KNOWLEDGE ENGINEERING DES MANAGEMENTS DER INFORMATIONSSYSTEMSICHERHEIT

ENTWICKLUNG EINER DIAGNOSE-SHELL ZUR UNTERSTÜTZUNG VON INFORMATIONSSYSTEMSICHERHEIT

DISSERTATION ZUR ERLANGUNG DES AKADEMISCHEN GRADES EINES
DOKTORS DER WIRTSCHAFTSWISSENSCHAFTEN (DR. RER. POL.)

DURCH DEN FACHBEREICH WIRTSCHAFTSWISSENSCHAFTEN DER
UNIVERSITÄT DUISBURG-ESSEN
STANDORT ESSEN

VORGELEGT VON
DIPL.-WIRT.INFORM. SVEN PETER WIEGAND,
GEBOREN IN LUANDA/ANGOLA

DISPUTATION: 06.02.2004

ERSTGUTACHTER: UNIV.-PROF. DR. GÜNTHER PERNUL

ZWEITGUTACHTER: UNIV.-PROF. DR. STEFAN EICKER

Inhaltsübersicht

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Definitionsverzeichnis

Abkürzungsverzeichnis

AES	Advanced Encryption Standard
AG	Aktiengesellschaft
AIFCW	Air Force Information Warface Center
AktG	Aktiengesetz
ALE	Annualized Loss Expectancy
AOL	American Online
ASIS	Anwenderanforderungen an die Sicherheit der Informationsverarbeitung
Aufl.	Auflage
BCM	Business Continuity Managements
BDSG	Bundesdatenschutzgesetz
BS	British Standard
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSP	Baseline Security Policy
bzgl.	bezüglich
bzw.	beziehungsweise
CBR	Case-Based Reasoning
CC	Common Criteria
CCTA	Central Computer and Telecommunications Agency
CERT	Computer Emergency Response Team
cf	certainty factors
CFR	Code Federal Regulations
CobiT	Control Objectives for Information and Related Technology
COFC	Commercially Oriented Functionality Class for Security Evaluation
CoP	Code of Practice
COSSAC	Computer Systems Security Analyser and Configurator
CRAMM	CCTA Risk Analysis and Management Method
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria
CSP	Critical Security Parameters
DARPA	Defense Applied Research Projects Agency
DB	Datenbank
DES	Digital Encryption Standard
DFÜ	Datenverübertragung
Diagnose-WBS	Wissensbasiertes Diagnosesystem
DIN	Deutsches Institut für Normung e.V.
DoD	Departement of Defense
DSB	Datenschutzbeauftragter
DSS	Digital Signature Standard
DuD	Datenschutz und Datensicherheit
EAL	Evaluation Assurance Level
ECMA	European Computer Manufactures Association
E-COFC	Extended Commercially Oriented Functionality Class for Security Evaluation
E-Commerce	Electronic Commerce
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
EGG	Elektronisches Geschäftsverkehr-Gesetz
E-Government	Electronic Government
EIS	Executive Information Systems
engl.	englisch
ERM	Entity-Relationship-Model
ESS	Excecutive Support Systems
ETA	Event Tree Analysis
EUS	Entscheidungsunterstützendes System
EVA	Eingabe, Verarbeitung, Ausgabe
EVG	Evaluationsgegenstand
f.	folgende

ff.	fortfolgend
FIPS	Federal Information Processing Standards
FIRST	Forum of Incident Response and Security Teams
FMEA	Failure Mode und Effects Analysis
FQS	Forschungsgemeinschaft Qualitätssicherung e.V.
FTA	Fault Tree Analysis
FÜV	Fernmeldeverkehr-Überwachungs-Verordnung
GmbH	Gesellschaft mit beschränkter Haftung
GMD	Gesellschaft für Mathematik und Datenverarbeitung
GPOSS	Geschäftsprozeß-orientiertes Simulations-System
GPS	General Problem Solver
H.	Heft
Hrsg.	Herausgeber
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
i.d.R.	in der Regel
IEC	International Electrotechnical Commission
IEC	International Electrotechnical Commission
IS	Informationssystem
ISACA	Information Systems Audit and Control Association
ISi	Informationssicherheit
ISO	International Organization for Standardization
IT	Informationstechnik
ITSEC	Trusted Computer Systems Evaluation Criteria
IV	Informationsverarbeitung
Jg.	Jahrgang
KADS	Knowledge Acquisition and Documentation Structuring
KE	Knowledge Engineering
KES	Zeitschrift für Kommunikations- und EDV-Sicherheit
KI	Künstliche Intelligenz
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereichen
LAN	Local Area Network
LDSG SH	Landesdatenschutzgesetz Schleswig-Holstein
LNAI	Lecture Notes in Artificial Intelligence
MIKE	Model-based and Incremental Knowledge Engineering
MSS	Management Support Systeme
NASA	National Aeronautics and Space Administration
NBS	National Bureau of Standard
NIST	National Institute of Standards and Technology
nnb.	nicht näher bestimmt
o. J.	ohne Jahr
o. Jg.	ohne Jahrgang
o. O.	ohne Ortsangabe
o. V.	ohne Verfasser
PC	Personal Computer
PP	Protection Profile
RAID	Redundant Array of Inexpensive Disks
RAMeX	Risk Analysis and Management eXpert system
RSD	Rapid Secure Development
RTF	Rich-Text Format
S.	Seite
SHA	Secure Hash Standard
SigG	Signaturgesetz
SINUS	Sichere Nutzung von Online-Diensten
SiSSA	Sicherheits-Schwachstellenanalyse
SQL	Structured Query Language
ST	Security Target
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstgesetz
TDSV	Telekommunikations-Datenschutzverordnung
TK	Telekommunikation
TKG	Telekommunikationsgesetz

TKÜV	Entwurf eines Telekommunikations-Überwachungsverordnung
TKV	Telekommunikations-Kundenschutzverordung
TRAW	Knowledge Based Threat and Risk Analysis of Workflow-Bases Applications
TÜV	Technischer Überwachungsverein
u.a.	unter anderem
ULD SH	Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein
UML	Unified Modeling Language
URL	Uniform Resource Locators
USA	Unites States of America
USV	Unterbrechungsfreie Stromversorgung
UZ	Unternehmensziele
Vgl.	Vergleiche
WBS	Wissensbasiertes System
WWW	World Wide Web
XML	Extensible Markup Language
XPS	Expertensystem
z.B.	zum Beispiel
z.T.	zum Teil
zfbf	Schmalenbachs Zeitschrift für betriebswirtschaftliche Forschung
zit.	zitiert

1 Einführung

1.1 Motivation

Motivation dieser Arbeit ist die Unterstützung des Informationssystemsicherheitsmanagements (kurz IS-Sicherheitsmanagement) durch das Knowledge Engineering (KE). Mit Hilfe des KE entsteht ein tiefes und gründliches Verständnis der Problemlösungsprozesse des IS-Sicherheitsmanagements auf verschiedenen Abstraktionsstufen, auch wenn das Wissen in impliziter Form vorhanden ist. Als Ergebnis des KE werden das IS-Sicherheitswissen und die Problemlösungsprozesse des IS-Sicherheitsmanagements explizit durch ein Expertisemodell beschrieben und mit Hilfe eines wissensbasierten Systems (WBS) operationalisiert.

Knowledge Engineering

Das Knowledge Engineering ist ein Teilbereich der Künstlichen Intelligenz (KI) und beinhaltet alle Tätigkeiten und Überlegungen zur Erfassung, Verwaltung und Verarbeitung großer praxisrelevanter Wissensbestände[1]. *„Künstliche Intelligenz ist eine wissenschaftliche Disziplin, die das Ziel verfolgt, menschliche Wahrnehmungs- und Verstandesleistungen zu operationalisieren und durch Artefakte, kunstvoll gestaltete technische - insbesondere informationsverarbeitende - Systeme verfügbar zu machen“*[2]. Obwohl die KI und somit auch das KE als Teilgebiet in der Informatik verankert sind[3], besitzen sie einen stark ausgeprägten interdisziplinären Charakter. Dies ergibt sich aus der kognitionswissenschaftlichen Komponente und den damit zusammenhängenden wissenschaftlichen Disziplinen, wie Philosophie, Psychologie, Linguistik und den Neurowissenschaften. Aber auch aus den vielfältigen Anwendungsgebieten der KI - wie z.B. Sprach- und Bildverstehen, Robotik, neuronale Netze oder Software Agenten - erwächst eine Fülle von vielfachen Interdependenzen.

Management der Informationssystemsicherheit

Das Management der Informationssystemsicherheit umfasst die gesamten Aktivitäten zur geplanten und dauerhaften Gestaltung der IS-Sicherheit einer Institution[4]. Die Informationssystemsicherheit ist ein wichtiges Managementproblem, das auf allen Ebenen des Unternehmensmanagements zu finden ist[5]. Grundlage für die Problemlösungsprozesse des IS-Sicherheitsmanagements bilden das IS-Sicherheitswissen und die IS-Sicherheitsmanagementstrategien[6]. Die wissensbasierte Analyse des IS-Sicherheitswissens und der IS-Sicherheitsstrategien[7] des IS-Sicherheitsmanagements und deren explizite Beschreibung durch ein Expertisemodell bilden die Basis für die Operationalisierung in einem wissensbasierten System.

---

[1] Vgl. Puppe/Stoyan/Studer (2000), S. 599
[2] Görz/Wachsmuth (2000), S. 1
[3] Vgl. Kurbel (1992), S. 4 und Stickel/Groffmann/Rau (1998) S. 403
[4] Vgl. Oppliger (1997), S. 21 und Konrad (1998), S. 46
[5] Vgl. Wehner (1995), S. 27; Brandao (1996), S. 1; Petzel (1996), S. 9; Plate (1997), S. 373 und Karger (1999), S. 157
[6] Vgl. Hartmann/Karger (2001), S. 381
[7] Für den Begriff „IS-Sicherheitsmanagementstrategien“ wird im Rahmen der Arbeit verkürzt „IS-Sicherheitsstrategien“ verwendet.

