Becker, Jörg (Ed.) et al.

Working Paper

IT-Risiken: Ursachen, Methoden, Forschungsperspektiven

Arbeitsberichte des Instituts für Wirtschaftsinformatik, No. 128

Provided in Cooperation with:
University of Münster, Department of Information Systems

Suggested Citation: Becker, Jörg (Ed.) et al. (2010) : IT-Risiken: Ursachen, Methoden, Forschungsperspektiven, Arbeitsberichte des Instituts für Wirtschaftsinformatik, No. 128, Westfälische Wilhelms-Universität Münster, Institut für Wirtschaftsinformatik, Münster

This Version is available at:
https://hdl.handle.net/10419/59568

Westfälische
Wilhelms-Universität
Münster

› IT-Risiken

Ursachen, Methoden, Forschungsperspektiven

Arbeitsbericht Nr. 128

wissen.leben
WWU Münster

WIRTSCHAFTS
INFORMATIK

Arbeitsberichte des Instituts für Wirtschaftsinformatik
Herausgeber: Prof. Dr. J. Becker, Prof. em. Dr. H. L. Grob,
Prof. Dr.-Ing. B. Hellingrath, Prof. Dr. S. Klein, Prof. Dr. H. Kuchen,
Prof. Dr. U. Müller-Funk, Prof. Dr. G. Vossen

Arbeitsbericht Nr. 128

IT-Risiken

Ursachen, Methoden, Forschungsperspektiven

Herausgeber: Jörg Becker, Philipp Bergener, Mathias Eggert,
Marcel Heddier, Sara Hofmann, Ralf Knackstedt, Michael Räckers

ISSN 1438-3985

Vorwort

IT-Skandale gehören zur heutigen Gesellschaft wie die IT selbst. Sie treten regelmäßig auf und werden dabei durch eine Vielzahl von Publikationsorganen in der Öffentlichkeit thematisiert. Die Folgen sind vielfältig. Auf der einen Seite sind häufig Angestellte oder Kunden eines Unternehmens oder einer Institution betroffen, deren Daten veröffentlicht oder ausgespäht wurden oder die einen darüber hinausgehenden Schaden erleiden. Auf der anderen Seite sind diese Skandale mit einem Reputationsschaden für die involvierten Unternehmen verbunden, beispielsweise mit einem Vertrauensverlust oder mit finanziellen Schäden. Wie lassen sich diese Risiken in der Verwendung von IT strukturieren, was sind typische Muster der Risiken, die zu regelmäßigen Skandalen führen? Was sind Erfolgsfaktoren, um diese IT-Risiken und Schäden beherrschbar zu machen? Zur Lösung dieser komplexen Aufgabe existieren unterschiedliche Ansätze wie Compliance-Methoden, Möglichkeiten der (Software-)Zertifizierung oder die Modellierung rechtlicher Anforderungen während der Entwicklung von IT-Systemen.

Die vorliegenden Beiträge sind im Rahmen des Bachelor-Vertiefungsmoduls *Rechtsinformatik/Informationsrecht* entstanden, das im Sommersemester 2010 am Institut für Wirtschaftsinformatik an der Westfälischen Wilhelms-Universität stattfand und sich zur Aufgabe gemacht hat, in diesem Spannungsfeld von IT und Rechtsfragen zu arbeiten. Die Ergebnisse des Seminars wurden von den teilnehmenden Studierenden auf der Fachtagung MEMO2010 – Methoden und Werkzeuge zur Verwaltungsmodernisierung präsentiert und mit Mitarbeitern und Experten aus dem öffentlichen Verwaltungsumfeld diskutiert.

Im ersten Teil gibt *Judith-Maria Bracke* einen Einblick in Merkmale und Eigenschaften von Skandalen, um dann anhand identifizierter Ablauf-, Aufbau- und Ursachenstrukturen historische IT-Skandale aus verschiedenen Bereichen der Gesellschaft zu untersuchen. Diese Untersuchung dient dem Überblick über vorhandene Problemfelder im Bereich des Einsatzes von IT. Im anschließenden Kapitel untersuchte *Willi Bühler* IT-Risiken in allgemeiner Form. Eine ausgedehnte Typologisierung der Risikoarten als Ergebnis dieser Arbeit soll dabei helfen, Risiken, welche durch den Einsatz von IT entstehen, sicherer erkennen und behandeln zu können. *Jan Ringas* widmete sich der Frage, welche Konsequenzen IT-Skandale haben können, wenn diese in der Öffentlichkeit thematisiert werden. Dabei spielen sowohl politische Organisationen als auch Publikationsorgane eine wichtige Rolle, um IT-Risiken in das Bewusstsein der Bevölkerung und die öffentliche Diskussion zu bringen. Aus diesem Grund werden Publikationsorgane und politische Organisationen vorgestellt, kategorisiert und deren Rolle in der öffentlichen Diskussion dargestellt.

Im zweiten Teil wurde untersucht, wie Unternehmen auf Risiken, welche durch den Einsatz von IT entstehen, reagieren können. Klassischerweise kann das Unternehmen

dabei mit typischen Risikostrategien (z. B. Risikovermeidung, Risikoreduzierung) versuchen, auf Risiken einzugehen. Risikostrategie und Risiken sind dabei vom Unternehmen abhängig, basieren sie doch auf der Frage, wie viel Risiko ein Unternehmen eingehen möchte, um bestimmte Chancen für sich zu eröffnen. So muss die Erstellung einer Unternehmensrisikostrategie unter Berücksichtigung der Risikotragfähigkeit, der technisch-organisatorischen Voraussetzungen und sonstiger relevanter Unternehmenseinflüsse erfolgen. Dabei sollte generell verhindert werden, dass Straftaten im Unternehmen oder aus dem Unternehmen heraus begangen werden können. Eine wichtige Rolle spielt dabei Compliance, wie *Mario Nolte* in seinem Kapitel herausarbeitete. Zur Herstellung der Compliance bedarf es organisatorischer Maßnahmen, welche mit Hilfe von Governance-Frameworks im Unternehmen implementiert werden können. Diese Frameworks wurden hier auf Berücksichtigung von rechtlichen Anforderungen untersucht. Eine weitere Möglichkeit, rechtliche Anforderungen organisatorisch einzubinden, stellt deren Berücksichtigung in der Prozessmodellierung dar. *Dominik Heddier* klassifizierte deshalb einige unterschiedliche Konzepte, welche zum einen Compliance-Anforderungen und rechtliche Anforderungen in Prozessmodellen explizieren und zum anderen die Rechtstreue automatisiert überprüfen. Auch die Zertifizierung von Anwendungssystemen und der Anwendungssystemerstellung spielt eine immer größere Rolle, da viele Unternehmen und Verbraucher sehr hohe Ansprüche an die Qualität und die Sicherheit von IT-Produkten haben. Deshalb sind formelle Nachweise der IT-Qualität beziehungsweise definierte Sicherheitsstandards sehr gefragt. *Stefan Laube* gibt zunächst eine Übersicht über die wichtigsten Zertifikate und ihre zu Grunde liegenden Standards, um anschließend darzustellen, welche Bedeutungen Zertifikate und Normen in der Rechtsprechung haben.

Der dritte Teil gibt einen Überblick über die Forschung in der Rechtsinformatik und im Informationsrecht. Dazu bereitete *Fabian Kohl* eine Forschungslandkarte, eine innovative Plattform zur Kommunikation von Forschungsergebnissen und Projekten, auf. Als schließende Klammer dieses Arbeitsberichts wurden in Zusammenarbeit mit *Fleur Fritz* vom Institut für Medizinische Informatik und Bioinformatik, *Eva-Maria Herring* und *Julia Seiler* vom Institut für Informations-, Telekommunikations- und Medienrecht, *Dominik Meiländer* vom Institut für Informatik sowie *Eric Meyer* vom Institut für Genossenschaftswesen Beiträge zur interdisziplinären Perspektive von Informationsrecht und Rechtsinformatik zusammengetragen.

Mein besonderer Dank gilt den genannten Studierenden des Vertiefungsmoduls Rechtsinformatik/Informationsrecht, die den Großteil des vorliegenden Arbeitsberichts verfasst haben, sowie den beteiligten Wissenschaftlern. Auch danke ich *Philipp Bergener*, *Mathias Eggert*, *Marcel Heddier*, *Sara Hofmann*, *PD Dr. Ralf Knackstedt* und *Dr. Michael Räckers* für die inhaltliche und redaktionelle Betreuung des Vertiefungsmoduls.

Münster im Oktober 2010 Prof. Dr. Jörg Becker

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AktG	Aktiengesetz
B2B	Business to Business
BCC	Backwards Compliance Checking
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BITCOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BPMN-Q	Business Process Modelling Notation Query
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik
BVDW	Bundesverband Digitale Wirtschaft
CC	Common Criteria
CEM	Common Methodology for Information Security Evaluation
CMMI	Capability Maturity Model Integration
CMMI-ACQ	CMMI for Acquisition
CMMI-DEV	CMMI for Development
CMMI-SVC	CMMI for Services
COSO	Comittee of Sponsoring Organizations of the Treadway Commission
COTS	Commercial off-the-shelf
CSI	5. ITIL Buch: Continual Service Improvement
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria
DEHSt	Deutsche Emissionshandelsstelle
DIN	Deutsches Institut für Normung
DTCC	Design-Time Compliance Checking
EAL	Evaluation Assurance Level
ELENA	elektronischer Entgeltnachweis
ElsterLohn	elektronische Lohnsteuererklärung
EN	Europäische Norm
FBRAM	Frame-based Requirements Analysis Method
FCC	Forward Compliance Checking
FCL	Formal Contract Language
G-CTL	Graphical Computational Tree Logic
GmbHG	Gesetz betreffend die Gesellschafen mit beschränkter Haftung
GoB	Grundsätze ordnungsgemäßer Buchführung
IDW	Institut der Wirtschaftsprüfer
IEC	International Electrotechnical Commission
iNTACS	International Assessor Certification Scheme
INTRSA	International Registration Scheme for Assessors
IRIS	Internationales Rechtsinformatik Symposium
ISMS	Informationssicherheits-Managementsysteme
ISO	International Organization for Standardization
IT	Informationstechnologie
ITIL	Information Technology Infrastructure Library
ITSEC	Information Technology Security Evaluation Criteria
ITSM	IT Service Management

KontraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
MiFiD	Markets in Financial Instruments Directive
MPG	Medizinproduktegesetz
OCL	Object Constraint Language
OGC	UK Office of Government Commerce
PCI DSS	Payment Card Industry Data Security Standard
PLTL	Past Linear time Temporal Logic
PMBoK	Project Management Body of Knowledge
PS	Prüfstandard
QM	Qualitätsmanagement
RAL-GZ	RAL Gütezeichen
REALM	Regulations Expressed As Logical Models
RTCC	Real-Time Compliance Checking
SD	2. ITIL Buch: Service Design
SEC	United States Securities and Exchange Commission
SEI	Software Engineering Institute
SLA	Service Level Agreement
SLM	Service Level Management
SO	4. ITIL Buch: Service Operation
SPICE	Software Process Improvement and Capability Determination
SQuaRE	Software product Quality Requirements and Evaluation
SSt	1. ITIL Buch: Service Strategy
ST	3. ITIL Buch: Service Transition
TCSEC	Trusted Computer System Evaluation Criteria
TGA	Trägergemeinschaft für Akkreditierung GmbH
TÜV	Technischer Überwachungs-Verein
UML	Unified Modeling Language
UPS	Uninterruptible power supply
USV	Unterbrechungsfreie Stromversorgung

I Klassifizierung von IT-Risiken und deren Thematisierung in der Öffentlichkeit

1 IT-Skandale – Ein historischer Überblick

Judith-Maria Bracke

1.1 Grundlagen zur Bedeutung und Betrachtung von Skandalen

1.1.1 Etymologische Betrachtung des Skandalbegriffes

Im Folgenden wird zunächst die Etymologie des Skandalbegriffes von dessen Ursprung aus entwickelt, bevor anschließend die grundlegenden Eigenschaften und Merkmale von Skandalen aufgezeigt werden, anhand derer im nachfolgenden Kapitel die Betrachtung vergangener IT-Skandale strukturiert wird. Nutzt man den Service einer Internetsuchmaschine, so ergibt die Suche nach dem Begriff „Skandal“ knapp 10 Millionen Ergebnisse und untermauert so den Eindruck, dass Skandale in der heutigen Zeit in den Medien allgegenwärtig sind. Die Existenz von Skandalen erstreckt sich über die Bereiche der Wirtschaft und Politik bis hin zu den Bereichen der Bildung, Religion und Kirche.[1] Grenzt man die Suche auf den Begriff „IT-Skandale“ ein, so ergeben sich immer noch mehr als 1,3 Millionen Suchergebnisse. In den folgenden Abschnitten wird durch die strukturierte Untersuchung mehrerer IT-Skandale verdeutlicht, wie zahlreich und weit verbreitet sich die Missstände im Bereich des Einsatzes von Informationstechnologie darstellen.

Der Ursprung des Begriffs „Skandal“ liegt im griechischen Wort „scàndalon“ sowie im lateinischen Wort „scandalum“. Über das dem Lateinischen entstammende französische Wort „scandale“ fand das Wort „Skandal“ im 16. Jahrhundert letztendlich seinen Weg in die deutsche Sprache. Hatte der Begriff der griechischen und lateinischen Sprache noch Bedeutungen wie „anstoßen“ oder „Ärgernis“, so konkretisierte sich die Bedeutung in der französischen und deutschen Sprache zu etwas, was gegen Sitten und Gebräuche verstößt, also als anstößiges Vorkommnis bezeichnet werden kann.[2]

In der Literatur existieren mehrere Definitionen des Skandalbegriffes. Im Folgenden seien vier Definitionen vorgestellt, um vor allem die Weiterentwicklung des Skandalverständnisses im Laufe der Zeit darzustellen. Im Bedeutungswörterbuch des Dudens ist ein Skandal ein „*Vorkommnis, Geschehen, das große Empörung hervorruft… Ärgernis, Aufsehen*“.[3] In

[1] Vgl. Kepplinger (2009), S. 196.
[2] Vgl. o. V. (1989).
[3] O. V. (1985).

englischsprachigen Lexika wird der Begriff des Skandals etwas genauer definiert und sowohl unter religiösen Gesichtspunkten *„discredit brought upon religion by unseemly conduct in a religious person“* als auch moralischen *„loss of or damage to reputation caused by actual or apparent violation of morality or propriety”* und gesellschaftlichen Gesichtspunkten „*a circumstance or action that offends propriety or established moral conceptions or disgraces those associated with it”*[4] betrachtet und erklärt.

Die dritte Definition stammt von dem Soziologieprofessor THOMPSON der Universität Cambridge, welcher im Zuge seiner wissenschaftlichen Ausarbeitungen eine Arbeitsdefinition des Skandalbegriffes benutzt, welche die bis dahin meist religiösen Assoziationen der Skandalbetrachtung außen vorlässt: *„As a working definition, we could say that ‚scandal' refers to actions or events involving certain kinds of transgressions which become known to others and are sufficiently serious to elicit a public response”.*[5] THOMPSON spricht in seiner Definition damit bereits drei grundlegende Faktoren eines Skandals an und zwar die Existenz einer Verfehlung, das Bekanntwerden dieser Verfehlung und die Reaktion der Öffentlichkeit darauf.

Eine in der aktuellen Literatur oft zitierte Begriffsdefinition ist die des Kommunikationswissenschaftlers KEPPLINGER, welche besagt, ein Skandal sei „*ein Missstand, der nach einhelliger Ansicht der Urteilenden bedeutend ist, vermeidbar gewesen wäre, durch schuldhaftes Verhalten hervorgerufen wurde und deshalb allgemein Empörung hervorruft.“*[6] Somit ist ein Skandal zunächst ein Missstand. KEPPLINGER folgert zudem, dass nicht jeder Missstand zu einem Skandal wird, jedoch den meisten Skandalen ein Missstand zu Grunde liegt.[7] Zur Konkretisierung der einen Skandal herbeiführenden Umstände nennt KEPPLINGER folgende fünf Bedingungen.

- Der Missstand muss als bedeutsam erscheinen.
- Der Missstand muss allgemein als vermeidbar erscheinen.
- Der Missstand muss durch schuldhaftes Verhalten verursacht worden sein.
- Die Bedeutsamkeit des Missstandes und die Art seiner Ursachen müssen allgemeine Empörung hervorrufen.
- Die allgemeine Empörung geht mit massiven Forderungen nach Konsequenzen einher.

[4] o. V. (2010m).
[5] Thompson (2000), S. 13.
[6] Kepplinger, Ehming & Hartung (2002), S. 81.
[7] Vgl. Kepplinger (2001), S. 62.

Die von KEPPLINGER erarbeitete Definition des Skandals besitzt den für diese Arbeit notwendigen Detailgrad zur Betrachtung eines Skandals und wird daher der Untersuchung der IT-Skandale zu Grunde gelegt.

Ausgehend von dieser Betrachtung ist zwischen der Entstehung und der Skandalierung eines Missstandes zu unterscheiden. Der Begriff Skandalierung beschreibt die Entwicklung eines Missstandes hin zu einem Skandal, welche erst durch Vorliegen der oben genannten Bedingungen stattfinden kann. Als grundsätzliche Voraussetzung ist zudem anzumerken, dass eine oder mehrere Personen Kenntnis vom Missstand haben und bestrebt sind, diesen Missstand in die Öffentlichkeit zu tragen. Im Umkehrschluss ist daraus zu folgern, dass nur diejenigen Missstände und Skandale in die Analyse dieses Artikels einbezogen werden können, die einer hinreichend großen Öffentlichkeit bzw. von den Medien bekannt gemacht und dokumentiert worden sind. Legt man hier als Beispiel die Sichtweise des Bundesdatenschutzbeauftragten Schaar zugrunde, so stellen die in der Öffentlichkeit bekannten und diskutierten Skandale zum Thema Datenschutz nur die „Spitze des Eisberges“ [8] dar.

1.1.2 Merkmale und Eigenschaften von Skandalen

Jeder Missstand ist in seinen Geschehnissen einzigartig und ohne weitere Strukturierung schwer mit anderen Missständen vergleichbar. Daher ist es notwendig vor einer näheren Untersuchung von Skandalen ein Bild über skandaltypische Abläufe, Rollen, Ursachen und Gesellschaftsbereiche zu entwickeln.

Skandaltypische Abläufe

Der Verlauf von Skandalen ist in der Regel vergleichbar und folgt vom Zeitpunkt des Skandalierungsbeginns bis zur Entscheidung über Konsequenzen einer Dramaturgie ähnlich der eines Theaterstückes.[9] Eine Einteilung des Skandalverlaufs in relevante Ereignisabschnitte kann anhand einer bereits existierenden Einteilung von öffentlichen Themen durch LUHMANN vorgenommen werden. LUHMANN gliedert den Ablauf öffentlicher Thematisierungen in fünf Phasen[10]: *Latente Phase, Durchbruchphase, Popularitätsphase, Kulminationspunkt* und *Ermüdungsphase.*

Dieser in Phasen gegliederte Ablauf kann auf den Verlauf von Skandalen übertragen werden und ergibt so fünf klar abgrenzbare Phasen der Skandalierung eines Missstandes:[11]

[8] Jahberg (2010).
[9] Vgl. Burkhardt (2006) S. 178; Kolb (2005), S. 120 ff.
[10] Vgl. Luhmann (1983), S. 18-19.
[11] Vgl. Burkhardt (2006), S. 181.

- *Latente Phase:*
  Der Missstand liegt vor aufgrund einer Verletzung von Gesetzen oder Normen. Diese Phase vor der Skandalierung kann eine Zeitspanne von Tagen oder auch Jahren umfassen. Während dieser Phase ist der Missstand mindestens den involvierten Personen bekannt und kann über Gerüchte bereits schon sog. Teilöffentlichkeiten, wie es z. B. Hauptstadtjournalisten sind[12], bekannt sein, ohne dass eine Initiierung der Skandalierung stattgefunden hat. Missstände können in die nächste Phase übergehen oder aber nie über diese erste Phase hinauskommen.

- *Durchbruchphase:*
  Diese Phase steht für den Beginn der Skandalierung. Der Missstand und begleitende Vorwürfe an den oder die Schuldigen werden in den Medien thematisiert und somit öffentlich gemacht.

- *Popularitätsphase:*
  In dieser Phase entscheidet es sich, ob die notwendige Bedingung der „allgemeinen Empörung" erfüllt wird und der Missstand zu einem Skandal wird. Die Popularitätsphase ist dadurch gekennzeichnet, dass einerseits die Empörung über Medienberichte widergespiegelt wird und andererseits der oder die in der Durchbruchphase identifizierte(n) Schuldige(n) mit Erklärungen und Rechtfertigungen an die Öffentlichkeit gehen.

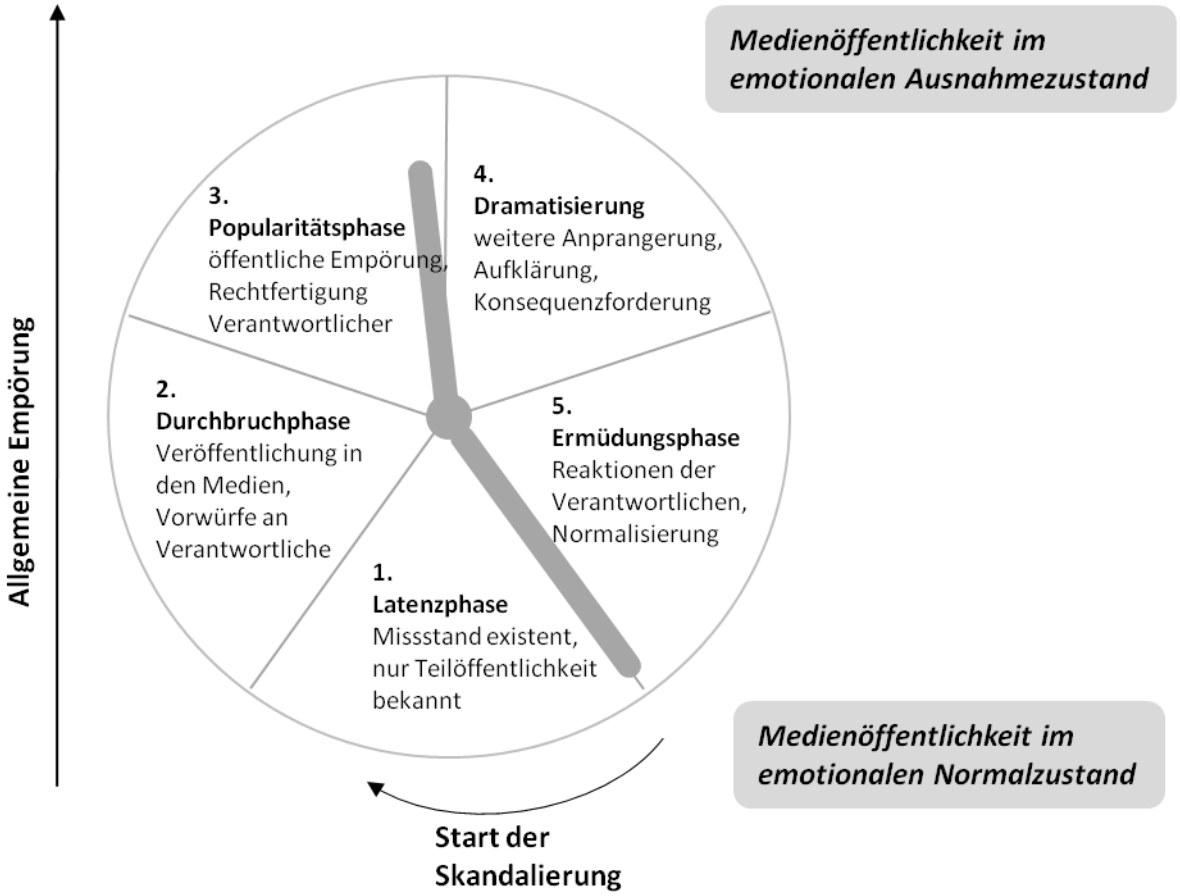
- *Dramatisierung:*
  Es folgt eine Zeit der weiteren öffentlichen Anprangerung, Rechtfertigung, Aufklärung und zuletzt der Forderung nach Konsequenzen. Der Druck auf die Verantwortlichen des Missstandes wächst und kann beispielsweise in Forderungen nach Rücktritt, Schadensersatz oder Gesetzesänderungen gipfeln.

- *Ermüdungsphase:*
  Diese Phase ist gekennzeichnet durch entsprechende Reaktionen seitens der verantwortlichen Personen oder Institutionen. Diese Reaktionen können z. B. Rücktritt, Entschuldigung oder Gesetzesänderungen sein und ziehen im Anschluss einen Rückgang des öffentlichen Interesses nach sich.

Die Phasen der Skandalierung zeichnen in ihrer Bedeutung und Ablauffolge sowohl ein Bild der journalistischen Berichterstattungsverläufe als auch der Höhen und Tiefen öffentlicher Empörung. BURKHARDT fasst die Phasen der Skandalierung und den einhergehenden

[12] Vgl. Burkhardt (2006), S. 179.

Grad der Empörung der Öffentlichkeit in einer „Skandaluhr“ zusammen, um die Dramaturgie der Skandalierung zu verdeutlichen (vgl. Abb 1.1).



Quelle: Burkhardt (2006).

Abb. 1.1 Die Skandaluhr als Phasenmodell der Skandalierung

Skandaltypische Akteure

So wie sich der Ablauf eines Skandals gemäß Abbildung 1.1 durch eine Phasenaufteilung strukturieren lässt, ist auch eine Strukturierung der beteiligten Akteure eines Skandals möglich. Es können acht unterschiedliche Rollen im Rahmen von Skandalierungen definiert werden:[13]

- *Verursacher*
  haben den skandalierten Missstand bewusst oder unbewusst herbeigeführt.

- *Nutznießer*
  profitieren vom Missstand, ohne dass sie ihn verursacht haben müssen.

[13] Vgl. Kepplinger, Ehming & Hartung (2002), S. 98 f.

- *Betroffene bzw. Geschädigte*
  erleiden Schaden durch den Missstand.

- *Skandalierte*
  werden öffentlich angeprangert für den Missstand, eventuell auch ungerechtfertigt.

- *Trittbrettfahrer*
  profitieren vom Skandal, ohne selbst als Skandalierer in Erscheinung zu treten.

- *Skandalierer*
  prangern den Missstand und die vermeintlichen oder tatsächlichen Verursacher an.

- *Informanten*
  sind Träger von Insider-Informationen, die den Missstand betreffen.

- *Außenstehende Beobachter*
  sind nicht in den Missstand involviert und verfolgen interessiert die Geschehnisse.

Die Rollen in einem Skandal schließen sich nicht notwendigerweise gegenseitig aus, so dass eine Person zur gleichen Zeit oder nacheinander auch mehrere Rollen einnehmen kann.

Skandaltypische Ursachen

Alle Missstände haben ihre Ursachen in sachlichen Gründen. Hier können gemäß KEPPLINGER neun verschiedene Gründe identifiziert werden[14]: *Fehlentscheidungen, Fehlentwicklungen, Unterlassungen und Passivität, Mangelzustände, Schäden, kriminelles und sittenwidriges Verhalten, Verfahrensmängel, Eigennutz* sowie *Missachtung legitimer Interessen.* Missstände können sowohl einen als auch mehrere dieser sachlichen Gründe zur Ursache haben.

Skandaltypische Gesellschaftsbereiche

Wie bereits im Eingangsabschnitt erwähnt, existieren Missstände bzw. ereignen sich Skandale in nahezu allen Bereichen der Gesellschaft beispielsweise der Wirtschaft, Kirche, Politik oder Bildung. Insgesamt können basierend auf der Studie von KEPPLINGER14 verschiedene Bereiche unterschieden werden[15]: *Politik, Wirtschaft, Infrastruktur, Soziales, Umwelt, Medien, Bildung, Recht & Sicherheit, Kultur, Finanzwesen, Privatleben & Individueller Bereich, Religion & Kirche, Gesundheitswesen* und *Sport & Freizeit.* Vom Gesell-

[14] Vgl. Kepplinger, Ehming & Hartung (2002), S. 31 f.
[15] Vgl. Kepplinger, Ehming & Hartung (2002), S. 37.

schaftsbereich des (skandalierten) Missstandes abgegrenzt werden muss der Charakter eines Geschehens.

Charakteristika von Missständen

Der Charakter eines Missstandes ist nicht abhängig vom Gesellschaftsbereich des Geschehens und kann durch mehr als nur eine Ausprägung gekennzeichnet sein. Die Ergebnisse aus KEPPLINGERs Studie zeigen insgesamt sieben mögliche Ausprägungen auf:

- *Politisch,*
- *wirtschaftlich,*
- *sozial,*
- *moralisch,*
- *ökologisch,*
- *rechtlich* und
- *kulturell*.[16]

Einzelne Missstände können zum Teil durch mehrere Ausprägungen charakterisiert werden, weil z. B. sowohl wirtschaftliche als auch politische Aspekte zu Grunde liegen. Es sei nochmals konstatiert, dass die charakteristischen Ausprägungen und die Gesellschaftsbereiche, in denen Missstände auftreten, nicht miteinander verknüpft sind. So kann ein Skandal in der Politik durchaus wirtschaftlicher Natur sein, ebenso wie in der Wirtschaft soziale oder politische Missstände eintreten können.[17]

1.2 Untersuchung von IT-Skandalen

1.2.1 Abgrenzung des Betrachtungshorizonts von IT-Skandalen und „Untersuchungsmethodik“

Da der Einsatz von Informationstechnologie heute in allen Gesellschaftsbereichen Realität ist, bietet sich eine entsprechende Vielzahl von (skandalierten) Missständen aus eben diesen Bereichen. Die Betrachtung von IT-Skandalen über alle Bereich hinweg wäre zwar von hohem Interesse, ist aber im gegebenen Rahmen nicht umzusetzen. Daher wird eine Ein-

[16] Vgl. Kepplinger, Ehmig & Hartung (2002), S. 35 f.
[17] Vgl. Kepplinger, Ehmig & Hartung (2002), S. 36.

grenzung der 14 identifizierten Bereiche auf vier in die Analyse einzubeziehende Gebiete vorgenommen. Ausschlaggebende Kriterien für die Betrachtung eines Bereichs sind zum einen die Häufigkeit skandalierter Missstände in den vergangenen Jahren und zum anderen die Bedeutung dagewesener Skandale. Die Bedeutung eines Skandals ist durch viele unterschiedliche Kriterien bestimmbar, jedoch sollen hier ausschlaggebend die Zahl an Betroffenen, das Ausmaß des verursachten Schadens (materieller oder immaterieller Art) sowie die dem Skandal zu Grunde liegende Motivation der Verursacher mit einbezogen werden.

Gemessen an der Häufigkeit von Missständen sind laut der empirischen Analyse von KEPPLINGER ET AL. die Bereiche Wirtschaft, Politik sowie Verkehrswesen und Infrastruktur am häufigsten betroffen.[18] Die Recherche nach skandalierten Missständen in deutschen Tages- bzw. Onlinezeitungen (vgl. Anlage A) unterstützt diese Ergebnisse einerseits, ergibt aber auch Schwerpunkte in den Bereichen des Finanzwesens und des Gesundheitswesens. Hierbei ist Skandalen im Bereich des Gesundheitswesens allein aufgrund der Sensibilität der zu verarbeitenden Daten und der aktuellen Entwicklungen im Gesundheitswesen im Bereich des Einsatzes von IT eine verstärkte Aufmerksamkeit zuzuwenden.

Die Gesellschaftsbereiche Finanzwesen, Politik und Verwaltung sowie Gesundheitswesen werden aufgrund der Konzentration von skandalierten Missständen im Bereich des Einsatzes von Informationstechnologie bei gleichzeitig inhaltlich heterogenen Skandalsachverhalten in die nähere Untersuchung mit einbezogen. Durch die den Skandalen zu Grunde liegenden Sachverhalte kann ein relativ breites Bild der (Problem-)Situation im Bereich des Einsatzes von IT entwickelt werden.

Die übrigen Gesellschaftsbereiche werden nicht in die Untersuchung mit einbezogen, beanspruchen aber alle für sich die Existenz von Missständen und Problemen im Bereich des Einsatzes von Informationstechnologie. Im Rahmen der in Anlage A aufgeführten Liste vergangener IT-Skandale können zu einigen dieser Bereiche mehrere Vorfälle vergangener Jahre eingesehen werden.

Die Analyse der Skandale wird anhand der Bearbeitung und Beantwortung zentraler Leitfragen vorgenommen, um ein klar strukturiertes und umfassendes Bild der untersuchten Geschehnisse zu erhalten. Die Leitfragen sind in ihrer Struktur an die in den Abschnitten zuvor behandelten Eigenschaften und Merkmale von Missständen und Skandalen angelehnt:

1. Wie war der Zustand vor Eintreten des Missstandes?

[18] Vgl. Kepplinger, Ehming & Hartung (2002), S. 35.

2. Wie tritt der Missstand ein bzw. welche Geschehnisse führen zum Missstand?
3. Welche sachlichen Gründe und Charakteristika liegen dem Missstand zugrunde?
4. Wodurch ist der Ablauf der Skandalierung gekennzeichnet?
5. Welche Konsequenzen – sowohl kurz- als auch langfristig – entstanden aus dem Skandal?

Das Ziel dieser leitfragenorientierten Vorgehensweise und damit verbundenen Informationsbreite und -tiefe ist es, zu Grunde liegende Problemfelder und Handlungsbedarfe, welche in ihrer Vielzahl und inhaltlichen Weite in den nachfolgenden Abschnitten weiter behandelt werden, zu identifizieren.

Die der Skandal-Analyse zu Grunde liegenden Quellen sind vorrangig Presseartikel deutscher Zeitungen und Magazine. Die Skandalierung von Missständen erfolgt zwar immer wieder auch durch entsprechende Berichterstattung in TV und Rundfunk, aber es zeigt sich, dass über die Gesamtheit an Skandalen hinweg – gerade im Hinblick auf eher regionale Skandale – keine durchgängige und tiefgehende Berichterstattung stattfindet. Um somit eine homogene Basis der Betrachtung einzelner Skandale zu erstellen, erfolgt die Einschränkung relevanter Quellen ausschließlich auf Artikel der Print- und Onlinemedien.

Auf Grund der effizienteren Analysemöglichkeit ist die Suche ausschließlich auf Online-Portalen durchgeführt worden. Dabei wurden etablierte, überregionale und regionale Zeitungsportale bzw. die Archive dieser Portale unter Verwendung folgender Schlagworte durchsucht: *„Skandal“*, *„IT-Skandal“, „Datenschutz“, „Datenskandal“, „Datenpanne“, „Datendiebstahl“, „Datenklau“, „IT-Panne“, „Internetkriminalität“ „Phishing*“ und *„Cyberkriminalität*“. Die Archive der *„Frankfurter Allgemeine Zeitung“*, der *„Financial Times Deutschland“*, des *„Spiegel Online“*, der *„Süddeutschen Zeitung“*, der *„Zeit“* und des *„Stern“* ermöglichten durch die zahlreichen Suchergebnisse einen Blick bis in die Anfänge der Informationstechnologie und der damit verbundenen ersten Skandale im Jahr 1968.

Ausgehend von den ersten Suchergebnissen meist überregional bekannter IT-Skandale ermöglichte die Suchmaschine „*Google*“ eine vertiefte Recherche und Analyse einzelner Vorfälle über Einträge und Artikel in Blogs, Online-Zeitschriften und Online-Netzwerken, wie beispielsweise *„Heise online“, „Computerwoche“*, *„Glasdemokratie.to“*, *„bigbrotherawards.de“*, *„datenleck.net“*, *„projekt-datenschutz.de“*, *„techchannel.de“*, oder *„ZDNet.de“*. Die zur Suche genutzten Schlagworte waren zum einen konkrete Begriffe bereits bekannter IT-Skandale und zum anderen die bereits vorher genutzten Schlagworte. Die weitere Recherche erfolgte einerseits über den jeweiligen Artikeln zu-

geordnete themengleiche Artikel und andererseits über in diesen Portalen existierende „Skandal-Listen“. Die Skandal-Listen führten die Recherche auf eine neue Ebene, da hier insbesondere nur regional bekannte IT-Skandale aufgelistet sind und die Online-Portale entsprechender regionaler Zeitungen zur weiteren Recherche herangezogen werden können.

Durch die Betrachtung mehrerer Quellen zu einzelnen Skandalthemen soll sichergestellt werden, ein möglichst objektives und umfassendes Bild des betrachteten Analyseobjekts zu erhalten. Sofern es einer Objektivierung des Sachverhaltes dienlich ist, werden zudem die Inhalte offizieller Online-Seiten des Bundes bzw. der Bundesländer in die Analyse mit einbezogen. In diesem Zusammenhang ist zu beachten, dass sich auch durch Berichte unterschiedlicher Medien nicht zwingend eine objektive Sichtweise ergeben muss, da diese bestenfalls erst durch die Gesamtheit an Informationen aller skandaltypischen Akteure zu erreichen wäre.

1.2.2 Die historische Entwicklung von IT-Skandalen

In der heutigen Zeit und Gesellschaft ist der Einsatz von Informationstechnologie (IT) zweifellos unverzichtbar. IT umfasst „alle technischen Einrichtungen, welche dazu dienen Informationen technisch zu bearbeiten“.[19] Durch den Einsatz von IT können Aufgaben schneller und einfacher erledigt und Abläufe störungsfreier und flexibler gestaltet werden.[20] IT-Skandale sind Skandale, die aufgrund des (teils unzureichend gesicherten) Einsatzes von Informationstechnologie entstehen konnten. Somit ist das zentrale Kriterium, welches zur Auswahl und Betrachtung von Skandalen herangezogen wird, der Einsatz von IT und die aus diesem Einsatz resultierenden Missstände.

Die Einschränkung der betrachteten Skandale auf diejenigen Skandale mit Bezug zur Informationstechnologie legt im Weiteren den Zeitraum der betrachteten Skandale fest auf die Zeit der 1960er-Jahre bis heute. Mit der Erfindung und Entwicklung der elektronischen Datenverarbeitung in den 1960er-Jahren vollzog sich auch im Rahmen der Informationsverwaltung der BRD der bedeutende Schritt von der Papier- bzw. Karteikartenverwaltung hin zur elektronischen Speicherung und Verarbeitung von Daten. Einhergehend mit der rasanten Entwicklung der elektronischen Datenverarbeitung (EDV) in den öffentlichen Verwaltungen der BRD wuchsen in Juristen- und Verwaltungskreisen die Diskussionen um die Notwendigkeit neuer gesetzlicher Datenschutzregelungen, welche im Rahmen der geplanten Einführung eines zentralen Bundes-Datenbanknetzes ihren Höhepunkt fanden. Die Grundidee des Bundes-Datenbanknetzes bestand darin, eine zentrale Datenbank einzufüh-

[19] Wildhaber (1993), S. 8.
[20] Vgl. Pohlmann (2006), S. 405.

ren, welche die Daten aller Bundesbürger beinhaltet und über entsprechende Bürger-Personenkennzeichen-Zuordnungen alle Daten den entsprechenden Bürgern zuordenbar und abrufbar macht.

Die Veröffentlichung der Pläne zu einer zentralen Speicherung aller Bürgerinformationen und der Einführung eines Personenkennzeichens lösten Ende der 1970er-Jahre die ersten intensiven Diskussionen in der Öffentlichkeit über den Einsatz von EDV in der öffentlichen Verwaltung und den Umgang mit personenbezogenen Daten aus. Die Ergebnisse dieser intensiven Auseinandersetzungen führten nicht nur zur Zerschlagung der Pläne eines zentralen Bundes-Datenbanknetzes, sondern hatten im weiteren Verlauf auch die ersten gesetzlich manifestierten Regelungen – zunächst nur auf Ebene der Bundeländer – zum Datenschutz zur Folge. Hierbei ist hervorzuheben, dass mit der Erlassung des ersten Gesetzes zum Datenschutz das Bundesland Hessen 1970 das weltweit erste und bis heute älteste formelle Datenschutzgesetz verabschiedete.[21]

Dieser Rückblick in die Anfänge der EDV zeigt, wie eng bereits damals der Einsatz von IT und die Existenz bzw. Entwicklung entsprechender rechtlicher Regelungen, die im Rahmen des IT-Einsatzes einzuhalten sind, verknüpft waren. Im Weiteren ist der Verlauf der letzten Jahrzehnte durch die rasante Verbreitung und den zunehmenden Einsatz von komplexer strukturierter Hard- und Software gekennzeichnet. Auch wenn Veränderungen der Rechts- und Gesetzeslage nicht in dem gleichen Maße stattgefunden haben, so gibt es z. B. im Bereich des Bundesdatenschutzgesetzes (BDSG) wichtige Veränderungen bzw. Meilensteine zu konstatieren. Das BDSG nimmt insofern eine bedeutende Rolle bei der historischen Betrachtung von IT-Skandalen ein, als dass die Recherche nach IT-Skandalen ergab, dass einem Großteil damaliger und auch heutiger IT-Skandale der Missbrauch von Daten zu Grunde liegt.

Eine Auflistung sämtlicher recherchierter IT-Skandale im Zeitraum von 1965 bis heute kann der Anlage A entnommen werden. Trotz einer nicht vollständigen Abbildung aller recherchierten IT-Skandale illustriert Abbildung 1.2 die steigende Häufigkeit von IT-Skandalen in den letzten drei Jahren. Eine eindeutige Erklärung für die Zunahme von IT-Skandalen kann nicht gegeben werden, da mindestens zwei Faktoren für den Anstieg verantwortlich gemacht werden können:

- Entwicklung der weltweiten Vernetzung durch das Internet und entsprechende Online-Medien, welche Informationen unmittelbar und schneller an die Öffentlichkeit gelangen lassen, als es früher jemals der Fall war.

[21] Vgl. Ishii & Lutterbeck (2000).

- Zunehmende Komplexität eingesetzter IT in allen relevanten Gesellschaftsbereichen führt zu komplexeren Problemen und Schwachstellen, welche im schlimmsten Falle in IT-Skandalen gipfeln können.

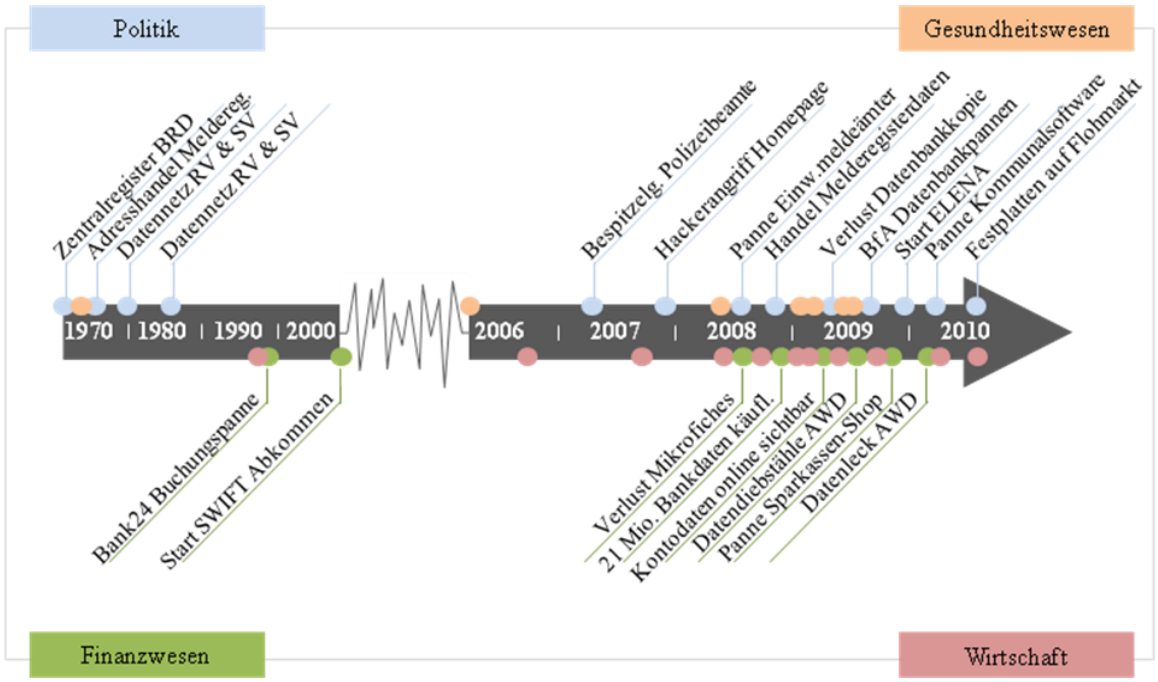
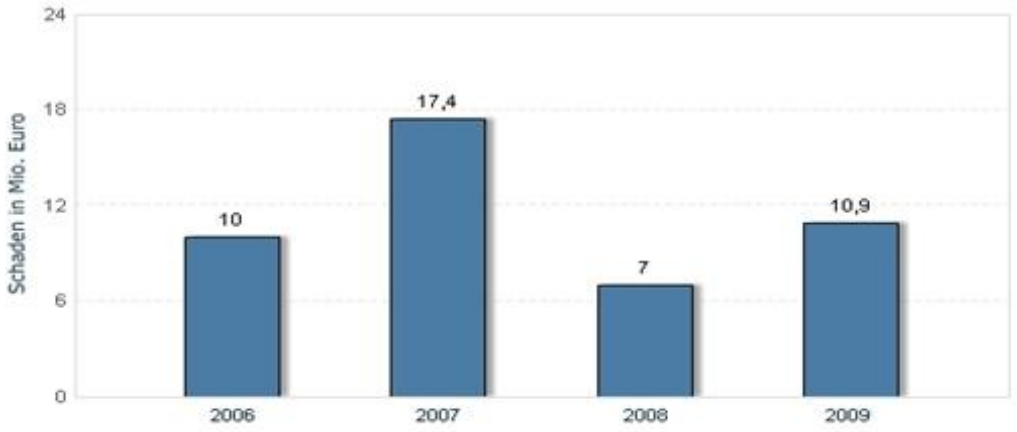


Abb. 1.2: IT-Skandale in Politik, Finanzwesen, Gesundheitswesen und Wirtschaft

Von den bisher betrachteten IT-Skandalen abzugrenzen ist die kriminelle Nutzung von IT gegenüber Privatpersonen. Dies kann in Form von Hackerattacken, Virusinfektionen oder dem sogenannten Phishing auftreten und hat sowohl den Schaden der angegriffenen Person zum Ziel als auch das Ziel der persönlichen Bereicherung von Seiten des Angreifers. Insbesondere beim Phishing, welches eine Wortzusammensetzung von „Passwort“ und „Fishing“ darstellt,[22] ist laut den Statistiken des Bundeskriminalamtes weiterhin ein Zuwachs der Fallzahl sowie des entstandenen Schadens zu verzeichnen. Wie es die Zahlen der Abbildung 1.3 vermuten lassen, haben die Vorfälle nach einem Rückgang im Jahr 2008 in Deutschland wieder zugenommen. Im Jahr 2009 wurden ca. 2.900 Phishing-Fälle gemeldet.[23]

Der historische Rückblick zeigt insgesamt, dass schon in der jüngsten Zeit der IT-Nutzung Missstände entstanden und skandaliert wurden und dass im Verlauf der Jahrzehnte bzw. insbesondere der letzten vier Jahre eine signifikante Steigerung bezüglich der Häufigkeit von IT-Skandalen zu verzeichnen ist.

[22] Vgl. o. V. (2010).
[23] Vgl. BITKOM (2010).



Quelle: Vgl. BITKOM (2010).

Abb. 1.3: Höhe des finanziellen Schadens (in Mio. Euro) durch Phishing in Deutschland seit 2006

1.2.3 Analyse bedeutender IT-Skandale

Die Untersuchung wird für die im vorherigen Kapitel ausgewählten jeweiligen gesellschaftlichen Bereiche durchgeführt. Eine Verteilung der betrachteten IT-Skandale und deren betroffener Gesellschaftsbereiche sind in Abbildung 1.4 aufgeführt.

Aus der Verteilung geht hervor, dass insbesondere die Gesellschaftsfelder Finanzwesen, Politik und Wirtschaft von besonderer Bedeutung sind. Diese Bereiche haben sowohl die meisten dokumentierten Fälle als auch die meisten von dem IT-Skandal betroffenen bzw. geschädigten Personen.

Finanzwesen

Phishing-Attacke auf CO_2-Emissionshändler:
In Anlehnung an die Vereinbarungen zur Treibhausgasreduzierung des Kyoto-Protokolls werden in Deutschland seit 2005 sogenannte Abgasrechte (Rechte zum Ausstoß von Treibhausgasen) zwischen Industrieunternehmen und Energieerzeugern gehandelt, um somit in kurzer Zeit Einsparungen beim Ausstoß des klimaschädlichen Gases CO_2 zu erreichen.[24] Überflüssige bzw. fehlende Abgasrechte werden von CO_2-Emissionshändlern über ihre jeweiligen Handelskonten bei der Deutschen Emissionshandelsstelle (DEHSt) an der Börse gehandelt.

[24] Vgl. Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (2010).

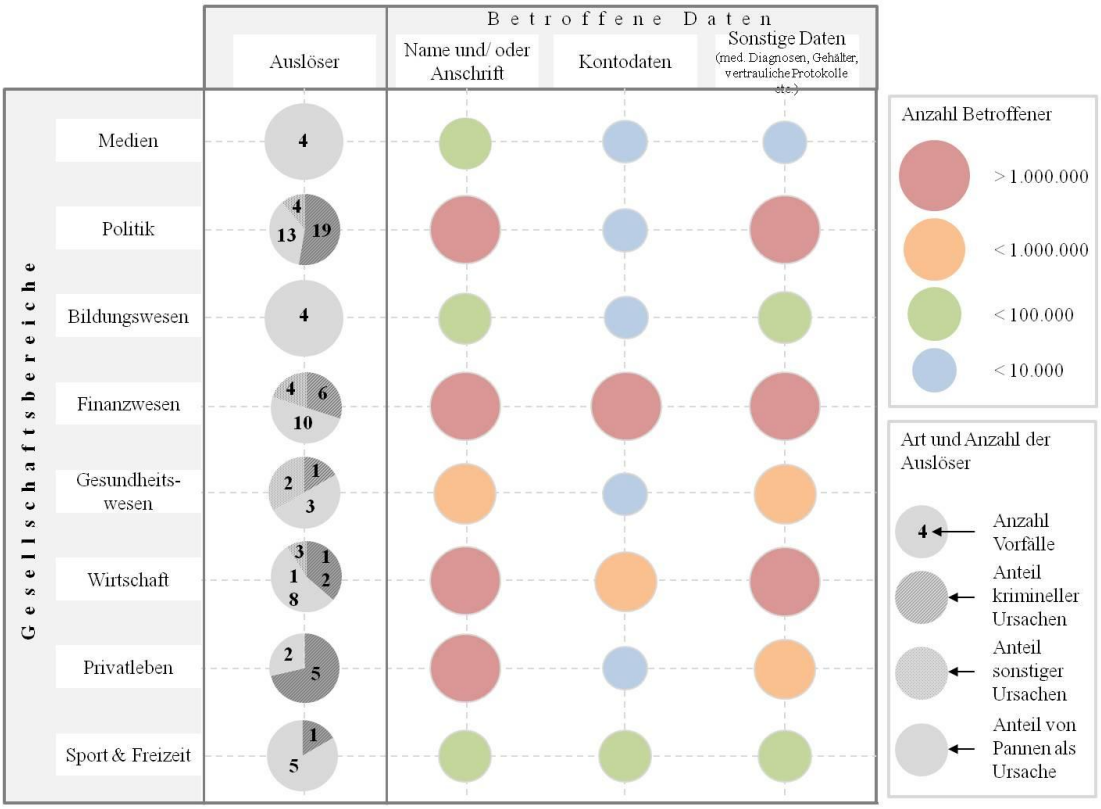


Abb. 1.4: Überblick IT-Skandale von 1968-2010 und deren Gesellschaftsbereiche

Am Morgen des 28. Januar 2010 versendeten Betrüger eine E-Mail an bis zu 16.680 bei nationalen Registern registrierte CO_2-Emissionshändler bzw. Handelskontobevollmächtigte von Unternehmen im In- und Ausland und gaben sich als die jeweils nationale Registerbehörde des Emissionshandels aus.[25] Die Mail gab an, vor Sicherheitslücken im Rahmen des Emissionshandels zu warnen, und forderte die Händler dazu auf, einen Prozess zur Installation eines zusätzlichen Sicherungspaketes anzustoßen, welches von einer angeblichen Sicherheitsfirma zur Verfügung gestellt wurde. Außerdem forderte die Mail dazu auf, die sonstigen Kontodaten zu überprüfen und dem zur Vereinfachung bereitgestellten Link zu folgen. Durch das Verwenden des Links und die Eingabe der Nutzerdaten samt Passwort konnten die Daten abgefangen werden und wurden innerhalb kürzester Zeit dazu genutzt, das jeweilige Handelskonto durch Übertragung der Zertifikate auf Konten in Dänemark und England zu leeren.

Insgesamt konnten so 250.000 Zertifikate gestohlen und an nichtsahnende Unternehmen weiterverkauft werden. Diese erwarben die Zertifikate im guten Glauben, was somit eine Rückabwicklung der Transaktionen für die bestohlenen Unternehmen unmöglich machte und ein Schaden von knapp 3,3 Millionen Euro verursachte. Allein ein einzelnes Unter-

[25] Vgl. Kroehnert (2010), S. 1 f.

nehmen hatte hierbei einen Schaden in Höhe von 1,2 Millionen Euro zu verbuchen.[26] Als Ursachen für diesen Missstand können sowohl kriminelle Absichten als auch Verfahrensmängel festgestellt werden. Verfahrensmängel deshalb, weil gemäß des Benutzerhandbuches der DEHSt vorgesehen ist, dass Transaktionen auf den Handelskonten nur durch zwei Kontobevollmächtigte, also durch Eingabe von zwei Passwörtern, durchgeführt werden können. Wäre diese Regelung bei allen CO_2-Emissionshändlern beachtet worden, hätte mit den einzeln abgefangenen Nutzernamen und Passwörtern kein Missbrauch betrieben werden können.

Die Skandalierung des Missstandes in den Fachmedien begann unmittelbar am Tag des Betrugs, noch bevor der mögliche Schaden beziffert werden konnte. Nachdem der Schaden konkret beziffert werden konnte, fand der Skandal drei Tage später auch Erwähnung in den überregionalen Tageszeitungen und wurde zumeist mit „weiterer Skandal" betitelt, da im Rahmen vergangener und gegenwärtiger Mehrwertsteuerbetrügereien bereits Schäden in dreistelliger Millionenhöhe verursacht wurden. Die durch die Medien ebenfalls angeprangerte Registrierungsstelle DEHSt wies jegliche Mitverantwortung für die Geschehnisse von sich[27], auch wenn erst am späten Nachmittag eine Mail mit einem entsprechenden Warnhinweis an alle Kontoinhaber versandt wurde.[28] Knapp drei Wochen nach dem Vorfall äußerte sich die DEHSt nochmals zu Vorwürfen der Mitverantwortung und verkündete gleichzeitig eine Erhöhung der Sicherheitsvorkehrungen durch Einfuhr einer Signaturkarte und langfristig auch durch die zukünftige Nutzung des elektronischen Personalausweises.[29] Anfang Juli, also Monate später, wurde in den Medien bekanntgegeben, dass das mit 1,2 Mio. Euro am meisten geschädigte Unternehmen, die Papierfirma Drewsen, Klage gegen die DEHSt einreichte, da aufgrund mangelnder Sicherheitsvorkehrungen im Zertifikate-Handel der Diebstahl der Zertifikate überhaupt erst möglich gemacht wurde.[30]

Politik und Verwaltung

Elektronischer Entgeltnachweis (ELENA):
Das Projekt ELENA stellt zwar (noch) keinen klassischen IT-Skandal dar, jedoch zeigt es in seiner Konzeption und Umsetzung mehrere kritische Themen auf, welche in naher Zukunft zum Auftreten eines Missstandes und einem anschließenden Skandal führen könnten. Ausgangspunkt des Projektes ELENA ist die sogenannte Doppelbürokratie bei der Beantragung von Sozialleistungen durch Arbeitnehmer. Möchte ein Arbeitnehmer Sozialleistungen wie z. B. Wohngeld beantragen, so wird ein entsprechender Antrag bei einer Be-

[26] Vgl. Gassmann (2010a).
[27] Vgl. Gassmann (2010b).
[28] Vgl. Kroehnert (2010), S. 2.
[29] Vgl. Gassmann (2010c).
[30] Vgl. Gassmann (2010d).

hörde abgeholt und zum Ausfüllen an den Arbeitgeber weitergegeben. Der Arbeitgeber füllt den schriftlichen Antrag aus (alle dazu notwendigen Daten liegen beim Arbeitgeber bereits in elektronischer Form vor) und gibt diesen zurück an den Arbeitnehmer, welcher wiederum zur Behörde geht und den Antrag einreicht. Dort wird der Antrag elektronisch erfasst, berechnet und in einem nachfolgenden Bescheid bewilligt oder abgelehnt.[31] Aus Gründen der Effizienzsteigerung und Kosteneinsparung wurde das Projekt ELENA ins Leben gerufen. Ab Januar 2010 sind alle Arbeitgeber dazu verpflichtet worden, einen festgelegten Satz von Arbeitnehmerdaten je Arbeitnehmer elektronisch an ein Zentralregister zu übermitteln. Die im Rahmen des ELENA-Projekts zur Verfügung gestellte Datei zum Überblick über die übermittelten Datensätze bzw. Datensatzbausteine umfasst 42 Seiten. Dem Anhang B kann eine grobe Zusammenfassung der übermittelten Daten entnommen werden.

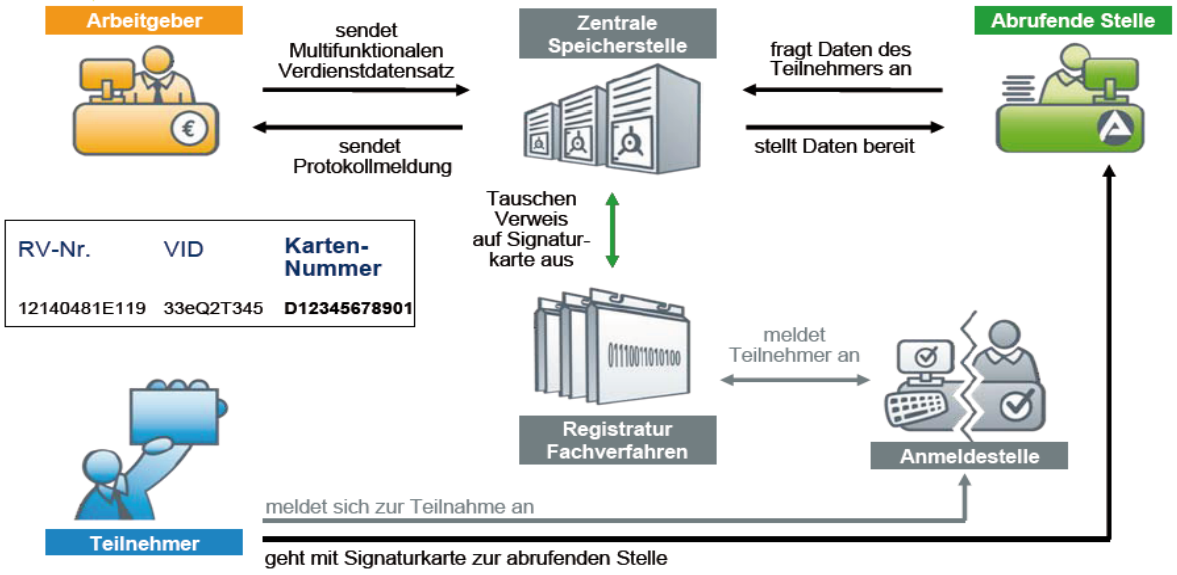
Insgesamt werden so seit Januar 2010 die Daten von knapp 40 Millionen Beschäftigten an die zentrale Speicherstelle übermittelt und abgespeichert. Ein antragstellender Arbeitnehmer kann ab 2012 mit Hilfe einer Signaturkarte den Abruf seiner Daten aus der zentralen Speicherstelle ermöglichen und so eine Bearbeitung und Berechnung seines Antrags erwirken (vgl. Abbildung 1.5). Im Rahmen von ELENA ist bisher kein für die Öffentlichkeit bedeutender Missstand im Zusammenhang mit dem IT-Einsatz eingetreten, der skandaliert hätte werden können. Trotzdem wird das Verfahren an sich in den Medien beständig thematisiert und angeprangert. Die Kernpunkte dieser medialen Proteste sind dabei der Umfang und die Sensibilität der gespeicherten Daten, die fehlende Freiwilligkeit und Möglichkeit, nicht an der Datenübertragung teilzunehmen sowie die Speicherung der Daten „auf Vorrat“, d. h. viele Daten werden abgespeichert, ohne dass der entsprechende Arbeitnehmer vielleicht jemals soziale Leistungen beantragt. Die Speicherung findet also nur präventiv statt, was hinsichtlich der Sensibilität und des Umgangs der Daten die Frage nach der Angemessenheit aufwirft. Der Höhepunkt der Skandalierung des ELENA-Verfahrens schien Ende März 2010 erreicht, als beim Bundesverfassungsgericht eine von 22.000 Bürgern unterstützte Verfassungsbeschwerde gegen das ELENA-Verfahren eingereicht wurde.[32]

Unabhängig von den bereits in den Medien thematisierten Kritikpunkten sind unter dem Gesichtspunkt möglicher zukünftiger IT-Skandale im Rahmen von ELENA weitere wichtige Kernfragen identifizierbar:

- Wie wird der (aufgezwungene) Einsatz der Signaturkarte vor Missbrauch geschützt?

[31] Vgl. Deutsche Rentenversicherung & Bund (2010).
[32] Vgl. FoeBuD e.V. (2010).

- Wie wird die Integrität der gespeicherten Daten sichergestellt?
- Wie ist gewährleistet, dass auch kleine und mittelständische Betriebe mit ausreichender Soft- und Hardware ausgestattet sind, um eine sichere Übertragung der Daten zu gewährleisten?
- Welche Maßnahmen werden getroffen, um die unverschlüsselte Übertragung der Daten vor Diebstahl oder Manipulation zu schützen?
- Welche Maßnahmen – zusätzlich zur Verschlüsselung der Daten – werden getroffen, um den unauthorisierten Datenzugriff oder Datenmanipulation im Rahmen der Speicherung zu verhindern? Bietet die Verwendung eines zentralen Schlüssels ausreichend Sicherheit?
- Wie wird sichergestellt, dass die gespeicherten Daten nach vier Jahren gelöscht werden? Welche Maßnahmen existieren, um eine ordnungsgemäße „Entsorgung" der Daten zu gewährleisten?



Quelle: Deutsche Rentenversicherung (2010).

Abb. 1.5: Das ELENA-Verfahren im Überblick

Dies seien nur die unter IT-Gesichtspunkten besonders kritischen Punkte bezüglich des ELENA-Verfahrens. Diese Fragen basieren zum Teil auf den Erfahrungen aus vergangenen IT-Skandalen im Bereich der Politik. Als Beispiel sei hierzu auf den Vorfall in deutschen Kommunen im April 2010 verwiesen. Eine in etwa 800 Kommunen eingesetzte Software sorgte dafür, dass interne Dokumente wie z. B. Protokolle nicht öffentlicher Sitzungen oder andere vertrauliche Dokumente für jedermann im Internet abrufbar waren.

Grund hierfür war weniger eine Sicherheitslücke in der Software, sondern eine nicht sicherheitsgerechte Installation und Einrichtung des Systems. Durch die Befolgung der durch den Softwarehersteller gegebenen Sicherheitshinweise und Installationsanleitungen hätte die Datenpanne vermieden werden können. Dies war in mehreren hundert Kommunen nicht der Fall.[33] Weitere Beispiele ergeben sich aus den Fällen nicht ordnungsgemäßer Entsorgung von sensiblen Daten in öffentlichen Verwaltungen. Sei es, dass Festplatten mit sensiblen Steuerdaten auf dem Flohmarkt auftauchten[34] oder dass auf Computern von Softwarefirmen mit echten anstatt mit Testdaten ein neues Softwaresystem für ein Rathaus getestet wurde und durch fehlendes Löschen 400.000 sensible Daten in fremde Hände gelangten.[35] Diese und andere IT-Skandale aus der Vergangenheit sind es, die das Misstrauen gegenüber dem als „Datenmonster" betitelten ELENA-Verfahren erhöhen. Der Status quo im Fall ELENA kann abschließend folgendermaßen charakterisiert werden:

- Aufgrund der scharfen Kritik am Umfang der gespeicherten Daten wurden Anfang des Jahres 2010 bereits Anpassungen am zu übermittelnden Datensatz vorgenommen und eine weitere Überarbeitung nicht ausgeschlossen.[36]

- Noch im März, also bereits drei Monate nach Start des ELENA-Verfahrens, verhinderten technische Probleme eine reibungslose Datenverarbeitung bei der zentralen Speicherstelle sowie eine ordnungsgemäße Dokumentation seitens der Unternehmen.[37]

- Anfang Juli führten die Verachtfachung der kalkulierten Kosten des ELENA-Verfahrens und andauernde technische Mängel zu ersten Äußerungen seitens der Regierung, das Verfahren „auf Eis zu legen".[38] Vier Wochen nach diesen ersten Äußerungen und breiter Zustimmung seitens Politik und Wirtschaft schien das vorläufige Ende des ELENA-Verfahrens beschlossene Sache zu sein. Eine endgültige Entscheidung wird erwartet.[39]

Es bleibt somit abzuwarten, ob und wann das ELENA-Verfahren gestoppt wird und inwiefern anschließend Änderungen und Nachbesserungen für eine langfristige Wiederaufnahme durchgeführt werden.

[33] Vgl. Wolters, Theo & Ostrop (2010) und Schömig (2010).
[34] Vgl. Richter (2010).
[35] Vgl. Rüeck & Römer (2010).
[36] Vgl. Patalong (2010).
[37] Vgl. Klein (2010).
[38] Vgl. Dpa (2010).
[39] Vgl. Siegmund (2010).

Gesundheitswesen

IT-Probleme beim Universitätsklinikum Hamburg:

Das als „modernstes Krankenhaus Europas“ bezeichnete Universitätsklinikum Hamburg (UKE) stellt aufgrund seiner Fortschrittlichkeit und IT-Einbindung einen Krankenhaus-Prototyp der Zukunft dar. Mit der im Februar 2009 stattgefundenen Eröffnung eines neuen Gebäudekomplexes wurde auch eine neue Computertechnik in Betrieb genommen. Patientenakten existieren nur noch in elektronischer Form und Ärzte nehmen zu ihren Visiten einen Computer mit.[40]

Im Zusammenhang mit dem Krankenhausaufenthalt einer prominenten Patientin trat der erste IT-Skandal des UKE auf. Nachdem sie im Januar operiert worden war, drangen Informationen über deren Gesundheitszustand an die Öffentlichkeit. Möglich war dies durch die hauseigene Software zur Verwaltung der elektronischen Krankenakten, welche nahezu allen 5.800 Mitarbeitern des UKE den Zugriff auf alle Informationen aller existierenden Krankenakten gewährte. Dies ermöglichte es mehreren Mitarbeitern des UKE, aus reiner Neugierde Einblick in die Krankenakte einer Patientin zu nehmen und sogar die gewonnenen Informationen an die Öffentlichkeit weiterzugeben. Nach Überprüfung der Zugriffsprotokolle stellte das UKE Strafanzeige aufgrund der Weitergabe personenbezogener Daten und erließ die interne Regelung, dass Zugriffe auf Patientendaten außerhalb des Ermächtigungskreises ohne medizinischen oder administrativen Anlass verboten seien. Eine Veränderung des Zugriffsrechtemanagements scheint allerdings nicht erfolgt zu sein.[41]

Etwa drei Monate nach dem ersten IT-Skandal folgte der zweite kritische IT-Vorfall im Hamburger Universitätsklinikum. Aufgrund eines zwölfstündigen Ausfalls des Computersystems im Labor der UKE musste die Notaufnahme für mehrere Stunden geschlossen sowie die Untersuchung von Blutproben auf das Notwendigste beschränkt werden. Im Zuge dieses Systemausfalls und der Einschränkungen im Labor konnten zahlreiche der eigentlich auszuwertenden Blutproben nicht mehr verwendet werden. Das UKE ließ verlautbaren, dass: „die Mitarbeiter ... alles Menschenmögliche getan [haben], um die Patientenversorgung nicht zu gefährden.“ [42] Dieser Zustand kann aber nicht darüber hinwegtäuschen, dass ein Computerausfall über einen so langen Zeitraum in einem so sensiblen Bereich als schwerwiegend und bisweilen patientengefährdend einzustufen ist.

