatsaustellungs-Zweck sowie Policy-Einschränkungen (vgl. [CSF+08], [NDJ01]).

5.1.3.6. Anti-Malware-Infrastruktur, Proxying, Firewalling und Intrusion Detection

Die Abschnitte 3.5.9 „Antimalware-Einrichtungen“, 3.5.10 „Firewalling und Proxying“ und 3.5.11 „Intrusion Detection Systeme (IDS)“ befassen sich mit den Eigenschaften und den Potenzialen für den Forschungsnetzeinsatz der genannten Sicherheitsarchitekturbestandteile.

IAM, UTM: Der Abschnitt 3.5.9 „Antimalware-Einrichtungen“ erörtert die Vor- und Nachteile des Einsatzes von Lösungen für das sogenannte Unified Threat-Management (UTM) bzw. Identity- and Access-Management (IAM). Die Erkenntnisse dieses Vergleichs stehen z. T. im Widerspruch zu der Empfehlung zur Speicherung der Zugriffsrechte in der

[10] Zum Beispiel beschreibt die Key-Usage-Erweiterung die Eignung eines *Data Encipherment*-Schlüssels zur Verschlüsselung von Benutzerdaten und eines *Key-Agreement*-Schlüssels zur Vereinbarung eines Session-Keys.

[11] Der Einsatz von Richtlinienzuordnungen und ihre Praxistauglichkeit in einer dynamischen Struktur sind jedoch umstritten.

[12] Im Gegensatz zu einem untergeordneten hierarchischen Modell, in dem Pfadangaben innerhalb des Zertifikats enthalten sind, und somit die Vertrauenspfade leicht gefunden werden können, werden bei der Pfadsuche in hybriden Strukturen Heuristiken eingesetzt.

Patientenliste, die beispielsweise in [RDSP06] präferiert wird. In dieser Arbeit wird die Meinung vertreten, dass die IAM-Technologie einsatzreif ist, um mehrere Sicherheitsprobleme wie beispielsweise die Abbildung von temporären Zugriffsrechten zu bewältigen. Sie stellt einen wertvollen Baustein der Forschungsnetzsicherheitsinfrastruktur dar, mit dessen Hilfe, mehrere Einstiegslöcher für einen Angriff konsequent geschlossen werden können (vgl. [Hud07]).

Proxying: Bei der Diskussion um die Sinnhaftigkeit des Proxy-Einsatzes im Bereich der medizinischen Forschung sind insbesondere die vom Proxy gewährleistete Trennungs- und Filterungsfunktion vom Interesse. Mithilfe von Proxy-Servern ließen sich außerdem Redundanzen aufbauen, die für die höheren Ausfallsicherheit und Verfügbarkeit sorgen können. Interessant für den Forschungsnetzeinsatz wäre außerdem die Anwendung des Reverse-Proxy-Prinzips: Hier könnte der Proxy-Server die Lastverteilungsfunktion übernehmen. Zudem kann der Proxy-Server auch als eine Zwischenstufe eingesetzt werden, die die direkten Angriffe auf die kritischen Systeme verhindert. Ein ähnlicher Ansatz wurde bereits im Zusammenhang mit der sicheren Arbeitsumgebung angesprochen, wobei die „Rolle der Zwischenstufe“ in diesem Fall z. B. von einer abgesicherten Terminal-Server-Umgebung übernommen wird. Der dabei erwähnte Nachteil des sogenannten Single Point of Failure gilt auch für den Proxy-Server. Man könnte von der Annahme ausgehen, dass die Gesamtrisikosituation durch einen Reverse-Proxy sogar verschlimmert wäre, da hier ein – zum Applikationsserver zusätzlicher – Angriffspunkt geschaffen wird. In der Tat nimmt man häufig einen Zusammenhang zwischen der Verwundbarkeit eines Systems und dessen Komplexität an (vgl. [bsi08f]). Im Endeffekt ist die häufig anzutreffende Aufteilung in Web-, Applikations- und Datenbankserver ein Resultat aus diesem Zusammenhang, denn würde man die drei Funktionen in einem System zusammenfassen, wäre die Wahrscheinlichkeit für eine Sicherheitslücke und dadurch das gesamte Sicherheitsrisiko wesentlich höher. Zusätzlich fehlt bei einem „All in One“-Aufbau die Möglichkeit, Zwischenstufen z. B. in Form von Applikationsfiltern einzubauen. Ein Reverse-Proxy-Server hat i. d. R. eine geringere Komplexität als z. B. ein Applikationsserver, sodass durch dessen Einsatz eine eher höhere Sicherheit des Aufbaus zu erwarten wäre (vgl. [Som03]). Parallel zu den Überlegungen hinsichtlich der Komplexität des Produktes ist die Verbreitung bzw. Einsatzhäufigkeit von Systemkomponenten zu berücksichtigen. Die Verbreitung von vollständigen Proxy-Servern ist wesentlich geringer als die der Applikationsserver. Dies kann sowohl als Nach- als auch Vorteil ausgelegt werden: Einerseits erwartet man von einer stark verbreiteten Applikation eine höhere Sicherheit, da hier viele Parteien an einer sicheren Konfiguration interessiert sind. Dementsprechend schneller sollten die Sicherheitslücken aufgedeckt und behoben werden. Andererseits wird ein Angriff auf eine stark verbreitete Software lukrativer, da er

bei vielen Installationen eingesetzt werden kann.[13]

Firewalling: Die beiden wichtigsten Empfehlungen für den sicheren Firewalling-Einsatz im Abschnitt 3.5.10 „Firewalling und Proxying“ können als *Redundanz* und *Mehrstufigkeit* zusammengefasst werden (vgl. [SCB03], [GKZ01]). Ein in der Abbildung 7 auf der Seite 59 dargestelltes Beispiel der Systemaufteilung auf die einzelnen Netzsegmente verdeutlicht die beiden Prinzipien anhand eines zweistufigen DMZ-Aufbaus mit einer zusätzlichen Trennung zwischen den Client- und Serversystemen. Die Platzierungsmöglichkeiten für die VPN- und IDS-Sensoren im Falle eines generischen zweistufigen DMZ-Aufbaus mit einem zwischen den beiden Firewalls geschalteten Applikation Level Gateway werden analysiert. Die Inhalte der Abschnitte 3.5.5 „Zugangsszenarien von Netzteilnehmern zu den Forschungsnetzdiensten“ und 3.5.11 „Intrusion Detection Systeme (IDS)“ werden verwendet, um die Vorteilhaftigkeit der Kombinationsmöglichkeiten der beiden Technologien für einen generischen DMZ-Aufbau und die Praxistauglichkeit aufgrund der eingesetzten Verbindungsverschlüsselung zu untersuchen.

Intrusion Detection: Die Inhalte des Abschnitts 3.5.11 „Intrusion Detection Systeme (IDS)“ orientieren sich am in den vorhergehenden Abschnitten der Arbeit vorgestellten und weiterentwickelten generischen Aufbau. Grob können diese in Form der Trennung zwischen den *IDAT*- und *MDAT*-Servern, einem dreistufigen DMZ-Aufbau und dem Einsatz einer Lockdown-Arbeitsumgebung für die Teilnehmer zusammengefasst werden. Von den im Abschnitt 3.5.11 „Intrusion Detection Systeme (IDS)“ vorgestellten IDS-Technologien werden die Ansätze der host- und netzwerkbasierten Intrusion-Erkennung verwendet,[14] um die Einsatzmöglichkeiten für die Intrusion Detection-Systeme aufzuzeigen. Der Einsatz von Verschlüsselungstechnologie wird durch die unterbreitete Einsatzempfehlung im Zusammenhang mit der netzwerkbasierten Intrusion-Erkennung berücksichtigt (vgl. [NN01]). Insgesamt sind Intrusion Detection Systeme als eine sinnvolle Ergänzung des Sicherheitsmaßnahmenportfolios zu verstehen (vgl. [LO09], [KSV07], [Mar05]).

5.1.3.7. Monitoring- und Protokollierungsaspekte

Der Abschnitt 3.5.12 „Monitoring und Protokollierung“ befasst sich mit der manuellen und automatischen Erfassung und Überwachung von Zuständen und Vorgängen. Es werden die Anforderungen an das Monitoring von forschungsnetzüblichen administrativen und nicht

[13] Würde jemand auch mit durchschnittlichen IT-Kenntnissen seinen eigenen Webbrowser ohne Verwendung der Standard-Engines programmieren und diesen Browser nur selbst einsetzen, wäre dies vermutlich der sicherste und unsicherste Browser zugleich. Die Unsicherheit würde aus einer zu erwartenden Vielzahl von Sicherheitslücken resultieren. Trotzdem wäre dieser Browser sicherer als die anderen von professionellen Entwickler-Teams und Sicherheitsexperten erstellten weit verbreiteten Produkte, solange sich niemand für die Daten dieser Person interessieren würde.

[14] Anstelle von hostbasierten IDS wäre der Einsatz von hybriden IDS denkbar.

administrativen Vorgängen diskutiert. Außerdem werden die Anforderungen an die Aufbewahrungsdauer von Protokolldaten untersucht. Dabei wird die Auffassung vertreten, dass die erforderliche Aufgabenerfüllung für die Bestimmung der Aufbewahrungsdauer maßgebend ist. Folgt man dieser Logik, darf die Aufbewahrungsdauer der bei den in erster Linie zur Aufklärung von eventuellen Straftaten gesammelten Daten die Verjährungsfristen nach StGB nicht unterschreiten. Die wohl größte Schwierigkeit einer solchen Betrachtungsweise besteht in der Bewertung der Notwendigkeit bestimmter Protokolldaten für die Aufklärung dieser oder jener Straftat. Folglich muss von der potenziell schwerwiegendsten Straftat mit den daraus resultierenden Aufbewahrungsfristen von beispielsweise 100 Jahren oder einer dauerhaften Aufbewahrung bei unverjährenden Verbrechen für sämtliche Protokolldaten ausgegangen werden, was mit Sicherheit absurd wäre. Vielmehr würden solche Praktiken gegen andere gesetzliche Bestimmungen verstoßen z. B. in Form des Datenschutzgesetzes, das eine Löschung/Sperrung von Daten nach dem Wegfall der Notwendigkeit für die Datenspeicherung bzw. -verarbeitung vorsieht.[15] Das Thema der Datenaufbewahrung kann in der vorliegenden Arbeit somit nicht als endgültig geklärt betrachtet werden und bedarf weitergehender Untersuchungen.

Ein weiterer Teil des Abschnitts beschäftigt sich mit der Eignung von sogenannten Watermarking-Verfahren, um die nichtberechtigte Weitergabe von Forschungsnetzdaten zu unterbinden bzw. diese nachträglich zu untersuchen. Trotz der teilweise fortgeschrittenen Technologie lässt sich eine nur bedingte Eignung von Watermarking-Verfahren für die Erkennung bzw. Verhinderung des Datendiebstahls feststellen. Das Watermarking könnte sich jedoch bei der nachträglichen forensischen Untersuchung von Sicherheitsvorfällen als hilfreich erweisen (vgl. [PCL07], [SD05], [NPL04], [CMS+00]).

Auch die Eignung von Notar- und Zeitstempeldiensten wird untersucht, wobei grundlegend festgestellt werden muss, dass die Notardienste als Zeitstempeldienst-Erweiterung sich im Bereich der Forschungsnetze vielfältig einsetzen lassen. So kann man beispielsweise Zeitstempel an ein Dokument anbringen, um später verifizieren zu können, dass dieses Dokument zu einem bestimmten Zeitpunkt in einer bestimmten Form vorgelegen hat. Mithilfe des Zeitstempeldienstes kann außerdem festgestellt werden, wann eine bestimmte Version des vorliegenden Dokuments erstellt wurde. Im Bereich „Protokollierung“ können Zeitstempeldienste verwendet werden, um die nachträglichen Veränderungen an den Protokollierungsdaten feststellen zu können (vgl. [LBG08]). Der Einsatz von verketteten Listen aus erzeugten Zeitstempeln kann für die eindeutige Reihenfolge der Transaktionselemente sorgen, sodass keine Transaktionen nachträglich hinzugefügt oder entfernt werden können.

[15] Beispielsweise Verstoß gegen §§ 3a, 35 Abs. 2 BDSG oder wenn anwendbar § 45i Abs. 1 TKG.

5.2. Diskussion der Bedrohungsszenarien für die medizinischen Forschungsnetze

Die Analyse der Bedrohungssituation hat eine systematische Identifikation und Abschätzung der für ein Forschungsnetz relevanten Bedrohungen als Ziel. Die Bedrohungsrelevanz ist maßgeblich für die Ausrichtung einer Sicherheitspolitik. Als zwei mögliche Vorgehensweisen der Risikoanalyse werden im Abschnitt 4.3 „Qualitative Bewertung der Bedrohungs- und Risikosituation“ der schutzbedarfsorientierte und der bedrohungsorientierte Ansatz vorgestellt.

5.2.1. Schutzbedarfsorientierter Ansatz

Bei der schutzbedarfsorientierten Betrachtung erfolgt im ersten Schritt eine Einschätzung der Kernprozesse bzw. Dienste in einem Forschungsnetz im Hinblick auf die Einhaltung der Sicherheitskriterien.[16] Eine ähnliche Vorgehensweise wird häufig in der Industrie für die Einschätzung des Schutzbedarfs von Arbeitsprozessen eingesetzt. Dabei werden die Prozesseinzelschritte und bestimmte kritische Ressourcen oder Daten[17] in einer Matrixform gegenübergestellt. Auf je mehr solche Ressourcen ein Prozess zugreift, desto kritischer wird dieser eingeschätzt und umso mehr Augenmerk auf seine Absicherung ist erforderlich (vgl. [Mül11, S. 162 f.]). Da die untersuchten Dienste bzw. Prozesse fast ausschließlich auf die gleich kritischen Ressourcen zugreifen, wird zusätzlich – basierend auf der im Anhang D „Qualifizierung von Sicherheitskriterien“ erstellten Aufteilung – der Schutzbedarf der Prozesse ermittelt. Die Einteilung erfolgt u. a. auf der Basis der Ausführungen in [Die08], [DC06], [RDSP06], [SPR+06] und [SSS06]. Trotz der vorgenommenen Begründung für die abgegebenen Einschätzungen bleiben die Bewertungen der Prozesskritikalitäten subjektiv und sollen nur nach einer Anpassung der Qualifizierung an die Gegebenheiten des jeweiligen Forschungsnetzes für die Schutzbedarfsermittlung übernommen werden.
In Wirklichkeit können die für ein Forschungsnetz zu berücksichtigenden Risiken oft miteinander kaum verglichen werden. Eine umfassende Aufzählung und Klassifikation der Gefahren für diverse Infrastrukturen können [bsi11d] entnommen werden. Nur ein kleiner Teil der in diesen Katalogen beschriebenen Angriffe ist für ein Forschungsnetz tatsächlich relevant.
So wird ein Forschungsnetz i. d. R. (bzw. zum größten Teil) von der öffentlichen Hand finanziert, was zwar den Geldzufluss einschränkt, seine Höhe jedoch im Voraus planbar macht. In Verbindung mit einem festen Budget eliminiert diese Finanzierungsform die meisten Liquiditäts- und Bonitätsrisiken. Ein Forschungsnetz führt keinen wirtschaftlichen

[16] Untersuchte Sicherheitskriterien: Authentizität, Integrität, Konformität, Robustheit, Verbindlichkeit, Verfügbarkeit und Vertraulichkeit.

[17] Beispielsweise Zugang zum Kreditorenkonto, Zugriff auf Personaldaten, vertrauliche Vertragsinformationen etc.

Betrieb; auch die volkswirtschaftlichen Risiken wie Änderung des Kreditzinsniveaus oder der Bevölkerungsstruktur haben keinen direkten Einfluss auf den Forschungsnetzbetrieb. Die sonstigen *marktwirtschaftlichen Risiken* (Patentstreits, Nachfrageänderung etc.) haben ebenfalls eine geringe Relevanz für ein Forschungsnetz. Die personellen Risiken (z. B. fluktuationsbedingter Know-how-Verlust, längere Krankheit der Administrationskräfte) können kaum zum Einstellen des Forschungsbetriebs führen. *Politische Veränderungen* können dagegen den Forschungsnetzbetrieb stark beeinflussen. Dazu zählen u. a. Gesetzesänderungen, die die Sammlung und Auswertung von personenbezogenen Daten betreffen bzw. einschränken, und der Einfluss von Sicherheitsbehörden, die z. B. eine permanente Kontrolle über die Forschungsnetzdaten verlangen können, was einen datenschutzrechtlich unbedenklichen Forschungsbetrieb unmöglich machen würde. Schwierig zu lösen ist auch das Problem der Weiterführung der Forschung nach dem Auslaufen der Förderung, wenn die maximale Förderdauer von acht Jahren erreicht worden ist und die Kosten auf die anderen laufenden Projekte nicht weitergegeben werden können (vgl. [Rie04]). Da in einem Forschungsnetz nur die für die Forschung notwendigen Daten gesammelt werden, ein Forschungsnetz nicht die Gesetzgebung beeinflussen kann und auch – aufgrund der öffentlichen Finanzierung – nicht in ein anderes Land ausweichen kann, sind solche Risiken für die Bewertung der Risikostruktur eines Forschungsnetzes irrelevant. Die negativen Änderungen auf diesen Gebieten könnten zwar zum Einstellen des Forschungsbetriebs führen, man verfügt jedoch über keinerlei Mittel, um dieser Entwicklung entgegenzuwirken.

5.2.2. Bedrohungsorientierter Ansatz

Für die Identifikation der möglichen Angriffsszenarien gilt ein rational handelnder Angreifer[18] mit Gewinnerzielungsabsicht i. d. R. als Annahme und ist bei der Konstruktion von Angriffsbäumen[19] üblich (vgl. [BLP+06]). Die Gestaltung bedrohungsorientierter Modelle ist i. d. R. einfacher als die der schutzbedarfsorientierten Modelle. Dies hängt mit der ökonomischen Rationalität der Angreifer sowie dem meist damit verbundenen Bekanntwerden der Folgen dieser Angriffe zusammen (vgl. [Chr11]). Auch die häufig aus Geltungsdrang handelnden – insbesondere jugendlichen – Angreifer sind bei der durchgeführten Analyse berücksichtigt, um das Szenario zu vervollständigen. Bei der Einschätzung der wahrscheinlichsten von Kriminellen ausgehenden Angriffe wird die Suche nach potenziellen Opfern sowie die Erpressung einzelner Patienten als möglich betrachtet.
Eine Meldung von „The Washington Post“ im Mai 2009 [Kre09] hat die praktische Relevanz eines vorher als absurd angesehenen Angriffsszenarios bewiesen. Im geschilderten Fall wollten die Angreifer die Daten von über acht Millionen amerikanischen Schmerzpatienten

[18]Die Angreiferrolle können auch wirtschaftliche Organisationen bzw. Behörden etc. übernehmen. In diesen Fällen kann die Motivation der Angreifer abweichen.

[19]Die Beschreibung einzelner Angriffsszenarien in Form eines Angriffsbaums, ist in der Abbildung 22 auf der Seite 245 visualisiert.

sowie über 35 Millionen Rezepte vom Server des „Virginia Prescription Monitoring"-Programms gegen ein Lösegeld in Höhe von zehn Millionen US-Dollar eintauschen. Dabei wurden sämtliche Patientendaten auf den Servern der Betreiber verschlüsselt und die Backups gelöscht. Die Angreifer hinterließen ein Erpresser-Schreiben mit der Angabe einer E-Mail-Adresse und versprachen, das Passwort für die verschlüsselte Datenbankkopie nach der Lösegeldzahlung auszuliefern (vgl. [wik09]).
Zwar wurde das oben beschriebene Angriffsszenario bei der Erstellung des Angriffsbaums diskutiert, jedoch als unwahrscheinlich und als praktisch irrelevant abgelehnt. Zu unglaublich erschien ein derlei aussichtsloser Erpressungsversuch aufgrund des für die Erpresser nicht lösbaren Problems der Geldübergabe: Die länderübergreifend zusammen arbeitenden Ermittlungsbehörden und Provider lassen den Kriminellen keine Hoffnung, mit der Beute spurlos entkommen zu können. Auch die grundlegende Frage, ob Lösegelder bei einem solchen Erpressungsversuch gezahlt worden wären, ist angebracht. Schließlich besteht keine Garantie, dass die Kriminellen ihr Versprechen einhalten und das Passwort nach dem Erhalt des Lösegeldes tatsächlich herausgeben. Zusätzlich hatten die Kriminellen den Zugriff auf die unverschlüsselten Daten, sind noch im Datenbesitz und könnten, die Daten später an die pharmazeutische Industrie bzw. Banken oder Versicherungen zu verkaufen versuchen.
Der zweifelhafte Anreiz für die Behörden, die Lösegeldforderung der Kriminellen zu erfüllen bzw. das ungelöste Problem der Geldübergabe könnten den Erpressungsversuch als dilettantisch erscheinen lassen. Gleichwohl kann diese Erpressung auch andere Motive als Ursache haben. So könnten die Angreifer beispielsweise versucht haben, mit ihrer öffentlichen Erpressung die Aufmerksamkeit auf die Problematiken der Handhabung von vertraulichen medizinischen Daten im Netz zu lenken. Auch eine Handlung aus Geltungsdrang ist nicht auszuschließen, wobei hier ebenfalls die Erregung der öffentlichen Aufmerksamkeit als Intention dienen könnte. Abschließend bleibt festzuhalten, dass dieser Vorfall in Anbetracht der aktuell öffentlich verfügbaren Informationen eher als eine Kuriosität erscheint, die keinen Aufschluss über die tatsächliche Angreifermotivation zulässt. Es bleibt zu hoffen, dass in naher Zukunft zusätzliche Informationen verfügbar sein werden, die zu einem besseren Verständnis dieses Vorfalls beitragen.
Die aus den beiden Blickperspektiven[20] durchgeführten Analysen geben einen Eindruck über die möglichen Schadensszenarien, erlauben jedoch keine objektive Beantwortung der Frage, die Implementierung welcher der möglichen Sicherheitsmaßnahmen den größten Nutzen für das Sicherheitsniveau eines Forschungsnetzes bringen würde. Eine Analyse etablierter Ansätze zur Bewertung des Nutzens von Sicherheitsmaßnahmen wurde durchgeführt, um die Lösungsmöglichkeiten für diese Problemstellung zu identifizieren.

[20] Angreifer und Verteidiger.

5.3. Diskussion der Ansätze des Sicherheits- und Risikomanagements in medizinischen Forschungsnetzen

Das Verständnis der Informationssicherheit veränderte sich im Laufe der vergangenen Jahre. Aus dem notwendigen Übel wurde ein unentbehrlicher Erfolgsfaktor. Maßgebend für diese Veränderung sind nicht nur die aktualisierten rechtlichen Anforderungen, sondern auch diverse marktwirtschaftliche Anreize für das Anbieten von sicheren Diensten und Systemen (vgl. [AM06]). Die vielzähligen Sicherheits-Frameworks sollen helfen, das Sicherheitsniveau einer Organisation messen und erhöhen zu können. Im Abschnitt 4.1 „Verwendung von S&R-Ansätzen in der medizinischen Forschung“ werden die in der Praxis ihre Verwendung findenden und auch für den praktischen Einsatz geplanten bzw. diskutierten Sicherheits- und Risikomanagementansätze beschrieben. Im Abschnitt A.1 „Untersuchung der Wirksamkeitsbewertung von Sicherheitsmaßnahmen mithilfe von etablierten S&R-Frameworks“ erfolgt eine Deskription, wie die Bewertung der Wirksamkeit von Sicherheitsmaßnahmen durchgeführt werden kann. Dabei werden sowohl die zuvor für die medizinische Forschung aufgelisteten als auch weitere in der Praxis außerhalb der medizinischen Forschung etablierten Ansätze analysiert. Die Untersuchung der Wirksamkeit von Sicherheitsmaßnahmen ist insbesondere im Hinblick auf die Einschätzung des Zustandes eines Risiko- und Sicherheitsportfolios und für die damit unmittelbar zusammenhängende Entscheidung für die Umsetzung eines Sicherheitsmaßnahmenkatalogs relevant (vgl. [Als10, S. 8]).
Die dargestellte Vielfalt der Ansätze sowie die Erkenntnis, dass kein einheitlicher, von allen Parteien anerkannter, Standard für die Untersuchung der Wirksamkeit von Sicherheitsmaßnahmen existiert, spiegelt die Komplexität der Materie sowie die Sachlage wider, dass es den gängigen Kennzahlensystemen oft an Aussagekraft, Interpretierbarkeit und offenbar an Objektivität mangelt. Die Sicherheit als Größe ist abstrakt und nur schwer messbar. Dementsprechend problematisch ist die Ermittlung belastbarer Kennzahlen für die Bewertung der Notwendigkeit bzw. Sinnhaftigkeit von Sicherheitsmaßnahmen (vgl. [Fen10], [HV10], [Jan09], [NV09], [SA09], [SPK09], [Trc09], [Wei09], [AAP08], [PJAS06], [TSSS06], [irc05, S. 31 f.]).
Die Sicherheitskennzahlensysteme können grundsätzlich in zwei Kategorien eingeteilt werden. Die erste Kategorie betrachtet die Sicherheit aus der Prozessperspektive. Die Kennzahlen solcher Systeme orientieren sich an die Vollständigkeit der Prozessbeschreibung, die Prozesseffektivität sowie deren Einhaltung. Die zweite Kategorie orientiert sich an den Ergebnissen der Risikoanalysen und -bewertungen. Da die Kennzahlen primär als Werkzeuge zur Prozesssteuerung zu verstehen sind, bedarf es hierfür der Definition von Sollwerten. Durch die Messung und Interpretation der Abweichung zwischen den Soll- und den Ist-Werten kann der Bedarf für die Änderung der Prozesse abgeleitet werden. Diese Überlegung liegt der Vielzahl der offiziellen Standards zugrunde, wie beispielsweise den

zuvor in dieser Arbeit beschriebenen *NIST 800-55* oder *ISO 27004* (s. a. Abschnitt A.1). Man betrachtet die Messung der Effektivität von Sicherheitsmaßnahmen und leitet daraus eine fortwährende Überwachung und Verbesserung des Sicherheitsniveaus ab. Die Mehrheit der aktuellen Standards beschränkt sich auf triviale Kennzahlenbeispiele und bewertet die Systemsicherheit nicht anhand von einzelnen technischen Systemeigenschaften, sondern aus der Sicht der Prozesse und Policies (vgl. [Str10], [SW10]). Die untersuchten Frameworks enthalten eine generische Anleitung zur Auswahl bzw. Erstellung von Sicherheitsmetriken, jedoch keine Methodik zur Unterstützung der Organisation bei der Metrikauswahl, die am besten den sicherheitstechnischen Zielen dieser Organisation entsprechen (vgl. [FBTW10]). Im Abschnitt B.2 ist eine Reihe weiterer Arbeiten und Ansätze zur Messung der Wirksamkeit von Sicherheitsmaßnahmen aufgelistet, die im Rahmen einer systematischen Literaturrecherche analysiert wurden (s. a. Abschnitt 2.1.1.4).
Die eine Vielzahl von unterschiedlichen Ansätzen der Risikobewertung verwendenden *SIEM-Produkte* ermöglichen die zentralisierte Sammlung, Speicherung und Auswertung von Sicherheitsinformationen. Trotzdem beklagt man oft die geringe Substanz solcher Systeme bzw. der von ihnen verwendeten Messansätze. Ein beliebter Kritikpunkt besteht darin, dass ein SIEM-System keine Kennzahlen erzeugen kann, die nicht ohne das System zu ermitteln wären. Eine weitere Herausforderung besteht in der Interpretation der teilweise unzusammenhängenden Sicherheitsmetriken, die von unterschiedlichen Teilen der Organisation auf der operativen Ebene gesammelt werden (vgl. [Str10], [BMGS09]). Die damit verbundene resultierende fehlende strategische Sichtweise auf die Sicherheits- und Risikopolitik der Organisation wird oft als ein weiterer Kritikpunkt gesehen (vgl. [Fen10].)
Die *SAS-Systeme* haben mit den gleichen Herausforderungen wie die *SIEM-Produkte* zu kämpfen. Insbesondere für die Auswertungen der Vulnerability-Scanner ist es oft nicht ersichtlich, ob die Ergebnisse der Scans mit der Sicherheitspolicy übereinstimmen. Die Güte der Ergebnisse ist von dem Umfang und der Qualität der Vulnerability-Datenbank abhängig und kann im Zusammenhang mit den bereits eingesetzten Sicherheitsprodukten an Aussagekraft verlieren. Die Anwendung aktiver Scanning-Methoden kann zudem den Betrieb erheblich stören (vgl. [KS05]).

5.4. Objektivierung der Wirksamkeit von Sicherheitsmaßnahmen mithilfe des quantitativen dynamischen S&R-Managementkonzeptes „dynSRM“ als Mittel der Risikoanalyse

Untersuchungen zeigen, dass nicht alle Sicherheitsausgaben das Sicherheitsniveau einer Organisation positiv verändern. Vielmehr geht man davon aus, dass etwa ein Drittel der Sicherheitsausgaben keine nennenswerte positive Beeinflussung des Sicherheitsnive-

aus bewirkt (vgl. [BRT07]). Ein gut durchdachter, gezielter Einsatz des verfügbaren Sicherheitsbudgets ist daher von immenser Bedeutung.
Im Abschnitt 4.4 „Herleitung eines Konzeptes für das quantitative dynamische Sicherheits- und Risikomanagement“ wird – aufbauend auf den Konzepten der Risikomatrix und des Nettorisikos nach [Mül11] – ein Konzept zur Bewertung der Risikotragbarkeit und Optimierung des Risikoportfolios entwickelt. Die Einführung der zusätzlichen Risikobewertungskomponente „Schwachstellenpotenzial“ ermöglicht eine Berechnung der Effizienz von Sicherheitsmaßnahmen in Abhängigkeit vom individuellen Risikoportfolio. Das vorgestellte Konzept hat die Optimierung des Risikoportfolios eines Forschungsnetzes zum Ziel, worunter eine effizientere Ressourcenverteilung zwecks Erreichung eines möglichst hohen Sicherheitsniveaus zu verstehen ist.
Das im Rahmen dieser Arbeit ausgearbeitete und im Abschnitt 4.4 vorgestellte Konzept ermöglicht eine investitionsorientierte Bewertung der Sicherheitsprozesse in einem Forschungsnetz. Im Gegensatz zu der weit verbreiteten oft subjektiven Schätzung der Relevanz eines Schadensszenarios und dessen Höhe, die ihre Schwächen spätestens bei der Schätzung der Eintrittswahrscheinlichkeit offenbart (vgl. [BLP$^+$06]), eröffnet die vorgestellte erweiterte Betrachtungsweise neue Optimierungsmöglichkeiten für das Sicherheits- und Risikoportfolio. Das Basiskonzept „dynSRM“ ist im Zusammenhang mit der Sicherheits- und Risikoportfolio-Bewertung generisch anwendbar; seine Anwendungsfelder können auch außerhalb der medizinischen Forschung liegen. Das Konzept bietet breite Einsatzmöglichkeiten durch die potenzielle Verwendbarkeit unterschiedlicher Datenquellen für die Bestimmung von Risikovektoren und Sicherheitsmaßnahmen sowie durch die vielfältigen Möglichkeiten für die Ableitung von quantitativen Sicherheitsmetriken.
Eine sinnvolle praktische Realisierung des Konzeptes erfordert eine möglichst objektive Bestimmung der Risikovektoren $|m(r_1\vec{r}_2)|$. So kann die Länge eines Vektors durch eine Vielzahl von ms beeinflusst werden, die nicht nur unterschiedliche Ansätze der Risikobekämpfung, sondern auch unterschiedliche Produkte, Ausbaustufen und Konfigurationen eines Ansatzes sein können.
Zeitgemäße medizinische Forschung und Versorgung setzen auf solche kollaborative Technologien wie Netzwerke von Dienstleistern („networks of care providers“) und GRID-Systeme, sodass eine Vielzahl unterschiedlicher Institutionen und unabhängiger Forscher sowie die von ihnen verwendeten Ressourcen auf mehrere Standorte aufgeteilt sein können, wobei diese Aufteilung oft transparent bzw. kaum zentral kontrollierbar ist (vgl. [KBB$^+$09], [MRWC09], [OK09], [Pfe09], [Win09]). Die Anwendbarkeit des in dieser Arbeit vorgestellten Risikobetrachtungsansatzes bei der Verwendung solcher kollaborativen Technologien bedarf weiterer Untersuchungen.

5.5. Einordnung des vorgeschlagenen Konzeptes zur Effizienzbewertung von Sicherheitsmaßnahmen

Im Abschnitt 5.3 „Diskussion der Ansätze des Sicherheits- und Risikomanagements in medizinischen Forschungsnetzen“ wird eine Einteilung der Ansätze für die Messung der Informationssicherheit in zwei Kategorien vorgenommen. Der in dieser Arbeit unterbreiteter Vorschlag zur dynamischen Messung des Sicherheitsniveaus gehört zu der Kategorie der Messansätze, die sich mit der Risikoanalyse und -bewertung befassen. Im Mittelpunkt des vorgeschlagenen Ansatzes steht eine einheitliche Basis an Risikovektoren, die für eine Vielzahl von Forschungsnetzen gelten sollen. Nach der Parametrisierung dieser Datenbasis mit individuellen Daten eines Forschungsnetzes wie beispielsweise Datenart- und -menge, Angaben zu den verwendeten Plattformen, Einsatz von Outsourcing etc. erfolgt die Berechnung einer individuellen Gefährdungslage. Durch die Umsetzung von Sicherheitsmaßnahmen kann diese nun verändert werden, wobei bei der Entscheidung für den umzusetzenden Sicherheitsmaßnahmenkatalog die Notwendigkeit, die Wirksamkeit und die Verhältnismäßigkeit von Maßnahmen berücksichtigt werden müssen. Das gesetzte Ziel dieser Betrachtung ist die Erfüllung sämtlicher maßgeblichen Anforderungen unter einer möglichst effektiven Verwendung des zur Verfügung stehenden Sicherheitsbudgets.
Als Ausgangsbasis für die Definition von Risikovektoren werden im Abschnitt 4.4 „Herleitung eines Konzeptes für das quantitative dynamische Sicherheits- und Risikomanagement“ die BSI-Gefährdungskataloge vorgeschlagen. In dieser Konstellation beruht das Konzept des dynamischen Sicherheit- und Risikomanagements auf einem soliden Fundament, das sich im praktischen Einsatz bewährt hat. In gewisser Hinsicht bietet das Konzept sogar eine logische Weiterentwicklung des BSI-Modells, in dem die Effizienz von Maßnahmenkombinationen bewertet wird. Die Beschränkung der untersuchten Zielgruppe auf die medizinischen Forschungsnetze in Deutschland stellt sicher, dass der betrachtete Komplex einen überschaubaren Umfang an vergleichbaren Bedingungen aufweist. Dazu gehören beispielsweise die rechtlichen Rahmenbedingungen für die Verarbeitung von personenbezogenen Daten sowie die durch die Arbeiten der Arbeitsgruppe Datenschutz der TMF e.V. und in durchgeführten Rechtsgutachten ermittelten Anforderungen an die teilweise gemeinsam verwendeten Dienste und Produkte.[21] Diese Gemeinsamkeiten erlauben die Definition wichtigster Komponenten und der für diese Komponenten notwendigen Sicherheitskriterien für ein Forschungsnetz, die nun im Hinblick auf ihre Erfüllung bewertet werden können.
Das vorgeschlagene Konzept stellt eine quantitative Bewertungsmethode für die Sicherheit einer Forschungsnetzinfrastruktur dar. Der Ansatz erfüllt die aus [Wey88] abgeleiteten vier Kriterien der Sicherheitsmetriken, die in der Publikation „Information Security Models and Metrics“ [Wan05] in Form von Axiomen aufgestellt wurden und als formale Mindestanforderung an die Sicherheitsmetriken gelten. Die Kriterien sind im vorliegenden

[21] Beispielsweise Pseudonymisierungsdienst, PID-Generator etc.

Fall wie folgt zu interpretieren: differenzierte Sicherheitsbewertungen für unterschiedliche Infrastrukturen, gleiche Bewertung für die gleichen Infrastrukturen, Berücksichtigung externer Faktoren, die Abhängigkeit der Bewertung von der Reihenfolge der Komponenten bzw. der Maßnahmen. Dies korrespondiert mit den in [Wil09, S. 9 .ff] und [CSS+08, S. viii] geforderten Qualitätskriterien Messbarkeit, Bedeutung, Konsistenz und Wiederholbarkeit sowie Beeinflussbarkeit[22]. Ähnlich lautende Anforderungen werden in [Jaq07] definiert. Die zusätzliche Anforderung nach mehreren Messkriterien[23] kann durch die Definition mehrerer Zielfunktionen erfüllt werden (vgl. [SA10]). Auch die durch manche Experten verlangte „Übersichtlichkeit“[24] kann im Konzept durch die Auswahl eines angemessenen Detaillierungsgrades leicht erreicht werden (vgl. [BKY11, S. 6 f.], [Fab10, S. 19 f.], [XWZ+09, S. 428 f.], [Hec08], [LA05, S. 8], [Man05], [MR05]).
Aufgrund des generischen, modularen Aufbaus des Konzeptes ist die Verwendung von mehreren Metriksystemen möglich. Bei Bedarf erlaubt dies einen zweck- und zielgruppenspezifischen Einsatz von Sicherheitsmetriken, da davon auszugehen ist, dass kein Metriksystem sämtliche Anforderungen hinsichtlich Informationsbedarf und -gehalt, Verfügbarkeit, Vollständigkeit etc. erfüllen kann (vgl. [PC10, S. 52], [Bro09, S. 77], [Pir07]).
Das vorgeschlagene Bewertungskonzept berücksichtigt die ISO 27004-Empfehlung für den Metrik-Aufbau (s. a. Abschnitt A.1.1 „ISO-Normenreihe (ISO 2700X)“) und passt in das vom ISO-Standard empfohlene Metrik-Modell (siehe Abbildung 16 auf der Seite 204): Das Konzept sieht die Anreicherung der Basismetriken durch die organisationsspezifischen Informationen und die Erstellung der spezifischen abgeleiteten Risikovektoren vor; die variablen Risikoportfoliobewertungsfunktionen G_n übernehmen im vorgestellten Modell die Korrelierungsfunktion und erlauben die Berechnung der Risikoportfoliogüte (vgl. [KLR+10b]).

[22] Im Sinne der Eignung bzw. Verwendbarkeit der Metriken, um auf ihrer Basis Entscheidungen zur Verbesserung des Sicherheitsniveaus treffen zu können.

[23] At least one unit of measure.

[24] Succinctness.

5.6. Kritische Bewertung des Konzeptes zum dynamischen Sicherheits- und Risikomanagement

Im Folgenden werden die notwendigen Voraussetzungen für den praktischen Einsatz des „dynSRM“-Konzeptes sowie dessen Optimierungspotenziale diskutiert.

5.6.1. Wirtschaftlichkeit als Verhältnismäßigkeitskriterium für die Sicherheitsinvestitionen

Die Berechnung der Wirtschaftlichkeit für die Sicherheitsinvestitionen stellt sich oft als ein Problem dar. Eine möglichst objektive Berechnung ist jedoch notwendig, wenn eine Entscheidung zwischen der Implementierung mehrerer Sicherheitsmaßnahmen erfolgen soll, die dazu noch auch nur teilweise umgesetzt werden können. In den meisten Fällen ist eine Kombination mehrerer Sicherheitsmaßnahmen erforderlich, um einem Risiko effektiv zu begegnen. Aus betriebswirtschaftlicher Sicht steht im Mittelpunkt der zu lösenden Aufgabenstellung die Return on Invest-Berechnung für die Sicherheitsinvestition, auch als ROSI bezeichnet (vgl. [Kle06]).
Eine ausführliche und fundierte Auseinandersetzung mit dem Thema ROI-Berechnung für die Sicherheitsinvestitionen erfolgt im Kapitel 5 „Measuring Return on Investment (ROI) in Physical, Personnel, IT, and Operational Security Controls“ des Buches „Complete Guide to Security and Privacy Metrics : Measuring Regulatory Compliance, Operational Resilience, and ROI“ [Her07, S. 687-752] von Debra Herrmann. Innerhalb des genannten Kapitels kann z. B. die Berechnung der Kosten eines Sicherheitsvorfalls hervorgehoben werden, die in der vorliegenden Arbeit beispielsweise aus Vereinfachungsgründen mit K angegeben wurden. Debra Herrmann leitet eine ausführliche Definition der Kosten eines Sicherheitsvorfalls ab und kommt zu der folgenden umfassenden Kostenzusammensetzung (vgl. [Her07, S. 700]):[25]

$$K_t = (K_p + K_{temp} + K_r + K_v) - (S - P)$$

Die in der vorliegenden Arbeit vorgeschlagene Dreikomponentenaufteilung stellt eine Vereinfachung der Wirtschaftlichkeitsberechnung für die Sicherheitsinvestitionen dar und kann bei der Weiterentwicklung des Konzeptes durch das in [Her07] vorgestellte oder ein vergleichbares ROSI-Modell[26] ergänzt werden, das beispielsweise eine feinere Abstufung für die Schäden in Folge von sicherheitsrelevanten Schadensereignissen und einem zeitversetzten Kapitalrückfluss berücksichtigt (vgl. [Bro09, S. 25 ff.]). Die Anwendung der

[25] K_t: Gesamtkosten; K_p: dauerhafte Kosten des Vorfalls (Ersatz für Gebäude, Equipment, Hilfsstoffe und Personal); K_{temp}: temporäre Kosten des Sicherheitsvorfalls (Ersatz für Gebäude, Equipment, Hilfsstoffe und Personal); K_r: Gesamtkosten der direkten sowie indirekten Kosten (Wiederherstellung, erneute Schulungen, Verzug); K_v: Verdienstausfall (auch zukünftig); S: Schadensersatz; P: zuordenbare Versicherungsprämie.

[26] Return on Security Investment.

Kostenbetrachtung in ihrer vollen Komplexität ist jedoch im Umfeld der medizinischen Forschungsnetze in Form von internen/externen Zinsflussberechnungen kaum notwendig, da der Schwerpunkt der gewählten Betrachtung in der Entscheidung zwischen mehreren Sicherheitsmaßnahmen zugunsten einer möglichst vorteilhaften Maßnahmenkombination und nicht einer möglichst präzisen betriebswirtschaftlichen Berechnung des ROSI liegt.

5.6.2. Weiterentwicklungspotenzial des Konzeptes

Ein in dieser Arbeit nur oberflächlich behandelter Aspekt, ist die aus dem Risikomatrix-Konzept abgeleitete Definition der Risikotragbarkeit. Die im Buch von Martin Kütz „Kennzahlen in der IT“ [Küt09, S. 316 ff.] behandelten Ansätze können als Ausgangsbasis für die Definition der Risikotragbarkeit für ein Forschungsnetz sowie der passenden Sicherheitsfunktionen verwendet werden.
Das in der vorliegenden Arbeit vorgestellte Konzept der dynamischen Risikobewertung stellt eine deutliche Verbesserung im Vergleich zu der subjektiven Schätzung der Risikorelevanz und der zu erwartenden Schadenshöhe dar. Die Aufsplittung der Eintrittswahrscheinlichkeitskomponente in organisationsspezifische und -neutrale Faktoren erlaubt eine präzisere Einschätzung der Notwendigkeit von Sicherheitsmaßnahmen im Falle eines konkreten Forschungsnetzes. Als Grundvoraussetzungen für den praktischen Einsatz gilt eine zuverlässige gemeinsame, auf eine Vielzahl von Forschungsnetzen anwendbare Datenbasis für die Risikovektoren, sowie eine einheitliche und möglichst realitätsnahe Berechnungsvorschrift für die Schadenshöhen, die noch entwickelt und für die teilnehmenden Forschungsnetze zentral gepflegt werden muss (vgl. [Jaq07, S. 31. f.]). Die zentrale Erstellung einer solchen Datenbasis ist jedoch aufgrund der vergleichbaren Sicherheitsmerkmale der medizinischen Forschungsnetze mit einem vertretbaren Aufwand möglich (s. a. Abschnitte 3.1, 3.2).
Einen weiteren bedeutenden Aspekt stellt die Individualisierung der Sicherheitsfunktionen dar: Die Sicherheitsmaßnahmen besitzen unterschiedliche Kosten und Auswirkungen auf die Reduktion der Gefährdungssituation. Die Annahmen über die durchschnittlichen Kosten und vor allem über die Wirksamkeit der Maßnahmen sollen zentral und organisationsunabhängig getroffen werden. Gleichzeitig benötigt man eine Möglichkeit, die organisationsspezifischen Daten in das Berechnungsmodell wie z. B. die Anzahl der Mitarbeiter, Angaben zu den verwendeten Systemen, Systemkomponenten etc. einzubringen, um dadurch eine höhere Aussagekraft des modellierten Systemaufbaus zu erreichen. Neben den Risikovektoren müssen somit auch die Sicherheitsmaßnahmen parametrisierbar sein, um die Eigenheiten der einzelnen Forschungsnetze möglichst realitätsnah abbilden zu können.
Das vorgestellte Konzept des dynamischen Sicherheits- und Risikomanagements ist ein vielversprechender Ansatz, mit dessen Hilfe eine Objektivität bei der Auswahl von Sicherheitsmaßnahmenportfolios erreicht werden kann.

5.7. Zusammenfassung der Diskussion

In den vorhergehenden Abschnitten dieses Kapitels wurden die Ergebnisse der Arbeit im Kontext des gegenwärtigen Wissensstandes eingeordnet und in diesem Zusammenhang ausgewertet. Der erste Diskussionsabschnitt 5.1 „Bewertung des Aufbaus der Sicherheitsarchitektur für die medizinischen Forschungsnetze“ analysiert kritisch die Potenziale des Zusammenspiels zwischen den organisatorischen, administrativen und technischen Aspekten der Sicherheitsvorkehrungen, deren für die medizinische Forschung spezifischen Eigenschaften im Kapitel 3 „Bestandteile der Sicherheitsarchitektur für medizinische Forschungsnetze“ ausführlich untersucht und erörtert werden. Im Abschnitt 5.2 wird die durchgeführte schutzbedarfs- und bedrohungsorientierte Analyse diskutiert. Die Inhalte der beiden ersten Abschnitte des Kapitels 4 „Entwicklung eines Konzeptes für das dynamische S&R-Management“ werden im Abschnitt 5.3 „Diskussion der Ansätze des Sicherheits- und Risikomanagements in medizinischen Forschungsnetzen“ kritisch bewertet. Die von den etablierten Sicherheits- und Risikomanagement-Frameworks vorgeschlagenen Mess- und Steuerungsverfahren und insbesondere solche, die in den medizinischen Forschungsnetzen bereits ihre Verwendung finden, werden kritisch begutachtet. Die späteren Kapitelabschnitte befassen sich mit dem in dieser Arbeit vorgeschlagenen Konzept des dynamischen Sicherheits- und Risikomanagements „dynSRM“. Anschließend erfolgt die Einordnung des Konzeptes „dynSRM“ in das Gefüge der etablierten und existierenden Mess- und Steuerungsansätze. Der letzte Diskussionsabschnitt 5.6 „Kritische Bewertung des Konzeptes zum dynamischen Sicherheits- und Risikomanagement“ befasst sich mit den Optimierungs- und Weiterentwicklungspotenzialen des „dynSRM“-Konzeptes.

6. Zusammenfassung und Ausblick

6.1. Zusammenfassung

Für die Durchführung einer qualifizierten medizinischen Forschung sind die Speicherung und die Auswertung einer Vielzahl von forschungsrelevanten Patientendaten unabdingbar. In diesem Zusammenhang ergeben sich hohe Datenschutz- und Datensicherheitsanforderungen an die Datenprozessierung in den medizinischen Forschungsnetzen. Angesichts des enormen und kontinuierlich steigenden Koordinationsaufwandes zwischen den Datenschutz- und Datensicherheitsverantwortlichen, der zunimmt und für die einzelnen Forschungsverbünde nur schwer zu bewältigen ist, ist eine möglichst effiziente Verwendung der verfügbaren Ressourcen wichtig. Zudem stellt sich die Frage, inwieweit die vielfältigen möglichen Sicherheitsmaßnahmen im Hinblick auf den Maßnahmennutzen bzw. die -notwendigkeit angemessen sind, und wie es um die Möglichkeit einer zentralisierten Steuerung des Sicherheitsmaßnahmenportfolios bestellt ist.

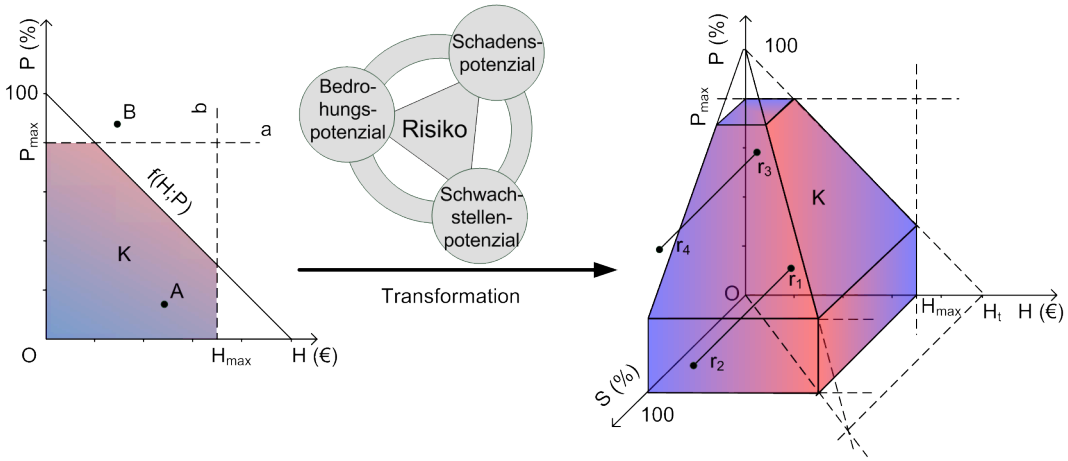

Abbildung 15.: Das Basiskonzept des dynamischen Sicherheits- und Risikomanagements „dynSRM“: Eine Kombination der Risikomatrix und des Nettorisikokonzeptes nach [Mül11] bildet die Grundlage des Konzeptes „dynSRM“. Durch die Transformation werden die in der Risikomatrix als Punkte dargestellten Risiken in die Risikovektoren des „dynSRM“-Konzeptes übertragen.

Im Rahmen der vorliegenden Arbeit werden die für die medizinischen Forschungsnetze bestehenden Risiken im Hinblick auf ihr Gefahrenpotenzial analysiert und die für die Gefahrenbewältigung notwendigen Bestandteile der Sicherheitsarchitektur entwickelt und vorgestellt. Für eine objektive Entscheidung zugunsten eines bestimmten Sicherheitsmaßnahmenkatalogs als Ausprägung einer Sicherheitsarchitektur ist eine quantitative

Bewertung der Risikosituation für ein medizinisches Forschungsnetz erforderlich. Diese erfolgt über einen Zwischenschritt: Die Gefährdungslage wird zuerst qualitativ eingeschätzt. Hierfür kommen zwei Ansätze zum Tragen: Der erste Ansatz basiert auf der Bewertung der Risikopotenziale für die vom Forschungsnetz angebotenen Dienste und für die daran beteiligten Ressourcen. Der zweite Ansatz setzt sich mit den potenziellen Angreifern und ihren Motivationen auseinander. Für die objektive Auswahl von Sicherheitsmaßnahmen wird anschließend ein *neuartiger quantitativer Messansatz* des Risikostandes in einem Forschungsnetz empfohlen. Das in der Arbeit entwickelte Konzept des dynamischen Sicherheits- und Risikomanagements "dynSRM"basiert auf der Kombination der Risikomatrix und des Nettorisikokonzeptes nach [Mül11], das die Eintrittswahrscheinlichkeit eines Risikos in die externe (bestehende Risiken) und interne (implementierte Sicherheitsmaßnahmen) Komponente aufteilt.
Die in der Abbildung 15 dargestellte Transformation überführt einen Punkt der Risikomatrix, der ein Risiko darstellt, in einen Einheitsvektor im „dynSRM"-Konzept. Der Risikovektor, dessen Ursprung stets auf der Ebene $E_{H;P}$ liegt, verläuft parallel zu der S-Achse. Die Länge eines solchen Vektors kann nun durch das Einleiten von sicherheitsrelevanten Maßnahmen (m) reduziert werden ($|m(r_1\vec{r}_2)| \leq |r_1\vec{r}_2|; |r_1\vec{r}_2| \leq 100$). Die Tragbarkeit eines Risikos kann somit auf folgende Frage zurückgeführt werden: *Liegen sämtliche Punkte des Risikovektors innerhalb des für die Menge tragbarer Risiken stehenden Körpers K* (vgl. [GDH$^+$10])?
Angesichts der vergleichbaren Sicherheitsanforderungen der medizinischen Forschungsverbünde (vgl. [RDSP06]) wird vorgeschlagen, die *Kataloge mit Risikovektoren und Sicherheitsmaßnahmen zentralisiert zur Verfügung zu stellen*. Die Sicherheitsaufgaben aus den einzelnen Forschungsnetzen, die zunehmend höhere Professionalisierungsanforderungen mit sich bringen, sind an eine übergeordnete koordinierende Stelle zu übertragen. Die regelmäßige Aktualisierung der zentralen Risiko- und Sicherheitsmaßnahmenkataloge ermöglicht es den Forschungsverbünden, ihr Risikoportfolio dynamisch neu zu bewerten.
Um das Funktionsprinzip des Konzeptes „dynSRM" an einem praktischen Beispiel zu veranschaulichen, werden die Risikovektoren und die Sicherheitsmaßnahmen aus den BSI IT-Grundschutzkatalogen verwendet (vgl. [bsi11d]). Anschließend wird ein um die Portfoliogütefunktion ergänztes Modell in einer prototypischen Implementierung umgesetzt. Auf diese Weise wird die Implementierbarkeit des „dynSRM"-Konzeptes belegt.
Im Rahmen einer systematischen Literaturrecherche wird untersucht, welche Sicherheits- und Risikomanagement-Normen, -Standards und -Frameworks derzeit in der medizinischen Forschung eingesetzt bzw. empfohlen werden. Die festgestellten und analysierten Schwächen und Inkompatibilitäten der untersuchten Ansätze erschweren die Bewertung und die Vergleichbarkeit der Sicherheitsstände einzelner Forschungsnetze. Das in dieser Arbeit entwickelte und vorgestellte Konzept des dynamischen Sicherheits- und Risikomanagements ermöglicht eine objektive quantitative Bewertung des Risikoportfolios für ein Forschungsnetz. Die Ergebnisse der durchgeführten Literaturrecherche belegen und bewei-

sen, dass das Konzept „dynSRM“ eine Innovation auf dem Gebiet der Sicherheitsbewertung und -steuerung darstellt und die maßgeblichen Qualitätskriterien für eine quantitative Sicherheitsmessmethode erfüllt (vgl. [PC10], [Fab10], [Bro09], [CSS+08], [Pir07], [Wan05]).

6.2. Schlussfolgerung und Ausblick

Die während der Erstellung dieser Arbeit gewonnenen Erkenntnisse lassen schlussfolgern, dass die meisten für die medizinischen Forschungsnetze relevanten Schadensszenarien sich mit einem – den Forschungsnetzen zumutbaren – Aufwand verhindern oder zumindest abmildern lassen. Eine wichtige Voraussetzung dafür ist eine zielgerichtete Vorgehensweise, die beispielsweise mithilfe einer gemeinsamen Sicherheitsarchitekturbeschreibung effizienter gestaltet werden kann. Die vorliegende Arbeit setzt sich sowohl mit den Sicherheitsanforderungen an die medizinischen Forschungsnetze als auch mit den Anforderungen der Forschungsnetze an die Sicherheitsmaßnahmen auseinander und ist als ein erweiterungsfähiges Rahmenwerk der Forschungsnetzsicherheit zu verstehen. Dieses Rahmenwerk erfasst die aktuellen Erkenntnisse auf dem Gebiet der Informationssicherheit und unterbreitet Ergänzungsvorschläge in Form von teilweise bereits bestehenden aber auch neuen Konzepten.

Eines dieser Vorschläge ist das im Rahmen der Arbeit entwickelte Konzept für das dynamische Sicherheits- und Risikomanagement „dynSRM“. Als Mess- und Steuerungsinstrument für die Sicherheitsarchitektur erlaubt es eine Bewertung der Sicherheits- und Risikosituation und leistet Unterstützung bei der Entscheidung über die Zusammensetzung des Sicherheitsmaßnahmenportfolios. Durch die zentralisierte Gestaltung von Sicherheits- und Risikokatalogen können Synergieeffekte genutzt werden: Die für eine qualitativ hochwertige, objektive Bewertung der Gefährdungslage notwendige Kompetenz kann an einer zentralen Stelle aufgebaut werden, wodurch die einzelnen Forschungsverbünde entlastet werden können. Die Anwendung des Konzeptes kann die Argumentation für die Notwendigkeit der Implementierung von Sicherheitsmaßnahmen in den Forschungsverbünden objektivieren und somit erleichtern. Eine regelmäßige Aktualisierung der zentralen Kataloge sorgt für die dynamische stets aktuelle Einschätzung des Sicherheits- und Risikoportfolios in den einzelnen Forschungsnetzen.

Der rasanten Entwicklung im Bereich Informationssicherheit Rechnung tragend wurden in der vorliegenden Arbeit nur wenige konkrete Produkte als Lösungsmöglichkeiten genannt. Vielmehr wurde angestrebt, die grundlegenden hinter den konkreten Lösungen stehenden Technologien aufgrund ihrer längeren Beständigkeit zu beschreiben. Somit hat die vorliegende Arbeit ein stabiles Grundgerüst, das eine zeitgemäße, erweiterungsfähige Basis für die Sicherheitsarchitektur der medizinischen Forschungsnetze bietet.

Literaturverzeichnis

[AAP08] Aime, Marco D. ; Atzeni, Andrea S. ; Pomi, Paolo C.: The Risks with Security Metrics. *In: Proceedings of the 4th ACM workshop on Quality of Protection (QoP'08)*. New York, NY, USA : ACM, November 2008, S. 65–70

[AASM11] Aissa, Anis B. ; Abercrombie, Robert K. ; Sheldon, Frederick T. ; Mili, Ali: Defining and Computing a Value Based Cyber-Security Measure. In: *Information Systems and e-Business Management* 11 (2011), Nr. 4, S. 1–21

[ABC+11] Antony, Gisela ; Buckow, Karoline ; Chan, Andrew ; Gold, Ralf ; Hemmer, Bernhard ; Jochim, A. ; Kieseier, Bernd ; Paul, Friedemann ; Posevitz-Fejfar, Anita ; Rienhoff, Otto ; Schippling, Sven ; Starck, Michaela ; Stroet, Anke ; Weber, Frank ; Wiendl, Heinz ; Winkelmann, Alexander: *Datenschutzkonzept für das Kompetenznetz Multiple Sklerose (KKNMS)*. (2011). – Beziehbar über die TMF

[ACPZ01] Adams, Carlisle ; Cain, Pat ; Pinkas, Denis ; Zuccherato, Robert: *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*. (2001). `http://www.ietf.org/rfc/rfc3161.txt`, Abruf: 3.3.2012

[AD01] Alberts, Christopher J. ; Dorofee, Audrey J.: *OCTAVE Method Implementation Guide*. (2001). `http://www.sei.cmu.edu/downloads/octave/OCTAVE_OMIG.zip`, Abruf: 3.3.2012. – Version 2.0

[AE08] Ahlers, Ernst ; Endres, Johannes: Fernzugriff übers Internet. In: *c't special* 8 (2008), Nr. 1, S. 124–127

[AJ10] Appari, Ajit ; Johnson, Eric M.: Information Security and Privacy in Healthcare : Current State of Research. In: *International Journal of Internet and Enterprise Management* 6 (2010), Nr. 4, S. 279–314

[Als10] Alshboul, Abdullah: Information Systems Security Measures and Countermeasures : Protecting Organizational Assets from Malicious Attacks. In: *Communications of the IBIMA* 10 (2010), Nr. 48687, S. 1–9

[AM06] Anderson, Ross ; Moore, Tyler: The Economics of Information Security. In: *Science* 314 (2006), Nr. 5799, S. 610–613

[AMR07] Alhazmi, Omar H. ; Malaiya, Yashwant K. ; Ray, Indrajit: Measuring, Analyzing and Predicting Security Vulnerabilities in Software Systems. In: *Computers & Security* 26 (2007), Nr. 3, S. 219–228

[And03] Anderson, Ross: *Trusted Computing : Frequently Asked Questions*. (2003). `http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html`, Abruf: 11.1.2012. – Version 1.1

[ans04] ANSI INCITS, International Committee for Information Technology Standards (Hrsg.): *Security Standard ANSI INCITS 359-2004 for Role Based Access Control (RBAC)*. (2004). `http://www.techstreet.com/cgi-bin/detail?product_id=1151353`, Abruf: 3.3.2012

[ANT06] Arora, Ashish ; Nandkumar, Anand ; Telang, Rahul: Does Information Security Attack Frequency Increase with Vulnerability Disclosure? An Empirical Analysis. In: *Information Systems Frontiers* 8 (2006), Nr. 5, S. 350–362

[ATX08] Arora, Ashish ; Telang, Rahul ; Xu, Hao: Optimal Policy for Software Vulnerability Disclosure. In: *Management Science* 54 (2008), Nr. 4, S. 642–656

[axe99] AXENT Technologies, Inc. (Hrsg.): *Everything You Need to Know About Intrusion Detection*. (1999). `http://www.neocom.pl/dokumenty/Axent/ids2.pdf`, Abruf: 3.3.2012

[Axe08] Axelrod, Warren C.: Accounting for Value and Uncertainty in Security Metrics. In: *Information System Control Journal* 6 (2008), S. 1–6

[Bac03] Bachfeld, Daniel: *Mit roher Gewalt : Angriff auf Passwörter in Windows-Netzwerken*. (2003). `http://www.heise.de/security/Mit-roher-Gewalt--/artikel/40744`, Abruf: 11.1.2012

[Bay11] Bayuk, Jennifer L.: Alternative Security Metrics. *In: Eighth International Conference on Information Technology : New Generations*. Las Vegas, NV, USA : ITNG, April 2011, S. 943–946

[BBM+08] Bartol, Nadya ; Bates, Brian ; Mercedes-Goertzel, Karen ; Winograd, Theodore ; Karon, Cynthia: *Measuring Cyber Security and Information Assurance* / Information Assurance Technology Analysis Center (IATAC). NJ, USA, Mai 2008. `http://iac.dtic.mil/iatac/download/cybersecurity.pdf`, Abruf: 20.12.2011. – State-of-the-Art Report

[BC96] Barrows, Randolph C. ; Clayton, Paul D.: Privacy, Confidentiality, and Electronic Medical Records. In: *Journal of the American Medical Informatics Association* 3 (1996), Nr. 2, S. 139–148

[Bea12] Beale, Jay: *BASTILLE-LINUX : The Bastille Hardening Program*. (2012). `http://bastille-linux.sourceforge.net/`, Abruf: 3.3.2012

[Bel06] Bellovin, Steven M.: On the Brittleness of Software and the Infeasibility of Security Metrics. In: *Security & Privacy, IEEE* 4 (2006), Nr. 4, S. 96

[BGH+06] Becker, Regina ; Goebel, Jürgen W. ; Hummel, Michael ; Ihle, Peter ; Kiehntopf, Michael ; Leopold, Christian ; Pommerening, Klaus ; Rienhoff, Otto ; Sellge, Eva ; Semler, Sebastian C.: *Bestandsaufnahme und Charakterisierung von Biobanken : Systematisierung, wissenschaftliche Bewertung, Finanzierungsmodelle und Konzepte zu Datenschutz und Patienteneinwilligung* / Telematikplattform für Medizinische Forschungsnetze e.V. (TMF). Berlin, Juni 2006 (P999061). – TMF-Gutachten Biobanken. – Version 1.20 – Beziehbar über die TMF

[BKY11] Barabanov, Rostyslav ; Kowalski, Stewart ; Yngström, Louise: *Information Security Metrics : State of the Art* / Stockholm University, Department of Computer and System Sciences. Stockholm, Sweden, März 2011. `https://secprj.dsv.su.se/coins/files/Information_security_metrics_-_State_of_the_art.pdf`, Abruf: 19.12.2011 (DSV Report Series No 11-007). – Forschungsbericht

[BL73] Bell, David E. ; LaPadula, Leonard J.: *Secure Computer Systems : Mathematical Foundations : An Electronic Reconstruction by Len LaPadula of the Original*. 1973. `http://www.albany.edu/acc/courses/ia/classics/belllapadula1.pdf`, Abruf: 3.3.2012 (MITRE 2547). – Technical Report. – Volume I

[BLP+06] Buldas, Ahto ; Laud, Peeter ; Priisalu, Jaan ; Saarepera, Märt ; Willemson, Jan: Rational Choice of Security Measures via Multi-Parameter Attack Trees. In: López, Javier (Hrsg.): *Critical Information Infrastructures Security* Bd. 4347. Berlin/Heidelberg : Springer-Verlag, 2006. – ISBN 3-540690832, S. 235–248

[BM08] Boyer, Wayne ; McQueen, Miles: Ideal Based Cyber Security Technical Metrics for Control Systems. In: Lopez, Javier (Hrsg.) ; Hämmerli, Bernhard (Hrsg.): *Critical Information Infrastructures Security* Bd. 5141. Berlin/Heidelberg : Springer-Verlag, 2008. – ISBN 978-3540890959, S. 246–260

[BMGS09] Beres, Yolanta ; Mont, Marco C. ; Griffin, Jonathan ; Shiu, Simon: Using Security Metrics Coupled with Predictive Modeling and Simulation to Assess Security Processes. *In: Proceedings of the 3rd International Symposium on Empirical Software Engineering and Measurement (ESEM'09).* Washington, DC, USA : IEEE Computer Society, Oktober 2009, S. 564–573

[BMS06] Balzarotti, Davide ; Monga, Mattia ; Sicari, Sabrina: Assessing the Risk of Using Vulnerable Components. In: Gollmann, Dieter (Hrsg.) ; Massacci, Fabio (Hrsg.) ; Yautsiukhin, Artsiom (Hrsg.): *Quality of Protection : Security Measurements and Metrics* Bd. 23. New York, NY, USA : Springer-Verlag, Juni 2006. – ISBN 978-0387290164, S. 65–78

[BN08] Böhme, Rainer ; Nowey, T: Economic Security Metrics. In: Eusgeld, Irene (Hrsg.) ; Freiling, Felix C. (Hrsg.) ; Reussner, Ralf (Hrsg.): *Dependability Metrics* Bd. 4909. Berlin Heidelberg : Springer-Verlag, 2008. – ISBN 978-3540245513, S. 176–187

[Böh10] Böhme, Rainer: Security Metrics and Security Investment Models. In: Echizen, Isao (Hrsg.) ; Kunihiro, Noboru (Hrsg.) ; Sasaki, Ryôichi (Hrsg.): *Advances in Information and Computer Security* Bd. 6434. Berlin/Heidelberg : Springer-Verlag, 2010. – ISBN 978-3642168246, S. 10–24

[Bor08] Borchers, Detlef: Karte ohne Eigenschaften : Die Infrastruktur für die elektronische Gesundheitskarte. In: *c't – Magazin für Computertechnik* 8 (2008), Nr. 18, S. 76–81

[Bou05] Boulanger, Alan: Open-Source Versus Proprietary Software : Is One More Reliable and Secure Than the Other? In: *IBM Systems Journal* 44 (2005), Nr. 2, S. 239–248

[BP01] Burnett, Steve ; Paine, Stephen: *Kryptographie : RSA Security's Official Guide.* Bonn : Mitp-Verlag, 2001. – ISBN 978-3826607806

[BP07] Baer, Walter S. ; Parkinson, Andrew: Cyberinsurance in IT Security Management. In: *IEEE Security and Privacy* 5 (2007), Nr. 3, S. 50–56

[Bro09] Brotby, Krag W.: *Information Security Management Metrics : A Definitive Guide to Effective Security Monitoring and Measurement.* Boca Raton, Florida, USA : CRC Press, Auerbach, 2009. – ISBN 978-1420052855

[BRR99] Buckovich, Suzy A. ; Rippen, Helga E. ; Rozen, Michael J.: Driving Toward Guiding Principles. In: *Journal of the American Medical Informatics Association* 6 (1999), Nr. 2, S. 122–133

[BRT07] Baker, Wade H. ; Rees, Loren P. ; Tippett, Peter S.: Necessary Measures : Metric-Driven Information Security Risk Assessment and Decision Making. In: *Communications of the ACM* 50 (2007), Nr. 10, S. 101–106

[BS06] Beckmann, Michael ; Sax, Ulrich ; TMF, Telematikplattform für Medizinische Forschungsnetze e. V. (Veranst.): *Bericht aus dem Kompetenznetz Angeborene Herzfehler*. Berlin, Geschäftsstelle TMF e. V. am 11.12.2006. – Sicherheitskonzepte in der vernetzten medizinischen Forschung : TMF-Workshop. – Beziehbar über die TMF

[BS08] Bachfeld, Daniel ; Steffen, Andreas: VPN-Protokolle und Standards. In: *c't special* 8 (2008), Nr. 2, S. 62–67

[BSB07] Brocke, Jan vom ; Strauch, Gereon ; Buddendick, Christian: Return on Security Investments : Design Principles of Measurement Systems Based on Capital Budgeting. In: Mayr, Heinrich C. (Hrsg.) ; Karagiannis, Dimitris (Hrsg.): *ISTA*(LNI) Bd. 107. Kharkiv, Ukraine : GI, Mai 2007, S. 21–32

[bsi05] BSI, Bundesamt für die Sicherheit in der Informationstechnik (Hrsg.): *Konzeption von Sicherheitsgateways*. (2005). `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/Konz_SiGw_pdf.pdf?__blob=publicationFile`, Abruf: 3.3.2012. – Version 1.0

[bsi08a] BSI, Bundesamt für die Sicherheit in der Informationstechnik (Hrsg.): *BSI-Standard 100-1 : Managementsysteme für Informationssicherheit (ISMS)*. (2008). `https://www.bsi.bund.de/cae/servlet/contentblob/471450/publicationFile/31048/standard_1001.pdf`, Abruf: 25.12.2011. – Version 1.5

[bsi08b] BSI, Bundesamt für die Sicherheit in der Informationstechnik (Hrsg.): *BSI-Standard 100-2 : IT-Grundschutz-Vorgehensweise*. (2008). `https://www.bsi.bund.de/cae/servlet/contentblob/471452/publicationFile/31047/standard_1002.pdf`, Abruf: 25.12.2011. – Version 2.0

[bsi08c] BSI, Bundesamt für die Sicherheit in der Informationstechnik (Hrsg.): *BSI-Standard 100-3 : Risikoanalyse auf der Basis von IT-Grundschutz*. (2008). `https://www.bsi.bund.de/cae/servlet/contentblob/471454/publicationFile/31046/standard_1003.pdf`, Abruf: 25.12.2011. – Version 2.5

[bsi08d] BSI, Bundesamt für die Sicherheit in der Informationstechnik (Hrsg.): *BSI-Standard 100-4 : Notfallmanagement*. (2008). `https://www.bsi.bund.de/cae/servlet/contentblob/471452/publicationFile/31047/standard_1002.pdf`, Abruf: 25.12.2011. – Version 1.0

[bsi08e] BSI, Bundesamt für die Sicherheit in der Informationstechnik (Hrsg.): *Guide for the Transition from CC v2.3 to CC v3.1 for ADV : The Common Criteria Portal*. (2008). http://www.commoncriteriaportal.org/adv_tg.html, Abruf: 3.3.2012

[bsi08f] BSI, Bundesamt für die Sicherheit in der Informationstechnik (Hrsg.): *Sichere Informationstechnik für unsere Gesellschaft*. 2008. https://www.bsi.bund.de/cae/servlet/contentblob/487524/publicationFile/30755/bsi_jahresbericht_2006-2007_pdf, Abruf: 3.3.2012 (BSI JB 2006-2007). – BSI-Jahresbericht

[bsi09a] BSI, Bundesamt für die Sicherheit in der Informationstechnik (Hrsg.): *Common Criteria : ISO/IEC 15408*. (2009). https://www.bsi.bund.de/cae/servlet/contentblob/486784/publicationFile/35316/F06CommonCriteria_pdf.pdf, Abruf: 3.3.2011

[bsi09b] BSI, Bundesamt für die Sicherheit in der Informationstechnik (Hrsg.): *IT Sicherheit auf Basis der Common Criteria : Ein Leitfaden*. (2009). https://www.bsi.bund.de/cae/servlet/contentblob/487910/publicationFile/30228/cc_leitf_pdf.pdf, Abruf: 24.4.2011

[bsi11a] BSI, Bundesamt für die Sicherheit in der Informationstechnik (Hrsg.): *Ergänzung zum BSI-Standard 100-3 : Verwendung der elementaren Gefährdungen aus den IT-Grundschutz-Katalogen zur Durchführung von Risikoanalysen*. (2011). https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1003_ergaenzung_pdf.pdf?__blob=publicationFile, Abruf: 25.12.2011. – Version 2.5

[bsi11b] BSI, Bundesamt für die Sicherheit in der Informationstechnik (Hrsg.): *Gefährdungskatalog G 0 „Elementare Gefährdungen“*. (2011). https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Gefaehrdungskatalog-G0-ElementareGefaehrdungen.pdf?__blob=publicationFile, Abruf: 25.12.2011. – Version 2.5

[bsi11c] BSI, Bundesamt für die Sicherheit in der Informationstechnik (Hrsg.): *Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik*. (2011). https://www.bsi.bund.de/ContentBSI/Themen/ZertifizierungundAnerkennung/ZertifierungnachCCundITSEC/ITSicherheitskriterien/CommonCriteria/cc.html, Abruf: 16.3.2011

[bsi11d] BSI, Bundesamt für die Sicherheit in der Informationstechnik (Hrsg.): *IT-Grundschutz-Kataloge*. (2011). https://www.bsi.bund.de/cln_174/DE/Themen/weitereThemen/ITGrundschutzKataloge/itgrundschutzkataloge_node.html, Abruf: 1.1.2012. – 12. Ergänzungslieferung

[bsi11e] BSI, Bundesamt für die Sicherheit in der Informationstechnik (Hrsg.): *Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz*. (2011). `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Vergleich_ISO27001_GS.html`, Abruf: 3.3.2012. – 12. Ergänzungslieferung

[Bur05] Burnett, Mark: *Perfect Passwords : Selection, Protection, Authentification*. Rockland, Massachusetts, USA : Syngress Media, 2005. – ISBN 978-1597490412

[CD09] Cottin, Claudia ; Döhler, Sebastian: *Risikoanalyse : Modellierung, Beurteilung und Management von Risiken mit Praxisbeispielen*. Wiesbaden : Vieweg+Teubner, 2009. – ISBN 978-3834805942

[CFF+04] Chiachiarella, Fred ; Fasting, Uwe ; Fey, Tilo ; Leppler, Stefan ; Lux, Gisbert ; Lubb, Peter ; Moser, Andreas ; Otten, Günther ; Schlattmann, Johannes ; Schumann, Sven ; Schweizer, Lothar ; Souren, Franz-Josef ; Ausschuss Betriebswirtschaft und Informationstechnologie Gesamtverband der Deutschen Versicherungswirtschaft e. V. (Hrsg.): *Das Risiko Trusted Computing für die deutsche Versicherungswirtschaft : Positionspapier der deutschen Versicherungswirtschaft*. (2004). `http://www.gdv-online.de/tcg/pos_tcg.pdf`, Abruf: 3.3.2012. – Band 13 der Schriftenreihe des Betriebswirtschaftlichen Institutes des GDV

[Chr11] Christin, Nicolas: Network Security Games : Combining Game Theory, Behavioral Economics, and Network Measurements. *In: Conference on Decision and Game Theory for Security*. College Park, Maryland, USA : GameSec, November 2011, S. 1–3

[cis04] CISWG, Corporate Information Security Working Group (Hrsg.): *Report of the Best Practices and Metrics Teams* / Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census. 2004. `http://net.educause.edu/ir/library/pdf/CSD3661.pdf`, Abruf: 20.12.2011. – Technical Report. – Revised 10.01.2005

[cis06] Cisco Systems, Inc. (Hrsg.): *Cisco and Microsoft Unveil Joint Architecture for NAC-NAP Interoperability*. (2006). `http://newsroom.cisco.com/dlls/2006/prod_090606.html`, Abruf: 17.5.2010

[cit11] Citrix Systems, Inc. (Hrsg.): *All Products : Citrix Knowledge Center*. (2011). `http://support.citrix.com/product/`, Abruf: 11.3.2011

[CMS+00] Coatrieux, Gouenou ; Maitre, H. ; Sankur, Bulent ; Rolland, Y. ; Collorec, R.: Relevance of Watermarking in Medical Imaging. *In: Proceedings*

of the Information Technology Applications in Biomedicine (2000 IEEE EMBS). Arlington, VA, USA : IEEE Computer Society, November 2000, S. 250–255

[CNO08] Courtois, Nicolas T. ; Nohl, Karsten ; O'Neil, Sean: *Algebraic Attacks on the Crypto-1 Stream Cipher in MiFare Classic and Oyster Cards* / Cryptology ePrint Archive. 2008. http://eprint.iacr.org/2008/166, Abruf: 24.4.2011 (2008/166). – Research Announcement. – Version: 20080414:185254

[CS07] Case, Gary ; Spalding, George ; OGC, Office of Government Commerce (Hrsg.): *ITIL V3 : Continual Service Improvement*. 2. überarb. Aufl. London, UK : TSO, The Stationery Office, 2007. – ISBN 978-0113310494

[CSF+08] Cooper, David ; Santesson, Stefan ; Farrell, Stephen ; Boyen, Sharon ; Housley, Russel ; Polk, Tim W.: *RFC 5280 : Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. (2008). http://tools.ietf.org/rfc/rfc5280.txt, Abruf: 24.4.2011

[CSS+08] Chew, Elizabeth ; Swanson, Marianne ; Stine, Kevin ; Bartol, Nadya ; Brown, Anthony ; Robinson, Will ; NIST, National Institute of Standards and Technology (Hrsg.): *Performance Measurement Guide for Information Security*. (2008). http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf, Abruf: 18.11.2011. – NIST Special Publication 800-55. – Revision 1

[CW07] Cannon, David T. ; Wheeldon, David ; OGC, Office of Government Commerce (Hrsg.): *ITIL V3 : Service Operation*. 2. überarb. Auflage. London, UK : TSO, The Stationery Office, 2007. – ISBN 978-0113310463

[CYK04] Chaula, Job A. ; Yngström, Louise ; Kowalski, Stewart: Security Metrics and Evaluation of Information Systems Security. *In: Proceedings of the ISSA 2004 Enabling Tomorrow Conference*. Pretoria, South Africa : ISSA, Juni 2004, S. 1–12

[dat11] Datenschutzzentrum Schleswig-Holstein (Hrsg.): *GG, BDSG, LDSG, StGB, Patientendatenschutz im Krankenhaus*. (2011). https://www.datenschutzzentrum.de/medizin/krankenh/patdskh.htm#1, Abruf: 18.3.2011

[Dav02] Davis, Carlton R.: *IPSec : Tunneling im Internet*. Bonn : Mitp-Verlag, 2002. – ISBN 978-3826608094

[DB11] Datta, S. P. ; Banerjee, Pranab: Guideline for Performance Measures of Information Security of IT Network and Systems. In: *International Journal of Research and Reviews in Next Generation Networks* 1 (2011), Nr. 1, S. 39–43

[DBN10] Das, Tathagata ; Bhagwan, Ranjita ; Naldurg, Prasad: Baaz : A System for Detecting Access Control Misconfigurations. *In: Proceedings of the 19th USENIX conference on Security (USENIX Security'10).* Berkeley, CA, USA : USENIX Association, 2010, S. 161–176

[DC96] DiLonardo, R. L. ; Clarke, R. V.: Reducing the Rewards of Shoplifting : An Evaluation of Ink Tags. In: *Security Journal* 7 (1996), Nr. 1, S. 11–14

[DC06] Debold, Peter ; CIOffice, Universität Göttingen: *Datensicherheit und Datenschutz im Nationalen Register und Kompetenznetz Angeborene Herzfehler.* (2006). `http://www.kompetenznetz-ahf.de/fileadmin/documents/knahf_datenschutzkonzept_ver_1_24.pdf`, Abruf: 24.4.2011. – Version 1.24 – Beziehbar über die TMF

[Dep03] Department of Health and Human Services: *45 CFR Parts 160, 162, and 164 Health Insurance Reform : Security Standards; Final Rule.* Federal Register, Vol. 68, No. 34, (2003)

[Der07] Der Bayerische Landesbeauftragte für den Datenschutz: *Merkblatt zum Datenschutz bei medizinischen Studien mit Patientendaten.* (2007). `http://www.datenschutz-bayern.de/technik/orient/merkblatt_med_studien.html`, Abruf: 24.4.2011. – Version 1.0

[Deu10] Deutscher Ethikrat: *Humanbiobanken für die Forschung : Stellungnahme.* Berlin : Hermann Schlesener KG, 2010. – ISBN 978-3941957053

[DHH05] DHHS, Department of Health and Human Services: *Basics of Security Risk Analysis and Risk Management.* (2005). `http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf`, Abruf: 20.2.2011. – Revision 3/2007

[DHS08] DHS, U.S. Department of Homeland Security: *DHS Risk Lexicon.* (2008). `http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf`, Abruf: 22.12.2011

[Die08] Dierks, Christian: *Pseudonymisierungsverpflichtung bei Anwendungsfällen mit gleichzeitigem Versorgungs- und Forschungsbezug und Fragen zur Relevanz des Medizinproduktegesetzes (MPG)* / Telematikplattform für Medizinische Forschungsnetze e. V. (TMF). 2008 (P039031). – Teilgutachten zu Fragen des Datenschutzes in klinischen Studien. – S. B1-B44. – Version 1.0 – Beziehbar über die TMF

[DL11] Dunaev, Dmitriy ; Lengyel, László: Information Security : Concepts, Indicators, Measurements. In: *Theoretical and Applied Aspects of Cybernetics.* Kiew, Ukraine : TAAC, Februar 2011 (TAAC'11), S. 22–24

[DO05] Demotes-Mainard, Jacques ; Ohmann, Christian: European Clinical Research Infrastructures Network: Promoting Harmonisation and Quality in European Clinical Research. In: *Lancet* 365 (2005), Nr. 9454, S. 107–108

[Dog10] Dogaheh, Morteza A.: Introducing a Framework for Security Measurements. *In: 2010 IEEE International Conference on Information Theory and Information Security.* Beijing, China : ICITIS, Dezember 2010, S. 638–641

[Dom01] Domhan, Gregor: *LAN-Sicherheitskonzept und Aufbau eines Firewall-Systems.* Aalen, Fachhochschule, Diplomarbeit, 2001. `http://www.domhan.de/Diplomarbeit.pdf`, Abruf: 15.3.2009

[DR08] Dierks, Tim ; Rescorla, Eric: *The Transport Layer Security (TLS) Protocol Version 1.2.* (2008). `http://tools.ietf.org/rfc/rfc5246.txt`, Abruf: 24.4.2011

[DSMS07] Drepper, Johannes ; Semler, Sebastian C. ; Mohammed, Yassene ; Sax, Ulrich: Aktuelle Themen des Datenschutzes und der Datensicherheit in der biomedizinischen Forschung. In: *Grid-Computing in der biomedizinischen Forschung : Datenschutz und Datensicherheit.* München : Urban & Vogel, Februar 2007. – ISBN 978-3899352375, S. 25–36

[Eck07] Eckert, Claudia: *IT-Sicherheit : Konzepte – Verfahren – Protokolle.* 5. überarb. Aufl. München : Oldenbourg Wissenschaftsverlag, 2007. – ISBN 978-3486582703

[emc11] EMC, EMC Corporation (Hrsg.): *Form 8-K : Pursuant to Section 13 or 15 (d) of the Securities Exchange Act of 1934* / United States Securities and Exchange Commission. Washington, DC, USA, März 2011 (04-2680009). – Current Report

[ems12] EMSCB, European Multilaterally Secure Computing Base (Hrsg.): *Towards Trustworthy Systems with Open Standards and Trusted Computing.* (2012). `http://www.emscb.de/content/pages/Einleitung.htm`, Abruf: 15.1.2012

[EW06] Eberstein, Huberta ; Wolf, Andreas ; Christian-Albrechts-Universität Kiel (Hrsg.): *Datenmanagementkonzept für popgen : Populationsgenetische Untersuchung klinischer Phänotyp-Genotyp-Beziehungen in Nord-Schleswig-Holstein.* (2006). – Version 0.4 – Beziehbar über die TMF

[Fab08] Faber, Frank: Unter Verdacht : Eine russische Bande professionalisiert das Cybercrime-Business. In: *c't – Magazin für Computertechnik* 8 (2008), Nr. 11, S. 92–96

[Fab10] Faber, Eberhard: Measuring Information Security : Guidelines to Build Metrics. In: Pohlmann, Norbert (Hrsg.) ; Reimer, Helmut (Hrsg.) ; Schneider,

Wolfgang (Hrsg.): *ISSE 2009 Securing Electronic Business Processes*. Wiesbaden : Vieweg+Teubner, 2010. – ISBN 978-3834809582, S. 17–26

[FBTW10] Fruehwirth, Christian ; Biffl, Stefan ; Tabatabai, Mohamed ; Weippl, Edgar: Addressing Misalignment Between Information Security Metrics and Business-Driven Security Objectives. *In: Proceedings of the 6th International Workshop on Security Measurements and Metrics (MetriSec'10)*. New York, NY, USA : ACM, 2010, S. 1–7

[Fen10] Fenz, Stefan: Ontology-based Generation of IT-Security Metrics. *In: Proceedings of the ACM Symposium on Applied Computing (SAC'10)*. New York, NY, USA : ACM, 2010, S. 1833–1839

[FGHK05] Ferraiolo, David ; Gavrila, Serban ; Hu, Vincent ; Kuhn, Richard D.: Composing and Combining Policies Under the Policy Machine. *In: Proceedings of the 10th ACM Symposium on Access Control Models and Technologies (SACMAT'05)*. New York, NY, USA : ACM, Februar 2005, S. 11–20

[FHM+07] Freeman, Trevor ; Housley, Russel ; Malpani, Ambarish ; Cooper, David ; Polk, Tim W.: *RFC 5055 : Server-Based Certificate Validation Protocol (SCVP)*. (2007). http://tools.ietf.org/rfc/rfc5055.txt, Abruf: 3.3.2012

[FK92] Ferraiolo, David ; Kuhn, Richard: Role-Based Access Controls. *In: Proceedings of the 15th NIST-NCSC National Computer Security Conference (NCSC'92)*. Baltimore, MD, USA : NIST, Oktober 1992, S. 554–563

[FK95] Ferraiolo, David ; Kuhn, Rick ; NIST, National Institute of Standards and Technology (Hrsg.): *An Introduction to Role-Based Access Control*. (1995). http://csrc.nist.gov/rbac/NIST-ITL-RBAC-bulletin.html, Abruf: 3.3.2012. – NIST/ITL Bulletin

[Foo97] Food and Drug Administration: *Title 21 : Foods and Drugs I : Food and Drug Administration Department of Health and Human Services Subchapter A : General Part 11 : Electronic Records;Electronic Signatures*. 62 FR 13464. (1997). http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11, Abruf: 3.3.2012

[FPW07] Faisst, Ulrich ; Prokein, Oliver ; Wegmann, Nico: Ein Modell zur dynamischen Investitionsrechnung von IT-Sicherheitsmaßnahmen. In: *Zeitschrift für Betriebswirtschaft* 77 (2007), Nr. 5, S. 511–538

[Fra97] Fraser, Barbara: *Request for Comments : 2196 : Site Security Handbook*. (1997). http://www.ietf.org/rfc/rfc2196.txt, Abruf: 3.3.2012

[Fra10] Frankenstein, Ronny: Qual der Wahl : Zwei Rahmenwerke zur IT-Sicherheit unter der Lupe. In: *iX special* 10 (2010), Nr. 3, S. 142–146

[FRG05] Fickert, Tim ; Richter, Gerd ; Gerling, Rainer W.: VPN im heterogenen Netz : Anwenderbericht aus der Max-Planck-Gesellschaft. In: *<kes> – The Information Security Journal* 5 (2005), Nr. 1, S. 8–10

[Fri95] Fritz, Wolfgang: *Marketing-Management und Unternehmenserfolg*. 2. überarb. und erg. Aufl. Stuttgart : Schaeffer-Poeschel, 1995. – ISBN 3-79100946X

[FSG+01] Ferraiolo, David ; Sandhu, Ravi ; Gavrila, Serban ; Kuhn, Richard D. ; Chandramouli, Ramaswamy: Proposed NIST Standard for Role-Based Access Control. In: *ACM Transactions on Information and System Security* 4 (2001), Nr. 3, S. 224–274

[GDH+10] Grenz, Michael ; Dickmann, Frank ; Helbing, Krister ; Pommerening, Klaus ; Sax, Ulrich: Aspekte der Optimierung des Sicherheits- und Risikomanagements in medizinischen Forschungsnetzen. In: Schmücker, Paul (Hrsg.) ; Elsässer, Karl-Heinz (Hrsg.) ; Hayna, Steffen (Hrsg.): *55. GMDS-Jahrestagung*. Dietzenbach : Antares Computer Verlag GmbH, September 2010, S. 647–649

[Gee10] Geer, Daniel E. Jr.: A Time to Rethink. In: *IEEE Security & Privacy Magazine* 8 (2010), Nr. 4, S. 86–87

[GK07] Goebel, Jurgen W. ; Krawczak, Michael: Juristische Grundlagen von Biomaterialbanken : Mehr Rechtssicherheit fur Betreiber und Spender in Deutschland. In: *it – Information Technology* 49 (2007), Nr. 6, S. 339–344

[GK10] Günther, Andreas ; Kuhn, Stefan: *Datenschutzkonzept des deutschen DPLD Registers und Biobank des GOLDnet : German Network for Diffuse Parenchymal Lung Diseases (Deutsches Netzwerk für diffus parenchymatöse Lungenerkrankungen)*. (2010). – Version 1.1 – Beziehbar über die TMF

[GKZ01] Goddard, Steve ; Kieckhafer, Roger M. ; Zhang, Yuping: An Unavailability Analysis of Firewall Sandwich Configurations. *In: Proceedings of the 6th International Symposium on High-Assurance Systems Engineering (HASE 2001)*. Albuquerque, NM, USA : IEEE Computer Society, 2001, S. 139–148

[GM08] Günther, Andreas ; Müller, Johannes: *Datenschutzkonzept des European IPF Network : Natural course, Pathomechanisms and Novel Treatment Options in Idiopathic Pulmonary Fibrosis*. (2008). – Version 1.5 – Beziehbar über die TMF

[GMNP02] Georgiadis, Christos K. ; Mavridis, Ioannis K. ; Nikolakopoulou, Georgia ; Pangalos, George I.: Implementing Context and Team Based Access

Control in Healthcare Intranets. In: *Medical Informatics and the Internet in Medicine* 27 (2002), Nr. 3, S. 185–201

[Gre03] Grenz, Michael: *Intrusion Detection-Systeme : Erstellung eines Implementierungskonzeptes für Delta Lloyd Deutschland AG*. Mannheim, Berufsakademie, Diplomarbeit, 2003

[Gua09] Guarda, Paolo: Data Protection, Information Privacy, and Security Measures : An Essay on the European and the Italian Legal Frameworks. In: *Ciberspazio e diritto* (2009), S. 65–92

[GV07] Grimm, Christian ; Voigt, Gabriele V.: Sicherheit als Service. In: *Grid-Computing in der biomedizinischen Forschung : Datenschutz und Datensicherheit*. München : Urban & Vogel, Februar 2007. – ISBN 978-3899352375, S. 78–85

[Han11] Handy, Matthias: *Datenschutzkonzept für das Nationale Lipid-Apherese-Register*. (2011). – Version 2.0 – Beziehbar über die TMF

[Hay93] Hayes, Read: *Shoplifting Control*. Orlando, FL, USA : Prevention Press, 1993. – ISBN 978-9994950973

[Hay10] Hayden, Lance: *It Security Metrics : A Practical Framework for Measuring Security & Protecting Data*. New York, USA : McGraw Hill, 2010. – ISBN 978-0071713405

[HDR+10] Helbing, Krister ; Demiroglu, Sara Y. ; Rakebrandt, Fabian ; Pommerening, Klaus ; Rienhoff, Otto ; Sax, Ulrich: A Data Protection Scheme for Medical Research Networks : Review after Five Years of Operation. In: *Methods of Information in Medicine* 49 (2010), Nr. 5, S. 601–607

[Hec08] Hecker, Artur: On System Security Metrics and the Definition Approaches. *In: Proceedings of the Second International Conference on Emerging Security Information, Systems and Technologies (SECUWARE'08)*. Washington, DC, USA : IEEE Computer Society, August 2008, S. 412–419

[Her07] Herrmann, Debra S.: *Complete Guide to Security and Privacy Metrics : Measuring Regulatory Compliance, Operational Resilience, and ROI*. Boca Raton, Florida, USA : Auerbach Publishers Inc., 2007. – ISBN 978-0849354021

[Her10] Herzog, Pete ; ISECOM, Institute for Security and Open Methodologies (Hrsg.): *OSSTMM 3 : Open Source Security Testing Methodology Manual : Contemporary Security Testing and Analysis*. (2010). `http://www.isecom.org/mirror/OSSTMM.3.pdf`, Abruf: 11.1.2012. – Version 3.0

[HH07] Hansen, Markus ; Hansen, Marit: Auswirkungen von Trusted Computing auf die Privatsphäre. In: *Trusted Computing : Ein Weg zu neuen IT-Sicherheitsarchitekturen.* Wiesbaden : Vieweg+Teubner, Dezember 2007. – ISBN 978-3834803092, S. 209–220

[HHH06] Haschberger, Birgit ; Herrmann, Ralf ; Hesse, Janina: *Meldung an das Deutsche Hämophilieregister.* (2006). – Version 3.3 – Beziehbar über die TMF

[HHM+05] Hamouda, Osamah ; Hergersberg, Peter ; Menhorn, Vera ; Nonnemacher, Michael ; Reimann, Georg ; Salzberger, Bernd ; Stausberg, Jürgen ; Wöhrmann, Andrej ; Ebert, Jürgen ; Gründel, Ralf: *Telematik-Plattform : Kompetenznetz HIV/AIDS : Fachkonzept.* (2005). – Version 2.8 – Beziehbar über die TMF

[HIB+06] Harnischmacher, Urs ; Ihle, Peter ; Berger, Bettina ; Goebel, Jürgen ; Scheller, Jürgen: *Checkliste und Leitfaden zur Patienteneinwilligung : Grundlagen und Anleitung für die klinische Forschung.* Berlin : Mwv Medizinisch Wissenschaftliche Verlagsges., 2006. – ISBN 978-3939069256

[hip11] HIPAA College (Hrsg.): *Privacy and Security.* (2011). `http://hipaacollege.com/Privacy_and_Security.html`, Abruf: 20.12.2011

[HN07] Hickethier, Majida ; Nieves, Michael ; OGC, Office of Government Commerce (Hrsg.): *ITIL V3 : Service Strategy.* 2. überarb. Auflage. London, UK : TSO, The Stationery Office, 2007. – ISBN 978-0113310456

[Hoe01] Hoeper, Katrin: *Angriffsdetektierung : Anomalieerkennung und Schwellenwertanalyse.* (2001). `http://www.ruhr-uni-bochum.de/dv/lehre/seminar/angr-detect/angr-detect.pdf`, Abruf: 11.01.2012

[HP06] Humphreys, Ted ; Plate, Angelika: *Measuring the Effectiveness of Your ISMS Implementations Based on ISO/IEC 27001.* London, UK : BSI Standards, 2006. – ISBN 978-0580460159

[HPFS02] Housley, Russell ; Polk, Tim W. ; Ford, Warwick ; Solo, David: *RFC 3280 : Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.* (2002). `http://www.ietf.org/rfc/rfc3280.txt`, Abruf: 24.4.2011

[HSD05] Häber, Anke ; Schmuecker, Paul ; Dujat, Carl: *Leitfaden für das rechnerunterstützte Dokumentenmanagement und die digitale Archivierung von Patientenunterlagen im Gesundheitswesen.* Darmstadt : GIT-Verlag, 2005. – ISBN 3-928865412

[HSD07] Herzog, Almut ; Shahmehri, Nahid ; Duma, Claudiu: An Ontology of Information Security. In: *International Journal of Information Security* 1 (2007), Nr. 4, S. 1–23

[Hud07] Hudson, Sally: *Privileged Password Management : Combating the Insider Threat and Meeting Compliance Regulations for the Enterprise.* (2007). `http://www.cyber-ark.com/pdf/IDC_White_Paper.pdf`, Abruf: 16.3.2011

[HV08] Hartz, Tobias ; Verst, Hendrick: *Datenschutzkonzept KernPäP : Internetgestützte Dokumentation zur Optimierung der kooperativen, palliativ-medizinischen Versorgung in der Pädiatrischen Onkologie.* (2008). – (Vorläufige) Version 2008.08.31 – Beziehbar über die TMF

[HV10] Hulitt, Elaine ; Vaughn, Rayford B.: Information System Security Compliance to FISMA Standard : A Quantitative Measure. In: *Telecommunication Systems* 45 (2010), Nr. 2–3, S. 139–152

[HWE05] Herold, Ralf ; Weiss, Karin ; Eisenreich, Bernard: *Datenschutzkonzept „TMI-Server“ : Austausch von medizinischen Bilddaten im Kompetenznetz Pädiatrische Onkologie und Hämatologie.* (2005). – Version 1.1 – Beziehbar über die TMF

[IB12] Idika, Nwokedi ; Bhargava, Bharat: Extending Attack Graph-Based Security Metrics and Aggregating Their Application. In: *IEEE Transactions on Dependable and Secure Computing* 9 (2012), Nr. 1, S. 75–85

[ibm12] IBM, Inc. (Hrsg.): *Rational Software Architect.* (2012). `http://www-142.ibm.com/software/products/de/de/ratisoftarch/`, Abruf: 31.07.2012

[ich96] ICH, International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use (Hrsg.): *Harmonised Tripartite Guideline : Guideline for Good Clinical Practice E6(R1).* (1996). `http://www.ich.org/LOB/media/MEDIA482.pdf`, Abruf: 2.4.2009. – Current Step 4 Version Including the Post Step 4 Corrections

[Ill02a] Illmann, Torsten: *Datenschutzkonzept in CAPNetz : Kompetenznetz ambulant erworbene Pneumonie.* (2002). – Version 1.2.1 – Beziehbar über die TMF

[Ill02b] Illmann, Torsten: *Sichere Datenübertragung in CAPNETZ : Kompetenznetz ambulant erworbene Pneumonie.* (2002). – Version 1.0 – Beziehbar über die TMF

[int10] Intel, Inc. (Hrsg.): *Intel® vPro™ Technology for Notebook and Desktop PCs.* (2010). `http://www.intel.com/technology/vpro/index.htm`, Abruf: 17.5.2010

[irc05] IRC, INFOSEC Research Council (Hrsg.): *Hard Problem List*. (2005). http://www.infosec-research.org/docs_public/20051130-IRC-HPL-FINAL.pdf, Abruf: 20.12.2011

[ISA07] ISACA, Information Systems Audit and Control Association (Hrsg.): *COBIT 4.1 : Framework, Control Objectives, Management Guidelines, Maturity Models*. Rolling Meadows, IL, USA : IT Governance Institute, 2007. – ISBN 1-933284722

[iso05] ISO/IEC (Hrsg.): *ISO/IEC 27001:2005 : Information Technology : Security Techniques : Information Security Management Systems: Requirements*. (2005). http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103, Abruf: 3.2.2012

[iso08a] ISO, International Organization for Standardization (Hrsg.): *ISO 9001:2008 : Quality Management Systems : Requirements*. (2008). http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=46486, Abruf: 20.12.2011

[iso08b] ISO/IEC (Hrsg.): *ISO/IEC 27799:2008 : Health Informatics : Information Security Management in Health Using ISO/IEC 27002*. (2008). http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=41298, Abruf: 22.12.2011

[iso09] ISO/IEC (Hrsg.): *ISO/IEC 27004:2009: Information Technology : Security Techniques : Information Security Management : Measurement*. (2009). http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42106, Abruf: 3.2.2012

[iss03] ISSEA, International Systems Security Engineering Association (Hrsg.): *Systems Security Engineering Capability Maturity Model (SSE-CMM) : Model Description Document*. (2003). http://www.sse-cmm.org/docs/ssecmmv3final.pdf, Abruf: 26.12.2011. – Version 3.0

[Jan09] Jansen, Wayne: *Directions in Security Metrics Research* / National Institute of Standards and Technology. Gaithersburg, MD, US, 2009. http://csrc.nist.gov/publications/nistir/ir7564/nistir-7564_metrics-research.pdf, Abruf: 3.3.2012 (NISTIR 7564). – Interagency Report. – MD 20899-8930

[Jaq07] Jaquith, Andrew: *Security Metrics : Replacing Fear, Uncertainty, and Doubt*. Upper Saddle River, New Jersey, USA : Addison-Wesley, 2007. – ISBN 978-0321349989

[JM10] Joh, HyunChul ; Malaiya, Yashwant K.: A Framework for Software Security Risk Evaluation using the Vulnerability Lifecycle and CVSS Metrics. *In: Proceedings of the 2010 International Workshop on Risk and Trust in Extended Enterprises*. San Jose, CA, USA : RTEE, November 2010, S. 430–434

[JP07] Jungbauer, Marian ; Pohlmann, Norbert: Integrity Check of Remote Computer Systems Trusted Network Connect. In: *ISSE/SECURE 2007 Securing Electronic Business Processes*. Wiesbaden : Vieweg+Teubner, September 2007. – ISBN 978-3834803467, S. 228–237

[KA98] Kent, Stephen ; Atkinson, Randall: *Security Architecture for the Internet Protocol*. (1998). `http://www.ietf.org/rfc/rfc2401.txt`, Abruf: 3.3.2012