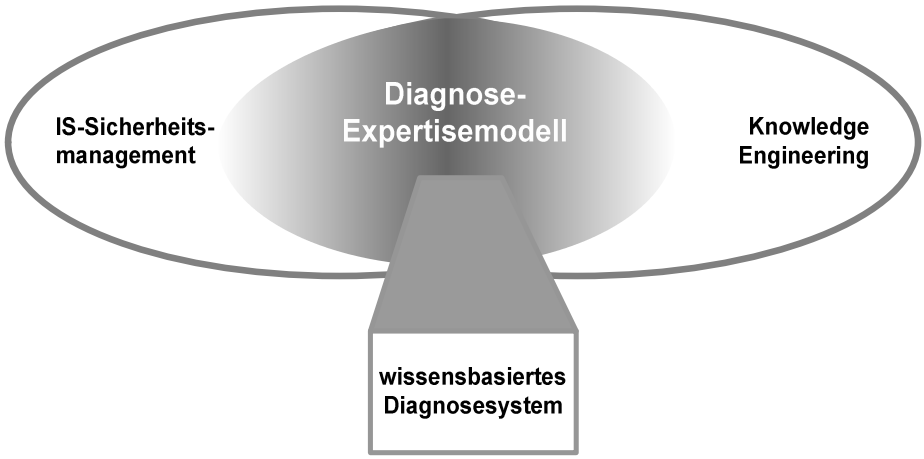


Abbildung 1: Motivation der Arbeit

Die Motivation der Arbeit liegt in der Zusammenführung der Bereiche IS-Sicherheitsmanagement und Knowledge Engineering, deren Ergebnisse in einem Expertisemodell münden und dessen Operationalisierung durch ein WBS erfolgt.

IS-Sicherheitsmanagement als Diagnoseaufgabe

In der Arbeit wird die Entwicklung des wissensbasierten Diagnosesystems (Diagnose-WBS) zur Unterstützung des IS-Sicherheitsmanagements durch das KE bestimmt. Diagnoseprobleme[8] stellen einen wichtigen Anwendungsbereich des KE dar. Ein wesentliches Charakteristikum der wissensbasierten Diagnose ist, dass Merkmale, Lösungen und deren Lösungswissen explizit dargestellt sowie Lösungen aus einer Menge vorgegebener Alternativen ausgewählt werden.

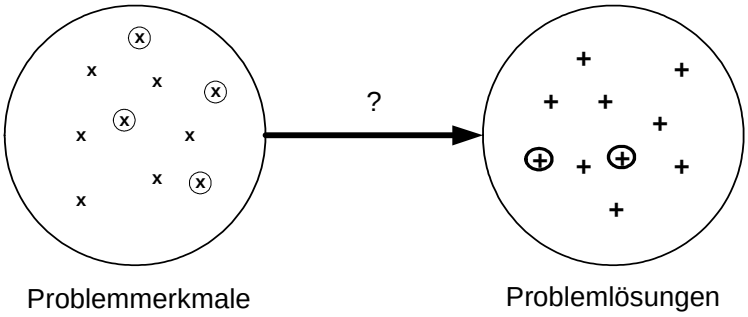


Abbildung 2: Grundprinzip der Diagnostik[9]

Der Lösungsprozess der wissensbasierten Diagnose beruht auf Problemen mit folgenden grundlegenden Eigenschaften:

- Der Problembereich besteht aus Problemmerkmalen (Merkmale, Wirkungen) und Problemlösungen (Lösungen, Ursachen), die voneinander getrennt sind. Zwischen beiden Bereichen bestehen mehrstufige Abhängigkeiten, was sich als Lösungswissen zwischen den Merkmalen und deren Lösung ausdrückt.
- Durch die wissensbasierte Diagnose erfolgt eine explizite Beschreibung der Abhängigkeiten von Merkmalen und Lösungen. Bei sicherem Wissen liegen meist eine oder mehrere

[8] Im Rahmen der Arbeit wird der Begriff „Diagnostik“ als Synonym für den Begriff „Diagnose“ verwendet.
[9] Vgl. Puppe et al (1996), S. 3

direkte „verknüpfte“ Lösungen vor. Dies ist bei unsicherem Wissen nicht möglich, da hier eine Unsicherheit zwischen den ermittelten Merkmalen und den „verknüpften“ Lösungen besteht.

- Das Diagnoseproblem umfasst eventuell eine unvollständige Teilmenge an (erhobenen) Merkmalen; das Ergebnis setzt sich aus einer oder mehreren Lösungen zusammen. Dieser Umgang mit Mehrfachlösungen stellt ein schwieriges Problem für die Diagnostik dar.
- Die Teilaufgabe der Diagnose ist zu bestimmen, welche (weiteren) Merkmale zusätzlich benötigt werden, um die Qualität der Diagnose bzw. Lösung zu verbessern.

Die Diagnose wird vielfach auf den Problemgebieten angewendet, die zwar eine komplexe Struktur haben, jedoch eine überschaubare Anzahl von häufig wiederkehrenden, stereotypischen Lösungsmustern besitzen[10]. Weite Bereiche des Problemtyps IS-Sicherheit erfüllen dieses Kriterium, denn viele Merkmale und Lösungen aus dem Bereich der IS-Sicherheit sind über 20 Jahre wohl bekannt. Hierbei haben sich wiederkehrende, stereotypische Lösungsmuster herausgebildet, die z.B. in Kriterienwerken manifestiert sind[11]. Die Merkmals- und Lösungsmuster des IS-Sicherheitswissens werden zu Konzepten (z.B. Risiken, Sicherheitsschwachstellen, Maßnahmen, Gefahren usw.) zusammengefasst, die bei diagnostischen Problemlösungsprozessen angewandt werden.

1.2 Wissen und Information im Kontext des Knowledge Engineerings

“*Wissen wird als Erkenntnis von Sachverhalten (Mustern) oder als Bewußtsein entsprechender Denkinhalte definiert; der Zweck von Wissen besteht in der Vorbereitung und Durchführung von Handlungen und Entscheidungen*“[12]. Wissen bildet somit die Grundlage für das Entscheiden (z.B. in Form von Entscheidungsregeln oder explizit formulierten Entscheidungsmodellen) und Handeln, wobei das „Wissensmanagement“ den Entscheidungsträger bei dem Erwerb, Zugriff, Nutzung und Weitergabe von Wissen unterstützt[13]. Dabei verwendet das Wissensmanagement Methoden und computergestützte Systeme des Knowledge Engineerings (z.B. WBS)[14], um die Verwaltung des Wissens, den Zugriff und die explizite Verarbeitung des Wissens zu gestalten.

Durch die facettenreiche Verwendung des Begriffs „Wissen“ in unterschiedlichen Anwendungsbereichen ist es ersichtlich, dass eine eindeutige allgemeine akzeptierte Definition des Begriffs „Wissen“ nicht möglich ist[15]. Um eine Einordnung für die Arbeit zu erlangen, dient die folgende Abbildung.

[10] Vgl. Puppe (1990), S. 43
[11] Vgl. Voßbein, R. (1994b), S. 64
[12] Voß/Gutenschwager (2001), S. 24
[13] Vgl. Fink/Schneidereit/Voß (2001), S. 78 und Staab et al. (2001), S. 27
[14] Vgl. Schreiber et al. (2000), S. 82 und Preece et al. (2001), S. 37
[15] Vgl. Walter (1990), S. 2 und Servatius (1993), S. 34

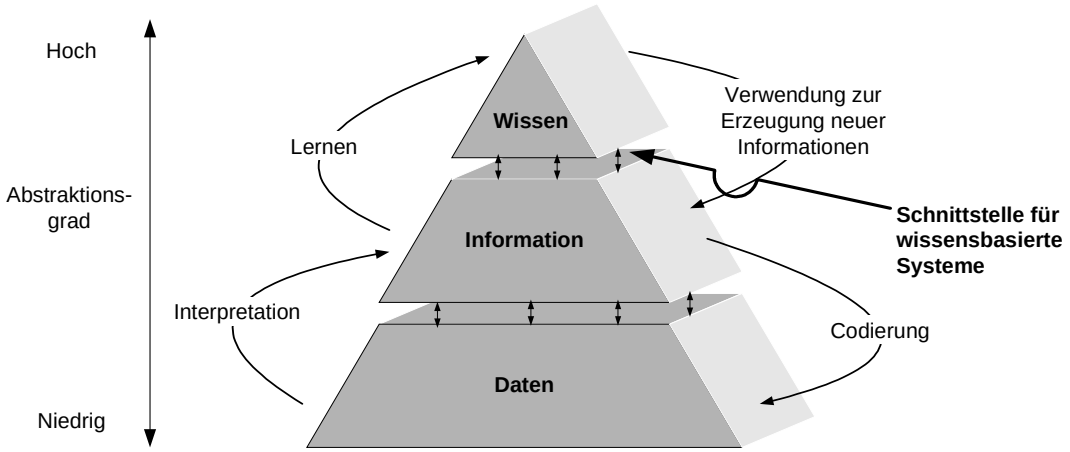


Abbildung 3: Daten, Informationen und Wissen[16]

Aus Daten entstehen Informationen, wenn diese in einem bestimmten Kontext interpretiert werden bzw. Bedeutung erlangen[17]. Wissen und Information sind eng miteinander verbunden, denn „*Wissen wird durch Aufnahme und Einbindung von Information in (bestehendes) Wissen aufgebaut bzw. wird Information aus bestehendem Wissen mitgeteilt*“[18], bzw. „*Wissen besteht aus vielen Informationen sowie der Kenntnisse über die Zusammenhänge der Informationen*“[19]. „*Wissen kann folglich als eine verarbeitete Information angesehen werden*“[20].