Als Konsequenzen aus der Häufung von Vorfällen am UKE wurde im Anschluss an die „Pannenserie“ eine lückenlose Auflistung aller Vorkommnisse seit Neueröffnung durch die Wissenschaftsbehörde der Stadt Hamburg gefordert. Wenn auch nicht bundesweit, so hat

[40] Vgl. Göttsche (2009).
[41] Vgl. Wunder (2009).
[42] Haarmeyer (2009).

die Häufung von Problemen, seien sie organisatorischer als auch technischer Art, in der Region Hamburg für Aufregung bzw. Empörung gesorgt und den Druck auf die Klinikverantwortlichen hinsichtlich entsprechender Konsequenzen erhöht. Die zugrundeliegenden Ursachen der Pannenserie des UKE Hamburg liegen sowohl in Mangelzuständen bei Zugriffsmanagement und Softwarestabilität, als auch im sittenwidrigen Verhalten der Angestellten.

Krankenkassen:
Ein letztes Beispiel entstammt dem Bereich der Krankenkassen. Im August 2005 wurden Krankenkassen wie z.B. die AOK Brandenburg „Opfer" eines durch die T-Systems nicht behobenen Softwarefehlers. Im Rahmen von 32.000 automatischen Meldungen der Bundesagenturen für Arbeit an die Krankenkasse wurden fälschlicherweise 18.000 Stornierungen übermittelt. Somit mussten sämtliche Meldungen von Hand überprüft werden, was bei der Mehrheit der gesetzlichen Krankenkassen in der Bundesrepublik zu Tausenden Stunden Mehrarbeit und etwa 80 Millionen Euro Zusatzkosten führte.[43] Neben den Kosten ist auch die gesundheitliche Versorgung der betroffenen Krankenkassenmitglieder in Gefahr gewesen. Etwa dann, wenn ein storniertes Mitglied eine Arztbehandlung benötigt hat.

1.3 Schlussbetrachtung und Ansatz einer Analyse von IT-Skandalen

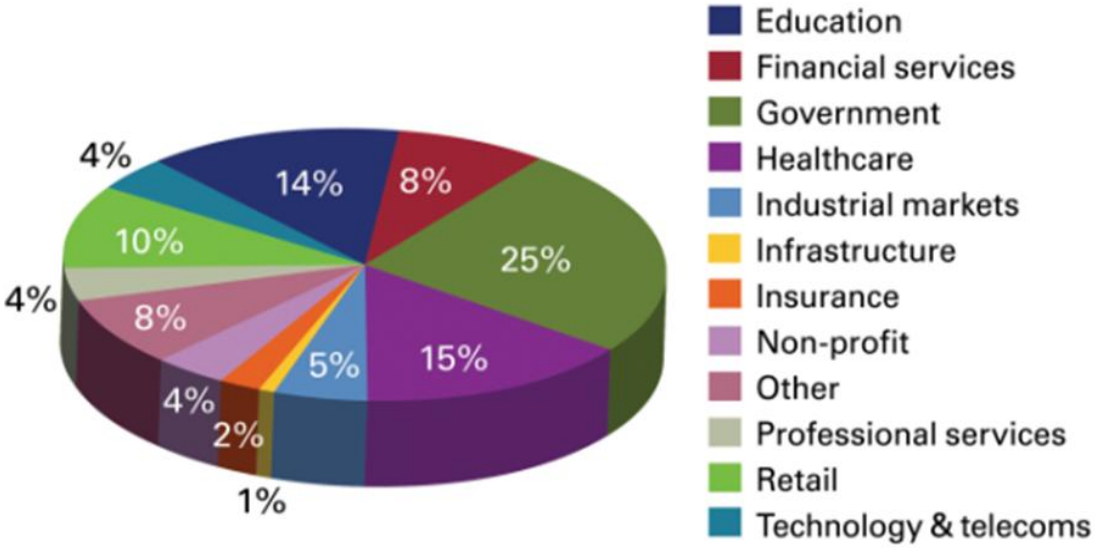
Abschließend ist unter Einbezug der betrachteten IT-Skandale und der Häufigkeit des Auftretens von Skandalen die Bedeutung der Beschäftigung mit den zu Grunde liegenden Problemfeldern zu betonen. Es zeigte sich, dass in den betrachteten Bereichen eine Vielzahl unterschiedlichster Skandale eintreten kann. Die Abgrenzung der betrachteten Gesellschaftsbereiche erfolgte anhand der Häufigkeit und Heterogenität von IT-Skandalen. Trotzdem entbehren auch die nicht betrachteten Bereiche nicht einer allgemeinen Bedeutung im Geflecht der Nutzung von IT und der daraus entstehenden Missstände bzw. Skandale.

Insbesondere die Bereiche Finanzwesen, Gesundheitswesen sowie Politik bzw. öffentliche Verwaltung konnten im Rahmen der durchgeführten Recherche als Gebiete zahlreicher Skandale identifiziert werden. Wenn diese Zuordnung der Bereiche in mehr und weniger relevante Skandal-Bereiche auch auf keiner allzu großen Datengrundlage basiert, so kann diese Annahme durch die Ergebnisse einer aktuellen KPMG-Studie im internationalen Umfeld bestätigt werden.

Insbesondere die Bereiche Bildung, Financial Services, Politik und Healthcare sind von IT-Skandalen bzw. Datenverlusten betroffen (vgl. Abbildung 1.6). Die Vielzahl der Skandale

[43] Vgl. Kaufmann (2008).

geht zwar auf recht unterschiedliche Ursachen zurück, jedoch zeigen sich teils wiederkehrende Muster. So sind in den verschiedenen Bereichen oftmals Datenpannen durch „falsche“ oder nicht ausreichend sorgfältige Softwarebedienung zu verzeichnen. Ein anderer Schwerpunkt kann hinsichtlich des kriminellen und sittenwidrigen Verhaltens identifiziert werden. Institutionen und Unternehmen aller Bereiche werden dauerhaft der Bedrohung durch Hacker bzw. sogenannte Cyberkriminelle ausgesetzt.



Quelle: KPMG International (2009).

Abb. 1.6: Bereichsanteile an Vorfällen des Datendiebstahls und -verlustes

Im Bereich der Verwaltungsmodernisierung, dem das ELENA-Verfahren zuzuordnen ist, konnte auch bei vergangenen Projekten wie der Gesundheitskarte festgestellt werden, dass die Komplexität der Verwaltungsvorgänge und des geltenden Rechts im Zusammentreffen mit der Komplexität der notwendigen IT-Strukturen die Projekte weit überdimensioniert werden lässt, was zum Projektende hin zur Folge hat, dass die Ideen wieder verworfen werden. So ist es geschehen im Rahmen der Gesundheitskarte und Gleiches droht auch beim ELENA-Verfahren einzutreten.

2 Typologisierung der Risiken des Einsatzes von IT

Willi Bühler

2.1 Motivation

Die umfassende Betrachtung von IT-Risiken resultiert aus einem stark gestiegenen Einsatz von IT und den hieraus hervorgegangenen Missständen und Skandalen im Umfeld der Informationstechnologie. Besonders die aus Reputationsschäden und Schadensersatzansprüchen hervorgehenden finanziellen Einbußen tragen zu einer gesteigerten Wahrnehmung der zugrundeliegenden IT-Risiken bei.

In der heutigen Geschäftswelt ist der Verzicht auf IT-Systeme undenkbar.[44] Nicht nur aufgrund neuartiger Vertriebsstrukturen und Geschäftsmodelle, die auf IT basieren, sondern auch und besonders weil der deutsche Gesetzgeber eine Vielzahl von elektronisch übermittelten Daten fordert, ist der Einsatz von IT-Systemen unerlässlich. Beispielhaft können hier das elektronische Handels- und Genossenschaftsregister sowie die Regularien ElsterLohn II, elektronische Meldungen zur Sozialversicherung oder ELENA genannt werde. Um IT-Risiken zu minimieren, ist natürlich die Reduktion von IT auf ein Mindestmaß möglich, jedoch stellen Schnittstellenprobleme zwischen Papier und IT eine große Barriere dar, die nur mit erheblichem Verwaltungsmehraufwand kompensiert werden kann. Den Grundgedanken des Gesetzgebers, dass gerade durch den Gebrauch elektronischer Meldungen Kosten eingespart werden können, würde durch diesen Ansatz kompromittiert, da der Mehraufwand auch höhere Ausgaben mit sich ziehen würde.

Ausgehend von diesem Sachverhalt wird in diesem Kapitel eine Einordnung der IT-Risiken in den unternehmerischen Kontext vorgenommen und eine ursachenbasierte Typologisierung durchgeführt.

Hierzu wird der Begriff des Risikos zunächst aus einer betriebswirtschaftlichen Perspektive definiert. In Anlehnung hieran wird schließlich die Herangehensweise an die Thematik des IT-Risikos aufgezeigt und die Methodik der Analyse erläutert. Die Analyse gliedert sich in zwei Teilabschnitte. Im ersten Schritt werden IT-Risiken in den Bezug zu Unternehmensrisiken gesetzt und hinsichtlich ihrer Merkmale eingeordnet, während der zweite Schritt die Typologisierung des IT-Risikos hinsichtlich seiner Eigenschaften und Ausprägungen beinhaltet.

[44] Vgl. hier und im Folgenden Bundesregierung (2009); Hirschmann & Romeike (2004), S. 13 nach Klempt (2007), S. 47.

Abschließend werden exemplarisch IT-Skandale unter dem Aspekt der Typologisierung betrachtet. Im Gegensatz zur Kategorisierung der Skandale im vorangegangenen Kapitel, die auf der Betrachtung der gesellschaftlichen Bereiche beruht, wird die Kategorisierung im Folgenden anhand des unternehmerischen Ursprungs, der Ursachen und Ausprägungen durchgeführt.

2.2 Grundlagen zu Risiken und morphologischen Analysen

2.2.1 Risikobegriff

Vielfältige Definitionen des Begriffs Risiko finden sich nicht nur in der Umgangssprache, sondern auch im besonderen Maße in der Literatur wieder.[45] Dem lateinischen *riscare*, das in etwa so viel bedeutet wie *Klippen umschiffen*, und dem griechischen Wort *riza*, *die Wurzel, über die man stolpern kann*, entlehnt, konzentriert sich der Begriff primär auf die negative Zielabweichung eines erwarteten Zielzustandes.[46]

Der Risikobegriff ist besonders in der Wirtschaftswissenschaft weit verbreitet und verursacht insofern ein Problem, als der immer gleiche Begriff in verschiedenen Bereichen meist mit unterschiedlichen Bedeutungsinhalten verwendet wird.[47] Daher differenziert PIAZ im betriebswirtschaftlichen Kontext zwischen den folgenden Risikoauffassungen[48]:

- Risiko als Gefahr einer Fehlentscheidung
- Risiko als Gefahr einer Zielabweichung
- Risiko als Informationszustand
- verlustbezogene Risikoauffassung und
- planorientierte Risikoauffassung.[49]

Wie diese Aufzählung zeigt, können Risiken in ursachen- und wirkungsseitige Grundrichtungen unterteilt werden.[50] Risiken, die aufgrund unvollkommener Information verursacht werden, beeinflussen die Ergebnisse der zur Wahl stehenden Handlungsalternativen.[51] Somit ist die zukünftige Situation lediglich eine Folgewirkung der getroffenen Entscheidung.[52] Da den Risiken Sollvorstellungen zu Grunde liegen, welche in der tatsächlichen

[45] Vgl. Helten (1994), S. 1 f. nach Hechenblaikner (2006), S. 8; Müller-Reichhart (1994), S. 9 ff., Brink & Romeike (2005), S. 58; Wagner (2000) nach Prokein (2008), S. 7.
[46] Vgl. Erasim (2002), S. 3; Piaz (2002), S. 10; Klempt (2007), S. 22; Wagner (2000) nach Prokein (2008), S. 7.
[47] Vgl. Piaz (2002), S. 10; Klempt (2007), S. 22.
[48] Vgl. Klempt (2007), S. 22.
[49] Vgl. Piaz (2002), S. 11.
[50] Vgl. Piaz (2002), S. 12; Hechenblaikner (2006), S. 8.
[51] Vgl. Piaz (2002), S. 12.
[52] Vgl. Piaz (2002), S. 12.

Situation nicht eintreten, beinhalten definitorische Auffassungen, welche von Risikowirkungen ausgehen, die Möglichkeit einer Zielverfehlung.[53]

Im WIRTSCHAFTSINFORMATIK-LEXIKON heißt es hierzu: *„Die Wahrscheinlichkeit des Eintretens eines unerwünschten Ereignisses oder Zustands in einem bestimmen Zeitraum an einem bestimmten Objekt (z. B. einem Projekt) und der damit verbundene Schaden, also Eintrittswahrscheinlichkeit mal Schadenshöhe.“*[54]

Die im deutschen Sprachgebrauch oftmals mit dem Risikobegriff einhergehenden, meist negativen Assoziationen entspringen dem ausfallorientierten Risikoverständnis.[55] Hierbei wird, im Gegensatz zum entscheidungsorientierten Ansatz, lediglich die Gefahr einer negativen, nicht jedoch die Eventualität einer positiven Zielabweichung betrachtet.[56] BÜSCHGEN bezeichnet jene Ziel- und Planabweichungen, die zu einem positiven Ergebnis führen, als Chance.[57]

Hierauf aufbauend ist Schaden also ein schlagend gewordenes Risiko und stellt die absolute Differenz der Abweichung des eingetretenen Ereignisses vom geplanten Ziel sowohl in positiver wie auch negativer Dimension dar.[58] Die Schadenshöhe setzt sich dabei aus dem bezifferbaren und indirekt bezifferbaren Schaden zusammen, wobei sich erstgenannter aus unmittelbarem und mittelbarem Schaden errechnet. Für indirekt bezifferbare Schäden sind Reputationsschäden oder Opportunitätskosten, wie zum Beispiel entgangene Geschäfte, denkbar.

Auch das zuvor und im Zusammenhang mit Risiko oftmals genannte Schlagwort Gefahr bietet die Eventualität, dass etwas nicht Kalkuliertes, in der Regel Negatives, eintritt. Jedoch beinhaltet der Begriff keine Eintrittswahrscheinlichkeit und auch das Auswirkungsmaß (der Schaden) kann unbekannt sein.

2.2.2 IT-Risiko

Explizite Definitionen des Begriffs IT-Risiko finden sich selten in der Literatur. Eine mögliche Definition von KRCMAR lautet: *„IT-Risiken werden als unzureichende Erfüllung der Unterstützungs- und Enablerfunktion des Informationsmanagements für Geschäftsprozesse verstanden. Dies umfasst sowohl die Sicherstellung einer funktionsfähigen Infrastruktur*

[53] Vgl. Piaz (2002), S. 12.
[54] Heinrich, Heinzl & Roithmayr (2004).
[55] Vgl. Schierenbeck & Lister (2002), S. 183 nach Prokein (2008), S. 7; Schaich, Schmidt & Weber (2010), Vers. 9; Piaz (2002), S. 10.
[56] Vgl. Prokein (2008), S. 7.
[57] Vgl. Büschgen (1998), S. 865 nach Hechenblaikner (2006), S. 8.
[58] Vgl. hier und im Folgenden Seibold (2006), S. 13.

und den sicheren Betrieb von Informationssystemen als auch die termin- und bedarfsgerechte Durchführung von IT-Projekten sowie die Festlegung geeigneter IT-Strategien.“[59] Ergänzend sei angemerkt, dass auch Supportprozesse (hier: Unterstützungsfunktion) für die Wertschöpfung notwendig sind und somit einen Teil der Geschäftsprozesse darstellen.

Zu erwähnen ist auch die besondere Rolle von strategischen IT-Risiken, wie z. B. die Festlegung einer geeigneten IT-Strategie, und Risiken aus IT-Projekten, da sie im weiteren Verlauf dieser Arbeit im Sinne der Regelungen der Baseler Eigenkapitalvereinbarung (Basel II) vom IT-Risiko abgegrenzt werden.[60]

2.2.3 Morphologische Analyse

Die morphologische Analyse stellt eine systematische Kreativitätsmethode zur vollständigen Erfassung und vorurteilsfreien Betrachtung eines komplexen Problembereiches dar.[61] Um diesem Anspruch gerecht zu werden, wird das Gesamtproblem zunächst in Teilprobleme aufgegliedert, um schließlich eine Vielzahl von Lösungsmöglichkeiten zu ermitteln. Das Kernstück dieser Analysemethode bildet der sogenannte morphologische Kasten. In dieser tabellenähnlichen Darstellungsform stellt die linke Spalte die Teilprobleme, meist auch Merkmale oder Dimensionen genannt, dar, während zeilenweise die Lösungsalternativen bzw. Ausprägungen eingetragen werden.

<table>
<tr><th>Dimension</th><th colspan="6">Ausprägung</th></tr>
<tr><td>Dimension 1</td><td>Ausprägung 1.1</td><td>Ausprägung 1.2</td><td>Ausprägung 1.3</td><td colspan="3">Ausprägung 1.4</td></tr>
<tr><td>Dimension 2</td><td colspan="2">Ausprägung 2.1</td><td colspan="4">Ausprägung 2.2</td></tr>
<tr><td rowspan="2">Dimension 3</td><td colspan="4">Ausprägung 3.1</td><td colspan="2">Ausprägung 3.2</td></tr>
<tr><td>Auspr. 3.1.1</td><td>Auspr. 3.1.2</td><td>Auspr. 3.1.3</td><td>Auspr. 3.1.4</td><td>Auspr. 3.2.1</td><td>Auspr 3.2.2</td></tr>
</table>

Abb. 2.1: Beispieldarstellung eines morphologischen Kastens

Abb 2.1 zeigt den schematischen Aufbau eines morphologischen Kastens. Durch Einfärbung wie bei Ausprägung 1.3 wird die Einordnung eines Objektes in den Kasten deutlich gemacht. Eine weitere Darstellungsform wird in Dimension 3 genutzt. Ausprägungen 3.1.1-3.1.4 stellen hierbei die Kategorien der Ausprägung 3.1 dar, während 3.2.1-3.2.2 die Ausprägung 3.2 verfeinern.

[59] Krcmar (2000), S. 359 ff. nach Hechenblaikner (2006), S. 17.
[60] Vgl. Hechenblaikner (2006), S. 17.
[61] Vgl. hier und im Folgenden Klempt (2007), S. 69 f.

Aufgrund des multidimensionalen Merkmalraums bei der Risikotypologisierung wird die morphologische Analyse im Folgenden angewandt, da die Darstellung durch eine Baumstruktur oder ein Netz, bedingt durch das Auftreten orthogonaler Risikokategorien unvollständig bzw. undurchsichtig wäre.

2.3 Morphologische Analyse des IT-Risikos

2.3.1 Einordnung des IT-Risikos in den Kontext von Unternehmensrisiken

Die Typologisierung von IT-Risiken gliedert sich in zwei Teile. Zunächst erfolgt die Einordnung des IT-Risikos in den Kontext des Unternehmensrisikos. Darauf aufbauend werden die Eigenschaften und Ausprägungen des IT-Risikos behandelt werden.

Die Risikolandschaft von Unternehmen ist äußerst heterogen und komplex.[62] Ein möglicher strukturierter Ansatz, um diese Komplexität zu beherrschen, ist , Unternehmensrisiken nach ihrer Natur (Sach- oder Personenrisiko, finanzielles Risiko), nach ihrem Ursprung in der internen oder externen Umwelt des Unternehmens (z. B. Absatz-, Wettbewerbsrisiken, Technik- und Personalrisiken), nach zeitlichen Dimensionen bzw. Auswirkungen (strategische oder operative Risiken) sowie nach Unternehmens- und Verantwortungsbereichen (z. B. Geschäftsbereich, Absatzregion) zu unterscheiden.[63]

Häufige Verwendung findet die Unterscheidung der Unternehmensrisiken in die folgenden Kategorien: [64]

- Marktrisiken
- Ausfallrisiken
- Liquiditätsrisiken
- Operationelle Risiken und
- sonstige Risiken.

Marktrisiken werden als Gefahr einer negativen Entwicklung des Marktes verstanden, äußern sich also als Schwankungen des Cashflows oder des Eigenkapitalwertes infolge von Preisänderungen an den Finanzmärkten.[65] Hierzu zählen Aktienkurs-, Zins-, Währungs-, Rohstoffpreis- und Immobilienrisiken.[66]

[62] Vgl. hier und im Folgenden Piaz (2002), S. 14.
[63] Vgl. Rosenkranz & Missler-Behr (2005), S. 145; Romeike (2003), S. 167 nach Klempt (2007), S. 46; Piaz (2002), S. 14.
[64] Vgl. Prokein (2008), S. 9; Klempt (2007), S. 46.
[65] Vgl. Piaz (2002), S. 16; Prokein (2008), S. 9.
[66] Vgl. Eisele (2004), S. 27 nach Prokein (2008), S. 9; Piaz (2002), S. 16.

Die Kategorie der **Ausfallrisiken**, oft auch als Gegenparteirisiken angeführt, beschreibt den Umstand einer Nichterfüllung der (kredit-)vertraglichen Pflichten durch die zahlungsunfähige oder -unwillige Gegenpartei.[67] Ausfallrisiken treten bei Banken hauptsächlich in Form von Kreditrisiken auf, doch werden sie infolge der zusätzlichen Nutzung des Internets als Vertriebskanal auch für Unternehmen zunehmend relevant.[68] Denn Zahlungsverzögerungen und -ausfälle stellen große Problemfaktoren beim E-Commerce dar.[69]

Liquiditätsrisiken beschreiben die Gefahr, dass aufgrund von zeitlichen oder betragsmäßigen Inkongruenzen bei der Mittelbeschaffung nicht alle Zahlungsverpflichtungen fristgerecht erfüllt werden können.[70] Ausschlaggebend sind hier hauptsächlich Schwankungen bei Ein- und Auszahlungen.[71] Zur Vermeidung von Liquiditätsrisiken hat z. B. im Finanzsektor die Bankenaufsicht Liquiditätsgrundsätze erlassen, die eine Mindestliquidität sicherstellen sollen. Das Halten ausreichender liquider Mittel ist für ein Finanzinstitut unabdinglich, jedoch ist eine allzu große Liquidität für die Rentabilität abträglich, so dass es sich hierbei um eine schwierige Entscheidungsaufgabe mit erheblichen Unsicherheitsfaktoren handelt.[72]

Teilweise findet sich in der Literatur auch der Begriff des Abwicklungsrisikos als „general term used to designate the risk that settlement in a transfer system will not take place as expected."[73] Nach PIAZ beinhaltet diese Risikokategorie per Definition wiederum Markt-, Kredit- und Liquiditätsrisiken. Dies lässt sich anhand der zwei bedeutendsten Ursachen für Abwicklungsrisiken, des zeitlichen Auseinanderfallens von Geschäftsabschluss und -abwicklung sowie von Lieferung und Zahlung erklären. Hierbei kann es bspw. zu einem Markt- bzw. Kreditrisiko kommen, wenn ein höherer Wiederbeschaffungspreis besteht, respektive zu einem Zins- und Kapitalverlust beim Ausfall der Gegenseite. Ein System, welches Abwicklungsrisiken auszuschließen vermag, existiert bislang nicht.[74]

Die Ursachen der **operationellen Risiken**[75] entstammen ursprünglich dem bankinternen Bereich.[76] Hierbei umfasst der Begriff sämtliche betriebliche Risiken, die einen Verlust

[67] Vgl. Piaz (2002), S. 17; Prokein (2008), S. 9.
[68] Vgl. Prokein (2008), S. 9.
[69] Vgl. Raab & Siegl (2007), S. 35 nach Prokein (2008), S. 9.
[70] Vgl. Hofacker (1997), S. 136 nach Piaz (2002), S. 19; Eisele (2004), S. 24 nach Prokein (2008), S. 9.
[71] Vgl. Prokein (2008), S. 9.
[72] Vgl. Piaz (2002), S. 20; Schweizer Bundesgesetz über die Banken und Sparkassen (BankG), Art. 4.
[73] CPSS & IOSCO (2001), S. 48.
[74] Vgl. Piaz (2002), S. 20.
[75] Bemerkenswert ist, dass vielfach Synonyme für operationelles Risiko verwandt werden: während im englischen Sprachraum nahezu immer der Begriff *Operational Risk* Anwendung findet, reichen die Begrifflichkeiten in den deutschsprachigen Publikationen von *operationelle Risiken*, *operationale Risiken*, *operative Risiken* bis hin zu *Betriebsrisiken*. In dieser Arbeit werden jedoch ausschließlich *Operational Risk* oder *operationelles Risiko* verwendet, da *Betriebsrisiko* lediglich das Risiko der direkten Geschäftsabwicklung abbildet und das *operative Risiko* als Gegenstück zum *strategischen Risiko* gesehen werden kann. Vgl. Einhaus (2005), S. 7 ff. nach Klempt (2007), S. 47; Beeck & Kalser (2000), S. 636 f. nach Hechenblaikner (2006), S. 9.

herbeiführen können, jedoch werden operationelle Risiken im Gegensatz zu z. B. Marktrisiken nicht bewusst eingegangen, sondern entstehen vielmehr automatisch durch Aufnahme der Geschäftstätigkeit.[77] Nicht zuletzt kennzeichnen sich die operationellen Risiken durch das Merkmal des ausschließlichen Downside-Risks. Das bedeutet, dass den möglichen Verlusten keine Ertragschancen gegenüberstehen. Zur abschließenden Definition des operationellen Risikos existiert eine Vielzahl teils ähnlich, teils widersprüchlicher Ansätze. Die am weitesten verbreitete und auch weitgehend akzeptierte Begriffserklärung entstammt Basel II, einem Katalog für Eigenkapitalvorschriften des Basler Ausschusses für Bankenaufsicht:[78]

„Operational Risk is defined as the risk of loss resulting from inadequate or failed internal processes, people or systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk.“[79]

Diese Definition enthält sowohl die Ursachen des operationellen Risikos als auch deren Wirkungen.[80] Die Ursachen werden dabei zunächst in externe und interne Faktoren unterteilt. Externe Ursachen wirken von außerhalb auf das Unternehmen ein und können von diesem nicht beeinflusst werden, wie bspw. Elementarereignisse. Dagegen liegen interne Ursachen im Bereich von Prozessen, Menschen und Technik. Weiterhin werden auch Risiken, die rechtlicher Natur sind, betrachtet. Risiken, die aus strategischen Entscheidungen hervorgehen oder im Zusammenhang mit der Reputation des Unternehmens stehen, werden hingegen explizit ausgeschlossen.

Unter Rechtsrisiken werden jene Risiken verstanden, die aus einer ungenügenden Dokumentation, einer fehlenden Durchsetzbarkeit von Forderungen gegenüber der Gegenpartei und einer unsicheren Gesetzgebung hervorgehen.[81] Hierdurch besteht jederzeit die Möglichkeit der rechtlichen Anfechtung des Geschäfts durch beliebige Vertragsparteien. Weitergehend werden ebenfalls regulatorische und steuerrechtliche Risiken zu dieser Kategorie gezählt, wie z. B. die Unmöglichkeit, Aufsichtsvorschriften zu erfüllen. Aufgrund der stark variierenden gesetzlichen Grundlagen für jene Vorschriften können Risikopotenziale mit weitreichender Wirkung entstehen, die meist durch ungenaues Verständnis der Rechte

[76] Vgl. Hechenblaikner (2006), S. 9.
[77] Vgl. hier und im Folgenden Hechenblaikner (2006), S. 13; Prokein (2008), S. 10; Klempt (2007), S. 47.
[78] Vgl. Prokein (2008), S. 10; Geiger & Piaz (2001), S. 792 nach Hechenblaikner (2006), S. 9.
[79] Rünger & Walther (2004), S. 10; Hechenblaikner (2006), S. 9. Die deutsche Übersetzung hierzu lautet: Operationelles Risiko ist definiert als *„[…] die Gefahr von Verlusten, die infolge einer Unzulänglichkeit oder des Versagens von internen Verfahren, Menschen oder Systemen oder infolge externer Ereignisse eintreten. Diese Definition schließt Rechtsrisiken ein, nicht jedoch strategische Risiken.“* Basler Ausschuss für Bankenaufsicht (2004), S. 127 nach Prokein (2008), S. 10.
[80] Vgl. hier und im Folgenden Hechenblaikner (2006), S. 9 f.
[81] Vgl. hier und im Folgenden Piaz (2002), S. 18 f.

verursacht werden, was wiederrum zu unfreiwilligen Rechtsübertretungen führen kann. Auch der stetige Wandel in der Rechtsprechung stellt ein Risikopotenzial dar.

Es besteht in der Literatur Konsens darüber, dass IT-Risiken einen zentralen Bestandteil der operationellen Risiken ausmachen.[82] Dies liegt in der Tatsache begründet, dass in vielen Fällen die Geschäftsprozesse in Unternehmen – insbesondere im Finanzbereich – vollständig durch Informationssysteme determiniert sind.

Die letzte Kategorie der **sonstigen Risiken** dient als „Auffangbecken" all jener Risiken, die keine Zuordnung zu einer der bereits erwähnten Risikokategorien erlauben.[83] Hierzu zählen primär uneinheitlich ausgelegte Risikokategorien, wie etwa Risiken strategischer Art. In Abb. 2.2 sind alle Ausprägungen eines Unternehmensrisikos als erste Ebene des morphologischen Kasten dargestellt. Da IT-Risiken in die Kategorie der operationellen Risiken einzuordnen sind, ist diese Kategorie farblich hervorgehoben.

Dimension	**Ausprägung**				
Unternehmensrisiken	Marktrisiken	Kreditrisiken	Liquiditätsrisiken	Operationelle Risiken	sonstige

Abb. 2.2: Darstellung der Unternehmensrisiken

Die Dimension des Zeithorizonts soll der Unterscheidung zwischen dem strategischen und operativen Risiko dienen. Obgleich die strategische Ausprägung, wie zuvor erläutert, für operationelle Risiken nicht relevant ist, wird sie hier dennoch zur Vollständigkeit erwähnt.

Das **strategische Risiko** wird wie folgt definiert: *„Strategische Risiken betreffen die verfolgte Risikopolitik des Unternehmens und sind von langfristigem und grundsätzlichem Charakter. Dies können bspw. Risiken aus Grundsatzentscheidungen wie der verfolgten Geschäftsstrategie oder der Zusammenstellung des Produkt- und Leistungsportfolios sein."*[84] Zu dieser Kategorie lassen sich nach HECHENBLAIKNER auch IT-Projekte und IT-Strategien zählen, die im Folgenden aber nicht weiter betrachtet werden.[85]

Operative Risiken *„hingegen sind bereichsbezogen und von kürzerer Dauer und bezeichnen die Gefahr von unmittelbaren oder mittelbaren Verlusten, die aus der Unangemessenheit oder dem Versagen von internen Verfahren, Menschen und Systemen oder aus exter-*

[82] Vgl. hier und im Folgenden Erasim (2002), S. 3; Hirschmann & Romeike (2004), S. 13 nach Klempt (2007), S. 47.
[83] Vgl. hier und im Folgenden Piaz (2002), S. 21.
[84] Einhaus (2005) S. 20 f nach Klempt (2007), S. 47.
[85] Vgl. Hechenblaikner (2006), S. 17. Wie bereits ausgeführt, soll diese Arbeit im Einklang mit den Regelungen der Basler Eigenkapitalvereinbarungen stehen. Daher werden Risiken aus IT-Strategien und IT-Projekten ausgeschlossen. Vgl. Hechenblaikner (2006), S. 17 und Unterkapitel II2.2.2.

nen Ereignissen resultieren.“.[86] Hierbei sei angemerkt, dass die Benennung der Kategorie **Menschen** mit eben jenem Begriff implizieren würde, dass hier auch die unter externe Risiken fallenden Angriffe von Personen von außerhalb des Unternehmens erfasst würden. Da hier jedoch nur Risiken aus dem Verhalten von Mitarbeitern einzuordnen sind, wird diese Kategorie folgerichtig im weiteren Verlauf mit „Mitarbeiter“ bezeichnet.[87]

IT-Risiken lassen sich in der Dimension Zeithorizont als zweite Ebene des morphologischen Kastens der Ausprägung **operativ** zuordnen (vgl. Abb. 2.3).

Dimension	**Ausprägung**				
Unternehmensrisiken	Marktrisiken	Kreditrisiken	Liquiditätsrisiken	Operationelle Risiken	sonstige
Zeithorizont	Operativ		Strategisch		

Abb. 2.3: Darstellung der Unternehmensrisiken und des Zeithorizontes

2.3.2 Eigenschaften und Ausprägungen des IT-Risikos

Nach der Einordnung des IT-Risikos in das Feld **operativ** werden im Folgenden die Eigenschaften und mögliche Ausprägungen von IT-Risiken untersucht.

IT-Risiken können ursachenbasiert in **interne** und **externe** IT-Risiken unterschieden werden (Abb. 2.4).[88] Externe Ursachen sind primär dadurch gekennzeichnet, dass sie nicht im Einflussbereich des Unternehmens liegen, aber Auswirkungen in Form von Schäden hervorrufen können.[89] Besonders naheliegend ist dies bei Risiken, die aus Elementarereignissen wie z. B. Bränden, Erdbeben, Überschwemmungen oder Stürmen resultieren. Darüber hinaus kommen als weitere Ursachen außenstehende Dritte durch kriminelle Handlungen (bspw. Betrug, Überfälle, Einbrüche, Hacker-Angriffe etc.) oder durch ungewolltes Fehlverhalten in der Zusammenarbeit mit dem Unternehmen ebenso wie Änderungen im geltenden Rechtssystem (Rechtsänderungen) in Frage. Dieser Gesetzeswandel erfasst schließlich die Komponente des Rechtsrisikos.[90]

[86] Vgl. Einhaus (2005), S. 21; Romeike (2003), S. 169 nach Klempt (2007), S. 47.
[87] Vgl. Hechenblaikner (2006), S. 12.
[88] Vgl. Hechenblaikner (2006), S. 11.
[89] Vgl. hier und im Folgenden Rünger & Walther (2004), S. 11; Hechenblaikner (2006), S. 11; Romeike & Hager (2009), S. 376; Schierenbeck (2001), S. 337 nach Prokein (2008), S. 11.
[90] Vgl. Unterkapitel II2.3.1 Rechtsrisiken.

Interne Ursachen sind im Einflussbereich des Unternehmens und können grob in Mitarbeiter, Prozesse und Systeme unterschieden werden.[91] Die Risikoursache von Mitarbeitern liegt dabei im falschen Verhalten, welches in bewusstes und unbewusstes Fehlverhalten unterschieden wird. Fehler aufgrund von Irrtum, Fahrlässigkeit oder Unvermögen werden dem unbewussten Fehlverhalten zugeordnet, während Betrug, Diebstahl, Sachbeschädigung etc. den bewussten Fehltritten zugerechnet werden. Erfasst werden auch die Gefahr von ungewollten Mitarbeiterabwanderungen besonders aus Schlüsselpositionen sowie die Gefahr durch ungenügend qualifiziertes Personal. Erhebungen im Bankensektor haben gezeigt, dass 61% der operationellen Verlustfälle der Risikoursache Mitarbeiter zuzuordnen waren.

Die Gefahr von fehlerhaft konzipierten Geschäftsabläufen wird dagegen der Risikokategorie Prozesse zugeordnet. Prozessrisiken werden dabei als alle Risiken verstanden, die durch Fehler innerhalb des Flusses bzw. der Transformation von Materialien, Tätigkeiten, Entscheidungen oder Informationen entstehen. Hierzu zählen fehlerhafte Arbeitsanweisungen und mangelnde interne Kontrollen, wie z. B. die Überwachung von Geschäften. Ferner können Fehler aus der falschen manuellen oder automatisierten Ausführung eines Prozesses resultieren.

Komplettiert werden die internen Ursachen durch Risiken aus Systemen. Denkbar sind hier bspw. Verluste, die aus mangelnder Zugriffssicherheit der Datenbestände, Netzzusammenbrüchen, Computerviren oder Hackeraktivitäten hervorgehen. Doch auch nicht funktionierende oder falsch implementierte IT-Systeme rufen Risiken dieser Kategorie hervor. Das hohe Wachstum im Bereich des E-Commerce für Unternehmen sowie die zunehmende Automatisierung und Technologisierung der Bankleistungen bewirken einen starken Anstieg der IT-Risiken und messen ihnen zunehmend mehr Bedeutung zu.

Dimension	**Ausprägung**	
Ursachen	intern	exern

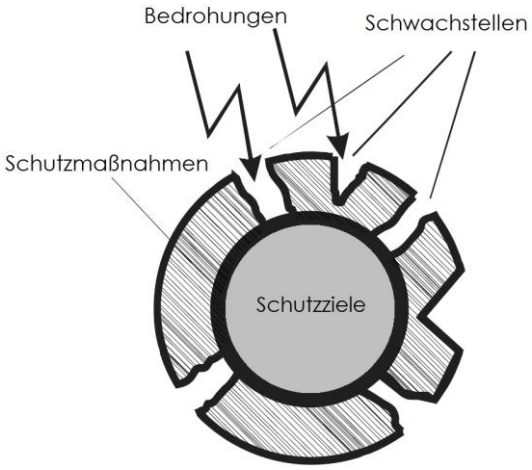
Abb. 2.4: Darstellung der Ursachen von IT-Risiken

Für die weitere Charakterisierung von IT-Risiken ist es hilfreich, eine zusätzliche Definition des IT-Risikos heranzuziehen, um die Eigenschaften von IT-Risiken weiter zu konkretisieren:

[91] Vgl. hier und im Folgenden Rünger & Walther (2004), S. 10 ff; Hechenblaikner (2006), S. 9 ff; Romeike & Hager (2009), S. 376; Schierenbeck (2001), S. 337 nach Prokein (2008), S. 11.

IT-Risiko sei nach PROKEIN *„die Gefahr der Realisierung von Verlusten, die infolge der Verletzung eines oder mehrerer der Schutzziele […] aufgrund eines durchgeführten Angriffs unter Ausnutzung von Schwachstellen eintreten.“*[92] Angriffe stellen diesbezüglich umgesetzte Bedrohungen dar, die exogen gegeben und allgegenwärtig sind.[93]

In Anlehnung an die Begriffsklärung lassen sich die nachfolgenden Komponenten als ausschlaggebend identifizieren: die Verletzung eines oder mehrerer Schutzziele, die umgesetzte Bedrohung sowie die Ausnutzung von Schwachstellen. Den Kern dieser Definition stellt dabei die Verbindung zwischen potenziellen Schwachstellen und darauf potenziell einwirkenden Bedrohungen dar.[94] Ein Risiko entsteht, wenn eine Bedrohungen auf eine Schwachstelle trifft.[95] Dieses Risiko führt zu einem Schaden (Realisierung von Verlusten), wenn es schlagend wird, sprich eines oder mehrere Schutzziele verletzt (vgl. Abb. 2.5).



In Anlehnung: Königs (2009), S. 117.[96]

Abb. 2.5: Wirkungszusammenhänge zwischen Schwachstellen, Bedrohungen und Schutzzielen

Hierauf aufbauend werden die genannten Aspekte im Verlauf dieses Abschnitts als Ausgangspunkt für die Charakterisierung des IT-Risikos dienen.

Es werden vier Typen von **Bedrohungen** bzw. Angriffen (nach BSI: Gefahrenkatalog) unterschieden: Organisatorische Mängel, menschliches Fehlverhalten, technisches Versagen und höhere Gewalt (vgl. Abb. 2.6).[97]

[92] Prokein (2008), S. 11.
[93] Vgl. Prokein (2008), S. 11.
[94] Vgl. Bräuhäuser et al. (2002), S. 57 nach Hechenblaikner (2006), S. 18.
[95] Vgl. hier und im Folgenden Kersten (1995), S. 80 nach Hechenblaikner (2006), S. 18.
[96] Vgl. hierzu auch Hechenblaikner (2006), S. 18 ff; Prokein (2008), S. 13 ff.
[97] Vgl. hier und im Folgenden Bundesamt für Sicherheit in der Informationstechnik (2009), S. 339 ff; Prokein (2008), S. 13 f; Hechenblaikner (2006) S. 19 f; Informationswirtschaft & E.V. (2008), S. 18 ff.

Organisatorische Mängel sind den internen Bedrohungen zuzuordnen. Hier entstehen Bedrohungen aus fehlerhaft aufgesetzten oder durchgeführten Prozessen in Zusammenhang mit IT-Systemen, wie z. B. mangelhafte Zugriffskontrollen auf IT-Systeme, fehlerhafte Wartung, nicht geklärte Zuständigkeiten, fehlende oder unvollständige Richtlinien und Dokumentationen, unzureichende Verarbeitung von IT-Sicherheitskonzepten oder mangelnde Fortbildung und Schulung der Mitarbeiter zum Thema IT-Sicherheit sowie Bedrohungen aufgrund einer fehlerhaften Organisation der Infrastruktur, was im weiteren Sinne zur Prozessorganisation gezählt werden kann.

Die Kategorie des **menschlichen Fehlerverhaltens** kann sowohl aus dem unternehmensinternen als auch aus dem -externen Bereich resultieren. Es wird zwischen bewusstem und unbewusstem Fehlverhalten unterschieden. Das Fehlverhalten muss im Zusammenhang mit IT stehen, das heißt, ein entsprechendes Schutzziel muss beeinträchtigt werden.

Dass dagegen eine außenstehende Person zufällig und unbeabsichtigt das IT-System eines Unternehmens erheblich bedroht, ist eher auszuschließen, wenn auch nicht unmöglich. Folglich liegt der Fokus auf der vorsätzlichen Handlung, die durch Angriffe von außen in Form von Viren, Würmern, Trojanischen Pferden, Hacks geprägt und mittels Angreiferstärke und -typ charakterisiert wird.

Auch die Bedrohung des **technischen Versagens** kann sowohl dem unternehmensinternen wie auch dem -externen Bereich entstammen. Als externe Faktoren werden hierbei Vorkommnisse wie z. B. Stromausfälle, Leitungsprobleme oder Ausfälle des Extranets angesehen. Die weitaus häufigeren Ursachen für ein technisches Versagen liegen jedoch innerhalb des Unternehmens, die z. B. in der Form von Defekten an Hardwarekomponenten, Softwarefehlern, Verlust von Daten aufgrund von Fehlern in der Speicherung oder Ausfall einer Datenbank, Störungen im Intranet etc. auftreten. Diese Kategorie stellt dabei die klassische Kernbedrohung für IT-Systeme dar.

Eine ausschließlich externe Form der Bedrohung stellt die **höhere Gewalt** dar, die teilweise das Ausmaß einer Katastrophe annehmen kann. Hierzu zählen bspw. Elementarereignisse wie Sturm, Erdbeben, Blitzeinschläge, Erdbeben, Überschwemmungen oder auch nichtnatürliche Ereignisse wie Flugzeugabstürze oder Terroranschläge. Wie auch bei den zwei erstgenannten Bedrohungskategorien ist hier die unmittelbare Auswirkung auf die IT-Systeme in Betracht zu ziehen.

Dimension	**Ausprägung**			
Ursachen	intern		extern	
Bedrohungen	Organisatorische Mängel	Menschliches Fehlverhalten	Technisches Versagen	Höhere Gewalt

Abb. 2.6: Darstellung von Ursachen und Bedrohungen

Schwachstellen stellen wie eingehend erläutert die zweite Komponente des IT-Risikos dar, die bei Kontakt mit einer Bedrohung zur Verletzung eines Schutzziels und somit zu einem Schaden führt. Um mögliche Schwachstellen im Bereich der IT zu identifizieren, können diese anhand ihrer Komponenten Hard- und Software, Netze und Daten, betrachtet werden (vgl. Abb. 2.7).[98]

Als **Hardware** werden alle materiellen technischen Komponenten eines IT-Systems wie Prozessoren, interne und externe Speicher und Peripheriegeräte (Ein- bzw. Ausgabegeräte) verstanden.

Um Hardware zu betreiben und sinnvoll nutzen zu können, wird **Software** benötigt, bei der zwischen System- und Anwendungssoftware unterschieden wird. Systemsoftware, wie z. B. das Betriebssystem, ist die Grundlage zur Verwendung der Hardware, während Anwendungssoftware die vom Benutzer gewünschte Funktionalität zur Verfügung stellt.

Da die Aufgabe eines IT-Systems in der Erfassung, Bearbeitung, Speicherung und Übertragung von **Daten** besteht, verkörpern Daten eine wesentliche Komponente des IT-Systems und somit ebenfalls eine potenzielle Schwachstelle.

Auch **Netze** sind aufgrund der in den letzten Jahren zunehmenden Vernetzung ein wesentlicher Bestandteil von IT. Dabei wird zwischen Netzwerken innerhalb eines Unternehmens (z. B. Intranet) und Netzen zwischen Unternehmen und/oder Privatpersonen (z. B. Internet) unterschieden.

Die mit dem System befassten Menschen, sprich das **IT-anwendende Personal**, gelten ebenso als potenzielle Schwachstelle wie auch die **Infrastruktur** rund um das IT-System in Form von Gebäuden, Verkabelung, Räumen etc. Ein typischer Anwenderfehler ist z. B. die schriftliche Niederlegung eines Zugangspasswortes auf einem am Monitor angebrachten Post-It Zettel.

[98] Vgl. hier und im Folgenden Bundesamt für Sicherheit in der Informationstechnik (2009); Romeike & Hager (2009), S. 376; Fink et. al. (2001), S. 13 ff.; Hansen & Neumann (2001), S. 649 ff. und Theil (1995), S. 22 nach Hechenblaikner (2006), S. 18 f.

Dimension	**Ausprägung**					
Ursachen	intern			extern		
Bedrohungen	Organisatorische Mängel	Menschliches Fehlverhalten		Technisches Versagen		Höhere Gewalt
Schwachstellen	Software	Hardware	Daten	Netze	IT-anwendendes Personal	Infrastruktur

Abb. 2.7: Darstellung von Ursachen, Bedrohungen und Schwachstellen

Schutzziele drücken den Soll-Zustand von zu schützenden Objekten (z. B. IT-Anwendungssoftware) aus und charakterisieren die Sicherheitsanforderungen an die eingesetzten IT-Systeme sowie die darauf aufbauenden Schutzmaßnahmen.[99] Wird eines oder mehrere der Schutzziele durch einen Angriff, also das Zusammentreffen einer Bedrohung auf eine Schwachstelle verletzt, so definiert das Schutzziel unmittelbar die Wirkung des Angriffs. Das bedeutet, dass der Schaden bzw. das Schadensausmaß unmittelbar vom verletzten Schutzziel abhängig ist. Es wird zwischen den Schutzzielen Vertraulichkeit, Integrität, Verfügbarkeit und Zurechenbarkeit unterschieden, die in den 1980er Jahren definiert und in den 1990ern durch MÜLLER, PFITZMANN und RANNENBERG ergänzt wurden.

Vertraulichkeit bedeutet, dass die Informationen ausschließlich dem durch den Besitzer autorisierten Personenkreis zugänglich sein dürfen. Besonders für Unternehmen bzw. Verwaltungen, die personenbezogene, sensible Daten speichern und verarbeiten, ist es eminent wichtig, dass Daten nicht an Unberechtigte gelangen. Zusätzlich zu einem möglichen Reputationsverlust zieht ein Verstoß gegen die entsprechenden Vorschriften des BDSG auch rechtliche Konsequenzen nach sich.

Das Schutzziel der **Integrität** schließt ein, dass Informationen lediglich in der vorgesehenen Weise erzeugt, verändert oder ergänzt werden und somit weder fehlerhaft noch verfälscht sind. Daten können absichtlich z. B. durch Manipulation oder unabsichtlich z. B. durch Übertragungsfehler verändert werden. Der Verlust von Integrität kann zu Fehlentscheidungen führen.

Dass dem Benutzer Informationen in der erforderlichen Weise (in vereinbarter Darstellung und Zeit) zur Verfügung stehen, gewährleistet die **Verfügbarkeit**. Das Schutzziel beinhaltet, dass Hardware, Software und Netze dem Anwender voll funktionsfähig zur Verfügung

[99] Vgl. hier und im Folgenden Königs (2009), S. 117 ff.; Prokein (2008), S. 11 ff.; Hechenblaikner (2006), S. 22 f.; Romeike & Hager (2009), S. 374 f.

stehen und auch auf die notwendigen Daten zugegriffen werden kann. Ein länger andauernder Verlust der Verfügbarkeit des IT-Systems kann beim Unternehmen erhebliche Schäden hervorrufen und sogar zur Insolvenz (denkbar für Unternehmen mit ausschließlichem E-Commerce) führen.

Als letztes, aber nicht weniger bedeutsames Schutzziel wird die **Zurechenbarkeit** (auch Verbindlichkeit) genannt. Sie gewährleistet, dass auf elektronischem Wege getätigte Transaktionen nicht abstreitbar sind, d. h. dass die digital festgehaltenen Informationsinhalte nachweislich nicht verändert worden sind und deshalb vom Urheber nicht bestritten werden können. Besonders bei Online-Geschäften oder dem Online-Banking, bei denen die eigenhändige Unterschrift nicht geleistet werden kann, muss Verbindlichkeit gemeinsam mit Authentizität gegeben sein, um als entsprechendes Beweismittel dienen zu können. Authentizität stellt dabei die Identität des Kommunikationspartners sicher.

Wurde eines der Schutzziele verletzt, kann dies zu erheblichem finanziellem Schaden führen.[100] Dabei wird zwischen direkten finanziellen Schäden und Folgeschäden unterschieden. Direkter Schaden drückt sich z. B. in der Ersatzbeschaffung einer Hardwarekomponente oder Nachbesserungen in der Software aus, wohingegen Folgeschäden bzw. Opportunitätskosten ausgefallene Geschäfte, Folgegeschäfte oder Schadensersatzklagen umfassen.

Zur Verdeutlichung des Sachverhaltes seien die folgenden Beispiele genannt und anschließend erläutert:

1) Die Angestellte einer Reinigungsfirma entleert während ihrer Tätigkeit infolge eines Missgeschicks den Putzeimer im Serverraum. Durch das entwichene Wasser entsteht ein Kurzschluss an einer Mehrfachsteckdose, an die der zentrale Server des Unternehmens angeschlossen ist. Die Folge ist ein Totalausfall der gesamten IT.

2) Ein Berater einer beliebigen Bank versäumt, während der Finanzberatung einen Kunden über die Risiken im Wertpapierhandel aufzuklären.
    a) Vorsätzliches Versäumnis
    b) Versäumnis aufgrund von Unachtsamkeit

3) Eine Person dringt
    a) in eine Bankfiliale ein und fordert unter Waffengewalt den Kassierer auf, ihm Bargeld auszuhändigen.

[100] Vgl. hier und im Folgenden Hechenblaikner (2006), S. 24.

b) in die elektronische Kundendatenbank einer Kreditkartenorganisation ein und manipuliert abertausende Datensätze.

Die erste Begebenheit beschreibt eine unternehmensinterne Bedrohung, die auf ein unbewusstes Fehlverhalten (Fahrlässigkeit) zurückgeht. Hierbei handelt es sich um die Bedrohung „Menschliches Fehlverhalten“, die auf eine Schwachstelle im Bereich Infrastruktur trifft und als Konsequenz das Schutzziel „Verfügbarkeit“ verletzt.

Das zweite Beispiel umschreibt ein nach 2a) bewusstes und nach 2b) unbewusstes Fehlverhalten aus dem internen Bereich. Allerdings wird hierbei kein IT-Schutzziel verletzt. Daher handelt es sich zwar um ein operationelles Risiko, das aber nicht dem Bereich der IT-Risiken zuzuordnen ist.

Bei beiden Fällen der dritten Annahme handelt es sich um ein unternehmensexternes Fehlverhalten. Während in der Ausprägung 3a) kein IT-Schutzziel tangiert wird, werden in 3b) die Schutzziele der Integrität und der Vertraulichkeit verletzt. Demzufolge ist die kriminelle Begebenheit 3a) ein operationelles Risiko, aber kein IT-Risiko, während in 3b) ein IT-Risiko in Form einer Bedrohung „Menschliches Fehlverhalten“ bei einer Schwachstelle „Daten“ besteht.

Abb. 2.8 zeigt den vollständigen morphologischen Kasten zur Einordnung von IT-Risiken. Die Dimensionen oberhalb der gestrichelten Linie ordnen IT-Risiken in den allgemeinen Risiko-Kontext ein, während die Dimensionen unterhalb verschiedene Ausprägungen von IT-Risiken darstellen.

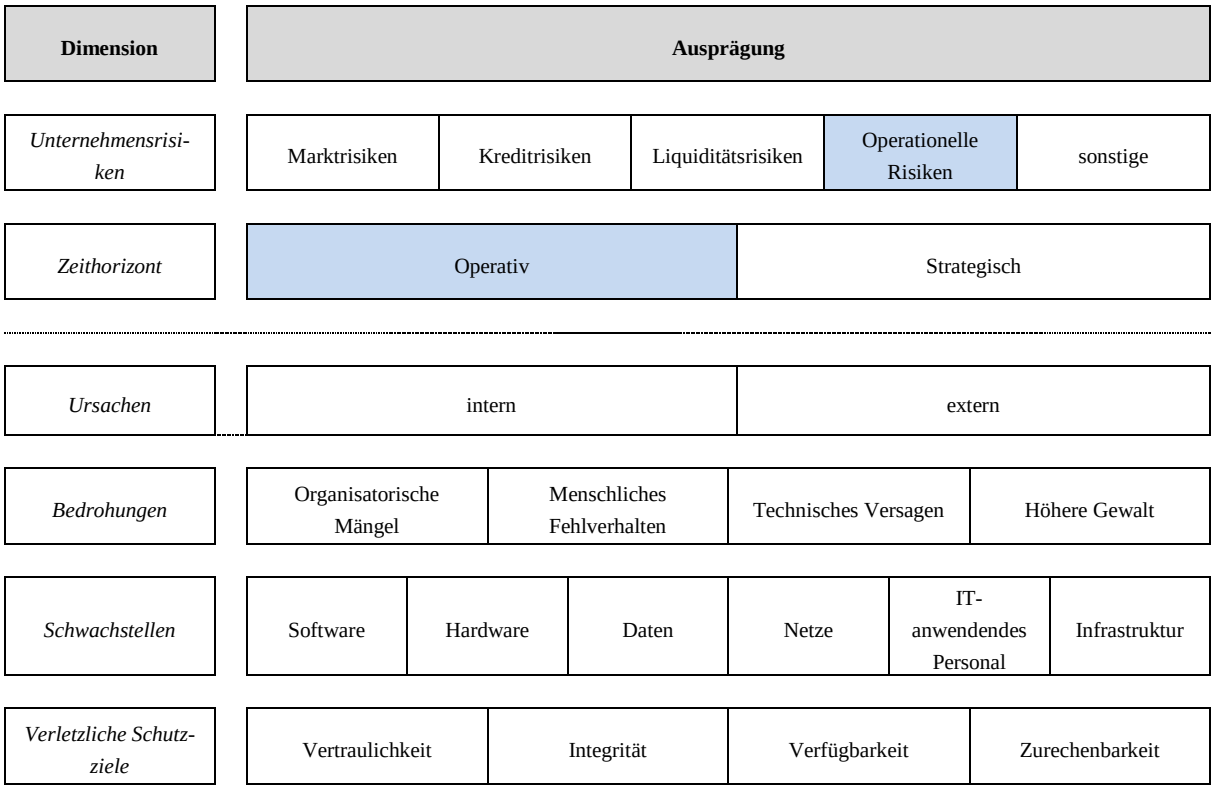


Abb. 2.8: Darstellung des Ergebnisses der morphologischen Analyse

2.4 Anwendung der Typologisierung

Im Folgenden wird die Anwendung des morphologischen Kastens anhand von zwei Beispielen, ELENA und dem CO_2-Emissionshandel, illustriert, die bereits im vorangegangenen Kapitel vorgestellt wurden und unterschiedliche Aspekte des IT-Risikos beleuchten.[101] Dabei gilt die Einschränkung, dass ausschließlich Risiken betrachtet werden, die nach Umsetzung des Projektes entstanden sind oder entstehen könnten.

Ausgehend von den obigen Erläuterungen und der Grundvoraussetzung, dass beide Beispiele im täglichen Geschäftsablauf durch IT unterstützt werden, können die hieraus resultierenden Risiken innerhalb der unternehmerischen Risikolandschaft eingeordnet werden. Im Sinne der Typologisierung sind sie daher den operationellen Risiken zugehörig und finden sich aufgrund der Explikation von Projektrisiken im operativen Zeithorizont wieder.

2.4.1 ELENA

ELENA unterliegt einigen potenziellen Bedrohungen, die bislang noch nicht umgesetzt wurden. Hierzu zählen organisatorische Mängel ebenso wie das menschliche Fehlverhalten. Im Fall der organisatorischen Mängel begründet sich dies aus Erfahrungen, die wäh-

[101] Siehe hierzu zweites Kapitel dieses Arbeitsberichtes.

rend des Betriebs des IT-Systems der Bundesagentur für Arbeit gemacht wurden. Ein falsches IT-Sicherheitskonzept im Sinne der Rechte- und Rollenzuweisung oder mangelnde Zugriffskontrollen waren ausschlaggebende Faktoren für die Missstände bei der Bundesagentur für Arbeit und sind hier ebenso denkbar. Auch das menschliche Fehlverhalten, das sich in einer vorsätzlichen Handlung wie z. B. dem unautorisierten Zugriff auf Daten oder der Manipulation von Daten am Speicherort bzw. alternativ bei der Übertragung äußert, stellt ein erhebliches Bedrohungspotenzial dar, welches in Kombination mit den organisatorischen Mängeln die gespeicherten, sensiblen Daten erheblich gefährden kann. Demzufolge zählen Daten, Software und Netze zu den potenziellen Schwachstellen. Weiterhin kann das IT-anwendende Personal als vierte Schwachstelle ausgemacht werden, da es bspw. Signaturkarten verlieren oder Trojaner im Anhang von E-Mails zur Ausspähung von Passwörtern ausführen und somit das gesamte System gefährden könnte. Damit bestehen interne und externe Ursachen für IT-Risiken. Als verletzliche Schutzziele werden die Vertraulichkeit, Integrität und Zurechenbarkeit identifiziert, da weder der Zugriff durch Unberechtigte, die Manipulation der Daten noch eine falsche Identität verhindert werden können. Untenstehend befindet sich die grafische Veranschaulich der erläuterten Sachverhalte (vgl. Abb. 2.9).

Dimension	**Ausprägung**					
Ursachen	**intern**			**extern**		
Bedrohungen	Organisatorische Mängel	Menschliches Fehlverhalten		Technisches Versagen		Höhere Gewalt
Schwachstellen	Software	Hardware	Daten	Netze	IT-anwendendes Personal	Infrastruktur
Verletzliche Schutzziele	Vertraulichkeit	Integrität		Verfügbarkeit		Zurechenbarkeit

Abb. 2.9: Einordnung des ELENA

2.4.2 CO_2-Emissionswertehandel

Das Beispiel des CO_2-Emissionswertehandels schildert in Ergänzung zu ELENA, bei dem bislang lediglich potenzielle Bedrohungen aufgezeigt wurden, einen tatsächlichen Angriff. Ausgehend von einer kriminellen Handlung, die sich in der Schaffung einer Phishing-E-Mail ausdrückte und der Tatsache, dass mehrere Verantwortliche auf diese E-Mail reagierten und ihre Nutzerdaten preisgaben, lassen sich die Bedrohung menschliches Fehlverhalten und die Schwachstelle des IT-anwendenden Personals identifizieren Auch hier lie-

gen also interne und externe Ursachen vor. Hieraus ergaben sich die Verletzung der Vertraulichkeit und der Zurechenbarkeit, da Unberechtigte auf die Zertifikate zugreifen konnten und diese unter falscher Identität veräußerten (vgl. Abb. 2.10).

Dimension	**Ausprägung**					
Ursachen	intern			extern		
Bedrohungen	Organisatorische Mängel	Menschliches Fehlverhalten		Technisches Versagen		Höhere Gewalt
Schwachstellen	Software	Hardware	Daten	Netze	IT-anwendendes Personal	Infrastruktur
Verletzliche Schutzziele	Vertraulichkeit	Integrität		Verfügbarkeit		Zurechenbarkeit

Abb. 2.10: Einordnung des Trojaners im CO_2-Emissionswertehandel

3 IT-Risiken thematisierende Publikationsorgane und politische Organisationen

Jan Ringas

3.1 Zum Einfluss von Publikationsorganen und politischen Organisationen auf das politische Geschehen

Um IT-Risiken zu identifizieren und zu minimieren bzw. Vorgehensweisen zu ermitteln, die diese Risiken möglichst gering halten, haben sich *politische Organisationen* gebildet, die die Ergebnisse ihrer Arbeit der Öffentlichkeit mitteilen, z. B. um diese zum Gegenstand der öffentlichen Diskussion zu machen. Das Beispiel der Piratenpartei verdeutlicht, wie ein (vermeintlicher) IT-Skandal wie das Sperren von Webseiten durch eine spezifische Gruppe an die Öffentlichkeit getragen wird und so von einer breiten Masse thematisiert wird. Unterstützend wird die Verbreitung der Arbeit und der Anliegen dieser politischen Organisationen in der Öffentlichkeit von *Publikationsorganen* begleitet.

Das Ziel dieses Abschnitts ist es, eine Kategorisierung von Publikationsorganen vorzunehmen und ausgewählte, IT-Risiken thematisierende Publikationsorgane anhand dieser Kategorisierung vorzustellen. Im Weiteren werden politische Organisationen vorgestellt und an konkreten Fällen von (vermeintlichen) IT-Risiken und IT-Skandalen aufgezeigt, welche Rolle die politischen Organisationen und Publikationsorgane gespielt haben und wie es gegebenenfalls im Zusammenspiel gelungen ist, Einfluss auf die Gesetzgebung oder die Anwendung von Recht zu nehmen.

3.2 Kategorisierung von Publikationsorganen und exemplarische Vorstellung wichtiger Vertreter

Ein Publikationsorgan ist eine „Zeitung, Zeitschrift einer politischen od. gesellschaftlichen Vereinigung“[102]. Aufgrund der wachsenden Bedeutung des Internets werden in dieser Arbeit auch Publikationen, die über das Internet veröffentlicht werden, zu den Publikationsorganen gezählt.[103]

[102] O. V. (2000), S. 704.

[103] Diese Erweiterung des ursprünglichen Begriffs des Publikationsorganes nach DONSBACH ET AL. ist zulässig. Die Autoren stellen Online-Medien – zumindest zum Teil je nach Art des Inhalts – als eine Erweiterung der Printmedien dar. Vgl. Donsbach et al. (2003), S. 310 ff.

Kategorisierung

Nach STROHMEIER lassen sich die Massenmedien aufteilen in Printmedien, Medien des Rundfunks (Hörfunk und Fernsehen) sowie Online-Medien bzw. das Internet (vgl. Tab. 3.1).[104] Diese drei *Medienarten* lassen sich nach den Merkmalen Vermittlungsleistung sowie Wirkung kategorisieren.

Die *Vermittlungsleistung* bezeichnet den Umfang an Informationen, die das jeweils betrachtete Medium vermitteln kann. Printmedien weisen die höchste Vermittlungsleistung auf, weshalb sie „grundsätzlich mehr Substanz bzw. ‚breitere' oder ‚tiefere' Informationen als der Rundfunk bieten"[105] können. Durch den Zeitaufwand, den das Verfassen, Drucken und der Transport zum Leser beansprucht, kann die Aktualität von Printmedien nicht der von Rundfunk- oder Online-Medien entsprechen. Daher sind Printmedien vor allem dazu geeignet, in Rundfunk- oder Online-Medien bereits vermittelte Informationen zu vertiefen und zu erweitern. Die Vermittlungsleistung der Rundfunkmedien ist geringer als die der Printmedien, da diese durch die Darstellung in Ton – und beim Fernsehen zusätzlich in Bild – zur Verknappung gezwungen sind („Damit ist das Fernsehen zur Personalisierung, Symbolisierung und Verkürzung von politischen Ereignissen gezwungen"[106]). Die Vermittlungsleistung von Online-Medien lässt sich durch die dezentrale Organisation und fehlende Kontrolle von Inhalten nur schwer allgemein charakterisieren, jedoch weist dieses Medium durch die Verbindung von Darstellung in Ton, Bild und Text je nach Inhalt sowohl die hohe Aktualität der Rundfunkmedien als auch die hohe Vermittlungsleistung der Printmedien auf.

Bei der *Wirkung* weisen die drei Medientypen ebenfalls Unterschiede auf. So ist die Wirkung der Printmedien im Vergleich zu den Rundfunkmedien sehr schwach suggestiv, während die Wirkung der Rundfunkmedien äußerst suggestiv ist. Dies hängt nach STROHMEIER davon ab, wie die Informationen von den Konsumenten der Medientypen aufgenommen werden: Während der Zeitungsleser selbst bestimmen kann, was er wann wie oft und wie intensiv liest, ist der Konsument von Rundfunkmedien davon abhängig, in welcher Form welche Informationen wann gesendet werden. Bei den Online-Medien gilt, wie bei der Vermittlungsleistung, dass diese je nach Art der publizierten Information entweder eher die Charakteristika der Printmedien oder die der Rundfunkmedien aufweisen.[107]

[104] Vgl. hier und im Folgenden: Strohmeier (2004), S. 28 f.
[105] Strohmeier (2004), S. 28.
[106] Strohmeier (2004), S. 40.
[107] Vgl. Strohmeier (2004), S. 48ff.

Merkmal	Ausprägungen		
Medienart	Printmedien	Rundfunkmedien	Online-Medien
Vermittlungsleistung	Hohe Informationskapazität	Hörfunk: sehr geringe Informationskapazität Fernsehen: geringe Informationskapazität	Vereint Printmedien und Rundfunkmedien, abhängig von Publizist
Wirkung	Weniger subtil und suggestiv	Subtil und suggestiv	Abhängig von Publizist

In Anlehnung: Strohmeier (2004).

Tab. 3.1: Kategorisierung der Medientypen Printmedien, Rundfunkmedien und Online-Medien

Vertiefend kategorisiert STROHMEIER *Printmedien* nach ihrem Erscheinungsrhythmus, ihrem Vertriebsweg, dem Verbreitungsgebiet, dem Informationsstil sowie dem Grad der journalistischen Unabhängigkeit (vgl. Tab. 3.2).[108]

Beim *Erscheinungsrhythmus* wird unterschieden zwischen Tageszeitungen, Wochenzeitungen und Nachrichtenmagazinen. Tageszeitungen erscheinen täglich (montags bis samstags), während Wochenzeitungen und Nachrichtenmagazine nur einmal in der Woche erscheinen. Die unterschiedlichen Erscheinungsrhythmen beeinflussen die Art der Berichterstattung: Während Tageszeitungen über das Geschehen des Vortags berichten, beziehen sich Wochenzeitungen verstärkt auf Hintergrundinformationen und weiter gehende Zusammenhänge. Nachrichtenmagazine unterscheidet von den Wochenzeitungen, dass die Inhalte häufig die Form von „zu ‚Storys' verarbeiteten Nachrichten, die in besonderer Weise auf einen investigativen (…) Journalismus schließen lassen"[109], annehmen.

Das Merkmal *Vertriebsweg* unterteilt sich in zwei Kategorien: Abonnement oder Straßenverkauf. Abonnementzeitungen werden in der Regel direkt an die Haushalte geliefert, während Straßenverkaufszeitungen nur zu einem geringen Teil im Abonnement zugestellt werden.[110]

Bei der Kategorie *Verbreitungsgebiet* unterscheidet STROHMEIER zwischen überregionalen und regionalen Zeitungen. Für überregionale Zeitungen ist charakteristisch, dass diese landesweit vertrieben werden, während regionale Zeitungen eine lokale Anbindung an ihren spezifischen Erscheinungsort aufweisen.

Der *Informationsstil* lässt sich ebenfalls in zwei Charakteristika unterscheiden: Boulevardzeitungen oder Qualitätszeitungen. Während Boulevardzeitungen reißerisch aufgemachte Inhalte präsentieren, in denen „bunte, vermischte und unterhaltungsorientierte Informatio-

[108] Vgl. Strohmeier (2004), S. 28 ff.
[109] Strohmeier (2004), S. 31 ff.
[110] Vgl. hier und im Folgenden Strohmeier (2004), S 32ff.

nen bzw. Darstellungen“[111] dominieren, weisen Qualitätszeitungen „eine seriöse Berichterstattung auf, die auf eine boulevardmäßige Aufbereitung von Informationen verzichtet“[112].