[Kag01] Kagermann, Heinz: *Authentifizierung und Single Sign-On in Unternehmensportalen*. Mannheim, Universität, Diplomarbeit, Oktober 2001

[KB11] Kowalski, S. ; Barabanov, R.: Modelling Static and Dynamic Aspects of Security : A Socio-Technical View on Information Security Metrics. In: *12th International Symposium on Models and Modeling Methodologies in Science and Engineering* Bd. 27. Orlando, FL, USA : IMCIC, 2011, S. 5

[KBB+09] Krefting, Dagmar ; Bart, Julian ; Beronov, Kamen ; Dzhimova, Olga ; Falkner, Jürgen ; Hartung, Michael ; Hoheisel, Andreas ; Knoch, Tobias A. ; Lingner, Thomas ; Mohammed, Yassene ; Peter, Kathrin ; Rahm, Erhard ; Sax, Ulrich ; Sommerfeld, Dietmar ; Steinke, Thomas ; Tolxdorff, Thomas ; Vossberg, Michal ; Viezens, Fred ; Weisbecker, Anette: Medigrid: Towards a User Friendly Secured Grid Infrastructure. In: *Future Generation Computer Systems* 25 (2009), Nr. 3, S. 326–336

[KC08] Kilbridge, Peter M. ; Classen, David C.: The Informatics Opportunities at the Intersection of Patient Safety and Clinical Informatics. In: *Journal of the American Medical Informatics Association* 15 (2008), Nr. 4, S. 397–407

[kes12] kes: *Lexikon der Informations-Sicherheit*. (2012). `http://www.kes.info/lexikon/`, Abruf: 11.1.2012

[KH06] Kovacich, Gerald L. ; Halibozek, Edward P.: *Security Metrics Management : How to Measure the Costs and Benefits of Security*. Oxford, UK : Butterworth-Heinemann, 2006. – ISBN 978-0750678995

[KK11] Kivimaa, Jüri ; Kirt, Toomas: Evolutionary Algorithms for Optimal Selection of Security Measures. *In: Proceedings of the 10th European Conference on Information Warfare and Security at the Tallinn University of Technology*. Tallinn, Estonia, Juli 2011, S. 172–184

[Kle06] Kleinfeld, Abe: Measuring Security. In: *Information Systems Security* 15 (2006), Nr. 5, S. 7–12

[klr10a] KLR, Kinderlungenregister (Hrsg.): *Datenschutzkonzept Kinderlungenregister.* (2010). – Version 1.3 – Beziehbar über die TMF

[KLR+10b] Kanstrén, Teemu ; López, Oscar ; Ros, Saioa ; Savola, Reijo ; Evesti, Antti ; Pentikäinen, Heimo ; Hecker, Artur ; Ouedraogo, Moussa ; Hätönen, Kimmo ; Halonen, Perttu ; Blad, Christophe ; López, Oscar ; Ros, Saioa: Towards an Abstraction Layer for Security Assurance Measurements. *In: Proceedings of the Fourth European Conference on Software Architecture Companion Volume (ECSA'10).* New York, NY, USA : ACM, 2010, S. 189–196

[KMY10] Krautsevich, Leanid ; Martinelli, Fabio ; Yautsiukhin, Artsiom: Formal Approach to Security Metrics : What Does „More Secure" Mean for You? *In: Proceedings of the Fourth European Conference on Software Architecture : Companion Volume (ECSA'10).* New York, NY, USA : ACM, 2010, S. 162–169

[KMY11] Krautsevich, Leanid ; Martinelli, Fabio ; Yautsiukhin, Artsiom: Formal Analysis of Security Metrics and Risk. In: Ardagna, Claudio A. (Hrsg.) ; Zhou, Jianying (Hrsg.): *WISTP* Bd. 6633. Springer-Verlag, 2011. – ISBN 978-3642210396, S. 304–319

[KP10] Krockenberger, Katja ; Plotnicki, Lukasz ; Arbeitskreis Nierentransplantation in der Gesellschaft für Pädiatrische Nephrologie (Hrsg.): *Datenschutzkonzept für das online NTx Register : Anhang III.* (2010). – Version 1.3 – Beziehbar über die TMF

[kpm04] KPMG (Hrsg.): *Fraud Survey 2004 : Forensic Advisory.* (2004). http://www.kpmg.com.au/aci/docs/Fraud-Survey-2004.pdf, Abruf: 3.3.2012

[KR07] Krissler, Jan ; Rütten, Christiane: Feine Linien : Wie leicht sich Fingerabdrucksensoren austricksen lassen. In: *c't – Magazin für Computertechnik* 7 (2007), Nr. 12, S. 102–103

[Kre06] Krempl, Stefan: Big Brother 2.0 : Der Bürger im Fadenkreuz der Terrorismusbekämpfung. In: *c't – Magazin für Computertechnik* 6 (2006), Nr. 24, S. 214–220

[Kre09] Krebs, Brian: *Hackers Break Into Virginia Health Professions Database, Demand Ransom.* (2009). http://voices.washingtonpost.com/securityfix/2009/05/hackers_break_into_virginia_he.html, Abruf: 11.1.2012

[KS05] Kotenko, Igor ; Stepashkin, Mihail: Analyzing Vulnerabilities and Measuring Security Level at Design and Exploitation Stages of Computer Network Life

Cycle. In: Gorodetsky, Vladimir (Hrsg.) ; Kotenko, Igor (Hrsg.) ; Skormin, Victor (Hrsg.): *Computer Network Security* Bd. 3685. Berlin/Heidelberg : Springer-Verlag, September 2005. – ISBN 3-54029113X, S. 311–324

[KS09] Kriha, Walter ; Schmitz, Roland: *Sichere Systeme : Konzepte, Architekturen und Frameworks*. Berlin : Springer-Verlag, 2009. – ISBN 978-3540789581

[KSP+07] Kark, Khalid ; Stamp, Paul ; Penn, Jonathan ; Bernhardt, Sarah ; Dill, Alissa: *Defining an Effective Security Metrics Program : Best Practices*. (2007). http://www.forrester.com/imagesV2/uplmisc/DefiningAn_EffectiveSecurityMetricsProgram.pdf, Abruf: 27.12.2011

[KSSL06] Kissel, Richard ; Scholl, Matthew ; Skolochenko, Steven ; Li, Xing ; NIST, National Institute of Standards and Technology (Hrsg.): *Guidelines for Media Sanitization : Recommendations of the National Institute of Standards and Technology*. (2006). http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf, Abruf: 3.3.2012. – NIST Special Publication 800-88. – MD 20899-8930

[KSV07] Kompella, Ramana R. ; Singh, Sumeet ; Varghese, George: On Scalable Attack Detection in the Network. In: *IEEE/ACM Transactions on Networking* 15 (2007), Nr. 1, S. 14–25

[Küt09] Kütz, Martin: *Kennzahlen in der IT : Werkzeuge für Controlling und Management*. 3. überarb. und erw. Aufl. Heidelberg : dpunkt-Verlag, 2009. – ISBN 978-3898645799

[LA05] Lioy, Antonio ; Atzeni, Andrea: Why to Adopt a Security Metric? A Brief Survey. *In: Proceeding of the 1st ACM Workshop on Quality of Protection (QoP2005)*. New York, NY, USA : Springer-Verlag, 2005, S. 1–12

[Law06] Lawerenz, Chris: *Datenschutzkonzept für die translationale Datenbank iCHIP in molekularbiologischer und klinischer Forschung*. (2006). – Beziehbar über die TMF

[LBG08] Le, Duc-Phong ; Bonnecaze, Alexis ; Gabillon, Alban: Signtiming Scheme Based on Aggregate Signature. *In: Proceedings of the IEEE International Conference on the Intelligence and Security Informatics (ISI 2008)*. Washington, DC, USA : IEEE Computer Society, Juni 2008, S. 145–149

[Leh04] Lehmann, Thomas M.: *Digitale Wasserzeichen : Bilddaten sicher übertragen*. (2004). http://www.aerzteblatt.de/archiv/44795?src=toc, Abruf: 3.3.2012

[LFK+11] LeMay, Elizabeth ; Ford, Michael D. ; Keefe, Ken ; Sanders, William H. ; Muehrcke, Carol: Model-based Security Metrics Using ADversary VIew

Security Evaluation (ADVISE). *In: 2011 Eighth International Conference on Quantitative Evaluation of SysTems*. Aachen, Germany : QEST, September 2011, S. 191–200

[LM07] Lacy, Shirley ; Macfarlane, Ivor ; OGC, Office of Government Commerce (Hrsg.): *ITIL V3 : Service Transition*. 2. überarb. Aufl. London, UK : TSO, The Stationery Office, 2007. – ISBN 978-0113310487

[LO09] Liu, Simon ; Ormaner, Jerry: From Ancient Fortress to Modern Cyberdefense. In: *IT Professional* 11 (2009), Nr. 3, S. 22 –29

[Lod03] Lodderstedt, Torsten: *Model Driven Security : from UML Models to Access Control Architectures*. Freiburg, Universität, Dissertation, 2003. http://www.freidok.uni-freiburg.de/volltexte/1253/, Abruf: 3.3.2012

[log09] LogMeIn, Inc. (Hrsg.): *LogMeIn Hamachi : Instant, Zero Configuration VPN*. (2009). https://secure.logmein.com/products/hamachi/vpn.asp, Abruf: 17.3.2009

[Lor06] Lorenzen, Klaus F.: *ALPHADIN.BST : BibTeX Standard bibliography style „alpha“*. (2006). http://svn.hilbri.ch/sudoku/doc/alphadin.bst, Abruf: 11.4.2010

[LR07] Lloyd, Vernon ; Rudd, Colin ; OGC, Office of Government Commerce (Hrsg.): *ITIL V3 : Service Design*. 2. erw. Aufl. London, UK : TSO, The Stationery Office, 2007. – ISBN 978-0113310470

[Lut07] Lutz, Jochen: *Datenschutzkonzept des Kompetenznetzes Vorhofflimmern*. (2007). – Version 0.99d – Beziehbar über die TMF

[Mac98] Mackenbrock, Markus: *IT-Sicherheitskriterien : Artikel zu Common Criteria (Version 2.0), Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik*. (1998). http://www.bsi.bund.de/cc/cc_20d.htm, Abruf: 18.3.2009

[MAM+99] Myers, Michael ; Ankney, Rich ; Malpani, Ambarish M. ; Galperin, Slava ; Adams, Carlisle: *RFC 2560 : X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*. (1999). http://www.ietf.org/rfc/rfc2560.txt, Abruf: 24.4.2011

[Man05] Manas-Argemi, Jose A.: Security Metrics and Measurements for IT. In: *UPGRADE – The European Journal for the Informatics Professional* VI (2005), Nr. 4, S. 28–30

[Mar05] Marin, Gerald A.: Network Security Basics. In: *IEEE Security & Privacy Magazine* 3 (2005), Nr. 6, S. 68–72

[Mar08] Marckmann, Georg: Gesundheit und Gerechtigkeit. In: *Bundesgesundheitsblatt : Gesundheitsforschung : Gesundheitsschutz* 51 (2008), Nr. 8, S. 887–894

[MH07] Meyers, Michael ; Harris, Shon: *CISSP : Certified Information Systems Security Professional : Das Zertifikat für IT-Sicherheit, optimale Vorbereitung.* 2. überarb. Aufl. Heidelberg : Mitp-Verlag, 2007. – ISBN 978-3826617454

[mic08] Microsoft Corporation (Hrsg.): *Netzwerkzugriffsschutz : Network Access Protection.* (2008). `http://msdn.microsoft.com/de-de/library/cc730902.aspx`, Abruf: 3.3.2012

[Mie10] Mielck, Andreas: Sozial-epidemiologische und ethische Ansätze zur Bewertung der gesundheitlichen Ungleichheit. In: *Ethik in der Medizin* 22 (2010), Nr. 3, S. 235–248

[Min03] Mink, Martin: *Sicheres Single Sign-On für Webdienste.* Darmstadt, Technische Universität, Diplomarbeit, April 2003

[Min08] Minckwitz, Gunter ; GBG Forschungs GmbH (Hrsg.): *Register zur Langzeitbeobachtung von Teilnehmerinnen an Brustkrebsstudien : German Breast Group.* (2008). – Beziehbar über die TMF

[Mit03] Mitnick, Kevin D.: *Die Kunst der Täuschung.* Bonn : Mitp-Verlag, 2003. – ISBN 978-3826609992

[MM03] Manns, Michael ; Müller, Thomas: *Datenschutz im Kompetenznetz Hepatitis.* (2003). – Version 1.0 – Beziehbar über die TMF

[MO11] Mataracioglu, Tolga ; Ozkan, Sevgi: Governing Information Security in Conjunction with COBIT and ISO 27001. In: *International Journal of Network Security & Its Applications* 3 (2011), Nr. 4, S. 111–116

[Moh07] Mohammed, Yassene: Erweiterte Sicherheit und Datenschutz Techniken. In: *Grid-Computing in der biomedizinischen Forschung : Datenschutz und Datensicherheit.* München : Urban & Vogel, Februar 2007. – ISBN 978-3899352375, S. 70–77

[Moh08] Mohammed, Yassene: *Data Protection and Data Security Concept for Medical Applications in a Grid Computing Environment.* Göttingen, Universität, Dissertation, 2008. `http://webdoc.sub.gwdg.de/diss/2008/mohammed/mohammed.pdf`, Abruf: 3.3.2012

[Mos02] Moschgath, Marie-Luise: *Kontextabhängige Zugriffskontrolle für Anwendungen im Ubiquitous Computing*. Darmstadt, Technische Universität, Dissertation, Mai 2002. http://deposit.ddb.de/cgi-bin/dokserv?idn=967834457, Abruf: 3.3.2012

[MR05] Maxion, Roy A. ; Roberts, Rachel R. M.: Methodological Foundations : Enabling the Next Generation of Security. In: *IEEE Security and Privacy Magazine* 3 (2005), Nr. 2, S. 54–57

[MRWC09] Manion, Frank ; Robbins, Robert ; Weems, William ; Crowley, Rebecca: Security and Privacy Requirements for a Multi-Institutional Cancer Research Data Grid: An Interview-Based Study. In: *BMC Medical Informatics and Decision Making* 9 (2009), Nr. 31, S. 40

[MST06] Mohammed, Yassene ; Sax, Ulrich ; TMF, Telematikplattform für Medizinische Forschungsnetze e. V.: *Sicherheit im Grid? Erste Erfahrungen aus dem MediGRID-Projekt*. Berlin, Geschäftsstelle TMF e. V. am 11.12.2006. – Sicherheitskonzepte in der vernetzten medizinischen Forschung : TMF-Workshop. – Beziehbar über die TMF

[MT06] Mörike, Michael (Hrsg.) ; Teufel, Stephanie (Hrsg.): *Kosten & Nutzen von IT-Sicherheit*. Heidelberg : dpunkt-Verlag, 2006. – ISBN 978-3898643801

[Mül11] Müller, Klaus-Rainer: *IT-Sicherheit mit System : Integratives IT-Sicherheits-, Kontinuitäts- und Risikomanagement – Sicherheitspyramide – Standards und Practices – SOA und Softwareentwicklung*. 4. erw. und aktual. Aufl. Wiesbaden : Vieweg+Teubner, 2011. – ISBN 978-3834815361

[Müß06] Müssig, Sven: Haben Sicherheitsinvestitionen eine Rendite? In: Mörike, Michael (Hrsg.) ; Teufel, Stephanie (Hrsg.): *Kosten & Nutzen von IT-Sicherheit*. Heidelberg : dpunkt-Verlag, 2006. – ISBN 978-3898643801, S. 35–43

[MW02] Metschke, Rainer ; Wellbrock, Rita: *Datenschutz in Wissenschaft und Forschung*. (2002). http://www.datenschutz-berlin.de/attachments/47/Materialien28.pdf, Abruf: 3.2.2012. – 3. überarb. Aufl.

[NB04] Neumann, Manuela ; Brüderle, Andreas: *Brain-Net : Nationale Hirngewebedatenbank : Datenschutzkonzept*. (2004). – Version 3.0 – Beziehbar über die TMF

[ncb12] NCBC, National Center for Biomedical Computing (Hrsg.): *i2b2 Software : Informatics for Integrating Biology & the Bedside*. (2012). https://www.i2b2.org/software/index.html, Abruf: 12.2.2012

[nci12] NCI, National Cancer Institute (Hrsg.): *caBIG® : Cancer Biomedical Informatics Grid®*. (2012). `http://cabig.cancer.gov/`, Abruf: 11.1.2012

[NDJ01] Nash, Andrew ; Duane, William ; Joseph, Celia: *PKI : e-security implementieren*. Bonn : Mitp-Verlag, 2001. – ISBN 978-3826607813

[nis12] NIST, National Institute of Standards and Technology (Hrsg.): *NVD Common Vulnerability Scoring System Support v2*. (2012). `http://nvd.nist.gov/cvss.cfm`, Abruf: 3.3.2012

[NN01] Northcutt, Stephen ; Novak, Judy: *IDS : Intrusion Detection : Spurensicherung im Netz*. Bonn : Mitp-Verlag, 2001. – ISBN 978-3826607271

[Nor00] Norton, Stephen P.: *Circle of Security*. (2000). `http://www2.giac.org/certified_professionals/practicals/gsec/221.php`, Abruf: 28.10.2010

[nov11] Novell, Inc. (Hrsg.): *AppArmor Application Security for Linux*. (2011). `http://www.novell.com/linux/security/apparmor/`, Abruf: 16.3.2011

[NP07] Nichols, Elizabeth A. ; Peterson, Gunnar: A Metrics Framework to Drive Application Security Improvement. In: *IEEE Security & Privacy Magazine* 5 (2007), Nr. 2, S. 88–91

[NPL04] Narayanan, Sreeram ; Poovendran, Radha ; Li, Mingyan: Tracing Medical Images Using Multi-Band Watermarks. *In: Proceedings of 26th International Conference of IEEE Engineering in Medicine and Biology Society (IEMBS'04)*. Washington, DC, USA : IEEE Computer Society, September 2004, S. 3233–3236

[nsa09] NSA/CSS, National Security Agency/Central Security Service (Hrsg.): *SELinux Documentation*. (2009). `http://www.nsa.gov/research/selinux/docs.shtml`, Abruf: 16.3.2011

[NV09] Neto, Afonso A. ; Vieira, Marco: Untrustworthiness : A Trust-Based Security Metric. *In: Proceedings of the Fourth International Conference on Risks and Security of Internet and Systems (CRiSIS 2009)*. Toulouse, France : IEEE Computer Society, Oktober 2009, S. 123–126

[NV10] Neto, Afonso A. ; Vieira, Marco: Benchmarking Untrustworthiness : An Alternative to Security Measurement. In: *International Journal of Dependable and Trustworthy Information Systems (IJDTIS)* 1 (2010), Nr. 2, S. 32–54

[NZW02] Northcutt, Stephen ; Zeltser, Lenny ; Winters, Scott: *Inside Network Perimeter Security : The Definitive Guide to Firewalls, Virtual Private Networks (VPNs), Routers, and Intrusion Detection Systems*. Boston, USA : New Riders, 2002. – ISBN 978-0735712324

[obj12] Object Management Group, Inc. (Hrsg.): *UML Resource Page*. (2012). http://www.uml.org/, Abruf: 3.3.2012

[Oeb12] Oebbeke, Alfons: *ARCHmatic-Glossar und -Lexikon*. (2012). http://www.glossar.de/glossar/index.htm, Abruf: 11.1.2012

[OK09] Ohmann, Christian ; Kuchinke, Wolfgang: Future Developments of Medical Informatics from the Viewpoint of Networked Clinical Research : Interoperability and Integration. In: *Methods of Information in Medicine* 48 (2009), Nr. 1, S. 45–54

[OLH+08] Oster, Scott ; Langella, Stephen ; Hastings, Shannon ; Ervin, David ; Madduri, Ravi ; Phillips, Joshua ; Kurc, Tahsin ; Siebenlist, Frank ; Covitz, Peter ; Shanbhag, Krishnakant ; Foster, Ian ; Saltz, Joel: caGrid 1.0 : An Enterprise Grid Infrastructure for Biomedical Research. In: *Journal of the American Medical Association* 15 (2008), Nr. 2, S. 138–149

[owa12] OWASP Foundation (Hrsg.): *OWASP AJAX Security Project*. (2012). http://www.owasp.org/index.php/Category:OWASP_AJAX_Security_Project, Abruf: 3.3.2012

[Pay06] Payne, Shirley C. ; SANS Institute (Hrsg.): *A Guide to Security Metrics : SANS Security Essentials GSEC Practical Assignment*. (2006). http://www.sans.org/reading_room/whitepapers/auditing/guide-security-metrics_55, Abruf: 20.12.2011. – Version 1.2e

[PB06] Pohlmann, Norbert ; Blumberg, Hartmut: *Der IT-Sicherheitsleitfaden : Das Pflichtenheft zur Implementierung von IT-Sicherheitsstandards im Unternehmen*. 2. aktual. Aufl. Heidelberg : Mitp-Verlag, 2006. – ISBN 978-3826616358

[PBB+96] Poole, Josef ; Barkley, John ; Brady, Kevin ; Cincotta, Anthony ; Salamon, Wayne: *Distributed Communication Methods and Role-Based Access Control for Use in Health Care Applications* / National Institute of Standards and Technology. Gaithersburg, US, 1996. http://hissa.nist.gov/rbac/poole/ir5820/nistir5820.htm, Abruf: 18.3.2009 (NISTIR 5820). – NIST Internal Report

[PC10] Pfleeger, Shari ; Cunningham, Robert: Why Measuring Security Is Hard. In: *IEEE Security & Privacy Magazine* 8 (2010), Nr. 4, S. 46–54

[PCL07] Puentes, John ; Coatrieux, Gouenou ; Lecornu, Laurent: Secured Electronic Patient Records Content Exploitation. In: Bali, Rajeev K. (Hrsg.) ; Dwivedi, Ashish N. (Hrsg.): *Healthcare Knowledge Management : Issues, Advances and Successes*. New York, NY, USA : Springer-Verlag, 2007 (Health Informatics). – ISBN 978-1441922120, S. 160–175

[PDKB08] Pommerening, Klaus ; Debling, Desiree ; Kaatsch, Peter ; Blettner, Maria: Register zu seltenen Krankheiten : Patientencompliance und Datenschutz. In: *Bundesgesundheitsblatt : Gesundheitsforschung : Gesundheitsschutz* 51 (2008), Nr. 5, S. 491–499

[PE06] Psille, Daniel E. A. ; Eschweiler, Jörg: *Security@Work : Pragmatische Konzeption und Implementierung von IT-Sicherheit mit Lösungsbeispielen auf Open-Source-Basis*. Berlin : Springer-Verlag, 2006. – ISBN 978-3540220282

[Pfe09] Pfeiffer, Karl-Peter: Future Development of Medical Informatics from the Viewpoint of Health Telematics. In: *Methods of Information in Medicine* 48 (2009), Nr. 1, S. 55–61

[PFGG09] Pervaiz, Zahid ; Ferraiolo, David ; Gavrila, Serban ; Ghafoor, Arif: *Access Control for Healthcare using Policy Machine*. 2009. `http://www.cerias.purdue.edu/ssl/techreports-ssl/2009-20.pdf`, Abruf: 19.3.2011 (CERIAS 2009-20). – Technical Report

[Pfl09] Pfleeger, Shari L.: Useful Cybersecurity Metrics. In: *IT Professional* 11 (2009), Nr. 3, S. 38–45

[Pir07] Pironti, John P.: Developing Metrics for Effective Information Security Governance. In: *Information Systems Control Journal* 2 (2007), S. 33–37

[PJAS06] Pamula, Joseph ; Jajodia, Sushil ; Ammann, Paul ; Swarup, Vipin: A Weakest-Adversary Security Metric for Network Configuration Security Analysis. *In: Proceedings of the 2nd ACM workshop on Quality of Protection (QoP'06)*. New York, NY, USA : ACM, 2006, S. 31–38. – ACM ID: 1179502

[Poh06] Pohlmann, Norbert: Wie wirtschaftlich sind die IT-Sicherheitsmaßnahmen? In: Mörike, Michael (Hrsg.) ; Teufel, Stephanie (Hrsg.): *Kosten & Nutzen von IT-Sicherheit*. Heidelberg : dpunkt-Verlag, 2006. – ISBN 978-3898643801, S. 26–34

[Pom07] Pommerening, Klaus: Das Datenschutzkonzept der TMF für Biomaterialbanken : The TMF Data Protection Scheme for Biobanks. In: *it – Information Technology* 49 (2007), Nr. 6, S. 352–359

[Pom09] Pommerening, Klaus: *Identitätsmanagement mit dem PID-Generator der TMF für das KPOH*. (2009). `http://www.staff.uni-mainz.de/pommeren/Artikel/IDman_Pommerening.pdf`, Abruf: 25.12.2011

[Pom10a] Pommerening, Klaus: Personalisierte Medizin und Informationstechnologie – Aspekte des Datenschutzes. In: Niederlag, Wolfgang (Hrsg.) ; Lemke,

Heinz U. (Hrsg.) ; Rienhoff, Otto (Hrsg.): *Personalisierte Medizin und Informationstechnologie* Bd. 15. Dresden : Health Academy, 2010. – ISBN 978-3000303524, S. 239–250

[Pom10b] Pommerening, Klaus ; TMF, Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V. (Veranst.): *Tools zum ID-Management in der klinischen Forschung : Einführung.* Berlin am 24.9.2010. – TMF Tools zum ID-Management : TMF-Workshop. – Beziehbar über die TMF

[Pom11a] Pommerening, Klaus: Medizinische Forschung auf höchstem (Sicherheits-)Niveau. In: *Wissensmanagement* 13 (2011), Nr. 7, S. 28–29

[Pom11b] Pommerening, Klaus ; TMF, Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V. (Veranst.): *V039-03 Fortschreibung der generischen Datenschutzkonzepte der TMF.* Berlin am 24.3.2011. – Sitzung der Arbeitsgruppe Datenschutz. – Beziehbar über die TMF

[pon11] Ponemon Institute, LLC (Hrsg.): *2010 Annual Study : U.S. Cost of a Data Breach* / Symantec Corporation. 2011. `http://www.symantec.com/content/en/us/about/media/pdfs/symantec_ponemon_data_breach_costs_report.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Mar_worldwide_costofdatabreach`, Abruf: 2.5.2011. – Annual Report

[PRDS05] Pommerening, Klaus ; Reng, Carl-Michael ; Debold, Peter ; Semler, Sebastian C.: Pseudonymisierung in der medizinischen Forschung – das generische TMF-Datenschutzkonzept. In: *GMS Medizinische Informatik, Biometrie und Epidemiologie* 1 (2005), Nr. 3 : Doc17

[PSE04] Paulson, James W. ; Succi, Giancarlo ; Eberlein, Armin: An Empirical Study of Open-Source and Closed-Source Software Products. In: *IEEE Transactions on Software Engineering* 30 (2004), Nr. 4, S. 246–256

[PSM+08] Pommerening, Klaus ; Sax, Ulrich ; Müller, Thomas ; Speer, Ronald ; Ganslandt, Thomas ; Drepper, Johannes ; Semler, Sebastian C.: Integrating eHealth and Medical Research : The TMF Data Protection Scheme. In: Blobel, Bernd (Hrsg.) ; Pharow, Peter (Hrsg.) ; Nerlich, Michael (Hrsg.): *eHealth : Combining Health Telematics, Telemedicine, Biomedical Engineering and Bioinformatics to the Edge.* Berlin : IOS Press, 2008, S. 5–10

[PSM+09] Pommerening, Klaus ; Sax, Ulrich ; Müller, Thomas ; Speer, Ronald ; Ganslandt, Thomas ; Drepper, Johannes ; Semler, Sebastian C.: Das TMF-Datenschutzkonzept für medizinische Datensammlungen und Biobanken.

In: Fischer, Stefan (Hrsg.) ; Maehle, Erik (Hrsg.) ; Reischuk, Rüdiger (Hrsg.): *GI Jahrestagung (LNI)* Bd. 154. Lübeck : GI, 2009, S. 1744–1757

[Pup06] Puppe, Christoph ; TMF, Telematikplattform für Medizinische Forschungsnetze e. V. (Veranst.): *ISO 27001/Grundschutzhandbuch : Einführung in den Nachweis der IT-Sicherheit durch Zertifizierung oder Selbsterklärung.* Berlin, Geschäftsstelle TMF e. V. am 11.12.2006. – Sicherheitskonzepte in der vernetzten medizinischen Forschung : TMF-Workshop. – Beziehbar über die TMF

[RDSP06] Reng, Carl-Michael ; Debold, Peter ; Specker, Christof ; Pommerening, Klaus: *Generische Lösungen der TMF zum Datenschutz für die Forschungsnetze in der Medizin.* Berlin : Mwv Medizinisch Wissenschaftliche Verlagsges., 2006. – ISBN 978-3939069041

[RHJ08] Rossnagel, Alexander ; Hornung, Gerrit ; Jandt, Silke: Teil-Rechtsgutachten zu den datenschutzrechtlichen Fragen der medizinischen Forschung. In: *Rechtsgutachten zum Datenschutz in der medizinischen Forschung im Auftrag der Telematikplattform für Medizinische Forschungsnetze e. V. (TMF).* Kassel : TMF, März 2008, S. C1–C75. – TMF-Produktnummer: P039031, Version 1.0 – Beziehbar über die TMF

[Rie04] Rienhoff, Otto: Bedeutung der Kompetenznetze für die Innere Medizin. In: *Medizinische Klinik* 99 (2004), Nr. 7, S. 407–411

[RLV+01] Rienhoff, Otto (Hrsg.) ; Laske, Caroline (Hrsg.) ; Van Eecke, Patrick (Hrsg.) ; Wenzlaff, Paul (Hrsg.) ; Piccolo, Ursula (Hrsg.): *Legal Framework for Security in European Healthcare Telematics : Studies in Health Technology and Informatics, V. 74.* Amsterdam, Niederlande : IOS Press, 2001. – ISBN 1-586030493

[Roe05] Roetzer, Florian: *Auto und Fingerkuppe weg.* (2005). `http://www.heise.de/tp/r4/artikel/19/19798/1.html`, Abruf: 19.3.2009

[Ron04] Ronellenfitsch, Michael: *Dreiunddreißigster Tätigkeitsbericht des Hessischen Datenschutzbeauftragten.* (2004). `http://www.datenschutz.hessen.de/_old_content/tb33/tb33.pdf`, Abruf: 1.5.2010

[Ron05] Ronellenfitsch, Michael: *Vierunddreißigster Tätigkeitsbericht des Hessischen Datenschutzbeauftragten.* (2005). `http://www.datenschutz.hessen.de/_old_content/tb34.pdf`, Abruf: 1.5.2010

[RSK+10] Ross, Ron ; Swanson, Marianne ; Katzke, Stuart ; Stoneburner, Gary ; Graubart, Richard ; Turner, Glenda ; Porter, Esten ; Hodge, Bennett ;

Dempsey, Kelley ; Rogers, George ; Johnson, Arnold ; Enloe, Christian ; NIST, National Institute of Standards and Technology (Hrsg.): *Recommended Security Controls for Federal Information Systems and Organizations*. (2010). http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf, Abruf: 3.2.2012. – NIST Special Publication 800-53. – Revision 3

[RTH+10] Ross, Ron ; Toth, Patricia ; Hodge, Bennett ; Stoneburner, Gary ; Porter, Esten ; Quigg, Karen ; Sherald, Terry ; Gouldmann, Peter ; Chiu, Jonathan ; Dempsey, Kelley ; Johnson, Arnold ; Enloe, Christian ; NIST, National Institute of Standards and Technology (Hrsg.): *Guide for Assessing the Security Controls in Federal Information Systems and Organizations : Building Effective Security Assessment Plans*. (2010). http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf, Abruf: 3.3.2012. – NIST Special Publication 800-53A. – Revision 1

[RVRK05] Renner, Thomas ; Vetter, Michael ; Rex, Sascha ; Kett, Holger: *Open Source Software : Einsatzpotenziale und Wirtschaftlichkeit : Eine Studie der Fraunhofer-Gesellschaft*. Stuttgart : Fraunhofer IRB Verlag, 2005. – ISBN 3-816770088

[SA09] Savola, Reijo M. ; Abie, Habtamu: Identification of Basic Measurable Security Components for a Distributed Messaging System. *In: Proceedings of the Third International Conference on Emerging Security Information, Systems and Technologies (SECURWARE'09)*. Washington, DC, USA : IEEE Computer Society, Juni 2009, S. 121–128

[SA10] Serrelis, Emmanouil ; Alexandris, Nikolaos: Measuring Network Security. In: Bazzi, Alessandro (Hrsg.): *Radio Communications*. Vukovar, Croatia : In-Teh, April 2010. – ISBN 978-9533070919, S. 673–688

[San96] Sandhu, Ravi S.: Role Hierarchies and Constraints for Lattice-Based Access Controls. *In: Proceedings of the 4th European Symposium on Research in Computer Security (LNCS)*. Berlin/Heidelberg : Springer-Verlag, 1996, S. 65–79. – Bd. 1146

[Sav09] Savola, Reijo M.: A Security Metrics Taxonomization Model for Software-Intensive Systems. In: *Journal of Information Processing Systems* 5 (2009), Nr. 4, S. 197–206

[SBE11] Stolfo, Sal ; Bellovin, Steven M. ; Evans, David: Measuring Security. In: *IEEE Security & Privacy Magazine* 9 (2011), Nr. 3, S. 60–65

[SBH+07] Safran, Charles ; Bloomrosen, Meryl ; Hammond, Edward W. ; Labkoff, Steven ; Markel-Fox, Suzanne ; Tang, Paul C. ; Detmer, Don E.: Toward a National Framework for the Secondary Use of Health Data : An American Medical Informatics Association White Paper. In: *Journal of the American Medical Informatics Association* 14 (2007), Nr. 1, S. 1–9

[SC08] Sennewald, Charles A. ; Christman, John H.: *Retail Crime, Security, and Loss Prevention : An Encyclopedic Reference*. Oxford, UK : Butterworth Heinemann, 2008. – ISBN 978-0123705297

[SCB03] Smith, Robert N. ; Chen, Yu ; Bhattacharya, Sourav: Cascade of Distributed and Cooperating Firewalls in a Secure Data Network. In: *IEEE Transactions on Knowledge and Data Engineering* 15 (2003), Nr. 5, S. 1307–1315

[SCFY96] Sandhu, Ravi S. ; Coyne, Edward J. ; Feinstein, Hal L. ; Youman, Charles E.: Role-Based Access Control Models. In: *IEEE Computer* 29 (1996), S. 38–47

[Sch99] Schier, Kathrin: *Vertrauenswürdige Kommunikation im elektronischen Zahlungsverkehr*. Hamburg, Universität, Dissertation, Juni 1999. `http://deposit.ddb.de/cgi-bin/dokserv?idn=957624921`, Abruf: 3.3.2012

[sch03] SchlumbergerSema (Hrsg.): *Trustcenter für medizinische Kompetenznetze : Policy*. (2003). `http://www.kinderkrebsinfo.de/sites/kinderkrebsinfo/content/e1676/e1806/e6499/e7131/e7132/Policy_CCI_ger.pdf`, Abruf: 11.01.2012. – Version 0.1.6

[Sch04] Schneier, Bruce: *Secrets & Lies : IT-Sicherheit in einer vernetzten Welt*. Heidelberg : dpunkt-Verlag, 2004. – ISBN 978-3898643023

[Sch05a] Schechter, Stuart E.: Toward Econometric Models of the Security Risk from Remote Attacks. In: *IEEE Security and Privacy Magazine* 3 (2005), Nr. 1, S. 40–44

[Sch05b] Schneier, Bruce: *Crypto-Gram Newsletter, 15.04.2005*. (2005). `http://www.schneier.com/crypto-gram-0504.html`, Abruf: 2.5.2010

[Sch07] Schmidt, Jürgen: Die Super-Trojaner : So arbeiten moderne Schädlinge. In: *c't – Magazin für Computertechnik* 7 (2007), Nr. 2, S. 86–89

[Sch08] Schlattmann, Johannes ; GDV, Gesamtverband der Deutschen Versicherungswirtschaft e. V. (Veranst.): *Herausforderungen in der IT-Sicherheit – aktuelle Schwerpunkte und Aktivitäten : Informationsveranstaltung IT-Security, Betriebswirtschaft und Informationstechnologie des GDV*. Köln am 8.5.2008. –

Informationsveranstaltung IT-Security Betriebswirtschaft und Informationstechnologie des GDV

[Sch09] Schimkowitsch, Scott E.: *Key Components of an Information Security Metrics Program Plan* / University of Oregon. Eugene, Oregon, US, Juli 2009. https://scholarsbank.uoregon.edu/xmlui/handle/1794/9479, Abruf: 20.12.2011. – Capstone Report

[SD05] Steinebach, Martin ; Dittmann, Jana: Secure Production of Digital Media. In: Hemmje, Matthias (Hrsg.) ; Niederee, Claudia (Hrsg.) ; Risse, Thomas (Hrsg.): *From Integrated Publication and Information Systems to Information and Knowledge Environments* Bd. 3379. Heidelberg : Springer-Verlag, 2005. – ISBN 978-3540245513, S. 79–86

[SD07] Speer, Ronald ; Drepper, Johannes: *Sicherheitskonzepte in medizinischen Forschungsverbünden : Anwendung des IT-Grundschutzes : Sicherheitskonzepte.* 2007 (V016-01). – Abschlussbericht. – Beziehbar über die TMF

[Sem05] Semler, Sebastian C. ; GMDS, Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (Veranst.): *Archivierungsaspekte aus Sicht der klinischen Forschung – Archivierung von Forschungsunterlagen : Hannöversche Archivtage, 21. Treffen der GMDS AG AKU.* Hannover am 16.6.2005. – Hannöversche Archivtage, 21. Treffen der GMDS AG AKU

[Ser01] Sergl, Marita G.: *Konzepte und Komponenten für die Zugriffskontrolle in verteilten, heterogenen Krankenhaus-Informationssystemen am Beispiel des Mainzer Universitätsklinikums.* Mainz, Universität, Dissertation, 2001. http://deposit.ddb.de/cgi-bin/dokserv?idn=963927140, Abruf: 3.3.2012

[SG96] Swanson, Marianne ; Guttmann, Barbara ; NIST, National Institute of Standards and Technology (Hrsg.): *Generally Accepted Principles and Practices for Securing Information Technology Systems.* (1996). http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf, Abruf: 3.3.2012. – NIST Special Publication 800-14

[SG09] Sowa, Sebastian ; Gabriel, Roland: Multidimensional Management of Information Security : A Metrics Based Approach Merging Business and Information Security Topics. *In: Proceedings of the International Conference on Availability, Reliability and Security (ARES'09).* Washington, DC, USA : IEEE Computer Society, März 2009, S. 750–755

[SGF02] Stoneburner, Gary ; Goguen, Alice ; Feringa, Alexis ; NIST, National Institute of Standards and Technology (Hrsg.): *Risk Management Guide for Information Technology Systems : Recommendations of the National Institute of*

Standards and Technology. (2002). http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf, Abruf: 20.12.2011. – NIST Special Publication 800-30

[SH11] Savola, Reijo M. ; Heinonen, Petri: A Visualization and Modeling Tool for Security Metrics and Measurements Management. *In: 2011 Information Security for South Africa*. Johannesburg, South Africa : ISSA, August 2011, S. 1–8

[SHF01] Stoneburner, Gary ; Hayden, Clark ; Feringa, Alexis ; NIST, National Institute of Standards and Technology (Hrsg.): *Engineering Principles for Information Technology Security : A Baseline for Achieving Security*. (2001). http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf, Abruf: 3.3.2012. – NIST Special Publication 800-27. – MD 20899-8930

[sie12] Siemens Enterprise Communications (Hrsg.): *CRAMM : The Total Information Security Toolkit*. (2012). http://www.cramm.com/, Abruf: 11.1.2012

[SM07] Slevin, Lindi A. ; Macfie, Alex: Role Based Access Control for a Medical Database. *In: Proceedings of the 11th IASTED International Conference on Software Engineering and Applications (SEA'07)*. Anaheim, CA, USA : ACTA Press, 2007, S. 226–233

[Sok99] Sokol, Bettina: *Vierzehnter Datenschutzbericht der Landesbeauftragten für den Datenschutz Nordrhein-Westfalen*. (1999). https://www.ldi.nrw.de/mainmenu_Service/submenu_Berichte/Inhalt/14_DSB/14__Datenschutzbericht.pdf, Abruf: 24.4.2011

[Som03] Sommerlad, Peter: Reverse Proxy Patterns. *In: Proceedings of the 8th European Conference on Pattern Languages of Programs (EuroPLoP 2003)*. Irsee, Germany : Hillside Group, Inc., Juni 2003, S. C6,1–23

[Sow09] Sowa, Sebastian: *Information-Security-Business-Performance-Measurement und -Management im Kontext von Compliance und Unternehmungszielen*. Bochum, Universität, Institut für Sicherheit im E-Business (ISEB), Dissertation, 2009. http://nbn-resolving.de/urn:nbn:de:hbz:294-27428, Abruf: 20.12.2011

[Spe04] Speer, Ronald: *Datenschutzkonzept Kompetenznetz „Herzinsuffizienz"*. (2004). – Version 0.6 – Beziehbar über die TMF

[Spe06] Speer, Ronald ; TMF, Telematikplattform für Medizinische Forschungsnetze e. V. (Veranst.): *Erfahrungen bei der Erstellung und Umsetzung von Sicherheitskonzepten im IT-Verbund IMISE/KKSL*. Berlin, Geschäftsstelle TMF e. V. am 11.12.2006. – Sicherheitskonzepte in der vernetzten medizinischen Forschung : TMF-Workshop. – Beziehbar über die TMF

[Spe11] Spengler, Brad: *Grsecurity Official Homepage.* (2011). http://www.grsecurity.net/index.php, Abruf: 16.3.2011

[Spi07] Spitzer, Michael: *Datenschutzkonzept Teleradiologie-Plattform im HIT-Verbund : Austausch von medizinischen Bilddaten im Rahmen des HIT-Studienverbundes der Deutschen Kinderkrebsstiftung.* (2007). – Version 20070403 – Beziehbar über die TMF

[SPK09] Stango, Antonietta ; Prasad, Neeli R. ; Kyriazanos, Dimitris M.: A Threat Analysis Methodology for Security Evaluation and Enhancement Planning. *In: Proceedings of the Third International Conference on Emerging Security Information, Systems and Technologies (SECURWARE'09).* Washington, DC, USA : IEEE Computer Society, Juni 2009, S. 262–267

[SPR+06] Simon, Jürgen W. ; Paslack, Rainer ; Robienski, Jürgen ; Goebel, Jürgen W. ; Krawczak, Michael: *Biomaterialbanken – Rechtliche Rahmenbedingungen.* Berlin : Mwv Medizinisch Wissenschaftliche Verlagsges., 2006. – ISBN 978-3939069140

[SS00] Schoenberg, Roy ; Safran, Charles: Internet Based Repository of Medical Records That Retains Patient Confidentiality. In: *British Medical Journal* 321 (2000), Nr. 7270, S. 1199–1203

[SS05] Sax, Ulrich ; Schmidt, Stefan: Integration of Genomic Data in Electronic Health Records : Opportunities and Dilemmas. In: *Methods of Information in Medicine* 44 (2005), Nr. 4, S. 546–550

[SSS06] Skrowny, Daniela ; Staub, Tobias ; Sax, Ulrich: *Beschreibungen der Sequenzgrafiken der AG Datenschutz : Revision der Datenschutzkonzepte.* (2006). – Version 0.80

[SST+07] Sinclair, Sara ; Smith, Sean W. ; Trudeau, Stephanie ; Johnson, M. E. ; Portera, Anthony ; Department of Computer Science Dartmouth College (Hrsg.): *Information Risk in the Professional Services : Field Study Results from Financial Institutions and a Roadmap for Research* / Tuck School of Business at Dartmouth. Hanover, NH, US, Juni 2007. http://mba.tuck.dartmouth.edu/digital/Research/ResearchProjects/DataFinancial.pdf, Abruf: 16.3.2011. – Research Report

[Sta09] Stausberg, Jürgen ; TMF, Telematikplattform für Medizinische Forschungsnetze e. V. (Hrsg.): *Bericht zu Projekt V054-01 IT-Strategie Teilprojekt 4 : Analyse der Anforderungen und des Ausstattungsstandes an IT für medizinische Forschungsregister (Bestandsaufnahme, Anforderungskatalog, Realisierungsvorschläge und Roadmap)* / Ludwig-Maximilians-Universität,

Institut für Medizinische Informationsverarbeitung, Biometrie und Epidemiologie. München, September 2009. – Bericht zum Teilprojekt 4 im Rahmen des TMF-Projektes „IT-Strategie“. – Beziehbar über die TMF

[Ste01] Steyer, Ralph: *Java 2 : Professionelle Programmierung mit J2SE Version 1.3*. München : Markt+Technik, 2001. – ISBN 978-3827260390

[Ste06] Steinebach, Martin ; GMDS, Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (Veranst.): *Aspekte der Datensicherheit : Das digitale Wasserzeichen : 11. Fachtagung der GMDS e. V. „Praxis der Informationsverarbeitung in Krankenhaus und Versorgungsnetzen“*. Frankfurt am Main am 31.5.2006

[Sti05] Stiel, Hadi: IAM, UTM etc. : Identity-, Access- und Unified-Threat-Management als Unterstützer einer Sicherheits-Strategie von „innen“. In: *<kes> – The Information Security Journal* 5 (2005), Nr. 5, S. 21

[Str99] Strobel, Stefan: *Firewalls : Einführung, Praxis, Produkte*. 2. erw. und aktual. Aufl. Heidelberg : dpunkt-Verlag, 1999. – ISBN 978-3932588495

[Str10] Strobel, Stefan: Schutzfaktor : Messbarkeit der IT-Sicherheit. In: *iX special* 10 (2010), Nr. 3, S. 156–159

[SW05] Siebenlist, Frank ; Welch, Von ; GlobusWORLD (Veranst.): *Grid Security : The Globus Perspective*. Boston, MA am 7.2.2005. – GlobusWORLD 2005

[SW10] Schlaak, Bastian ; Wäldin, Markus ; Wirtschaftswissenschaftliche Fakultät der Georg-August-Universität Göttingen (Hrsg.): *Messung der Informationssicherheit in der Praxis : Zusammenfassung der Ergebnisse einer empirischen Studie*. (2010). `http://www.uni-goettingen.de/de/document/download/ce1f2a9a06a0c9b192e6720c068bd1de-en.pdf/Studie%20-%20Messbarkeit%20von%20Informationssicherheit%20in%20der%20Praxis.pdf`, Abruf: 21.12.2011

[TBC00] Titterington, Graham ; Bassanese, Paola ; Chappell, Caroline: *E-business Security : New Directions and Successful Strategies*. (2000). `http://www.ovum.com/cgi-bin/showPage.asp?doc=/research/ebs/TOC/default.htm`, Abruf: 11.12.2006

[tcg09a] TCG, Trusted Computing Group (Hrsg.): *Server Specifications*. (2009). `http://www.trustedcomputinggroup.org/developers/server/specifications`, Abruf: 15.3.2011

[tcg09b] TCG, Trusted Computing Group (Hrsg.): *Whitepapers*. (2009). `https://www.trustedcomputinggroup.org/downloads/whitepapers`, Abruf: 20.3.2009

[tcg12] TCG, Trusted Computing Group (Hrsg.): *Developers : Trusted Network Connect : Resources*. (2012). `http://www.trustedcomputinggroup.org/developers/trusted_network_connect/resources`, Abruf: 11.1.2012

[tel11] TeleTrusT Deutschland e. V. (Hrsg.): *European Bridge CA*. (2011). `http://www.teletrust.de/european-bridge-ca/`, Abruf: 16.3.2011

[the10] The SANS Institute (Hrsg.): *The SANS Security Policy Project*. (2010). `http://www.sans.org/resources/policies/`, Abruf: 17.5.2010

[the12] TheGT SecurtiyTeam (Hrsg.): *GT 5.0.3 Security : Key Concepts*. (2012). `http://www.globus.org/toolkit/docs/5.0/5.0.3/security/key/#securityKey`, Abruf: 11.1.2012

[tih12] Tihanyi, Balazs (Hrsg.): *NClass : Free UML Class Designer*. (2012). `http://nclass.sourceforge.net/`, Abruf: 12.6.2012

[TK03] Tipton, Harold F. (Hrsg.) ; Krause, Micki (Hrsg.): *Information Security Management Handbook*. 5. Aufl. Boca Raton, Florida, USA : Auerbach Publishers Inc., 2003. – ISBN 978-0849319976

[tmf10] TMF (Hrsg.): *Satzung des TMF e. V.* (2010). `http://www.tmf-ev.de/Ueber_uns/SatzungTMFeV.aspx`, Abruf: 11.1.2012

[tmf12] TMF (Hrsg.): *Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V. : Arbeitsgruppe Datenschutz*. (2012). `http://www.tmf-ev.de/Arbeitsgruppen_Foren/AGDS.aspx`, Abruf: 11.1.2012

[Töp09] Töpfer, Armin: *Erfolgreich Forschen : Ein Leitfaden für Bachelor-, Master-Studierende und Doktoranden*. Berlin : Springer-Verlag, 2009. – ISBN 978-3540799719

[Tou05] Touriño-Troitiño, Marina: IT Security Audits from a Standardization Viewpoint. In: *UPGRADE – The European Journal for the Informatics Professional* VI (2005), Nr. 4, S. 31–35

[Trc09] Trcek, Denis: Security Metrics Foundations for Computer Security. In: *The Computer Journal* 53 (2009), Nr. 7, S. 1106–1112

[TSSS06] Torres, José M. ; Sarriegi, Jose M. ; Santos, Javier ; Serrano, Nicolás: Managing Information Systems Security : Critical Success Factors and Indicators

to Measure Effectiveness. In: KATSIKAS, Sokratis K. (Hrsg.) ; LOPEZ, Javier (Hrsg.) ; BACKES, Michael (Hrsg.) ; GRITZALIS, Stefanos (Hrsg.) ; PRENEEL, Bart (Hrsg.): *Information Security* Bd. 4176. Berlin/Heidelberg : Springer-Verlag, 2006. – ISBN 3-540383417, S. 530–545

[Vah08] VAHLDIEK, Axel: Die Überall-Software : Ihre komplette Arbeitsumgebung auf dem USB-Stick. In: *c't – Magazin für Computertechnik* 7 (2008), Nr. 14, S. 84–86

[VAM+01] VENTER, Craig J. ; ADAMS, Mark D. ; MYERS, Eugene W. ; LI, Peter W. ; MURAL, Richard J. ; SUTTON, Granger G. ; SMITH, Hamilton O. ; ET AL.: The Sequence of the Human Genome. In: *Science* 291 (2001), Nr. 5507, S. 1304–1351

[Vat11] VATTIG, Robert: *Informationssicherheit in Kliniken: Erstellung eines IT-Grundschutz-Profils für Kliniken auf Basis des BSI Standards 100-2.* Lausitz, Fachhochschule, Diplomarbeit, April 2011. `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Extern/Diplomarbeiten/Robert_Vattig_pdf.pdf?__blob=publicationFile`, Abruf: 15.12.2011

[Ver06] VERPLANCKE, Philippe ; TMF, Telematikplattform für Medizinische Forschungsnetze e. V. (Veranst.): *IT-Sicherheit bei Konfiguration und Betrieb eines Studiensoftwaresystems.* Berlin, Geschäftsstelle TMF e. V. am 11.12.2006. – Sicherheitskonzepte in der vernetzten medizinischen Forschung : TMF-Workshop. – Beziehbar über die TMF

[Vis11] VISHWAKARMA, Prabhat K.: Optimizing and Analysing the Effectiveness of Security Hardening Measures Using Various Optimization Techniques as Well as Network Management Models Giving Special Emphasis to Attack Tree Model. In: *International Journal of Network Security & Its Applications* 3 (2011), Nr. 4, S. 100–109

[VV10] VAISH, Abhishek ; VARMA, Shirshu: Parameter Extraction for Measurement of the Effective Information Security Management : Statistical Analysis. In: *International Journal of Computer and Electrical Engineering* 2 (2010), Nr. 4, S. 654–659

[Wal02] WALDER, Bob: *Intrusion Detection Systems* / NSS Labs. Austin, Texas, USA, 2002. `http://www.nss.co.uk/grouptests/ids/edition4/index.htm`, Abruf: 20.3.2009 (Edition 4). – Group Test Report

[Wan05] WANG, Andy Ju A.: Information Security Models and Metrics. *In: Proceedings of the 43rd Annual Southeast Regional Conference (ACM-SE 43).* New York, NY, USA : ACM, 2005, S. 178–184. – Bd. 2

[War08] Wartmann, Tim: Risiko 2.0 : Eine Analyse der Sicherheit von Ajax. In: *c't – Magazin für Computertechnik* 8 (2008), Nr. 2, S. 130–135

[WB09] Walther, Stefan ; Becker, Kurt: Betrieb von IT-Systemen im Gesundheitswesen. In: Johner, Christian (Hrsg.) ; Haas, Peter (Hrsg.): *Praxishandbuch IT im Gesundheitswesen : Erfolgreich einführen, entwickeln, anwenden und betreiben*. München : Hanser Fachbuchverlag, März 2009. – ISBN 978-3446415560, S. 375–402

[WBS08] Workman, Michael ; Bommer, William H. ; Straub, Detmar: Security Lapses and the Omission of Information Security Measures : A Threat Control Model and Empirical Test. In: *Computers in Human Behavior* 24 (2008), Nr. 6, S. 2799–2816

[Web07] Weber, Ralph: *Probandenversicherung : Grundsätze*. (2007). `http://www.ethik.med.uni-rostock.de/fileadmin/user_upload/dateien/probandenversicherung.pdf`, Abruf: 24.4.2011

[Wei09] Weiss, Steffen O.: *A Model to Quantitatively Assess the Security of Organizations*. Erlangen, Universität, Dissertation, 2009. `http://www.opus.ub.uni-erlangen.de/opus/volltexte/2009/1264/pdf/SteffenWeissDissertation.pdf`, Abruf: 3.3.2012

[wek12] WEKA MEDIA GmbH & Co. KG (Hrsg.): *Lexikon Datenschutz-Praxis*. (2012). `http://www.datenschutz-praxis.de/lexikon/`, Abruf: 11.1.2012

[Wel03] Wellbrock, Rita: Datenschutzrechtliche Aspekte des Aufbaus von Biobanken für Forschungszwecke. In: *Medizinrecht* 21 (2003), Nr. 2, S. 77–82

[Wel05] Welch, Von ; The Globus Security Team (Hrsg.): *Globus Toolkit Version 4 Grid Security Infrastructure : A Standards Perspective*. (2005). `http://www.globus.org/toolkit/docs/4.0/security/GT4-GSI-Overview.pdf`, Abruf: 3.3.2012. – Version 4

[Wey88] Weyuker, Elaine J.: Evaluating Software Complexity Measures. In: *IEEE Transactions on Software Engineering* 14 (1988), Nr. 9, S. 1357–1365

[Wie03] Wiese, Birgitt: *Grobkonzept Datenschutz KN Demenzen*. (2003). – Vorabinformation – Beziehbar über die TMF

[Wie05] Wieser, Hans ; SIT, Fraunhofer-Institut für Sichere Informationstechnologie (Veranst.): *Identity Lifecycle Management : SIT-Sicherheitsforum 2005, Identity Management*. Darmstadt am 1.12.2005. – SIT-Sicherheitsforum 2005 Identity Management

[wik09] Wikileaks (Hrsg.): *Over 8m Virginian Patient Records Held to Ransom, 30 Apr 2009*. (2009). http://wikileaks.org/wiki/Over_8M_Virginian_patient_records_held_to_ransom,_30_Apr_2009, Abruf: 11.5.2009

[wik12] Wikimedia Foundation Inc. (Hrsg.): *Wikipedia : The Free Encyclopedia*. (2012). http://www.wikipedia.org/, Abruf: 11.1.2012

[WIL+08] Wang, Lingyu ; Islam, Tania ; Long, Tao ; Singhal, Anoop ; Jajodia, Sushil: An Attack Graph-Based Probabilistic Security Metric. In: Atluri, Vijay (Hrsg.): *Proceeedings of the 22nd Annual IFIP WG 11.3 Working Conference on Data and Applications Security*. Berlin/Heidelberg : Springer-Verlag, 2008, S. 283–296. – Bd. 5094

[Wil09] Wilshusen, Gregory C.: *Information Security : Concerted Effort Needed to Improve Federal Performance Measures* / United States Government Accountability Office. 2009. http://www.gao.gov/new.items/d09617.pdf, Abruf: 18.11.2011 (GAO-09-617). – GAO-Report

[Win09] Winter, Alfred: The Future of Medical Informatics : Some Perspectives of Intra- and Inter-Institutional Information Systems. In: *Methods of Information in Medicine* 48 (2009), Nr. 1, S. 62–65

[wip06] WIPO, World Intelectual Property Organization (Hrsg.): *WO/2007/107130 : Wireless Internet Client*. (2006). http://www.wipo.int/pctdb/en/wo.jsp?wo=2007107130&IA=DE2006001984&DISPLAY=STATUS, Abruf: 20.3.2009

[Wir08] Wirth, Sebastian: *Hinweise zur Risikoanalyse und Vorabkontrolle nach dem Hamburgischen Datenschutzgesetz*. (2008). http://www.hamburg.de/contentblob/254546/data/hinweise-zur-risikoanalyse-und-vorabkontrolle.pdf, Abruf: 20.3.2009

[WJSN10] Wang, Lingyu ; Jajodia, Sushil ; Singhal, Anoop ; Noel, Steven: k-Zero Day Safety : Measuring the Security Risk of Networks against Unknown Attacks. In: Gritzalis, Dimitris (Hrsg.) ; Preneel, Bart (Hrsg.) ; Theoharidou, Marianthi (Hrsg.): *Proceedings of the 15th European Conference on Research in Computer Security*. Berlin/Heidelberg : Springer-Verlag, 2010, S. 573–587. – Bd. 6345

[Wöh08] Wöhrmann, Andrej: *Datenschutzkonzept der Stiftung Präventivmedizin*. (2008). – Version 0.8 – Beziehbar über die TMF

[Woh11] Wohlmacher, Petra: *Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung : Übersicht über geeignete Algorithmen*. (2011). http://www.bundesnetzagentur.de/SharedDocs/

Downloads/DE/BNetzA/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/2011_2_AlgoKatpdf.pdf?__blob=publicationFile, Abruf: 11.01.2012

[Woo06] Woody, Carol: *Applying OCTAVE : Practitioners Report* / Carnegie Mellon University. Pittsburgh, Pennsylvania, USA, Mai 2006. http://www.sei.cmu.edu/reports/06tn010.pdf, Abruf: 3.3.2012 (CMU/SEI-2006-TN-010). – Technical Note

[Xie10] Xie, Huagang: *Linux Intrusion Detection System (LIDS)*. (2010). http://www.lids.org/, Abruf: 16.3.2011

[XWZ+09] Xie, Anming ; Wen, Weiping ; Zhang, Li ; Hu, Jianbin ; Chen, Zhong: Applying Attack Graphs to Network Security Metric. *In: Proceedings of the International Conference on Multimedia Information Networking and Security (MINES'09)*. Washington, DC, USA : IEEE Computer Society, November 2009, S. 427–431. – Bd. 1

[zen09] Zentralinstitut für die kassenärztliche Versorgung in der Bundesrepublik-Deutschland (Hrsg.): *Elektronischer Heilberufsausweis : Hintergrund*. (2009). http://www.zi-berlin.de/hpc/hintergrund.php, Abruf: 20.3.2009

[Zie06] Ziegler, Jörg: Web Based Training unterstützt die Risikominimierung. In: *it security* 6 (2006), Nr. 5

[Zim08] Zimmermann, Steffen: IT-Portfoliomanagement : Ein Konzept zur Bewertung und Gestaltung von IT. In: *Informatik-Spektrum* 31 (2008), Nr. 5, S. 460–468

Abkürzungsverzeichnis

ADAT	Identifizierende Arztdaten
AIK	Attestation Identity Key
ALE	Annualized Loss Expectancy
AMG	Arzneimittelgesetz
ARL	Authority Revocation List
ARO	Annual Rate of Occurrence
ASP	Application Service Provider
AXIS	Apache eXtensible Interaction System
BCP	Business-Continuity-Plan
BDSG	Bundesdatenschutzgesetz
BMB	Biomaterialbank
BMBF	Bundesministerium für Bildung und Forschung
BITKOM	Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
bzw.	beziehungsweise
CA	Certification Authority
CAG	Citrix Access Gateway
CC	Common Criteria
CERT	Community Emergency Response Team
CERT/CC	Coordination Center
CISWG	Corporate Information Security Working Group
COBIT	Control Objectives for Information and Related Technology
CMP	Certificate Management Protocol
CMS	Centers for Medicare & Medicaid Services
CPS	Citrix Presentation Server
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
CVSS	Common Vulnerability Scoring System
d. h.	das heißt
DAA	Direct Anonymous Attestation
DB	Datenbank
DBMS	Datenbankmanagementsystem
DDV	Datendirektverbindung
DMZ	Demilitarisierte Zone
DRM	Digital Rights Management
DoD	Department of Defense
DoS	Denial of Service
dynSRM	dynamisches Sicherheits- und Risikomanagement

EAL	Evaluation Assurance Level
EJB	Enterprise Java Beans
EK	Endorsement Key
EMSCB	European Multilaterally Secure Computing Base
engl.	englisch
EPA	Elektronische Patientenakte
ESP	Encapsulating Security Payload
eVB	elektronische Versicherungsbestätigung
etc.	et cetera
f.	folgend(e)
FDA	Food and Drug Administration
ff.	folgende
GAO	(United States) Government Accountability Office
GCP	Good Clinical Practice
ggf.	gegebenenfalls
GoBS	Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme
GdPDU	Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen
GDV	Gesamtverband der Deutschen Versicherungswirtschaft e.V.
G-UCON	Grid Usage Control Modell
HIPAA	Health Insurance Portability and Accountability Act
HPC	Health Professional Card
i. d. R.	in der Regel
IAM	Identity- and Access-Management
IATAC	Information Assurance Technology Analysis Center
ICAP	Internet Content Adaptation Protocol
ID	Intrusion Detection
$IDAT$	Identifizierende Personenstammdaten (Identifikationsdaten)
$IDAT^A$	Teilmenge der identifizierenden Personenstammdaten, die für den Aufruf eines Patientendatensatzes erforderlich sind ($IDAT^A \subseteq IDAT$)
IKE	Internet Key Exchange
inkl.	inklusiv(e)
IRC	INFOSEC Research Council
ISAKMP	Internet Security Association and Key Management Protocol
ISECOM	Institute for Security and Open Methodologies
ISM	Information Security Management
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISP	Internet Service Provider
ISSEA	International Systems Security Engineering Association
ITIL	IT Infrastructure Library

ITS	siehe ITSK
ITSCM	IT Service-Continuity-Management
ITSEC	Information Technology Security Evaluation Criteria
ITSK	Die deutschen IT-Sicherheitskriterien
IuK	Information und Kommunikation
J2EE	Java-Plattform, Enterprise Edition
JAAS	Java Authentication and Authorization Service
JACC	Java Authorization Contract for Containers
JAX-WS	Java API for XML Web Services
JAXB	Java Architecture for XML Binding
JAXP	Java API for XML Processing
JAXR	Java API for XML Registries
JDBC	Java Database Connectivity
JMS	Java Message Service
JMX	Java Management Extensions
JTA	Java Transaction API
JCA	J2EE Connector Architecture
JSF	Java Server Faces
JSON	JavaScript Object Notation
JSP	JavaServer Pages
JSTL	JavaServer Pages Standard Tag Library
KPOH	Kompetenznetz Pädiatrische Onkologie und Hämatologie
LabID	Probennummer. Zufallszahl, kennzeichnet die Laborprobe, wird nur in der Behandlungsdatenbank gespeichert
MDAT	Medizinische Daten
$MDAT^*$	*MDAT* verschlüsselt
$MDAT^S$	selektierte Teilmenge der medizinischen Daten $MDAT^W$, die einem Wissenschaftler zur Verfügung gestellt wird
$MDAT^W$	wissenschaftlich relevanter Teil der Behandlungsdaten
NAS	Network Attached Storage
NCI	National Cancer Institute
NGSCB	Next Generation Secure Computing Base
NIH	National Institutes of Health
NIST	National Institute of Standards and Technology
o. g.	oben genannt(e)
OCL	Object Constraint Language
OID	Objekt-Identifikatoren
OWASP	Open Web Application Security Project
PC	Personal Computer
PCR	Platform Configuration Registers

PEM	Privacy Enhanced Mail
PID	Patientenidentifikator
PKI	Public Key Infrastructure
POH	Pädiatrische Onkologie und Hämatologie
PPP	Point-to-Point Protocol
PRF	Pseudo Random Function
PSE	Private Security Environment
PSN	Pseudonym
RA	Registration Authority
RAND	**R**esearch **and D**evelopment
RAV	Risk Assessment Value
RDB	Referenzdatenbank
REST	Representational State Transfer
ROI	Return on Investment
ROSI	Return on Security Investment
RöV	Röntgenverordnung
RZ	Rechenzentrum
S&R(-Management)	Sicherheits- und Risikomanagement
S.	Seite
s. a.	siehe auch
SCM	Service-Continuity-Management
SDB	Studiendatenbank
SID	Session Identifier
SIEM	Security Information and Event Management
SigG	Signaturgesetz
SLA	Service-Level-Agreement
SLE	Single Loss Expectancy
SNP	Single Nucleotide Polymorphismus
SOAP	Simple Object Access Protocol
sog.	so genannt(e,er,es)
SOP	Standard Operating Procedure
SRM	Security Risk Management
SPAN	System Performance ANalyzer
SSE-CMM	Systems Security Engineering – Capability Maturity Model
StAX	Streaming APIs for XML Parsers
StrlSchV	Strahlenschutzverordnung
TC	Trustworthy Computing
TCG	Trusted Computing Group
TCPA	Trusted Computing Platform Alliance (TCPA)
TCSEC	Trusted Computer System Evaluation Criteria

TempID	Temporäre ID, ersetzt während einer Anfrage *IDAT* zwecks $MDAT^W \rightarrow IDAT$-Zuordnung
TLS	Transport Layer Security
TMF	Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V.
TMI	Telemedizinische Infrastruktur
TNC	Trusted Network Connect
TPM	Trusted Platform Module
TCSEC	Trusted Computer System Evaluation Criteria
u. a.	unter anderem
u. U.	unter Umständen
UDP	User Datagram Protocol
usw.	und so weiter
UTM	Unified Threat-Management
v. a.	vor allem
vgl.	vergleiche
vs.	versus
WCCP	Web Cache Control Protocol
WS	Web Services
WSE	Microsoft Web Services Enhancements
WSS	Web Services Security
XSS	Cross-Site-Scripting
z. B.	zum Beispiel
z. T.	zum Teil

Glossar

24/7: Die Bezeichnung 24/7 symbolisiert ständige Bereitschaft bzw. Verfügbarkeit einer Dienstleistung oder seltener die Fähigkeit zum Dauerbetrieb eines Produkts. Die Abkürzung steht für 24 Stunden am Tag, 7 Tage die Woche.

3DES: Abkürzung für Triple-DES. 3DES ist eine Variante des symmetrischen Blockverschlüsselungsverfahrens DES (siehe *DES*). Triple-DES gleicht den Nachteil des als schwach geltenden kurzen DES-Schlüssels durch eine Dreifachverschlüsselung aus.

ADAT: Daten, die einen teilnehmenden Arzt des *Forschungsverbunds* beschreiben, insbesondere Name und Kontaktdaten. *ADAT* werden meist als Teil der *OrgDAT* behandelt.

AES: Abkürzung für Advanced Encryption Standard. Vom US-amerikanischen *NIST* im Jahr 2001 vorgestellter offizieller Kryptostandard für die USA. In einem vom *NIST* ausgeschriebenen Wettbewerb um den Nachfolger des DES (Data Encryption Standard) wurden in einer ersten Sichtung zunächst 15 Kandidaten ermittelt. Von diesen kamen im August 1999 schließlich fünf Kandidaten in die engere Ausscheidung: MARS (IBM), RC6 (RSA Laboratories), RIJNDAEL, Serpent (Ross Anderson, Eli Biham, Lars Knudsen) und Twofish (Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson). Mitte 2001 entschied sich das *NIST* für die von den belgischen Kryptographen Vincent Rijmen und Joan Daemen entwickelte symmetrische Blockchiffrierung namens RIJNDAEL. Die Blocklänge und die Schlüssellänge des AES/RIJNDAEL können unabhängig voneinander die Werte 128, 192 oder 256 Bit aufweisen. Jeder Block wird zunächst in eine zweidimensionale Tabelle mit vier Zeilen geschrieben, dessen Zellen ein Byte groß sind. Die Anzahl der Spalten variiert somit je nach Blockgröße von 4 (128 Bit) bis 8 (256 Bit). Die Blöcke werden nun nacheinander bestimmten Transformationen unterzogen. Aber anstatt jeden Block einmal mit dem Schlüssel zu chiffrieren, wendet AES/RIJNDAEL verschiedene Teile des Schlüssels nacheinander auf den Klartextblock an. Die Anzahl dieser Runden variiert und ist von Schlüssellänge und Blockgröße abhängig.

Ajax: Kompositum aus Asynchronous *JavaScript* und *XML*. Eine Technologie, mit der Daten zwischen Client und Server mittels *JavaScript* ausgetauscht werden können, ohne dass die gesamte Webseite neu geladen werden muss. Der Begriff AJAX geht auf den im Februar 2005 veröffentlichten Artikel Ajax: A New Approach to Web

Applications von Jesse James Garrett von der Firma Adaptive Path zurück. Dort wird die bis dahin XMLHTTPRequest (Extensible Markup Language – Hypertext Transfer Protocol – Request) genannte Technologie unter dem einprägsameren Namen AJAX einem breiteren Publikum vorgestellt.

ALE: Erwartungswert für den pro Jahr aufgrund von Sicherheitsgefährdungen zu erwartenden Schaden. $ALE = ARO \times SLE$. ALE: Annualized Loss Expectancy; ARO: Annual Rate of Occurrence; SLE: Single Loss Expectancy.

Anonymisierung: Anonymisierung ist die Aufhebung der *Personenbezogenheit* von Daten zu einer Person. Anonymisierung bedingt, dass eine Zuordnung der Daten zu einer Person technisch und inhaltlich nicht mehr möglich ist oder aber eine Reidentifizierung inhaltlich nur noch mit unverhältnismäßig großem Aufwand möglich wäre, sodass ein Erfolg höchst unwahrscheinlich erscheint. Anonymisierung liegt beispielsweise beim Verändern der personenbezogenen Daten in der Art vor, dass die Einzelangaben über die persönlichen oder sachlichen Verhältnisse des *Patienten* oder *Probanden* nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Hiervon abgeleitet kann man, je nach theoretischer Möglichkeit der *Reidentifizierung*, zwischen vollkommener und faktischer Anonymisierung unterscheiden. *Vollkommene Anonymisierung* liegt vor, wenn eine nicht nur technisch, sondern auch inhaltlich absolut irreversible Abtrennung der *Personenbezogenheit* besteht, d. h. wenn auch theoretisch aus dem Inhalt der Daten nicht mehr auf eine Person zurückgeschlossen werden kann. *Faktische Anonymität* besteht dann, wenn diese Möglichkeit des Rückschlusses bei bestimmten Datenkonstellationen (Alleinstellungsmerkmale oder Kombination vieler Datensätze) theoretisch nicht ausgeschlossen ist, aber praktisch mit so hohem Aufwand verbunden wäre, dass sie nach der allgemeinen Lebenserfahrung unverhältnismäßig und unwahrscheinlich erscheint (vgl. [RHJ08, S. 29]). Erscheint diese Reidentifizierung aus dem Inhalt der Daten heraus wieder möglich, so ist die formal vollzogene Anonymisierung unvollständig und es herrscht wieder *Personenbezogenheit*. Als formale Anonymisierung bezeichnet man den Anonymisierungsvorgang, unabhängig davon, ob faktische oder vollkommene Anonymität erreicht wird oder nicht. Zur Legaldefinition des Begriffs Anonymisierung siehe § 3 Abs. 6 BDSG.

Archivierung: Dauerhafte Aufbewahrung von Daten auf geeigneten Datenträgern. Im Kontext der medizinischen Forschungsnetze ist die Archivierung beispielsweise für klinische oder auch *epidemiologische Studien* relevant, wobei mindestens der Stand zum Zeitpunkt der Auswertung eingefroren werden soll.

Arzneimittelgesetz: Das Arzneimittelgesetz (Gesetz über den Verkehr mit Arzneimitteln, AMG) ist in Deutschland ein Gesetz des besonderen Verwaltungsrechts zur Ein-

und Ausfuhr und zum Verkehr mit Arzneimitteln. Das AMG stellt strikte, auch datenschutzrechtlich relevante, Anforderungen an die Durchführung einer *klinischen Studie*.

Arzt, behandelnder: Der Arzt, der einen *Patienten* erstmals erfasst, d. h. dessen *Stammdaten* erstmals anlegt, wird vom Forschungsnetz als dessen behandelnder Arzt geführt. Jeder weitere Arzt, der Daten zu diesem *Patienten* erfassen und auch die Vorbefunde dieses *Patienten* einsehen möchte, muss sich – nach eingeholter Zustimmung des *Patienten* – dem Forschungsnetz gegenüber in geeigneter Weise als behandelnder Arzt autorisieren. Erst dann wird er für den Zugang dieses *Patienten* als behandelnder Arzt in der klinischen Datenbank frei geschaltet.

Ausschuss Datenschutz: Der Ausschuss Datenschutz ist ein *Gremium* eines *Forschungsverbundes*, das die Regelung aller mit dem Datenaustausch und dem Datenzugang zusammenhängenden Fragen verantwortet. Dem Ausschuss Datenschutz kommen folgende fachlichen Aufgaben zu:

- Bewertung und Bewilligung der Anträge von Wissenschaftlern auf die Bereitstellung von Forschungsdaten, welche Ziel, Weg und Datenbedarf darstellen.
- Bewertung und Bewilligung von Anträgen auf Übermittlung von Forschungsergebnissen an *Patienten* durch deren behandelnde Ärzte.
- Die Beauftragung der zentralen Dienste und die Verabschiedung der Policies und Nutzungsordnungen für diese zentralen Dienste, welche die für Datenschutz und Datensicherheit relevanten Regeln enthalten. Der Ausschuss Datenschutz kann auch durch ein *Gremium* verkörpert werden, das andere Aufgaben hat (und anders bezeichnet wird), z. B. Vorstand. Der Datenschutzbeauftragte des *Forschungsverbunds* soll diesem *Gremium* angehören; seine vom Datenschutzgesetz definierten Rechte und Pflichten sind dadurch unberührt. Die Aufgaben des Ausschusses Datenschutz gehen über die gesetzlich definierten Aufgaben des Datenschutzbeauftragten hinaus.

Authentifikation: siehe *Authentifizierung*.

Authentifizierung: Authentifizierung ist der Nachweis (Verifizierung) einer behaupteten Eigenschaft einer Partei, die beispielsweise ein Mensch, ein Gerät, ein Dokument oder eine Information sein kann, und die dabei durch ihren Beitrag ihre *Authentisierung* durchführt. Im englischen Sprachraum wird zwischen den Aktionen beider Parteien syntaktisch nicht unterschieden. Im deutschen Sprachraum ist diese Unterscheidung oft auch nicht zu finden.

Authentisierung: siehe *Authentifizierung*.

AXIS: Apache Axis (Apache eXtensible Interaction-System) ist eine SOAP-Engine zur Konstruktion von darauf basierenden Web Services und Client-Anwendungen. Axis wird häufig als Java-Servlet innerhalb eines Servlet-Containers (beispielsweise Apache Tomcat) betrieben, der Web Services für Java-Klassen anbietet. Mit den Tools JAVA2WSDL und WSDL2JAVA wird der Entwickler dabei unterstützt, automatisch eine robuste Schnittstelle in Java zu erzeugen, ohne sich direkt mit der Funktionsweise von SOAP befassen zu müssen.

Bastion Host: Ein besonders gesichertes exponiertes Gateway, das aus einem ungesicherten Netz angesprochen werden kann und Angriffe jedweder Art abwehren soll. Im Bereich des Internets – ein Rechner, über den alle Netzwerkzugriffe aus und in das weltweite Internet gehen.

Behandlungszusammenhang: Daten und *Proben* werden im Behandlungszusammenhang gewonnen, wenn sie im Rahmen der Behandlung eines *Patienten* von einem Arzt oder dem Mitarbeiter einer Klinik oder sonstigen klinischen Einrichtung erhoben werden und ihre Zweckbestimmung in der Analyse für Zwecke der weiteren Behandlung des *Patienten* zu sehen ist. Daten und *Proben* aus dem Behandlungszusammenhang sind durch die ärztliche *Schweigepflicht* besonders geschützt, solange sie diesen nicht verlassen. Sollen Daten oder Proben aus dem Behandlungszusammenhang auch für weitergehende Forschungszwecke verwendet werden, ist vor der Probenerhebung grundsätzlich eine zusätzliche Information des *Patienten* über diese Zwecke sowie seine entsprechende *Einwilligung* erforderlich. Das Pendant zu im Behandlungszusammenhang gewonnenen Daten und *Proben* sind solche, die im *Forschungszusammenhang* erhoben werden.

Benefit Denial: Unter dem Begriff „Benefit Denial“ werden (Informationssicherheits-)Maßnahmen zusammengefasst, die die Straftat für die Angreifer unrentabel machen sollen.

Beschlagnahmefestigkeit: Beschlagnahmefestigkeit ist der durch Rechtsvorschriften konstituierte Schutz von Gegenständen (Sachen, Akten, Unterlagen, Daten etc.) gegenüber beweissichernden Maßnahmen der Strafverfolgungsbehörden. Beschlagnahmeverbote ergeben sich aus verschiedenen Prozessordnungen, insbesondere aus § 97 Abs. 1 StPO. Im Unterschied zu personenbezogenen Unterlagen bei Rechtsanwälten, Notaren und Ärzten unterliegen Forschungsdaten und *Proben* keinem solchen Beschlagnahmeschutz. Das gilt somit auch für Daten und *Proben* von medizinischen Forschungsverbünden. Zum Thema Beschlagnahmefestigkeit und Forschungsgeheimnis siehe auch [RHJ08, S. 56], [SPR+06, S. 161 ff.].

BildDAT: Bilder aus bildgebenden Verfahren der Medizin, die in digitaler Form vorliegen und mit organisatorischen oder technischen Begleitdaten (*OrgDAT*) versehen sind.

Analysedaten aus Bildern werden in der Regel den *MDAT* zugeschlagen, da sie – im Gegensatz zu Probenanalysedaten – geringes Reidentifizierungspotenzial besitzen. Das Restrisiko der *Reidentifizierung* ist dadurch zu begründen, dass z. B. mithilfe von Schichtbilddaten morphologische Patienteninformationen rekonstruiert werden können (s. a. Abschnitt 4.3.1 „Schutzbedarfsorientierte Analyse“).

Bilddatenbank: Eine Bilddatenbank ist eine Einrichtung, die medizinische Bilder (*BildDAT*) sammelt, ggf. aufbereitet, ggf. durch demographische und krankheits- bzw. fragestellungsbezogene (*MDAT*) Daten des *Probanden* ergänzt und Bilder sowie evtl. Daten in geeigneter Form für Forschungszwecke zur Verfügung stellt.

Biomaterialbanken: Auch Biobanken, Probenbanken, Gewebebanken, Genbanken, Probensammlung. Einrichtungen, die *Proben* menschlicher Körpersubstanzen (Gewebe, Blut, Zellen, ganze Organe etc.) sammeln bzw. Anteile solcher Substanzen extrahieren (z. B. Serum oder DNA), diese durch Daten des Probanden (personenbezogen, krankheitsbezogen) ergänzen und Proben und Daten in geeigneter Form für Forschungszwecke zur Verfügung stellen.

BIOS: Abkürzung für Basic Input Output System (Basissystem für Ein- und Ausgabe). In der Informationstechnologie das System für die Ein- und Ausgabeanforderungen an die Hardware eines Computers.

Brute-Force: Von engl. brute (brutal, brachial) und force (Gewalt, Stärke). Allgemein steht Brute-Force für Angriffe auf verschlüsselte Nachrichten, indem alle theoretisch möglichen Schlüsselkombinationen durchprobiert werden. Im weiteren Sinn gehört zum Brute-Force auch das Durchprobieren von Passwörtern und Benutzerkennungen, um an bestimmte Netze, Dienste, Datenbanken usw. heranzukommen.

Bundesdatenschutzgesetz: Das deutsche Bundesdatenschutzgesetz (BDSG) regelt zusammen mit den Datenschutzgesetzen der Länder und anderen bereichsspezifischeren Regelungen den Umgang mit personenbezogenen Daten, die in IT-Systemen oder manuell verarbeitet werden.

Bürgschaft: Die Bürgschaft ist ein einseitig verpflichtender Vertrag, durch den sich der Bürge gegenüber dem Gläubiger eines Dritten (des sogenannten Hauptschuldners) verpflichtet, für die Erfüllung der Verbindlichkeiten des Dritten einzustehen. Der Gläubiger will sich durch die Bürgschaft im Falle einer Zahlungsunfähigkeit seines Schuldners absichern. Meistens handelt es sich bei dem Dritten um einen Darlehensnehmer und bei dem Gläubiger um eine Bank, die das Darlehen gewährt. Die Bürgschaft sichert damit als eigene Leistungsverpflichtung des Bürgen gegenüber dem Gläubiger die Schuld des Dritten (Hauptschuld).

CC: Abkürzung für Common Criteria (Gemeinsame Kriterien). Kurzform für Common Criteria for Information Technology Security Evaluation (Gemeinsame Kriterien

für die Prüfung und Bewertung der Sicherheit von Informationstechnik (IT)). Im Bereich der IT-Sicherheit Bezeichnung für gemeinsame, auf der Basis von *ITSEC* (Information Technology Security Evaluation Criteria) und *TCSEC* erarbeitete sogenannte Evaluationskriterien (ISO/IEC CD 15408), die von Vertretern aus den USA, Kanada, Großbritannien, den Niederlanden, Frankreich und Deutschland entwickelt und Ende Mai 1998 (Version 2.0) mit dem Ziel veröffentlicht wurden, die weltweite Anerkennung von Sicherheitszertifikaten für die danach zertifizierten Produkte zu erreichen. Analog zu *ITSEC* unterscheiden diese Kriterien Sicherheitsanforderungen an Funktionalität und Vertrauenswürdigkeit eines Systems. Hinsichtlich der Vertrauenswürdigkeit umfassen die Common Criteria sieben vordefinierte Stufen, die sogenannten Evaluationsstufen (Evaluation Assurance Level, EAL): von EAL 1 (niedrigste Stufe) bis EAL 7 (höchste Stufe).

CHAP: Abkürzung für Challenge Handshake Authentication Protocol. Ein in der Konfigurationsphase eines PPP-Links (Point-to-Point Protocol) eingesetztes Protokoll zur *Authentifikation* zwischen den verbundenen Systemen.

COBIT: Abkürzung für „Control Objectives for Information and Related Technology“. Von der ISACA (Information Systems Audit and Control Association) spezifizierte Sammlung logisch strukturierter Best-Practice-Empfehlungen zum Management IT-gestützter, geschäftsrelevanter Prozesse. Durch die Integration von Sicherheits- und Kontrollanforderungen verschiedener Standards und Methoden zum Management und zur Kontrolle von Informationstechnologien (IT) stellt COBIT eine Methode zur Etablierung eines adäquaten Sicherheits- bzw. Kontrollumfelds bereit. Darüber hinaus umfasst COBIT Mechanismen, um die Vollständigkeit und die Effektivität eines solchen Kontrollumfelds zur Begrenzung der entstehenden Risiken prüfen zu können.

Code-Freeze: Der Code-Freeze (im Deutschen gelegentlich auch als Einfrieren des Quellcodes bekannt) bezeichnet innerhalb eines Softwareprojekts den Zeitpunkt, ab dem sich der Quellcode der Software bis zur endgültigen Freigabe der aktuellen Version nicht mehr ändern soll. Erlaubt sind allerdings noch Änderungen zur Behebung von im Test der Software entdeckten Fehlern von größerer Relevanz. In der Praxis der Softwareentwicklung wird der Code-Freeze in der Regel mehrere Wochen, u. U. auch Monate vor der geplanten Veröffentlichung einer Softwareversion festgelegt, damit noch ausreichend Zeit für das Testen der endgültigen Version der Software bleibt.

Compliance-Software: Unter Compliance-Software werden Werkzeuge verstanden, die die Konformität von Systemen zu den bestimmten Richtlinien oder Gesetzen überprüfen. Dies geschieht i. d. R. durch Softwareagenten, die Daten von Systemen sammeln und diese an eine zentrale Auswertungsstelle weiterleiten.

Cracker: Im Fachjargon Person, die ohne Berechtigung in ein Computersystem unter Umgehung des Sicherheitssystem eindringt um an sensible Daten zu gelangen. Im Gegensatz zu *Hackern*, die dieses Eindringen nur zu ihrem persönlichen Vergnügen durchführen, verursachen Cracker oft bewusst Schäden oder nehmen diese zumindest billigend in Kauf.

Cross-Site Scripting: Cross-Site Scripting (XSS) bezeichnet das Ausnutzen einer Sicherheitslücke, wobei Informationen aus einem Kontext, in dem sie nicht vertrauenswürdig sind, in einen anderen Kontext eingefügt werden, wo sie als vertrauenswürdig gelten. Aus diesem vertrauenswürdigen Kontext wird dann ein Angriff gestartet.

Cyber-Terrorismus: Cyber-Terrorismus ist eine spezielle Form des Terrorismus, der mithilfe von Internet-Technologien Angriffe auf Computersysteme verübt. Es gibt kontroverse Meinungen über den Cyber-Terrorismus. Manche Warner prophezeien Schreckensszenarien mit Tausenden von Toten durch falsch gesteuerte Schleusentore, veränderte Zusammensetzung von Medikamenten oder gar atomare Katastrophen durch Überlisten der Sicherheitssysteme und Manipulieren der bestehenden Programme. Gleichzeitig gibt es viele gelegentliche Warner bis zu denen, die von bloßer Panikmache sprechen und den Cyber-Terrorismus für irreal halten. Fakt ist: Als Cyber-Terrorismus bezeichnet man Computerkriminalität, speziell im Internet, die terroristische Hintergründe hat.

Cybersquatting: Cybersquatting (engl. squatter = Hausbesetzer) ist eine abfällige Bezeichnung für das Registrieren von Internetdomains, die dem Registrierenden eigentlich nicht zustehen, oder die er selber nicht nutzen will. Der Cybersquatter bietet diese Domains dann einem rechtmäßigeren Interessenten zu einem (möglicherweise) überhöhten Preis an; ein Akt, der von manchen als Erpressung angesehen wird.

Cyberstalking: Cyberstalking ist eine neue Form des Mobbings und der Verfolgung anderer Personen, bei der sich Täter oder Täterin der neuen Medien bedienen. Besonders beliebt bei Cyberstalkern sind die Möglichkeiten des Internets.

Datenkategorien in einem medizinischen Forschungsnetz: Bei einem Forschungsnetz fallen unterschiedliche Datenkategorien an. Im Einzelnen werden folgende logische Datenkategorien unterschieden: *IDAT*, *LabID*, *MDAT*, *BildDAT*, *OrgDAT*, *PID*, *ProbDAT* und *PSN*.

Datentreuhänder: Der Datentreuhänder ist eine unabhängige Stelle mit besonderer Geheimhaltungspflicht, z. B. ein Notar oder ein externer Arzt. Der Datentreuhänder tritt zwischen eine Forschungsdaten besitzende Stelle und den *Forscher* und sichert dadurch die Rechte der betroffenen *Patienten* und *Probanden*. Er anonymisiert oder

pseudonymisiert die von der Daten besitzenden Stelle übermittelten personenbezogenen Daten und übermittelt nur die anonymisierten bzw. pseudonymisierten Daten an den *Forscher* weiter. Auf diese Weise bleibt der Kreis derjenigen, die Kenntnis von personenbezogenen Daten erhalten, eng begrenzt, und die Datensicherheit kann effektiv gewährleistet werden. Die durch den Datentreuhänder wahrgenommene Funktion eines vertrauenswürdigen Dritten kann noch verstärkt werden, wenn dieser einer Berufsgruppe angehört, die gesetzlich zur Verschwiegenheit verpflichtet ist und deren Unterlagen und Daten einem Beschlagnahmeschutz unterliegen (z. B. Rechtsanwälte, Notare). Datentreuhänder werden bereits von einigen *medizinischen Kompetenznetzen* eingesetzt (z. B. Kompetenznetz Parkinson e. V.).

Datenverarbeitende Stelle: Die für die Verarbeitung personenbezogener Daten *verantwortliche Stelle*.

DBMS: Abkürzung für „Database Management System“ (Datenbankmanagementsystem). Die auf eine Datenbank (Database System) bezogene Sammlung von Programmen, die die anwendungsunabhängige, dauerhafte Speicherung von Daten in der betreffenden Datenbank ermöglicht und die damit verbundene Verwaltung übernimmt. Eine weitere Aufgabe eines DBMS ist die Bereitstellung von verschiedenen Sichten (Views) auf die gespeicherten Daten, die Konsistenzprüfung der Daten (Integritätssicherung), die Autorisationsprüfung, die Behandlung gleichzeitiger Zugriffe verschiedener Benutzer (Synchronisation) und das Bereitstellen einer Datensicherungsmöglichkeit für den Fall von Systemausfällen.

Depseudonymisierung: Befugte Wiederherstellung des Personenbezugs von anonymisierten oder pseudonymisierten Daten und *Proben*. Dies wird durch Umkehrung des *Pseudonymisierungsverfahrens* erreicht. Depseudonymisierung wird in bestimmten Anwendungsfällen als kontrollierter Vorgang aktiv betrieben, z. B. bei der Rückübermittlung von Forschungserkenntnissen an einen *Patienten*, die auf der Basis pseudonymisierter Daten gewonnen wurden. Davon zu unterscheiden ist die *Reidentifizierung* als unbefugte Wiederherstellung des Personenbezugs (s. a. *Anonymisierung*, *Pseudonymisierung*).

DES: Abkürzung für Data Encryption Standard. Von IBM im Auftrag der US-Regierung entwickeltes Blockverschlüsselungsverfahren, das 1978 in den USA standardisiert wurde (ANSI X3.92) und sich in vielen Bereichen weltweit durchsetzen konnte.

Diffie-Hellmann: Der Diffie-Hellman-Schlüsselaustausch ist ein aus dem Jahr 1976 zurückgehendes Verfahren (Algorithmus) zum sicheren Austausch von kryptografischen Schlüsseln zwischen zwei Teilnehmern über unsichere Kanäle. Dazu werden die Eigenschaften diskreter Logarithmen ausgenutzt. Die Sicherheit des Verfahrens basiert auf der Verwendung einer sogenannten Einwegfunktion. Hierbei macht man

sich die Tatsache zunutze, dass es zwar sehr einfach ist eine Zahl zu potenzieren, die Berechnung des diskreten Logarithmus einer Zahl nur mit sehr großem Aufwand möglich ist.

Digest: Ein Message Digest ist eine kryptografische Einweg-Hash-Funktion (s. a. *Hashwert*).

DLCI: Abkürzung für Data Link Connection Identifier. Logische Verbindungsadresse beim Frame Relay (FR), die sich an das LAPD des D-Kanal-Protokolls (DSS1) im ISDN anlehnt. Der DLCI dient zur Identifizierung der festen (PVC, Permanent Virtual Circuit) und gewählten (SVC, Switched Virtual Circuit) virtuellen FR-Verbindungen.

DoS: Abkürzung für „Denial of Service“ (Diensteversagung, Diensteverweigerung). Im Internet benutzte Bezeichnung für eine Situation, in der ein Rechner (Server) durch viele echte oder falsche Anfragen oder große Datenmengen so überlastet wird, dass er seine eigentlichen Aufgaben nicht mehr erfüllen kann und unter Umständen sogar abstürzt. In Anlehnung daran bezeichnet man eine Angriffsart, die darauf abzielt, bestimmte Dienste oder einen bestimmten Server zu blockieren, als Denial-of-Service-Angriff (DoS-Angriff). Beim sogenannten Distributed Denial of Service (DDoS), einer Variante des DoS-Angriffs, wird eine Software über das Internet oder ein anderes Computernetz verteilt, die es ermöglicht, einen DoS-Angriff auf ein bestimmtes Ziel gleichzeitig von verschiedenen Orten aus zu starten.

DRM: Abkürzung für Digital Rights Management, dt. Digitale Rechteverwaltung oder Digitales Rechtemanagement (DRM). Oberbegriff für Systeme, die die Einhaltung von Urheberrechten an „digitalen“ Inhalten (Dokumente, Dateien usw.) überwachen. Die dabei eingesetzten Methoden sind in der Regel die Verschlüsselung und sogenannte digitale Wasserzeichen. Ziel ist die Kontrolle über die Verbreitung digitaler Inhalte und die Einhaltung der damit verbundenen Rechte im Bereich des Electronic Commerce (E-Commerce) und anderer digitaler Medien. Insbesondere geht es dabei um die Verhinderung der Verbreitung von „Raubkopien“.

Dumpster Diving: Von engl. dumpster (Müllcontainer, Mülleimer) und to dive (tauchen, abtauchen), auch als Trashing bezeichnet. Im *Social Engineering* eingesetzte Spionageattacke, die sich in der unmittelbaren Umgebung einer Person oder mehrerer Personen (Human Based Social Engineering) abspielt. Darunter versteht man im engeren Sinne das Entwenden von Papiermüll, um diesen nach verwertbaren Informationen zu durchsuchen. Häufig dient Dumpster Diving der Vorbereitung von Angriffen.

Dynamische Finanzanalyse: Dynamische Finanzanalyse (Dynamic Financial Analysis) ist eine Simulationsmethode, bei der Informationen über die Verteilung von verbuchten

Prämien, Schadensquoten, Eigenkapital etc. aus stochastisch erzeugten Szenarien entnommen werden.

Einwilligungserklärung: Die vom Datenschutzrecht geforderte Voraussetzung zur Verarbeitung personenbezogener Daten des Betroffenen, sofern diese nicht aufgrund eines Gesetzes erlaubt ist. Die Einwilligungserklärung eines *Patienten* oder *Probanden* ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist zuvor über den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung seiner Daten und *Proben* aufzuklären (informed consent). Die Wirksamkeit der Einwilligungserklärung erfordert deren Schriftform. Soll sie zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben. Materiellrechtlich setzt die Einwilligungserklärung die Einsichtsfähigkeit des Erklärenden voraus. Zu den gesetzlichen Anforderungen an die Einwilligungserklärung siehe § 4a Abs. 1 BDSG; siehe dort auch den Sonderfall in § 4a Abs. 2 BDSG, wenn im Bereich der wissenschaftlichen Forschung durch die Schriftform der bestimmte Forschungszweck erheblich beeinträchtigt würde; in einem solchen Fall kann u. U. auf das Erfordernis der Schriftlichkeit verzichtet werden. Zur Klarstellung der Eigentumsverhältnisse bzw. der Verfügungs- und Nutzungsrechte an einer Probe empfiehlt es sich, diese in einem mit der Einwilligungserklärung verbundenen Vertrag zwischen *Proband* und Proben erhebender Stelle zu regeln (vgl. [HIB+06]).

Elementarschäden: Elementarschäden sind Schäden, die durch das Wirken der Elemente an menschlichem Gut verursacht werden. Als Elementarschäden werden insbesondere Schäden betrachtet, die von Überschwemmungen und Erdbeben verursacht werden.

Epidemiologie: Die Epidemiologie ist ein medizinisches Fachgebiet, das sich mit den Ursachen und Folgen sowie der Verbreitung von gesundheitsbezogenen Einflüssen und Ereignissen in einer Bevölkerung beschäftigt. Die Epidemiologie untersucht somit jene Faktoren, die zu Gesundheit und Krankheit von Individuen und Populationen beitragen und ist deshalb die Basis aller Maßnahmen, die im Interesse der Volksgesundheit unternommen werden.

Epidemiologische Studie: Eine *Studie*, bei der Fragestellungen der *Epidemiologie* bearbeitet werden.

Firebird: Firebird ist der Open Source Spin-Off des kommerziellen relationalen Datenbankmanagementsystems „InterBase“.

Forscher: Personen, die die Daten des *medizinischen Forschungsverbunds* für Forschungszwecke nutzen. Die Forscher können der *Trägereinrichtung* des Verbundes selbst angehören (interne Forschung) oder aus anderen Einrichtungen kommen (externe Forschung). Der Forscher als Nutzer tritt mit seinen Anforderungen (Spezifikation der Erkrankung, Randparameter wie Alter und Komorbiditäten, Anforderungen an

die Daten oder Proben bzw. deren Analyse etc.) an den *Forschungsverbund* heran und erhält nach Durchlaufen eines geregelten Verfahrens Daten und gegebenenfalls auch Proben auf der Grundlage eines Abgabevertrags.

Forschungsdatenbank: Datenbank, in der medizinische Daten aus den in einem *Forschungsnetz* zusammengeschlossenen medizinischen Einrichtungen und *Studien* langfristig gesammelt werden. Zweck ist die wissenschaftliche Auswertung, auch über längere Zeiträume hinweg. Im Gegensatz zu einer *klinischen Datenbank* beschränkt sich der Bezug zum *Patienten* nur auf die Möglichkeit, Daten aus verschiedenen Quellen und von anderen Zeitpunkten korrekt zusammenzuführen.

Forschungsverbund: siehe *Medizinisches Forschungsnetz*.

Forschungsvorhaben: Ein Forschungsvorhaben kann in unterschiedlichen Formen durchgeführt werden. Am verbreitetsten sind *klinische Studien*, also die wissenschaftliche Auswertung diagnostischer und therapeutischer Maßnahmen am kranken Patienten, und *epidemiologische Studien*, also die bevölkerungsbezogene Untersuchung einer Erkrankung und ihrer Ursachen. Letztere kann als Survey, als Screening, retrospektive Studie, prospektive Studie, Kohortenstudie oder Interventionsstudie durchgeführt werden.

Forschungszusammenhang: Daten und *Proben*, mit denen *Forschungsvorhaben* durchgeführt werden, stehen im Forschungszusammenhang. Sie können direkt im Forschungszusammenhang erhoben oder aus dem *Behandlungszusammenhang* in den Forschungszusammenhang überführt werden. Im Forschungszusammenhang werden Daten und *Proben* auch erhoben, wenn zum Zeitpunkt ihrer Gewinnung bereits klar ist, dass diese unabhängig von einer konkreten Behandlung oder in Ergänzung ihrer Verwendung im *Behandlungszusammenhang* in eine Datenbank für die Forschung integriert werden sollen. In diesem Fall ist der *Patient* oder *Proband*, soweit dies zum Zeitpunkt der Daten- oder Probengewinnung schon möglich ist, ausführlich über die geplante Verwendung aufzuklären, und seine schriftliche *Einwilligung* ist einzuholen.

Fortgeschrittene Signatur: Die fortgeschrittene Signatur entspricht in weiten Teilen der gesetzeskonformen Signatur nach dem deutschen Signaturgesetz. Sie soll in rechtlicher Hinsicht künftig der handschriftlichen Unterschrift gleichgestellt werden und vor Gericht als Beweis gelten. Fortgeschrittene Elektronische Signaturen sind Signaturen, die ausschließlich dem sogenannten Signaturschlüssel-Inhaber zugeordnet sind, die Identifizierung des Signaturschlüssel-Inhabers ermöglichen, mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Framework: Als Framework (engl. „Rahmenstruktur“) bezeichnet man einen Ordnungsrahmen. In dieser Arbeit wird der Framework-Begriff synonym zu den Begriffen *Sicherheitsframework* sowie Sicherheits- und Risikomanagementframework (S&R-Framework) bzw. Informationssicherheitsframework verwendet. In der vorliegenden Arbeit wird die Bezeichnung Framework als Oberbegriff für *Normen*, *Standards*, Verfahrensbibliotheken und *Frameworks* verwendet (s. a. *Risikomanagement-Standard*).

Freie Software: Freie Software ist Software, deren Lizenz es ausdrücklich erlaubt, sie für jeden Zweck zu nutzen, sie beliebig zu kopieren, studieren, zu verändern und weiter zu verteilen. Der Quelltext ist frei zugänglich, und muss auch frei zugänglich bleiben. Lizenzen, die diese Freiheiten nicht gewähren, werden im Gegenzug als proprietär oder unfrei bezeichnet.

Genom: Als Genom oder auch Erbgut wird eine Gesamtheit der vererbbaren Nukleinsäure einer mehr oder weniger autonomen Struktur bezeichnet. Diese autonome Struktur kann ein Virus, eine Zelle, ein Organell oder ein Organismus sein. Zumeist handelt es sich bei der vererbbaren Nukleinsäure um DNA. Das Genom enthält Informationen, die zur Entwicklung (Ontogenese) der Bau- und Leistungsmerkmale eines Lebewesens oder eines Virus notwendig sind. Diese Informationen sind in der Basensequenz der DNA verschlüsselt. Daneben enthält es Basensequenzen, die strukturelle Bedeutung für die Organisation der DNA haben oder deren Bedeutung noch nicht bekannt ist.

Good Clinical Practice: Good Clinical Practice (Gute Klinische Praxis, GCP) bezeichnet nach ethischen und praktischen Gesichtspunkten aufgestellte, vom aktuellen Stand der wissenschaftlichen Erkenntnis abhängige Regeln für die Durchführung von medizinischen Behandlungen oder klinischen Tests.

Gremium: Der Begriff Gremium bezeichnet die Zusammenarbeit von Personen in einer Gruppe (Ausschuss, Kollegium), die sich zum Zweck der Beratung über einen speziellen Themenkomplex bzw. der Beschlussfassung über diesen Themenbereich über einen längeren Zeitraum hinweg bildet (s. a. *Ausschuss Datenschutz*).