Wissen besitzt zusätzlich eine „Zweckorientierung“, wodurch „…*Erwartungen bei der Aufnahme von Informationen in Wissen und bestimmte Absichten bei der Entnahme von Informationen aus Wissen* […] *vorhanden sein müssen*“[21]. Durch die verknüpfte Aufnahme von mehreren Informationsbestandteilen entsteht Wissen, was auch als Lernen bezeichnet werden kann. Wird das Wissen wiederum „zweckorientiert“ angewendet, können in Kombination aus Wissen und bekannten Informationen neue Informationen extrahiert werden, wobei das Wissen hier als Informationsgenerator dient. Diese Informationen können z.B. als Entscheidungsgrundlage dienen, die dann wiederum als Daten codiert werden können. WBS befinden sich in der Schnittstelle zwischen Wissen und Information, denn einerseits sollen WBS Wissen repräsentieren, andererseits sollen sie aus repräsentiertem Wissen neue Informationen generieren.

Ein weiteres Unterscheidungsmerkmal von Information und Wissen ist der höhere Abstraktions- und Komplexitätsgrad von Wissen. So unterscheidet Turban Information und Wissen durch die beiden Dimensionen „Abstraktion“ und „Quantität“, wobei Wissen den höchsten Abstraktionsgrad und die niedrigste Menge aufweist, da hier eine große Verdichtung in Folge der Vernetzung von Informationen erfolgt[22]. Dies bedeutet, dass kleine Mengen an Wissen zu einer sehr großen Informationsmenge führen können. Für die Darstellung von Informationen in einem Datenformat wird wiederum eine größere Menge an Daten benötigt.

[16] Vgl. Turban/Aronson (1998), S. 203 und Fink/Schneidereit/Voß (2001), S. 69
[17] Vgl. Krcmar (2000), S. 11
[18] Heinrich (2001) S. 131
[19] Schwarzer/ Krcmar (1996), S. 9
[20] Fink/Schneidereit/Voß (2001), S. 69
[21] Heinrich (2001) S. 131
[22] Vgl. Turban (1998), S. 203

1.3 Entwicklungsmethodologien des Knowledge Engineerings

Voraussetzung für eine erfolgreiche Entwicklung und Nutzung des WBS ist zuvor ein systematischer Entwicklungsprozess, der als „Knowledge Engineering“ bezeichnet wird. „Der Begriff „systematisch“ impliziert den Einsatz einer Entwicklungsmethodologie, die sich auch an ökonomischen-technischen Zielsystemen der Unternehmen und allgemeinen Prinzipien orientiert, welche durch Methoden und Techniken realisiert und durch Werkzeuge unterstützt werden“[23]. Obwohl viele Parallelen zu der Entwicklung von „traditionellen“ Softwaresystemen (Software Engineering[24]) bestehen, ist es aufgrund der speziellen Eigenschaften eines WBS erforderlich, einen eigenständigen Entwicklungsprozess für solche Systeme zu prägen[25].

Folgende Punkte zeigen die Unterschiede zu dem Software-Engineering auf[26]:

- Die Probleme, die mit WBS gelöst werden, können als „unvollständig spezifizierte Funktion“ bezeichnet werden. Es wird ausgedrückt, dass die Probleme sehr komplex sind oder noch nicht vollständig verstanden werden. Somit kann ein solches System nicht vollständig vorab spezifiziert werden, sondern die Spezifikation muss in enger Zusammenarbeit mit dem Knowledge Engineer[27] (Entwickler) und Fachexperten erstellt werden[28].
- Für die zu lösenden Probleme ist die Komplexität des Problems i.d.R. so groß, dass nur kleine Probleminstanzen lösbar sind. Dies bedeutet, dass das Problem eingeschränkt gelöst wird bzw. die Lösung nur approximiert werden kann. So werden Heuristiken verwendet, um eine Lösung zu erreichen, die aber häufig nicht die Optimallösung oder lediglich eine Teillösung beinhaltet. Die „traditionelle“ Software dagegen besitzt den Charakter eines „Number-crunching“ Systems, das große Mengen von Daten durch einheitliche Algorithmen verarbeitet.
- Im WBS wird das Wissen explizit repräsentiert, wohingegen in konventionellen Programmen das Wissen in Algorithmen bzw. direkt im Programmcode implementiert bzw. „hineinprogrammiert“ ist. Dies gilt insbesondere für das Problemlösungswissen. So erfordern in traditionellen Softwaresystemen Änderungen oft umfangreiche Modifizierungen des Programmcodes. Dies verursacht eine niedrige Flexibilität gegenüber Veränderungen des Wissens und zusätzlich eine starke Abhängigkeit von den Programmierern des Systems.[29]

Das Knowledge Engineering hat in den letzten Jahrzehnten einen Paradigmenwechsel von den Ansätzen des Wissenstransfers hin zu den Ansätzen der Wissensmodellierung erfahren[30]. Dieser Paradigmenwechsel wird auch als Übergang vom WBS der ersten Generation hin zum

[23] Vgl. Hoppe (1992), S. 30
[24] „*Software Engineering* [ist] *der gesamte Bereich, der sich auf der Basis der Software-Technologie mit dem ingenieursmäßigen Entwerfen, Entwickeln, Validieren, Anwenden und Warten von Software einschließlich der damit verbundenen Strategien, Prinzipien, Methoden, Verfahren, Techniken und Werkzeugen beschäftigt.*“ Stickel/Groffmann/Rau (1998), S. 652
[25] Vgl. Preece et al. (2001), S. 36
[26] Vgl. Angele/Fensel/Studer (1998), S. 169 f.
[27] Wissensingenieur wird in der Arbeit als Synonym für Knowledge Engineer verwendet.
[28] Knowledge Engineer und Fachexperte können eventuell die gleiche Person darstellen.
[29] Vgl. Zelewski (1989), S. 19 und Kurbel (1992), S. 17
[30] Vgl. Studer/Benjamins/Fensel (1998), S. 162

WBS der zweiten Generation bezeichnet. Verbunden mit dem Paradigmenwechsel existieren folgende Entwicklungsmethodologien für das Knowledge Engineering[31]:

- transferorientierte Ansätze und
- modellierungsorientierte Ansätze.

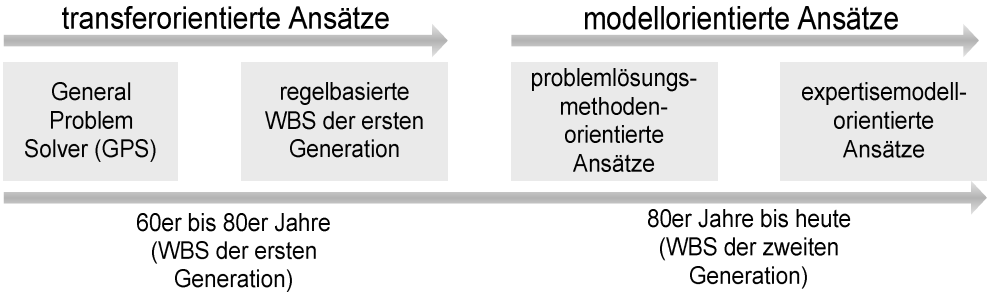


Abbildung 4: Historische Entwicklung des KE

Transferorientierte Ansätze

Anfang der 50er bis Ende der 60er Jahre wurden erste WBS in Form eines „General Problem Solvers“ (GPS) erstellt. Das GPS sollte eine allgemeine Problemlösungsfähigkeit umfassen, um somit auf jedes Problem angewandt zu werden. Die Problemlösung erfolgte durch geeignete Operationen, welche die Differenz zwischen dem Ausgangszustand und dem Zielzustand reduzieren sollten. Die Annahme eines generellen Problemlösers hat sich aber als unrealistisch herausgestellt[32].

In dem nächsten Jahrzehnt wurden WBS entwickelt, die auf Produktionsregeln und Frames unter der Annahme basierten, dass der menschliche Verstand mit vorwärts- und rückwärtsverketteten Produktionsregeln funktioniert und die menschlichen Wissensstrukturen durch Frames abgebildet werden können. Der Experte wird somit nur systematisch ausgefragt, um sein Wissen direkt in eine Wissensbasis zu übertragen, was einem Transferansatz entspricht[33]. Diese Vorgehensweise wird durch das Prototyping unterstützt, da schnell funktionsfähige WBS erstellt werden können[34]. Bei diesen Ansätzen wird nach Erhebung einer relativ kleinen Menge von Fallbeispielen ein WBS-Prototyp erstellt, der als ein ausführbares Modell definiert werden kann. Nach weiteren Wissenserhebungen wird der jeweilige Prototyp iterativ erweitert und verfeinert, bis er den an ihn gestellten Anforderungen genügt.

Auf Basis dieser Vorgehensweise wurden in den 80er Jahren regelbasierte WBS erstellt, die durch einen starren Regelinterpreter das Fachwissen auswerten. Die Wissensbasis besteht i.d.R. aus Frames und Produktionsregeln, die durch einen vorwärts- und rückwärtsorientierten Regelinterpreter ausgewertet werden. In der Abbildung 5 werden die beschriebenen Komponenten als typischer Kern eines WBS der ersten Generation dargestellt.