Zuletzt unterscheidet STROHMEIER Zeitungen nach ihrem Grad der *journalistischen Unabhängigkeit*. Typen, nach denen unterschieden wird, sind Partei- oder Verbandszeitungen und (im weitesten Sinne) neutrale Zeitungen. Während Partei- oder Verbandszeitungen als „reine Sprachrohre einer Partei oder eines Verbands“ definiert werden, die „somit bewusst und offiziell parteiisch“[113] sind, werden als neutrale Zeitungen alle Zeitungen definiert, „die sich nicht als Artikulationsorgan einer spezifischen Partei oder eines spezifischen Verbandes verstehen“. STROHMEIER weist allerdings darauf hin, dass dies nicht bedeute, dass diese Zeitungen immer objektiv berichten.

Merkmal	Ausprägungen		
Erscheinungsrhythmus	Täglich	Wöchentlich (Zeitung)	Wöchentlich (Nachrichtenmagazin)
Vertriebsweg	Abonnement	Straßenverkauf	
Verbreitungsgebiet	Überregional	Regional	
Informationsstil	Boulevardzeitungen	Qualitätszeitungen	
Grad der journalistischen Unabhängigkeit	Partei- oder Verbandszeitung	Neutrale Zeitungen (im weitesten Sinne)	

In Anlehnung: Strohmeier (2004).

Tab. 3.1: Kategorisierung von Printmedien

Beispiele für IT-Risiken thematisierende Publikationsorgane

IT-Zeitschriften, Schwerpunkt allgemeine Themen

Tiefer gehend als themenübergreifende Tageszeitungen berichten IT-Zeitschriften. Beispiele für derartige Zeitschriften sind *c't*, *iX*, *Computer Bild* oder *Chip*. Auch diese Zeitschriften sind Organe, deren Herausgeber ein kommerzielles Ziel verfolgen, was daher die Themenwahl und Berichterstattung einschränken kann. Diese Zeitschriften wenden sich zwar an die allgemeine Bevölkerung, jedoch wird durch die Art der Inhalte der Fokus eher auf den Teil der Bevölkerung gesetzt, der sich für IT interessiert und in diesem Bereich über Fachwissen verfügt.

Branchenspezifische (IT-)Fachzeitschriften

Eine weitere Form der Publikationsorgane stellen die branchenspezifischen (IT-)Fachzeitschriften dar. Diese Zeitschriften wenden sich an einzelne Branchen und be-

[111] Strohmeier (2004), S. 33.
[112] Strohmeier (2004), S. 33.
[113] Strohmeier (2004), S. 34.

handeln dabei auch Themen, die im Zusammenhang mit IT in dieser Branche von Bedeutung sind und beachtet werden sollten. Beispiele für derartige (IT-)Fachzeitschriften sind die *Computerwoche*, welche sich an IT-Manager richtet, oder *Der neue Kämmerer*, welcher sich an die öffentlichen Verwaltungen richtet.

DANA (Datenschutznachrichten)

Die Zeitschrift DANA ist das Publikationsorgan der Deutschen Vereinigung für Datenschutz e. V, welche viermal im Jahr erscheint.[114] Inhalte der Zeitschrift sind Aufsätze und Informationen zum Einsatz und zu Gefahren von elektronischer Datenverarbeitung, aktuelle Entwicklungen im Bereich Datenschutz, Rechtsprechungen und Gesetzesänderungen sowie Hinweise auf Veröffentlichungen der Bundes- und Landesdatenschutzbeauftragten. Die Zielgruppe der Zeitschrift ist die allgemeine Bevölkerung („Datenschutz geht alle etwas an. Sagen Sie es weiter“[115]), da allerdings nur Vereinsmitglieder die Zeitschrift kostenlos erhalten, richtet sich die Zeitschrift schwerpunktmäßig an Interessierte des Themas IT-Risiken – dabei insbesondere zum Thema Datenschutz.

3.3 Politische Organisationen

Der Duden bezeichnet eine politische Organisation als „Gruppe, Verband mit [sozial]politischen Zielen“.[116] Diese Arbeit behandelt daher Verbände und Gruppen, die sich gebildet haben, um IT-Risiken zu thematisieren und politische Interessen im Zusammenhang mit diesen durchzusetzen. Exemplarisch werden im Folgenden politische Organisationen im Kontext der Aufdeckung und des Öffentlichmachens von IT-Risiken und IT-Skandalen vorgestellt.

FoeBud e. V.

Der Verein FoeBud e. V. wurde 1987 gegründet und „setzt sich für Bürgerrechte, ungehinderte Kommunikation und Datenschutz ein“[117]. Diese Organisation wurde ausgewählt, da sie sowohl durch die BigBrother Awards Deutschland, bei denen sie Jury-Mitglied ist, als auch durch andere Aktivitäten einen hohen Bekanntheitsgrad aufweist. Die BigBrother Awards Deutschland sind eine Preisverleihung, bei der jährlich Personen, Firmen und auch öffentliche Verwaltungen einen Negativpreis erhalten, wenn sie durch ihre Aktivitäten das Recht auf informationelle Selbstbestimmung oder andere Persönlichkeitsrechte verletzt haben.

[114] Vgl. hier und im Folgenden o. V. (2010f).
[115] O. V. (2010f).
[116] O. V. (2000), S. 705.
[117] O. V. (2010j).

Ein prominenter Preisträger war Otto Schily sowohl im Jahre 2001 „für sein Eintreten gegen Bürgerrechte, Datenschutz und informationelle Selbstbestimmung unter dem Deckmantel der Terrorbekämpfung“[118] als auch im Jahre 2005 „für die undemokratische Einführung des biometrischen Reisepasses, für sein ‚Lebenswerk‘, nämlich für den Ausbau des deutschen und europäischen Überwachungssystems auf Kosten der Bürger- und Freiheitsrechte und für seine hartnäckigen Bemühungen um die Aushöhlung des Datenschutzes unter dem Deckmantel von Sicherheit und Terrorbekämpfung“[119]. Ein weiterer prominenter Preisträger aus der Politik war das Bundesministerium für Wirtschaft und Technologie im Jahre 2008, und zwar „für die Verabschiedung des Gesetzes über das ELENA-Verfahren und die damit verbundene Zwangseinführung der elektronischen Signatur“[120].

Neben der Tätigkeit in der Jury der BigBrother-Awards ist der FoeBud e. V. in weiteren Bereichen tätig, beispielhaft seien hier die Kampagne gegen den Einsatz von RFID („Stop RFID“) sowie die Bereiche Videoüberwachung, Biometrie, Vorratsdatenspeicherung, Zensur, Arbeitnehmerdatenschutz sowie die Einführung der Gesundheitskarte genannt.

Stoppt die e-Card

Das Bündnis Stoppt die e-Card bildete sich als Reaktion auf die geplante Einführung der Gesundheitskarte, die laut Bundesministerium für Gesundheit die Leistungsfähigkeit der Ärztinnen und Ärzte durch einen schnellen und sicheren Zugang zu und Austausch von Informationen steigern soll. Das Bündnis kritisiert, dass ein „unabhängiger und demokratischer Diskussionsprozess in der Öffentlichkeit“ fehlt und die Öffentlichkeit daher nicht angemessen über die Schwachpunkte und Gefahren der e-Card informiert ist.[121]

Laut dem Bündnis weist die Gesundheitskarte mehrere Schwachpunkte und Gefahren auf. Zum einen habe die Einführung der Gesundheitskarte hohe Verwaltungskosten zur Folge, die auf Kosten der Behandlung der Patienten gingen. Zum anderen würden persönliche Daten der Patienten in einer zentralen Datenbank gespeichert und verwaltet, was unter anderem sichere Zugriffsrechte voraussetze, die nicht ausreichend geklärt seien. Zuletzt wird kritisiert, dass der Nutzen der Gesundheitskarte nicht das Ausmaß erreichen werde, wie dies behauptet wird. Das Bündnis „Stoppt die e-Card“ hat eine Petition gestartet, die bislang (Stand: Juli 2010) über 739.000 Personen unterzeichnet haben. Das Bündnis leistet dabei ausschließlich Aufklärungsarbeit über Risiken und Gefahren des IT-Einsatzes. Es ist in seiner Arbeit politisch aktiv (so zum Beispiel durch das Starten ihrer Petition), jedoch nicht aktiv an der Gesetzgebung beteiligt.

[118] O. V. (2010a).
[119] O. V. (2010a).
[120] O. V. (2010a).
[121] Siehe hier und im Folgenden o. V. (2010l).

Deutsche Vereinigung für Datenschutz e. V.

Die Deutsche Vereinigung für Datenschutz e. V. wurde im Jahre 1977 gegründet, Anlass waren die ersten Datenschutzgesetze, die zuvor verabschiedet wurden. Der Verein ist ebenfalls in der Jury der BigBrother-Awards Deutschland vertreten. Ähnlich wie das Bündnis Stoppt die e-Card will der Verein die Bevölkerung über Nachteile und Risiken des IT-Einsatzes informieren. Auf der offiziellen Homepage ist dazu zu lesen: „[Die] Aufgabe [besteht] weniger darin, Datenskandale aufzudecken, sondern vorrangig darin, die Bevölkerung über Gefahren des Einsatzes elektronischer Datenverarbeitung und der möglichen Einschränkung des Rechts auf informationelle Selbstbestimmung zu beraten und aufzuklären“[122].

Bundesamt für Sicherheit in der Informationstechnik

Beim Bundesamt für Sicherheit in der Informationstechnik (BSI) handelt es sich um eine staatliche Organisation, die Auskunft zu verschiedenen IT-sicherheitsrelevanten Themen gibt. Dazu gehören Themen wie die Biometrie, E-Government, Sicherheitsberatung oder auch Zertifizierung und Akkreditierung.[123] Das BSI führt Studien zu diesen Themen durch. Ergebnisse dieser Studien werden im Internet auf der Homepage des BSI sowie in der Zeitschrift „<kes>“ veröffentlicht. Das BSI leistet Aufklärungsarbeit und ist beratend – durch die Wirkung ihrer Publikationen – im politischen Umfeld aktiv.

Piratenpartei Deutschland

Die Piratenpartei Deutschland wurde am 10.09.2006 gegründet. In ihrem Parteiprogramm werden unter anderem Ziele wie die „Verteidigung der Bürgerrechte“ sowie die Stärkung des „Rechts auf informationelle Selbstbestimmung“ genannt. Diese Partei ist im Gegensatz zu den im Bundestag vertretenen Parteien nicht in allen für eine (Regierungs-)Partei relevanten Themen mit einer eigenen Meinung vertreten, vielmehr konzentriert sie sich auf ein Kernthema, die Freiheit im Netz.[124] Einzuordnen ist diese Organisation als eine unabhängige Organisation, welche zum Ziel hat, den etablierten Parteien durch die selbst erzeugte Aufmerksamkeit auf das Thema IT-Risiken hinzuweisen.

ChaosComputerClub e. V.

Der ChaosComputerClub e. V. (CCC) wurde 1981 als ein Zusammenschluss von Hackern gegründet, um die „Möglichkeiten der gerade aufkommenden elektronischen Datennetze

[122] o. V. (2010n).
[123] Vgl. hier und im Folgenden o. V. (2010b).
[124] Vgl. Blumberg (2010), S. 19.

(…) einer kreativen Nutzung zuzuführen“[125]. In den nachfolgenden Jahren konnte der CCC z. B. durch Aktionen, welche die Schwachstellen von Systemen aufdeckten, diesen Charakter einer einfachen Hackervereinigung ändern zu einer Organisation, die IT-Risiken und deren Gefahren für die Bevölkerung thematisierte. Heute behandelt der CCC Themen wie Biometrie, Vorratsdatenspeicherung, die Elektronische Gesundheitskarte oder Zensur und Netzneutralität.[126] Der CCC ist ebenfalls Bestandteil der Jury der BigBrother-Awards Deutschland.

3.4 Rolle der IT-Risiken thematisierenden politischen Organisationen und Publikationsorgane in Datenskandalen

Für das Entstehen eines Skandals ist es erforderlich, dass ein Informant, der Wissen über einen Missstand besitzt (oder dies vortäuscht), den Skandalierer darüber informiert. Diese Rolle des Informanten kann unter anderem durch die IT-Risiken thematisierenden politischen Organisationen eingenommen werden, da diese durch ihre Arbeit das Vorhandensein eines Missstandes erkennen können. Die Publikationsorgane, die ebenfalls IT-Risiken thematisieren, nehmen dann entweder die Rolle des Skandalierers ein, nachdem die politischen Organisationen mit ihren Informationen zu dem Missstand an sie herangetreten sind, und prangern den Missstand und den Skandalierten öffentlich an oder sie nehmen die Rolle des neutralen Beobachters ein und berichten lediglich über die Skandalierung.[127]

Nicht jeder Missstand wird zum Skandal. Dies kann daran liegen, dass der Missstand nicht entdeckt wird, es kann aber auch daran liegen, dass der Missstand in den Massenmedien nicht thematisiert wird und dadurch die für einen Skandal erforderliche öffentliche Empörung nicht vorhanden ist. Die fehlende Thematisierung eines Missstandes in den Medien lässt sich nach STROHMEIER damit erklären, dass diese aus der Fülle an vorliegenden Informationen diejenigen auswählen müssen, die am ehesten eine Berichterstattung wert sind. Als Folge dieser Selektion entscheiden die Massenmedien damit darüber, „welche Themen öffentlich und somit zu einem Thema auf der Publikums- bzw. Bevölkerungsagenda werden (können) und welche nicht.“[128]

Einführung des Elektronischen Entgeltnachweises (ELENA)

Mit ELENA sollten ab dem 01. Januar 2010 Arbeitgeber Daten ihrer Arbeitnehmer an ein Zentralregister senden, damit diese dort Behörden zur Verfügung stehen (z. B. zur Berechnung der Höhe des einem Antragstellers zustehenden Arbeitslosengeldes).

[125] Vgl. o. V. (2010e).
[126] Vgl. o. V. (2010d).
[127] Vgl. Kepplinger, Ehming & Hartung (2002), S. 121 ff.
[128] Strohmeier (2004), S. 120.

Gegen die Einführung von ELENA hatten mehrere Organisationen Bedenken formuliert, allerdings ohne, dass in den Massenmedien ausführlich darüber berichtet wurde.[129] Auch nach der Veröffentlichung des Gesetzbeschlusses im Bundesgesetzblatt vom 01. April 2009 war die Öffentlichkeit noch nicht für das Thema sensibilisiert. Erst nachdem zwei Petitionen gegen ELENA eingereicht wurden, wurde die Berichterstattung in den Massenmedien ausführlicher. So berichteten diese über den Umfang der für ELENA gesammelten Daten (Streik- und Fehlzeiten sollten mit übermittelt werden), was eine Diskussion in der Öffentlichkeit anstieß. Zwar wurden die Petitionen nicht von genügend Personen unterzeichnet, so dass der Petitionsausschuss des Bundestages nicht tätig wurde, jedoch führte die wachsende Berichterstattung über den hohen Umfang an gesammelten Daten dazu, dass zunächst dieser Umfang verringert wurde und aktuell sogar geprüft wird, ob ELENA vollständig gestoppt werden sollte.[130]

Einführung der elektronischen Gesundheitskarte

Das Gesundheitsministerium wollte in diesem Fall eine Karte einführen, auf der persönliche Daten des Versicherten wie z. B. sein Foto, sein Name gespeichert sein sollten. Zusätzlich sollte die elektronische Gesundheitskarte Daten wie eine Dokumentation über die bisher verschriebenen Arzneimittel oder Vorerkrankungen speichern. Als Vorteile nannte das Gesundheitsministerium, dass die Daten zentral gespeichert würden, so dass die behandelnden Ärzte einfach auf die relevanten Daten zugreifen könnten.[131]

Datenschützer kritisierten unter anderem, dass die genannten Vorteile nicht in der Höhe gegeben seien, wie dies dargestellt sei. Aufgrund von Protestaktionen, z. B. vom Bündnis Stoppt die e-Card (u. a. eine Petition gegen die e-Card), wurde in der Öffentlichkeit eine Diskussion über die Nachteile der elektronischen Gesundheitskarte angestoßen, so dass die Einführung der elektronischen Gesundheitskarte durch die notwendigen Anpassungen verzögert wurde und diese bis heute noch nicht stattgefunden hat.

Skandal bei der Deutschen Bahn

Angestellte der Deutschen Bahn wurden ohne ihr Wissen und ohne, dass ein Anfangsverdacht bestand, ausgespäht, um Fälle von Korruption aufzudecken[132]. Aufgedeckt wurde dieser Missstand durch einen anonymen Informanten, was zeigt, dass in einer Skandalierung die Rolle des Informanten nicht zwangsläufig durch eine politische Organisation eingenommen werden muss. Die Rolle des Skandalierers wurde jedoch auch hier

[129] Vgl. o. V. (2010g).
[130] Vgl. o. V. (2010h).
[131] Vgl. o. V. (2010c).
[132] Vgl. http://stern.de/wirtschaft/news/unternehmen/daten-skandal-bahn-bespitzelte-eigene-mitarbeiter-652179.html.

von den Massenmedien eingenommen. Die Rolle des Skandalierten hatte der Vorstandschef der Deutschen Bahn Hartmut Mehdorn inne, dem die zögerliche Informationspolitik nach Bekanntwerden des Missstandes angelastet wurde. Die Berichterstattung in den Medien und die damit verbundenen Forderungen nach Konsequenzen hatten letztendlich den Rücktritt des Skandalierten zur Folge, was in diesem Fall die Macht und den Einfluss der Medien deutlich macht.

Metro-Skandal

Im Kontext des sogenannten Metro-Skandals nahm das Bündnis StopRFID die Rolle eines investigativ tätigen Informanten ein. Das Bündnis konnte aufdecken, dass das Unternehmen Metro seinen Testkunden die Risiken des Einsatzes von RFID-Chips verschwieg und diese auch nicht darüber informierte, dass sich in ihren Kundenkarten ein solcher RFID-Chip befand.[133] Nach dieser Aufdeckung und anderen Maßnahmen wie öffentlichen Demonstrationen wurden die Medien aufmerksam und berichteten über den Fall.[134] Diese Berichterstattung hatte zur Folge, dass die Metro AG die Kundenkarten mit den RFID-Chips zurücknahm und die betroffenen Kunden in Form von 50 Payback-Punkten entschädigte.[135]

[133] Vgl. o. V. (2010i).
[134] Vgl. o. V. (2010k); Giese (2008).
[135] Vgl. o. V. (2010i).

II Methoden zur Prävention von IT-Risiken in Unternehmen

4 IT-Compliance in IT-Governance-Frameworks

Mario Nolte

4.1 Zusammenhang von rechtlichen Anforderungen und IT-Governance

Die Einhaltung von rechtlichen Anforderungen aber auch die Einhaltung von anderen Vorgaben, Normen und Standards wird heute unter dem Begriff der *Corporate Compliance* diskutiert,[136] wobei sich diese Rechtstreue natürlich nicht von selbst in einem Unternehmen vollziehen kann. Compliance erfordert ein proaktives Vorgehen der Geschäftsführung, welches sich auf das gesamte Unternehmen auswirken muss.[137] Der Informationstechnologie (IT) kommt dabei eine besondere Bedeutung zu, stellt sie (mit zunehmender Durchdringung des Unternehmens) doch immer mehr Informationen zur Verfügung, von deren Richtigkeit das Unternehmen selbst, aber auch der Vorstand rechtlich abhängig ist.[138] Die von den Anteilseignern geforderte organisatorische Ausrichtung an regulatorischen Vorgaben wird hinsichtlich der IT von der *IT-Governance* erfasst. Sie stellt die Verantwortung von Führungskräften dar, Organisationsstrukturen und Prozesse so zu gestalten, dass die Unternehmens-IT dazu beiträgt, die Organisationsstrategie abzubilden und die Ziele zu erreichen.[139] Dabei bedient sich die IT-Governance so genannter *Frameworks*, die ihrerseits Methoden zusammenfassen, welche industrieübergreifend hohe Ähnlichkeit haben und sich in der Praxis bewährt haben.[140]

Um zu prüfen, wie weit der rechtliche Anspruch der Compliance durch den organisatorischen Aspekt in Form der IT-Governance Frameworks unterstützt wird, soll im Fokus dieses Kapitels die Frage stehen, *welchen Beitrag die IT-Governance Frameworks zur Sicherstellung der Compliance* (also zur Vermeidung von Rechtsbruch) liefern können. Dazu werden zunächst die regulatorischen Rahmenbedingungen und anschließend die populärsten IT-Governance Frameworks herausgearbeitet. Anschließend werden diese Frameworks auf Erfüllung der erarbeiteten rechtlichen Anforderungen hin untersucht, nachdem kurz auf die Vorgehensweise eingegangen wurde. Abschließend wird ein Überblick über die Untersuchung gegeben, wobei auch mögliche Aussagen über die angemessene Berücksichtigung von Compliance-Anforderungen in den betrachteten Frameworks abgeleitet werden sollen.

[136] Vgl. Teubner & Feller (2008), S. 402.
[137] Vgl. Vetter (2007), S. 33.
[138] Vgl. Heschl & Middelhoff (2005), S. 9.
[139] Vgl. IT Governance Institute (2005), S. 6.
[140] Vgl. Johannsen & Goeken (2006), S. 14.

4.1.1 IT-Compliance – regulatorischen Rahmenbedingungen an die Unternehmens-IT

Die Vielzahl von Gesetzen und Vorgaben, welche die *IT-Compliance* betreffen, macht es schwierig, den Begriff und die Thematik in einen festen Rahmen zu bringen, zumal die Einhaltung von IT-Compliance dadurch erschwert wird, dass aus den unterschiedlichsten Fachrichtungen Anforderungen an die IT gestellt werden.[141] So werden in Zusammenhang mit der IT-Compliance oftmals Gesetze genannt, welche Regelungen für die Informationstechnologie oder das Finanzwesen betreffen.[142] Hier sind beispielsweise Begriffe wie *Datenschutz-Compliance*[143] oder *SOX-IT-Compliance*[144] zu finden. In einigen Fällen wird der Begriff IT-Compliance jedoch auch durch die Angabe von Gesetzen konkretisiert, so dass erkennbar ist, zu welchen rechtlichen Vorgaben die Rechtstreue erreicht werden soll. Um dennoch wenigstens eine allgemeine Aussage über die Erfüllung von gesetzlichen Anforderungen, insbesondere der Ordnungsmäßigkeit und der Sicherheitsanforderungen, treffen zu können, wird eine IT-Compliance-Checkliste[145] genutzt (Abbildung 4.1), welche die Compliance-Bereiche *Sicherheits- und Notfallkonzept, Dokumentationspflichten, Elektronische Archivierung von E-Mails, IT-Security und Zertifizierung sowie IT-Dienstleister* behandelt:

	IT-Compliance-Bereich / Fragestellung	Compliant	Non compliant
		Ja	**Nein / weiß nicht**
1	**Gibt es für Ihre IT ein Sicherheits- und Notfallkonzept?** - Automatisches Backup / Spiegelung der Server - Masterplan für Systemabsturz und Recovery-Maßnahmen - Redundante Server, USV für bestimmte Server		
2	**Werden die Dokumentationspflichten eingehalten?** - Dokumentation des Risikomanagements - Verfahrensverzeichnis nach BDSG - Schriftliche Dokumentation des ECM / DMS		
3	**E-Mail und Internetnutzung** - Gibt es eine IT-Richtlinie und E-Mail-Policy? Ist die private Nutzung ausreichend geregelt? - Gibt es eine Regelung bezüglich der Zugriffs-, Editier- und Löschrechte der Nutzer? - Erfolgt eine (Echtzeit-) Archivierung der geschäftlichen E-Mails im Originalformat? - Gibt es Vorgaben bezüglich der Ablage von geschäftlichen E-Mails oder ein (softwaregestütztes) automatisches E-Mail-Management?		

[141] Vgl. Rath (2009), S. 151.
[142] Vgl. Teubner & Feller (2008), S. 404.
[143] Vgl. Sowa (2010).
[144] Vgl. Ritschel, Hochstein, Josi & Brenner (2006).
[145] Vgl. Rath (2009), S. 165.

	IT-Compliance-Bereich / Fragestellung	Compliant	Non compliant
4	**Archivierung** - Gibt es ein Archivierungskonzept, das die Einhaltung der Aufbewahrungsfristen sicherstellt? - Ist die Revisionssicherheit / GDPdU-Konformität des Archivierungssystems gewährleistet? - Ist die Archivierung an ein ECM oder DMS gekoppelt?		
5	**Zertifizierung / Standards** - Sind Ihre IT-Systeme oder Teile davon zertifiziert? - Kommen IT-Standards bei Ihnen zum Einsatz? - Wird ein Lizenzmanagement eingesetzt?		
6	**IT-Security** - Werden die einschlägigen IT-Standards (etwa BSI-Standards) eingehalten? - Gibt es eine effektive Spam-Abwehr, einen aktuellen Virenfilter, effektive Firewalls? - Gibt es ein Lizenzmanagement?		
7	**Beauftragung von IT-Dienstleistern** - Sind Ihre externen IT-Dienstleister auf die Einhaltung von IT-Compliance verpflichtet? - Ist der Outsourcing-Vertrag auf einem aktuellen Stand? - Gibt es personalisierte SLA?		

Quelle: Rath (2009), S. 166.

Abb. 4.1: IT-Compliance-Checkliste

Sicherheits- und Notfallkonzept

Die Forderung nach einem Sicherheits- und Notfallkonzept ergibt sich indirekt aus einer Vielzahl von gesetzlichen Vorgaben. Für den deutschen Rechtsraum ist dabei das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) zentral, welches als Artikelgesetz mehrere Gesetze von unterschiedlichstem Inhalt vereint. Dabei fordert das KonTraG mit § 91 Aktiengesetz (AktG), ein *Überwachungssystem zur Früherkennung existenzgefährdender Entwicklungen* einzurichten. Damit sind Vorkehrungen zur Vermeidung von Vermögensschäden zu treffen, so dass auch entsprechende Vorkehrungen zum Schutz der Informationssysteme zu treffen sind.[146] Für andere Gesellschaftsformen ergeben sich ähnliche Forderungen aus den entsprechenden Regelungen, wie etwa § 43 GmbHG oder auch § 347 HGB.[147] Neben diesen allgemeinen Forderungen existieren für den Finanzsektor spezielle Regelungen zur IT-Sicherheit und zur Erstellung eines IT-Notfallkonzepts als Teil des Risikomanagements, ist doch der Finanzsektor in besonderer Weise von der IT

[146] Vgl. Federrath & Pfitzmann (2006), S. 288.
[147] Vgl. Rath (2009).

abhängig. So fordert die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) mit Abschnitt AT 7.2 in ihren Mindestanforderungen an das Risikomanagement (MaRisk), dass die IT-Systeme Integrität, Verfügbarkeit, Authentizität sowie Vertraulichkeit von Daten sicherstellen müssen, so dass insbesondere die IT-Sicherheitsziele aus § 2 BSIG erfüllt werden sollen.[148]

Dokumentationspflichten

Die bereits benannten Leitlinien für die Unternehmensüberwachung zur Früherkennung existenzgefährdender Entwicklungen (KontraG, GmbHG etc.) aber auch internationale Regelungen wie der Sarbanes Oxley Act erfordern ein adäquates Risikomanagementsystem.[149] Neben der Tatsache, dass dieses Risikomanagement schon aus Gründen der Nachvollziehbarkeit und Transparenz dokumentiert sein sollte, ergibt sich die Notwendigkeit der Dokumentation auch aus gesetzlichen Vorgaben. So fordert § 93 Abs. 2 AktG vom Vorstand den Nachweis über dessen sorgfältiges Handeln, so dass schon im Sinne dieser Nachweispflicht ein dokumentiertes Risikomanagement notwendig ist. Ähnlich stellt sich auch die Situation im Datenschutz dar: Hier empfiehlt sich das *Verfahrensverzeichnis* schon aus Gründen der Kostenreduzierung bei der Erfüllung der datenschutzrechtlichen Anforderungen.[150] Darüber hinaus ist das Verfahrensverzeichnis aber auch zur Erfüllung des § 4e BDSG notwendig, welcher von jeder staatlichen oder privaten Stelle die *Dokumentation* des Umgangs mit personenbezogenen Daten fordert. Werden Dokumenten-Management-Systeme (DMS) genutzt, so sind zahlreiche gesetzliche Anforderungen zu beachten. Neben der Zivilprozessordnung, welche den Beweismittelcharakter eines elektronischen Dokuments regelt[151], sind auch Forderungen des HGB und der Abgabenordnung (AO) zu beachten, welche nachfolgend im Compliance-Bereich der *Archivierung* erläutert werden. Hinsichtlich der Dokumentationspflichten ist beim Einsatz eines DMS im Sinne der Grundsätze ordnungsgemäßer Buchführung (GoB) das Verfahren so zu dokumentieren, dass die Prüfbarkeit und Nachvollziehbarkeit gewährleistet ist.[152]

Elektronische Archivierung und E-Mails

Werden Dokumente elektronisch archiviert, gelten selbstverständlich die gleichen gesetzlichen Pflichten wie bei der Archivierung von Dokumenten in Papierform. So sind Aufbewahrungsfristen nach § 257 HGB, aber auch nach § 147 AO in Abhängigkeit vom archivierten Dokument zu beachten und auch die GoB müssen, im Fall von rechnungsrelevan-

[148] Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (2009).
[149] Vgl. Seibold (2006), S. 1.
[150] Vgl. BITKOM (2007), S. 8.
[151] Vgl. Hackel & Roßnagel (2008), S. 8.
[152] Vgl. Probst & Röder (2007), S. 2.

ten Belegen, weiterhin anwendbar sein. Kommt es bei der Vorbereitung, dem Abschluss und der Durchführung eines Handelsgeschäftes zur elektronischen Korrespondenz (z. B. E-Mail), so ist diese im Sinne des § 239 Abs. 3 ebenfalls so zu archivieren, dass eine Veränderung nicht möglich sein darf.[153]

IT-Security und Zertifizierung

Die Verpflichtung, IT-Systeme und deren Informationen gegen Angriffe von innen und außen zu schützen, ergibt sich implizit aus verschiedenen Gesetzen. Neben § 91 Abs. 2 AktG fordert vor allem die allgemeine Sorgfaltspflicht des Vorstandes in § 93 Abs. 1 AktG, dass die Unternehmensleitung zur Etablierung effektiver *IT-Sicherheitsmaßnahmen* und deren Kontrolle verpflichtet ist.[154] Daneben fordern aber auch § 109 TKG oder § 9 BDSG „angemessene technische Vorkehrungen" bzw. „angemessene technische und organisatorische Maßnahmen" zum Schutz der IT, so dass die IT-Sicherheit zu gewährleisten ist.[155] Ist diese IT-Sicherheit zu belegen, so kann es unter Umständen sinnvoll sein, funktionsfähige Informationssicherheits-Managementsysteme verifizieren zu lassen und eine *Zertifizierung* anzustreben.[156]

IT-Dienstleister

Wird die Datenverarbeitung des Unternehmens ausgelagert (Outsourcing), so sind neben datenschutzrechtlichen Pflichten, welche sich durch die Weitergabe der Daten ergeben (§ 4b ff. BDSG), auch hinsichtlich der Risiken Überlegungen anzustellen, so dass auch das Risikomanagement berührt wird. Diese Risiken können beim Outsourcing unter anderem durch unklare Zuständigkeiten oder das abgehende IT-Know-how entstehen, was als solches eine höhere Abhängigkeit von einem externen IT-Dienstleister mit sich bringt.[157] Die Überlegungen hinsichtlich des Risikomanagements sollten dabei Haftungsregelungen aus dem KonTraG, Sorgfaltspflichten aus dem GmbHG, Bestimmungen zur Überprüfung der ausgelagerten Buchführung aus dem HGB, aber auch Vorschriften für das Kontrollsystem aus dem SOX umfassen,[158] so dass der Outsourcing-Vertrag alle Rechte und Pflichten detailliert regeln muss.

[153] Vgl. Rath (2009), S. 158.
[154] Vgl. Rath (2009), S. 156.
[155] Vgl. Eckhardt (2008), S. 2.
[156] Vgl. Rath (2009), S. 156.
[157] Vgl. Hodel, Berger & Risi (2006), S. 185.
[158] Vgl. BITKOM (2006), S. 28.

4.1.2 IT-Governance-Frameworks – etablierte Verfahren zur IT-Steuerung

Für die Beachtung und Einbindung der regulatorischen Rahmenbedingungen spielt die Unternehmensorganisation eine erhebliche Rolle. Hierfür haben sich zahlreiche Best Practices in Form von Frameworks etabliert. Als *Framework* wird dabei ein Rahmenvorschlag verstanden, welcher im Sinne einer Grundkonzeption bei dem Entwurf eines Systems Anwendung findet.[159] Vom Charakter her entsprechen diese Best Practices einer Handlungsanleitung für den organisatorischen Aufbau des Unternehmens.[160]

Zwar steht derzeit kein *umfassendes* Modell für die Überwachung und Steuerung von IT-Prozessen zur Verfügung,[161] jedoch kann die IT-Governance durch zahlreiche Frameworks unterstützt werden, die sich dem Zweck und damit der Verwendung nach unterscheiden. Frameworks für *Governance*, *IT-Governance*, *Service Management*, *Sicherheitsmanagement*, *Qualitätsmanagement mit Maturity Assessment* sowie *Projekt Management*[162] haben dabei in zahlreichen Formen Einzug in die Praxis gehalten. Welche Frameworks in der Praxis Verwendung finden und welchem Zweck sie dabei zugeordnet werden können, kann der Tabelle 4.1 entnommen werden. Dabei wurden die Bereiche Maturity Assessment und Qualitätsmanagement zusammengefasst, versteht sich das CMMI Framework selbst doch als Framework, welches das Qualitätsmanagement unterstützt.[163]

Verwendungszweck	Unterstützendes Framework
Corporate Governance	COSO
IT-Governance	CobiT, Val IT
Service Management	ITIL, MOF, IBM IT PM, HP ITSM
Sicherheitsmanagement	IT-Grundschutz
Qualitätsmanagement & Maturity Assessment	CMMI, EFQM
Projekt Management	PRINCE 2, PMBoK,

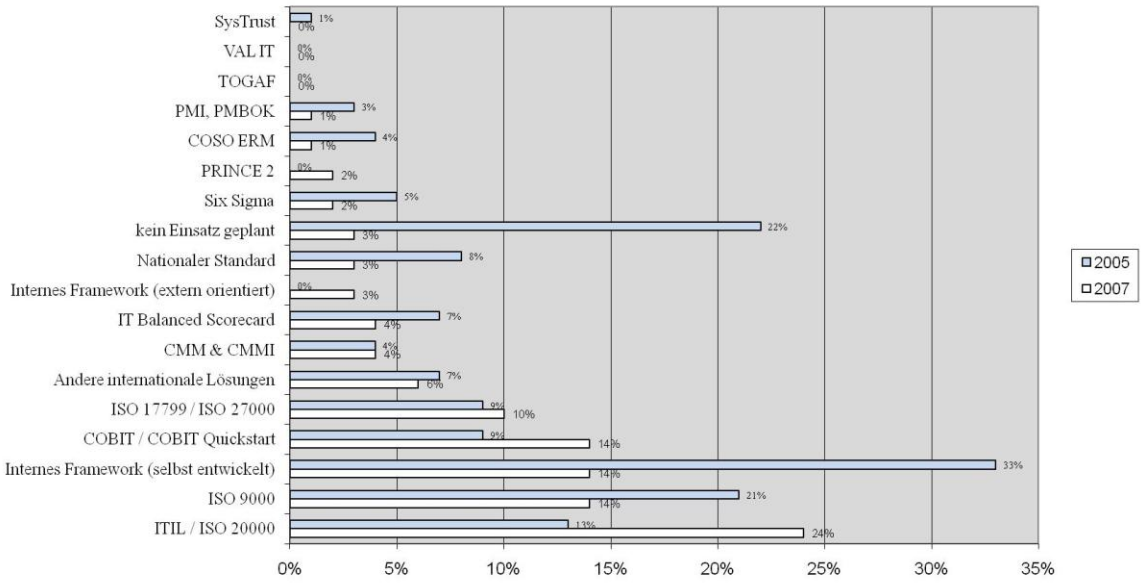
In Anlehnung: Johannsen & Goeken (2006), S. 15.

Tab. 4.1: Frameworks zur Unterstützung der IT-Governance und ihr Verwendungszweck

Um einen Überblick über die Verbreitung der IT-Governance in der Praxis zu erhalten, wurden im Jahr 2007 durch das IT-Governance Institute (ITGI) in Zusammenarbeit mit Pricewaterhouse Coopers 749 IT-Verantwortliche (CIO- bzw. CEO-Ebene) verschiedens-

[159] Vgl. Heinrich nach Heschl & Middelhoff (2005).
[160] Von diesen Frameworks klar zu unterscheiden sind Zertifikate, welche auf Standards und Normen (bspw. ISO 9000 ff., ISO 27001) basieren und in Kapitel 7 dieses Arbeitsberichtes thematisiert werden.
[161] Vgl. Heschl & Middelhoff (2005b), S. 9.
[162] Vgl. Johannsen & Goeken (2006), S. 15.
[163] Vgl. Kneuper (2003), S. 3.

ter Länder und Branchen befragt und das Ergebnis 2008 als „IT Governance Global Status Report“ veröffentlicht. Die Umfrage kam dabei unter anderem zu dem Ergebnis, dass vermehrt Aktivitäten zur Implementierung der IT-Governance geplant sind,[164] wobei die IT-Verantwortlichen Best Practices sowie Frameworks zu den am besten geeigneten Methoden zur Umsetzung der IT-Governance bewerteten.[165] Das Ergebnis gibt Auskunft darüber, welche Frameworks derzeit in den Unternehmen Verwendung finden bzw. für den Einsatz eingeplant wurden. Alle Frameworks sind zusammen mit ihrer relativen Nennung in Abbildung 4.2 dargestellt.



Quelle: ITGI (2008), S. 36.

Abb. 4.2: Populäre IT-Governance Frameworks

4.1.3 Vorgehen zur Untersuchung

Auf Basis der Umfrageergebnisse wurde je Verwendungszweck das jeweils populärste Framework hinsichtlich der Berücksichtigung rechtlicher Rahmenbedingungen untersucht.

Die folgenden Quellen wurden für die Untersuchung der einzelnen Frameworks verwendet:

[164] Vgl. ITGI (2008), S. 37.
[165] Vgl. ITGI (2008), S. 33.

Framework	Quelle(n)
COSO	Moeller (2007)
COBIT	IT Governance Institute (2007)
ITIL	Office of Government Commerce (2007a-e)
IT-Grundschutz-Kataloge	Bundesamt für Sicherheit in der Informationstechnik (2009)
CMMI	Software Engineering Institute (2006)
PmBoK	Project Management Institute (2004)

Tab. 4.2: Verwendete Quellen zu den IT-Governance Frameworks

Alle durch die IT-Compliance-Checkliste (vgl. Abbildung 4.2) vorgegebenen Kriterien wurden sodann mittels der jeweiligen Inhaltsverzeichnisse logisch zugeordnet. Als Hilfe wurde dabei auch die nachfolgende Tabelle 4.3 mit assoziierten Wörtern genutzt, um Zusammenhänge über die Glossare und Indizes der untersuchten Framework-Beschreibungen herzustellen. Da der IT-Compliance-Bereich *Zertifizierung* mit seinen Kriterien zum Einsatz von Standards bei allen untersuchten Frameworks per se bereits gegeben ist, wurde dieser Bereich der IT-Compliance-Checkliste nur genutzt, um anzugeben, welches Zertifikat mittels des Frameworks erreicht werden kann. Ebenso wurde auf eine Betrachtung des Kriteriums *Einhaltung von IT-Standards* im IT-Compliance-Bereich *IT-Security* verzichtet, hängt dieses Kriterium doch von der Umsetzung des Frameworks in der implementierenden Organisation ab.

IT-Compliance		Assoziierte Wörter	
Bereich	**Kriterium**	**Deutsch**	**Englisch**
Sicherheits- und Notfallkonzept	automatisches Backup	Datensicherung, Sicherungskopie	Recovery, restore
	Serverspiegelung	Redundante Cluster	Mirroring
	Masterplan für Systemabsturz und Recovery Maßnahmen	Notfallplan, Katastrophenplan, Notfallrechenzentrum	Continuity plan, Major catastrophe, Emergency
	Redundante Server	Ausweichserver	Redundant
	USV	Strom, Spannung, Energieunterbrechung	UPS, Power
Dokumentations-pflichten	Risikomanagement	Risiko	Documentation, record, risk
	Verfahrensverzeichnis nach BDSG	Abläufe, Prozesse	Documentation, processes
	ECM /DMS	Dokumentenmanagement, Scan	Enterprise Content Management
E-Mail & Internet	IT-Richtlinie	IT-Konzept	Policy, guideline
	E-Mail Policy	E-Mail Richtlinie	
	Rechteverwaltung	Benutzerverwaltung, Zugriffsrechte	Access permissions, Usermanagement
	Archivierung der Mails	Archivierung, elektronischer Schriftverkehr	
	E-Mail Verwaltung	E-Mail Management	
Archivierung	Archivierungskonzept inkl. Aufbewahrungsfristen		Archive, Record retention periods
	Revisionssicherheit des Archivierungssystems		Audit, auditing acceptability
	Kopplung der Archivierung an ECM / DMS	Dokumentenmanagement	
Zertifizierung	Erreichbares Zertifikat		Certificate
IT-Security	effektive Spam Abwehr, Virenfilter	Mailfilter,	Firewall
	Lizenzmanagement	Softwareverträge,	Licence, application management

IT-Dienstleister	Verpflichtung auf Compliance	IT-Compliance, Compliance Framework	
	Vertragliche Regelung	Rechte, Pflichten, Outsourcing-Vertrag	Contract, agreement, IT Service Management, Service Sourcing, Outsourcing
	personalisierte SLA	SLM	

Tab. 4.3: Assoziierte Wörter zur Untersuchung der IT-Governance-Frameworks

4.1.4 Untersuchung der IT-Governance-Frameworks auf IT-Compliance

Die Untersuchung eines jeden Frameworks muss immer vor dem Hintergrund des Zwecks und des Aufbaus von den jeweiligen Frameworks gesehen werden. Daher werden der Zweck und die Struktur der nachfolgend untersuchten Frameworks kurz erläutert, wobei auch auf Herausgeber und Zielgruppe eingegangen werden soll. Die Aktualität kann in Anlehnung an die Abbildung 4.2 bei allen hier behandelten Frameworks angenommen werden, wird diese doch durch den gegenwärtigen Einsatz in der Praxis bestätigt. Nach einigen Hinweisen zur Untersuchung wird immer eine Tabelle angegeben, welche Auskunft darüber gibt, an welcher Stelle das jeweilige Framework die zuvor erläuterten Compliance-Kriterien erfüllt. Sofern erläuternde Hinweise zum untersuchten Aspekt gegeben wurden, ist dies mit (*) in der Tabelle vermerkt.

4.1.4.1 Corporate Governance: COSO Enterprise Risk Management Framework

Das COSO Enterprise Risk Management Framework (COSO-ERM-Framework)[166] ist ein von der Organisation (Comitee of Sponsoring Organizations of the Treadway Commission) entwickeltes Rahmenwerk für Kontrollsysteme, welches auf dem COSO-Modell aufbaut. Das COSO-Modell selbst stellt dabei einen von der SEC anerkannten Standard für interne Kontrollen dar, welcher mittels Kernprinzipien und -konzepten, einer einheitlichen Terminologie sowie klarer Anweisungen und Hilfestellungen so erweitert wurde, dass heute mit dem COSO-ERM-Framework ein Rahmenwerk für das unternehmensweite Risikomanagement vorliegt.[167]

Durch den unternehmensweiten Fokus werden IT-spezifische Themen nur im elften Kapitel thematisiert. Hier wird das Thema *Masterplan für Systemabsturz* zwar zunächst auch nur kurz in einer Checkliste für kommerziell erworbene Software behandelt, später mit der Seite 309 jedoch genauer betrachtet. An dieser Stelle wird auch der Masterplan für das gesamte Unternehmen eingefordert. Folglich kann das Kriterium *Masterplan für Systemabsturz* als erfüllt gewertet werden. Nicht erfüllt blieb dagegen die Forderung nach einer *USV*. Zwar wird die Stromversorgung im Abschnitt *Effective IT Continuity Planning* the-

[166] Vgl. hier und im Folgenden Moeller (2007).
[167] Vgl. COSO (2004).

matisiert, jedoch bleibt die Notfallbetrachtung an dieser Stelle aus. Alle anderen festgestellten Zusammenhänge werden explizit dargestellt, wobei natürlich immer das Risikomanagement im Fokus steht, dessen *Dokumentation* mit dem Aufbau *risk identification model frameworks* direkt im zweiten Kapitel gefordert wird.

IT-Compliance		**Framework**
Bereich	**Kriterium**	**COSO**
Sicherheits- und Notfallkonzept	automatisches Backup	Kap. 11 S.297
	Serverspiegelung	k. A.
	Masterplan für Systemabsturz und Recovery Maßnahmen	Kap. 11 S.305, Kap. 11 S. 309
	Redundante Server	k. A.
	USV	k. A. *
Dokumentationspflichten	Risikomanagement	Kap. 2 S. 24
	Verfahrensverzeichnis nach BDSG	k. A.
	ECM /DMS	k. A.
E-Mail & Internet	IT-Richtlinie	Kap. 11 S. 296
	E-Mail Policy	k. A.
	Rechteverwaltung	k. A.
	Archivierung der Mails	k. A.
	E-Mail-Verwaltung	k. A.
Archivierung	Archivierungskonzept inkl. Aufbewahrungsfristen	k. A.
	Revisionssicherheit des Archivierungssystems	k. A.
	Kopplung der Archivierung an ECM / DMS	k. A.
Zertifizierung	Erreichbares Zertifikat	k. A.
IT-Security	effektive Spam-Abwehr, Virenfilter	Kap. 11 S. 314
	Lizenzmanagement	k. A.
IT-Dienstleister	Verpflichtung auf Compliance	k. A.
	Vertragliche Regelung	k. A.
	personalisierte SLA	k. A.

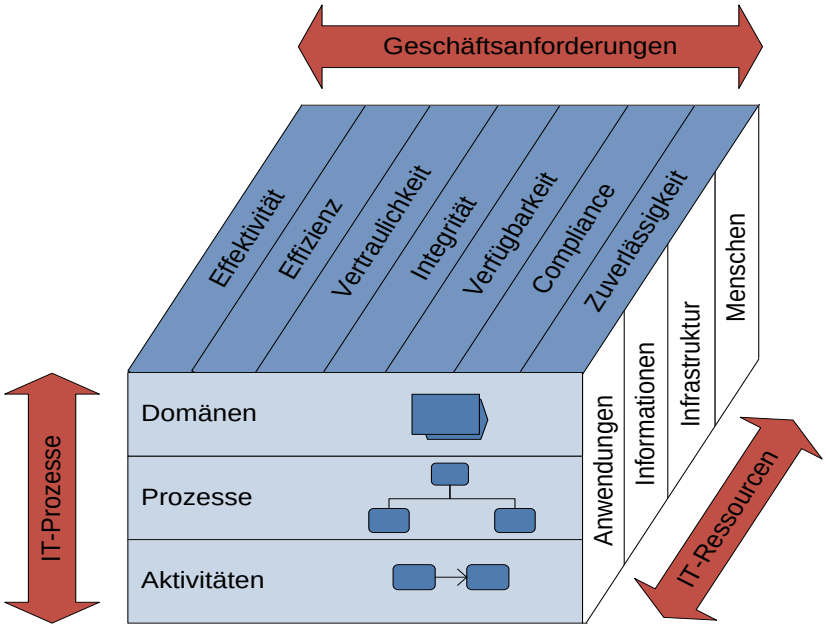
Tab. 4.4: IT-Compliance im COSO ERM-Framework

4.1.4.2 IT-Governance: COBIT

Zur Kontrolle der gesamten IT eines Unternehmens setzt COBIT[168] auf *Kontrollziele* für die Informationstechnologie, was sich aus dem Akronym *Control Objectives for Information and related Technology* ergibt. Ursprünglich für das Audit von IT-Systemen durch die Information Systems Audit and Control Foundation (ISACF) entwickelt, wurde das Framework im Jahr 1999 an das IT Governance Institut (ITGI) übertragen. Heute erfasst COBIT in der Version 4.1 die gesamte IT-Governance mittels einer umfassenden Beschreibung der Kontrollziele für IT-Prozesse. *Kontrollziele* sind dabei Aussagen zum gewünschten Ergebnis bzw. Zweck eines Prozesses, welche mittels Kontrollverfahren erreicht werden sollen. Dabei wird das Management von IT-Ressourcen auf drei Ebenen

[168] Vgl. hier und im Folgenden IT Governance Institute (2007).

betrachtet. Auf der untersten Ebene werden *Aktivitäten* beschrieben, welche benötigt werden, um ein Resultat zu erreichen. Diese Aktivitäten werden zu Gruppen zusammengefasst, welche in COBIT als *Prozesse* bezeichnet werden und so spezifische Kontrollen zulassen. Wiederum gruppiert ergeben diese Prozesse *Domänen*, welche häufig auch den Organisationsanforderungen der IT-Bereiche entsprechen. Durch die Erweiterung der COBIT-Struktur um die Dimensionen IT-Ressourcen und Geschäftsanforderungen ergibt sich der in Abbildung 4.3 dargestellte Governance-Würfel, welcher einen guten Überblick über die gesamte Struktur von COBIT gibt.[169]



In Anlehnung: IT Governance Institute (2007), S. 25.

Abb. 4.3: Governance-Würfel nach COBIT

Für die Prozesse existieren derzeit die Domänen Planung & Organisation (PO), Akquisition & Implementierung (AI), Delivery & Support (DS) sowie Monitoring und Evaluierung (ME). In der nachfolgenden Untersuchung werden somit die Prozesse (unter Angabe der Domäne und einer einstelligen Ziffer) oder auch die Kontrollziele (unter Angabe der Domäne und einer zweistelligen Ziffer) angegeben, welche das IT-Compliance-Kriterium beinhalten.

Mit dem Ziel, den Betrieb der IT auch im Falle einer größeren Störung zu gewährleisten, diskutiert der Prozess *DS 4 Continuity Management* die Themen *Backup* und auch den *Notfallplan*, welcher seinerseits auf einem *Service Continuity Management Framework*

[169] Vgl. Goltsche (2006), S. 25.

basieren soll.[170] Das Thema der *Serverspiegelung* wird dabei in der gleichen Domäne unter dem Kontrollziel *DS 4.9 Offsite Backup Storage* behandelt, wobei sich hier aus dem Begriff „offsite" auch die Forderung nach *redundanter Datenspeicherung* ergibt. Indirekte Erwähnung findet die USV, jedoch fordern DS 12.2 und DS 12.5, dass physikalische Sicherheitsmaßnahmen und das Anlagenmanagement so einzusetzen sind, dass der Betrieb des Unternehmens gewährleistet werden kann, so dass (hier mit der beispielhaften Erwähnung der Stromversorgung) auch dieses Kriterium als erfüllt angesehen werden kann. Das *Verfahrensverzeichnis nach BDSG* bleibt in dieser konkreten Form unberücksichtigt. Nutzt man jedoch das im Prozess *AI 4 Enable Operation and Use* erwähnte Verfahrensverzeichnis (konkret AI 4.3 und AI 4.4), so kann auch dieser Punkt als erfüllt angesehen werden. Das Entwickeln und Ausrollen einer *IT-Richtline* wird explizit im *PO 6 Communicate Management Aims and Direction* gefordert, wobei die hier zu erwartende Anforderung nach einer *E-Mail Richtlinie* unerwähnt bleibt, so dass dieses Kriterium als nicht erfüllt gewertet wurde. Mit dem Kontrollziel *11.2 Storage and retention arrangements* werden Verfahren für Datenspeicherung und -archivierung und hier insbesondere Vorkehrungen hinsichtlich der gesetzlichen Aufbewahrungsvorgaben gefordert, so dass das Compliance-Kriterium *Archivierungskonzept inkl. Aufbewahrungsfristen* hier seine Berücksichtigung findet. Ähnlich wird auch das Kriterium *Lizenzmanagement* nicht direkt gefordert, jedoch bindet das Kontrollziel *DS 9.1 Configuration Repository and Baseline* auch Software-Lizenzen ein, so dass das *Lizenzmanagement* an dieser Stelle gefordert wird.[171] Während die vertragliche Regelung der Beziehungen zum IT-Dienstleister direkt mit dem Kontrollziel *AI 5.2 Supplier Contract Management* gefordert wird, ergibt sich die *personalisierte Regelung* der SLA indirekt aus den Forderungen des Prozesses *DS 2 Manage third-party Services*, welcher die Regelung *klarer* Rollen, Erwartungen und Aufgaben mit Dritten fordert. Der hier gegebene Hinweis auf Compliance bezieht sich jedoch lediglich auf die Übereinstimmung der vom Drittanbieter ausgeführten Arbeiten mit den vertraglichen Regelungen, so dass die *Verpflichtung auf Compliance* im Sinne der Übereinstimmung mit regulatorischen Vorgaben an dieser Stelle keine Beachtung findet. Erwartungsgemäß hätte dieser Aspekt wenigstens im Prozess *ME 3 Ensure Compliance with external Requirements* Berücksichtigung finden können; da er jedoch auch hier unerwähnt blieb, wird dieses Kriterium als nicht erfüllt gewertet.

[170] Vgl. Goltsche (2006), S. 114.
[171] Vgl. Goltsche (2006), S. 131.

IT-Compliance		Framework
Bereich	**Kriterium**	**COBIT**
Sicherheits- und Notfallkonzept	automatisches Backup	DS 4.1 (S. 114) *
	Serverspiegelung	DS 4.9 (S. 114)*
	Masterplan für Systemabsturz und Recovery Maßnahmen	DS 4.2 (S. 114) *
	Redundante Server	DS 4.9 (S.114) *
	USV	DS 12.2 & DS 12.5 (S.146) *
Dokumentationspflichten	Risikomanagement	PO 9 (S. 63)
	Verfahrensverzeichnis nach BDSG	AI 4 (S.85)
	ECM /DMS	k. A.
E-Mail & Internet	IT-Richtlinie	PO 6 (S. 51) *
	E-Mail Policy	k. A. *
	Rechteverwaltung	AI 2.4 (S. 84), AI 4.2 (S. 94)
	Archivierung der Mails	k. A.
	E-Mail-Verwaltung	k. A.
Archivierung	Archivierungskonzept inkl. Aufbewahrungsfristen	DS 11.2 (S. 144)
	Revisionssicherheit des Archivierungssystems	k. A.
	Kopplung der Archivierung an ECM / DMS	k. A.
Zertifizierung	Erreichbares Zertifikat	k. A.
IT-Security	effektive Spam-Abwehr, Virenfilter	DS 5.9 (S. 118)
	Lizenzmanagement	AI 5.4 (S. 90) & DS 9.1 (S. 134)
IT-Dienstleister	Verpflichtung auf Compliance	k. A. *
	Vertragliche Regelung	AI 5.2 (S. 90)*
	personalisierte SLA	DS 2 (S.105)*

Tab. 4.5: IT-Compliance im COBIT-Framework

4.1.4.3 Service Management: ITIL

ITIL steht für Information Technology Infrastructure Library und stellt einen von dem UK Office of Government Commerce (OGC) herausgegebenen Best Practice Leitfaden dar, welcher als Richtlinie zum systematischen Aufbau und zum Betrieb einer durchgängig abgestimmten, professionellen IT-Servicestruktur zu verstehen ist.[172] ITIL fasst dabei aus der Praxis gewonnene Erkenntnisse, Modelle und Architekturen in sechs Büchern zusammen, welche neben der Einführung zu ITIL die Themen Servicestrategie (SSt),[173] Serviceentwurf (SD),[174] Serviceüberführung (ST),[175] Servicebetrieb (SO),[176] und kontinuierliche Serviceverbesserung (CSI)[177] behandeln. Dabei werden nicht der genaue Ablauf oder die notwendigen Werkzeuge vorgegeben, sondern vielmehr Checklisten, Aufgaben und Verfahren gefordert, welche von einer IT-Organisation umgesetzt werden sollten. Mit der Ein-

[172] Vgl. Olbrich (2006), S. 1 ff.
[173] Vgl. hier und im Folgenden Office of Government Commerce (2007a).
[174] Vgl. hier und im Folgenden Office of Government Commerce (2007b).
[175] Vgl. hier und im Folgenden Office of Government Commerce (2007c).
[176] Vgl. hier und im Folgenden Office of Government Commerce (2007d).
[177] Vgl. hier und im Folgenden Office of Government Commerce (2007e).

führung von ITIL soll das Ziel verfolgt werden, in der IT klar definierte Schnittstellen mit konkreten Ansprechpartnern, Zuständigkeiten und Verantwortlichkeiten zu erhalten, so dass flachere und flexiblere Strukturen ermöglicht werden.[178]

Da es sich bei den ITIL-Büchern ursprünglich um einen Standard aus Großbritannien handelt, konnte eine konkrete Forderung nach einem *Verfahrensverzeichnis nach BDSG* nicht festgestellt werden. Die im Rahmen des *IT-Service Continuity Management (ITSCM)* geforderten Dokumentationen der ITSCM-Pläne können jedoch bei Angabe bestimmter Aspekte (welche personenbezogenen Daten durch welches automatisierte Verfahren verarbeitet, genutzt, aber auch geschützt werden) entsprechend interpretiert werden. Deshalb gilt dieses IT-Compliance-Kriterium als erfüllt.

Das Thema *IT-Dienstleister* und damit Outsourcing wird in ITIL an verschiedensten Stellen behandelt, so dass das Outsourcing in der Service Strategy im Kapitel 6.5 Sourcing Strategy zu finden ist, wogegen konkretere Vorgaben im Buch *Service Design* im vierten Kapitel *Service Design Process* gemacht werden. Dabei ergibt sich die Forderung nach einer vertraglichen Regelung aus dem Abschnitt 4.2.1, welcher neben der Definition der Ziele des Service Level Managements (SLM) auch deren Dokumentation fordert, wobei das Thema *Compliance* jedoch unerwähnt bleibt. Die Forderung nach Einhaltung der Compliance kann lediglich aus dem Abschnitt 3.6.5 *Design of measurement systems and metrics* gefolgert werden. Da sich diese Forderung jedoch nicht explizit an IT-Dienstleister richtet, wird das Compliance-Kriterium als nicht erfüllt angesehen.

Ebenso wie das Thema der IT-Dienstleister wird auch auf das Thema *Lizenzmanagement* an verschiedenen Stellen im Buch *Service Operation* eingegangen. Neben der Erläuterung der Lizenztypen für ITSM-Tools im Kapitel 8.5 wird das Lizenzmanagement für Server explizit im Kapitel 5.4 gefordert. Für andere Anwendungen (beispielsweise Desktop-Anwendungen) wird das Lizenzmanagement nur indirekt gefordert, indem im Abschnitt 6.5 Application Management Aktivitäten aufgeführt werden, welche auf ein Lizenzmanagement abzielen (z. B. Unterstützung des IT-Finanz-Managements durch Identifizierung der Kosten für den Betrieb von Anwendungen).

[178] Vgl. Bock et al. (2006), S. 17.

IT-Compliance		Framework
Bereich	**Kriterium**	**ITIL**
Sicherheits- und Notfallkonzept	automatisches Backup	SO 5.2.3
	Serverspiegelung	SD 4.5.5.2 (S.132)
	Masterplan für Systemabsturz und Recovery Maßnahmen	SD 4.5.5.3 (S.135)
	Redundante Server	SD 4.5.5.2 (S.132)
	USV	SD 4.5.5.2 (S.132)
Dokumentationspflichten	Risikomanagement	SD 4.5.8 (S. 140)
	Verfahrensverzeichnis nach BDSG	SD 4.5.8 (S. 140)*
	ECM /DMS	k. A.
E-Mail & Internet	IT-Richtlinie	SD 4.6.4.2 (S. 142)
	E-Mail Policy	SD 4.6.4.2 (S. 142)
	Rechteverwaltung	SO 7.6 (S. 160)
	Archivierung der Mails	k. A.
	E-Mail-Verwaltung	k. A.
Archivierung	Archivierungskonzept inkl. Aufbewahrungsfristen	SO 5.6 (S. 97)
	Revisionssicherheit des Archivierungssystems	k. A.
	Kopplung der Archivierung an ECM / DMS	k. A.
Zertifizierung	Erreichbares Zertifikat	ISO 20000
IT-Security	effektive Spam-Abwehr, Virenfilter	SD 4.6.4.2 (S. 142)
	Lizenzmanagement	SO 5.4 (S. 95), SO 8.5 (S. 166)*
IT-Dienstleister	Verpflichtung auf Compliance	k. A. *
	Vertragliche Regelung	4.2.1 (S. 65)*
	personalisierte SLA	SD 4.2.5.1 (S. 68)

Tab. 4.6: IT-Compliance im ITIL-Framework

4.1.4.4 Sicherheitsmanagement: IT-Grundschutz-Kataloge

Die IT-Grundschutz-Kataloge[179] (vormals IT-Grundschutz-Handbuch) werden vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegeben und geben Empfehlungen, um einen *angemessenen* Schutz für alle Informationen einer Institution zu erreichen. Mit derzeit rund 4.000 Seiten richten sich die IT-Grundschutz-Kataloge an Behörden und Unternehmen, welche IT-Sicherheitskonzepte realisieren möchten. Die *Bausteinkataloge* enthalten Kurzbeschreibungen über Sachverhalte, so dass sie einen Überblick über die Gefährdungslage für die betrachteten Komponenten geben. Die *Gefährdungskataloge* offenbaren mögliche Gefahrenpotenziale, welche anhand der M*aßnahmenkataloge* zu minimieren sind. Die Erfüllung des Compliance-Kriteriums hängt damit von der Umsetzung der in den IT-Grundschutz-Katalogen genannten Maßnahmen ab, so dass die Untersuchung den Fokus auf den Maßnahmenkatalog legt.

[179] Vgl. hier und im Folgenden Bundesamt für Sicherheit in der Informationstechnik (2009).

Da die einzelnen Maßnahmen recht konkret formuliert sind (teilweise zielen Maßnahmen auf bestimmte Soft- und Hardwareprodukte ab), ergibt sich die Erfüllung einzelner Compliance-Kriterien oftmals aus verschiedenen Maßnahmen. So wird zwar keine direkte Forderung nach einer *Serverspiegelung* gestellt, jedoch ergibt sich die Erfüllung dieses Kriteriums aus den Maßnahmen M 2.126 *Erstellung eines Datenbanksicherheitskonzeptes* und M 2.148 *Sichere Einrichtung von Novell Netware 4.x Netzen* sowie den allgemeinen Forderungen des Bausteins B 1.4 *Datensicherung*. Die Forderung nach *redundanten Servern* ergibt sich im Maßnahmenkatalog aus dem Abschnitt *M 6.43 Einsatz redundanter Webserver* in der konkreten Forderung nach redundanten Windows-Servern sowie dem Abschnitt M 6.53 *redundante Auslegung der Netzkomponenten*, welcher als solches die redundante Auslegung sämtlicher Netzkomponenten, also auch der im Netz befindlichen Server, fordert. Das Thema Risikomanagement spielt zwar an mehreren Stellen der IT-Grundschutz-Kataloge eine Rolle, jedoch bleibt dabei *die Forderung nach der Dokumentation des Risikomanagements* unberücksichtigt. So wird beispielsweise mit M 6.116 die Existenz eines Risikomanagements vorausgesetzt und auch die in M 3.45 dargestellte Schulung zur Informationssicherheit setzt mit Modul fünf auf einem Risikomanagement auf, jedoch bleibt die Schaffung und Dokumentation desselben ungeklärt. Ebenso existiert auch keine zentrale Forderung nach einer *IT-Richtlinie*, jedoch werden zahlreiche Richtlinien erwähnt (M 2.167, M 2.279) und auch als Beispiele zur Verfügung gestellt,[180] so dass dieses Kriterium als erfüllt gewertet werden kann. Die Forderung nach *Lizenzmanagement* ergibt sich zum einen aus der Richtung des Anforderungsmanagements (M 2.439), zum anderen wird das Lizenzmanagement aber auch im Sinne der Compliance mit der Maßnahme M 2.340 *Beachtung rechtlicher* Rahmenbedingungen thematisiert. Die ebenfalls in dieser Maßnahme erwartete *Verpflichtung der IT-Dienstleister auf Compliance* konnte jedoch nicht erfüllt werden und auch die Maßnahme M 2.253 macht zwar *konkrete* Vorgaben für die *Vertragsgestaltung* mit IT-Dienstleistern, berührt dabei aber nicht das Thema Compliance.

IT-Compliance		**Framework**
Bereich	**Kriterium**	**IT-Grundschutz**
Sicherheits- und Notfallkonzept	automatisches Backup	M 6.33, M 6.34
	Serverspiegelung	M 2.148, M 2.126, B 1.4*
	Masterplan für Systemabsturz und Recovery Maßnahmen	M 6.8x
	Redundante Server	M 6.43, M 6.53 *
	USV	M 1.28
Dokumentationspflichten	Risikomanagement	k. A. *
	Verfahrensverzeichnis nach BDSG	M 7.8
	ECM/DMS	M 2.259

[180] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2010).

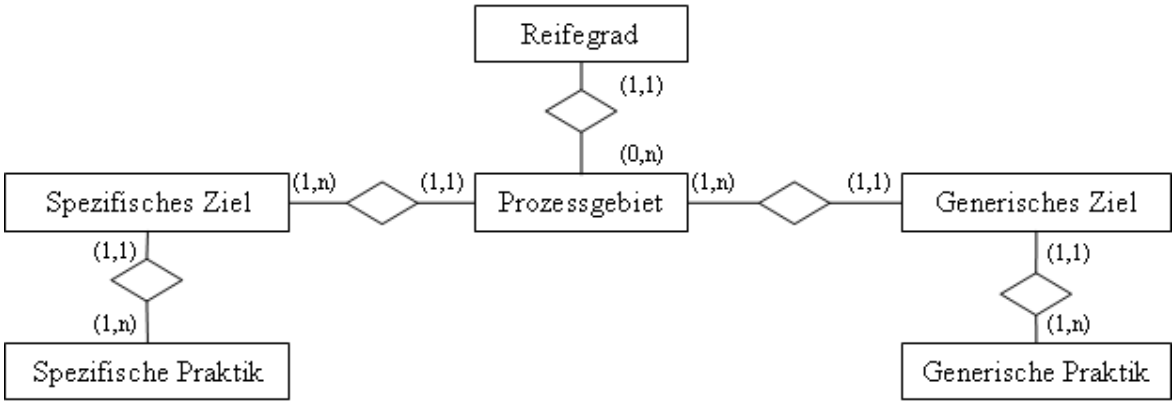
IT-Compliance		Framework
Bereich	**Kriterium**	**IT-Grundschutz**
E-Mail & Internet	IT-Richtlinie	M 2.167, M 2.279*
	E-Mail Policy	M 2.118
	Rechteverwaltung	M 2.8
	Archivierung der Mails	M 6.90
	E-Mail-Verwaltung	k. A.
Archivierung	Archivierungskonzept inkl. Aufbewahrungsfristen	M 2.243
	Revisionssicherheit des Archivierungssystems	M 4.169
	Kopplung der Archivierung an ECM / DMS	
Zertifizierung	Erreichbares Zertifikat	ISO 27001
IT-Security	effektive Spam-Abwehr, Virenfilter	M 2.214
	Lizenzmanagement	M 2.340, M 2.439*
IT-Dienstleister	Verpflichtung auf Compliance	k. A.*
	Vertragliche Regelung	M 2.253*
	personalisierte SLA	M 2.253*

Tab. 4.7: IT-Compliance im IT-Grundschutz Katalog

4.1.4.5 Maturity Assessment: CMMI

Unter dem Begriff Capability Maturity Model Integration (CMMI) werden *mehrere Referenzmodelle* zusammengefasst, welche durch das Software Engineering Institute der Carnegie Mellon Universität herausgegeben werden. Alle Referenzmodelle bieten dabei Praktiken und Methoden, welche Organisationen bei der Entwicklung und Instandhaltung hochwertiger Produkte und Dienstleistungen unterstützen sollen.[181] Dabei berühren sie unter anderem Arbeitsabläufe eines oder mehrerer Fachgebiete und beschreiben einen evolutionären Verbesserungsweg von unreifen Ad-hoc-Arbeitsabläufen (Reifegrad 1: Initial) hin zu systematischen Arbeitsabläufen (Reifegrad 5: Optimierend) mit verbesserter Qualität und Wirksamkeit.[182] Damit die angestrebten Verbesserungsbemühungen möglichst *unterschiedliche Gruppen* einer Organisation berücksichtigen und *unternehmensweite* Prozessverbesserung erreicht wird, definiert ein CMMI-Modell Ziele und Praktiken, welche als solche recht abstrakte Anforderungen darstellen.[183] Sowohl Ziele als auch Praktiken können dabei in *generischer* und *spezifischer* Form vorkommen, beziehen sich jedoch stets auf *Prozessgebiete*, die ihrerseits Anforderungen in einem Themenbereich bündeln.[184] Die Prozessgebiete werden im CMMI zu Reifegraden zusammengefasst,[185] so dass der Reifegrad einer Organisation von der Erfüllung der (generischen und spezifischen) Ziele von bestimmten Prozessgebieten abhängt. Die Abbildung 4.4 beschreibt die Zusammenhänge der genannten Elemente und damit die interne Struktur als Metamodell.