Hacker: Im Fachjargon Person, die Freude daran hat bzw. es als kreative oder intellektuelle Herausforderung betrachtet, sich in komplizierte Programmsysteme einzuarbeiten. Anders als der normale Benutzer, der es vorzieht, nur das funktionale Minimum eines Programms zu erlernen, versucht ein Hacker, die Möglichkeiten des Programms auszureizen oder gar zu erweitern.

Hashfunktion: Eine Hashfunktion bildet eine Menge von Eingabewerten auf eine kleinere Menge von Ausgabewerten mit geringerem Informationsgehalt ab.

Hashwert: Der Hashwert eines Wertes ist das Ergebnis der Anwendung einer *Hashfunktion* auf diesen Wert.

HIPAA: Health Insurance Portability and Accountability Act ist ein in den USA verabschiedetes Gesetz, das einen Abschnitt enthält, in dem die standardisierten Mechanismen für elektronischen Datenaustausch, Sicherheit und Vertraulichkeit aller zum Gesundheitswesen gehörigen Informationen festgelegt werden.

HMAC: Abkürzung für Hash-based Message Authentication Code, auch Hashed Message Authentication Code geschrieben. In mehreren RFCs spezifizierter Mechanismus zur *Authentifikation* (*Authentifizierung*) von Nachrichten, der kryptografische *Hashfunktionen* verwendet.

Homonym: Ein Homonym ist ein Wort (in diesem Zusammenhang – *PID*), das für verschiedene Begriffe (hier – *IDATs*) stehen kann.

HPC: Der elektronische Heilberufsausweis (Health Professional Card) ist eine Schlüsseltechnologie für alle zurzeit im Gesundheitsbereich diskutierten Anwendungslösungen für die elektronische Kommunikation. Umfassende nationale Anwendungen wie die neue elektronische Gesundheitskarte, das elektronische Rezept, die elektronische *Patientenakte* aber auch die effiziente Unterstützung der Disease-Managementprogramme benötigen für den Zugriff auf medizinische Daten den elektronischen Heilberufsausweis. Darüber hinaus sind zahlreiche weitere sektorale Anwendungsfelder absehbar, wie etwa die Online-Fortbildung oder die elektronische Abrechnung.

ICAP: ICAP ist ein schlankes Protokoll, um einen Remote Procedure Call für HTTP auszuführen. ICAP-Clients können HTTP-Daten an einen ICAP-Server weitergeben, der seinerseits die Inhalte umformt oder bearbeitet (adaptiert). Ein ICAP-Client ist im Normalfall ein Proxy, der HTTP-Requests von einem Browser entgegennimmt. Die Daten werden zu einem ICAP-Server gesendet, um dort bearbeitet zu werden. Diese Bearbeitung kann ein URL-Check, Virenscan etc. sein.

IDAT: siehe *Identifkationsdaten*.

Identifikationsdaten: Personendaten oder identifizierende *Stammdaten* (*IDAT*). Personenidentifizierende Daten umfassen Name, Geburtsort, Geburtsdatum usw. des *Patienten* oder *Probanden*. Sie werden vom Arzt oder der Klinik bzw. dem Studienzentrum erhoben und je nach Organisation des *Forschungsverbundes* bei der erhebenden Stelle oder in einer zentralen *Patientenliste* gespeichert. Es ist auch möglich, dass die *IDAT* bei beiden Stellen gespeichert werden.

Identity- and Access-Management: Die Hauptaufgabe des Identity- and Access-Managements (IAM) besteht in der Reduktion der Vielzahl der Kennungen und personenbezogenen Informationen, die die Benutzer für den Zugriff auf Ressourcen (Anwendungen) benötigen. Im Rahmen der IAM versucht man, eine Vielzahl der Kennungen in einer einzigen digitalen Identität des Anwenders zusammenzufassen.

IDS: siehe *Intrusion Detection System*.

IKE: Internet Key Exchange ist ein IPSec-(Internet Protocol Security-) Standardprotokoll, das zur Absicherung des Aufbaus von Virtual Private Networks (*VPN*) sowie des Remote-Zugriffs auf Computer oder Netzwerke verwendet wird. Im IETF Request for Comments (RFC) 2409 spezifiziert, definiert IKE eine automatische Verhandlungs- und Authentifizierungsmethode für IPSec-Sicherheitsbeziehungen (Security Associations).

Infektionsepidemiologie: Infektionsepidemiologie ist eine medizinische Fachdisziplin, die sich mit der *Epidemiologie* von übertragbaren Erkrankungen (Infektionskrankheiten und parasitäre Erkrankungen), also ihrem räumlichen und zeitlichen Auftreten, beschäftigt. Die Infektionsepidemiologie untersucht Übertragungswege und Erregerreservoirs für die Ausbreitung dieser Erkrankungen und beschreibt diese in mathematischen Modellen. Aus ihnen werden Prognosen zur Ausbreitung und Handlungsanweisungen zur Vermeidung abgeleitet (s. a. *Epidemiologie*).

Informationssicherheit: Oberbegriff aller Aspekte zum Schutz von Informationen vor Verlust, unbefugter Veränderung und unbefugter Kenntnisnahme. Die Informationssicherheit umfasst sowohl elektronisch gespeicherte und verarbeitete Information als auch mündliche oder schriftliche Information.

Informationssicherheits-Framework: siehe *Framework*.

Informationssicherheitsmaßnahme: siehe *Sicherheitsmaßnahme*.

Ingres®: Ingres® ist ein relationales *DBMS*, welches unter einer Open-Source-Lizenz (CA Trusted Open Source License – CATOSL) verfügbar ist. Ingres® zeichnet sich durch einfache Anpassbarkeit und Skalierbarkeit aus und ist für kritische Anwendungsbereiche geeignet.

IP-Adresse: Abkürzung für Internet-Protocol-Adresse, auch als Internetadresse bezeichnet. Im Adressierungsschema des Internet Protocol der Version 4 (IPv4) gib es 32-Bit-Folgen, die gewöhnlich in vier durch Punkte getrennte Bytes (Oktetts) in Dezimalnotation (Dotted-decimal Notation) geschrieben werden.

IPSec: Abkürzung für Internet Protocol Security. In der Internet Engineering Task Force (IETF) ist IPSec eine Arbeitsgruppe, die sich mit Erweiterungen des Internet Protocol (IP) befasst, mit denen die Integrität, Authentizität und Vertraulichkeit der IP-Kommunikation gesichert werden.

ISAKMP/Oakley: Internet Security Association and Key Management Protocol. Es handelt sich um einen Verschlüsselungsalgorithmus zum Schlüsselmanagement zwischen zwei Gateways, die IPSec benutzen. ISAKMP und Oakley sind grundlegende Bestandteile von *IKE* .

ISO/OSI-Modell: Auch als OSI-Referenzmodell (Open Systems Interconnection), OSI-Architektur- und -ebenenmodell bezeichnet. Ein von der ISO (International Organization for Standardization) entwickelter globaler Rahmen für die Standardisierung offener Kommunikation zwischen kooperierenden Systemen. Der Rahmen zerlegt, losgelöst von speziellen Implementierungen, den Funktionskomplex Kommunikation in sieben schichtdiskrete hierarchische Teilprozesse, die in die sieben OSI-Schichten eingebettet sind. Die in den Schichten residierenden Instanzen der kooperierenden Systeme erbringen Kommunikationsdienste für die jeweils nächsthöhere Schicht. Dabei stützen sie sich auf die Dienste der darunterliegenden Schichten. Die Bedingungen für die schichtbezogene Kooperation unter den verbundenen Systemen reglementiert das Schichtenprotokoll.

ISO: Abgeleitet vom ursprünglichen Namen „International Standard Organization“, heute benutzte Kurzbezeichnung für International Organization for Standardization (franz. Organisation Internationale de Normalisation (OIN)). Ziel der Organisation ist es, mithilfe weltweiter Standards den internationalen Austausch von Gütern und Dienstleistungen sowie die Entwicklung der Zusammenarbeit auf geistigem, wissenschaftlichem, technischem und wirtschaftlichem Gebiet zu fördern. Die Arbeitsergebnisse der ISO werden als Internationale *Standards* (IS) veröffentlicht.

IT-Grundschutz: Vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegebene Sammlung von Mindestanforderungen und entsprechenden Anleitungen zur Absicherung von Computern und Netzen. IT-Grundschutz bietet eine einfache Methode, dem Stand der Technik entsprechende IT-Sicherheitsmaßnahmen zu identifizieren und umzusetzen. Das BSI stellt zahlreiche Werkzeuge zur Verfügung, um ein angemessenes Sicherheitsniveau zu erreichen, wie z. B. die BSI-Standards zum IT-Sicherheitsmanagement, die IT-Grundschutz-Kataloge und das GSTOOL. Dazu gehört aber auch die ISO 27001-Zertifizierung auf Basis von IT-Grundschutz, die sowohl eine Prüfung des IT-Sicherheitsmanagements als auch der konkreten IT-Sicherheitsmaßnahmen auf Basis von IT-Grundschutz umfasst. Die IT-Grundschutz-Kataloge beinhalten die Baustein-, Maßnahmen- und Gefährdungskataloge (s. a. Abschnitt A.1.5 „BSI IT-Grundschutz“).

ITSEC: Abk. für Information Technology Security Evaluation Criteria. Festgelegte Evaluationskriterien für die Zertifizierung informationstechnischer Systeme, ursprünglich abgestimmt zwischen Deutschland, Frankreich, Großbritannien und den Niederlanden. Mittlerweile gelten die ITSEC innerhalb aller Länder der Europäischen Union. Die Kriterien bewerten die Funktionalität (functionality) nach Vertrauenswürdigkeit (assurance) der Wirksamkeit und Vertrauenswürdigkeit der Korrektheit.

ITSK: Abkürzung für IT-Sicherheitskriterien, engl. IT Security Criteria. Die „Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (IT)“ –

auch als „Grünbuch“ bezeichnet – wurden 1989 von der damaligen Zentralstelle für Sicherheit in der Informationstechnik (ZSI), der Vorgängerorganisation des heutigen „Computer Emergency Response Team für Bundesbehörden (CERT-Bund)“ des Bundesamtes für Sicherheit in der Informationstechnik (BSI), veröffentlicht. Die ersten fünf der beschriebenen zehn Funktionalitätsklassen entsprechen denen des „Orange Book“. Als ein Maß für die Vertrauenswürdigkeit in die beschriebene Funktionalität wurden acht hierarchische Qualitätsstufen eingeführt. Dieses mit den ITS erstmals eingeführte Konzept der Trennung von Funktionalität und Qualität findet sich sowohl in den *ITSEC* als auch den Common Criteria (*CC*) wieder.

J2EE: Abkürzung für Java 2 (Platform) Enterprise Edition, heute als „Java Platform Enterprise Edition (Java EE)“ bezeichnete Java-Spezifikation. In J2EE werden Softwarekomponenten und Dienste definiert, die primär in der Programmiersprache Java erstellt werden.

JavaScript: Ursprünglich mit LiveScript bezeichnete, von Brendan Eich bei Netscape entwickelte und im Dezember 1995 vorgestellte Java-basierte, objektorientierte Skriptsprache für den Einsatz in der Internetkommunikation, genauer gesagt zur Ausführung bestimmter Aktionen innerhalb des Webbrowsers.

JSON: *JavaScript* Object Notation (JSON) ist ein unabhängiges Datenaustauschformat. Der am meisten betonte Unterschied von JSON zu *XML* ist die etwas kompaktere Codierung von Datenstrukturen, wodurch im Vergleich zu *XML* weniger Overhead produziert wird. *XML* ist eine Auszeichnungssprache (Markup Language) und somit vielseitiger einsetzbar als JSON, welches keine Auszeichnungssprache, sondern ein Datenaustauschformat ist.

k-Anonymität: Eine Datensammlung ist k-anonym, wenn die Kombination der auch in anderen Datensammlungen vorhandenen Attribute in k verschiedenen Datensätzen innerhalb der Datensammlung vorkommt, anders ausgedrückt, wenn es mindestens k Datensätze gibt, auf die das externe Wissen passt. Als andere Datensammlungen sind die zu berücksichtigen, die einem potenziellen Angreifer zum Abgleich zur Verfügung stehen könnten. Hierbei sind insbesondere öffentlich verfügbare oder soziodemographische Datenzusammenstellungen zu berücksichtigen. Das Grundprinzip kann auch auf pseudonymisierte Datensammlungen übertragen werden.

Kennzahl: siehe *Metrik*.

Kerberos: Ein am Massachusetts Institute of Technology (MIT) entwickeltes System zur gesicherten *Authentifikation* von Benutzern (Clients) in Datennetzen mit einem symmetrischem Schlüsselmanagement. Dabei erhält der Client auf Anforderung von einem Kerberos-Server ein so genanntes „Kerberos-Ticket“ mit (verschlüsselter)

Authentifikationsinformation, das dem Client erlaubt, bestimmte Dienste auf einem anderen Rechner in Anspruch zu nehmen.

Kerckhoffs-Prinzip: Auch als Prinzip von Kerckhoffs, engl. Kerckhoffs Principle oder Kerckhoffs Assumption, bezeichnet. Vom niederländisch-französischen Kryptographen Auguste Kerckhoffs von Nieuwenhof (1835–1903) formulierte Voraussetzung für ein wirksames Kryptosystem: „Die Sicherheit eines Kryptosystems darf nicht von der Geheimhaltung des Algorithmus abhängen. Die Sicherheit gründet sich ausschließlich auf die Geheimhaltung des Schlüssels."

Keylogger: Dt. Tastaturrecorder. Oberbegriff für Software und/oder Hardware, die die Tastaturanschläge eines Computernutzers aufzeichnet, um sie zu einem späteren Zeitpunkt analysieren oder wiedergeben zu können.

Klinische Studie: Eine klinische Studie dient zur Prüfung des Einflusses einer medizinischen Behandlung auf eine Krankheit unter kontrollierten Randbedingungen; Gegenstand einer klinischen Studie kann auch die Prüfung einer präventiven oder diagnostischen Maßnahme sein.

Kompetenznetze in der Medizin: Kompetenznetze in der Medizin sind ab 1999 vom Bundesministerium für Bildung und Forschung (BMBF) initiierte überregionale, krankheitsspezifische Forschungsnetzwerke, deren Ziel die Verbesserung der Zusammenarbeit in der horizontalen (Verknüpfung der Forschergruppen von der Grundlagenforschung bis zur Versorgungsforschung) und der vertikalen (Transfer von Wissen zwischen Forschung und Versorgung) Ebene ist. Im Rahmen des Gesundheitsforschungsprogramms hat das BMBF zu vier Zeitpunkten insgesamt 21 krankheitsspezifische Kompetenznetze in die Förderung aufgenommen (s. a. *TMF*).

Kompromittierung: Ein System wird als kompromittiert betrachtet, wenn Daten manipuliert sein könnten, und wenn der Administrator des Systems keine Kontrolle über die korrekte Funktionsweise mehr hat bzw. ein Angreifer sein Ziel erreicht hat. Dies muss nicht zwangsläufig die Manipulation von Daten implizieren. Wenn es einem Angreifer z. B. gelingt den Schlüssel eines Kryptosystems zu bekommen, ist dieses System ebenfalls kompromittiert, also unterwandert, ohne dass der Angreifer Daten geändert hat. Ein beobachtender Angreifer kann somit ein System ebenfalls kompromittieren. Typischerweise tritt dies nach einem *Malware*-Befall oder durch einen gezielten Einbruch durch *Cracker* auf. Ein derartig manipuliertes System ist als nicht mehr vertrauenswürdig anzusehen.

Konsil: Als Konsil bezeichnet man in der Medizin die patientenbezogene Beratung eines Arztes durch einen ärztlichen Kollegen, meist einen Facharzt. Der Begriff findet häufig im Krankenhaus Anwendung, wenn ein Arzt einer anderen Fachrichtung

hinzugezogen wird. Der beauftragte Arzt (Konsiliarius) legt seine Empfehlungen zur Diagnostik oder Therapie meist schriftlich nieder.

Konzept: Klar umrissener Plan, Programm für ein Vorhaben (s. a. *Modell*, *Sicherheitskonzept*).

Koordinierungszentrum für Klinische Studien: Ein Koordinierungszentrum für Klinische Studien (KKS) ist eine vom Bundesministerium für Bildung und Forschung (BMBF) geförderte Einrichtung, die an den Universitäten; die personelle und logistische Ressourcen vor Ort zur Verfügung stellt, um *klinische Studien* nach international anerkannten Qualitätsstandards zu planen, durchzuführen und auszuwerten. Dabei werden auch *Studien* im Auftrag Dritter, etwa industrieller Partner, betreut. Die einzelnen Koordinierungszentren sind im KKS-Netzwerk zusammengeschlossen und Mitglieder in der TMF – *Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V.* (s. a. *TMF*).

LabID: siehe *Probennummer*.

LaGrande: siehe *Trusted Execution Technology*.

MAC-Adresse: Die MAC-Adresse (Media Access Control, auch LAN-Adresse genannt) ist die Hardwareadresse vieler Netzwerkgeräte (vor allem Netzwerkkarten), die zur eindeutigen Identifikation des Geräts im Netzwerk dient.

Malware: Von „Malicious“ (engl. böswillig) und „Software“ abgeleitetes Kunstwort für alle Arten von Programmen, die in eher unfreundlicher oder sogar in bösartiger Absicht geschrieben wurden.

Man-in-the-Middle-Angriff: Im Bereich der IT-Sicherheit ein „Angriff (Attacke) durch die Person in der Mitte“, bei dem der Angreifer „in der Leitung“ beiden Kommunikationspartnern den jeweils anderen Partner vorspielt.

MDAT: Forschungsdaten oder medizinische Daten. *MDAT* ist die übergreifende Bezeichnung für Daten, die zum Zwecke der Forschung in der zentralen Datenbank eines *Forschungsverbundes* gespeichert werden. *MDAT* umfassen in der Regel klinische Sachverhalte wie Befunde und Diagnosen sowie soziodemographische Daten, die eine entsprechende Klassifikation des *Patienten* oder *Probanden* zu wissenschaftlichen Zwecken erlauben. Zu den soziodemographischen Daten gehören neben Alter, Geschlecht und Bildung auch Lifestylefaktoren wie etwa Ernährungsgewohnheiten sowie Umweltdaten, die eine relevante Exposition des *Patienten* gegenüber Klima, Luftverschmutzung oder Lärm näher charakterisieren. Mit dem medizinischen Datensatz werden auch die sonstigen Begleitdaten gespeichert, die u. a. das Vorliegen der *Einwilligungserklärung*, den Ort der *Archivierung*, den Umfang der Einwilligung, die Identität behandelnder Ärzte und die Daten erhebende Stelle umfassen

(vgl. [SPR+06]). $MDAT^*$: $MDAT$ verschlüsselt, $MDAT^S$: selektierte Teilmenge der medizinischen Daten $MDAT^W$, die einem Wissenschaftler zur Verfügung gestellt wird, $MDAT^W$: wissenschaftlich relevanter Teil der Behandlungsdaten.

Medizinische Kompetenznetze: siehe *Kompetenznetze in der Medizin*.

Medizinischer Forschungsverbund: siehe *Medizinisches Forschungsnetz*.

Medizinisches Forschungsnetz: Ein medizinisches Forschungsnetz ist eine vernetzte Organisation mit dem Zweck, Daten oder Proben für die medizinische Forschung zu sammeln, langfristig aufzubewahren und für verschiedene, oft noch nicht feststehende wissenschaftliche Fragestellungen (s. a. *Forschungsvorhaben*, *Studien*) auszuwerten. Medizinisches Forschungsnetz umfasst *medizinische Kompetenznetze*, *Koordinierungszentren für klinische Studien*, *Biomaterialbanken* und andere, meist krankheitsspezifische Forschungsnetze und *Register*. In vielen Fällen gibt es eine enge Verzahnung mit der medizinischen Versorgung, d. h., *Behandlungszusammenhang* und *Forschungszusammenhang* gehen ineinander über. In manchen Situationen, z. B. bei *seltenen Erkrankungen*, ist sinnvolle klinische Forschung erst durch die Vernetzung möglich. Ein Forschungsnetz kann eine lose Kooperation von *Forschern* verschiedener Kliniken aber auch eine öffentlich rechtliche oder privatrechtliche Organisation sein (s. a. *Trägereinrichtung*).

Medizinprodukte-Gesetz (MPG): Das Medizinprodukte-Gesetz enthält die technischen, medizinischen und Informations-Anforderungen sowie Betreiber- und Anwendervorschriften für Medizinprodukte.

Medizinprodukte-Studie (MPG-Studie): Eine solche *Studie* dient der Bewertung eines Medizinprodukts (z. B. Messgeräts) und verfolgt das Ziel, die Konformität des Produkts mit den Anforderungen des *Medizinprodukte-Gesetzes* festzustellen; das Erreichen des Ziels wird durch ein CE-Kennzeichen bestätigt.

Metrik: siehe *Sicherheitsmetrik*.

Modell: Form, Beschaffenheit, Maßverhältnisse veranschaulichende Ausführung eines (vorhandenen oder) noch zu schaffenden Gegenstandes in bestimmtem (besonders verkleinerndem) Maßstab (s. a. *Konzept*).

MPG: siehe *Medizinprodukte-Gesetz*.

MPLS: Abkürzung für Multiprotocol Label Switching. Von der Arbeitsgruppe MPLS der Internet Engineering Task Force (IETF) betriebenes Standardisierungsprojekt zur Integration von IP- (Internet Protocol) und ATM-Systemen (Asynchronous Transfer Mode) durch die Verbindung von Layer-2-Funktionalität (ATM-Switching) mit Layer-3-Funktionalität (IP-Routing).

MySQL: MySQL ist eine freie Datenbankmanagementsoftware, die seit einiger Zeit unter der GNU General Public License (GPL) steht. MySQL gehört zu den am weitesten verbreiteten Open-Source-Programmen und bringt eine große Anzahl von bequemen Administrationswerkzeugen mit sich.

Nationales Genomforschungsnetz: Das Nationale Genomforschungsnetz (NGFN) wird seit 2001 vom Bundesministerium für Bildung und Forschung (BMBF) gefördert, um die Funktion der menschlichen Gene aufzuklären. Ungefähr 600 Wissenschaftler unterschiedlichster Fachrichtungen versuchen durch Vernetzung dieser Fachgebiete die genetischen Ursachen von „Volkskrankheiten“ wie Krebs, Herzschwäche und Alkoholismus zu erforschen (s. a. *TMF*).

Netzwerke für seltene Erkrankungen: *Seltene Erkrankungen* sind nicht wirklich selten. Nach der in Europa gültigen Definition ist eine Erkrankung „selten“, wenn weniger als einer von 2.000 Menschen unter einem spezifischen Krankheitsbild leidet. Diese meist genetisch bedingten Erkrankungen sind oft schwer therapierbar. Außerdem gibt es zu wenig Informationen und kaum systematische Studienmöglichkeiten, die eine zielgerichtete Therapie erlauben. Daher fördert das BMBF den Aufbau von krankheitsspezifischen Netzwerken zu seltenen Erkrankungen (s. a. *TMF*).

Newsgroup: Im Internet eingerichtete, moderierte oder nicht moderierte elektronische Plattform für den zeitentkoppelten Nachrichtenaustausch (Asynchronous Communication) zwischen einer offenen oder beschränkten Gruppe von Internetbenutzern (Diskussionsteilnehmern), technisch realisiert beispielsweise als Teil einer Website.

NIST: Abkürzung für „National Institute of Standards and Technology“. Das NIST wurde 1901 als National Bureau of Standards (NBS) durch den amerikanischen Kongress zur Unterstützung von Industrie, Handel, wissenschaftlichen Institutionen und Regierungsstellen gegründet. Die Hauptforschungsgebiete in den NIST-Laboratorien betreffen die Bereiche Gebäude- und Feuerschutz, Chemiewissenschaft und -technologie, Elektrotechnik und Elektronik, Informationstechnologie, Verfahrenstechnik, Materialkunde und Physik.

Norm: Eine Norm ist eine allseits rechtlich anerkannte und durch ein Normungsverfahren beschlossene, allgemeingültige sowie veröffentlichte Regel zur Lösung eines Sachverhaltes. Alle Instanzen eines Normungsverfahrens wurden durchlaufen, anschließend wurde sie beschlossen und veröffentlicht. Voraussetzung für eine Norm ist, dass sie technisch ausgereift ist und einen Nutzen für den Anwender hat (s. a. *Standard*).

Nutzer: siehe *Forscher*.

OpenBSD: OpenBSD ist ein BSD-basiertes UNIX-ähnliches Betriebssystem, welches unter der BSD-Lizenz entwickelt wird. OpenBSD ist bekannt für das Beharren

seiner Entwickler auf Quelloffenheit, freie Dokumentation, kompromisslose Stellung gegenüber Softwarelizenzen, guten kommerziellen Support und v. a. Fokus auf Computersicherheit. Das fundamentalste Konzept von OpenBSD ist das Streben nach einem einfachen, sauberen und sicheren Betriebssystem. Aufgrund der Sicherheitsverbesserungen wird OpenBSD in den Bereichen eingesetzt, die gegen *Cracker* und *DoS*-Angriffe geschützt sein müssen. Als Nachteile von OpenBSD werden häufig Performance und Skalierung genannt, die hinter den Werten üblicher Betriebssysteme liegen. Außerdem verlangt die Administration eines OpenBSD-Systems dem Administrator besondere Kenntnisse ab.

OrgDAT: Organisationsdaten. OrgDAT sind Begleitdaten eines Datensatzes oder einer Probe, die an unterschiedlichen Stellen erhoben werden können. So erfasst etwa die Proben gewinnende Stelle die Probenart und gegebenenfalls die Informationen zu Probenentnahme und Präanalytik. In der Probenbank werden die Begleitdaten einer Probe mit weiteren Informationen wie etwa den Umständen von Konservierung, Lagerung und Qualität gespeichert.

Patient: Patient und *Proband* sind die Personen, die dem *Forschungsverbund* Daten zu ihrer Gesundheit und Materialien ihres Körpers zu Zwecken der biomedizinischen Forschung zur Verfügung stellen. Erfolgt die Datengewinnung oder Probenentnahme im *Behandlungszusammenhang*, ist der Spender Patient. Erfolgt die Datengewinnung oder Probenentnahme im *Forschungszusammenhang*, ist der Spender *Proband*. Vom Patienten bzw. *Probanden* ist die *Einwilligungserklärung* einzuholen, die über die Weiterverwendung der Daten und *Proben* zu Forschungszwecken entscheidet. Mit ihm ist auch der Vertrag abzuschließen, in dem die Eigentums- und Nutzungsrechte an der Probe festgelegt werden.

Patientenakte: Unter einer Patientenakte wird die Gesamtheit der über diesen *Patienten* gespeicherten Informationen verstanden, die in Form einer abgeschlossenen Dokumentation, z. B. von einem Arzt, verantwortet sind. Diese können in einer einheitlichen zentralen Datenbank oder in einem verteilten Krankenhausinformationssystem gespeichert sein.

Patientendaten: Patientendaten sind im Sinne des Gesetzes alle Daten über einen *Patienten*, die im Rahmen der Behandlung im Krankenhaus erhoben werden sowie die Personendaten von Angehörigen, Bezugspersonen und sonstigen Dritten, die im Zusammenhang mit der Behandlung bekannt werden (Ehepartner, Arbeitgeber etc.).

Patientenidentifikator: Der Patientenidentifikator (*PID*) ist der eindeutige Ordnungsparameter für einen in einen *Forschungsverbund* eingeschlossenen *Patienten* oder *Probanden*. Die Erzeugung des *PID* wird durch die anmeldende Stelle veranlasst.

Der *PID* wird gemeinsam mit den *IDAT* in der Patientenliste gespeichert. In der Regel soll der *PID* nicht sprechend sein; er kann dann als *Pseudonym* erster Stufe dienen.

Patienteninformation: Die Patienteninformation bildet die informationelle Grundlage für die nachfolgende *Einwilligungserklärung* des *Patienten* oder *Probanden* im Hinblick auf den Umgang der entnehmenden Stelle sowie des *Forschungsverbundes* mit den gewonnenen Daten und *Proben* (informed consent). Die Patienteninformation enthält eine Fülle von Einzelangaben (Items), die dem Einwilligenden die Tragweite seiner nachfolgenden *Einwilligungserklärung* vor Augen führen soll. Für die Datenerhebung im Rahmen *klinischer Studien* wurden Modelle solcher Patienteneinwilligungen entwickelt, die von der *TMF* auf die Besonderheiten bei *medizinischen Forschungsverbünden* angepasst wurden (vgl. [HIB+06]).

Personenbezogenheit: Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Bei Daten bzw. Biomaterialien beziehen sich die Einzelangaben auf den Datensatz oder die Probe (Name des *Probanden*, Angaben zu dessen Gesundheitszustand usw.) oder ergeben sich aus der Probe bzw. deren Analyse, bei der etwa die genetische Ausstattung des *Probanden* ermittelt werden kann. Zur allgemeinen Legaldefinition der Personenbezogenheit vgl. § 3 Abs. 1 BDSG. Man unterscheidet bei der Ausgestaltung des Personenbezugs eine grundsätzliche *Personenbeziehbarkeit* von der tatsächlichen Personenbezogenheit. *Personenbeziehbarkeit* setzt voraus, dass Angaben theoretisch einer Person zugeordnet werden können. *Personenbezogenheit* liegt dann vor, wenn diese Zuordnung auch tatsächlich, ohne Aufwand vorgenommen werden kann, z. B. wenn die Person direkt und offen lesbar benannt wird. Das Gegenstück zur Personenbezogenheit ist die Anonymität. Nach der geltenden Auffassung ist die Personenbezogenheit kein statisches Kriterium. Vielmehr ist diese von der Person des Datenverwenders abhängig und kann mit der Zeit variieren (vgl. [RHJ08, S. 28]). Eine Reduzierung der Personenbezogenheit erfolgt durch die *Pseudonymisierung*. Die befugte Wiederherstellung des Personenbezugs eines pseudonymisierten Datensatzes oder einer pseudonymisierten Probe erfolgt auf dem Wege der *Depseudonymisierung*. Die unbefugte Wiederherstellung der Personenbezogenheit einer anonymisierten oder pseudonymisierten Probe wird als *Reidentifizierung* (oder Re-Identifikation) bezeichnet. Um dies zu verhindern, ist das Reidentifizierungsrisiko abzuschätzen, oft für jeden Einzelfall.

Personenstammdaten: siehe *Identifikationsdaten*.

PGP: Abkürzung für Pretty Good Privacy. Ein von Philip (Phil) R. Zimmermann entwickeltes und frei verfügbares Verfahren (Applikationsprogramm), das insbesondere in der Mailkommunikation zur Verschlüsselung eingesetzt wird. Es handelt sich

um ein Public-Key-Verfahren, das mit zwei Schlüsseln arbeitet: einem privaten Schlüssel (Private Key) und einem öffentlichen Schlüssel (*Public Key*), die beide einmal gemeinsam generiert werden.

Pharming: Auch als DNS-Spoofing bezeichnet. Im Umfeld des Internets eine Attacke, bei der ein Angreifer die Internetadresse (IP-Adresse) eines bekannten Domainnamens durch seine eigene ersetzt. Voraussetzung ist der Zugang zu einem DNS-Server (DNS, Domain Name System) eines Providers. Alle Anfragen an diese Domain werden nun an die gefälschte IP-Adresse weitergeleitet. Hinter dieser IP-Adresse verbergen sich oft gefälschte Webseiten der Original-Domain, die den Nutzer dazu verleiten, seine Nutzerdaten und Passwörter einzugeben.

Phishing: Kurz für Phishing Mail. Kunstwort aus engl. Password (Passwort) und Fishing (Fischen, Angeln). Phishing, eine Form des *Social Engineering*, bezeichnet eine illegale Vorgehensweise, die darauf abzielt, an wichtige vertrauliche Daten anderer Internetnutzer zu gelangen.

PID: siehe *Patientenidentifikator*.

Portscan: Im Bereich der Internetsicherheit ein Angriff, bei dem der Angreifer durch systematisches Scannen aller adressierten Ports festzustellen versucht, welche Dienste und Prozesse auf dem Zielrechner zum Angriffszeitpunkt ablaufen.

PostgreSQL: PostgreSQL ist ein freies, objektrelationales Datenbankmanagementsystem (ORDBMS). Seine Entwicklung begann in den 1980er Jahren; seit 1997 wird die Software von einer Open-Source-Community weiterentwickelt. PostgreSQL ist weitgehend konform mit dem SQL-Standard ANSI-SQL 92, d. h. alle geforderten Funktionen sind verfügbar und verhalten sich wie definiert; anders als bei manchen kommerziellen sowie nicht kommerziellen Konkurrenzprodukten.

Proband: siehe *Patient*.

ProbDAT: siehe *Probenanalysedaten*.

Probe: Dem menschlichen Körper zu diagnostischen oder wissenschaftlichen Zwecken entnommene Substanz. Der Begriff Probe wird im Zusammenhang mit Biobanken synonym zum Begriff Material oder Biomaterial verwendet. Beispiele für Proben unterschiedlichster Art sind Gewebe, Körperflüssigkeiten, Zellen, RNA, DNA, Organe.

Probenanalysedaten: Die mit *ProbDAT* bezeichneten Ergebnisse der Probenanalyse werden je nach Bedarf an anfragende *Forscher* übermittelt. Die ihnen zugrunde liegenden Analysen können sowohl von den der Probenbank angeschlossenen Labors als auch von kooperierenden Einrichtungen durchgeführt werden. *ProbDAT* können potenziell rückbeziehbare Daten darstellen wie etwa im Fall von Genotypen. Ihre Speicherung sollte daher separat von anderen Daten erfolgen.

Probennummer: Die Probennummer (*LabID*) bezeichnet die ursprüngliche Nummer der *Probe*, die entweder von der probengewinnenden Stelle oder von der Probenbank vergeben wird. Bei der *LabID* kann es sich auch um einen Barcode handeln, der maschinenlesbar ist und maschinell weiterverarbeitet werden kann. Vergeben verschiedene probengewinnende Stellen eine *LabID*, so müssen Überschneidungen der Nummernkreise vermieden werden. Falls die Probenbank die *LabID* vergibt, erhält sie mit der *Probe* eine Fallnummer oder einen identifizierenden Datensatz zur entsprechenden Zuordnung des *Patienten*. Wird eine *Probe* aliquotiert, so können für die Teilproben zusätzliche *LabID* vergeben werden (*LabID2*, *LabID3* etc.), deren Zuordnung zur *LabID* der Mutterprobe allerdings in der Probenbank gespeichert werden sollte. Die *LabID* wird entweder durch die probengewinnende Stelle oder durch das verarbeitende bzw. analysierende Labor an die zentrale Datenbank gemeldet. In der zentralen Datenbank wird statt der *LabID* eine transformierte *LabIDtrans* gespeichert, um eine direkte Zuordnung von Datensatz und *Probe* zu vermeiden.

Promiscuous Modus: Der Promiscuous Modus bezeichnet einen bestimmten Empfangsmodus für netzwerktechnische Geräte. In diesem Modus liest das Gerät den gesamten ankommenden Datenverkehr an dem in diesen Modus geschalteten Netzwerkinterface.

Proteom: Die Gesamtheit aller Proteine in einem Lebewesen, einem Gewebe, einer Zelle oder einem Zellkompartiment wird als Proteom bezeichnet (z. B. Proteom des Menschen, der Kartoffelknolle, der Bakterienzelle, des Zellkerns etc.).

Protokoll: Allgemein ist das Protokoll das festgelegte Verfahren für den Austausch von Nachrichten in Kommunikationssystemen.

Pseudonym: Das Pseudonym (*PSN*) ist ein nichtsprechender Identifikator eines *Patienten* oder *Probanden* (Buchstaben oder Zahlen, die nicht auf die personenidentifizierenden Daten rückschließen lassen.).

Pseudonymisierung: §3 Abs. 6a BDSG: „Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.“ Dies kann beispielsweise durch die Ersetzung des Probandennamens durch eine Kennnummer geschehen. Man kann die Pseudonymisierung daher als eine eingeschränkte *Anonymisierung* auffassen. Ziel der Pseudonymisierung ist es aber nicht, den Personenbezug irreversibel abzutrennen, sondern lediglich durch ein eindeutiges Kennzeichen – ein *Pseudonym* – zu ersetzen, das für sich genommen die Identifikation der dahinter stehenden Person ausschließt oder aber wesentlich erschwert. Grundsätzlich bleiben pseudonymisierte Daten allerdings personenbeziehbar: Es existiert ein Geheimnisträger, der die Zuordnung von Person zu *Pseudonym* (Kennnummer) kennt oder

wiederherstellen kann und entsprechend vertrauenswürdig und geschützt sein muss. Der Nutzen, diese Abschwächung der Reduktion des Personenbezugs in Kauf zu nehmen, besteht in der Möglichkeit, die individuelle Veränderung personenbezogener Daten, z. B. einen Krankheitsverlauf, über die Zeit zu studieren, wofür eine mehrfache Zuordnung von Daten zur identischen Person zu verschiedenen Zeitpunkten erforderlich ist, ohne dass während dieses langen Beobachtungszeitraums die Identität der Person bekannt sein muss. Es existieren mehrere Pseudonymisierungsverfahren (einstufige und mehrstufige Pseudonymisierung, Einweg-Verfahren zur Pseudonymisierung, dezentrale und zentrale Pseudonymisierung u. a.). Die Pseudonymisierung wird bezüglich der Sicherheit gegen Wiederherstellung der *Personenbezogenheit* durch die *Anonymisierung* übertroffen.

PSN: siehe *Pseudonym*.

Public Key: Unter einem öffentlichen Schlüssel (engl. public key) versteht man in asymmetrischen Kryptosystemen Schlüssel, die jedem bekannt sein dürfen und z. B. zur Verschlüsselung eines Klartextes in einen Geheimtext genutzt werden können. Kennt ein Angreifer den öffentlichen Schlüssel, so kann er daraus dennoch weder auf den zugehörigen privaten Schlüssel oder die verschlüsselte Nachricht schließen. Die Geheimtexte können nur mit dem privaten Schlüssel wieder entschlüsselt werden. Bei digitalen Signaturverfahren ermöglicht der öffentliche Schlüssel die Prüfung digitaler Signaturen, erlaubt aber weder die Berechnung des zugehörigen privaten Schlüssels noch die Erstellung einer gültigen Signatur.

Qualitative Risikoanalyse: Die im Rahmen der *Risikoidentifikation* ermittelten Risiken werden qualifiziert; hierzu gehört die Priorisierung (basierend auf der Wahrscheinlichkeit des Schadenseintritts und dessen Auswirkungen). In dieser Arbeit erfolgt die qualitative Risikoanalyse mithilfe der schutzbedarfs- und bedrohungsorientierten Ansätze. Manche Definitionen der Risikoanalyse sehen zusätzlich die sog. semiquantitative Risikoanalyse vor. Bei der semiquantitativen Methode erhalten die qualitativen Risikomerkmale (z. B. Risiko „hoch“, „mittel“, „niedrig“) Zahlenwerte zugeordnet (z. B. 1, 2, 3) (vgl. [DHS08, S. 23,32], s. a. *Quantitative Risikoanalyse*).

Quantitative Risikoanalyse: Nach der *qualitativen Risikoanalyse* werden die Risiken mithilfe von *Sicherheitsmetriken* quantitativ bewertet im Hinblick auf die Risikowirkung und die Gegenmaßnahmen.

RAND: Das von *SSL* zur Schlüsselgenerierung verwendete Verfahren.

Rechteindustrie: Unter dem Begriff Rechteindustrie werden die gewinnorientierten Rechteverwertungsgesellschaften zusammengefasst, deren Gewinne z. T. auf der Verwertung der Rechte am geistigen Eigentum beruhen. Die bekanntesten Vertreter der Rechteindustrie sind Bertelsmann, Sony und Time-Warner.

Register: Ein Register ist eine systematische Sammlung von Informationen zu bestimmten Erkrankungen. Charakteristikum eines Registers ist die angestrebte Vollzähligkeit (typischerweise mindestens 95% aller einschlägigen Fälle). Ein Register kann sowohl im *Versorgungs-* als auch im *Forschungszusammenhang stehen*.

Reidentifizierung: Im Wege der Reidentifizierung wird der Personenbezug von anonymisierten oder pseudonymisierten Daten und *Proben* unbefugt wieder hergestellt. Eine Reidentifizierung kann einerseits durch Korrumpierung eines *Pseudonyms* oder eines Anonymisierungs- oder Pseudonymisierungsverfahrens erfolgen. Andererseits kann eine hinreichende Konstellation von in der Summe eindeutig einer Person zuzuweisenden Daten („Alleinstellungsmerkmalen“) im formal anonymisierten Datensatz vorliegen. Ist diese Datenkonstellation in Vergleichsdatenbanken oder in persönlichem Wissen mit offenem Personenbezug bekannt, so kann aus dem Inhalt der Daten – trotz formaler Abtrennung der personenidentifzierenden Daten – auf die Person rückgeschlossen werden, d. h. es kann eine Reidentifizierung durch Inferenzen auf der Basis datenimmanenter Identifizierungsrisiken erfolgen (s. a. *Depseudonymisierung*).

REST: Der Begriff Representational State Transfer (REST) bezeichnet einen Softwarearchitekturstil für verteilte Hypermedia-Informationssysteme. Derzeit findet unter dem Banner von REST eine Rückbesinnung auf grundlegende Webtechnologien statt, um die Implementierungen verteilter, webbasierter Systeme zu vereinfachen.

Reverse Engineering: Erforschung bestehender Systemkomponenten und deren Beziehungen untereinander, verbunden mit der Generierung von Darstellungen des untersuchten Systems auf unterschiedlichen Abstraktionsniveaus. Im Softwarebereich versteht man unter Reverse Engineering, dass der Sourcecode von kompilierten Programmen oder der Aufbau von Dateien durch bestimmte Verfahren ermittelt wird.

Risikobewertung: siehe *qualitative Risikoanalyse* und *quantitative Risikoanalyse*.

Risikoidentifikation: Während der Risikoidentifikation werden Risiken (potenzielle Behinderungen) mit verschiedenen Methoden identifiziert und dokumentiert (s. a. *qualitative Risikoanalyse*).

Risikomanagement-Standard: Ein Risikomanagement-Standard ist ein auf die formalen Abläufe und Strukturen zur Risikohandhabung in Organisationen gerichteter Standard. Es existieren mehrere nationale Standards von Normungsinstituten sowie *Frameworks* von Gremien und Standesorganisationen. Risikomanagement-Standards für das *Risikomanagement* in Organisationen stellen eine Art normierter Managementsysteme dar, die Organisationen als Hilfsmittel zur Gestaltung formalisierter Risikomanagementsysteme dienen (s. a. *Standard*).

Risikomanagement: Engl. Risk Management. Gemäß DIN EN 14971 ist Risikomanagement die systematische Anwendung von Managementgrundsätzen, Verfahren und Praktiken auf die Analyse (Risk Analysis), die Bewertung (Risk Assessment) und die Kontrolle (Risk Control) von Risiken. In der Informationstechnologie ist das Risikomanagement das methodische Vorgehen zur Erkennung, Bewertung, Handhabung und Reduzierung von Risiken (s. a. *Framework*).

Risikovektor: In dieser Arbeit wird der Risikovektorbegriff im Zusammenhang mit dem Konzept „dynSRM“ verwendet. Die Risikovektoren entstehen durch die Kombination des Konzeptes der Risikomatrix mit dem Konzept des Nettorisikos. Der Ursprung eines Risikovektors liegt auf der Ebene $E_{H;P}$ (potenzielle Schadenshöhe und Wahrscheinlichkeit des Schadenseintritts). Ein Risikovektor verläuft parallel zu der S-Achse (Schwachstellenpotenzial). Die Länge eines Risikovektors kann durch das Einleiten von Sicherheitsmaßnahmen reduziert werden (s. a. Abschnitt 4.4.1).

Robustheit: In der Informatik wird der Begriff Robustheit auch verwendet, um die Eigenschaft eines Verfahrens zu beschreiben, auch unter ungünstigen Bedingungen noch zuverlässig zu funktionieren. Oft ist damit gemeint, dass ein Algorithmus auch dann noch ein korrektes Ergebnis liefert, wenn der schlimmste Fall (Worst-Case) eintritt. Ein Verfahren erkennt beispielsweise Fehlersituation und geht damit um.

Rootkit: Im Bereich der Informationssicherheit ein Satz von Softwarewerkzeugen, der es einem Eindringling erlaubt, ein System unbemerkt und ungestört zu manipulieren. Der Hauptzweck eines Rootkits besteht darin, den Angreifer zu verbergen und den Rechner für entfernte Zugriffe zu öffnen bzw. offen zu halten. Das Kit kann eindringende *Malware* tarnen und bietet ihr Entfaltungsmöglichkeiten.

Routing: Engl. für Leitweglenkung, Leitwegbestimmung, Wegauswahl. In paketorientierten Kommunikationssystemen die Entscheidung von Vermittlungsknoten (z. B. X.25-Paketvermittlung) oder dedizierten Routern (z. B. IP-Router), welchen Weg (Route, Passage) eine Datei oder ein Dateifragment nehmen soll, um zum Empfänger zu gelangen.

RSA: Eine bekannte und gut untersuchte Variante der asymmetrischen Verschlüsselung (Public-Key-Verfahren). Die Abkürzung RSA steht für die drei Erfinder des 1978 veröffentlichten Verschlüsselungsalgorithmus (Ronald Rivest, Adi Shamir, Len Adleman). RSA kann zur Erzeugung einer digitalen Signatur, zur Verschlüsselung und zum Schlüsselaustausch eingesetzt werden. Das Verfahren basiert auf der mathematischen Schwierigkeit, große Zahlen zu faktorisieren.

Rucksackproblem: Das Rucksackproblem ist ein Optimierungsproblem der Kombinatorik. Aus einer Menge von Objekten, die jeweils ein Gewicht und einen Nutzenwert haben, soll eine Teilmenge ausgewählt werden, deren Gesamtgewicht eine vorgegebene

Gewichtsschranke nicht überschreitet. Unter dieser Bedingung soll der Nutzenwert der ausgewählten Objekte maximiert werden.

S&R-Framework: siehe *Framework*.

S&R-Management: siehe *Sicherheits- und Risikomanagement*.

SAML: Abkürzung für Security Assertion Markup Language, dt. etwa „Auszeichnungssprache für Sicherheitsbestätigungen". Ein von OASIS (Organization for the Advancement of Structured Information Standards) spezifiziertes *XML*-basiertes Framework zum Austausch von Sicherheitsinformationen zwischen Geschäftspartnern über das Internet (E-Commerce).

Schweigepflicht: Die ärztliche Schweigepflicht ist die ethische und rechtliche Pflicht des Arztes, Verschwiegenheit über alles zu wahren, was ihm bei der Ausübung seines Berufes über einen *Patienten* bekannt wird. Schon die Tatsache des Arztbesuchs fällt unter die Schweigepflicht. Die Schweigepflicht gilt für den Arzt, Zahnarzt, den Angehörigen eines anderen Heilberufs, der eine staatlich geregelte Ausbildung erfordert, für Angehörige medizinisch-technischer Assistenzberufe, medizinische Dokumentare und für medizinische Informatiker, sofern sie zum Behandlungsteam des verantwortlichen Arztes gehören, d. h. seiner direkten Weisungsbefugnis unterliegen. Die Rechtsgrundlage bilden §§ 203, 204 StGB; in diesen Vorschriften des Strafgesetzbuches wird die Verletzung der Schweigepflicht unter Strafe gestellt.

SCVP: Das Server-based Certificate Validation Protocol (SCVP) ist ein Internetprotokoll, das es Clients ermöglicht, den Aufbau einer X.509-Zertifikatskette und deren Validierung auszulagern. Dies wird vor allem bei Clients, die mit dem Kettenaufbau und der Validierung aufgrund fehlender Ressourcen oder Protokolle überlastet sind, benötigt. SCVP kann dem Client alle Aufgaben (Aufbau der Kette, Überprüfung auf Widerruf, Validierung) einer vollständigen Zertifikatsprüfung abnehmen.

Secret Sharing: Unter Secret Sharing (verteiltes Geheimnis) versteht man eine Technik, ein Geheimnis (meist eine Zahl) unter einer gewissen Anzahl von sogenannten Spielern aufzuteilen. Keine der Personen kann ohne die anderen das Geheimnis rekonstruieren. Je nach System ist nur eine Teilmenge der Spieler notwendig, um das Geheimnis zu bestimmen. Als Dealer wird derjenige Spieler bezeichnet, der die Aufteilung vornimmt.

Security Risk Management: siehe *Sicherheits- und Risikomanagement*.

Selbstbestimmungsrecht: Das informationelle Selbstbestimmungsrecht ist das Recht jedes Menschen, grundsätzlich selbst darüber zu bestimmen, wer was wann und bei welcher Gelegenheit über ihn erfährt. Es basiert nach der grundsätzlichen Entscheidung des Bundesverfassungsgerichts (sog. Volkszählungsurteil aus dem

Jahr 1983) auf den Grundrechten des Art. 2 Abs. 1 GG (freie Entfaltung der Persönlichkeit) sowie des Art. 1 Abs. 1 GG (Schutz der Menschenwürde). Freie Entfaltung der Persönlichkeit setzt nach dieser Entscheidung des Bundesverfassungsgerichts unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher im Grundrecht des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG eingeschlossen. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Ihren einfachgesetzlichen Niederschlag finden diese Grundaussagen des Bundesverfassungsgerichts in den Vorschriften der Datenschutzgesetze sowie in datenschutzrelevanten Vorschriften vieler anderer Gesetze.

Seltene Erkrankungen: siehe *Netzwerke für seltene Erkrankungen*.

Session-Hijacking: Session-Hijacking (auf deutsch etwa: Entführung einer Kommunikationsverbindung) ist ein Angriff auf eine verbindungsbehaftete Datenkommunikation zwischen zwei Computern. Während die Teilnehmer einer verbindungslosen Kommunikation Nachrichten ohne definierten Bezug miteinander austauschen, wird bei einer verbindungsbehafteten Kommunikation zunächst eine logische Verbindung (Sitzung, engl. Session) aufgebaut. Authentifiziert sich einer der Kommunikationspartner gegenüber dem anderen innerhalb der Sitzung, stellt diese eine Vertrauensstellung dar. Ziel des Angreifers ist es, durch die Entführung dieser Sitzung die Vertrauensstellung auszunutzen, um die gleichen Privilegien wie der rechtmäßig angemeldete Benutzer zu erlangen.

SGML: Abkürzung für Standard Generalized Markup Language. Internationaler Standard, der 1986 von der ISO zur Beschreibung der logischen Struktur und des Inhalts eines Dokuments in ISO 8879 definiert wurde.

Sicherheits- und Risikomanagement: Auch *Security Risk Management* (SRM) bzw. S&R-Management. Allgemein die Subsumierung von Verfahren zur Analyse und zur Bewertung von Sicherheitsrisiken sowie zur Definition und zur Implementierung geeigneter Schutz- und Kontrollmechanismen, die die Erreichung eines spezifizierten Sicherheitsniveaus gewährleisten.

Sicherheitsarchitektur: Unter einer Sicherheitsarchitektur wird die Gesamtheit der *Sicherheitskonzepte* und der daraus abgeleiteten *Informationssicherheitsmaßnahmen* verstanden.

Sicherheitsframework: siehe *Framework*.

Sicherheitskonzept: Die Gesamtheit der realisierten oder noch zu realisierenden dokumentierten Vorgaben der *Sicherheitsrichtlinien* einer Organisation.

Sicherheitsmaßnahme: Verfahrensweise oder Mechanismus, die/der dazu dient, Sicherheitsrisiken zu steuern, zu reduzieren und diesen entgegenzuwirken. Die (konkreten) Sicherheitsmaßnahmen werden aus (allgemeineren) *Sicherheitsrichtlinien* abgeleitet.

Sicherheitsmetrik: Ein System von Parametern, Kennzahlen/-größen und/oder Merkmalen, das der Bewertung der Informationssicherheit (inklusive Prozesse, Strategien, Produkte, Systeme etc.) dient. Oft gehören dazu auch Merkmale, die nicht quantitativ erfassbaren Größen entsprechen. In diesem Fall spricht man von qualitativen Sicherheitsmetriken.

Sicherheitsrichtlinie: Dokumentierte allgemeine *Sicherheitsmaßnahmen* im Sinne offizieller Vorgaben einer Organisation, die einen einzuhaltenden Rahmen vorgeben. Sicherheitsrichtlinien stellen Regelwerke für zentrale Dienste bereit, die das Sicherheitspotenzial der eingesetzten Informationssicherheitsinstrumente sowie den Zugriff und die Verwendung geschützter Daten festlegen und organisatorisch in definierten Verantwortlichkeiten verankern. Die Betreiber und die Nutzer werden über die notwendigen Maßnahmen und Abläufe informiert und zu einem planmäßigen, regelgerechten Handeln verpflichtet.

Single Sign-On: Universelles Konzept für die Anmeldeadministration mit zentralem Zugang der Benutzer zu den unterschiedlichsten Anwendungen. Single Sign-On (SSO) soll verhindern, dass sich ein Benutzer beim Zugriff auf viele verschiedene Rechnersysteme gegenüber jedem System mit einem individuellen Passwort authentifizieren muss.

SLA: Abkürzung für Service Level Agreement, dt. Dienstgütevereinbarung, teilweise auch als Dienstleistungsvereinbarung bezeichnet. In der Telekommunikation schriftliche Vereinbarung zwischen einem Kunden (Dienstnehmer) und einem Dienstanbieter über die gegen Entgelt bereitzustellenden Telekommunikationsdienste und deren Dienstgüte.

Snapshot: Ein zu einem bestimmten Zeitpunkt erstellter Abzug des Hauptspeichers oder Bildschirmspeichers, der auf einem Datenträger gespeichert werden kann.

Sniffer: Im Bereich der IT-Sicherheit Software zur Durchführung passiver Angriffe bzw. Ausspionierung („Schnüffeln“) von Informationen, beispielsweise im Internet durch das Mitlesen von IP-Paketen.

Social Engineering: Social Engineering (auch Social Hacking) ist das Erlangen vertraulicher Informationen durch Annäherung an Geheimnisträger mittels gesellschaftlicher Kontakte. Dieses Vorgehen wird von Geheimdiensten und Privatdetektiven seit Langem praktiziert, der Begriff wird jedoch meist im Zusammenhang mit Computerkriminalität verwendet, da er hier das Gegenstück zum rein technischen Vorgehen (Engineering) beim Eindringen in fremde Systeme bildet.

Spam: Im Internet-Jargon Bezeichnung für einen der Netiquette widersprechenden Umgang der Medien E-Mail (Mail Spam/Spamming) und USENET für Rundsendungen, offiziell als Unsolicited Commercial E-Mail (UCE), aber auch als Junk-Mail oder Mail-Bombing bezeichnet.

Sponsor: Auftraggeber und Hauptverantwortlicher einer *Studie*. Bei Arzneimittelstudien ist der Sponsor in der Regel ein Pharma-Unternehmen, bei wissenschaftsgetriebenen *Studien* in der Regel die Universität oder Forschungseinrichtung, der der Initiator der *Studie* angehört. §4 AMG: „Sponsor ist eine natürliche oder juristische Person, die die Verantwortung für die Veranlassung, Organisation und Finanzierung einer klinischen Prüfung bei Menschen übernimmt." Als Sponsoren von *klinischer Studien* treten die pharmazeutische Industrie, Universitätsinstitute oder -kliniken sowie staatliche, halbstaatliche und sonstige Forschungsinstitute und Einrichtungen des Gesundheitswesens auf.

Spoofing: Von engl. spoofing (Manipulation, Verschleierung); auch mit Masquerade oder Impersonation bezeichnet. In der Informationssicherheit aktiver, manipulierender Angriff (Attacke), der auf der Vorspiegelung einer falschen Identität, beispielsweise einer Person, beruht; üblicherweise während des Versuchs, (unautorisiert) Zugriff auf ein System zu erhalten.

SSH: Abkürzung für Secure Shell. Bezeichnung sowohl für ein kryptografisches Protokoll als auch für eine konkrete Implementierung dieses Protokolls. Ursprünglicher Protokollentwickler war Tatu Ylönen aus Finnland, der die Secure Shell an der Technischen Universität Helsinki entwickelte.

SSL: Abkürzung für Secure Socket Layer. Von Netscape entwickeltes Sicherheitsprotokoll, das die Datenkommunikation über das Internet, insbesondere zwischen Client (Browser) und Server, schützen soll.

Stammdaten: siehe *IDAT*.

Standard Operating Procedure: Dokument, welches das Vorgehen innerhalb eines Arbeitsprozesses beschreibt.

Standard: Ein Standard ist eine vergleichsweise einheitliche oder vereinheitlichte, weithin anerkannte und meist auch angewandte (oder zumindest angestrebte) Art und Weise, etwas herzustellen oder durchzuführen, die sich gegenüber anderen Arten und Weisen durchgesetzt hat. Im Bereich Technik und Naturwissenschaften findet der Begriff im Allgemeinen Verwendung als Oberbegriff für Vereinheitlichungen, die sich ungeplant infolge gesellschaftlicher Prozesse und Erfahrungen der Praxis ergeben, entwickelt und als eine Art stillschweigende Übereinkunft („Konvention") etabliert haben (s. a. *Norm*).

Stateful Inspection: Eine dynamische Paketfiltertechnik, die nicht nur das einzelne Datenpaket untersucht, sondern dieses auch einem logischen Kontext zuordnet. Eine Firewall mit Stateful Inspection merkt sich den Zustand einer Verbindung. Kann sie dann ein neu eintreffendes Paket einer erlaubten Verbindung zuordnen, kann das Paket passieren.

Steganografie: Besondere Form der Kryptografie. Mithilfe der Steganografie wird versucht, die Existenz einer Nachricht zu verschleiern. So lassen sich beispielsweise Textnachrichten (wie Urheberrechtshinweise) in Grafik-, Audio- oder Videodateien versteckt abspeichern und übertragen.

Studie: siehe *Forschungsvorhaben*.

Studiendatenbank: Datenbank, in der die Daten einer oder mehrerer, auch multizentrischer, *klinischer Studien* oder epidemiologischer Studien zentral gesammelt und verwaltet werden.

Switch: Im Bereich der Rechnernetze in LAN-Technologie Oberbegriff für Netzkoppelelemente mit der Funktionalität einer „Multiport-Brigde“, die auf der Sicherungsschicht, d. h. auf der Schicht 2 der OSI-Architektur (Layer-2-Switch), arbeiten.

Synonym: Unter dem Synonym versteht man ein gleichbedeutendes Wort. Für ein Signifikant (in diesem Zusammenhang – *IDAT*) gibt es also mehrere Signifikanten (hier *PIDs*).

Taxonomie: Eine Taxonomie ist ein einheitliches Verfahren oder Modell, um Objekte eines gewissen Bereichs nach bestimmten Kriterien zu klassifizieren, d. h. sie in bestimmte Kategorien oder Klassen einzuordnen.

TCPA: siehe *Trusted Computing Group*.

TCSEC: Abkürzung für Trusted Computer System Evaluation Criteria. Titel eines vom US-amerikanischen Verteidigungsministerium (Department of Defense, DoD) im Jahr 1985 veröffentlichen Standardisierungsdokuments mit Evaluierungskriterien für die Prüfung und Bewertung der Sicherheit der Informationstechnik. TCSEC wird im Allgemeinen als Orange Book bezeichnet. TCSEC ist ein von der US-Regierung herausgegebener Standard für die Bewertung und Zertifizierung der Sicherheit von Computersystemen. TCSEC wurde vor allem in den USA verwendet, in Europa und anderen Teilen der Welt setzte man auf den *ITSEC*-Standard (in Deutschland zunächst auf *ITSK*). Alle diese Standards sind in einem neuen Standard, den Common Criteria, aufgegangen.

Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V.: Dachorganisation von *medizinischen Forschungsverbünden* zwecks Identifikation und

Lösung gemeinsamer organisatorischer, rechtlicher und technologischer Fragestellungen. Zu den Mitgliedern der TMF gehören die *Kompetenznetze in der Medizin*, die *Koordinierungszentren für Klinische Studien*, eine Reihe von *Netzwerken zu seltenen Erkrankungen*, infektionsepidemiologische Netzwerke, das *Nationale Genomforschungsnetz* und verschiedene weitere medizinische Forschungseinrichtungen. Nähere Informationen über die TMF befinden sich unter `http://www.tmf-ev.de`.

Teilnehmer: siehe *Forscher*.

TempID: Temporäre ID, ersetzt während einer Anfrage *IDAT* zwecks $MDAT^W \rightarrow IDAT$-Zuordnung.

TMF: *Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V.*

Trägereinrichtung: Träger des medizinischen Forschungsnetzes ist die Einrichtung oder Institution, die rechtlich für die Daten- und Probensammlung verantwortlich ist. Dies kann eine Universität, eine Klinik oder ein Zusammenschluss verschiedenartiger Einrichtungen in Form einer juristischen Person (etwa einer GmbH oder eines eingetragenen Vereins) oder einer anderen Rechtsform (Gesellschaft bürgerlichen Rechts, Stiftung des privaten Rechts usw.) sein. Der Träger des medizinischen Forschungsnetzes kann den eigentlichen Datenbank- oder Biomaterialbank-Betrieb einer anderen Stelle (dem sogenannten Betreiber) übertragen. Dieser Betreiber muss nicht notwendigerweise der Trägerinstitution der Biobank angehören. Hierbei handelt es sich dann um eine Datenverarbeitung im Auftrag.

Trusted Computing Group: Die Trusted Computing Group (TCG) ist eine internationale, von der Industrie getriebene Standardisierungs-Organisation, die einen offenen Standard für Trusted-Computing-Plattformen entwickelt. TCG hat im Jahre 2003 die Standardisierungsarbeit der ehemaligen Trusted Computing Platform Alliance (*TCPA*) adoptiert und setzt diese fort.

Trusted Execution Technology: Trusted Execution Technology (TXT) ist eine Bezeichnung von Intel (ehemals LaGrande Technology) für eine Erweiterung, die in diverse neuere CPUs von Intel integriert ist. TXT basiert auf einem Konzept der *Trusted Computing Group* (TCG, ehemals *TCPA*), geht aber noch weit darüber hinaus. So soll es durch TXT keinem auch noch so hoch privilegierten Programm mehr erlaubt sein, auf Daten oder Code einer anderen Anwendung zuzugreifen. Dazu ist aber zusätzlich ein TPM-Chip auf der Hauptplatine nötig.

Überspannung: Überspannung ist eine elektrische Spannung in elektrischen Systemen, die den Toleranzbereich deren Nennspannung überschreitet. Überspannungen führen zu einem Störfall oder Fehlerfall, wenn sie Bauelemente oder Bestandteile der Anlagen zerstören.

USV: Unterbrechungslose Stromversorgung (USV), engl. Uninterruptable Power Supply (UPS). In Informationstechnologie und Telekommunikation Stromversorgungseinrichtung, die den angeschlossenen „Verbrauchern“ (aktive IT-/TK-Komponenten/-Geräte) eine kontinuierliche elektrische Energieversorgung hoher Verfügbarkeit sicherstellt. Dazu gehört insbesondere die Überbrückung von Ausfällen der öffentlichen oder lokalen Stromversorgung.

Value at Risk: Der Value at Risk (VaR) bezeichnet ein Risikomaß, das den geschätzten, maximalen (Marktwert-)Verlust einer Risikoposition nach einer vorgegebenen Periode (Haltedauer) angibt, der mit einer bestimmten Wahrscheinlichkeit unter üblichen Marktbedingungen nicht überschritten wird.

Vektor: Im allgemeinen Sinn versteht man unter einem Vektor ein Element eines Vektorraums, d. h. ein Objekt, das zu anderen Vektoren addiert und mit Zahlen, die als Skalare bezeichnet werden, multipliziert werden kann (s. a. *Risikovektor*).

Verantwortliche Stelle: Das BDSG definiert die verantwortliche Stelle als jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt (§3 Abs. 7 BDSG).

Verhältnismäßigkeit: Der Begriff Verhältnismäßigkeit beschreibt eine Abwägung und findet in dieser Arbeit Verwendung im Zusammenhang mit den *Informationssicherheitsmaßnahmen*. Die Verhältnismäßigkeit steht dabei für Erforderlichkeit im Sinne des begründeten Verzichts auf einige Redundanzen oder der Implementierung von „einfacheren“ Sicherheitsvorkehrungen. Mangelnde Ressourcen gelten nicht als ein Verhältnismäßigkeitskriterium (vgl. [Pom11b]).

Versorgungsdatenbank: Eine Datenbank, in der *Patientendaten* gespeichert werden, die der unmittelbaren Versorgung des *Patienten* dienen. In einem Krankenhaus ist eine solche Datenbank Teil des Krankenhaus-Informationssystems (KIS), in der Arztpraxis Teil der Praxis-Software. Im Rahmen der integrierten Versorgung werden institutionsübergreifende Datenbanken aufgebaut, in denen die *Patientenakten* gespeichert werden. Eine Nutzung der Daten aus einer Versorgungsdatenbank zu wissenschaftlichen Zwecken darf nur in anonymisierter Form oder mit einer expliziten Einwilligung der Betroffenen geschehen.

VPN: Abkürzung für Virtual Private Network, dt. Virtuelles Privates Netz. In der paketvermittelten Datenkommunikation steht die Bezeichnung für geschlossene logische Datennetze mit verbindungsorientierter Übertragung (z. B. virtuelle Wählverbindungen oder Festverbindungen) oder verbindungsloser Übertragung.

Web 2.0: Unter der Bezeichnung „Web 2.0“ werden neue Formen der Nutzung und der Vernetzung des Internets bzw. des World Wide Web (kurz Web) zusammengefasst,

die sich etwa seit den Jahren 2003/2004 herausgebildet und durchgesetzt haben. Die Versionszählung „2.0“ suggeriert dabei eine deutliche qualitative Veränderung bzw. Weiterentwicklung gegenüber dem herkömmlichen Internet „1.0“.

Web Service: Oberbegriff für Softwarebausteine, die Programme, die auf unterschiedlichen Netzwerkrechnern laufen, über das Internet zu einer Anwendung miteinander verknüpfen. Als großer Vorteil der Webservices gelten die geringen Kosten der Verknüpfung im Vergleich mit herkömmlichen Integrationsmethoden. Daher gelten Webservices als zentrale Bausteine des Distributed Computing im Internet und somit als Schlüssel zu einer einfachen Vernetzung der Geschäftsprozesse in und zwischen Unternehmen.

Web Services Security: Vom Konsortium OASIS (Organization for the Advancement of Structured Information Standards) im März 2004 in seiner ersten Version vorgestellter Sicherheitsstandard für die Verschlüsselung und die Sicherstellung der Integrität von SOAP-Nachrichten (Simple Object Access Protocol). Der Standard definiert Sicherheits-Token als Erweiterungen des SOAP-Headers. Ein Token kann Schlüsselpaare, Authentifizierungsinformationen einschließlich einer Signatur, Autorisierung sowie einen Zeitstempel enthalten und begleitet die Nachricht von Anfang bis zum Ende ihres Weges.

Widerruf: Unter dem Widerruf der Daten- oder Probenverwendung versteht man die teilweise oder vollständige Rücknahme der *Einwilligungserklärung* mit der Folge, dass Daten und *Proben* vom *Forschungsverbund* nicht bzw. nur noch in eingeschränktem Maße für eigene oder fremde *Forschungsvorhaben* verwendet werden dürfen. Aus der Vereinbarung mit dem *Patienten* oder *Probanden* kann sich nach dem Widerruf der *Einwilligungserklärung* auch die Pflicht ergeben, Daten zu löschen oder zu anonymisieren bzw. die Probe an den *Probanden* herauszugeben, sie zu vernichten oder zumindest zu anonymisieren. Es sind auch Fälle denkbar, in denen ein Widerruf der *Einwilligungserklärung* ausgeschlossen ist (etwa nach dem *AMG*).

WORM: WORM ist die Abkürzung für write once read multiple (times) oder write once read many (times) (= „einmal beschreiben, mehrmals lesen“). WORM bezieht sich meist auf bei Computern verwendete Speichermedien, die nur einmal mit Daten beschrieben werden können, um sie danach beliebig oft auszulesen. Die WORM-Technologien haben die Aufgabe, Schreibschutz für die Speichermedien zu erzeugen; die so geschriebenen Daten sollen anschließend weder abgeändert noch überschrieben noch gelöscht werden können. WORM-Medien werden für alle Arten von digitalen Archiven als Speichermedium eingesetzt. Diese kommen bei großen Mengen an unveränderbaren Dokumenten zum Einsatz, die beispielsweise in Gesetzen und Compliance-Regelungen wie SOX, GDPdU, Basel II etc. gefordert werden.

Wörterbuchangriff: Engl. Dictionary Attack. Im Bereich der Informationssicherheit ein

relativ simpler, aber in manchen Fällen sehr effektiver kryptografischer Angriff auf verschlüsselte Nachrichten. Im Unterschied zum Angriffstyp *„Brute-Force“* wird der Schlüsselraum (Key Space), d. h. die Menge aller Schlüssel, mit der ein Verschlüsselungsverfahren arbeitet, zur Suche eingeschränkt. Dazu unerlässlich sind allerdings Kenntnisse über die Qualität der Schlüssel.

WSE: Abkürzung für Web Services Enhancements. Eine von Microsoft bereitgestellte Erweiterung für das .NET Framework. Sie dient der Unterstützung von Webservices im .NET Framework, die auf *XML*, SOAP (Simple Object Access Protocol) und WSDL (Web Services Description Language) aufbauen.

Xen: Von der britischen University of Cambridge entwickelter Virtual Machine Monitor (VMM), der der GNU General Public License (GNU GPL) unterliegt. Das universitäre Xen-Projekt kooperiert seit Anbeginn eng mit der informationstechnischen Industrie, insbesondere mit Intel, Hewlett Packard, Novell, Red Hat, AMD und IBM. Kernkomponente von Xen ist der so genannte Hypervisor. Er fungiert als eine Art Meta-Betriebssystem und bildet eine abstrahierende Softwareschicht zwischen der Hardware und den Gast-Betriebssystemen. Diese Architektur wird als Paravirtualisierung bezeichnet: Der Kernel des Xen-Betriebssystems muss angepasst werden, damit der Gast fortan mit der Hypervisor-Schicht und nicht direkt mit der Hardware kommuniziert.

XML: Eine im Februar 1998 von der Internetorganisation W3C (World Wide Web Consortium) verabschiedete Spezifikation einer Metasprache für die Beschreibung von Dokumenten und Daten, d. h. eines universellen Austauschformates für jede Art von Nachrichten. Mit dem vollständig zu HTML (Hypertext Markup Language) kompatiblen XML ist es beispielsweise möglich, im World Wide Web (Web) jedes Webdokument mit einer Struktur zu versehen, die der eines Katalogs ähnelt.

Zero-Knowledge-Beweis: Im Bereich der IT-Sicherheit der Nachweis über den Besitz eines kryptografischen Geheimnisses, ohne dieses preiszugeben und ohne dass ein Dritter durch einen oder mehrere solchen/er Nachweis/e etwas über das Geheimnis selbst erfährt.

Zoonose: Zoonosen (von griechisch zoon „Lebewesen“ und nosos „Krankheit“) sind von Tier zu Mensch und von Mensch zu Tier übertragbare Infektionskrankheiten.

Zugriffskontrolle: Zugriffskontrolle (engl. access control) bezeichnet die Überwachung des Zugriffs auf bestimmte Ressourcen. Im Konkreten entscheidet die Zugriffskontrolle, ob der Zugang zu einer bestimmten Ressource gewährt oder verwehrt wird. Das Ziel der Zugriffskontrolle ist die Sicherstellung der Integrität, Vertraulichkeit und Verfügbarkeit von Informationen.

Zugriffskontrollsystem: Ein System zur Gewährleistung der *Zugriffskontrolle*.

Abbildungsverzeichnis

Tabellenverzeichnis

Anhang

A. Sicherheits- und Risikomanagement

A.1. Untersuchung der Wirksamkeitsbewertung von Sicherheitsmaßnahmen mithilfe von etablierten S&R-Frameworks

Als besonders gut etabliert und im Einsatz weit verbreitet gelten die Frameworks der ISO-Normenreihe, COBIT, ITIL, NIST und BSI IT-Grundschutz (vgl. [SW10]). Die von diesen Frameworks verwendeten Messansätze der Informationssicherheit sollen im Folgenden untersucht werden. Eine Reihe weiterer Ansätze wie beispielsweise OSSTMM, OCTAVE, CRAMM, SIEM- und SAS-Systeme etc. wird ebenfalls – auch wenn weniger intensiv – analysiert.

A.1.1. ISO-Normenreihe (ISO 2700X)

Die ISO-Normen gehören zu den bekanntesten Standards. Mit der ISO 27000-Reihe versucht die „International Organization for Standardization“ (ISO) eine umfangreiche Instrumentensammlung bereitzustellen, um mit deren Hilfe alle bedeutenden Aspekte der Informationssicherheit abbilden zu können (vgl. [Hay10, S. 224 ff.]).
Die ISO-Norm ISO/IEC 27001:2005[1] fordert im Abschnitt 4.2 „Establishing and managing the ISMS“ die Begutachtung von Risiken und Erstellung eines dafür erforderlichen Kennzahlensystems. [iso05, S. 4 f.]:

c) *„Define the risk assessment approach of the organization (...)*

d) *Identify the risks (...)*

e) *Analyse and evaluate the risks (...)*

f) *Identify and evaluate options for the treatment of risks (...)*

g) *Select control objectives and controls for the treatment of risks.“*

[1] „ISO/IEC 27001:2005 : Information Technology : Security Techniques : Information Security Management Systems : Requirements.“

Im Unterabschnitt 4.2.3 „Monitor and review the ISMS“ wird die Messung der Effektivität des ISM-Systems verlangt. [iso05, S. VI]: *„The Organization shall do the following (...) Undertake regular reviews of the effectiveness of the ISMS (..) taking into account results of security audits, incidents, results from effectiveness measurements, suggestions and feedback from all interested parties (...) measure the effectiveness of controls to verify that security requirements have been met.“* Eine Konkretisierung der Anforderungen und Zielsetzungen zur Informationssicherheit erfolgt im Anhang A der ISO-Norm 27001:2005 in tabellarischer Form und deckt folgende Themenbereiche ab: „A.5 Security Policy“, „A.6 Organization of information security“, „A.7 Asset management“, „A.8 Human resources security“, „A.9 Physical and environmental security“, „A.10 Communications and operations management“, „A.11 Access Control“, „A.12 Information systems acquisition, development and maintenance“, „A.13 Information security incident management“, „A.14 Business continuity management“, „A.15 Compliance“ (vgl. [iso05, S. 13 ff.]).
Aufgrund der generischen Natur bleiben die Anforderungen und Zielsetzungen der ISO-Norm 27001 allgemein formuliert. So heißt es beispielsweise: *„A.10.4 Protection against malicious and mobile code“* [iso05, S. 19]: *„Objective: To protect the integrity of software and information (...) Control: Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.“* oder „A.11 Access control“ [iso05, S. 22]: *„Objective: To control access to information (...) Control: An access control policy shall be established, documented, and reviewed based on business and security requirements for access.“*
Die Konkretisierung der Messbarkeit der Implementierung eines ISMS (Information Security Management System) nach ISO 27001 erfolgt in der ISO-Norm „ISO/IEC 27004:2009[2] [iso09]. ISO 27004 enthält Empfehlungen, wie die Messbarkeitsanforderungen von ISO 27001 erfüllt werden können, und berücksichtigt folgende Bereiche [iso09, S. VI f.]:

a) *„developing measures (i. e. base measures, derived measures and indicators);*

b) *implementing and operating an Information Security Measurement Programme;*

c) *collecting and analysing data;*

d) *developing measurement results;*

e) *communicating developed measurement results to the relevant stakeholders;*

f) *using measurement results as contributing factors to ISMS-related decisions;*

g) *using measurement results to identify needs for improving the implemented ISMS, including its scope, policies, objectives, controls, processes and procedures; and*

[2] „ISO/IEC 27004:2009 : Information Technology : Security Techniques : Information Security Management : Measurement.“

h) *facilitating continual improvement of the Information Security Measurement Programme.“*

Das in ISO 27004 verwendete Modell zur Messung der Informationssicherheit wird aus der ISO-Norm ISO/IEC 15939:2007[3] übernommen. Das empfohlene Modell enthält das Element der Basismetriken[4] als die einfachste Variante der Kennzahlen, die durch die Anwendung eines Messverfahrens auf die Attribute eines Messobjektes entstehen. Mehrere Basismetriken können zu einer sogenannten abgeleiteten Metrik[5] kombiniert bzw. mithilfe einer Messfunktion[6] verknüpft werden. Mithilfe von Indikatoren werden bestimmte Attribute bewertet, die aus einem analytischen Modell entwickelt werden. Das analytische Modell kann sowohl auf die Basismetriken als auch auf die abgeleiteten Metriken angewendet werden. Mithilfe der Messergebnisse[7] wird die Effektivität der ISMS-Implementierung durch die Interpretation der Indikatoren im Hinblick auf die Entscheidungskriterien bewertet. Die Entscheidungskriterien können ihrerseits auf eine Vielzahl von Indikatoren angewendet werden. Die Spezifikation der Performance erfolgt durch die Definition von Zielsetzungen, die sich aus den Sicherheitszielen des ISMS ableiten. Abbildung 16 veranschaulicht die Zusammenhänge zwischen den drei Kernelementen des Modells: Messobjekt, Metriken und ISMS-Zielsetzung.
Der Anhang B der ISO-Norm 27004 listet einige Beispiele für die Zusammensetzung der Metriken auf und veranschaulicht den Ansatz. Das Messkonzept setzt sich aus der Verknüpfung der ISO-Norm in Form von Kontrollen und der Metriken nach ISO 27004. So verlangt beispielsweise die ISO 27001-Kontrolle A.8.2.2, dass alle Mitarbeiter und relevanten Drittparteien die für sie notwendigen Informationssicherheitsschulungen erhalten, und diese Schulungen regelmäßig aufgefrischt werden (vgl. [iso09, S. 16]). In ISO 27004 wird ein Metrik-Konstrukt B.1.2 „Information Security Training“ vorgeschlagen, um den Grad der Compliance messen zu können. Als Basismetrik dient die Anzahl der Mitarbeiter, die das Training bereits absolviert haben (x) bzw. noch erhalten müssen (y). Es wird der Vorschlag unterbreitet, als Messfunktion $x/y * 100$ zu benutzen; als Indikatoren dienen die Säulendiagramme im zeitlichen Verlauf. Das analytische Modell legt die Schwellenwerte fest, die den Erreichungsgrad der Kontrolle nach der Grün/Gelb/Rot-Methode bewerten und daraus die Entscheidungskriterien für die (Nicht)Intervention[8] begründen (vgl. [iso09, S. 27 f.]).

[3] „ISO/IEC 15939:2007 : Systems and Software Engineering : Measurement Process.“

[4] Base measure.

[5] Derived measure.

[6] Measurement function.

[7] Measurement results.

[8] Grün: Keine Aktion erforderlich. Gelb: Zusätzliche Informationen müssen eingeholt werden. Rot: Intervention bzw. Ursachenanalyse erforderlich.

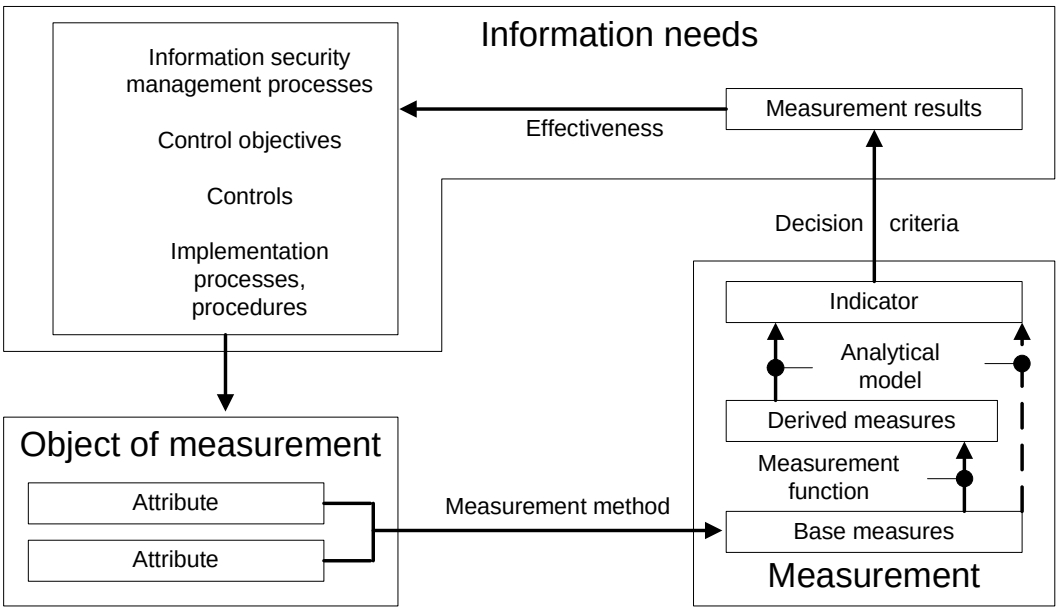

Abbildung 16.: Modell zur Messung der Informationssicherheit nach ISO 27004: Das Modell wird aus der ISO-Norm ISO/IEC 15939:2007 „Systems and software engineering : Measurement process“ übernommen und enthält drei Kernelemente: Messobjekt, Metriken und ISMS-Zielsetzung.

Manche der vorgeschlagenen Metriken stehen im Widerspruch zu der Forderung der ISO 27001-Norm, reproduzierbare und vergleichbare Ergebnisse zu erzielen. So schlägt z. B. der Metrikansatz B.6 „Protection against Malicious Code“ die Anzahl der durch die Malware verursachten Sicherheitsvorfälle (m) bzw. die Anzahl der verhinderten Malware-Angriffe als Basis-Metrik (n) vor. Als Datenquelle sollen dabei die Malware-Logs und Incident-Reports verwendet werden. Die Stärke des Malware-Schutzes soll die abgeleitete Metrik m/n widerspiegeln (vgl. [iso09, S. 45 f.]).

Eine solche Metrik eignet sich kaum zur Effektivitätsmessung einer Sicherheitsmaßnahme und zum Ableiten von korrigierenden Maßnahmen. So sagt z. B. eine gestiegene Anzahl der verhinderten Malware-Angriffe wenig aus: Sie könnte auf eine größere Anzahl von Angriffen oder aber auch auf eine Änderung der Erkennungsmethode z. B. in Folge von Sicherheitsupdates zurückgeführt werden. Demzufolge kann aus der genannten Metrik noch nicht einmal abgeleitet werden, ob die festgestellte Veränderung positiv oder negativ ist (vgl. [Str10, S. 157], [Axe08]). Ähnliche Bedenken gelten auch für die Ableitung des Sicherheitsstandes aus den prozentualen Anteilen von Systemen oder Komponenten, die bestimmte Sicherheitsmaßnahmen implementiert haben. Die teilweise Erfüllung bestimmter Sicherheitsanforderungen bedeutet nicht, dass das Risiko sich im gleichen Verhältnis automatisch reduziert (vgl. [BM08]).

Eine Reihe weiterer ISO-Normen, die jedoch nicht Bestandteile der ISO 2700X-Reihe sind, stehen im Zusammenhang mit dem IT-Sicherheitsmanagement, -Governance und -Qualitätsmanagement und werden im Folgenden beschrieben.

ISO 27799: In der internationalen Norm ISO 27799:2008[9] [iso08b] werden die für ein Informationssicherheits-Managementsystem im Gesundheitswesen spezifischen Anforderungen definiert. Die Notwendigkeit für diese spezifische Vorgehensweise wird mit der besonderen Schutzbedürftigkeit der medizinischen Daten begründet. [iso08b, S. 8]: „This identifying information is of great potential value to those who would use it to commit identity theft and so must be rigorously protected. The health environment, with its unique threats and vulnerabilities, should therefore be considered with special care.“ Im Anhang A der ISO-Norm werden 25 der für die Sicherheit im Gesundheitsbereich geltenden Risiken aufgeführt. Die empfohlene Vorgehensweise zur Risikoanalyse lehnt sich an die ISO-Normen ISO/IEC 27001 und ISO/IEC TR 13335-3[10]. Die Besonderheiten der Anwendung der ISO-Norm 27002 für die personenbezogenen medizinischen Daten werden im Abschnitt 7 „Healthcare implications of ISO/IEC 27002“ erläutert. Aufgrund der durch die Abstimmung mit den Datenschutz- und Datensicherheitsverantwortlichen in mehreren Ländern gesammelten Erfahrungen wird angenommen, dass bereits im Falle der Nichteinhaltung einer der 39 Kontrollen von ISO 27002 von einer generellen Nichterfüllung der internationalen Standards[11] auszugehen ist. Anschließend werden die Besonderheiten der genannten Kontrollen für die medizinischen Umgebungen erläutert.

ISO 38500: Die ISO-Norm 38500:2008[12] beschreibt die Bestandteile des IT-Governance-Frameworks. Im Mittelpunkt der Norm stehen sechs Prinzipien, die nach einer „good corporate governance of IT“ zu befolgen sind: Verantwortung, Strategie, Akquise, Performance, Konformität und menschliches Verhalten.[13] Die wichtigsten Bestandteile des anschließend vorgestellten IT-Governance Modells sind die Bewertung, Steuerung und Überwachung. Im dritten Kapitel wird beispielhaft jedoch nicht abschließend erörtert wie die sechs Grundprinzipien anhand der drei Grundbausteine des Modells angewendet werden sollen. In der Norm erfolgt nur ein allgemeiner Hinweis auf die Notwendigkeit der Überwachung der IT-Performanz mithilfe eines dazu passenden Messsystems, ohne dieses System jedoch näher zu beschreiben (vgl. [iso08b, S. 6 ff.]).

---

[9] 27799:2008: Health Informatics: Information Security Management in Health Using ISO/IEC 27002.

[10] Die ISO-Norm „ISO/IEC 13335-3: Information technology : Guidelines for the management of IT Security : Part 3: Techniques for the management of IT Security“ wurde am 04.06.2008 durch die Norm ISO/IEC 27005 „Information Technology : Security Techniques : Information Security Risk Management“ teilweise abgelöst. Diese Norm liegt in der Zwischenzeit in einer aktualisierten Version „ISO/IEC 27005:2011“ vor.

[11] Compliance.

[12] ISO/IEC 38500:2008 : Corporate Governance of Information Technology

[13] Responsibilty, Strategy, Acquisition, Performance, Conformance and Human Behaviour.

ISO 9001: Die ISO-Norm 9001:2008[14] [iso08a] definiert die Anforderungen an ein Qualitätsmanagement-System (QM-System) und legt die Basis für ein umfassendes QM-System. Das Thema der Messbarkeit wird in den Abschnitten 7.6 „Control of monitoring and measuring equipment“ und 8 „Measurement, analysis and improvement“ bzw. 8.2 „Monitoring and measurement“ behandelt. Dabei wird die Anforderung gestellt, ein Control Monitoring und Measurement-System zu installieren. Diese Empfehlung erfolgt jedoch allgemein, sodass unbeantwortet bleibt, wie ein solches System im Zusammenhang mit den Sicherheitsmaßnahmen bzw. der Bewertung ihrer Sinnhaftigkeit und Notwendigkeit zu bewerten ist.

Notwendigkeit von Sicherheitsinvestitionen: Eine Möglichkeit zur Durchführung der Kosten-Nutzen-Analyse auf der Basis der ISO-Normen beschreiben Ted Humphreys und Angelika Plate in ihrem Buch „Measuring the Effectiveness of Your ISMS Implementations Based on ISO/IEC 27001“. Sie definieren die Effektivität von Informationssicherheitsmaßnahmen wie folgt:[15]

Effektivität von Informationssicherheitsmaßnahmen = potenzielle Schäden - effektive Schäden = vermiedene Schäden (vgl. [HP06, S. 21])

Die Autoren schlagen außerdem eine mögliche grafische Darstellung des Risikoportfolios in Form eines sogenannten Spinnennetzdiagramms vor. Die Abbildung 17 illustriert den Ansatz.

Das Spinnennetzdiagramm soll die Änderung des Risikoprofils einer Organisation im zeitlichen Verlauf erkennbar machen. Im Mittelpunkt des an ISO 27001 angelehnten Ansatzes steht die Definition der Risikotragbarkeit im Zusammenhang mit den einzelnen Kernbereichen der Organisation wie beispielsweise Personal, Produktion, Kernprozesse etc. Ein Vergleich der Ist-Werte mit dem angestrebten Risikoportfolio ermöglicht Aufschlüsse darüber, in welchen Bereichen Sicherheitsinvestitionen sinnvoll sind (vgl. [HP06, S. 30]). Die Abbildung 17 zeigt beispielhaft die Veränderung des Risikoportfolios für zwei Messzeiträume: t_1 und t_2. Das Risikoportfolio zum Zeitpunkt t_2 ist in allen Bereichen deutlich näher an der Sollvorgabe als das Risikoportfolio zum Zeitpunkt t_1. Lediglich die Messungen für den Bereich Personal liegen außerhalb des geduldeten Risikobereichs. Aufgrund dieser Beobachtung könnte z. B. die Notwendigkeit weiterer Investitionen im Personalbereich ermittelt werden, oder es könnte sich eine Änderung der Messmethodik bzw. eine Anpassung der Zielvorgaben ergeben.

[14] „9001:2008 : Quality Management Systems : Requirements“.

[15] Potenzielle Schäden: Erwartete Schäden zum Zeitpunkt der Entdeckung oder Meldung des Sicherheitsvorfalls; effektive Schäden: die sich nach der Untersuchung und der Wiederherstellung nach dem Sicherheitsvorfalls ergebenden Schäden; vermiedene Schäden: potenzielle Schäden – effektive Schäden als positives Ergebnis der Untersuchung und Wiederherstellung nach dem Sicherheitsvorfall.

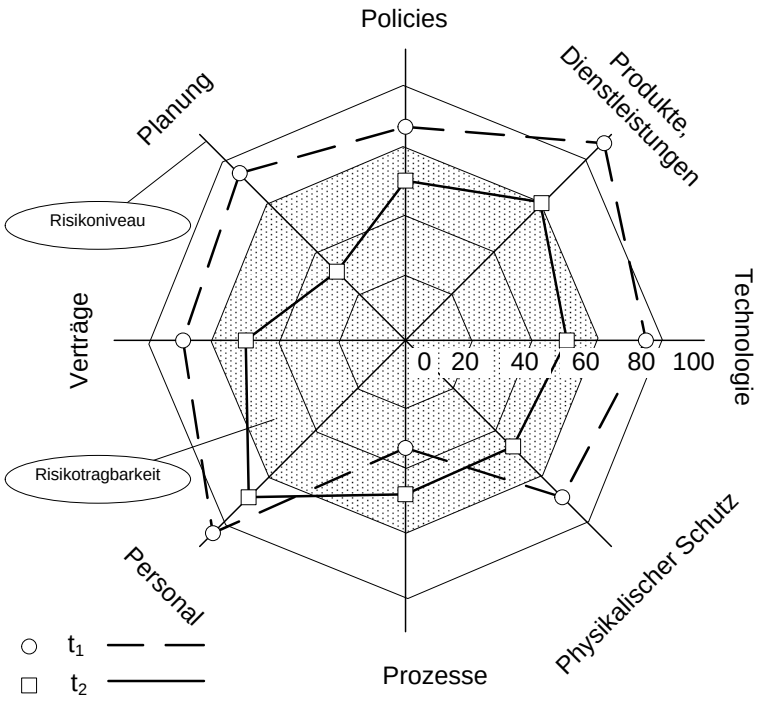

Abbildung 17.: Grafische Darstellung des Risikoportfolios mithilfe eines Spinnennetzdiagramms: Nach der Definition der Risikotragbarkeit erfolgt eine wiederholte Messung des Risikoniveaus. Ein Vergleich der Ist-Werte mit der Soll-Vorgabe erlaubt Aufschlüsse über die Notwendigkeit von Sicherheitsinvestitionen in bestimmten Bereichen.

A.1.2. COBIT 4.1

Das COBIT IT-Governance-Framework gliedert die Aufgaben der IT in Prozesse und sogenannte Control Objectives.[16] Im Rahmen der Control Objectives wird primär definiert, welche Anforderungen umgesetzt werden sollen. Die Art und Weise der Umsetzung wird i. d. R. nicht näher spezifiziert.

In der untersuchten Version 4.1 des COBIT-Frameworks [ISA07] sind insbesondere die Abschnitte PO9, DS5, DS12 und ME3[17] in Bezug auf die Informationssicherheitsmaßnahmen relevant. Einige der vorgeschlagenen Metriken bedürfen zusätzlicher Informationen, um eine Aussagekraft zu entfalten bzw. um interpretiert zu werden. Die Tabelle 4 fasst die wichtigsten Informationssicherheitsmaßnahmen des COBIT-Frameworks zusammen.

Bei vielen der vorgeschlagenen Metriken benötigt man Vergleichswerte, um die Größen interpretieren zu können. So hat beispielsweise der prozentuale Anteil der Sicherheitsausgaben am IT-Budget dann eine Aussagekraft, wenn eine Vergleichbarkeit mehrerer Institutionen gegeben ist. Einige der vorgeschlagenen Metriken können nur mithilfe ergänzender Informationen interpretiert werden. Beispielsweise hat eine erhöhte Anzahl der neu identifizierten Risiken im Zusammenhang mit einer geänderten Vorgehensweise zur Risikoidentifikation

[16] Oft werden die „Control Objectives“ als Kontrollziele übersetzt.

[17] PO9: Assess and Manage IT Risks (Plan and Organise), DS5: Ensure Systems Security (Deliver and Support), DS12: Manage the Physical Environment (Deliver and Support), ME3: Ensure Compliance With External Requirements (Monitor and Evaluate).

PO9	Percent of critical IT objectives covered by risk assessment.	PO9	Percent of IT risk assessments integrated in the IT risk assessment approach.
PO9	Percent of identified critical IT events that have been assessed.	PO9	Number of newly identified IT risks (compared to previous exercise).
PO9	Number of significant incidents caused by risks that were not identified by the risk assessment process.	PO9	Percent of identified critical IT risks with an action plan developed.
PO9	Percent of IT budget spent on risk management (assessment and mitigation) activities.	PO9	Frequency of review of the IT risk management process.
PO9	Percent of approved risk assessments.	PO9	Number of actioned risk monitoring reports within the agreed-upon frequency.
PO9	Percent of identified IT events used in risk assessments.	PO9	Percent of risk management action plans approved for implementation [ISA07, S. 65].
DS5	Number of incidents with business impact.	DS5	Number of systems where security requirements are not met.
DS5	Time to grant, change and remove access privileges.	DS5	Number and type of suspected and actual access violations.
DS5	Number of violations in segregation of duties.	DS5	Percent of users who do not comply with password standards.
DS5	Number and type of malicious code prevented.	DS5	Frequency and review of the type of security events to be monitored.
DS5	Number and type of obsolete accounts.	DS5	Number of unauthorised IP addresses, ports and traffic types denied.
DS5	Percent of cryptographic keys compromised and revoked.	DS5	Number of access rights authorised, revoked, reset or changed [ISA07, S. 119].
DS12	Amount of downtime arising from physical environment incidents.	DS12	Number of security exposures arising from physical environment incidents.
DS12	Number of incidents due to physical security breaches or failures.	DS12	Number of incidents of unauthorised access to computer facilities.
DS12	Frequency of training of personnel in safety, security and facilities measures.	DS12	Percent of personnel trained in safety, security and facilities measures.
DS12	Number of risk mitigation tests conducted in the last year.	DS12	Frequency of physical risk assessment and reviews [ISA07, S. 147].
ME3	Cost of IT non-compliance, including settlements and fines.	ME3	Number of non-compliance issues reported to the board or causing public comment or embarrassment including settlements and fines.
ME3	Number of non-compliance issues reported to the board or causing public comment or embarrassment.	ME3	Number of critical non-compliance issues identified per year.
ME3	Frequency of compliance reviews.	ME3	Average time lag between identification of external compliance issues and resolution.
ME3	Average time lag between publication of a new law or regulation and initiation of compliance review.	ME3	Training days per IT employee per year related to compliance [ISA07, S. 163].

Tabelle 4.: Potenzielle Informationssicherheitsmetriken nach COBIT 4.1: PO9 : Assess and Manage IT Risks, DS5 : Ensure Systems Security , DS12 : Manage the Physical Environment, ME3 : Ensure Compliance With External Requirements.

eine andere Bedeutung als z. B. bei einer unveränderten Umgebung und könnte beispielsweise lediglich bedeuten, dass die alte Vorgehensweise zur Risikoidentifikation weniger effektiv oder präzise als die neue ist. Auch eine geringere Anzahl der neu identifizierten Risiken könnte bedeuten, dass die aktuell getroffenen Sicherheitsmaßnahmen effektiv sind; gleichzeitig ist jedoch auch denkbar, dass die verwendete Messmethode die neuen Risiken weniger zuverlässig identifiziert. Einige der im COBIT-Framework vorgeschlagenen Metriken werden erst ab einer bestimmten Organisationsgröße relevant bzw. finden hoffentlich im Bereich der medizinischen Forschung nie ihre Anwendung als Qualitätsmerkmal: beispielsweise die Anzahl der öffentlichkeitswirksamen Sicherheitsvorfälle (vgl. [ISA07]).

A.1.3. ITIL V.3

Die Abkürzung ITIL steht für „IT Infrastructure Library“ und bezeichnet eine Sammlung von sogenannten Best Practices zur Umsetzung eines IT-Service-Managements (ITSM). ITIL ist kein Standard im eigentlichen Sinn, sondern eine Verfahrensbibliothek in Form eines Regelwerkes, die Beschreibungen für die Prozesse, Werkzeuge und Organisationsaufbau enthält. Im Mittelpunkt von ITIL stehen die Planung, Umsetzung und Optimierung von IT-Serviceleistungen. Als oberstes Ziel gilt dabei die Erreichung von Unternehmens- bzw. Organisationszielen. Der Security-Managementprozess nach ITIL stellt eine Beschreibung zur systematischen Erreichung der Sicherheit in allen Organisationsbereichen dar. Dieser

Prozess basiert auf Anforderungen, die durch die sogenannten Service-Level-Agreements definiert sind. Die Erreichung der SLAs wird mithilfe von Kennzahlen überprüft, dadurch kann die Abweichung von Anforderungen quantifiziert und somit gemessen werden. Die zum Zeitpunkt der Analyse aktuelle Version 3 des ITIL-Frameworks enthält fünf Kernelemente:

- Service Strategy [HN07]
- Service Design [LR07]
- Service Transition [LM07]
- Service Operation [CW07]
- Continual Service Improvement [CS07]

Das aus der operativen Perspektive geschriebene zweite ITIL-Buch „Service Design“ enthält Empfehlungen zur Durchführung von Risikoanalysen und der daraus abgeleiteten Handhabung von Risiken. ITIL empfiehlt den Einsatz eines sogenannten Management of Risk-Frameworks (M_o_R), das in der Abbildung 18 dargestellt ist [LR07, S. 224].

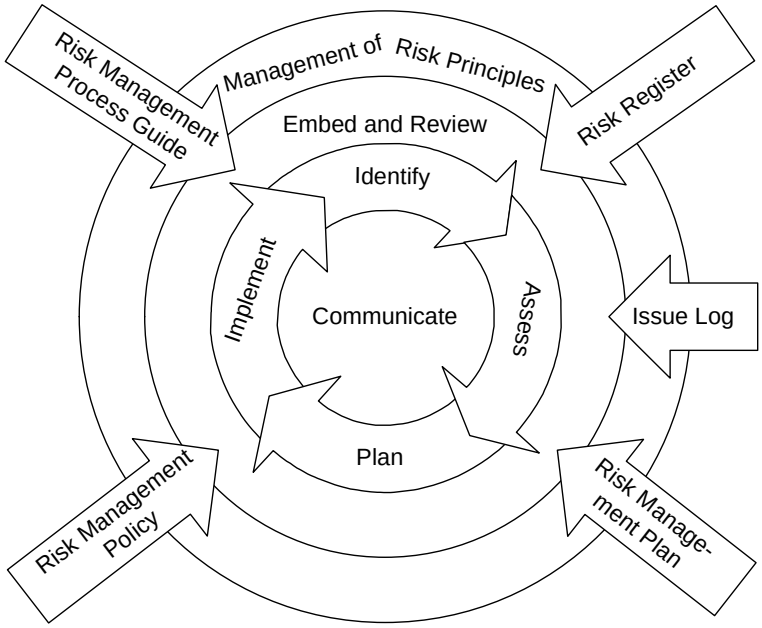

Abbildung 18.: Das M_o_R-Framework nach ITIL V.3: Die Kernbestandteile des Frameworks sind die Unternehmensprinzipien, der M_o_R-Ansatz, die Umsetzung und Überprüfung der M_o_R-Prozesse, die Prozesse selbst und die Kommunikation.

Das in ITIL empfohlene M_o_R-Framework besteht aus folgenden Elementen:

- den M_o_R-Prinzipien, die aus der Unternehmensführung abgeleitet werden und die Praxis des Risikomanagements bestimmen,
- dem M_o_R-Ansatz, der die M_o_R-Prinzipien in mehreren Dokumenten festhält; dazu gehören die Risk Management Policies, die Prozessbeschreibung, die Pläne, die Risikoregister und die Problem-Logs,
- den M_o_R-Prozessen, die sich in vier Hauptschritte einteilen lassen: Risikoidentifizierung, -analyse sowie Planung und Umsetzung von M_o_R-Maßnahmen,

- der Einbindung und der regelmäßigen Überprüfung der Prozesse,
- der Kommunikation über die bestehenden Gefahren und über weitere relevante Aspekte des Risikomanagements.