[31] Vgl. Kirchhoff (1994), S. 119; Borndorff-Eccarius (1998), S. 34; Herrmann (1997), S. 22-26 und Frick (1998), S. 283
[32] Vgl. Reimer (1991), S. 1
[33] Vgl. Puppe/Stoyan/Studer (2000), S. 602
[34] Vgl. Angele/Fensel/Studer (1998), S. 169

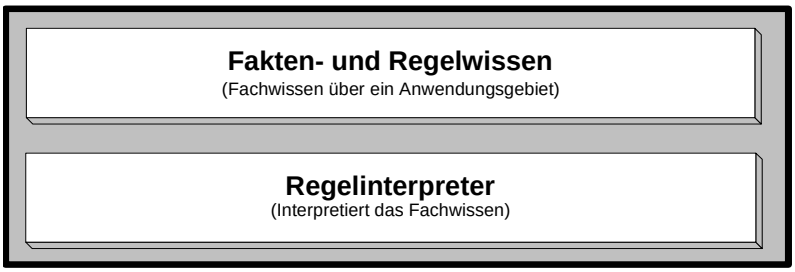


Abbildung 5: Kern eines WBS der ersten Generation[35]

Der Transferansatz, auf dem die meisten WBS basieren[36], geht davon aus, dass menschliches Wissen nur erhoben und ohne Veränderung in eine Wissensbasis überführt wird. Dies impliziert die Annahme, ein Modell aus Produktionsregeln und Frames stelle den menschlichen Verstand und die Wissensstrukturen dar und ließe sich mit erhobenem Wissen „auffüllen“[37]. Es erfolgt direkt eine Wissensoperationalisierung, wobei die Analyse der Problemlösung vernachlässigt wird. Das führt zur negativen Folge, dass Problemlösungsprozesse nicht explizit modelliert, sondern implizit in dem Regelinterpreter repräsentiert werden[38]. Es entstanden zwar erfolgreiche Prototypen mit kleinen Wissensbasen und experimentellem Charakter für einen begrenzten Anwendungsfall, jedoch bei einem praktischen Einsatz in größerem Umfang scheitern diese Systeme.

Modellierungsorientierte Ansätze

Im Laufe der Zeit haben sich die Annahmen, das zu lösende Problem dem WBS anzupassen, als problematisch erwiesen[39], denn durch die direkte Übertragung des menschlichen Wissens in einen künstlichen Problemlöser werden ohne kritische Reflexion Annahmen über Prinzipien des menschlichen „Problemlösers“ gemacht. Daraus hat sich seit Mitte der 80er Jahre die Überzeugung durchgesetzt, dass die Entwicklung eines WBS nicht durch den Transfer des Wissens auf einer vorgefertigten Wissensbasis beruht, sondern eine Modellierungsaktivität darstellt. „*Wissen vom Experten erwerben wird gesehen als Prozeß der Suche nach den angemessenen Modellumrissen und der ingenieurmäßigen Konstruktion eines Problemlösungsmodells mit allen benötigten Wissensbeständen. Dieses Modell ist kein Modell im Sinne der Abbildung von existierender Realität, sondern ein Modell im Sinne von vereinfachter Konstruktion einer zukünftigen Realität*“[40].

[35] Vgl. Kurbel (1991), S. 18
[36] Vgl. Angele/Fensel/Studer (1998), S. 187
[37] Vgl. Angele/Fensel/Studer (1998), S. 169
[38] Vgl. Frick (1998), S. 294
[39] Vgl. Pfeifer/Rothenfluh (1994), S. 44
[40] Puppe/Stoyan/Studer (2000), S. 603. Vgl. auch Wedekind et al. (1998), S. 267

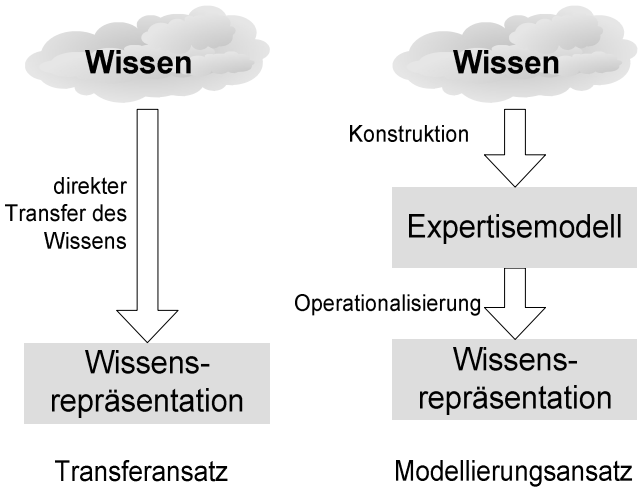


Abbildung 6: Transfer- und Modellierungsansatz

Im Rahmen der Arbeit wird ebenfalls der konstruktivorientierte Modellbegriff verwendet, der im Gegensatz zu dem abbildungsorientierten Modellbegriff nicht versucht, die Realität abzubilden. Die Konstruktion ist somit nicht eine Abbildung bzw. Reproduktion eines „realen Systems", sondern die Wirklichkeit, die über die Erkenntnisleistung eines Subjektes wahrgenommen wird. Dies bedeutet, dass es keine subjektunabhängige erkennbare Realität gibt. Hiermit wird dem abbildungsorientierten Modellbegriff die Grundlage entzogen, die darauf aufbaut, dass die Realität ohne subjektive Wahrnehmungsleistung erkennbar ist.[41]

Somit erfolgt das KE des IS-Sicherheitsmanagements in der Arbeit nicht auf Basis eines Transferprozesses von IS-Sicherheitswissen direkt in die Regel- oder/und Frame-Strukturen, sondern durch die Konstruktion eines Expertisemodells, welches konzeptuell und epistemologisch die IS-Sicherheitsstrategien und das benötigte IS-Sicherheitswissen beschreibt. Aufgabe ist es jedoch nicht, ein kognitives abbildungsorientiertes Modell eines Experten zu erstellen, da dieses wegen der subjektiven Wahrnehmung und wegen der fehlenden Struktur und Stofflichkeit von Computern (noch) nicht möglich ist[42]. Aus diesem Grund werden Modelle „konstruiert", welche angewandt auf eine zukünftige Realität „ähnliche" Resultate erzeugen wie der menschliche Experte[43].

Die Grundlagen der folgenden problemlösungsmethodenorientierten und expertisemodellorientierten Ansätze bilden die von Newell geforderte Trennung der Wissensebene von der symbolischen Verarbeitung[44]. Diese Ansätze ermöglichen eine Beschreibung der Problemlösungsprozesse auf einer hohen abstrahierten Ebene. *„Hiermit verbindet sich der Anspruch, die Wissensinhalte und ihre Funktion für einen Systemzweck ins Zentrum der Modellierungstätigkeit zu stellen und zu abstrahieren von der Form der symbolischen Darstellung des Wissens und den symbolverarbeitenden Prozeduren, die die Funktionalität eines Systems hervorbringt"*[46]. Die Wissensebene beinhaltet somit eine abstrahierte Beschreibung der Domäne

[41] Vgl. Schütte (1998), S. 49
[42] Vgl. Lenz (1991), S. 43
[43] Vgl. Studer/Benjamins/Fensel (1998), S. 163
[44] Vgl. Newell (1982)
[46] Görz/Wachsmuth (2000), S. 8

mittels eines Expertisemodells auf einer epistemologischen Ebene unabhängig von der späteren Operationalisierung auf der Symbolebene.

1.3.1 Problemlösungsmethodenorientierte Ansätze

Mitte der 80er Jahre entstanden die ersten methodischen Ansätze zur modellorientierten Entwicklung von Problemlösungsmethoden. Dabei standen nicht mehr die universellen Problemlösungen im Vordergrund, sondern spezifische Problemlösungsmethoden, die auf bestimmte Problemtypen ausgerichtet waren. Heute existieren umfangreiche Sammlungen von Problemlösungsmethoden, die auf das jeweilige Anwendungsgebiet überführt werden können.

Pioniere der modellorientierten Ansätze waren u.a. Clancy (heuristische Klassifikation[47]), Marcus, McDermott und Puppe (Role-Limiting Methods[48] und Configurable Role-Limiting Methods[49]) und Chandrasekaran (Generic-Task[50] und Task-Structure[51]). Deren Ergebnisse finden sich in modernen Ansätzen des Knowledge Engineerings (z.B. CommonKADS[52] und MIKE[53]) wieder, da sie für die Analyse des Problemlösungswissens von herausragender Bedeutung sind[54]. Gemeinsam ist diesen Ansätzen die Darstellung der wesentlichen Rolle von Problemlösungsmethoden für die Erstellung von WBS[55].

„*Problemlösungsmethoden (problem solving methods) bestimmen, wie Wissen zur Problemlösung verwendet wird.*“[56]. Die Aufgabe der Problemlösungsmethoden besteht in der expliziten Beschreibung von Problemlösungsprozessen auf der Wissensebene. Hierbei werden im Unterschied zum WBS der ersten Generation problemspezifische Methoden verwendet, die nicht nur zur Auswertung von erworbenem Wissen dienen, sondern zusätzlich die Akquisition und Strukturierung des Wissens unterstützen. Der Auswahl und Konstruktion von Problemlösungsmethoden wird somit eine besondere Rolle zugeteilt, da sie sehr eng mit der Wissensakquisition verbunden ist.

Heuristische Klassifikation

Die heuristische Klassifikation kann als erste umfassende Umsetzung der Überführung einer Problemlösungsmethode auf die Wissensebene bezeichnet werden[57]. Clancey hat 1985 durch Untersuchung mehrerer WBS der ersten Generation festgestellt, dass deren unterschiedliches Problemlösungsverhalten sich zu einer heuristischen Klassifikation abstrahieren lässt. Damit war es zum ersten Mal möglich, das Problemlösungsverhalten der heuristischen Klassifikation auf einer Wissensebene, und zwar unabhängig von der jeweiligen Repräsentationsform (z.B. Prädikatenlogik, Produktionsregeln oder Frames), zu beschreiben.