[181] Vgl. Software Engineering Institute (2006), S. 3.
[182] Vgl. Software Engineering Institute (2006), S. 6.
[183] Vgl. Kneuper (2003), S. 29.
[184] Vgl. Heilmann & Kneuper (2003), S. 64.
[185] Vgl. Kneuper (2003), S. 13.



Quelle: Kneuper (2003), S. 18.

Abb. 4.4: CMMI-Metamodell der stufenförmigen Darstellung für ein Anwendungsgebiet

In den Jahren 2006 und 2009 wurden durch das SEI ausgewählte CMMI-Komponenten zu so genannten *Konstellationen* zusammengefasst und veröffentlicht. Diese Konstellationen haben einen fachlichen Fokus,[186] wobei gegenwärtig drei CMMI-Modelle durch das SEI betreut und weiterentwickelt werden. *CMMI for Development* (CMMI-DEV)[187] soll dabei die Verbesserung von Organisationen unterstützen, welche selbst Software und Systeme entwickeln, wohingegen *CMMI for Acquisition* (CMMI-ACQ)[188] Organisationen unterstützen soll, welche Software und Systeme einkaufen, diese aber nicht selbst entwickeln. *CMMI for Services* (CMMI-SVC)[189] nimmt vom IT-Bezug Abstand und legt den Fokus auf die Entwicklung von ausgereiften Dienstleistungen.[190] Da die *Prozessgebiete* oftmals in allen drei Modellen Verwendung finden und auch die Anforderungen einem Themenbereich zugeordnet sind, wurden sie als Grundlage der Untersuchung gewählt. Die Zuordnung des Prozessgebiets zum unten verwendeten Prozessgebietskürzel und die Zuordnung des Prozessgebiets zur konkreten Konstellation kann dabei dem Anhang D entnommen werden.

Das Thema *Backup* wird in CMMI in allen drei Konstellationen aufgegriffen. Spielt es beim CMMI-DEV und CMMI-ACQ vornehmlich im Bereich des Konfigurationsbackups eine Rolle, so werden für Servicebetriebe, welche mit Daten arbeiten, im CMMI-SVC konkrete Backup-Maßnahmen aller Daten gefordert. Im gleichen Prozessgebiet des SCON wird auch ein Plan gefordert, welcher im Falle einer Betriebsstörung anzuwenden ist, so dass hier der *Masterplan für Systemabsturz* als gefordert angesehen werden kann. Das

[186] Vgl. Software Engineering Institute (2006), S. ii.
[187] Vgl. hier und im Folgenden Software Engineering Institute (2006).
[188] Vgl. hier und im Folgenden Software Engineering Institute (2007).
[189] Vgl. hier und im Folgenden Software Engineering Institute (2009).
[190] Vgl. Software Engineering Institute (2009), S. 3.

Thema Stromversorgung wird zwar im Rahmen des CAM behandelt, jedoch liegt hier der Fokus auf der *Kapazitätsplanung* und nicht auf der *Notfallversorgung bzw. USV*, welche im Rahmen der Compliance gefordert werden, so dass dieses Kriterium als nicht erfüllt bewertet wurde. Das Thema *Risikomanagement* wird in allen Konstellationen im Prozessgebiet RSKM behandelt, wobei dessen Dokumentation mit dem Verweis auf einen Plan zum Risikomanagement sichergestellt ist. Die konkrete Forderung nach einer *IT- und einer E-Mail Richtlinie* ließe sich zwar mit der Forderung nach Richtlinien aus dem Prozessgebiet DAR erfüllen, jedoch zielen die dort geforderten Richtlinien auf die formalen Bewertungsprozesse ab und nicht auf die Sensibilisierung der Benutzer hinsichtlich IT-relevanter Sicherheitsbelange. Diese Verhaltensregelung ließe sich mit den im Prozessgebiet OPD geschilderten Prozess-Assets und Standards erreichen, so dass diese Forderung als erfüllt angesehen werden kann. Die Rechteverwaltung ist sowohl beim CMMI-DEV wie auch beim CMMI-SVC im Prozessgebiet CM geregelt. Während das Prozessgebiet im Sinne der CMMI-DEV Rechte und Pflichten hinsichtlich des Konfigurationsmanagements anspricht, zielt die im CMMI-SVC erwähnte Benutzerverwaltung auf die *Zugriffsrechte* aller Endbenutzer ab. *Lizenzmanagement* wird grundsätzlich in allen drei Konstellationen in einem anderen Kontext behandelt. Während CMMI-ACQ dem Thema Lizenzmanagement quasi ein ganzes Kapitel widmet und CMMI-SVC die Verwaltung der Lizenzen unter den Vereinbarungen mit den Anbietern thematisiert, sieht auch das CMMI-DEV den Aspekt Lizenzmanagement im Prozessgebiet PI vor. Hier ist jedoch die Verwaltung aus Anbietersicht gemeint, so dass das Kriterium als nicht erfüllt gewertet wurde. Das Thema *Archivierung* bleibt unberührt, so dass es in keinem der CMMI-Konstellationen als erfüllt gewertet werden kann. Die in den Prozessgebieten AM und SAM geforderten formellen Vereinbarungen für Lieferanten und die hier erwähnte Praktik des Dokumentierens erfüllen zwar das Kriterium der vertraglichen Regelung, jedoch bleiben die Anforderungen der Prozessgebiete dabei so unspezifisch, dass *personalisierte SLA* als unberücksichtigt gelten.

IT-Compliance		**Framework**		
Bereich	**Kriterium**	**CMMI-DEV**	**CMMI-ACQ**	**CMMI-SVC**
Sicherheits- und Notfallkonzept	automatisches Backup *	CM (S. 120) PI (S. 306)	CM (S. 171)	SCON (S. 407)
	Serverspiegelung	k. A.	k. A.	k. A.
	Masterplan für Systemabsturz und Recovery Maßnahmen	OT (S. 278)	OT (S. 259)	SCON (S. 408)*
	Redundante Server	k. A.	k. A.	STSM (S. 480)
	USV	k. A.	k. A.	k. A. *
Dokumentationspflichten	Risikomanagement *	RSKM (S. 421)	RSKM (S. 362)	RSKM (S. 374)
	Verfahrensverzeichnis nach BDSG	k. A.	k. A.	k. A.
	ECM /DMS	k. A.	k. A.	k. A.

IT-Compliance		Framework		
Bereich	**Kriterium**	**CMMI-DEV**	**CMMI-ACQ**	**CMMI-SVC**
E-Mail & Internet	IT-Richtlinie	OPD (S. 229) *	OPD (S. 228) *	OPD (S. 265) *
	E-Mail Policy	OPD (S. 229) *	OPD (S. 228) *	OPD (S. 265) *
	Rechteverwaltung	CM (S. 138)*	k. A.	CM (S. 177)*
	Archivierung der Mails	k. A.	k. A.	k. A.
	E-Mail-Verwaltung	k. A.	k. A.	k. A.
Archivierung *	Archivierungskonzept inkl. Aufbewahrungsfristen	k. A.	k. A.	k. A.
	Revisionssicherheit des Archivierungssystems	k. A.	k. A.	k. A.
	Kopplung der Archivierung an ECM / DMS	k. A.	k. A.	k. A.
Zertifizierung	Erreichbares Zertifikat	Appraisal nach CMMI		
IT-Security	effektive Spam-Abwehr, Virenfilter			IRP (S. 212)
	Lizenzmanagement	k. A.*	SSAD (S. 371)*	SAM (S. 393)*
IT-Dienstleister	Verpflichtung auf Compliance	k. A.	k. A.	SAM (S. 394)
	Vertragliche Regelung	SAM (S. 444)*	AM (S.86)*	SAM (S. 388)*
	personalisierte SLA	k. A. *	k. A. *	k. A. *

Tab. 4.8: IT-Compliance in den CMMI-Referenzmodellen

4.1.4.6 Project Management: PMBoK Guide

Vom Project Management Institute (PMI) herausgegeben, hat sich das Project Management Body of Knowledge (PMBoK)[191] heute als weit verbreiteter Standard für das Projektmanagement etabliert. Durch die Mitglieder des PMI wird der Standard laufend weiterentwickelt, so dass gerade durch die Teilnahme vieler Praktiker ein aktuelles Framework vorliegt, welches auch einen hohen Praxisbezug hat.[192] Sein Aufbau gliedert sich in drei Hauptabschnitte, wobei im ersten Abschnitt (*PM-Framework)* eine allgemeine Einführung gegeben wird. Der zweite Abschnitt spezifiziert alle *Prozessmanagement-Prozesse,* welche zur Verwaltung eines Projekts benötigt werden. Im dritten Abschnitt werden die Projektmanagement-Prozesse in neun *Wissensgebiete* eingeordnet (z. B. Zeitmanagement oder Risikomanagement), wobei für jeden Prozess Inputs, Outputs, Methoden und Werkzeuge beschrieben werden.

Ziel des PMBoK ist es, Wissen und Methoden für das Projektmanagement zur Verfügung zu stellen und dabei so allgemein zu bleiben, dass Wissen und Werkzeuge für die meisten Projekte nutzbringend sind.[193] Entsprechend bleiben *informationstechnische Details* wie Virenschutz und IT-Richtlinien unberührt. Jene als erfüllt bewerteten Kriterien sind zwar auch nur vor dem Hintergrund des Projektmanagements durch das PMBoK gefordert, je-

[191] Vgl. hier und im Folgenden Project Management Institute (2004).
[192] Vgl. Seibold (2006), S. 196.
[193] Vgl. Project Management Institute (2004), S. 3.

doch wurden sie im Sinne einer *ganzheitlichen* IT-Compliance als erfüllt bewertet. So wird zwar mit Kapitel 11.6.1 nur der Risiko-Management-Plan für Projekte gefordert, jedoch ist dieser Plan als Bestandteil der Dokumentationspflichten zu erbringen, so dass er als erfüllt angesehen wurde. Kapitel 12 bleibt hingegen allgemeiner und regelt dabei sämtliche Leistungen, welche durch Dritte für das Projekt erbracht werden können.[194] Die Forderung nach *vertraglicher Regelung* wird als erfüllt bewertet, da der IT-Dienstleister als Dritter angesehen werden kann.

IT-Compliance		**Framework**
Bereich	**Kriterium**	**PMBoK Guide**
Sicherheits- und Notfallkonzept	automatisches Backup	k. A.
	Serverspiegelung	k. A.
	Masterplan für Systemabsturz und Recovery Maßnahmen	k. A.
	Redundante Server	k. A.
	USV	k. A.
Dokumentationspflichten	Risikomanagement	Kap. 11.6.1*
	Verfahrensverzeichnis nach BDSG	k. A.
	ECM /DMS	k. A.
E-Mail & Internet	IT-Richtlinie	k. A. *
	E-Mail Policy	k. A. *
	Rechteverwaltung	k. A. *
	Archivierung der Mails	k. A. *
	E-Mail-Verwaltung	k. A. *
Archivierung	Archivierungskonzept inkl. Aufbewahrungsfristen	k. A.
	Revisionssicherheit des Archivierungssystems	k. A.
	Kopplung der Archivierung an ECM / DMS	k. A.
Zertifizierung	Erreichbares Zertifikat	k. A.
IT-Security	effektive Spam-Abwehr, Virenfilter	k. A. *
	Lizenzmanagement	k. A.
IT-Dienstleister	Verpflichtung auf Compliance	k. A.
	Vertragliche Regelung	12.2.3 S. 282, 12.5 S. 290*
	personalisierte SLA	k. A.

Tab. 4.9: IT-Compliance im PMBoK Guide

4.2 Zusammenfassung

Die Ergebnisse aller Untersuchungen zusammengefasst und nebeneinander aufbereitet, ergeben den in der Tabelle 4.11 dargestellten Vergleich. Dabei werden die Ergebnisse der drei Konstellationen von CMMI zusammengefasst.

[194] Vgl. Project Management Institute (2004), S. 269.

IT-Compliance		Framework					
Bereich	**Kriterium**	COSO	Cobit	ITIL	IT-Grund.	CMMI	PMBoK
Sicherheits- und Notfallkonzept	automatisches Backup	ok	ok	ok	ok	ok	
	Serverspiegelung		ok	ok	ok		
	Masterplan für Systemabsturz und Recovery Maßnahmen	ok	ok	ok	ok	ok	
	Redundante Server		ok	ok	ok	ok	
	USV		ok	ok	ok		
Dokumentations-pflichten	Risikomanagement	ok	ok	ok		ok	ok
	Verfahrensverzeichnis nach BDSG		ok	ok	ok		
	ECM /DMS				ok		
E-Mail & Internet	IT-Richtlinie	ok	ok	ok	ok	ok	
	E-Mail Policy			ok	ok	ok	
	Rechteverwaltung		ok	ok	ok	ok	
	Archivierung der Mails				ok		
	E-Mail-Verwaltung						
Archivierung	Archivierungskonzept inkl. Aufbewahrungsfristen		ok	ok	ok		
	Revisionssicherheit des Archivierungssystems				ok		
	Kopplung der Archivierung an ECM / DMS						
Zertifizierung	Erreichbares Zertifikat			ok	ok	ok	
IT-Security	effektive Spam-Abwehr, Virenfilter	ok	ok	ok	ok	ok	
	Lizenzmanagement		ok	ok	ok		
IT-Dienstleister	Verpflichtung auf Compliance					ok	
	Vertragliche Regelung		ok	ok	ok	ok	ok
	personalisierte SLA		ok	ok	ok		

Tab. 4.10: IT-Compliance der IT-Governance-Frameworks im Vergleich

Sieht man von den Unterschieden beim Vergleich der einzelnen Frameworks einmal ab, so offenbart die zeilenweise Betrachtung bemerkenswerte Ähnlichkeiten bei der Nicht-Berücksichtigung einzelner Compliance-Kriterien. Hier scheinen gerade im Bereich der organisatorischen Einbindung von DMS-Systemen Lücken zu bestehen, welche Compliance-Verstöße bei der Revisionssicherheit, aber auch bei den GoB nach sich ziehen können. Ebenso scheint das Thema der E-Mail-Verwaltung und der ordnungsgemäßen Archivierung der Mails in den Frameworks noch nicht ausreichend abgebildet zu sein. Erfolgen hier keine individuellen, unternehmensspezifischen Vorgaben entsteht die Möglichkeit, dass gegen das HGB verstoßen wird und Handelsgeschäfte damit juristisch angreifbar werden. Ebenso ist es auch erforderlich, IT-Dienstleister mit organisationseigenen Mitteln auf Compliance zu verpflichten, ist dieser Aspekt doch nur in einem der Governance-Frameworks berücksichtigt.

Abschließend sei ausdrücklich davor gewarnt, die generalisierten Zusammenhangsaussagen zwischen den IT-Governance-Frameworks und den Compliance-Anforderungen auf detaillierte Zusammenhänge zu übertragen: Nicht nur die Tatsache, dass die Verwendung

des Frameworks von der konkreten Umsetzung abhängt, sondern auch der Umstand, dass die Erfüllung rechtlicher Vorgaben oftmals erst ex post beurteilt werden kann, muss Berücksichtigung finden. Aussagen zur IT-Compliance bleiben damit letztendlich von der implementierenden Organisation abhängig.

5 Modellierung von rechtlichen Anforderungen in Informationsmodellen

Dominik Heddier

5.1 Motivation

Rechtlichen Anforderungen gerecht zu werden, ist ein unabdingbarer Faktor für jedes Unternehmen. Diese Anforderungen erstrecken sich über die Erfüllung spezifischer Normen bis hin zur korrekten Implementierung von gesetzlich vorgeschriebenen internen Kontrollen.[195] In der Praxis suchen konkurrierende Unternehmen teilweise gezielt nach Versäumnissen oder Gesetzesübertretungen der jeweiligen Konkurrenten, um die eigene Stellung zu stärken und das betroffene Unternehmen zu schwächen. Ein erfolgreiches Geschäftsprozessmanagement ist ein bedeutender Faktor und ein wichtiges Werkzeug für jedes Unternehmen, um die eigenen Ziele effizient und effektiv zu erreichen.[196] Deshalb ist es auch eine Notwendigkeit, innerhalb dieser Geschäftsprozesse die Einhaltung rechtlicher und vertraglicher Anforderungen (im Folgenden auch Compliance genannt) zu gewährleisten.[197] Regulierer legen den Unternehmen auf nationaler und internationaler Ebene eine wachsende Anzahl an Regulationen auf. MiFiD, KontraG und Basel II sind hier prominente Beispiele.[198] Eine sachgemäße Visualisierung und Überprüfung dieser Regulationen kann Kosten einsparen und Rechtssicherheit schaffen. Aus diesem Grund haben sich bereits eine Vielzahl wissenschaftlicher Veröffentlichungen mit der Problematik beschäftigt und eine Reihe von Ansätzen vorgestellt, welche bei der Einhaltung von Vorschriften unterstützen können. In diesem Kapitel wird der Fokus auf diejenigen Ansätze gelegt, die hierzu Methoden der Informationssystem-Modellierung verwenden.

5.2 Umfang der Literaturrecherche

Als Literaturgrundlage wurden überwiegend sowohl Zeitschriftenartikel als auch Konferenzbände verwendet, welche über Online-Literaturdatenbanken gesucht wurden. Es wurden hauptsächlich folgende Datenbanken mit Hilfe eines Schlagwortkatalogs durchsucht:

- ACM Digital Library (Association for Computing Machinery)[199]
- EBSCO Host[200]
- Google Scholar[201]

[195] Vgl. El Kharbili et al. (2008), S. 107.
[196] Vgl. Weske (2007), S. 4.
[197] Vgl. et al. (2008), S. 107.
[198] Vgl. IDS Scheer AG (2008), S. 4 f.
[199] http://portal.acm.org/dl.cfm.
[200] http://search.ebscohost.com.
[201] http://scholar.google.com.

- WISO Datenbanken[202]
- SpringerLink Online-Bibliothek[203]

Die folgenden Schlagwörter wurden alleine und in verschiedenen Kombinationen in den Suchfeldern der Datenbanken eingegeben:

- Compliance
- Model
- Modelchecking
- Semantic
- Rechtliche Anforderungen
- Restriktion
- Restriction
- Vertrag
- Contract
- Process Model
- Modell
- Business Process Model
- Geschäftsprozess
- Datenschutz
- Regulation
- Method
- Legal
- Law
- Prozessmodell
- Compliance-Checking
- Compliance-Engineering
- Business Policies
- Rechtliche Modellierung
- Legal Requirements

Zusätzlich zum Schlagwortkatalog wurden einige Ansätze über eine Breiten- und Tiefensuche anhand der Abschnitte zum „Related Work“ in bereits identifizierten Veröffentlichungen gefunden. Des Weiteren wurde in den oben genannten Datenbanken nach weiteren Veröffentlichungen von bereits gefundenen Autoren gesucht.

[202] http://www.wiso-net.de.
[203] http://www.springerlink.com.

Da eine vollständige Darstellung aller Ansätze im Rahmen dieses Beitrages nicht möglich ist, wird im Folgenden eine möglichst repräsentative Auswahl unterschiedlicher Ansätze vorgestellt. Eine vollständige Liste aller identifizierten Ansätze findet sich in Anhang B.

5.3 Rechtliche Anforderungen in Modellen

5.3.1 Forschungsrichtungen der Verbindung von rechtlichen Anforderungen und Modellen

Eine sehr prominente Gruppe von Methoden zur Kombination von rechtlichen Anforderungen und Modellen ist die der so genannten Compliance Checker. Diese Verfahren durchlaufen meist automatisch vorhandene Prozessmodelle und überprüfen diese auf Einhaltung oder Verstoß von vordefinierten Regeln. In vielen Fällen müssen die Prozessmodelle dabei in einer besonderen Form und Sprache vorliegen oder speziell bearbeitet werden, damit die Model-Checker-Algorithmen fehlerfrei arbeiten können. Um gesetzliche Vorgaben überhaupt maschinell verarbeiten zu können, werden Regulationen bei vielen Ansätzen in logischen Sprachen formalisiert. Eine rechtliche Anforderung wird somit aus dem Gesetzes- oder Vertragstext in eine formale Repräsentation überführt, deren Einhaltung ein Algorithmus berechnen kann.

Eine etwas simplere Form der Integration rechtlicher Anforderungen in Prozessmodelle ist die Annotation. Eine Reihe von Ansätzen geht den Weg, verschiedene Modellierungssprachen so zu verwenden oder zu erweitern, dass staatliche Regulationen oder vertragliche Bindungen in Form von Kommentarkästchen im Prozessmodell visualisiert werden. Erweiterungen solcher Herangehensweisen verlinken diese annotierten rechtlichen Informationen mit hinterlegten Detailbeschreibungen der Anforderung oder dem entsprechenden Auszug des Gesetzestextes selbst.

Eine andere Herangehensweise in der Literatur beschäftigt sich damit, die vertragliche oder gesetzliche Anforderung an sich zu modellieren, um diese im Anschluss besser zu verstehen oder die eigenen Prozesse in dieses Modell zu integrieren. Die dabei entstehenden Modelle können unter anderem dafür verwendet werden, Verantwortlichkeiten in einer vertraglichen Beziehung zweier Organisationen genauer zu spezifizieren und somit Rechtsstreitigkeiten vorzubeugen.

Es werden auch Versuche unternommen, Gesetzestexte mit sogenannten Markup-Befehlen zu versehen, damit eine Art Parser die nun mit Semantikinformationen ausgestatteten Textpassagen einlesen und teilautomatisiert in Prozessmodelle überführen kann.

5.3.2 Kriterien zur Einordnung der untersuchten Ansätze

Logische Sprache: Dieses Kriterium beschreibt, ob eine logische Sprache für die Modellierung der rechtlichen Anforderungen benutzt wird. Als logische Sprache sind Sprachen wie die „Object Constraint Language“ (OCL)[204] oder auch die von Governatori vorgestellte Formal Contract Language (FCL) (oder auch RuleML) zu verstehen.[205] Die logischen Sprachen sind unter anderem gut dafür geeignet, vorhandene Modellierungssprachen so zu ergänzen, dass Restriktionen exakter als durch simple Annotationen ausgedrückt werden können.[206]

FCC DTCC: Das erste Akronym steht für „Forward Compliance Checking“, während das zweite Akronym für Design-Time Compliance Checking steht. Dies ist eine Untergliederung, die aussagt, an welcher Stelle und zu welcher Zeit die Compliance überprüfende Maßnahme ausgeführt wird. Die Kategorie FCC sagt aus, dass es sich um einen proaktiven Ansatz handelt im Gegensatz zum „Backward Compliance Checking“ (BCC), bei dem es sich um eine reaktive Herangehensweise handelt. DTCC fokussiert FCC auf die Ansätze, die schon zur „Design Time“, also in der Modellierungsphase, aktiv werden. Dadurch soll garantiert werden, dass Prozesse in jedem Fall den rechtlichen Anforderungen genügen. Es werden sogenannte Model-Checker eingesetzt, die Prozessmodelle mit Hilfe von Techniken wie „Compliance-Patterns“, zusätzlicher „Semantische[r] Schichten“[207] oder Compliance-Templates auf Rechtssicherheit überprüfen.

FCC RTCC: Wie das DTCC ist das „Real-Time Compliance Checking“ eine Form des FCC. Die Unterscheidung zum DTCC ist notwendig, da beim RTCC auch Informationen benötigt werden, die nur zur Laufzeit verfügbar sind. So können Geschäftsanweisungen oder Anforderungen wie die Einhaltung von Service Level Absprachen erst mit Laufzeitinformationen bewertet und entschieden werden.[208]

BCC: Während FCC eher einen präventiven Charakter hat, konzentriert sich „Backward Compliance Checking“ auf ein reaktives Vorgehen. Dafür werden die „Spuren“, die ein Geschäftsprozess hinterlässt, verwendet. Diese „Spuren“ treten meist in Form von „Ausführungs-Protokollen“ auf. Da diese Protokolle in der Regel mit Data-Mining-Techniken oder Prozessanalysemethoden ausgewertet werden, lässt sich BCC auch gut dem Bereich des Controllings und des Geschäftsprozess-Reengineering zuordnen.[209]

[204] Vgl. Richters & Gogolla (1998), S. 449.
[205] Vgl. Governatori (2005), S. 20 ff.
[206] Vgl. Richters & Gogolla (1998), S. 449.
[207] Vgl. et al. (2008), S. 108 f.
[208] Vgl. El Kharbili, Stein, Markovic (2008), S. 8.
[209] Vgl. El Kharbili, Stein, Markovic (2008), S. 8.

Automatisierung: Dieses Kriterium gibt an, ob der vorgestellte Ansatz vollständig oder teilweise automatisiert wurde oder automatisierbar ist. In Zeiten steigender Prozesskomplexität und anwachsender Datenmengen spielt Automatisierung eine immer entscheidendere Rolle. Eine semantische Prozessmodellanalyse einer Prozesslandschaft eines größeren Unternehmens würde ohne eine zumindest teilweise automatisierte Analyse unverhältnismäßig lange dauern.

Toolunterstützung: Wenn es für den jeweiligen Ansatz ein Software-Tool gibt, welches die Ausführung des Ansatzes unterstützt, oder es eine für den Ansatz entwickelte Erweiterung für ein bestehendes Tool gibt, wird dieses Kriterium erfüllt.

Gegenstand Prozess: Dieses Kriterium wurde verwendet, um die Zielsetzung des jeweiligen Ansatzes genauer zu spezifizieren. Viele Methoden beschränken sich darauf, rechtliche Anforderungen so in bestehende Modelle zu integrieren, dass ein rechtssicheres Verhalten entweder garantiert oder unterstützt wird. Als eine alternative Form der Zielsetzung wird der Versuch verstanden, vertragliche oder rechtliche Anforderungen in Prozessmodelle zu überführen, um diese daraufhin besser zu verstehen oder differenzierter behandeln zu können. Das Kriterium „Gegenstand Prozess“ wird erfüllt, wenn die erstere Zielsetzung zutrifft.

Gegenstand Anforderung: Dieses Kriterium wird erfüllt, wenn die in der Kriterienbeschreibung „Gegenstand Prozess“ zuletzt genannte Zielsetzung zutrifft, also vertragliche oder rechtliche Anforderungen in Prozessmodelle überführt wurden, um diese daraufhin besser zu verstehen oder differenzierter behandeln zu können.

Sprachen: Um rechtliche Anforderungen erfolgreich in Modellen abbilden zu können, werden eine oder mehrere Modellierungssprachen verwendet. Dabei können vorhandene Sprachen verwendet oder erweitert, Elemente verschiedener Sprachen kombiniert oder auch neue Sprachen entwickelt werden. Um einen besseren Überblick über die im Folgenden vorgestellten Ansätze geben zu können, wird in der letzten Spalte der Kategorisierung angegeben, welche Sprache verwendet wurde.

5.3.3 Einordnung der untersuchten Ansätze

Ansatz von DE MOURA ARAUJO, SCHMITZ, ALENCAR und CORREA (1)

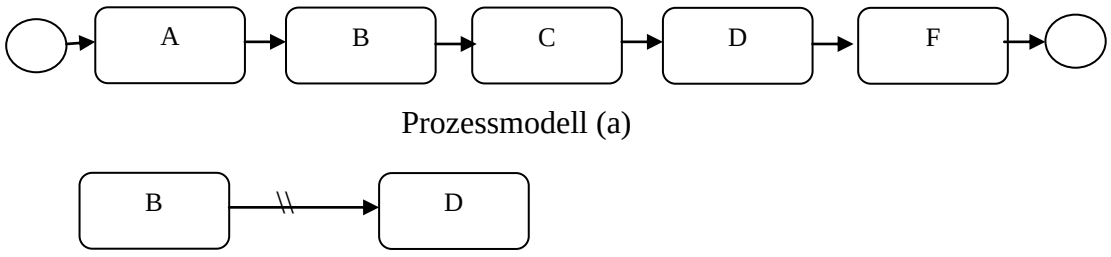
Ziel des RTCC-Ansatzes von DE MOURA ET AL. ist die Modellierung von Compliance-Regeln in einem Geschäftsprozess.[210] Nach der Identifikation der relevanten Anforderun-

[210] Vgl. De Moura Araujoet al. (2010), S. 146.

gen wird ein Klassendiagramm erstellt, an das die in OCL übersetzten Regeln annotiert werden. Anschließend wird das Prozessmodell erstellt, in dem die OCL-Restriktionen als Vor- und Nachbedingungen erscheinen. Danach werden solange Szenarien-Objekte erzeugt und simuliert, bis das gewünschte Konfidenzlevel an Prozess-Compliance erreicht wurde.[211] Wird ein Verstoß gegen die Compliance Regeln erkannt, bricht der Algorithmus ab und macht den Prozessanalysten auf den Missstand aufmerksam.[212] Der vorgeschlagene Algorithmus ist automatisiert und durch das eigens dafür entwickelte Tool „Process Validator" unterstützt. Die OCL-Ausdrücke werden mithilfe des Tools „USE" bewertet.[213]

Ansatz von AWAD, DECKER und WESKE (2)

AWAD, DECKER und WESKE entwickelten eine automatisierte Methode, Geschäftsprozessmodelle auf Compliance-Verstöße zu untersuchen. Für diese Zwecke verwenden sie die um eine Query-Funktion erweiterte Modellierungssprache *Business Process Modelling Notation* (BPMN-Q). Regeln, wie zum Beispiel rechtliche Anforderungen, werden in Form von Queries ausgedrückt. Mit Hilfe dieser Queries lassen sich in einem ersten Schritt die für die Compliance-Analyse relevanten Prozesse identifizieren.[214] Eine Query kann als Muster verstanden werden, nach dem der Prozess durchsucht wird. Das Prozessmodell und die Query werden zunächst in Form eines Graphen dargestellt (Vgl. Abb. 5.1). Ein Prozess wird als relevant eingestuft, wenn das Muster des Query-Graphen auf den Prozessgraphen passt.[215]



In Anlehnung: Awad, Decker, & Weske (2008), S. 329

Abb. 5.1: Querygraph

Um Regeln in Queries zu transformieren, werden alle in der Regel genannten Aktivitäten in die Query eingefügt. Die Query in Abb. 5.1 setzt die Regel um, dass die Aktivität B vor der Aktivität D ausgeführt werden muss. Wird keine Übereinstimmung gefunden, kann mit Sicherheit von einem Compliance-Verstoß ausgegangen werden. Wird das Muster jedoch

[211] Vgl. De Moura Araujoet al. (2010), S. 146.
[212] Vgl. De Moura Araujoet al. (2010), S. 149.
[213] Vgl. De Moura Araujoet al. (2010), S. 148.
[214] Vgl. Awad, Decker & Weske (2008), S. 327 f.
[215] Vgl. Awad, Decker & Weske (2008), S. 330.

erkannt, kann Non-Compliance jedoch noch nicht ausgeschlossen werden, da die Querys nicht alle Szenarien bewerten können, die durch semantische Operatoren wie Or/And-Operatoren hervorgerufen werden können.[216] Eine weitere Limitation dieses Vorgehens besteht in der Bestimmung der Richtung der Abhängigkeit. Es kann entweder gelten, dass einer Aktivität A unbedingt eine Aktivität B folgen muss oder dass vor B unbedingt A ausgeführt worden sein muss. Dieses Problem werden durch Erweiterung der BPMN-Q um die Konzepte *precedes* und *leads to* gelöst.[217]

Um das automatisierte Model-Checking durchzuführen, werden die Queries zunächst in die *Past Linear time Temporal Logic* (PLTL) überführt.[218] Gleichzeitig werden die zu überprüfenden Prozessmodelle auf die relevanten Teile reduziert und über Petri-Netze hin zu endlichen Automaten transformiert.[219]

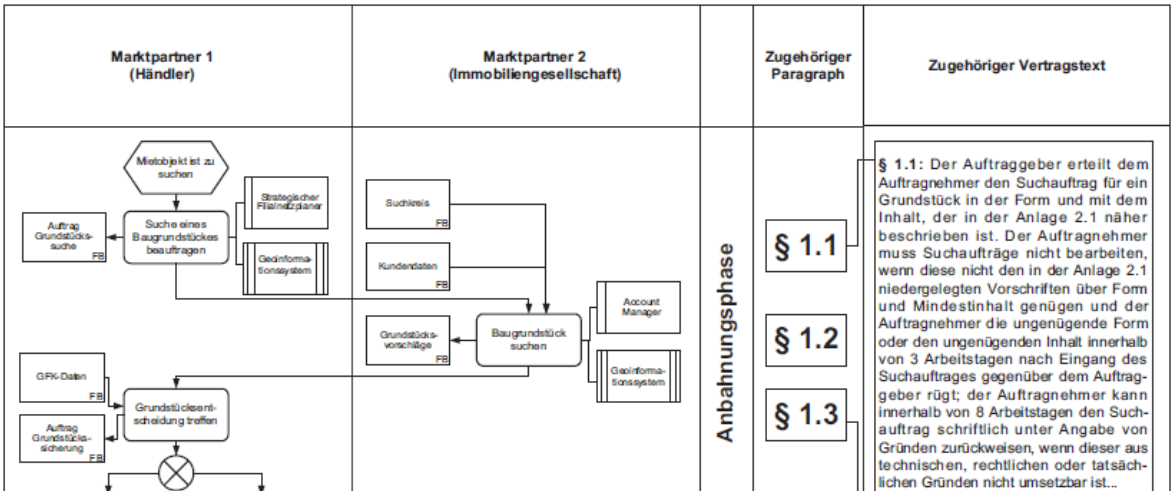
Der Compliance-Checking-Vorgang wird durch das BPMN-Tool Oryx, einen Petri-Netz-Generator, den Deadlockchecker LoLA, einen PLTL-Generator und den Model-Checker NuSMV unterstützt.[220] Da bei diesem Ansatz keine Informationen aus Protokollen oder der Laufzeitumgebung verwendet werden, handelt es sich um DTCC. Der Ansatz kann allerdings um die Konzepte *data awareness* und *anti-patterns* erweitert werden. Data awareness berücksichtigt zusätzlich den Status aktueller Daten in Queries[221], während anti-patterns automatisch erzeugte Queries sind, welche gezielt nach Compliance-Verstößen statt nach der Einhaltung dieser suchen.[222] Die Einbeziehung von Laufzeitdaten in den Analysevorgang lässt eine Einordnung in den Bereich der RTCC-Methoden zu.

Ansatz von BECKER, KLOSE und SCHNEIDER (3)

Um den Vorgang der Vertragsgestaltung übersichtlicher und kostengünstiger zu gestalten, empfehlen BECKER, KLOSE und SCHNEIDER, diesen Vorgang prozessmodellgestützt mit einer um Vertragsklauseln erweiterten Prozessmodellierungssprache durchzuführen. Durch diese Methode soll sowohl die Qualität der Verträge gesteigert als auch die Anzahl der Nachverhandlungen reduziert werden, denn durch die erweiterten Prozessmodelle werden die Verantwortlichkeiten der Vertragspartner besser geklärt.[223] Nachdem die Prozesse mo-

[216] Vgl. Awad, Decker & Weske (2008), S. 330.
[217] Vgl. Awad, Decker & Weske (2008), S. 331.
[218] Vgl. Awad, Decker & Weske (2008), S. 335 f.
[219] Vgl. Awad, Decker & Weske (2008), S. 333.
[220] Vgl. Awad, Decker & Weske (2008), S. 338.
[221] Vgl. Awad, Weidlich & Weske (2009), S. 510.
[222] Vgl. Awad & Weske (2009), S. 2 ff.
[223] Vgl. Becker, Klose & Schneider (2003), S. 12 f.

delliert wurden, ergänzen Juristen in Zusammenarbeit mit den Fachabteilungen die Modelle um die Vertragsinhalte, die nicht direkt daraus ersichtlich sind (vgl. Abb. 5.2).[224]



Quelle: Becker, Klose & Schneider (2003) S. 20.

Abb. 5.2: Beispiel Vertrags-Prozessmodell

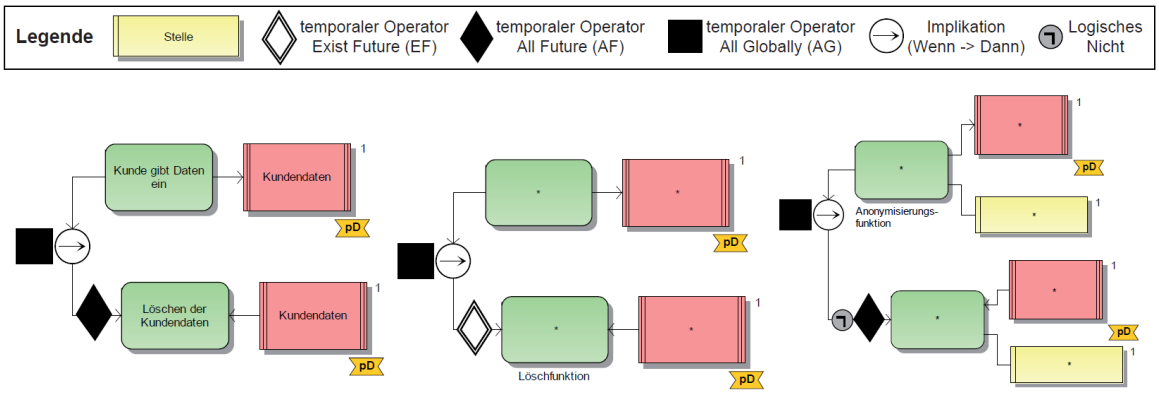
Diese Methode fällt sowohl in die Kategorien FCC-DTCC als auch BCC, da sie zum einen bei Nachverhandlungen als Referenz zur Verifizierung von Compliance-Verstößen herangezogen werden kann, zum anderen durch das Explizieren der Anforderungen ein rechtskonformes Verhalten bereits im Voraus unterstützen soll. Dabei wird das ARIS-Tool-Set empfohlen.[225] Gegenstand der Modellierung sind bei diesem Ansatz die Vertragsinhalte, welche nach Abschluss des Vertrages ähnlich wie rechtliche Anforderungen behandelt werden müssen.

Ansatz von FEJA, WITT, BROSCHE, SPECK und PRIETZ (4)

Die Methode von FEJA ET AL. dient der einfacheren Einhaltung der §§ 4, 14, 19, 20, 34 und 35 BDSG, indem sie die Integration von Datenschutzanforderungen auf Prozessebene ermöglicht. Dafür geeignete Modellierungsnotationen sind die Ereignisgesteuerte Prozesskette (EPK) und die Unified Modeling Language (UML). Unterstützt wird die Modellierung durch das Tool ARIS Business Architect.[226] Die Integration der Datenschutzaspekte erfolgt in Form von Annotationen an das Modell. Zusätzlich wird eine Sichtentrennung vorgeschlagen, um eine Trennung der einzelnen Modellierungsaspekte zu erreichen. Dadurch lassen sich beispielsweise die Datenschutzaspekte für Personen, welche diese Informationen nicht benötigen, ausblenden.[227] Um mit einem Modellprüfverfahren (Model-Checker) automatisch nach dem Nichteinhalten von Datenschutzbestimmungen suchen zu

[224] Vgl. Becker, Klose & Schneider (2003), S. 15.
[225] Vgl. Becker, Klose & Schneider (2003), S. 21.
[226] Vgl. Feja & Witt (2010), S. 156.
[227] Vgl. Feja & Witt (2010), S. 158.

können, werden mit Hilfe der grafischen Computational Tree Logic (G-CTL) Regeln bestimmt[228], welche später in die für den Computer lesbare Enterprise Privacy Authorization Language (EPAL) transformiert werden.[229] Der Regelsatz leitet sich aus dem Gesetzestext sowie einer Reihe an vordefinierten Schutzzielen ab.[230] In Abb. 5.3 wird dargestellt, wie Datenschutz-Regeln in der G-CTL-Notation beschrieben werden. Durch die Operatoren EF, AF und AG wird der Geltungsbereich der Regeln angegeben bzw. eingeschränkt. Regel (a) der Abb. 5.3 beschreibt demnach, dass bei Eingabe personenbezogener Kundendaten diese in jedem möglichen Prozessausgang auch wieder gelöscht werden müssen. Zur Kategorisierung der personenbezogenen Daten wird eine Verbindung des Prozessmodells mit einer Datenbank empfohlen. In der Datenbank werden die Daten in Cluster wie Identitätsdaten, physiologische Daten und Persönlichkeitsdaten aufgeteilt. Dieses zusätzliche Datenmodell erleichtert die Wiederverwendbarkeit und die Einordnung zu den personenbezogenen Daten.[231]



(a) szenariospezifische Löschregel (b) allgemeingültige Löschregel (c) domänenspezifische Anonymisierungsregel

Quelle: Feja et al. (2010), S. 160.

Abb. 5.3: Modellierung von Regeln mit G-CTL

Der Ansatz verwendet keine Laufzeitinformationen oder Protokolle, sondern beschränkt sich darauf, Modelle während des Modellierungsvorganges auf Verstöße gegen die Datenschutzbestimmungen zu untersuchen. Aufgrund dieser Tatsache gehört er zur Kategorie der FCC DTCC.

Ansatz von BREAUX (5)

BREAUX schlägt eine Methode vor, die mit Hilfe eines Parsers Gesetzestexte teilautomatisiert in Prozessmodelle überträgt, um somit die Arbeit von Compliance-Auditoren zu ver-

[228] Vgl. Feja & Witt (2010), S. 160.
[229] Vgl. Feja & Witt (2010), S. 157.
[230] Vgl. Rost & Pfitzmann (2009), S. 353 ff.
[231] Vgl. Feja & Witt (2010), S. 162.

einfachen. Dazu verwendet er die „Frame-based Requirements Analysis Method“ (FBRAM). Diese Methode baut auf einer Ontologie auf (upper ontology), welche Ausdrücke aus Gesetzes- und Anforderungstexten in Klassen kategorisiert. Diese Klassen sollen die wesentlichen Aspekte repräsentieren, welche in einem Gesetzes- und Anforderungstext vorkommen können. Der Autor identifiziert die folgenden Klassen: Erlaubnis (Permission), Obligation, Unterlassung (Refrainment) und Verbot (Exclusion).[232]

Die Kernidee der Methode ist es, in einem semantischen Prozess aus den Regulationen des Gesetzgebers formale, rechtliche Anforderungen zu gewinnen und gleichzeitig die Zurückverfolgbarkeit zu gewährleisten. Für diese Zwecke wird der entsprechende Gesetzestext mit Hilfe einer kontextfreien Markup-Sprache annotiert. Zunächst werden ganze Blöcke mit entsprechenden Bezeichnern versehen, um sie in eine der vier oben erwähnten Klassen zu kategorisieren. Anschließend werden die einzelnen Blöcke ebenfalls mit Markup-Bezeichnern versehen, sodass ersichtlich wird, welche Ausdrücke Subjekt, Objekt, Prädikat, Modalität, Bedingung oder Ausnahme sind. Mit einem Parser-Tool lassen sich nun die Textausschnitte in Templates überführen.[233]

Damit die gewonnenen rechtlichen Anforderungen verwendet werden können, müssen diese von einem Prozessanalysten in die bestehenden Prozesse integriert werden. Dazu wird in vier Schritten vorgegangen:

- Identifizierung des Akteurs innerhalb des Templates und Erzeugung einer entsprechenden Swimlane[234] (falls noch nicht vorhanden).
- Erzeugung eines Aktivitätssymbols, wobei der Text des Symbols sich aus dem identifizierten Prädikat und dem Objekt zusammensetzt.
- Erzeugung eingehender Konnektoren oder Aktivitäten, welche Bedingungen oder Ausnahmen darstellen.
- Annotation des Anforderungs-Templates in Form eines Kommentars an diese abgeleitete Aktivität.[235]

Mit dieser Methode lassen sich Aktivitäten innerhalb von Prozessmodellen direkt aus dem Gesetzestext ableiten. Jedoch ist dieses Vorgehen sehr fehleranfällig und bedarf der Hilfe

[232] Vgl. Breaux & Powers (2009), S. 273.
[233] Vgl. Breaux & Powers (2009), S. 274.
[234] Swimlanes sind ein Konstrukt in der Prozessmodellierung. Ein Prozessmodell wird hierbei in „Bahnen“ aufgeteilt. Jede Bahn steht für eine Person oder Personengruppe. Dadurch kann die Verteilung von Verantwortlichkeiten übersichtlicher gestaltet werden.
[235] Vgl. Breaux & Powers (2009), S. 275.

eines Prozessanalysten, um Regeln abzuleiten, Mehrdeutigkeiten zu spezifizieren und Lücken im Gesetzestext abzufangen.[236]

Diese Methode verwendet keine Laufzeit- oder Vergangenheitsdaten, sondern konzentriert sich auf ex-ante-Compliance Modellierung. Daher gehört sie zur Kategorie DTCC. Es werden keine logischen Sprachen zum Ausdrücken der Regulationen verwendet und es findet keine wesentliche Automatisierung statt.

Ansatz von GIBLIN, LIU, MÜLLER, PFITZMANN und ZHOU (6)

Eine Methode, rechtliche und geschäftliche Anforderungen in ihrem gesamten Lebenszyklus zu erfassen und zu modellieren, stellen GIBLIN ET AL. vor. Mit Hilfe der REALM (Regulations Expressed As Logical Models)-Methode wird ein systematischer Compliance Management Ansatz vorgestellt, welcher der ansteigenden Komplexität und Breite von regulatorischen Anforderungen gewachsen sein soll. Für diese Zwecke wird sich eines Metamodells bedient, das dazu dient, eine große Menge an rechtlichen Anforderungen mit einer einheitlichen, geteilten Sprache und Semantik zu formalisieren. Zusätzlich lässt sich durch Wiederverwendbarkeit Modellierungsaufwand einsparen und Zurückverfolgbarkeit der Anforderungen bis zum Gesetzestext in die Modelle einbauen. Das REALM-Model besteht aus drei Teilen: Einem Konzeptmodel, einem Compliance-Regelsatz und Metadaten.[237] Im Konzeptmodell werden die beteiligten Konzepte (z. B. Kunde, Bank, Konto eröffnen usw.) festgehalten und ihre Beziehungen untereinander dargestellt. Hierbei wird der Compliance-Experte durch ein vorkonfiguriertes UML-Profil unterstützt. Der Compliance-Regelsatz des REALM-Metamodells wird in temporaler Logik ausgedrückt und basiert auf dem Konzeptmodell. Die Metadaten, welche dem Modell hinzugefügt werden, können entweder Verknüpfungen der formalisierten regulatorischen Anforderungen oder Lebenszyklusrestriktionen sein, welche den Gültigkeitszeitraum oder das Auslaufdatum der jeweiligen Anforderung angeben.[238]

Um einen ganzheitlichen Compliance Management Lebenszyklus umsetzen zu können, schlagen GIBLIN ET AL. ein Vorgehen in sechs Schritten vor.

1. Festlegung des Geltungsbereichs der rechtlichen Anforderung
2. Formalisierung der rechtlichen Anforderung in einem REALM-Modell
3. Ist-Analyse der betroffenen Bereiche im Unternehmen
4. Fehleranalyse: Abweichungen von REALM-Modell und Ist-Analyse-Modell

[236] Vgl. Breaux & Powers (2009) S. 276.
[237] Vgl. Giblin et al. (2005), S. 38.
[238] Vgl. Giblin et al. (2005), S. 42 ff.

5. Einführung der REALM-Modelle in die Zielsysteme
6. Kontinuierliche Compliance-Überwachung und Durchsetzung[239]

Der oben beschriebene Ansatz fällt in die Kategorie DTCC, da bei der Abweichungsanalyse des REALM-Modells zum Ist-Modell keine Laufzeit- oder Protokolldaten verwendet werden, sondern durch Umstrukturierung rechtssichere Prozesse entstehen sollen. Im Rahmen der Literaturrecherche wurde für dieses Vorgehen kein spezifischeres Tool gefunden. Stattdessen wird ein UML-Editor verwendet, der ein vorkonfiguriertes Profil nutzt. Des Weiteren ist dieser Ansatz nicht zur automatischen Durchführung gedacht, sondern erfordert manuelle Bearbeitung durch einen Prozessanalysten. Im REALM-Modell wird versucht, eine Anforderung möglichst formal darzustellen. Erst wenn beim Vergleich dieses Modells mit den aktuellen Prozessmodellen eine Divergenz ermittelt wird, werden die REALM-Modelle in die Prozessmodelle integriert. Aus diesem Grund wird der vorliegende Ansatz in die Kategorie „Gegenstand: Anforderung“ eingeordnet.

Ansatz von GOEDERTIER und VANTHIENEN (7)

GOEDERTIER und VANTHIENEN entwickelten eine Methode, die mit Hilfe einer eigens entwickelten temporalen, logischen Sprache Rechte und Pflichten eines Unternehmens explizierten, um diese anschließend automatisiert in Prozessmodellen darzustellen. Dabei ist dieses automatisch generierte Prozessmodell nicht dafür gedacht, bestehende Prozessmodelle zu ersetzen, sondern diese in Hinblick auf Compliance zu verifizieren und zu validieren. Die verwendete logische Sprache PENELOPE (Process ENtailment from the ELicitation of Obligations and PErmissions) unterscheidet sich von anderen logischen Sprachen dadurch, dass sie mit dem Ziel entwickelt wurde, Kontrollflüsse zu generieren, die rechtlichen Anforderungen genügen. Dafür stellt diese Sprache eine Reihe an logischen Operatoren bereit. Ist ein Sachverhalt ausreichend in PENELOPE spezifiziert und enthält keine Livelocks, Deadlocks oder Widersprüche, kann mit einem Algorithmus die formale Darstellung in eine grafische Darstellung überführt werden. Dazu wird eine XML-Datei automatisiert erzeugt, die sich über ein eigens entwickeltes Visio-Plugin grafisch in BPMN anzeigen lässt.[240]

Betrachtungsgegenstand des Ansatzes ist die Anforderung an sich, da das entstehende Prozessmodell nur zur Validierung des bestehenden Prozessmodells genutzt wird. Aufgrund der Tatsache, dass bei der Compliance-Überprüfung keine Laufzeit- oder Vergangenheitsdaten verwendet werden, handelt es sich hierbei um einen DTCC-Ansatz.

[239] Vgl. Giblin et al. (2005), S. 40 f.
[240] Vgl Goedertier & Vanthienen (2006), S. 6 ff.

Ansatz von KARAGIANNIS (8)

Um rechtlichen Anforderungen bezüglich Qualität und Risiko genügen zu können, verwendet KARAGIANNIS, ähnlich dem REALM-Ansatz, Metamodelle. Um dies zu erreichen, werden regulatorische Aspekte bereits auf Meta- und Meta-Meta-Ebene spezifiziert. Es wird zur Durchsetzung von rechtlichen Anforderungen eine Kombination der Geschäftsprozesse und des jeweiligen Modells, das die Risiken und Kontrollmechanismen abbildet, verwendet. Das Metamodell dient als Grundstein für die Definitionen von potenziellen Risiken und den zugehörigen Kontrollen. Durch diese Festlegung auf Meta-Ebene soll die Verknüpfung der alltäglichen Geschäftsprozesse zu den jeweiligen Risiken expliziert und besser überwacht werden können. [241]

Dieser Ansatz kann durch das Tool ADONIS unterstützt werden und ist zum Zeitpunkt des Prozessdesigns durchzuführen (DTCC). Es findet keine automatisierte Compliance-Überprüfung statt und der Betrachtungsgegenstand ist der Prozess an sich, da versucht wird, über die Metamodell-Definition eine rechtlich korrekte Modellierung der Prozesse zu erzwingen.

Ansatz von KNACKSTEDT, BRELAGE und KAUFMANN (9)

Ausgangspunkt für die Entwicklung der Methode stellt die Evaluation einer Reihe von Modellierungssprachen für Webanwendungen in Hinsicht auf ihre Tauglichkeit zur Modellierung von rechtlichen Anforderungen dar. Eine vielversprechende Sprache (eW3DT) wurde exemplarisch erweitert, um den aufgestellten Bedingungen zu genügen. Die Grundform von eW3DT repräsentiert jede Seite einer Internetpräsenz in einem eigenen Symbolkasten, welcher zusätzliche Informationen über die Homepage, wie z. B ob es sich um eine dynamische oder statische Seite handelt, enthält. Um das Erweiterungspotenzial aufzudecken, wurde zunächst ein Metamodell der Sprache erstellt. Anschließend wurden neue Sprachkonzepte und dazugehörige textuelle und grafische Repräsentationsformen eingefügt. Die folgenden vier Konzepte wurden als Erweiterungen vorgeschlagen:

- Interne Sicht: Integration einer Prozessmodellierungstechnik, um die reinen Daten mit den Funktionen zu verbinden. Die gewählte Prozessmodellierungstechnik ist die erweiterte Ereignisgesteuerte Prozesskette.
- Datensichten und Repräsentationen: Die zu grob granulierte Datenstruktur von eW3DT wurde durch die um Sichtenbildung erweiterte Entity-Relationship-Modellierung ersetzt. Zweckgebundenheiten von Daten, die gerade im BDSG eine

[241] Vgl. Karagiannis (2008), S.1162 ff.

wichtige Rolle spielen, werden durch eine Tabelle abgebildet, die für jedes relevante Tupel aus Funktion und Datensicht die erlaubte Verwendung dokumentiert.

- Aktualität: Das maximal erlaubte Alter eines Inhaltes wird eingetragen.
- Status von Eingabefeldern: Um beispielsweise den Status der Checkbox „AGB bestätigen“ abbilden zu können, wurde ein Feld für den Selektionsstatus hinzugefügt.[242]

Mit diesen Erweiterungen und einem entsprechend angepassten Modellierungstool, welches die Sichtentrennung unterstützt, ist die Modellierungstechnik eW3DT gut geeignet, gesetzliche Anforderungen sowohl in der Ablaufreihenfolge als auch in Hinblick auf die Verwendung der Daten übersichtlich abzubilden. Compliance wird hier zum Designzeitpunkt sichergestellt. Das Vorgehen bei dieser Modellierungssprache ist nicht automatisiert und legt den Schwerpunkt darauf, rechtliche Aspekte bei der Webseitengestaltung entsprechend in einem Modell abzubilden.

Ansatz von LY, KNUPLESCH, RINDERLE-MA, GOESER, REICHERT und DADAM (10)

LY ET AL. entwickeln ein Toolset, mit dessen Hilfe sowohl DTCC als auch RTCC ermöglicht werden soll. Zurzeit wurden für das SeaFlows-Toolset bereits Model-Checker Funktionen zum Erstellzeitpunkt implementiert. Diese Funktionen beinhalten strukturelle und datenbezogene Compliance-Checker-Techniken. Ähnlich dem Ansatz von AWAD, DECKER und WESKE (2) können rechtliche Anforderungen in Form von grafischen Regeln eingegeben werden. Zusätzlich steht ein Aktivitätsrepository zur Verfügung, welches für eine einheitliche Modellierung und Begriffsbenutzung sorgt. Auf dieses Repository kann auch der Prozessanalyst beim Erstellen der Regeln zugreifen und somit wesentlich bessere Ergebnisse erzielen, da der Model-Checker mit konsistenteren Daten versorgt werden kann.[243] Um die grafenbasierten Compliance-Regeln spezifizieren zu können, wurde eine eigene Modellierungssprache geschaffen. Die eingegebenen Regeln werden wieder ähnlich dem Ansatz (2) als Muster abgebildet, nach denen im Prozessmodell gesucht wird. So werden bei dem strukturellen Model-Checker Kriterien der Prozessstruktur automatisch aus den Regeln abgeleitet. Das Tool ist eingebettet in ein bestehendes Prozessmodellierungstool, womit es einem Prozessmodellierer möglich ist, das Modell beim Erstellungsvorgang sofort auf Compliance zu überprüfen. Wenn die zu beachtenden rechtlichen Restriktionen korrekt eingegeben wurden und der Prozessmodellierer die im Repository vorgegebenen Aktivitäten verwendet, kann ein vorläufiger Compliance Check auch von Mitarbeitern durchgeführt werden, die keine juristischen Kenntnisse haben.

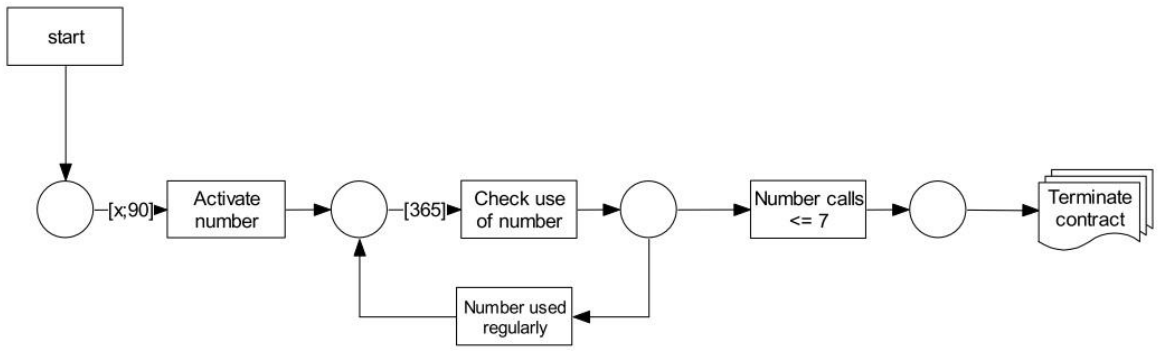
[242] Vgl. Knackstedt, Brelage & Kaufmann (2006), S. 33 ff.
[243] Vgl. Ly et al. (2010), S. 2.

Der zusätzlich implementierte „Data-aware"-Compliance-Checker arbeitet ähnlich der in (2) beschriebenen Erweiterung und beachtet die verschiedenen Status, welche die Laufzeitdaten annehmen können.[244]

Ansatz von OLBRICH und SIMON (11)

Der Ansatz verwendet Petri-Netze, um eine formale Workflow Darstellung zu erreichen.[245] Die Petri Netze werden um die Dimension Zeit erweitert und besitzen jeweils nur einen leeren Start- und Endpunkt. Diese Spezialform wird im Folgenden Modul-Netz genannt. Ist-Prozess und Anforderung werden nun jeweils in ein Modul-Netz überführt. Neben der dabei entstehenden formalen Darstellung lässt sich ein automatisierter Compliance Check durchführen, indem die Schnittmenge aus dem Anforderungs-Netz und dem Ist-Prozess-Netz gebildet wird. Wenn dabei keine Prozesselemente des Ist-Prozess-Netzes verloren gehen, kann davon ausgegangen werden, dass die Anforderung erfüllt wurde.

Der Zeitaspekt wird mit Hilfe von Zeitstempeln auf den Token[246] und mit Vorbedingungen an den eingehenden Kanten der Transitionen realisiert. In Abbildung Abb. 5.4 wird mit diesen Werkzeugen beispielsweise unter anderem dargestellt, dass eine aktive Telefonnummer jedes Jahr (alle 365 Tage) darauf geprüft werden soll, ob mehr als sieben Anrufe getätigt wurden. [247]



Quelle: Olbrich & Simon (2005), S.8.

Abb. 5.4: Darstellung eines Modul-Netzes mit Erweiterung um Zeitaspekt

Der als letztes vorgestellte Ansatz von Olbrich und Simon kann sowohl als DTCC-Technik als auch zur RTCC eingesetzt werden. Um RTCC jedoch betreiben zu können, muss eine Schnittstelle zwischen dem Tool, welches das Modul-Netz verwaltet, und dem Management-Informationssystem, welches Laufzeitdaten bereitstellt, implementiert werden. So

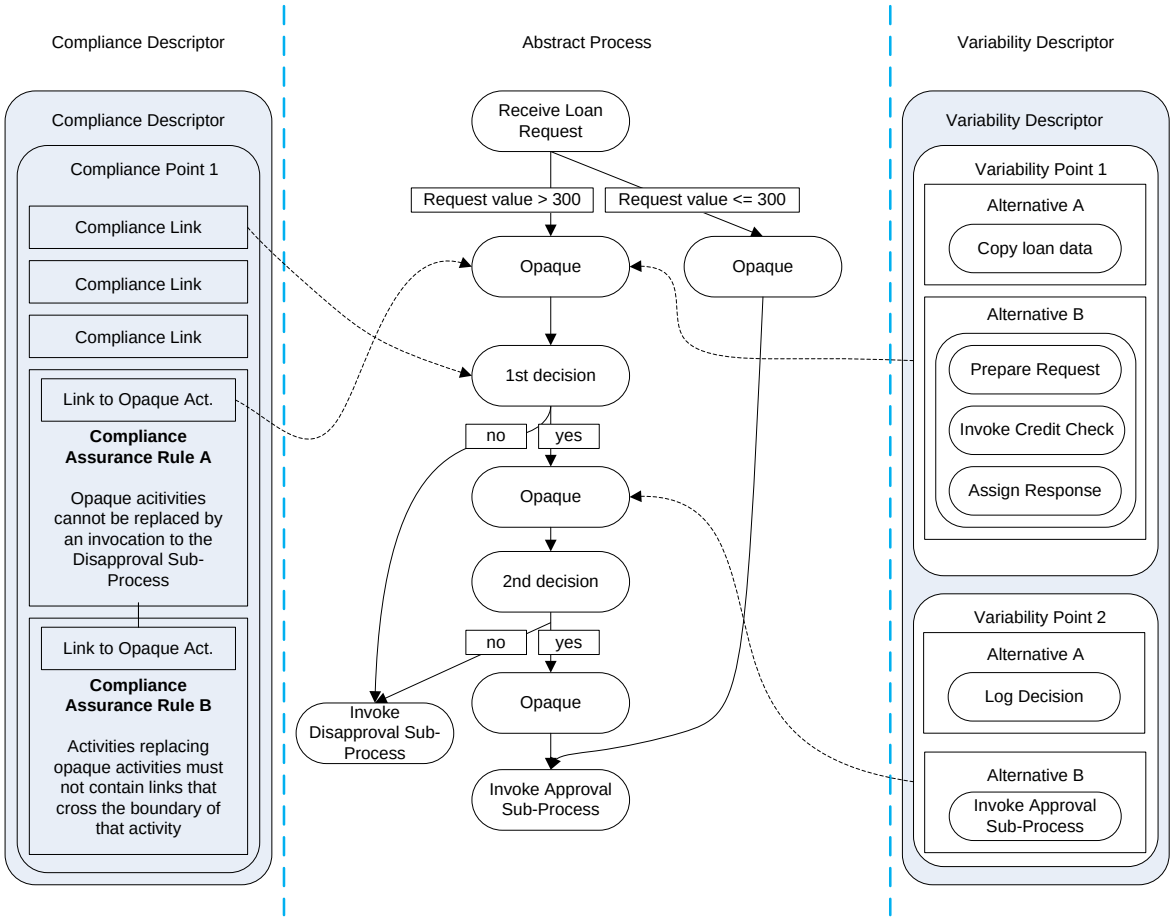
[244] Vgl. et al. (2010), S. 3ff.
[245] Vgl. Olbrich & Simon (2005), S. 5.
[246] Token repräsentieren Objekte, die ein Petri-Netz durchlaufen. Dargestellt werden sie durch Zahlen oder Wahr-/Falsch-Werte in den Statussymbolen des Netzes.
[247] Vgl. Olbrich & Simon (2005), S. 5 f.

könnte zur Laufzeit bestimmt werden, ob ein Workflow gegen zeitliche oder strukturelle Bedingungen verstößt. Der Vorgang ist teilautomatisierbar und versucht, über einen modellüberprüfenden Vorgang rechtlichen Anforderungen genügende Workflow-Modelle zu erzeugen.

Ansatz von SCHLEICHER, ANSTETT, LEYMANN, and MIETZNER (12)

Im Rahmen dieses Ansatzes wird eine Methodik entwickelt, eine rechtssichere Modellierung mittels sogenannter Compliance Templates zu garantieren. Mit Hilfe dieser, von einem Compliance Experten bereits vorbereiteten Vorgaben, soll es selbst einem Prozessmodellierer ohne jegliche Vorkenntnisse in juristischen Fragestellungen möglich sein, rechtskonforme Prozess- und Workflowmodelle zu erzeugen. Ein solches Compliance Template ist in drei Bereiche aufgeteilt. Einen abstrakten Geschäftsprozess, einen Variabilitäts- und einen Compliancebeschreiber. Im abstrakten Prozess sind bereits implizit einige rechtliche Vorgaben umgesetzt. Zusätzlich befinden sich im Prozess Platzhaltersymbole, die von einem Prozessmodellierer gefüllt werden können. Damit bei diesem Vorgang ebenfalls ein rechtskonformes Verhalten des Prozesses garantiert werden kann, wurden die Variabilitäts- und Compliancebeschreiber eingeführt. Variabilitätsbeschreiber geben ähnlich dem Prozessbausteinsatz der PICTURE-Methode[248] ein Spektrum von einzufügenden Aktivitäten vor, während über den Compliancebeschreiber zusätzliche, nicht implizit implementierbare rechtliche Einschränkungen spezifiziert werden. So kann an dieser Stelle festgelegt werden, dass in ein bestimmtes Platzhalterfeld eine festgelegte Aktivität nicht eingefügt werden darf, da dadurch beispielsweise ein gesetzlich vorgeschriebener Prüfvorgang umgangen worden wäre (vgl. Abb. 5.5)[249].

[248] Vgl. Becker et al. (2007).
[249] Vgl. Schleicher et al. (2009), S. 62ff.



Quelle: Vgl. Schleicher et al. (2009), S. 63.

Abb. 5.5: Compliance Template

Weiterhin stellen SCHLEICHER ET AL. eine Überführung der im Compliancebeschreiber formulierten Regel in eine formale Sprache vor, um nach dem Modellierungsvorgang einen automatisierten Compliance Check durchführen zu können. Ein großer Vorteil dieser Methode liegt in der hohen Wiederverwendbarkeit der einzelnen Templates sowie in der Möglichkeit, Mitarbeiter aus der Fachabteilung, welche eine gute Vorstellung vom Soll-Prozess haben, jedoch die rechtlichen Einschränkungen nicht kennen, ihre eigenen Prozesse modellieren zu lassen.[250]

Dieser Ansatz hat DTCC-Charakter und ist in gewissen Teilen automatisierbar. Zurzeit gibt es hierfür noch keine Toolunterstützung, diese ist aber in Planung. Ziel dieser Methodik ist es, einen Geschäftsprozess zu erstellen, welcher den rechtlichen Anforderungen genügt.

[250] Schleicher et al. (2009), S. 65 ff.

Zusammenfassung

Um einen Überblick über die Vielzahl der untersuchten Ansätze zu ermöglichen, wird die Einordnung derselben anhand der in Tabelle 5.1 definierten Kriterien noch einmal in tabellarischer Form zusammengefasst.