Die M_o_R-Methodik erfordert eine Risikoanalyse und die Entwicklung von Risikoprofilen z. B. in Form einer Risikomatrix (vgl. [LR07, S. 226 ff.]). In ITIL wird eine prozessorientierte Betrachtungsweise des Information Security Managements (ISM) bevorzugt angewendet. Der Abschnitt 4.6 „Information Security Management“ der zweiten ITIL-Kernpublikation „Service-Design“ enthält eine detaillierte Beschreibung der Komponenten des ISM-Prozesses. Bei der Beschreibung des ISM-Prozesses erfolgt ein Verweis auf die ISO 27001-Norm als eine Möglichkeit für eine unabhängige standardisierte ISMS-Zertifizierung (vgl. [LR07, S. 244 ff.]).
Der Unterabschnitt 4.6.7 „Key Performance Indicators“ erlaubt einen kurzen Einblick in das Thema der Sicherheitsmetriken. Es werden einige weniger konkrete Beispiele für den Aufbau solcher Metriken genannt: beispielsweise die prozentuale Veränderung bei den gemeldeten Sicherheitsvorfällen und ihre Bedeutung, die Anzahl der (Nicht)Übereinstimmungen zwischen den Policies und dem ISM-Prozess, der Anteil der Prozesse, die mit den Sicherheitspolicies übereinstimmen (vgl. [LR07, S. 256 ff.]).
Zum Aufbau der eigentlichen Metriken wird auf die fünfte Publikation „Continual Service Improvement“ [CS07] verwiesen; der zweite Teil enthält eine stark verallgemeinerte Beschreibung der Aspekte, die für die Qualitätsmessung des Prozess-Designs und der Ergebnisse. Erneut wird eine prozessorientierte Sichtweise gewählt; die Bedeutung der Metriken als Mittel zur Verhaltensänderung der beteiligten Einheiten bzw. zur Erreichung der Unternehmensziele wird unterstrichen. Mithilfe eines hierarchischen Metrik-Konzeptes, dem sogenannten Metrik-Baum, soll der Informationsfluss in Abhängigkeit von den Aufgaben der beteiligten Einheiten gesteuert werden (vgl. [LR07, S. 76 ff.]).
Die fünfte Publikation der ITIL-Reihe behandelt ausführlich die Bedeutung und den Aufbau des Risikomanagements (vgl. [CS07, S. 195 ff.].) Eine detaillierte Anleitung zum Aufbau, zur Anwendung und zur Weiterentwicklung von Metriken erfolgt im Abschnitt 4.1.2 „Metrics and Measurement“. Es wird zwischen drei Arten von Metriken (Technologie-, Prozess- und Service-Metriken) unterschieden. Im Mittelpunkt der vorgeschlagenen Metriken stehen – dem ITIL-Ansatz entsprechend – die Erhöhung der Kundenzufriedenheit, die Verbesserung der Service-Qualität, die Optimierung der IT-Kosten etc. Die Publikation formuliert einige Anforderungen an die KPI-Auswahl in Bezug auf die Aussagekraft, Handhabung, Anpassungsfähigkeit und Zielsetzung der Indikatoren. Im Mittelpunkt steht die ITIL-spezifische prozessorientierte Sichtweise der Metrik-Entwicklung und -Anwendung. Konkrete Vorschläge für geeignete Informationssicherheitsmetriken werden nicht unterbreitet (vgl. [CS07, S. 98-104]).

A.1.4. NIST 800-X (Special Publications)

Das National Institute of Standards and Technology (NIST) hat mehrere Veröffentlichungen über die IT Sicherheits-Policies, -prozeduren und -standards herausgegeben. Insbesondere soll die sogenannte 800-Serie der NIST-Publikationen eine praxisorientierte und kosteneffektive Umsetzung eines höheren Sicherheitsniveaus unterstützen. Neben den notwendigen Maßnahmen und Prozeduren beschreiben die NIST-Anleitungen Kriterien für die Ermittlung und die Dokumentation von Sicherheitsbedrohungen und Implementierung von Sicherheitsmaßnahmen.

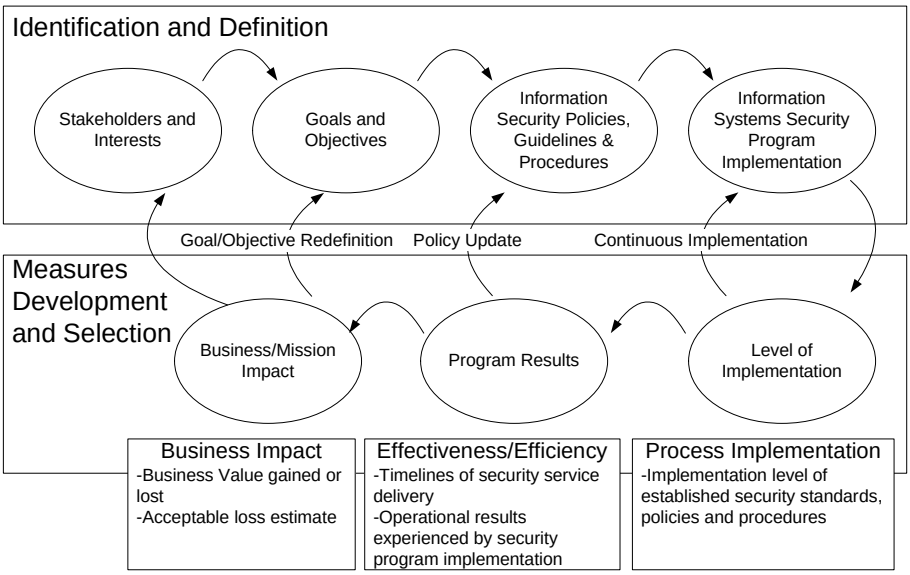

Abbildung 19.: Prozess der Ermittlung der notwendigen Sicherheitsmaßnahmen nach NIST 800-55: Die Ermittlung notwendiger Sicherheitsmaßnahmen erfolgt in zwei Hauptschritten. Diese sind die Identifikation und die Definition der Ziele sowie die Entwicklung spezifischer Messbarkeitskriterien [CSS+08, S. 25].

Als besonders relevant in Bezug auf die Sicherheitsmetriken erweist sich die NIST-Publikation 800-55[18] [CSS+08]. Diese NIST-Veröffentlichung ist eng verknüpft mit den NIST-Publikationen 800-53[19] [RSK+10] und 800-53A[20] [RTH+10]. Die beiden NIST-Standards liegen in den aktualisierten Versionen vor und lösen den veralteten Standard NIST 800-26[21] ab. Sie sollen für die Spezifikation und Begutachtung der Sicherheitskontrollen verwendet werden.

In NIST 800-55 wird zwischen drei Arten von Sicherheitskennzahlen unterschieden: zur Messung der Implementierungsvollständigkeit, Effizienz bzw. Effektivität und Bedeutung der Sicherheitskennzahl für die Organisation (vgl. [CSS+08, S. 13 f.]):

[18] „Performance Measurement Guide for Information Security“.

[19] „Recommended Security Controls for Federal Information Systems and Organizations“.

[20] „Guide for Assessing the Security Controls in Federal Information Systems and Organizations : Building Effective Security Assessment Plans“.

[21] „Security Self-Assessment Guide for Information Technology Systems“.

Bezeichnung	Kennzahl	Typ	SP 800-53
Security Budget	Percentage of the agency's information system budget devoted to information security	Impact	SA-2
Vulnerability Management	Percentage of high vulnerabilities mitigated within organizationally defined time periods after discovery	Efficiency	RA-5
Access Control	Percentage of remote access points used to gain unauthorized access	Effectiveness	AC-17
Awareness and Training	Percentage of information security personnel that have received security training	Implementation	AT-3
Audit and Accountability	Average frequency of audit records review and analysis for inappropriate activity	Efficiency	AU-6
Certification, Accreditation, and Security Assessments	Percentage of new systems that have completed certification and accreditation prior to their implementation	Effectiveness	CA-6
Configuration Management	Percentage approved and implemented configuration changes identified in the latest automated baseline configuration	Implementation	CM-2, CM-3
Contingency Planning	Percentage of information systems that have conducted annual contingency plan	Effectiveness	CP-4
Identification and Authentication	Percentage of users with access to shared accounts	Effectiveness	AC-2, AC-3, IA-2
Incident Response	Percentage of incidents reported within required time frame per applicable incident category	Effectiveness	IR-6
Maintenance	Percentage of system components that undergo maintenance in accordance with formal maintenance schedule	Efficiency	MA-2, MA-6
Physical and Environmental	Percentage of physical security incidents allowing unauthorized entry into facilities containing information systems	Effectiveness	PE-6
Planning	Percentage of employees who receive authorized access to information systems only after they sign an acknowledgement that they have read and understood rules of behavior	Implementation	PL-4, AC2
Personal Security	Percentage of individuals screened before being granted access to organizational information and information systems	Implementation	AC-2, PS-3
Risk Assessment	Percentage of vulnerabilities remediated within organization-specified time frames	Efficiency	RA-5, CA-5
System and Services Acquisition	Percentage of system and services acquisition contacts that include security requirements and or specifications	Implementation	SA-4
System and Communications Protection	Percentage of mobile computers and devices that perform all cryptographic operations using FIPS 140-2 validated cryptographic modules operating in approved modes of operation	Implementation	SC-13
System and Information Integrity	Percentage of operating system vulnerabilities for which patches have been applied or that have been otherwise mitigated	Implementation and Effectiveness	SI-2

Tabelle 5.: Potenzielle Informationssicherheitsmetriken nach NIST 800-55: Die Vorschläge für die Sicherheitsmetriken beinhalten Messkriterien für die Implementierungsvollständigkeit, die Effizienz bzw. die Effektivität und die Bedeutung der Sicherheitskennzahl. Die Beispiele dienen lediglich als Anhaltspunkte und sollen durch die, für eine Organisation passenden, im Rahmen eines Definitionsprozesses entwickelten, Metriken ersetzt bzw. verfeinert werden (vgl. [CSS+08, S. A1 ff.]). Die Bedeutung der in der Spalte „SP 800-53“ aufgelisteten Nummern der Kontrollen wird in der Tabelle 6 erläutert.

- Die Implementierungskennzahlen spiegeln den Umsetzungsfortschritt von Sicherheitsprogrammen, Sicherheitsmaßnahmen, Policies und Prozeduren wider. Als Beispiel für die Implementierungskennzahlen kann der prozentuale Anteil von Systemen mit genehmigten Sicherheitsplänen oder Systemen mit einer ordentlichen Konfiguration der Passwort-Policies genannt werden.

- Die Kennzahlen zur Messung der Effektivität bzw. Effizienz sollen die Korrektheit der Umsetzung von Sicherheitsmaßnahmen wiedergeben. Die Effektivität steht dabei für die „Robustheit“ der Maßnahmen, und die Effizienz reflektiert die zeitliche Komponente. Als Beispiel für die Effektivität kann die Anzahl von Sicherheitsvorfällen aufgrund von falsch konfigurierten Zugangskontrollen genannt werden. Unter den Effizienzbegriff würde beispielsweise der prozentuale Anteil von Systemen fallen, die von der regelmäßigen Wartung nicht erfasst werden.

- Die die Bedeutung von Sicherheitsmaßnahmen widerspiegelnden Kennzahlen sind organisationsspezifisch und hängen von den Zielen der Organisation ab. Als Beispiel wird das Niveau des öffentlichen Vertrauens in die Sicherheitsmaßnahmen der Institution genannt. Auch die Kostenvermeidung in Folge von Sicherheitsmaßnahmen wird als Beispiel angegeben.

CNTL NO.	Control Name	CNTL NO.	Control Name
AC-2	Account Management	IR-6	Incident Reporting
AC-3	Access Enforcement	MA-2	Controlled Maintenance
AC-17	Remote Access	MA-6	Timely Maintenance
AT-3	Security Training	PE-6	Monitoring Physical Access
AU-6	Audit Review, Analysis and Reporting	PL-4	Rules of Behavior
CA-5	Plan of Action and Milestones	PS-3	Personnel Screening
CA-6	Security Authorization	RA-5	Vulnerability Scanning
CM-2	Baseline Configuration	SA-2	Allocation of Resources
CM-3	Configuration Change Control	SA-4	Acquisitions
CP-4	Contingency Plan Testing and Exercises	SC-13	Use of Cryptography
IA-2	Identification and Authentication (Organizational Users)	SI-2	Flaw Remediation

Tabelle 6.: Erläuterung zu den Sicherheitsmaßnahmen nach NIST 800-53: Die Übersicht enthält als Ergänzung zu der Tabelle 5 die den Nummern der Kontrollen entsprechenden Bezeichnungen nach NIST 800-53 (vgl. [RSK+10]).

In NIST 800-55 wird eine prozessorientierte Struktur für die Betrachtung von Sicherheitsmaßnahmen vorgeschlagen, die aus den folgenden Komponenten besteht: Identifikation und Definition der Ziele sowie Entwicklung spezifischer Messbarkeitskriterien. Der Prozessbestandteil „Identifikation und Definition“ sieht die Ermittlung von Stakeholder-Gruppen und Zielen vor; die Sicherheitspolicies und Prozeduren werden betrachtet, um anschließend die potenziellen Datenquellen für die Metriken zu begutachten. Im zweiten Prozessschritt werden die Kennzahlen für die drei o. g. Arten von Sicherheitskennzahlen definiert.

Die Abbildung 19 auf der Seite 211 veranschaulicht die beschriebenen Prozessschritte (vgl. [CSS+08, S. 24 ff.]).
Angesichts der beschriebenen prozessorientierten Ansatzes bei der Auswahl der Maßnahmen wird die Frage nach konkreten Möglichkeiten, die Sicherheitsinvestitionen zu bewerten, in der NIST-Publikation nur kurz behandelt (vgl. [CSS+08, S. 29 f.]). Der Anhang A enthält einige potenzielle Sicherheitsmetriken, die in der Tabelle 5 zusammengefasst sind.

A.1.5. BSI IT-Grundschutz

Die BSI IT-Grundschutz-Kataloge werden vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegeben und stellen eine Dokumentensammlung dar. Das gesetzte Ziel dieser Sammlung ist die Vermeidung, Erkennung und Bekämpfung sicherheitsrelevanter Vorfälle in den IT-Umgebungen. Ein standardmäßiges Sicherheitsniveau soll durch Basissicherheitsmaßnahmen erreicht werden, die sich in infrastrukturelle, organisatorische, personelle und technische Kategorien einteilen. Zur Integration der ISO-Normvorgaben sind die Empfehlungen des BSI zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen und Maßnahmen in den sogenannten BSI-Standards zusammengefasst:

- 100-1: Managementsysteme für Informationssicherheit (ISMS) [bsi08a]
- 100-2: IT-Grundschutz-Vorgehensweise [bsi08b]
- 100-3: Risikoanalyse auf der Basis von IT-Grundschutz [bsi08c]
- 100-4: Notfallmanagement [bsi08d]

Der erste BSI-Standard (Managementsysteme für Informationssicherheit) ist kompatibel zum ISO 27001-Standard und enthält Empfehlungen anderer Standards der ISO 2700X-Reihe (s. a. Abschnitt A.1.1 „ISO-Normenreihe (ISO 2700X)“). Ein ausführlicher Vergleich der beiden Rahmenwerke zur Informationssicherheit befindet sich in [bsi11e] (vgl. [Fra10]). Die Auswahl und die Anpassung der Sicherheitsmaßnahmen werden im zweiten BSI-Standard (IT-Grundschutz-Vorgehensweise) angesprochen. Dabei tritt die Angemessenheit einer Maßnahme in der Vordergrund: Diese leitet man aus den Kriterien Wirksamkeit (Effektivität), Eignung (praktische Umsetzbarkeit), Praktikabilität (leichte Verständlichkeit und Anwendbarkeit), Akzeptanz und Wirtschaftlichkeit ab. Es wird nicht ausgeführt, wie die genannten Kriterien geprüft werden können (vgl. [bsi08b, S. 63 f.]). Im dritten BSI-Standard (Risikoanalyse auf der Basis von IT-Grundschutz) wird die von dem BSI empfohlene Vorgehensweise zur Risikoanalyse beschrieben. Diese bietet sich an, wenn die Organisation bereits mit IT-Grundschutz arbeitet und versucht, die Risikoanalyse möglichst fließend an die IT-Grundschutzanalyse anzubinden. Der Ansatz richtet sich u. a. an die Organisationen mit einem (sehr) hohen Schutzbedarf in mindestens einem der drei Grundwerte: Vertraulichkeit, Integrität oder Verfügbarkeit. Die

Abbildung 20 veranschaulicht den Zusammenhang zwischen dem Basis-IT-Grundschutz und der Risikoanalyse.

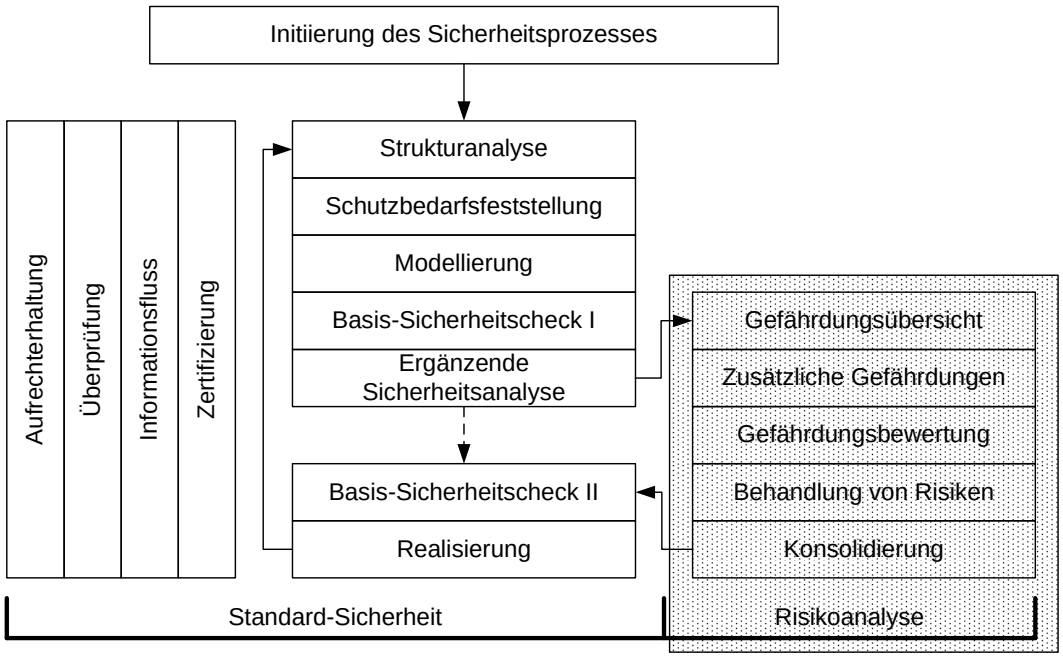

Abbildung 20.: Risikoanalyse nach dem BSI-Standard 100-3 als Bestandteil des Sicherheitsprozesses (vgl. [bsi08c, S. 5]): Die Risikoanalyse bietet sich besonders dann an, wenn die Organisation bereits mit IT-Grundschutz arbeitet, und ein erweiterter Sicherheitsbedarf festgestellt wird.

Die für die Entscheidung über die Umsetzung bestimmter Maßnahmen maßgebliche Eintrittswahrscheinlichkeit von Ereignissen wird vom BSI als eine subjektive und schwer zu ermittelnde Größe identifiziert. Aus diesem Grund wird diese nur indirekt anhand der Identifikation und Bewertung von Gefährdungen ermittelt. Die Risikoanalyse beginnt mit der Erstellung einer *Gefährdungsübersicht*, wobei die Bedrohungen, Schwachstellen und Risiken nicht separat untersucht werden. Als Nächstes empfiehlt der BSI, die Eigenschaften Vertraulichkeit, Integrität und Verfügbarkeit für die relevanten Zielobjekte zu bewerten und die relevanten Gefährdungen aus den Gefährdungskatalogen pro Zielobjekt aufzulisten. Unter den *zusätzlichen Gefährdungen* werden solche Gefährdungen verstanden, die für die untersuchten Objekte gelten und keine expliziten Bestandteile der Gefährdungskataloge sind.

Im Rahmen der nun folgenden *Bewertung der Gefährdungen* wird für jedes Zielobjekt einzeln empirisch untersucht, ob die (getroffenen) Standard-Sicherheitsmaßnahmen einen verlässlichen Schutz gegen alle Aspekte der Gefährdungen bieten. Die dabei zu verwendenden Prüfkriterien sind die Vollständigkeit, die Mechanismenstärke und die Zuverlässigkeit. Die von den Maßnahmen nicht zuverlässig abgedeckten Gefährdungen werden zu *Risiken*, für deren *Behandlung* Risikoreduktion, -vermeidung, -übernahme oder -transfer als Methoden zur Verfügung stehen. Das Ziel der *Konsolidierung des Sicherheitskonzeptes* ist dessen Bereinigung. Als Vorstufe werden die Sicherheitsmaßnahmen auf ihre Eignung zur Abwehr von Risiken, ihr gegenseitiges Zusammenwirken, die Benutzer-

freundlichkeit sowie die Angemessenheit untersucht. Nach der durchgeführten Konsolidierung sollte ein möglichst stimmiger und effizienter bzw. effektiver Maßnahmenkatalog entstehen (vgl. [bsi08c, S. 9 ff.]). Die hohe Anzahl von Einzelgefährdungen[22] erschwerte die Durchführung der Risikoanalyse. Aus diesem Grund fasste BSI die spezifischen Gefährdungen in 46 generischen Gefährdungen zusammen. Diese sogenannten elementaren Gefährdungen wurden mit der zwölften Ergänzungslieferung der BSI IT-Grundschutz-Kataloge veröffentlicht (vgl. [bsi11a], [bsi11b]).

A.1.6. Weitere Standards und Messansätze der Informationssicherheit

Die wichtigsten Merkmale einer Reihe weiterer Ansätze zur Messung der Informationssicherheit und der Wirksamkeitsbewertung von Sicherheitsmaßnahmen werden im Folgenden beschrieben.

A.1.6.1. Open Source Security Testing Methodology Manual (OSSTMM)

Das Open Source Security Testing Methodology Manual wurde erstmals im Jahr 2001 von der ISECOM[23] veröffentlicht und ist ein Standard zur Durchführung technischer Audits. Seit Dezember 2010 liegt OSSTMM in der dritten Version[24] vor und enthält neben einer einheitlichen Test-Methodik die Testabschnitte (Channels) für die physikalischen, menschlichen, drahtlosen, telekommunikations- und datennetzwerkspezifischen Komponenten einer Infrastruktur. OSSTMM beschreibt, welche Vorbereitungen für die Sicherheitstests durchzuführen sind, wie die Tests absolviert werden müssen, und wie die Testergebnisse zu bewerten sind.
Im Bereich der Sicherheitsmetriken arbeitet OSSTMM mit der sogenannten Attack Security Surface Metrik, die in RAV-Einheiten[25] gemessen wird. Dabei bedient man sich einer Delta-Methode für die Bewertung der Angriffspotenziale, um die sicherheitstechnische Entwicklung einer Infrastruktur im zeitlichen Verlauf verfolgen zu können. Die aktuelle OSSTMM-Version untersucht verstärkt solche Assets, die einen Wert für den Angreifer bzw. für den Angegriffenen darstellen. Die Herleitung des Sicherheitsniveaus erfolgt mithilfe des sogenannten Attack Surface Security Metrics-Kalkulators z. B. in Form eines Excel-Templates. Nach der Eingabe mehrerer Werte, die beispielsweise die Dienste, ihre Sicherheitslücken und die Sicherheitsmaßnahmen berücksichtigen, erhält man einen

[22] In der 12 Ergänzungslieferung des BSI vom August 2011 sind ca. 450 Einzelgefährdungen aufgelistet.

[23] Institute for Security and Open Methodologies.

[24] Stand Dezember 2011: Die OSSTMM-Releases 3.1 und 3.2 haben den Beta-Status und werden daher im Folgenden nicht berücksichtigt.

[25] Risk Assessment Value.

RAV-Wert, der mit den Werten anderer Organisationen verglichen werden können soll (vgl. [Her10, S. 62 ff.]).

A.1.6.2. Operationally Critical Threat Asset and Vulnerability Evaluation (OCTAVE)

Diese an der Carnegie Mellon Universität in Zusammenarbeit mit dem CERT/CC[26] entwickelte Methode zur Risikobewertung ist frei verfügbar und stützt sich auf Checklisten, Formblätter und Moderationsleitfäden. Der Ansatz setzt auf die Aktivierung des unternehmenseigenen Know-hows und auch die Einbeziehung externer Unterstützung in Form von Expertenwissen; insbesondere größere Organisationen[27] gehören zu der Zielgruppe der Anwender. Das OCTAVE-Framework eignet sich für den Einsatz in Einrichtungen des Gesundheitswesens (vgl. [AJ10, S. 296 f.], [Woo06, S. 13 f.]) und sieht eine Weiterentwicklung in Richtung ISO 27001 vor (s. a. Abschnitt A.1.1 „ISO-Normenreihe (ISO 2700X)“).
Nach der Durchführung einer Risiko- und Bedrohungsanalyse liefert OCTAVE eine strategische Beurteilung und Planung für die Informationssicherheit. Im Mittelpunkt des OCTAVE-Frameworks steht die betriebswirtschaftliche und nicht die technische Sichtweise. Die von OCTAVE vorgeschlagene Vorgehensweise ist phasenorientiert und sieht in der untersuchten Version 2 drei Phasen vor (vgl. [AD01]):

- Phase 1
  - Process 1: Identify Senior Management Knowledge
  - Process 2: Identify Operational Area Management Knowledge
  - Process 3: Identify Staff Knowledge
  - Process 4: Create Threat Profiles
- Phase 2
  - Process 5: Identify Key Components
  - Process 6: Evaluate Selected Components
- Phase 3
  - Process 7: Conduct Risk Analysis
  - Process 8, Workshops: Develop and Select Protection Strategy

Die für diesen Arbeitsabschnitt besonders relevante Risikoanalyse wird als Prozess 7 der dritten Phase beschrieben. Stark vereinfacht lässt sich das empfohlene Verfahren in die Schritte Risikoidentifizierung, Definition der Messbarkeitskriterien mit der anschließenden Zuweisung von Eintrittswahrscheinlichkeiten unterteilen. Das Prinzip ist somit mit der Risikomatrix vergleichbar (vgl. [AD01, Vol. 9a S. I7-5 ff.]).

[26] CERT Coordination Center.

[27] Ab 300 Personen.

A.1.6.3. CCTA Risk Analysis and Management Method (CRAMM)

Das CRAMM-Framework [sie12] wurde ursprünglich von der britischen Behörde CCTA[28] entwickelt und sieht eine dreistufige Vorgehensweise für die Identifikation und Analyse von Risiken und für die anschließende Ermittlung von Gegenmaßnahmen vor.
Für die Datensammlung werden Meetings, Interviews sowie strukturierte Fragebögen verwendet. Nach der Asset-Identifizierung und -Bewertung bedient sich CRAMM für die Durchführung der anschließenden Risiken- und Risikoanfälligkeitsanalysen eines Tools mit einer hinterlegten Risikodatenbank. Die gewählte Sicht orientiert sich vor allem am Management und weniger an den technischen Fragestellungen. Die bereits erwähnte Risikodatenbank spielt bei der Auswahl der durchzuführenden Sicherheitsmaßnahmen eine wichtige Rolle. Die Maßnahmen in der Datenbank werden hierarchisch, in Gruppen geordnet und mit Prioritäten versehen hinterlegt, was die Identifikation der wirksameren Sicherheitsmaßnahmen erleichtern soll (vgl. [sie12]).

A.1.6.4. SIEM-Systeme

Der Begriff „Security Information and Event Management“ (SIEM) steht für eine Vielzahl von Ansätzen, mit deren Hilfe ein Überblick über die Sicherheitsinfrastruktur einer Organisation an einer zentralen Stelle ermöglicht werden soll. Dafür werden die sicherheitsrelevanten Informationen mehrerer Systeme wie beispielsweise Firewalls, IDS und Virenscanner gesammelt, ausgewertet und den Administratoren in aggregierter Form zur Verfügung gestellt. Die SIEM-Systeme zeichnen sich durch ihre Fähigkeiten zur Datensammlung und -korrelation sowie längerfristigen Datenaufbewahrung aus. Neben der Benachrichtigungsfunktion unterstützt die Mehrheit der aktuellen SIEM-Lösungen die Überwachung der Einhaltung von Sicherheits- und Governance-Richtlinien mithilfe von sogenannten Informationsanalyse-Dashboards.
Einige der bekanntesten SIEM-Produkte sind Novell Sentinel, RSA enVision, IBM Tivoli Security Information and Event Manager, ArcSight ESM, LogLogic ST and LX, netForensics nFX Cinxi/SIM One, Check Point Eventia, eIQ Networks SecureVue, CA eTrust Security Command Center, Symantec (NSDQ:SYMC) SIM appliance, SenSage Enterprise Security Analytics (ESA) und Q1 Labs QRadar.

A.1.6.5. SAS-Systeme

Unter dem Begriff „SAS“ werden die sogenannten Security Analysis Systeme bzw. Vulnerability Systeme zusammengefasst. Die Hauptaufgabe solcher Systeme ist die Ermittlung vorhandener Sicherheitslücken in der Systemkonfiguration. Weitere Einsatzgebiete der SAS-Systeme sind die Ermittlung bzw. Ableitung des Sicherheitsniveaus aus den Testergebnissen und die Report-Generierung.

[28] Central Computer and Telecommunications Agency.

Sowohl modellbasierte und als auch imitative Ansätze[29] finden in den SAS-Systemen ihre Verwendung. Die generische Architektur eines SAS-Systems ist in [KS05, 314 f.] ausführlich dargestellt. Einige der bekanntesten SAS-Systeme bzw. Vulnerability Scanner sind NetRecon, bv-Control for Internet Security (HackerShield), Retina CS, CyberCop Scanner und Nessus Security Scanner.

A.1.6.6. HIPAA Security Series

Im Rahmen des amerikanischen Gesetzes „Health Insurance Portability and Accountability Act“ (HIPAA) werden Mechanismen für die Gewährleistung der Sicherheit und Vertraulichkeit von zum Gesundheitswesen gehörigen Informationen festgelegt: In § 164.308(a)(1)(ii)(A) wird die Durchführung einer Risikoanalyse gefordert. [Dep03, S. 8377]: *„Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.“* Die Notwendigkeit der Umsetzung von Sicherheitsmaßnahmen, um das Risikoniveau ausreichend zu senken, wird in § 164.308(a)(1)(ii)(B) festgehalten: *„Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).“*
Im Zusammenhang mit HIPAA sind die vom CMS (Centers for Medicare & Medicaid Services) herausgebrachten Empfehlungen zur Umsetzung der als „Security Rule“ bekannten „Security Standards for the Protection of Electronic Protected Health Information“ von Interesse. Die „Security Series“ der CMS besteht aus insgesamt sieben Dokumenten (vgl. [hip11]); die sechste Publikation „Basics of Risk Analysis & Risk Management“ befasst sich mit der Risikoanalyse und dem Risikomanagement. Die in [DHH05] unterbreiteten Risikoanalyseempfehlungen lehnen sich an den NIST-Standard 800-30 „Risk Management Guide for Information Technology Systems“ und beschreiben insgesamt acht Schritte zur Durchführung von Risikoanalysen (vgl. [SGF02, S. 10 ff.]):

1. Abgrenzung des Analyseobjektes,
2. Datensammlung,
3. Identifizierung und Dokumentation von Bedrohungen und Verwundbarkeiten,
4. Prüfung der vorhandenen Sicherheitsmaßnahmen,
5. Ermittlung der Wahrscheinlichkeit für den Bedrohungseintritt,
6. Ermittlung des potenziellen Schadens des Bedrohungseintritts,
7. Ermittlung des Risikoniveaus und
8. Identifizierung der Sicherheitsmaßnahmen und Vervollständigung der Dokumentation.

Das Risikomanagement nach [DHH05] besteht aus drei Elementen, die jeweils nur kurz erläutert werden:

1. Entwicklung und Implementierung eines Risikomanagementplanes,
2. Implementierung der Sicherheitsmaßnahmen und
3. Bewertung und Pflege der Sicherheitsmaßnahmen.

[29] Beispielsweise Angriffsbäume, graphenbasierte Ansätze etc.

Bei der Ermittlung der Wahrscheinlichkeit einer Bedrohung erfolgt die Empfehlung, die in den vorhergehenden Schritten gesammelten Informationen auszuwerten und eine Einteilung in die Kategorien „hoch“, „mittel“ und „niedrig“ vorzunehmen. Für die Bestimmung des potenziellen Schadens wird die Verwendung von sowohl qualitativen als auch quantitativen Ansätzen empfohlen, ohne jedoch die dahinter stehenden Methodiken genauer zu beschreiben (vgl. [DHH05, S. 10 f.], s. a. Abschnitt A.1.4 „NIST 800-X (Special Publications)“).

A.1.6.7. Circle of Security

Der „Circle of Security“-Ansatz [Nor00] beinhaltet ein wiederholtes Durchlaufen von drei Phasen des Sicherheitsprozesses: Protection, Detection und Response. Dadurch soll eine kontinuierliche Verbesserung des Sicherheitsniveaus gewährleistet werden. Im Konzept wird vermerkt, dass der „Circle of Security“-Ansatz nicht neu ist, und es wird auf das „Lifecycle Security“-Modell der im Jahr 2000 von Symantec Corporation übernommenen Axent Technologies, Inc. verwiesen. Das „Lifecycle Security“-Modell von Axent ist in der Abbildung 21 dargestellt (vgl. [axe99, S. 16]).

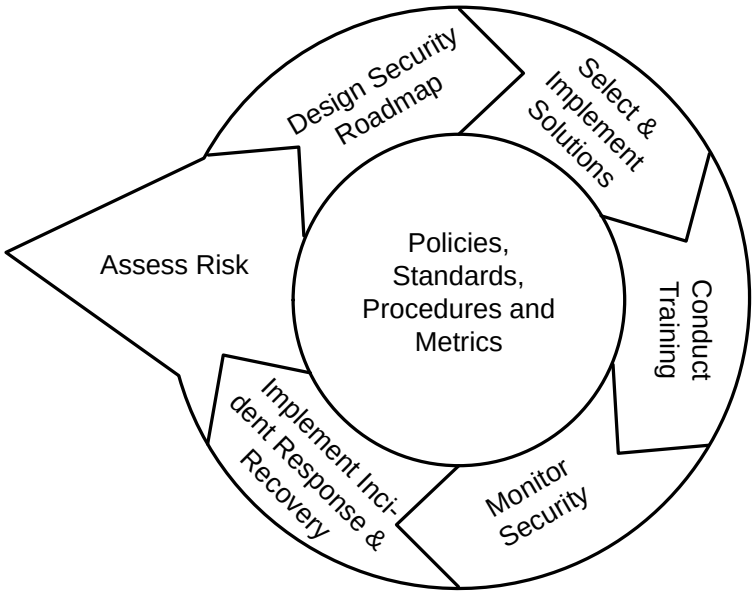

Abbildung 21.: Das Model „Lifecycle Security“ von Axent Technologies, Inc. wurde mit der Zielsetzung entwickelt, die Sicherheitsbedürfnisse systematisch zu erfüllen. Die Methodik soll den Kunden in den Phasen Entwurf, Implementierung, Wartung und Modifikation von Sicherheitsarchitekturen unterstützen.

Mithilfe des „Lifecycle Security“-Modells sollen die Unternehmensrisiken aktiv bekämpft werden. Die maßgeblichen Sicherheitsrichtlinien und die gesetzlichen bzw. regulatorischen Anforderungen sollen ermittelt werden. Anschließend sollen die bestehenden Verwundbarkeiten herausgefunden und die Wirksamkeit bestehender Maßnahmen gegen diese Verwundbarkeiten untersucht werden. Beim Feststellen von inakzeptablen Risiken sollen die Sicherheitsmaßnahmen überdacht und weiterentwickelt werden (vgl. [axe99]).

Im Bereich des Risikomanagements werden die in [SHF01][30] vorgestellten Aufbauprinzipien der IT-Sicherheit[31] verwendet. Diese NIST-Publikation enthält eine Beschreibung grundsätzlicher Prinzipien sowie deren Bedeutung während der einzelnen fünf Phasen des Systemlebenszyklus[32] (vgl. [SG96, S. 22 ff.]).

A.1.6.8. SSE-CMM, ISSEA

Das von der International Systems Security Engineering Association (ISSEA) entwickelte „Systems Security Engineering Capability Maturity Model“ (SSE-CMM) diente als Basis für den ISO-Standard ISO/IEC 21827[33]. Die Zielsetzung des SSE-CMM-Modells besteht in der Erhöhung der Reife der Sicherheitsengineering-Prozesse. SSE-CMM beschreibt die notwendigen Eigenschaften des Security Engineering-Prozesses einer Organisation und berücksichtigt dabei folgende Punkte:

- Produkt- bzw. Systemlebenszyklus,
- Organisation inklusive Management,
- Überschneidungen mit anderen Systemen, Soft- und Hardware, menschlichen Komponenten etc.,
- Wechselbeziehungen mit anderen Organisationen.

Insgesamt sind im SSE-CMM 22 Prozesse (PA01 - PA22) definiert, die der Entwicklung einer Sicherheitsmetrik bedürfen, um damit das Reifegrad messen zu können. Die für die Metrik-Entwicklung verwendete Methodik weist diverse Übereinstimmungen mit der in NIST 800-55 [CSS+08] verwendeten Systematik auf (vgl. [CYK04], s. a. Abschnitt A.1.4 „NIST 800-X (Special Publications)“). Die für das Sicherheits- und Risikomanagement besonders relevanten Themen sind im sechsten Kapitel „Security Base Practices“ [iss03] zusammengefasst und berücksichtigen folgende Punkte:

PA01: Administration der Sicherheitskotrollen,
PA02: Schätzung der Auswirkungen,
PA03: Schätzung der Sicherheitsrisiken,
PA04: Schätzung der Bedrohungen,
PA05: Schätzung der Verwundbarkeiten,
PA06: Erstellung des Sicherheitsnachweises,[34]

[30] Zum Zeitpunkt der [Nor00]-Publikation lag das Dokument als Entwurf vor.

[31] Engineering Principles for IT-Security.

[32] Zum Beispiel [SHF01, S. 6 f.]: „Principle 1: Establish a sound security policy as the „foundation“ for design. (...) Principle 2: Treat security as an integral part of the overall system design.“

[33] „ISO/IEC 21827 : Information Technology : Security Techniques : Systems Security Engineering : Capability Maturity Model (SSE-CMM).“

[34] Build Assurance Argument.

PA07: Koordination der Sicherheit,
PA08: Sicherheitsmonitoring,
PA09: Kommunikation der Sicherheit,
PA10: Spezifizierung der Sicherheitsbedürfnisse,
PA11: Verifizierung und Validierung der Sicherheit.

Die Prozesse der Risikoschätzung PA03, der Ermittlung von Bedrohungs- und Verwundbarkeitsinformationen (PA04, PA05) sowie der Ermittlung der möglichen Auswirkungen (PA02) bilden zwar separate Abschnitte, hängen jedoch unmittelbar zusammen. Das Ziel des entsprechenden CMM-Prozesses besteht in der Ermittlung von Kombinationen aus Gefahr, Verwundbarkeit und Auswirkung[35] mit einem signifikanten Gefährdungspotenzial. Die dabei ermittelten Informationen dienen als Ausgangsbasis für die Definition der Sicherheitsbedürfnisse (PA10) und für die Kommunikation der Sicherheit (PA09) (vgl. [iss03, S. 134]).

A.2. Generische Empfehlung für die Gestaltung einer Sicherheitsleitlinie

Die bestimmende Rolle bei der Ausgestaltung von Sicherheitsmaßnahmen spielt die Ebene der Sicherheitspolitik, die im Modell der Sicherheitspyramide nach [Mül11] als die oberste, richtungweisende Ebene verstanden wird (s. a. Abschnitt C.5). Eine Sicherheitsleitlinie fasst die Aussagen der Sicherheitspolitik zusammen und verfolgt die Absicht, Bemühungen einzelner Forschungsnetzbereiche im Hinblick auf die Erreichung eines gemeinsamen Ziels zu konsolidieren: das Vorantreiben der medizinischen Forschung unter Berücksichtigung der maßgeblichen gesetzlichen Rahmenbedingungen. Die Leitlinie bildet die Grundlage für die Planung und Umsetzung eines risikogerechten und angemessenen Sicherheitsarchitekturkonzeptes. Die Leitlinie soll regelmäßig auf ihre Aktualität geprüft werden und als ein obligatorisch zu berücksichtigendes Element bei der Vertragsgestaltung gesehen werden (vgl. [PB06]). Behandelt man die Sicherheit als einen kontinuierlichen Prozess, bei dem die Zielkonflikte sowie eine unsystematische Vorgehensweise bzw. falsche Methodik vermieden werden müssen, so erhält die Sicherheitsleitlinie eine große Bedeutung (vgl. [bsi11d, M 2.192], [PB06]).

- Das primäre Ziel eines medizinischen Forschungsnetzes besteht in der Optimierung der Kommunikation zwischen Wissenschaftlern, behandelnden Ärzten und Patienten.
- Neben der Gewinnung wissenschaftlich wertvoller Erkenntnisse steht eine möglichst geringe Beeinträchtigung des Patienten durch den Behandlungsprozess sowie die Wiederherstellung der individuellen Gesundheit des Patienten unter Berücksichtigung maßgeblicher gesetzlicher Anforderungen an oberster Stelle.

[35] Threat, Vulnerability, Impact.

- Obwohl eine absolute Sicherheit erstrebenswert ist, kann eine solche nicht realisiert werden. Das Risiko einer Kompromittierung des Forschungsnetzes muss durch die Einhaltung eines durchdachten und für alle Parteien zumutbaren Sicherheitskonzeptes minimiert werden.

- Die Teilnehmer des Forschungsnetzes sollen durch die Umsetzung der Sicherheitsmaßnahmen nicht unnötig belastet werden. Sicherheitsmaßnahmen sollen die Arbeit des Netzes nicht behindern.

- Das Forschungsnetz soll nicht nur gegen Attacken externer Angreifer immun sein, sondern auch Insiderangriffe abwehren können.

- Das an § 3a BDSG angelehnte Minimalprinzip gilt als Leitsatz: Im Rahmen der medizinischen Forschungsnetze wird versucht, so wenig Patientendaten wie für eine sinnvolle Forschung notwendig sind, zu erheben und zu nutzen (s. a. Anhang E „Auszüge aus BDSG und StGB“).

- Für alle Dienste des Forschungsnetzes sollen die Prinzipien des generellen Verbots sowie der minimalen Rechte und Dienste gelten. Diese Prinzipien besagen, dass alle nicht explizit erlaubten Transaktionen verboten sind; nur die für die Durchführung der Aufgaben notwendigen Rechte (und nicht mehr) werden gewährt. Einem Forschungsnetzteilnehmer werden nur die tatsächlich von ihm benötigten Dienste zur Verfügung gestellt. Forschungsnetzteilnehmer dürfen ihrerseits die ihnen verfügbaren Ressourcen nur in dem ihnen erlaubten Umfang nutzen. Bei der Durchführung von besonders sicherheitskritischen Operationen wird außerdem das Vier-Augen-Prinzip gelebt. Bei der Erhebung und Zur-Verfügung-Stellung von Daten ist das Prinzip der Datensparsamkeit zu beachten.

- Alle Teilnehmer des Forschungsnetzes sollen mit den ihnen zur Verfügung gestellten Ressourcen verantwortungsvoll umgehen.

- Ein durchdachtes Versionierungskonzept und Regeln für das Testen und Inproduktionsnahme von Applikationsversionen sollen die Verfügbarkeit und Qualität der vom Forschungsnetz angebotenen Dienste steigern.

- Um die benötigte Nachvollziehbarkeit zu gewährleisten, müssen alle sicherheitsrelevanten Ereignisse aufgezeichnet werden. Die Aufzeichnungen müssen in ihrer Art angemessen und nicht veränderbar sein, sie müssen genügend Informationen enthalten, um die Sicherheitsvorfälle bewerten zu können.

- Das erwünschte Sicherheitsniveau kann nur erreicht werden, wenn die Sicherheitsstandards von allen organisatorischen Bestandteilen und Teilnehmern des Forschungsnetzes nicht nur akzeptiert, sondern auch gelebt werden.

- Der Ausschuss Datenschutz soll den Sicherheitsmanagementprozess aktiv unterstützen.
- Nur mit der permanenten Weiterentwicklung der Sicherheitsstandards und der Einhaltung von Qualitätsstandards können die Risiken für das Forschungsnetz rechtzeitig erkannt und Gegenmaßnahmen ergriffen werden.

A.3. Qualitative schutzbedarfsorientierte Analyse der Forschungsnetzdienste

A.3.1. Zentrale Patientenliste

Die zentrale Patientenliste ist der Ort des Identitätsmanagements. Sie ist das Kernstück eines medizinisches Forschungsnetzes, das besonders geschützt werden muss. Nach der generischen Datenschutzlösung der TMF wird die Patientenliste örtlich und technisch in zwei Teildatenbanken aufgebrochen, die sich über den *PID* verknüpfen lassen (vgl. [RDSP06]). Die beiden Teildatenbanken (*IDAT* und *MDAT*) enthalten *PID*, die bei Verknüpfung von Datensätzen beider Datenbanken als Schlüssel verwendet werden. Im generischen Datenschutzkonzept wird empfohlen, die Administration der beiden Datenbanken von zwei organisatorisch unabhängigen Administrationsteams durchführen zu lassen (vgl. [DC06]).

Zentrale Patientenliste						
Authentizität	Integrität	Konformität	Robustheit	Verbindlichkeit	Verfügbarkeit	Vertraulichkeit
3	3	5	2	3	1	5

Tabelle 7.: Bewertung der Sicherheitskriterien für die zentrale Patientenliste

- Die *Authentizität* als Sicherheitskriterium[36] steht bei der zentralen Patientenliste zwar nicht an vorderster Stelle; die Verletzung dieses Sicherheitskriteriums kann jedoch zu einem immensen Schaden für das Forschungsnetz führen. So kann der Zugriff auf eine „unechte“ Patientenliste die Forschungsergebnisse beeinflussen bzw. bei der Rückführung von Ergebnissen können falsche Patienten angesprochen werden. Der wohl größte Schaden könnte jedoch entstehen, wenn es den Angreifern gelingen würde, die Forschungsnetzteilnehmer oder -systeme dazu zu bringen, die Änderungen/Neueinträge etc. in einer untergeschobenen Patientenliste durchführen zu lassen. Dies würde eine Offenlegung von Patientendaten zur Folge haben.
- Die Verletzung der *Integrität* einer Patientenliste z. B. durch Manipulation kann zu der Verfälschung von Forschungsergebnissen führen. Die absichtliche Variante dieser

[36]Die Qualifizierung von Sicherheitskriterien kann dem Anhang D entnommen werden.

Sicherheitsverletzung ist zwar wenig wahrscheinlich, könnte jedoch in Form von technischen und menschlichen Fehlern, Fehlkonzeptionen etc. eintreten. Eine Folge dieser Sicherheitsverletzung könnte eine temporäre Einstellung des Forschungsbetriebs bis zur endgültigen Störungsbehebung sein.

- Die Verletzung der *Konformität* im Hinblick auf die geltenden Normen, Gesetze etc. durch die Patientenliste kann zu der Einstellung des Forschungsnetzbetriebs, zur Beschlagnahme der Forschungsdatenbank und zu Klagen diverser Betroffener führen.

- Die *Robustheit* der Patientenliste spielt dann eine Rolle, wenn die Forschungsnetzdaten im Behandlungszusammenhang verwendet werden. Im üblichen Forschungsnetzbetrieb ist die Verletzung der Robustheit, die zu kurzfristigen Ausfällen führt, i. d. R. akzeptabel. Verlust der Integrität, Authentizität etc. als Folgen dieser Sicherheitsverletzung können dagegen nicht geduldet werden.

- Die Verletzung der *Verbindlichkeit* gelieferter Informationen kann zur Verfälschung der Forschungsergebnisse führen. Große Schäden können dann erwartet werden, wenn infolgedessen Patienten falsch beraten oder behandelt werden.

- Die *Verfügbarkeit* der Patientenliste spielt nur im Behandlungszusammenhang eine wichtige Rolle. Im Forschungszusammenhang führen die kurz- bis mittelfristigen Ausfälle der Patientenliste zu keinen gravierenden Schadensszenarien.

- Die *Vertraulichkeit* ist das wohl wichtigste Sicherheitskriterium für die Patientenliste. Es sind mehrere Szenarien denkbar, in denen bereits die Bruchteile von Informationen zu einem erheblichen Schaden für das Forschungsnetz oder gar zur Einstellung des Forschungsnetzbetriebs führen können. So stellt z. B. bei sogenannten tabuisierten Krankheiten bereits die Zugehörigkeit eines Patienten zum Forschungsnetzbetrieb eine schützenswerte Information dar; die Veröffentlichung medizinischer Daten einer einzigen Person des öffentlichen Interesses kann zu irreparablen Imageschäden führen.

A.3.2. PID-Dienst

Der *PID*-Dienst ermöglicht einen verwechslungsfreien und fehlerlosen Zugang auf krankheitsbezogene Patienteninformationen für behandelnde Ärzte. Die Erzeugung von Patientenidentifikatoren (*PID*) erfolgt unter Vermeidung von Synonymen und Homonymen. Die erzeugten Zeichenketten sind eindeutig und nicht sprechend. Das Zurückrechnen von Patientendaten aus dem *PID* ist nicht möglich. Bei den folgenden Ausführungen wird ein zentraler *PID*-Dienst angenommen (vgl. [RDSP06]).
Der *PID*-Dienst kann vom Angreifer des Forschungsnetzes ausgenutzt werden. Da bereits die Tatsache, dass die Daten einer Person in einem Forschungsnetz aufgenommen wurden, eine schützenswerte Information ist, und der *PID*-Dienst für viele Forschungsnetzteilnehmer

PID-Dienst						
Authentizität	Integrität	Konformität	Robustheit	Verbindlichkeit	Verfügbarkeit	Vertraulichkeit
3	3	4	3	5	1	4

Tabelle 8.: Bewertung der Sicherheitskriterien für den PID-Dienst

verfügbar ist,[37] darf nicht angezeigt werden, ob bei einer *PID*-Anfrage ein neuer *PID* erzeugt oder ein bereits existierender *PID* angezeigt wird. Es dürfen auch keine Hinweise im Hinblick auf das Vorhandensein von Homonymen erfolgen, da ein Angreifer Daten ihm bekannter Personen eingeben könnte, um so das Vorhandensein einer bestimmten Person in der Patientendatenbank zu prüfen. Es sollte eine allgemeine Meldung angezeigt werden, die auf mehrere Ursachen zutreffen könnte. Eine eindeutige Vorgangsnummer sollte anschließend generiert und dem Benutzer angezeigt werden mit der Bitte, den *PID*-Helpdesk unter der Angabe dieser Nummer zu kontaktieren. Gleichzeitig sollte der Vorfall protokolliert[38] und auf potenziellen Missbrauch untersucht werden. Die *PID*-Datenbank ist somit als ein kritischer Bereich des Forschungsnetzes anzusehen. Denn außer identifizierenden Daten enthalten die *PID*-Tabellen u. a. die Zeitpunkte der ersten und der letzten *PID*-Anforderungen sowie Informationen über die anfordernden Stellen. Diese Daten lassen Rückschlüsse auf den Krankheitsverlauf und somit auf den Gesundheitszustand des Patienten zu. Auch die Erzeugung/Löschung von Synonymen könnte vom Angreifer ausgenutzt werden, um die Identitäten der Patienten zu ermitteln. Ein solcher Angriff ist jedoch weniger wahrscheinlich als ein Homonym-Missbrauch.

- Die Verletzung der *Authentizität* des *PID*-Dienstes könnte dazu führen, dass die Angreifer Einsicht in die vertraulichen Patientendaten bekommen. Dieses Szenario ist besonders bei einem Man-in-the-Middle-Angriff denkbar. Ein solcher Angriff ist relativ aufwendig und würde dem Angreifer Zugriff auf einige wenige Datensätze ermöglichen.

- Die *Integritätsverletzungen* des *PID*-Dienstes könnten zu der Verfälschung der Forschungsnetzdaten führen. Lang andauernde unbemerkte Verfälschungen/Manipulationen der *PID*-Ergebnisse könnten in verfälschten schwer zu korrigierenden Forschungsnetzdaten resultieren.

- Der *PID*-Dienst ist eines der Hauptbestandteile eines Forschungsnetzes. Seine *Konformität* zu den maßgeblichen gesetzlichen Regelungen ist die Voraussetzung für die Genehmigung/Aufrechterhaltung des Forschungsnetzbetriebs. Die Schnittstellen und

[37] Auch ein Dritter könnte den *PID*-Dienst missbrauchen, in dem er falsche Identität annimmt, um beispielsweise die Erzeugung eines Homonyms anzustreben.

[38] Patientendaten und Anforderer.

die Funktionalität des *PID*-Dienstes sind klar definiert und eingegrenzt. Die Nichteinhaltung von diversen geltenden Regelungen ist im Vergleich zu der Patientenliste wesentlich unwahrscheinlicher.

- Der *PID*-Dienst muss eine *Robustheit* gegen diverse technische oder menschliche Fehler besitzen. Der Versuch der Ausnutzung des *PID*-Dienstes zur Vorbereitung und Durchführung von Angriffen ist möglich.

- Die *PID*-Abfrageergebnisse sind maßgebend für die Qualität der Forschungsnetzdaten. Die Ergebnisse sollen nach Möglichkeit keine Synonyme und Homonyme enthalten. Die Ergebnisse sollen einen höchsten Grad von *Verbindlichkeit* aufweisen, insbesondere angesichts des Einsatzes des *PID*-Dienstes im Behandlungszusammenhang.

- Die *Verfügbarkeit* des *PID*-Dienstes hat insbesondere im Behandlungszusammenhang Relevanz, da der Dienst für eine eindeutige Identifizierung des Patienten und evtl. zum Abruf seiner Akte verwendet wird. Im Forschungsbetrieb ist die Verfügbarkeit des Dienstes von geringer Bedeutung und wird z. B. bei der Zurückführung von Forschungsergebnissen an den Patienten eingesetzt.

- Die *Vertraulichkeit* der Patientendaten hat die höchste Priorität. Die vom *PID*-Dienst gelieferten Ergebnisse dürfen keine Schlussfolgerungen auf die Zugehörigkeit eines Patienten zum Forschungsnetz erlauben. Um dies zu vermeiden, existiert eine Reihe von Maßnahmen (z. B. Verwendung sogenannter *TempIDs*, Nichtumkehrbarkeit des *PID* auf die Patientendaten, keine Speicherung von *TempIDs* etc. (vgl. [RDSP06])). Bei einer konsequenten Anwendung der genannten Maßnahmen ist das Missbrauchspotenzial durch eine Vertraulichkeitsverletzung des *PID*-Dienstes als gering einzuschätzen. Das Ausspähen von Patientendaten kann eine erhebliche Bedrohung für das Fortbestehen des Forschungsnetzes bedeuten.

A.3.3. Rückmeldung von Forschungsergebnissen

Die Rückmeldung von Forschungsnetzdaten an die im Behandlungsprozess Beteiligten erfolgt mit der Option zur eindeutigen Identifizierung der von den Forschungsergebnissen betroffenen Patienten. Bei der Bewertung der Kritikalität dieses Prozesses wird auf die Prozessbeschreibung nach [SSS06] zurückgegriffen. Der Prozess wird vom Forscher angestoßen, der sich an den Datentreuhänder wendet, der seinerseits den Datenbankbetreiber kontaktiert. Nach der Prüfung der Patienteneinwilligung erhält der behandelnde Arzt Informationen, die er an den Patienten weitergibt.

- Aufgrund der mehrstufigen Gestaltung des Vorgangs ist eine böswillige Einflussnahme auf den Prozess unwahrscheinlich. Selbstverständlich bleibt die Weitergabe

Rückmeldung von Forschungsergebnissen						
Authentizität	Integrität	Konformität	Robustheit	Verbindlichkeit	Verfügbarkeit	Vertraulichkeit
2	2	1	2	4	1	5

Tabelle 9.: Bewertung der Sicherheitskriterien für die Rückmeldung von Forschungsergebnissen

von falschen Informationen in betrügerischer Absicht möglich. Insbesondere ist die *Authentizität* von Informationen im letzten Prozessschritt (Arzt informiert den Patienten) schützenswert. Zu diesem Zeitpunkt besteht ein Vertrauensverhältnis zwischen den beiden Akteuren; die Überprüfung der Authentizität von Informationen wäre außerdem durch das Einholen von Meinungen weiterer Ärzte möglich.

- Eine Verletzung der *Integrität* dieses Dienstes kann zur negativen Einflussnahme auf die Patienten führen, indem z. B. Falschinformationen über die Behandlungsmöglichkeiten für bestimmte Krankheiten an die Patienten mit betrügerischer Absicht geleitet werden. Grundsätzlich ist das Missbrauchspotenzial dieses Dienstes (insbesondere am Anfang des Prozesses) als gering einzuschätzen, auch wenn die unerwünschte Patientenreidentifizierung nicht komplett ausgeschlossen werden kann.

- Die *Konformitätsverletzungen* des Vorgangs sind unwahrscheinlich, da der gesamte Prozess durch mehrere Vertragswerke (Einwilligung und Einverständniserklärung des Patienten, Teilnahmeantrag des Forschers etc.) abgesichert ist. Konformität des letzten Prozessschrittes wird durch den Behandlungszusammenhang abgesichert.

- Die *Robustheit* des Verfahrens ist vernachlässigbar.

- Die große Bedeutung der *Verbindlichkeit* der an die Patienten kommunizierter Informationen wird durch die Natur der Inhalte begründet. In vielen Fällen werden diese Informationen über die Lebensqualität eines Patienten oder gar sein Leben entscheiden. Die negativen Folgen der Verbindlichkeitsverletzung werden durch das Know-how des Arztes abgemildert, der aufgrund seiner Erfahrung bestimmte Feststellungen hinterfragen und bei Unklarheiten weitere Auskünfte einholen kann.

- Die *Verfügbarkeit* des Dienstes wird nicht als kritisch erachtet. Viele der Prozessvorgänge erfolgen manuell und setzen eine Vorlaufzeit voraus.

- Die im Rahmen der Rückmeldung von Forschungsergebnissen weitergegebenen Informationen haben einen hohen *Vertraulichkeitsbedarf* und bringen ein nicht zu vernachlässigendes Missbrauchsrisiko mit sich.

A.3.4. Pseudonymisierung von Patientendaten

Die Pseudonymisierung von Patientendaten erfolgt mithilfe eines symmetrischen kryptografischen Algorithmus. Empfohlen wird die Verwendung von 3DES oder AES, wobei die Transformation von *PID* in *PSN* auf einer SmartCard ausgeführt werden soll, damit der geheime Schlüssel die Karte nicht verlässt. Die Schlüssel zu den Pseudonymen sollen an einer einzigen zentralen gut geschützten Stelle gespeichert werden. Die Pseudonymisierung erfolgt mehrstufig. Die Risikoeinschätzung der ersten Pseudonymisierungsstufe (*PID*-Generator) wurde bereits durchgeführt; hier wird die Pseudonymisierung von Einträgen vor der Weitergabe an die Wissenschaftler analysiert. Eine ausführliche Spezifikation des Pseudonymisierungsdienstes befindet sich in [RDSP06]. Rechtliche Aspekte der Pseudonymisierung sind dem Rechtsgutachten von Christian Dierks zu entnehmen (vgl. [Die08]). Ungleich größere Risikopotenziale gelten in Verbindung mit der bedingten Pseudonymisierung und der in einem späteren Abschnitt behandelten Anonymisierung vom Bildmaterial, biologischen Proben und den daraus gewonnenen Daten. Bei Speicherung von biologischen Proben und insbesondere bei Bilddaten innerhalb eines Forschungsnetzes müssen besondere Sicherheitsvorkehrungen getroffen werden. So enthalten z. B. die Schichtbilddaten Informationen, aus denen mithilfe dreidimensionaler Rekonstruktionsverfahren morphologische Informationen über einen Patienten gewonnen werden können. Ein Gesicht kann anhand der Computertomografie des Schädels rekonstruiert werden, was die Identifikation des Patienten nach dem Abgleich mit anderen Quellen möglich macht. Identifizierende Patientendaten sollen mit besonderer Vorsicht in das Bildmaterial integriert werden. Die unwiderrufliche Entfernung von identifizierenden Patientendaten kann durch die sogenannte Schwärzung erfolgen. Da bestimmte Datenformate und medizinische Geräte die nachträgliche Schwärzung nicht immer unterstützen, muss sichergestellt werden, dass für die Datensammlung und Aufbewahrung nur Datenformate und Geräte eingesetzt werden, die diese Anonymisierung des Bildmaterials erlauben (vgl. [SPR+06], [DC06, S. 48 f.]). Weitere Spezifika dieser Datenart werden im Abschnitt 4.3.2 „Bedrohungsorientierte Analyse“ erläutert.

Die *PID* $\leftrightarrow$ *PSN*-Umwandlung erfolgt auf einigen wenigen dafür konzipierten SmartCards mithilfe eines symmetrischen Verschlüsselungsverfahrens. Der Verlust einer solchen Karte ist mit einem hohen Reidentifizierungsrisiko für Patienten verbunden. Aus diesem Grund ist bei den für Pseudonymisierung verwendeten SmartCards auf größte physikalische Sicherheit zu achten. Die eingesetzten Karten sollen stets den aktuellen Sicherheitsstandards entsprechen und gegen bekannte Angriffe resistent sein. Es ist selbstverständlich, dass die alten Exemplare der o. g. Karten bei der Schlüsselaktualisierung eingesammelt und sicher aufbewahrt werden müssen. Von der Speicherung des neuen und der alten Pseudonymisierungsschlüssel auf der neuen Karte ist abzuraten, denn dies würde die Anzahl der im Falle des Kartenverlusts ausgespähten Datensätze erhöhen. Beim Verlust einer solchen Karte ist die Verwendung weiterer Karten mit dem gleichen Schlüssel sofort einzustellen.

Ebenso sollen nach dem Bekanntwerden des Vorfalls keine, mit dem alten Schlüssel pseudonymisierten, Daten verwendet werden. Die Teilnehmer des Forschungsnetzes müssen, ihre Datenbestände durch die mit dem aktuellen Schlüssel pseudonymisierten ersetzen, falls symmetrische Verschlüsselung mit einem einzigen Schlüssel eingesetzt wird. Beim Einsatz zufälliger Schlüssel zur *PSN*-Generierung entfällt dieser Schritt.

- Obwohl der *Authentizitätsverlust* beim Pseudonymisierungsdienst unwahrscheinlich ist, hätte eine solche Sicherheitsverletzung weit reichende Folgen für das Fortbestehen des Forschungsnetzes. Die von den Angreifern „pseudonymisierten“ Daten würden die erwünschte Patientenreidentifizierung erschweren und eine unerwünschte Reidentifizierung ermöglichen. Das davon ausgehende Missbrauchspotenzial ist allerdings als gering einzuschätzen, da dieser Dienst nur forschungsnetzintern verfügbar ist; die Authentizität der teilnehmenden Ressourcen ist mit einem vertretbaren Aufwand feststellbar.

- Die Folgen der *Integritätsverletzung* durch Manipulation sind mit den Folgen des *Authentizitätsverlusts* vergleichbar. Die Wahrscheinlichkeit der beiden Sicherheitsverletzungen ist ungefähr gleich groß und wird durch Release-Management und Monitoring verringert.

- Nach der anfänglichen Genehmigung des Verfahrens und bei der Einhaltung entsprechender Auflagen ist die Verletzung der *Konformität* kaum möglich.

- Bei einer Festlegung von Schnittstellen und bei eindeutigen Eingabeparametern ist das Verfahren als *robust* einzuschätzen.

- Die zuverlässige Funktionsweise des Pseudonymisierungsverfahrens und die *Verbindlichkeit* der Informationen sind Voraussetzungen für die Rückführung von Forschungsergebnissen an die Patienten. Verletzung und Missbrauch des Sicherheitskriteriums „Verbindlichkeit“ sind unwahrscheinlich.

- Da dieser Teil des Pseudonymisierungsdienstes lediglich im Forschungszusammenhang verwendet wird, stellt die Verletzung der *Verfügbarkeit* kein großes Risiko für das Forschungsnetz dar. Auch längere Ausfälle des Dienstes sind i. d. R. akzeptabel.

- Die *Vertraulichkeitsverletzungen* bringen dagegen eine Erhöhung des Rückidentifizierungsrisikos mit sich. Das Bekanntwerden der verwendeten Pseudonymisierungsschlüssel kann zum Einstellen des Forschungsnetzbetriebs führen. Das Risiko des *Vertraulichkeitsverlusts* in Folge eines Fehlers (Schwäche) des verwendeten Verschlüsselungsverfahrens ist als gering einzustufen.

Pseudonymisierung von Patientendaten						
Authen-tizität	Inte-grität	Konfor-mität	Robust-heit	Verbind-lichkeit	Verfüg-barkeit	Vertrau-lichkeit
3	2	1	1	3	1	5

Tabelle 10.: Bewertung der Sicherheitskriterien für die Pseudonymisierung von Patientendaten

A.3.5. Anonymisierung von Patientendaten

Bei der Anonymisierung von Patientendaten werden die personenbezogenen Informationen derart modifiziert, dass die Daten einem Patienten nicht mehr zugeordnet werden können. Die Anonymisierung kann z. B. beim Widerrufen der Einwilligung zur Datenweitergabe, -verarbeitung und -speicherung durch den Patienten oder nach dem Ablauf der vereinbarten Frist[39] verlangt werden, in der die Daten in einer nicht anonymisierten Form verarbeitet werden dürfen. Die folgenden Ausführungen erfolgen in Anlehnung an das in [SSS06] beschriebene Anonymisierungsszenario. Die Themenbereiche Personenbezogenheit, Anonymisierung und Pseudonymisierung von Forschungsdaten werden ausführlich in [MW02, S. 19 ff.]. dargestellt.

- Die *Authentizitätsverletzung* des Anonymisierungsdienstes kann von einem Angreifer zur Ermittlung der Zugehörigkeit von Patienten zu einem bestimmten Forschungsnetz ausgenutzt werden. Bei der Anonymisierung aufgrund des Zurückziehens der Einwilligung (und nicht aufgrund des Ablaufs der Aufbewahrungsperiode) kann der Angreifer auf wertvolle Patienteninformationen hoffen. Diese Sicherheitsverletzung kann jedoch nur eine kurze Zeit unbemerkt bleiben. Spätestens bei der erfolgten Benachrichtigung über die Anonymisierung der Daten würde man Verdacht schöpfen. Die Tatsache, dass der Patient als Laie nicht jeden Betrugsversuch erkennen wird, lässt Platz für ein Restrisiko; die alternative Rückmeldung der Anonymisierungsergebnisse an den behandelnden Arzt wäre jedoch in vielerlei Hinsicht problematisch.

- Manipulationsversuche des Anonymisierungsdienstes und der daraus resultierende *Integritätsverlust* sind dagegen wahrscheinlich und auch existenzbedrohend für ein Forschungsnetz. Gelingt es dem Angreifer, eine Beziehung zwischen der Patientenidentität und den „anonymisierten“ Daten herzustellen, kann er an schutzwürdige Informationen gelangen.

- Nach der anfänglichen Genehmigung des Anonymisierungsprozesses und bei der Einhaltung der Prozessabläufe sind die Verstöße gegen die *Konformität* des Verfahrens kaum möglich.

[39] Zum Beispiel nach Ablauf von sechs Jahren nach der letzten Behandlung (vgl. [RDSP06]).

Anonymisierung von Patientendaten						
Authen-tizität	Inte-grität	Konfor-mität	Robust-heit	Verbind-lichkeit	Verfüg-barkeit	Vertrau-lichkeit
2	5	1	1	1	1	4

Tabelle 11.: Bewertung der Sicherheitskriterien für die Anonymisierung von Patientendaten

- Durch die fest definierten Schnittstellen und die eindeutigen Eingabeparameter ist der Anonymisierungsvorgang als *robust* einzuschätzen.
- Die *Verbindlichkeit* der Dienstinformationen spielt lediglich in Beziehung mit dem Selbstbestimmungsrecht des Patienten über seine persönlichen Daten eine Rolle. Ein Verstoß gegen die Verbindlichkeit würde aufgrund des Wesens des Dienstes im Verlust der *Konformität* resultieren.
- Die *Verfügbarkeit* des Anonymisierungsdienstes ist i. d. R. irrelevant. Auch längere Ausfälle des Dienstes gefährden das Fortbestehen des Forschungsnetzes nicht und sind akzeptabel.
- Die *Vertraulichkeitsverletzung* des Anonymisierungsdienstes ist kein gern gesehenes Szenario, birgt jedoch ein geringeres Schadenspotenzial in sich als die *Vertraulichkeitsverletzung* des Pseudonymisierungsdienstes.

A.3.6. Public Key-Infrastruktur

Die Einrichtung einer *Public Key-Infrastruktur* (PKI) ist die Voraussetzung für einen sicheren und verbindlichen Austausch von Informationen. Der PKI-Einsatz erlaubt eine sichere Authentifikation[40] sowie eine fortgeschrittene elektronische Signatur nach SigG. Besonders interessant ist dieser Forschungsnetzdienst in Zusammenhang mit der HPC-Verbreitung. Weiterführende Informationen befinden sich in den Abschnitten 3.5.6 „Verzeichnisdienste (LDAP, OCSP)“ und 3.5.7 „Ticketing, Single Sign-On (SSO)“.

- Das Vertrauen in die *Authentizität* dieses Dienstes hat die höchste Priorität. Dies gilt nicht nur für die Verwendung der PKI-Infrastruktur für die Benutzerauthentifikation, sondern hat auch Auswirkungen auf die Verbindlichkeit der vorgenommenen Einträge, der ausgetauschten Nachrichten etc.
- Die PKI des Forschungsnetzes darf nicht manipulierbar sein. Die Aufrechterhaltung der *Integrität* ist die Voraussetzung für die *Authentizität* und die *Verbindlichkeit*.

[40] Verwendung der PKI zu Authentifikationszwecken ist im Abschnitt 3.5.3 „Authentifizierung von Forschungsnetzteilnehmern“ dargestellt.

Public Key Infrastruktur						
Authen-tizität	Inte-grität	Konfor-mität	Robust-heit	Verbind-lichkeit	Verfüg-barkeit	Vertrau-lichkeit
5	5	1	5	5	5	3

Tabelle 12.: Bewertung der Sicherheitskriterien für die PKI-Dienste

- *Konformitätsverletzungen* sind bei der Einhaltung maßgeblicher gesetzlicher Vorschriften und Auflagen[41] kaum möglich.
- Die PKI-Dienste werden von vielen (externen) Teilnehmern in Anspruch genommen, die versuchen könnten, sie zu manipulieren. Der Schutz gegen solche Manipulationsversuche erfordert *Robustheit* der eingesetzten Verfahren und Prozesse.
- Die *Verbindlichkeit* der Informationen ist unmittelbar mit der Authentizitäts- und Integritätseigenschaften verbunden und stellt ebenfalls höchste Ansprüche an die Implementierung der PKI-Dienste.
- Die Erledigung vieler kritischer Forschungsnetzaufgaben setzt die *Verfügbarkeit* des Dienstes voraus. Lediglich kurzzeitige Ausfälle könnten überbrückt werden. Die PKI-Infrastruktur ist ausfallsicher und redundant auszulegen.
- Die Verletzung der *Vertraulichkeit* ist bei einem normenkonformen Betrieb wenig risikoreich. Selbstverständlich ist die Kompromittierung von Patientendaten als Folge der Dienstmanipulationen oder Authentizitätsverletzungen möglich. Die Sicherheit der eingesetzten Kryptografie- und Verzeichnisdiensttechnologien kann nach dem aktuellen Kenntnisstand als hoch eingestuft werden.

A.3.7. Teilnehmerservice zur Beantragung und Verteilung von Chipkarten und Softwarezertifikaten

Die Spezifikation des *Teilnehmerservice zur Beantragung und Verteilung von Chipkarten und Softwarezertifikaten* sowie deren Verlängerung und Sperrung ist in der Zertifizierungsrichtlinie des Trustcenters von [sch03] ausführlich beschrieben. Die wichtigsten Merkmale des Dienstes und die sicherheitsrelevanten Anforderungen sind im Abschnitt 3.5.7 „Ticketing, Single Sign-On (SSO)“ zusammengefasst.

- Die *Authentizität* der teilnehmenden Parteien ist die Grundvoraussetzung für das sichere Funktionieren diverser anderer Dienste. Durch strenge Überprüfungsmaßnahmen (z. B. persönlicher Antrag unter Vorlage des Personalausweises, Sicherheitsmaßnahmen der CAs etc.) ist die Authentizitätsverletzung unwahrscheinlich.

[41] Zum Beispiel in Bezug auf den Betrieb der HPC-Infrastruktur.

Verteilung von Chipkarten und Softwarezertifikaten						
Authentizität	Integrität	Konformität	Robustheit	Verbindlichkeit	Verfügbarkeit	Vertraulichkeit
4	4	1	2	2	1	5

Tabelle 13.: Bewertung der Sicherheitskriterien für die Zertifikat- und Chipkartenverteilung

- Manipulationsversuche und der daraus resultierende *Integritätsverlust* sind zwar für das Forschungsnetz gefährlich; die Vielfältigkeit der Sicherheitsmaßnahmen (Vier-Augen-Prinzip, Mehrstufigkeit des Verfahrens, zuverlässige Identitätsüberprüfung, verlässliche Verteilungskanäle etc.) macht eine erfolgreiche Manipulation jedoch unwahrscheinlich.

- Bei der Einhaltung ursprünglich genehmigter Mechanismen ist die Gefahr der *Konformitätsverletzung* als gering einzustufen.

- Die kritischen Prozessschritte laufen innerhalb der abgesicherten Forschungsnetzumgebungen bzw. innerhalb der sicheren Infrastruktur der Forschungsnetzpartner ab und werden zum großen Teil manuell durchgeführt. Die *Robustheit* des Verfahrens wird kaum beansprucht.

- Die *Verbindlichkeit* verteilter Daten/Zertifikatsinformationen kann leicht und mit nur geringem Know-how überprüft werden (z. B. Authentizität der CA), sodass für die Verbindlichkeit des Dienstes nur geringe Risiken bestehen.

- Lediglich Teile des Dienstes, die für die Verifizierung von Informationen verfügbar sein müssen, sind geschäftskritisch und müssen hohe Verfügbarkeitsanforderungen erfüllen. Dieser Bestandteil des Dienstes ist jedoch eher dem Verzeichnisdienst zuzuordnen. Durch die vorwiegend manuellen Prozesse und geringe Häufigkeit der Inanspruchnahme des Dienstes können dessen *Verfügbarkeitsanforderungen* als gering eingestuft werden.

- Innerhalb des Vorgangs werden keine Patientendaten ausgetauscht. Auch Informationen über das medizinische Personal eines Forschungsnetzes können anderen Quellen mit einem geringeren Aufwand entnommen werden. Da die Verwendung von Softwarezertifikaten in vielen Fällen die Regel ist, wird der *Vertraulichkeit* ausgetauschter Informationen höchste Bedeutung beigemessen.

A.3.8. Qualitätssicherungsservice

Die Sicherstellung der Richtigkeit eingegebener Daten (Qualitätssicherung) erfolgt mehrstufig: Nach einer automatischen Prüfung findet eine manuelle Prüfung der Daten auf

ihre Richtigkeit statt. Die manuelle Überprüfung wird von internen Forschungsnetzteilnehmern vorgenommen, die schreibenden Zugriff auf die Forschungsdatenbank(en) brauchen. Sämtliche Änderungen/Korrekturen werden protokolliert und regelmäßig einem Audit unterzogen. Qualitätssicherungsservice ist ein kritischer Forschungsnetzdienst, da für den Vergleich mit früher erhobenen Daten die sogenannten Kontextdaten (bestehend aus *PID* und *MDAT*) temporär gespeichert werden, die ihrerseits für einen Angreifer interessant sein könnten. Um diese Art der Angriffe vorzubeugen, dürfen die Kontextdaten nur in verschlüsselter Form temporär gespeichert werden. Es ist empfehlenswert, keine direkte Verbindung zwischen einem Klinik-PC/Arzt-PC und dem Qualitätssicherungsserver zu erlauben, denn die Daten müssen für die Verarbeitung entschlüsselt werden, was sie für einen Angreifer auslesbar macht (vgl. [RDSP06]). Die Datenqualitätssicherung ist auf Systemen in einem separaten LAN-Segment durchzuführen, das nur von innerhalb des administrativen Bereichs des Forschungsnetzes erreichbar sein darf.

- Da ein großer Teil der Forschungsnetzinformationen das Qualitätssicherungsservice passieren müssen, bevor sie in die Forschungsdatenbank aufgenommen werden, hat die Gewährleistung der *Authentizität* des Dienstes eine hohe Priorität. Ein Angreifer, dem es gelingt, die Stelle des Qualitätssicherungsservice einzunehmen, erhält eine exzellente Ausgangsbasis für weitere Angriffe und in vielen Fällen direkte Rückidentifizierungsmöglichkeiten.

- Ein manipulierter Qualitätssicherungsdienst kann als Ausgangspunkt für einen Angriff dienen oder selbst zu einer Plattform für die Durchführung des Angriffs werden. Die Gewährleistung der *Integrität* des Dienstes ist aus diesem Grund von entscheidender Bedeutung.

- Die Qualitätssicherung muss die *Konformitäts*-Eigenschaft zu sämtlichen geltenden Gesetzesregelungen und Normen erfüllen, wenn unmittelbar auf vertrauliche Patientendaten zugegriffen wird. Die Verletzung der Konformität wird unwahrscheinlich, wenn bei der Qualitätssicherung lediglich auf pseudonymisierte oder gar auf anonymisierte Daten zugegriffen wird.

- Obwohl die Qualitätssicherung ein interner Prozess ist, dessen Datenarten und Schnittstellen fest definiert sind, besteht die Möglichkeit, dass die eventuell vorhandenen Schwachstellen des Dienstes z. B. durch die Dateneingaben ausgenutzt werden. Die eingesetzten Verfahren müssen gegen die Angriffe dieser Art *robust* sein.

- Auch wenn Qualitätssicherungsservice keine Datenausgaben im engeren Sinne produziert, kann man die *Verbindlichkeits*-Eigenschaft des Dienstes in den durchgeführten Datenänderungen und -korrekturen erkennen. Es muss nachvollzogen werden können, von wem, wann und aus welchem Grund eine bestimmte Änderung im Rahmen

Qualitätssicherungsservice						
Authentizität	Integrität	Konformität	Robustheit	Verbindlichkeit	Verfügbarkeit	Vertraulichkeit
5	5	3	3	4	1	5

Tabelle 14.: Bewertung der Sicherheitskriterien für den Qualitätssicherungsservice

der Qualitätssicherung erfolgte. Bei einer solchen Interpretation ist dem Sicherheitskriterium *„Verbindlichkeit“* die höchste Bedeutung beizumessen. Die abgemilderte Kritikalitätseinstufung ist auf die geringen Missbrauchspotenziale zurückzuführen.

- Obwohl die Qualitätssicherung für die angemessene Datenqualität unabdingbar ist, sind (auch längere) Ausfälle des Dienstes akzeptabel (*Verfügbarkeit*), wenn andere Prozesse nicht betroffen werden, und eine nachträgliche Qualitätssicherung möglich ist.

- Sowohl die automatische als auch die manuelle Prüfung bieten eine erhebliche Angriffsfläche, da die beiden Prozesse Einsicht in die vertraulichen Patientendaten benötigen. Die größten Missbrauchspotenziale dieses Dienstes bestehen bei den internen Teilnehmern und können durch entsprechende Vertragsgestaltung, Schulungen, Kontrollmaßnahmen etc. reduziert werden. Trotzdem ist die *Vertraulichkeit* des Qualitätssicherungsservice ein bedeutendes Sicherheitskriterium.

A.3.9. Datenexport und Datenabruf

Der Datenexport und Datenabruf von anonymisierten bzw. (beim Vorliegen einer entsprechenden Genehmigung durch den Ausschuss Datenschutz) pseudonymisierten Behandlungsdaten zu wissenschaftlichen Zwecken.

- Bei einer engeren Betrachtung des Datenexports bleiben die Benutzerauthentifizierung, Datenpseudonymisierung und -anonymisierung bzw. anschließende Datenspeicherung und Verarbeitung außerhalb des Prozesses. Lediglich die Sabotageversuche von Forschungsprojekten in Form von *Authentizitätsverletzungen* (z. B. durch das Einstreuen von Falschinformationen) könnten von Relevanz sein. Gleichzeitig kann die Authentizität der Forschungsnetzdaten relativ leicht mithilfe der bereits erwähnten PKI-Infrastruktur überprüft werden.

- Datenexport basiert auf dem Minimalprinzip: Jeder Teilnehmer darf die Einsicht höchstens in die Daten erhalten, für die er zugriffsberechtigt ist. Die mit der Verletzung der *Integrität* verbundenen Gefahren, die z. B. einem Teilnehmer Zugriff auf eine größere Datenmenge ermöglichen, müssen ernst genommen werden.

Datenexport und Datenabruf						
Authen-tizität	Inte-grität	Konfor-mität	Robust-heit	Verbind-lichkeit	Verfüg-barkeit	Vertrau-lichkeit
1	3	5	5	5	1	3

Tabelle 15.: Bewertung der Sicherheitskriterien für den Datenexport und Datenabruf

- Im Forschungszusammenhang ist der Datenabruf für viele Teilnehmer der wichtigste Grund für die Forschungsnetzteilnahme. Datenabruf ist sozusagen das wichtigste *„Produkt“*, das ein Forschungsnetz einem externen Kunden (Forscher) anbietet. Sämtliche Verletzungen der *Konformität* des Prozesses wären schnell öffentlich bekannt und könnten zur Einstellung des Forschungsnetzbetriebs führen.

- Insbesondere beim Online-Datenabruf spielt die *Robustheit* des Verfahrens, an dem viele externe Teilnehmer mit unterschiedlich konfigurierten Systemen von einer Vielzahl von Lokationen beteiligt sind, eine große Rolle. Systeme müssen bei Fehleingaben stets adäquat reagieren können. Mehr Informationen über den Zugriff von externen Teilnehmern befinden sich in den Abschnitten 3.5.5 „Zugangsszenarien von Netzteilnehmern zu den Forschungsnetzdiensten“ und 3.5.1 „Sichere Arbeitsumgebung“.

- Beim Datenabruf ist die *Verbindlichkeit* von Informationen unmittelbar mit der Konformität verknüpft. Es muss zuverlässig nachvollzogen werden können, wer, wann und welche Daten erhalten hat. Eine Verletzung dieses Sicherheitskriteriums ist somit als Konformitätsverlust zu deuten.

- Die *Verfügbarkeit* des lediglich im Forschungszusammenhang verwendeten Datenexports hat keine große Relevanz auf das Fortbestehen des Forschungsnetzes. Auch bei lang anhaltenden Ausfällen des Dienstes würden die Forscher kaum ihre Zusammenarbeit mit einem Forschungsnetz auflösen.

- Bei der bereits erwähnten „engen“ Betrachtung des Prozesses werden die Pseudonymisierungs- bzw. Anonymisierungsprozesse nicht berücksichtigt. Es wird also davon ausgegangen, dass die Reidentifizierung anhand von exportierten Daten nicht möglich ist. Bei einer Reihe von Forschungsnetzdaten lässt sich der Personenbezug jedoch nur schwer entfernen, wie z. B. bei Biomaterialien und den daraus gewonnenen Daten.

A.3.10. Verwaltung von Zugriffsrechten

Die Bestimmung und Verwaltung von Zugriffsberechtigungen wird von dem Security-Administrator und dem Administratoren-Team ausgeführt. Die Durchführung dieser Aufgabe unterliegt einer ständigen Kontrolle und muss durch organisatorische und administrative Maßnahmen begleitet werden (s. a. Abschnitt 3.5.4).

Verwaltung von Zugriffsrechten						
Authen-tizität	Inte-grität	Konfor-mität	Robust-heit	Verbind-lichkeit	Verfüg-barkeit	Vertrau-lichkeit
5	5	5	3	5	3	5

Tabelle 16.: Bewertung der Sicherheitskriterien für die Verwaltung von Zugriffsrechten

- Die Vergabe und Verwaltung von Zugriffen wird durch die Antragstellung initiiert. Die *Authentizität* der Informationen, die dem Administrationsteam vorgelegt werden, hat höchste Bedeutung für die Fehlerfreiheit des Prozesses. Schließlich werden die Berechtigungen aufgrund der Informationen vergeben, die von einer zuverlässigen Quelle stammen sollen. Es müssen zusätzliche Kontrollmechanismen in Form von obligatorischen Rückmeldungen an die Initiatoren des Vorgangs implementiert werden.
- Die Verwaltung von Zugriffsrechten darf nicht manipuliert werden können, um einer Person mehr Zugriffsrechte als erforderlich bzw. erlaubt zu verschaffen. Somit werden höchste Anforderungen an die *Integrität* des Dienstes gestellt.
- Die Einhaltung diverser gesetzlicher Anforderungen und vertraglicher Vereinbarungen bei der Bestimmung von Zugriffsrechten erhebt hohe Ansprüche an die *Konformität* des Verfahrens.
- Die Vergabe von Berechtigungen erfolgt durch internes qualifiziertes Personal, was die *Robustheits*-Anforderungen minimiert.
- Die während des Berechtigungsvergabe-Prozesses ausgetauschten Informationen müssen den teilnehmenden Personen eindeutig zugeordnet werden können. Die *Verbindlichkeitsanforderungen* an den Prozess sind hoch.
- Auf die *Verfügbarkeit* des Dienstes wird nur im Fall der Deaktivierung von Benutzer-Accounts großer Wert gelegt. Es ist sogar empfehlenswert, die Prozesse der Neuanlage oder Änderung eines Benutzers und der Deaktivierung eines Benutzerkontos loszukoppeln. Aufgrund der Mehrstufigkeit des Verfahrens, in dem mehrere Schritte manuell durchgeführt werden, sind kurz- bis mittelfristige Ausfälle des Dienstes akzeptabel (vgl. [RDSP06]).
- Insbesondere bei den Systemen mit Ein-Faktor-Authentifizierung (z. B. Benutzername und Passwort) ist die *Vertraulichkeit* der Informationen von besonderer Bedeutung.

A.3.11. Handhabung von Biomaterialien und den daraus gewonnenen Daten

Eine besondere Herausforderung sind für ein Forschungsnetz das Sammeln und das Zurverfügungstellen von Biomaterialien und der daraus gewonnenen Daten (vgl. [Deu10,

S. 78 f.], [Wel03]). Die damit verbundenen Risiken werden im Folgenden untersucht. Die Biomaterialien können in Form von Proben sowohl zentral als auch dezentral (bei den Partnern) in Probenbehältern gelagert werden. Jeder Probenbehälter wird mit einer Probennummer versehen, um Proben später reidentifizieren zu können. Die dezentral gelagerten Proben werden in den meisten Fällen auch dezentral verarbeitet. Es wird zwischen folgenden Probenarten unterschieden:

- *Gewebe:* Ein durch einen chirurgischen oder endoskopischen Eingriff gewonnenes Gewebe. Dieses Gewebe kann pathologisch verändert oder aber auch einfach „begleitend" sein.
- *Körperflüssigkeiten:* Blut und Blutbestandteile (Plasma, Serum), Punktatflüssigkeit, Liquor, Speichel, Tränenflüssigkeit und Harn zählen zu den Körperflüssigkeiten.
- *Zellen:* Zellen werden entweder eingefroren oder in Zellkulturen weiter gezüchtet. Durch die sogenannte Kultivierung werden Zellen zu einer fast unerschöpflichen Quelle molekulargenetischer Analyse.
- *DNA:* Wird aus allen Zellarten gewonnen und beinhaltet die Erbsubstanz-Informationen.
- *RNA:* Wird aus allen Zellarten isoliert und ist im Vergleich zu DNA viel instabiler. Aus RNA-Proben können ähnliche Daten wie aus der DNA gewonnen werden.

Die Aufbewahrung biologischer Proben und Daten innerhalb des Forschungsnetzes bringt für Patienten ein erhöhtes Reidentifizierungsrisiko mit sich. Einige der o. g. Probenarten können verwendet werden, um Patienten des Forschungsnetzes zu reidentifizieren (z. B. DNA und RNA[42]). So reicht die Analyse einiger weniger SNPs[43] (Single Nucleotide Polymorphismus) aus, um einen Menschen eindeutig zu identifizieren.[44] Für eine eindeutige Identifikation bedarf es derzeit noch einer Vergleichsprobe, deren Aufbereitung und Auswertung das Vorhandensein einer speziellen Ausrüstung und des entsprechenden Know-hows erfordert. Durch Fortschritte in der Forschung wird die Aufbereitung und Auswertung von biologischen Proben zunehmend einfacher. Es ist davon auszugehen, dass in Zukunft die Datengewinnung aus biologischen Proben weitestgehend automatisch ohne spezielles

[42]Das Proteom eines Organismus kann ebenfalls zu Identifikationszwecken verwendet werden, auch wenn die identifizierenden Informationen schwieriger als im Falle eines Genoms zu extrahieren sind. Der Forschung ist zu verdanken, dass zunehmend mehr Zusammenhänge zwischen Genom und Proteom bekannt werden, sodass die Personenidentifikation mittels der RNA-Analyse in Zukunft denkbar ist.

[43]Ca. 70 SNPs.

[44]Man spricht vom genetischen Fingerabdruck. [SS05, S. 548]: *„... confidentiality and privacy concerns have to be addressed for two reasons: the genomic data is much more predictive of the patient's health status than any other test, and the genome is uniquely identifiable."* (vgl. [VAM+01]).

Wissen durchgeführt werden kann. Der verstärkte Einsatz personenbezogener Informationen durch diverse Behörden mit „Sicherheitsaufgaben“, Speicherung und Auswertung dieser Daten sowie die zukünftige Vereinfachung in Handhabung von biologischen Proben und den daraus gewonnenen Daten lassen den Schluss über die künftige Verbreitung von Referenzdateien mit genetischen Fingerabdrücken zu. Diese könnten zu einer vereinfachten Reidentifizierung von Patienten beitragen.
Biomaterialien unterscheiden sich von anderen im medizinischen Forschungsnetz aufbewahrten Daten dadurch, dass sie identifizierende Informationen beinhalten, die nicht weggelassen oder vergröbert werden können (vgl. [GK07], [SPR+06]). Proben lassen sich also nicht zuverlässig anonymisieren. Trotzdem ist die Reidentifizierungsgefahr, die von biologischen Proben ausgeht, nicht so groß wie die von den daraus gewonnenen Daten. Proben müssen nämlich physisch entwendet und anschließend (noch) relativ aufwendig analysiert werden. Die aus den Proben gewonnenen und in der Datenbank abgespeicherten Daten lassen sich dagegen schnell und kostengünstig kopieren; die Probendaten bringen zurzeit ein höheres Reidentifizierungspotenzial mit sich als die Proben selbst. Die Aufnahme von Biomaterialien in ein Forschungsnetz hat einen erheblichen Einfluss auf dessen Struktur. Man spricht von der Erweiterung der Nutzung gesammelter Daten in der Menge, Zeit und Zweckbestimmung (vgl. [SPR+06], [Ron05], [Ron04]):

- Eine sinnvolle molekulargenetische Forschung ist nur mit der Erreichung einer bestimmten kritischen Masse an Biomaterialien und Daten möglich. Dafür werden Daten überregional (auch international) gesammelt und evtl. ebenfalls aufbereitet/ausgewertet und aufbewahrt.

- Proben und die daraus gewonnenen Daten können für diverse, derzeit noch nicht vorgesehene, Aufgaben verwendet werden, was sich im deren Umfang widerspiegelt.

- Biomaterialien haben aufgrund ihres hohen Wertes für die Forschung einen wesentlich längeren „Lebenszyklus“ und können der Forschung zum Teil zeitlich unbegrenzt zur Verfügung stehen.

Diese Eigenschaften erfordern Beachtung diverser rechtlicher Details und Aspekte der längerfristigen Datenspeicherung bzw. Probenaufbewahrung. Ein entsprechendes Rechtsgutachten sowie die Zusammenstellung der maßgeblichen Rechtsvorschriften kann den rechtlichen Rahmenbedingungen für Biomaterialdatenbanken entnommen werden [SPR+06] (vgl. [Pom07]).[45]

[45] Zukünftiger medizinischer Fortschritt ist für die Konzepte zur Handhabung von biologischen Proben zu berücksichtigen, da die Aufbewahrung von Proben über einen längeren Zeitraum als in den generischen Datenschutzkonzepten der TMF vorgeschlagenen sechs Jahren erfolgt.

A.4. Qualitative bedrohungsorientierte Analyse der Struktur potenzieller Angreifer und Angriffsszenarien in einem Forschungsnetz

Wenn es darum geht, die Angriffsmuster für eine Unternehmensinfrastruktur zu ermitteln, genügt meistens die Auseinandersetzung mit der Frage: Wie könnte ein Angreifer durch seinen Angriff Vorteile erlangen und/oder dem Unternehmen einen Schaden zufügen? In vielen Fällen sind diese beiden Aspekte eng miteinander verknüpft. Es sind auch Fälle denkbar, in denen Schaden verursacht wird, ohne dass der Angreifer selbst davon profitiert. Die Motivation vieler typischer Angriffe ist die Bereicherungsabsicht.
In einem Forschungsnetz existieren keine Dienste, die ein Angreifer missbrauchen könnte, um Geldtransaktionen direkt zu tätigen. Die technische Ausrüstung eines Forschungsnetzes (PCs der Mitarbeiter, Hardwarezubehör, Softwarelizenzen etc.) sind für einen seriösen Angreifer keine nennenswerte Beute. Patientendaten und Forschungsergebnisse sind die sogenannten Datenjuwelen des Forschungsnetzes; ihr Wert übersteigt den Wert der technischen Ausrüstung eines Forschungsnetzes um ein Vielfaches (vgl. [NN01]). Die größte Gefahr für ein Forschungsnetz besteht im Bekanntwerden personenbezogener medizinischer Daten z. B. durch Folgen ungewollter Patientenreidentifizierung. Eine solide Ausgangsbasis für die Bestimmung der Vorgehensweise zur bedrohungsorientierten Risikoanalyse ist in der NIST-Publikation 800-33 beschrieben (vgl. [SGF02, S. 9 ff.], s. a. Abschnitt A.1 „Untersuchung der Wirksamkeitsbewertung von Sicherheitsmaßnahmen mithilfe von etablierten S&R-Frameworks“).
Immer wieder erscheinen in der Presse Schlagzeilen über die sogenannten Phishing-Angriffe. Betrüger versuchen, Personendaten auszuspähen, um diese beispielsweise an Interessenten zu verkaufen. Diese Art von Angriffen stellt für ein Forschungsnetz ebenfalls eine große Gefahr dar, obwohl die Identifikation eines Patienten nur für die am Behandlungsprozess Beteiligten möglich sein soll. Die restlichen Netzteilnehmer[46] haben keinen Zugang zu den identifizierenden Daten (vgl. [RDSP06]). Eine Ausnahme bildet die Überlassung von pseudonymisierten Behandlungsdaten an die Wissenschaftler. Um eine spätere Rückführung von Forschungsergebnissen zu gewährleisten, werden Daten mithilfe eines symmetrischen Verschlüsselungsverfahrens pseudonymisiert. Sollte ein Angreifer die pseudonymisierten Daten und den für den jeweiligen Export verwendeten Schlüssel besitzen, ist er in der Lage, die Patienten zu reidentifizieren. Aus diesem Grund soll die Aufbewahrung von Pseudonymisierungsschlüsseln unter besonders strengen Bedingungen erfolgen. Die Pseudonymisierungsschlüssel sollen gelöscht werden, sobald die Rückführung von Ergebnissen nicht mehr notwendig/sinnvoll ist. Eine mögliche Lösung an der Stelle wäre die Verwendung von Einweg-*PSNs*. Für jeden neuen Pseudonymisierungsvorgang könnte man beispielsweise

[46] Zum Beispiel wissenschaftlich tätige Mitarbeiter des Forschungsnetzes, nicht behandelnde Ärzte etc.

einen zufälligen Schlüssel erzeugen, mit dem man die dem Wissenschaftler ausgehändigten Daten pseudonymisiert. Die so erzeugten Schlüssel würde man sicher aufbewahren, bis die Notwendigkeit zur Depseudonymisierung entsteht, oder die Daten beispielsweise nach einer bestimmten Zeit anonymisiert werden. Im Falle der Anonymisierung würde es ausreichen, den dazugehörigen Schlüssel zu löschen. Um die Daten zu depseudonymisieren, benötigt man einen Hinweis auf den verwendeten Schlüssel. Dies kann z. B. eine eindeutige Nummer bzw. ein Zeitstempel sein. Ebenfalls denkbar wäre die Verschlüsselung des neuen Schlüssels mit dem „Generalschlüssel“ des Forschungsnetzes. Diesen „verpackten“ Schlüssel würde man mit einer jeden pseudonymisierten Auswertung mitgeben. Beim Depseudonymisierungsbedarf müsste der zufällig erzeugte Schlüssel wieder entziffert und seinerseits zur Wiedergewinnung des *PID* verwendet werden. Ein Verlust des „Generalschlüssels“ würde in diesem Fall bedeuten, dass der Angreifer den zufällig erzeugten Schlüssel dechiffrieren und somit die *PIDs* der Patienten ermitteln kann. Lediglich die Erzeugung von „Referenzdatenbanken“ ohne Kenntnis des Generalschlüssels und somit Angriffe auf den o. g. Schlüssel wären erschwert.[47]

Sollte der Angreifer Login-Informationen eines behandelnden Arztes ausspähen, hätte er höchstens Zugang zu dessen Patientendaten. Nur in seltensten Fällen[48] würde sich ein solcher Angriff lohnen. Wesentlich gewinnbringender wäre dagegen das Ausspähen einer größeren Menge von Patientendaten. Er könnte z. B. durch Sniffing-Angriffe versuchen, entweder die Identitäten mehrerer behandelnder Ärzte[49] oder Administrationskräfte des Forschungsnetzes zu kompromittieren. Denkbar wäre es außerdem, dass der Angreifer gezielt versucht, die Daten einiger weniger (oder gar eines einzelnen) Patienten auszuspähen. Dies könnte dann der Fall sein, wenn diese Daten für ihn einen höheren Wert darstellen.[50] Ein Angreifer könnte auch versuchen, die Forschungsergebnisse der Netzwerkteilnehmer zu seinem finanziellen Vorteil zu nutzen. Es ist nicht auszuschließen, dass diese Art von Angriffen von professionellen Angreifern durchgeführt wird, die im Dienste großer interessierter Organisationen stehen.[51] Da Patientendaten unabhängig von der Behandlungsdatenbank

[47] Ein verschlüsselter *PID* in einer jeden neuen pseudonymisierten Auswertung würde einen anderen Wert ergeben. Dadurch wäre die Sammlung von Referenzdaten für einen Depseudonymisierungsangriff oder einen Angriff gegen den kryptografischen Schlüssel erschwert.

[48] Zum Beispiel bei prominenten Patienten.

[49] Da Wissenschaftler keinen Zugang zu den identifizierenden Daten haben, kann man mit einer Ärzte-ID wesentlich wertvollere Informationen gewinnen.

[50] Zum Beispiel ein Arbeitgeber, der mehr über den gesundheitlichen Zustand seines (potenziellen) Angestellten erfahren möchte.

[51] Sicherheitsexperten beobachten eine zunehmende Kommerzialisierung der Angreifer-Szene. Eine wachsende Zahl von IT-Experten macht das Erstellen von Malware und Ausspähen von fremden Daten zu ihrer Haupttätigkeit (vgl. [Fab08]). Manche Autoren sprechen gar von neuen Märkten, in denen das Know-How und die Infrastruktur für Angriffe gehandelt werden (vgl. [Sch05a]), und schlagen die Einführung eines Index, der analog zum beispielsweise Dow Jones die Entwicklung dieser Märkte reflektieren soll (vgl. [Gee10]).

existieren, und *PID* das einzige Verbindungsglied zwischen den beiden Datenbanken ist, könnte der Angreifer versuchen, eine der beiden Datenbanken unter seine Kontrolle zu bringen. Abhängig davon, welche der beiden Datenbanken er kompromittiert, könnte er versuchen, entsprechende Informationen aus der anderen Datenbank zu gewinnen.[52] Eine erhöhte Reidentifizierungsgefahr entsteht dabei durch den Abgleich von externen Informationen sowie Datenakkumulation. Diese Gefahren sowie Schutzmechanismen werden im Abschnitt C.3.8 „Verschlüsselung und Signaturen“ angesprochen. Das absolute Schreckensszenario für ein Forschungsnetz ist die gleichzeitige Kompromittierung der beiden Datenbanken mit Patienten- und Behandlungsdaten, die über *PID* zusammengeführt werden könnten. Maßnahmen in einem solchen Fall sind im Abschnitt 3.3.3 „Organisation und Gestaltung von Notfallvorsorgemaßnahmen“ beschrieben.
Ein Angreifer könnte schließlich auch destruktiv vorgehen oder ein destruktives Vorgehen androhen, um beispielsweise Geld vom Forschungsnetzbetreiber zu erpressen. Er könnte z. B. versuchen, die Arbeit des Forschungsnetzes zu diskreditieren indem er das Vertrauen der Öffentlichkeit dem Netz entzieht oder einfach die in seiner Gewalt befindlichen Daten für die Forschung unbrauchbar macht oder dies androht.[53] Ein Angreifer könnte außerdem versuchen, die Zugriffsberechtigungen bestimmter Ärzte zu manipulieren oder deren Zugänge zu deaktivieren,[54] was zu einem DoS-Angriff führen würde. Folgende Angreiferprofile sind wahrscheinlich (vgl. [SGF02, S. 13 ff.]):

- *Mitarbeiter und Teilnehmer des Forschungsnetzes:* Mitarbeiter und Teilnehmer des Forschungsnetzes könnten versuchen, Zugang zu Daten bestimmter Patienten zu erhalten. Dies kann sowohl aus persönlicher Neugier, wegen des möglichen Verkaufs der Daten an Dritte (z. B. Presse oder Wirtschaft) oder aufgrund des äußeren Drucks (Erpressung, Nötigung etc.) erfolgen. Außerdem könnte ein Forschungsnetzteilnehmer aus persönlichen oder finanziellen Gründen an der Sabotage des Forschungsnetzbetriebs interessiert sein. Dies könnte er durch die Veröffentlichung von Daten oder durch die Störung des Betriebs (DoS) erreichen. Eine nicht zu unterschätzende Gefahr birgt auch die ungewollte z. B. durch Nachlässigkeit des Mitarbeiters bzw. Forschungsnetzteilnehmers hervorgerufene Preisgabe von Informationen in sich.