---

[47] Vgl. Clancy (1985)
[48] Vgl. Marcus (1988) und Puppe (1990)
[49] Vgl. Poeck/Gappa (1993) und Puppe et al. (1996)
[50] Vgl. Chandrasekaran (1986)
[51] Vgl. Chandrasekaran/Johnson/Smith (1992)
[52] KADS = Knowledge Acquisition and Documentation Structuring. KADS wurde z.T. später auch als Akronym für „Knowledge Analysis and Design Support“ verwendet.
[53] MIKE = Model-based and Incremental Knowledge Engineering
[54] CommonKADS und MIKE werden in Kapitel 1.3.2 erläutert.
[55] Vgl. Fensel (2000), S. 7
[56] Puppe/Stoyan/Studer (2000), S. 617
[57] Vgl. Chandrasekaran/Johnson/Smith (1992), S. 126

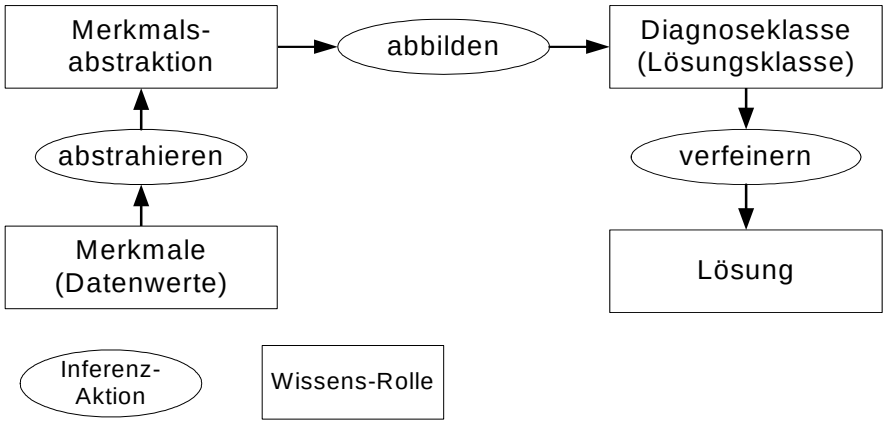


Abbildung 7: Konzept der heuristischen Klassifikation[58]

Am Beispiel der heuristischen Klassifikation sollen die wesentlichen Eigenschaften einer Problemlösungsmethode charakterisiert werden[59]:

- Es werden die benötigten Inferenz-Aktionen und deren Abarbeitungsstruktur festgelegt.
- Die Wissens-Rollen determinieren die „Rolle“, die das jeweilige Domänenwissen für die Inferenz-Aktionen spielt. Durch die Wissens-Rollen können domänenunabhängige generische Konzepte generiert werden.

Die Problemlösungsmethode beschreibt Inferenzen (z.B. abstrahieren, abbilden und verfeinern) und Wissens-Rollen (z.B. Merkmale, abstrahierte Merkmale, Lösungsklassen und Lösungen) unabhängig von der jeweiligen Domäne, wodurch die Problemlösungsmethode auf verschiedene Problembereiche, wie z.B. die Medizin oder das IS-Sicherheitsmanagement, anwendbar ist.

Role-Limiting und Generic-Task Ansatz

Ab Mitte der 80er Jahre wurden der Role-Limiting und Generic-Task Ansatz auf den Erkenntnissen von Clancey entwickelt. Die Problemlösungsmethoden dieser Ansätze basieren auf den vorgegebenen Inferenz-Strukturen, definieren aber zusätzlich die Repräsentationsform der Wissens-Rollen. Somit werden die Struktur der Inferenzen und die Repräsentationsform des Domänenwissens festgelegt (Strong Interaction Problem Hypothesis)[60].

Die Eingabe des anwendungsspezifischen Domänenwissens erfolgt dadurch, dass Wissens-Rollen mit entsprechenden Konzepten der Domäne gefüllt werden. Somit steuern die Problemlösungsmethoden den Prozess der Wissensakquisition, indem festlegt wird, welche Wissensart benötigt und in welcher Form das Wissen repräsentiert wird. Die Anwendung besteht im günstigen Fall darin, eine adäquate Problemlösungsmethode auszuwählen und das anwendungsspezifische Domänenwissen einzugeben. Diese „Werkzeugkästen“ enthalten eine Sammlung von ausführbaren Problemlösungsmethoden, die über vorgefertigte Wissensrepräsentationsformen verfügen[61].

[58] Vgl. Clancey (1985), S. 296; Puppe (1990), S. 21 und Hoppe (1992), S. 78
[59] Vgl. Studer/Benjamins/Fensel (1998), S. 164
[60] Vgl. Bylander/Chandrasekaran (1988), S. 66; Frick (1998), S. 296 und Fensel (2000), S. 22
[61] Vgl. Hoppe (1992), S. 89

Dies vereinfacht zwar die Wissensakquisition; die Wiederverwendung des repräsentierten Domänenwissens wird jedoch für andere Problemlösungsmethoden vermindert. Des Weiteren beschreiben die Problemlösungsmethoden häufig nur grob den „realen“ Problemlösungsprozess der Domäne, da die Anpassung der Problemlösungsmethoden an die Domäne nur in einem begrenzten Rahmen möglich ist. Zudem ist häufig eine Kombination von verschiedenen Problemlösungsmethoden nötig, wobei die feste Struktur der Problemlösungsmethoden, insbesondere bei dem Role-Limiting Ansatz, eine freie Kombination verhindert[62].

Konfigurierbare Aufgaben-Problemlösungsmethoden Ansätze
Aus den oben aufgeführten Nachteilen wurden die Ansätze weiterentwickelt. Die Grundlage der folgenden Ansätze ist die Trennung zwischen

- Aufgabenklassen bzw. Problemklassen, welche den Problemtyp beschreiben und
- (unterschiedliche) Methoden, die Problemlösungen für die jeweilige Aufgabenklassen bereitstellen.

Es existiert eine Vielzahl von unterschiedlichen Aufgabenklassen mit z.T. jeweils unterschiedlichen Inhalten. Im Rahmen der Arbeit soll sich an die folgende Differenzierung von Puppe und Schreiber gehalten werden[63]:

- Diagnose[64] bzw. Analytic Task.
  Generische Strategie: Die Lösung wird aus einer Menge vorgegebener Alternativen ausgewählt.
- Konstruktion bzw. Synthetic Task.
  Generische Strategie: Die Lösung wird aus Bausteinen zusammengesetzt.

Prinzipiell gehen diagnostische bzw. analytische Aufgabenklassen von einem bestehenden System (z.B. Informationssysteme, Unternehmensorganisation oder IS-Sicherheitskonzept) aus. Die Diagnoseaufgabe hat als Eingang das bestehende System und produziert als Ergebnis bestimmte Eigenschaften des Systems (Analyse). Bei konstruktiven bzw. synthetischen Aufgabenklassen existiert noch kein System, da die Aufgabe die Konstruktion eines Systems beinhaltet (Synthese). Der Eingang besteht i.d.R. aus Anforderungen und Restriktionen für das zu konstruierende System[65].

Konstruktive Probleme bzw. Aufgaben sind im Allgemeinen schwerer zu lösen als diagnostische Probleme, da der Lösungsraum bei der Konstruktion wesentlich größer ist. Auch ist die Aufgabenklasse Konstruktion mit ihren eigenständigen Teilbereichen - wie z.B. Planung, Konfiguration oder Scheduling - erheblich heterogener als die Diagnoseaufgabe. Eine eindeutige Differenzierung zwischen Diagnose und Konstruktion lässt sich nicht immer durchführen. Wenn z.B. bei der Diagnostik mehrere Lösungen ausgewählt werden und diese voneinander

[62] Vgl. Studer/Benjamins/Fensel (1998), S. 167
[63] Vgl. Puppe et al. (1996), S. 1 und Schreiber et al. (2000), S. 125
[64] Bei Puppe wird keine Differenzierung zwischen Klassifikation und Diagnose durchgeführt. Vgl. dazu Puppe et al. (1996), S. 1
[65] Vgl. Schreiber et al. (2000), S. 124

ander abhängig sind, müssen diese Teillösungen eventuell zu einer Gesamtlösung „konstruiert“ werden. Umgekehrt lassen sich manche Planungs- und Konfigurationsprobleme als eine Hintereinanderschaltung von mehreren Auswahlproblemen interpretieren[66].

Task-Structure Ansatz

Der Task-Structure Ansatz stellt eine Weiterentwicklung des Generic-Task Ansatzes dar, indem einer Aufgabenklasse mehrere alternative Problemlösungsmethoden zugeordnet werden, die wiederum in mehrere Teilaufgaben zerlegt werden können. Eine Aufgabe, wie z.B. die Diagnoseaufgabe, wird durch deren Eigenschaften und Ziele beschrieben. So kann eine IS-Sicherheitsdiagnoseaufgabe als Eingangsmerkmale beobachtete Fehlfunktionen eines IS-Sicherheitssystems haben. Das Ziel der Aufgabe ist, die Ursachen für diese Fehlfunktionen zu ermitteln. Der Diagnoseaufgabe sind verschiedene Methoden, wie z.B. abstrahieren, selektieren oder verfeinern, zugeordnet, um die Aufgabe zu bewältigen[67]. Diese Aufgaben und Methoden-Strukturen werden in Form von Hierarchien dargestellt, wodurch eine Problemlösungsmethoden-Bibliothek entsteht. Hierbei wird eine möglichst hohe Unabhängigkeit der Problemlösungsmethode von einer konkreten Domäne gefordert[68]. Ein Beispiel für den Task-Structure Ansatz bietet die Strukturierung der „Diagnose“ in Teilaufgaben und Methoden nach Benjamins (1993).