Kriterien / Autoren	Logische Sprachen	FCC		BCC	Automatisierung	Tool-Unterstützung	Betrachtungsgegenstand		Modellierungssprache
		DTCC	RTCC				Prozess	Anforderung	
Araujo (1)	✓		✓		✓	✓	✓		OCL, UML
Awad (2)	✓	(✓)	✓		✓	✓	✓		BPMN-Q, Petri-Netze
Becker (3)		✓		✓		✓		✓	EPK
Feja (4)	✓	✓			✓	✓	✓		EPK, G-CTL
Breaux (5)		✓				✓		✓	BPMN, FBRAM
Giblin (6)		✓		✓				✓	REALM, UML
Goedertier (7)	✓	✓			✓	✓		✓	PENELOPE
Karagiannis (8)		✓				✓	✓		ADOxx
Knackstedt (9)		✓					✓		eW3DT, EPK, ERM
Ly (10)		✓	✓		✓	✓	✓		AristaFlow
Olbrich (11)		✓	✓		✓		✓		Petri-Netze
Schleicher (12)	✓	✓			(✓)		✓		WS-BPEL

Tab. 5.1: Einordnung der Ansätze

6 Zertifizierung von IT-Anwendungen

Stefan Laube

6.1 Bedeutung der Zertifizierung von IT-Anwendungen

Die Art und der Umfang von Pflichten für IT-Hersteller werden zum einen durch die Erwartungen des Verkehrs, zum anderen maßgeblich vom Erkenntnisstand von Wissenschaft und Technik mitbestimmt.[251] Soll der Nachweis von IT-Qualität oder definierter Sicherheitsstandards einer IT-Anwendung erbracht werden, so bieten sich hierfür Zertifikate an.[252] Gesetzlich sind jedoch haftungsrechtliche Auswirkungen von Zertifikaten nicht ausdrücklich geregelt und nicht abschließend geklärt.[253] Es gibt unzählige Zertifikate, die im Internet angeboten werden, darunter verbandseigene und staatliche Gütesiegel sowie TÜV-Plaketten und „reihenweise inzestuöse Auszeichnungen unter Geschäftspartnern".[254]

Bezüglich der Zertifizierung von IT-Anwendungen stellen sich somit die Fragen: Auf Basis welcher Standards wird zertifiziert? Und kommt Zertifikaten – ob von privaten Zertifizierungsstellen oder denen des BSI (Bundesamt für Informationssicherheit) – eine haftungsbefreiende Wirkung zu? Dies soll im Folgenden beantwortet werden.

6.2 Typologisierung von Standards und Normen zur Zertifizierung von IT-Anwendungen

6.2.1 Standards und Normen

Es gibt zahlreiche Gremien, die Sicherheitsstandards und Normen entwickeln. Unter einem Standard sind verschiedene, in einem Konsensprozess entstandene Spezifikationen zu verstehen. Normen werden aufgrund öffentlicher Erarbeitungsverfahren und ihrer Zugänglichkeit sowie einer laufenden Anpassung an den Stand der Technik als anerkannte Regeln der Technik angesehen. Sie sind Standards, bei denen der Konsens in einem öffentlichen Einspruchsverfahren[255] hergestellt wurde. Rechtlich gelten Normen häufig als antizipierte Sachverständigenaussage.[256]

[251] Vgl. Spindler (2007), S. 65.
[252] Vgl. Helmbrecht (2009), S. 45.
[253] Vgl. Spindler (2007), S. 71.
[254] Bell (2009), S. 46.
[255] In einem öffentlichen Einspruchsverfahren hat die Öffentlichkeit Gelegenheit, Einwände gegen eine geplante Norm vorzubringen.
[256] Vgl. Hohler (2007), S. 822.

Um das für einen entwickelten Standard verantwortliche Gremium zu identifizieren, ist die Zeichenkette zu Beginn der Standard-Kurzbezeichnung zu betrachten. Bei ISO/IEC-Standards handelt es sich um internationale Normen der internationalen Normenorganisation ISO und der International Electronical Commission (IEC). Diese Normen wurden nach einem Konsensverfahren entwickelt und in einer öffentlichen Umfrage bestätigt. Bei mit der Zeichenkette EN beginnenden Standards handelt es sich um Europäische Normen, ebenfalls nach einem Konsensverfahren entwickelt und in einer öffentlichen Umfrage bestätigt. Beginnt die Zeichenkette mit der Kurzbezeichnung DIN, so liegt eine deutsche Norm zugrunde. DIN EN bezeichnet Normen, die aus Europäischen Normen in das deutsche Normenwerk übernommen wurden. Andere Bezeichnungen (Beispiel: IDW PS 330) deuten auf von Interessengruppen, Behörden oder Konsortien erarbeitete Standards hin. Diese Standards wurden nach Regeln der jeweiligen Vereinigung erarbeitet. Diese Regeln legen Mitwirkungsmöglichkeiten fest und sehen gegenüber den Normungsorganisationen eingeschränkte Konsensrahmen vor.[257]

Die technische Ausreifung eines Gebietes ist die Voraussetzung für sinnvolle Normungsarbeit. Bei Software ist diese Ausreifung noch nicht vollständig abgeschlossen, weshalb Software-Entwickler heutzutage einer unübersichtlichen Auswahl von Hunderten verschiedener Normen und Standards ausgesetzt sind, die von verschiedensten privaten und staatlichen Organisationen entwickelt wurden.[258]

6.2.2 Haftungsrechtliche Bedeutung von technischen Normen

Private Normungsorganisationen wie z. B. der DIN e.V. erlassen keine Rechtsnormen. Laut der Rechtsprechung handelt es sich bei diesen Normen vielmehr um auf freiwillige Anwendung angelegte Empfehlungen der privaten Normungsorganisationen. Eingesetzte überbetriebliche technische Normen im Haftungsrecht haben nach ständiger Rechtsprechung des BGH viel mehr die Bedeutung, dass sie zur Bestimmung des nach der Verkehrsauffassung zur Sicherheit Gebotenen in besonderer Weise geeignet sind. Dies gilt insbesondere für DIN-Normen, bei deren Einhaltung eine tatsächliche Vermutung für die Wiedergabe der anerkannten Regeln der Technik besteht, die nicht unterschritten werden darf. Normen können somit den Inhalt von Verkehrspflichten[259] konkretisieren, binden Zivilgerichte allerdings mangels Rechtsnormqualität nicht, da sie die Sorgfaltsanforderungen nicht abschließend bestimmen.

[257] Vgl. BITCOM & DIN (2009), S. 6.
[258] Vgl. Hohler (2007), S. 822.
[259] Eine Verkehrspflicht ist eine Verhaltenspflicht zur Absicherung von Gefahrenquellen. Ein Unterlassen dieser Verhaltenspflicht kann zu Schadensersatzansprüchen führen.

Die Festlegung von allgemeingültigen Sicherheitsstandards im IT-Bereich wird durch den rasanten Fortschritt der Softwareentwicklung be- oder sogar verhindert. Da diese allgemeingültigen Sicherheitsstandards nicht existieren, kann es hinsichtlich der Sicherheitserwartungen des Verkehrs praktisch zu keiner Konkretisierung durch technische Normen kommen.[260]

Durch die Zertifizierung und Prüfung von IT-Produkten in bestimmten Bereichen, in denen eine nötige Mindestsicherheit konkretisiert ist, können Produktstandards jedoch rechtliche Wirkung entfalten. Das Ergebnis ist, dass Standards nach dem derzeitigen Stand grundsätzlich nur sektorspezifisch Wirkung entfalten können. Passen Standardisierungen auf ein aktuell hergestelltes Produkt, so können sie als Konkretisierung der Verkehrspflichten und der geschuldeten Sorgfalt rechtlich verwertet werden.[261]

6.2.3 Standards als Grundlage für Softwarezertifikate

Zertifikate bauen auf gegebenen Standards bzw. Normen auf. Softwarezertifizierung hat die Aufgabe der Untersuchung und Beurteilung von Software anhand von vordefinierten Kriterien durch einen neutralen Dritten. Werden die vordefinierten Kriterien erfüllt, so wird dies in Form eines Zertifikates bescheinigt. Ein Softwarezertifikat hat zwei Ziele: Auf der einen Seite soll es gegenüber den Adressaten (Revisoren, Aufsichtsbehörden, Käufer oder Anwender) die Erfüllung der zertifizierten Kriterien dokumentieren, andererseits dient es dem Softwarehersteller als Teil seiner Qualitätssicherung. Die Standards legen fest, wie bei einer Zertifizierung vorzugehen ist.

Durch das Typologisieren verschiedener Standards lassen sich verschiedene Kategorien von Softwarezertifikaten definieren. Im Allgemeinen wird zwischen produkt-, prozess- und projektorientierter Softwarezertifizierung unterschieden:

- Produktorientierte Softwarezertifizierung befasst sich mit der Zertifizierung von Eigenschaften eines Softwareproduktes.
- Prozessorientierte Softwarezertifizierung behandelt die Zertifizierung der Aufbau- und Ablauforganisation des Produktionsprozesses und somit der Softwareherstellung. Bei dieser Art der Zertifizierung ist zu beachten, dass keine Prüfung eines konkreten Softwareproduktes mittels Qualitätsmerkmalen erfolgt.[262]

[260] Vgl. Hoeren (2008), Rn 94.
[261] Vgl. Spindler (2007), S. 66 ff.
[262] Vgl. Back et al. (2001), S. 424 f.

- Bei der projektorientierten Softwarezertifizierung erfolgt eine Prüfung des Herstellungsprojektes.[263]

Im Speziellen haben produkt-, prozess- und projektorientierte Softwarezertifizierung zwei weitere Unterkategorien: Zertifizierung von IT-Sicherheit und Zertifizierung von IT-Qualität.

Kategorie	Standard	Beschreibung/Titel
Produktstandard	RAL-GZ 901; DIN 66285; DIN ISO/IEC 12119	Mindeststandards für Gütebedingungen
Produktstandard	DIN ISO/IEC 15408	Standard zur Evaluierung von IT-Sicherheit (Common Criteria Standard)
Produktstandard	ISO/IEC 25000	Software-Engineering – Qualitätskriterien und Bewertung von Softwareprodukten (SQuaRE)
Produktstandard	ISO/IEC 25051	Software-Engineering – Softwareproduktbewertung – Qualitätsanforderungen an kommerzielle serienmäßig produzierte Softwareprodukte (COTS) und Prüfanweisungen
Produktstandard	DIN EN ISO 9241	Ergonomie der Mensch-System-Interaktion – Teil 110: Grundsätze der Dialoggestaltung
Prozessstandard	DIN ISO/IEC 27001	Standard der Informationssicherheits-Managementsysteme (ISMS)
Prozessstandard	IT-Grundschutz	Standard der Informationssicherheits-Managementsysteme (ISMS)
Prozessstandard	PCI DSS	Sektor-Spezifische Sicherheits-Managementsysteme
Prozessstandard	IDW PS 330	Standard für Wirtschaftsprüfer zur Prüfung der IT rechnungslegungsrelevanter Systeme
Prozessstandard	DIN EN ISO 9000 ff.	Normen für Qualitätsmanagementsysteme
Prozessstandard	DIN ISO/IEC 15504, SPICE (Software Process Improvement and Capability Determination)	Standards zur Bewertung von Unternehmensprozessen mit Schwerpunkt Softwareentwicklung
Produktstandard sowie Prozessstandard	IDW PS 880	Die Prüfung von Softwareprodukten
Projektstandard	IDW PS 850	Projektbegleitende Prüfung bei Einsatz von Informationstechnologie

Tab. 6.1: Prospektprüfungsstandards zur Softwarezertifizierung[264]

In Tabelle 6.1 sind die gängigsten Prospektprüfungsstandards zur Softwarezertifizierung aufgelistet. Einige dieser Standards sind in dem „Kompass der IT-Sicherheit“, herausgegeben von dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) sowie dem Deutschen Institut der Normung e.V. (DIN), klassifiziert. Hierbei handelt es sich um Standards zur prozess- und produktorientierten Softwarezertifi-

[263] Vgl. Back et al. (2001), S. 424 f.
[264] Vgl. Bächle (1996), S. 4; BITCOM & DIN (2009), S. 4, 12 f.; Hohler (2007), S. 823; Brauer (2002), S. 7; Wagner & Dürr (2008), S. 15.

zierung.[265] Neben diesen Standards gibt es repräsentative, international gültige Normen die eine produktorientierte Softwarezertifizierung von IT-Qualität ermöglichen.

Die Prospektprüfung nach dem RAL-GZ 901 Standard ist ein Beispiel für produktorientierte Softwarezertifizierung, die eine vom Hersteller vorgegebene IT-Qualität bestätigt. Bei dieser Prüfung werden ausschließlich Softwareeigenschaften, die der Hersteller in der Produktbeschreibung nennt, überprüft.

Eine Prospektprüfung nach den Standards des IDW PS 880 verlangt dagegen eine Kombination der Ansätze der produktorientierten sowie prozessorientierten Softwarezertifizierung und dient der Bestätigung von IT-Sicherheit sowie IT-Qualität.

Werden die vorgestellten Standards typologisiert, so ergibt sich folgende Tabelle, mit Hilfe derer sich Softwarezertifikate von verschiedenen Anwendern einordnen lassen (vgl. Abb. 6.1).

<table>
<tr><th>Merkmal</th><th>Prozessorientierte Softwarezertifizierung</th><th>Produktorientierte Softwarezertifizierung</th><th>Projektorientierte Softwarezertifizierung</th></tr>
<tr><td>IT-Sicherheit</td><td>DIN ISO/IEC 27001;
IT-Grundschutz;
PCI DSS;
IDW PS 330</td><td>Common Criteria;
DIN ISO/IEC 15408</td><td>---</td></tr>
<tr><td rowspan="2">IT-Qualität</td><td rowspan="2">DIN EN ISO 9000 ff.;
DIN ISO/IEC 15504;
SPICE Verbunden mit DIN EN ISO 9000 ff.</td><td>RAL-GZ 901;
DIN 66285;
DIN ISO/IEC 12119;
ISO/IEC 25051;
DIN EN ISO 9241;
ISO/IEC 25000 (9126)</td><td>IDW PS 850</td></tr>
<tr><td colspan="2">IDW PS 880</td></tr>
</table>

Abb. 6.1: Typologisierung der Standards

6.2.4 Haftungsrechtliche Bedeutung von Zertifikaten

Die zivil- bzw. haftungsrechtlichen Auswirkungen von Zertifikaten sind bislang nicht abschließend geklärt. Zertifikate stellen keine endgültigen Definitionen von einzuhaltenden Sicherheitsanforderungen des Herstellers dar und bewirken somit keine pauschale Entlastung des Herstellers. Auch die haftungsrechtliche Verantwortung geht durch eine Zertifizierung nicht vom Hersteller auf den Zertifizierer über. Der Hersteller darf sich also auch nicht darauf verlassen, dass Zertifizierer von IT-Anwendungen alle Mängel eines Produktes aufdecken. Hinsichtlich der Zertifizierungsstelle spielt es dabei keine Rolle, ob sie privat, z. B. der TÜV, oder eine Behörde, wie das Bundesamt für Sicherheit in der Informationstechnik, ist. Die zivilrechtliche Haftung des Herstellers bleibt unberührt.

[265] Vgl. BITCOM & DIN (2009), S. 4.

In § 6 Abs. 4 Medizinproduktegesetz (MPG) wird ausdrücklich klargestellt, dass ein Konformitätsbewertungsverfahren[266] die zivil- und strafrechtliche Verantwortlichkeit unberührt lässt. Dieser Grundsatz, der eine Umsetzung der Medizin-Produktrichtlinie darstellt, und andere Grundsätze gelten auch für IT-Produkte. Eine Zertifizierung dokumentiert zunächst lediglich die Einhaltung von (Mindest-) Anforderungen der zugrundeliegenden technischen Norm. Haben Zertifikate jedoch Einfluss auf die Erwartungen der Nutzer, so können sie in beschränktem Umfang bei der Bestimmung von Verkehrspflichten relevant werden.

Zertifikate können die Erwartungen beim Kunden oder Verbraucher hinsichtlich der Qualität oder der Sicherheit erhöhen. Sollte das der Fall sein, so muss sich das zertifizierte Unternehmen an den Erwartungen orientieren und darf mit seinem Produkt oder seiner Produktionstätigkeit nicht von ihnen abweichen. Somit erhalten Zertifikate eine deutliche Aussagekraft für den Bereich der Werbung. Für Zertifikate von IT-Produkten muss derzeit davon ausgegangen werden, dass die Sicherheitserwartungen sowie Qualitätserwartungen der Nutzer erst signifikant steigen, wenn sich in einem Produktbereich einzelne Prüfmethoden durchgesetzt haben. Da der Inhalt von Zertifizierungen aber weitestgehend, aufgrund der Schnelllebigkeit von verschiedenen Standards und Normen, unbekannt bleibt, kann der Einsatz von Zertifikaten für IT-Produkte die Sicherheitserwartungen entsprechender Kreise selten steigern. Eine Ausnahme stellen Softwarekäufe zwischen Unternehmen dar, sobald es sich um den Kauf von Individualsoftware handelt. Hierbei werden die Erwartungen beim Käufer durch die Einhaltung von Normen für Sicherheit und Qualität durch den Hersteller beeinflusst.[267]

Zertifikaten für IT-Produkte können auch nur eingeschränkte beweisrechtliche Bedeutungen beigemessen werden. Regelmäßig können sie den konstruktionsverantwortlichen Hersteller nicht entlasten. Im Einzelfall kommt Zertifizierungen anhand anerkannter technischer Normen eine indizielle Bedeutung für den Normkonformitätsnachweis zu. Diese Indizwirkung zugunsten des Herstellers besteht nur, wenn Ist-Standards zertifiziert wurden. Da sich Standards aber schnell weiterentwickeln, müssen häufig Prüfungen der IT-Produkte durchgeführt werden, bevor eine Rechtsprechung erfolgen kann.[268]

[266] Nach der internationalen Norm ISO/IEC 17000:2004 ist Konformitätsbewertung definiert als „Darlegung, dass festgelegte Anforderungen bezogen auf ein Produkt, einen Prozess, ein System, eine Person oder eine Stelle erfüllt sind".
[267] Vgl. Spindler (2007), S. 71 ff.
[268] Vgl. Spindler (2007), S. 83 f.

6.2.5 Zuordnung verschiedener Zertifizierungsstellen zu Standards und Normen

Abgesehen von staatlich vergebenen Zertifikaten besteht das Problem, dass viele Verbände, wie der TÜV und andere, die Verbraucher mit Tausenden von Zertifikaten überschwemmen, wobei die Aussagekraft der Zertifikate schwindet.[269] Aufgrund der Schnelllebigkeit und der unüberschaubaren Menge von IT-Zertifikaten können sich Sicherheitserwartungen bei Verbrauchern und Kunden sehr schwierig etablieren. „Die Fülle kursierender Zertifikate und Möchtegern-Testate macht den erwünschten Effekt zunichte und stiftet bloß Verwirrung".[270]

Ein gutes Beispiel hierfür ist der TÜV Rheinland, der unter dem Logo TUVdotCom rund 2500 Kennzeichen vereint. Einheitliche Zertifikate sind, wie sie beispielsweise von TÜV Nord und Süd sowie TÜV Hessen und Saarland zu erwarten wären, nicht in Sicht, da die Unternehmen in Konkurrenz stehen. „Die Marke TÜV profitiert zweifellos davon, dass sie als quasi amtlich angesehen ist und hierzulande [eine bekannte] Prüfinstanz"[271] ist. Jedoch ist der TÜV längst privatwirtschaftlich organisiert. Der Marketing-Manager des TÜV Nord räumt ein: „Man muss schon genau hinschauen, um zu erkennen, wofür unsere bald zwei Dutzend Siegel im Einzelnen stehen".[272]

Von vielen Experten werden Verbände in der Verantwortung gesehen, die eine Hierarchie für Softwaresiegel erstellen sollen. Jedoch bereichern Verbände wie die BITKOM oder der Bundesverband Digitale Wirtschaft (BVDW) die Siegelflut um eigene Kategorien, was eine Harmonisierung des Marktes derzeit illusorisch macht.

Die *Zertifizierung von IT-Sicherheit* wird in Deutschland vom Bundesamt für Sicherheit in der Informationstechnik vorgenommen.[273] Das BSI kann außerdem Prüfstellen akkreditieren[274], damit diese die notwendige Kompetenz, Unabhängigkeit und Objektivität bescheinigt bekommen, um in geordneter und nachvollziehbarer Weise Zertifizierungen von IT-Sicherheit durchführen zu können. Eine Liste der vom BSI akkreditierten Prüfstellen findet sich auf der Internetseite des BSI.[275] Über das BSI oder eine vom BSI akkreditierte Prüfstelle können folgende Softwarezertifikate erteilt werden:

- *Zertifikate nach Common Criteria, DIN ISO/IEC 15408*: Hierbei wird eine technische Prüfung gemäß den Sicherheitskriterien, die vom BSI allgemein anerkannt und

[269] Vgl. Bell (2009), S. 46.
[270] Bell (2009), S. 46.
[271] Bell (2009), S. 46.
[272] Bell (2009), S. 46.
[273] Vgl. BSIG §3 Abs. 1 S. 5.
[274] Eine Akkreditierung ist die formelle Anerkennung der Kompetenz einer Prüfstelle durch eine unabhängige Stelle, bestimmte Prüfungen oder Evaluierungen durchzuführen.
[275] Einzusehen sind sämtliche Prüfstellen auf der Internetseite des BSI: https://www.bsi.bund.de.

öffentlich bekannt gemacht wurden, durchgeführt. Für die Sicherheitsevaluierung von IT-Produkten und IT-Systemen wird bei dieser Norm ein Kriterienwerk definiert. Außerdem legen die Common Criteria Anforderungen an die Vertrauenswürdigkeit von IT-Produkten und IT-Systemen fest.[276]

- *Zertifikate nach IT-Grundschutz*: Diese Zertifizierung stellt zusammen mit den Empfehlungen von Standard-Sicherheitsmaßnahmen, die in IT-Grundschutzkatalogen niedergeschrieben sind, einen De-Facto-Standard für IT-Sicherheit dar. Der IT-Grundschutz Katalog beschreibt Anforderungen an das IT-Sicherheitsmanagement sowie IT-Sicherheitsmaßnahmen aus verschiedensten Bereiche. Im Jahre 2006 wurde das Vorgehen nach IT-Grundschutz an die DIN ISO/IEC 27001 angepasst, damit auch der internationale Standard für Informationssicherheits-Managementsysteme (ISMS) abgedeckt werden kann.[277]

Neben dem BSI und dessen akkreditierten Prüfstellen gibt es weitere private Institutionen, die IT-Sicherheit zertifizieren. Das Institut der Wirtschaftsprüfer (IDW) gibt beispielsweise mit dem Standard IDW PS 330 einen Leitfaden für Wirtschaftsprüfer zur Prüfung von IT-Systemen, die rechnungslegungsrelevant sind, heraus. Außerdem entwickelte das IDW weitere Standards zur Zertifizierung von IT-Qualität. Wie das BSI kann das IDW Prüfstellen für eine Softwarezertifizierung nach ihren Standards akkreditieren.[278] Diese Standards sind:

- *Zertifikate nach IDW PS 330*: Zur prozessorientierten Softwarezertifizierung werden hierbei IT-Risikoindikatoren herangezogen, um IT-Risiken zu identifizieren und analysieren. Dieser Standard dient der Sicherheitszertifizierung.[279]

- *Zertifikate nach IDW PS 880*: Der IDW PS 880 definiert einen Prüfungsstandard zur Erteilung und Verwendung von Softwarebescheinigungen. Der Standard „zeigt die Anforderungen auf, die bei der Prüfung von Softwareprodukten und der Erteilung von Bescheinigungen zu Softwareprodukten zu beachten sind, wenn diese für die Ordnungsmäßigkeit der Rechnungslegung von Bedeutung sind“.[280] Es werden bei der Zertifizierung nach IDW PS 880 eine bestimmte Qualität des Herstellungsprozesses sowie bestimmte Softwareeigenschaften verlangt. Somit liegt eine produkt- wie auch prozessorientierte Softwarezertifizierung vor.[281]

[276] Vgl. BITCOM & DIN (2009), S. 43.
[277] Vgl. BITCOM & DIN (2009), S. 20; Eschweiler & Psille (2006), S. 142 f.
[278] Eine Liste akkreditierter Stellen findet sich auf der Internetseite des IDW: http://www.idw.de.
[279] Vgl. BITCOM & DIN (2009), S. 37.
[280] Philipp (1999), S. 3.
[281] Vgl. Back et al. (2001), S. 425.

- *Zertifikate nach IDW PS 850*: Dieser Standard zur projektorientierten Softwarezertifizierung prüft bereits während der Durchführung eines Projektes die Entwicklung, Einführung, Änderung oder Erweiterung IT-gestützter Rechnungslegungssysteme. Die projektbegleitende Prüfung basiert auf dem IDW Prüfstandard IDW PS 330.[282]

Eine weitere Möglichkeit zur *prozessorientierten Softwarezertifizierung* von IT-Sicherheit bieten die Standards PCI DSS (Payment Card Industry Data Security Standard) und DIN ISO/IEC 27001.

- *Zertifikate nach PCI DSS*: Dieser sektorspezifische Standard stellt ein Sicherheitsrahmenwerk für Kreditkartenunternehmen dar und hält zur Kontrolle der Bereiche logische Sicherheit und physikalische Sicherheit eine umfassende Anforderungsliste bereit.[283] Zertifizierungsstellen sind beispielsweise privatwirtschaftliche Unternehmen wie die Acertigo AG[284] oder die OPTIMAbit GmbH.[285]

- *Zertifizierung nach DIN ISO/IEC 27001*: Dieser Standard beschreibt die grundlegenden Anforderungen an ein Informationssicherheits-Managementsystem (ISMS), das häufig in Unternehmen oder Behörden eingesetzt wird. Dabei stellt der Standard im Rahmen eines Prozess-Ansatzes die Anforderungen an ein ISMS dar, die mittelbar zur Informationssicherheit beitragen. Der DIN ISO/IEC 27001 wird wegen seiner engen methodischen Anlehnung an den DIN EN ISO 9000 ff. Standard als ein Qualitätsstandard für Managementsysteme bzgl. Informationssicherheit angesehen. Akkreditierte Zertifizierungsstellen für eine DIN ISO/ISE 27001 Zertifizierung können auf der Internetseite der Trägergemeinschaft für Akkreditierung (TGA) GmbH abgerufen werden.[286]

Alle weiteren in Abb. 6.1 aufgelisteten Standards dienen der *Zertifizierung von IT-Qualität*. Weit verbreitete, die Software- und Systementwicklung bestimmende, Qualitätsstandards zur *prozessorientierten Softwarezertifizierung* sind die Normreihe DIN EN ISO 9000 ff. und der Standard SPICE.[287]

- *Zertifikate nach DIN EN ISO 9000 ff.*: Die Normreihe DIN EN ISO 9000 ff. besteht aus Qualitätsmanagementnormen, die Anforderungen an das Qualitätsmanagement

[282] Vgl. IDW (2008), S. 2.
[283] Vgl. BITCOM & DIN (2009), S. 23.
[284] Internetseite der Acertigo AG: http://www.acertigo.com.
[285] Internetseite der OPTIMAbit GmbH: http://optimabit.com.
[286] Internetseite der TGA: http://www.tga-gmbh.de.
[287] Vgl. Wallmüller (2007), S. 163.

eines Software-Herstellungsprozesses beschreiben.[288] Sie eignen sich zum Aufbau eines modernen Qualitätsmanagementsystems. Eine Liste akkreditierter Zertifizierer dieser Qualitätsnormen befindet sich im Internet.[289]

- *Zertifikate nach SPICE, DIN ISO/IEC 15504*: SPICE ist ein internationaler Standard, der Unternehmensprozesse bewertet. Sein Schwerpunkt liegt auf dem Softwareentwicklungsprozess. Der Standard ist eine internationale Übereinkunft zum Thema Software Process Assessment und dient dabei der Bewertung, ob eine Softwareentwicklungs-Vorgehensweise dem derzeitigen Stand der Technik entspricht.[290] Anders als bei der DIN EN ISO 9000 ff. Normreihe werden bei SPICE zunächst Personen, sogenannte Assessors bzw. Appraiser, von anerkannten Akkreditierungsstellen zertifiziert. Daraufhin können diese Personen Zertifikate für Prozesse gemäß DIN ISO/IEC 15504 zertifizieren. Der Standard ist in fünf Teile aufgeteilt, wobei während der Software-Tests Verfahrensweisen dieses Standards wie z. B. die systematische Erzeugung von Prüffällen oder die systematische Durchführung von Programmabläufen eingesetzt werden. SPICE ist eng mit dem DIN EN ISO 9000 ff. Normenwerk verbunden und stützt sich auch auf Normen wie die ISO/IEC 12207 – Prozesse im Software-Lebenszyklus.[291] SPICE Prozesszertifizierungsstellen sind z. B. die Gesellschaft für Prozessmanagement[292] oder die wibas GmbH[293]. SPICE Personenzertifizierungen werden nach Qualifizierungsschemata wie iNTACS und INTRSA vorgenommen.

Die *produktorientierte Softwarezertifizierung von IT-Qualität* findet üblicherweise über privatwirtschaftliche Unternehmen statt. Am häufigsten finden die Produktnormen ISO/IEC 25000, ISO/IEC 25051, DIN EN ISO 9241 und RAL-GZ 901 Anwendung. Die Norm RAL-GZ 901 wurde inzwischen durch die DIN ISO/IEC 12119 abgelöst.[294] Der Markt von privatwirtschaftlichen Software-Siegel Anbietern ist jedoch überfüllt, wodurch der erwünschte Effekt von Zertifikaten verloren geht.[295] Nachfolgend seien dennoch einige Unternehmen genannt, die anhand der erwähnten Produktnormen zertifizieren. Der TÜV Rheinland bietet Zertifizierungsverfahren an, die in der Regel vier bis zwölf Wochen dauern. Dabei kostet ein Zertifikat je nach Aufgabenstellung zwischen 1500 € und Beträgen in siebenstelliger Höhe. Diese Beträge fallen auch an, wenn der Zertifikatsanwärter durch-

[288] Vgl. Brause (2005), S. 227.
[289] Liste akkreditierter Zertifizierer der DIN EN ISO 9000 ff. Normreihe: http://www.quality.de/g0000010.htm.
[290] Vgl. Liggesmeyer (2009), S. 385.
[291] Vgl. Liggesmeyer (2009), S. 385.
[292] Internetseite der Gesellschaft für Prozessmanagement: http://www.prozesse.at.
[293] Internetseite der wibas GmbH: http://www.wibas.de.
[294] Vgl. Hohler (2007), S. 823.
[295] Vgl. Bell (2009), S. 46.

fällt.[296] Dabei verwendet der TÜV Rheinland ein sehr breites Spektrum an Normen und Standards.[297] Auch der TÜV Süd, in Konkurrenz zum TÜV Rheinland, bietet verschiedene Softwareprüfungen an Hand der erwähnten Standards an:[298]

- *Zertifikate nach ISO/IEC 25000 bzw. ISO/IEC 9126*: Diese Norm wird zur produktorientierten Zertifizierung von Softwarequalität genutzt. Sie definiert Richtlinien für eine Serie internationaler Standards im Bereich der Qualitätsanforderungen eines Softwareproduktes und deren Evaluierung. Der Name der Serie lautet „Software product Quality Requirements and Evaluation" (SQuaRE). Zur Definition von Anleitungen zum Einsatz der Standards bedient sich die Norm der Qualitätsmerkmale Funktionalität, Zuverlässigkeit, Benutzbarkeit, Effizienz, Änderbarkeit und Übertragbarkeit.[299] Diese Qualitätsmerkmale von Software sind in der DIN 66272 definiert.[300]

- *Zertifikate nach ISO/IEC 25051*: Diese Norm zur Softwareproduktbewertung definiert Anforderungen an COTS Software Produkte, d. h. seriengefertigte Produkte aus dem Softwaresektor, sowie Prüfanweisungen. Auch diese Norm bedient sich der Qualitätsmerkmale der DIN 66272.[301]

- *Zertifikate nach ISO 9241*: Die Norm „Ergonomie der Mensch-System-Interaktion" gibt Richtlinien zur Interaktion zwischen Mensch und Computer. Dazu werden Anforderungen an Peripheriegeräte und Software gegeben, um den Benutzern von IT-Anwendungen das Arbeiten zu erleichtern.[302]

- *Zertifikate nach DIN ISO/IEC 12119*: Diese Norm trägt den Titel „Software-Erzeugnisse – Qualitätsanforderungen und Prüfbestimmungen" und bestimmt, ausgehend von den sechs Softwarequalitätsmerkmalen der DIN 66272, Anforderungen an ein Softwareprodukt. Des Weiteren legt die Norm das Prüfverfahren auf Erfüllung der Anforderungen fest.[303]

[296] Vgl. Bell (2009), S. 47.
[297] Normen und Standards des TÜV Rheinland befinden sich auf der Internetseite: http://www.tuv.com.
[298] Normen und Standards des TÜV Süd befinden sich auf der Internetseite: http://www.tuev-sued.de.
[299] Vgl. Eicker, Hegmanns & Malich (2007), S.11.
[300] Vgl. Hohler & Villinger (1998), S. 67.
[301] Siehe http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=37457.
[302] Siehe http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=38896.
[303] Vgl. Hohler & Villinger (1998), S. 66.

6.3 Ausgewählte Zertifikate für IT-Anwendungen

6.3.1 Zertifizierung nach Common Criteria, DIN ISO/IEC 15408

Zur Zertifizierung der Sicherheit von IT-Produkten stellen die „Common Criteria for Information Technology Security Evaluation“ international anerkannte Kriterien bereit. Im Softwarebereich sind z. B. Datenbanken, Firewalls, Betriebssysteme, PC-Sicherheitsprodukte sowie VPN-Produkte typische Produktklassen, die zertifiziert werden. Besondere Risiken, die mit den Common Criteria abgedeckt werden, stellen die Bedrohungen von Vertraulichkeit und Integrität digitaler Dokumente sowie die Verfügbarkeit von Dienstleistungen dar. Dabei bestehen die Common Criteria aus drei Teilen.[304]

Im ersten Teil (Einführung und allgemeines Modell) der Common Criteria werden Geltungsbereiche sowie Grundlagen der IT-Sicherheitsevaluation erläutert. Zudem werden sogenannte Schutzprofile (Protection Profiles) und Sicherheitsvorgaben (Security Targets) für das zu prüfende Produkt, auch Evaluationsgegenstand genannt, beschrieben.

Der zweite Teil (Funktionale Sicherheitsanforderungen) beinhaltet einen umfangreichen Katalog von Funktionalitätsanforderungen. Dieser Katalog stellt ein empfohlenes Angebot zur Beschreibung der Produktfunktionalität dar, jedoch kann von diesem Angebot unter Begründung abgewichen werden.

Im dritten Teil (Anforderungen an die Vertrauenswürdigkeit) sind Prüfaufwand, -genauigkeit und -tiefe aufgelistet. Es ist bei einer Prüfung stets wichtig, dass ein Evaluationsergebnis auf einem Vertrauenswürdigkeitspaket (dies kann beispielsweise eine Vertrauenswürdigkeitsstufe sein) basiert.[305]

Die Common Criteria bieten zur Prüfung sieben verschiedene Stufen an (Vertrauenswürdigkeitsstufen (EAL), vgl. Tabelle 6.2). Je höher eine Prüfstufe ausfällt, desto größer sind der Umfang und die Tiefe der Prüfung. Im kommerziellen Umfeld finden üblicherweise die Stufen EAL1 bis EAL4 Verwendung.

[304] Vgl. BSI (2009), S.12.
[305] Vgl. BSI (2009), S.12.

CC EAL	Bedeutung
EAL1	Funktionell getestet
EAL2	Strukturell getestet
EAL3	Methodisch getestet und überprüft
EAL4	Methodisch entwickelt, getestet und durchgesehen
EAL5	Semiformal entworfen und getestet
EAL6	Semiformal verifizierter Entwurf und getestet
EAL7	Formal verifizierter Entwurf und getestet

Tab. 6.2: Sieben Vertrauenswürdigkeitsstufen der CC[306]

Common Criteria (CC)-Prüfungen werden durch eine international abgestimmte Methodologie („Common Methodology for Information Security Evaluation“ (CEM)) in vergleichbarer Weise durchgeführt.[307] Es wird mit den CC keine Überprüfung von IT-Produkten definiert, sondern eine gemeinsame Basis für die Bewertung mittels elf Funktionsklassen (Zweiter Teil der CC, Funktionale Sicherheitsanforderungen) festgelegt. Das Ziel der CC ist somit eine vergleichbare Überprüfung, und damit Zertifizierung, von IT-Produkten, wobei die Vertrauenswürdigkeitsstufen zur Prüfung von Funktionsklassen unterschiedlich wählbar sind. Diese Funktionsklassen beschreiben die für ein Produkt sicherheitsrelevanten Vorgänge und sind „allgemeine Grundfunktion der Sicherheitsarchitektur eines zu zertifizierenden Produktes bzw. einer Produktklasse wie z. B. der Schutz der Benutzerdaten, die Privatsphäre, Kommunikation oder Sicherheitsprotokollierung“.[308] Jede Funktionsklasse der CC ist bei einer Prüfung getrennt und in einer bestimmten Vertrauenswürdigkeitsstufe zu bewerten, jedoch muss nicht jede Funktionsklasse bewertet werden.

Eine Sicherheitsbewertung wird daraufhin durch Schutzprofile ermöglicht. Schutzprofile stellen Dokumente von Anwendern dar, wobei die Anwender auf Basis der elf Funktionsklassen Sicherheitsbedürfnisse formal beschreiben und daraufhin registrieren können. Schutzprofile sind also produktunabhängige Sicherheitserwartungen von Anwendern, mit denen Sicherheitsanforderungen an ganze Kategorien von IT-Produkten und IT-Systemen definiert werden können, ohne auf konkrete Implementierung Bezug zu nehmen. Herstellern werden diese Schutzprofile als Produktvorgaben bereitgestellt. Gegen ein aus den Schutzprofilen konkretisiertes Sicherheitsziel können daraufhin Evaluationen von Produkten auf den unterschiedlichen Vertrauenswürdigkeitsstufen durchgeführt werden. Schutzprofile werden somit halbstandardisiert für Sicherheitsbedürfnisse von IT-Anwendungen erstellt. Indem die Schutzprofile der CC für bestimmte Bereiche eine nötige Mindestsicherheit konkretisieren, kann der Produktstandard (mittelbar) eine rechtliche Wirkung entfalten.[309] Die für Produktklassen definierten Schutzprofile stellen Normierungen für die

[306] Vgl. Hermann (2003), S. 180 ff.
[307] Vgl. BSI (2009), S.13.
[308] Spindler (2007), S. 69.
[309] Vgl. Spindler (2007), S. 68 f.

jeweiligen Produktklassen dar und dienen als Orientierung für die Pflichtenbestimmung. Sie dienen und wirken als Mindestanforderungen an alle Produkte, die die in den Schutzprofilen enthaltenen Ziele erfüllen sollen. Damit kommt dem Standard eine sehr hohe Bedeutung hinsichtlich der Sicherheitserwartungen im Verkehr zu. Er ist Pflichtvoraussetzung für viele Anwendungen im Hochsicherheitsbereich.[310]

Auf Veranlassung des Herstellers oder eines Vertreibers kann eine CC-Zertifizierung eines Produktes durchgeführt werden. Die Prüfung selbst wird von anerkannten Prüfstellen des Bundesamts für Sicherheit in der Informationstechnik durchgeführt, der Antragsteller kann die Prüfstelle aus der Prüfstellenliste des BSI[311] selbst wählen. Dabei ist die Dauer eines Zertifizierungsverfahrens abhängig von der gewählten Prüftiefe (EAL-Stufe) für die jeweilige Funktionsklasse. Alle Ergebnisse eines Zertifizierungsverfahrens werden in einem Zertifizierungsreport festgehalten. In diesem Report, der auch das Sicherheitszertifikat sowie den detaillierten Zertifizierungsbereich enthält, finden sich vor allem Einzelheiten zur Bewertung des Produktes sowie Hinweise und gegebenenfalls Auflagen für den Anwender.[312]

Die an einem Zertifizierungsprozess beteiligten Parteien sind also auf der einen Seite der Antragsteller bzw. Hersteller des Produktes und auf der anderen Seite die Prüfstelle sowie die BSI-Zertifizierungsstelle. Der Antragsteller beantragt zunächst eine Zertifizierung bei einer Zertifizierungsstelle des BSI. Daraufhin muss er der Zertifizierungsstelle das zu zertifizierende Produkt mit den erforderlichen Nachweisen bereitstellen, um im positiven Fall nach der Evaluierung das BSI-Sicherheitszertifikat sowie den Zertifizierungsreport zu erhalten. Die Prüfstelle ist für die Prüfung des Produktes gemäß des Regelwerkes der CC zuständig.[313] Nach der Prüfung müssen die Prüfresultate an die BSI-Zertifizierungsstelle und den Hersteller übergeben werden. Die BSI-Zertifizierungsstelle begleitet alle bei Prüfstellen stattfindenden Prüfungen und muss den Zertifizierungsreport erstellen. Natürlich wird vom BSI auch das Zertifikat vergeben. Sofern der Hersteller sein Einverständnis gibt, kann das BSI den erstellten Zertifizierungsreport sowie das vergebene Zertifikat auf der BSI-Webseite veröffentlichen. Außerdem hat das BSI bei allen Fragen des Herstellers bzgl. der Zertifizierung eine beratende Funktion und unterstützt den Hersteller bei der Erarbeitung von Sicherheitsvorgaben.[314]

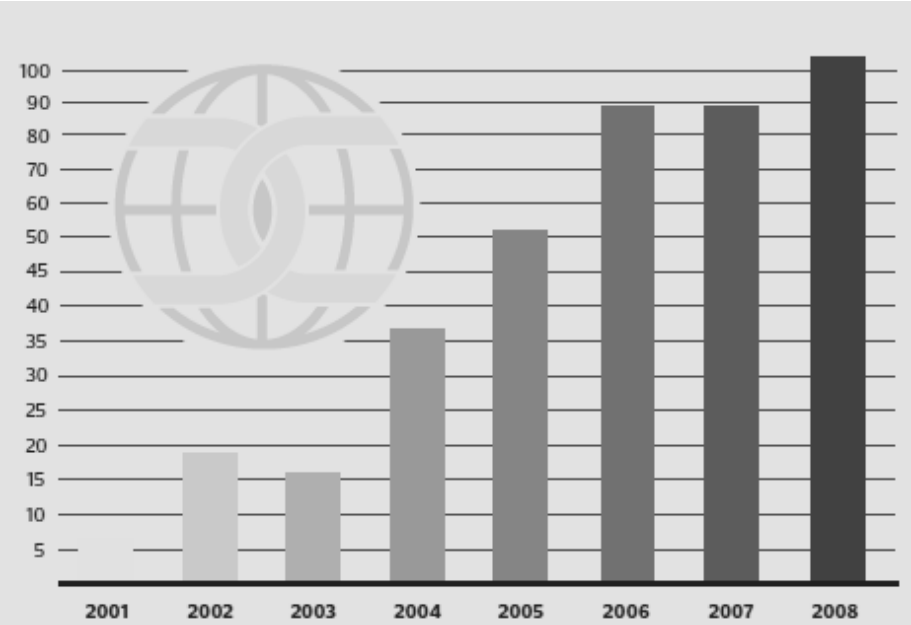
Jedes vergebene CC-Zertifikat bezieht sich nur auf die zertifizierte Produktversion. Es bestätigt die Produkt-Vertrauenswürdigkeit gemäß den zum Zeitpunkt der Ausstellung vor-

[310] Vgl. Schwögler (2008), S. 1 f.
[311] Einzusehen sind sämtliche Prüfstellen auf der Internetseite des BSI: https://www.bsi.bund.de.
[312] Vgl. BSI (2009), S.14.
[313] Einzusehen ist das Regelwerk der Common Criteria unter: http://www.commoncriteriaportal.org.
[314] Vgl. BSI (2009), S.15.

handenen Sicherheitsvorgaben. Um Angriffe auf das Produkt dauerhaft abwehren zu können, besteht die Möglichkeit einer regelmäßigen Überprüfung der Widerstandsfähigkeit im Rahmen eines Assurance Continuity-Programms des BSI. Sollten sich Änderungen an dem IT-Produkt ergeben, so kann die Gültigkeit eines Zertifikates aufrecht erhalten werden, indem der Antragsteller eine Re-Zertifizierung oder ein Maintenance-Verfahren beantragt.

Auch in Rechtsschriften finden die CC häufig Anwendung. Es existieren Verordnungen, in denen die CC als Anforderungen an IT-Anwendungen genannt werden. So befindet sich beispielsweise in der Fahrpersonalverordnung (FPersV) eine Anlage (2) zu § 3, Zertifizierungsinfrastruktur, in der unter R5.10 die Sicherheitsanforderung Common Criteria EAL 4 an das PIN-Kartensystem für einen elektronischen Fahrtenschreiber gestellt ist.

Die aktuelle Common Criteria DIN ISO/IEC 15408 Version ist die Version 3.1. Dabei setzen sich die CC aus dem „Orange-Book (TCSEC)“ der USA, den kanadischen Kriterien (CTCPEC) sowie dem europäischen Standard „Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC)“ zusammen.[315] Produkte, die eine CC-Zertifizierung haben, finden sich auf der offiziellen Webseite des Standards.[316] Auch wird die Anzahl der durch das BSI vergebenen CC-Zertifikate pro Jahr angegeben (vgl. Abb. 6.2). Ebenfalls sind Schutzprofile für bestimmte Produktklassen auf dieser Webseite einzusehen.[317]



Quelle: BSI (2009), S. 19.

Abb. 6.2: BSI-Zertifikate nach Common Criteria

[315] Vgl. BSI (2009), S.13.
[316] Produkte mit CC Zertifizierung: http://www.commoncriteriaportal.org/products.html.
[317] CC Schutzprofile für Produktklassen: http://www.commoncriteriaportal.org/pp.html.

6.3.2 Zertifizierung nach DIN EN ISO 9000 ff.

Eine Zertifizierung des Qualitätsmanagements ist durch die Standards DIN EN ISO 9000 ff., insbesondere ISO 9001, möglich. Da ein Softwarezertifikat dieser Normreihe eine deutliche Aussagekraft hinsichtlich des Softwareerstellungsprozesses eines Produktes hat, kann es im abgesteckten Rahmen Einfluss auf Sicherheitserwartungen des Verkehrs nehmen. Der Einfluss dieses Standards ist deswegen abgesteckt, da die Normen für eine Haftung nach § 823 Abs. 1 BGB nur im Kontext B2B und im Wesentlichen beim Kauf von Individualsoftware herangezogen werden kann. Außerdem stellt der Standard nur Anforderungen an das Softwareproduktionsverfahren und nicht an die Sicherheit eines Softwareproduktes. Software ist aufgrund ihrer Komplexität praktisch nicht fehlerfrei zu implementieren. Das Qualitätsmanagement und insbesondere die Normen DIN EN ISO 9000 ff. zielen darauf ab, ein Softwareprodukte möglichst fehlerarm und hochwertig zu erstellen. Dabei dient die Zertifizierung der Einhaltung von Qualitätsstandards.[318] Die Normreihe DIN EN ISO 9000 ff. besteht in ihrer überarbeiteten Fassung ISO 9000:2000 aus den einzelnen Normen DIN EN ISO 9000, 9001 und 9004.

Um Softwareprodukte fehlerarm zu implementieren, wird sich bei IT-Projekten verschiedener Softwaretestverfahren bedient. Während der Implementierung von Individualsoftware wird dabei dafür plädiert, vertragliche Regelungen zwischen den Vertragspartnern hinsichtlich der Dauer und Art eines Abnahmeverfahrens zu treffen. Dadurch kann ständig eine vertraglich vereinbarte Beschaffenheit sichergestellt werden. Um Fehlschläge bei IT-Projekten zu vermeiden, sind Softwaretestverfahren ein unabdingbarer Bestandteil der Qualitätssicherung nach DIN EN ISO 9000 ff. Juristen beziehen die Testverpflichtungen zur vertragsgemäßen Erfüllung im Sinne der §§ 438 Abs. 2, 640 BGB und § 377 HGB lediglich auf die Phase der Abnahme. Beim Erstellen von Individualsoftware ist es darum sinnvoll, alle Entwicklungsphasen der Software mit den dazugehörigen Tests in dem Projektvertrag zu erfassen.[319]

Die Norm ISO 9000 beschreibt Grundlagen für Qualitätsmanagementsysteme und klärt Begrifflichkeiten zum Thema Qualität und Qualitätsmanagement. Sie gibt einen Überblick über Verantwortlichkeiten und qualitätsbezogene Ziele, die von einer Organisation erfüllt und festgeschrieben werden sollten. Außerdem enthält die Norm weitere Abschnitte zur Beurteilung von Qualitätsmanagement-Systemen und zum Nutzen der Dokumentation des Systems.[320]

[318] Vgl. Spindler (2007), S. 74 f.
[319] Vgl. Hoeren & Spittka (2009).
[320] Vgl. Brauer (2002), S. 12; Esch et al. (2006), S. 132.

Eine zentrale Bedeutung für ein Qualitätsmanagement-System kommt der Norm DIN EN ISO 9001 zu. Muss eine Organisation nach außen den Nachweis erbringen, dass sie Produkte bereitstellt, die Kundenforderungen sowie behördliche Forderungen erfüllen, so legt diese Norm die Nachweisforderungen an ein Qualitätsmanagement-System fest. Sie enthält Hinweise und Forderungen zum Aufbau eines normkonformen Qualitätsmanagement-Systems. Zudem erläutert sie Möglichkeiten, wie Normforderungen ausgeschlossen werden können, falls diese nicht die Qualität des erzeugten Produktes betreffen.[321]

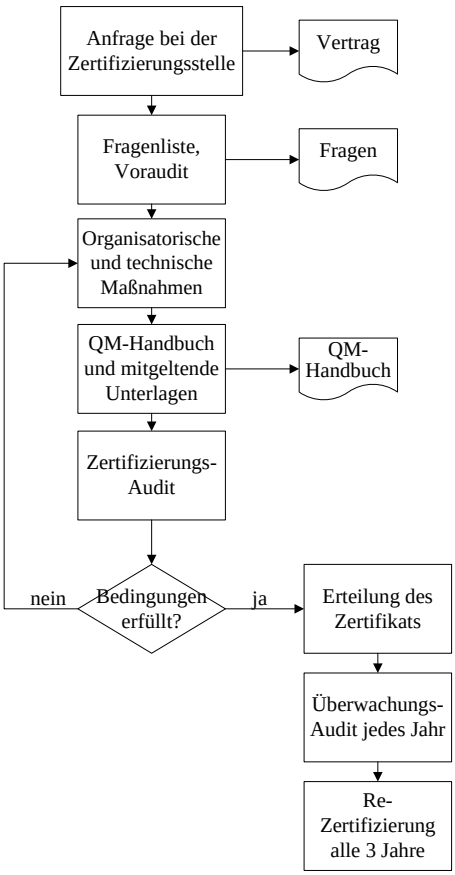
Zur Betrachtung der Wirksamkeit und Wirtschaftlichkeit eines Qualitätsmanagement-Systems wird ein Leitfaden in der Norm DIN EN ISO 9004 bereitgestellt. Trotz unterschiedlicher Anwendungsbereiche ist diese Norm zusammen mit ISO 9001 als konsistentes Paar entwickelt worden. Ihr Ziel ist die Verbesserung der Kundenzufriedenheit, der Zufriedenheit anderer Parteien wie z. B. Umweltverbände und Behörden sowie der Leistungsverbesserung der Organisation. Da die ISO 9004 oftmals als Leitfaden zur Leistungsverbesserung über die Forderungen der ISO 9001 herangezogen wird, ist sie nicht für Zertifizierungszwecke vorgesehen. Eine Zertifizierung wird ausschließlich auf Basis der ISO 9001 vorgenommen.[322]

Der Beschluss zur Einführung eines Qualitätsmanagement-Systems wird üblicherweise von der Geschäfts- oder Unternehmensleitung getroffen. Die Leitung muss dabei gleichzeitig einen Qualitätsmanagement-Beauftragten ernennen, dessen Hauptaufgabe die Einführung und spätere Pflege des Systems ist. Desweiteren muss die Leitung qualitätsbezogene Unternehmensziele in Form einer Qualitätspolitik festlegen. Um die Qualitätsziele zu erreichen, muss sich jeder Mitarbeiter, der an dem Herstellungsprozess des Produktes beteiligt ist, mit den Zielen des Unternehmens identifizieren. Der Grund hierfür ist, dass mit der Einführung eines Qualitätsmanagement-Systems häufig Veränderungen in den Arbeitsabläufen der Mitarbeiter einhergehen. Außerdem müssen die Unternehmensziele verständlich formuliert sein, was eine für das Unternehmen passende Definition des Qualitätsbegriffes sowie der Qualitätspolitik voraussetzt.[323]

Nachdem ein Qualitätsmanagement-System erfolgreich in einem Unternehmen eingeführt wurde, kann dieses zertifiziert werden (vgl. Abb. 6.3). Zur Zertifizierung nach ISO 9001 muss zunächst ein Antrag auf Zertifizierung an eine staatlich anerkannte Zertifizierungsstelle gestellt werden. Durch einen Vertragsabschluss verpflichtet sich die Zertifizierungsstelle zur Begleitung des Unternehmens durch das Zertifizierungsverfahren. Zusätzlich sollte ein Unternehmen, parallel zum Zertifizierungsvorgang, auch beraten werden. Diese

[321] Vgl. Brauer (2002), S. 12 ff.; Esch et al. (2006), S. 132.
[322] Vgl. Brauer (2002), S. 12 ff.; Esch et al. (2006), S. 132.
[323] Vgl. Brauer (2002), S. 14 f.

Beratung kann allerdings nicht von der Zertifizierungsstelle selbst, sondern ausschließlich von Dritten vorgenommen werden: Selbstprüfungen werden bei der ISO 9001 Zertifizierung von Qualitätsmanagement-Systemen nicht angewendet.[324]



In Anlehnung: Brauer (2002), S. 38.

Abb. 6.3: Schema der Zertifizierung eines Qualitätsmanagement-Systems nach DIN EN ISO 9001

Das eigentliche Zertifizierungsaudit wird zur Prüfung der im Qualitätsmanagement-Handbuch sowie in anderen Unterlagen dokumentierten Verfahren eingesetzt. Die dabei zu Grunde liegende Zertifizierungsnorm ist die DIN EN ISO 9001. Während des Zertifizierungsaudits werden alle Bestandteile des Qualitätsmanagement-Systems und alle Prozesse stichprobenartig geprüft. Zur Prüfung wird eine umfangreiche Audit-Fragenliste der Zertifizierungsstelle verwendet. Die Audit-Fragenliste muss dabei alle Forderungen der Norm erfüllen. Alle gefundenen Schwachstellen werden während der Zertifizierung in Abweichungsberichten festgehalten und anschließend mit dem Unternehmen besprochen. In diesen Berichten wird zwischen nicht-kritischen und kritischen Abweichungen differenziert, wobei alle kritischen Abweichungen vor der Zertifizierung durch die Zertifizierungsstelle

[324] Vgl. Brauer (2002), S. 37.

behoben werden müssen. Für nicht kritische-Abweichungen muss eine Frist von sechs Monaten zur Behebung der Schwachstelle eingehalten werden.[325]

Insbesondere bei der Vergabe von Projekten, seien es IT-Projekte zur Implementierung von Individualsoftware oder andere öffentliche Ausschreibungen, wird häufig eine ISO 9001-Zertifizierung als Nachweis der fachlichen Eignung verlangt. Ähnlich wie die Common Criteria finden auch die Qualitätszertifizierung nach ISO 9001 häufig in Rechtsschriften Verwendung, um Produktqualität vorauszusetzen. Im Europarecht gelten beispielsweise Verordnungen zur Festlegung der qualitativen Anforderungen an Luftfahrtdaten und Luftfahrtinformationen für den einheitlichen europäischen Luftraum. Begründet ist dies im Verkehrs- und Verbraucherschutz. Anforderungen an das Qualitäts-, Sicherheits- und Gefahrenabwehrmanagement, die in Artikel 10 der Verordnung (EU) Nr. 73/2010 genannt wurden, können durch eine ISO 9001-Zertifizierung nachgewiesen werden (Anhang 7 der Verordnung).

[325] Vgl. Brauer (2002), S. 39 f.

III Forschungsausblick

7 Forschungsprojekte in der Rechtsinformatik und im Informationsrecht

Fabian Kohl

7.1 Rechtsinformatik und Informationsrecht als Untersuchungsgegenstand

Rechtsinformatik und Informationsrecht sind zwei wissenschaftliche Disziplinen, die historisch und fachlich eng miteinander verbunden sind. Die Rechtsinformatik entstand vor dem Hintergrund des zunehmenden Einsatzes von Informationstechnik in Wirtschaft und Verwaltung.[326] Etwa zur gleichen Zeit entwickelte sich die Disziplin des Datenschutzrechts, welches später als Rechtsgebiet in das Informationsrecht eingeordnet wurde.[327] Die Entwicklung in den folgenden Jahrzehnten hat dazu geführt, dass die Rechtsinformatik heute eine Form der angewandten Informatik ist. Das Informationsrecht gilt hingegen als eine rechtswissenschaftliche Querschnittsdisziplin. Prägend für die Rechtsinformatik und das Informationsrecht sind ihre Interdisziplinarität, welche sich in der Rechtsinformatik eher fachrichtungsübergreifend darstellt, sich im Informationsrecht dagegen über mehrere Teildisziplinen erstreckt. Die Bedeutung der Rechtsinformatik und des Informationsrechts für zukünftige Entwicklungen ist dabei unbestritten.[328] Dies macht es umso wichtiger, eine breit aufgestellte Übersicht über Akteure, Ergebnisse und Verteilungen der heutigen Forschungslandschaft zu erlangen.

Im Folgenden wird eine Forschungslandkarte der Universität Münster vorgestellt, die ein strukturiertes Speichern und Auffinden von Forschungsergebnissen der Rechtsinformatik und des Informationsrechts unterstützt. Um Inhalte für die Forschungslandkarte zu erzeugen, wurde eine systematische Recherche durchgeführt, deren Konzeption und Umsetzung ausführlich erläutert wird. Abschließend wird mit Hilfe der Forschungslandkarte die aktuelle Forschungssituation charakterisiert und eine Bewertung vorgenommen.

7.2 Forschungslandkarte

Die Interdisziplinarität der Rechtsinformatik und des Informationsrechts erschwert es den beteiligten Akteuren, sich einen Überblick über die aktuelle Forschungssituation zu verschaffen. Die daraus resultierende fehlende Übersicht bringt negative Effekte mit sich. So kann es zu Doppelforschung kommen, wenn zwei Forschungsakteure keine Kenntnis voneinander haben. Gleichzeitig wird vorhandenes Synergiepotential nicht ausgeschöpft, da

[326] Vgl. Lenk et al. (1997), S. 3 nach Knackstedt al. (2010), S. 1.
[327] Vgl. hier und im Folgenden Knackstedt et al. (2010), S. 3.
[328] Vgl. Pallas (2008), S. 2

mögliche Partner nichts voneinander wissen. Um diese negativen Effekte zu unterbinden, wurde die Forschungslandkarte „Rechtsinformatik und Informationsrecht“ entwickelt.[329] Sie basiert auf dem Referenzmodell von KNACKSTEDT ET AL. (2009)[330], nutzt die Ontologie für Forschungscommunities von SURE ET AL. (2005)[331] und den europäischen Datenaustauschstandard für Forschungsinformationen CERIF[332]. Die Forschungslandkarte ist als soziales Netzwerk aufgebaut, wird also durch die Nutzer befüllt. Das automatisierte Aufbauen der Datenbank durch Metadaten-Harvesting, das viele, aber heterogene Daten bereitstellt, wurde hier bewusst nicht gewählt. Vielmehr ist für die Forschungslandkarte die Qualität der Daten vorrangig.[333]

Dabei können Daten aus verschiedenen Bereichen eingepflegt werden:

- Forschungseinrichtungen, universitär wie auch außeruniversitär, werden als Organisation eingetragen.
    - Innerhalb der Organisationen werden Forschungsprojekte durchgeführt, welche ebenfalls separat eingepflegt werden können.
    - Das primäre Artefakt der Forschungslandkarte stellt das Forschungsergebnis dar. Es repräsentiert die Erkenntnisse einzelner Projekte.
    - Zur weiteren Beschreibung der Forschungsergebnisse besteht die Möglichkeit, Publikationen einzugeben und auf die zugehörigen Ergebnisse zu verweisen.

Über die reine Datenhaltung hinaus stellt das Forschungsportal vielfältige Funktionen bereit:

- Die verschiedenen Daten werden untereinander verknüpft. So können beispielsweise jederzeit über die Auswahl einer Organisation die zugeordneten Forschungsergebnisse eingesehen werden.
- Eine Suchfunktion, die sowohl auf Bezeichnungsfeldern als auch auf Freitexten agiert, erleichtert den Zugang zu relevanten Informationen.
- Die Forschungsergebnisse können sowohl in einem Freitext als auch über ein Klassifizierungssystem differenziert beschrieben werden.

[329] Siehe http://www.foka-riir.de.
[330] Vgl. Knackstedt et al. (2009) nach Knackstedt et al. (2010), S. 4.
[331] Vgl. Sure, et al. (2005) nach Knackstedtet al. (2010), S. 4.
[332] http://www.eurocris.org.
[333] Vgl. Knackstedtet al. (2010), S. 4.

- Um den Gedankenaustausch unter den Wissenschaftlern weiter zu fördern, bietet die Forschungslandkarte außerdem Wiki-Funktionen an.

- Durch den Einsatz der Open-Source-OLAP-Servers Mondrian334 können über die Forschungslandkarte statistische Analysen vorgenommen werden. Darüber hinaus gibt eine Heatmap (siehe Abb. 7.1) einen schnellen Überblick über Forschungsakteure und -schwerpunkte.

Gerade die Möglichkeit, die Forschungsergebnisse strukturiert zu klassifizieren, stellt eine der Stärken der Forschungslandkarte dar. Die folgenden Auswertungskategorien werden aktuell unterstützt:

- Forschungsergebnistyp (Aufsätze, Dissertationen, Gutachten, Handbücher/Monografien, rechtliche Kommentare, technische Umsetzungen, Modelle, Konzepte, Theorien und empirische Untersuchungen),

- Anwendungsbranche (branchenübergreifend, Chemie, Finanzdienstleistungen, Gesundheitswesen, Interorganisationssysteme, Öffentliche Verwaltung etc.),

- Anwendungsfokus (unternehmensintern, B2B, B2C etc.),

- Adressiertes Fachgebiet (Datensicherheit, Informationsrecht, Rechtsinformatik etc.),

- Praxiseinsatz (1-5, 6-10, >10 Praxiseinsätze, bisher nicht im Einsatz etc.),

- Realisationsgrad (Entwicklung abgeschlossen, in Entwicklung etc.),

- involvierte Rechtsgebiete (Öffentliches Recht, Strafrecht, Zivilrecht etc.). [335]

[334] http://www.mondrian.de.
[335] Vgl. Knackstedt et al. (2010), S. 5.

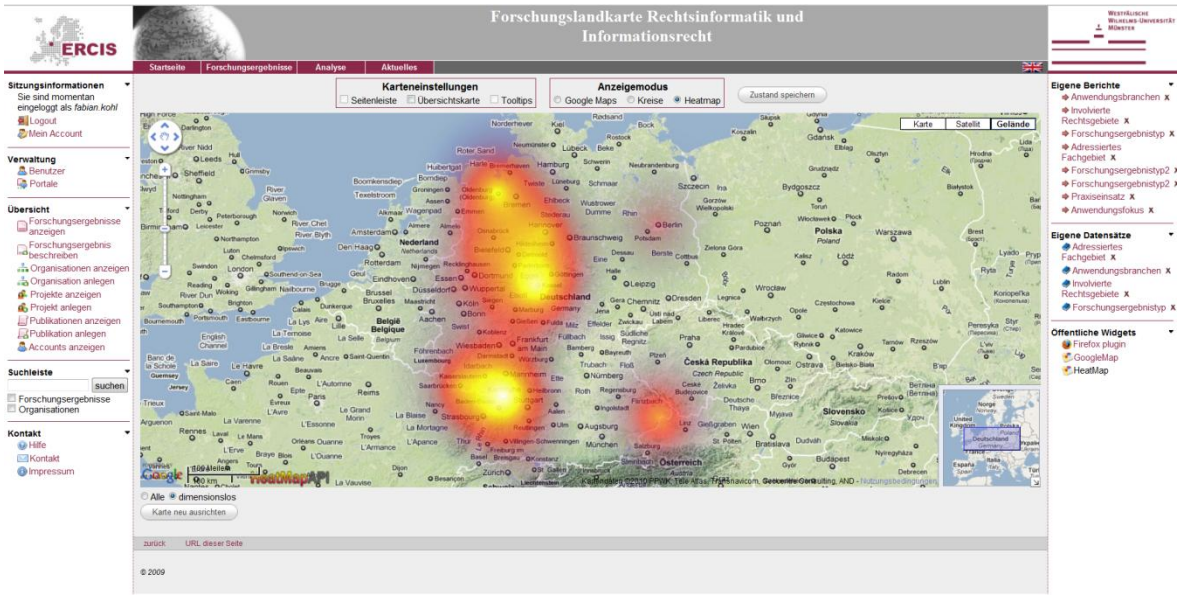


Abb. 7.1: Screenshot der Forschungslandkarte Rechtsinformatik und Informationsrecht

7.3 Recherche

7.3.1 Vorgehen

Das Forschungsfeld der Rechtsinformatik und des Informationsrechts ist sehr vielschichtig und wenig übersichtlich. Durch die interdisziplinäre Ausrichtung können Forschungsprojekte in verschiedenen Fachrichtungen entstehen. Forschungsprojekte und -ergebnisse allein über die proprietären, universitären Informationssysteme umfassend zu identifizieren, ist eine sehr zeit- und ressourcenintensive Vorgehensweise. Teilweise stehen solche Systeme gar nicht zur Verfügung. Eine Suche über allgemeine Zeitschriftendatenbanken deckt nicht das ganze Spektrum der Forschungslandschaft ab. Aufgrund dieser Problemstellungen ist für die vorliegende Recherchearbeit ein anders strukturierter Ansatz gewählt worden, der andere Quellen als Suchgrundlage nutzt. Die Leitfragen für die Lokalisation dieser Recherchegebiete waren dabei:

- Wer finanziert eine mögliche Forschung?
- Wo tauschen sich Forscher aus?
- Gibt es eventuell Organisationen oder Verbände, die sich auch mit dem Thema befassen?

Abgeleitet aus diesen Fragen ergaben sich die Recherchefelder Geldgeber, Fachkonferenzen und -zeitschriften und Organisationen. Geldgeber für Forschungen aller Art ist in

Deutschland die Deutsche Forschungsgemeinschaft (DFG), die 2008 ein Fördervolumen von 2,65 Milliarden € hatte[336], und das Bundesministerium für Bildung und Forschung (BMBF) mit einem Etat von 10,9 Milliarden € für das Jahr 2010[337]. Bei beiden ist die Suche nach geförderten Projekten aufgeteilt. Die DFG unterhält zum einen eine Datenbanksuche für Forschungsvorhaben.[338] Zum anderen stellt die DFG auch noch eine Datenbank für die Suche nach Institutionen bereit. [339] Durch das BMBF werden auch zwei verschiedene Recherchemöglichkeiten angeboten. Über den Förderkatalog lassen sich sogar mehrere ministeriale Datenbanken nach Forschungsprojekten durchsuchen. Von besonderer Bedeutung ist das Bundesministerium für Wirtschaft und Technologie. Außerdem lässt sich über eine Suchmaschine[340] nach geförderten Institutionen suchen.

Im Bereich der Konferenzen wird das Internationale Rechtsinformatik Symposium (IRIS) berücksichtigt. Es findet bereits seit 1998 statt und dient als Austauschplattform für verschiedene Forschungsrichtungen. Doch auch auf den Konferenzen aus dem Bereich der Wirtschaftsinformatik, der „Multikonferenz Wirtschaftsinformatik“ und der „Internationalen Konferenz Wirtschaftsinformatik“, werden Beiträge zu Themen der Rechtsinformatik und des Informationsrechts veröffentlicht. Des Weiteren gibt es Fachkonferenzen, die sich mit dem Thema der rechtssicheren Archivierung beschäftigen. Auf dem deutschen EDV-Gerichtstag in Saarbrücken wird jedes Jahr der Dieter Meurer Förderpreis vergeben. Er zeichnet Arbeiten mit rechtsinformatischem und informationsrechtlichem Hintergrund aus.

Bei den Organisationen sei zuerst die Gesellschaft für Informatik genannt. Zu ihr gehört der Fachbereich der Informatik in Recht und öffentlicher Verwaltung, in dem sich der Fachausschuss der Rechtsinformatik befindet. Innerhalb des Ausschusses gibt es Fachgruppen zu den Themengebieten Informationsrecht, juristische Informationssysteme und Rechtsfragen der e-Wirtschaft und des Internets. Einige der Fachgruppen sind hier noch im Aufbau begriffen. Der Informationsdienst der Wissenschaft ist ein digitales Veröffentlichungsorgan, welches Pressemitteilungen der angeschlossenen Mitgliedseinrichtungen einem breiten Publikum zugänglich macht. Mitglieder sind momentan 800 Institutionen sowie 45.000 Abonnenten. Derzeit sind ca. 180.000 Pressemitteilungen auf der Webseite verfügbar.[341] Eine weitere Organisation ist das Unabhängige Landeszentrum für Datenschutz Schleswig Holstein. Es unterstützt zusammen mit universitären Einrichtungen verschiedene Forschungsprojekte.