- *Wirtschaftliche Organisationen:* Die Vertreter der Wirtschaft (z. B. Versicherungsunternehmen, Banken oder Arbeitgeber) wären vermutlich entweder an den Daten

[52] Zum Beispiel kompromittierte Patientendatenbank: „Welche Einträge existieren in der Behandlungsdatenbank für den Patienten mit dem *PID* „ABC“?“ Kompromittierte Behandlungsdatenbank: „Welche Patienten wurden in der letzten Zeit mit dem Medikament „XYZ“ behandelt?“

[53] So existieren Schädlinge, die Benutzerdaten verschlüsseln. Der Besitzer wird aufgefordert, eine Geldsumme auf das Konto des Erpressers zu überweisen mit der Aussicht, den Schlüssel für seine Daten wieder zu bekommen. Auch die Erpressungsversuche durch die Androhung von DDoS fanden mehrmals statt.

[54] Ein Angreifer könnte z. B. versuchen die „Identitäten“ bestimmter Ärzte zu „stehlen“ oder durch das mehrmalige Falschanmelden mit entsprechenden Kennungen die Benutzerkonten zu deaktivieren.

bestimmter Patienten oder aber auch an den Daten eines größeren Personenkreises interessiert. Banken und Versicherungen sind ständig auf der Suche nach Nischenmärkten, um dem weicher werdenden Markt zu entfliehen. Sollte es gelingen, Patientendaten in einem größeren Umfang zu reidentifizieren, wäre man z. B. in der Lage, einen risikoreichen Kundenstamm von dem Verkauf bestimmter (Versicherungs)Produkte auszuschließen. Gleichzeitig könnte man auch ein bestimmtes Produkt, das an die besonderen Bedürfnisse eines Personenkreises angepasst ist, herzustellen und das optimierte Produkt an diese Personen zu verkaufen, was zu einem Konkurrenzvorsprung führen würde. Wirtschaft kann außerdem an den Datensätzen einzelner Personen (z. B. zwecks besserer Risikoeinschätzung) interessiert sein. Gelegentlich kommt es zu einer rechtlichen Auseinandersetzung zwischen Vertragsparteien. So wird z. B. oft die Frage gestellt, ob die gesundheitliche Beeinträchtigung einer Person als Folge des Schadenereignisses oder als Kumulation der bereits vorhandenen Vorschäden/Vorerkrankungen einzustufen ist. Obwohl die illegal erworbenen Patienteninformationen vom Gericht generell als nicht verwertbare Beweismittel angesehen werden,[55] könnten diese Anhaltspunkte liefern, um bei den ärztlichen Gutachten gezielt nach entsprechenden Beweisen zu suchen. Auch bei der Vergabe von Großaufträgen könnten die Forschungsnetzinformationen wertvoll sein, wenn man sich über den Zustand des Auftragnehmers informieren möchte. Informationen über den gesundheitlichen Zustand des Geschäftsführers eines Partnerunternehmens können die Auftragsvergabe beeinflussen.

- *Strafverfolgungsbehörden und Geheimdienste:* Forschungsdaten können die Begehrlichkeiten der bei den Ermittlungen ihre Grenzen überschreitenden Strafverfolgungsbehörden und Geheimdienste wecken. Analog zu wirtschaftlichen Organisationen können diese sowohl an Daten einzelner Patienten als auch an kompletten Datenstämmen interessiert sein.

- *Öffentlichkeit und Presse:* Ein weiterer dankbarer Abnehmer für Informationen jeglicher Art ist die Öffentlichkeit. Besonders bei prominenten Patienten ist es anzunehmen, dass verstärkt Versuche unternommen werden, um Einzelheiten im Hinblick auf den Gesundheitszustand dieser Personen zu erfahren.

- *Kriminelle:* Kriminelle könnten versuchen, durch Erpressung der Probanden finanzielle Vorteile zu erlangen. Da die Massenerpressung relativ aufwendig und vor Strafverfolgungsbehörden schwer zu verschleiern ist, ist die Gewinnung einzelner Datensätze und gezielte Erpressung von Individuen wahrscheinlicher. Selbstverständlich ist auch für Kriminelle der gesamte Datenstamm als Ausgangspunkt, um potenzielle Erpressungsopfer ausfindig zu machen, von großem Interesse.

[55] Vgl. § 245 StPO Abs. 1, 2 StPO. Bei Abwesenheit von weiteren Beweismitteln außer illegal erworbener (hier – Patientendaten aus dem Forschungsnetz) werden die illegal gesammelten Daten vom Gericht nicht anerkannt.

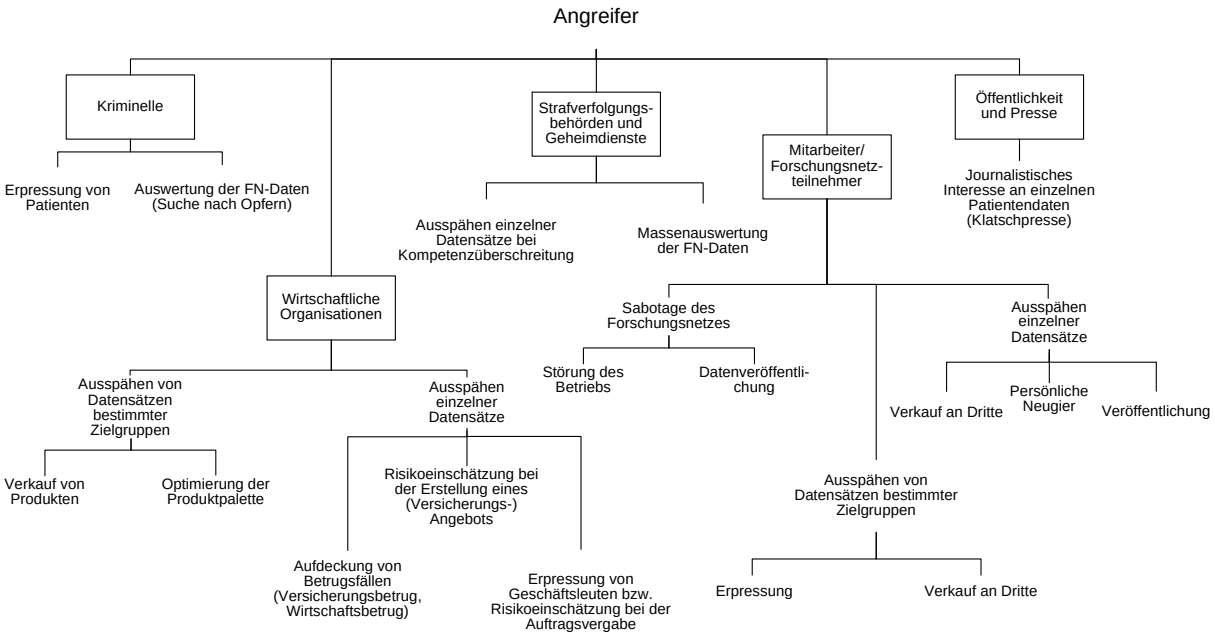

Abbildung 22.: Angreifer und ihre Motive: Die Motive unterschiedlicher Angreifer können sich überschneiden. In vielen Fällen ist ein Angreifer auf das Interesse einer Drittpartei (Presse, Wirtschaft etc.) an den Forschungsnetzdaten angewiesen.

Die dargestellten Bedrohungsszenarien verdeutlichen die möglichen Überschneidungen, die es zwischen den Motiven mehrerer Angreifer geben kann. Sie zeigen auf, dass in den meisten Fällen ein Angreifer auf das Interesse einer Drittpartei (Presse, Wirtschaft etc.) an den Forschungsnetzdaten angewiesen ist. Die Abbildung 22 stellt die Angreifer und ihre Motive in Form eines sogenannten Angriffsbaumes grafisch dar.

B. Systematische Literaturrecherche

B.1. Vorgehensweise bei der Durchführung der Literaturrecherche

Die Primärsuche wurde in den zehn Literaturdatenbanken durchgeführt:

KVK: Der Karlsruher Virtuelle Katalog (KVK) ist eine übergreifende Suchoberfläche für Bibliotheks- und Buchhandelskataloge im Internet weltweit.

MEDLINE/PubMed: PubMed ist ein Service der National Library of Medicine und beinhaltet 15 Millionen Artikel im Bereich der Biomedizin.

ISI Web of Science: ISI Journal Citation Reports, JCR, JCR Science Edition, JCR Social Sciences Edition, ISI Web of Knowledge.

DNB: Der gesetzliche Sammelauftrag der Deutschen Nationalbibliothek (DNB) umfasst ab 1913 in Deutschland veröffentlichte Medienwerke (auf der Grundlage des Pflichtexemplarrechts) und im Ausland veröffentlichte deutschsprachige Medienwerke, Übersetzungen deutschsprachiger Medienwerke in andere Sprachen und fremdsprachige Medienwerke über Deutschland.

Springer ZBS: Zentralblattsystem des Springer-Verlags bzw. SpringerLink/Springer Online Journal Archives. Das Archiv enthält die Volltexte von über 1.050 Zeitschriften des Springer-Verlages (einschließlich Kluwer), i. d. R. ab Volume 1 bis zum Jahr 2002. Ab 2009 ist das Lecture Notes Archiv in den Springer Online Journal Archives enthalten.

CC MED: Die Literaturdatenbank CC MED (Current Contents Medizin) weist Aufsätze aus über 1.300 deutschsprachigen oder in Deutschland verlegten Zeitschriften ab dem Erscheinungsjahr 2000 nach, die meist nicht in PubMed ausgewertet werden. Insofern ergänzt die Recherche in CC MED eine Literatursuche in PubMed.

ACM Digital Library: Recherche in den elektronischen Publikationen der Association for Computing Machinery (ACM): Zeitschriften, Kongressberichte, Newsletters, Reviews, Special Interest Groups u. a.; mit Zugriff auf den Volltext, der in der Regel als pdf-Datei angeboten wird.

IEEE Digital Library: Die Datenbank bietet den Volltextzugriff auf ca. 2 Mio. Dokumente von IEEE (Institute of Electrical and Electronics Engineers):

- ca. 151 IEEE Journals, Magazines, Transactions,

- über 1.000 IEEE Conference Proceedings (ca. 10.000 Einzelschriften),
- über 2.100 gültige IEEE Normen/Standards.

Enthalten sind außerdem Publikationen der IEE/IET (Institution of Engineering and Technology) (ca. 25 IET Journals und ca. 2.400 IET Conference Proceedings, Colloquium und Seminar Digests.)

ASTM: Die ASTM International (ursprünglich American Society for Testing and Materials) ist eine internationale Standardisierungsorganisation mit Sitz in West Conshohocken, USA. Auf der ASTM-Webseite sind über 12.000 Dokumente zu den technischen Standards für Waren und Dienstleistungen veröffentlicht.

Google Scholar: Google Scholar bietet eine allgemeine Suche nach wissenschaftlicher Literatur. Folgende Bereiche und Quellen werden für die Suche verwendet: Seminararbeiten, Magister-, Diplom- sowie Doktorarbeiten, Bücher, Zusammenfassungen und Artikel, die aus Quellen wie akademischen Verlagen, Berufsverbänden, Magazinen für Vorabdrucke, Universitäten und anderen Bildungseinrichtungen stammen.

Die Tabelle 17 fasst die verwendeten Suchbegriffe mit den vergebenen Rankingwerten zusammen. Die Tabelle 18 protokolliert die Ergebnisse der Suche für den einzelnen Literaturdatenbanken.

Definition und Klassifikation der Suchbegriffe

Primär-suche	Sicherheit AND (Metrik* OR Messen OR Messung* OR Kennzahl* OR Messbarkeit)	Security AND (Metric* OR Measure* OR Measurement* OR Measuring OR Measurability)

Präzisierung der Suche auf der Basis des Suchbegriff-Rankings

Such-begriffe	Effektivität, Effizienz, Kennzahlensystem(e), Kosten-Nutzen-Analyse, KNA, Sicherheitsinvestition(en), Sicherheitsmaßnahme(n), Wirksamkeit, Framework(s), Rahmen, Rahmenwerk(e)	Efficiency, Effectiveness, Performance, Figure(s), Ratio(s), Ratio System(s), Cost Benefit Analysis, CBA, Security Invest(s) or Investment(s), Safety or Security Measure(s), Effectiveness, Efficiency, Framework(s)

Ranking	Deutsch	Englisch	Häufig verwendete Begriffe und Ausdrücke
2	Analyse	Analysis, Assessment	Risikoanalyse
1	Bewertung, Bewerten	Assess, Assessment	Risikoanalysen & Bewertungen
2	Effektivität ISMS	Effectiveness of Information Security System (ISMS)	
2	Effektivität von Sicherheitskontrollen	Effectiveness of Security Controls	
1	Effektivität, Effizienz	Efficiency, Effectiveness, Performance	Effektivität & Sicherheitsmaßnahmen
3	Effektivität/Effizienz der Informationssicherheit	Effectiveness of Information Security	
2	Effektivitätsmessung	(Effectiveness or Efficiency) and (Measurement or Metrics or Measure)	
1	Framework(s), Rahmen, Rahmenwerk(e)	Framework(s)	
2	Investition(en)	Invest(s), Investment(s)	
3	IT-Sicherheit, Informationssicherheit	IT Security, Information Security	Messbarkeit & IT-Sicherheit
1	Kennzahl(en)	Figure(s), Ratio(s)	
1	Kennzahlensystem(e)	Ratio System(s)	
1	Kosten-Nutzen-Analyse, KNA	Cost Benefit Analysis, CBA	
3	Management	Management	Sicherheitsmanagement
2	Maßnahme(n)	Measure(s), Measurement(s)	
0	Messbarkeit	Measurability	Messbarkeit & IT-Sicherheit
2	Messkriterien	Measurement Criteria	
2	Messverfahren	Measurement Approach	
0	Metrik(en), Messen, Messung(en), Kennzahl(en)	Metric(s), Measure(s), Measurement(s), Measuring	
3	Niveau	Level	Niveau des Risikos
3	Portfolio	Portfolio	
3	Quantifizieren	Quantify	
3	Risiko/Risiken	Risk(s)	Risikoanalyse
3	Risiko/Risiken	Risk(s)	Niveau des Risikos
2	Risikoanalyse(n)	Risk Analysis	Risikoanalysen & Bewertungen
2	Risikobewertung, Risikoabschätzung	Risk Evaluation	
3	Risikomanagement	Risk Management	
3	Risikoportfolio	Risk Portfolio	
3	Risiskobewertung, Risikobeurteilung	Risk Assessment	
2	Schlüsselindikator, Leisttungsindikator	Key Performance Indicator, KPI	
0	Sicherheit	Security	Sicherheitsmanagement
1	Sicherheitsinvestition(en)	Security Invest(s) or Investment(s)	Wirtschaftlichkeit von Sicherheitsinvestitionen
1	Sicherheitsmaßnahme(n)	Safety or Security Measure(s)	
2	Steuerung	Control(s)	Steuerung von Sicherheitsinvestitionen
1	Wirksamkeit	Effectiveness, Efficiency	
2	Wirtschaftlichkeit, Kosteneffizienz, Kosteneffektivität	Cost Effectiveness, Cost Efficiency	Wirtschaftlichkeit von Sicherheitsinvestitionen

Ranking-Legende		Einschränkung der Suchtreffer	
0	Primäre Suche	Voreinstellung, Jahr der Publikation:	2005 - 2011
1	Präzisierung der Suche	Voreinstellung, Sprachen:	Englisch, Deutsch
2	Sekundäre Filterung der Suchergebnisse		
3	Verwendung im Kontext mit anderen Begriffen		

Tabelle 17.: Bestimmung der Suchbegriffe: Während der ersten Phase der systematischen Literaturrecherche wurden die Bestandteile des Themas in Fachtermini übertragen, systematisch gesammelt und als Suchbegriffe und ihre Relevanz (Ranking) für das Thema „Sicherheits- und Risikometriken“ in tabellarischer Form notiert (s. a. Abschnitt 2.1.1.4 „Systematische Literaturrecherche“).

Datenbank	Link	Such-datum	Verwendete Suchbegriffe	Einschränkung	#Suchtreffer
KVK (Karlsruher Virtueller Katalog)	http://rzblx10.uni-regensburg.de/dbinfo/detail.php?bib_id=subgo&titel_id=930	17.12.2011	En: security AND (metric* OR measure* OR measurement* OR measuring OR measurability); KOBV: 133, Stdtbibl. Berlin: 54, SWB: 106, DNB: 42, GBV: 306, HEBIS: 42 De: Sicherheit AND (Metrik* OR Messen OR Messung* OR Kennzahl* OR Messbarkeit); KOBV: 6, Stdtbibl. Berlin: 1, SWB: 5, DNB: 38, GBV: 13, HEBIS: 5	Sprachen: En, De Publ.-Jahr: 2005-2011	En: 683 De: 68
MEDLINE/ PubMed	http://rzblx10.uni-regensburg.de/dbinfo/detail.php?bib_id=subgo&colors=&ocolors=&lett=f&titel_id=294	17.12.2011	En: security AND metric* (1 Suchtreffer), security AND measure* (97 Suchtreffer), security AND measurement* (18 Suchtreffer), security AND measuring (18 Suchtreffer), security AND measurability) De: Sicherheit AND Metrik*, Sicherheit AND Messen, Sicherheit AND Messung*, Sicherheit AND Kennzahl*, Sicherheit AND Messbarkeit	Sprachen: En, De Publ.-Jahr: 2005-2011	En: 7 De: 0
ISI Web of Science	http://rzblx10.uni-regensburg.de/dbinfo/detail.php?bib_id=subgo&titel_id=359	18.12.2011	En: security AND (metric* OR measure* OR measurement* OR measuring OR measurability) De: Sicherheit AND (Metrik* OR Messen OR Messung* OR Kennzahl* OR Messbarkeit)	Sprachen: En, De Publ.-Jahr: 2005-2011	En: 157 De: 1
DNB (Deutsche Nationalbibliothek)	https://portal.d-nb.de/	18.12.2011	En: security AND metric* (4 Suchtreffer), security AND measure* (6 Suchtreffer), security AND measurement* (4 Suchtreffer), security AND measuring (4 Suchtreffer), security AND measurability (19 Suchtreffer) De: Sicherheit AND Metrik*, Sicherheit AND Messen (1 Suchtreffer), Sicherheit AND Messung* (11 Suchtreffer), Sicherheit AND Messbarkeit	Sprachen: En, De Publ.-Jahr: 2005-2011	En: 37 De: 12
Zentralblattsystem des Springer-Verlags bzw. Springer-Link/Springer Online Journal Archives	http://rzblx10.uni-regensburg.de/dbinfo/detail.php?bib_id=subgo&titel_id=6261	17.12.2011	En: security and (metric* or measure* or measurement* or measuring or measurability) De: Sicherheit AND (Metrik* OR Messen OR Messung* OR Kennzahl* OR Messbarkeit)	Sprachen: En, De Publ.-Jahr: 2005-2011	En: 45 De: 0
CC MED (Current Contents Medizin)	http://rzblx10.uni-regensburg.de/dbinfo/detail.php?bib_id=subgo&colors=&ocolors=&lett=fs&titel_id=453	17.12.2011	En: security AND (metric* OR measure* OR measurement* OR measuring OR measurability) De: Sicherheit AND (Metrik* OR Messen OR Messung* OR Kennzahl* OR Messbarkeit)	Sprachen: En, De Publ.-Jahr: 2005-2011	En: 194 De: 32
ACM Digital Library	http://rzblx10.uni-regensburg.de/dbinfo/detail.php?bib_id=subgo&titel_id=3162	17.12.2011	En: security and metric* (Suchtreffer 28), security and measure* (Suchtreffer 8), security and measuring (Suchtreffer 9), security and measurability (Suchtreffer 2) De: Sicherheit and Metrik*, Sicherheit and Messen, Sicherheit and Messung*, Sicherheit and Kennzahl*, Sicherheit and Messbarkeit	Sprachen: En, De Publ.-Jahr: 2005-2011	En: 47 De: 0
IEEE Digital Library	http://rzblx10.uni-regensburg.de/dbinfo/detail.php?bib_id=subgo&titel_id=2172	17.12.2011	En: security AND metric* (Suchtreffer 49), security AND measure* (Suchtreffer 88), security AND measuring (Suchtreffer 18), security AND measurability (Suchtreffer 1) De: Sicherheit AND Metrik*, Sicherheit AND Messen, Sicherheit AND Messung*, Sicherheit AND Kennzahl*, Sicherheit AND Messbarkeit	Sprachen: En, De Publ.-Jahr: 2005-2011	En: 156 De: 0
ASTM, American Society for Testing and Materials	http://www.astm.org/Standard/index.shtml	18.12.2011	En: security AND metric* (Suchtreffer 41), security AND measure* (Suchtreffer 160), security AND measurement (Suchtreffer 173), security AND measuring (Suchtreffer 139), security AND measurability De: Sicherheit AND Metrik*, Sicherheit AND Messen, Sicherheit AND Messung*, Sicherheit AND Kennzahl*, Sicherheit AND Messbarkeit	Sprachen: En, De Publ.-Jahr: 2005-2011	En: 673 De: 0
Google Scholar	http://scholar.google.de	18.12.2011	En: security metric (36 Suchtreffer), security metrics (191 Suchtreffer), security measure (112 Suchtreffer), security measures (467 Suchtreffer), security measurement (143 Suchtreffer), security measurements (51 Suchtreffer), security measuring (160 Suchtreffer), security measurability (3 Suchtreffer) De: Sicherheit Metrik, Sicherheit Metriken, Sicherheit Messen, Sicherheit Messung (2 Suchtreffer), Sicherheit Messungen, Sicherheit Kennzahl, Sicherheit Kennzahlen, Sicherheit Messbarkeit	Sprachen: En, De Publ.-Jahr: 2005-2011 Mindestens Zusammenfassungen	En: 1.163 De: 2

Tabelle 18.: Systematische Literaturrecherche: Die Primärsuche berücksichtigte zehn Literaturdatenbanken und lieferte 3.275 Suchtreffer.

B.2. Ausgewählte Publikationen zur Messung des Sicherheitsniveaus und Effizienzbewertung von Sicherheitsmaßnahmen

Verweis, Titel: [AAP08], *„The Risks with Security Metrics“*

Ansatz/Inhalte: Neben der Vorstellung eines Metrikansatzes, der auf der Fehler- bzw. Angriffsbaumanalyse basiert, enthält diese Publikation einige Aussagen über die Qualität von Sicherheitsmetriken. Die Autoren stellen fest, dass die Vorteilhaftigkeit einer Sicheheitsmetrik an ihrer Zielsetzung zu messen ist und im Laufe der Zeit variieren kann.

Verweis, Titel: [AASM11], *„Defining and Computing a Value Based Cyber-Security Measure“*

Ansatz/Inhalte: Vorschlag für eine Stakeholderanalyse-basierte Sicherheitsmetrik. Im Mittelpunkt der Betrachtung stehen die unterschiedlichen Zielsetzungen und Bewertungen der Stakeholder im Hinblick auf die Verfügbarkeit eines Systems.

Verweis, Titel: [AD01], *„OCTAVE Method Implementation Guide“*

Ansatz/Inhalte: Die beschriebene an der Carnegie Mellon University in Zusammenarbeit mit dem CERT/CC entwickelte Methode zur Risikobewertung ist frei verfügbar und stützt sich auf Checklisten, Formblätter und Moderationsleitfäden. Der Aufwand für die Durchführung der Risikoanalyse nach der OCTAVE-Methodik ist vergleichbar hoch und erfordert von den Beteiligten fortgeschrittenes Fachwissen (s. a. Abschnitt A.1.6.2).

Verweis, Titel: [AJ10], *„Information Security and Privacy in Healthcare : Current State of Research“*

Ansatz/Inhalte: Abriss der Fachpublikationen zu den Themen Sicherheit und Datenschutz im Gesundheitswesen. Der Anhang enthält eine tabellarische Übersicht der Publikationen, die in 16 Themenbereiche und drei Kategorien (Design, quantitativ und qualitativ) eingeteilt werden (vgl. [AJ10, S. 310 f.]).

Verweis, Titel: [Als10], *„Information Systems Security Measures and Countermeasures: Protecting Organizational Assets from Malicious Attacks“*

Ansatz/Inhalte: Im Artikel werden die Ergebnisse einer Befragung von 56 Sicherheitsverantwortlichen vorgestellt. Bemerkenswert ist der erbrachte statistische Beweis für die Sinnhaftigkeit der Messung des Informationssicherheitsniveaus, da die Messung zur Implementierung von Sicherheitsmaßnahmen und damit zur Erhöhung des Sicherheitsniveaus führt.

Verweis, Titel: [AM06], *„The Economics of Information Security“*

Ansatz/Inhalte: Der Artikel erörtert die Frage nach der Notwendigkeit bzw. Angemessenheit von Sicherheitsinvestitionen aus einer makroökonomischen Perspektive.

Verweis, Titel: [Axe08], *„Accounting for Value and Uncertainty in Security Metrics“*

Ansatz/Inhalte: Der Artikel bietet eine kritische Auseinandersetzung mit den gängigen Arten und etablierten Ansätzen von Sicherheitsmetriken.

Verweis, Titel: [Bay11], *„Alternative Security Metrics“*

Ansatz/Inhalte: Eine kritische Auseinandersetzung mit der aktuellen Praxis im Bereich der Sicherheitsmetriken.

Verweis, Titel: [BBM+08], *„Measuring Cyber Security and Information Assurance“*

Ansatz/Inhalte: In diesem IATAC-Bericht erfolgt eine umfassende Analyse der aktuellen Informationssicherheitsansätze. Neben einer ausführlichen Darstellung des Fortschritts in diesem Bereich wird auf die Notwendigkeit weiterer Forschung nach verlässlichen aussagekräftigen Messansätzen der Informationssicherheit hingewiesen.

Verweis, Titel: [BKY11], *„Information Security Metrics : State of the Art“*

Ansatz/Inhalte: Eine ausführliche Zusammenfassung der aktuellen Ansätze und Probleme der Informationssicherheitsmetriken. Der Report berücksichtigt sowohl die etablierten Normen, Standards und Frameworks als auch die in diesem Bereich geführten Forschungsarbeiten.

Verweis, Titel: [BLP+06], *„Rational Choice of Security Measures via Multi-Parameter Attack Trees“*

Ansatz/Inhalte: Im Mittelpunkt der vorgestellten, auf Angriffsbäumen basierenden, Sicherheitsmetrik steht ein rational handelnder Angreifer. Die Angemessenheit von Sicherheitsinvestitionen wird aus der Abschätzung der Lukrativität von Angriffsszenarien abgeleitet.

Verweis, Titel: [BMGS09], *„Using Security Metrics Coupled with Predictive Modeling and Simulation to Assess Security Processes“*

Ansatz/Inhalte: Die Autoren begründen eine größere Bedeutung von prozessorientierten Sicherheitsmetriken mit der Schwierigkeit, die in unterschiedlichen Teilen einer Organisation gesammelten Kennzahlen sinnvoll zu interpretieren.

Verweis, Titel: [BMS06], *„Assessing the Risk of Using Vulnerable Components“*

Ansatz/Inhalte: Die Autoren beschreiben eine quantitative, graphenbasierte Sicherheitsmetrik. Bei der Berechnung der Angriffspfade steht der minimale Aufwand für einen Angriff im Mittelpunkt. Der Aufbau der Systemarchitektur, die verfügbaren Verwundbarkeiten, die Komponenten und ihre Verbindungen werden dabei berücksichtigt.

Verweis, Titel: [Bro09], *„Information Security Management Metrics : A Definitive Guide to Effective Security Monitoring and Measurement“*

Ansatz/Inhalte: Das Buch bietet im zweiten Kapitel eine gut strukturierte Übersicht der aktuellen Technologien im Bereich der Sicherheitsmetriken. Im dritten Kapitel werden die Eigenschaften von praktisch verwertbaren Sicherheitsmetriken untersucht.

Verweis, Titel: [BRT07], *„Necessary Measures : Metric-Driven Information Security Risk Assessment and Decision Making“*

Ansatz/Inhalte: Der Artikel enthält eine Reihe von Verbesserungsvorschlägen für die Entwicklung von Sicherheitsmetriken. Besonders bemerkenswert ist die Feststellung, dass aktuell ca. ein Drittel der Sicherheitsausgaben keinen positiven Effekt auf die Informationssicherheit haben.

Verweis, Titel: [BSB07], *„Return on Security Investments : Design Principles of Measurement Systems Based on Capital Budgeting“*

Ansatz/Inhalte: Die Autoren zeigen mehrere Möglichkeiten für die ROSI-Definition. Anschließend erörtern sie einen eigenen auf einem Investitionsplan basierenden ROSI-Berechnungsansatz. Als Zahlenbasis werden die Erfahrungswerte aus der Vergangenheit verwendet.

Verweis, Titel: [cis04], *„Report of the Best Practices and Metrics Teams“*

Ansatz/Inhalte: Der Report der CISWG-Arbeitsgruppe enthält 99 Beispielmetriken, die in drei Kategorien (Board, Management und Technik) eingeteilt werden. Die Autoren weisen ausdrücklich darauf hin, dass die Installation aller aufgelisteten Metriken mit einem beträchtlichen Aufwand verbunden ist. Aus diesem Grund schlagen sie eine Einteilung in einen Basissatz mit 65 und einen SME-Satz (Small und Medium Enterprises) mit lediglich 40 Metriken vor.

Verweis, Titel: [CSS+08], *„Performance Measurement Guide for Information Security“*

Ansatz/Inhalte: Eine in Zusammenhang mit den Informationssicherheitsmetriken häufig zitierte Publikation der NIST 800-Reihe. Für nähere Informationen siehe Abschnitt A.1.4 „NIST 800-X (Special Publications)“.

Verweis, Titel: [DB11], *„Guideline for Performance Measures of Information Security of IT Network and Systems“*

Ansatz/Inhalte: Eine an die NIST-Standards angelehnte allgemeine Beschreibung des Prozesses für die Entwicklung von Sicherheitsmetriken.

Verweis, Titel: [DL11], *„Information Security : Concepts, Indicators, Measurements“*

Ansatz/Inhalte: Die vorgestellte Definition der Sicherheit basiert auf drei Faktoren: Vertraulichkeit, Integrität und Verfügbarkeit. Diese Faktoren setzen sich aus den

hierarchisch aufgebauten, präziser werdenden System-, Dienst-, und Prozesseigenschaften zusammen. Eine gewichtete Kombination einzelner Faktoren wird für die Messung des Sicherheitsniveaus vorgeschlagen.

Verweis, Titel: [Dog10], *„Introducing a Framework for Security Measurements“*

Ansatz/Inhalte: Vorschlag für ein Framework zur Sicherheitsmessung[1], das auf einem schutzbedarfsorientierten Ansatz für eine sogenannte semiquantitative Sicherheitsmetrik basiert (vgl. [DHS08]).

Verweis, Titel: [Fab10], *„Measuring Information Security : Guidelines to Build Metrics“*

Ansatz/Inhalte: Der Autor beschreibt die Notwendigkeit und die Vorteile von Sicherheitsmetriken. Anschließend wird die Erstellung von Metriken erläutert, und die Anforderungen an die Messansätze werden genannt.

Verweis, Titel: [Fen10], *„Ontology-based Generation of IT-Security Metrics“*

Ansatz/Inhalte: Vorschlag für die Methodik zur automatisierten Erzeugung von ISO 27001-konformen Sicherheitsmetriken, um die Kontrolleffizienz und die Compliance einer Organisation mit den Informationssicherheitsstandards zu messen.

Verweis, Titel: [FPW07], *„Ein Modell zur dynamischen Investitionsrechnung von IT-Sicherheitsmassnahmen“*

Ansatz/Inhalte: Vorstellung eines betriebswirtschaftlichen Ansatzes zum Bewerten der Vorteilhaftigkeit von Sicherheitsinvestitionen auf der Basis der Kapitalwertmethode. Der Artikel enthält eine, im Jahr 2006 erstellte, tabellarische Übersicht der ausgewählten Veröffentlichungen zum Thema Risikomanagement bzw. IT-Sicherheitsmanagement [FPW07, S. 517].

Verweis, Titel: [Hec08], *„On System Security Metrics and the Definition Approaches“*

Ansatz/Inhalte: Eine ausführliche Darstellung der existierenden Ansätze zur Beschreibung von Sicherheitsmetriken und ihrer Klassifikation.

Verweis, Titel: [Her07], *„Complete Guide to Security and Privacy Metrics : Measuring Regulatory Compliance, Operational Resilience, and ROI“*

Ansatz/Inhalte: Eine umfangreiche[2] Referenz zum Aufbau von Metrik-Systemen mit den Schwerpunkten Compliance, Verfügbarkeit und ROI. Der Ansatz orientiert sich an der Gesetzgebung und den Standards in den USA und Kanada (Sarbanes-Oxley Act, HIPAA etc.). Die Metrik-Vorschläge werden mit einer Vielzahl von Beispielen untermauert. Das Buch bietet eine ausführliche Auseinandersetzung mit der Thematik der ROI-Berechnung für die Sicherheitsinvestitionen.

[1] Security Measurement Framework.

[2] Und teilweise langatmige.

Verweis, Titel: [Her10], *„OSSTMM 3 : Open Source Security Testing Methodology Manual : Contemporary Security Testing and Analysis“*

Ansatz/Inhalte: OSSTMM wurde erstmals im Jahr 2001 von der ISECOM veröffentlicht und ist ein Standard zur Durchführung technischer Audits. Die Sicherheitsmetriken werden im vierten Kapitel „Operational Security Metrics“ ausführlich beschrieben. Die gewählte Betrachtungsweise ist „Asset Value“-bezogen und verwendet die sogenannten RAV-Einheiten zur Darstellung des Sicherheitsniveaus (vgl. [Her10, S. 62 ff.]).

Verweis, Titel: [HP06], *„Measuring the Effectiveness of Your ISMS Implementations Based on ISO/IEC 27001“*

Ansatz/Inhalte: Hilfestellung zur Effektivitätsmessung der ISMS-Implementierung unter Benutzung von ISO/IEC 17799:2005 als Vorgänger von ISO/IEC 27002:2005 und ISO/IEC 27001:2005. Die Publikation enthält Anleitung zur Entwicklung von passenden Metriken auf der Basis der genannten ISO-Standards (s. a. Abschnitt A.1.1).

Verweis, Titel: [IB12], *„Extending Attack Graph-Based Security Metrics and Aggregating Their Application“*

Ansatz/Inhalte: Im Artikel werden die Weiterentwicklungsmöglichkeiten für die Angriffspfad-basierten Metrikansätze beschrieben. Bemerkenswert ist die Untersuchung der Einsatzmöglichkeiten mehrerer Metriken für den Vergleich des Sicherheitsniveaus (decision metrics) und Ermittlung weiterführender Informationen zum errechneten Sicherheitsstand (assistive metrics).

Verweis, Titel: [irc05], *„Hard Problem List“*

Ansatz/Inhalte: Diese IRC-Publikation[3] bezeichnet die Entwicklung von aussagekräftigen Sicherheitsmetriken als eines der acht aktuellen Herausforderungen auf dem Gebiet der Informationssicherheit. Bemerkenswerterweise enthält die Publikation einen Vorschlag für den „Zehnjahresplan“, nach welchem die quantitativen Sicherheitsmetriken mindestens die Qualität der Risikokennzahlen im Finanzwesen erreichen sollen.

Verweis, Titel: [iso08a], *„ISO 9001:2008 : Quality Management Systems : Requirements“*

Ansatz/Inhalte: Die ISO-Norm 9001:2008 definiert die Anforderungen an das Qualitätsmanagement (QM) und bildet die Basis für ein umfassendes Qualitätsmanagement-System (QM-System). Das Thema der Messbarkeit der QM-Performance wird in den Abschnitten 7.6 „Control of monitoring and measuring equipment“ und 8 „Measurement, analysis and improvement“ bzw. 8.2 „Monitoring and measurement“ behandelt. Dabei wird die Anforderung gestellt, ein Control Monitoring- und Measurement-System zu installieren. Diese Empfehlung bleibt jedoch allgemein formuliert, sodass

[3] INFOSEC Research Council.

unbeantwortet bleibt, wie ein solches System im Zusammenhang mit den Sicherheitsmaßnahmen bzw. der Bewertung ihrer Sinnhaftigkeit und Notwendigkeit einzuordnen ist.

Verweis, Titel: [Jan09], *„Directions in Security Metrics Research“*

Ansatz/Inhalte: Diese häufig zitierte NIST-Publikation beschreibt die existierenden Sicherheitsmetrikansätze und erläutert die Notwendigkeit für die weitere Forschung auf diesem Gebiet.

Verweis, Titel: [Jaq07], *„Security Metrics : Replacing Fear, Uncertainty, and Doubt“*

Ansatz/Inhalte: Eine durch die Simplifizierung der Zusammenhänge oft enttäuschende Einführung in die Sicherheitsmetriken als Referenzwerk. Die Nachteile gängiger Sicherheitsmetriken (z. B.: ALE-Methode) werden teilweise gut und ausführlich dargestellt.

Verweis, Titel: [JM10], *„A Framework for Software Security Risk Evaluation using the Vulnerability Lifecycle and CVSS Metrics“*

Ansatz/Inhalte: Vorschlag für ein CVSS-basiertes Framework zur Messung der Softwaresicherheit. Der Vorschlag sieht die Ableitung von Auswirkungen von Softwareverwundbarkeiten aus den CVSS-Informationen vor.

Verweis, Titel: [KB11], *„Modelling Static and Dynamic Aspects of Security : A Socio-Technical View on Information Security Metrics“*

Ansatz/Inhalte: Der Artikel enthält eine ausführliche Darstellung der aktuellen Ansätze im Bereich der Sicherheitsmetriken.

Verweis, Titel: [KH06], *„Security Metrics Management : How to Measure the Costs and Benefits of Security“*

Ansatz/Inhalte: Eine Übersicht der möglichen Sicherheitsmetriken begleitet von Überlegungen zu deren Gestaltungsmöglichkeiten und Bedeutung. Die Kapitel II bis IV beschäftigen sich mit den administrativen, physikalischen und operationellen Metriken, die an einem praktisch angelehnten Beispiel anhand eines fiktiven Unternehmens präsentiert werden.

Verweis, Titel: [Kle06], *„Measuring Security“*

Ansatz/Inhalte: Besonders interessant ist die Sicht des Autors auf die ROI-Berechnung der Sicherheitsinvestitionen: Da diese keinen Ertrag erbringen, bedeuten die Sicherheitsausgaben in erster Linie Kosten. Wenn die getätigten Sicherheitsinvestitionen effektiv wirken, kommt es nicht zu einem Sicherheitsvorfall. Dadurch ist die für die ROSI-Kalkulation häufig angewendete Analogie zu der Opportunitätskostenberechnung nur bedingt anwendbar.

Verweis, Titel: [KLR+10b], *„Towards an Abstraction Layer for Security Assurance Measurements“*

Ansatz/Inhalte: Ausgehend von der in [HSD07] vorgestellten Taxonomie wird eine Abstraktionsschicht für die Sicherheitsmetriken vorgestellt. Diese Schicht soll eine Stabilität der Messbarkeit trotz der Veränderung des Systems und der für dieses System geltenden Risiken sicherstellen.

Verweis, Titel: [KMY10], *„Formal Approach to Security Metrics : What Does „More Secure“ Mean for You?“*

Ansatz/Inhalte: Versuch, einen formalisierten Vergleich von Sicherheitsmetriken zu ermöglichen. Neben einigen Beispielmetriken wie beispielsweise der Anzahl der möglichen Angriffe, den Mindestkosten eines Angriffs und der Angriffsreduktion werden in dieser Publikation die bisherigen/historischen Versuche zur Formalisierung der Qualitätsbewertung von Sicherheitsmetriken diskutiert.

Verweis, Titel: [KMY11], *„Formal Analysis of Security Metrics and Risk“*

Ansatz/Inhalte: Versuch einer formalen Definition für die Sicherheitsmetriken. Bemerkenswert ist die Feststellung, dass die Sicherheitsmetriken und die Risiken i. d. R. unabhängig voneinander definiert werden.

Verweis, Titel: [KS05], *„Analyzing Vulnerabilities and Measuring Security Level at Design and Exploitation Stages of Computer Network Life Cycle“*

Ansatz/Inhalte: Simulationsbasierter Ansatz zur Messung der Netzwerksicherheit in Verbindung mit einem SAS-System (s. a. Abschnitt A.1.6.5 „SAS-Systeme“).

Verweis, Titel: [KSP+07], *„Defining an Effective Security Metrics Program : Best Practices“*

Ansatz/Inhalte: In diesem Bericht wird die Unausgereiftheit der aktuellen Messansätze der Informationssicherheit durch eine Forrester-Studie untermauert. Anschließend wird der Vorschlag unterbreitet, die Sicherheitsmetriken aus der Perspektive der Eignung dieser Metriken für die Erfüllung der Organisationsziele bzw. der Unterstützung strategischer Managemententscheidungen zu entwickeln.

Verweis, Titel: [Küt09], *„Kennzahlen in der IT : Werkzeuge für Controlling und Management“*

Ansatz/Inhalte: Systematische Betrachtung verschiedener etablierter Kennzahlensysteme. Im Mittelpunkt dieses aus der Controllingsicht geschriebenen Referenzwerks steht die Steuerung der IT-Dienstleister.

Verweis, Titel: [LA05], *„Why to Adopt a Security Metric? A Brief Survey“*

Ansatz/Inhalte: Neben einer Untersuchung von Faktoren, die für die Intensivierung der

Forschungsbemühungen nach belastbaren Sicherheitskennzahlen sprechen, nennt diese Publikation fünf Eigenschaften, die eine effiziente und nützliche Sicherheitsmetrik erfüllen muss: Klarheit, Objektivität, Wiederholbarkeit, Einfachheit und Übersichtlichkeit (im Sinne von Priorisierung bzw. Konzentration auf bedeutsame Informationssicherheitsaspekte).[4]

Verweis, Titel: [LFK+11], *„Model-based Security Metrics Using ADversary VIew Security Evaluation (ADVISE)“*

Ansatz/Inhalte: Die vorgestellte quantitative Sicherheitsmetrik basiert auf der Einteilung von potenziellen Angreifern in Gruppen in Abhängigkeit von ihren Zielsetzungen, ihnen zur Verfügung stehenden Mitteln, Ressourcen etc. Anschließend wird untersucht, welche Angriffspfade für ein System existieren, und wie lukrativ diese für die betrachteten Angreiferkategorien sind.

Verweis, Titel: [Man05], *„Security Metrics and Measurements for IT“*

Ansatz/Inhalte: Neben der Skizzierung einer Taxonomie für die Sicherheitsmetriken mit der Angabe einiger Beispiele werden die Qualitätsanforderungen an die Sicherheitsmetriken erörtert.

Verweis, Titel: [MO11], *„Governing Information Security in Conjunction with COBIT and ISO 27001“*

Ansatz/Inhalte: Der Artikel untersucht die Vor- und Nachteile der ISMS-Steuerung durch die Kombination von COBIT und ISO 27001 (s. a. Abschnitte A.1.1, A.1.2).

Verweis, Titel: [MT06], *„Kosten & Nutzen von IT-Sicherheit“*

Ansatz/Inhalte: Im Mittelpunkt des HMD-Heftes steht die Wirtschaftlichkeitsbetrachtung von Sicherheitsinvestitionen. Insbesondere die Beiträge [Müß06] und [Poh06] bieten einen guten Einblick in das Thema „Return on Security Investment“ (ROSI) und diverse ROSI-Messansätze.

Verweis, Titel: [NV10], *„Benchmarking Untrustworthiness : An Alternative to Security Measurement“*

Ansatz/Inhalte: Ein Vorschlag für die Entwicklung einer Sicherheitsmetrik, die im Gegensatz zu den meisten Ansätzen nicht die Wahrscheinlichkeit und die Höhe von Schadensereignissen bewertet, sondern die verfügbaren Informationen über ein System (Konfiguration, Wartung etc.) nutzt, um dessen Sicherheitsniveau zu ermitteln.

Verweis, Titel: [Pay06], *„A Guide to Security Metrics : SANS Security Essentials GSEC Practical Assignment“*

[4] Clarity, Objectiveness, Repeatability, Easiness, Succinctness.

Ansatz/Inhalte: Enthält allgemeine Vorschläge für die Entwicklung von Metrik-Programmen. Liefert Ansätze für die Entwicklung von Sicherheitsfunktionen, Risikovektoren sowie Definition und Bestimmung der Risikotragbarkeit.

Verweis, Titel: [PC10], *„Why Measuring Security Is Hard“*

Ansatz/Inhalte: In ihrem Artikel stellen die Autoren neun Gründe dar, die ihrer Ansicht nach die Messung der Sicherheit erschweren. Als Problemfelder werden u. a. die zwischen den Systemen bestehenden Verknüpfungen, die durch die Angreifer verursachten Umgebungsänderungen aber auch die Unterschiede in unserer Wahrnehmung der Sicherheit genannt. Zusätzlich schlagen die Autoren Strategien vor, die zur Bewältigung der genannten Herausforderungen beitragen können.

Verweis, Titel: [Pfl09], *„Useful Cybersecurity Metrics“*

Ansatz/Inhalte: Im Artikel werden mehrere Anforderungen für die sinnvolle Gestaltung von Sicherheitsmetriken diskutiert. Die Autorin erörtert außerdem die Unzulänglichkeit der derzeit eingesetzten Messverfahren. Im Mittelpunkt der Publikation steht die Aussage, dass die aktuell gemessenen und ausgewerteten Daten keine verlässlichen Aussagen über den Sicherheitsstand einer Organisation erlauben.

Verweis, Titel: [Pir07], *„Developing Metrics for Effective Information Security Governance“*

Ansatz/Inhalte: Das vorgestellte Basis-Framework für die Sicherheitsmetriken berücksichtigt die mitarbeiter-, prozess-, prozedur-, technologie- und Compliance-orientierten Perspektiven. Unterschiedliche Stakeholder benötigen mehrere auf ihre Bedürfnisse abgestimmte Sicherheitsmetriken.

Verweis, Titel: [PJAS06], *„A Weakest-Adversary Security Metric for Network Configuration Security Analysis“*

Ansatz/Inhalte: Im Rahmen eines graphenbasierten Ansatzes wird die Sicherheit eines Netzwerks bzw. einer Infrastruktur untersucht. Dabei findet eine quantitative Metrik Anwendung, die auf der Basis eines Modells der Netzwerkkonfiguration und einer Menge von Sicherheitslücken die Mindestanforderungen an den Angreifer ermittelt, der ein bestimmtes Ziel (Zustand) verfolgt.

Verweis, Titel: [SA10], *„Measuring Network Security“*

Ansatz/Inhalte: Die Publikation enthält eine Taxonomie der Sicherheitsmetriken und erörtert die Qualitätsanforderungen für die Sicherheitskenzahlen nach [Jaq07]: Konsistenz, günstige Messbarkeit, Quantifizierbarkeit, Verwendung mehrerer Metriken, Gewichtung, Wiederholbarkeit sowie Vergleichbarkeit.[5]

[5]Consistently measured, cheap to gather, expressed as a number, uses at least one unit of measure, contextually specific, partial weight, repetitiveness, comparability.

Verweis, Titel: [SBE11], *„Measuring Security“*

Ansatz/Inhalte: Eine abstrakte überblicksartige Darstellung der Herausforderungen im Bereich der Entwicklung von Sicherheitsmetriken und der für die Verbesserung aktueller Ansätze erforderlichen Voraussetzungen (vgl. [Bel06]).

Verweis, Titel: [Sch09], *„Key Components of an Information Security Metrics Program Plan“*

Ansatz/Inhalte: In diesem Report setzt sich der Autor mit den Empfehlungen zum Implementieren eines Sicherheitsmetrik-Programms auseinander und unterbreitet einen darauf aufbauenden, aus fünf Elementen bestehenden, Vorschlag: Initiierung, Metrikentwicklung, Datensammlung und -analyse, Reporting und Pflege.

Verweis, Titel: [SG09], *„Multidimensional Management of Information Security : A Metrics Based Approach Merging Business and Information Security Topics“*

Ansatz/Inhalte: Das vorgeschlagene Modell berücksichtigt sowohl die externen (gesetzlichen, regulatorischen und vertraglichen) als auch die internen (individuelle Schutzbedürfnisse der Organisation) Anforderungen, die in Form von konzentrischen Kreisen visualisiert werden. In Verbindung mit den Metrikansätzen soll dadurch die Verknüpfung externer Anforderungen mit den internen Zielen überwacht und gesteuert werden können.

Verweis, Titel: [SGF02], *„Risk Management Guide for Information Technology Systems : Recommendations of the National Institute of Standards and Technology“*

Ansatz/Inhalte: Eine häufig zitierte NIST-Publikation über die Risikoanalysestrategie mit dem Ziel, die einzelnen Risiken zu erkennen und zu bewerten, um dadurch das Gesamtrisiko besser einschätzen zu können. Im Mittelpunkt stehen die Risikoanalyse und -verringerung. Das dabei verfolgte Ziel ist die Reduktion des Restrisikos, das nach Möglichkeit quantifizierbar und akzeptierbar werden soll.

Verweis, Titel: [SH11], *„A Visualization and Modeling Tool for Security Metrics and Measurements Management“*

Ansatz/Inhalte: Vorstellung eines Visualisierungstools für ein hierarchisches Sicherheitsmetrikmodell (vgl. [Sav09]).

Verweis, Titel: [Sow09], *„Information-Security-Business-Performance-Measurement und -Management im Kontext von Compliance und Unternehmungszielen“*

Ansatz/Inhalte: Neben einem vom Autor entwickelten Modell zur Überführung der ISM-Anforderungen in ein Zielsystem enthält diese Dissertation eine akribisch erstellte Aufstellung der gängigen Sicherheitsmetriken [Sow09, S. LXXIII]. Die extrahierten Kennzahlen werden nach der Publikation und bei Bedarf nach Kategorien gruppiert.

Verweis, Titel: [SPK09], *„A Threat Analysis Methodology for Security Evaluation and Enhancement Planning“*

Ansatz/Inhalte: Die im Paper vorgeschlagene Methodik zur Bedrohungsanalyse und -bekämpfung berücksichtigt drei Phasen: Bedrohungsmodellierung, Asset-Verlinkung und Bedrohungsbekämpfung. Als interessant erscheint die für die Bedrohungsanalyse vorgeschlagene Kombination der Angriffsbäume mit dem CVSS-Scoring.

Verweis, Titel: [Str10], *„Schutzfaktor : Messbarkeit der IT-Sicherheit“*

Ansatz/Inhalte: Im Artikel beschreibt der Autor anschaulich die Probleme aktueller Sicherheitsmetriken und erörtert die Notwendigkeit für den Einsatz mehrerer Kennzahlensysteme in Abhängigkeit von der Zielsetzung und der Zielgruppe.

Verweis, Titel: [SW10], *„Messung der Informationssicherheit in der Praxis : Zusammenfassung der Ergebnisse einer empirischen Studie“*

Ansatz/Inhalte: Auswertung einer Studie, in deren Rahmen über 600 deutschsprachige Unternehmen zur ihrer Vorgehensweise zur Messung der Informationssicherheit befragt wurden. Die Analyseergebnisse beinhalten die Häufigkeit bzw. Verbreitung einzelner Standards und berücksichtigen u. a. die Branche, Mitarbeiterzahl und die Position der an der Studie teilgenommenen Sicherheitsverantwortlichen. Der Bericht ermittelt außerdem die aktuell bestehenden Herausforderungen der Informationssicherheit.

Verweis, Titel: [TSSS06], *„Managing Information Systems Security : Critical Success Factors and Indicators to Measure Effectiveness“*

Ansatz/Inhalte: Die Autoren teilen 76 rudimentäre Sicherheitsmetriken (z. B. prozentualer Anteil der Mitarbeiter mit einer Sicherheitszertifizierung, Anzahl der Sicherheitsaudits pro Monat, Anzahl durchgeführter BCP-Tests etc.) in zwölf Kategorien ein: „Sicherheitsarchitektur“, „Sicherheitsstrategie“, „dynamische Evaluierung der Sicherheitseffizienz“, „Risikobewertungsprozess“ etc. Diese bezeichnen sie als „kritische Erfolgsfaktoren“ (critical success factors). Nach Meinung der Autoren soll durch die Implementierung und die Befolgung möglichst vieler dieser Faktoren ein hohes Niveau an Sicherheit erreicht werden können.

Verweis, Titel: [Vis11], *„Optimizing and Analysing the Effectiveness of Security Hardening Measures Using Various Optimization Techniques as Well as Network Management Models Giving Special Emphasis to Attack Tree Model“*

Ansatz/Inhalte: Mithilfe eines Angriffsbaums soll die für eine Organisation optimale Kombination von Sicherheitsmaßnahmen ermittelt werden. Im Mittelpunkt steht dabei die auf die Verfolgung mehrerer Sicherheitsziele ausgerichtete Optimierung des Sicherheitsmaßnahmenportfolios.

Verweis, Titel: [Wan05], *„Information Security Models and Metrics“*

Ansatz/Inhalte: In der Publikation werden vier aus [Wey88] abgeleiteten formalen Anforderung an die Qualität von Sicherheitsmetriken in Form von Axiomen vorgestellt. Die Erfüllung dieser Anforderungen gilt als notwendige jedoch nicht als ausreichende Bedingung.

Verweis, Titel: [WIL+08], *„An Attack Graph-Based Probabilistic Security Metric“*

Ansatz/Inhalte: Die vorgeschlagene Sicherheitsmetrik basiert auf den Angriffsbäumen. Die Autoren berücksichtigen sowohl die Kumulation von Bedingungen[6] als auch das Vorhandensein von Zyklen in den Angriffsgraphen.

Verweis, Titel: [Wil09], *„Information Security : Concerted Effort Needed to Improve Federal Performance Measures“*

Ansatz/Inhalte: In diesem GAO-Bericht[7] werden u. a. vier Qualitätskriterien für die Sicherheitsmetriken beschrieben: Messbarkeit, Bedeutung, Wiederholbarkeit und Konsistenz sowie Beeinflussbarkeit.[8]

Verweis, Titel: [WJSN10], *„k-Zero Day Safety : Measuring the Security Risk of Networks against Unknown Attacks“*

Ansatz/Inhalte: Mithilfe einer simulationsbasierten Sicherheitsmetrik wird die Sicherheit einer Infrastruktur bewertet. Die Autoren konzentrieren sich auf die Berechnung der Softwaresicherheit unter Berücksichtigung der noch nicht (öffentlich) bekannten Angriffe (Zero-Day Exploits).

Verweis, Titel: [XWZ+09], *„Applying Attack Graphs to Network Security Metric“*

Ansatz/Inhalte: Die Autoren stellen einen Entwurf für ein angriffspfad-basiertes, aus fünf Teilen[9] bestehendes Sicherheitskennzahlensystem vor.

[6] Beispielsweise gleichzeitige Existenz und potenzielle Ausnutzung mehrerer Sicherheitslücken.

[7] United States Government Accountability Office.

[8] Measurable, meaningful, repeatable and consistent, and actionable (vgl. [Wil09, S. 9]).

[9] Security index, target of evaluation, elementary attribute, composition algorithm, and arithmetic operators.

C. Sicherheitsrichtlinien für medizinische Forschungsnetze

C.1. Versicherungsschutz als organisatorisches Sicherheitsinstrument

Der Abschluss von Versicherungsverträgen gehört zu den wirksamen organisatorischen Sicherheitsmaßnahmen. Beispielsweise kann ein Forschungsnetz für Schäden, die seine Mitarbeiter/Teilnehmer anderen durch ihre betriebliche Tätigkeit zufügen, haftbar gemacht werden. Risikotransfer in diesem Fall könnte in Form einer *Betriebshaftpflichtversicherung* erfolgen.
Die *Betriebshaftpflichtversicherung* reduziert finanzielle Risiken aus Personen-, Sach- oder aus den beiden Schadensarten resultierende Vermögensschäden. In Verbindung mit der Haftpflichtversicherung ist auch der Abschluss eines *Strafrechtsschutzvertrages* interessant, der die Forschungsnetzmitarbeiter im Falle von fahrlässig begangenen Straftaten absichert. Falls die Aufbewahrung oder Analyse von Forschungsmaterialien etc. die Lagerung von umweltrelevanten Stoffen erfordert, kann auch der Abschluss einer *Umwelthaftpflichtversicherung* empfehlenswert sein. Bedarf an dieser Art der Versicherung ist jedoch in den seltensten Fällen vorhanden, denn ein solcher Versicherungsschutz lohnt sich erst bei Überschreitung einer bestimmten Menge an gelagerten Gefahrstoffen.
Bei der Durchführung von Studien mit der Involvierung von Probanden ist der Abschluss einer *Probandenversicherung* Pflicht. Die Probandenversicherung sichert ein Forschungsnetz im Falle von Ansprüchen ab, wenn es im Rahmen der Studie zu Schädigungen der Probanden kommen sollte. Abhängig von der Art der Studie kann das Risiko auch von der bereits erwähnten Betriebshaftpflichtversicherung abgedeckt sein. Eine detaillierte Abgrenzung der beiden Versicherungsarten erfolgt in [Web07].
Abhängig von der Art der betriebenen medizinischen Forschung kann der Abschluss einer *Betriebsschließungsversicherung* sinnvoll sein. Bei dieser Art der Versicherungsleistung handelt es sich um einer Form der *Betriebsunterbrechungsversicherung*, die meistens auf die lebensmittelverarbeitenden Betriebe zugeschnitten ist. Die Betriebsschließungsversicherung greift, wenn ein Betrieb mit meldepflichtigen Krankheitserregern kontaminiert ist, und die Behörden eingreifen müssen, um z. B. die kontaminierten Bereiche zu desinfizieren. Aus den verfügbaren Versicherungspaketen wäre für ein Forschungsnetz die Deckung

von Desinfektionsaufwänden und Kosten für Ermittlung/Beobachtung interessant. In diesem Zusammenhang soll auch die *Ertragsausfallversicherung* nicht unerwähnt bleiben. Bei Störungen des Betriebsablaufs sichert der Versicherungsschutz die Fortzahlung von Gehältern, Mieten und Zinsleistungen. Die typischen versicherten Gefahren sind Einbruchsdiebstahl, Raub, Sturm und Hagel, Feuer, Leitungswasser, innere Unruhen und Elementarschäden. Die Relevanz einer solchen Versicherungsdeckung für das Forschungsnetz ist vom Einzelfall abhängig und kann beispielsweise dann gegeben sein, wenn das Forschungsnetz sich zur Leistungserbringung gegenüber einer Drittpartei[1] verpflichtet und dafür zusätzliche Kapazitäten aufbaut (Mitarbeiter, Anlagen etc.). Ist ein Forschungsnetz aufgrund von einer der erwähnten Gefahren nicht in der Lage, die vereinbarte Leistung zu erbringen, kann der Leistungsabnehmer (abhängig von der Vertragsgestaltung) seine Leistungen verweigern, was zu einer Finanzierungslücke führt. Ein solches Szenario ist jedoch bei den meistens durch die öffentliche Hand finanzierten Forschungsvorhaben auf die Ausnahmefälle beschränkt. Der evtl. notwendige Versicherungsumfang wird sich auf die in Verbindung mit einem konkreten Forschungsvorhaben aufgebauten „Überkapazitäten“ beschränken. Aus den gleichen Gründen ist eine *Forderungsausfall-Versicherung* für ein Forschungsnetz fast irrelevant. Der Abschluss einer solchen Versicherung wäre nur dann sinnvoll, wenn der Geldrückfluss für die aufgebauten „Überkapazitäten“ nach deren Anschaffung oder in Form von (un)regelmäßigen Zahlungen erfolgen würde. Die in solchen Fällen üblicherweise verwendeten *Bürgschaften* wären auf ihre bessere Eignung zu untersuchen. Die EDV-Anlagen eines Forschungsnetzes können durch den Abschluss einer *Elektronik-Versicherung* gegen Diebstahl, Manipulationen, Defekte, Verlust, Bedienungsfehler und Fahrlässigkeit, Sabotage und Terrorismus, höhere Gewalt etc. versichert werden. In seltensten Fällen wird jedoch die Versicherung der Geräte[2] an sich im Vordergrund stehen. Vielmehr geht es um die Folgekosten, die z. B. durch die Manipulation einer EDV-Anlage entstehen können. Falls kostspielige Ausrüstung gegen Einbruchdiebstahl, Feuer, Elementarschäden und dergleichen geschützt werden soll, wäre eine *Inhaltsversicherung* mit Wertanpassung evtl. besser geeignet. Die Inhaltsversicherung würde die Reparatur bzw. Wiederbeschaffung der von einer Drittpartei (Sponsoren) dem Forschungsnetz überlassenen und beschädigten Ausrüstung ermöglichen. Die Deckung erstreckt sich auch auf die Feuerlösch-, Abbruchs- und Aufräumungskosten. Auch die evtl. anfallenden Kosten für die Wiederherstellung von Akten/Unterlagen, Wiedergewinnung vom Probenmaterial etc. werden ersetzt.[3] Eine *Transportversicherung* bzw. *Werkverkehrsversicherung* ist dann notwendig, wenn kostspielige (medizinische) Ausrüstung bewegt wird und gegen Unfall, Diebstahl, Beschädigung etc. abgesichert werden muss. Oft ist die Transportversicherungs-Deckung in dem Inhaltsversicherungs-Paket bereits enthalten.

[1] Zum Beispiel Sponsor, ein anderes Forschungsnetz, Kliniken etc.

[2] IuK-Geräte, Mess- und Steuerungstechnik, medizinische Ausrüstung etc.

[3] Zur Versicherbarkeit der Sachrisiken einer Biomaterialbank siehe [SPR+06, S. 97 f.].

Der Deckungsumfang einer *Vertrauensschadenversicherung* kann unterschiedlich festgelegt werden und erstreckt sich üblicherweise auf die von Betriebsangehörigen und sonstigen Vertrauenspersonen vorsätzlich verursachten Vermögensschäden. Beim Abschluss eines solchen Vertrages ist darauf zu achten, dass die Ausschlussklauseln des Versicherungsvertrags nicht die für das Forschungsnetz relevanten Risiken enthalten. Eine übliche Vertrauensschadenversicherung bietet u. a. Deckung gegen folgende, für ein medizinisches Forschungsnetz relevante Risiken:

- *Vermögensschäden durch vorsätzliche Handlungen von Vertrauenspersonen.*[4] In der Regel werden auch ehemalige Arbeitnehmer während einer gewissen Zeit[5] sowie Aushilfskräfte, Praktikanten, Zeitarbeitskräfte etc. in einem Schadensfall als Vertrauenspersonen eingestuft. Auch den Drittparteien, wie z. B. Personen, die im Rahmen von Dienstleistungs- und Wartungsverträgen im Auftrag des Forschungsnetzes tätig sind, wird Vertrauensperson-Status zuerkannt.

- *Die von einer unbekannten Vertrauensperson verursachten Schäden*, wobei bereits eine Wahrscheinlichkeit der Zugehörigkeit des Stifters zum Kreis von Vertrauenspersonen in vielen Fällen ausreichend ist.

- *Schäden, die durch Ansprüche Dritter*[6] aufgrund von unerlaubten Handlungen von Vertrauenspersonen entstehen.

- *Schäden Dritter, die durch gefälschte Anweisungen* entstanden sind. Dieser Punkt deckt Schäden, die z. B. durch Vorspiegelung der Identität eines Forschungsnetzmitarbeiters entstehen.

- *Schäden, die durch vorsätzlichen Datenmissbrauch/Computermissbrauch*[7], durch Vertrauenspersonen oder Dritte hervorgerufen werden.

Der Abschluss eines solchen Versicherungsvertrages sorgt für die Kalkulierbarkeit der in einem Schadensfall entstehenden Kosten und bringt eine gewisse „Kontinuität“ in die Ausgabenstruktur des Forschungsnetzes. In einem Schadensfall werden Aufwendungen für externes Personal, Überstunden zur Schadenslokalisierung im EDV-System und Wiederherstellung von Informationen vom Versicherer übernommen. Dabei ist sowohl die Wiederherstellung von EDV-Daten als auch die Wiederinstandsetzung (Neuinstallation,

[4] Vermögensschäden, die nach gesetzlichen Bestimmungen über unerlaubte Handlungen zum Schadensersatz verpflichten.

[5] Üblicherweise bis zu drei Monate nach dem Verlust ihrer Eigenschaft als Vertrauensperson.

[6] Zum Beispiel Patient, dessen Daten unrechtmäßig veröffentlicht wurden.

[7] Unrechtmäßiger Zugang zu einem Computersystem, böswillige Behinderung oder Fälschung der Funktionen eines Computersystems, böswillige Einführung von Programmen oder Daten (Malware) in ein Computersystem, Fälschung oder wissentliche Verwendung von gefälschten digitalen Dokumenten.

Konfiguration, Verteilung etc.) der Software gemeint. Die durch die Wiederherstellungsarbeiten verursachten Mehrkosten sowie Kosten, die mit der Beauftragung eines externen Unternehmens zwecks Schadenermittlung anfallen, sind gedeckt. Aufwendungen für Aufklärung und Rekonstruktion des Schadenherganges bzw. Ermittlung der Schadenshöhe werden vom Versicherer getragen. Externe Rechtsverfolgungskosten (u. a. Gerichtskosten), die bei der Geltendmachung von Schadenersatzansprüchen gegen den Schadenverursacher anfallen, trägt ebenfalls das Versicherungsunternehmen.
In diesem Zusammenhang soll die in der letzten Jahren an Bedeutung und Popularität gewinnende *D&O-Versicherung* (Directors' and Officers' Liability Insurance) erwähnt werden, die den Vorgesetzten einen Schutz gegen ihre Haftungsrisiken bietet. Der Abschluss einer Haftpflichtversicherung für die Geschäftsführer wird auch in [SPR+06] empfohlen, um eine persönliche Haftung des Vorstandes im delikt- oder strafrechtlichen Bereich zu umgehen. [SPR+06, S. 93]: „In jedem Fall empfiehlt es sich, eine entsprechende Haftpflichtversicherung abzuschließen, die die Risiken aus einer Vorstandstätigkeit weitestgehend abdeckt."
Im Falle einer gerichtlichen Auseinandersetzung wird es von Bedeutung sein, beweisen zu können, dass Maßnahmen zum Datenschutz und Datensicherheit in einem angemessenen Umfang getroffen wurden. Für ein Forschungsnetz kann es empfehlenswert sein, sich regelmäßig der Durchführung eines Datenschutzaudits, wie es der Gesetzgeber in § 9a BDSG spezifiziert, bzw. einer Datenschutzzertifizierung mit dem Datenschutzsiegel zu unterziehen.[8] Prüfung und Bewertung der Schutzeinrichtungen durch unabhängige Gutachter geben die notwendige Sicherheit für das Forschungsnetz im Falle eines Rechtsstreits. Außerdem sind die positiven Einflüsse des Audits auf die Sicherheit des Forschungsnetzes nicht zu unterschätzen. Die Erlangung einer qualifizierten Zertifizierung für das Informationssicherheits-Managementsystem oder andere Komponenten ist allerdings aufgrund des mit der Zertifizierung verbundenen Aufwandes nur dann anzustreben, wenn sie vom Gesetzgeber oder sonstigen Regulierungsbehörden ausdrücklich verlangt wird. Dies ist jedoch im Bereich der medizinischen Forschung umstritten, da derzeit keine Zertifizierungen für die Qualität des Datenschutzes bzw. der Datensicherheit existieren, die die separaten Prüfungen durch Datenschutzbehörden und Ethikkommissionen ersetzen können (vgl. [DSMS07, S. 34]).
Die im Oktober 2005 veröffentlichte ISO/IEC 27001:2005 kann zwar für eine qualifizierte Zertifizierung nicht verwendet werden, eignet sich jedoch für Auditoren zur Verifizierung des Umsetzungsgrades von Sicherheitsstandards. Insbesondere die übersichtliche Gliederung in Managementgebiete (Security Policy, Organisation of Information Security, Asset Management, Human Resources Security, Physical and Environmental Security etc.) und die Aufzählung der Aufgaben/Maßnahmen machen ISO 27001 für die Auditing-Zwecke interessant.
Des Öfteren decken Versicherungen keine Vermögensschäden, die als Folge von Terrorismus entstehen. Auch wenn der Begriff des Cyber-Terrorismus derzeit noch nicht den Einzug in die Deutschen Gerichte gefunden hat und die Begriffsdefinition selbst umstritten ist, wäre

[8] Siehe Auszug aus BDSG im Anhang E „Auszüge aus BDSG und StGB".

eine Terrorausschlussklausel für das Forschungsnetz nachteilig. Gerne schließen Versicherungsgesellschaften Vermögensschäden aus, die als Folge der Verbreitung von vertraulichen Informationen oder Geschäftsgeheimnissen entstanden sind. Da gerade solche Schäden für ein Forschungsnetz am wahrscheinlichsten sind, wäre ein solcher Ausschluss im Bedingungswerk nicht akzeptabel. Manche Vertragswerke machen außerdem eine Bereicherungsabsicht des Täters zu der Deckungsvoraussetzung. Da die Bereicherungsabsicht bei vielen Computerangriffen nicht gegeben ist,[9] und ein Täter auch aus purem Geltungszwang oder Rache handeln kann, ist ein solcher Ausschluss ebenfalls nicht wünschenswert. Die meisten Bedingungswerke machen allerdings bei computerbasierten Angriffen eine Ausnahme und erkennen auch Schäden durch Angriffe ohne Bereicherungsabsicht an.
Im Abschnitt 3.3.2 „Personale Aspekte für den Betrieb von Forschungsnetzen“ wird die Bedeutung des Personals für die Forschungsnetzsicherheit erläutert. Zwei Feststellungen spiegeln die Bedeutung des Personals für einen sicheren Forschungsnetzbetrieb wider:

- Mitarbeiter eines Forschungsnetzes sind für dessen Sicherheit maßgeblich.
- Eine arbeitnehmerfreundliche Personalpolitik schafft Anreize, sicherheitsbewusst zu handeln.

Angesichts der niedrigen tariflich festgelegten Gehälter, oft unbezahlter Mehrarbeit und eines eingeschränkten Spielraums für die extrinsische Motivation der Mitarbeiter[10] müssen die verfügbaren knappen finanziellen Mittel eines Forschungsnetzes gezielt und gut durchdacht eingesetzt werden, um die Mitarbeiter zu motivieren. Eine freiwillige *Gruppenunfallversicherung* für die Forschungsnetzmitarbeiter ist mit relativ geringen finanziellen Belastungen für das Forschungsnetz bzw. daran beteiligten Einrichtungen verbunden; der gleiche Versicherungsumfang eines vom Mitarbeiter privat abgeschlossenen Versicherungsvertrags kostet i. d. R. das Mehrfache an Prämie. Freiwillige Arbeitgeberleistungen dieser Art sind kostengünstige wirksame Mittel der Motivationssteigerung.
Trotz einer (hoffentlich) arbeitnehmerfreundlichen Beschäftigungspolitik sind Konfliktsituationen mit den Arbeitnehmern nicht zu vermeiden. Die häufigsten Fälle sind Streitigkeiten um Gehalts- und Überstundenforderungen, Zeugnisse und Beurteilungen sowie Mobbing-Vorwürfe. Der Abschluss einer *Arbeitsrechtsschutz-* bzw. *Disziplinar- und Standesrechtsschutzversicherung* gewährt dem Forschungsnetz bei Streitigkeiten aus Arbeits- und Dienstverhältnissen die notwendige Sicherheit. Auch eine Reihe weiterer Deckungen aus dem Rechtsschutzbereich wäre für ein Forschungsnetz sinnvoll. So gewährleistet z. B. die *Daten-Rechtsschutzversicherung* die Abwehr gegen Auskunftsklagen nach dem Bundesdatenschutzgesetz. Diese Maßnahme kann ergänzend zu der im Abschnitt 3.4 „Administrative

[9] Dies trifft besonders häufig auf jugendliche Täter zu. Zusätzliche Informationen zur Motivation von Angreifern befinden sich im Abschnitt 4.3.2 „Bedrohungsorientierte Analyse“.

[10] Zum Beispiel Beförderung, Gehaltserhöhung, Bonus etc. Einige der relevanten Faktoren werden im Praxishandbuch „IT im Gesundheitswesen“ [WB09] genannt.

Aspekte von Sicherheitsrichtlinien“ beschriebenen beschlagnahmesicheren Unterbringung von Forschungsnetzdaten eingesetzt werden.

C.2. Merkmale von administrativen Sicherheitsrichtlinien

C.2.1. Vergabe von Serviceaufträgen

Viele der in dieser Arbeit vorgeschlagenen Sicherheitsmaßnahmen sind kostenintensiv, sowohl in der Einführung als auch im späteren Betrieb. Man muss davon ausgehen, dass kein Forschungsnetz im Alleingang die zur Implementierung aller vorgeschlagenen Sicherheitskonzepte notwendigen finanziellen Mittel aufbringen kann. Ein möglicher Ausweg aus dieser Situation ist der kosteneffiziente Einkauf von IT-Dienstleistungen von einer extra dafür gegründeten nicht gewinnorientierten Organisation[11], die ein standardisiertes Sicherheitsniveau den als Kunden agierenden Forschungsnetzen anbietet. Bei der Konsolidierung von IT-Dienstleistungen könnte beispielsweise der TMF e. V., der sich als Ansprechpartner in Fragen medizinischer Forschung versteht und die Verbesserung der Forschungsinfrastruktur zum Ziel erklärt, eine beratende Rolle spielen. Da die eigentliche Erbringung von IT-Dienstleistungen im Sinne der Zurverfügungstellung von Ressourcen bisher nicht zu den Kernkompetenzen der Organisation gehört, muss geprüft werden, ob die Kompetenzerweiterung in diese Richtung sinnvoll ist. Unter der Beibehaltung des aktuellen Kompetenzbereichs durch TMF könnte ein weiterer IT-Dienstleistungsverein oder eine IT-Dienstleistungs-gGmbH gegründet werden. Die Finanzierung der Körperschaft könnte z. B. durch Gebühren der leistungsbeziehenden Forschungsnetze, Spenden, staatliche Zuschüsse etc. erfolgen. Da die Organisation durch ihre Dienstleistungen Wissenschaft und Forschung fördert, ist der Gemeinnützigkeitsnachweis sehr wahrscheinlich und führt zu einer Steuerbegünstigung der Körperschaft (Befreiung von der Körperschafts- und Gewerbesteuer, Ausstellungsberechtigung für Zuwendungsbestätigungen etc.). Von den beiden o. g. Gesellschaftsformen wäre die der gGmbH die vorteilhaftere, denn eine gGmbH vereint die Vorteile von gewinnorientierten und gemeinnützigen Organisationen. Eine gGmbH kann außerdem qualitativ hochwertigere Dienstleistungen durch einen Geschäftsführer und hauptamtliche Mitarbeiter anbieten, die für die erforderlichen Professionalität sorgen. Die Kosteneffizienz einer serviceorientierten Architektur, bei der die Dienstleistungen von externen Service-Providern bezogen werden, belegen die Ausführungen in [HDR+10]. Solche Service-Provider werden i. d. R. öffentlich finanziert und geben lediglich die variablen Kostenanteile für die erbrachten Leistungen an die Forschungsnetze weiter. Die Einhaltung der vereinbarten gemeinsamen SLAs erhöht die Zuverlässigkeit und Sicherheit der Forschungsnetzdienste. Außerdem kann eine transparente Aufteilung von Risiken und Verantwortlichkeiten sowie eine schnellere Reaktionsfähigkeit auf Technologieänderungen und neue Standards

[11] Non-Profit-Organisation.

durch die Kompetenzbündelung erreicht werden. Einen bestehenden Verbesserungsbedarf in diesem Bereich bestätigt der TMF-Bericht zum Projekt „V054-01 IT-Strategie Teilprojekt 4“. Danach beruht die aktuelle Zusammenarbeit im Forschungsbereich oft auf einem Vertrauensverhältnis und nicht auf den verbindlichen SLA-Vereinbarungen (vgl. [Sta09, S. 25]).

C.2.2. Reaktion auf Sicherheitsvorfälle

Die Reaktion auf die Sicherheitsvorfälle ist ein Bestandteil der administrativen Schutzmaßnahmen. Die Anzahl und die Vielfalt der möglichen Sicherheitsvorfälle lassen keine vollständige Beschreibung sämtlicher denkbarer Szenarien zu. Im Folgenden werden die wichtigsten administrativen Schritte aufgezeigt, die im Kompromittierungsfall einiger, der Meinung des Autors nach bedeutender, Infrastrukturbestandteile bzw. Dienste durchgeführt werden müssen.

Kompromittierung der *IDAT*-Datenbank: In diesem Fall hat ein Angreifer Zugriff auf Einträge der Patientendatenbank. Er könnte nun versuchen, *IDAT* mit den Informationen aus der Behandlungsdatenbank zu kombinieren. Die bei der Kompromittierung der *IDAT*-Datenbank empfohlene Vorgehensweise lautet:

1. *IDAT*- und *MDAT*-DBs für nicht administrative Zugriffe sperren.
2. Betroffenen Personenkreis informieren.
3. Neue *PIDs* erzeugen und zwischen den beiden Datenbanken replizieren.
4. Die kompromittierten *PIDs* in der $MDAT^W$-Datenbank durch neu erzeugte *PIDs* ersetzen.
5. Um spätere Zuordnung der medizinischen und den Patientendaten gewährleisten zu können, muss die Zuordnung von PID_{alt} zu PID_{neu} in einer separaten Datenbank festgehalten werden.
6. Sicherheitsvorfall untersuchen und Ursache der Kompromittierung ermitteln.
7. Entdeckte Sicherheitslücken beseitigen.
8. *IDAT*-DB in Betrieb nehmen.

Kompromittierung der $MDAT^W$-Datenbank: In diesem Fall hat ein Angreifer Zugriff auf Einträge der Behandlungsdatenbank. Er könnte nun versuchen, die zu den Behandlungsdaten gehörenden Patientendaten zu ermitteln. Die bei der Kompromittierung der $MDAT^W$-Datenbank empfohlene Vorgehensweise lautet:

1. *IDAT*- und *MDAT*-DBs für nicht administrative Zugriffe sperren.
2. Neue *PIDs* erzeugen und zwischen den beiden Datenbanken replizieren.
3. Die kompromittierten *PIDs* in der *IDAT*-Datenbank durch neu erzeugte *PIDs* ersetzen.
4. Um spätere Zuordnung der medizinischen und den Patientendaten gewährleisten zu

können, muss die Zuordnung von PID_{alt} zu PID_{neu} in einer separaten Datenbank festgehalten werden.
5. Sicherheitsvorfall untersuchen und Ursache der Kompromittierung ermitteln.
6. Entdeckte Sicherheitslücken beseitigen.
7. $MDAT^W$-DB in Betrieb nehmen.

Gleichzeitige Kompromittierung der *IDAT* und $MDAT^W$: Die empfohlene Vorgehensweise lautet:

1. *IDAT* und *MDAT* für nicht administrative Zugriffe sperren.
2. Betroffenen Personenkreis ermitteln und über den Sicherheitsvorfall informieren.
3. Neue *PIDs* erzeugen und zwischen den beiden Datenbanken replizieren.
4. Die kompromittierten *PIDs* in der *IDAT*- und $MDAT^W$-Datenbank durch neu erzeugte *PIDs* ersetzen.
5. Um spätere Zuordnung der medizinischen und den Patientendaten gewährleisten zu können, muss die Zuordnung von PID_{alt} zu PID_{neu} in einer separaten Datenbank festgehalten werden.
6. Sicherheitsvorfall untersuchen und Ursache der Kompromittierung ermitteln.
7. Entdeckte Sicherheitslücke beseitigen.
8. $MDAT^W$- und *IDAT*-DBs in Betrieb nehmen.

Beschädigung des PIN Briefes:

1. Beim Feststellen der Beschädigung des PIN-Briefes durch dezentralen Benutzerservice sind sämtliche Zertifikate der dazu gehörenden Karte unverzüglich zu sperren.
2. Die entsprechende SmartCard ist zu vernichten. Eine neue SmartCard und PIN-Brief sind zu bestellen.

Verlust/Kompromittierung der SmartCard oder der Software-PSE:

1. Beim Verlust der SmartCard oder (beim begründeten Verdacht der) Kompromittierung des Softwarezertifikats sind sämtliche betroffenen Zertifikate des Benutzers unverzüglich zu sperren.
2. Die Sperrung erfolgt durch einen schriftlichen Antrag des Zertifikatinhabers persönlich beim dezentralen Benutzerservice unter Vorlage des Lichtbildausweises.
3. Für die Neubeantragung der Ersatzzertifikate/SmartCard gelten die generellen Regeln des Forschungsnetzes.

Unerlaubtes (vermutetes) Kopieren der Software-PSE:

1. Beim Feststellen unerlaubter Kopien der Software-PSE müssen die davon betroffenen Zertifikate unverzüglich gesperrt werden.
2. Für die Sperrung und Neubeantragung der Zertifikate gelten die gleichen Regeln wie beim Verlust der SmartCard oder des Softwarezertifikats.

Kompromittierung der PSE:

1. Sollte die Kompromittierung der PSE festgestellt werden, sind sämtliche betroffenen Zertifikate unverzüglich zu sperren.
2. Vor dem Einspielen neuer Zertifikate muss die Integrität der PSE-Umgebung gewährleistet werden.
3. Für die Sperrung und Neubeantragung der Zertifikate gelten die gleichen Regeln wie beim Verlust der SmartCard.

Kompromittierung der Zertifikate/Kompromittierung der PIN:

1. Die Kompromittierung der PIN ist der Kompromittierung von Zertifikaten gleichzusetzen.
2. Bei der PIN-Kompromittierung ist die Vorgehensweise analog wie beim Verlust der SmartCard oder der Software-PSE.

Unerlaubte Sperrung von Zertifikaten:

1. Sollte es trotz aller Sicherheitsmaßnahmen zu einer unerlaubten Sperrung von Zertifikaten kommen, müssen diese durch den Antrag des Zertifikatinhabers entsperrt werden.
2. Für die Antragstellung zum Entsperren der Zertifikate gelten die gleichen Anforderungen, wie für das Neubeantragen der Zertifikate.
3. Der Vorfall ist zu untersuchen.

Grobe Verletzung der Richtlinien durch Forschungsnetzteilnehmer:

1. Beim Feststellen einer groben Verletzung der Richtlinien durch Forschungsnetzteilnehmer sind sämtliche Accounts/Zertifikate des Teilnehmers zu sperren.
2. Personendaten des Teilnehmers sind beim zentralen Benutzerservice zu speichern, um den Zugang zum Forschungsnetz für die o. g. Person zukünftig zu verhindern.
3. Beim Vorliegen (oder beim begründeten Verdacht) einer Straftat müssen sämtliche (Verbindungs-)Daten des Teilnehmers gesichert werden, um ggf. später den Strafvollzugsbehörden zur Verfügung gestellt werden zu können.

C.3. Merkmale von technischen Sicherheitsrichtlinien

C.3.1. Aspekte der Sicherung und der Ausfallsicherheit für die Softwarearbeitsumgebungen

C.3.1.1. Softwarebasierte Sicherung der Arbeitsumgebung

Unternehmen setzen vermehrt virtuelle Laufzeit-Umgebungen in Verbindung mit Compliance-Software ein, was nicht nur die Ausführung von Anwendungen auf Plattformen

erlaubt, mit denen sie eigentlich nicht kompatibel sind, sondern auch eine bessere Kontrolle über die Systemlandschaft ermöglicht. Terminal-Services ersetzen inzwischen die gesamten lokalen Anwendungsinstallationen auf der Client-Seite. So erhält z. B. der Client-PC eine Citrix-Client-Installation, die die Anzeigefunktion übernimmt. Die Anwendungen (Office, organisationsinterne Applikationen etc.) laufen dagegen in der kontrollierten Umgebung des Citrix-Servers. In Verbindung mit einem Compliance-Tool ist diese Lösung relativ sicher, denn die unerwünschte Software kann nur schwer auf den abgesicherten Applikationsservern installiert werden.

Eine Compliance-Software gewährleistet die Übereinstimmung der System-Konfiguration mit den relevanten Sicherheitsstandards. Da die Restriktionen von Hard- und Software der Netzwerkteilnehmer sich kaum durchsetzen lassen, ist der Einsatz von Compliance-Software allerdings nur schwer vorstellbar und wenig effektiv. Ein direkter Zugriff auf eine webbasierte Anwendung, die in einem Unternehmen bedenkenlos über den Webbrowser erfolgen kann, wäre für ein Forschungsnetz nicht empfehlenswert, denn die Webserver-Zugriffe könnten auch von nicht vertrauenswürdigen Systemen ausgehen. Der Einwand, dass das Onlinebanking bereits seit Jahren nur mit einem Browser-Zugriff und keiner Überprüfung der System-Integrität eines Bankkunden stattfindet, ist nicht unberechtigt. Im Zusammenhang mit der Speicherung und Verarbeitung von vertraulichen Patientendaten wäre die Analogie in diesem Fall jedoch nicht ganz korrekt. Der Unterschied zwischen einem Forschungsnetzteilnehmer und einem, von seinem Privat-PC das Onlinebanking betreibenden Anwender, besteht in der Art der ausgetauschten/abgerufenen Daten. Ein Online-Bankkunde riskiert bei Nichteinhaltung bestimmter Sicherheitsregeln „nur“ seinen eigenen Kontostand. Ein Forschungsnetzteilnehmer, der von einem unsicheren System arbeitet, kann die Daten Tausend anderer Personen gefährden. Es wäre sorglos anzunehmen, dass jeder, der an dem Forschungsnetz teilnimmt, die höchste Sicherheit seines Systems gewährleisten kann.

Eine Lösungsmöglichkeit für das beschriebene Problem besteht in der Erzeugung einer Zwischenstufe vor dem direkten Zugriff auf den Web- bzw. Applikationsserver: Man sperrt Zugriffe auf die Dienste des Forschungsnetzes für alle Applikationen, die nicht innerhalb einer Lockdown-Umgebung ausgeführt werden. Dies veranschaulicht die Abbildung 23: Ein Forschungsnetzteilnehmer nimmt Verbindung zu einem Lockdown-Server auf. Nun sind zwei Szenarien denkbar: Die virtuelle Umgebung läuft auf dem Client-Rechner oder auf dem Lockdown-Server. Im ersten Fall bedarf es einer komplizierten Laufzeitumgebung, die mit jeder Ausprägung des Client-Systems kompatibel sein muss. Der Applikationsserver übermittelt dem Client die Versionsinformationen der aktuellen Umgebung, damit der Client seine Lockdown-Umgebung bei Bedarf aktualisieren kann. Der Client kann nun die Authentizität des signierten Installationspakets anhand der auf der SmartCard gespeicherten Server-Signatur verifizieren. Nach seiner Initialisierung muss nun der Client seinerseits dem Server die Integrität seiner Umgebung beweisen. Nun können die für die Forschung/Behandlung notwendigen Anwendungen in einer sicheren Umgebung ausgeführt

werden.[12] Angesichts der potenziell hohen Teilnehmeranzahl und einer weiten räumlichen Verteilung der Teilnehmer ist der Einsatz eines Patchmanagementwerkzeugs empfehlenswert. Das Werkzeug muss in der Lage sein, die Patch-Stände der Teilnehmergeräte zu ermitteln, die Updates an die Teilnehmer auszuliefern und den Vorgangsstatus zu verfolgen. Eine angemessen detaillierte Reportfunktion und die Möglichkeit, zum letzten stabilen Anwendungsstatus zurückzukehren, sind ebenfalls notwendig.

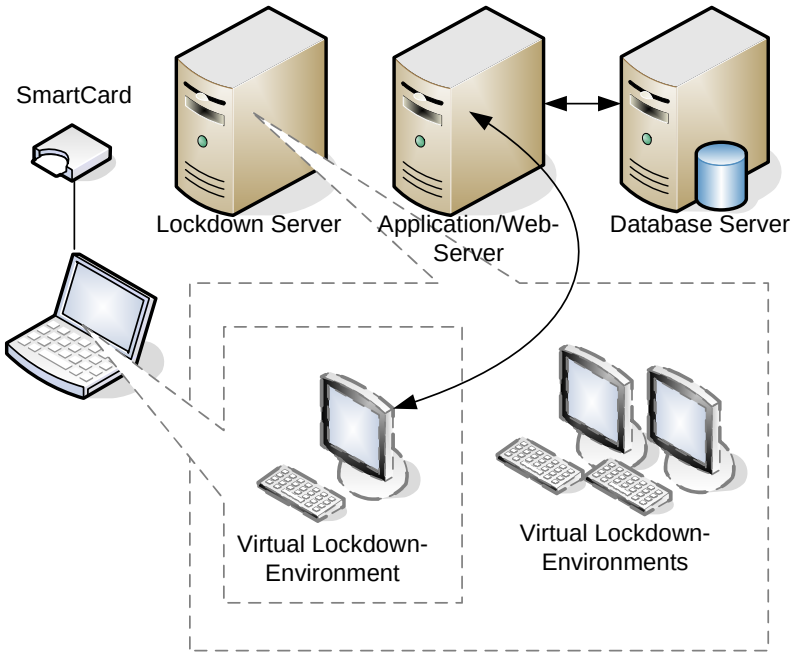

Abbildung 23.: Lockdown-gesicherte Arbeitsumgebung: Durch das Einfügen einer Zwischenstufe in Form der virtuellen Umgebung (sowohl auf dem Client-Rechner als auch auf dem Lockdown-Server möglich) können die Web- bzw. Applikationsserver vor einem direkten Zugriff geschützt werden.

In regelmäßigen Zeitabständen erscheinen Presseberichte über Unternehmen, die unabsichtlich Malware-verseuchte Produkte frei geben – ein Resultat der unzureichenden Qualitätssicherung. Die pauschale Annahme, eine signierte Software wäre sicher, ist schlichtweg falsch. Es sollte vermieden werden, dass ein einziger Entwickler in der Lage ist, die neue Softwareversion oder den Update-Patch selbstständig ohne vorhergehende tiefgründige Überprüfung zu signieren. Es wird empfohlen, die Releases der Softwareumgebung erst nach einer entsprechenden Überprüfung auf Schadenssoftware in Anwesenheit mindestens eines Vertreters des Forschungsnetzes und eines Entwicklers signieren zu lassen. Der Einsatz eines sogenannten Secret-Sharing-Verfahrens kann dafür sorgen, dass niemand im Alleingang die Signierung durchführen kann. Das System, auf dem die Releases signiert werden, darf an das Intra- bzw. Internet nicht angeschlossen sein.
Im Gegensatz zu der oben beschriebenen Virtualisierungslösung wird auf dem Client-PC bei einer Terminal-basierten Lösung keine vollwertige Laufzeitumgebung installiert. Nur ein

[12]In diesem Zusammenhang ist die Einrichtung von Arbeitsumgebungen auf den mobilen Speichermedien wie USB-Sticks denkbar. Eine ausführliche Bestandsaufnahme über die Möglichkeiten und Grenzen dieses Ansatzes befindet sich in [Vah08].

schlanker leicht zu pflegender Client wird aufgespielt, was die Erhöhung der Teilnehmerzahl mit einfachsten Mitteln möglich macht. Eine Terminal-basierte Lösung vereinfacht die Bereitstellung von Updates und Patches und verringert den administrativen Aufwand durch Vereinheitlichung der Administrationswerkzeuge. Durch Zentralisierung ist eine erweiterte Protokollierung der sicherheitsrelevanten Benutzeraktionen möglich. Das wohl bekannteste Terminal Service-Produkt ist Citrix.

Citrix-Technologie: Ein großer Vorteil einer Citrix-basierten Lösung ist die weitestgehende Plattformunabhängigkeit. Citrix wird von den meisten marktüblichen Geräten und Betriebssystemen unterstützt: Windows, Macintosh, UNIX, Linux, Thin Clients, PDAs und sogar Mobiltelefonen. Durch seine weite Verbreitung und langjährigen Einsatz hat die Citrix-Plattform viele Kinderkrankheiten hinter sich gelassen. Aufgrund der marktdominierenden Stellung des Unternehmens ist davon auszugehen, dass eventuell auftretende Sicherheitslücken auch in Zukunft schnell beseitigt werden. Im Vergleich zu dem beschriebenen Software-Boot-Ansatz wäre der Citrix-Betrieb für das Forschungsnetz vermutlich kosteneffektiver, da die Entwicklung und Wartung der virtuellen Umgebung komplett entfallen würde.
Es existieren diverse Möglichkeiten, Citrix-Technologie im Rahmen des Forschungsnetzes einzusetzen. Die empfehlenswerte Basis-Konfiguration besteht aus dem sogenannten Citrix Presentation Server (CPS) in Verbindung mit dem Citrix Access Gateway (CAG) und ist in der Abbildung 24 dargestellt. Ein Forschungsnetzteilnehmer verbindet sich über Citrix Access Gateway mit dem Citrix Presentation Server und erhält dadurch eine einheitliche vordefinierte Arbeitsumgebung. Die Authentifikation erfolgt über eine SmartCard.[13] Die ausgetauschten Daten werden innerhalb eines SSL-Tunnels übertragen, der von CAG unterstützt wird. Der Citrix-Client kann dabei vom CAG über das Web mit wenig Aufwand verteilt werden. CAG bietet außerdem eine Sicherheitscheck-Funktionalität: Es stellt sicher, dass Geräte der Forschungsnetzteilnehmer die Sicherheitsanforderungen des Forschungsnetzes erfüllen, die für eine Verbindung mit dem CPS vorgeschrieben sind (OS-Stand, installierte Patches etc.). Mithilfe des CSG ist es möglich, situationsspezifische Rechte auf Basis von Zugriffsszenarien (z. B. Zugriff aus bestimmten Forschungsnetzsegmenten, das verwendete Endgerät etc.) zu definieren.[14]
Auf dem CPS werden nur fest definierte Applikationen freigegeben. Im Zweifel ist das nur eine bestimmte Version des Webbrowsers. Der auf dem CPS ausgeführte Browser wird für Informationsabruf und -eingabe (vom Forschungsnetz-Applikationsserver bzw. dem dazugehörigen Webserver) verwendet. Durch den beschriebenen Aufbau wird dem Client

[13] Authentifikationsmethoden werden im Abschnitt 3.5.3 „Authentifizierung von Forschungsnetzteilnehmern“ ausführlich erläutert.

[14] Weitere Informationen zum Thema Zugriffssteuerung befinden sich im Abschnitt 3.5.4 „Rollenbasierte Rechtevergabe (RBAC)“.

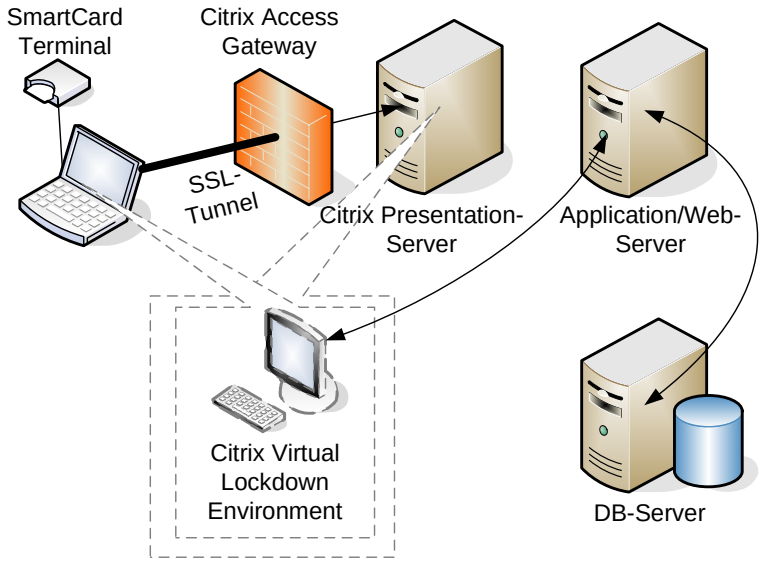

Abbildung 24.: Vorschlag für den Citrix-Einsatz in einem Forschungsnetz: Die abgebildete Konfiguration besteht aus einem Citrix Presentation Server (CPS) in Verbindung mit dem Citrix Access Gateway (CAG).

die Möglichkeit genommen, direkte Angriffe gegen den Applikationsserver zu starten: Die restriktiv definierte Arbeitsumgebung auf dem CPS bietet dem Angreifer kaum Chancen dafür. Man ist nicht in der Lage, die Browser-Software zu manipulieren oder durch andere Software zu ersetzen. Durch die Firewall- bzw. Filter-Platzierung zwischen dem CPS und dem Applikationsserver sowie zwischen dem Applikationsserver und den Datenbankservern wird zusätzliche Sicherheit geschaffen.

Selbstverständlich bringt die Citrix-Lösung nicht nur Vorteile mit sich. Aufgrund des zentralistischen Aufbaus sind die Citrix-Applikationsserver ein willkommener Angriffspunkt. Gelingt es einem Angreifer die Citrix-Server-Farm zu übernehmen, hat er potenziell Zugriff auf Daten sämtlicher Benutzer. CPS und CAG zählen aus diesem Grund zu den kritischen Infrastrukturbestandteilen, die einem verschärften Audit unterliegen müssen. Auch die Abhängigkeit von einem Softwarehersteller muss als Risiko berücksichtigt werden. Eine Übersicht der verfügbaren Citrix-Technologie befindet sich unter [cit11].

Mit seinem Produkt „Wireless Internet Client“ (WI-Client) stellte das Unternehmen W-IC Systems seinen Kunden eine Terminalserver-Arbeitsumgebung zur Verfügung, bei der sich der Citrix Metaframe Terminal Service-Client auf einem USB-Stick mit integriertem Fingerabdruck-Scanner befand. Damit konnte sich ein authentifizierter Benutzer von jedem internetfähigen Windows-System an seinem virtuellen Arbeitsplatz bei W-IC Systems arbeiten. Das Unternehmen warb mit hoher Verfügbarkeit und Sicherheit der Lösung: Laut dem Anbieter erfolgte die Datenspeicherung gespiegelt und wurde durch regelmäßige Backups unterstützt, das Rechenzentrum wurde durch eine zusätzliche Anti-Malware-Lösung gegen Angriffe aus dem Internet geschützt. Als ein wichtigstes Verkaufargument nannte der Anbieter die Diebstahlsicherheit der Lösung: Beim Abhandenkommen des USB-Sticks würde der Angreifer keinen Zugriff auf die Daten des Benutzers erhalten.

Trotz der auf der Seite des Anbieters angepriesenen Vorteile wäre eine analoge Lösung

für den Einsatz in medizinischen Forschungsnetzen ungeeignet: Die relativ schwache biometrische Authentifizierung bietet nicht die erforderliche Sicherheit.[15] Die Beschränkung auf Windows als einzige unterstützte Client-Umgebung könnte von vielen Teilnehmern nicht akzeptiert werden. Gegen diese Lösung spricht auch die Überlassung der Forschungsnetzdaten einem privaten Dritt-Unternehmen, das an dem Verkauf dieser Daten evtl. interessiert sein könnte. Außerdem bietet die Lösung keine Überprüfungsmöglichkeiten des Client-Systems an.[16] Ein weiterer Nachteil der Lösung war ihre Unflexibilität: Für den auf dem USB-Stick gespeicherten Citrix-Client bestehen keine Update-Möglichkeiten. Somit sind die Updates nur durch den kostspieligen Stick-Austausch möglich.
Leider lässt sich heute nicht mehr feststellen, aus welchen Gründen der im Jahr 2006 noch aktive Anbieter sein Angebot des WI-Clients inzwischen eingestellt hat; die Webseite des Unternehmens ist nicht mehr aufrufbar. Die Ursachen könnten sowohl in der fehlenden Praxistauglichkeit der Lösung, technischen Umsetzungsschwierigkeiten, mangelnder Wirtschaftlichkeit, Patentstreitigkeiten oder aber in auch diversen anderen Gründen liegen. Lediglich die Spezifikation des Verfahrens auf der Seite der Weltorganisation für geistiges Eigentum erinnert noch an diese Lösung (vgl. [wip06]). Trotz diverser K.o.-Kriterien der beschriebenen Lösung für den Forschungsnetzeinsatz kann ein ähnlicher Ansatz für die Entwicklung einer für das Forschungsnetz geeigneter Lösung verfolgt werden.

Einsatz der TPM-Technologie: Obwohl der flächendeckende TPM-Einsatz auf der Client-Seite nicht möglich ist, gilt dies nicht für die Systeme, die sich im Eigentum des Forschungsnetzes befinden. So kann es sinnvoll sein, im Server- und Administrationsbereich TPM-fähige Systeme einzusetzen.[17] Ein TPM-Chip ist in der Lage, Manipulationen an den Systemkomponenten zu erkennen. Obwohl die Server-Systeme von dieser Eigenschaft nur wenig profitieren, da deren physikalische Sicherheit i. d. R. gewährleistet ist, kann diese bei Administrationssystemen sinnvoll eingesetzt werden. Mithilfe des TPM-Chips ist es möglich, die Administrationsrechner zu identifizieren und zu authentifizieren.
Auf den Administrationssystemen sollen keine Patientendaten gespeichert werden. Da dies nicht immer garantiert ist,[18] sollen sich die Daten auf den Administrationssystemen nur in verschlüsselter Form befinden. Mithilfe des TPM wird hierfür eine Hashsumme der Hardwarekenndaten gebildet. Dadurch wird ein System eindeutig und kann nicht nachgebildet werden. Die Sicherheit auf der kryptografischen Seite garantiert das eingesetzte

[15] Siehe dazu Abschnitt 3.5.3 „Authentifizierung von Forschungsnetzteilnehmern“.

[16] Die daraus resultierenden Gefahren wurden bereits erläutert.

[17] Einige Sicherheitsexperten warnen jedoch vor dem möglichen Kontrollverlust über die eigene Infrastruktur bedingt durch den Einsatz der TC-Technologie. So empfahl z. B. Johannes Schlattmann auf dem IT-Sicherheitskongress des GDV die Abschaltung der TPM-Funktionalität bei TPM-fähiger Hardware, um den o. g. Kontrollverlust zu vermeiden (vgl. [Sch08]).