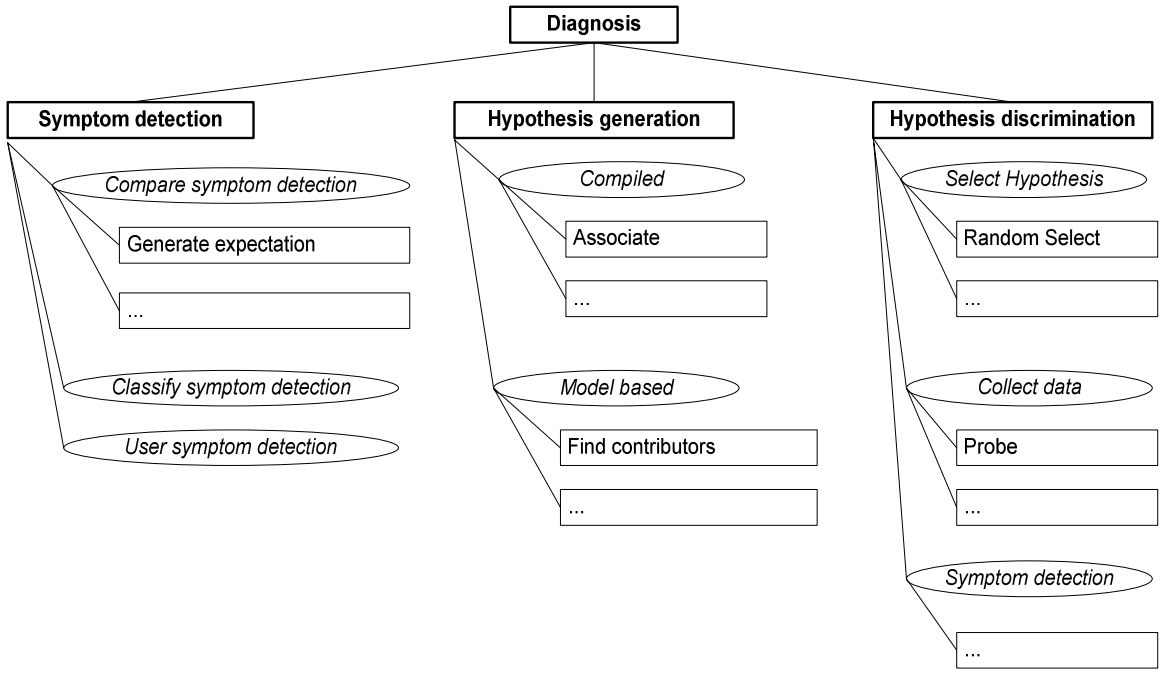


Abbildung 8: Grundkonzept für eine strukturierte Darstellung der Problemlösungsmethoden der Diagnose nach dem Task-Structure Ansatz[69]

[66] Vgl. Puppe et al. (1996), S. 1
[67] Vgl. Chandrasekaran/Johnson/Smith (1992), S. 128
[68] Vgl. Fensel (2000), S. 23
[69] Verkürzte Zusammenfassung der Abbildung in Benjamins (1995), S. 97-98 und S. 101. Vgl. auch Fensel (2000), S. 34

Die Teilaufgaben bzw. Basis-Inferenzen[70]

- Merkmalserkennung
- Hypothesengenerierung
- Hypothesenüberprüfung

werden im Rahmen des IS-Sicherheitsexpertisemodells erläutert.

Configurable Role-Limiting Methods Ansatz

Der Configurable Role-Limiting Methods Ansatz basiert ebenfalls auf der Zerlegung der Problemlösung einer Aufgabenklasse in Teilaufgaben und Methoden. Der Ansatz beinhaltet zudem „gemeinsame" Methoden wie Datenauswahl, Datenerfassung und Datenabstraktion, die für alle Problemlösungsmethoden von Relevanz sind. Das verwendete gemeinschaftliche bzw. „kollektive" Wissen der unterschiedlichen Diagnosemethoden bezeichnet Puppe als diagnostisches Basiswissen[71].

Zusätzlich existieren spezifische Problemlösungsmethoden für die Hypothesengenerierung und -überprüfung (heuristische oder überdeckende Bewertung), die auf spezifischem diagnostischem Problemlösungswissen (z.B. auf sicherem, heuristischem oder kausalem Wissen) basieren. Somit besitzen die spezifischen Diagnosemethoden Annahmen bzw. Voraussetzungen bzgl. der zugrunde liegenden Wissenstypen oder die Methode wird durch das bezeichnende Problemlösungswissen charakterisiert.

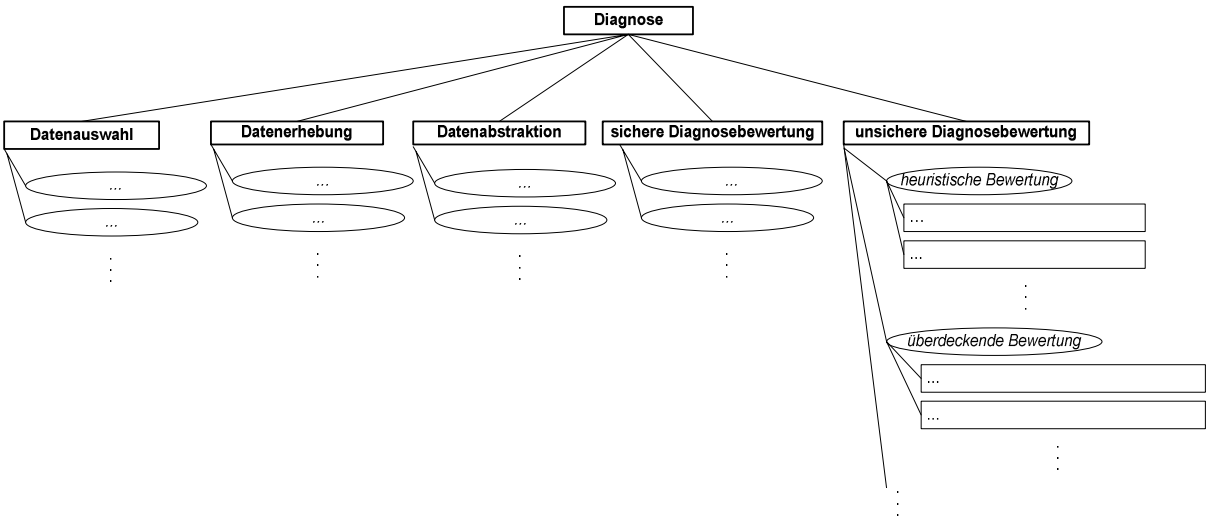


Abbildung 9: Grundkonzept für eine strukturierte Darstellung der Problemlösungsmethoden der Diagnose nach dem Configurable Role-Limiting Methods Ansatz[72]

Die Unflexibilität bei den „reinen" Role-Limiting Methoden wird vermieden, da die Problemlösungsmethoden konfigurierbar sind. Weiterhin besteht eine gesteuerte Wissensakquisition, da die Methoden Annahmen über die Wissensstruktur und den Wissenstyp der Domäne spezifizieren. Die Wissens-Rollen repräsentieren einen festen Wissenstyp, die in den Methoden unterschiedliche „Rollen spielen". *„Für die verschiedenen Teilaufgaben der Problemlösungsmethoden liegen vorgefertigte Modellvarianten vor, aus denen bei der Spezifikation der aktuellen Problemlösungsmethode ausgewählt werden kann. Durch Zusammenstellung dieser*

[70] Teilaufgaben werden im weiteren Verlauf der Arbeit auch als „Basis-Inferenzen" bezeichnet.
[71] Vgl. Puppe (1996), S. 78
[72] Vgl. Puppe (1998), S. 639

Einzelprozeduren entsteht die konfigurierte Lösung des Gesamtverfahrens."[73] Hierdurch ist es möglich, konfigurierbare Werkzeuge zu erstellen, denn durch diesen Ansatz kann eine konfigurierte Problemlösungsmethode durch Kopplung von unterschiedlichen Methoden (Modellvarianten) und Wissens-Rollen abgebildet werden. Die Problemlösungsmethode wird zusammengesetzt, indem eine passende Methode ausgewählt und konfiguriert wird, der Wissens-Rollen zugeordnet sind. Diese Wissens-Rollen können die Domänenkonzepte aufnehmen bzw. Domänenwissen in Problemlösungsmethoden überführen.

1.3.2 Expertisemodellorientierte Ansätze

Zentraler Bestandteil des heutigen KE ist das Expertisemodell, das Wissen explizit auf der höheren Wissensebene beschreibt. Während bei den Transferansätzen die Wissensakquisition „implizit" durch den Transfer des Wissens in einem WBS durchgeführt wird, wird bei den modellorientierten Ansätzen zunächst ein Expertisemodell als Ergebnis der Wissensakquisition konstruiert, das explizit das Problemlösungswissen und das Domänenwissen beschreibt und eine Schnittstelle zur Wissensoperationalisierung darstellt[74].

CommonKADS

KADS beschreibt eine Methodologie zur Erstellung von WBS, die auf Forschungsarbeiten von Wielinga und Breuker der Universität Amsterdam basiert und eine breite Akzeptanz insbesondere im europäischen Raum erlangt hat[75]. Auf Basis des KADS-I Ansatzes wurde 1990 das Folgeprojekt KADS-II[76] ins Leben gerufen. Das KADS-Projekt endete 1994, dessen Ergebnis im kommerziellen Standard CommonKADS dargestellt ist. Der CommonKADS Ansatz wird ständig weiterentwickelt; die Ergebnisse wurden von Schreiber zusammenfassend veröffentlicht[77].