[336] Vgl. Döben et al. (2008), S. 153.
[337] Bundesministerium für Bildung und Forschung (2010).
[338] http://gepris.dfg.de/gepris/OCTOPUS/.
[339] http://research-explorer.dfg.de/research_explorer.de.html.
[340] http://www.forschungsportal.net/.
[341] http://idw-online.de/de/idwnews.

Bei den Fachzeitschriften finden sich zwei Zeitschriften, die ausschließlich digital erscheinen. Als Recherchequelle bietet sich dabei vor allem JurPC[342] an. JurPC ist eine Internet-Zeitschrift für Rechtsinformatik und Informationsrecht und erscheint bereits seit 1989. Herausgegeben wird sie von Maximilian Herberger, Professor an der Universität Saarbrücken und Vorsitzender des EDV-Gerichtstages. Das Journal of Intellectual Property, Information Technology and E-Commerce Law, kurz JIPITEC[343], ist eine einschlägige, allerdings noch recht junge Zeitschrift..[344]

Zur Konkretisierung der Suche in Datenbanken wurde eine Schlagwortliste mit den folgenden Begriffen genutzt:

- Rechtsinformatik,
- Informationsrecht,
- Recht,
- Computer,
- IT,
- Jura,
- Modellierung,
- Zertifizierung,
- Rechtsautomat.

Darüber hinaus wurden bei den großen Geldgebern, also dem Bundesministerium für Bildung und Forschung und der Deutschen Forschungsgemeinschaft, auch direkt über bereits bekannte Institutionen nach Projekten gesucht. Tabelle 7.1 dient als Logbuch für die Recherche. Ihr ist zu entnehmen, welche Bereiche untersucht wurden, und sie zeigt Potentiale für die Erweiterung der Suche auf.

[342] http://www.jurpc.de.
[343] http://www.jipitec.eu/.
[344] Eine Übersicht über Fachzeitschriften zum Thema Informationsrecht findet sich z. B. bei Hoeren (2010), S. 22f.

Recherchefeld	Bezeichnung	Konkretisierung der Suche
Geldgeber	DFG	Schlagwortliste, Institutionen
	BMBF	Schlagwortliste, Institutionen
	Deutsche Stiftung für Recht und Informatik	Schlagwortliste
Konferenzen	Internationales Rechtsinformatik Symposium (IRIS)	Jahrgang: 2010 (teilweise)
	Multikonferenz Wirtschaftsinformatik	Jahrgänge: 2010, 2008, 2006, 2004
	Wirtschaftsinformatik	Jahrgang: 2009
	Fachkonferenzen zur rechtssicheren Archivierung	Jahrgänge: 2005, 2007
	Fachtagung Verwaltungsinformatik und Fachtagung Rechtsinformatik	Jahrgang: 2010
	Deutscher EDV-Gerichtstag	Jahrgänge: Preisträger 2003-2009
	DSRI Herbstakademie	Programm
Organisationen	Gesellschaft für Informatik	Projekte
	Informationsdienst Wissenschaft	Schlagwortliste
	Unabhängiges Landeszentrum für Datenschutz	Projekte
	Deutsche Stiftung für Recht und Informatik	Herbstakademie, Förderpreise
Fachzeitschriften	JurisPC	Schlagwortliste
	JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law	Ausgabe

Tab. 7.1: Recherchefelder und Suchgegenstände

7.3.2 Überblick über die Ergebnisse

Nach Durchführung der Recherche[345] befinden sich in der Forschungslandkarte (Ausgangswert jeweils in Klammern):

- 92 (41) Forschungsergebnisse,
- 55 (22) Projekte,
- 55 (43) Organisationen und
- 29 (0) Publikationen.

Vor allem die Zahlen im Bereich der Forschungsergebnisse und Projekte sind gestiegen. Auch bei den Organisationen hat es noch leichte Zuwächse gegeben.

Gerade die Suche über die Geldgeber DFG und BMBF war wenig erfolgreich. Das Auffinden von neuen Forschungsprojekten über die angebotenen Recherchemöglichkeiten gestal-

[345] Stand 12.07.2010.

tete sich nicht einfach. Auch die Datenbanksuche über das BMBF verlief weitestgehend erfolglos. Nicht zu empfehlen ist momentan die Suche über den Webauftritt der Gesellschaft für Informatik, da er sich teilweise noch im Aufbau befindet. Dadurch sind manche Fachbereiche weniger bis gar nicht gepflegt worden. Etwas interessanter gestaltete sich die Suche über das IDW. Das Recherchefeld der Konferenzen lieferte sehr gute Ergebnisse. Durch die thematische Ausrichtung der Konferenzen waren die Beiträge von vornherein potentialbehaftet. Gerade über die IRIS ließen sich viele sehr unterschiedliche Ansätze identifizieren. Auch über die ausgewählten Organisationen war es teilweise möglich, neue Ergebnisse zu sammeln. Die Forschungsprojekte des Unabhängigen Landeszentrums für Datenschutz Schleswig Holstein waren nicht sehr zahlreich, dafür thematisch passgenau. Bei den Fachzeitschriften war eine richtige Recherche nur bei JurPc möglich. Hier finden sich Beiträge aus verschiedenen Fachrichtungen, wodurch die Suche im Archiv der Zeitschrift teilweise neue Ansätze liefert.[346]

Als Beispiele für die identifizierten Forschungsergebnisse werden drei Forschungsergebnisse aus den Bereichen (Wirtschafts-)Informatik, der Sprachforschung und der Rechtswissenschaft vorgestellt, die aufgrund ihrer Zugehörigkeit zu unterschiedlichen Forschungsdisziplinen die unterschiedlichen Strömungen in der Rechtsinformatik und im Informationsrecht verdeutlichen:

- Das Projekt McLaw[347] an der Universität Oldenburg wurde vom Departement für Informatik durchgeführt. Geforscht wurde dabei unter anderem nach Möglichkeiten, die Anforderungen für einen rechtsicheren Vertragsschluss auch auf mobilen Endgeräten sicherzustellen. Ein Ergebnis des Projekts ist die Entwicklung einer Methode zum automatischen Abgleich von AGB. Um einen Kaufvertrag rechtsgültig abzuschließen, bedarf es der Übermittlung der AGB an den Käufer. Aufgrund der beschränkten Größe von Handydisplays ist eine einfache textuelle Übermittlung nicht rechtens, da nicht zumutbar. Die Lösung des Projektteams sieht vor, dass der Nutzer seine ABG-Präferenzen auf einem Server abgelegt. Dort werden gleichzeitig auch die AGB der Händler gespeichert. Sollte sich nun ein Vertragsschluss anbahnen, wird über den Server ein einfacher Abgleich der Präferenzen mit den ABG des Händlers durchgeführt. Im Falle einer Übereinstimmung kann das Geschäft reibungslos abgewickelt werden. Kommt es zu Nicht-Übereinstimmungen kann der Kunde immer noch situativ entscheiden, ob er dem Geschäft trotzdem zustimmt.

- Das Department of Computal Linguistics der Universität des Saarlandes verfolgt einen sprachwissenschaftlichen Ansatz, der darauf abzielt, aus Gerichtsurteilen au-

[346] http://www.foka-riir.de/kmp/?q=node/2490.
[347] http://medien.informatik.uni-oldenburg.de/mclaw/.

tomatisch Definitionen herauszufiltern. Formal sind die gewonnenen Definitionen zwar rechtlich nicht bindend, dienen aber als Orientierung für die Rechtsprechung.[348] Als Beispiel sei hier die Definition der beweglichen Sache gemäß BGB genannt. Ob elektrischer Strom unter die Definition des BGB fällt, konnte durch ein gerichtliches Urteil[349] geklärt werden. Aufgrund der Masse an Urteilstexten liegt die Nutzung eines automatisierten Verfahrens auf der Hand, das entsprechendes Wissen nutzbar macht. Im Zuge des Verfahrens wird zuerst der Text eines Gerichtsurteils mittels eines selbst entwickelten Parsers erfasst und in XML übersetzt. Danach kann der Text auf für Definitionen typische Passagen untersucht werden. Die entdeckten Passagen werden anschließend in die Bestandteile einer Definition zerlegt. Innerhalb der erarbeiteten Definitionen können nun Suchabfragen durchgeführt werden.

- Bei Forschungsergebnissen aus den Rechtswissenschaften handelt es sich meistens um die Lösung von datenschutzrechtlichen Fragestellungen. Hierzu zählt auch die Dissertation „Vorgangsbearbeitungssysteme in der öffentlichen Verwaltung“ von LAUE.[350] Er untersucht in seiner Arbeit die rechtlichen Rahmenbedingungen und Gestaltungsanforderungen für einen generischen Prozess „Allgemeines Antragsverfahren“. Dabei werden zuerst die technischen Rahmenbedingungen und Verfahrensabläufe erarbeitet. Anschließend wird der nationale Rechtsrahmen abgesteckt. Um abschließend beides in Einklang zu bringen, bedient sich der Verfasser einer Methode zur rechtsgemäßen Gestaltung (KORA). Sie stellt sicher, dass auch auf Verfassungsniveau formulierte Gesetze als technische Anforderungen interpretiert werden können. Dabei werden in einem sukzessiven Prozess erst verfassungsrechtliche Vorgaben formuliert, aus denen rechtliche Anforderungen entstehen, die wiederum zu rechtlichen Kriterien werden. Aus den Kriterien können technische Gestaltungsziele synthetisiert werden, aus denen dann die finalen technischen Gestaltungsvorschläge formuliert werden.[351] LAUE kommt zu dem Schluss, dass rechtsgemäße Technikgestaltung möglich ist, dabei aber vor allem die rechtzeitige Einbeziehung der rechtlichen Anforderungen in den Entwicklungsprozess von hoher Bedeutung ist. Um diese Anforderungen zu definieren, liefert er mit KORA die entsprechende Methode.

[348] Vgl. Walter (2006), S. 1.
[349] Vgl. RG, IV. Strafsenat, 20.10.1896 g. W. Rep. 2609/96, RGSt. Bd. 29, S.111f..
[350] Vgl. Laue (2009), S. 37.
[351] Vgl. Laue (2009), S. 122.

7.4 Analyse der Forschungssituation

Bei der Betrachtung der Forschungslage spielen verschiedene Interessengruppen eine Rolle. Deshalb wird im Folgenden die Analyse aus drei verschiedenen Perspektiven durchgeführt. Gerade für Forscher ist die Betrachtung der Forschungssituation von primärem Interesse. Aber auch die bereits erwähnten Geldgeber sind an einem Überblick interessiert, müssen sie doch ihre vorhandenen Mittel mit Bedacht einsetzen. Als dritte Perspektive erscheinen die Nutznießer der Forschung, sprich die Praktiker, als sinnvoll. Letztendlich sind sie es, die Forschung umsetzen und ihr damit einen Teil ihrer Legitimation verschaffen. Für die folgende Betrachtung der aktuellen Forschungssituation wird auf die Daten der Forschungslandkarte und das entsprechende Analysewerkzeug zurückgegriffen.

Für den Forscher sind zahlreiche Informationen über die aktuelle Forschungslage von Interesse. Ihn treibt die Suche nach vorhandenem Wissen ebenso an wie die Aufdeckung von neuen Forschungsgebieten oder -lücken. Um diesen Informationsbedürfnissen zu begegnen, bedarf es verschiedenster Auswertungen. Zuerst liegt eine Betrachtung der adressierten Fachgebiete nahe. In der Häufigkeitsverteilung (siehe Abbildung 7.2) wird deutlich, dass die juristischen Fachgebiete, wie Informationsrecht und Datenschutz, sehr stark vertreten sind. Die klassischerweise eher der (Wirtschafts-)Informatik zuzuordnenden Fachgebiete Rechtsinformatik und Datensicherheit umfassen nur ca. ein Viertel der Forschungsergebnisse.

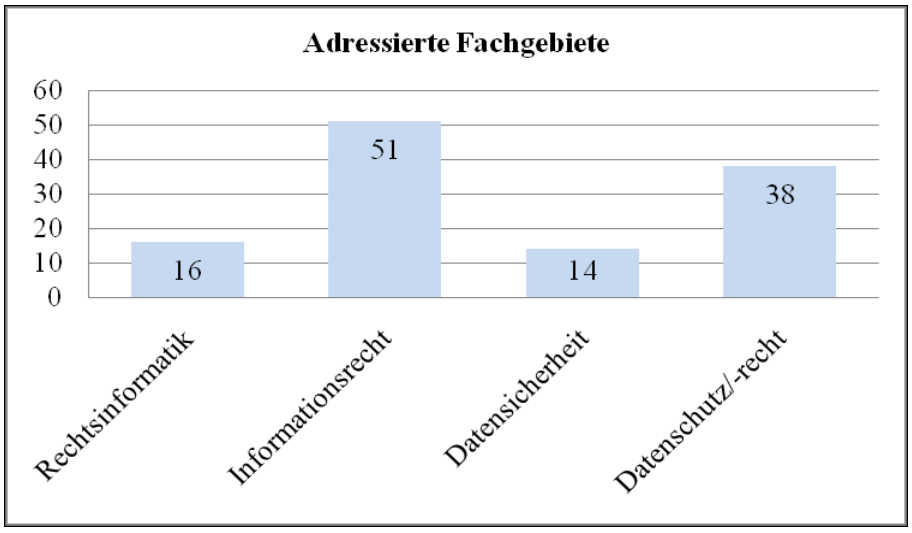


Abb. 7.2: Häufigkeitsverteilung adressierte Fachgebiete

Dieser Trend setzt sich fort, betrachtet man die Forschungsergebnistypen in Abbildung 7.3. Sortiert[352] man die Kategorien wieder nach Recht (Aufsatz, Kommentar, Gutachten, Empi-

[352] Annahme mittels Stichprobe bestätigt.

rische Untersuchung) und (Wirtschafts-)Informatik (Modelle, Umsetzung, Prototyp)[353], zeigen sich auch hier mehr Ergebnisse im juristischen Bereich. Die Ergebnisse der Betrachtungen lassen also den Schluss zu, dass es mehr Forschung von juristischer Seite gibt. Vorsichtig formuliert könnte man hier einen Forschungsbedarf in der (Wirtschafts-)Informatik ausmachen.

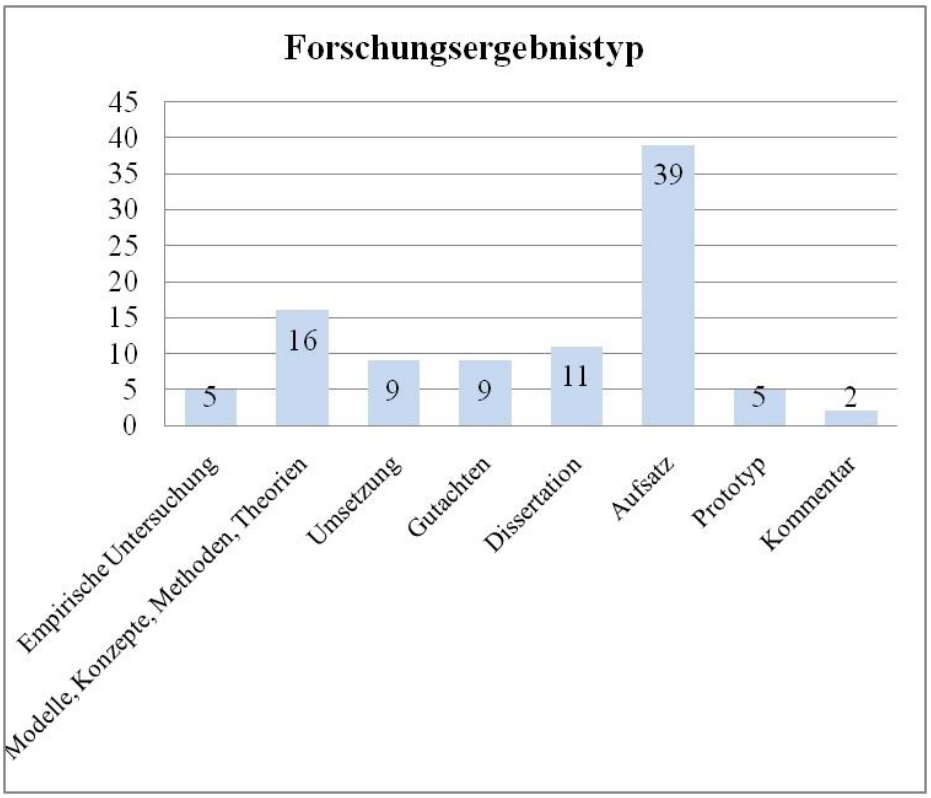


Abb. 7.3: Häufigkeitsverteilung Forschungsergebnistyp

Ebenfalls von Interesse ist aber auch die Frage nach der Art und Zielrichtung der Forschungsergebnisse. Aus der Betrachtung des Anwendungsfokus in Abbildung 7.4 zeigt sich ein Übergewicht an geschäftsorientierten Anwendungen (B2B, B2C) im Gegensatz zu den verwaltungsorientierten (G2C, G2B). Bei der Aussagekraft dieser Auswertung sollte aber auch die relativ geringe Zahl der Einordnungen, nämlich 28, beachtet werden.

[353] Dissertationen sind schwer zuzuordnen und wurden daher nicht berücksichtigt.

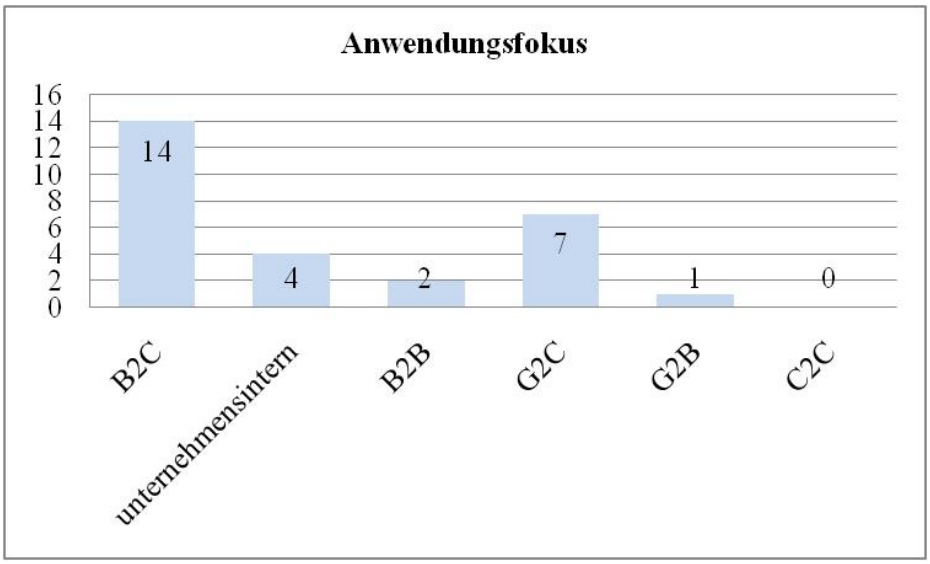


Abb. 7.4: Häufigkeitsverteilung Anwendungsfokus

Als weitere Perspektive wird diejenige des Praktikers berücksichtigt. Die Häufigkeitsverteilung der Praxiseinsätze (siehe Abbildung 7.5) zeigt, dass nur sieben Einsätze dokumentiert sind. Gleichzeitig ist aber der Anteil der Ergebnisse ohne Angabe sehr hoch.

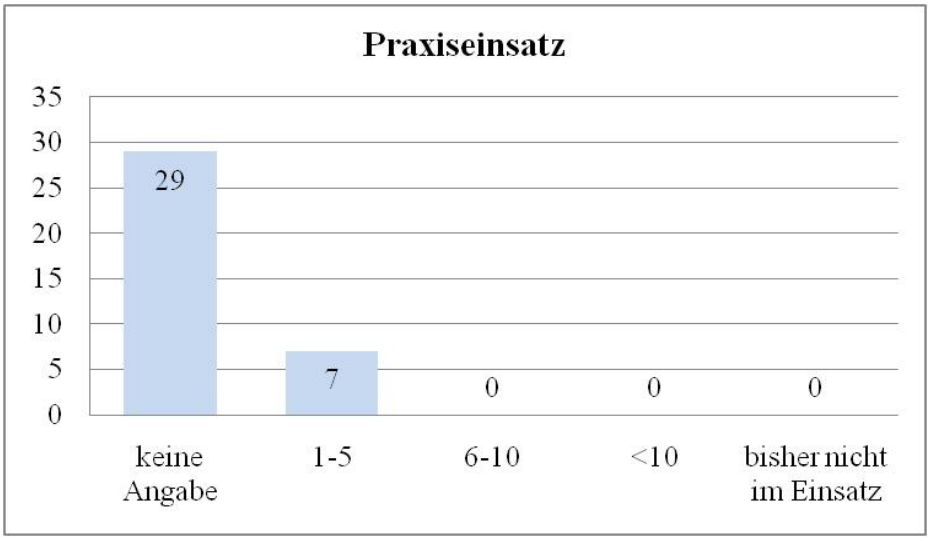


Abb. 7.5: Häufigkeitsverteilung Praxiseinsatz

Um das Bild der Forschungssituation aus Praxissicht zu komplettieren, erscheint auch eine Betrachtung der angesprochenen Branchen sinnvoll. Aus Abbildung 7.6 wird deutlich, dass keine Fokussierung auf einer Branche vorliegt, vielmehr sind branchenübergreifende Lösungen vorherrschend.

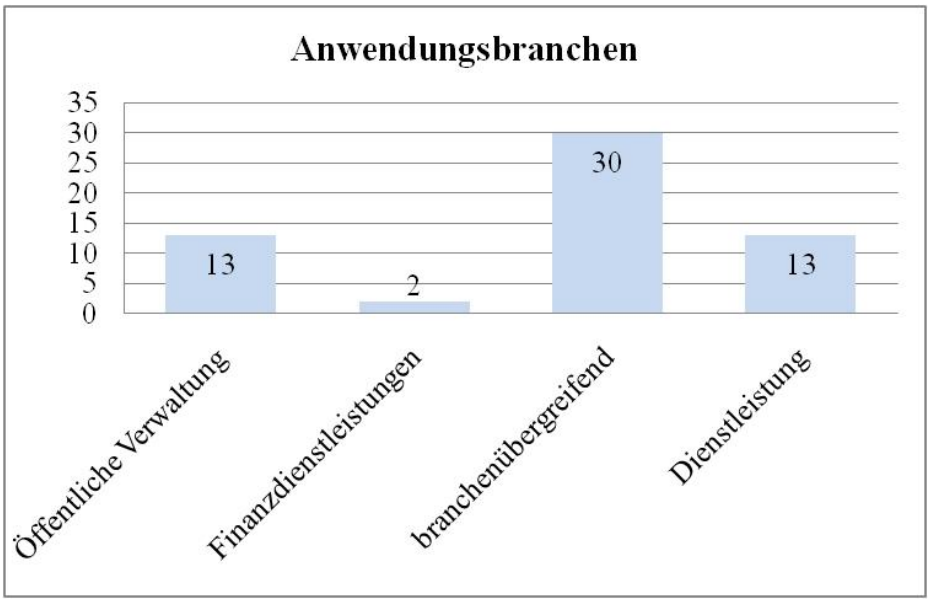


Abb. 7.6: Häufigkeitsverteilung Anwendungsbranchen

Die Betrachtungen lassen zwei Interpretationen zu. Einerseits könnte man argumentieren, dass praxisnahe Forschung durchaus vorhanden ist, es an einer Umsetzung in die Praxis aber mangelt. Andererseits liegt bei dem hohen Anteil der Ergebnisse ohne Angabe zum Praxiseinsatz die Vermutung nahe, dass die Aussagekraft der Datenbasis noch Verbesserungspotenziale aufweist.

Informationen über Qualität und Effektivität von Forschungseinrichtungen sind für Geldgeber von Interesse. Ebenso interessant sind aber auch Informationen über bisher unerforschte Fachgebiete. Diese könnten eine finanzielle Unterstützung benötigen, um sich möglicherweise zu etablieren. Wenn man Quantität mit Qualität gleichsetzt, ist das Aufspüren von Forschungsschwerpunkten ein guter Ansatz, um mögliche Förderpartner zu identifizieren. Eine erste schnelle Übersicht liefert dafür die Heatmap der Forschungslandkarte (siehe Abbildung 7.1). Neben den Forschungsschwerpunkten im Raum Münster und Karlsruhe ist auch die Region um Kassel als Brennpunkt zu benennen. Um eine Aussage über unerforschte Fachgebiete machen zu können, ist eine Betrachtung der adressierten Fachgebiete (siehe Abbildung 7.2) notwendig, genauso wie sie schon bei den Forschern erfolgt ist. Entsprechend kommt man hier zu der gleichen Aussage, dass der (wirtschafts-) informatische Anteil ausbaufähig ist.

Die begonnene Pflege und Nutzung der Forschungslandkarte sollte in weiterführenden Arbeiten intensiviert werden. Wünschenswert wäre das Entstehen einer aktiven „Social Community“, welche nicht nur aktuelle Projekte und Erkenntnisse beisteuert, sondern sich untereinander austauscht und damit die Forschung weiter vorantreibt. Dazu müssen andere Wissenschaftler gewonnen werden. Denkbar wäre hierfür eine aktive Ansprache von Vertretern bereits eingepflegter Institutionen.

8 Forschungsperspektiven im Kontext Informationstechnik und Recht

Philipp Bergener, Patrick Delfmann, Mathias Eggert, Fleur Fritz, Marcel Heddier, Eva-Maria Herring, Sara Hofmann, Ralf Knackstedt, Dominique Meiländer, Eric Meyer, Michael Räckers, Julia Seiler

8.1 Notwendigkeit interdisziplinärer Forschung

Die interdiziplinäre Ausrichtung der Rechtsinformatik und des Informationsrechts kann zur Vitalisierung beider Disziplinen beitragen.[354] Projekte zur Implementierung von Informationssystemen verlangen unter anderem eine Zusammenarbeit zwischen Juristen, Informatikern, Wirtschaftsinformatikern, Mathematikern, Medizinern und Verwaltungswissenschaftlern. Die Einbindung der rechtlichen Expertise in den Entwicklungsprozess von Informationssystemen adressiert typische Fragestellungen der Wirtschaftsinformatik. Die Grenzen der formalen Transformierbarkeit von Rechtvorschriften in Algorithmen fordert das Forschungsinteresse von Mathematikern und Informatikern heraus. Gerade im Bereich der softwaretechnischen Unterstützung von Prozessen in Krankenhäusern gilt es, eine Vielzahl von Fragen aus datenschutzrechtlicher Sicht in Zusammenarbeit mit den handelnden Medizinern zu klären. Die hohe Regelungsdichte, die für Verwaltungsprozesse prägend ist, legt es nahe, bei der Einführung von IT-Systemen Informatiker, Rechtswissenschaftler und Verwaltungswissenschaftler eng miteinander zu verzahnen.

Im Folgenden werden zunächst aus Sicht der Disziplinen Rechtswissenschaften, Wirtschaftsinformatik und Wirtschaftswissenschaften weiterführende Forschungsfragen zum Verhältnis von Informationstechnik und Recht entwickelt. Im Anschluss wird der disziplinenbezogene Fokus durch die Erörterung ausgewählter Anwendungsbereiche ergänzt.

8.2 Disziplinspezifische Forschungsperspektiven

8.2.1 Rechtswissenschaften

Das Informationsrecht ist eine neue Rechtsdisziplin, welche die Rechtsordnung aufgrund des stetigen Fortschritts im Bereich moderner Informationstechnologien vor neue Herausforderungen stellt. Es geht dabei ganz allgemein um die Erforschung von Rechtsfragen, die sich durch den Einsatz elektronischer Datenverarbeitung stellen. Da Informationen einen hohen wirtschaftlichen Wert besitzen, ist es gerade unter zivilrechtlichen Gesichtspunkten von enormer Bedeutung, wem welche Informationen in welchem Umfang „gehören“. Der

[354] Vgl. Knackstedt et al. (2010).

Begriff Informationsrecht umschreibt letztendlich eine Querschnittsmaterie und fügt sich nicht in den herkömmlichen Kanon „Zivilrecht, Öffentliches Recht und Strafrecht“ ein. Im Mittelpunkt stehen Rechtsfragen aus dem Bereich des Urheberrechts, des gewerblichen Rechtsschutzes, des elektronischen Handels, der Telekommunikation, des Vertragsrechts, des Wettbewerbs- und Kartellrechts sowie des Datenschutzrechts.

Mit der zunehmenden Bedeutung der EDV in den siebziger Jahren traten auch die damit verbundenen Risiken vermehrt in den Fokus der Öffentlichkeit.[355] Insbesondere wurde erstmals über den Schutz personenbezogener Daten diskutiert. War das Datenschutzrecht bislang nur eine Disziplin unter vielen bei der Fortentwicklung des IT-Rechts, so ist es gerechtfertigt, dem Datenschutzrecht nunmehr eine besonders hervorgehobene Bedeutung beizumessen.[356]

Mit § 9 BDSG hat der Gesetzgeber eine Vorschrift eingeführt, die für den Fall der automatisierten Verarbeitung und Nutzung personenbezogener Daten dazu verpflichtet, technische und organisatorische Maßnahmen so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht werden. Datensicherheit ist damit ein Thema, mit dem sich jede Stelle zwingend auseinandersetzen muss, die mit personenbezogenen Daten in Kontakt kommt, und zwar unabhängig davon, ob es sich dabei um eine öffentliche oder nicht-öffentliche Stelle handelt oder in welchem quantitativen Umfang eine Datenverarbeitung stattfindet.[357]

Ziel der Norm ist es, durch den ordnungsgemäßen Ablauf der Datenverarbeitung sowie durch geeigneten Einsatz von Sicherheitsmaßnahmen den Verlust, die Beschädigung oder den Missbrauch personenbezogener Daten zu verhindern bzw. das Risiko dieser Ereignisse zu minimieren. Nur so kann das Persönlichkeitsrecht des Betroffenen gewährleistet werden, was nach § 1 BDSG der übergeordnete Zweck des Datenschutzes ist.

Die Schutzwirkung der zu treffenden Maßnahmen muss dabei in einem angemessenen Verhältnis zum Aufwand stehen, den diese verursachen. Neben dem Aufwand ist bei der Auswahl geeigneter Maßnahmen auf die Art der zu schützenden personenbezogenen Daten bzw. auf deren Schutzbedarf abzustellen, was mittels einer Risikoanalyse bewertet werden kann.[358]

Welche Sicherheitsmaßnahmen im Einzelnen getroffen werden sollten, wird in einer Anlage zu § 9 BDSG konkretisiert. Es handelt sich dabei lediglich um abstrakte Zielvorgaben,

[355] Vgl. Hoeren (2010), S. 21.
[356] Moos (2010), S. 166.
[357] Vgl. Däubler, Klebe und Wedde (1996), § 9 Rn. 10.
[358] Vgl. Gola und Schomerus (2007), § 9 Rn. 9.

deren Ausgestaltung im Ermessen des einzelnen Unternehmens liegt. Das Ermessen ist dahingehend begrenzt, dass insgesamt die Schutzziele Verfügbarkeit, Authentizität und Integrität der Daten angemessen gewährleistet werden müssen. Zudem müssen bei der Auslegung der möglichen Kontrollmaßnahmen die Entwicklungen, die seit dem Erlass des Katalogs im Bereich der Datensicherheit und speziell im Zusammenhang mit IT-Sicherheit eingetreten sind, berücksichtigt werden.

Beispielhaft werden im Rahmen der Anlage zu § 9 BDSG folgende Kontrollen genannt:

Nr. 1: Zutrittskontrolle (z. B. Mitarbeiter- und Berechtigungsausweise)

Nr. 2: Zugangskontrolle (z. B. Verschlüsselung von Daten, Passwörter)

Nr. 3: Zugriffskontrolle (z. B. Einrichtung eines Benutzerverwaltungssystems)

Nr.4: Weitergabekontrolle (z. B. Absicherung der elektronischen Kommunikationswege durch Einrichten von geschlossenen Netzwerken)

Nr. 5: Eingabekontrolle (Detaillierte Protokollierung jeglicher Erstellung, Veränderung und Entfernung von Datensätzen)

Nr. 6: Auftragskontrolle (z. B. Klare Kompetenzabgrenzungen)

Nr. 7: Verfügbarkeitskontrolle (z. B. Regelmäßige Erstellung von vollwertigen Sicherungskopien; Erstellung eines umfassenden Notfallkonzepts)

Nr. 8: Trennungsgebot (z. B. Trennung von Test- und Produktivsystem)[359]

Um diese abstrakten Zielvorgaben weiter auszuformen, können auch der Rückgriff auf bewährte Informationssicherheitsstandards wie bspw. die Grundschutzstandards und -kataloge des Bundesamts für Sicherheit in der Informationstechnik (BSI) hilfreich sein.[360] Diese geben detaillierte Empfehlungen für den Einsatz von IT-Systemen mit dem Ziel einer grundlegenden Sicherheit.

Ein nicht nur auf ökonomischer Ebene sehr wesentlicher Teil des Informationsrechts beschäftigt sich mit der Erstellung, Behandlung und Abwicklung von Verträgen mit IT-Bezug, das IT-Vertragsrecht. Auch hierbei handelt es sich nicht um eine einzige homogene Gesetzesmaterie, vielmehr werden bei der Gestaltung von Vertragswerken mit IT-Bezug regelmäßig eine ganze Reihe von rechtlichen Vorgaben tangiert und relevant, wobei es

[359] Beispiele aus Taeger und Gabel (2010), § 9 Rn. 44 ff.
[360] Vgl. https://www.bsi.bund.de und Abschnitt 4.

teilweise auch noch immer hochumstritten ist, welche Regelungen genau Anwendung finden sollen.[361]

Maßgeblicher Ausgangspunkt ist hier – wie so oft – das BGB. Allerdings stammt dieser Gesetzestext in seinen größten Teilen aus dem Beginn des vorigen Jahrhunderts. Entsprechend einfach lässt sich erkennen, dass die in ihm normierten Regelungen kaum auf moderne, hochkomplexe IT-Verträge passen. Bedingt durch diese Tatsache ergeben sich eine ganze Reihe von rechtlichen Verwerfungen, die bis heute kaum zufriedenstellend gelöst sind.[362] Zwar gibt es erste Lösungsansätze, wie beispielsweise das Change-Request-Verfahren[363], aber auch diese lösen das generelle Problem nicht in zufriedenstellender Art und Weise.

Nicht zuletzt auf diese Situation wird auch die Tatsache gegründet, dass viele IT-Großprojekte scheitern: Am Anfang der Vertragsbeziehung wissen die Parteien in der Regel noch nicht, was genau sie eigentlich von dem Projekt erwarten, geschweige denn, wie sich diese Erwartungen in die Realität umsetzen lassen. Es handelt sich um komplexe Langzeitverträge[364], deren Abwicklung über das geltende Recht nur schwer möglich ist. Gerade an dieser Stelle besteht nicht nur vermehrter juristischer Forschungsbedarf, um in Zukunft die rechtliche Komponente solcher IT-Projekte besser steuern zu können, sondern auch ein Bedarf zu interdisziplinärer Zusammenarbeit zwischen den Bestellern eines Projektes, den IT-Entwicklern und den beteiligten Juristen.

8.2.2 Wirtschaftsinformatik

Ein Ansatz, um auf die Problematik der rechtskonformen Gestaltung von IT-Systemen zu reagieren, ist die Entwicklung von Methoden, welche sicherstellen, dass IT-Systeme den rechtlichen Anforderungen entsprechen. Diese Methoden gliedern sich in zwei unterschiedliche Verfahren. Zum einen ist die gestaltungsorientierte Entwicklung von Informationsmodellierungsmethoden ein adäquater Weg, rechtliche Anforderungen in Informationsmodellen abzubilden. Zum anderen kann durch die (teil-) automatisierte Überprüfung bereits existierender Modelle eine Rechtsverletzung leicht erkannt und behoben werden. Hierbei ist auch die Modellüberprüfung während der Modellierungsphase möglich.

Grundlage der Informationssystemgestaltung ist die Transformation von Sprachkonstrukten. Abbildung 8.1 verdeutlicht die Transformation im Bereich der Informationstechnik am Beispiel einer einfachen natürlichsprachlichen Anwendungsbeschreibung, welche über den

[361] Vgl. Müller-Hengstenberg (2010), S. 1181 ff.
[362] So auch: Hoeren (2007), Rn. 356.
[363] Exemplarisches Muster einer solchen Vereinbarung in: Hoeren (2007), Rn. 570.
[364] Siehe dazu grundlegend Nicklisch (1987).

Zwischenschritt einer grafischen Repräsentation in eine formale Kunstsprache transformiert wird.

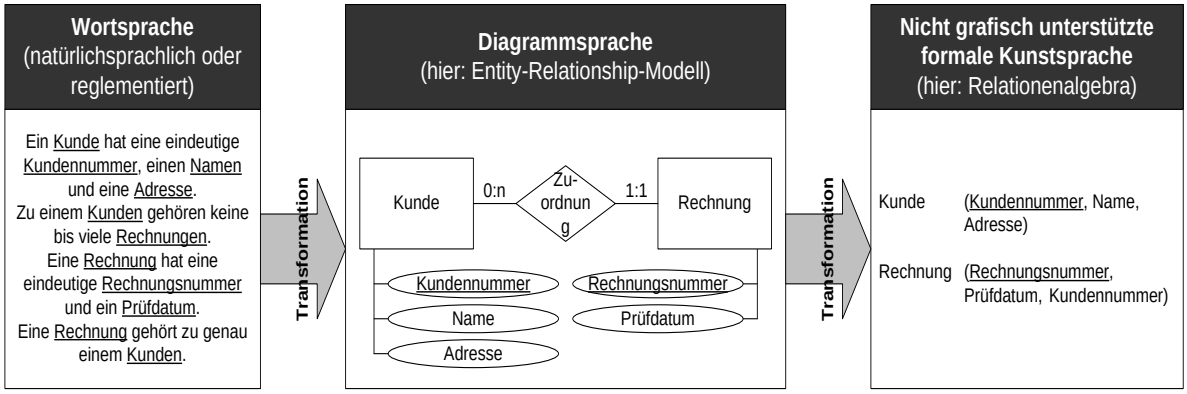


Abb. 8.1: Transformation von natürlicher Sprache in formale Sprache[365]

Forschungsschwerpunkt der Informationsmodellierung ist die Entwicklung von Modellierungsmethoden für unterschiedliche Anwendungsgebiete. Allerdings ist nur ein Teil dieser Methoden in der Praxis auch von Bedeutung.[366] Hier sind z. B. Entity-Relationship-Modelle, die Unified Modeling Language (UML) oder die in der ARIS-Methode integrierten Ereignisgesteuerten Prozessketten (EPK) zu nennen. Die bekannten Modellierungsmethoden verfügen jedoch nur eingeschränkt über Möglichkeiten, alle rechtlichen Anforderungen abzubilden. Zur Darstellung dieser Sachverhalte dominieren in der Forschung eher Ansätze zur mathematischen oder ontologischen Formalisierung des Rechts mit dem Ziel der automatischen Inferenz.[367] Erste Ansätze zur Integration in Modellierungssprachen nutzen in der Praxis kaum relevante Modellierungsmethoden wie die User Requirements Notation (URN)[368] oder definieren lediglich allgemeine Konzepte ohne Rückgriff auf eine konkrete Modellierungsmethode.[369]

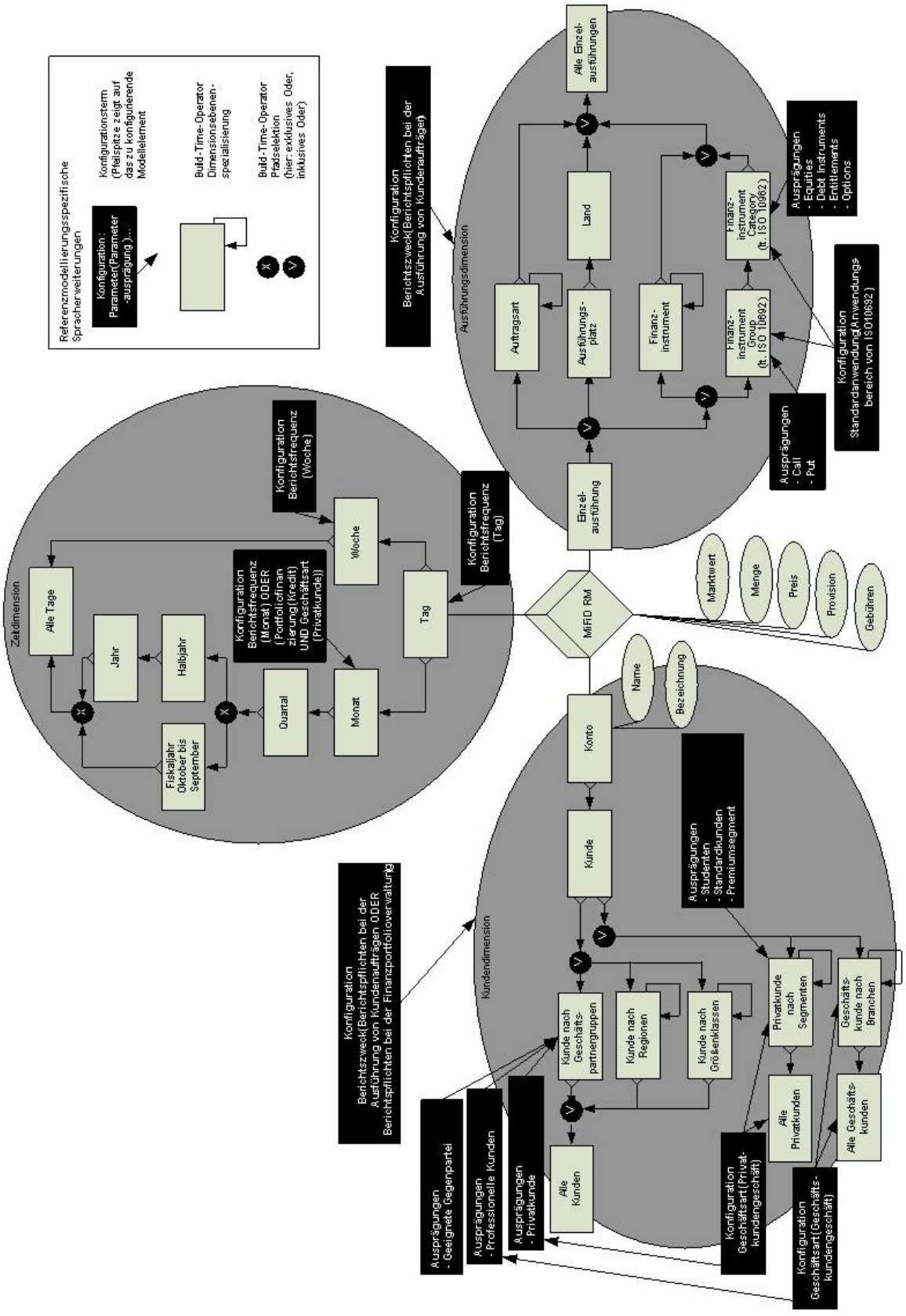
Im Bereich der Evaluation von Informationsmodellierungsmethoden finden sich vor allem Ansätze, die sich auf ontologischer Ebene mit der Ausdrucksfähigkeit der Methoden beschäftigen.[370] Empirische Untersuchungen des praktischen Nutzens von Informationsmodellierungsmethoden sind dagegen nur selten zu finden.[371] Im Bereich der Referenzmodellierung gibt es inzwischen eine Vielzahl von Modellen für unterschiedliche Anwendungsbereiche. So listet die Seite *Reference Model Catalogs* (http://rmk.iwi.uni-sb.de/catalog.php) über 90 Referenzmodelle auf. Referenzmodelle für rechtliche Konzepte

[365] Vgl. Knackstedt (2004).
[366] Vgl. Fettke (2009).
[367] Z. B. Breaux, Vail, & Anton (2006); Breuker & Hoekstra (2004).
[368] Vgl. Ghanavati, Amyot, & Payton (2007).
[369] Vgl. Namiri & Stojanovic (2007).
[370] Vgl. Recker, Rosemann, Indulska, & Green (2009).
[371] Vgl. Fettke (2009).

finden sich hier jedoch nicht. Auch eine empirische Validierung der Referenzmodelle findet sich nur in einem Fall (ITIL). Insgesamt stehen auch hier eher ontologische Evaluationsansätze im Vordergrund.[372]

Die konfigurative Informationsmodellierung stellt einen zentralen Ansatz zur Modellierung rechtlicher Anforderungen dar, deren Thematik auf einer Reihe von Vorarbeiten zum Thema Referenzmodellierung für die Entwicklung von Data Warehouse Systemen[373] sowie zur Entwicklung rechtssicherer Web-Anwendungen[374] basiert. Während *Knackstedt (2004)* die Entwicklung einer Modellierungsmethode für fachkonzeptionelle Referenzmodelle zur Managementunterstützung forciert, befassen sich *Knackstedt & Klose (2005)* mit der Konfiguration solcher Referenzmodelle zur adaptierten Anwendung in Data Warehouse Systemen. Darauf aufbauend beschreiben *Goeken & Knackstedt (2008)* eine Erweiterung der multidimensionalen Modellierung, welche die Erstellung von konfigurativen Modellen in einem zwei Phasen einschließenden Entwicklungsprozess umfasst. Ein Ergebnis dieser Arbeit ist das MiFID-Referenzmodell[375], welches in Abbildung 8.2 dargestellt ist.

[372] Vgl. Fettke & Loos (2004).
[373] Vgl. Knackstedt (2004); Knackstedt & Klose (2005); Goeken & Knackstedt (2007).
[374] Vgl. Knackstedt, Brelage & Kaufmann (2006).
[375] Markets in Financial Instruments Directive – MiFID.



Quelle: Goeken & Knackstedt (2008), S. 53.

Abb. 8.2: MiFID Referenzmodell

Die Berücksichtigung rechtlicher Aspekte in fachkonzeptionellen Methoden zur Entwicklung von Web-Anwendungen haben *Knackstedt, Brelage & Kaufmann (2006)* untersucht und gezeigt, dass rechtliche Anforderungen in der grafisch darstellbaren Modellierung unzureichende Berücksichtigung finden. Zur präzisen Spezifikation von fachlichen Anforderungen, die im Rahmen der Konstruktion von Informationssystemen (d. h. Softwaresysteme und die sie umgebende Organisation) zu stellen sind, haben sich konzeptionelle Modelle als unverzichtbares Hilfsmittel erwiesen.[376] Um die Rechtskonformität von Informationssystemen sicherzustellen, ist es vorteilhaft, entsprechende konzeptionelle Modelle bereits so zu gestalten, dass diese schon ein rechtskonformes Szenario repräsentieren. Bisher wird die Rechtskonformität entweder durch Abgleich des bereits entwickelten Informationssystems oder in einer früheren Phase durch Abgleich der bereits entwickelten konzeptionellen Modelle überprüft. Als Grundlage der Überprüfung dienen dabei rechtliche Bestimmungen, die in Form von natürlichsprachlich verfassten Gesetzestexten vorliegen. Das skizzierte Vorgehen birgt die Gefahr, dass ein bereits existentes konzeptionelles Modell bzw. Informationssystem aufgrund gegebenenfalls nicht oder unzureichend eingehaltener gesetzlicher Bestimmungen aufwändig modifiziert bzw. seine technischen Teile stillgelegt werden müssen. Weiterhin gestaltet sich das Verfahren selbst in vielen Fällen aufwändig, da natürlichsprachlich verfasste Bestimmungen mit formal spezifizierten Eigenschaften des Informationssystems abgeglichen werden müssen.

Um Modelle auf ihre rechtliche Konformität hin zu überprüfen, ist die Forschung im Bereich der linguistischen Standardisierung unerlässlich. Insbesondere Verfahren, welche die Eindeutigkeit von natürlichsprachlichen Aussagen in konzeptionellen Informationssystemmodellen sicherstellen, werden benötigt. Zum einen muss eine standardisierte und semantisch eindeutig beschriebene natürlichsprachliche Grammatik vorgegeben werden, zum anderen wird die Konformität der in den Modellen getroffenen Aussagen bereits während der Modellierung forciert.[377] Die technische Umsetzung einer solchen Modellprüfung ist in Abbildung 8.3 dargestellt.

Arbeiten zur syntaktischen und semantischen Analyse von konzeptionellen Modellen sind in Form eines generischen Verfahrens zur Strukturmustersuche bereits entwickelt worden.[378] Das Verfahren zeichnet sich dadurch aus, dass es auf beliebige Modellierungssprachen – d. h. beliebige Graph-ähnliche Strukturen anwendbar ist. Diese Eigenschaft lässt eine Wiederverwendbarkeit einerseits in der strukturellen Formalisierung von Gesetzestex-

[376] Vgl. Kottemann & Konsynski (1984); Karimi (1988).
[377] Vgl. hierzu Delfmann et al. (2008); Becker et al. (2009a); Becker et al. (2009b); Delfmann, Herwig, Lis (2009a); Delfmann, Herwig, Lis (2009b); Delfmann et al. (2009a); Becker et al. (2010).
[378] Vgl. hierzu Becker et al. (2009c); Delfmann et al. (2009b).

ten, andererseits im Analyseverfahren zum Abgleich von gesetzlichen Vorschriften und konzeptionellen Informationssystemmodellen erwarten.

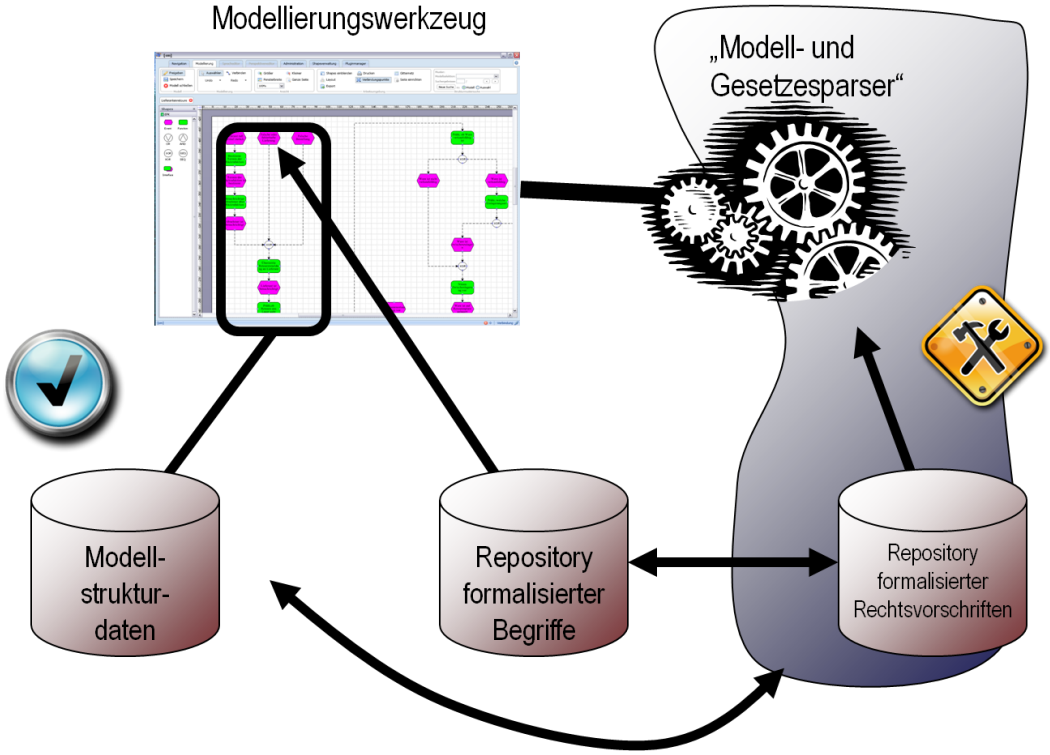


Abb. 8.3: Technische Umsetzung der Prüfung von Modellen auf Gesetzeskonformität

Die vorgestellten Forschungsarbeiten im Bereich der Modellierung und Überprüfung von rechtlichen Anforderungen führen zu einer Reihe von Fragen, welche in zukünftigen Forschungsprojekten Berücksichtigung finden sollten. Wie etwa lassen sich ausgewählte, etablierte Instrumente der Modellierung von Prozessen, Berichtspflichten, Datenbankanwendungen und Internetauftritten weiterentwickeln, damit sie besser zur Reduktion rechtlicher Verstöße in der Informationssystemgestaltung beitragen? Darüber hinaus sollte generell die Frage beantwortet werden, welche Gestaltungsfaktoren und Anwendungskontexte von Modellierungssprachen und Referenzmodellen die Reduktion von Rechtsverstößen beeinflussen.

Zur Sicherstellung der Einhaltung gesetzlicher Vorschriften durch (teil-) automatisierte Anleitungen des Informationssystemkonstrukteurs ist es notwendig, für die Informationssystementwicklung relevante Gesetzestexte in eine formale Form zu überführen. Hieran schließt sich die Frage der Machbarkeit einer solchen Formalisierung an. Aber auch Fragen nach der Akzeptanz und Effektivität eines solches Verfahrens zur Prüfung von Modellen müssen im Rahmen einer Evaluation gestellt werden. Lässt sich der Gesetzgeber in der Formulierung von Gesetzen überzeugen, Gesetze modellierungskonform zu formulieren?

8.2.3 Wirtschaftswissenschaften

Sowohl rechtliche Restriktionen für ihr eigenes Handeln wie auch die Informationsstrukturierung und -verarbeitung spielen für Unternehmen heute eine herausragende Rolle. Als neues Phänomen tritt dabei in jüngster Zeit die Kombination dieser beiden Themen hinzu: die rechtliche Behandlung der Informationsverarbeitung in Unternehmen aber auch zwischen Unternehmen. Hierbei ergeben sich neue Fragestellungen, die in unterschiedlichen Bereichen des Managements, insbesondere im Bereich des Risikomanagements ihren Niederschlag finden. Das IT-Recht ist ein sich (rasch) entwickelnder Rechtszweig. Mit neuen Gesetzen, Verordnungen und Gerichtsentscheidungen werden ständig neue Eigentumsrechte definiert bzw. verändert, was nachhaltigen Einfluss auf die Unternehmensaktivitäten hat. Vor diesem Hintergrund gilt es, die mikroökonomischen Folgen von Entscheidungen zu analysieren, die explizit auf Grundlage von solchen rechtlichen Risiken getroffen bzw. nicht getroffen wurden. Welche Schäden werden also durch IT-Risiken in Zusammenhang mit einem komplexen Rechtssystem verursacht? Insbesondere stellt sich also auch die Frage, wie solche rechtliche (IT-)Risiken in Unternehmen abgebildet und abgearbeitet werden können bzw. wo solche Risiken nicht absicherbar sind und welche Folgen dieses für Unternehmensentscheidungen hat.

Ein weiterer Trend für Unternehmen ist die Zunahme der Wertschöpfung in kooperativen Arrangements. Neue Informations- und Kommunikationstechnologien erlauben es, einzelne Wertschöpfungsschritte von Partnerunternehmen durchführen zu lassen oder zusammen mit Partnerunternehmen durchzuführen, was neue Herausforderungen für das Management der eigenen Wertschöpfung bedeutet, da alte Managementtechniken, die auf eine unternehmensinterne Steuerung abzielen, nicht oder nur sehr bedingt auf unternehmensgrenzenüberschreitende Aktivitäten übertragen werden können. In der Folge sollen deshalb Informations- und Rechtsfragestellungen in Kooperationen von Unternehmen untersucht und auf offene Fragen hingewiesen werden.

Für ein erfolgreiches Management ist eine sorgfältige Planung der Kooperation von grundlegender Bedeutung. Hierfür lässt sich ein rekursives Fünf-Schritte-Schema nutzen, das wesentliche Elemente einer erfolgreichen Kooperationsplanung und -durchführung enthält (vgl. Abbildung 8.4). Nachfolgend werden nicht alle Handlungen dargestellt, die in jedem Schritt erforderlich sind, sondern vielmehr wird ein Fokus auf rechtliche Aspekte und Informationsprobleme gelegt.

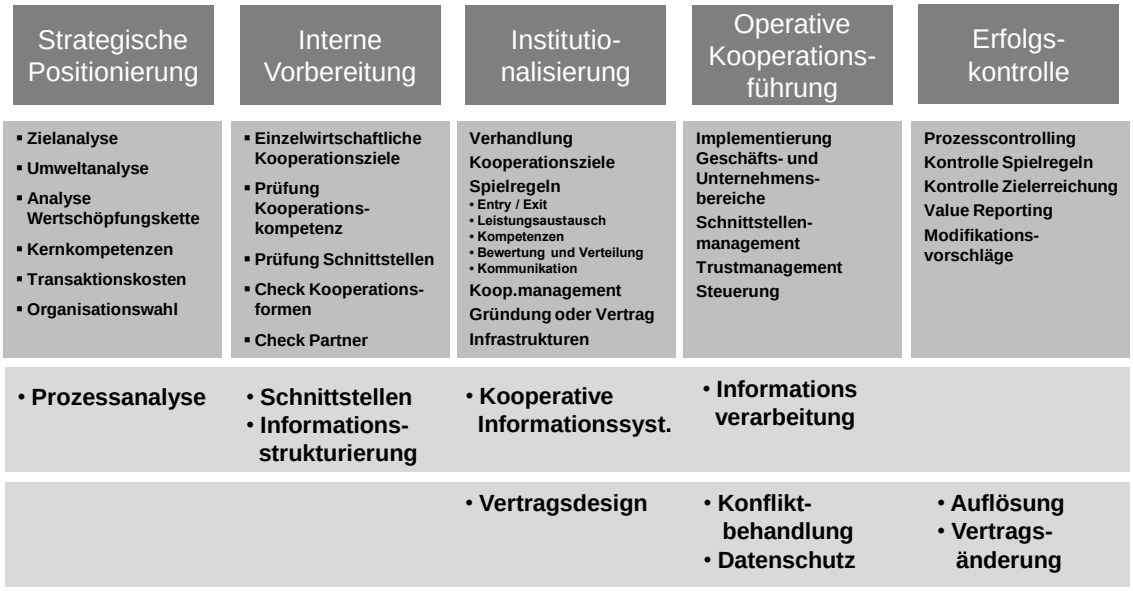


Abb. 8.4: Fünf-Schritte-Schema des Kooperationsmanagements und die Integration von Informations- und Rechtsfragestellungen

Strategische Positionierung

Vor einer Kooperation ist zunächst die eigene strategische Positionierung innerhalb der Gesamtwertschöpfungskette eines Produktes bzw. einer Dienstleistung zu untersuchen. Grundlage hierfür ist eine detaillierte und feingliedrige Ausdifferenzierung der Wertschöpfungskette, die insbesondere die Normtätigkeiten und die Schnittstellen zwischen den einzelnen Wertschöpfungsschritten analysiert. Festzuhalten ist, welche Produkte, Dienstleistungen und Informationen zwischen den Wertschöpfungsschritten ausgetauscht werden. Besonders die Untersuchung des Informationsaustausches bzw. des Informationsflusses wird häufig vernachlässigt und trägt damit zum Scheitern einer Kooperation bei oder führt zu einer unbefriedigenden, weil suboptimalen Kooperationsperformance. Die Unternehmen haben dann zu bestimmen, in welchen Teilen der Wertschöpfungskette sie ihre Kernkompetenzen sehen und welche Abhängigkeiten für sie bei der Auslagerung oder der Kooperation mit Partnern für sie bestehen. Dabei bemisst sich die Abhängigkeit nicht allein am Bezugs- oder Vertriebsvolumen, das über die betrachtete Schnittstelle läuft, sondern auch an der Relevanz der bezogenen Leistungen. Dieses impliziert, dass detailliertes Wissen über einzelne Komponenten in Bezug auf das Endprodukt vorhanden sein muss.

Interne Vorbereitung

Kommt man nach der strategischen Analyse und der strategischen Positionierung zum Schluss, dass Teile der Wertschöpfung von Partnern übernommen werden oder in Zusammenarbeit mit Partnern erfolgen sollen, so ist als nächstes die eigene Kooperationsfähigkeit

zu prüfen bzw. herzustellen. Dies umfasst insbesondere eine Konkretisierung der Schnittstellen zwischen den beteiligten Partnern. Dazu ist es erforderlich, Instrumente zu entwickeln, die eine solche systematische und damit verlässliche Analyse unterstützen. Es muss also eine Informationssystematisierung der Prozessanalyse stattfinden, die es erlaubt, erschöpfend die für eine Transaktion über eine Schnittstelle bereitzustellenden, notwendigen Informationen zu ermitteln und zu strukturieren. Darauf aufbauend sind bestimmte (Qualitäts-)Standards zu definieren, die bei der Informationsübermittlung eingehalten werden müssen, und es muss rechtlich abgesichert werden, dass die bereitgestellten Informationen vom Partner nicht für andere Zwecke verwandt werden können. Schließlich ist auch die technische Ausgestaltung der Informationsübermittlung zu gestalten. Dieses betrifft insb. die Gestaltung geeigneter Informationsformate und die Definition von Zugriffsrechten auf Informationen und Informationssysteme.

Institutionalisierung

In der Institutionalisierungsphase muss der Rahmen für die Kooperation der Unternehmen gesetzt werden. Dazu gehören die Fixierung der gemeinsamen Kooperationsziele, die Formulierung von Spielregeln, das Aufsetzen und die Verankerung des Kooperationsmanagements in den beteiligten Unternehmen und die Bereitstellung der notwendigen Infrastruktur. Unter Informationsaspekten ist die Implementierung der in Schritt 2 konzipierten Informationsstrukturen zwischen den Partnern zu leisten. Klare Kommunikationsstrukturen und klar zugewiesene Kompetenzen sind ein wesentlicher Erfolgsfaktor von Unternehmenskooperationen. Aus rechtlicher Perspektive ist die Gestaltung des Kooperationsvertrages von zentraler Bedeutung. Ob und mit welcher Tiefe ein solcher Vertrag geschlossen wird, ist nicht eindeutig zu beantworten, da sich die Partner hier mit einem Trade-Off konfrontiert sehen. Einerseits bedeutet ein detailliert formulierter Kooperationsvertrag eine Absicherung der wechselseitig zu erbringenden Leistungen, andererseits schränkt er die Handlungsfähigkeit der Partner mit wachsendem Detaillierungsgrad stärker ein, so dass auch kostenreduzierende individuelle Handlungen unter Umständen nicht ausgeschöpft werden bzw. sogar durch den Vertrag ausgeschlossen sein können. Dadurch können Neuverhandlungen nötig werden. Es ist also zwischen dem Stabilitätsnutzen und dem Flexibilitätsnutzen aus einer Kooperation abzuwägen.

Forschungsbedarf im Bereich der Rechtsinformatik besteht darin, die rechtlichen Anforderungen an einen Kooperationsvertrag informationell zu strukturieren und dabei die Anforderungen an diese Kooperation aus den Schritten 2 und 3 zu berücksichtigen. Dabei geht es dann aber nicht allein um die rechtliche Strukturierung des Problems, sondern auch um die Berücksichtigung des gerade dargestellten ökonomischen Trade-offs, der in einer reinen

Rechtsbetrachtung so nicht darstellbar ist. Es geht also um die Erarbeitung eines ökonomischen Rechtsinformatik-Modells.

Operative Kooperationsführung

Im operativen Kooperationsmanagement erfolgt die Steuerung der Kooperation über die in Schritt 3 (Institutionalisierung) bereitgestellten Systeme. Dieses beinhaltet insbesondere die Überwachung der Schnittstellen und den Austausch mit den Kooperationspartnern. Von rechtlicher Seite ist hier die Behandlung und Lösung von Konflikten relevant, die einerseits durch – möglicherweise beabsichtigte – Vertragslösungen und andererseits durch unterschiedliche Interpretationen von Inhalten eines Kooperationsvertrages hervorgerufen werden.

Es ist fraglich, inwiefern auch an dieser Stelle rechtsinformatische Systeme bei der strukturierten Abarbeitung solcher Konflikte hilfreiche Unterstützung leisten können. Da es bei der Konfliktbehandlung tendenziell auch um Verfahren der Rechtsmediation geht, könnte eine Forschungsfrage die Rechtsinformatik der Rechtsintermediation betreffen.

Erfolgskontrolle

Die Erfolgskontrolle umfasst einerseits die Überprüfung der Ziele (und ihrer Operationalisierung) der Kooperation und andererseits die Kontrolle der Einhaltung der Spielregeln bzw. der eingegangenen vertraglichen Verpflichtungen. Rechtlich kann dieses entweder die Änderung, die Konkretisierung oder die Auflösung des Kooperationsvertrages bedeuten. Unter Informationsaspekten sind unter Umständen die eingeräumten Informationsrechte und -pflichten sowie die eingerichteten Informationskanäle zu modifizieren und auf ihre Effizienz hin zu überprüfen.

8.3 Anwendungsbereiche

8.3.1 Öffentliche Verwaltung

Die öffentliche Verwaltung ist im Vergleich zur privaten Wirtschaft in deutlich stärkerem Ausmaß durch rechtliche Regularien geprägt. Sie folgt gemäß dem Weberschen Bürokratiemodell dem Prinzip der Regelgebundenheit des Verwaltungshandelns. Demnach ist die Verwaltung in ihrem Handeln an Gesetze, Verordnungen und Erlässe sowie Geschäftsordnungen und andere verwaltungsspezifische Detailregelungen gebunden.[379]

[379] Vgl. Weber (1922); Becker, Algermissen, Falk (2007), S. 7.

Auch im Rahmen des e-Government, das die Unterstützung des Verwaltungshandelns mit Informations- und Kommunikationstechnologie zum Gegenstand hat, spielen rechtliche Vorgaben eine zentrale Rolle. So gut wie alle IT-Verfahren, die im Bereich der öffentlichen Verwaltung eingesetzt werden, müssen die entsprechenden Regelungen vollumfänglich umsetzen und operationalisieren. Hier gilt es zudem, den Schutz und die Sicherheit sensibler Bürgerdaten, die in solchen Systemen gehalten werden, sicherzustellen.[380]

Der Reifegrad von e-Goverment-Lösungen wird zumeist mit Hilfe von Stufenmodellen beurteilt.[381] Auf der untersten Stufe steht dabei eine einfache Informationsbereitstellung, gefolgt von der Bereitstellung von Formularen und einfacher 2-Wege-Kommunikation z. B. via e-Mail. Auf der nächst höheren Stufe werden transaktionale Dienstleistungen eingeordnet, bei denen eine vollständig elektronische Abwicklung der Dienstleistung stattfindet. Je nach Autor beziehen sich weitere Stufen zum einen auf die horizontale und vertikale Integration von Dienstleistungen zwischen Behörden und zum anderen auf die proaktive und personalisierte Erbringung derselben.[382] Im Rahmen der Ausgestaltung von e-Government-Dienstleistungen kann die Gesetzgebung auch als Treiber zur Modernisierung wirken. Als zentrales Beispiel der vergangenen Jahre ist hier die EU-Richtlinie 2006/123/EG über Dienstleistungen im Binnenmarkt (EU-DLR) zu nennen. Die Richtlinie schreibt unter anderem vor, dass ein in der EU ansässiger Dienstleister alle für die Aufnahme und Ausübung seiner Tätigkeit notwendigen Verfahren aus der Ferne, elektronisch und über einen einheitlichen Ansprechpartner (EAP) abwickeln kann. Damit wird die Realisierung eines One-Stop-Governments, wie es in der Theorie immer wieder beschrieben und gefordert wird, für diesen Bereich in Europa verpflichtend.[383] Die Umsetzung der EU-DLR bedingt einen starken Fokus auf die entsprechenden Prozesse der beteiligten Behörden. Um eine effiziente, IT-gestützte Verzahnung derselben zu ermöglichen sowie den EAP mit entsprechenden Informationen zu versorgen, ist eine zielgerichtete Erfassung mit Hilfe entsprechender Prozessmodelle notwendig.[384]

Auch zukünftig ergeben sich im Wechselspiel zwischen gesetzlicher Regulierung des Verwaltungshandelns und der Unterstützung desselben mit IKT im Rahmen des e-Governments eine Reihe interessanter Fragestellungen. Ein wichtiger Bereich ist hier der Umgang mit Daten in der öffentlichen Verwaltung. Einerseits ist es vor dem Hintergrund einer angestrebten horizontalen und vertikalen Integration von Verwaltungen erstrebenswert, einen möglichst reibungslosen Datenaustausch zu ermöglichen. Auch für den Bürger

[380] Vgl. zu Ansätzen, die entsprechende Sicherheitsanforderungen abbilden, z. B. Yu (2009).
[381] Vgl. Layne, Lee (2001).
[382] Zu eGovernment-Reifegrad-Modellen vgl. u. a. Andersen, Henriksen (2006); Capgemini (2009); Layne, Lee (2001); Moon (2002).
[383] Vgl. zum Konzept des One-Stop-Governments z. B. Wimmer (2002); Gouscos et al. (2007).
[384] Vgl. Bergener, Pfeiffer, Räckers (2009); Hogrebe, Nüttgens (2008).

sind wiederholte Abfragen derselben Daten durch Behörden oft nur schwer nachzuvollziehen. Auf der anderen Seite erheben Verwaltungen häufig besonders sensible Daten der Bürger, die eines entsprechenden Schutzes bedürfen. Insofern stellt sich hier die Frage, wie eine e-Government-Integration bei gleichzeitiger Berücksichtigung des Datenschutzes bewältigt werden kann. Gleichzeitig ist zu untersuchen, ob rechtliche Regelungen zum Datenschutz zumindest bei weniger sensiblen Daten nicht gelockert werden können, um eine bessere Datenintegration zu gewährleisten. Als besonders sensible Daten kann in diesem Zusammenhang die Stimmabgabe von Wahlen gesehen werden. Insofern stellt sich hier die Frage, ob und wie sich e-Voting im Rahmen des deutschen Wahlrechts realisieren lässt und welche technischen Risiken damit verbunden sind.