[18] Es ist nicht auszuschließen, dass manche Auslagerungs- und temporäre Dateien solche Daten beinhalten.

und derzeit als sicher geltende RSA-Verfahren mit der Schlüssellänge von 2048 Bit. Die Manipulation des TPM-Moduls führt zu einer Zerstörung der Daten. Diese Hashsumme kann auch für die Verschlüsselung der Systemdaten verwendet werden (Sealing & Signing). Sollte es dem Angreifer gelingen, einen Datenträger mit den Patientendaten aus dem administrativen Bereich zu entwenden, wäre er trotzdem nicht in der Lage, diese an einem anderen System auszulesen.
Endorsement Key Pair (EK) verlässt nie das TPM-Modul. Aus diesem Grund werden mithilfe des Endorsement Keys die sogenannten Attestation Identity Keys (AIK) eingesetzt, die vom TPM erzeugt werden und den Chip verlassen können. Um die Zugehörigkeit eines AIKs zu einem EK zu beweisen, werden im Rahmen von Direct Anonymous Attestation (DAA) die sogenannten Zero-Knowledge-Beweise eingesetzt. Ein Zero-Knowledge-Beweis stellt sicher, dass die Authentizität von AIKs bewiesen wird, ohne den EK bekannt zu geben. TPM stellt außerdem einen Hardware-basierten Zufallsgenerator zur Verfügung, der für die Erzeugung von sicheren Schlüsseln verwendet werden kann.
Ein TPM ermöglicht Einrichtung geschützter Bereiche (z. B. für die Ausführung besonders kritischer Operationen (Verschlüsselung) oder für die Aufbewahrung von Schlüsseln), sodass auch eine mit Superuser-Berechtigungen ausgeführte Malware diese Bereiche nicht kompromittieren kann. TPM ist außerdem in der Lage, diverse Validierungsvorgänge durchzuführen. Mithilfe des TPMs können die Authentizität von Systemen (Signierung von PCRs durch AIK) und die Authentizität gegenüber von Systemen (Systemdaten in Verbindung mit AIK) überprüft werden. Der Einsatz von TPM-fähigen Serversystemen innerhalb des Forschungsnetzes kann eine zuverlässige Authentifikation von Servern (Vermeidung von Spoofing-Angriffen), Sicherstellung der Systemintegrität und die Erzeugung von zuverlässigen kryptografischen Schlüsseln ermöglichen. Ausführliche Informationen zu den Eigenschaften der TPM-Technologie befinden sich in [tcg09a] bzw. [tcg09b].

C.3.1.2. Ausfallsicherheit der Arbeitsumgebung

Auch die Ausfallsicherheit eines Systems ist ein Bestandteil des Konzeptes „sichere Arbeitsumgebung“. In der heutigen IT-Welt ist der Trend zu der Virtualisierung von Laufzeitumgebungen zu erkennen. Die Hardwareressourcen eines Systems oder Systemverbundes können beispielsweise mithilfe von VMWare- bzw. Virtual-PC-Technologien auf mehrere virtuelle Systeme aufgeteilt werden. So könnte z. B. ein einziges großes, gegen Hardwareausfälle durch Redundanzen abgesichertes System, Platz für einen virtuellen Rechner-Cluster bieten (siehe Abbildung 25). Eine solche Lösung wäre z. B. mithilfe der VMWare ESX-Server- oder Xen-Technologie möglich.
Eine kostengünstige und gleichzeitig sichere Alternative besteht im Einsatz von geclusterten virtuellen Systemen. Bei diesem Ansatz werden unterschiedliche virtuelle Clusterknoten auf mehrere physikalische Maschinen verteilt. Kommt es zu einem Hard- oder Softwareproblem bei einem der Hostsysteme, können ihn die virtuellen Cluster-Mitglieder ersetzen. In der

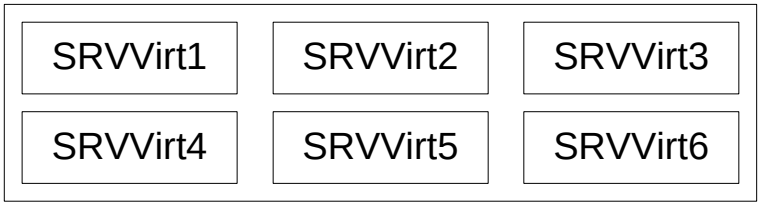

Abbildung 25.: Mehrere virtuelle Systeme auf einem hochverfügbaren Server: Ein einziges großes, gegen Hardwareausfälle durch Redundanzen abgesichertes System kann als Basis für einen virtuellen Rechner-Cluster dienen.

Abbildung 26 sind Knoten von zwei Applikationsclustern (SRVVIRT1 und SRVVIRT3 sowie SRVVIRT2 und SRVVIRT4) auf zwei physikalische Maschinen (System1 und System2) aufgeteilt. Sollte eines der beiden Systeme ausfallen, würden die virtuellen Clusterknoten des zweiten Systems weiterhin funktionieren.

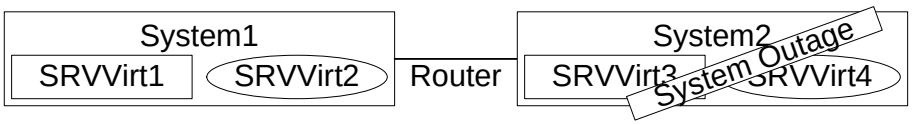

Abbildung 26.: Vier virtuelle Clusterknoten verteilt auf zwei physikalische Systeme: Die Knoten von zwei Applikationsclustern (SRVVIRT1 und SRVVIRT3 sowie SRVVIRT2 und SRVVIRT4) befinden sich auf zwei physikalischen Maschinen (System1 und System2). Beim Ausfall eines der beiden physikalischen Systeme würden die virtuellen Clusterknoten auf dem anderen System weiterhin funktionieren.

Der in der Abbildung 27 dargestellte Aufbau kann eingesetzt werden, um den Teilnehmern individualisierte Arbeitsumgebung zu garantieren: Ein Netzteilnehmer baut im ersten Schritt eine Verbindung zum Virtualisierungsserver auf, auf dem die abgesicherte Umgebung ablaufen wird. Um die Serverkapazitäten zu schonen, darf sich die Arbeitsumgebung nicht permanent im Speicher des Servers befinden. Aus diesem Grund ist es sinnvoll, die Arbeitsumgebung eines Teilnehmers in Form eines Images[19] zu speichern. Da die primäre Aufgabe des Virtualisierungsservers nicht in der längerfristigen Speicherung von großen Datenmengen besteht, soll die Lagerung von verschlüsselten Images auf einem extra für diese Aufgabe dedizierten System erfolgen. Dieses System benötigt keine großen Prozessor- oder Arbeitsspeicherkapazitäten, sondern lediglich den für die Image-Aufbewahrung notwendigen Speicher und kann z. B. in Form eines NAS-Systems implementiert werden. Im zweiten Schritt wird die um ein Image-Attribut erweiterte Benutzerdatenbank abgefragt, wobei z. B. die ID des Teilnehmer-Images mitgeteilt wird. Ein Teilnehmer kann mehrere Images besitzen, sodass eine solche Abfrage auch mehrere Ergebnisse liefern kann (Schritt 2). Nun ruft der Virtualisierungsserver das notwendige Image in den Schritten 3 und 4 in verschlüsselter Form ab. Die Entschlüsselung erfolgt im Schritt 5 mithilfe des nur dem Netzteilnehmer bekannten Schlüssels. Anschließend wird das virtuelle System des Teilnehmers gestartet und ihm zur Verfügung gestellt (Schritt 6).
Zur Aufbewahrung des Schlüssels zur Ver- und Entschlüsselung des Software-Images

[19]Hier ist das Image des virtuellen Systems gemeint.

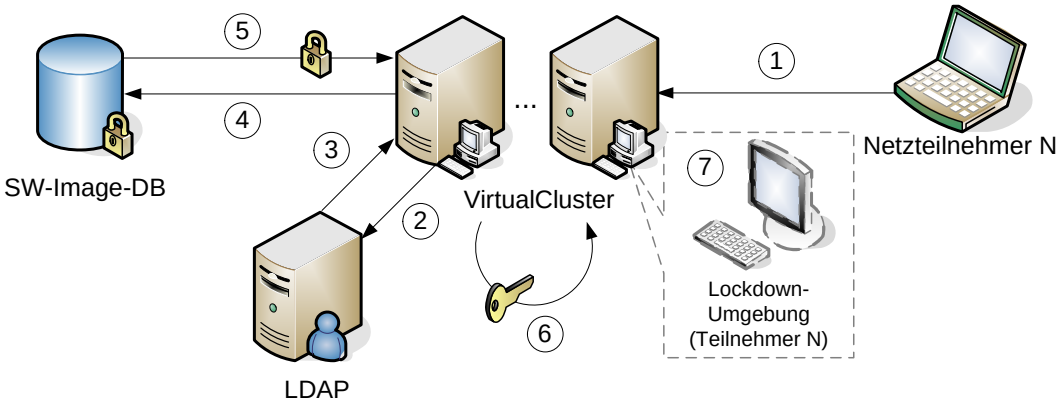

Abbildung 27.: Vorschlag für den Aufbau einer Virtualisierungsinfrastruktur: Die Kernkomponenten der Virtualisierungsinfrastruktur sind ein – für die Zurverfügungstellung einer sicheren Arbeitsumgebung zuständiger – Virtualisierungsserver und eine durch Verschlüsselung abgesicherte Image-Datenbank. Die Zuordnung eines Images zum Teilnehmer erfolgt mithilfe von Informationen aus dem Verzeichnisdienst.

würde sich der Image- oder der Virtualisierungsserver anbieten. Denkbar wäre auch die Speicherung des Image-Schlüssels als ein weiteres Attribut auf dem Directory-Server oder gar lokal auf dem Client. Aus der Sicht des Autors eignet sich die Speicherung des Schlüssels auf dem Client-System oder auf dem Virtualisierungsserver am wenigsten. Die Client-Umgebung könnte nämlich kompromittiert werden; der Schlüssel kann auch verloren gehen, falls es z. B. zu einem Festplattencrash des Clients kommt. Die Speicherung von Schlüsseln auf dem Virtualisierungsserver selbst unterliegt diesen Gefahren kaum, ist jedoch bedenklich aufgrund der Images, die auf dem Server vor dem Lade-Vorgang 6 entschlüsselt werden. Dies könnte einem Angreifer eine Art von Known-Plain-Text-Angriffen ermöglichen. Auch eine hohe Anzahl der sich auf diesem System befindenden Teilnehmer wäre im Falle einer Sicherheitslücke des Virtualisierungsservers ein Risiko. Die Speicherung der Schlüssel als Bestandteil des Images oder die Ablage auf dem Image-Server selbst wäre bezüglich der o. g. Bedrohung weniger kritisch. Die Ansammlung von Schlüsseln und Softwareimages wäre lediglich dann bedenklich, wenn das auf der SmartCard verwendete Verschlüsselungsverfahren unsicher wäre. In diesem Fall hätte ein die Image-Datenbank übernommener Angreifer die Möglichkeit, Images aller Teilnehmer zu entschlüsseln. Die Speicherung des Schlüssels als ein weiteres Attribut in der Directory-Struktur neben der Image-Kennung ist am unproblematischsten. In diesem Fall sind die Images getrennt von den Schlüsseln aufbewahrt, die wiederum durch die technische Sicherheit des Directory-Servers gegen Diebstahl und Verlust geschützt sind.
Die beschriebene Virtualisierung der Laufzeitumgebung bietet eine bequeme Basis für die Kontrolle der Arbeitsumgebung. Die virtuellen Systeme verändern nicht die Konfiguration des eigentlichen Host-Systems und müssen nicht der Sicherheitspolicy des Geräteinhabers entsprechen. Um die Forschungsnetz-konforme Konfiguration der virtuellen Systeme zu gewährleisten, kann das virtuelle System nach seiner Aktivierung Verbindung zu einem der Richtlinien-Server des Forschungsnetzes aufbauen. Aufgrund der übermittelten Daten entscheidet der Richtlinien-Server, ob das untersuchte Gerät den Richtlinien entspricht

und leitet seine Auswertung an den Anmelde-Service weiter. Es ist empfehlenswert, neben dem Vollzugriff und der vollständigen Zurückweisung des Systems (wegen Nichtvertrauenswürdigkeit) einen weiteren Quarantänezustand einzuführen. Dieser Status wird dem virtuellen System dann zugewiesen, wenn es diesem zwar noch kein Vollzugriff gewährt werden kann, die dafür erforderlichen Voraussetzungen allerdings von dem System noch erfüllt werden können. Ein solches System könnte z. B. dann mit dem Update-Server verbunden werden,[20] um die Sicherheitsupdates zu beziehen. Zusätzlich zu den bereits erwähnten Zuständen sollen weitere „eingeschränkte“ Zustände definiert werden. Die Restriktionen sollen in Verbindung mit Benutzerkennung errechnet werden und können z. B. in Form von der Anzahl der maximal zulässigen Anfragen pro Zeitintervall, der Art verfügbarer Dienste, gelieferter Daten etc. erfolgen.

C.3.2. Anbindungsmöglichkeiten für externe Forschungsnetzteilnehmer

Die externen Teilnehmer des Forschungsnetzes sind mit Außendienstmitarbeitern eines Unternehmens vergleichbar. Für die Anbindung des Außendienstes bzw. der Heimarbeitsplätze existieren mehrere Konzepte, wobei die meisten davon von einer bestimmten Beschaffenheit der Clients ausgehen und folglich auf ein Forschungsnetz nur bedingt anwendbar sind.

Standleitung, MPLS: Eine der sichersten und gleichzeitig der kostspieligsten Möglichkeiten wäre die Anbindung über eine Standleitung für sämtliche Forschungsnetzteilnehmer. Solche Leitungen (auch als Datendirektverbindung bekannt) sind von dem Zugriff der Öffentlichkeit abgesichert. Lediglich Mieter der Leitung haben exklusiven Zugriff auf die Daten, die durch diese übertragen werden. Sämtliche Daten, die über solche Leitungen übertragen werden, sind per Definition sicher gegen die Sniffing-Angriffe.[21] Der größte Nachteil einer Standleitung ist der Kostenfaktor. Die meisten Anbieter binden die Entfernungskomponente in ihre Preiskalkulation ein, sodass die Datendirektverbindung (DDV) für internationale Forschungsnetzteilnehmer kaum zu bezahlen wäre. Sie würden vergleichsweise hohe Kosten auf der Seite des Forschungsnetzes und der Netzteilnehmer verursachen und sind deswegen für den o. g. Zweck nicht empfehlenswert. Auch wenn die Anbindung der Netzteilnehmer nicht über DDV erfolgen kann, ist diese Form der Anbindung für die Verbindung zwischen den Forschungsnetz-Datenbankservern zu empfehlen. In der Tat ist eine dedizierte Standleitung eine sinnvolle Art, die Netzsegmente mit *IDAT*- und *MDAT*-

[20] Um die Kompromittierungsrisiken des Forschungsnetzes über den Update-Server zu minimieren, darf dieser nicht vollständig in das Forschungsnetz integriert werden. Es ist sinnvoll, den Update-Server in einem separaten, vom Rest des Netzwerks getrennten, LAN bzw. VLAN-Segment zu platzieren.

[21] Da es zumindest theoretisch keine weiteren Teilnehmer gibt, die auf die Daten zugreifen könnten. Lediglich der Netzbetreiber wäre in der Lage, die Kommunikation zu überwachen. Diese Form der Anbindung wird beispielsweise vom GDV allen am eVB-Verfahren teilnehmenden Versicherungsunternehmen aufgezwungen.

Servern miteinander zu verbinden. Etwas kostengünstiger als eine „echte“ Standleitung ist eine MPLS-basierte Verbindung. Durch sogenannte Labels (Paketkennzeichen) auf Layer 2 ist ein Anbieter in der Lage, Pakete mehrerer Teilnehmer gleichzeitig über dieselbe Leitung zu verschicken, wobei bei den Teilnehmern der Eindruck entsteht, sie würden eine dedizierte Verbindung verwenden. Die Sicherheit eines MPLS-Tunnels ist relativ hoch; ein Angriff setzt den Zugriff auf das Netz des Providers voraus.[22] Sollte innerhalb des Forschungsnetzes ein MPLS-VPN eingesetzt werden, muss dafür gesorgt werden, dass Daten nur verschlüsselt übertragen werden.

Wählleitung: Eine zugegeben etwas antiquierte Alternative besteht in der Verwendung von Wählleitungen. Forschungsnetzteilnehmer könnten sich mit Modems oder ISDN-Karten am RAS-Server des Forschungsnetzes einwählen und mithilfe von Benutzernamen und Passwort authentifizieren. Viele Remote-Lösungen sehen außerdem eine zusätzliche Sicherheitskomponente in Form eines Rückrufs des Remote-Teilnehmers vor. Obwohl dieses Element zusätzliche Sicherheit mit sich bringt, wird seine Wirkung durch die Schwachstellen in den anderen Elementen eines Sicherheitskonzeptes ausgehebelt. Ein Beispielszenario eines solchen Angriffs beschreibt [Str99]. Da bei einer üblichen Wählverbindung die Daten unverschlüsselt übertragen werden, müsste man Verschlüsselung einsetzen, um das Senden von Daten im Klartext zu vermeiden. Außerdem wurde bereits auf die Schwächen der passwortbasierten Authentifikation hingewiesen, von derem Einsatz im Bereich des Forschungsnetzes abzuraten ist. Ein weiterer Nachteil der wählleitungsbasierten Lösung besteht in ihren hohen Kosten.

Virtuelle Private Netze (VPN): Die für das Forschungsnetz bezahlbare und gleichzeitig sichere Art der Teilnehmeranbindung ist die Verwendung von VPNs. Dabei ist der Einsatz von Verschlüsselung unabdingbar, da reine VPN-Definition diesen nicht impliziert.[23] Grundsätzlich wird zwischen drei VPN-Arten unterschieden: host-to-host, host-to-gateway und gateway-to-gateway.
Host-to-host VPNs: Host-to-host VPNs werden eingesetzt, um eine sichere Verbindung zwischen zwei Systemen herzustellen. Theoretisch ist es möglich, die gesamte Kommunikation innerhalb des Forschungsnetzes durch verschlüsselte VPN-Verbindungen zu sichern; dies wäre jedoch mit einem enormen Ressourcenaufwand verbunden. Außerdem ist eine direkte Kommunikation zwischen den einzelnen Forschungsnetzteilnehmern nicht vorgesehen. Die Kommunikation innerhalb des „Kerns“ des Forschungsnetzes erfolgt dagegen in einer kontrollierten Umgebung, in der Sniffing-Angriffe per Definition nicht möglich sein sollten. Die zusätzliche Verwendung von VPNs würde hier höhere Kosten ohne einen nennenswerten Gewinn für die Forschungsnetzsicherheit bedeuten.

[22] Einbruch in die Vermittlungsstellen des Providers bzw. Ausgraben der Leitungen.

[23] Auch ein ungesicherter Klartexttunnel ist ein VPN.

Host-to-gateway VPN: Der Einsatz von host-to-gateway VPNs ist denkbar, um die Kommunikation zwischen den einzelnen Netzwerkteilnehmern und den Lockdown-Servern zu sichern (siehe Abbildung 28). Die Verbindung zwischen den Lockdown-Servern und dem Applikations-Cluster soll dagegen unverschlüsselt erfolgen, da diese in einer kontrollierten Umgebung stattfindet. Zudem würde eine verschlüsselte VPN-Verbindung den IDS-Sensoren kein sinnvolles Abhören und Auswerten der Kommunikation erlauben.

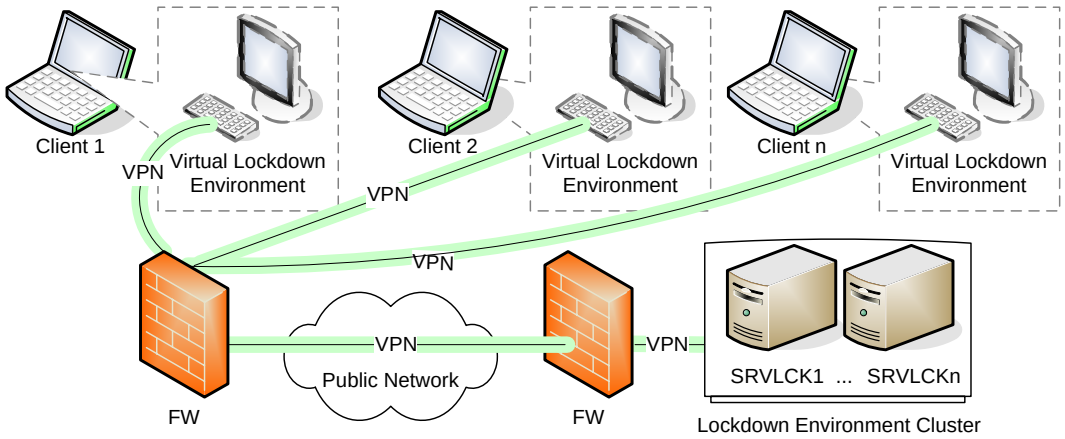

Abbildung 28.: Einsatzvorschlag für die host-to-gateway VPNs: Die Lockdown-Server agieren als VPN-Endpunkt. Die Verschlüsselung gewährleistet eine sichere Datenübertragung von den Clients zu der Lockdown-Umgebung.

Gateway-to-gateway VPN: Die Aufrechterhaltung einer VPN-Verbindung ist mit einem hohen Ressourcenverbrauch verbunden. Besonders bei Client-Systemen werden die Rechenkapazitäten beansprucht. Die sogenannten gateway-to-gateway VPNs können für die Entlastung der Clients sorgen. Der Einsatz von gateway-to-gateway VPNs soll dann gestattet werden, wenn sich mehrere Forschungsnetzteilnehmer im Forschungsnetzwerk permanent befinden, und die Sicherheit ihrer Verbindungen zu dem VPN-Gateway gegen Sniffing-Angriffe als hinreichend bewertet wird (siehe Abbildung 29).

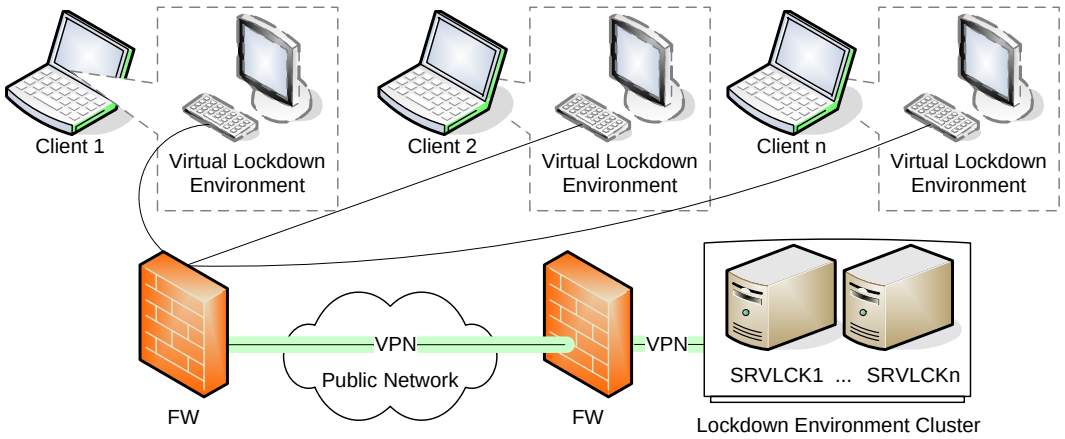

Abbildung 29.: Einsatzvorschlag für die gateway-to-gateway VPNs: Wenn mehrere Clients sich in einer vertrauenswürdigen Infrastruktur befinden, und eine sichere Datenübertragung zwischen dem Client-Subnetz und der Lockdown-Umgebung über eine unsichere Verbindung gewährleistet werden soll, können die gateway-to-gateway VPNs eingesetzt werden.

Die Verschlüsselung einer VPN-Verbindung kann auf mehreren Ebenen erfolgen (vgl. [NZW02]):

- Applikationsebene (Application Layer, OSI-Ebene 7 (z. B. SSH, PGP, S/MIME, PEM, SSL)),
- Transportebene (Transport Layer, OSI-Ebene 4 (z. B. Filterung von Zugriffen auf die TCP-Ports durch die Änderung des herstellerspezifischen IP-Stacks)),
- Netzwerkebene (Network Layer, OSI-Ebene 3 (z. B. IPSec)) (vgl. [Eck07, S. 711 ff.]),
- Streckenebene (Data Link Layer, OSI-Ebene 2 (z. B. PPTP, L2F, L2TP)).

Die Verschlüsselung auf Applikationsebene kann z. B. mithilfe von PGP oder SSH realisiert werden. Auf der Transportebene kann beispielsweise SSL eingesetzt werden. Eine verschlüsselte Verbindung auf der Netzwerkebene kann mithilfe von solchen Protokollen wie IPSec aufgebaut werden. Der Vorteil eines VPN-Tunnels auf Netzwerkebene besteht darin, dass im Gegensatz zu den beiden o. g. Methoden solche Kommunikationsdetails wie verwendete Kommunikationsprotokolle, Ports etc. verschleiert werden können. Lediglich die IP-Adressen werden bekannt gegeben, um ein problemloses Routing gewährleisten zu können. Protokolle wie L2TP (Layer 2 Tunneling Protokoll) und PPTP (Point-to-Point Tunneling Protokoll) sorgen für die Verschlüsselung auf der Streckenebene.[24] Die häufig für die Authentifizierung von PPTP-Verbindungen eingesetzte verbesserte Version des Challenge-Response-Verfahrens (MSCHAPv2) schützt den Schlüssel nur unzureichend. Seit der Jahrtausendwende sorgt das Zertifikate und MD5-Hashes unterstützende Extensible Authentication Protocol (EAP) für höhere Sicherheit des Protokolls. Das seit Windows XP von Microsoft unterstützte L2TP besitzt keine eigene Verschlüsselung und verwendet IPSec, sodass für solche VPNs das von IPSec gewährleistete Sicherheitsniveau maßgeblich ist. Weitere Nachteile von PPTP sind die mit vielen Routern auftretenden Probleme und unverschlüsselte Übertragung von Kenndaten, was einige NAT-Router in die Lage versetzt, die Call-IDs der Clients zu protokollieren (vgl. [BS08], [Eck07, S. 699 f.]).
Obwohl die Verschlüsselung von VPN-Verbindungen auf mehreren Ebenen durch den Einsatz von unterschiedlichen Protokollen/Tools erfolgen kann, entsprechen nicht alle dieser Techniken den vom Forschungsnetz gestellten Anforderungen. Eine für das Forschungsnetz geeignete VPN-Lösung muss folgende Kriterien erfüllen:

[24] PPTP wird hauptsächlich unter Windows eingesetzt und baut eine verschlüsselte PPP-Brücke auf. Dabei ist PPP für die Authentifizierung, Aushandlung von IP-Adressen, Bestimmung von Paketgrößen und Verschlüsselung zuständig. Die Authentifizierung und die Aushandlung von Schlüsseln zählen zu den Schwächen des PPP und somit des PPTP. Die Teilnehmer werden durch ein Challenge-Response-Verfahren (MSCHAPv1) authentifiziert, wobei der Server eine Klartextnachricht an den Client sendet, der diese seinerseits verschlüsselt und zurückschickt. Diese aus 24 Bytes bestehende LM-Hash-Nachricht lässt sich mit einem vertretbaren Aufwand knacken (vgl. [Bac03]).

- Die *Vertraulichkeit* einer VPN-Verbindung muss durch verwendete Verschlüsselung gewährleistet werden. Die verwendeten Verschlüsselungsalgorithmen und ihre Schlüssellängen müssen so gewählt werden, dass ein erfolgreicher Angriff auf die Verschlüsselung nach den aktuellen Erkenntnissen der Informatik praktisch nicht durchführbar ist.

- Die *Datenintegrität* einer VPN-Verbindung wird mithilfe von Signaturen und Hashwerten erreicht. Es muss gewährleistet werden, dass die Informationen während der Übermittlung nicht manipuliert werden können.

- Die *Authentizität* von Informationen ist innerhalb eines Forschungsnetzes von enormer Bedeutung, da eine erhöhte Gefahr von Man-in-the-Middle-Angriffen besteht (s. a. Abschnitt 3.5.5 „Zugangsszenarien von Netzteilnehmern zu den Forschungsnetzdiensten“). So könnte sich ein Angreifer als ein Forschungsnetzserver auszugeben, um beispielsweise die Login-Informationen von den Forschungsnetzteilnehmern auszuspähen.

- Die VPN-Lösung muss *auf offenen Standards* basieren und von der Mehrzahl der Anwender akzeptiert werden. Der Einsatz von proprietären VPN-Lösungen ist nicht empfehlenswert (s. a. Abschnitt C.3.2.3 „CryptoGuard VPN (CGVPN):“).

- Manche Forschungsnetzdienste könnten eine *Echtzeitfähigkeit* der VPN-Lösung erfordern. In solchen Fällen ist der Einsatz von Software-VPNs zu überprüfen, denn die wenigsten (Software-)Lösungen werden diese Anforderung erfüllen können.

Eine VPN-Lösung bringt allerdings nicht nur Vorteile mit sich. Jedes über VPN verschicktes Datenpaket erhält zusätzliche Header-Informationen oder wird in ein sogenanntes Wrapper-Paket verpackt. Der entstehende Paket-Overhead kann zu unerwarteten Problemen führen und muss bei der Konzeption der Infrastruktur des Netzwerkkerns eines Forschungsnetzes berücksichtigt werden. Die größeren Pakete können zu einer erhöhten Paket-Segmentierung führen, was wiederum in einer schlechteren Leitungsperformance resultiert. Ein weiterer Nachteil des VPN-Einsatzes für das Forschungsnetz besteht in den evtl. zu erwartenden höheren Kosten, die bei Störungsbeseitigung anfallen können, denn die VPN-Paketinformationen sind erst nach der Entschlüsselung einsehbar. Dies kann z. B. zum Mehraufwand bei der Behebung von diversen Leitungsstörungen führen. Die VPN-Verschlüsselung kann außerdem die Installation erwünschter Überwachungseinrichtungen problematisch werden lassen. Die Platzierung von IDS-Sensoren in einer VPN-Umgebung muss wohl überlegt sein, da die Verschlüsselung eine sinnvolle Datenauswertung an vielen Stellen nicht zulässt. Der in mancher Literatur zu findende Hinweis auf die zusätzliche CPU-Auslastung aufgrund der eingesetzten Verschlüsselung und die dadurch reduzierte Verarbeitungsgeschwindigkeit ist heute kaum noch relevant.

C.3.2.1. PKI-Einsatz beim VPN-Aufbau

Für die Erstellung einer sicheren VPN-Verbindung wird die Verwendung der bereits angesprochenen forschungsnetzeigenen PKI empfohlen. Um beispielsweise eine sichere host-to-gateway-Verbindung herzustellen, könnte der Client einen signierten öffentlichen Schlüssel vom VPN-Gateway anfordern und ihn auf seine Gültigkeit überprüfen. Das VPN-Gateway würde dann das empfangene Zertifikat (den von CA signierten Schlüssel) des Clients, wie in der Abbildung 30 dargestellt, seinerseits verifizieren.

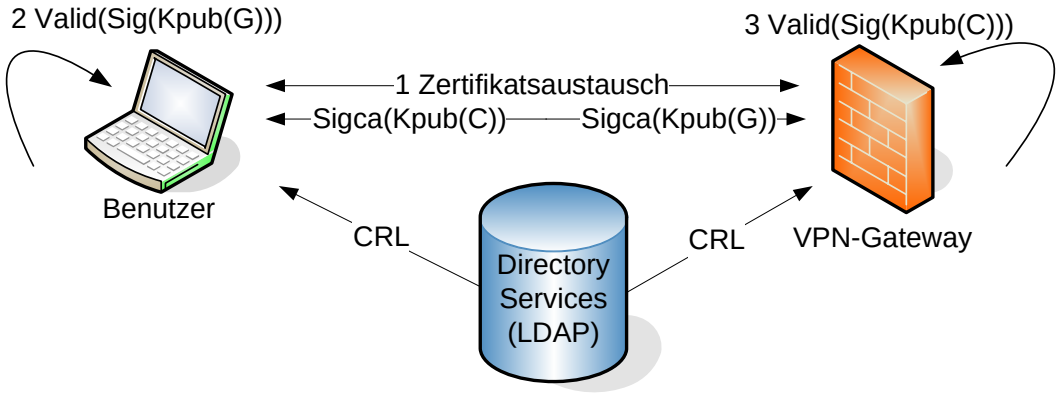

Abbildung 30.: Zertifikatsvalidierung mithilfe von CAs: Für die Herstellung einer sicheren host-to-gateway-Verbindung fordert der Client einen signierten öffentlichen Schlüssel vom VPN-Gateway an und prüft dessen Gültigkeit. Das VPN-Gateway prüft seinerseits das empfangene Client-Zertifikat.

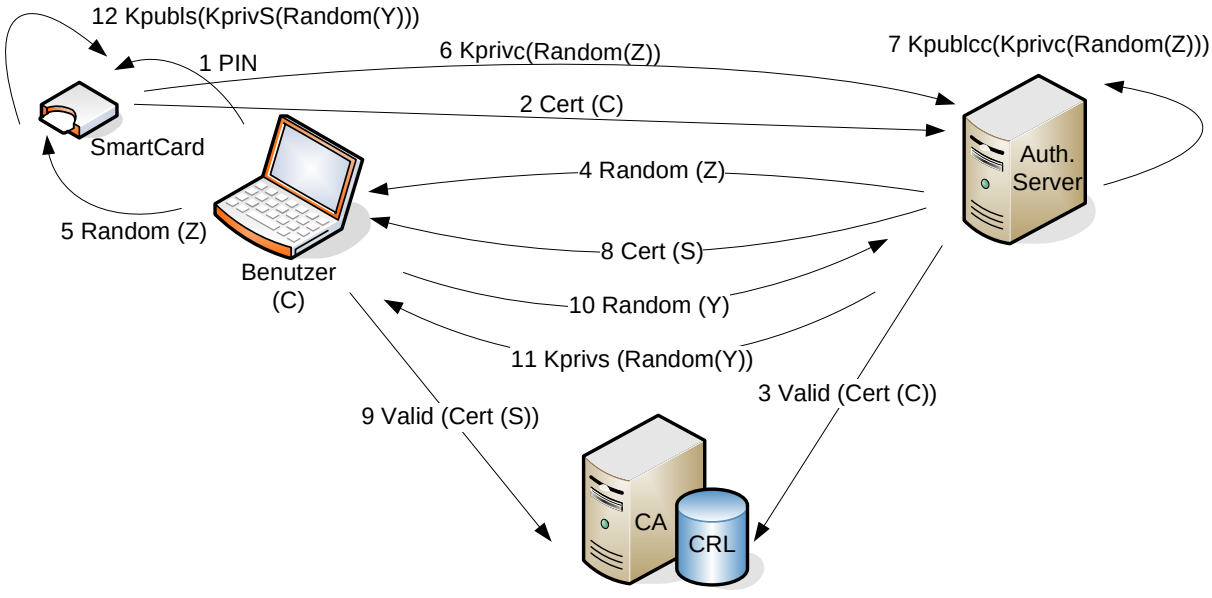

Abbildung 31.: Authentifikation mithilfe der PKI: Um Man-in-the-Middle-Angriffen vorzubeugen, können der Client und der Server einem Verifikationsverfahren analog zum IPSec-Main Mode unterzogen werden.

Auch eine sichere Client-Authentifikation beim VPN-Verbindungsaufbau ist durch den PKI-Einsatz möglich. Der vorgeschlagene Ablauf des Authentifikationsprozesses ist in der Abbildung 31 dargestellt. Der private Schlüssel und das Zertifikat werden dabei auf der Karte durch die PIN-Eingabe frei geschaltet. Das Zertifikat wird anschließend an

den Server verschickt, dort wird dessen Gültigkeit beispielsweise mithilfe einer Certificate Revocation List (CRL) und der CA-Unterschrift verifiziert. Um die Identität des Clients zu überprüfen, wird vom Server eine Zufallszahl erzeugt und an den Client geschickt. Diese muss vom Client mit seinem privaten Schlüssel verschlüsselt und an den Server zurückgeschickt werden. Der Server kann nun die Identität des Kommunikationspartners mithilfe des entsprechenden öffentlichen Schlüssels überprüfen. Um Man-in-the-Middle-Angriffe vorzubeugen, wird sich die Serverseite einer ähnlichen Authentifizierungsprozedur unterziehen müssen.[25]

C.3.2.2. Empfehlenswerte Standards

Die Struktur des Forschungsnetzes macht die Verwendung von offenen und nicht proprietären Standards im Bereich VPN notwendig. So bietet sich z. B. der Einsatz von IPSec mit dem Schlüssel-Managementverfahren IKE an. IPSec ist ein übergreifender Standard für sichere Kommunikation mit TCP/IP und ist ein Überbegriff für mehrere Protokolle. IPSec zeichnet sich aus durch Vertraulichkeit der Daten, Authentizität der Absenders und des Empfängers, Integrität der Daten, Nichtabstreitbarkeit und besteht aus folgenden Grundelementen:

- *Security-Protokolle* (Authentifikationsheader (AH) bietet authentifizierte aber unverschlüsselte Übertragung) und ESP (Encapsulating Security Payload – verschlüsselte authentifizierte Kommunikation).
- *Security Associations (SA)*(Verwaltung von Beziehungen (SA) zwischen Kommunikationspartnern. Dieser IPSec-Bestandteil ist für das Aushandeln von Algorithmen und Security-Protokollen zuständig).
- *Key-Management* (Schlüsselaustausch und Schlüsselerneuerung) erfolgt entweder manuell oder automatisch durch IKE (Internet Key Exchange).
- *Algorithmen* (Verschlüsselungsverfahren) (vgl. [Dav02], [Str99], [KA98]).

IPSec kann im transparenten oder auch im sogenannten Tunnel-Modus eingesetzt werden. Im Tunnel-Modus erhält ein Datenpaket einen Wrapper.[26] IKE basiert auf ISAKMP/Oakley und wird für das Key-Management und für das Aushandeln von Security Associations eingesetzt.

[25]Das beschriebene Verfahren entspricht dem sogenannten Main Mode von IPSec, welcher in der ersten Phase der Verschlüsselungsvereinbarung und Authentifizierung (Internet Key Exchange) verwendet wird.

[26]Der Wrapper wird zum Bestandteil eines neuen Pakets.

C.3.2.3. IPSec-Alternativen

Der Vorteil von IPSec gegenüber anderen Verfahren zur verschlüsselten Datenübertragung (wie z. B. SSL) liegt in der Anwendungsunabhängigkeit. So arbeitet beispielsweise SSL auf der Socket-Ebene und muss in die Anwendung integriert werden. IPSec kann dagegen beliebigen Datenverkehr übertragen.

CryptoGuard VPN (CGVPN): Gegen eine IPSec-basierte Lösung könnte der relativ hohe Einführungsaufwand sprechen. So arbeiten die IPSec-Gateways als Router und machen die Umkonfigurierung des Netzes erforderlich, was in einem heterogenen Umfeld nicht immer trivial ist. Selbstverständlich existieren auch Alternativen zu IPSec/SSL. So entschloss sich z. B. die Max-Planck-Gesellschaft für den Einsatz eines proprietären VPN-Produkts des Unternehmens Compumatica secure networks GmbH (CryptoGuard VPN (CGVPN)). Die VPN-Lösung wurde für ca. 80 Institute und Einrichtungen, die an dem Deutschen Forschungsnetz angeschlossen sind, eingeführt.[27] Im von den Geräten des Herstellers unterstützen CG-Modus wird lediglich der Datenanteil eines Datagramms verschlüsselt. Die IP- und TCP/UDP-Header des Original-Pakets bleiben erhalten; Firewall-Regelwerke müssen dadurch nicht angepasst werden. Ein CGVPN-System arbeitet wie eine Bridge und erfordert lediglich eine IP-Adresse für Konfigurationszwecke. Die restlichen Netzwerkkomponenten müssen bei der Umstellung nicht umkonfiguriert werden. Man entschloss sich für den CGVPN-Einsatz nicht zuletzt aufgrund einer guten Performance, die nach Angaben des Herstellers wesentlich schneller als IPSec ist (vgl. [FRG05]).
Auch wenn der Anwenderbericht[28] durchwegs positiv war, ist eine solche Lösung für den Einsatz in einem medizinischen Forschungsnetz nicht optimal. Neben den betriebswirtschaftlichen Bedenken wie Abhängigkeit vom Anbieter, Zukunftssicherheit der Lösung, Maintenance-Garantie etc. existiert eine Reihe von sicherheitsrelevanten Aspekten, die gegen den Einsatz einer proprietären Lösung sprechen. So wird z. B. in der Dokumentation des o. g. Herstellers das eingesetzte Verschlüsselungsverfahren nicht angegeben – ein Verstoß gegen das Kerckhoffs-Prinzip. Die Güte einer Sicherheitslösung lediglich an der Einfachheit der Implementierung und den guten Performancewerten[29] zu messen, ist höchst bedenklich. Eine proprietäre VPN-Lösung kann auch aufgrund der heterogenen Landschaft des Forschungsnetzes, die sich durch Hinzunahme und Abgang von Teilnehmern stark ändern kann, nicht eingesetzt werden. Die neuen Teilnehmer wären gezwungen, ihre bereits existierenden Sicherheitslösungen durch die neuen proprietären zu ersetzen,[30] was evtl. zu einer Hemmschwelle für die Kooperation zum Forschungsnetz werden könnte.

[27] Eine Infrastruktur, die sich durch starke Heterogenität auszeichnet.

[28] Details zum Anwenderbericht sind unter [FRG05] zusammengefasst.

[29] Zwei der Entscheidungskriterien bei der Auswahl der VPN-Lösung laut [FRG05].

[30] Da die bereits vorhandenen Lösungen den neuen proprietären Standard mit höchster Wahrscheinlichkeit nicht unterstützen würden.

Hamachi: Eine ebenfalls für ein Forschungsnetz nicht akzeptable Lösung wäre die Verwendung der Infrastruktur eines Drittanbieters zum VPN-Aufbau, wie es z. B. beim Hamachi-VPN der Fall ist (vgl. [log09]). Die Verwendung der Server einer fremden Firma zur Übertragung vertraulicher Daten ist ein Widerspruch in sich. Außerdem legt der Hamachi-Hersteller die Funktionsweise des Protokolls nicht vollständig frei, was eine Bewertung der Vertraulichkeit des Verfahrens erschwert.

SSL-VPN: Eine Alternative zu den IPSec-VPNs sind die in den letzten Jahren stark populär gewordenen SSL-VPNs. Die auf SSL/TLS basierenden Lösungen zeichnen sich durch relativ einfache Konfiguration und verlässliche Sicherheit aus. Grundsätzlich kann zwischen zwei Arten von SSL-VPNs unterschieden werden: VPNs, die eine Client-Installation erfordern und solchen, die ohne einen VPN-Client[31] auskommen. Der Einsatz von VPNs, die keine Client-Installation erfordern, ist innerhalb des Forschungsnetzes nicht empfehlenswert, da sie die Vertrauensstellung zwischen dem Client und dem Server nicht garantieren. Es wäre unmöglich festzustellen, von welcher Lokation ein Forschungsnetzteilnehmer die Verbindung aufnimmt. Selbstverständlich könnte man mithilfe diverser (Browser-)Plugins eine Sicherheitsüberprüfung des Clients erzwingen; die Ergebnisse einer solchen Prüfung wären jedoch nicht verlässlich. Schließlich würde die Aussage über das Sicherheitsniveau eines Systems vom System selbst kommen. Würde man sich ein kompromittiertes System als ein Haus mit einem sich darin befindenden Einbrecher vorstellen, könnte eine solche Sicherheitsprüfung mit einem Kontrolltelefonat verglichen werden. Das Risiko, dass der Einbrecher selbst den Hörer abnimmt und berichtet, dass alles in Ordnung sei, ist nicht zu vernachlässigen. Um die Identität der beiden Kommunikationspartner erfolgreich überprüfen zu können, bedarf es also einer VPN-Lösung, die eine vorhergehende Konfiguration erfordert.[32] Eine auf SSL bzw. TLS basierende Lösung „OpenVPN“ erfüllt diese Sicherheitsanforderung.[33]
Die Unterschiede zwischen SSL und TLS sind marginal: Das ursprünglich von Netscape entwickelte SSL wurde fast vollständig von IETF als TLS 1.0 übernommen. Die Unterschiede liegen in der zur Schlüsselerzeugung verwendeten Funktionen (PRF vs. RAND) und der HMAC-Fähigkeit von TLS. Im Internet wird meistens eine unidirektionale Authentifizierung in Verbindung mit SSL verwendet: Lediglich die Identität des Servers wird verifiziert. In TLS-VPNs werden die beiden Seiten mithilfe von Zertifikaten authentisiert; fast vierzig Sicherheitskontexte diverser Kombinationen von RSA, DH, AES, MD5 etc. werden unterstützt.
Für das Tunneling von Ethernet- und IP-Paketen sowie aller darüber liegenden Protokolle verwendet das auf TLS basierende OpenVPN bevorzugt das zustandslose UDP-Protokoll.

[31] Clientless SSL-VPN.

[32] Die Authentifikation von Client-Systemen wird im Abschnitt 3.5.1 „Sichere Arbeitsumgebung“ erläutert.

[33] Die Webseite des unter GPL stehenden Produktes befindet sich unter `http://openvpn.net/`.

Dadurch werden die evtl. durch die Ineinanderschachtelung von TCP-Flusskontrollalgorithmen entstehenden Verbindungsabbrüche und hohe Latenzzeiten vermieden. Laut der TLS-Spezifikation unterstützt TLS jedoch nur verbindungsorientierte Protokolle (TCP) (vgl. [DR08]). Um UDP trotzdem verwenden zu können, täuscht OpenVPN dem TLS einen eigenen TCP-Layer vor und wickelt die gesamte Kommunikation im Hintergrund über eine UDP-Verbindung. Dadurch entfällt die Notwendigkeit zur Authentifizierung von IP-Adressen und Portnummern, was TLS sowohl zur Kopplung von Netzwerken als auch Verbindung von einzelnen Systemen geeignet macht.

C.3.3. Aspekte der Zusammenführung von Patientendaten mithilfe der Ajax-, Java- und Terminalserver-Technologie

Die Zusammenführung von Patientenliste (*IDAT*)und Behandlungsdatenbank ($MDAT^W$) erfolgt im Behandlungszusammenhang in Form eines sequenziellen Zugriffs, dessen Ablauf ausführlich in [RDSP06, S. 20 ff.] beschrieben ist.

C.3.3.1. Angriffsszenarien bei einer Ajax-basierten Datenzusammenführung

Die Ajax-basierte Datenzusammenführung kann sowohl auf der Client-Seite als auch auf dem Transportweg ausgespäht werden. In diesem Abschnitt werden die beiden Angriffsarten sowie die Möglichkeiten ihrer Vorbeugung untersucht.

Angriffe auf dem Client: Der JavaScript-Code wird auf dem Client ausgeführt, sodass keine Möglichkeit existiert, den Code clientseitig zuverlässig gegen ein unbefugtes Einsehen zu schützen. Die Code-Analyse kann für die Vorbereitung von Angriffen auf andere Komponenten (z. B. auf den Server und die auf dem Server liegenden Daten) verwendet werden. Solange die Client-Konfiguration von seinem Besitzer bestimmt wird, besteht keine Möglichkeit, dies zu unterbinden. Solche Maßnahmen wie das Deaktivieren des Browser-Caches oder das Verschleiern des Codes können die Angriffe lediglich erschweren, diese jedoch nicht verhindern (vgl. [War08]). Aus diesem Grund dürfen solche sicherheitsrelevanten Funktionen wie die Zugriffskontrolle, Validierung von Parametern, Passwort-Verifizierung etc. nicht auf dem Client ausgeführt werden. Im Modell A der generischen Datenschutzkonzepte der TMF erfolgt die kritische Operation der Zusammenführung von *IDAT* und *MDAT* auf dem Client. Die Sicherheit dieses Ansatzes basiert somit auf der Sicherstellung der Integrität der Client-Umgebung, was den Einsatz sicherer Hardware bzw. einer aufwendig herzustellenden sicheren Software Lockdown-Umgebung voraussetzt (siehe Abschnitt 3.5.1 „Sichere Arbeitsumgebung“).
Diverse clientseitige Angriffsszenarien sind bei einer Ajax-Anwendung vorstellbar. Die dabei geltenden Gefahren ähneln den auf dem Transportweg lauernden Risiken, denn auch hier können die im Hintergrund aufwendig über mehrere Pseudonymisierungsstufen zusammengeführten Daten vom Angreifer an einer zentralen Stelle „bequem“ ausgespäht

werden. Der Hauptunterschied zwischen den Gefahren, die von der Client-Seite ausgehen, und den Gefahren im Hinblick auf den Transportweg besteht darin, dass ein Client-Angreifer primär die auf diesem Client angezeigten Daten ausspähen kann. Im Unterschied zum Angriff auf dem Transportweg können die auf dem Client gewonnenen Daten vom Angreifer i. d. R. mit weitaus weniger Aufwand zusammengeführt werden, da für den Angreifer hier das Wissen über die Datenstruktur entfällt. Bereits die Installation eines einfachen Malware-Programms zum Erstellen von Screenshots reicht aus, um die bereits zusammengeführten Patientendaten auszuspähen. Im Unterschied zu den Angriffen auf dem Transportweg handelt es sich dabei ausschließlich um aktive Angriffe, die die Integrität des Client-Systems verletzen.
Bei einer Reihe von Angriffen auf der Client-Seite können nicht nur die auf dem kompromittierten System angezeigten Daten betroffen sein. Bei Verwendung von Webservices werden die Daten über standardisierte Schnittstellen zur Verfügung gestellt (z. B. SOAP oder REST). Aufgrund ihrer offenen Architektur könnten diese Schnittstellen zum Kopieren der gesamten Forschungsdatenbestände missbraucht werden. Die Abhilfe kann hier durch eine Limitierung der Anfragen per Client für eine bestimmte Zeitspanne erfolgen. Einer der möglichen Ansätze wäre auch der Einsatz von Web Services Security (WS-Security).
Von einem kompromittierten Client-System können auch die Angriffe gegen die Server oder andere Netzteilnehmer gestartet werden. Die Schutzmaßnahmen gegen solche Angriffe werden in den Abschnitten 3.5.1 „Sichere Arbeitsumgebung“ und 3.5.5 „Zugangsszenarien von Netzteilnehmern zu den Forschungsnetzdiensten“ beschrieben.
Eine weitere mit dem Ajax-Einsatz verbundene Problematik ist auch als das sogenannte Polling-Problem bekannt. Die Ursache des Polling-Problems besteht darin, dass bei der asynchronen Kommunikation nicht der Server eine Datenänderung mitteilt, sondern der Client beim Server nachfragen muss, ob eine Änderung des Anwendungszustands stattgefunden hat. Dies resultiert in einer erhöhten Auslastung des Webservers, der für jede Client-Anfrage einen neuen Thread erzeugt, und erschwert die Skalierbarkeit einer Ajax-Anwendung. Ein Angreifer könnte z. B. das Polling-Problem für die DoS-Angriffe auf den Server ausnutzen.

Angriffe auf dem Transportweg: Die Angriffe auf dem Transportweg sind i. d. R. von passiver Natur. Bei dieser Angriffsart geht es hauptsächlich um das Mitprotokollieren von Daten, die beispielsweise im Behandlungszusammenhang zwischen dem Rechner des behandelnden Arztes und der Patientenliste bzw. der Behandlungsdatenbank ausgetauscht werden. Das Abhören von Daten kann durch eine Verschlüsselung unterbunden werden (s. a. Abschnitt C.3.8 „Verschlüsselung und Signaturen“).
Unabhängig davon, wie die Verschleierung der Patientenidentität erfolgt,[34] müssen die behandelnden Ärzte sowohl die identifizierenden Informationen eines Patienten eingeben als

[34]Zum Beispiel mithilfe einer mehrstufigen Pseudonymisierung über *IDAT* und *TempID*.

auch auf die Behandlungsdaten des Patienten zugreifen können. Somit erhält ein Lauscher den Zugriff auf die auf dem Bildschirm des Arztes angezeigten Patienteninformationen unabhängig von den im Hintergrund ablaufenden Pseudonymisierungsoperationen. Die von einem solchen Angriff ausgehende Gefahr wächst mit der Anzahl der Datensätze, die ein Angreifer auf diesem Wege abfangen kann. Kann der Angreifer Daten, die zwischen einem oder einigen wenigen behandelnden Ärzten und der Behandlungsdatenbank ausgetauscht werden, abfangen, ist der potenzielle Schaden bei Weitem nicht so groß, wie im Falle, wenn ein Angreifer den Datenaustausch zwischen allen Teilnehmern eines Forschungsnetzes abfangen kann. Kennt der Angreifer die verwendete Datenstruktur, kann er, in Abhängigkeit von den ausgetauschten Daten, innerhalb kürzester Zeit größere Teile der Patientendatenbank ausspähen.

Nicht alle Angriffe auf dem Transportweg erfolgen ausnahmslos passiv. So kann beispielsweise der Angreifer versuchen, durch das Einspielen von Datenpaketen in die Leitung bzw. durch die Manipulation und das erneute Versenden von Paketen, die Konfiguration der Client- oder Server-Systeme zu manipulieren und diese zu einer Fehlfunktion bzw. Nichtverfügbarkeit zu bewegen. Ein Angreifer könnte beispielsweise die im JSON- oder XML-Format verschickten Daten abfangen, sie mit dem Schadcode versehen und anschließend an den Client weiterleiten, um ihn zu kompromittieren. In einem solchen Fall dient ein Angriff auf dem Transportweg als Vorbereitung auf einen clientseitigen Angriff. Die Verschlüsselung der Pakete auf dem Transportweg (z. B. mittels SSL), Signierung der verschickten Daten (z. B. mithilfe von XML-enc oder XML-dsig) und auch die clientseitige Validierung der Daten (z. B. mit XmlValidatingReader für Microsoft .NET) können hier als Gegenmaßnahmen eingesetzt werden.

XMLHttpRequest in Verbindung mit JavaScript bildet die Basis für die meisten Ajax-Angriffe. Eine ausführliche Beschreibung der zwei häufigsten Ajax-Angriffe „JavaScript Hijacking“ und „XSS Prototype Hijacking“ befindet sich in [War08]. Solche Angriffe lassen sich durch eine sogenannte Whitelisting-Validierung vermeiden, die lediglich die vom Entwickler freigegebenen Eingabemöglichkeiten zulässt. Zusätzliche Sicherheit kann durch die Verwendung vom sogenannten Escaping[35] erreicht werden.

Bei den Angriffen, die nicht primär auf die Verletzung der Datenvertraulichkeit abzielen, besteht auf den ersten Blick eine nur geringe Gefahr für die Patientendaten. Es sind jedoch auch Szenarien denkbar, in denen der Angreifer versuchen könnte, die Fehlfunktion der Serverseite auszunutzen, um beispielsweise eine große Menge von Patientendaten zu manipulieren. Besonders im Behandlungszusammenhang können die Auswirkungen eines solchen Angriffs schwerwiegend sein, da sie die Behandlung von Patienten negativ beeinträchtigt können. So kann die Nichtverfügbarkeit von behandlungsrelevanten Patientendaten oder gar Manipulation der Patientenakte zu einer falschen Behandlung des Patienten führen (s. a. Abschnitt 4.3 „Qualitative Bewertung der Bedrohungs- und Risikosituation“).

[35] Ersetzung der Sonderzeichen durch die entsprechenden HTML-Code-Kombinationen.

Für die Verwendung der Ajax-Technologie bleibt festzuhalten, dass der größte Teil der bei den Datenzusammenführung relevanten aktiven Angriffe durch den Einsatz von Verschlüsselungstechnologie während der Datenübertragung unterbunden werden kann (s. a. Abschnitt C.3.8 „Verschlüsselung und Signaturen“). Die Replay-Angriffe, in denen der Angreifer die abgefangenen (auch verschlüsselten) Datenpakete erneut verschickt, um beispielsweise den Client oder den Server zu einer Fehlfunktion zu bewegen, können mithilfe von Einmal-Tokens abgewehrt werden. Auch die physikalische Absicherung der Kommunikationswege kann die Vorbereitung und Durchführung von Abhörangriffen erschweren. Ein Teil der aktiven Angriffe, die insbesondere auf die (physikalische) Störung der Kommunikation abzielen, kann nur durch zusätzliche organisatorische und administrative Maßnahmen bewältigt werden (s. a. Abschnitte 3.3 „Organisatorische Aspekte von Sicherheitsrichtlinien“ und 3.4 „Administrative Aspekte von Sicherheitsrichtlinien“).

C.3.3.2. Nutzung der Java-Sicherheitsfunktionen für die Datenzusammenführung

Unabhängig von der Art der eingesetzten Java-Technologie, bringt die Java-Plattform diverse Sicherheitsfunktionen mit, die sich auf mehrere Ebenen verteilen. Die erste Sicherheitsschicht bildet die Sprache selbst mit dem Compiler und den vorhandenen Java-Klassen. Bei der Ausführung des kompilierten Codes überwacht die Laufzeitumgebung den Bytecode und verifiziert die Einhaltung der zentralen Sicherheitsregeln. Die nächste Ebene der Überprüfung bildet der die Zugriffsrechte für die Objekte vergebende Classloader. Anschließend überwacht der sogenannte Security-Manager das Verhalten vom ausgeführten Java-Code zur Laufzeit, um eventuell schadhafte Transaktionen zu erkennen.
Aufgrund ihres Designs wurde Java einer Vielzahl von programmiersprachenspezifischen Missbrauchsmöglichkeiten beraubt. So verzichtet man in Java auf die Zeigerarithmetik, ungeprüfte Typumwandlung, Pointer sowie manuelle Speicherallokation und -freigabe. Folgende Aspekte des Java-Designs sollen die höheren Sicherheitsansprüche erfüllen:

- Die der Sprache Java zugrunde liegende strikte Objektorientiertheit verhindert unerwünschte Zugriffe auf die Datenstrukturen.
- Die Benutzung finaler Klassen, Variablen und Methoden erlaubt eine Verifikation der Code-Stabilität und verhindert gleichzeitig eine unerwünschte Veränderung des bereits geprüften Codes.
- Eine strenge Typisierung und sichere statische sowie dynamische Typumwandlung sorgen für die Kompatibilität des Kompilierzeittypen mit dem Laufzeittypen.
- Der Ausschluss von direkten Zeigern und die stattdessen verwendeten Objektreferenzen sorgen dafür, dass die Zulässigkeit der Zugriffe vor der Ausführung geprüft wird.

- Der Zugriff auf die Methoden und Variablen kann lediglich über die Namen erfolgen, wodurch der Byte-Code auf seine Integrität einfacher überprüft werden kann (vgl. [KS09, S. 187 ff.], [Ste01]).

Für die in diesem Abschnitt untersuchte Zusammenführung, Anzeige und Eingabe von klinischen Daten eignet sich die aus modularen Komponenten bestehende für mehrschichtige Anwendungen konzipierte Architektur der Java-Plattform Enterprise Edition (J2EE). Die Server-Komponente der Forschungsanwendung kann dabei auf dem für Deployment, Komponentenmanagement und -kommunikation zuständigen Java EE Applikationsserver laufen. Außerdem unterstützt ein Applikationsserver das Transaktions-Management, die Verzeichnisdienste, die Kapselung der Ressourcenzugriffe auf die Laufzeitumgebung[36] sowie diverse weitere Sicherheitsfunktionen. Dem Applikationsserver ist ein für die Darstellung der Inhalte zuständiger Web-Container vorgeschaltet. Die Abbildung 32 veranschaulicht einen solchen Aufbau.
Um die administrative und die organisatorische Trennung von *IDAT* und *MDAT* zu demonstrieren, werden zwei getrennte Applikationsserver abgebildet, die von einem dritten Applikationsserver aufgrund der Daten-Zusammenführung kontaktiert werden. Durch diesen Aufbau unterhält der Client die Verbindung lediglich zum Webserver, was den bereits beschriebenen problemträchtigen parallelen Zugriff auf die *IDAT*- und *MDAT*-Server entbehrlich macht. Dies vereinfacht die Gewährleistung der erforderlichen Neutralität der Daten zusammenführenden Stelle. Der Nachteil des Aufbaus ist das Vorhandensein der Daten wenn auch nur für eine kurze Zeit sowohl auf dem Web- als auch auf dem Applikationsserver. Wenn die beiden Infrastrukturbestandteile physikalisch zusammengelegt werden, reduziert dies nur scheinbar die „Angriffsfläche", da die potenziellen Sicherheitslücken der Web- und Applikationsserver nun auf einer Maschine vorhanden sind. Außerdem verhindert die Zusammenlegung eine Filterung der zwischen den beiden Servern ausgetauschten Daten auf dem Transportweg. Die tatsächliche Funktionsaufteilung zwischen den beiden Applikationsservern und dem Web-Container wird dabei nicht festgelegt, dies resultiert aus einer z. T. redundanten Aufzählung der Java-Module.
Um die Risiken des Aufbaus zu reduzieren, ist eine sichere Konfiguration der Daten zusammenführenden Server empfehlenswert. Es muss sichergestellt werden, dass die Daten in den Server-Caches in kurzen Zeitabständen – im optimalen Fall sofort nach der Auslieferung des Datensatzes an den Client – geleert werden. Die Client-Server-Kommunikation sowie die Datenübertragung zwischen den organisatorisch getrennten Servern kann mithilfe von Verschlüsselung gesichert werden.

[36] Zum Beispiel Netzwerk, Speicher etc.

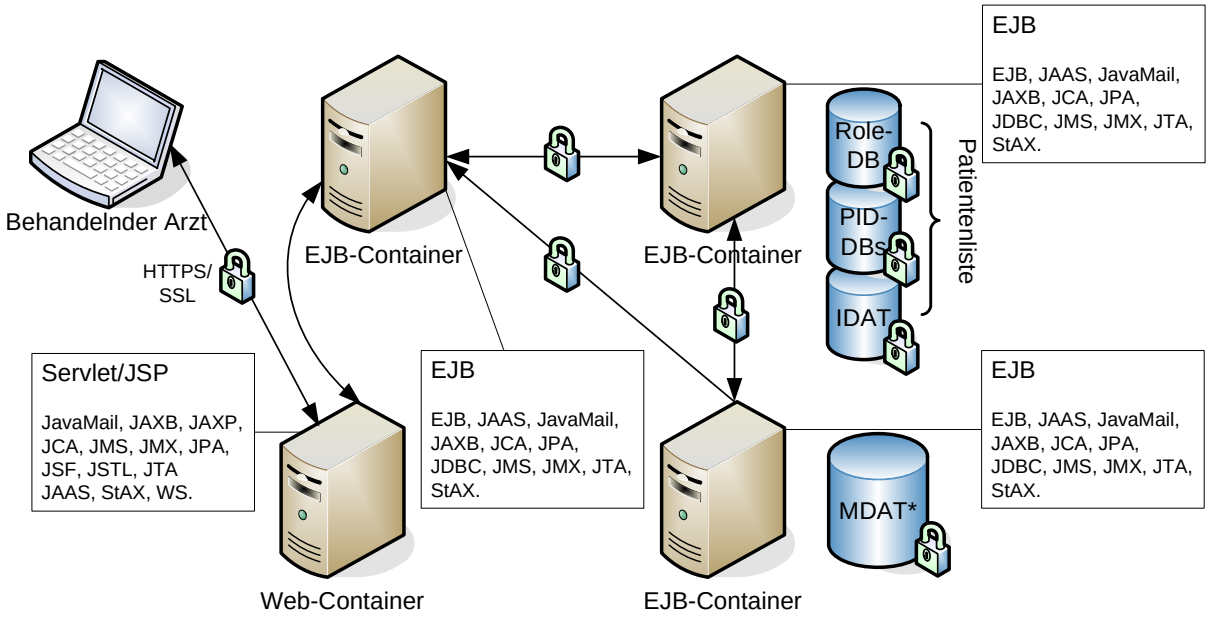

Abbildung 32.: Mögliche Realisierung einer Forschungsnetzanwendung mithilfe der Java-Technologie: Zwei getrennte Applikationsserver veranschaulichen die administrative und die organisatorische Trennung zwischen *IDAT* und *MDAT*. Der Client unterhält seine Verbindung lediglich zum Webserver, wodurch der sicherheitstechnisch problemträchtige parallele Zugriff auf die beiden Applikationsserver vermieden wird.

C.3.4. Aspekte des Einsatzes von Zwei-Wege-Authentifizierungskonzepten

C.3.4.1. PIN-Code + Passwort auf SmartCard/Token

Diese Option ist relativ einfach zu implementieren, da jedes Betriebssystem passwortbasierte Authentifizierung erlaubt und zentral verfügbare Informationen: Benutzername/Passwort benutzt. Der Benutzer muss sich nur den PIN-Code merken, der sein eigentliches Passwort freischaltet. Das auf der SmartCard gespeicherte Passwort (bzw. mehrere Passwörter) kann besonders lang und demzufolge gegenüber einem Brute-Force-Angriff nicht anfällig sein. Authentisierung mithilfe eines passwortgeschützten Tokens ist eine sogenannte Zweiwege-Authentisierung[37] und ist ein wirksames Schutzmittel gegen Lauschangriff und Angriffe durch das Erraten des Passworts. Sie ist auch ein gutes Mittel gegen die Verwendung von schwachen Passwörtern oder gegen die Passwortweitergabe. Eine Zweiwege-Authentifizierung schützt vor aufgeschriebenen und leicht zugänglichen[38] Passwörtern. Diese Methode eignet sich sowohl für die verstärkte Absicherung von Betriebssystemanmeldungen als auch für Web- bzw. Applikationszugänge, arbeitet allerdings ohne Public-Key-Infrastruktur (PKI), die für einige Dienste des Forschungsnetzes (z. B. sicheren E-Mail-Austausch) benötigt wird.
Die Sicherheit von derzeit existierenden SmartCards ist unterschiedlich gut. Sie hängt von

[37] Two Factor Authentication.

[38] Wie z. B. die unter der Tastatur klebenden Zettel mit Zugangsdaten.

solchen Faktoren ab wie verwendeter Algorithmus, Schlüssellänge, dessen Aufbewahrung und Erzeugung etc. Außerdem ist auch die physikalische Sicherheit des Mediums von Bedeutung, denn sollte es dem Angreifer gelingen, die SmartCard zu disassemblieren, spielen die o. g. Sicherheitsmechanismen kaum eine Rolle mehr.

C.3.4.2. Biometrisches Merkmal + Passwort/Zertifikat auf SmartCard

Aufgrund der unzuverlässigen biometrischen Erkennung bringt diese Variante wenig Vorteile und erfordert zusätzlichen Administrationsaufwand für die Installation der dafür notwendigen Infrastruktur (vgl. [KR07]). Die Praxis hat außerdem gezeigt, dass der Einsatz von biometrischen Authentisierungsmerkmalen zu einigen abstrusen Angriffstaktiken geführt hat. So schnitten z. B. Kriminelle in Malaysia einem Autobesitzer seinen Zeigerfinger ab, um sein mit biometrischer Authentisierung geschütztes Fahrzeug zu entführen (vgl. [Roe05]). Wegen der verbreiteten Einführung von biometrischen Systemen sind Kriminelle in Russland zu dem für die Fahrzeugbesitzer wesentlich gefährlicheren Autoraub übergegangen, wenngleich die Fälle des Autodiebstahls seltener geworden sind. Wegen der derzeit noch nicht ausgereiften Erkennungstechniken und der potenziellen Gefahr für den Authentifizierenden ist der Einsatz von biometrischer Erkennung innerhalb des Forschungsnetzes nicht empfehlenswert.

C.3.4.3. PIN-Code + Zertifikat auf SmartCard/Token

Ein Zertifikat wird von einer sogenannten Certificate Authority (CA) signiert und hat eine beschränkte Lebensdauer (z. B. ein Jahr). Der Einsatz von Zertifikaten ist die Basis für die Erhöhung der Sicherheit in mehreren Forschungsnetzbereichen. So können Zertifikate z. B. für die E-Mail-Signierung und Verschlüsselung eingesetzt werden. Sie können außerdem zur elektronischen Zutrittskontrolle verwendet werden. Dies ist insbesondere für die sicherheitsrelevanten Bereiche des Forschungsnetzes (Serverräume, Administrationskonsolen etc.) relevant (vgl. [sch03]).
Im Forschungsnetzbereich eignet sich eine zweistufige Hierarchie der Zertifizierungsstellen. Das Trustcenter für medizinische Forschungsverbünde könnte die Rolle der Root-Instanz übernehmen. Die Aufgabe dieser Instanz besteht in der Signierung von Zertifikaten untergeordneter CAs und ihrer vertrauenswürdigen Verknüpfung. Das Root-Zertifikat und Zertifikate untergeordneter CAs werden nicht zum Signieren von einzelnen Dokumenten verwendet. Die Identifizierung und Registrierung der Endanwender ist die Aufgabe von dezentralen Teilnehmerservices (Registration Authorities). Da die Root-CA keiner weiteren CA untergeordnet ist, wird ihr öffentlicher Schlüssel als Bestandteil des selbstsignierten Zertifikats veröffentlicht. Zusätzlich wird der öffentliche Root-Schlüssel auf sichere Weise allgemein zugänglich gemacht, damit sich jeder von der Authentizität und der Integrität des Root-Zertifikats überzeugen kann. Abbildung 33 veranschaulicht diese Option für den Aufbau der CA-Infrastruktur.
Die sicherheitsrelevanten Aspekte der PKI-Infrastruktur sind mit der unmittelbaren Rolle

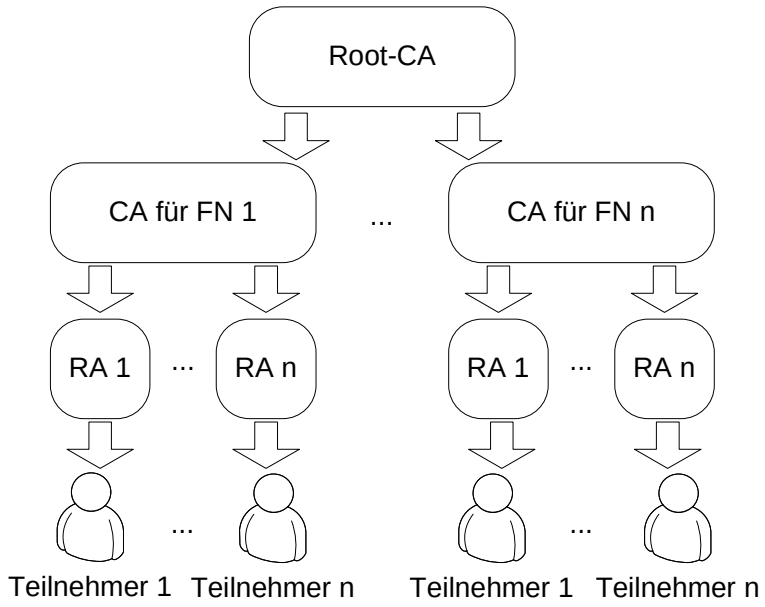

Abbildung 33.: Ein möglicher Aufbau der CA-Infrastruktur: Abgebildet ist eine zweistufige Hierarchie der Zertifizierungsstellen. Die Aufgabe der Root-Instanz besteht in der Signierung von Zertifikaten untergeordneter CAs und ihrer vertrauenswürdigen Verknüpfung.

des PKI-Bestandteils verbunden. Besonders strikte Sicherheitsvorkehrungen gelten für die CAs und sollen hier kurz erwähnt werden:[39]

- Zutritts- und Einbruchsmeldekontrolle für CA-Systeme.
- Aufteilung der Infrastruktur in physikalisch getrennte Bereiche (z. B. für Schlüsselgenerierung und -zertifizierung).
- Ausnahmslose Durchsetzung des Vier-Augen-Prinzips bei sämtlichen administrativen Operationen.
- Obligatorische Protokollierung der administrativen Operationen sowie eine regelmäßige Kontrolle der Aufzeichnungen sind von einem unabhängigen Auditor durchzuführen.
- Sicherheitsprüfung des administrativen Personals.
- Feststellung der Identität jedes Schlüsselinhabers vor der Zertifizierung zur Vermeidung des Zertifikatmissbrauchs.
- Einhaltung von empfohlenen Mindestschlüssellängen (vgl. [Woh11]).

Auch für die Zertifikate der Teilnehmer gelten strikt zu beachtende Sicherheitsvorschriften:

- Die Zertifikate sind auf einer gegen Hardwareangriffe resistenten SmartCard gespeichert und werden mit einem PIN-Code gesichert.
- Beim Verdacht auf Kompromittierung erfolgt eine unverzügliche Sperrung des Zertifikats. Ein Zertifikat soll außerdem dann gesperrt werden, wenn die Angaben im Zertifikat ungültig geworden sind.
- Sämtliche Teilnehmerzertifikate haben eine begrenzte Lebensdauer (i. d. R. – ein Jahr) und werden nach dem Ablauf dieser Zeit neu erstellt (vgl. [sch03]).

[39]Eine vollständige Auflistung sicherheitsrelevanter Maßnahmen für die CA-Betreiber kann [sch03] entnommen werden.

- Nur Zertifikate, die die Mindestanforderungen der CAs erfüllen (Schlüssellänge, Name des Inhabers etc.), können signiert werden.

Um die Gefahr eines Sniffing-Angriffs während der PIN-Eingabe zu minimieren, sollen nach Möglichkeit SmartCard-Terminals mit Tastatur verwendet werden. Beim Einsatz von Lesegeräten ohne Tastenfeld ist die PIN-Eingabe über die PC-Tastatur nicht empfehlenswert.

C.3.4.4. PIN-Code + One-Time-Passwort am Token

Diese Methode gehört derzeit zu den sichersten Authentifizierungsmöglichkeiten, da ein ausgespähtes Passwort nach einer kurzen Zeitspanne ungültig wird. Die Verwendung dieser Methode erfordert keine Anschaffung der Zusatzhardware für den Arbeitsplatz, ist jedoch mit hohen Investitionen in die Infrastruktur verbunden. Außerdem wird diese Authentifikationsmethode nicht von allen Anwendungen unterstützt, sodass evtl. ein Änderungsbedarf für die bereits bestehenden Systeme/Applikationen besteht. Eine große Gefahr ist außerdem die mangelnde Benutzerakzeptanz, da der Anwender zusätzlich zu dem bereits vorhandenen HPC ein weiteres Authentifikationsmerkmal erhält (Token), was für ihn mit zusätzlichen Kosten verbunden ist.

C.3.4.5. Sicherheitsrisiken beim Einsatz von SmartCards

Die Verwendung einer SmartCard löst nicht automatisch sämtliche Sicherheitsprobleme. SmartCards bringen auch diverse Risiken mit sich. Diese resultieren zum Teil aus einer hohen Anzahl der Parteien, die bei der Erstellung/Einführung von SmartCards beteiligt sind:

- *Karteninhaber:* Diese Rolle wird von den Nutzern und vom Administrationspersonal des Forschungsnetzes übernommen.
- *Dateneigentümer:* das Forschungsnetz als Rechtsperson[40] oder die Nutzer.
- *Terminalbesitzer:* Nutzer und Administrationspersonal.
- *Kartenaussteller:* z. B. SchlumbergerSema Competence Center Informatik (CCI) GmbH (vgl. [RDSP06]).
- *Karten- und Softwarehersteller.*

Es ist denkbar, dass alle in der Abbildung 34a dargestellten Rollen von unterschiedlichen Teilnehmern ausgeübt werden. Für ein Forschungsnetz reduziert sich die Anzahl relevanter Parteien i. D. R. auf drei, da unterschiedliche Rollen von den gleichen Parteien wahrgenommen werden (s. a. Abbildung 34b).

Die wahrscheinlichen SmartCard-Angriffe richten sich gegen das SmartCard-Terminal (Ein Angreifer versucht z. B. Terminals zu manipulieren, um einen Angriff gegen die SmartCard-

[40] Ausführliche Informationen zur Auswahl der passenden Rechtsform für ein Forschungsnetz sind in [SPR+06, S. 10 f.] zu finden.

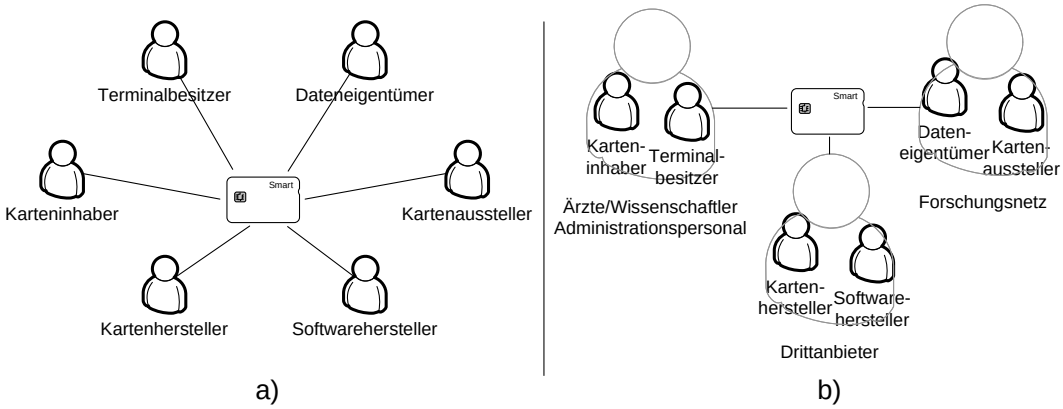

Abbildung 34.: SmartCard-Parteien: Durch die Annahme von mehreren Rollen durch die gleichen Teilnehmer reduziert sich die Anzahl der relevanten SmartCard-Parteien auf drei.

Daten mithilfe von Reverse Engineering, Fehleranalyse, Zeitanalyse etc. durchzuführen.). SmartCards müssen gegen solche Arten von Angriffen resistent sein.

Am häufigsten kombiniert man eine Chipkarte mit der Eingabe einer PIN-Nummer bzw. eines Passworts. Für diesen Zweck eignet sich der „elektronische Heilberufsausweis“ (HPC), der durch folgende Merkmale gekennzeichnet ist:

- Personalisierung[41] auf den Inhaber,
- optisch und elektronisch lesbare Ausweisung der Heilberufszugehörigkeit des Inhabers,
- richtlinienkonforme technische Ausgestaltung und
- Funktion für eine qualifizierte Signatur (vgl. [zen09]).

In Verbindung mit einem Passwort kann HPC für die Benutzerauthentifizierung verwendet werden. Manche Autoren führen eine weitere Unterscheidungen und benutzen häufig Begriffe *„What you know“* (Passwort), *„What you have“* (Chipkarte), *„What you are“* (Biometrie) und empfehlen eine Kombination mindestens zwei dieser Verfahren für die Authentifizierung. Einige Nachteile der biometrischen Authentifizierung wurden bereits vorgestellt. Hinzuziehung von Biometrie als drittes obligatorisches Authentifikationsmerkmal würde aus der heutigen Sicht keine nennenswerten Vorteile für die Sicherheit des Forschungsnetzes bedeuten. Die Benutzung der durch Passwörter geschützten Chipkarten erfüllt das Sicherheitsbedürfnis des Forschungsnetzes für die Benutzerauthentifizierung und bringt mehrere Vorteile mit sich:

- Sämtliche kryptografischen Operationen werden ausschließlich auf der Karte ausgeführt, sodass der kryptografische Schlüssel die Karte nie verlässt.
- SmartCards können mit folgenden Sicherheitsmerkmalen ausgestattet werden:
  - Speicherschutzfunktionen,
  - Detektion von Unter- und Überspannungen,
  - Zugriffskontrolle auf Objekte.

[41] Personalisierung beinhaltet die Eintragung von Daten, Zertifikaten und PIN auf dem Chip sowie eine optische Personalisierung (Aufdruck auf der HPC enthält Namen, Vornamen, Titel, Namenszusatz, Geburtsdatum, Organisation, Organisation Unit, E-Mail-Adresse, Rolle(n)).

- SmartCards können weitere Daten speichern und für andere, dem Forschungsnetz fremde Funktionen verwendet werden.

Empfehlung für den Einsatz: In den vorhergehenden Abschnitten wurden mehrere Authentifikationsverfahren vorgestellt, die alle ihre Vor- und Nachteile besitzen (z. B. Einfachheit der Implementierung vs. unzureichender Schutz der simplen passwortbasierten Authentifikation). Aufgrund der in diesem Abschnitt dargelegten Erkenntnisse erscheint der Einsatz von PIN-Code-geschützten Zertifikaten auf SmartCards im Forschungsnetzbereich empfehlenswert.

C.3.5. Beschreibung eines RBAC-Konzeptes mithilfe von SecureUML

In diesem Abschnitt werden die für ein medizinisches Forschungsnetz relevanten Anwendungsfälle zusammenfassend dargestellt. Anschließend werden die Potenziale der erweiterten RBAC-Definition „SecureUML“ nach Torsten Lodderstedt [Lod03] an einigen Anwendungsfällen erörtert (s. a. Abschnitt 3.5.4).
Die Planung eines Zugriffskonzeptes beginnt mit der Zusammenfassung von Anwendungsfällen und Akteuren, die von dem Berechtigungskonzept unterstützt werden sollen. Für diese stark verallgemeinerte Sicht eignen sich die UML-Anwendungsfalldiagramme. Abbildung 35 fasst die wichtigsten innerhalb eines Forschungsnetzes auftretenden Anwendungsfälle zusammen. Eine ausführliche Beschreibung der meisten dieser Anwendungsfälle in Form von Sequenzdiagrammen ist in [SSS06] zu finden. In dieser Arbeit werden die Sicherheitsaspekte von einigen besonders sicherheitsrelevanten Anwendungsfällen mithilfe der SecureUML-Syntax näher beschrieben. Zwecks Übersichtlichkeit wurden im abgebildeten Anwendungsfalldiagramm nicht alle Abhängigkeiten und Beziehungen eingezeichnet.

Beschreibung der Anwendungsfälle: Die Rolle „Monitor“, deren Hauptaufgabe in der Sicherstellung der Datenqualität besteht, nimmt im Forschungsnetz eine besondere Stellung ein. Die Berechtigungen der Rolle „Monitor“ sind in der Abbildung 36 dargestellt. Der Monitor erhält Zugriff auf die Dateneingaben und die Datenbanken mit Referenzdaten, um diese miteinander abgleichen zu können. Dateneingabe und -korrektur erfolgt ausschließlich durch Ärzte bzw. Dokumentationskräfte, die als „ausführende Organe“, d. h. mit gleichen Berechtigungen wie Ärzte agieren. Aus diesem Grund wird es in dem Diagramm auf die explizite Rolle „Dokumentationskraft“ verzichtet. Dafür schickt Monitor eine entsprechende Nachricht an die für die Eingaben zuständigen Personen, die ihre Eingaben korrigieren oder löschen können. Der Informationsaustausch mit dem Monitoring erfolgt ebenfalls über Nachrichtenversand.
Der Anwendungsfall „Benutzerdatenverwaltung“ ist in der Abbildung 37 dargestellt. Die Passwortänderung ist ein Bestandteil dieses Anwendungsfalls. Jeder Benutzer soll in

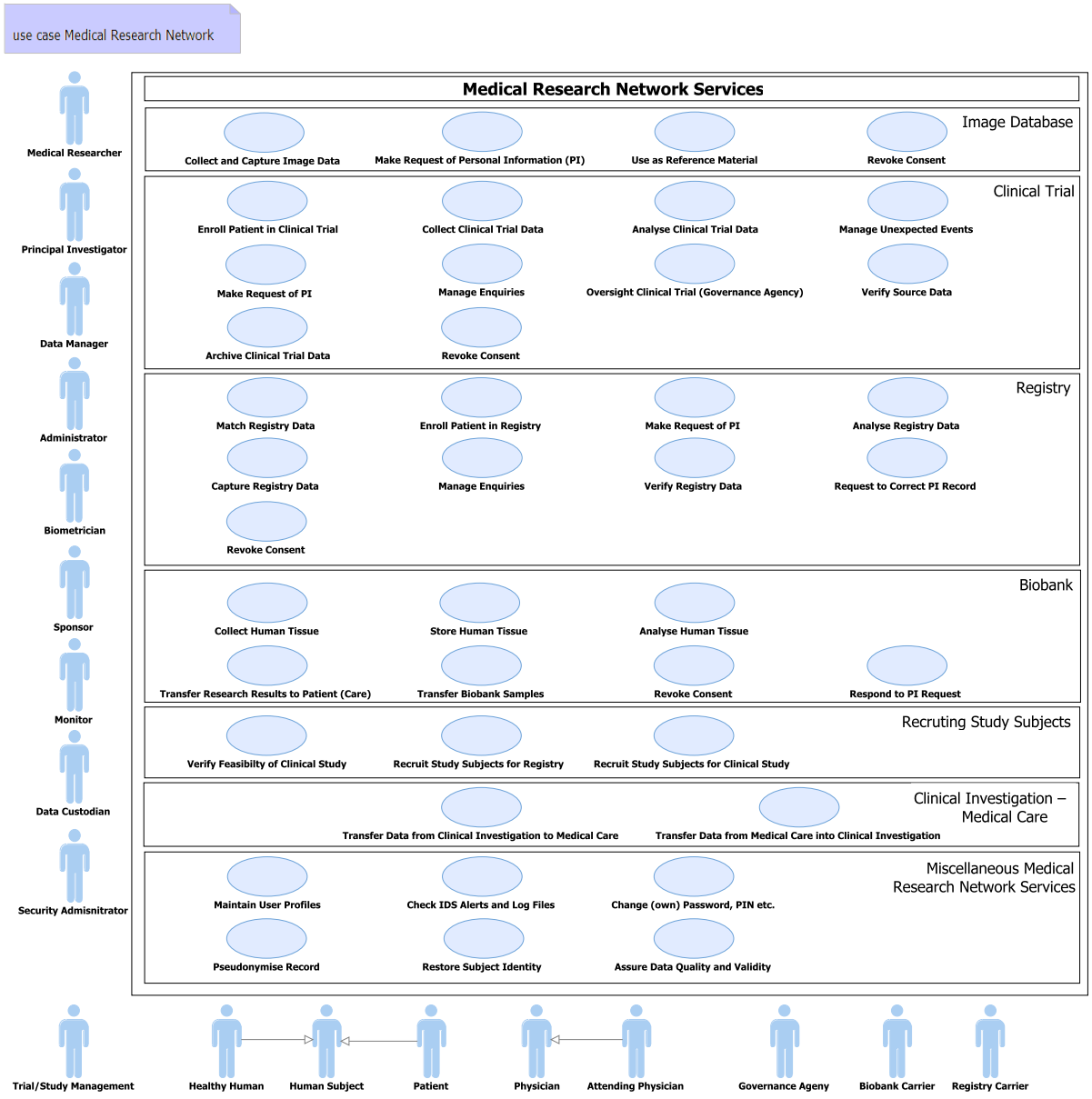

Abbildung 35.: Akteure und Anwendungsfälle als Ausgangsbasis für ein Berechtigungskonzept: Die Darstellung dieser stark verallgemeinerten Sicht erfolgt in Form eines UML-Anwendungsfalldiagramms. Aus Gründen der Übersichtlichkeit enthält das Diagramm nicht alle Abhängigkeiten und Beziehungen.

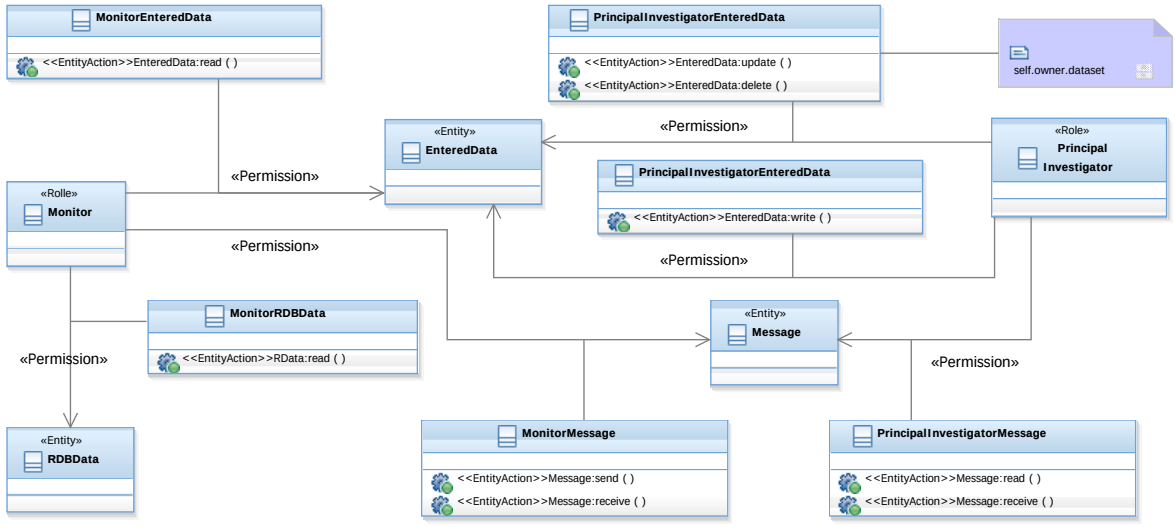

Abbildung 36.: Zugriffsberechtigungen für die Rolle „Monitor“: Die Hauptaufgabe der Rolle „Monitor“ bzw. „Data Monitoring Committee (DMC)“ besteht in der Sicherstellung der Datenqualität. Der Monitor erhält Zugriff auf die Dateneingaben und die Datenbanken mit Referenzdaten (RDB), um diese miteinander abgleichen zu können.

der Lage sein, sein Passwort bzw. seine PIN etc. zu ändern.[42] Administratoren können nicht nur eigene Passwörter, sondern auch die Passwörter anderer Benutzer sowie deren Daten ändern. Sie können außerdem neue Accounts einrichten, diese verändern oder aber auch löschen. Voraussetzung dafür ist die Erteilung eines entsprechenden Auftrags vom Security-Administrator. Bedingt durch die unterschiedlichen Tätigkeitsbereiche erbt die Rolle „Security-Administrator“ keine Berechtigungen von der Administrator-Rolle.

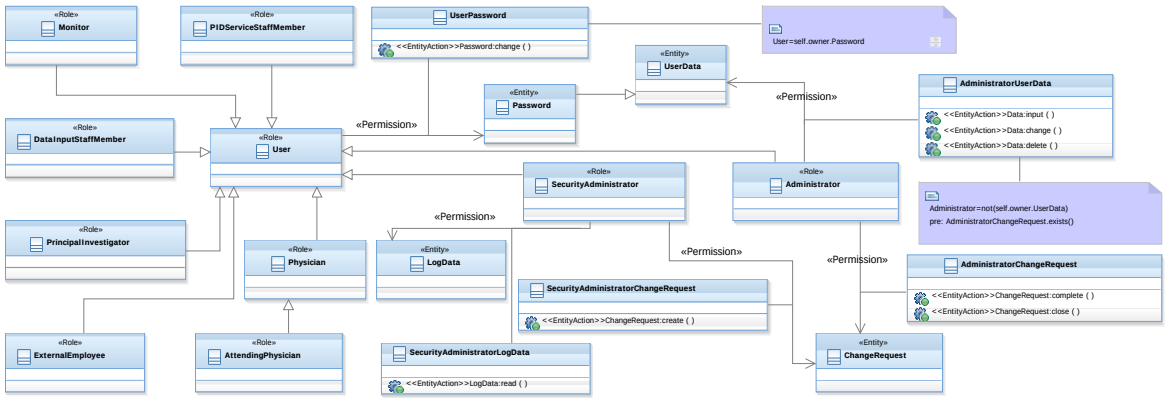

Abbildung 37.: RBAC-Modell der Benutzerdatenverwaltung: Bedingt durch die unterschiedlichen Tätigkeitsbereiche erbt die Rolle „Security-Administrator“ keine Berechtigungen von der Rolle „Administrator“. Zusätzlich zu der Verwaltung von Benutzerdaten übernimmt ein Security-Administrator die regelmäßige Kontrolle von sicherheitsrelevanten Logdaten.

Security-Administrator verwaltet die Identitäten/Rollen innerhalb des Forschungsnetzes und erteilt die Aufträge für die entsprechenden Anpassungen. Die Ausführung sei-

[42]Die jeweilige Ausprägung hängt von der gewählten Authentifikationsform ab. Diverse Formen der Benutzerauthentifikation wurden im Abschnitt 3.5.3 „Authentifizierung von Forschungsnetzteilnehmern“ behandelt.

ner Aufträge obliegt den Systemadministratoren. Ein Administrator ist dem Security-Administrator organisatorisch nicht untergeordnet. Dies beinhaltet eine zusätzliche Kontrolle nach dem „Vier-Augen-Prinzip“. Ergänzend zu der Verwaltung der Benutzerdaten übernimmt Security-Administrator regelmäßige Kontrolle der Logdaten. Dazu gehören z. B. die IDS-, Firewall-, Antivirensoftwaremeldungen etc. Für diese Daten benötigt Security-Administrator Leseberechtigung. In [RDSP06] wird vorgeschlagen, die rollenbasierten Zugriffsberechtigungen von Systembetreuern bzw. anderen Forschungsnetzmitarbeitern vergeben zu lassen. Aufgrund der in dieser Arbeit präferierten Aufgabenverteilung darf diese Tätigkeit nur vom Security-Administrator ausgeführt werden.

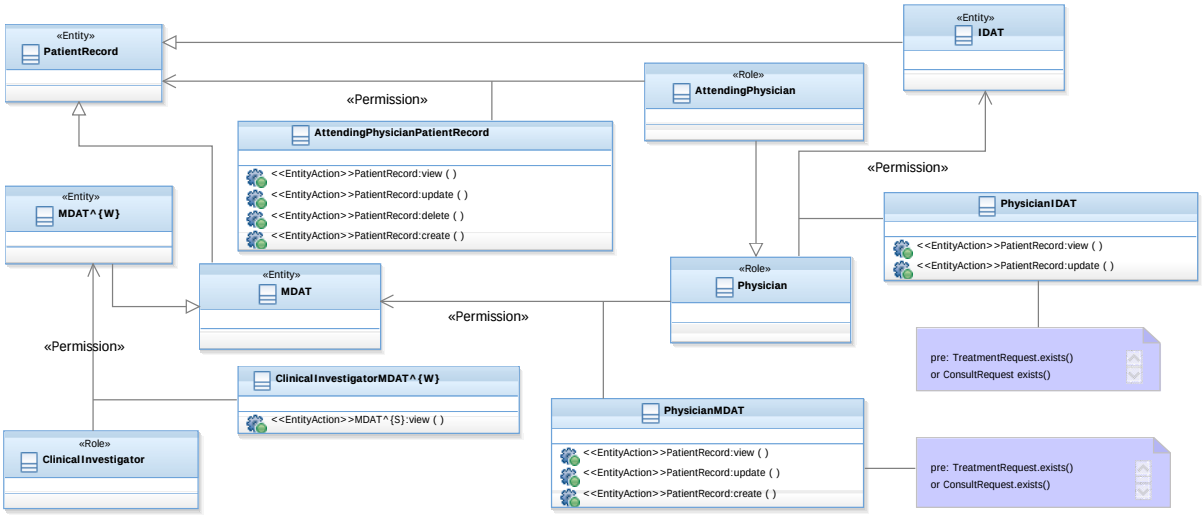

Abbildung 38.: RBAC-Modell des Zugriffs auf Patientendaten: Ein Wissenschaftler darf nur auf den wissenschaftlich relevanten Teil der Behandlungsdaten zugreifen. Die Rolle „Behandelnder Arzt“ besitzt erweiterte Zugriffsrechte für die Patientendaten und kann diese abrufen, aktualisieren, neu anlegen oder löschen.

Forscher sind Wissenschaftler, die anhand Proben und Daten medizinische Forschung betreiben. Sie können der Trägereinrichtung bzw. einer ihrer Teileinrichtungen angehören (interne Forschung) oder aus anderen Einrichtungen kommen (externe Forschung) (vgl. [BGH+06, S. 13]). Patientendaten können in einem Modell als Kombination aus medizinischen Daten (*MDAT*) und Identifikationsdaten (*IDAT*) dargestellt werden. Ein Wissenschaftler darf nur auf eine Untermenge der medizinischen Daten – auf den sogenannten wissenschaftlich relevanten Teil der Behandlungsdaten – zugreifen. Die Abfrageergebnisse eines Wissenschaftlers sind eine selektierte Teilmenge der medizinischen Daten ($MDAT^S$). Die Rolle „Behandelnder Arzt“ hat erweiterte Zugriffsberechtigungen auf Patientendaten: Sie können abgerufen, aktualisiert, neu angelegt oder gelöscht werden. Die Rolle „Arzt“ besitzt eingeschränkte Zugriffsrechte auf die Patientendaten. So darf z. B. ein mit der Behandlung beauftragter Arzt keine neuen *IDAT*-Datensätze im Behandlungszusammenhang anlegen. Er darf allerdings die Identifikationsdaten eines Patienten aktualisieren (z. B. bei Adressänderung, beim Namenswechsel durch Heirat etc.), die vorhandenen *MDAT*-Einträge abrufen, diese editieren oder neue erzeugen. In beiden Fällen ist die Erteilung eines Behandlungsauftrags notwendig. Die Zusammenhänge der beschriebenen Zugriffsberechtigungen sind in der Abbildung 38 dargestellt.

Die Aufgabe der Mitarbeiter des PID-Dienstes besteht in der Aktualisierung und Übermittlung von PID-Listen. Um eine Depseudonymisierung durchzuführen, bedarf es einer entsprechenden Autorisierung. Eine ausführliche Beschreibung der Zwecke und der Voraussetzungen für die Depseudonymisierung von Patienteneinträgen befindet sich in [RDSP06]. Die mithilfe von SecureUML beschriebenen Rollen-Berechtigungen des Pseudonymisierungsdienstes sind in der Abbildung 39 dargestellt.

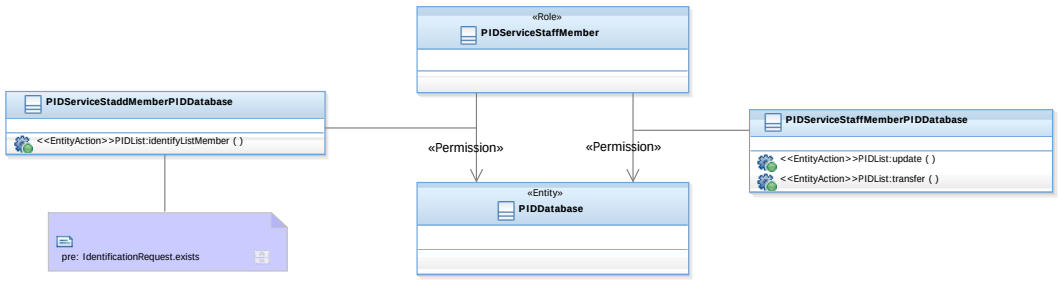

Abbildung 39.: RBAC-Modell des Pseudonymisierungsdienstes: Die Durchführung eines Depseudonymisierungsvorgangs bedarf einer entsprechenden Autorisierung.

Nicht zuletzt soll der Fall berücksichtigt werden, dass sich entweder der Benutzer oder das System, auf dem er arbeitet, nicht authentifizieren können. In solchen Fällen muss er Benutzerservice kontaktieren können, der ihm bei der Behebung des Problems zur Seite steht. Dies kann z. B. die Entsperrung seiner ID oder die Unterstützung beim Aufspielen von Sicherheits-Updates sein. In der Abbildung 40 wird deswegen zwischen den authentifizierten und nicht authentifizierten Benutzern unterschieden. Die authentifizierten Benutzer nehmen die ihnen zugewiesenen Rollen an und können die für diese Rollen vorgesehenen Dienste des Forschungsnetzes in Anspruch nehmen. Nicht authentifizierte Benutzer können dagegen Unterstützung des Benutzerservices anfordern. Selbstverständlich ist dieser Dienst auch für alle authentifizierten Forschungsnetzteilnehmer verfügbar.

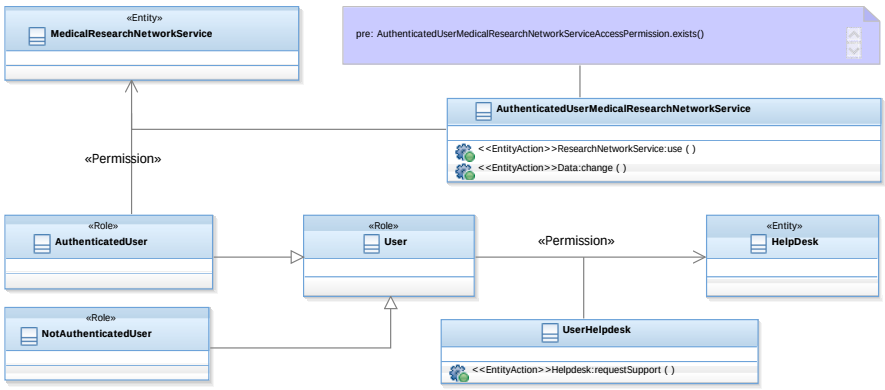

Abbildung 40.: Zugriff auf die Forschungsnetzdienste: Nach einer erfolgreichen Authentifikation können autorisierte Benutzer die für ihre Rollen vorgesehenen Dienste des Forschungsnetzes in Anspruch nehmen. Nicht authentifizierte Benutzer können Unterstützung des Benutzerservices anfordern.