Das Grundverständnis des KADS Ansatzes basiert auf Abstraktions- und Modellierungsprozessen von der Wissensakquisition bis zur Implementierung des WBS[78]. Der KADS Ansatz erweiterte die oben genannten Ansätze durch ein umfangreiches Expertisemodell, wobei die differenzierte Darstellung der Aufgabenklassen und der Problemlösungsmethoden in den KADS Ansatz einfließt[79].

Der CommonKADS-Ansatz erweitert den KADS-Ansatz durch eine Anbindung an das Knowledge Management und mittels der einheitlichen Modellierung auf Basis der objektorientierten UML-Notation. Der CommonKADS Ansatz besitzt aber nicht den Anspruch einer vollständigen Knowledge Management Methodologie, sondern der Ansatz sieht sich als ein wichtiges Werkzeug für die Umsetzung des Knowledge Managements[80].

[73] Puppe/Stoyan/Studer (2000), S. 625
[74] Vgl. Frick (1998), S 295 und Studer/Benjamins/Fensel (1998), S. 168
[75] Vgl. Heller (1996), S. 75
[76] Projektbezeichnung: ESPRIT-Projekt P5248
[77] Vgl. Schreiber et al. (2000). Informationen über CommonKADS auch im Internet: URL: http://www.commonKADS.uva.nl (Stand: September 2002)
[78] Vgl. Hoppe (1992), S. 60
[79] Vgl. Frick (1998), S. 317
[80] Vgl. Schreiber et al. (2000), S. 82

Den entscheidenden Beitrag des CommonKADS bilden drei Ebenen des Expertisemodells, die auch in anderen KE-Ansätzen zu finden sind[81].

- Die Aufgaben- bzw. Kontrollebene spezifiziert die zu lösende Aufgabe und deren Teilaufgaben. Es ist notwendig, neben den Inferenz-Schritten die Problemlösungsmethoden durch Kontrollstrukturen zu ergänzen. Die Kontrollstrukturen werden bis auf die Inferenzebene verfeinert.
- Die Inferenzebene beschreibt den Lösungsprozess mit Hilfe von Inferenzen und Wissens-Rollen. Die Abhängigkeiten zwischen Inferenzen und Wissens-Rollen werden durch eine Inferenz-Struktur abgebildet. Wissens-Strukturen können unterschiedliche Domänen-Konzepte (z.B. aus der IS-Sicherheit oder Medizin) annehmen.
- Auf der Domänenebene wird das domänenspezifische Wissen beschrieben, das zur Problemlösung benötigt wird. Dabei werden Konzepte der Domäne modelliert, wie z.B. Schwachstellen oder Maßnahmen der IS-Sicherheit, die auf Wissens-Rollen von Problemlösungsmethoden überführt werden.

In dem folgendem Beispiel wurde die Problemlösungsmethode „heuristische Klassifikation“ auf das Problem der Schwachstellen-Diagnose angewendet.

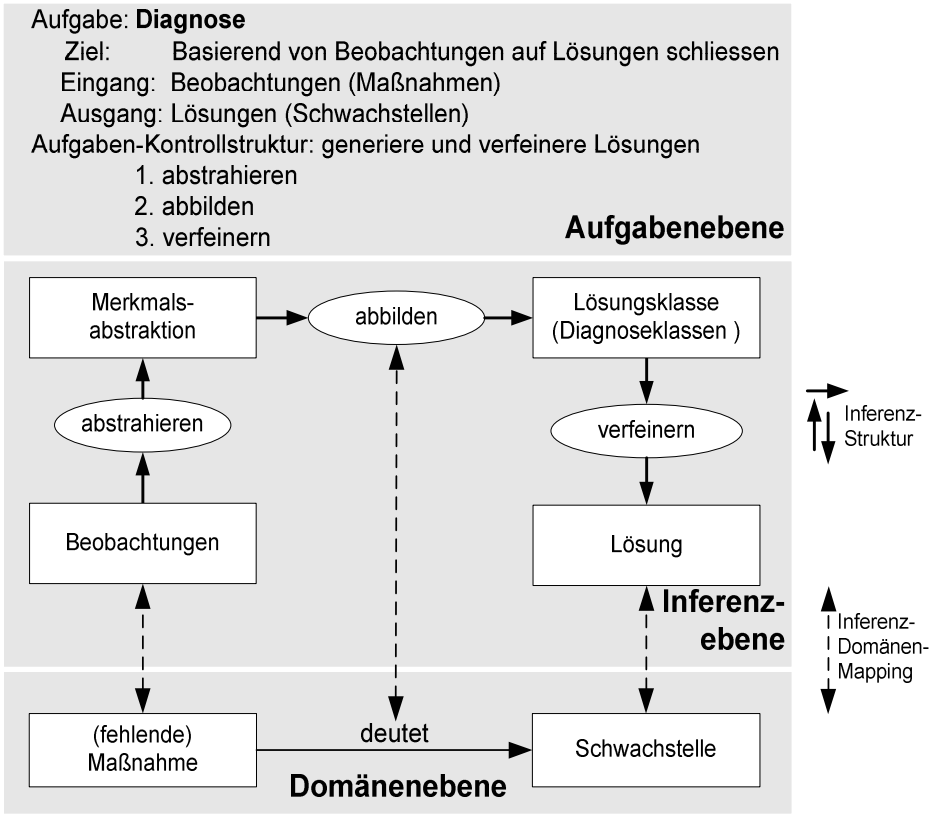


Abbildung 10: Beispiel eines Expertisemodells für die Schwachstellen-Diagnose auf Basis der Problemlösungsmethode „heuristische Klassifikation“[82]

[81] Vgl. Studer/Benjamins/Fensel (1998), S. 169-170
[82] Erweitert in Anlehnung an Studer/Benjamins/Fensel (1998), S. 169 und Schreiber et al. (2000), S. 107

Durch die Problemklasse Diagnose werden Schwachstellen auf Basis von erhobenen (fehlenden) Maßnahmen ermittelt. Dafür werden die Konzepte „Maßnahme“ und „Schwachstelle“ auf die Wissens-Rollen und Inferenz-Struktur der „heuristischen Klassifikation“ überführt (Inferenz-Domänen-Mapping).

Der CommonKADS Ansatz ermöglicht eine weitgehende Unabhängigkeit zwischen der Domäne und der Problemlösungsmethode. Diese Sichtweise der Unabhängigkeit der Domäne von der Problemlösungsmethode und umgekehrt steht im Widerspruch zur „Strong Interaction Problem Hypothesis“ der Configurable Role-Limiting Methods orientierten Ansätze, denn die Role-Limiting Ansätze nehmen eine Abhängigkeit zwischen der Struktur der Domäne und der Problemlösungsmethode an[83]. Die von CommonKADS geforderte Unabhängig zwischen den Ebenen wird durch die „Relative Interaction Hypothesis“ relativiert, die davon ausgeht, dass z.T. gewisse Abhängigkeiten bzw. gegenseitige Anforderungen zwischen der Struktur des Domänenwissens und dem Aufgabentyp bestehen[84]. So stellen Problemlösungsmethoden Anforderungen an die Domäne, die nicht so einschränkend sind wie bei den „Strong Interaction Problem Hypothesis“ Ansätzen.

MIKE

Der MIKE-Ansatz[85] wurde um die Forschungsgruppe von Studer an der Universität Karlsruhe entwickelt, um die Phasen der WBS-Entwicklung von der Wissenserhebung über die Expertisemodellierung bis hin zur Implementierung des WBS zu unterstützen. Das Vorgehensmodell besteht aus Aktivitäten und deren Ergebnissen, die auch als Dokumente bezeichnet werden. Die Zielsetzung von MIKE ist, die Distanz zwischen dem menschlichen Wissen und dessen Repräsentation in einem WBS zu überwinden[86].

Der Wissensakquisitionsprozess beginnt mit der Erhebung des Anwendungswissens und dessen Problemlösungsprozesse (z.B. IS-Sicherheitswissen und -strategien). Die Ergebnisse der Erhebungen (z.B. durch Interviews und Beobachtungen) werden in natürlich-sprachlicher Form in einem Wissensprotokoll abgelegt. Durch die Interpretation des Wissensprotokolls werden die relevanten Strukturen, z.B. Datenabhängigkeiten einzelner Problemlösungsschritte, in einer informellen Beschreibungssprache dargestellt. Damit wird eine Kommunikation zwischen Fachexperten und dem Knowledge Engineer ermöglicht.

Die informelle Beschreibung stellt die Grundlage für das KARL-Modell dar. Diese informelle Beschreibung ähnelt dem Expertisemodell der CommonKADS[87]. In dem KARL-Modell erfolgt eine konzeptuelle Formalisierung und Operationalisierung des Strukturmodells. Die Struktur bleibt erhalten, die Komponenten aber werden mit einer formalen Sprache (KARL-Sprache) beschrieben. Durch das KARL-Modell werden auch die funktionalen Anforderungen abgedeckt, wobei nicht-funktionale Anforderungen wie Portabilität, Effizienz oder Wartbarkeit zusätzlich durch das Entwurfsmodell beschrieben werden. Das Entwurfsmodell wird anschließend in ein lauffähiges System implementiert. Durch die frühe Operationalisierung der MIKE-Modelle sind im Gegensatz zu dem CommonKADS Ansatz unterschiedliche Stadien von Prototypen möglich, da jede Phase einer Verfeinerung der vorhergehenden Phase entspricht.