Weitere Forschungsfelder ergeben sich durch neue regulatorische Maßnahmen auf nationaler und europäischer Ebene. Ein Beispiel dafür ist die Einführung des elektronischen Personalausweises in Deutschland. Dieser ermöglicht es, Verwaltungsdienstleistungen, die eine Unterschrift oder eine persönliche Identifikation von Seiten des Bürgers voraussetzen, im Rahmen des e-Governments auf transaktionalem Niveau anzubieten.[385] Hier gilt es zu untersuchen, wie sich Verwaltungsprozesse durch den Einsatz des elektronischen Personalausweises reorganisieren und optimieren lassen, so dass gleichzeitig Anforderungen an Datenschutz und Datensicherheit gewahrt bleiben. Weitere potentielle Forschungsfragen können sich durch Änderungen der Gesetzgebung z. B. auf den Gebieten der elektronischen Signatur und des e-Procurement ergeben.

Schließlich ist noch die Zusammenarbeit zwischen Verwaltungen und der Privatwirtschaft im Rahmen von Public-Private-Partnerships bei der Erstellung und dem Betrieb von IKT als Forschungsfeld zu nennen. Hier ist aus juristischer Sicht zu untersuchen, wie rechtliche Rahmenbedingungen und Verträge ausgestaltet werden müssen, um einerseits eine effiziente Kooperation zu ermöglichen, und andererseits Datenschutz und Datensicherheit zu gewährleisten. Weiterhin stellt sich in diesem Bereich die Frage, welche wettbewerbsrechtlichen Konsequenzen sich aus der Vorgabe von Standards im Rahmen von IKT-Beschaffung bzw. entsprechenden Ausschreibungen ergeben.

8.3.2 Verteilte Middleware für Online-Computerspiele

Interaktive Echtzeitanwendungen und insbesondere Online-Computerspiele erleben in den letzten Jahren einen starken Popularitätsschub und stellen inzwischen einen ernstzunehmenden Wirtschaftsfaktor mit hohem Potential dar[386]. Diese Anwendungen benutzen verteilte Systeme zur Bereitstellung von Rechen- und Kommunikationsleistung. Zwar ermög-

[385] Vgl. Reichl, Roßnagel, Müller (2005).
[386] Vgl. Heng (2009); Video Game Sales Wiki (2009); GamesBrief (2010).

lichen verteilte Systeme potentiell die Echtzeitinteraktion von tausenden Benutzern in einer einzelnen Anwendungsinstanz, allerdings ist die Entwicklung von effizienten verteilten Anwendungen äußerst komplex und sehr fehleranfällig. Daher werden bei der Entwicklung von interaktiven Echtzeitanwendungen häufig verteilte Middlewarelösungen benötigt, die von den komplexen Details der Kommunikation in verteilten Systemen abstrahieren. Ein Beispiel für eine verteilte Middleware zur Erstellung von industriellen interaktiven Echtzeitsystemen ist das an der Universität Münster entwickelte Real-Time Framework (RTF).[387]

Durch die immer stärkere Verflechtung der Spieler mit den virtuellen Welten wird die Beeinflussung von Online-Spielen durch kriminelle Angriffe auf die Anwendung (sogenanntes Cheating) zu einem ernstzunehmenden Problem. Die Motivationen für Cheating sind unterschiedlich und reichen von dem Schaffen unfairer Vorteile im Wettbewerb mit anderen Spielern bis hin zum systematischen Betrug, der auf finanziellen Gewinn abzielt, z. B. durch den Diebstahl virtueller Güter mit realwirtschaftlichem Gegenwert. In allen Fällen entstehen sowohl bei den Nutzern als auch bei den Betreibern von Online-Spielen erhebliche persönliche und wirtschaftliche Schäden. Demnach besteht ein hohes wirtschaftliches Interesse an der Absicherung von interaktiven, vernetzten Echtzeitanwendungen gegen kriminelle Angriffe.

Während viele Betrugsmöglichkeiten bereits durch fehlerhafte oder unsichere Software begünstigt werden, setzen andere Cheatingmethoden auf die aktive Manipulation der Software oder der Kommunikation im Netzwerk.

Die Angriffspunkte und -methoden auf interaktive Anwendungen wurden bereits exemplarisch auf dem Gebiet der Online-Computerspiele untersucht.[388] Allerdings belegen immer wieder auftauchende Betrugsvorgänge, dass bisher keine hinreichenden Mechanismen zur Vermeidung und Aufdeckung von Angriffen existieren oder die bestehenden Mechanismen aufgrund ihrer Praxisuntauglichkeit nicht von den Entwicklern interaktiver Anwendungen genutzt werden.

Die Absicherung von virtuellen Welten in Online-Computerspielen ist demnach eine komplexe und wichtige Aufgabe, welche die Kombination von Methoden der Informatik, Gesetzgebung und Wirtschaftswissenschaften erfordert.[389]

Technische Maßnahmen gegen Cheating bestehen einerseits in der Entwicklung verteilter Middleware Systeme, welche die Erstellung von robusten Softwaresystemen unterstützen,

[387] Vgl. Glinka et al. (2008).
[388] Vgl. Hoglund, McGraw (2007); Pritchard (2000).
[389] Vgl. Gorlatch et al. (2010).

und andererseits in der Erforschung und Integration von Abwehrmechanismen in bestehende verteilte Systeme. RTF integriert bereits einige Mechanismen zum Schutz gegen Angriffe und zur Erkennung von schadhaftem Verhalten.[390]

Technische Maßnahmen zum Schutz gegen Angriffe und zur Aufzeichnung illegalen Verhaltens müssen mit rechtlichen Gegebenheiten und Möglichkeiten abgestimmt werden, damit die Aufzeichnung von Verstößen und Schäden vor Gericht gegen den Angreifer geltend gemacht werden kann. Dabei wird es insbesondere um die Fragen gehen, inwieweit einerseits Strafnormen in der Lage sind, Verhaltensänderungen unter den spezifischen Bedingungen der einschlägigen Tätergruppen und Tatbedingungen zu bewirken. Andererseits wird zu klären sein, welche Veränderungen im Verhalten legal agierender Nutzer infolge weiter gehender strafrechtlicher Reglementierung und Kontrolle drohen (z. B. infolge der Scheu vor einem „gläsernen" Nutzerprofil bei umfassender Vorratsdatenspeicherung).

Die Einbeziehung von ökonomischen Gesichtspunkten ist erforderlich, um den Aufwand einzelner Präventions- und Abwehrmaßnahmen gegen ihren Nutzen abzuschätzen. Insbesondere der Einfluss von Cheating auf die breite Masse der Spieler muss analysiert werden, um z. B. den Grad zu bestimmen, bis zu dem böswilliges Verhalten toleriert wird, bzw. die Grenze, bei welcher der Betreiber des Online-Spiels zahlende Kunden verliert.

Durch die effiziente und praxisnahe Entwicklung von Präventiv- und Gegenmaßnahmen, welche die Angriffe auf interaktive Anwendungen einschränken oder verhindern, wird die Grundlage für neue derartige Anwendungen gebildet, bei denen die Sicherheit und Vertraulichkeit der Kommunikation eine große Rolle spielt, z. B. E-Learning, Echtzeitsimulationen, virtuelle soziale Netzwerke etc.

8.3.3 Gesundheitswesen

Zur wirksamen Behandlung von Krankheiten und weiteren klinischen Forschung wird IT im Gesundheitswesen hauptsächlich eingesetzt, um die klinischen Patientendaten zu dokumentieren, zu verwalten und zu verteilen. Es geht darum, die richtigen Informationen zur richtigen Zeit in angemessener Form den berechtigten Personen verfügbar zu machen. Da hochsensible Daten erfasst und ausgetauscht werden, stellt sich die Frage, welche Folgen riskante Entscheidungen zur Nutzung von Informationstechnik im Gesundheitswesen haben. Risiken in den eingesetzten IT-Verfahren sind im Gesundheitswesen von besonderer Bedeutung und gerade die zentrale Verfügbarkeit von gesundheitlich relevanten Informationen spielt dabei eine große Rolle. Krankenhausinformationstechnik und die elektronische Gesundheitsakte belegen diesen Trend. Bei der Konzeption solcher Systeme müssen

[390] Vgl. Ferris, Surridge, Glinka (2009).

in besonderem Maße Vorgaben des Datenschutzes berücksichtigt werden. Andersherum müssen allerdings auch bei der Weiterentwicklung des derzeitigen Rechtsstandes die Risiken der Nicht-Nutzung von IT für Patienten bewertet werden. Die Nichtverfügbarkeit von medizinischen Daten und das Fehlen von automatischen Erinnerungsfunktionen bzw. Warnsystemen bei Kontraindikationen erhöht das Risiko von Behandlungsfehlern. Zudem erzeugt es unnötige Arbeitsaufwände bei medizinischem Personal, welche in der heutigen gesellschaftlichen Situation des Ärztemangels und der steigenden Patientenzahlen problematisch sind.

Dem Management des IT-Risikos kommt in der Domäne Gesundheitswesen eine besondere Bedeutung zu. Es motiviert folgende Forschungsfragen:

- Welche Folgen können riskante Entscheidungen zur Nutzung oder Nicht-Nutzung von Informationstechnik im Gesundheitswesen haben?
- Wie kann das Rechtssystem die Voraussetzungen für die Gestaltung von Informationssystemen im Gesundheitswesen mit akzeptablem Risiko unterstützen?
- Wie muss IT im Gesundheitswesen konzipiert werden, um gesetzliche Anforderungen umzusetzen?

Zentrales Rechtsthema im Gesundheitswesen ist der Datenschutz. Grundsätzlich gilt ein Verbot der Weitergabe von Daten mit den Ausnahmen des Erlaubnisvorbehaltes und der expliziten Einwilligung. Weiterhin gelten die Grundsätze der Zweckbindung, der Erforderlichkeit, der Datenvermeidung bzw. -sparsamkeit und des Rechtes auf informationelle Selbstbestimmung. Im Krankenhaus bedeutet dies neben der berufsbedingten Schweigepflicht konkret, dass Daten nur im Behandlungszusammenhang erhoben und genutzt werden dürfen oder wenn eine Verwaltungsnotwendigkeit besteht. Für Universitätskliniken gilt außerdem, dass Daten auch für Forschung und Lehre weiterverwandt werden dürfen. Hier sind dann speziell Pseudonymisierung bzw. Anonymisierung zu beachten.

Bei der Nutzung von Patientendaten im Behandlungszusammenhang besteht allerdings das Risiko, dass nicht immer deutlich entschieden werden kann, welche Daten zum Behandlungskontext gehören und welche nicht. Beispielsweise ist die derzeitige Entscheidung hierzu im Universitätsklinikum Münster, dass nur Falldaten der eigenen Klinik sichtbar sind. Somit gehen allerdings wichtige Informationen über Erkrankungen und Therapien aus anderen Kliniken verloren. Wären diese verfügbar, hätten die behandelnden Ärzte eine breitere Entscheidungsbasis und könnten zudem Datenredundanzen vermeiden.

Zusätzlich zur Routineversorgung werden Patientendaten auch zur klinischen Forschung verwandt. Meistens geschieht die Datensammlung allerdings in gesonderten IT-Systemen

und es entsteht eine heterogene System- und Datenlandschaft, was das Finden und Auswerten von benötigten Informationen erschwert. Schnittstellen zwischen Systemen und geeignete Verfahren, um Daten aus den Systemen abzufragen, sind meistens nur unter erheblichen Kosten möglich, da Anbieter ihre Systeme weitestgehend „abschotten". Hier stellt sich die Frage, ob dies kartell- bzw. wettbewerbsrechtlich neu bewertet werden müsste.

Eine weitere Fragestellung im Rahmen von klinischen Studien und vor dem Hintergrund des Datenschutzes ist außerdem, wie Systeme gestaltet werden können, so dass behandelnde Ärzte auf potentielle Studienpatienten aufmerksam gemacht werden und Studienkoordinatoren Patienten gegebenenfalls sogar krankenhausübergreifend suchen und finden können.

Auch außerhalb des Krankenhauses gibt es viele Szenarien, an denen Recht und IT aufeinander treffen und es einer Neubewertung der Chancen und Risiken bedarf. Beispielsweise gibt es Bestrebungen, eine elektronische Medikamentenakte zur Übermittlung von Rezepten und zur Speicherung von ausgehändigten Medikamenten einzuführen. Dies wäre vorteilhaft, um bei gegebenen Kontraindikationen automatisch Warnungen ausgeben zu können. Allerdings stellt sich die Frage, wo diese Informationen gespeichert werden und wer welche Rechte auf Informationsspeicherung und ggf. -weitergabe hat.

Literaturverzeichnis

Andersen, K., & Henriksen, H. (2006). E-government maturity models: Extension of the Layne and Lee model. *Government Information Quarterly, 23(2)*, 236-248.

Araujo, B. d., Schmitz, E. A., Correa, A. L., & Alencar, A. J. (2010). A method for validating the compliance of business processes to business rules. In *2010 ACM Symposium on Applied Computing, Sierre, Switzerland* (S. 145-149). Retrieved from http://portal.acm.org/citation.cfm?id=1774088.1774117

Awad, A., & Weske, M. (2009). Visualization of compliance violation in business process models. In *5th Workshop on Business Process Intelligence BPI*. Retrieved from http://www.bpmn-editor.org/pub/Public/AhmedAwad/21-Awad.pdf

Awad, A., Decker, G., & Weske, M. (2008). In *Lecture Notes in Computer Science: Vol. 5240. Efficient Compliance Checking Using BPMN-Q and Temporal Logic. Business Process Management* (S. 326-341). Berlin: Springer. Retrieved from http://www.springerlink.com/index/v27691892m4m54qn.pdf

Awad, A., Weidlich, M., & Weske, M. (2009). Specification, Verification and Explanation of Violation for Data Aware Compliance Rules. In *Service-Oriented Computing/ServiceWave'09* (S. 500–515). Berlin: Springer. Retrieved from http://www.springerlink.com/index/GK48120165065717.pdf

Bächle, M. (1996). *Anforderungen an das Qualitätsmanagement der Softwareentwicklung, Produkt- und Prozeßnormen*. Retrieved from http://tobias-lib.uni-tuebingen.de/volltexte/2007/3113/pdf/abwi14.pdf

Back, A., Becker, J., König, W., Krallmann, H., Rieger, B., Scheer, A., Seibt, D., et al. (2001). *Lexikon der Wirtschaftsinformatik (4. Aufl.).* Berlin: Springer. Retrieved from http://books.google.com/books?id=KhnQer-rzRgC&pgis=1

Becker, J., Klose, K., & Schneider, M. (2003). Prozessmodellbasierte Vertragsgestaltung in überbetrieblichen Kooperationen. In P. Sinz, E. J. Plaha & M. Neckel (Hrsg.), *Modellierung betrieblicher Informationssysteme - MobIS* (S. 7-23). Bonn: Köllen.

Becker, J., Algermissen, L., & Falk, T. (2007). *Prozessorientierte Verwaltungsmodernisierung. Prozessmanagement im Zeitalter von E-Government und New Public Management*. Berlin: Springer.

Becker, J., Algermissen, L., Pfeiffer, D., & Räckers, M. (2007). Bausteinbasierte Modellierung von Prozesslandschaften mit der PICTURE-Methode am Beispiel der Universitätsverwaltung Münster. *Wirtschaftsinformatik*, 49(4), 267-279.

Becker, J., Delfmann, P., Herwig, S., & Lis, L. (2009c). A Generic Set Theory-based Pattern Matching Approach for the Analysis of Conceptual Models. In *Lecture Notes in Computer Science: Vol. 5829. Proceedings of the 28th International Conference on Conceptual Modeling (ER 2009)* (S. 41-54). Berlin: Springer.

Becker, J., Delfmann, P., Herwig, S., Lis, L., & Stein, A. (2009a). Towards Increased Comparability of Conceptual Models - Enforcing Naming Conventions through Domain Thesauri and Linguistic Grammars. In *Proceedings of the 17th European Conference on Information Systems, Verona, Italy (ECIS 2009*).

Becker, J., Delfmann, P., Herwig, S., Lis, L., & Stein, A. (2009b). Formalizing Linguistic Conventions for Conceptual Models. In *Lecture Notes in Computer Science: Vol. 5829. Proceedings of the 28th International Conference on Conceptual Modeling (ER 2009)* (S. 70-83). Berlin: Springer.

Beek, H., & Kaiser, T. (2000). Quantifizierung von Operational Risk mit Value-at-Risk. In L. Johanning & B. Rudolph (Hrsg.), *Handbuch Risikomanagement (Band 1): Risikomanagement für Markt-, Kredit- und operative Risiken* (S. 633-653). Bad Soden: Uhlenbruch.

Bell, M. (2009). Sonderbare Siegel-Flut. *Digital Business, 30*, 46-47.

Bergener, P., Pfeiffer, D., & Räckers, M. (2009). How to inform the point of single contact? – A business process based approach. In *Proceedings of the 9. Internationale Tagung Wirtschaftsinformatik: Business Services: Konzepte, Technologien, Anwendungen. (Band 2)* (S. 635-655). Wien: OCG.

BITKOM & DIN. (2009). Kompass der IT-Sicherheitsstandards, Leitfaden und Nachschlagewerk (4. Auflage). Berlin: Autor. Retrieved from http://www.bitkom.org/files/documents/Kompass_der_IT-Sicherheitsstandards_haftung_%282%29.pdf

BITKOM. (2006). Compliance im IT-Outsourcing. Berlin: Autor. Retrieved from http://webdoc.sub.gwdg.de/univerlag/2010/mkwi/01_management_und_methoden/it-_und_geschaeftsstrategien_in_der_globalisierung/02_compliance_im_it-outsourcing.pdf

BITKOM. (2007). *Verfahrensverzeichnis und Verarbeitungsübersicht nach BDSG*. Berlin: Autor.

BITKOM (2008). *IT-Risiko- und Chancenmanagement im Unternehmen*. Berlin: Autor. Retrieved from https://www.sicher-im-netz.de/files/documents/unternehmen/Bitkom_Leitfaden_IT-Risikomanagement.pdf

BITKOM. (2010). *Internet-Kriminelle weiten Aktivitäten aus*. Berlin: Autor. Retrieved from http://www.bitkom.org/de/presse/61330_61310.aspx

Blumberg, F. (2010). *Partei der „ digital natives "? Eine Analyse der Genese und Etablierungschancen der Piratenpartei*. Berlin: Konrad-Adenauer-Stiftung e.V.

Bock, W., Macek, G., Oberndorfer, T., & Pumsenberger, R. (2006). ITIL - Zertifizierung nach BS 15000 / ISO 20000. Bonn: Galileo Press.

Bräuhäuser, M., Blitzinger, P., & Lorenz, C. (2002). Qualitative Risikoanalyse – Methodische Vorgehensweise in der IT-Beratungspraxis. In P. Roßbach, P., H. Locarek-Junge (Hrsg.), IT-*Sicherheitsmanagement in Banken* (S. 55-69), Frankfurt a. M.: Bankakademie-Verlag.

Brauer, J. (2002). *DIN EN ISO 9001:2000 ff. umsetzen. Gestaltungshilfen zum Aufbau Ihres Qualitätsmanagementsystems (3. Aufl.)*. München: Hanser.

Brause, R. (2005). *Kompendium der Informationstechnologie*. Berlin: Springer. Retrieved from http://www.springerlink.com/content/rr73p025534505t8/?p=ae5c7fea626747adbed7987259172674&pi=1

Breaux, T. D., & Powers, C. (2009). Early Studies in Acquiring Evidentiary, Reusable Business Process Models for Legal Compliance. In *2009 Sixth International Conference on Information Technology: New Generations (Vol. 191), Las Vegas, Nevada* (S. 272-277).

BSI. (2009). *Zertifizierte IT-Sicherheit, Prüfstandards für IT-Sicherheit Technische Richtlinien und Schutzprofile*. Retrieved from https://www.bsi.bund.de/cae/servlet/contentblob/476492/publicationFile/51081/zertifizierte-IT_pdf.pdf

BSIG (2009). *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) vom 14.08.2009. BGBl I*. Retrieved from http://www.gesetze-im-internet.de/bundesrecht/bsig_2009/gesamt.pdf

Büschgen, H. E. (1998). *Bankbetriebslehre: Bankgeschäfte und Bankmanagement (5. Aufl.).* Wiesbaden: Gabler.

Bundesministerium für Bildung und Forschung. (2010). *Eckdaten zum Haushalt 2010*. Retrieved from http://www.bmbf.de/pub/Eckdaten_EPL30_2010.pdf

Bundesministerium für Umwelt Naturschutz und Reaktorsicherheit. (2010). *Kurzinfo Emissionshandel.* Retrieved from http://www.bmu.de/emissionshandel/kurzinfo/doc/4016.php

Bundesamt für Sicherheit in der Informationstechnik. (2009). *IT-Grundschutz-Kataloge 2009 - 11. Ergänzungslieferung - November 2009*. Retrieved from https://www.bsi.bund.de/cae/servlet/contentblob/478418/publicationFile/54741/it-grundschutz-kataloge_2009_EL11_de.pdf

Bundesamt für Sicherheit in der Informationstechnik. (2010). *Musterrichtlinien und Beispielkonzepte*. Retrieved from https://www.bsi.bund.de/cln_183/ContentBSI/grundschutz/kataloge/hilfmi/muster/musterrichtlinien/musterrichtlinien.html

Bundesanstalt für Finanzdienstleistungsaufsicht. (2009). *Mindestanforderungen an das Risikomanagement*. Retrieved from http://www.bafin.de/cln_170/nn_722758/SharedDocs/Veroeffentlichungen/DE/Service/Rundschreiben/2009/rs__0915__ba__marisk.html

Bundesministerium für Bildung und Forschung. (2010). *Haushalt*. Retrieved from http://www.bmbf.de/de/96.php

Bundesregierung. (2009). *REGIERUNGonline - Kleine und mittlere Unternehmen – Beispiele für Vereinfachungsmaßnahmen*. Retrieved from http://www.bundesregierung.de/Content/DE/StatischeSeiten/Breg/Buerokratieabbau/kleine-und-mittlere-unternehmen.html#doc810310bodyText19

Burkhardt, S. (2006). *Medienskandale. Zur moralischen Sprengkraft öffentlicher Diskurse*. Köln: Herbert von Halem Verlag.

Capgemini. (2009). *Smarter, Faster, Better eGovernment. 8th Benachmark Measurement*. Retrieved from http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/egov_benchmark_2009.pdf

COSO. (2001). *Unternehmensweites Risikomanagement - Übergreifendes Rahmenwerk.* New York: Autor.

CPSS, IOSCO. (2001). *Recommendations for Securities Settlement Systems*. Retrieved from http://www.bis.org/publ/cpss42.pdf

Däubler, W., Klebe, T., & Wedde, P. (1996). *Bundesdatenschutzgesetz*. Köln: Bund-Verlag.

Delfmann, P., Herwig, S., & Lis, L. (2009a). Konfliktäre Bezeichnungen in Ereignisgesteuerten Prozessketten – Linguistische Analyse und Vorschlag eines Lösungsansatzes. In *Proceedings des 8. GI-Workshops EPK 2009: Geschäftsprozessmanagement mit Ereignisgesteuerten Prozessketten. Berlin, Germany 2009.*

Delfmann, P., Herwig, S., & Lis, L. (2009b). Unified Enterprise Knowledge Representation with Conceptual Models - Capturing Corporate Language in Naming Conventions. In *Proceedings of the 30th International Conference on Information Systems (ICIS 2009). Phoenix, Arizona, USA, 2009*.

Delfmann, P., Herwig, S., Lis, L., & Stein, A. (2009a). Eine Methode zur formalen Spezifikation und Umsetzung von Bezeichnungskonventionen für fachkonzeptionelle Informationsmodelle. In *Lecture Notes in Informatics: Vol. 141. Proceedings der Tagung Modellierung betrieblicher Informationssysteme (MobIS) 2008. Saarbrücken* (S. 23-38). Bonn: Köllen.

Delfmann, P., Herwig, S., Lis, L., & Stein, A. (2009b). Supporting Distributed Conceptual Modelling through Naming Conventions. A Tool-based Linguistic Approach. *Enterprise Modelling and Information Systems Architectures, 4* (2), 3-20.

Deutsche Rentenversicherung & Bund. (2010). *ELENA - CEBIT Präsentation*.

Döben, E., Finetti, M., Köster, D. T., Pretzer, C., Rateike, D. J., Schiffer, H., Streier, D. E., et al. (2008). *Deutsche Forschungsgemeinschaft, Jahresbericht 2008*. Paderborn: Bonifatius Druck-Buch-Verlag.

Donsbach, W., Kepplinger, H. M., Mathes, R., Noelle-Neumann, E., Petersen, T., Reumann, K., Ricker, R., et al. (2003). Der Journalist. In E. Noelle-Neumann, W. Schulz & J. Wilke (Hrsg.), *Lexikon Publizistik Massenkommunikation*. Frankfurt a. M.: Fischer Taschenbuch Verlag, S. 78-125.

Dpa. (2010). Regierung prüft "Elena"-Stopp wegen Kostenexplosion. *Handelsblatt*. Retrieved from http://www.handelsblatt.com/newsticker/politik/regierung-prueft-elena-stopp-wegen-kostenexplosion;2613189

Eckhardt, J. (2008). Rechtliche Grundlagen der IT-Sicherheit. *Datenschutz und Datensicherheit - DuD, 32*(5), 330-336.

Eicker, S., Hegmanns, C., & Malich, S. (2007). *Auswahl von Bewertungsmethoden für Softwarearchitekturen*. Retrieved from http://www.icb.uni-due.de/fileadmin/ICB/research/research_reports/ICBReport14.pdf

Einhaus, C. (2005). *Potenziale des Wissensmanagements zur Behandlung operationeller Risiken in der Kreditwirtschaft*. Frankfurt a. M.: Frankfurt School Verlag.

Eisele, B. (2004). *Value-at-Risk-basiertes Risikomanagement in Banken*. Wiesbaden: Deutscher Universitätsverlag.

El Kharbili, M., Stein, S., Markovic, I., & Pulvermüller, E. (2008). Towards a framework for semantic business process compliance management. In A. S. Sadiq, M. Indulska & M. Z. Muehlen (Hrsg.), *GRCIS Workshop - CAISE Conference*. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.142.9939&rep=rep1&type=pdf

El Kharbili, M., De Medeiros, A., Stein, S., & van Der Aalst, W. (2008). *Business process compliance checking: Current state and future challenges. Modelling Business Information Systems* (S. 107-113). Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.146.547&rep=rep1&type=pdf

Erasim, E. (2002). *Sicherheit in Informationssystemen*. Zürich, Schweiz: vdf Hochschulverlag AG. Retrieved from http://books.google.com/books?id=4Mou1oyUZdQC&pgis=1

Esch, K., Klaudy, E. K., Micheel, B., & Stäbe-Blossey, S. (2006). *Qualitätskonzepte in der Kindertagesbetreuung*, 129-187. Berlin: Springer.

Eschweiler, J., & Psille, D. E. (2006). *Security@Work*. Berlin: Springer.

Federrath, H., & Pfitzmann, A. (2006). IT-Sicherheit. In M. Wind & D. Kröger (Hrsg.), *Handbuch IT in der Verwaltung* (S. 273-292). Berlin: Springer. doi:10.1007/3-540-46272-4_12

Feja, S., Witt, S., Brosche, A., Speck, A., & Prietz, C. (2010). Modellierung und Validierung von Datenschutzanforderungen in Prozessmodellen. In M. A. Wimmer et al. (Hrsg.), *Vernetzte IT für einen effektiven Staat - Gemeinsame Fachtagung Verwaltungsinformatik und Fachtagung Rechtsinformatik* (S. 155-166). Bonn: Köllen.

Ferris, J., Surridge, M., & Glinka, F. (2009). Securing Real-Time On-Line Interactive Applications in edutain@grid. In E. César, M. Alexander & A. Streit et al. (Hrsg.), *Lecture Notes in Computer Science*: Vol. 5415. *Euro-Par 2008 Workshops - Parallel Processing 2008*, S. 371-381. Berlin: Springer.

Fettke, P. (2009). Ansätze der Informationsmodellierung und ihre betriebswirtschaftliche Bedeutung: Eine Untersuchung der Modellierungspraxis in Deutschland. *zfbf – Schmalenbachs Zeitschrift für betriebswirtschaftliche Forschung, 8(5)*, 550-580.

Fettke, P., & Loos, P. (2004). Referenzmodellierungsforschung. *Wirtschaftsinformatik, 46(5)*, 331-340.

Fink, A., Schneidereit, G., & Voß, S. (2001). *Grundlagen der Wirtschaftsinformatik*. Heidelberg: Physica-Verlag.

FoeBuD e.V. (2010). Verfassungsbeschwerde ELENA Verfahrensgesetz. *FoeBud e.V.*. Retrieved from http://www.foebud.org/datenschutz-buergerrechte/arbeitnehmerdatenschutz/elena/verfassungsbeschwerde-elena-verfahrensgesetz.pdf/view

GamesBrief (2010). Retrieved from http://www.gamesbrief.com/2010/06/the-online-games-market-was-worth-15-billion-in-2009-and-will-grow-to-20-billion-in-2010/

Gassmann, M. (2010). Emissionshändler müssen besser aufpassen. *Financial Times Deutschland*. Retrieved from http://www.ftd.de/unternehmen/industrie/:nutzer-selber-schuld-emissionshaendler-muessen-besser-aufpassen/50069609.html

Gassmann, M. (2010). Emissionsstelle dichtet Sicherheitslecks ab. *Financial Times Deutschland*. Retrieved from http://www.ftd.de/unternehmen/industrie/:konsequenz-aus-phishing-attacken-emissionsstelle-dichtet-sicherheitslecks-ab/50078760.html

Gassmann, M. (2010). Hacker greifen Emissionshändler an. *Financial Times Deutschland*. Retrieved from http://www.ftd.de/unternehmen/finanzdienstleister/:gestohlene-co2-zertifikate-hacker-greifen-emissionshaendler-an/50069112.html

Gassmann, M. (2010). Phishing-Opfer verklagen Umweltbundesamt. *Financial Times Deutschland*. Retrieved from http://www.ftd.de/it-medien/medien-internet/:millionenschaeden-phishing-opfer-verklagen-umweltbundesamt/50137738.html

Geiger, H., & Piaz, J.-M. (2001). Identifikation und Bewertung von operationellen Risiken. In H. Schierenbeck, B. Rolfes & S. Schüller (Hrsg.), *Handbuch Bankcontrolling* (S. 789-802). Wiesbaden: Gabler.

Ghanavati, S., Amyot, D., & Payton, L. (2007). Towards a Framework for Tracking Legal Compliance in Healthcare. In J. Krogstie, A. Opdahl & G. Sindre (Hrsg.), *Lecture Notes in Computer Science: Vol. 4495. Proceedings of the 19th international conference on Advanced information systems engineering, Trondheim, Norway* (S. 218-232). Berlin: Springer.

Giblin, C., Liu, A. Y., Müller, S., Pfitzmann, B., & Zhou, X. (2005). Regulations expressed as logical models (REALM). In M.-F. Moens & P. Spyns (Hrsg.), *Proceedings of the 18th Annual Conference on Legal Knowledge and Information Systems* (S. 37-48). Brussels, Belgium: IOS Press. Retrieved from http://books.google.com/books?hl=en&lr=&id=5Ie3HI3t6qEC&oi=fnd&pg=PA37&dq=Regulations+expressed+as+logical+models+(REALM)&ots=AO2TpguuBa&sig=54hbeDIjWRW8OQtEMVnBujWwYVs

Giese, K. (2008). Funkende Kleidung. *Die Tageszeitung*. Retrieved from http://www.taz.de/1/politik/schwerpunkt-ueberwachung/artikel/1/funkende-kleidung/

Glinka, F., Ploss, A., Gorlatch, S., & Müller-Iden, J. (2008). High-level development of multiserver online games. *International Journal of Computer Games Technology, 5*, 1-16.

Goedertier, S., & Vanthienen, J. (2006). Designing compliant business processes with obligations and permissions. In S. D. J. Eder (Hrsg.), *Lecture Notes in Computer Science: Vol. 4103. Business Process Management Workshops* (S. 5–14). Berlin: Springer. Retrieved from http://www.springerlink.com/index/U726682846184JW0.pdf

Goeken, M., & Knackstedt, R. (2007). Multidimensional Reference Models for Data Warehouse Development. In J. Filipe et al. (Hrsg.), *Proceedings of the 9th Inter-*

national Conference on Enterprise Information Systems, ICEIS 2007, June 2007 Funchal/Portugal. Berlin: Springer.

Goeken, M., & Knackstedt, R. (2008). Referenzmodellgestütztes Compliance Reporting am Beispiel der EU-Finanzmarktrichtlinie MiFID. *HMD – Praxis der Wirtschaftsinformatik 263*, 47-57.

Göttsche, M. (2009). Betrieb im neuen UKE nach Plan angelaufen. *TOPNEWS.de*. Retrieved from http://www.topnews.de/betrieb-im-neuem-uke-nach-plan-angelaufen-335283

Gola, P., & Schomerus, R. (2007). *Bundesdatenschutzgesetz*. München: Beck.

Goltsche, W. (2006). *COBIT - kompakt und verständlich*. Wiesbaden: Vieweg+Teubner.

Gorlatch, S., Meiländer, D., Bartholomäus, S., Fujita, H., Theurl, T., Hoeren, T., Heghmanns, M., & Boers, K. (2010). Cheating Prevention in Virtual Worlds: Software, Economic and Law Aspects. *New Trends in Software Methodologies, Tools and Techniques - Proceedings of the 9th SoMeT_10,* (S. 268-289), IOS Press.

Gouscos, D., Kalikakis, M., Legal M., & Papadopoulou S. (2007). A general model of performance and quality for one-stop e-Government service offerings. *Government Information Quarterly, 24(4)*, 860-885.

Governatori, G. (2005). Representing business contracts in RuleML. *International Journal of Cooperative Information Systems, 142(3),* 181–216. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.94.3345&rep=rep1&type=pdf

Haarmeyer, J. (2009). Das interne Protokoll der Computer Panne im UKE. *Hamburger Abendblatt*. Retrieved from http://www.abendblatt.de/hamburg/kommunales/article1105084/Das-interne-Protokoll-der-Computer-Panne-im-UKE.html

Hackel, S., & Roßnagel, A. (2008). Langfristige Aufbewahrung elektronischer Dokumente. In D. Klumpp, H. Kubicek, A. Roßnagel & W. Schulz (Hrsg.), *Informationelles Vertrauen für die Informationsgesellschaft (S. 199-207).* Berlin: Springer.

Hansen, R., & Neumann, G. (2001). *Wirtschaftsinformatik 1*. Stuttgart: UTB.

Hechenblaikner, A. (2006). *Operational Risk in Banken*, 8-30. Wiesbaden: DUV. doi: 10.1007/978-3-8350-9269-3.

Heilmann, H., & Kneuper, R. (2003). CMM(I) - Capability Maturity Model (Integration). Ein Rahmen zur Gestaltung von Softwareentwicklungsprozessen. In H. Heilmann & S. Strahringer (Hrsg.), *HMD - Praxis der Wirtschaftsinformatik: Heft 231. Neue Konzepte in der Softwareentwicklung* (S. 63 – 70). Heidelberg: dpunkt.verlag GmbH.

Heinrich, D. D., Heinzl, D. D., & Roithmayr, M. D. (2004). *Wirtschaftsinformatik-Lexikon*. München: Oldenbourg.

Helmbrecht, U. (2009). *Leitfaden Informationssicherheit - IT- Grundschutz kompakt*. Bonn: BSI.

Heng, S. (2009). Ernstzunehmender Wirtschaftsfaktor mit viel Potenzial – PC-Games, Konsolen-Games und mobile Games. *Deutsche Bank Research 72*. Retrieved

from http://www.dbresearch.de/PROD/DBR_INTERNET_DE-PROD/PROD0000000000242755.pdf

Hermann, D. (2003). *Using the common criteria for IT security evaluation*. New York, USA: Auerbach Publications. Retrieved from http://books.google.com/books?hl=de&lr=&id=-ec_jID0LJIC&pgis=1

Hirschmann, S., &, Romeike, F. (2004). *IT-Sicherheit als Ratingfaktor*. RATINGaktuell, 1, 12-18.

Heschl, J. &, Middelhoff, D. (2005). *IT Governance - Modelle zur Umsetzung und Prüfung*. Norderstedt: Books on Demand GmbH.

Hodel, M., Berger, A., & Risi, P. (2006). *Outsourcing realisieren*. Wiesbaden: Vieweg+Teubner. Retrieved from http://books.google.de/books?hl=de&lr=&id=kESyU9qAV1sC&oi=fnd&pg=PR5&dq=risiken+beim+outsourcing&ots=jUw_O1kgh8&sig=k5r5HhOglcV6y1reB8DkmZt88SA#v=onepage&q=Risiken&f=false

Hoeren, T. (2007). *IT-Vertragsrecht*, Köln: Verlag Otto Schmidt.

Hoeren, T. (2010). *Online-Skript Internetrecht*, Retrieve from http://vg00.met.vgwort.de/na/8181c8ca7c1ad67f6567?l=http://www.uni-muenster.de/Jura.itm/hoeren/materialien/Skript/Skript_Internetrecht_Februar2010.pdf

Hoeren, T. (2008). *IT-Verträge*.

Hoeren, T. (2010). *IT-Recht*. Retrieved from http://www.uni-muenster.de/Jura.itm/hoeren/materialien/Skript/Skript_IT-Recht_Februar2010.pdf

Hoeren, T., & Spittka, J. (2009). Aktuelle Entwicklungen des IT-Vertragsrechts - ITIL, Third Party Maintainance, Cloud Computing und Open Source Hybrids. *MMR, 583.*

Hoglund, G., & McGraw, G. (2007). *Exploiting Online Games: Cheating Massively Distributed Systems*. Toronto: Addison-Wesley Professional

Hogrebe, F., & Nüttgens, M. (2008). Integrierte Produkt- und Prozessmodellierung: Rahmenkonzept und Anwendungsfall zur EU-Dienstleistungsrichtlinie. In P. Loos, M. Nüttgens, K. Turowski & D. Werth (Hrsg.), Lecture Notes in Informatics: Band 141. *Proceedings of the Modellierung betrieblicher Informationssysteme (MobIS) 2008* (S. 239-252). Bonn: Köllen.

Hohler, B. (2007). Qualitätsmanagement bei der Software-Entwicklung. In W. Masing & R. Schmitt (Hrsg.), *Handbuch Qualitätsmanagement* (S. 817-846). München: Hanser. Retrieved from http://books.google.de/books?hl=de&lr=&id=vox39Ud7QLUC&oi=fnd&pg=PR5&dq=37.4+%22Qualit%C3%A4tsmerkmale+von+Software%22&ots=_lR5ix7U50&sig=MdwGM85isVB7y10pDj8nZPN-Xm8#v=onepage&q=37.4%22Qualit%C3%A4tsmerkmale von Software%22&f=false

Hohler, B., & Villinger, U. (1998). Normen und Richtlinien zur Prüfung und Qualitätssicherung von Steuerungssoftware. *Informatik-Spektrum, 21*, 63-72.

IDS Scheer AG. (2008). *Governance, Risk & Compliance Management with ARIS.*

idw - idw Aktuell. Düsseldorf: Autor. Retrieved from http://idw-online.de/de/idwnews

IDW. (2008). *Entwurf IDW Prüfungsstandard: Projektbegleitende Prüfung bei Einsatz von Informationstechnologie (IDW EPS 850)*. Düsseldorf: Autor. Retrieved from http://www.iwi.uni-annover.de/cms/images/stories/upload/lv/sosem08/ITG/idw_20eps_20850.pdf

Ishii, K., & Lutterbeck, B. (2000). *Ein Blick zurück: Anfänge der EDV und des Datenschutzes in der Bundesrepublik Deutschland*. Retrieved from http://ig.cs.tu-berlin.de/oldstatic/w99/1332l501/t11-02/

IT Governance Institute. (2005). *CoBiT 4.0 Deutsche Version*. Rolling Meadows: Autor.

IT Governance Institute. (2007). *CoBiT 4.1. Deutsche Version*. Rolling Meadows: Autor.

IT Governance Institute. (2008). *IT Governance Global Status Report - 2008*. Rolling Meadows: Autor.

Jahberg, H. (2010). Datenskandale - Die Dunkelziffer ist hoch. *Der Tagesspiegel*. Retrieved from http://www.tagesspiegel.de/wirtschaft/verbraucher/die-dunkelziffer-ist-hoch/1542016.html

Johannsen, W., & Goeken, M. (2006). IT-Governance - Neue Aufgaben des IT-Managements. In S. Strahringer & H. Fröschle (Hrsg.), *Praxis der Wirtschaftsinformatik: Vol. 250* (S. 7-17). Heidelberg: dpunkt.verlag GmbH.

Karagiannis, D. (2008). A business process-based modelling extension for regulatory compliance. In M. Bichler, T. Hess, H. Krcmar, U. Lechner, F. Matthes, A. Picot, B. Speitkamp & P. Wolf (Hrsg.), *Multikonferenz Wirtschaftsinformatik* (S. 1159-1173). Retrieved from http://ibis.in.tum.de/mkwi08/17_IT-Risikomanagement_-_IT-Projekte_und_IT-Compliance/07_Karagiannis.pdf

Karimi, J. (1988). Strategic Planning for Information Systems: Requirements and Information Engineering Methods. *Journal of Management Information Systems, 4(4)*, 5-24.

Kaufmann, M. (2008). Best of Datenschluder. *Manager Magazin*. Retrieved from http://www.manager-magazin.de/unternehmen/it/0,2828,druck-576086,00.html

Kepplinger, H. M. (2001). Die *Kunst der Skandalierung und die Illusion der Wahrheit*. München: Olzog Verlag.

Kepplinger, H. M. (2009). *Publizistische Konflikte und Skandale*. Wiesbaden: VS Verlag für Sozialwissenschaften.

Kepplinger, H. M., Ehming, S. C., & Hartung, U. (2002). *Alltägliche Skandale. Eine repräsentative Analyse regionaler Fälle*. Konstanz: UVK Verlagsgesellschaft mbH.

Kersten. H. (1995). *Sicherheit in der Informationstechnik: Einführung in Probleme, Konzepte und Lösungen*. München: Oldenbourg.

Klein, M. (2010). ELENA: Technische Probleme sorgen für mangelnde Transparenz. *eGovernment Computing*. Retrieved from http://www.egovernment-computing.de/projekte/articles/258763/

Klempt, P. (2007). *Effiziente Reduktion von IT-Risiken im Rahmen des Risikomanagementprozesses*. Dissertation, Ruhr-Uni Bochum. Retrieved from http://www-brs.ub.ruhr-uni-bochum.de/netahtml/HSS/Diss/KlemptPhilipp/diss.pdf

Knackstedt, R., Eggert, M., Gräwe, L., & Spittka, J. (2010). Forschungsportal für Rechtsinformatik und Informationsrecht. *Multimedia und Recht, 8*, 528-532.

Knackstedt, R., Lis, Ł., Stein, A., Becker, J., & Barth, I. (2009). Towards a Reference Model for Online Research Maps. *Proceedings of the European Conference on Information Systems (ECIS 2009)*.

Knackstedt, R. (2004). *Fachkonzeptionelle Referenzmodellierung einer Managementunterstützung mit quantitativen und qualitativen Daten. Methodische Konzepte zur Konstruktion und Anwendung*. Dissertation, Universität Münster.

Knackstedt, R., Brelage, C., & Kaufmann, N. C. (2006). Entwicklung rechtssicherer Web-Anwendungen Strukturierungsansatz, State-of-the-Art und ausgewählte Aspekte der fachkonzeptionellen Modellierung. *Wirtschaftsinformatik, 48*, 27-35.

Knackstedt, R., & Klose, K. (2005). Configurative Reference Model-Based Development of Data Warehouse Systems. In M. Khosrow-Pour (Hrsg.), *Managing Modern Organizations With Information Technology, Information Resources Management Association International Conference* (S. 32-39), Hershey, USA: IGI Publishing.

Kneuper, R. (2003). *CMMI - Verbesserung von Softwareprozessen mit Capability Maturity Model Integration*. Heidelberg: dpunkt.verlag GmbH.

Kolb, S. (2005). *Mediale Thematisierung in Zyklen: Theoretischer Entwurf und empirische Anwendung*. Köln: Herbert von Halem Verlag.

Königs, H. (2009). *IT-Risiko-Management mit System: Von den Grundlagen bis zur Realisierung - Ein praxisorientierter Leitfaden*. Wiesbaden: Vieweg+Teubner. Retrieved from http://books.google.com/books?hl=de&lr=&id=FFzDIdRnCBEC&pgis=1

Kottemann, J. E., & Konsynski, B. R. (1984). Information Systems Planning and Development: Strategic Postures and Methodologies. *Journal of Management Information Systems, 1(2)*, 45-63.

Krcmar. H. (2000). *Informationsmanagement*. Berlin: Springer.

Kroehnert, M. (2010). Emissionsbrief 01-2010. *Emissionshändler.com*. Retrieved from http://www.emissionshaendler.com/emh/PDF-Dateien/Emissionsbriefe 2010/CO2-Emissionsbrief 01-2010 Online-Raub und VAT-Betrug.pdf

Laue, P. (2009). *Vorgangsbearbeitungssysteme in der öffentlichen Verwaltung*. Kassel: University Press.

Layne, K., & Lee, J. (2001). Developing fully functional E-Government: A four stage model. *Government Information Quarterly, 18(2)*, 122-136.

Lenk, K., Fiedler, H., Reinermann, H., & Traunmüller, R. (1997*). Informatik in Recht und Verwaltung*. Heidelberg: von Decker.

Liggesmeyer, P. (2009). *Software-qualität: Testen, analysieren und verifizieren von Software*. Berlin: Spektrum Akademischer Verlag. Retrieved from http://books.google.com/books?hl=de&lr=&id=-eoerZI2fYIC&pgis=1

Luhmann, N. (1983). *Politische Planung. Aufsätze zur Soziologie von Politik und Verwaltung*. Opladen: Westdeutscher Verlag.

Ly, L., Knuplesch, D., Rinderle-Ma, S., & Goeser, K. (2010). SeaFlows Toolset-Compliance Verification Made Easy. In *CAiSE'10 Forum. Hammamet, Tunisia.* Retrieved from http://dbis.eprints.uni-ulm.de/662/

Moeller, R. R. (2007). *COSO Enterprise Risk Management*. Hoboken: John Wiley & Sons.

Moon, M. J. (2002). The Evolution of E-Government among Municipalities: Rhetoric or Reality?. *Public Administration Review, 62(4)*, 424-433. doi:10.1111/0033-3352.00196

Moos, F. (2010). Die Entwicklung des Datenschutzrechts im Jahr 2009. *K&R 2010, 3*, 166-173.

Namiri, K., & Stojanovic, N. (2007). Pattern-based design and validation of business process compliance. *Lecture Notes in Computer Science*, 4803, 59-76.

Nicklisch, F. (1987). *Der komplexe Langzeitvertrag*, Heidelberg: Müller, Jur. Verl.

o. V. (2000). Duden. Das Fremdwörterbuch (S. 823). Mannheim: Bibliographisches Institut & F. A. Brockhaus AG.

o. V. (2010a). Archiv. *BigBrother-Awards Deutschland*. Retrieved from http://www.bigbrotherawards.de/archive

o. V. (2010b). Themen. *Bundesamt für Sicherheit in der Informationstechnik*. Retrieved from https://www.bsi.bund.de/cln_183/sid_F09200F4583C0CA86614C211F384BB49/DE/Themen/themen_node.html

o. V. (2010c). Gesundheitskarte. *Bundesministerium für Gesundheit*. Retrieved from http://www.bmg.bund.de/DE/Gesundheit/Gesundheitskarte-Focuspage/gesundheitskarte__node.html

o. V. (2010d). Club. *Chaos Computer Club*. Retrieved from http://www.ccc.de/de/club

o. V. (2010e). Themen. *Chaos Computer Club*. Retrieved from http://www.ccc.de/de/topics

o. V. (2010f). DANA – Die Datenschutznachrichten. *Deutsche Vereinigung für Datenschutz*. Retrieved from http://datenschutzverein.de/datenschutznachrichten.html

o. V. (2010g). Elena soll gestoppt werden. *FOCUS*.Retrieved from http://www.focus.de/finanzen/recht/arbeitnehmerdaten-elena-soll-gestoppt-werden_aid_526715.html

o. V. (2010h). Informationen zu ELENA. *FoeBud e. V.* Retrieved from https://petition.foebud.org/FoeBuD/informationen-zu-elena

o. V. (2010i). Metro-Skandal. *FoeBud e. V.* Retrieved from http://www.foebud.org/rfid/metro/

o. V. (2010j). FoeBud e. V. Über uns. Retrieved from http://www.foebud.org/aboutus

o. V. (2010k).Metro-Skandal. *Telepolis*. Retrieved from http://www.heise.de/tp/r4/artikel/16/16803/1.html

o. V. (2010l). *Aktion: Stoppt die e-Card*. Retrieved from http://www.stoppt-die-e-card.de/index.php?/pages/aktion.html

o.V. (2010m). Scandal. *Encyclopedia Britannica Online*. Retrieved from http://www.britannica.com/bps/dictionary?query=scandal

o.V. (2010n). Deutsche *Vereinigung für Datenschutz. Vereinsprofil*. Retrieved from http://www.datenschutzverein.de/vereinsprofil_dvd.html

o.V. (1985). Skandal. In W. Müller (Hrsg.), *Duden Bedeutungswörterbuch*. Mannheim: Bibliographisches Institut & F. A. Brockhaus AG.

o.V. (1989). Skandal. In G. Drosdowski (Hrsg.), *Duden Etymologie: Herkunftswörterbuch der deutschen Sprache*. Mannheim: Bibliographisches Institut & F. A. Brockhaus AG.

Office of Government Commerce. (2007). *ITIL: Continual Service Improvement*. London: The Stationary Office.

Office of Government Commerce. (2007). *ITIL: Service Design*. London: The Stationary Office.

Office of Government Commerce. (2007). *ITIL: Service Operation*. London: The Stationery Office.

Office of Government Commerce. (2007). *ITIL: Service Strategy*. London: The Stationary Office.

Office of Government Commerce. (2007). *ITIL: Service Transition*. London: The Stationary Office.

Olbrich, A. (2006). *ITIL - kompakt und verständlich*. Wiesbaden: Vieweg+Teubner.

Olbrich, S., & Simon, C. (2005). The Influence of Legal Constraints on business pro-cess Modeling. In O. D. Sarikas, Z. Irani & T. Elliman (Hrsg.), *Proceedings of the eGovernment Workshop '05 (eGOV05) Vol. 05* (S. 1-13). London: Citeseer. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.98.419&rep=rep1&type=pdf

Pallas, F. (2008). Recht, Informatik und Neue Institutionenökonomik. Beitrag zum Wissenschaftlichen Forum Recht und Informatik (WiFoRI) von DSRI und DGRI, Würzburg, 14. März 2008.

Patalong, F. (2010). Wirtschaftsministerium will Nachbesserungen bei Elena-Datenbank. *Spiegel Online*. Retrieved from http://www.spiegel.de/netzwelt/netzpolitik/0,1518,druck-687304,00.html

Philipp, M. (1999). Software-Zertifizierung nach IDW PS 880. In *Proceedings 3rd Conference on Quality Engineering in Software Technology and VDE-ITG Workshop on Testing Non-Functional Software-Requirements (CONQUEST '99)* (S. 154-162). Retrieved from http://www.home.hs-karlsruhe.de/~phma0001/pub/conquest99.pdf

Piaz, J.-M. (2002). Risiko und Risikomanagement. In J.-M. Piaz (Hrsg.), *Operational Risk Management bei Banken* (S. 9-28). Zürich: Versus Verlag.

Pritchard, M. (2000). How to Hurt the Hackers: The Scoop on Internet Cheating and How You Can Combat It. *Gamasutra.com*. Retrieved from http://www.gamasutra.com/view/feature/3149/

Probst, A., & Röder, T. (2007). *Revisionssicherheit bei CMS bzw. DMS*. Retrieved from http://cms.fh-augs-

burg.de/report/2007/Probst_Andreas__Roeder_Thomas/RevisionssichereArchivierung.pdf

Project Management Institute. (2004). *A guide to the project management body of knowledge: PMBOK guide* (3. Auflage). Philadelphia: Autor.

Prokein, O. (2008). IT-Risiko und IT-Risikomanagement. In A. Picot, R. Reichwald, E. Franck & K. Möslein (Hrsg.), *IT-Risikomanagement* (S. 7-18). Wiesbaden: Gabler. Retrieved from http://www.springerlink.com/content/u5973522v8q5g67r

Raab, P., & Siegl, M. (2007). Nutzung von Kundendaten zur Minimierung des Forderungsausfallrisikos im Distanzhandel. *Wirtschaftsinformatik, 49(1),* 34-41.

Rath, M. (2009). Rechtliche Aspekte von IT-Compliance. In G. Wecker & H. van Laak (Hrsg), *Compliance in der Unternehmenspraxis* (S.149-165). Wiesbaden: Gabler. doi:10.1007/978-3-8349-8282-7

Recker, J., Rosemann, M., Indulska, M., & Green, P. (2009). Business process modeling: a comparative analysis. *Journal of the Association for Information Systems,* 10(4), 333-363.

Reichl, H., Roßnagel, A., & Müller, G. (2005). *Digitaler Personalausweis – Eine Machbarkeitsstudie*. Wiesbaden: Vieweg+Teubner.

Richter, H. (2010). Finanzamtsdaten auf dem Flohmarkt. *donaukurier.de*. Retrieved from http://www.donaukurier.de/nachrichten/bayern/Ingolstadt-Finanzamtsdaten-auf-dem-Flohmarkt;art155371,2288104

Richters, M., & Gogolla, M. (1998). On Formalizing the UML Object Constraint Language OCL. In T. W. Ling, S. Ram & M.-L. Lee (Hrsg.), *Lecture Notes in Computer Science: Vol. 1507. Proceedings of the 17th International Conference on Conceptual Modeling 1998* (S. 449-464). Berlin: Springer. Retrieved from http://www.springerlink.com/content/74bxqmgu9uted4fq

Ritschel, A., Hochstein, A., Josi, M., & Brenner, W. (2006). SOX-IT-Compliance bei Novartis. In H. Fröschle & S. Strahringer (Hrsg.), *Praxis der Wirtschaftsinformatik, Heft 250: IT-Governance* (S. 68 -77). Heidelberg: dpunkt.Verlag GmbH.

Rohde-Liebenau, B. (2007). Förderung der Corporate Compliance: „Mehr Zuckerbrot als Peitsche?“. *ERA Forum, 8(2),* 273-287. doi:10.1007/s12027-007-0019-2

Romeike, F. (2003). Risikoidentifikation und Risikokategorien. In F. Romeike & R. Finke (Hrsg.), *Erfolgsfaktor Risiko-Management* (S. 165-180). Wiesbaden: Gabler.

Romeike, F., & Hager, P. (2009). *Erfolgsfaktor Risiko-Management 2.0: Methoden, Beispiele, Checklisten*. Wiesbaden: Gabler. Retrieved from http://books.google.com/books?id=UX0uc8M8iuQC&pgis=1

Rosenkranz, F., & Missler-Behr, M. (2005). *Unternehmensrisiken erkennen und managen – Einführung in die quantitative Planung*. Springer: Heidelberg.

Rost, M., & Pfitzmann, A. (2009). Datenschutz-Schutzziele—revisited. *Datenschutz und Datensicherheit - DuD, 33(6),* 353–358. Berlin: Springer. Retrieved from http://www.springerlink.com/index/C31U58K320074028.pdf

Rüeck, J., & Römer, F. (2010). Datenschutz-Skandal in Schwaigern. *STIMME.de*. Retrieved from http://www.stimme.de/heilbronn/nachrichten/region/sonstige;art16305,1718480

Rünger, P., & Walther, U. (2004). *Die Behandlung der operationellen Risiken nach Basel II - ein Anreiz zur Verbesserung des Risikomanagements?*. Retrieved from http://fak6.tu-freiberg.de/fileadmin/Fakultaet6/alleArbeitspapiere25.9.2008/paper/2004/walther_14_2004.pdf

Schaich, P. D., Schmidt, K., & Weber, P. D. (2010). Stichwort: Risiko. In Gabler Verlag (Hrsg.), *Gabler Wirtschaftslexikon*. Wiesbaden: Gabler. Retrieved from http://wirtschaftslexikon.gabler.de/Archiv/6780/risiko-v9.html

Schierenbeck, H., & Lister, M. (2002). Risikomanagement im Rahmen der wertorientierten Unternehmenssteuerung. In R. Hölscher & R. Elfgen (Hrsg.), *Herausforderung Risikomanagement: Identifikation, Bewertung und Steuerung industrieller Risiken* (S. 181-204). Wiesbaden: Gabler.

Schleicher, D., Anstett, T., Leymann, F., & Mietzner, R. (2009). Maintaining Compliance in Customizable Process Models. In R. Meersman, T. Dillon & P. Herrero (Hrsg.), *Lecture Notes in Computer Science: Vol. 5870. On the Move to Meaningful Internet Systems: OTM 2009* (S. 60-75). Berlin: Springer. doi:10.1007/978-3-642-05148-7

Schömig, B. (2010). *Defizite beim Datenschutz*. Retrieved from http://kommune21.de/web/de/verwaltung,285_0_0_82.5,10436

Schwögler, S. (2008). Prüfsiegel ist eine Pflichtvoraussetzung für viele Anwendungen im Hochsicherheitsbereich Aruba Networks erhält als erster WLAN-Hersteller die Common-Criteria-Zertifizierung. *Computer Zeitung, 37,* 1-3.

Seibold, H. (2006). *IT-Risikomanagement*. München: Oldenbourg. Retrieved from http://books.google.com/books?hl=de&lr=&id=nFBQlUdXRyQC&pgis=1

Siegmund, T. (2010). Breite Front gegen Datensammelprojekt. *Handelsblatt*. Retrieved from http://www.handelsblatt.com/politik/deutschland/elena-breite-front-gegen-datensammelprojekt;2613656

Software Engineering Institute. (2006). *CMMI® for Development, Version 1.2*. Pittsburgh: Autor.

Software Engineering Institute. (2007). *CMMI® for Acquisition, Version 1.2.* Pittsburgh: Autor. Retrieved from http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA474820

Software Engineering Institute. (2009). *CMMI® for Services, Version 1.2*. Pittsburgh: Autor. Retrieved from http://www.sei.cmu.edu/reports/09tr001.pdf

Sowa, A. (2010). IT-relevante Aspekte einer Prüfung von Datenschutz-Compliance. *Datenschutz und Datensicherheit - DuD, 342*, 104-107. doi:10.1007/s11623-010-0045-z

Spindler, G. (2007). *Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären. Informationstechnik*. Bonn: BSI.

Strohmeier, G. (2004). *Politik und Massenmedien: Eine Einführung*. Baden-Baden: Nomos.

Taeger, J., & Gabel, D. (2010). *Kommentar zum BDSG*. Frankfurt a. M.: Recht und Wirtschaft.

Teubner, A., & Feller, T. (2008). Informationstechnologie, Governance und Compliance. *Wirtschaftsinformatik, 50(5),* 400-407. doi:10.1007/s11576-008-0081-6

Theil, M. (1995). *Risikomanagement für Informationssysteme*. Wien: Service Verlag.

Thompson, J. B. (2000). *Political Scandal. Power and visibility in the media age*. Malden, USA: Polity Press.

Vetter, E. (2007). Compliance in der Unternehmerpraxis. In G. Wecker & H. van Laak (Hrsg.), *Compliance in der Unternehmerpraxis* (S. 33-47). Wiesbaden: Gabler. Retrieved from http://www.springerlink.com/index/T6825J82G459K406.pdf

Video Game Sales Wiki (2009). *Video game industry*. Retrieved from http://vgsales.wikia.com/wiki/Video_game_industry

Wagner, K., & Dürr, W. (2008). *PP 051N: Reifegrad nach ISO/IEC 15504*. München: Hanser. Retrieved from http://books.google.com/books?hl=de&lr=&id=FcUtBM8mrR0C&pgis=1

Wallmüller, E. (2007). *SPI-Software Process Improvement mit Cmmi und ISO 15504.* München: Hanser. Retrieved from http://books.google.com/books?id=xutSHYjv9v4C&pgis=1

Walter, S. (2006). Computerlinguistische Methoden für die Rechtsterminologie. In E. Schweighofer, D. Liebwald, M. Drachsler & A. Geist (Hrsg.), *e-Staat und e-Wirtschaft aus rechtlicher Sicht - Tagungsband des 9. Internationalen Rechtsinformatik Symposions IRIS 2006* (S. 303-309). Stuttgart: Boorberg. Retrieved from http://www.coli.uni-saarland.de/projects/corte/IRIS05Beitrag.pdf

Weber, M. (1922). Wesen, Voraussetzung und Entfaltung der bürokratischen Herrschaft. In M. Weber (Hrsg.), *Wirtschaft und Gesellschaft* (S. 551-569). Tübingen: Mohr.

Weske, M. (2007). *Business Process Management: Concepts, Languages, Architec-tures.* Berlin: Springer. Retrieved from http://books.google.com/books?hl=de&lr=&id=QMyu_B1KTZIC&oi=fnd&pg=PA3&dq=Business+Process+Management:+Concepts,+Languages,+Architectures&ots=pXdSyGYnD1&sig=cwY7pDQqp9P40hArKV_tOiX6dKE

Wildhaber, B. (1993). *Informationssicherheit: Rechtliche Grundlagen und Anforderungen an die Praxis*. Zürich: Schulthess Polygraphischer Verlag.

Wimmer, M. A. (2002). Integrated Service Modelling for Online One-stop Government. *Electronic Markets, 12(3),* 149-156.

Wolters, T., & Ostrop, P. (2010). Datenleck bei Kommunen. *Ruhrnachrichten*. Retrieved from http://www.ruhrnachrichten.de/nachrichten/region/hierundheute/art1544,891534

Wunder, O. (2009). UKE-Skandal um Kranken-Daten. *Hamburger Morgenpost*. Retrieved from http://archiv.mopo.de/archiv/2009/20090228/hamburg/uke_skandal_um_kranken_daten.html

Yu, C.-C. (2009). Role-Based and Service-Oriented Security Management in the E-Government Environment. In M. A. Wimmer, H. J. Scholl, M. Janssen & R.

Traunmüller (Hrsg.), *Lecture Notes in Computer Science: Vol. 5693. Electronic Government – 8th International Conference, EGOV 2009, Linz, Austria, August/September 2009 Proceedings* (S. 364-375). Berlin: Springer.