Die in diesem Abschnitt vorgestellten RBAC-Modelle erheben keinen Anspruch auf Vollständigkeit. Die Darstellung diverser Nebenbedingungen für Zugriffe ist grafisch nur

ansatzweise möglich; ein ausgewachsenes Identitätsmanagementsystem ist notwendig, um die komplexen Berechtigungsstrukturen des Forschungsnetzes abzubilden. Zusätzlich zu der Rollendefinition müssen die Verhaltensregeln definiert werden, an die sich die Rolleninhaber zu halten haben. Diese Notwendigkeit resultiert aus der Tatsache, dass mehrere Rollen Berechtigungen für die Ausführung gleicher Aufgaben besitzen können. Ein typisches Beispiel ist z. B. die Rolle eines Administrators. Aufgrund seiner Tätigkeit hat das Administrationspersonal Zugriffsberechtigungen, die ihm Durchführung praktisch jeder Aufgabe innerhalb des Forschungsnetzes möglich machen. Selbstverständlich ist dies nicht immer erwünscht. So soll der *MDAT*-Datenbankadministrator keine Patienteneinträge verändern, obwohl seine Datenbankberechtigungen es nicht verhindern können. Zusätzlich zu der technischen Absicherung solcher Vorgänge sind organisatorische Maßnahmen notwendig.[43]
Bei der Erstellung des rollenbasierten Berechtigungskonzeptes gilt es, die Anzahl von verfügbaren Rollen überschaubar zu halten. Der Ansatz, jede erdenkliche Ausprägung einer Rolle als eine separate Rolle aufzufassen, ist zum Scheitern verurteilt. In den 90er Jahren versuchte man die sogenannten Rollenhierarchien zu definieren. Die Konstruktionen waren mehrstufig und schwer überschaubar. Ein komplexes, mit enormen Aufwand erstelltes Konzept, wird in kürzester Zeit obsolet; spätestens dann, wenn neue Rollen dazukommen oder bereits existierende Rollen nicht mehr benötigt werden. Eine erfolgreiche Diversifikation der Zugriffsrechte kann durch die Rollenparametrisierung[44] erreicht werden. Anzuwendende Policies sollen außerdem von der Umgebung des Endgerätes abhängen. So soll z. B. der administrative Zugriff auf die Datenbank über eine ungesicherte Leitung eines Internetcafés nicht zulässig sein. Die beiden Hauptziele solcher „umgebungssensitiven“ Policies sind der Schutz des Forschungsnetzes vor nicht richtlinienkonformen Systemen und gleichzeitig die Anpassung der Verteidigungsmechanismen an die Umgebungsbedingungen. So würde man beim Verdacht einer externen Kompromittierung des Forschungsnetzes an erster Stelle allen extern arbeitenden Teilnehmern den Zugriff zu dem Forschungsnetz verweigern, wobei die internen Teilnehmer (Administratoren) möglicherweise weiter arbeiten dürften, um den Sicherheitsvorfall zu untersuchen bzw. die Störung zu beheben.
Doch bereits eine kleinere Anzahl von Rollen und deren Ausprägungen kann zu schwer überschaubaren Konstrukten führen. Folgendes einfaches Beispiel veranschaulicht dies: Ein Teilnehmer des Forschungsnetzes (Rolle A) soll Daten in das Forschungsnetz eingeben, allerdings keine Daten aus dem Forschungsnetz auslesen können. Ein anderer Netzteilnehmer (Rolle B) darf die Daten lesen, allerdings nicht ändern und keine neuen Daten

[43] Ausführliche Informationen zu den organisatorischen und administrativen Maßnahmen befinden sich in den Abschnitten 3.3 „Organisatorische Aspekte von Sicherheitsrichtlinien“ und 3.4 „Administrative Aspekte von Sicherheitsrichtlinien“.

[44] Zum Beispiel Rolle „Arzt“, verfügbare Parameter: Lokation (1 - 15), Anschlusstyp (sicher, unsicher, unbekannt), Systemintegrität (vorhanden, nicht vorhanden, unbekannt), Behandlungszusammenhang zum Patient (gegeben, nicht gegeben) etc.

eingeben.[45] Das beschriebene Sicherheitskonstrukt wird ausgehebelt, wenn ein Teilnehmer mehrere Rollen (Rolle A und Rolle B) zugewiesen bekommt, denn er könnte dann beliebige Daten auslesen, analysieren und diese mit der für ihn günstigen Version überschreiben. Wenn man die Rollen nun durch die (evtl. nur zeitweise gültigen) Rollenausprägungen ersetzt, erhält man ein Konzept, das nur schwer zu überschauen ist.
Im Sicherheitskonzept des TMI-Servers wird explizit verlangt, dass die Rollen nicht kumuliert werden dürfen (vgl. [HWE05]). Das bedeutet, dass ein Anwender zu einem Zeitpunkt lediglich die Rechte einer einzigen Rolle ausüben kann, was die Möglichkeiten der Unterwanderung des Rollenkonzeptes reduziert. Im obigen Beispiel wäre das Sicherheitsmodell trotz dieser Einschränkung ausgehebelt, da der Netzteilnehmer den Rollenwechsel mehrmals hintereinander ausführen könnte. Ein Beispiel für die Belegung mehrerer Rollen ist die mögliche Doppelrolle „Arzt/Forscher“. Es ist wahrscheinlich, dass ein Forscher, der gleichzeitig Arzt ist, bestimmte Merkmalskombinationen im pseudonymisierten Datensatz wieder erkennt, was zu einer unbefugten Reidentifizierung von Patienten führen kann. Die für einen Patienten von dieser ungewollten Reidentifizierung ausgehende Bedrohung ist jedoch wegen der Bindung an die Schweigepflicht des forschenden Arztes als gering einzustufen (vgl. [BGH+06, S. 143]).

C.3.6. Aspekte der Verwendung von Verzeichnisdiensten in medizinischen Forschungsnetzen

C.3.6.1. Benutzerregistrierung bei einer Zertifizierungsstelle

Die Benutzerregistrierung bei einer CA kann auf unterschiedlichen Wegen erfolgen. So ist z. B. sowohl die Registrierung über den Web-Browser als auch das persönliche Abholen der Zertifikate bei einer RA denkbar. Ein Forschungsnetzteilnehmer erhält seine SmartCard mit den darauf gespeicherten Zertifikaten nach der Antragstellung von der RA (Benutzerservice), nachdem er sich bei der Anmeldung mithilfe des Personalausweises identifiziert hat (vgl. [RDSP06]). Da das Zertifikat auf der SmartCard gespeichert wird, ist eine lokale Schlüsselerzeugung durch den Benutzer wenig sinnvoll.
Es wird empfohlen, die Gültigkeit von Teilnehmerzertifikaten auf ein Jahr zu beschränken (vgl. [RDSP06]); trotzdem kann es Fälle geben, in denen Zertifikate früher widerrufen werden müssen.[46] Der Widerruf erfolgt durch die Aufnahme der mit einem Zeitstempel versehenen widerrufenen Zertifikate in eine Struktur. Dies kann z. B. mithilfe von sogenannten Certificate Revocation Listen (CRL) bzw. Authority Revocation Listen (ARL) oder Online Certification Status Protocol (OCSP) respektive Server-based Certificate

[45] Ergänzt um die Sicherheitseinstufung entspricht dies dem Zugriffskontrollenkonzept nach Bell-LaPadula (vgl. [BL73]).

[46] Zum Beispiel aufgrund der Kompromittierung des privaten Schlüssels oder eines Ausstellungsfehlers von Seiten der CA.

Validation Protocol (SCVP) erfolgen. Bei der Definition der Gültigkeitszeiträume für Zertifikate soll man die Realität nicht aus den Augen verlieren. Die Erstellung und Verteilung von neuen Zertifikaten, Einsammlung und Entsorgung alter SmartCards und weitere mit dem Zertifikataustausch verbundene Maßnahmen, erzeugen einen nicht unerheblichen Aufwand. Auch hier muss eine Abwägung zwischen einer etwas höheren Sicherheit bei einer kürzeren Gültigkeitsdauer von Zertifikaten und einem wesentlich höheren Mehraufwand beim häufigen Teilnehmer-Zertifikataustausch erfolgen. Angesichts der aus heutiger Sicht hohen Sicherheit eingesetzter kryptografischer Verfahren und der physikalischen Sicherheit von SmartCards kann die Verlängerung der Gültigkeit von Zertifikaten für Teilnehmer mit eingeschränkten Zugriffsrechten und „unkritische Systeme“ auf drei Jahre einen sinnvollen Kompromiss darstellen. Auf keinen Fall sollte man jedoch solche Entscheidung pauschal auf alle Systeme und Anwender des Forschungsnetzes aus Bequemlichkeit und auf Kosten der Sicherheit ausweiten.

C.3.6.2. Widerruf von Zertifikaten

Der Widerruf von Zertifikaten kann mithilfe von Zertifikatssperrlisten[47] erfolgen. Die CRLs erhalten die Signatur der CA, um Manipulationsversuche vorzubeugen. Nachteilig ist, dass sie keine Auskunft darüber geben, ob ein Zertifikat tatsächlich gültig ist, denn CRLs sind sogenannte Negativlisten. Des Öfteren werden die Sperrlisten verteilt abgelegt,[48] was bei Replikationsverzögerungen dazu führt, dass die CRLs lediglich die Vergangenheit abbilden und keine Aussage darüber erlauben, ob ein Zertifikat zum Zeitpunkt der Abfrage tatsächlich gültig ist. Die Verwendung von sogenannten Delta-CRLs kann die Dauer der Replikation deutlich verkürzen; besonders dann, wenn ein Zertifikat dringend widerrufen werden muss, bleibt die Replikationsdauer trotzdem nicht akzeptabel. Aus diesem Grund sollten die Forschungsnetze nach Möglichkeit das Online Certificate Status Protocol (OCSP) bzw. das Server-based Certificate Validation Protocol (SCVP) zur Gültigskeitsüberprüfung von Zertifikaten einsetzen.

OCSP/SCVP sind Protokolle, die die Statusabfrage von X.509-Zertifikaten zum Zeitpunkt einer Transaktion ermöglichen. Zum Beispiel benötigen beim OCSP die abfragenden Systeme einen HTTP- oder HTTPS-Zugriff auf den sogenannten OCSP-Responder, denn die beiden Protokolle dienen dem OCSP als Transportprotokolle. Der Client schickt eine Zertifikatgültigkeits-Anfrage an den OCSP-Responder, der ihm mit der Information über den aktuellen Status des Zertifikats antwortet. OCSP wird im RFC 2560 spezifiziert (vgl. [MAM+99]).

Besonders bei einer temporären Sperrung von Zertifikaten ist die Verwendung von OCSP vorteilhaft. Ein Zertifikat kann z. B. suspendiert werden, um dem aufwendigen Widerruf

[47] CRL: Certificate Revocation List, ARL: Authority Revocation List.

[48] Zum Beispiel aus Performancegründen oder wenn bestimmte Systeme nicht auf zentrale CRL zugreifen können bzw. dürfen.

und einer anschließenden Neuerzeugung des Zertifikats aus dem Weg zu gehen. So könnte z. B. das Zertifikat eines Administrators für die Dauer seines Urlaubs gesperrt und anschließend wieder entsperrt werden. Für den o. g. Zweck wäre allerdings die Verwendung von SCVP besser geeignet, das dieses Protokoll im Unterschied zum OCSP die Zertifikatstatusinformationen aus der Vergangenheit liefern kann. Eine CRL-basierte temporäre Sperrung wäre wenig sinnvoll, denn Systeme könnten auf die nicht aktualisierten CRLs zugreifen und würden dem aus dem Urlaub zurückgekehrten Administrator keine Autorisierung bis zum Abschluss des Replikationsprozesses erteilen.
Die bloße Gültigkeit eines Zertifikats bedeutet allerdings nicht automatisch, dass ein Teilnehmer oder eine Komponente dem Zertifikat auch vertrauen muss. Es ist denkbar, dass ein Benutzer einer Reihe von CAs nicht vertraut. Während ein einzelner Privatbenutzer die Vertrauenswürdigkeit noch selbst beurteilen kann, darf diese Entscheidung nicht den Teilnehmern bzw. den Komponenten des Forschungsnetzes überlassen werden. Dies erfolgt meistens durch die Verteilung der sogenannten Vertrauenslisten, in denen die vertrauenswürdigen CAs bzw. Zertifikate gespeichert sind. Doch besonders bei gegenseitigen Vertrauensstellungen zwischen mehreren Domänen sind die auf den Clients gespeicherten Listen vertrauenswürdiger Zertifikate nachteilig, da sie die Änderungen der Vertrauensstrukturen nur unzuverlässig abbilden. Vorteilhaft dagegen ist die Erzeugung von internen dynamischen Vertrauenslisten. Diese Listen verwalten die sogenannten Vertrauensbasen: CA-Zertifikate, denen ein Teilnehmer vertrauen soll bzw. darf. Die Vertrauensbasen könnten für die Forschungsnetzteilnehmer von den CAs bzw. RAs zentral verfügbar gemacht werden, da die Teilnehmer- und Komponentenzertifikate von ihnen ausgestellt werden und sie somit für den Teilnehmer automatisch als vertrauenswürdig gelten.

C.3.6.3. Verwendung von Zertifikaten für die Authentifizierung und die Autorisierung

In den Abschnitten 3.5.3 „Authentifizierung von Forschungsnetzteilnehmern“ und 3.5.4 „Rollenbasierte Rechtevergabe (RBAC)“ wurden einige Empfehlungen zur Benutzerauthentifizierung und -autorisierung unterbreitet. In diesem Zusammenhang ist die Verwendung von Zertifikaten ebenfalls von Bedeutung. Das Namensschema des X.500 kann den vollqualifizierten Namen des Zertifikats-Inhabers und auch des Zertifikats-Ausstellers speichern. Aus diesem Grunde können Sie für Authentifizierungszwecke eingesetzt werden. So könnte z. B. das Namensschema einer Forschungsnetz-Zertifizierungsstelle wie folgt aussehen:

```
(Country=DE, Organisation=FN1, OrganizationalUnit=Systems, Location=Berlin)
```

Ein in der Personalabteilung des Forschungsnetzes tätiger Mitarbeiter könnte folgendes Namensschema besitzen:

```
(Country=DE, Organisation=FN1, OrganizationalUnit=HR, Location=Hannover)
```

Der Vergleich beider Schemata lässt Schlüsse über die Zugriffsrechte des Zertifikatsinhabers zu. So wird der Zertifikatsinhaber wahrscheinlich Zugriff auf die Personalliste der in Hannover tätigen Forschungsnetzmitarbeiter haben, jedoch die in Berlin stehenden Server nicht administrieren können. Mithilfe dieser Technik könnte man ein Autorisierungssystem aufbauen, in dem die Zugriffsautorisierung auf Basis der Teilnehmer-Funktion (dargestellt durch Namensschema) und des Systemstandortes erfolgt. Problematisch wird ein solcher Aufbau, wenn ein Benutzer Zugriff auf Systeme mehrerer Standorte benötigt: Entweder müssen für seine Zugriffe mehrere Zertifikate erzeugt werden oder man nimmt eine komplizierte Struktur von CAs mit sich überlappenden Berechtigungen in Kauf. Alternativ können auch andere Zertifikatsfelder (z. B. Policy-Feld) eingesetzt werden, um die Zugriffsberechtigungen eines Benutzers abzubilden. Bei der im Abschnitt 3.5.3 „Authentifizierung von Forschungsnetzteilnehmern“ empfohlenen SmartCard-basierten Authentifizierung wäre die Freischaltung einer zusätzlichen Anwendung für den Benutzer mit der Erstellung eines neuen Zertifikats und folglich mit der Verteilung einer neuen SmartCard verbunden, was aufgrund der hohen Kosten und des Administrationsaufwandes kaum tragbar wäre (vgl. [NDJ01]).
Eine Lösungsmöglichkeit könnte z. B. in der Trennung zwischen den authentifizierenden und den autorisierenden Infrastrukturbestandteilen bestehen. PKI würde dabei die Verifikation der Teilnehmeridentität sicherstellen; ein Rechte-Server würde seinerseits die Autorisierung von Transaktionen übernehmen. Dieser Ansatz wird im Abschnitt 3.5.7 „Ticketing, Single Sign-On (SSO)“ erläutert (s. a. Abschnitt 3.5.4 „Rollenbasierte Rechtevergabe (RBAC)“).

C.3.6.4. Zertifikatshierarchien und Kreuzzertifizierung

Eine einzelne Zertifizierungsinstanz kann zu einem Zertifizierungs-Bottleneck mutieren, wenn PKI-Infrastrukturen mehrerer Forschungsnetze zusammengeführt werden, oder man einen gemeinsamen Dienstleister für die CA-Services einsetzt. In solchen Szenarien baut man eine Zertifikatshierarchie auf, indem die Root-CA ihre Befugnisse auf die untergeordneten Instanzen überträgt, die wiederum weitere untergeordnete Instanzen erzeugen können.
Ist die Zusammenführung von PKI-Infrastrukturen mehrerer Forschungsnetze nicht möglich, kann die sogenannte Kreuzzertifizierung für die Interaktion von PKI-Strukturen mehrerer Netze verwendet werden. Ein Vertrauenspfad, der die gegenseitige Vertrauensbeziehung herstellt, erfordert die Erzeugung von zwei Zertifikaten, die die beidseitigen Vertrauensbeziehungen zwischen den CAs abbilden. Ein solcher Aufbau gibt den teilnehmenden Forschungsnetzen sogar zusätzliche Sicherheit, denn bei der Kompromittierung des Schlüssels einer CA in einem streng hierarchischen Modell kann keinem Schlüssel innerhalb der PKI mehr vertraut werden. Im Falle der Kreuzzertifizierung ist lediglich die Vertrauensstellung zu der betroffenen CA gestört; der Rest der Forschungsnetz-PKI bleibt weiterhin vertrauenswürdig.

C.3.6.5. PKI-Vertrauensmodelle

Mehrere Einheiten, deren Zertifikate von der gleichen CA stammen, können zu sogenannten Vertrauensdomänen zusammengefasst werden. Wenn keine direkte Vertrauensstellung zwischen zwei Vertrauensdomänen (bzw. den Mitgliedern zweier Vertrauensdomänen) besteht, und man zur Herstellung dieser Vertrauensstellung auf eine vertrauenswürdige Drittpartei (CA) zurückgreifen muss, spricht man von einer *transitiven Vertrauensstellung*. Die Vertrauensstellung wird ihrerseits durch den sogenannten Vertrauenspfad abgebildet. Ein Vertrauensmodell beschreibt das für das Aufspüren und Durchsuchen der Vertrauenspfade maßgebliche Regelwerk.
Bei einem streng hierarchischen Aufbau stellt die sogenannte Blatt-CA (RA) Zertifikate für die Forschungsnetzteilnehmer, -server, -anwendungen und -module aus. Eine übergeordnete CA stellt Zertifikate für die RA oder eine andere, ihr untergeordnete, CA aus. Um die Vertrauensstellung zwischen zwei Komponenten in einem hierarchischen Modell zu überprüfen, muss eine für die beiden gemeinsame CA gefunden werden, zu der die beiden eine Vertrauensstellung besitzen. Dies führt nicht nur zu einem langen Vertrauenspfad und somit zu einer hohen Belastung übergeordneter CAs,[49] sondern setzt auch die Root-Instanz einem hohen Sicherheitsrisiko aus. Ein solches Vertrauensmodell basiert auf bidirektionalen Vertrauenspfaden und ist in der Praxis kaum vertreten. Viel öfter trifft man auf das Modell der sogenannten *untergeordneten Hierarchie*. In dem Modell der untergeordneten Hierarchie wird die Root-CA als gemeinsame Vertrauensbasis definiert, von der alle Vertrauensstellungen stammen. Dadurch gehen die kurzen Vertrauenspfade nur bis zum Zertifikat der Wurzelinstanz,[50] das für alle Teilnehmer in einem Verzeichnis bekannt gegeben wird. Die Wurzelinstanz wird also nur zur Zertifizierung von untergeordneten Instanzen eingesetzt, was im Normalbetrieb selten vorkommt. Die Vorteile dieses Modells sind die geringen administrativen Aufwände und eine gute Skalierbarkeit.
Die Verteilung von CA-Zertifikaten gestaltet sich aufgrund einer gemeinsamen Vertrauensbasis ebenfalls als leicht. Die Vertrauenspfade sind in einem solchen Modell fest und können gemeinsam mit dem Zertifikat übertragen werden. Ein hierarchisches Vertrauensmodell kann innerhalb einer autarken Forschungsnetzstruktur mit einem strengen hierarchischen Aufbau erfolgreich sein. Die Kooperation mit anderen Forschungsnetzen, Mitbenutzung von Diensten, Systemen etc. werden bei diesem Modell nur dann zuverlässig funktionieren, wenn die miteinander interagierenden Forschungsnetze sich auf eine gemeinsame Wurzel-CA einigen. Die unterschiedlichen Richtlinien der Forschungsnetze erschweren das Zusammenbringen bereits bestehender Infrastrukturen zusätzlich.
Das *Peer-to-Peer-Vertrauensmodell* basiert auf der bereits beschriebenen Kreuzzertifizierung und funktioniert nach dem Gleichstellungsprinzip für die in einer Vertrauensdomäne

[49] Bei drei Hierarchiestufen beträgt die maximale Pfadlänge fünf, bei vier Stufen – sieben Schritte.

[50] Und nicht bis zur Blatt-CA wie bei der allgemeinen Hierarchie.

teilnehmenden CAs. Beschränkt man sich aufgrund der höheren Verlässlichkeit nur auf die direkten Vertrauenspfade, muss jede CA alle anderen CAs der gleichen Vertrauensdomäne zertifizieren. Bei einer Anzahl n von CA ergeben sich dadurch $n * (n - 1)$ notwendige Zertifizierungsvorgänge,[51] was in einer schlechten Skalierbarkeit der Lösung resultiert.
Die Verwendung des Peer-to-Peer-Vertrauensmodells unter Berücksichtigung nur direkter Vertrauenspfade ist aufgrund des Verwaltungsoverheads nicht praktikabel. Als praxistauglich könnten sich dagegen die *Maschenmodelle* erweisen, bei denen der Zertifizierungspfad mehrere CAs durchlaufen kann. Durch die gezielte Verwendung von unidirektionalen oder bidirektionalen Zertifizierungen lassen sich mit dem Maschenmodell die untergeordnete bzw. die allgemeine hierarchische Struktur nachbilden. Die über mehrere Forschungsnetze einer Vertrauensdomäne hinaus gehenden Vertrauenspfade können bei unterschiedlichen Sicherheitsstandards problematisch werden. So könnte z. B. ein Forschungsnetz seinen Teilnehmern einen webbasierten Zugriff auf bestimmte Dienste erlauben, wobei das andere Forschungsnetz für die Nutzung dieser Dienste eine spezielle abgesicherte Umgebung voraussetzt. Trotz der unterschiedlichen Sicherheitsstandards der beiden Forschungsnetze hätten alle Teilnehmen die gleiche Vertrauensstellung aufgrund des Zertifizierungspfades. Abgesehen von diversen, mit der Handhabung von langen Zertifizierungspfaden verbundenen Problemen[52], bergen lange Zertifizierungspfade eine weitere Gefahr in sich: Wenn die Erzeugung zusätzlicher Zertifizierungen im Ermessen einzelner Forschungsnetze liegt, kann es zu unerwarteten Vertrauensstellungen kommen. Durch unachtsame Zertifizierung könnten forschungsnetzfremde Einrichtungen der Vertrauensdomäne beitreten. Zur Vorbeugung solcher Fälle dient die Einrichtung einer Policy Authority (Richtlinienstelle) für die Forschungsnetzgemeinschaft, die den Aufbau von Vertrauensstellungen steuert bzw. die Vertrauensdomänen-Mitgliedschaft einschränkt.
Im Zusammenhang mit Zertifizierungspfaden kommen die Verzeichnisdienste wieder ins Spiel, denn zur Ermittlung eines Zertifizierungspfades bedarf es sogenannter Cross-Certificate-Pair-Attribute. Der am besten geeignete Ort zur Speicherung solcher Attribute ist ein Verzeichnis. Da diese Verzeichnisse in unterschiedlichen Vertrauensdomänen liegen, ist der Zugriff auf die Verzeichnisinformationen für die Mitglieder anderer Vertrauensdomänen problematisch. Aus diesem Grund müssen in jeder Vertrauensdomäne (in jedem Forschungsnetz bzw. Forschungsnetzbereich) öffentlich verfügbare Verzeichnisse mit Informationen über die gegenseitigen Zertifikate verfügbar gemacht werden.

C.3.6.6. Gemeinsame Benutzung von Diensten von mehreren Forschungsnetzen

Das Ziel eines jeden Forschungsnetzes besteht in der Sammlung möglichst vieler forschungsrelevanter Daten. In dieser Arbeit wird die Auffassung vertreten, dass durch die

[51] Es liegt eine vollvermaschte Struktur vor.

[52] Bestimmung des kürzesten vertrauenswürdigsten Pfades, Optimierung der Zugriffe durch zusätzliche Zertifizierungspfade etc.

Synergieeffekte die Erreichung eines höheren Sicherheitsniveaus leichter erzielt werden kann (s. a. Abschnitt 3.4 „Administrative Aspekte von Sicherheitsrichtlinien“). Mehrere Faktoren müssen bei der Kooperation von Forschungsnetzen mit unterschiedlich aufgebauten Zertifikatsinfrastrukturen[53] berücksichtigt werden.
Bei gegenseitiger Verwendung von Diensten zwischen mehreren Forschungsnetzen, deren Zertifikatinfrastrukturen nach dem Modell der untergeordneten Hierarchie aufgebaut sind, sind mehrere Vorgehensweisen denkbar. Die wohl geläufigste Lösung ist die *gegenseitige Zertifizierung der Root-CAs*, wodurch der sogenannte innere Ring bzw. Hub gebildet wird. Der Nachteil dieses Aufbaus für die Forschungsnetze ist dessen bereits angesprochene schlechte Skalierbarkeit des vermaschten Modells. Um den Performanceproblemen aus dem Weg zu gehen, kann man entweder auf die Zwischenspeicherung viel genutzter Pfade zurückgreifen oder aber Abkürzungen innerhalb der Vertrauenspfade durch die gegenseitige *Zertifizierung innerhalb einer Hierarchie* erzeugen. Dies erfordert die Angabe einer Vertrauensbasis für die direkte Verbindung zwischen den Blatt-CAs (bzw. den untergeordneten CAs), da solche Verbindungen die gemeinsame Vertrauensbasis ignorieren. Die direkten Links bringen aber zusätzliche Komplexität mit sich und können zu den bereits erwähnten unerwünschten Vertrauensstellungen führen. Manche Autoren vertreten die Auffassung, dass *direkte Links* zur Lösung von den durch die Umstrukturierungen gewachsenen Problemen eines Vertrauensmodells unumgänglich sind, wenn man die Infrastruktur nicht komplett neu aufbauen will. Alternativ könnten mehrere Forschungsnetze die sogenannte *Bridge-CA* einrichten. Bridge-CA stellt gegenseitige Zertifikate für die Root-CAs der teilnehmenden Forschungsnetze aus und besteht i. d. R. aus einer zentralen Richtlinienstelle, einer (Bridge-)CA und einem (Bridge-)Verzeichnisdienst.

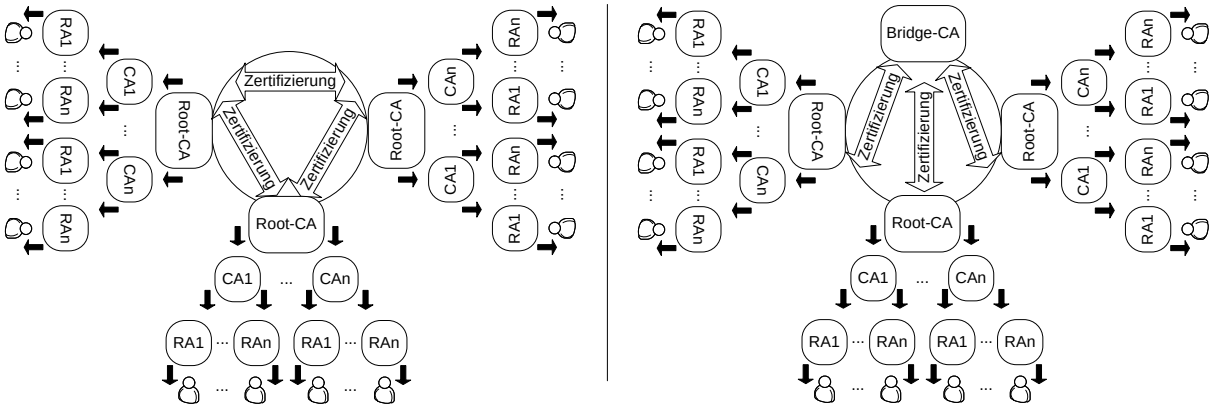

Abbildung 41.: Verknüpfte Hierarchie und Bridge-CA im Vergleich: Der schlechten Skalierbarkeit einer gegenseitigen Zertifizierung der Root-CAs kann mithilfe von sogenannten direkten Links begegnet werden. Eine Bridge-CA stellt gegenseitige Zertifikate für die Root-CAs der teilnehmenden Forschungsnetze aus und besteht i. d. R. aus einer zentralen Richtlinienstelle, einer (Bridge-)CA und einem (Bridge-)Verzeichnisdienst.

Die zentrale Richtlinienstelle wäre für die Zertifizierungsrichtlinien-Auswertung der teilnehmenden Forschungsnetze zuständig. Die Bridge-CA würde der gegenseitigen Zertifizierung

[53]Hier sind unterschiedliche Vertrauensmodelle gemeint.

der Root-CAs teilnehmender Forschungsnetze dienen.[54] Im gemeinsamen Verzeichnis erfolgt schließlich die Speicherung der Zertifizierungsinformationen. Die Verknüpfung von Vertrauensdomänen mithilfe gegenseitiger Zertifizierung und des Bridge-CA-Ansatzes ist in der Abbildung 41 dargestellt (vgl. [tel11], [NDJ01]).

C.3.7. Aspekte des Einsatzes von Single Sign-On in medizinischen Forschungsnetzen

C.3.7.1. Taxonomie von SSO-Systemen

In seinem Buch „IT-Sicherheit mit System“ unterscheidet Klaus-Rainer Müller zwischen folgenden Arten von Single Sign-On (vgl. [Mül11, S. 305 f.]):

- *Passwort-synchronisierende Systeme* übernehmen die Verwaltung von Benutzerpasswörtern und Kennungen. Der Benutzer meldet sich nur bei diesem System an; woraufhin das Passwort-synchronisierende SSO-System die Benutzeranmeldung bei allen weiteren Systemen übernimmt.
- *Ticket-basierte Systeme* vergeben befristete Zertifikate (Tickets), mit denen sich ein Programm des Benutzers bei den anderen Programmen authentisieren kann.
- *Zwischengeschaltete Systeme* können zentral oder dezentral funktionieren. Sie bilden eine Middleware-Komponente, die sich zwischen der primären Authentifizierungskomponente und der Anwendung einfügt. Bei dezentralen Systemen sind alle berechtigungsrelevanten Informationen auf einem Medium[55] gespeichert, das sich im Besitz des Teilnehmers befindet. Bei zentralen Systemen erfolgt die Rechteverwaltung auf einem einzigen System oder Systemverbund.
- *Föderierte Systeme* entstanden aus dem Versuch von Online-Dienst-Betreibern, ihren Kunden aufeinander aufbauende Dienstleistungen anzubieten. Durch die gemeinsame Nutzung von personenbezogenen Informationen entfällt die Notwendigkeit, die Änderung dieser Daten in jedes dieser Systeme erneut einzugeben. Die Angebotsgestaltung wird durch eine erweiterte Informationssammlung unterstützt.

C.3.7.2. Anforderungen an das SSO-System

Eine der beschriebenen SSO-Technologien besteht in der Aufrechterhaltung von mehreren aktiven Verbindungen zu unterschiedlichen Applikationen, die von einer Login-Session

[54] Es ist zu beachten, dass die Bridge-CA nicht zu der Wurzelinstanz der zusammengeführten Vertrauensdomänen wird.

[55] Zum Beispiel auf einer Chipkarte.

des Benutzers ausgehen. Der größte Nachteil dieses Ansatzes ist der hohe Ressourcenverbrauch, da mehrere Verbindungen aufgebaut, ACL/Directory-Zugriffe erfolgen und viele Datenpakete verschickt werden müssen, damit die Verbindungen nicht verloren gehen. Bei einer Vielzahl von Benutzern summiert sich das schnell zu einer beachtlichen Systemlast. Ein weiterer Nachteil sind die ständig aktiven Verbindungen (Sessions), die von einem Angreifer übernommen werden könnten.[56] Eine ressourcenschonende Alternative besteht in der Authentifizierung gegenüber einem Netzwerk-Service, der nicht die Authentifikationen bei allen verfügbaren Applikationen unmittelbar folgen. Die entsprechenden Authentifikationen erfolgen nur bei Bedarf, wenn der Benutzer bestimmte Dienste in Anspruch nimmt.

Aktuelle SSO-Lösungen bieten wesentlich mehr Funktionalität als Benutzerauthentifikation und Passwortverwaltung. Sie helfen beim zentralisierten Benutzermanagement, beherrschen rollenbasierte Berechtigungsvergabe und unterstützen beim Monitoring der Benutzeraktivitäten. Vor der Einführung eines SSO-System in einem Forschungsnetz müssen folgende Fragen beantwortet werden:

- Unterstützt das SSO alle notwendigen Applikationen ohne Anpassungen des Applikationscodes?
- Welche Plattformen (sowohl auf der Server- als auch auf der Client-Seite) werden vom Produkt unterstützt?
- Erfordert das System gleiche Authentifizierung für alle Applikationen?
- Welche Identifikations-Technologien werden unterstützt (Tokens, Chipkarten etc.)?
- Ist ein webbasierter Zugriff möglich? Wenn ja, welche Authentifizierungs- und Verschlüsselungsoptionen werden unterstützt?
- Kann die SSO-Anwendung zur Standardoberfläche auch für andere Systeme werden?
- Wie einfach können neue Applikationen in die Lösung integriert werden?
- Wie verträgt sich die Lösung mit der bereits vorhandenen PKI-Infrastruktur?

Um Mehrfacheingaben auf der Applikations- und auf der SSO-Seite bei jeder Änderung der Benutzerdaten (z. B. Passwortänderung, Änderung des Logins etc.) zu vermeiden, sollte das SSO-System die automatische Replikation dieser Daten beherrschen. Dies kann auf zwei Arten erfolgen: über API-basierte Agenten für die Aktualisierung der Applikationen oder mithilfe von Session-Agenten für die Anwendungen ohne entsprechende API-Unterstützung. Dabei muss das SSO-System die Zugriffskontroll-Dienste unterstützen, um einem Benutzer Zugriff auf die Applikation zu gewähren und seine Berechtigungen innerhalb dieser Anwendung zu bestimmen. Außerdem sollte das SSO-System die übertragenen Informationen verschlüsseln können, um diese vor dem unerwünschten Abhören zu schützen, und Logging-Funktionalitäten anbieten, damit die Applikationen ihre Log-Daten an das SSO-System zwecks Auswertung und Archivierung weiterleiten.

Das Produkt muss auch mobile Benutzer unterstützen, die sich an mehreren PCs anmel-

[56] Diese Art der Angriffe bezeichnet man als „Session-Hijacking“.

den können müssen. Selbstverständlich muss das System die Sicherheitsstandards des Forschungsnetzes erfüllen und die Umsetzung einer forschungsnetzkonformen Zugriffsberechtigungsstruktur erlauben. So darf ein Benutzer mit Administrationsrechten keine administrativen Aufgaben von einem als unsicher eingestuften System durchführen. In Notsituationen (Bekanntwerden eines Sicherheitsvorfalls) bleibt den Anwendern der Zugriff durch das SSO-System verwehrt. Lediglich dem mit der Fehlerbehebung beschäftigten Administrationspersonal wird die Arbeit an den Systemen gestattet.
Das verwendete SSO-System muss mehrbenutzerfähig sein: Mehrere Anwender können gleichzeitig an einer Workstation angemeldet sein. Verwechselung ihrer Identitäten oder ein unerwünschter Datenaustausch zwischen den parallel arbeitenden Benutzern dürfen vom SSO-System nicht zugelassen werden.
Das Sicherheitsniveau eines SSO-Systems darf die Sicherheit anderer Forschungsnetzanwendungen nicht unterschreiten. Dazu zählen u. a. die Unterstützung der anerkannten Authentifizierungsverfahren bzw. -standards, Protokollierung der Anmeldeversuche, Sperrung von Benutzeraccounts nach mehreren erfolglosen Anmeldeversuchen. Das SSO-System muss auch den sogenannten Inaktivitäts-Timer und das Sperren des Terminals beim Verlassen des Arbeitsplatzes anbieten. Sinnvoll ist außerdem die Anzeige der fehlgeschlagenen Anmeldeversuche bei der nächsten erfolgreichen Anmeldung (vgl. [TK03]).
Die Implementierung eines SSO-Systems darf den anfallenden Administrationsaufwand nur unwesentlich erhöhen; eigentlich wird vom System eine Reduzierung des administrativen Aufwandes erwartet. Das SSO-System muss eine einheitliche Administrationsoberfläche für möglichst viele Forschungsnetzanwendungen anbieten und die im Abschnitt 3.5.4 „Rollenbasierte Rechtevergabe (RBAC)“ vorgestellte rollenbasierte Berechtigungsvergabe unterstützen. Ein SSO-System, welches nur die Berechtigungsvergabe auf Benutzer/Applikations-Ebene anbietet, erfüllt diese Anforderung nicht.
Die mit Abstand wichtigsten Anforderungen an ein SSO-System sind die *Ausfallsicherheit* und *Fehlertoleranz*. Das SSO-System muss sowohl auf der Hardware- als auch auf der Softwareseite zuverlässig funktionieren.[57] Das System muss fehlertolerant sein; die Nichtverfügbarkeit von zugriffsrelevanten Informationen darf nicht zu Fehlentscheidungen des Systems führen. Das SSO-System und alle seine Komponenten müssen stets auf dem aktuellen Sicherheitsstand gehalten werden, um die eventuell bestehenden Angriffsmöglichkeiten zu reduzieren. Zusammenfassend müssen folgende Kriterien bei der Auswahl eines SSO-Systems für ein Forschungsnetz berücksichtigt werden (vgl. [TK03]):

- zentralisierte Administration,
- Unterstützung rollenbasierter Konzepte,
- Durchsetzung/Unterstützung von Sicherheitsstandards des Forschungsnetzes,
- Protokollierungsfunktion für sicherheitsrelevante Ereignisse und die Möglichkeit,

[57] Häufig wird ein 24/7-Betrieb notwendig sein.

mithilfe der erzeugten Log-Daten, die alten Datenstände wiederherzustellen,[58]
- differenzierte Protokollierungsfunktion für Benutzerzugriffe innerhalb von Applikationen,
- Unterstützung möglichst vieler der innerhalb des Forschungsnetzes verwendeten Plattformen/Applikationen,
- Batch/Script-Unterstützung für gleichzeitige Durchführung mehrerer Operationen,
- Plattformunabhängige Administration von Applikationszugriffen (gleiche Administrationsoberfläche für alle Applikationen),
- Erweiterbarkeit und Skalierbarkeit der Lösung bei Hinzunahme zusätzlicher Applikationen bzw. Unterstützung der phasenweisen Einführung,
- Offenlegung von Schnittstellen,[59]
- Testfunktion zur Prüfung von sicherheitsrelevanten Änderungen,
- hohe Verfügbarkeit, Fehlertoleranz und Skalierbarkeit der Lösung,[60]
- intuitiv zu bedienende, ergonomische Administrationsoberfläche.

C.3.7.3. Exkurs: Web-SSOs

Die bisher beschriebenen Anforderungen an ein Forschungsnetz-SSO unterscheiden sich teilweise orthogonal von den Anforderungen an die sogenannten Web-SSO-Systeme. So unterstreicht z. B. Martin Mink in seiner Diplomarbeit [Min03] die Vorteile einer dezentralen SSO-Lösung. Er argumentiert dabei mit der potenziellen Ausnutzung der zentralen Instanz – dem Single Point of Failure. Obwohl die Gültigkeit des Arguments auch für ein Forschungsnetz-SSO unbestreitbar ist, ist gerade die zentralisierte Kontrollmöglichkeit der Benutzerzugriffe ein Grund für die SSO-Einführung.
Auch die für Web-SSOs geforderte Anonymität und Pseudonymität der SSO-Nutzer sind innerhalb des Forschungsnetzes nicht erwünscht. Eine saubere lückenlose Protokollierung ist eine unabdingbare Voraussetzung für eine Aufklärung der evtl. auftretenden Sicherheitsvorfälle. Dies gilt auch für die geforderte Unverkettbarkeit von Benutzer-Handlungen. Die Reihenfolge bestimmter Transaktionen kann gegen die Forschungsnetz-Richtlinien verstoßen, obwohl die einzelnen Transaktionen unbedenklich sein können. Beim Einsatz eines Web-SSO Systems wird auf der Client-Seite i. d. R. keine Installation durchgeführt. Für ein Forschungsnetz ist diese Einschränkung ebenfalls kein Musskriterium. Die Forschungsnetzteilnehmer authentifizieren sich – laut Empfehlung im Abschnitt 3.5.3 „Authentifizierung von Forschungsnetzteilnehmern“ – mithilfe einer passwortgeschützten SmartCard. Die

[58] Zum Beispiel „Undo-Funktion“ bei Löschung eines Benutzer-Accounts.

[59] Zum Beispiel für die Implementierung zusätzlicher Reporting-Funktionalitäten.

[60] Obwohl ein gelegentlicher Ausfall des SSO-Systems im Forschungsbetrieb als akzeptabel hingenommen werden könnte, spielt die SSO-Verfügbarkeit im Behandlungszusammenhang eine wichtige Rolle.

Integrität dieser Systeme wird durch diverse Maßnahmen gewährleistet.[61] Dadurch entfällt auch die für Web-SSOs geltende Einschränkung, keine zusätzliche Software auf den Client-Systemen installieren zu dürfen.
Die Web-SSOs und das für den Forschungsnetzeinsatz vorgeschlagene System haben jedoch auch Gemeinsamkeiten. So müssen sichere Verschlüsselung und Benutzerauthentifizierung der SSO-Systeme garantieren, dass keine vertraulichen Informationen (sowohl Benutzer- als auch Patientendaten) für Dritte ungewollt sichtbar werden. Auch ein Forschungsnetzteilnehmer muss die Kontrolle über seine, im SSO-System gespeicherten, persönlichen Daten behalten können. Selbstverständlich müssen auch die beiden SSO-Arten konform zu dem geltenden Recht sein (vgl. [Min03], [Kag01]).

C.3.7.4. Ticketing

Derzeit existieren mehrere SSO-Produkte: .NET Passport, das Liberty Alliance Project, Virtual Identities des DotGNU Projektes, diverse Passwort-Manager etc. Alle Technologien, die diesen Systemen zugrunde liegen (abgesehen von Passwort-Managern) verwenden das sogenannte Ticketing-Verfahren. Das Ticket dient der Authentifizierung eines bereits authentifizierten Benutzers an einem anderen System. Verschlüsselung und Signierung der Tickets schützt sie gegen ungewollte Manipulationen. Um die Gefahr einer unzulässigen Nutzung der Tickets durch andere Personen zu minimieren, sind Tickets nur für eine bestimmte Zeit gültig. Ist die Gültigkeit eines Tickets abgelaufen, muss sich der Anwender erneut authentifizieren und erhält ein neues Ticket. Es existieren diverse Ticketing-Techniken, wobei viele der Ansätze weder Verschlüsselung noch zeitliche Gültigkeitsbeschränkung unterstützen. Einige der Ticketing-Techniken werden im Folgenden vorgestellt.

Cookies: Die wiederholt in negative Schlagzeilen geratenden *Cookies* sind kleine Datenpakete, die ein Webbrowser abspeichern bzw. an den Webserver versenden kann. Der Webserver kann die Gültigkeitsdauer eines Cookies und seine Sichtbarkeit auf Domänen-Ebene festlegen. Es wird zwischen persistenten und nicht persistenten Cookies unterschieden. Nicht persistente Cookies werden nach dem Beenden des Browsers gelöscht; persistente verfallen erst nach dem Ablauf eines eingetragenen Gültigkeitsdatums. Bei dem Cookie-basierten SSO werden die Ticketing-Informationen von der Erstauthentifizierungsinstanz auf dem Client in Form eines Cookies gespeichert. Die nachfolgenden Authentifizierungsinstanzen lesen dann die Inhalte des Cookies und somit das Ticket aus. Cookies in ihrer „reinen Form“ sind nur eine sicherheitstechnisch unzureichende Lösung für ein SSO-System, denn sie identifizieren nicht den Benutzer, sondern die Kombination „System-Benutzername-Browser“. Ein Benutzer, der mehrere Browser auf seinem System einsetzt, kann dadurch unterschiedliche Identitäten annehmen. Eine cookie-basierte Authentifizierung kann nicht zwischen

[61] Weitere Informationen zur virtualisierten abgesicherten Arbeitsumgebung, Malware-Scanner etc. befinden sich im Abschnitt 3.5.5 „Zugangsszenarien von Netzteilnehmern zu den Forschungsnetzdiensten“.

Benutzern unterscheiden, die das gleiche System und den gleichen Browser einsetzen. Cookies, die per HTTP – und somit im Klartext – versendet werden, können durch einen Sniffing-Angriff abgefangen werden. Eine verschlüsselte Übertragung der Cookie-Inhalte kann sie zwar gegen das Abhören, jedoch nicht gegen Cross-Site Scripting- (XSS) bzw. Cross-Site-Cooking-Angriffe schützen. Der Einsatz von SSL/TLS-SID ist wahrscheinlich die sicherste Variante, um Angriffe abzuwehren, die auf die SID-Kompromittierung während der Datenübertragung gerichtet sind. Bei Nichtverfügbarkeit dieser Option können die in Cookies gespeicherten SIDs mit einem Gültigkeitswert versehen bzw. zusätzliche Daten (zu der SID) zur Session-Identifikation verwendet werden (IP-Adresse, Version der Browsers etc.). Die SID könnte schließlich bei einer jeden neuen Anfrage neu generiert werden, was allerdings häufig zu Kompatibilitätsproblemen mit den Browser-Plugins bzw. Drittsoftware führt. Eine Benutzeridentifizierung mithilfe der Cookie-Technologie ohne zusätzliche Sicherheitsmaßnahmen ist sowohl den lokalen (z. B. das Auslesen des Tickets von einem anderen, parallel am System angemeldeten Benutzer) als auch den Remote-Angriffen[62] ausgesetzt. Daher müsste die Sicherheit der Cookie-basierten Benutzer- und Session-Identifizierung durch die beschriebenen Maßnahmen verstärkt werden.

Protokoll- und URL-Erweiterung: Eine andere Technik basiert auf der *Erweiterung des HTTP-Protokolls*, wobei einem HTTP-Request zusätzliche Header-Informationen hinzugefügt werden. Dies setzt voraus, dass sowohl der Webserver als auch der Browser diese HTTP-Erweiterung unterstützen, was wiederum eine zusätzliche Anpassung der Browser-Software bedeuten kann. Der entscheidende Nachteil dieser Technik besteht darin, dass die HTTP-Header von einem Browser ausgelesen werden und einem Angreifer dadurch ein gültiges Ticket geben können. Genauso ungeeignet für den Forschungsnetzeinsatz ist das Versenden von Tickets oder von Ticket-Verweisen in Form von *URL-Bestandteilen*[63]. Abgesehen von einigen technischen Einschränkungen[64] können die URLs in der Browser-Historie abgespeichert werden, was ebenfalls Raum für diverse Angriffe bietet. Die bereits beschriebenen Angriffe auf die Cookies mit dem Ziel der SID-Übernahme gelten auch für diese Techniken.

Versteckte Formularfelder: Häufig werden Ticketing-Informationen in *versteckten Formularfeldern* übertragen. Der einzige Vorteil dieser Technik im Vergleich zu der Protokollanpassung ist die nicht notwendige Browser-Modifikation. Vom Sicherheitsstandpunkt ist das Verstecken von Tickets in den Formularfeldern nicht weniger bedenklich als die beiden zuletzt genannten Ansätze.

---

[62] Zum Beispiel Cross-Site Scripting (XSS).

[63] Zum Beispiel `http://fnsrvapp1/confidential.html?SSO-Ticket=6A6A66446B605A625D6B819417`

[64] Zum Beispiel die maximale Länge einer URL.

HTTP-Weiterleitung: Auch die *HTTP-Weiterleitung* kann für webbasierte SSO-Systeme verwendet werden. Ein Webserver antwortet auf die Client-Anfrage mit einem Redirection-Statuscode[65] und gibt den sogenannten Location Response-Header (den neuen Speicherort der Ressource) zurück. In Verbindung mit Parameterübergabe kann diese Weiterleitung für die SSO-Funktion verwendet werden. Auch für diese Lösung gelten die bereits erwähnten Sicherheitsbedenken.

SAML: Die Security Assertion Markup Language (*SAML*) ist ein XML-Framework zum Austausch von Authentifizierungsinformationen. SAML ist ein ernst zu nehmender Standard im Bereich SSO, der durch die Einbindung von Verschlüsselung und Signaturen für Forschungsnetz-SSO empfehlenswert ist. Zusätzlich zu der Einsatzmöglichkeit im SSO-Bereich kann SAML für die Abwicklung verteilter Transaktionen[66] und für Autorisierungsdienste[67] verwendet werden.

JavaScript: Auch *JavaScript* lässt sich für webbasierte SSO-Lösungen einsetzen. Eine auf JavaScript basierende SSO-Lösung ist zwar für den Forschungsnetzeinsatz denkbar, kann aber auch problematisch sein. So bieten viele Java-Script-Lösungen keine ausreichende Sicherheit, weil bei einer Java-Script-Anwendung kein Compilerlauf notwendig ist, was die Nichtentdeckung von schweren Programmfehlern begünstigt. Außerdem wird eine Java-Script-Applikation auf dem System des jeweiligen Forschungsnetzteilnehmers ausgeführt – eine Umgebung, die manipulierbar ist.

Browser-Plugins: *Browser-Plugins* können ebenfalls als SSO-Technologie dienen. Solche Browser-Erweiterungen verwenden i. d. R. eine der in diesem Abschnitt beschriebenen SSO-Techniken.

SSL/TLS: Mithilfe von *SSL* bzw. *TLS* kann eine beidseitige Authentifizierung der Kommunikationspartner durchgeführt werden. Die Protokolle erlauben das Zusammenfassen mehrerer Verbindungen zu einer Sitzung, was das Aushandeln von Sicherheitsparametern bei einer neuen Verbindung überflüssig macht. Der Einsatz dieser Technologie für SSO bzw. ihre Kombination mit den beschriebenen Verfahren (z. B. Cookies) ist die sicherste der bisher beschriebenen Varianten.

C.3.7.5. Techologieüberblick

Die vorgestellte Liste der SSO-Ansätze ist sicherlich nicht vollständig. Es lassen sich weitere selbstkonzipierte Techniken für die SSO-Zwecke einsetzen. Innerhalb des Forschungsnetzes

[65] Zum Beispiel 301 für permanente oder 302 für temporäre Weiterleitung.

[66] Transaktionen, an denen mehrere Parteien beteiligt sind.

[67] Hierarchisch verschachtelte Web-Serviceaufrufe.

sollte jedoch von abenteuerlichen SSO-Basteleien Abstand genommen werden. Sicherheitsprobleme solcher Techniken wie die HTTP-Weiterleitung oder die Speicherung von Cookies lassen sich durch den Einsatz von kryptografischen Protokollen und PKI umgehen bzw. beseitigen. Diese sicheren Techniken werden von der Mehrheit kommerzieller auf dem Markt etablierter Lösungen verwendet, was ihren Einsatz innerhalb des Forschungsnetzes denkbar macht. Wenn die Anpassung eines vorhandenen (kommerziellen) Produktes an die Bedürfnisse des Forschungsnetzes nicht möglich ist, und eine interne spezialisierte SSO-Lösung entwickelt werden muss, sollen anerkannte Sicherheitsstandards[68] Anwendung finden. Die Sicherheitsaspekte des SSO-Einsatzes in den Forschungsnetzen dürfen nicht unterschätzt werden. Die einzuführende SSO-Architektur muss die Basis für weitere SSO-relevante Dienste (z. B. Identitätsmanagement) bilden, auf offenen Standards basieren und erweiterbar sein.

C.3.8. Verschlüsselung und Signaturen

C.3.8.1. Kommunikation

Die Kommunikation zwischen den Netzteilnehmern und -diensten soll verschlüsselt ablaufen. Dies gilt v. a. für den Datenabruf und den netzinternen Datenaustausch[69]. Zusätzlich sollen die im Forschungsnetz erstellten und ausgetauschten Dokumente signiert und verschlüsselt werden. Die Verbindung der Datenbankserver zu den Clients sowie Datenaustausch zwischen den Servern soll über eine SSL- bzw. IPSec-gesicherte Verbindung erfolgen (s. a. Abschnitt 3.5.5 „Zugangsszenarien von Netzteilnehmern zu den Forschungsnetzdiensten“).

C.3.8.2. Verbindlichkeitsdienste

Die Voraussetzung für die Verbindlichkeit einer Nachricht oder einer Aktion ist eine Public-Key-Infrastruktur. Für den Verbindlichkeitsnachweis müssen teilnehmende Personen oder Systemkomponenten registriert und ihre öffentlichen Schlüssel durch einen vertrauenswürdigen Dritten (CA) zertifiziert werden. Das Prinzip der Signierung ist vergleichsweise unkompliziert: Im einfachsten Fall verschlüsselt der Absender die Nachricht mit seinem privaten Schlüssel. Die Nachricht kann nun mithilfe seines öffentlichen Schlüssels entschlüsselt werden, was darauf schließen lässt, dass der Absender im Besitz des dazu gehörenden privaten Schlüssels ist. Der Besitz des privaten Schlüssels lässt wiederum auf die Identität des Absenders schließen. Aus Performance-Gründen empfiehlt es sich, nicht den gesamten Inhalt einer Nachricht zu signieren, sondern nur ihren Hashwert. Der Absender erzeugt also einen Hashwert seiner Nachricht, signiert ihn mit seinem privaten Schlüssel und verschickt ihn zusammen mit der Nachricht an den Empfänger. Der Empfänger ent-

[68] Zum Beispiel SAML in Verbindung mit SSL bzw. Zertifikaten.

[69] Zum Beispiel E-Mailing, Datendienste.

schlüsselt den Digest und vergleicht diesen mit dem von ihm selbst aus der Nachricht errechneten Hashwert. Stimmen die beiden Werte überein, ist die Identität des Absenders bewiesen. Der Digest muss Informationen über den für seine Erzeugung verwendeten Algorithmus enthalten (den sogenannten Algorithmusbezeichner), um die Angriffe mit einem alternativen Digest-Algorithmus zu verhindern. Ein Angreifer könnte nämlich den Hashwert der Nachricht erzeugen und versuchen, mit einem schwachen Hash-Erzeugungsverfahren den gleichen Hashwert für seine eigene Nachricht zu erstellen. Versucht er anschließend seine eigene Nachricht zusammen mit dem Digest des richtigen Absenders zu verschicken, wird der Betrug vom Empfänger nicht bemerkt.
Die Prüfung, ob die Daten tatsächlich vom Absender stammen, bezeichnet man als Authentifizierung. Man authentifiziert also die Identität des Absenders. Die Prüfung, ob die von einem Benutzer erzeugten Daten (z. B. während der Übertragung oder Speicherung) nicht geändert wurden, bezeichnet man als Integritätsprüfung. Die Überprüfung der Identität des Absenders einer Nachricht bzw. des Datenerzeugers bezieht sich auf die Verbindlichkeit der Daten. Die Unterzeichnung der Daten mit digitaler Signatur sichert die Verbindlichkeit einer Nachricht; der Unterzeichner kann nicht behaupten, die Daten würden von einer anderen Person stammen.
Bei der Generierung der Schlüsselpaare kann es zwei Szenarien geben: Die Schlüssel können entweder vom Teilnehmer selbst oder von einer vertrauenswürdigen Drittpartei generiert werden. Bei einer lokalen Schlüsselgenerierung durch den Teilnehmer wird die PKI des Forschungsnetzes entlastet. Außerdem ist ein solcher Schlüssel vertrauenswürdiger, da keine Drittpartei Kenntnis über den Schlüssel hat. Diese Vorgehensweise ist z. B. bei der Verwendung von Softwarezertifikaten denkbar, setzt allerdings das Vorhandensein entsprechender Soft- oder Hardware zur Schlüsselgenerierung bei den Teilnehmern voraus. Da in dieser Arbeit die Verwendung von auf den SmartCards gespeicherten Zertifikaten empfohlen wird, ist die zentralisierte Schlüsselerzeugung durch die CA oder RA vorzuziehen. Es sind auch Szenarien denkbar, die die Vorteile der beiden Methoden kombinieren: der Einsatz von mehreren Schlüsselpaaren. Die zentral generierten Schlüssel könnten für die Verschlüsselung genutzt werden; die von den Teilnehmern selbst generierten Schlüssel sorgen für die Verbindlichkeit. In diesem Fall muss allerdings zwischen der höheren Verbindlichkeit eines eigenhändig erzeugten Schlüssels und der höheren Sicherheit der SmartCard-Speicherung abgewogen werden. Generell kann ein Softwarezertifikat einfacher kompromittiert werden als ein auf der SmartCard gespeichertes. Auch aus diesem Grund ist die zentrale Schlüsselerzeugung zu bevorzugen.
Der Vollständigkeit halber soll hier auf die unterschiedliche Handhabung mehrerer Schlüssel hingewiesen werden. Ein für die Unterzeichnung verwendeter Schlüssel muss nicht gesichert werden. Beim Ausspähen oder beim Abhandenkommen des Schlüssels wird einfach ein neuer Schlüssel generiert. Nach dem Ablauf der Gültigkeitsdauer muss ein solcher Schlüssel vernichtet werden. Zusätzliche Sicherheit bietet der Einsatz eines Zeitstempel-

dienstes.[70] Im Gegensatz dazu muss ein zur Verschlüsselung verwendeter privater Schlüssel auch nach dem Ablauf seiner Gültigkeit verfügbar sein, um die Entschlüsselung älterer Dokumente zu ermöglichen. Die Sicherung des dazu gehörenden öffentlichen Schlüssels hängt von dem verwendeten Verfahren ab. So muss z. B. beim RSA-Verschlüsselungsverfahren der öffentliche Schlüssel nicht gespeichert werden, da er sich aus dem privaten Schlüssel des Paares ableiten lässt. Beim Schlüsselaustauschverfahren nach Diffie-Hellmann benötigt man dagegen den verwendeten öffentlichen Schlüssel zur Datenwiederherstellung. An dieser Stelle werden gezielt keine Empfehlungen für die einzusetzenden Hash- und Verschlüsselungsverfahren gegeben. Die Software für Verbindlichkeitsdienste muss einen flexiblen Wechsel der eingesetzten Verfahren ermöglichen.
Die in diesem Abschnitt diskutierten Verbindlichkeitsdienste lassen sich in einem Forschungsnetz vielfältig einsetzen. Besonders wichtig ist der Verbindlichkeitsnachweis beim Monitoring. Da die Forschungsnetzteilnehmer und -systeme mit eigenen Zertifikaten ausgestattet werden (s. a. Abschnitt 3.5.6 „Verzeichnisdienste (LDAP, OCSP)“), kann man diese mit einem vertretbaren Aufwand verwenden, um die Verbindlichkeit von Transaktionen zu verifizieren. So können z. B. die Anträge von Forschern auf Aushändigung bestimmter Daten oder die Beantragung zusätzlicher Zugriffsrechte mithilfe von Zertifikaten abgewickelt werden. Bei der Untersuchung von Sicherheitsvorfällen wäre der Verbindlichkeitsnachweis für Transaktionen oder für die von Systemen verschickten Nachrichten ebenfalls vom großen Nutzen.

C.3.8.3. Organisatorische Aspekte der PKI

Für den Betrieb der Forschungsnetz-PKI bestehen grundsätzlich drei Optionen:

- Beim *Outsourcing* der CA-Leistungen verlagert das Forschungsnetz die CA-Funktionen auf eine vertrauenswürdige Drittpartei. Dadurch kann sich ein Forschungsnetz auf seine eigentlichen Aufgaben konzentrieren und muss kein PKI-Know-how aufbauen.
- Im Rahmen des *Insourcings* stellt eine CA dem Forschungsverbund ihr Know-how und ihre Mitarbeiter zur Verfügung. Dadurch kann ein Forschungsnetz die internen Sicherheitsrichtlinien durchsetzen, ohne in die Infrastruktur der Drittpartei zu vertrauen und ohne ihr eigenes CA Know-how aufzubauen.
- Ein Forschungsnetz könnte auch eine eigene CA einrichten. Dies ermöglicht eine detaillierte Kontrolle eines jeden Aspektes der PKI-Infrastruktur.

Trotz diverser Vorteile der dritten Option, ist diese für ein Forschungsnetz aufgrund der damit verbundenen Kosten (Infrastruktur, Personal, Know-how-Aufbau, Erfüllung gesetzlicher Anforderungen etc.) kaum zu finanzieren. Es wird empfohlen, PKI-Infrastrukturen mehrerer Netze einem outgesourcten Anbieter anzuvertrauen. Die auf die PKI-Infrastrukturen

[70] Weiterführende Informationen zum Thema „Zeitstempeldienst“ befinden sich im Abschnitt 3.5.12 „Monitoring und Protokollierung“.

der Forschungsnetze spezialisierte CA wäre eine kostengünstige Alternative und könnte auch den Support des lokalen RA-Betriebs übernehmen. Aufgrund der Bedeutung der PKI-Infrastruktur und der damit verbundenen besonderen Anforderungen ist es ratsam, die ITIL-Empfehlungen zum Service von kritischen Diensten[71] zu berücksichtigen (vgl. [LM07, S. 351 f.]).
Bei der Entscheidung für oder gegen ein Outsourcing-Modell soll berücksichtigt werden, dass durch diese Entscheidung das eigene Know-how innerhalb der Organisation nicht aufgebaut bzw. gefördert wird. Dadurch kann es zu einer unerwünschten Abhängigkeit vom Anbieter kommen; das Treffen von kompetenten Entscheidung im outgesourcten Bereich wird erschwert (vgl. [GV07, S. 84]).

C.3.8.4. Mehrstufige Pseudonymisierung

Die Pseudonymisierung erfolgt innerhalb des Forschungsnetzes durch den mehrstufigen Einsatz kryptografischer Funktionen. Mehrstufige Pseudonymisierung sorgt dafür, dass auch bei der Akkumulation von Forschungsdaten das Reidentifizierungsrisiko für den Patienten nicht erhöht wird.
In der ersten Stufe der Pseudonymisierung wird dem Identifikationsdatensatz (*IDAT*) eine nicht sprechende Zeichenkombination (*PID*) zugeordnet. Hier bedient man sich des *PID*-Dienstes. In der zweiten Stufe der Pseudonymisierung wird der *PID* durch seine kryptografische Transformation ersetzt (*PSN*). Die Verschlüsselung erfolgt auf einer Chipkarte, sodass der verwendete Schlüssel die Karte nie verlässt und keine temporären Dateien zur Datenwiedergewinnung erhalten bleiben.
Beim Verdacht des Chipkartendiebstahls oder des Bekanntwerdens des Schlüssels müssen alle PSNs durch eine Neuverschlüsselung ersetzt werden. Um diese Aufgabe möglich zeitnah bewältigen zu können, müssen die im Voraus erstellten Karten mit einem Ersatzschlüssel in einer gesicherten Umgebung aufbewahrt werden. Beim Datenexport greift schließlich die dritte Pseudonymisierungsstufe; *PSN* wird für jeden Export i mithilfe eines symmetrischen Verschlüsselungsverfahrens in ein neues PSN_i umgewandelt (s. a. Abschnitt 4.3 „Qualitative Bewertung der Bedrohungs- und Risikosituation“).

C.3.9. Aspekte der Datenbanksicherheit

Forschungsnetzdaten können in mehr als zwei Datenbanken abgelegt werden. Im TMF-Gutachten für Biomaterialdatenbanken werden beispielsweise acht Datenbankinstanzen erwähnt; eine mögliche Datenaufteilung zwischen den Datenbanken ist in der Abbildung 42 dargestellt (vgl. [SPR+06, S. 150 f.]). Um die Angriffsmöglichkeiten auf die Datenbanksysteme zu minimieren, dürfen die Datenbank-Server keine weiteren Server-Dienste anbieten (z. B. File-Dienste, Intranet etc.). Ein Datenbankserver soll auf einem

[71] Safety critical services and high risk environments.

sogenannten gehärteten System installiert werden. Sämtliche für den DB-Betrieb nicht notwendigen Dienste, Module und Treiber sind zu deaktivieren. Derzeit existieren mehrere Ansätze/Projekte zur Härtung von Betriebssystemen,[72] wobei generell zwischen zwei möglichen Vorgehensweisen zu unterscheiden ist: Verwendung eines Systems, welches bereits bei der Konzeption auf seine Härtung optimiert wurde und die nachträgliche Abhärtung eines (bereits eingerichteten) Systems.[73] Grundsätzlich ist die erste der beiden Optionen zu bevorzugen. Vor einigen Jahren wurde oft empfohlen, die Widerstandsfähigkeit von Systemen durch den Einsatz von nicht beschreibbaren Medien bzw. durch das Starten des Systems bzw. den Anwendungen von einem besonders vertrauenswürdigen Netzwerkpfad zu erhöhen. Heute müsste zwischen dem damit verbundenen zusätzlichen Aufwand und den geringer werdenden Sicherheitsvorteilen abgewogen werden, denn die Angriffstechniken und -ziele haben sich im Laufe der Zeit verändert. Die modernen Angreifer legen einen großen Wert darauf, dass die Systemkompromittierung unerkannt bleibt. Viele Malware bleiben nur im flüchtigen Systemspeicher – nach dem Neustart verschwindet der Schädling aus dem System (vgl. [Sch07], [PE06]).

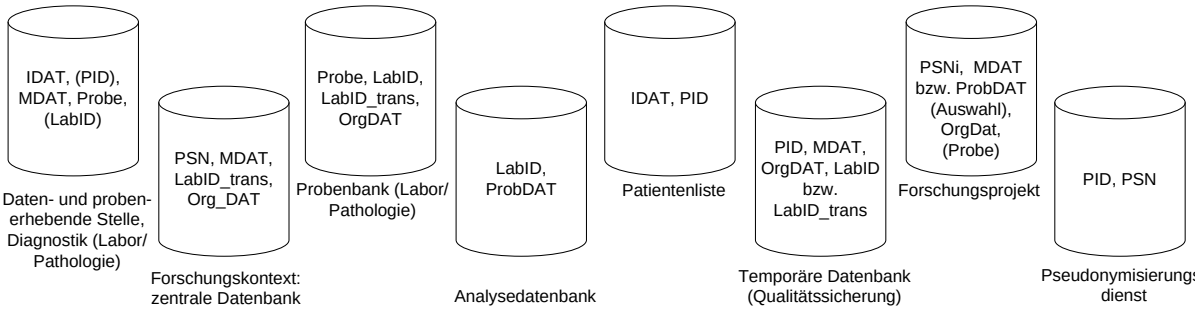

Abbildung 42.: Eine mögliche Datenaufteilung zwischen den Forschungsnetzdatenbanken nach [SPR+06].

Die Sicherheit von freien (Open Source) und proprietären Betriebssystemen ist ein stark debattiertes Thema. Es existieren unzählige Studien, die abwechselnd die Sicherheit und die sonstigen Vorteile des einen oder des anderen Ansatzes belegen (vgl. [Bou05], [RVRK05], [PSE04]). Diese Arbeit soll nicht zum Austragungsort des Streits um das sicherste Betriebssystem werden. Aufgrund persönlicher Erfahrungen und Präferenzen des Autors wird der Einsatz von mehreren unterschiedlichen freien, auf Sicherheit optimierten Betriebssystemen empfohlen. Durch den parallelen Einsatz unterschiedlicher DB-Betriebssysteme wird vermieden, dass derselbe Angreifer mehrere Forschungsnetz-Datenbanken durch die

[72] Zum Beispiel [Bea12], [nov11], [Spe11], [Xie10], [nsa09] etc.

[73] Relativ bekannt im Bereich der nachträglichen Abhärtung einer Unix/Linux-Distribution ist z. B. Bastille Linux. Dabei handelt es sich um einen Versuch, ein bestehendes Linux/Unix-System gegen Sicherheitslücken und Angriffe zu immunisieren. Als Basis-Distributionen lassen sich beispielsweise Red Hat, Fedora Core, SuSE, Mandrake, Debian und Gentoo nutzen.

Ausnutzung der gleichen Sicherheitslücke ausspäht.[74]
Die Sicherheit von Betriebssystemen ist kein einfaches Thema, denn die Sicherheitsstufe eines Systems ändert sich häufig[75] und ist von der Systemkonfiguration abhängig. Es ist daher empfehlenswert, unmittelbar kurz vor der Systemimplementierung die Entscheidung für ein System zu treffen, wobei solche Faktoren wie Know-how der Mitarbeiter, finanzielle Situation des Anbieters, Presseberichte in die Wahl einfließen sollen. Das Betriebssystem für eine Datenbank sollte auf einem dedizierten Hardwaresystem installiert werden. Von einer virtualisierten Umgebung im Datenbankbereich muss abgeraten werden; diese kann nämlich selbst Sicherheitslücken aufweisen und reduziert somit die Sicherheit der Datenbank. Für den Forschungsnetzeinsatz werden freie Datenbankmanagementsysteme wie beispielsweise MySQL, PostgreSQL, Firebird, Ingres® empfohlen.[76]
Unabhängig vom eingesetzten Betriebs- und Datenbankmanagementsystem ist eine regelmäßige Wartung der DB-Installation notwendig. Die relevanten Sicherheitspatches müssen stets zeitnah nach ihrem Erscheinen eingespielt werden. Serviceverträge garantieren eine schnelle Reaktionszeit bei evtl. auftretenden Problemfällen (s. a. Abschnitt 3.3.3 „Organisation und Gestaltung von Notfallvorsorgemaßnahmen“). Als sicherheitstechnisch sinnvoll erscheint die Forderung, die Datenbank-Server in abgesicherten Serverräumen aufzustellen (s. a. Abschnitt 3.4 „Administrative Aspekte von Sicherheitsrichtlinien“). Aufgrund der hohen Vertraulichkeit der Daten ist die Verwendung einer Online-Verschlüsselung empfehlenswert. Eine ausführliche Anleitung zum sicheren DB-Betrieb befindet sich unter [bsi11d].

Allgemeine Regeln zur Handhabung von Datenbanken: Wie auch in anderen Forschungsnetzbereichen ist eine strikte Trennung zwischen der Produktions- und der Testumgebung unabdingbar. Sämtliche Änderungen der Datenbankstrukturen müssen durch den Änderungsmanagementprozess evaluiert werden. Der Zugriff von Applikationen auf die Datenbank muss dem Prinzip der minimalen Rechte entsprechen. Dadurch wird verhindert, dass eine kompromittierte Applikation die Inhalte der Datenbank auf eine unerwünschte Art und Weise verändert bzw. auf die nicht zulässigen Datenbankbereiche zugreift. Um die Nachvollziehbarkeit von Datenbankänderungen zu gewährleisten, erhält jede zur Datenbankänderung berechtigte Person,[77] einen personifizierten Zugriff. Die Zugriffe der Personen müssen den im Abschnitt 3.5.3 „Authentifizierung von Forschungsnetzteilnehmern“ vorgestellten Regeln folgen. Die erteilten Berechtigungen müssen regelmäßig auf

[74]Diese Aussage gilt unter der Voraussetzung, dass die unterschiedlichen Datenbanken nicht die gleichen Sicherheitslücken aufweisen.

[75]Zum Beispiel durch das Bekanntwerden von Exploits, Einbringung von neuen Releases, Patch-Managementpolitik etc.

[76]Informationen zum OpenBSD und den genannten Datenbanksystemen befinden sich im Glossar.

[77]Zum Beispiel Mitglieder der Gruppe „Änderungsmanagement“.

ihre Notwendigkeit überprüft und beim Bedarf zeitnah zurückgenommen werden. Viele der in diesem Abschnitt beschriebenen Maßnahmen gelten auch für die Test- und Entwicklungsumgebungen des Forschungsnetzes, denn diese können Produktionsdaten enthalten.[78]

C.3.10. Proxying und Aspekte der VPN- und IDS-Platzierung in Verbindung mit Firewalling

C.3.10.1. Platzierung von VPN-Endpunkten und IDS-Sensoren

In den Abschnitten 3.5.5 „Zugangsszenarien von Netzteilnehmern zu den Forschungsnetzdiensten“ und 3.5.11 „Intrusion Detection Systeme (IDS)“ werden die VPN- und IDS-Technologien beschrieben, ohne auf die Platzierung von VPN-Endpunkten in Verbindung mit diesen Technologien einzugehen. Beim System eines einzelnen Forschungsnetzteilnehmers wird die lokale Installation der VPN-Software wohl die am wahrscheinlichsten anzutreffende Konfiguration sein. Die Sicherheit eines solchen Aufbaus ist nicht sonderlich hoch und weist die gleichen Probleme auf wie z. B. im Falle der Software-Firewalls. Da die Anschaffung teurer VPN-Hardware für alle Teilnehmer kaum durchzusetzen ist, sind die Software-VPNs jedoch eine akzeptable Lösung. Ein Forschungsnetz hat mehrere Möglichkeiten zur Platzierung von VPN-Endpunkten. Geht man von einem zweistufigen redundanten DMZ-Aufbau aus, ergeben sich die in der Abbildung 43 dargestellten Platzierungsmöglichkeiten für VPN-Endpunkte und IDS-Sensoren.

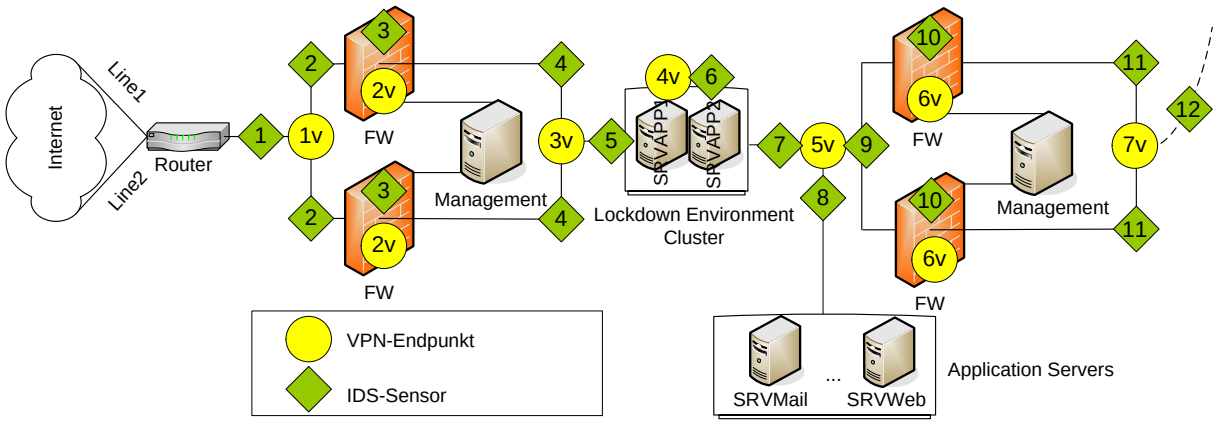

Abbildung 43.: Mögliche Platzierung für die VPN-Endpunkte und IDS-Sensoren: Bereits beim abgebildeten zweistufigen DMZ-Aufbau ergibt sich eine Vielzahl von Platzierungsmöglichkeiten für die IDS-Sensoren und VPN-Endpunkte. Bei der Auswahl der sinnvollen Kombinationen sind die zu prüfende Datenmenge und die Form der Daten (verschlüsselt bzw. nicht verschlüsselt) zu berücksichtigen.

Eindeutig nachteilig ist die Installation eines VPN-Endpunktes im Bereich 1v, denn dadurch

[78]Eine Klassifizierung der Daten in Bezug auf ihren Vertraulichkeitsbedarf wurde im Abschnitt C.6.3 „Datenklassifikation“ vorgenommen.

wäre dieser den Angriffen von außen ausgesetzt.[79] Platzierung der VPN-Endpunkte im Bereich 2v ist im Vergleich dazu wesentlich vorteilhafter, da viele der Firewall-Modelle VPN-fähig sind. Dies erspart die Installation zusätzlicher Hardware und sorgt dafür, dass die nachstehenden IDS-Sensoren[80] Daten in unverschlüsselter Form (und somit) auswertbar empfangen. Der große Nachteil der Einrichtung von VPN-Endpunkten auf der äußeren Firewall besteht im relativ hohen Kompromittierungsrisiko: Die äußere Firewall ist den Angriffen von außen ausgesetzt; eine evtl. Sicherheitslücke in der VPN-Implementierung bzw. -konfiguration kann von einem Angreifer ausgenutzt werden. Verglichen damit sind die Platzierungsmöglichkeiten 3v und 4v wesentlich unkritischer, wobei bereits die zu weite Platzierung vom VPN-Endpunkt 4v innerhalb der DMZ dem eigentlichen Ziel von VPN für das Forschungsnetz nicht unbedingt förderlich ist. Alle VPN-Endpunkte ab 5v bedeuten verschlüsselte Kommunikation an den Lockdown-Servern und sind somit nicht praktisch umsetzbar. Die Platzierungsmöglichkeiten 6v und 7v scheiden damit ebenfalls als nicht praktikabel aus.

Die VPN-Endpunkte sollten also nach Möglichkeit entweder in den Bereichen 3v oder 4v der Forschungsnetz-DMZ platziert werden. Bei dem VPN-Endpunkt an der Stelle 3v sollten keine IDS-Sensoren vor der Platzierungsmöglichkeit 5 installiert werden. Sollte der IDS-Sensor auch Filterungsfunktionen übernehmen, wäre ein Sensor in der Position 5 eher in der Lage, Angriffe zu erkennen als ein Sensor an der Stelle 6 sowie alle anderen nachgelagerten Sensoren. Erhöhte Sicherheit kann durch Filterung des Datenverkehrs vor und nach der Ausführung der Benutzerkommandos auf den Lockdown-Servern erreicht werden. Ein an dem Punkt 6 installierter auf der Applikationsebene arbeitender IDS-Sensor wäre in der Lage, schadhafte Benutzertransaktionen vor ihrem Eintreffen am Applikationsserver festzustellen und die Ausführung der entsprechenden Kommandos zu verweigern.

Auch die Positionierung des VPN-Endpunktes in 4v in Verbindung mit IDS-Sensorinstallation in 6 hat diverse Vorteile. Bei der Verwendung von softwarebasierten VPN- und IDS-Lösungen wäre diese Alternative vergleichbar kostengünstig. Bedenklich wäre lediglich die Rolle der Lockdown-Server, denn durch die Ausnutzung der evtl. vorhandenen Sicherheitslücken in der Lockdown-Umgebung könnte ein Angreifer die VPN- bzw. IDS-Konfiguration manipulieren. Aufgrund der o. g. Bedenken ist die Installation von VPN-Endpunkten/IDS-Sensoren an den Stellen 4v respektive 6 nicht empfehlenswert (vgl. [BS08], [Dom01], [Str99]).

[79] Dies gilt auch für die Installation der IDS-Sensoren an den Punkten 1 und 2, wobei in diesem Fall die von IDS-Sensoren empfangene Datenmenge relativ hoch ist.

[80] Inkl. IDS-Sensor 3.

C.3.10.2. Proxying

Unter einem Proxy-Server[81] versteht man ein sogenanntes Dual-Homed System, welches die Anfragen von mehreren Clients an einen Dienst (oder einer Menge von Diensten) verwaltet. Die Anfragen an die von einem Proxy-Server betreuten Dienste richten sich zunächst an den Proxy-Server selbst, der sich anschließend entweder mit dem entsprechenden Dienst verbindet oder die Anfrage zurückweist. Ein Proxy-Dienst wird meistens auf einem gehärteten System installiert und ist für Logging- und Auditing-Zwecke prädestiniert. Die wohl bekannteste Form eines Proxy-Servers ist der Web-Proxy. Ein Web-Proxy vermittelt zwischen einem Webbrowser und einem Internet-Server und erfüllt folgende Funktionen:

- *Filterungs- und Trennungsfunktion:* Durch entsprechende Proxy-Konfiguration können bestimmte Webseiten und -inhalte für den Zugriff gesperrt werden. Ein Proxy sorgt auch dafür, dass keine sicherheitsgefährdende direkte Verbindung zwischen dem Internet und dem LAN zustande kommt.

- *Protokollierungsfunktion:* Die Zugriffe von Benutzern auf Webdienste können protokolliert werden.

- *Caching und Bandbreitenkontrolle:* Durch die Zwischenspeicherung der Abfrageergebnisse kann ein Caching Proxy viele Anfragen selbst beantworten, ohne diese an die Server im Internet weiterzuleiten, was die Bandbreite schont und Performanceverbesserungen mit sich bringt. Ein Proxy kann auch die Lastverteilungsfunktion übernehmen, indem er für seine Anfragen weniger ausgelastete Verbindungen verwendet oder diese an weniger ausgelastete Server schickt.

- *Anonymisierung und Zugriffssteuerung:* Ein Proxy kann die Zugriffssteuerungsfunktion übernehmen, indem er nur die Abfragen authentifizierter Clients weiterleitet bzw. diese aufgrund von bestimmten Zugriffsmerkmalen einschränkt. Gleichzeitig kann ein Proxy dafür sorgen, dass die Zugriffe von Clients bei den Servern anonymisiert ankommen, indem er die Identität des Anfragenden verschleiert.

Eine pauschale Empfehlung für den Einsatz eines Proxy-Servers innerhalb des Forschungsnetzes kann nicht abgegeben werden. Ein Proxy-Server gehört zu den kritischen Infrastrukturbestandteilen und kann vom Angreifer für die Vorbereitung oder Weiterführung eines Angriffs ausgenutzt werden; die Einrichtung und Pflege eines Proxys sind mit zusätzlichem Aufwand verbunden. Trotzdem kann der Proxy-Einsatz für ein Forschungsnetz sinnvoll sein, um z. B. den Zugriff der Forschungsnetzmitarbeiter auf das Internet abzusichern. Die erwähnte Trennungs- und Filterungsfunktion kann beispielsweise dafür sorgen, dass keine unerwünschten Internet-Inhalte vom Forschungsnetzpersonal angesteuert werden. Die Protokollierungsfunktion sorgt für eine vereinfachte zentralisierte Erfassung

[81] Auch oft als „Application Gateway“ bezeichnet.

von sicherheitsrelevanten Ereignissen und kann bei der Untersuchung von Sicherheitsvorfällen hilfreich sein. Mithilfe von Proxy-Servern lassen sich auch die für eine höhere Verfügbarkeit/Ausfallsicherheit sorgenden Redundanzen aufbauen.
Ein für den Forschungsnetzeinsatz geeigneter Proxy sollte WCCP-Unterstützung[82] mitbringen, um den Aufbau von Redundanzen und Fehlertoleranz zu ermöglichen. Das Authentifizierungsmodul des Servers sollte den Einsatz von Teilnehmer-Zertifikaten unterstützen. Die eingesetzte Lösung soll flexible Steuerung Policy-basierter Zugriffe für Benutzer, Benutzergruppen, Netzwerksegmente und Systeme auf bestimmte Webseiten und Inhalte erlauben. Die für das Content-Filtering eingesetzte Datenbank soll die Erzeugung eigener Content-Kategorien ermöglichen und editierbar sein; die automatische Aktualisierung der sogenannten Blacklisten sollte mindestens ein Mal am Tag stattfinden. Der Proxy soll in der Lage sein, Instant-Messaging-Anwendungen/Protokolle zu blockieren bzw. solche Kommunikation zu protokollieren und sollte mit den ICAP-Virus-Scanning Servern kompatibel sein.
Interessant für den Forschungsnetzeinsatz ist auch die „Umkehrung“ des Proxy-Prinzips in Form eines sogenannten Reverse Proxy-Servers. Ein Reverse-Proxy wird üblicherweise bei externen Anfragen einem internen Server oder einem Serververbund davorgeschaltet, sodass alle an diese(n) Server gerichteten Anfragen zuerst beim Proxy-Server ankommen. Für den Einsatz eines Reverse-Proxys innerhalb des Forschungsnetzes sprechen mehrere sicherheitstechnische Überlegungen. Ein Reverse Proxy wird meist vor einem internen Webserver positioniert und ist somit eine zusätzliche Stufe, die direkte Client-Angriffe auf den dahinter liegenden Server abfängt. Durch seine Caching-Eigenschaft kann ein Reverse-Proxy andere Forschungsnetzserver entlasten, indem er die Client-Anfragen an die statischen Inhalte aus seinem Cash beantwortet. Seine Lastverteilungseigenschaften werden dann interessant, wenn mehrere Webserver hinter dem Reverse-Proxy platziert werden. Auch beim Ausfall der Server sorgt der Proxy für eine gesteigerte Ausfallsicherheit, da er die Client-Anfragen an die noch funktionierenden Server umleiten kann. Im Abschnitt 3.5.7 „Ticketing, Single Sign-On (SSO)“ wurde das Single Sign-On-Prinzip vorgestellt. Auch Reverse-Proxy lässt sich für die SSO-Zwecke einsetzen. Clients bedürfen einer einmaligen Anmeldung an dem Reverse-Proxy-Server; dieser übernimmt anschließend die Authentifizierung gegenüber den dahinter stehenden Webservern. Auch die Verlagerung der SSL-Zertifikate vom Webserver auf den Reverse-Proxy ist vorstellbar. Dadurch verschiebt man Zertifikate von einem i. d. R. leichter zu kompromittierenden Webserver auf den besser abgesicherten Proxy. Beim Zertfikat-basierenden SSL-Einsatz verwandelt sich ein Proxy-Server in einen SSL-Proxy, der die Entschlüsselung der Client-Anfragen übernimmt und diese an die Webserver weiterleitet (vgl. [bsi11d, M 4.223]).

[82] Web Cache Control Protocol.

C.3.11. IDS-Technologie und -Einsatzszenario in einem medizinischen Forschungsnetz

C.3.11.1. Erkennungstechniken

Die wohl bekannteste Technik der Intrusion Detection ist die *Signaturerkennung*. Die *Signaturerkennung* basiert auf der Suche nach bestimmten, für einen Angriff charakteristischen Sequenzen. So kann der Datenstrom auf typische Ports, charakteristische TCP/IP-Flags der Datenpakete oder verwendete Protokolle untersucht werden. Der Vorteil signaturbasierter Angriffserkennung liegt in der relativ einfachen Implementierung und zeichnet sich durch gute Erkennungsraten aus.
Ein großer Nachteil der signaturbasierten Angriffserkennung liegt darin, dass sogar die kleinsten Angriffsvariationen die Erstellung einer neuen Signatur notwendig machen können. Selbstverständlich können die Signaturen auch generisch gestaltet werden, um sie für eine ganze Reihe von Angriffen verwendbar zu machen. Generische Signaturen bringen jedoch eine erhöhte Gefahr von Fehlalarmen[83] mit sich.
Oft versuchen die Angreifer, ihre Angriffe durch Code-Modifikation, Fragmentierung oder Verschlüsselung für die signaturbasierte Erkennung unkenntlich zu machen. Für die Erkennung solcher Angriffe existieren mehrere Ansätze, die in der weiterführenden Literatur nachgelesen werden können (vgl. [NN01], [Hoe01]). Zwei weitere häufig verwendete Erkennungsansätze sind die Anomalienanalyse und die Intrusion Detection auf Protokollebene.
Intrusion Detection auf Protokollebene erfolgt durch die Analyse der Kommunikationsprotokolle. Aus den Datenpaketen werden zuerst Informationen extrahiert; anschließend nimmt das IDS die Rolle der Applikation ein, die diese Datenpakete erhalten sollte. So können die für eine bestimmte Anwendung nicht gültigen bzw. schädlichen Pakete erkannt werden.
Die auf Protokollebene arbeitenden IDS können auch die nicht erwünschten Dienste erkennen, auch wenn der Angreifer gezielt unverdächtige Ports verwendet. So kann z. B. ein File-Sharing- oder IRC-Dienst auf den von der Firewall zugelassenen Ports 21 (ftp), oder 80 (http) laufen. Auch veränderte Angriffe, die von der signaturbasierten Angriffserkennung nicht identifiziert werden, können durch Analyse auf Protokollebene erkannt werden. Die Nachteile dieser Technologie liegen in der vergleichsweise aufwendigen Implementierung und einem hohen Anteil von Fehlalarmen während der IDS-Einführungsphase.
Die auf *Anomalienanalyse* basierenden Intrusion-Detection-Systeme untersuchen die Abweichungen im Systemverhalten. Dafür muss der Normalzustand einer bestimmten Infrastruktur bekannt sein.[84] Manche anomalienbasierten IDS überwachen ein System eine Zeit

[83] „False Positives“

[84] Eine ausführliche Beschreibung der bei der Anomalienanalyse verwendeten Methoden befindet sich in [Hoe01].

lang (die sogenannte Lernphase) und unterbreiten anschließend einen Vorschlag für die Erstellung/Anpassung des IDS-Regelwerkes. Selbstverständlich besteht dabei die Gefahr, dass das Netzwerk bereits während der Lernphase des Intrusion-Detection-Systems Unregelmäßigkeiten und Abweichungen vom gewünschten Zustand aufweist,[85] sodass das IDS den eigentlichen Angriff oder dessen Vorbereitung als Bestandteil des Normalzustandes auffasst.

	Implementierung	Fehlkategorisierungsrate	Erkennungsrate/ neue Angriffe
Signaturerkennung	einfach	gering	niedrig
ID auf Protokollebene	mittelschwer	mittelhoch	hoch
Anomalienanalyse	aufwendig	hoch	hoch

Tabelle 19.: Intrusion Detection-Technologien im Vergleich: Die signaturbasierte Angriffserkennung ist relativ einfach zu implementieren, liefert gute Erkennungsraten für bekannte Angriffe und erzeugt nur wenige Fehlalarme. Die anomalienbasierte Erkennung eignet sich besser für die Erkennung von neuen Angriffen.

Bei der anomalienbasierten Angriffserkennung handelt es sich um einen heuristischen Ansatz. Man verwendet eine algorithmische Logik als Basis für die Entscheidungen. Solche Algorithmen können z. B. auf statistischen Auswertungen der Eigenschaften des zu untersuchenden Netzverkehrs basieren. Die Vorteile eines auf der Heuristik basierenden Systems liegen in dessen Fähigkeit, Angriffe zu erkennen, welche von keinem anderen bereits beschriebenen System erkannt werden können und in der gleichzeitigen Unabhängigkeit von den Angriffssignaturen. Die Nachteile liegen in der Notwendigkeit der Definition eines spezifischen Algorithmus/Regelwerks und dessen ständiger Anpassung an die Umgebungsveränderungen.
Die anomalienbasierten IDS können vollkommen neue unbekannte Angriffe erkennen, was auf Kosten des hohen Implementierungs- und Konfigurationsaufwands geht. Außerdem können die Alarme eines solchen Systems nicht mit hundertprozentiger Wahrscheinlichkeit als erkannte Angriffe identifiziert werden. Der Prozentsatz von „False Positives“ kann abhängig von der Systemkonfiguration sehr hoch sein. In der Tabelle 19 wurden die Eigenschaften der drei o. g. Erkennungsmethoden zusammengefasst (vgl. [Gre03]).

C.3.11.2. Arten von IDS

Hostbasierte IDS (HIDS): Die *hostbasierten IDS (HIDS)* verrichten ihre Arbeit unmittelbar auf dem zu schützenden System. Es existieren zwei Arten von hostbasierten IDS:

- *„Traditionelle HIDS“* überwachen Log-Dateien eines Systems, Kernelmeldungen, Systemdateien etc. Sie schlagen Alarm, sobald Unregelmäßigkeiten festgestellt werden. HIDS müssen direkt auf den zu überwachenden Systemen installiert werden

[85] Ein Angreifer könnte z. B. das Netzwerk während der Anpassungszeit systematisch nach Schwachstellen durchsuchen.

und bedürfen oft einer aufwendigen individuellen Anpassung. HIDS könnten zwar nicht zum Schutz jedes einzelnen Systems innerhalb des Forschungsnetzes verwendet werden, eignen sich jedoch für den Schutz der als kritisch geltenden Datenbanksysteme und Administrationsarbeitsplätze. Selbstverständlich können HIDS auch als Sensoren für ein globales IDS innerhalb des Forschungsnetzes eingesetzt werden, indem sie die zusammengetragenen Daten an eine zentrale Stelle innerhalb des Forschungsnetzes weiterleiten. Die aggregierten Daten erhöhen die Ergebnisgenauigkeit der Angriffserkennung beträchtlich.[86]

- Die *dateisystemintegritätsprüfenden IDS* erzeugen einen Snapshot des Systems mithilfe eindeutiger Hashwerte und verifizieren diesen in regelmäßigen Zeitabständen. Die dateisystemintegritätsprüfende IDS haben einen großen Nachteil: Alle legal durchgeführten Konfigurationsänderungen müssen von dem Snapshot erfasst werden, was bei den häufigen Systemupdates lästig werden kann. Die Reduzierung des Aufwands durch die Erhöhung des Zeitfensters, in dem Systemupdates und -überprüfungen durchgeführt werden, kann dazu führen, dass Angriffe erst mit einer größeren Verzögerung festgestellt werden.
  Eine Unterart der signaturbasierten IDS bilden die sogenannten Integritätschecker. Ein solches IDS[87] erstellt für ein System eine Datenbank mit CRC-Hashwerten für jede Datei, die es bei einem Systemscan neu errechnet und mit den gespeicherten Werten vergleicht. Da die Systemdateien sich (abgesehen von System-Updates) nicht ändern sollen, kann eine Abweichung der CRC-Werte auf die Kompromittierung hindeuten. Dieses Verfahren war noch bis vor wenigen Jahren wirksam, ist jedoch seit der Verbreitung der nur noch im flüchtigen Speicher anwesenden Rootkits bzw. Malware nahezu nutzlos. Der Grund für diese Entwicklung sind die geänderten Prioritäten der Malware-Autoren. Das Nichterkennen der Kompromittierung ist zunehmend wichtiger als der permanente Systembesitz. Häufig bleibt ein Schädling nur im flüchtigen Speicher, ohne permanente Spuren in der Systemkonfiguration zu hinterlassen. Nach dem Neustart ist eine solche Malware vom System verschwunden. Die zukünftigen Integritätschecker müssen ihre Aktivitäten auf die Speicherinhalte ausweiten. Die Anti-Malware-Hersteller haben erkannt, dass sie dafür die Hardwareunterstützung benötigen. So führte z. B. Intel die sogenannte Intel® vPro^{TM}-Technologie ein (vgl. [int10]). Diese erlaubt die Ausführung eines schlanken für die Sicherheitsapplikationen optimierten Kernels (und selbstverständlich der entsprechenden Anti-Malware-Applikationen) in einem für das Betriebssystem nicht sichtbaren manipulationssicheren Bereich. Die auf dieser Technologie basierenden

[86] So wird z. B. ein Portscan an einem der von HIDS überwachten Systeme nicht unbedingt als ein Angriff interpretiert. Mehrere Meldungen über die von einem bestimmten System ausgehenden Portscans erhöhen die Wahrscheinlichkeit der korrekten Klassifizierung eines Angriffs.

[87] Zum Beispiel die früheren Versionen von Tripwire.

Sicherheitslösungen sind immun gegen die bei den heutigen Schädlingen häufig anzutreffende Strategie, zunächst die Anti-Malware-Scanner zu deaktivieren bzw. ihre Erkennungsergebnisse zu manipulieren. Ein auf der Intel® vPro^{TM}-Technologie basierendes integritätsprüfendes IDS hätte gute Voraussetzungen bei der Erkennung aktueller Schädlinge.

Netzwerkbasierte IDS (NIDS): Die *netzwerkbasierten IDS (NIDS)* werden i. d. R. an den Grenzübergängen zwischen Netzwerksegmenten eingesetzt und untersuchen Datenpakete in Echtzeit auf Unregelmäßigkeiten. Um diese Unregelmäßigkeiten festzustellen, können sowohl Angriffssignaturen als auch Heuristik angewendet werden. Dafür werden die Sensoren in den sogenannten Promiscuous Modus versetzt und analysieren sämtliche Datenpakete, die in einem Netzsegment auftreten. Die Sensoren von NIDS werden i. d. R. an den Monitoring Ports von Switches und Routern angeschlossen.
Die Sensoren können weitestgehend unabhängig von der vorhandenen Systemlandschaft eingesetzt werden, was den Installations- und Konfigurationsaufwand beträchtlich reduziert. Im Vergleich zu HIDS ist der Integrationsaufwand von NIDS wesentlich geringer, da die Installation von NIDS keine schwerwiegenden Eingriffe in die Systemkonfigurationen erfordert. Trotzdem haben NIDS auch folgende Nachteile:

- In jedem überwachten Netzwerksegment muss mindestens ein dedizierter Sensor installiert werden, welcher in einer geswitchten Umgebung an den SPAN-Port eines Switches angeschlossen wird. Selbstverständlich können die Uplink-Ports verwendet werden, um mehrere Netzwerksegmente zu einem größeren logischen Segment zusammenzuschließen. Die sich durch die Zusammenschaltung erhöhende Datenmenge kann aber schnell die Durchsatzkapazitäten eines SPAN-Ports und des daran angeschlossenen Intrusion-Detection-Systems übersteigen.

- Mit den steigenden Datenraten wird die Kommunikationsanalyse zunehmend schwieriger. Nur die wenigsten Netzwerkkarten können mehr als anderthalb Millionen Datenpakete pro Sekunde annehmen. Viele kleinere Datenpakete (z. B. von je 64 Bytes) überfordern jede IDS Gigabit-Lösung lange vor der Ausschöpfung der maximalen Bandbreite; die Versuche, IDS-Sensoren direkt auf Backbones mit hohem Datendurchsatz zu platzieren, bleiben meist erfolglos. Dies macht eine gründliche Planung vor der NIDS-Implementierung unabdingbar.

- Die innerhalb des Forschungsnetzes häufig eingesetzte Verschlüsselung verhindert eine sinnvolle Datenanalyse an vielen Stellen. Selbstverständlich könnte man die NIDS-Sensoren mit den kryptografischen Schlüsseln ausstatten; dies würde sie jedoch zu willkommenen Angriffspunkten machen und die Anzahl kritischer Systeme im Netz erhöhen. Wie im Fall der Netzbandbreite kann die Abhilfe durch eine durchdachte Sensorplatzierung geschaffen werden (s. a. Abschnitt C.3.11 „IDS-Technologie und -Einsatzszenario in einem medizinischen Forschungsnetz“).

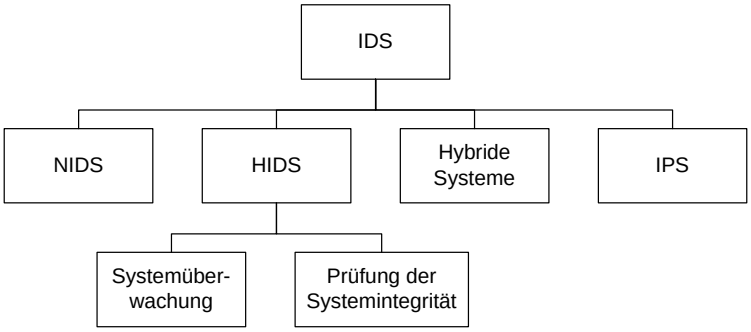

Abbildung 44.: Eine IDS-Taxonomie: Die beiden Basis-Technologien sind die hostbasierte und die netzwerkbasierte Intrusion-Erkennung. Die hybriden Systeme vereinen die Eigenschaften der beiden Technologien. Intrusion-Prevention-Systeme besitzen eine zusätzliche aktive Verhaltenskomponente.

Hybride IDS: In der Fachliteratur herrscht über den Begriff der hybriden IDS keine Einigkeit. Manche Autoren sehen in den hybriden IDS eine Teilmenge von netzwerkbasierten IDS, andere ordnen sie eher den hostbasierten IDS zu, dritte klassifizieren hybride IDS als einen selbstständigen IDS-Typ. Ein hybrides IDS wird unmittelbar auf dem zu schützenden System installiert und überwacht den Datenverkehr dieses Systems. Dabei kann es sich sowohl um Hardware- als auch um Softwarelösungen handeln. Der Einsatz eines Software-IDS kann sich negativ auf die Performance des zu schützenden Systems auswirken. Da die hybriden IDS lediglich den zu einem System gehörenden Datenverkehr untersuchen, sind sie meist weniger „leistungshungrig“ als die NIDS und können auch in Netzsegmenten mit hohem Datenaufkommen implementiert werden. Durch die unmittelbare Installation auf dem zu schützenden System können hybride IDS auch die in verschlüsselter Form übertragenen Daten problemlos auswerten.

Intrusion-Prevention-Systeme (IPS): Der Begriff des „Intrusion Prevention Systems“ (IPS) wurde ursprünglich von Marketingstrategen eingeführt, um den Absatz von IDS-Produkten ankurbeln. Tatsächlich handelt es sich bei IPS um Intrusion-Detection-Systeme, die über die reine Generierung von Warnmeldungen hinaus Funktionalitäten[88] bereithalten, die einen Angriff verhindern können. Eine der möglichen IDS-Taxonomien ist in der Abbildung 44 dargestellt (vgl. [NN01], [Gre03]).

C.3.11.3. Ein mögliches Szenario für den IDS-Einsatz

Auf der Basis der im Abschnitt 3.5 beschriebenen technischen Maßnahmen erscheint ein Einsatz der in der Abbildung 45 dargestellten IDS-Lösung als sinnvoll.

[88]So kann z. B. ein Inline-IPS im Alarmfall den Datenstrom verändern oder gar unterbrechen oder aber auch aktiv das Firewall-Regelwerk beeinflussen.

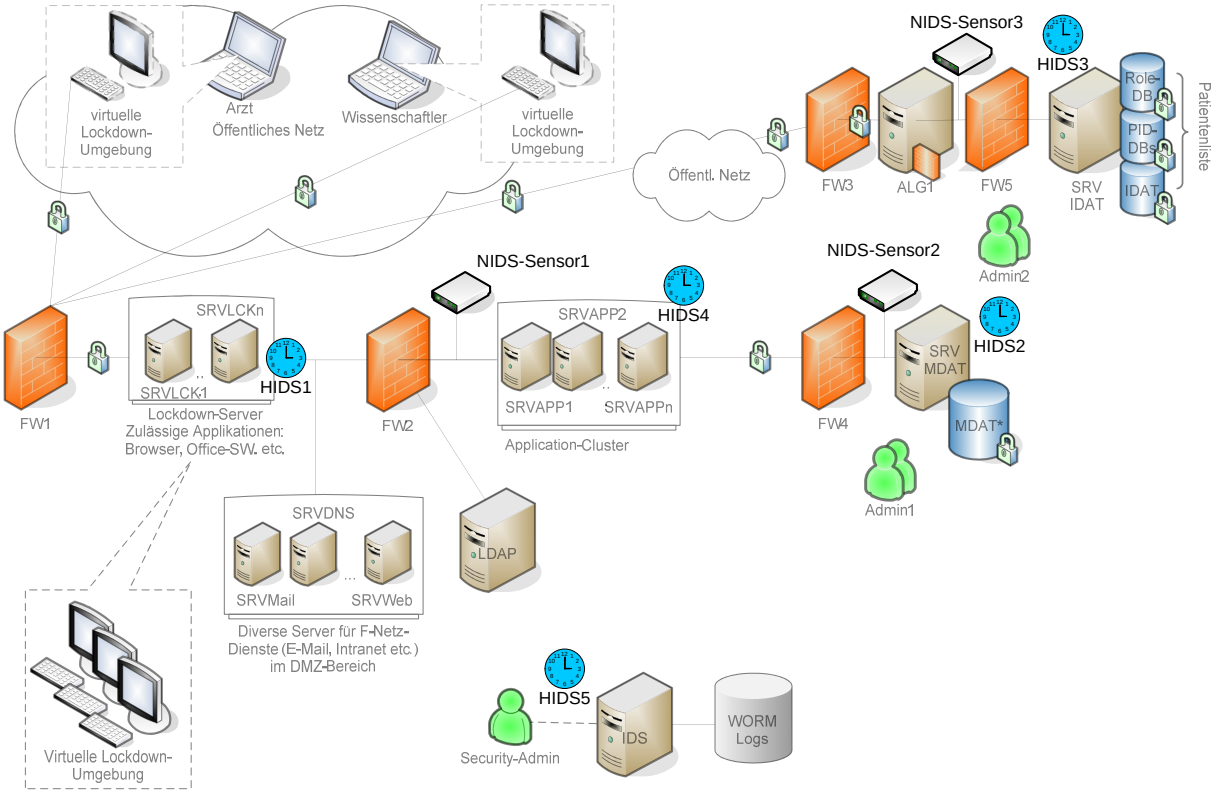

Abbildung 45.: Platzierungsmöglichkeiten für die IDS-Sensoren: Erst eine Kombination der netzwerk- und hostbasierten IDS-Technologien ermöglicht einen sinnvollen Schutz. Die Kommunikation der IDS-Komponenten soll verschlüsselt und nach Möglichkeit innerhalb eines dedizierten Netzwerksegments erfolgen.

IDS-Aufbau: Die von den IDS-Sensoren gesammelten und präparierten Daten werden an die zentrale IDS-Konsole geschickt, wo sie ausgewertet und auf ein WORM-Medium[89] in verschlüsselter Form geschrieben werden. Für die Übermittlung der IDS-Daten ist es ratsam, ein dediziertes Subnetz zu schaffen. Die Daten zwischen den IDS-Sensoren und dem IDS-Server dürfen ausschließlich in verschlüsselter Form übertragen werden.
Der IDS-Server selbst wird durch ein hostbasiertes IDS (HIDS5) geschützt, um die Integrität des kritischen Systems zu gewährleisten. Beim Einsatz einer virtualisierten (Citrix-ähnlichen) Laufzeitumgebung müssen die dafür zuständigen Server ebenfalls von einem HIDS (hier HIDS1) geschützt werden. Es ist davon abzuraten, dem HIDS1 Einfluss auf die Regelwerke von FW1 und FW2 zu gewähren. Die Regelwerke der beiden Firewalls sollen nur vom IDS-Server angepasst werden können, wobei unter der Anpassung nicht das automatische Eröffnen zusätzlicher Ports etc. zu verstehen ist, sondern die Möglichkeit, den Datenstrom zu unterbrechen. Die daraus resultierende erhöhte Gefahr für DoS muss in Kauf genommen werden, um das Forschungsnetz auch in Abwesenheit des Administrationspersonals zu schützen. NIDS-Sensor1 wird hinter der FW2 platziert, sodass die beim Sensor ankommenden Daten nicht verschlüsselt sind. Dies macht eine sinnvolle Datenauswertung möglich.

[89] Hier sind physikalische WORM-Medien gemeint. Beim Einsatz von softwarebasierten WORM-Lösungen müssen höhere Unsicherheiten in Kauf genommen werden.

Das eigentliche „Herz“ des Forschungsnetzes, der Applikationsserver, sollte von HIDS4 geschützt werden. Der Server mit der Patientenliste und der MDAT-Server sollen ebenfalls durch zwei hostbasierte ID-Systeme (HIDS2 und HIDS3) überwacht werden. Hinter den Firewall FW4 und dem Application Gateway ALG1 sollen außerdem zwei NIDS-Sensoren (NIDS-Sensor2 und NIDS-Sensor3) platziert werden. Zudem sollen HIDS2 und HIDS3 in der Lage sein, die Regelwerke der FW3, FW4 und FW5 so zu verändern, dass keine Datenkommunikation bis zum Einschreiten des Security-Administrators stattfindet.

C.3.12. Aspekte der Protokollierung und des Monitorings in medizinischen Forschungsnetzen

C.3.12.1. Verfahrens- und Systemüberwachung

Die Erfassung von Systemdaten und administrativen Transaktionen gehört zu der Systemüberwachung. Folgende Systemaktionen sollen in einem medizinischen Forschungsnetz überwacht werden:

- Die *Erzeugung von Benutzern und Berechtigungsvergabe* soll sowohl systemgesteuert als auch manuell protokolliert werden. Die systemgesteuerte Protokollierung kann z. B. auf der Basis von Aufzeichnungen des Identitätsmanagementsystems erfolgen und wird durch die manuellen Aufzeichnungen vervollständigt (s. a. Abschnitt 3.3.2 „Personale Aspekte für den Betrieb von Forschungsnetzen“).

- Die *Änderung der Systemkonfiguration* kann sowohl als automatische Aktualisierung als auch aufgrund von manuell durchzuführenden administrativen Maßnahmen erfolgen. Manche manuellen administrativen Eingriffe (z. B. Konfiguration eines neuen Systems oder Systemwiederherstellung nach einem Hardwareausfall) lassen sich kaum automatisch erfassen. Eine ausführliche manuell geführte Dokumentation soll diese Dokumentationslücke schließen. Die administrativen Transaktionen müssen grundsätzlich aufgezeichnet werden. Der dadurch entstehende Verwaltungsmehraufwand muss in Kauf genommen werden.

- Auf eine sorgfältige Protokollierung aller *Datensicherungs- und Datenwiederherstellungstransaktionen* muss geachtet werden. Dies ist die Voraussetzung für eine problemlose Datenwiederherstellung in einem Ernstfall und sorgt dafür, dass die Datensicherungen nicht zum Ausspähen von Informationen missbraucht werden. So dürfen z. B. die Sicherungsbänder[90] nur von einem engen Personenkreis unter Beachtung des Vier-Augen-Prinzips nachbestellt werden. Der Vorgang muss auf beiden Seiten[91] protokolliert werden. In regelmäßigen Zeitabständen müssen die Protokolldateien der beiden Parteien auf Unstimmigkeiten geprüft werden.

[90] Grundsätzlich sollte die Aufbewahrung der Sicherungsbänder bei einem unabhängigen Drittunternehmen erfolgen.

[91] Bänderaufbewahrung und -anforderung.

- Die Sicherheitspolicy des Forschungsnetzes definiert zulässige und unzulässige Benutzertransaktionen. Alle *unzulässigen Benutzeraktivitäten und Befugnisüberschreitungen* sind zu protokollieren. Alle feststellbaren Abweichungen vom Normalzustand sollen aufgezeichnet werden.

- Die *Anonymisierung bzw. Pseudonymisierung* von Forschungsnetzdaten gehört ebenfalls zu den Systemtransaktionen und muss überwacht werden.

- Die *Depseudonymisierung* von Patienteninformationen ist als ein besonderer Vorgang innerhalb des Forschungsnetzes zu sehen. Es ist zwischen zwei Arten der Depseudonymisierung in medizinischen Forschungsnetzen zu unterscheiden: Depseudonymisierung auf Regelbasis und Depseudonymisierung in Einzelfällen (vgl. [RDSP06]).

  – Bei der automatischen Depseudonymisierung von Patientendaten zwecks Qualitätssicherung wird *PSN* in *PID* überführt. Der automatische Vorgang wird von Systembetreuern im Auftrag des Ausschusses Datenschutz gestartet. Dabei reicht eine automatische Systemprotokollierung aus, wobei die depseudonymisierten Patientendatensätze (ihre identifizierenden Informationen) festgehalten werden müssen.

  – Die Depseudonymisierung aufgrund einer Patientenauskunft liefert das zu einem *PID* zugewiesene *PSN* mit den dazu gehörenden medizinischen Daten. Für den an diesem Vorgang beteiligten Pseudonymisierungsdienst ist die $PID \rightarrow PSN$-Umwandlung nicht von einer gewöhnlichen *PSN*-Anfrage zu unterscheiden. Die Anfrage nach den medizinischen Daten darf nur bei der vorliegenden Genehmigung vom Ausschuss Datenschutz erfolgen, der den Vorgang dokumentieren muss. Auch bei allen anderen Depseudonymisierungsanfragen (z. B. Beteiligung von Patienten an den Forschungsergebnissen) ist die Involvierung des Ausschusses Datenschutz unabdingbar). Die Vertreter des Datenschutz-Ausschusses und die auszuführende Partei haben die Vorgänge zu protokollieren und die Protokolleinträge in regelmäßigen Zeitabständen abzugleichen. Der Abgleich kann durch die Vereinbarung eines standardisierten Datensatzes für den Aufbau einer Abfrage automatisiert werden, sodass die Überprüfung vollautomatisch und zeitnah erfolgen kann.

Auch manche nicht administrativen Aktionen müssen der Überwachung und Aufzeichnung unterliegen:

- Die *Neueingabe und die Änderung von Patienteninformationen* müssen aufgezeichnet werden.

- Die *Anonymisierung* von Patientendaten und die *Löschung* von Informationen müssen ebenfalls protokolliert werden. Manche dieser Operationen erfolgen aufgrund einer Anweisung seitens des Ausschusses Datenschutz, andere automatisch (z. B. aufgrund von gesetzlichen Bestimmungen über Aufbewahrungsfristen für Personendaten).

- Auch die *Abfragen* der Forschungsnetzteilnehmer müssen protokolliert werden. Die Anzahl und die Art der an einen Forscher weitergegebenen Datensätze muss festgehalten werden. Einem Forscher werden nur die für ihn relevanten Teile der Datensätze zur Verfügung gestellt. Dabei kann auf die ressourcenintensive Speicherung der an einen Forscher weitergegebenen Daten verzichtet werden. Vielmehr reichen die Kenntnis über die Art der durchgeführten Abfrage sowie die Kenntnis über den Datenbankzustand aus, um die Ergebnisse dieser Abfrage reproduzieren zu können.

C.3.12.2. Aufbewahrungsfristen für Protokolldaten

Laut [bsi11d] sollte die Aufbewahrung von Protokolldaten die Dauer von einem Jahr nicht überschreiten; für gezielte Kontrollen empfiehlt man gar kürzere Speicherungsfristen. Protokolldaten werden zwangsläufig einen Anteil von medizinischen Daten enthalten, für die es eine Reihe vielfältiger Regelungen, jedoch keine eindeutige gibt. Eine umfassende Auseinandersetzung mit Speicherungsfristen für medizinische Daten ist unter [Sem05] zu finden. Danach ist die empfohlene Speicherungsdauer von der Art und Zusammenhang der Datengewinnung abhängig und kann bis zu 100 Jahre betragen.[92]
In vielen Fällen sind mehrere gesetzliche Regelungen zutreffend, sodass die Dauer der Aufbewahrung zu einer Auslegungssache wird. In dieser Arbeit wird die Meinung vertreten, dass die Aufbewahrungsdauer von Protokolldaten nach dem Maßstab ihrer Erforderlichkeit zur Aufgabenerfüllung bemessen werden muss. Da die in diesem Abschnitt beschriebenen Protokolldaten primär zur potenziellen Aufklärung von potenziellen Straftaten benötigt werden, dürfte hiernach die Aufbewahrungszeit für Protokolle die Verjährungsfristen von Straftaten nach StGB nicht unterschreiten.[93] Man kann die Aufbewahrungspflicht für Protokolldaten jedoch auch mit der für eine medizinische Behandlung obligatorischen Dokumentationspflicht verbunden sehen. Danach gibt es eine breite Spanne von Aufbewahrungszeiträumen: zwischen zehn Jahren bei einer ambulanten Behandlung und 30 Jahren für die Röntgenaufzeichnungen (nach der letzten Behandlung). Unter der Berücksichtigung der regelmäßigen Verjährungsfrist von 30 Jahren (§ 195 BGB) und unter Beachtung der Dreijahresfrist für den Herausgabeanspruch nach dem Verjährungseintritt (§ 852 BGB) errechnet man eine Aufbewahrungszeit für Protokolldaten von mindestens 33 Jahren. Wenn man den Verjährungsansatz weiter verfolgt, wird man feststellen, dass für Mord und Totschlag keine Verjährung eintritt (§ 78 StGB). Die mit solchen Fällen potenziell

[92] Zum Beispiel 100 Jahre nach StGB, 30 Jahre nach §§ 195, 199, 852 BGB, § 28 Abs. 3 RöV, zehn bzw. sechs Jahre nach AO, HGB, GoBS, GDPdU etc.

[93] In diesem Zusammenhang ist die sogenannte Verfolgungsverjährung relevant. Unter diesem Begriff wird die Zeitdauer verstanden, nach der ein Delikt nicht mehr verfolgt wird. Bei dem für Forschungsnetze relevanten Ausspähen von Daten (§ 202a StGB) beispielsweise betragen die Verjährungsfristen bis zu drei Jahren. Im Falle des Computerbetrugs (§ 263a StGB) sind es gar fünf Jahre. Die für ein Forschungsnetz relevanten Verbrechen sind im Abschnitt 4.3 „Qualitative Bewertung der Bedrohungs- und Risikosituation“ aufgelistet.

in Verbindung stehende Dokumentation müsste danach dauerhaft aufbewahrt werden (vgl. [HSD05]).

C.3.12.3. Rahmenbedingungen

Der erfolgreiche Einsatz von Protokollierung und Monitoring hängt von den folgenden Rahmenbedingungen ab:

- Die Zwangsläufigkeit, die Vollständigkeit und die Integrität von Protokollen sind zu gewährleisten.
- Kritische Kontrollen müssen nach dem Vier-Augen-Prinzip erfolgen. Die Korrektheit der Archivierungsvorgänge muss regelmäßig verifiziert werden. Beim Feststellen von Fehlern auf einem Archivmedium müssen die betroffenen Daten mithilfe des Backups wiederhergestellt werden. Die fehlerhaften Backup-Daten sind zu löschen bzw. bei einmalig beschreibbaren Datenträgern sind die Medien selbst zu vernichten.
- Um den Kontrollaufwand in Grenzen zu halten, sind automatisierte Verfahren für Routine-Kontrollen einzurichten.
- Maßnahmen/Konsequenzen bei Regelverstößen müssen vorab definiert werden.
- Eine zeitnahe Durchführung von Kontrollen kann Schäden mindern bzw. abwenden.
- Auf Basis der obigen Erkenntnisse muss ein Revisionskonzept erstellt werden, das regelmäßig erprobt und angepasst wird.

C.3.12.4. Watermarking

Bei einigen forschungsrelevanten Daten kann der Personenbezug nicht vollständig entfernt werden. Im Falle einer unzulässigen Nutzung dieser Daten könnte die Notwendigkeit entstehen, den Datenursprung festzustellen. Nicht alle Formen der unerwünschten Verbreitung von Forschungsnetzdaten können festgehalten werden. So ist es beispielsweise beinahe unmöglich, nachträglich festzustellen, von wem die Informationen aus der Patientenakte veröffentlicht wurden, solange es sich um Textdaten handelt. Die sogenannte analoge Lücke lässt sich bei Textinformationen nicht schließen.[94] Bei Bild-, Video- und Toninformationen kann dagegen das „Watermarking“-Verfahren eingesetzt werden (vgl. [Ste06], [Leh04]), um die unberechtigte Weitergabe vom Material nachträglich untersuchen zu können.
Das Watermarking-Prinzip ist nicht neu und entspricht dem seit Jahrtausenden bekannten Steganografie-Ansatz. Die digitalen Wasserzeichen beinhalten nicht wahrnehmbare Informationen, die dem Ton-, Video- oder Bildmaterial hinzugefügt werden.[95] Zusätzlich zur

[94] Das auf den ersten Blick sinnvolle Integrieren von präparierten Datensätzen in die Abfrageresultate ist nur in wenigen Fällen denkbar und kann z. B. Forschungsergebnisse verfälschen.

[95] Information Hiding.

Übertragungskontrolle lassen sich die digitalen Wasserzeichen für die Integritätsnachweise verwenden. Der Vorteil von digitalen Wasserzeichen im Gegensatz zu den Hashwerten besteht darin, dass ein Hashwert lediglich die Aussage ermöglicht, ob die Ursprungsdatei verändert wurde oder nicht; mithilfe des Watermarking kann man feststellen, welche Veränderungen am Ursprungsmaterial statt gefunden haben (vgl. [Ste06]). Außerdem überstehen die digitalen Wasserzeichen die Änderung der Speicherungsart (z. B. Abspeichern im neuen Dateiformat) und sogar die analoge Umwandlung (z. B. Abfilmen, Ausdrucken etc.). Sollten digitale Wasserzeichen in einem Forschungsnetz ihre Anwendung finden, so ist auf folgende Eigenschaften der eingesetzten Verfahren zu achten:

- *Sicherheit:* Widerstandsfähigkeit gegen gezielte Angriffe gegen das Wasserzeichen.
- *Robustheit:* Resistenz gegenüber (willkürlichen) Modifikationen wie z. B. Größenänderung, Zuschneiden oder (verlustbehaftete) Kompression bzw. die Wiederaufnahme des Materials von einer analogen Vorlage.
- *Wahrnehmbarkeit* (Sichtbarkeit, Hörbarkeit etc.) des Wasserzeichens für den menschlichen Wahrnehmungsapparat.
- *Detektierbarkeit* des Wasserzeichens z. B. mithilfe diverser statistischer Analyseverfahren.[96]
- *Kombinierbarkeit* mit anderen Verfahren.
- *Invertierbarkeit:* Unter Invertierbarkeit versteht man die Detektierbarkeit der Reihenfolge, in der mehrere kombinierbare Wasserzeichen(methoden) angewendet wurden. Bei robusten kombinierbaren Verfahren kann die Reihenfolge der Aufbringung von mehreren Wasserzeichen nicht festgestellt werden; die Herkunft (Authentizität) des Materials wäre somit nicht eindeutig identifizierbar.
- *Komplexität* bezeichnet den für die Aufbringung bzw. Extrahierung der Wasserzeichen benötigten Rechenaufwand.
- *Kapazität* beschreibt die Informationsmenge, die mithilfe des Verfahrens in einen Abschnitt des Mediums integriert werden kann.

Für den Einsatz in den medizinischen Forschungsnetzen können sich unsichtbare nicht wahrnehmbare Verfahren eignen. Die Verwendung von Watermarks darf die behandlungs- und forschungsrelevanten Informationen nicht verfälschen. Zusätzlich können sogenannte adaptive Verfahren eingesetzt werden. Dabei werden nur die medizinisch irrelevanten Inhalte mit einem Watermark versehen. So kann man z. B. Watermarks bei Bildern

[96] Zum Beispiel Analyse des Bild- oder Tonrauschens.

im Bildhintergrund unterbringen, damit die eigentlichen Bildinhalte unverändert bleiben (vgl. [Leh04]). Angesichts der heutzutage verfügbaren Rechenkapazitäten ist die Komplexität der eingesetzten Verfahren vernachlässigbar. Von der wasserzeichenbasierten Filterung des Forschungsnetzmaterials an einer zentralen Stelle wird abgeraten, da diese durch Verschlüsselung ausgehebelt werden kann. Die Kapazität des gewählten Verfahrens sollte vom Einsatzzweck abhängen: Sollte das Verfahren lediglich die Beziehung des Bildes zum Forschungsnetz belegen, ist ein robustes Verfahren mit geringer Kapazität sinnvoller als ein Verfahren mit hoher Kapazität, das z. B. eingesetzt werden kann, um Patienteninformationen im Medium abzulegen. Außerdem könnte die Kombination eines fragilen mit einem robusten Verfahren für den praktischen Forschungsnetzeinsatz einen Mehrwert ergeben. Das robuste Wasserzeichen würde die Authentizität und das fragile die Integrität des Materials sichern. Zusätzlich zur Integritätssicherung können durch die digitalen Wasserzeichen Modifikationen an einzelnen Bereichen/Abschnitten des Materials kenntlich gemacht werden. Dies könnte z. B. bei verlustbehafteten Änderungen Schlüsse darüber zulassen, ob behandlungs- oder forschungsrelevante Inhalte modifiziert wurden (vgl. [Leh04]).

C.3.12.5. Zeitstempeldienst

Bei der Ereignisprotokollierung ist die genaue Bestimmung des Durchführungszeitpunktes einer Transaktion wichtig. So kann beispielsweise der Ausführer einer Transaktion behaupten, dass seine Login-Daten bereits vor der Transaktionsausführung kompromittiert wurden oder die Protokolldaten fingiert (rückdatiert) sind. Ein Zeitstempeldienst kann für die Klärung von Fragestellungen dieser Art eingesetzt werden. Generell wird der Zeitstempeldienst verwendet, um die Existenz von Daten bzw. den Dateninhalt zu einem bestimmten Zeitpunkt zu beweisen. Man schickt dazu den Hashwert der zu stempelnden Daten an eine vertrauenswürdige Partei,[97] die ihrerseits die aktuelle Uhrzeit mithilfe einer präzisen Zeitmessung ermittelt und das Gebilde aus Daten und Uhrzeit mit dem eigenen privaten Schlüssel signiert. Eine Weiterentwicklung des Zeitstempeldienstes ist der elektronische Notardienst. Der maßgebliche Unterschied zwischen dem Zeitstempel- und dem Notardienst besteht in der Kenntnis des Notardienstes über die Dateninhalte und über die Identität des Antragstellers, der die Daten zu Unterzeichnung vorlegt. Dies ist nur ein Teil des Aufgabenfeldes eines realen Notars, denn ein Notar stellt zusätzlich sicher, dass das vorliegende Dokument freiwillig unterschrieben wird, und der Unterzeichner über die Konsequenzen seines Handelns informiert ist.
Die zwischenmenschlichen Faktoren wie Freiwilligkeit des Handelns und Kenntnisse über die mit der Unterzeichnung des Dokuments verbundenen Konsequenzen kann ein elektronischer Notardienst nicht berücksichtigen. Es kann vor Notardienst nicht verlangt werden, dass er über die genauen Inhalte des Dokuments Kenntnis hat, denn die Daten können in einem

[97] Sogenannte Time Stamping Authority (TSA).

dem Notardienst unbekannten Format vorliegen. Auch die automatische Datenauswertung bei bekannten Datenformaten ist nicht immer möglich. Somit können die Aufklärungs- und Belehrungspflicht eines Notars vom elektronischen Notardienst kaum erfüllt werden. Auch bezüglich der Implementierung der Notarfunktionen in Form eines elektronischen Dienstes existieren mehrere Auslegungen. In dieser Arbeit wird die Auffassung vertreten, dass die Identität des Absenders durch das Unterschreiben des Dokuments durch den Absender mithilfe seines privaten Schlüssels überprüft werden soll.
Trotz der oben erwähnten Einschränkungen könnte der Einsatz des Notardienstes im Bereich der Forschungsnetze anstelle des Zeitstempeldienstes vorteilhaft sein. Die Vorteile sind die eindeutige Bestimmung der Anforderer-Identität und die zusätzliche Sicherheit bei der Hash-Erzeugung. So wählt z. B. beim Zeitstempeldienst der Anforderer selbst das verwendete Hash-Verfahren,[98] das u. U. einen unsicheren Hashwert erzeugen kann. Der Angreifer könnte absichtlich ein wenig sicheres Verfahren für die Hash-Generierung auswählen und später versuchen, Daten zu erzeugen, die in Verbindung mit einer bestimmten Zeitangabe den gleichen Hashwert ergeben. Die einheitliche Hash-Erzeugung durch den Notardienst schafft somit zusätzliche Sicherheit.
Die Verwendung von Zeitstempel- bzw. Notardiensten ist zur Sicherung aller sicherheitsrelevanten Transaktionen auf einem nicht wiederbeschreibbaren Medium empfehlenswert. Die Zertifikatszuweisung an die teilnehmenden Systeme ist die Voraussetzung für eine zuverlässige Transaktionszuordnung. Die eingesetzten Hash- und Verschlüsselungsverfahren müssen stets auf ihre aktuelle Sicherheitseinstufung geprüft werden. Es ist empfehlenswert, die Signaturschlüssel der Dienste mindestens ein Mal im Jahr zu aktualisieren. Zusätzliche Sicherheit kann durch die strenge Reglementierung des Aufbaus der zu signierenden Daten erreicht werden. Ein fest definierter Datensatzaufbau für Logging-Informationen erschwert die Erzeugung von Datensätzen mit identischen Hashwerten.
Auch wenn nur die Hashwerte bzw. die verschlüsselten Daten signiert werden, ist es nicht empfehlenswert, den Notar- oder Zeitstempeldienst einer Drittpartei zu verwenden. Bei einer größeren zu signierenden Datenmenge können außerdem durch die forschungsnetzinterne Platzierung des Dienstes Performancevorteile erzielt werden. Der in die Forschungsnetzinfrastruktur integrierte Zeitstempeldienst müsste jedoch von einer unabhängigen Partei gewartet werden; das Administrationspersonal des Forschungsnetzes darf keinen administrativen Zugang zu den Komponenten des Zeitstempeldienstes erhalten (vgl. [NDJ01], [BP01], [ACPZ01]).

[98] Das Hash-Verfahren und die verwendete Schlüssellänge müssen vom Zeitstempeldienst akzeptiert werden.

C.4. Die Bedeutung der Einhaltung von Sicherheitsrichtlinien

Oft können nicht alle als notwendig identifizierten Sicherheitsrichtlinien gleichzeitig oder zeitnah umgesetzt werden. Die Gründe dafür können vielfältig sein. Eine objektive Abschätzung der Konsequenzen bei Nichteinhaltung von Sicherheitsrichtlinien ist von entscheidender Bedeutung. Dafür ist eine Risikoanalyse durchzuführen, bei der die negativen Folgen der Nichteinhaltung begutachtet werden sollen. Insbesondere muss der negative Einfluss auf die Forschungsnetzdienste im Hinblick auf die Einhaltung von Sicherheitskriterien[99] geklärt werden. Ein dafür zuständiges Gremium[100] muss die Ausnahmeanträge bzw. -meldungen bewerten und ggf. genehmigen. Aufgrund des schnellen technischen Progresses empfiehlt es sich, die Genehmigungen nur für eine begrenzte Zeit zu erteilen (z. B. für die Dauer von 18 Monaten). Nach dem Ablauf dieser Zeit ist eine erneute Überprüfung der Zulässigkeit der Ausnahmeregelung durchzuführen.

Schutzprofile Die Sicherheit der im Forschungsbetrieb eingesetzten Komponenten muss gemessen werden können. Dies kann durch die Evaluation der Systeme im Hinblick auf ihre Vertrauenswürdigkeit erfolgen. Vertrauenswürdig heißt, auf eine sichere und vorhersagbare Weise arbeiten zu können. Die Evaluierung stellt nicht fest, ob ein bestimmtes Produkt sicher ist, sondern überprüft die in den Entwicklungs- und Testphasen des Produktes eingesetzten Erstellungs- und Systemdesignverfahren und leitet deren Vertrauenswürdigkeit daraus ab.
Systemsicherheit kann auf einer Vielzahl von Weisen bewertet werden. Neben einer unüberschaubaren Menge von mehr oder weniger systematischen und z. T. proprietären Ansätzen existieren international akzeptierte Evaluationskriterien-Kataloge (CC[101], ITSEC, TCSEC etc.). Diverse Nachteile in TCSEC und ITSEC führten dazu, dass die beiden Kataloge in einem neuen Standard, dem CC aufgingen und später als internationaler Standard ISO/IEC 15408 veröffentlicht wurden.
Eine Beschreibung des Aufbaus der Evaluationskriterien-Kataloge ist nicht das Ziel dieses Abschnitts. Die Inhalte der Kataloge samt geschichtlichen Informationen werden in der weiterführenden Literatur ausführlich dargelegt (vgl. [bsi11c], [bsi09b], [MH07], [Mac98]). Stattdessen soll im Folgenden auf einen Teil der CC – die Schutzprofile – bzw. auf ihre potenziellen Verwendungsmöglichkeiten für die Informationssicherheit in der medizinischen Forschungsnetzinfrastruktur eingegangen werden.

[99] Integrität, Konformität, Robustheit, Verbindlichkeit, Verfügbarkeit und Vertraulichkeit.

[100] Zum Beispiel der Ausschuss Datenschutz.

[101] Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria for Information Technology Security Evaluation (CC)).

Schutzprofile sind Funktions- und Vertrauenswürdigkeitsanforderungen an eine bestimmte Produktkategorie, die spezifische Benutzerwünsche erfüllt. Die Schutzprofile können von den Software- und Hardwareherstellern formuliert werden. Die praktische Relevanz von Schutzprofilen für die Informationssicherheit im Gesundheitswesen wurde in [Vat11] untersucht. Auch Forschungsnetze können dadurch ihren Bedarf für eine bisher nicht existierende Sicherheitslösung beschreiben. Im Abschnitt 3.5.9 „Antimalware-Einrichtungen“ wurden die Anforderungen an ein IAM-System definiert. Da ein solches System eine Vielzahl von den bereits vorhandenen Infrastrukturbestandteilen und Forschungsnetzspezifika berücksichtigen muss, wäre die Zusammenfassung der Anforderungen an ein IAM-System eine geeignete Einsatzmöglichkeit für ein Schutzprofil. Auch die Anforderungen an eine sichere Arbeitsumgebung (s. a. Abschnitte 3.5.1 „Sichere Arbeitsumgebung“ und 3.5.5 „Zugangsszenarien von Netzteilnehmern zu den Forschungsnetzdiensten“) sowie die spezifischen Anforderungen an die Monitoring-Einrichtungen (s. a. Abschnitt 3.5.12 „Monitoring und Protokollierung“) könnten als Schutzprofile sinnvoll beschrieben werden. Bei der Schutzprofilerstellung werden die sogenannten Sicherheitsziele gesetzt, die die Spezifikation eines Produkts sowie die angestrebten Funktions- und Vertrauenswürdigkeitskriterien erläutern (vlg. a. [bsi08e]).
In Common Criteria werden zwei Arten von Sicherheitsanforderungen definiert: Funktionalität und Verlässlichkeit. Unter der Funktionalität ist das sicherheitsrelevante Verhalten des Produkts (Schutzniveau) zu verstehen. Die Verlässlichkeit steht für die Vertrauenswürdigkeit des Produktes in Bezug auf die Einhaltung der Anforderungen, die Zielerreichung und die Korrektheit der Implementierung. Auf der Basis der funktionalen und der verlässlichkeitsbezogenen Anforderungen werden die sogenannten Vertrauensstufen (EAL) gebildet.[102] Den Prozess der EAL-Zuweisung stellt die Abbildung 46 grafisch dar.

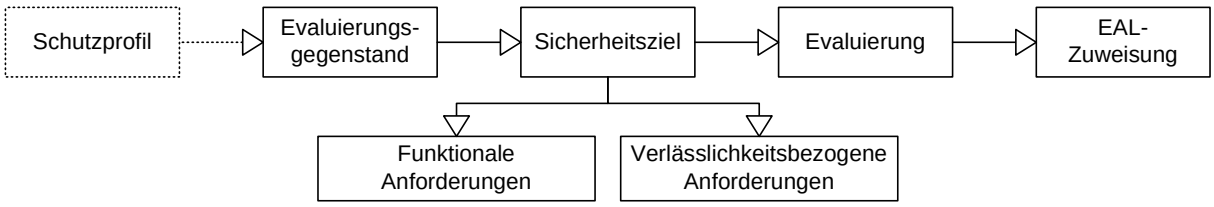

Abbildung 46.: Prozess der EAL-Zuweisung: Funktionalität und Verlässlichkeit sind zwei Arten von Sicherheitsanforderungen. Auf ihrer Basis werden die Vertrauensstufen (EAL) gebildet.

Auf der Basis der Schutzprofile kann eine Zertifizierung vorgenommen werden. Das Vorhandensein eines Schutzprofils ist jedoch keine obligatorische Voraussetzung für die Zertifizierung. Bei der Entscheidung für oder gegen eine Evaluierung für eine oder mehrere im Forschungsnetz eingesetzte Komponenten muss zuerst die evtl. gesetzlich oder vertraglich festgelegte Notwendigkeit untersucht werden. Da die Zertifizierung ein relativ

[102] CC sieht die Aufteilung in sieben Stufen von EAL1 (funktionell getestet) bis EAL7 (formal verifizierter Entwurf und getestet) vor.

aufwendiger Prozess ist, stellt sich die Frage, ob diese in allen Situationen, gemessen an der Bedrohungslage, der Art der Daten und der Rolle des zu evaluierenden Systems für die Forschungsnetzsicherheit, sinnvoll erscheint. Wenn keine die Vertrauenswürdigkeitsstufe bestimmenden gesetzlichen oder vertraglichen Anforderungen bei der Evaluierung des Produktes berücksichtigt werden müssen, wird die Vertrauenswürdigkeitsstufe in Abhängigkeit von den Evaluierungszielen festgelegt. Das erklärte Ziel einer Evaluierung besteht i. d. R. in der Erzielung eines erforderlichen Vertrauenswürdigkeitsgrades mit dem geringsten Aufwand. Höhere Evaluierungsstufen bedingen einen größeren Umfang der zu evaluierenden Funktionen und eine erhebliche Testtiefe, was in einem erhöhten Evaluationsaufwand resultiert.
Forschungsnetze können mithilfe von Schutzprofilen ihre eigenen Informationssicherheitsbedürfnisse und Sicherheitsstandards neben den Software- und Hardwareherstellern definieren. Es ist vorteilhaft, dass die Schutzprofile produktunabhängig erstellt werden können. Durch die Zusammenfassung der Funktions- und Vertrauenswürdigkeitsanforderungen wird ein großer Teil der Sicherheitsziele vollständig abgedeckt. Schutzprofile können als ein an ein konkretes Informationssicherheitsproblem orientiertes Bündel von Informationssicherheitskriterien verstanden werden. Die technische Stimmigkeit, Konsistenz und Vollständigkeit der Schutzprofile können in einem Evaluationsprozess nachgewiesen werden. Ein evaluiertes Schutzprofil kann als Grundlage für die Sicherheitsvorgaben an eine (spätere) Implementierung eines konkreten Produkts[103] dienen.
Der Informationsumfang von Schutzprofilen übersteigt jedoch die Inhalte eines Sicherheitsanforderungskatalogs. Vielmehr sind die Schutzprofile als ein flexibles Instrument zu verstehen, das die Vollständigkeit und die Widerspruchsfreiheit von Informationen durch eine Vielzahl von Hintergrund- und Zusatzinformationen in Form einer Abhängigkeitsliste unterstützt. Der Aufbau eines Schutzprofils ist in der Abbildung 47 grafisch dargestellt (vgl. [bsi11c], [bsi09a]).

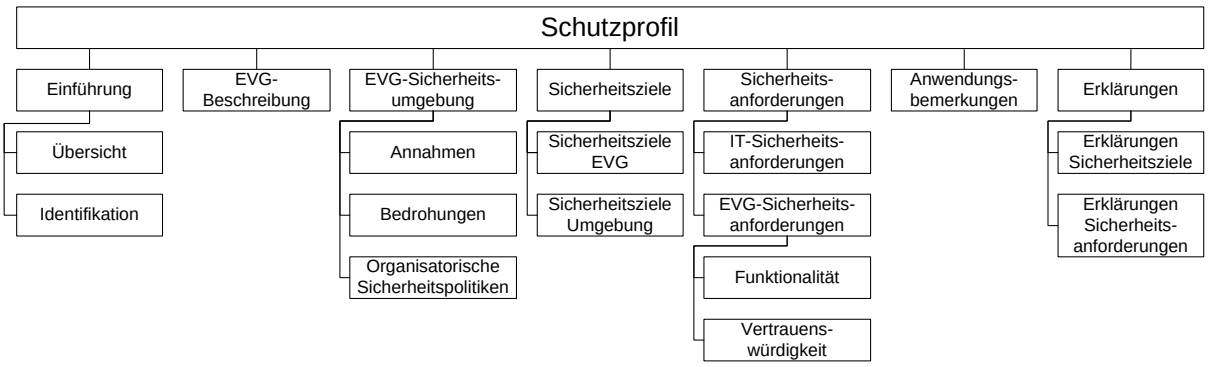

Abbildung 47.: Aufbau eines Schutzprofils: Mithilfe von Schutzprofilen können Forschungsnetze ihre eigenen produktunabhängigen Informationssicherheitsbedürfnisse und Sicherheitsstandards definieren.

Zusätzlich umfasst ein Schutzprofil eine Beschreibung der zu erwartenden Einsatzum-

[103] Zum Beispiel eines forschungsnetzeigenen IAM-Systems.

gebung für das Produkt und die Zielsetzungen dessen Nutzung. Auch die gesetzlichen Anforderungen (s. a. Abschnitte 3.1, 3.2) und die maßgeblichen Sicherheitsstandards (vgl. [DC06], [RDSP06], [SPR+06]) sowie Teile der Beschreibung der Bedrohungslage (s. a. Abschnitt 4.3) können sich in einem Schutzprofil wiederfinden.
Die vollständige Erfüllung der Sicherheitsziele durch die Spezifikation der Anforderungen an die Vertrauenswürdigkeit und an die Funktionalität ist das erklärte Ziel bei der Erstellung von Schutzprofilen. Das Vorhandensein eines Schutzprofils ist für die Evaluation nicht zwingend erforderlich. Die Erzeugung eines Schutzprofils ist jedoch aufgrund der Reduzierung des Aufwands bei einer Evaluierung empfehlenswert. Außerdem ermöglicht eine auf der Basis des gleichen Schutzprofils erfolgende Evaluation unterschiedlicher Produkte eine bessere Vergleichbarkeit. Durch die Darlegung der Sicherheitsanforderungen könnte man die existierenden Bedrohungen berücksichtigen und die Sicherheitspolitik eines Forschungsnetzes zielgerichtet umsetzen. Die funktionalen Sicherheitsanforderungen spiegeln sich in konkreten Sicherheitsfunktionen wider, da eine funktionale Anforderung durch mindestens eine Sicherheitsfunktion erfüllt werden muss. Die Sicherheitsfunktionen erfüllen ihrerseits mindestens eine Sicherheitsanforderung.
Die vorliegende Arbeit kann als Basis für die Erstellung der für den Forschungsnetzbetrieb notwendigen Schutzprofile dienen, wobei die vor der Schutzprofilerstellung erfolgende Bestimmung der Sicherheitspolitik sowie die Sicherheitsziele die Notwendigkeit für die Definition bestimmter Schutzprofile vorgeben. Die Schutzprofile bestimmen ihrerseits die Kerndaten zu den Risiken und der Angreiferstruktur und tragen dadurch zu einem zielgerichteten S&R-Management sowie zu einer optimierten Ressourcennutzung bei. Um zu veranschaulichen, dass ein gezieltes S&R-Management nicht ausschließlich durch Schutzprofile stattfinden kann, erfolgt in der Abbildung 48 eine Gegenüberstellung des Umfangs der Schutzprofile und der hierarchischen Dimension des generischen S&R-Pyramidenmodells nach Klaus-Rainer Müller [Mül11] (s. a. Abschnitt C.5), das alle Ebenen des S&R-Managements abdeckt.

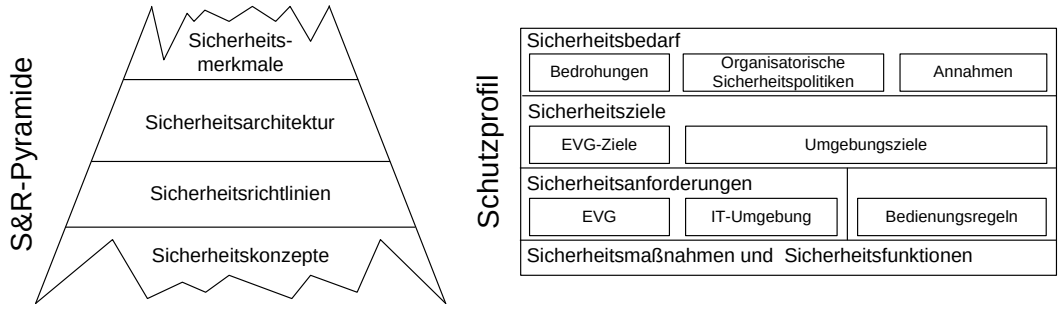

Abbildung 48.: Gegenüberstellung der Schutzprofile und des Konzeptes der Sicherheits- und Risikomanagementpyramide: Schutzprofile sind ein flexibles Sicherheitsinstrument und können als Bestandteile eines zielgerichteten Sicherheits- und Risikomanagements in das Sicherheitskonzept von Forschungsnetzen integriert werden.

Auffallend ist, dass die essenziellen Bestandteile des Sicherheits- und Risikomanagements nach der S&R-Pyramide „Sicherheitspolitik und Sicherheitsziele“ von den Schutzprofilen

nicht abgedeckt werden. Es werden auch nicht alle Bestandteile der Risikomerkmale durch die Schutzprofile unterstützt. Die Sicherheitsarchitektur und die daraus abgeleiteten Sicherheitsrichtlinien stimmen in großem Maße mit dem Umfang eines Schutzprofils überein. Das eigentliche Ziel eines Schutzprofils ist die Erzeugung eines produktunabhängigen Standards. Trotzdem können auch die hersteller- und produktabhängigen Komponenten in ein Schutzprofil einfließen, sodass ein Schutzprofil auch Teile der spezifischen Sicherheitskonzepte abdecken kann. Die Umsetzung der Sicherheitsmaßnahmen befindet sich dagegen außerhalb des Umfangs eines Schutzprofils.
Der Aufbau der Sicherheits- und Risikomanagementpyramide ist mehrdimensional. Auch der Aufbau eines Schutzprofils, bei dem die Annahmen über die Einsatzumgebung und die Einsatzziele etc. erfasst werden, kann als ein mehrdimensionales Gebilde verstanden werden, wobei hier die PRO-Dimension[104] der Sicherheits- und Risikomanagementpyramide gemeint ist. Die bei der S&R-Pyramide zusätzlich vorhandene Prüfung und Weiterentwicklung kann bei einem eigenständigen Schutzprofil aufgrund der – mit der S&R-Pyramide verglichen – wenig abgedeckten Dimensionen nicht sinnvoll erfolgen. Auch die Berücksichtigung des Prozess-, Dienstleistungs-, Ressourcen- und Produktlebenszyklus erfolgt bei einem Schutzprofil nicht.
Aus den genannten Gründen kann ein zielgerichtetes Sicherheits- und Risikomanagement nicht lediglich auf der Basis der Schutzprofilerzeugung erfolgen. Schutzprofile sind vielmehr ein flexibles Sicherheitsinstrument, welches in die globale S&R-Politik eines Forschungsnetzes integriert werden kann (s. a. Abschnitt 4.2 „Gezielte Ausgestaltung der Sicherheitsarchitektur für die medizinischen Forschungsnetze“).

C.5. RiSiKo-(Management-)Pyramide: ein generischer S&R-Ansatz

Die RiSiKo-(Management-)Pyramide[105] von Klaus-Rainer Müller [Mül11] ist ein generisches und verknüpfendes Rahmenwerk für den standardisierten Aufbau des Informationssicherheitsmanagements. Das Sicherheitspyramidenmodell wurde zuerst im Jahr 1995 publiziert und wird seitdem kontinuierlich erweitert. Die Sicherheitspyramide besteht aus sieben hierarchisch aufeinander aufbauenden Ebenen, einer Transformationsschicht, besitzt drei Dimensionen, enthält einen Regelkreis und einen Sicherheitsmanagementprozess. Die Abbildung 49 illustriert den Aufbau der Sicherheitspyramide.
Die erste Dimension der Pyramide stellt die Sicherheitshierarchie dar, deren Ebenen sich voneinander top-down ableiten. Die zweite Dimension umfasst die Prozesse, Ressourcen und die Organisation. Die dritte Dimension spiegelt die einzelnen Phasen im Prozesslebens-

[104] Prozesse, Ressourcen und Organisation.

[105] Auch als Sicherheitspyramide, auch S&R-Pyramide oder kurz SiPyr genannt.

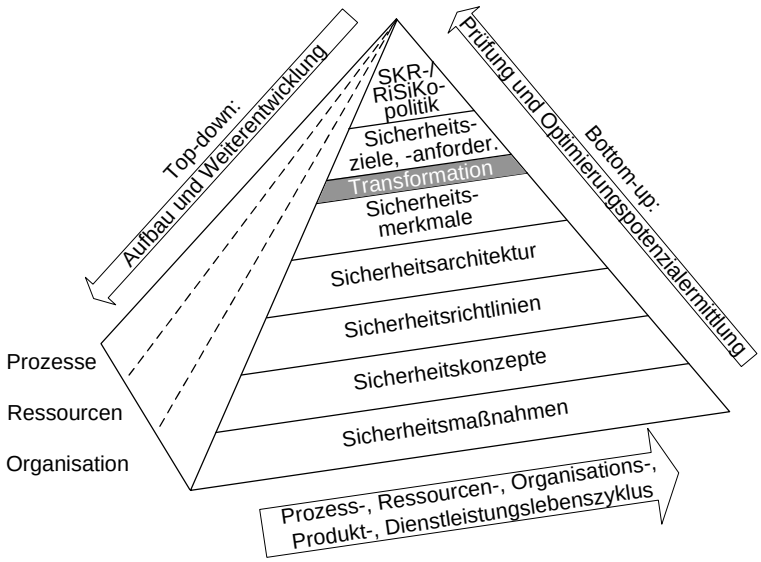

Abbildung 49.: Sicherheitsmanagementpyramide nach Klaus-Rainer Müller [Mül11, S. 120 f.]: Das generische Sicherheits-Framework, vom Autor auch als die Sicherheitspyramide V oder Sicherheitsmanagementpyramide V genannt, besitzt sieben hierarchisch gegliederte Ebenen, eine Transformationsschicht, drei Dimensionen, berücksichtigt einen Regelkreis und beinhaltet einen Sicherheitsmanagementprozess.

zyklus wider und orientiert sich an dem Phasenmodell. Ein Sicherheitsregelkreis und ein Sicherheitsmanagementprozess stehen für den Aufbau, die Steuerung und die Weiterentwicklung des Sicherheitsmanagements und umrahmen das Modell (vgl. [Mül11, S. 123 f.]). Die S&R-Pyramide enthält alle Bestandteile gängiger Sicherheits-Frameworks. Insbesondere die oberen abstrakteren Ebenen der Sicherheitspyramide könnten zentralisiert[106] gestaltet werden und für eine Vielzahl von Forschungsnetzen als eine solide vereinheitlichte Basis für das Sicherheits- und Risikomanagement dienen. Dadurch könnte man den Forschungsnetzen sowohl die Auswahl der notwendigen Grundelemente für Steuerung des Sicherheits- und Risikomanagements als auch die Sicherstellung eines adäquaten Sicherheitsniveaus erheblich erleichtern.

Die Einordnung der im Abschnitt A untersuchten Sicherheits-Frameworks in das Sicherheitspyramidenmodell erfordert wenig Aufwand und wäre sogar optional, wenn das im konkreten Fall eingesetzte S&R-Framework bekannt, und die Einzelheiten seiner Umsetzung ausreichend dokumentiert sind. Eine Gegenüberstellung des Modells und der geläufigsten Sicherheits-Frameworks beweist, dass das beschriebene Pyramidenmodell nicht bei der Auswahl eines S&R-Frameworks einschränkt und alle in dieser Arbeit untersuchten Frameworks abbilden kann (vgl. [Mül11, S. 67 ff.]).

[106] Beispielsweise im Rahmen der Arbeit der TMF.

C.6. Beispiele für die Richtliniengestaltung

Dieser Abschnitt enthält eine Sammlung von sicherheitsrelevanten Richtlinien, Standards und Regeln, die für einen sicheren Forschungsnetzbetrieb unerlässlich sind. Die im Folgenden vorgestellten Richtlinien weisen jedoch keine ausgeprägten Forschungsnetzspezifika auf und werden daher gesondert aufgeführt.

C.6.1. Anti-Malware-Policy

Folgende Regeln sollen im Rahmen der Malwarevorbeugung bzw. -bekämpfung gelten:

- Jedes am Forschungsnetz teilnehmende System muss mit einer regelmäßig aktualisierten Malwareerkennungssoftware bzw. einem Antivirenscanner ausgestattet werden.
- Die internen Systeme werden von einem zentralen Signaturserver unmittelbar nach der Verfügbarkeit neuer Signaturen mit Signaturupdates versorgt.
- Die Antivirenscanner der internen Systeme müssen für den On-Access-Modus konfiguriert sein.
- Das Herunterladen von Dateien aus verdächtigen Quellen bzw. das Öffnen von Anhängen der von unbekannten oder verdächtigen Absendern stammenden Nachrichten ist verboten.
- Die Wechselmedien (CDROMs, DVDs, externe Festplatten, USB-Sticks etc.) sind vor der Benutzung mit Anti-Malware-Programmen zu prüfen.
- Beim Feststellen der Malware oder beim Vorliegen eines begründeten Verdachts auf Malwareverseuchung muss sich der Forschungsnetzmitarbeiter an den technischen Support wenden. Sämtliche Versuche, die Kompromittierung bzw. ihre Spuren selbst zu beseitigen oder den Vorfall zu verschleiern, sind zu unterlassen.

C.6.2. Change Management

Alle Änderungen an der Produktionsumgebung sollen in einem Change-Management-Prozess begleitet werden. Eine Änderung kann im Hinzufügen, Verbessern, Entfernen von Soft- oder Hardware bestehen und muss mindestens wie folgt dokumentiert werden:

- Klassifizierung der Änderungsart (Infrastruktur, Hardware und Software),
- Identifizierung des Anforderers und Finanzierung,
- Spezifikation der Testpläne,
- Testnachweis und Freigabe vor der Inbetriebnahme,
- Zeitplan,
- Risiko- und Einflussbewertung,
- Änderungsanalyse unter Berücksichtigung aller anfallenden Kosten,
- die angemessenen Genehmigungen (Freigaben), die sich aus dem Vergleich mit dem Änderungsumfang ergeben.

Änderungen an den Produktionssystemen des Forschungsnetzes sind während der vereinbarten Wartungszeiten durchzuführen; nach Möglichkeit an Nichtarbeitstagen. Sollte der Einsatz von Forschungsnetzsystemen auch im Behandlungsprozess erfolgen und nicht auf die Werktage beschränkt sein, ist eine individuelle Vereinbarung für das Einspielen von Änderungen notwendig. Die Änderungen sollen in Abhängigkeit von ihren Prioritäten eingespielt werden. Die Einrichtung von Prioritätsklassen könnte wie folgt aussehen:

Priorität	Beschreibung
1:	Nicht produktionsrelevante Änderungen.
2:	Planmäßige Verbesserungen, Updates an den produktiven Systemen.
3:	Regelmäßig stattfindende Änderungen. Dazu gehören z. B. Monatsabschlussarbeiten, täglich durchzuführende Konfigurationsschritte etc.
4:	Änderungen mit festen Terminvorgaben. Dazu gehören z. B. Zeitumstellungen, Umstellungen aufgrund von gesetzlichen Vorgaben etc.
5:	Einspielung von sicherheitsrelevanten Updates, Patches etc.
6:	Notfalländerungen, die z. B. Ausnahmensituationen (Ausfall bzw. Kompromittierung von kritischen Forschungsnetzsystemen) beseitigen.

Um die Kontrollierbarkeit des Change-Management-Prozesses zu verbessern, sind Verantwortlichkeiten für den Prozessablauf festzulegen. Mehrere Rollen/Verantwortlichkeiten können von einer Person gleichzeitig angenommen werden. Bei der Vereinigung von Rollen ist jedoch das Aufgabentrennungsprinzip zu beachten (s. a. Abschnitt 3.5.4 „Rollenbasierte Rechtevergabe (RBAC)“). So darf z. B. die Rolle des Release-Administrators und die Rolle der Genehmigungsstelle nicht von der gleichen Person übernommen werden. Eine mögliche Rollenverteilung im Change-Management-Prozess sieht wie folgt aus:
Der *Änderungskoordinator* ist für die Einhaltung der Regeln des Prozesses Änderungsmanagement verantwortlich. Dem Änderungskoordinator obliegt die Erstellung, Aktualisierung und Weitergabe der Änderungsmanagementdokumentation. Sollte die durch den Koordinator gepflegte Kalenderübersicht Überschneidungen zwischen den geplanten Änderungen aufdecken, muss der Änderungskoordinator diese Information an die Entscheidungsfinder weiter kommunizieren. Ein Änderungskoordinator genehmigt außerdem die Durchführung von außerplanmäßigen Releases und übernimmt die Koordination in kritischen Release-Situationen.
Der *Änderungsadministrator* implementiert die Änderungen und führt die ihm übertragenen Aufgaben der Release-Überwachung und -Steuerung aus. Der Änderungsadministrator verifiziert und dokumentiert die (korrekte) Durchführung von Änderungen.
Der *Anforderer* initiiert die Änderungen. Diese Änderungen müssen an das Aufgabengebiet des Anforderers geknüpft sein; der Änderungsbedarf muss stets begründet werden. Neben dem Änderungskoordinator ist der Anforderer die einzige Stelle, die eine Änderung initiieren kann.
Die *Genehmigungsstelle* ist für die Zulassung bzw. Genehmigung von Änderungsanträgen zuständig. Nur die Änderungsanforderungen, die den internen und externen Richtlinien entsprechen, dürfen genehmigt werden.
Der *Tester* ist für die Durchführung und Dokumentation von Testfällen zuständig.

C.6.3. Datenklassifikation

Die Forschungsnetzdaten müssen vom Zeitpunkt ihrer Erfassung bis zu ihrer Vernichtung bzw. Anonymisierung in Abhängigkeit von ihrer Vertraulichkeitseinstufung angemessen geschützt werden. Die Klassifikation von Informationen in Bezug auf die Einhaltung des Sicherheitskriteriums *„Vertraulichkeit“* wird im Anhang C.6.9 „Vertraulichkeitseinstufung von Informationen“ behandelt (s. a. Anhang D „Qualifizierung von Sicherheitskriterien“). In der Tabelle 20 wurden die wichtigsten Sicherheitsmaßnahmen zur Handhabung von Daten unterschiedlicher Vertraulichkeitsstufen zusammengefasst.

Stufe	Maßnahmenbeschreibung
1:	Kontrolle der Daten auf Veränderung, Einsatz von Watermarks, um den Ursprung von Informationen feststellen zu können, Anbringung von gut lesbaren Hinweisen auf den Datenursprung auf die Medien.
2, 3:	Zugriffskontrolle, Regelungen für die Mitarbeiter bezüglich Weitergabe und Veröffentlichung von Informationen, Erstellung von Daten-Backups.
4, 5:	Kontrolle der Zugriffe nach dem „Need-to-know-Prinzip“, Auditing und Protokollierung der Zugriffe/Änderungen, verschlüsselte Datenübertragung und Datenaufbewahrung, verlässliche Vernichtung der Speichermedien, Einsatz von gehärteten Installationen, Pseudonymisierungs- und Anonymisierungstechniken.

Tabelle 20.: Maßnahmen zur Gewährleistung der Datenvertraulichkeit

Die Klassifikation der Daten bezüglich ihrer Vertraulichkeitseinstufung ist in vielen Fällen durch die Art der Daten vorbestimmt. Es empfiehlt sich, einen Katalog mit möglichen Datenarten in Hinsicht auf diverse Sicherheitskriterien zu erstellen und diesen allen relevanten Personen zur Verfügung zu stellen. In einigen Fällen ist eine eindeutige Klassifikation jedoch nicht möglich. In solchen Fällen ist es ratsam, stets von einer höheren Vertraulichkeitsstufe auszugehen bzw. beim Fehlen der notwendigen Anhaltspunkte die für die Vertraulichkeitseinstufung zuständige Person oder Gremium[107] zwecks Bestimmung der Vertraulichkeitsstufe zu kontaktieren. Der Katalog von Vertraulichkeitseinstufungen ist in regelmäßigen Zeitabständen auf seine Gültigkeit zu verifizieren.

C.6.4. Datensicherung und Datenaufbewahrung

Ein Forschungsnetz muss bestrebt sein, *Datensicherung und Datenaufbewahrung* zu gewährleisten, die den forschungsnetzinternen und gesetzlichen Vorschriften entsprechen. Dies gilt auch für die Drittparteien, von denen ein Forschungsnetz seine Leistungen bezieht. Die Überprüfung der Einhaltung von Vorschriften muss mindestens in jährlichen Zeitabständen erfolgen.

Die Datenaufbewahrung soll in Datenbanken erfolgen, die die maßgeblichen Sicherheitsanforderungen erfüllen (s. a. Abschnitt 3.5.8 „Datenbanksicherheit“). Der Zugriff von

[107] Zum Beispiel der Datenschutzbeauftragte oder der Ausschuss Datenschutz.

Programmen auf die Datenbankinhalte wird erst nach einer Authentifizierung gewährt. Die für die Authentifizierung verwendeten Zugriffsdaten dürfen nicht im Source-Code (als Code-Bestandteil) des Programms im Klartext oder in einem von extern zugänglichen Bereich (z. B. Webserver) vorliegen.
Die für den Datenbankzugriff notwendigen Benutzernamen und Passwörter müssen in einem für den öffentlichen Zugriff gesperrten Bereich aufbewahrt werden. Dies kann zwar eine Datei sein, es wird jedoch ausdrücklich die Verwendung von Verzeichnisdiensten für Authentifizierungszwecke empfohlen. Die Datenbankauthentifizierung erfolgt in diesem Fall analog zur Benutzerauthentifizierung im Auftrag des ausgeführten Programms. Im Falle der Speicherung innerhalb einer Datei darf diese lediglich die zur Authentifizierung notwendigen Komponenten (Benutzernamen, Passwörter, und die für den Zugriff notwendigen Parameter) enthalten.
Für die Verschleierung der Login-Daten dürfen keine selbst entwickelten bzw. leicht zu überwindenden Verfahren[108] eingesetzt werden; die Kryptografie-Richtlinie des Forschungsnetzes ist einzuhalten. Der Zugriff auf die Datenbank-Login-Daten soll nur dem Konfigurationsmanagement- und dem Datenbankmanagementteam gewährt werden. Die beiden Gruppen sind dafür zuständig, dass die Login-Informationen gemäß der Sicherheitsrichtlinie des Forschungsnetzes aktualisiert werden. Der Zugriff auf diese Datenbank muss nach dem „Need-to-know-Prinzip“ erfolgen.

C.6.5. Datenvernichtung

Wenn die gesetzlich geregelte maximale Aufbewahrungsdauer für digitale Daten erreicht worden ist bzw. wenn eine längere Aufbewahrung der Daten nicht mehr sinnvoll erscheint, müssen die Daten bzw. die diese Daten enthaltenden *Datenträger* vernichtet werden. Die Löschmaßnahmen sind von der Art der Speicherung abhängig. Die auf den PCs, Servern, Festplatten-Arrays etc. enthaltenen Daten müssen auf eine sichere Art gelöscht werden, sodass die Wiederherstellung dieser Daten nicht mehr möglich ist. Die sichere Löschung der Daten muss innerhalb des Forschungsnetzes erfolgen und darf einer Drittpartei (z. B. dem Hardwarelieferanten) nicht überlassen werden. Informationen auf magnetischen Datenträgern und Flash-Speichern (Bänder, ZIP-Disketten, USB-Sticks, Flash-Karten etc.) müssen ebenfalls sicher gelöscht werden. Bei der Löschung von USB-Sticks und Flash-Karten ist zu beachten, dass die gelöschten Daten i. d. R. mit einfachsten Mitteln wiederhergestellt werden können. Auch das Überschreiben der Daten muss nicht zu einer sicheren Vernichtung der Informationen führen, da die auf die minimierte Abnutzung des Datenträgers optimierte Firmware der Medien beim Überschreiben andere Speicherbereiche verwenden könnte. Die Verwendung von solchen Tools wie PGP Shredder & PGP Wipe führt nicht zu einer sicheren Datenvernichtung bei den Flash-Medien. Bei

[108] Beispielsweise die XOR-Verknüpfung.

den o. g. Speichermedien empfehlen sich die Erzeugung einer Datei mit zufälligen Inhalten in der Größe des Speichermediums und das mehrmalige Kopieren dieser Datei auf das Speichermedium. Optische Speichermedien (DVDs, CDs etc.) müssen physikalisch zerstört werden. Sollte die zukünftige Gesetzgebung schärfere oder abweichende Anforderungen an die *Datenvernichtung* stellen, haben diese Vorrang vor den hier aufgeführten Regelungen. Zeitlich begrenzte Sicherheit von kryptografischen Algorithmen macht die Verschlüsselung von Datenträgern nicht ausreichend, um eine dauerhafte Sicherheit der Daten zu garantieren und scheidet somit als „Datenvernichtungsmethode“ aus. Im Umkehrschluss bedeutet dies, dass auch für die verschlüsselten Daten die gleichen Regelungen einer sicheren Datenvernichtung gelten wie für die nicht verschlüsselten Daten.
Vor der Weitergabe von Forschungsnetzsystemen oder Speichermedien (z. B. beim Verschenken abgeschriebener Systeme oder bei der Zurückgabe abgeschriebener Systeme nach dem Leasing-Ablauf) müssen sämtliche Daten von den Systemen entfernt werden. Eine einfache Löschung der Daten ist nicht ausreichend. Genauso inakzeptabel zu diesem Zweck ist die Benutzung von Formatierungs- bzw. Partitionierungswerkzeugen. Beschädigte Datenträger, die nicht auf eine sichere Weise gelöscht werden können, müssen physikalisch zerstört werden. Zwecks einer besseren Kontrolle muss bei der Datenvernichtung durch das Administrationsteam festgehalten werden, welches System bzw. Datenträger gesäubert worden ist. Außerdem muss festgehalten werden, von wem und zu welchen Zwecken das System vor der Datenvernichtung eingesetzt wurde, von wem die Säuberung des Systems durchgeführt worden ist, und welche Datenvernichtungsmethoden dabei Anwendung fanden. Die im Rahmen der Datenvernichtung aufgetretenen Fehler sind zu protokollieren.
Neben den digital gespeicherten Daten müssen auch die in analoger Form aufbewahrten Dokumente (Papier, Folien etc.) sicher vernichtet werden können. Aufgrund der Art der von einem Forschungsnetz verarbeiteten Daten und einer zunehmenden Anzahl der Meldungen über erfolgreiche „Dumpster Diving“-Angriffe ist es empfehlenswert, von einem hohen Vertraulichkeitsbedarf aller Dokumente auszugehen und den Mitarbeitern des Forschungsnetzes die erforderlichen Mittel der Dokumentvernichtung (Papierschredder, Datenschutzcontainer etc.) zur Verfügung zu stellen. Bei der Datenvernichtung sind die Empfehlungen von [bsi11d] und [KSSL06] zu beachten.

C.6.6. Netzabsicherung

Die Absicherung der Forschungsnetzperipherie soll unter Berücksichtigung von gesetzlichen und forschungsnetzinternen Vorschriften erfolgen. Die Nichteinhaltung dieser Regelungen bzw. eine Abweichung von diesen Regelungen erfordert eine Ausnahmeerlaubnis des Ausschusses Datenschutz, die eine vorhergehende Risikoanalyse voraussetzt.

C.6.6.1. DMZ-Sicherheit

Alle Systeme, die mit den externen Systemen kommunizieren und nicht innerhalb des Forschungsnetz-LANs installiert sind, zählen zu den DMZ-Bestandteilen (inkl. Router, Switches etc.). Unter diese Kategorie fallen auch die ISP- und ASP-Systeme. DMZ entsteht durch die Trennung von Netzsegmenten voneinander, indem nur die tatsächlich benötigten Dienste zugelassen werden. Während vielfach die Verwendung mehrstufiger Firewall-Lösungen vorgeschlagen wird, wird des Öfteren vergessen, dass die Mehrstufigkeit des Aufbaus nicht automatisch eine höhere Sicherheit garantiert. Besonders oft anzutreffen ist z. B. die in der Abbildung 50 dargestellte Konstellation aus zwei hintereinander geschalteten Firewalls mit einer dazwischen platzierten DMZ.

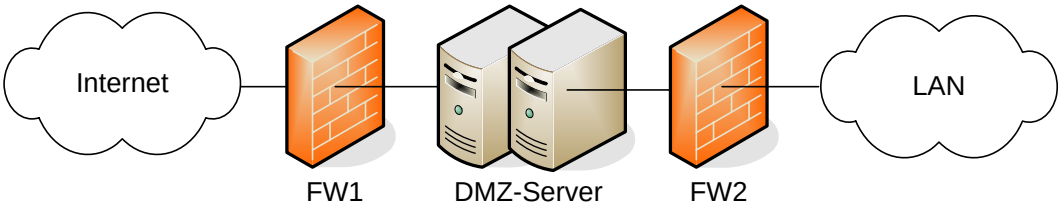

Abbildung 50.: Zweistufige Firewall-Lösung: Der DMZ-Bereich wird durch eine äußere (FW1) und eine innere (FW2) Firewall abgegrenzt. Oft wird die FW2 (aus Kostengründen) wegrationalisiert; der DMZ- und der LAN-Bereich werden als zwei separate Netzsegmente auf der FW1 durch Routing simuliert.

Ein solcher Aufbau erlaubt die Trennung sicherheitskritischer Serversysteme vom Forschungsnetz-LAN. Die innere Firewall wehrt Angriffe auf das LAN ab, die von kompromittierten DMZ-Systemen ausgeführt werden könnten und sorgt gleichzeitig dafür, dass diese Systeme aus dem LAN-Inneren schwerer anzugreifen sind.

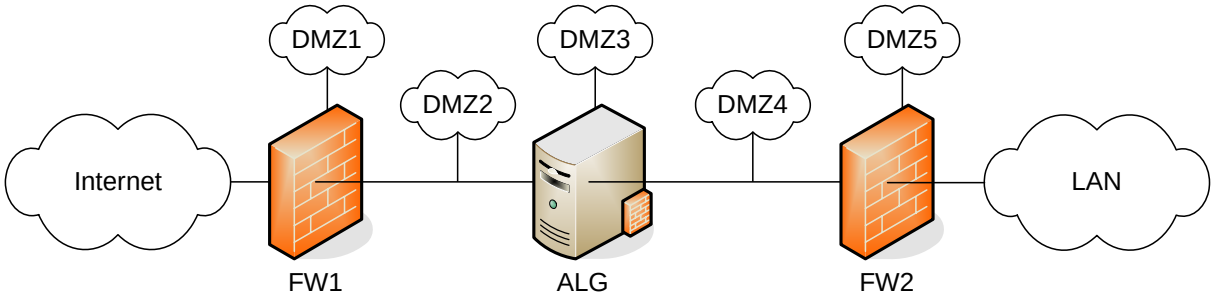

Abbildung 51.: Hintereinanderschaltung von FW1, ALG und FW2: Dieser vom BSI empfohlener Aufbau erlaubt zusätzliche Kontroll- und Protokollierungsmöglichkeiten, berücksichtigt jedoch noch keine Redundanzen.

Das Bundesamt für die Sicherheit in der Informationstechnik (BSI) empfiehlt die in der Abbildung 51 dargestellte Erweiterung des DMZ-Modells durch die Zwischenschaltung des sogenannten Application Level Gateways (ALG) zwischen FW1 und FW2. Ein solcher Aufbau erlaubt zusätzliche Kontroll- und Protokollierungsmöglichkeiten, denn die äußere und die innere Firewalls schützen den ALG und können die in seiner Konfiguration evtl. vorhandenen Fehler kompensieren (vgl. [bsi05, S. 42 ff.]). Doch auch dieser Aufbau hat einen entscheidenden Nachteil: Sollte die äußere (FW1) oder auch die innere Firewall

(FW2) deaktiviert werden, wird der Weg für (weitere) Angriffe frei. Bei bestimmten Wartungsarbeiten an einer der beiden Firewalls müsste auch bei diesem Aufbau das gesamte Netz von externen Verbindungen getrennt werden, denn ein ALG ist zur Filterung der über die Applikationsebene hinausgehenden Angriffe nur bedingt einsetzbar. Die Mehrstufigkeit einer Firewall-Lösung kann auch ihre Redundanz implizieren. Ein Beispielaufbau in der Abbildung 52 zeigt zwei parallel geschaltete Firewalls. Ein Management-Server befindet sich in einem separaten Management-Subnetz und wird zur Konfiguration der beiden Firewalls verwendet. Die beiden Firewalls können nicht nur sich gegenseitig bei Ausfällen vertreten, sondern nehmen auch am Load-Balancing teil, wobei die Last zwischen den parallel geschalteten Firewalls gleichmäßig verteilt wird.

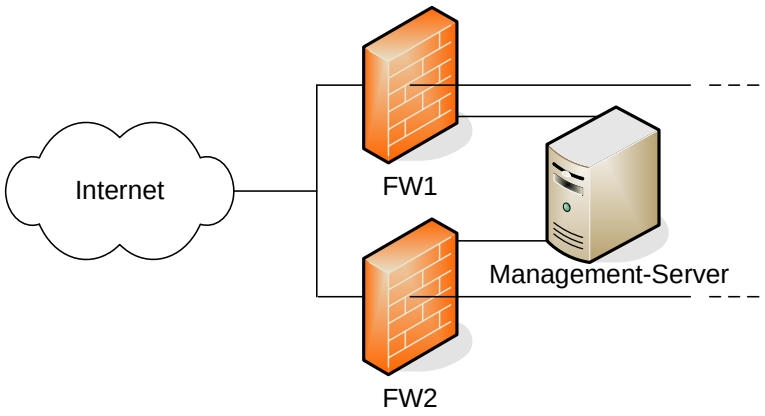

Abbildung 52.: Ein redundanter Firewall-Aufbau: Die beiden redundant geschalteten Firewalls werden mithilfe eines Management-Servers aus einem dedizierten Subnetz verwaltet. Dies erleichtert die Wartung, verbessert die Ausfallsicherheit und kann für die Lastverteilung eingesetzt werden.

C.6.6.2. Änderungen an den DMZ-Bestandteilen

Die DMZ-Bestandteile zählen zu den kritischen Systemen; nur Mitglieder des Konfigurationsmanagement-Teams sind berechtigt, Änderungen an der DMZ-Konfiguration durchzuführen. Die Löschung von Benutzeraccounts mit administrativem Zugriff auf die DMZ muss innerhalb von einem Arbeitstag nach der Auftragserteilung erfolgen. Es darf keine direkte Verbindung zwischen den DMZ-Systemen und dem Forschungsnetz-LAN bestehen; die Schnittstellen müssen durch eine Firewall (oder durch einen mehrstufigen Firewall-Aufbau) abgesichert werden (s. a. Abschnitt C.3.10 „Proxying und Aspekte der VPN- und IDS-Platzierung in Verbindung mit Firewalling“).
Die DMZ-Systeme sollten sich in einem Raum mit einem physikalisch abgesicherten Zugang befinden. Der Zugang zu den Räumlichkeiten darf nur einem engen Personenkreis erlaubt sein; die Liste der Zugriffsberechtigten muss regelmäßig (z. B. monatlich) auf ihre Aktualität überprüft werden. Wenn die Unterbringung der DMZ-Systeme in einem separaten Raum nicht möglich ist, müssen die Systeme zumindest in einem abschließbaren Server-Rack platziert werden.

Sämtliche Verbindungen zwischen den DMZ-Systemen und dem internen Netzwerk fallen unter die Richtlinie für den Remote-Zugriff (s. a. Abschnitt C.6.8 „Remote-Zugriff“). Einer sicheren Konfiguration von DMZ-Systemen ist eine besondere Bedeutung beizumessen. Die DMZ-Systeme müssen nach dem Minimalprinzip konfiguriert werden: Nur die tatsächlich notwendigen Dienste dürfen aktiviert sein. Die DMZ-Systeme müssen stets auf dem aktuellen Stand bezüglich Einspielung von Sicherheitspatches und -updates sein (s. a. Abschnitt C.6.1 „Anti-Malware-Policy“). Ein extra dafür eingerichteter Prozess muss sicherstellen, dass die Einspielung der Updates möglichst zeitnah stattfindet. Die Fernwartung der DMZ-Systeme darf nur über eine sichere (verschlüsselte) Verbindung erfolgen. Die Konfiguration der Systeme im DMZ-Bereich muss detailliert dokumentiert werden, wobei folgende Punkte in der Dokumentation erläutert werden müssen:

- Bezeichnung des Systems,
- ausgeführte Funktion,
- Angabe des Systembetreuers,
- Hardware- und Softwarekonfiguration.

Änderungen an dem Aufbau bzw. Konfiguration dieser Systeme müssen die Standardprozeduren des Forschungsnetzes durchlaufen (s. a. Abschnitt C.6.2 „Change Management“). Der Aufbau muss in regelmäßigen Zeitabständen (mindestens einmal jährlich, besser quartalsmäßig) auf seine Sicherheit untersucht werden.
Die im DMZ-Bereich verwendeten Hard- und Software müssen vor der Inbetriebnahme auf die Einhaltung von Standards verifiziert werden. Sämtliche Konfigurationsänderungen müssen den Forschungsnetzstandards entsprechen. Die als unsicher geltenden Dienste, Protokolle etc. müssen möglichst schnell durch die sicheren Alternativen ersetzt werden. Die Protokollierung der DMZ-Systeme muss detaillierter als die der sonstigen Systeme gestaltet sein und alle Sicherheitsanforderungen des Forschungsnetzes erfüllen. Es sollen u. a. folgende Ereignisse bedeutender eingestuft werden: nicht erfolgreiche Login- bzw. Zugriffsversuche, Verletzungen der Zugriffs-Policies, gescheiterte Versuche, höhere Zugriffsrechte zu erlangen.

C.6.6.3. DMZ-Aufbau

An den Aufbau von Forschungsnetz-DMZs werden mehrere Anforderungen gestellt. Diese beinhalten u. a. hoch verfügbare, redundante, unabhängige Internetverbindungen, redundantes Routing zum und vom Internet sowie innerhalb des DMZ-Bereichs, fehlertolerante, hoch verfügbare Firewall-Systeme und Load-Balancing-Fähigkeiten für die Server. Ein Vorschlag für den DMZ-Aufbau ist in der Abbildung 53 dargestellt.
Für den Forschungsnetzeinsatz gilt ein zweistufiger Firewall-Aufbau als Mindestvoraussetzung, ein dreistufiger Aufbau wird empfohlen (s. a. Abschnitt C.3.10). Die externen Firewalls überwachen den Zugriff auf Forschungsnetzsysteme aus dem Internet. Systeme, die direkt aus dem Internet erreichbar sind,[109] sind in Abhängigkeit von ihrer Funktion

[109] Zum Beispiel Mail- und Webserver.

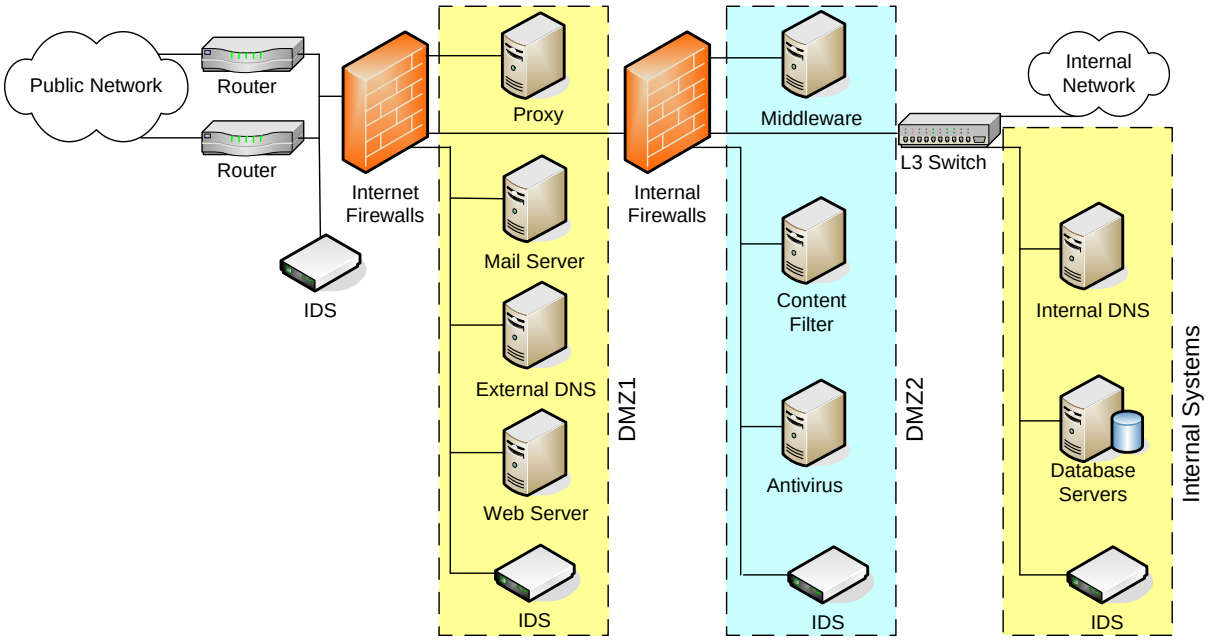

Abbildung 53.: Vorschlag für den DMZ-Aufbau: Die Server- und Client-Systeme werden in Abhängigkeit von ihrer Funktion auf die DMZ- bzw. Netzsegmente verteilt. Abhängig vom Infrastrukturaufbau können wesentlich mehr als nur die abgebildeten drei Server-Bereiche und ein Segment für das interne Netz notwendig sein.

in mehrere LAN- bzw. VLAN-Segmente aufzuteilen. Die in der ersten DMZ stehenden Systeme dürfen keinen direkten Zugriff auf das interne LAN des Forschungsnetzes haben. Die zweite Firewall schützt die Applikationsserver vor Angriffen, die von den aus dem Internet erreichbaren Systemen ausgehen könnten. Beim dreistufigen Aufbau wird ein sogenanntes Application Gateway eingesetzt, der die Daten auf dem OSI-Layer 7 filtert. Alle Systeme, die sich im DMZ-Bereich befinden, müssen gehärtete Installationen aufweisen und alle Dienste außer explizit erlaubten verweigern. In der DMZ2 werden Systeme platziert, auf die die in der DMZ1 stehenden Komponenten zugreifen können, auf die jedoch ein direkter Zugriff aus dem Internet nicht notwendig ist, und die Diensterfüllung keinen direkten Zugriff auf das Internet voraussetzt.[110]

Vor der Erstinbetriebnahme der DMZ darf kein Zugriff (außer er ist notwendig für Intrusion-Detection-, Monitoring-, Auditing- und Backup-Dienste) freigeschaltet sein. Keine offenen Applikationsports dürfen in den DMZ-Grundeinstellungen vorhanden sein. Der Zugriff auf die DMZ-Systeme muss sich auf das für die Administrationsaufgaben und für die Übertragung von Logdaten notwendige Minimum beschränken. Die Benutzer- und die Systemauthentifizierung muss die Kryptografiestandards des Forschungsnetzes erfüllen.

Die *Router-Konfiguration* muss mithilfe von ACLs und restriktiven Konfigurationseinstellungen abgesichert werden, um die Spoofing-Angriffe aus dem Internet aufdecken zu können. Der Zugriff auf die Router-Konfiguration soll nur für wenige interne Systeme freigeschaltet werden und darf nicht aus dem öffentlichen Netz möglich sein. Nur die in der Router-Konfiguration explizit zugelassenen Protokolle dürfen vom Router akzeptiert werden. Alle

[110] Zum Beispiel Applikationsserver, Middleware-Server, Directory-Server, Antivirus-Gateways etc.

Router dürfen lediglich Dienste zur Verfügung stellen, die für den Forschungsnetzbetrieb notwendig sind.
Der DMZ-Bereich muss von einem 24/7 Intrusion-Detection-System überwacht werden. Die Verwundbarkeitsanalysen[111] müssen mindestens einmal im Monat stattfinden, um die evtl. vorhandenen Schwachstellen möglichst zeitnah aufzudecken. Beim Bekanntwerden relevanter Sicherheitslücken der Forschungsnetzsysteme sollen ebenfalls Verwundbarkeitsanalysen durchgeführt werden.

C.6.7. Nutzung von Forschungsnetzsystemen

Folgendes ist im Zusammenhang mit der Nutzung von Forschungsnetzsystemen verboten:

- Verletzung von Rechten Dritter, die durch Patente, Geschäftsgeheimnisse etc. geschützt sind, wie z. B. Installation von nicht lizenzierter Software.
- Erstellung nicht autorisierter Kopien vom urheberrechtlich geschützten Material (z. B. unerlaubte Verbreitung von urheberrechtlich geschützten Aufnahmen, Büchern, Musik etc.).
- Verbreitung von Malware, Kettenbriefen, Versenden von Spam etc.
- Weitergabe von Login-Informationen.
- Benutzung forschungsnetzeigener Systeme oder Datenleitungen zum Abruf und zur Verbreitung von pornografischen, rassistischen, politischen, jugendgefährdenden oder in einer anderen Weise mit dem geltenden Recht oder den guten Sitten nicht zu vereinbarenden Inhalten.
- Abgabe von Angeboten/Erklärungen in betrügerischer Absicht.
- Störungen der Netzwerkkommunikation, es sei denn, dies ist ausdrücklich von den für die Sicherheit des Forschungsnetzes zuständigen Personen erwünscht (z. B. Sniffing, Flooding, Spoofing, DoS-Angriffe, Manipulation von Routing-Einträgen etc.).
- Durchführung von Portscans und Netzwerküberwachung, es sei denn, eine explizite Genehmigung der für die Sicherheit Verantwortlichen liegt vor.
- Unzulässige Weitergabe von Kontaktdaten der Forschungsnetzteilnehmer bzw. von Forschungsnetzdaten an Drittparteien.

C.6.8. Remote-Zugriff

Unter dem Begriff „Remote-Zugriff“ versteht man die Anbindung eines externen Systems an das interne Netz. Diese kann über eine Wahl- oder Standleitung, VPN etc. erfolgen. Insbesondere kann die Erledigung administrativer Aufgaben (z. B. Fernwartung) den Remote-Zugriff notwendig machen. Die Nutzung des Remote-Zugangs ist nur zu Forschungs- und administrativen Zwecken erlaubt.

[111] Vulnerability Assessments.

Die Remote-Zugänge sind potenzielle Einfallstore für die Angriffe und müssen besonders kontrolliert werden. Zu den Kontrollmaßnahmen zählen eine sichere Authentifizierung der zugreifenden Person mithilfe einer PIN-geschützten SmartCard mit Benutzerzertifikaten (s. a. Abschnitt 3.5.7 „Ticketing, Single Sign-On (SSO)“). Folgende Anforderungen müssen beim Remote-Zugriff erfüllt werden:

- Jeder Benutzer muss eindeutig identifiziert werden können. Die Benutzung generischer Accounts für mehrere Remote-Benutzer ist verboten. Der Remote-Zugang ist personalisiert (an eine Person gebunden) und darf unter keinen Umständen an eine andere Person weitergegeben werden.
- Die verwendeten Authentifizierungsmechanismen müssen den Forschungsnetzstandards entsprechen (s. a. Abschnitt 3.5.3 „Authentifizierung von Forschungsnetzteilnehmern“).
- Es müssen Kontrollmechanismen existieren, die den Benutzerzugriff nur auf die Bereiche/Systeme einschränken, für die der jeweilige Benutzer Autorisierung besitzt.
- Protokollierung von Zugriffen sowie nicht erfolgreichen Login-Versuchen (s. a. Abschnitt 3.5.12 „Monitoring und Protokollierung“).
- Alle Systeme mit dem administrativen Remote-Zugriff müssen die relevanten Forschungsnetzstandards bezüglich Hard- und Softwarekonfiguration erfüllen. Während des Remote-Zugriffs darf ein solches System keine weiteren (parallelen) Verbindungen mit dem Internet bzw. mit einem mit dem Internet verbundenen Netz aufbauen.
- Die von einem Forschungsnetzteilnehmer verwendeten Router müssen mindestens die Anforderungen von CHAP erfüllen.
- Die verwendeten Frame-Relays müssen mindestens die DLCI-Authentifizierungsanforderungen erfüllen.
- Die von den Forschungsnetzteilnehmern für den Remote-Zugriff verwendeten Systeme müssen die aktuellen Versionen der vom Forschungsnetz akzeptierten Antivirensoftware (inkl. Signaturupdates) einsetzen.
- Der Freischaltungsprozess für den Remote-Zugriff wird durch die Antragstellung eingeleitet. Der Antrag auf den Remote-Zugriff wird durch den Vorgesetzten des Forschungsnetzmitarbeiters gestellt und geht an den Verwalter[112] von Remote-Zugängen, der seinerseits den Antrag genehmigt und die Erstellung des Remote-Zugangs einleitet. Im Antrag auf den Remote-Zugriff muss die Notwendigkeit des Zugangs für den Mitarbeiter begründet werden; die für die Aufgabenerledigung notwendigen Ressourcen (Systeme, Applikationen etc.) müssen aufgelistet werden.

[112] Remote-Access-Administrator.

- Die Nichtmitarbeiter des Forschungsnetzes können Berechtigung für Remote-Zugriff erhalten (z. B. Mitarbeiter eines Drittanbieters). Solche Anträge bedürfen einer Genehmigung des Ausschusses Datenschutz; der Zugriff muss auf die zur Erledigung der Aufgaben notwendigen Rechte/Ressourcen beschränkt sein.
- Die während einer Remote-Verbindung übertragenen Daten müssen verschlüsselt werden. Die verwendeten Verschlüsselungsmechanismen müssen den Forschungsnetzstandards entsprechen.
- Änderungen sämtlicher im Zusammenhang mit dem Remote-Zugriff stehenden Dienste bzw. verwendeten Hardware, Software oder Verfahren bedürfen einer Genehmigung des dafür zuständigen Gremiums.
- Die Notwendigkeit von Remote-Verbindungen muss regelmäßig[113] verifiziert werden. Die Verbindung muss deaktiviert werden, sobald ihre Notwendigkeit nicht mehr gegeben ist.

C.6.9. Vertraulichkeitseinstufung von Informationen

Die Existenzberechtigung eines Forschungsnetzes beruht auf dem vertrauensvollen Umgang mit den Patientendaten, die nicht nur in den Datenbanken gespeichert, sondern auch auf dem Papier festgehalten, per E-Mail, via Telefon, mündlich oder visuell ausgetauscht werden können.
Es ist notwendig, eine Vertraulichkeitseinstufung von Informationen vorzunehmen. Unter *öffentlichen* Informationen versteht man Informationen, die von einer berechtigten Person als solche gekennzeichnet worden sind und ohne Schaden für das Forschungsnetz oder für eine Drittpartei[114] veröffentlicht werden dürfen. Von den öffentlichen Informationen sind die *vertraulichen* Informationen abzugrenzen. Es kann unterschiedliche Vertraulichkeitsstufen geben. So sind Patientendaten oder Informationen, die eine Patientenreidentifizierung erlauben, als *streng vertraulich* einzustufen. Eine Liste der Forschungsnetzmitarbeiter ist ebenfalls *vertraulich*, da sie zur Vorbereitung eines Angriffs dienen kann, hat jedoch eine wesentlich geringere Vertraulichkeitsstufe. Wenn die Zuordnung einer Vertraulichkeitsstufe vom Forschungsnetzmitarbeiter selbst nicht eindeutig festgelegt werden kann, ist er dazu angehalten, die Einstufung von der dafür zuständigen Person oder Gremium vornehmen zu lassen.
Zu den Informationen mit der *niedrigsten Vertraulichkeitsstufe* gehören technische und statistische Informationen. Forschungsnetzmitarbeiter, Dienstleister, Forschungsnetzteilnehmer, Behörden etc. können in solche Informationen einsehen. Sie können i. d. R. weitergegeben werden, mit der Einschränkung, dass sie nur dem Personenkreis, der ein

[113] Mindestens einmal jährlich.

[114] Teilnehmer, Patienten, Dienstleister etc.

berechtigtes Interesse nachweisen kann, verfügbar gemacht werden. Auch für die Aufbewahrung dieser Informationen sind lediglich rudimentäre Sicherheitsmaßnahmen erforderlich. Finanzielle, technische und persönliche Informationen können eine *höhere Vertraulichkeitseinstufung* haben. Solche Informationen dürfen i. d. R. einer Drittpartei nicht zugänglich gemacht werden. Der Zugang kann nur den Forschungsnetzmitarbeitern gewährt werden, die eine Verschwiegenheitserklärung unterschrieben haben. Auch die Aufbewahrung und Vernichtung von Datenträgern mit solchen Informationen erfordert besondere Sicherheitsvorkehrungen.[115]

Patienteninformationen, bestimmte technische Dokumentation, Login-Daten und weitere sicherheitsrelevante Informationen sind als *höchst vertraulich* einzustufen. Solche Informationen können nur in Ausnahmefällen einer Drittpartei zugänglich gemacht werden. Beim Zugriff, Aufbewahrung und Vernichtung solcher Daten müssen besondere Sicherheitsmaßnahmen eingehalten werden. So ist es empfehlenswert, solche Informationen nur in verschlüsselter Form bzw. in Tresoren zu speichern. Bei der digitalen Aufbewahrung ist die Verwendung von Systemen empfehlenswert, die keine Anbindung an das Forschungsnetz-LAN und das Internet haben (s. a. Abschnitte C.6.5 „Datenvernichtung“, C.6.4 „Datensicherung und Datenaufbewahrung“, vgl. [the10], [Fra97]).

[115] Beispielsweise Datenschutzcontainer für Papier, Entmagnetisierung von Bändern, Zerkleinerung im Partikelschnitt für optische Datenträger.

D. Qualifizierung von Sicherheitskriterien

Sämtliche zeitlichen und monetären Angaben in diesem Abschnitt sind Beispielwerte[1] und müssen durch die für ein konkretes Forschungsnetz relevanten Größen ersetzt werden (vgl. [bsi08b], [bsi08c]).

Stufe	Auswirkung
1:	keine
2:	gering
3:	mittel
4:	groß
5:	existenzbedrohend

Stufe	Bewertungskriterium
Finanzielle Auswirkungen von Schäden	
1:	Die Kosten des Schadens und dessen Beseitigung übersteigen nicht 10 €.
2:	Die Kosten des Schadens und dessen Beseitigung übersteigen nicht 100 €.
3:	Die Kosten des Schadens und dessen Beseitigung übersteigen nicht 1.000 €.
4:	Die Kosten des Schadens und dessen Beseitigung übersteigen nicht 10.000 €.
5:	Die Kosten des Schadens und dessen Beseitigung übersteigen 10.000 €.
Verbindlichkeit	
1:	Die Verbindlichkeit von Informationen ist kein relevantes Kriterium.
2:	Die Verbindlichkeit ist ein relevantes Sicherheitskriterium. Dessen Verletzung führt entweder zu keinen oder zu geringen Schäden.
3:	Die Verletzung der Verbindlichkeit kann zu mittleren Schäden führen.
4:	Die Verletzung der Verbindlichkeit kann zu großen Schäden führen.
5:	Die Verletzung der Verbindlichkeit kann die Existenz des Forschungsnetzes bedrohen.

[1] Angelehnt an [HV08], [Spi07] bzw. [HWE05].

Verfügbarkeit

1:	Ausfälle von bis zu zwei Wochen bringen keine Existenzbedrohung mit sich.
2:	Ausfälle mit einer Dauer von bis zu fünf Arbeitstagen können toleriert werden.
3:	Ausfälle mit einer Dauer von bis zu einem Arbeitstag können toleriert werden.
4:	Die maximale Ausfalldauer darf fünf Stunden nicht überschreiten.
5:	Das System muss eine 24/7-Verfügbarkeit aufweisen.

Konformität

1:	Die Konformität zu Gesetzen, Normen, Richtlinien spielt keine nennenswerte Rolle.
2:	Die Einhaltung der Konformität muss beachtet werden. Im Falle des Verstoßes gegen die Normen, Gesetze etc. ist kein nennenswerter Schaden zu erwarten.
3:	Die Verstöße gegen Konformität können zu mittelgroßen Schäden führen.
4:	Die Verletzung der Konformität kann zu großen Schäden führen, die jedoch nicht existenzbedrohlich sind.
5:	Die Verstöße gegen Gesetze, Normen etc. können zur Einstellung des Betriebs führen.

Integrität

1:	Die Integrität ist als Sicherheitskriterium irrelevant.
2:	Die Integrität ist ein relevantes Sicherheitskriterium. Eine Integritätsverletzung führt jedoch entweder zu keinen oder nur zu geringen Schäden.
3:	Die Verfälschung oder Manipulation können zu Schäden mittlerer Höhe führen.
4:	Die Verletzung der Integrität kann zu großen Schäden führen, die jedoch nicht den Fortbestand des Forschungsnetzes gefährden.
5:	Die Manipulation bzw. Verfälschung können zu existenzbedrohenden Schäden führen.

Robustheit

1:	Die Robustheit des Prozesses, Dienstes, Systems etc. ist irrelevant.
2:	Die Robustheit als Eigenschaft hat eine nicht zu vernachlässigende Bedeutung. Eine Verletzung des Sicherheitskriteriums führt jedoch zu keinen bzw. zu geringen Schäden.
3:	Die Verletzung der Robustheit kann zu Schäden mittlerer Höhe führen.
4:	Die Verletzung der Robustheit kann zu Großschäden führen.
5:	Die Robustheit hat als Sicherheitskriterium die höchste Priorität. Eine Verletzung der Robustheit kann zu existenzbedrohenden Schäden führen.

Vertraulichkeit

1:	Die Informationen sind öffentlich verfügbar. Vertraulichkeit ist kein relevantes Sicherheitskriterium.
2:	Organisationsinterne Informationen, auf die alle Mitarbeiter Zugriff haben. Die Bekanntgabe dieser Informationen kann geringe negative Auswirkungen haben.
3:	Nur ein definierter Personenkreis darf auf die Informationen zugreifen. Eine Veröffentlichung dieser Informationen kann zu Schäden mittlerer Höhe führen.
4:	Die Informationen haben eine hohe Vertraulichkeitseinstufung. Eine Veröffentlichung dieser Informationen kann mit einem hohen Schaden verbunden sein.
5:	Die Informationen haben die höchste Vertraulichkeitseinstufung. Eine Veröffentlichung dieser Informationen kann für das Forschungsnetz existenzbedrohend werden (s. a. Abschnitt C.6.3 „Datenklassifikation“).

Authentizität

1:	Die Authentizität des Kommunikationspartners bzw. von Informationen ist irrelevant.
2:	Die Sicherstellung der Authentizität ist ein relevantes Sicherheitskriterium. Die Authentizitätsverletzungen können zu geringen Schäden führen.
3:	Die Verletzung der Authentizität kann zu mittelgroßen Schäden führen.
4:	Die Verletzung der Authentizität kann zu großen Schäden führen, die jedoch nicht für den Fortbestand der Organisation kritisch sind.
5:	Die Authentizität von Informationen/Kommunikationspartnern etc. hat höchste Priorität. Die Verletzung des Sicherheitskriteriums kann zu existenzbedrohenden Schäden für das Forschungsnetz führen.

E. Auszüge aus BDSG und StGB

BDSG § 3 Weitere Begriffsbestimmungen. (1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

(2) Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen. Eine nicht automatisierte Datei ist jede nicht automatisierte Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann.

(3) Erheben ist das Beschaffen von Daten über den Betroffenen.

(4) Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im Einzelnen ist, ungeachtet der dabei angewendeten Verfahren:
1. Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung,
2. Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,
3. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass
   a) die Daten an den Dritten weitergegeben werden oder
   b) der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft,
4. Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken,
5. Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.

(5) Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

(6) Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

(6a) Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

(7) Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

(8) Empfänger ist jede Person oder Stelle, die Daten erhält. Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle. Dritte sind nicht der Betroffene sowie Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.
(9) Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben (...)

BDSG § 3a Datenvermeidung und Datensparsamkeit. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

BDSG § 9 Technische und organisatorische Maßnahmen. Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

BDSG § 9a Datenschutzaudit. Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt.

BDSG Anlage (zu § 9 Satz 1). Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,
1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),

2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtung zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.
Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

BDSG § 14 Datenspeicherung, -veränderung und -nutzung. (1) Das Speichern, Verändern oder Nutzen personenbezogener Daten ist zulässig, wenn es zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben erforderlich ist und es für die Zwecke erfolgt, für die die Daten erhoben worden sind. Ist keine Erhebung vorausgegangen, dürfen die Daten nur für die Zwecke geändert oder genutzt werden, für die sie gespeichert worden sind.

(2) Das Speichern, Verändern oder Nutzen für andere Zwecke ist nur zulässig, wenn (...)
7. es zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuchs oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen erforderlich ist (...)

BDSG § 15 Datenübermittlung an öffentliche Stellen. (1) Die Übermittlung personenbezogener Daten an öffentliche Stellen ist zulässig, wenn
1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Dritten, an den die Daten übermittelt werden, liegenden Aufgaben erforderlich ist und
2. die Voraussetzungen vorliegen, die eine Nutzung nach § 14 zulassen würden (...)

BDSG § 16 Datenübermittlung an nicht-öffentliche Stellen. (1) Die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen ist zulässig, wenn
1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach § 14 zulassen würden, oder
2. der Dritte, an den die Daten übermittelt werden, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Das Übermitteln von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) ist abweichend von Satz 1 Nr. 2 nur zulässig, wenn die Voraussetzungen vorliegen, die eine Nutzung nach § 14 Abs. 5 und 6 zulassen würden oder soweit dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist (...)

BDSG § 40 Verarbeitung und Nutzung personenbezogener Daten durch Forschungseinrichtungen. (1) Für Zwecke der wissenschaftlichen Forschung erhobene oder gespeicherte personenbezogene Daten dürfen nur für Zwecke der wissenschaftlichen Forschung verarbeitet oder genutzt werden.

(2) Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungszweck dies erfordert.

(3) Die wissenschaftliche Forschung betreibenden Stellen dürfen personenbezogene Daten nur veröffentlichen, wenn
1. der Betroffene eingewilligt hat oder
2. dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.

StGB § 203 Verletzung von Privatgeheimnissen. (1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als
1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,
2. Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlußprüfung,
3. Rechtsanwalt, Patentanwalt, Notar, Verteidiger in einem gesetzlich geordneten Verfahren, Wirtschaftsprüfer, vereidigtem Buchprüfer, Steuerberater, Steuerbevollmächtigten oder Organ oder Mitglied eines Organs einer Rechtsanwalts-, Patentanwalts-, Wirtschaftsprüfungs-, Buchprüfungs- oder Steuerberatungsgesellschaft,
4. Ehe-, Familien-, Erziehungs- oder Jugendberater sowie Berater für Suchtfragen in ei-

ner Beratungsstelle, die von einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts anerkannt ist.
4a. Mitglied oder Beauftragten einer anerkannten Beratungsstelle nach den §§ 3 und 8 des Schwangerschaftskonfliktgesetzes,
5. staatlich anerkanntem Sozialarbeiter oder staatlich anerkanntem Sozialpädagogen oder
6. Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen Verrechnungsstelle
anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als
1. Amtsträger,
2. für den öffentlichen Dienst besonders Verpflichteten,
3. Person, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnimmt,
4. Mitglied eines für ein Gesetzgebungsorgan des Bundes oder eines Landes tätigen Untersuchungsausschusses, sonstigen Ausschusses oder Rates, das nicht selbst Mitglied des Gesetzgebungsorgans ist, oder als Hilfskraft eines solchen Ausschusses oder Rates,
5. öffentlich bestelltem Sachverständigen, der auf die gewissenhafte Erfüllung seiner Obliegenheiten aufgrund eines Gesetzes förmlich verpflichtet worden ist, oder
6. Person, die auf die gewissenhafte Erfüllung ihrer Geheimhaltungspflicht bei der Durchführung wissenschaftlicher Forschungsvorhaben aufgrund eines Gesetzes förmlich verpflichtet worden ist,
anvertraut worden oder sonst bekanntgeworden ist. Einem Geheimnis im Sinne des Satzes 1 stehen Einzelangaben über persönliche oder sachliche Verhältnisse eines anderen gleich, die für Aufgaben der öffentlichen Verwaltung erfaßt worden sind; Satz 1 ist jedoch nicht anzuwenden, soweit solche Einzelangaben anderen Behörden oder sonstigen Stellen für Aufgaben der öffentlichen Verwaltung bekanntgegeben werden und das Gesetz dies nicht untersagt.

(2a) Die Absätze 1 und 2 gelten entsprechend, wenn ein Beauftragter für den Datenschutz unbefugt ein fremdes Geheimnis im Sinne dieser Vorschriften offenbart, das einem in den Absätzen 1 und 2 Genannten in dessen beruflicher Eigenschaft anvertraut worden oder sonst bekannt geworden ist und von dem er bei der Erfüllung seiner Aufgaben als Beauftragter für den Datenschutz Kenntnis erlangt hat.

(3) Einem in Absatz 1 Nr. 3 genannten Rechtsanwalt stehen andere Mitglieder einer Rechtsanwaltskammer gleich. Den in Absatz 1 und Satz 1 Genannten stehen ihre berufsmäßig tätigen Gehilfen und die Personen gleich, die bei ihnen zur Vorbereitung auf den Beruf tätig sind. Den in Absatz 1 und den in Satz 1 und 2 Genannten steht nach dem Tod des zur Wahrung des Geheimnisses Verpflichteten ferner gleich, wer das Geheimnis von dem Verstorbenen oder aus dessen Nachlaß erlangt hat.

(4) Die Absätze 1 bis 3 sind auch anzuwenden, wenn der Täter das fremde Geheimnis nach dem Tod des Betroffenen unbefugt offenbart.

(5) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.