IV Anhang

A Verzeichnis recherchierter IT-Skandale

Zeitpunkt/ Zeitraum der Datenverarbeitung	Beschreibung - kurz	Institution/ Unternehmung (Datenherkunft)	Bereich	Betroffene	Anzahl betroffener Personendaten
29.10.2009	Stadtwerke München: Gehälter der Aufsichtsräte in Massen-E-Mail verschickt	Stadtwerke München GmbH	Wirtschaft	Leitende Mitarbeiter	16
23.11.2009	AOK Niedersachsen schickt sensible Patientendaten an unbeteiligten Apotheker	AOK Niedersachsen	Wirtschaft	Versicherte	30
18.2.2010	Interne Daten von 40 Unternehmen offen zugänglich im Internet	Struktur- und Wirtschaftsförderungsgesellschaft (SWFG) und die Luckenwalder Regionalstelle der Industrie- und Handelskammer	Politik	Unternehmen	40
15.4.2009	Kandidatenliste für das Amt des Kulturbürgermeisters offen im Netz	Stadt Leipzig	Politik	Bürger	48
2005-2006	Überwachung hochrangiger Leute der Wirtschaft & Öffentlichkeit	Deutsche Telekom	Wirtschaft	Mitarbeiter	55
24.5.2008	Spitzelskandal bei der Deutschen Telekom	Aufsichtsräte, Manager und Journalisten	Wirtschaft	Leitende Mitarbeiter, Journalisten	55
1.11.2009	Datenversand an privates Mailpostfach	Alice	Wirtschaft	Neukunden	172
03.6.2009	Märkische Klinik: Zwei Festplatten mit Patientendaten verschwunden	Märkische Kliniken	Gesundheitswesen	Patienten	200
15.10.2008	Datenpanne bei Kinderkanal - Daten von Kindern waren zeitweise ungeschützt einsehbar	Kinderkanal	Medien	Online-Nutzer	200
30.3.2009	Abwrack-Prämie: Panne bei Onlinereservierung	Bundesamt für Wirtschaft und Ausfuhrkontrolle	Politik	Bürger	200
2007	Sicherung privater Dateien & Mails auf den Computern von Polizeibeamten zur möglichen späteren Bearbeitung/ Durchsuchung ohne das Wissen der Beamten	Polizeidirektion Dessau	Politik	Polizeibeamte	400
16.9.2009	Hunderte Bewerbungsunterlagen bei ebay versteigert	CSS-Marketing GmbH	Wirtschaft	Erwerbslose	500
1984	Programmierfehler sorgt für Veröffentlichung geheimer Namen und Telefonnummern in Wiesbadener Telefonbuch	Stadt Wiesbaden	Politik	Bürger	972
08.2.2009	Verlorener USB-Stick enthält Kranken-Befunde	Arztpraxis	Gesundheitswesen	Patienten	1.064
17.10.2009	Finanzdienstleister AWD gibt weiteres Datenleck bekannt: Interne Abrechnungen im Internet veröffentlicht	AWD	Finanzwesen	Mitarbeiter	1.500
06.2.2009	Bildungsträger Kolping legt sensible Daten offen	Kolping	Bildungseinrichtung	Erwerbslose	1.700
23.1.2009	www.geldkarte.de: Nutzerdaten offen im Netz	EURO Kartensysteme	Finanzwesen	Online-Nutzer	2000
25.9.2008	Die Axel-Springer-Tochter WBV Wochenblatt veröffentlichte versehentlich 2.000 Kundendaten auf einer Website	WBV Wochenblatt	Medien	Inserenten	2.000
1.11.2009	Ausspähung von Bewerberdaten aus Datenbank	Bundesagentur für Arbeit	Politik	Erwerbslose	2.500
09.3.2010	Persönliche Daten von Teilnehmern des Münster-Marathon auf DVD verschickt	Münster-Marathon e.V.	Sport & Freizeit	Teilnehmer	3.500

Zeitpunkt/ Zeitraum der Datenverarbeitung	Beschreibung - kurz	Institution/ Unternehmung (Datenherkunft)	Bereich	Betroffene	Anzahl betroffener Personendaten
18.12.2009	Datenleck an der Kreisvolkshochschule Goslar macht 8.000 sensible Teilnehmerdaten einsehbar	Kreisvolkshochschule	Bildungseinrichtung	Teilnehme	8.000
17.11.2009	Daten von 11.000 Kabel-Deutschland-Kunden frei im Netz zugänglich	Kabel Deutschland	Wirtschaft	Kunden	11.000
08.2.2010	Erneutes Datenleck beim Finanzdienstleister AWD: 12.000 sensible Kundendaten im Umlauf	AWD	Finanzwesen	Kunden	12.000
06.10.2008	14.000 Handynummern von Polizisten im Internet	Mitglied der Berliner Gewerkschaft der Polizei	Politik	Mitarbeiter	14.000
16.06.2010	Datenleck beim Wahlamt München löst munteren Handel mit hochsensiblen Daten aus.	Stadtverwaltung	Politik	Briefwähler	15.000
11.2.2009	DSDS-Bewerberdatenbank offen im Netz	RTL Televison	Medien	Teilnehmer	18.000
06.10.2009	Phishing-Angriffe auf Nutzerkonten bei Google Mail und Yahoo	Google und Yahoo	Wirtschaft	Kunden	20.000
01.10.2008	Datenleck bei der Universität Göttingen - 26.000 Studentendaten einsehbar	Universität Göttingen	Bildungseinrichtung	Studenten	26.000
1.10.2009	Diebstahl von Kundendaten eines Finanzdienstleisters	AWD	Finanzwesen	Kunden	27.000
16.10.2009	Mehrere Tausend Datensätze des Finanzdienstleisters AWD dem Norddeutschen Rundfunk (NDR) zugespielt	AWD	Finanzwesen	Kunden	27.000
06.07.2010	Über einen Link im Newsletter des Vereins waren für zwei Stunden die gespeicherten Daten, wie Namen, Adressen, Geburtsdaten und auch Kontonummern, von 34.700 Mitgliedern und Werder-Kunden öffentlich zugänglich.	SV Werder Bremen	Sport & Freizeit	Mitglieder und Kunden	34.700
04.7.2008	Persönliche Daten von mehr als 40.000 Testkäufern einsehbar	TNS Infratest GmbH	Wirtschaft	Mitarbeiter	40.000
1977	Adressensammlung und -weiterverkauf	Melderegister	Politik	Bürger	42.000
09.5.2008	Private Kontaktdaten von 44.000 Studenten der Universität Magdeburg frei zugänglich	Universität Magdeburg	Bildungseinrichtung	Studenten	44.000
19.1.2010	Leck bei Ruf-Jugendreisen: Daten von 50.000 Jugendlichen offen zugänglich im Netz	Ruf-Jugendreisen	Sport & Freizeit	Reisende	50.000
04.9.2008	Bewerberdatenbank von PricewaterhouseCoopers geknackt	PricewaterhouseCoopers	Wirtschaft	Bewerber	56.000
01.11.2007	Datendiebstahl bei Konzert- und Veranstaltungskarten-Vertrieb	Kartenhaus	Wirtschaft	Kunden	66.000
1.10.2009	Diebstahl von Kundendaten	Deutsche Telekom	Wirtschaft	Kunden	100.000
1968-1982	Basisdokumentation psychiatrischer Landeskrankenhäuser in Baden-Württemberg ohne Anonymisierung der Patienten	Landeskrankenhäuser	Gesundheitswesen	Patienten	100.000
28.10.2009	Neue Panne bei SchülerVZ: 100.000 Datensätze aufgetaucht	SchülerVZ	Privater Bereich	Online-Nutzer	100.000

Zeitpunkt/ Zeitraum der Datenverarbeitung	Beschreibung - kurz	Institution/ Unternehmung (Datenherkunft)	Bereich	Betroffene	Anzahl betroffener Personendaten
12.12.2008	Falschlieferung eines Paketes mit Mikrofichen, welche sensible Daten über Kreditkartenkunden enthielten	LBB Berlin	Finanzwesen	Kunden	130.000
20.10.2009	Datenleck bei bsmparty.de: Daten der gesamten Community im Umlauf	bsmparty.de	Privater Bereich	Online-Nutzer	130.000
1998-2007	Überwachung von Mitarbeitern	Deutsche Bahn	Wirtschaft	Mitarbeiter	173.000
1.8.2008	Weitergabe von Krankenversicherung-/ Patientendaten	DAK	Wirtschaft	Versicherte	200.000
1.11.2009	Rechnungen versehentlich im Online-Shopsystem zugänglich	Sparkassenverlag	Finanzwesen	Kunden	350.000
13.12.2009	350.000 Unternehmensdaten von Berliner Gewerbe automatisch ausgelesen und veröffentlicht	Berliner Gewerbeauskunft	Politik	Unternehmen	350.000
15.12.2009	Sensible Daten aus dem Schwaigerner Rathaus landen bei Firma in Nordrhein-Westfalen	Rathaus	Politik	Bürger, Mitarbeiter	400.000
25.06.2008	Panne in Einwohnermeldeämtern, Daten von 500.000 waren im Internet einsehbar	Meldeämter	Politik	Bürger	500.000
1.10.2009	Kopie von Profildaten aus Online-Portal	schülerVZ	Privater Bereich	Portalnutzer	1.000.000
11.2.2010	Datenleck bei der BKK Gesundheit: Unbekannte erpressen die Krankenkasse	BKK Gesundheit	Wirtschaft	Versicherte	1.500.000
12.8.2008	Verbraucherzentrale in Schleswig-Holstein erhält CDs mit 17.000 Datensätzen	Süddeutsche Klassenlotterie	Wirtschaft	Kunden	1.500.000
04.5.2010	Neuer Datenskandal bei SchülerVZ: 1,6 Millionen Datensätze abgefischt	SchülerVZ	Privater Bereich	Online-Nutzer	1.600.000
1.10.2009	Ausspähung von Bewerberdaten aus Datenbank	Bundesagentur für Arbeit	Politik	Erwerbslose	3.800.000
01.11.2007	Daten von Millionen von ebay-Kunden waren aufgrund eines Programmfehlers im Internet abrufbar	ebay.de	Wirtschaft	Kunden	6.000.000
k.a.	Speicherung von Versicherungsnehmern in zentraler Datenbank, sofern ein "kritischer Punktwert" erreicht wird und man von nicht rentablen Kunden oder Kunden mit hohem Risiko eines Versicherungsfalles oder sogar Betrug ausgeht.	Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV)	Wirtschaft	Versicherte	10.000.000
2001-2010	Weitergabe der Daten internationaler Banktransaktionen an die USA bzw. Speicherung der Daten auf US-Servern im Rahmen des SWIFT-Abkommens	Society for Worldwide Interbank Financial Telecommunication	Finanzwesen	Kunden	15.000.000
04.10.2008	17 Millionen T-Mobile-Kundendaten geklaut	T-Mobile	Wirtschaft	Kunden	17.000.000
1.9.2006	Diebstahl von Kundendaten und Angebot zum Weiterverkauf im Internet	Deutsche Telekom/ T-Mobile	Wirtschaft	Kunden	17.000.000
04.12.2008	Bankverbindungen von 21 Millionen Bundesbürgern auf dem Schwarzmarkt erhältlich	unterschiedlich	Finanzwesen	nicht verifizierbar	21.000.000
09.10.2008	30 Millionen Adress- und Bankdaten von Handy-Kunden online einsehbar	T-Mobile	Wirtschaft	Kunden	30.000.000

Zeitpunkt/ Zeitraum der Datenverarbeitung	Beschreibung - kurz	Institution/ Unternehmung (Datenherkunft)	Bereich	Betroffene	Anzahl betroffener Personendaten
1.1.2010	mtl. Sammlung von Mitarbeiterdaten zu allen Belangen des Beschäftigungsverhältnisses "auf Vorrat" im Rahmen des ELENA-Verfahrens	Bundesministerium für Wirtschaft & Technologie	Politik	Arbeitnehmer	40.000.000
1978	Lückenloses Datennetz durch Sozialversicherungsträger mit persönlichen Daten fast aller Bundesbürger	soziale Sicherungsträger	Politik	Bürger	45.000.000
1968	Pläne der Bundesregierung, ein zentrales Speicherregister zur Speicherung aller Bürgerinformationen einzurichten. Die Pläne wurden nach breiter Empörung und Protesten nicht umgesetzt	Bürger	Politik	Bürger	75.000.000
14.5.2010	Festplatten mit brisanten Steuerdaten auf Flohmarkt aufgetaucht [Update]	Bayerisches Landesamt für Steuern	Politik	Steuerzahler	Hunderte
21.1.2010	Weiteres Leck bei Ruf-Jugendreisen: Auch Buchungsdaten der Jugendlichen einsehbar	Ruf-Jugendreisen	Sport & Freizeit	Reisende	Tausende
06.3.2009	Kopie der Datenbanken von Grundbuchämtern verloren	Datenverarbeitungszentrum Mecklenburg-Vorpommern	Politik	Bürger	Einzelne
12.5.2010	Panne bei Vodafone: MobileMails fremder Kunden einsehbar	Vodafone	Wirtschaft	Kunden	Einzelne
14.7.2009	Panne bei der Sendungsverfolgung von DHL	DHL	Wirtschaft	Kunden	Einzelne
16.2.2009	Fehler im Verlagshaus Madsack macht Kundendaten sichtbar	Verlagshaus Madsack	Medien	Kunden	Einzelne
20.5.2009	Pressefotograf erhält monatelang E-Mails mit fremden Bankdaten	HSH Nordbank	Finanzwesen	Kunden	Einzelne
04.9.2009	Möglicher Missbrauch von MasterCard-Kreditkarten	MasterCard	Finanzwesen	Kunden	Hunderte
20.01.2009 - 27.01.20	Hunderte Datensätze von Kunden auf der Telekom-Website offen einsehbar	Deutsche Telekom	Wirtschaft	Kunden	Hunderte
13.10.2009	Deutsche Telekom: Hunderttausende Kontoverbindungsdaten von Kunden ins Ausland gelangt	Deutsche Telekom	Wirtschaft	Kunden	Hunderttausende
13.11.2009	Nach Datendiebstahl tauschen deutsche Banken Hunderttausende VISA und Mastercards aus	Dienstleister von Visa und Mastercard	Finanzwesen	Kunden	Hunderttausende
29.10.2009	Rechnungen von Hunderttausenden Libri-Kunden im Internet einsehbar	Libri	Wirtschaft	Kunden	Hunderttausende
30.10.2009	Weiteres Datenleck bei Libri: Auch Daten sämtlicher Online-Shops einsehbar	Libri	Wirtschaft	Kunden	Hunderttausende
30.3.2009	Kundendaten von Kabel Deutschland kursieren weltweit im Internet	Kabel Deutschland	Wirtschaft	Kunden	Hunderttausende
1999	Softwarefehler bei Geldautomat	Dresdner Bank	Finanzwesen	Bank	k.a.
16.10.2009	Hacker veröffentlichen Millionen von Schüler-Daten aus SchülerVZ im Internet	SchülerVZ	Privater Bereich	Online-Nutzer	Millionen
26.10.2009	Postbank gewährt Einblick in Millionen Girokonten ihrer Kunden	Postbank	Finanzwesen	Kunden	Millionen

Zeitpunkt/ Zeitraum der Datenverarbeitung	Beschreibung - kurz	Institution/ Unternehmung (Datenherkunft)	Bereich	Betroffene	Anzahl betroffener Personendaten
29.10.2007	Millionen von eBay-Identitäten offen im Netz	eBay	Wirtschaft	Kunden	Millionen
29.8.2008	Illegaler Handel mit Melderegisterdaten	Kommunale Meldeämter	Politik	Bürger	Millionen
1999	Buchungsfehler durch Softwarepanne	Bank24	Finanzwesen	Kunden	Tausende
01.09.2008	Veröffentlichung von Kundendaten im Internet aufgrund von Softwarepanne	Lustkatalog.de	Wirtschaft	Kunden	Tausende
04.12.2009	Private Daten von Kindern ungeschützt im Netz einsehbar	haefft.de	Privater Bereich	Online-Nutzer	Tausende
08.4.2010	Hacker klauen Kreditkartendaten von Wacken-Fans	Metaltix	Finanzwesen	Teilnehmer	Tausende
10.11.2009	Berliner Firma stellt 2.500 Stellenangebote beim Arbeitsamt ein, um an die Daten der Bewerber zu kommen	Bundesagentur für Arbeit	Politik	Erwerbslose	Tausende
10.11.2009	Kontodaten der PostOffice-Shop-Kunden online einsehbar	Deutsche Post	Finanzwesen	Kunden	Tausende
12.1.2010	Datenleck bei Online-Händler Spielegrotte: Kundendaten für jedermann einsehbar	SpieleGrotte	Privater Bereich	Online-Nutzer	Tausende
14.5.2010	Rote Hilfe e.V.: Festplatte mit Mitgliederdaten gestohlen	Rote Hilfe e.V.	Sport & Freizeit	Mitglieder	Tausende
15.3.2010	Datenleck bei Vodafone: Sensible Kundendaten auf dem Schwarzmarkt aufgetaucht	Vodafone	Wirtschaft	Kunden	Tausende
21.1.2009	Deutsche Bahn späht Tausende Mitarbeiter aus	Deutsche Bahn	Wirtschaft	Mitarbeiter	Tausende
26.11.2008	Geheime Kundendaten der Deutschen Telekom kursieren auf dem Schwarzmarkt	Deutsche Telekom	Wirtschaft	Kunden	Tausende
28.04.2010	Datenpanne in deutschen Kommunen: Software-Probleme machen vertrauliche Daten für jedermann online einsehbar	Stadtverwaltungen	Politik	Mitarbeiter der Stadtverwaltungen,	Zahlreiche
27.11.2009	Nürburgring-Affäre: CDU-Abgeordnete gestehen illegalen Zugriff auf Polizei-Datenbank	Polizei	Politik	Bürger	Zahlreiche
02.2.2009	Datenpanne bei 1&1: Verbindungsdaten liegen offen	1&1	Wirtschaft	Kunden	Zahlreiche
02.7.2009	Sparkasse Köln/Bonn soll Mitarbeiter- und Kundendaten ohne Anonymisierung an externen Berater geschickt haben	Sparkasse Köln/Bonn	Finanzwesen	Kunden	Zahlreiche
03.11.2009	Benutzer können 350.000 Rechnungen im Sparkassen-Shop einsehen	Deutscher Sparkassen Verlag GmbH	Finanzwesen	Kunden	Zahlreiche
04.11.2009	Datenlücke beim 1. FC Köln	1. FC Köln	Sport & Freizeit	Mitglieder	Zahlreiche
05.10.2009	Subpartner der Deutschen Telekom erhielten rechtswidrig Zugriff auf Kundendaten des Unternehmens	Deutsche Telekom	Wirtschaft	Kunden	Zahlreiche

Zeitpunkt/ Zeitraum der Datenverarbeitung	Beschreibung - kurz	Institution/ Unternehmung (Datenherkunft)	Bereich	Betroffene	Anzahl betroffener Personendaten
05.11.2009	Deutsche Bank gewährt Einblick in Kundenkonten	Deutsche Bank	Finanzwesen	Kunden	Zahlreiche
1.10.2009	fehlende Zugriffskontrolle auf sensible Daten von Erwerbslosen	Bundesagentur für Arbeit	Politik	Erwerbslose	Zahlreiche
12.11.2009	Weitere Sicherheitslücke bei AWD: Externe IT-Berater haben Zugriff auf Kundendaten	AWD	Finanzwesen	Kunden	Zahlreiche
18.9.2009	Bundesrat gibt grünes Licht für umstrittene Ausländerdatei	Bundesrat	Politik	Bürger	Zahlreiche
19.10.2009	Private Dokumente bei Google Text & Tabellen einsehbar	Google	Wirtschaft	Online-Nutzer	Zahlreiche
19.10.2009	Unbefugte gelangen an Daten der Karstadt-MasterCard-Kunden	KarstadtQuelle Bank	Finanzwesen	Kunden	Zahlreiche
19.9.2009	Deutsche Bank bespitzelt Aufsichtsrat	Deutsche Bank	Finanzwesen	Leitende Mitarbeiter	Zahlreiche
29.12.2009	Datenleck bei neuem MP3-Shop von Saturn	Saturn MP3-Shop	Wirtschaft	Kunden	Zahlreiche
2008	Softwarefehler in durch T-Systems entwickelte Software sorgt für zehntausende von Falschmeldungen seitens der Bundesagenturen für Arbeit an gesetzliche Kankenkassen	Bundesagentur für Arbeit	Gesundheitswesen	gesetzliche Krankenkassen und Versicherte	Zehntausende
05.10.2009	Hotmail-Konten geknackt und ins Internet gestellt	Hotmail	Wirtschaft	Kunden	Zehntausende
07.11.2007	Zurzeit ist auf die Seite www.aschaffenburg.de kein Zugriff möglich“, heißt es auf der Homepage der Stadtverwaltung. Dies dürfte noch eine Weile so bleiben. Denn der Internet-Auftritt ist einem Hacker zum Opfer gefallen. Bis die Einzelheiten des Angriffs geklärt sind, hat die Pressestelle als der zuständige Administrator die Seite aus dem weltweiten Netz genommen.	Stadtverwaltung	Politik	Stadt	
1.11.2009	Diebstahl von Kundendaten eines Finanzdienstleisters durch externe Berater	AWD	Finanzwesen	Kunden	
28.02.2010	internationale Phishing-Attacke auf CO2-Emissionshändler	DEHSt	Finanzwesen	Unternehmen	
01.02.2009	Fehlende Zugriffskontrolle für Abruf von elektronischen Patientenakten	UKE Hamburg	Gesundheitswesen	Patienten	
01.07.2009	Stundenlanger Ausfall des Labor-Computersystems	UKE Hamburg	Gesundheitswesen	Patienten	
01.08.2005	Übermittlung zehntausender falscher Storno-Mitteilungen durch die BfA an gesetzliche Krankenkassen	BfA	Gesundheitswesen	gesetzliche Krankenkassen	

B Datenbausteine im ELENA-Verfahren

Datenbausteine im ELENA-Verfahren I	Datenbausteine im ELENA-Verfahren II
• Steuerklasse • Faktor der Steuerberechnung • Kinderfreibetrag • Angaben zur Tätigkeit nach Tätigkeitsschlüssel der Bundesagentur für Arbeit • wöchentliche Arbeitszeit • Bruttoentgelt • Rentenversicherungsbezüge • Sozialversicherungsabzüge • Arbeitslosenversicherungsabzüge • Pflegeversicherungsabzüge • Lohnsteuer • Solidaritätszuschlag • Kirchensteuer • Name und Anschrift • Geburtsort, -datum und -name • Angaben zu Arbeitgeber und Betrieb • Beschäftigungsort • Vorfeld von Kündigungen • Schilderung von „vertragswidrigem Verhalten“ des Angestellten/Arbeiters • Gründe für eine fristgebunden erfolgte Kündigung • Vorruhestandsleistungen und -gelder • Abfindungsleistungen • Anzahl von Fehlzeiten • Beginn und Ende von Fehlzeiten	• Art der einzelnen Fehlzeiten • Höhe und Art sonstiger steuerpflichtiger Bezüge • Höhe und Art von steuerfreien Bezügen • Zeitpunkt des Beginns einer Ausbildung • voraussichtliches und tatsächliches Ende der Ausbildung • Arbeitgeber-Zuschuss zur freiwilligen Kranken- und Pflegeversicherung • Grund von Arbeitszeitänderungen • Arbeitsstunden – aufgeschlüsselt in Arbeitsstunden jeder einzelnen Kalenderwoche des Monats • Urlaubsanspruch und tatsächlich genommene Urlaubstage • Urlaubsentgelt • Angaben zu befristeten Arbeitsverhältnissen • Angaben zu Entlassungen und Kündigungen • Kündigungsgründe • Art der Zustellung der Kündigung • Auskunft über bereits erfolgte Abmahnungen

Quelle: ELENA (2009).

C Verzeichnis der recherchierten Modellierungsansätze

Autoren	Titel	Jahr	Veröffentlicht in:
De Moura Araujo, Bruno Schmitz, Eber Assis Correa, Alexandre Luis Alencar, Antonio Juarez	A method for validating the compliance of business processes to business rules	2010	2010 ACM Symposium on Applied Computing
Awad, Ahmed Weske, Mathias	Efficient Compliance Checking Using BPMN-Q and Temporal Logic	2008	Business Process Management
Awad, Ahmed Smirnov, Sergey Weske, Mathias	Resolution of Compliance Violation in Business Process Models: A Planning-based Approach	2009	R. Meersman, T. Dillon, P. Herrero: OTM2009, Part I, LNCS 5870
Awad, Ahmed Weidlich, Matthias Weske, Mathias	Specification, Verification and Explanation of Violation for Data Aware Compliance Rules	2009	L. Baresi, C.-H. Chi, and J. Suzuki: ICSOC-ServiceWave 2009, LNCS 5900
Awad, Ahmed Weske, Mathias	Visualization of compliance violation in business process models	2009	5th Workshop on Business Process Intelligence BPI
Becker, Jörg Klose, Karsten Schneider, Martin	Prozessmodellbasierte Vertragsgestaltung in überbetrieblichen Kooperationen	2003	Modellierung betrieblicher Informationssysteme - MobIS 2003
Breaux, Travis D.	Early Studies in Acquiring Evidentiary, Reusable Business Process Models for Legal Compliance	2009	2009 Sixth International Conference on Information Technology: New Generations
Breaux, Travis D. Antón, Annie I.	A systematic method for acquiring regulatory requirements: A frame-based approach	2007	6th International Workshop on Requirements for High Assurance Systems
Breaux, Travis D. Antón, Annie I. Boucher, Kent Dorfman, Merlin	IT Compliance: Aligning Legal and Product Requirements	2009	IT Professional, 2009
Breaux, Travis D. Vail, Matthew W. Antón, Annie I.	Towards regulatory compliance: Extracting rights and obligations to align requirements with regulations	2006	14th IEEE International Requirements Engineering Conference (RE'06)
Breaux, Travis	Exercising Due Diligence in Legal Requirements Acquisition: A Tool-supported, Frame-Based Approach	2009	2009 17th IEEE International Requirements Engineering Conference
Darimont, Robert Lemoine, Michel	Goal-oriented analysis of regulations	2006	ReMo2V, CAiSE
El Kharbili, M. Medeiros, A.K. Alves De Stein, S. van Der Aalst, WMP	Business process compliance checking: Current state and future challenges	2008	Modelling Business Information Systems

Autoren	Titel	Jahr	Veröffentlicht in:
Giblin, Christopher Müller, Samuel Pfitzmann, Birgit	From Regulatory Policies to Event Monitoring Rules: Towards Model-Driven Compliance Automation	2006	IBM Research Report
Giblin, Christopher Müller, Samuel Pfitzmann, Birgit	Regulations expressed as logical models (REALM)	2006	Proceedings of the 18th Annual Conference on Legal Knowledge and Information Systems
Ghanavati, Sepideh Amyot, Daniel Peyton, Liam	Towards a framework for tracking legal compliance in healthcare	2007	CAiSE 2007
Ghose, Aditya Koliadis, George	Auditing business process compliance	2007	Service-Oriented Computing – ICSOC 2007
Goedertier, Stijn Vanthienen, Jan	Designing compliant business processes with obligations and permissions	2006	Business Process Management Workshops
Goeken, Matthias Alter, Stefanie	Towards Conceptual Metamodeling of IT Governance Frameworks Approach-Use-Benefits	2009	42nd Hawaii International Conference on System Sciences - 2009
Goeken, Matthias Knackstedt, Ralf	Referenzmodellgestütztes Compliance Reporting am Beispiel der EU-Finanzmarktrichtlinie MiFID	2008	HMD - Praxis der Wirtschaftsinformatik
Weber, Ingo Governatori, Guido Hoffmann, Jörg Sadiq, Shazia	Detecting regulatory compliance for business process models through semantic annotations	2008	4th International Workshop on Business Process Design, Milan
Höhn, Sebastian Jürjens, Jan	Rubacon: automated support for model-based compliance engineering	2008	ICSE'08
K, Martin Gilliot, Maike	Automating Privacy Compliance with ExPDT	2008	10th IEEE Conference on E-Commerce Technology
Karagiannis, Dimitris	A business process-based modelling extension for regulatory compliance	2008	Multikonferenz Wirtschaftsinformatik 2008
Knackstedt, Ralf Kaufmann, Noogie C Brelage, Christian	Entwicklung rechtssicherer Web-Anwendungen	2006	Wirtschaftsinformatik
Knolmayer, Gerhard Endl, Rainer Pfahrer, Marcel	Modeling Processes and Workflows by Business Rules	2000	W. van der Aalst et al.: Business Process Management, LNCS 1806
Küster, Jochen Ryndina, Ksenia Gall, Harald	Generation of Business Process Models for Object Life Cycle Compliance	2007	G. Alonso, P. Dadam, and M. Rosemann: BPM 2007, LNCS 4714
Lu, Ruopeng Sadiq, Shazia Governatori, Guido	Compliance aware business process design	2007	3rd International Workshop on Business Process Design (BPD'07)
Lu, Ruopeng Sadiq, Shazia	Measurement of Compliance Distance in Business Processes	2008	Information Systems Management

Autoren	Titel	Jahr	Veröffentlicht in:
Governatori, Guido			
Ly, Lihn Thao Knuplesch, David Rinderle-Ma, Stefanie Göser, Kevin	SeaFlows Toolset-Compliance Verification Made Easy	2010	CAiSE'10 Forum
Kharbili, Marwane El Stein, Sebastian Markovic, Ivan Pulvermüller, Elke	Towards a framework for semantic business process compliance management	2008	GRCIS Workshop - CAISE Conference 2008
Milosevic, Zoran	Towards Integrating Business Policies with Business 2 Key Collaborative Business Process	2005	W.M.P. van der Aalst et al.: BPM 2005, LNCS 3649
zur Muehlen, Michael Indulska, Marta Kamp, Gerrit	Business process and business rule modeling languages for compliance management: a representational analysis	2007	CRPIT Volume 83
Namiri, Kioumars Stojanovic, Nenad	Using Control Patterns in Business Processes Compliance	2007	M. Weske, M.-S. Hacid, C. Godart: WISE 2007 Workshops, LNCS 4832
Namiri, Kioumars Stojanovic, Nenad	Pattern-based design and validation of business process compliance	2007	On the Move to Meaningful Internet Systems: OTM 2007
Olbrich, Sebastian Simon, Carlo	Process Modelling towards e-Government – Visualisation and Semantic Modelling of Legal Regulations as Executable Process Sets	2008	The Electronic Journal of e-Government
Olbrich, Sebastian Simon, Carlo	The Influence of Legal Constraints on business process Modeling	2005	Proceedings of the eGovernment Workshop '05 (eGOV05), Brunel University
Pesic, Maja Schonenberg, Helen Sidorova, Natalia van Der Aalst, Wil	Constraint-based workflow models: Change made easy	2007	CoopIS
Sackmann, Stefan Käahmer, Martin Gilliot, Maike Lowis, Lutz	A classification model for automating compliance	2008	10th IEEE Conference on E-Commerce Technology
Sackmann, Stefan Kähmer, Martin	ExPDT: Ein Policy-basierter Ansatz zur Automatisierung von Compliance	2008	Wirtschaftsinformatik
Schleicher, Daniel Anstett, Tobias Leymann, Frank Mietzner, Ralph	Maintaining Compliance in Customizable Process Models	2009	On the Move to Meaningful Internet Systems: OTM 2009
Feja, Sven Witt, Sören	Modellierung und Validierung von Datenschutzanforderungen in Pro-	2010	Vernetzte IT für einen effektiven Staat - Ge-

Autoren	Titel	Jahr	Veröffentlicht in:
Brosche, Andreas Speck, Andreas	zessmodellen		meinsame Fachtagung Verwaltungsinformatik und Fachtagung Rechtsinformatik
Weber, Ingo Governatori, Guido Hoffmann, Jörg Sadiq, Shazia	Detecting regulatory compliance for business process models through semantic annotations	2008	4th International Workshop on Business Process Design, Milan
Weber, Ingo Governatori, Guido Hoffmann, Jörg	Approximate compliance checking for annotated process models	2008	GRCIS'08
Wagner, Karl Klüuckmann, Jörg	Prozessdesign als Grundlage von Compliance Management, Enterprise Architecture und Business Rules	2006	AGILITÄT durch ARIS Geschäftsprozessmanagement - Jahrbuch Business Process Excellence 2006/2007

D Gegenüberstellung der aktuellen CMMI-Konstellationen

Kürzel	Bezeichnung	CMMI-DEV	CMMI-ACQ	CMMI-SRV
AM	Agreement Management		x	
ARD	Acquisition Requirements Development		x	
ATM	Acquisition Technical Management		x	
AVAL	Acquisition Validation		x	
AVER	Acquisition Verification		x	
CAM	Capacity and Availability Management			x
CAR	Causal Analysis and Resolution	x	x	x
CM	Configuration Management	x	x	x
DAR	Decision Analysis and Resolution	x	x	x
IPM	Integrated Project Management	x	x	x
IRP	Incident Resolution and Prevention			x
MA	Measurement and Analysis	x	x	x
OID	Organizational Innovation and Deployment	x	x	x
OPD	Organizational Process Definition	x	x	x
OPF	Organizational Process Focus	x	x	x
OPP	Organizational Process Performance	x	x	x
OT	Organizational Training	x	x	x
PI	Product Integration	x		
PMC	Project Monitoring and Control	x	x	x
PP	Project Planning	x	x	x
PPQA	Process and Product Quality Assurance	x	x	x
QPM	Quantitative Project Management	x	x	x
RD	Requirements Development	x		
REQM	Requirements Management	x	x	x
RSKM	Risk Management	x	x	x
SAM	Supplier Agreement Management	x		x
SCON	Service Continuity			x
SD	Service Delivery			x
SSAD	Solicitation and Supplier Agreement Development		x	
SSD	Service System Development			x
SST	Service System Transition			x
STSM	Strategic Service Management			x
TS	Technical Solution	x		
VAL	Validation	x		
VER	Verification	x		

E MEMO-Präsentation: IT-Skandale – Ursache, Reaktion, Prävention

Agenda

- IT-Skandale in der öffentlichen Verwaltung
- Skandalierung in den Medien
- Risiken des IT-Einsatzes
- Möglichkeiten der Risikoprävention

Handel mit Melderegisterdaten

Adressermittler speichern und verkaufen mehrere Millionen Meldedaten deutscher Bundesbürger

taz.de

29.08.2008 | 3 Kommentare

HANDEL MIT MELDEREGISTERDATEN

Die Schattenmeldeämter

Personenbezogene Daten der kommunalen Melderegister werden offenbar rechtswidrig von Privatfirmen gespeichert und verkauft.

VON V.MEDICK & D.SCHULZ

Und der Datenschatten der Bürger wird länger und länger... Foto:

Sie übernehmen die bürokratische Drecksarbeit: Adressmittler. Wartet eine Bank auf die Rückzahlung eines Kredits, schaltet sie solche Firmen ein. Adressmittler nehmen mit den Melderegistern Kontakt auf, um den Aufenthaltsort des säumigen Zahlers herauszufinden und die Daten der Bank zur Verfügung zu stellen. Nur der Bank - denn der Mittler darf die Daten nirgends speichern.

Handel mit Melderegisterdaten

- **Hintergrund**
  - Auskunft ggü. Finanzdienstleistern
  - Adressermittler als Dienstleister
  - Befugnis zur Datenweiterleitung
- **Missstand**
  - Speicherung der Melderegisterdaten
  - Aufbau einer Datenbank
  - Vertrieb der Melderegisterdaten
- **Konsequenzen**
  - Runderlass
  - Abmahnungen
  - Firmen weiterhin geschäftstätig


taz.de

Die Schattenmeldeämter

Personenbezogene Daten der kommunalen Melderegister werden offenbar rechtswidrig von Privatfirmen gespeichert und verkauft.

ELENA: Der nächste Skandal?


tagesschau.de

Suchbegriff

Schaar für "Renovierung" des Datenschutzrechts

Datenschützer fordern kritische Überprüfung von ELENA

Nachrichten ABO Anzeigen Shop Service Werbung

DERWESTEN

Das Portal der WAZ Mediengruppe

Fußball-WM Das Spezial von DerWesten

Startseite Lokales Sport Kultur Leben Videos Community

Im Westen Sauer- & Siegerland Westfalen Niederrhein Politik Wirtschaft Technik Panorama

Start > Extrem wissbegierige „Elena"

Hintergrund

Extrem wissbegierige „Elena"

Nachrichten, 01.01.2010, Dirk Hautkapp

EL|ENA

ELEKTRONISCHER ENTGELTNACHWEIS

WELT ONLINE

Nachrichten Debatte

Politik Wirtschaft Geld Sport Wisse

In den Nachrichten: Stanley McChrystal | Gruppe D | Sommer | Pisa-Studie

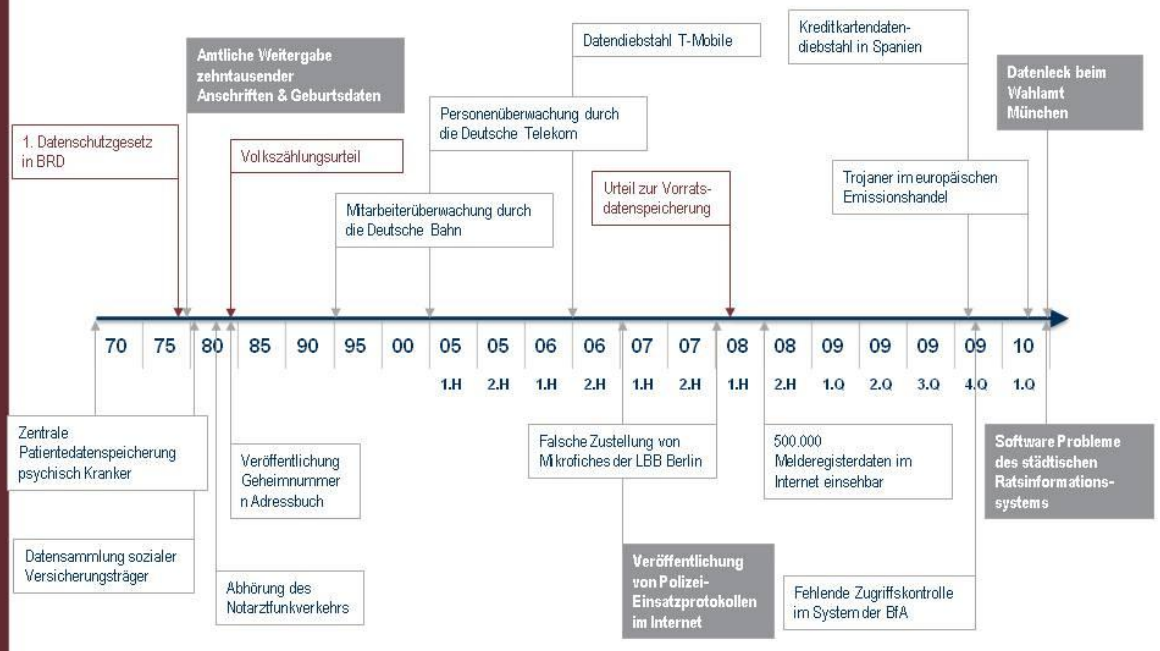
01.01.10 | ENTGELTNACHWEIS (169)

Scharfe Kritik am neuen Datenregister "Elena"

ELENA

- **Hintergrund**
  - Aufgeblähte Bürokratie durch Doppelarbeit
  - Effizienzsteigerung durch Einführung elektronisches Zentralregister & Signaturkarte
- **ELENA**
  - 41-seitiger Datenbogen
  - Speicherung der Daten auf Vorrat
    - Datenabruf erst ab 2012
- **Kritische Themen**
  - Sicherheit der Übertragung
  - Schutz des Zentralregisters vor Zugriffen
  - Missbrauch Signaturkarte

IT-Skandale im Überblick



Agenda

- IT-Skandale in der öffentlichen Verwaltung
- **Skandalierung in den Medien**
- Risiken des IT-Einsatzes
- Möglichkeiten der Risikoprävention

Medien

Medien sind Übermittler von Information bzw. Träger von Kommunikation

Medien der Massenkommunikation

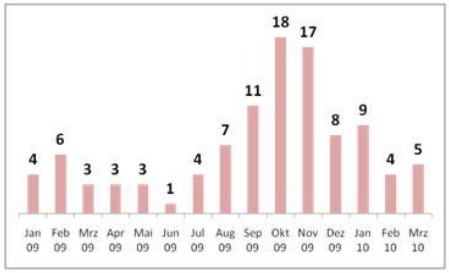
Printmedien	Rundfunk Medien	Online-Medien
Täglich/ wöchentlich	Vollprogramm/ Spartenprogramm	World Wide Web
Kauf/ Abbonement	Öffentlich-rechtlich/ privat	E-Mail Kommunikation
Boulevard/ Qualität		Newsgroups
Regional/ überregional		Blogs

Skandalierung und Medien

Zum Skandal kann nur werden, was als solcher in der Öffentlichkeit angeprangert wird. In der modernen Gesellschaft geschieht dies durch bzw. über die Medien

Missstand → Skandalierung Öfftl. Anprangerung → Öfftl. Aufklärung u. Anprangerung → Forderungen nach Konsequenzen

- Bedeutung der Online-Medien
- Häufigkeit von Skandalen



Agenda

- IT-Skandale in der öffentlichen Verwaltung
- Skandalierung in den Medien
- Risiken des IT-Einsatzes
- Möglichkeiten der Risikoprävention

Hintergründe IT-Risiken

Bedrohungen	Organisatorische Mängel	Menschliches Fehlverhalten	Technisches Versagen	Höhere Gewalt		
Schwachstellen	Software	Hardware	Daten	Netze	Anwender	Infrastruktur
Verletzl. Schutzziele	Vertraulichkeit	Integrität	Verfügbarkeit	Zurechenbarkeit		

ELENA

Bedrohungen	Organisatorische Mängel	Menschliches Fehlverhalten	Technisches Versagen	Höhere Gewalt		
Schwachstellen	Software	Hardware	Daten	Netze	Anwender	Infrastruktur
Verletzl. Schutzziele	Vertraulichkeit	Integrität	Verfügbarkeit	Zurechenbarkeit		

Agenda

- IT-Skandale in der öffentlichen Verwaltung
- Skandalierung in den Medien
- Risiken des IT-Einsatzes
- Möglichkeiten der Risikoprävention

Sicherheitsmanagement

- Ziele
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit
- Schwachstellen im IT-System: Risikoanalyse
- Frameworks & Standards
  - ISO/IEC 17799
  - IT-Grundschutzkataloge

Sicherheitsmanagement

- **IT-Grundschutzkataloge**
  - Herausgegeben vom BSI
  - Standard-Sicherheitsmaßnahmen für typische IT-Systeme

IT-Grundschutz-Kataloge

Bausteine	Gefährdung	Maßnahmen
Übergeordnete Aspekte	Höhere Gewalt	Infrastruktur
Sicherheit in der Infrastruktur	Organ. Mängel	Organisation
Sicherheit der IT-Systeme	Menschl. Fehlhandlungen	Personal
Sicherheit im Netz	Techn. Versagen	Hard- und Software
Sicherheit in Anwendungen	Vors. Handlungen	Kommunikation
		Notfallvorsorge

Rechtliche Bedeutung von Zertifikaten

- **Entstehung von Standards und Normen**
- **Kosten**
- **Aussagekraft**
  - Rechtlich nicht bindend
- **Prüfmethoden im IT-Produktbereich**
  - Common Criteria → Sicherheitszertifikate vom BSI

Zertifizierung nach Common Criteria

Schutzprofil	Funktionsklasse	Vertrauens-würdigkeitsstufe	Zertifikat des BSI
Schutzprofil digitales Wahlstift-System Schutzprofil für USB-Datenträger	Sicherheitsprotokollierung Kommunikation Kryptographische Unterstützung	Funktionell getestet Strukturell getestet Methodisch getestet und überprüft . . . Formal verifizierter Entwurf und getestet	Evaluation durch akkreditierte Prüfstellen Zertifizierung lediglich durch BSI

Hintergründe IT-Risiken

Bedrohungen	Organisatorische Mängel	Menschliches Fehlverhalten	Technisches Versagen	Höhere Gewalt		
Schwachstellen	Software	Hardware	Daten	Netze	Anwender	Infrastruktur
Verletzl. Schutzziele	Vertraulichkeit	Integrität	Verfügbarkeit	Zurechenbarkeit		

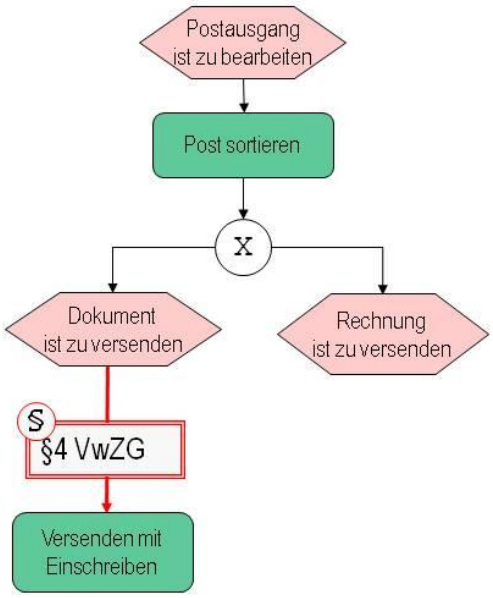
Rechtskonforme Abläufe

- **Permanenter Wandel im rechtlichen Umfeld**
- **Resultierender Prüfbedarf**
  - Strategische Ebene
  - Operative Ebene
- **Möglichkeiten:**
  - Modellierung rechtlicher Anforderungen
  - Rechtskonforme Technikgestaltung

http://www.foka-riir.de/

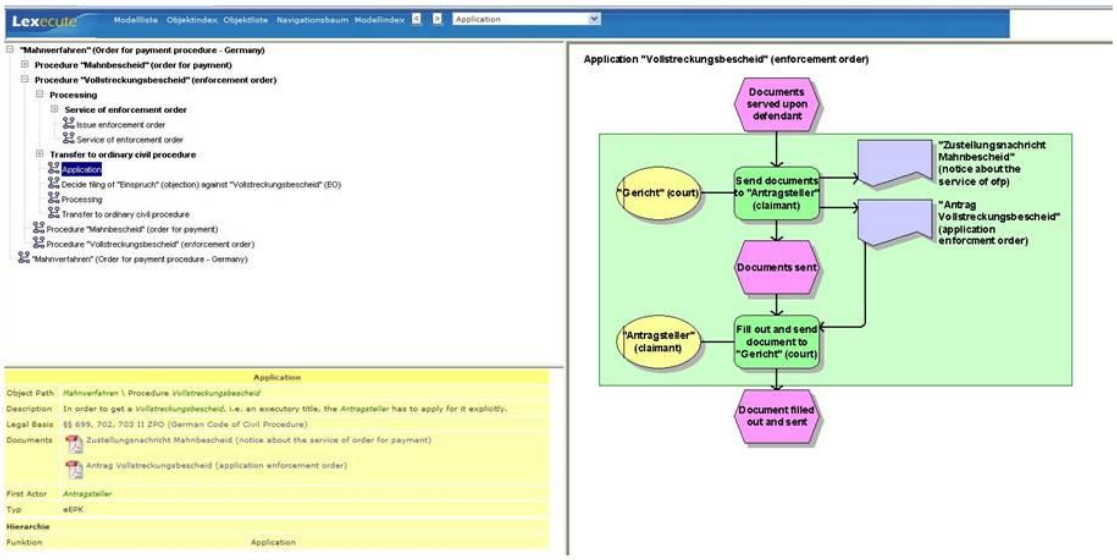
Modellierung rechtlicher Anforderungen

- **unkonventioneller Ansatz**
  - Integration rechtlicher Anforderungen in Prozessmodelle
  - Zu aufwendig
  - Zu wenig Informationen



Modellierung rechtlicher Anforderungen

Lexecute



Rechtskonforme Technikgestaltung

KORA

Rechtliche Vorgaben → Rechtliche Anforderungen → Technische Gestaltungsziele → Gestaltungs-vorschläge → 10100101

Vorgangsbearbeitungssystem in der öffentlichen Verwaltung

- Aus der Verfassung abgeleitete Gestaltungsziele
- Übertragbar auf alle Verwaltungs-Domänen
- Für allgemeine Antragsverfahren

Fazit

Arbeitsbericht

- Informationstisch
- Flyer
- Kostenloser Arbeitsbericht
- http://www.foka-riir.de/

Autoren- und Herausgeberverzeichnis

Prof. Dr. Jörg Becker, Philipp Bergener, Dr. Patrick Delfmann, Mathias Eggert, Marcel Heddier, Sara Hofmann, PD Dr. Ralf Knackstedt, Dr. Michael Räckers
Westfälische Wilhelms-Universität Münster
European Research Center for Information Systems (ERCIS)
{becker, ralf.knackstedt, michael.raeckers, philipp.bergener, mathias.eggert, marcel heddier, sara hofmann}@ercis.uni-muenster.de

Judith-Maria Bracke, Willi Bühler, Dominik Heddier, Fabian Kohl, Stefan Laube, Mario Nolte, Jan Ringas
Westfälische Wilhelms-Universität Münster
Judith-Maria.Bracke@gmx.de, willi.buehler@uni-muenster.de, d.heddier@uni-muenster.de, kohlfabian@gmx.de, stefan.laube@uni-muenster.de, Mario@nolte-netzwerk.de, jan.ringas@googlemail.com

Fleur Fritz
Westfälische Wilhelms-Universität
Institut für Medizinische Informatik und Biomathematik
Fleur.Fritz@ukmuenster.de

Eva-Maria Herring, Julia Seiler
Westfälische Wilhelms-Universität Münster
Institut für Informations-, Kommunikations- und Medienrecht (ITM)
{eva-maria.herring, jseil_01}@uni-muenster.de

Dominique Meiländer
Westfälische Wilhelms-Universität Münster
Institut für Informatik
d.meil@uni-muenster.de

Eric Meyer
Westfälische Wilhelms-Universität
Institut für Genossenschaftswesen
eric.meyer@wiwi.uni-muenster.de

Arbeitsberichte des Instituts für Wirtschaftsinformatik

Nr. 1 Bolte, Ch.; Kurbel, K.; Moazzami, M.; Pietsch, W.: Erfahrungen bei der Entwicklung eines Informationssystems auf RDBMS- und 4GL-Basis. Februar 1991.

Nr. 2 Kurbel, K.: Das technologische Umfeld der Informationsverarbeitung - Ein subjektiver 'State of the Art'-Report über Hardware, Software und Paradigmen. März 1991.

Nr. 3 Kurbel, K.: CA-Techniken und CIM. Mai 1991.

Nr. 4 Nietsch, M.; Nietsch, T.; Rautenstrauch, C.; Rinschede, M.; Siedentopf, J.: Anforderungen mittelständischer Industriebetriebe an einen elektronischen Leitstand - Ergebnisse einer Untersuchung bei zwölf Unternehmen. Juli 1991.

Nr. 5 Becker, J.; Prischmann, M.: Konnektionistische Modelle - Grundlagen und Konzepte. September 1991.

Nr. 6 Grob, H. L.: Ein produktivitätsorientierter Ansatz zur Evaluierung von Beratungserfolgen. September 1991.

Nr. 7 Becker, J.: CIM und Logistik. Oktober 1991.

Nr. 8 Burgholz, M.; Kurbel, K.; Nietsch, Th.; Rautenstrauch, C.: Erfahrungen bei der Entwicklung und Portierung eines elektronischen Leitstands. Januar 1992.

Nr. 9 Becker, J.; Prischmann, M.: Anwendung konnektionistischer Systeme. Februar 1992.

Nr. 10 Becker, J.: Computer Integrated Manufacturing aus Sicht der Betriebswirtschaftslehre und der Wirtschaftsinformatik. April 1992.

Nr. 11 Kurbel, K.; Dornhoff, P.: A System for Case-Based Effort Estimation for Software-Development Projects. Juli 1992.

Nr. 12 Dornhoff, P.: Aufwandsplanung zur Unterstützung des Managements von Softwareentwicklungsprojekten. August 1992.

Nr. 13 Eicker, S.; Schnieder, T.: Reengineering. August 1992.

Nr. 14 Erkelenz, F.: KVD2 - Ein integriertes wissensbasiertes Modul zur Bemessung von Krankenhausverweildauern - Problemstellung, Konzeption und Realisierung. Dezember 1992.

Nr. 15 Horster, B.; Schneider, B.; Siedentopf, J.: Kriterien zur Auswahl konnektionistischer Verfahren für betriebliche Probleme. März 1993.

Nr. 16 Jung, R.: Wirtschaftlichkeitsfaktoren beim integrationsorientierten Reengineering: Verteilungsarchitektur und Integrationsschritte aus ökonomischer Sicht. Juli 1993.

Nr. 17 Miller, C.; Weiland, R.: Der Übergang von proprietären zu offenen Systemen aus Sicht der Transaktionskostentheorie. Juli 1993.

Nr. 18 Becker, J.; Rosemann, M.: Design for Logistics - Ein Beispiel für die logistikgerechte Gestaltung des Computer Integrated Manufacturing. Juli 1993.

Nr. 19 Becker, J.; Rosemann, M.: Informationswirtschaftliche Integrationsschwerpunkte innerhalb der logistischen Subsysteme - Ein Beitrag zu einem produktionsübergreifenden Verständnis von CIM. Juli 1993.

Nr. 20 Becker, J.: Neue Verfahren der entwurfs- und konstruktionsbegleitenden Kalkulation und ihre Grenzen in der praktischen Anwendung. Juli 1993.

Nr. 21 Becker, K.; Prischmann, M.: VESKONN - Prototypische Umsetzung eines modularen Konzepts zur Konstruktionsunterstützung mit konnektionistischen Methoden. November 1993.

Nr. 22 Schneider, B.: Neuronale Netze für betriebliche Anwendungen: Anwendungspotentiale und existierende Systeme. November 1993.

Nr. 23 Nietsch, T.; Rautenstrauch, C.; Rehfeldt, M.; Rosemann, M.; Turowski, K.: Ansätze für die Verbesserung von PPS-Systemen durch Fuzzy-Logik. Dezember 1993.

Nr. 24 Nietsch, M.; Rinschede, M.; Rautenstrauch, C.: Werkzeuggestützte Individualisierung des objektorientierten Leitstands ooL. Dezember 1993.

Nr. 25 Meckenstock, A.; Unland, R.; Zimmer, D.: Flexible Unterstützung kooperativer Entwurfsumgebungen durch einen Transaktions-Baukasten. Dezember 1993.

Nr. 26 Grob, H. L.: Computer Assisted Learning (CAL) durch Berechnungsexperimente. Januar 1994.

Nr. 27 Kirn, St.; Unland, R. (Hrsg.): Tagungsband zum Workshop „Unterstützung Organisatorischer Prozesse durch CSCW“. In Kooperation mit GI-Fachausschuß 5.5 „Betriebliche Kommunikations- und Informationssysteme“ und Arbeitskreis 5.5.1 „Computer Supported Cooperative Work“, Westfälische Wilhelms-Universität Münster, 4.-5. November 1993. November 1993.

Nr. 28 Kirn, St.; Unland, R.: Zur Verbundintelligenz integrierter Mensch-Computer-Teams: Ein organisationstheoretischer Ansatz. März 1994.

Nr. 29 Kirn, St.; Unland, R.: Workflow Management mit kooperativen Softwaresystemen: State of the Art und Problemabriß. März 1994.

Nr. 30 Unland, R.: Optimistic Concurrency Control Revisited. März 1994.

Nr. 31 Unland, R.: Semantics-Based Locking: From Isolation to Cooperation. März 1994.

Nr. 32 Meckenstock, A.; Unland, R.; Zimmer, D.: Controlling Cooperation and Recovery in Nested Transactions. März 1994.

Nr. 33 Kurbel, K.; Schnieder, T.: Integration Issues of Information Engineering Based I-CASE Tools. September 1994.

Nr. 34 Unland, R.: TOPAZ: A Tool Kit for the Construction of Application Specific Transaction. November 1994.

Nr. 35 Unland, R.: Organizational Intelligence and Negotiation Based DAI Systems - Theoretical Foundations and Experimental Results. November 1994.

Nr. 36 Unland, R.; Kirn, St.; Wanka, U.; O'Hare, G. M. P.; Abbas, S.: AEGIS: AGENT ORIENTED ORGANISATIONS. Februar 1995.

Nr. 37 Jung, R.; Rimpler, A.; Schnieder, T.; Teubner, A.: Eine empirische Untersuchung von Kosteneinflußfaktoren bei integrationsorientierten Reengineering-Projekten. März 1995.

Nr. 38 Kirn, St.: Organisatorische Flexibilität durch Workflow-Management-Systeme?. Juli 1995.

Nr. 39 Kirn, St.: Cooperative Knowledge Processing: The Key Technology for Future Organizations. Juli 1995.

Nr. 40 Kirn, St.: Organisational Intelligence and Distributed AI. Juli 1995.

Nr. 41 Fischer, K.; Kirn, St.; Weinhard, Ch. (Hrsg.): Organisationsaspekte in Multiagentensytemen. September 1995.

Nr. 42 Grob, H. L.; Lange, W.: Zum Wandel des Berufsbildes bei Wirtschaftsinformatikern, Eine empirische Analyse auf der Basis von Stellenanzeigen. Oktober 1995.

Nr. 43 Abu-Alwan, I.; Schlagheck, B.; Unland, R.: Evaluierung des objektorientierten Datebankmanagementsystems ObjectStore. Dezember 1995.

Nr. 44 Winter, R.: Using Formalized Invariant Properties of an Extended Conceptual Model to Generate Reusable Consistency Control for Information Systems. Dezember 1995.

Nr. 45 Winter, R.: Design and Implementation of Derivation Rules in Information Systems. Februar 1996.

Nr. 46 Becker, J.: Eine Architektur für Handelsinformationssysteme. März 1996.

Nr. 47 Becker, J.; Rosemann, M. (Hrsg.): Workflowmanagement - State-of-the-Art aus Sicht von Theorie und Praxis, Proceedings zum Workshop vom 10. April 1996. April 1996.

Nr. 48 Rosemann, M.; zur Mühlen, M.: Der Lösungsbeitrag von Metadatenmodellen beim Vergleich von Workflowmanagementsystemen. Juni 1996.

Nr. 49 Rosemann, M.; Denecke, Th.; Püttmann, M.: Konzeption und prototypische Realisierung eines Informationssystems für das Prozeßmonitoring und -controlling. September 1996.

Nr. 50 v. Uthmann, C.; Turowski, K. unter Mitarbeit von Rehfeldt, M.; Skall, M.: Workflow-basierte Geschäftsprozeßregelung als Konzept für das Management von Produktentwicklungsprozessen. November 1996.

Nr. 51 Eicker, S.; Jung, R.; Nietsch, M.; Winter, R.: Entwicklung eines Data Warehouse für das Produktionscontrolling: Konzepte und Erfahrungen. November 1996.

Nr. 52 Becker, J.; Rosemann, M.; Schütte, R. (Hrsg.): Entwicklungsstand und Entwicklungsperspektiven Der Referenzmodellierung, Proceedings zur Veranstaltung vom 10. März 1997. März 1997.

Nr. 53 Loos, P.: Capture More Data Semantic Through The Expanded Entity-Relationship Model (PERM). Februar 1997.

Nr. 54 Becker, J.; Rosemann, M. (Hrsg.): Organisatorische und technische Aspekte beim Einsatz von Workflowmanagementsystemen. Proceedings zur Veranstaltung vom 10. April 1997. April 1997.

Nr. 55 Holten, R.; Knackstedt, R.: Führungsinformationssysteme - Historische Entwicklung und Konzeption. April 1997.

Nr. 56 Holten, R.: Die drei Dimensionen des Inhaltsaspektes von Führungsinformationssystemen. April 1997.

Nr. 57 Holten, R.; Striemer, R.; Weske, M.: Ansätze zur Entwicklung von Workflow-basierten Anwendungssystemen - Eine vergleichende Darstellung. April 1997.

Nr. 58 Kuchen, H.: Arbeitstagung Programmiersprachen, Tagungsband. Juli 1997.

Nr. 59 Vering, O.: Berücksichtigung von Unschärfe in betrieblichen Informationssystemen – Einsatzfelder und Nutzenpotentiale am Beispiel der PPS. September 1997.

Nr. 60 Schwegmann, A.; Schlagheck, B.: Integration der Prozeßorientierung in das objektorientierte Paradigma: Klassenzuordnungsansatz vs. Prozeßklassenansatz. Dezember 1997.

Nr. 61 Speck, M.: In Vorbereitung.

Nr. 62 Wiese, J.: Ein Entscheidungsmodell für die Auswahl von Standardanwendungssoftware am Beispiel von Warenwirtschaftssystemen. März 1998.

Nr. 63 Kuchen, H.: Workshop on Functional and Logic Programming, Proceedings. Juni 1998.

Nr. 64 v. Uthmann, C.; Becker, J.; Brödner, P.; Maucher, I.; Rosemann, M.: PPS meets Workflow. Proceedings zum Workshop vom 9. Juni 1998. Juni 1998.

Nr. 65 Scheer, A.-W.; Rosemann, M.; Schütte, R. (Hrsg.): Integrationsmanagement. Januar 1999.

Nr. 66 zur Mühlen, M.; Ehlers, L.: Internet - Technologie und Historie. Juni 1999.

Nr. 67 Holten R.: A Framework for Information Warehouse Development Processes. Mai 1999.

Nr. 68 Holten R.; Knackstedt, R.: Fachkonzeption von Führungsinformationssystemen – Instanziierung eines FIS-Metamodells am Beispiel eines Einzelhandelsunternehmens. Mai 1999.

Nr. 69 Holten, R.: Semantische Spezifikation Dispositiver Informationssysteme. Juli 1999.

Nr. 70 zur Mühlen, M.: In Vorbereitung.

Nr. 71 Klein, S.; Schneider, B.; Vossen, G.; Weske, M.; Projektgruppe PESS: Eine XML-basierte Systemarchitektur zur Realisierung flexibler Web-Applikationen. Juli 2000.

Nr. 72 Klein, S.; Schneider, B. (Hrsg): Negotiations and Interactions in Electronic Markets, Proceedings of the Sixth Research Symposium on Emerging Electronic Markets, Muenster, Germany, September 19 - 21, 1999. August 2000.

Nr. 73 Becker, J.; Bergerfurth, J.; Hansmann, H.; Neumann, S.; Serries, T.: Methoden zur Einführung Workflow-gestützter Architekturen von PPS-Systemen. November 2000.

Nr. 74 Terveer, I.: (In Vorbereitung).

Nr. 75 Becker, J. (Ed.): Research Reports, Proceedings of the University Alliance Executive Directors Workshop – ECIS 2001. Juni 2001.

Nr. 76, Klein, St.; u. a. (Eds.): MOVE: Eine flexible Architektur zur Unterstützung des Außendienstes mit mobile devices. (In Vorbereitung.)

Nr. 77 Knackstedt, R.; Holten, R.; Hansmann, H.; Neumann, St.: Konstruktion von Methodiken: Vorschläge für eine begriffliche Grundlegung und domänenspezifische Anwendungsbeispiele. Juli 2001.

Nr. 78 Holten, R.: Konstruktion domänenspezifischer Modellierungstechniken für die Modellierung von Fachkonzepten. August 2001.

Nr. 79 Vossen, G.; Hüsemann, B.; Lechtenbörger, J.: XLX – Eine Lernplattform für den universitären Übungsbetrieb. August 2001.

Nr. 80 Knackstedt, R.; Serries, T.: Gestaltung von Führungsinformationssystemen mittels Informationsportalen; Ansätze zur Integration von Data-Warehouse- und Content-Management-Systemen. November 2001.

Nr. 81 Holten, R.: Conceptual Models as Basis for the Integrated Information Warehouse Development. Oktober 2001.

Nr. 82 Teubner, A.: Informationsmanagement: Historie, disziplinärer Kontext und Stand der Wissenschaft. (in Vorbereitung).

Nr. 83 Vossen, G.: Vernetzte Hausinformationssysteme – Stand und Perspektive. Oktober 2001.

Nr. 84 Holten, R.: The MetaMIS Approach for the Specification of Management Views on Business Processes. November 2001.

Nr. 85 Becker, J.; Neumann, S.; Hansmann, H.: (Titel in Vorbereitung). Januar 2002.

Nr. 86 Teubner, R. A.; Klein, S.: Bestandsaufnahme aktueller deutschsprachiger Lehrbücher zum Informationsmanagement. März 2002.

Nr. 87 Holten, R.: Specification of Management Views in Information Warehouse Projects. April 2002.

Nr. 88 Holten, R.; Dreiling, A.: Specification of Fact Calculations within the MetaMIS Approach. Juni 2002.

Nr. 89 Holten, R.: Metainformationssysteme – Backbone der Anwendungssystemkopplung. Juli 2002.

Nr. 90 Becker, J.; Knackstedt, R. (Hrsg.): Referenzmodellierung 2002. Methoden – Modelle – Erfahrungen. August 2002.

Nr. 91 Teubner, R. A.: Grundlegung Informationsmanagement. Februar 2003.

Nr. 92 Vossen, G.; Westerkamp, P.: E-Learning as a Web Service. Februar 2003.

Nr. 93 Becker, J.; Holten, R.; Knackstedt, R.; Niehaves, B.: Forschungsmethodische Positionierung in der Wirtschaftsinformatik - epistemologische, ontologische und linguistische Leitfragen. Mai 2003.

Nr. 94 Algermissen, L.; Niehaves, B.: E-Government – State of the art and development perspectives. April 2003.

Nr. 95 Teubner, R. A.; Hübsch, T.: Is Information Management a Global Discipline? Assessing Anglo-American Teaching and Literature through Web Content Analysis. November 2003.

Nr. 96 Teubner, R. A.: Information Resource Management. Dezember 2003.

Nr. 97 Köhne, F.; Klein, S.: Prosuming in der Telekommunikationsbranche: Konzeptionelle Grundlagen und Ergebnisse einer Delphi-Studie. Dezember 2003.

Nr. 98 Vossen, G.; Pankratius, V.: Towards E-Learning Grids. 2003.

Nr. 99 Vossen, G.; Paul, H.: Tagungsband EMISA 2003: Auf dem Weg in die E-Gesellschaft. 2003.

Nr. 100 Vossen, G.; Vidyasankar, K.: A Multi-Level Model for Web Service Composition. 2003.

Nr. 101 Becker, J.; Serries, T.; Dreiling, A.; Ribbert, M.: Datenschutz als Rahmen für das Customer Relationship Management – Einfluss des geltenden Rechts auf die Spezifikation von Führungsinformationssystemen. November 2003.

Nr. 102 Müller, R.A.; Lembeck, C.; Kuchen, H.: GlassTT – A Symbolic Java Virtual Machine using Constraint Solving Techniques for Glass-Box Test Case Generation. November 2003.

Nr. 103 Becker, J; Brelage C.; Crisandt J.; Dreiling A.; Holten R.; Ribbert M.; Seidel S.: Methodische und technische Integration von Daten- und Prozessmodellierungstechniken für Zwecke der Informationsbedarfsanalyse. März 2004.

Nr. 104 Teubner, R. A.: Information Technology Management. April 2004.

Nr. 105 Teubner, R. A.: Information Systems Management. August 2004.

Nr. 106 Becker, J.; Brelage, C.; Gebhardt, Hj.; Recker, J.; Müller-Wienbergen, F.: Fachkonzeptionelle Modellierung und Analyse web-basierter Informationssysteme mit der MW-KiD Modellierungstechnik am Beispiel von ASInfo. Mai 2004.

Nr. 107 Hagemann, S.; Rodewald, G.; Vossen, G.; Westerkamp, P.; Albers, F.; Voigt, H.: BoGSy – ein Informationssystem für Botanische Gärten. September 2004.

Nr. 108 Schneider, B.; Totz, C.: Web-gestützte Konfiguration komplexer Produkte und Dienstleistungen. September 2004.

Nr. 109 Algermissen, L; Büchel, N.; Delfmann, P.; Dümmer, S.; Drawe, S.; Falk, T.; Hinzen, M.; Meesters, S.; Müller, T.; Niehaves, B.; Niemeyer, G.; Pepping, M.; Robert, S.; Rosen-

kranz, C.; Stichnote, M.; Wienefoet, T.: Anforderungen an Virtuelle Rathäuser – Ein Leitfaden für die herstellerunabhängige Softwareauswahl. Oktober 2004.

Nr. 110 Algermissen, L; Büchel, N.; Delfmann, P.; Dümmer, S.; Drawe, S.; Falk, T.; Hinzen, M.; Meesters, S.; Müller, T.; Niehaves, B.; Niemeyer, G.; Pepping, M.; Robert, S.; Rosenkranz, C.; Stichnote, M.; Wienefoet, T.: Fachkonzeptionelle Spezifikation von Virtuellen Rathäusern – Ein Konzept zur Unterstützung der Implementierung. Oktober 2004.

Nr. 111 Becker, J.; Janiesch, C.; Pfeiffer, D.; Rieke, T.; Winkelmann, A.: Studie: Verteilte Publikationserstellung mit Microsoft Word und den Microsoft SharePoint Services. Dezember 2004.

Nr. 112 Teubner, R. A.; Terwey, J.: Informations-Risiko-Management: Der Beitrag internationaler Normen und Standards. April 2005.

Nr. 113 Teubner, R. A.: Methodische Integration von Organisations- und Informationssystemgestaltung: Historie, Stand und zukünftige Herausforderungen an die Wirtschaftsinformatik-Forschung. Mai 2006.

Nr. 114 Becker, J.; Janiesch, C.; Knackstedt, R.; Kramer, S.; Seidel, S.: Konfigurative Referenzmodellierung mit dem H2-Toolset. November 2006.

Nr. 115 Becker, J.; Fleischer, S.; Janiesch, C.; Knackstedt, R; Müller-Wienbergen, F.; Seidel, S.: H2 for Reporting – Analyse, Konzeption und kontinuierliches Metadatenmanagement von Management-Informationssystemen. Februar 2007.

Nr. 116 Becker, J.; Kramer, S.; Janiesch, C.: Modellierung und Konfiguration elektronischer Geschäftsdokumente mit dem H2-Toolset. November 2007.

Nr. 117 Becker, J., Winkelmann, A., Philipp, M.: Entwicklung eines Referenzvorgehensmodells zur Auswahl und Einführung von Office Suiten. Dezember 2007.

Nr. 118 Teubner, A.: IT-Service Management in Wissenschaft und Praxis.

Nr. 119 Becker, J.; Knackstedt, R.; Beverungen, D. et al.: Ein Plädoyer für die Entwicklung eines multidimensionalen Ordnungsrahmens zur hybriden Wertschöpfung. Januar 2008.

Nr. 120 Becker, J.; Krcmar, H.; Niehaves, B. (Hrsg.): Wissenschaftstheorie und gestaltungsorientierte Wirtschaftsinformatik. Februar 2008.

Nr. 121 Becker, J.; Richter, O.; Winkelmann, A.: Analyse von Plattformen und Marktübersichten für die Auswahl von ERP- und Warenwirtschaftssysteme. Februar 2008.

Nr. 122 Vossen, G.: DaaS-Workshop und das Studi-Programm. Februar 2009.

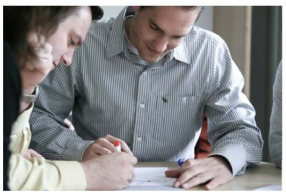
Nr. 123 Knackstedt, R.; Pöppelbuß, J.: Dokumentationsqualität von Reifegradmodellentwicklungen. April 2009.

Nr. 124 Winkelmann, A.; Kässens, S.: Fachkonzeptionelle Spezifikation einer Betriebsdatenerfassungskomponente für ERP-Systeme. Juli 2009.

Nr. 125 Becker, J.; Knackstedt, R.; Beverungen, D.; Bräuer, S.; Bruning, D.; Christoph, D.; Greving, S.; Jorch, D.; Joßbächer, F.; Jostmeier, H.; Wiethoff, S.; Yeboah, A.: Modellierung der hybriden Wertschöpfung: Eine Vergleichsstudie zu Modellierungstechniken. November 2009.

Nr. 126 Becker, J.; Beverungen, D.; Knackstedt, R.; Behrens, H.; Glauner, C.; Wakke, P.: Stand der Normung und Standardisierung der hybriden Wertschöpfung. Januar 2010.

Nr. 127 Majchrzak, T. A.; Kuchen, H.: Handlungsempfehlungen für erfolgreiches Testen von Software in Unternehmen, Februar 2010.



Arbeitsberichte des Instituts für Wirtschaftsinformatik

Kontakt
Institut für Wirtschaftsinformatik
✉ Leonardo-Campus 3, 48149 Münster
✆ +49 (251) 8338100
@ becker@ercis.uni-muenster.de
💻 http://www.wi.uni-muenster.de

WIRTSCHAFTS INFORMATIK

Westfälische Wilhelms-Universität Münster

ISSN 1438-3985