[83] Vgl. Puppe et al. (1996), S. 66
[84] Vgl. Studer/Benjamins/Fensel (1998), S. 170
[85] MIKE = Model-based and Incremental Knowledge Engineering
[86] Vgl. Angele/Fensel/Studer (1998), S. 180 ff.
[87] Vgl. Studer/Benjamins/Fensel (1998), S. 171

1.4 Vorgehensmodell der Arbeit

Das Vorgehensmodell der Arbeit basiert auf den wesentlichen Aspekten der vorhergehenden Kapitel.

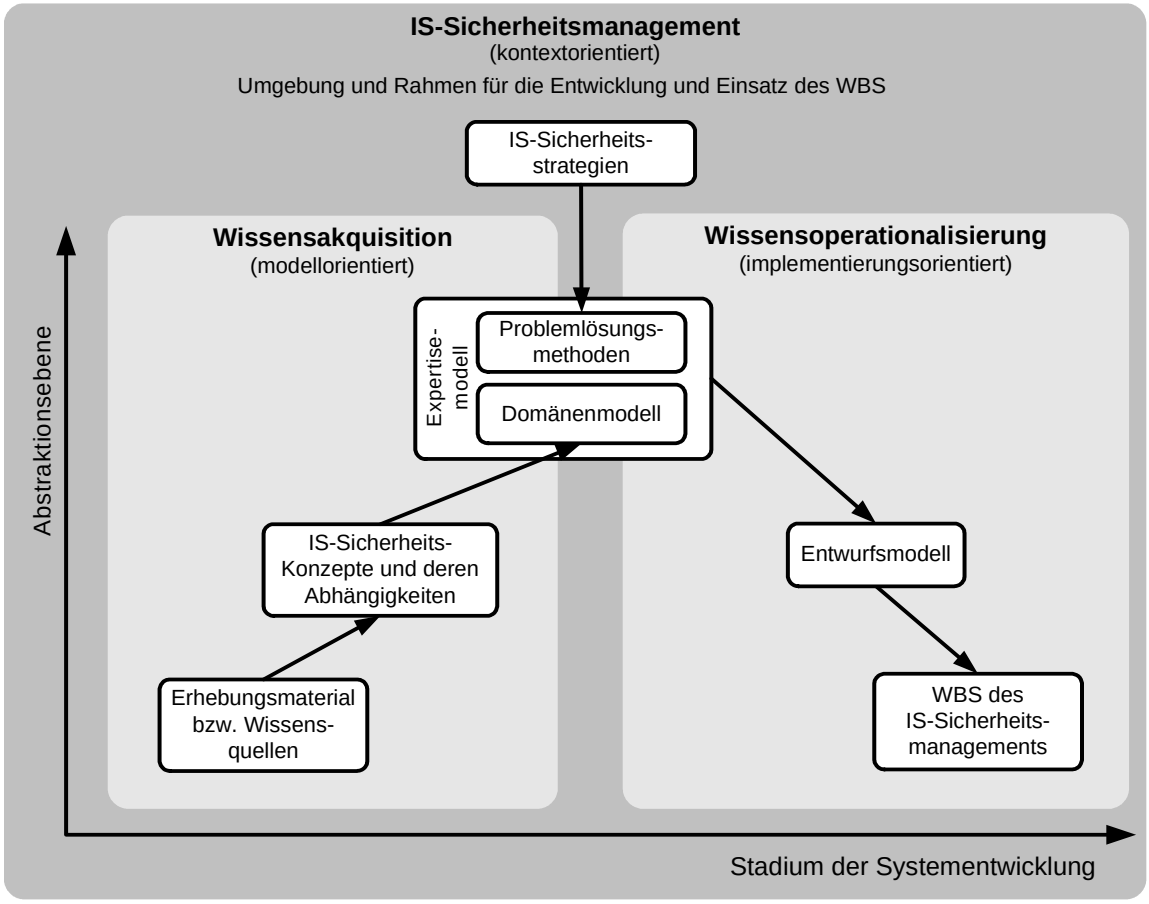


Abbildung 11: Entwicklungsrahmen des Knowledge Engineerings für das IS-Sicherheitsmanagement[88]

Zentrale Aufgabe des Knowledge Engineerings in der Arbeit ist es, die Lösungsprozesse des IS-Sicherheitsmanagements und das IS-Sicherheitswissen in einem Expertisemodell explizit abzubilden und dieses in ein WBS zu operationalisieren. Hierbei sind folgende Bereiche von Relevanz:

- IS-Sicherheitsmanagement bildet den Kontext des Knowledge Engineerings,
- Expertisemodell ist das Ergebnis der Wissensakquisition und
- Wissensoperationalisierung erfolgt durch ein Entwurfsmodell und dessen Implementierung durch ein WBS.

[88] Erweitert und angewandt auf das Knowledge Engineering des IS-Sicherheitsmanagements in Anlehnung an Lenz (1991), S. 112

IS-Sicherheitsmanagement

Für eine erfolgreiche Einbettung des WBS in das IS-Sicherheitsmanagement muss zuerst der Kontext verstanden werden. Wird der Kontext bei der Konstruktion des Expertisemodells nicht berücksichtigt, erfolgt eine ungenügende „Einbettung" des WBS in die Organisation der Institution[89]. Dafür ist es nötig, dass das WBS die unterschiedlichen Strategien des IS-Sicherheitsmanagements unterstützt und „versteht", um eine partielle oder vollständige Automatisierung wissensintensiver Aufgaben zu unterstützen. Die Problemlösungsprozesse des IS-Sicherheitsmanagements werden auf der Kontextebene durch ein „deskriptives" Modell der IS-Sicherheitsstrategien beschrieben, welches zudem auch die Grundlage für die Problemlösungsmethoden des Expertisemodells auf der Wissensebene darstellt.

Wissensakquisition

Die Analyse und Interpretation im Rahmen der Wissensakquisition ist eine Form der Wissensgewinnung durch das Zerlegen und Aufgliedern des IS-Sicherheitsmanagements in seine Komponenten. Es folgt eine Untersuchung der Eigenschaften und der Zusammenhänge dieser einzelnen Komponenten. Das Expertisemodell befindet sich dabei auf einem hohen abstrakten Niveau, welches der Wissensebene entspricht.

Basis für die Domänenebene ist die Identifizierung von IS-Sicherheitswissensquellen und deren Erhebung, wobei als Ergebnis der Erhebung insbesondere terminologische und inhaltliche Aspekte der IS-Sicherheit differenziert dargestellt werden. Das Ergebnis beinhaltet die Konzeptstrukturen des IS-Sicherheitswissens und deren Abhängigkeiten in einem Domänenmodell.

Ausgangspunkt für das Problemlösungswissen sind Strategien des IS-Sicherheitsmanagements, welche den Rahmen für die Entwicklung und den Einsatz des WBS geben. Ziel ist es, die strukturierenden Eigenschaften und Problemlösungsvorgänge der IS-Sicherheitsstrategien aufzudecken, um die Problemlösungsprozesse des IS-Sicherheitsmanagements durch adäquate Problemlösungsmethoden zu beschreiben. Die Problemlösungsmethoden benötigen für die Problemlösung ein Domänenmodell des IS-Sicherheitswissens. Hierfür werden Wissens-Rollen verwendet, die eine Überführung des Domänenmodells in die Problemlösungsmethoden erlauben.

Ergebnis ist ein Expertisemodell des IS-Sicherheitsmanagements, welches aus einem Domänenmodell und Problemlösungsmethoden besteht und weitgehend unabhängig von einer Operationalisierung auf einer abstrakten Wissensebene beschrieben wird[90]. Das Expertisemodell soll zudem als zusätzliche Schicht die konzeptionelle Distanz bzw. Lücke zwischen Akquisition auf der Wissensebene und Operationalisierung auf der Symbolebene verringern[91].

[89] Vgl. Schreiber et al. (2000), S. 26
[90] Vgl. Kingston (1998), S. 311
[91] Vgl. Lenz (1991), S. 114

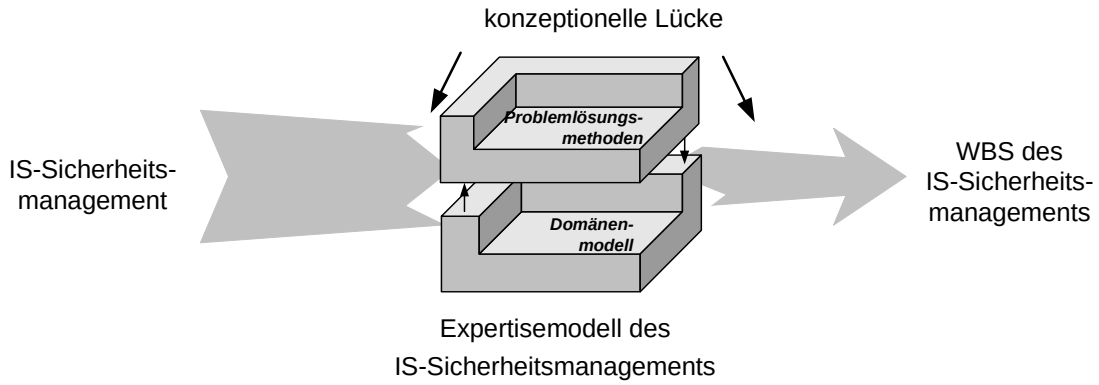


Abbildung 12: Konzeptionelle Lücke

Wissensoperationalisierung
Unter der Wissensebene ist die Symbolebene angesiedelt, die die Wissensoperationalisierung umfasst. Die Wissensoperationalisierung ist durch die Entwicklungsschritte eines Entwurfsmodells hin zu einem operativen System gekennzeichnet. Das Entwurfsmodell formalisiert die Repräsentationsformen und Problemlösungsmethoden für die folgende Implementierung. Dazu zählen Entwurfsentscheidungen sowie die Auswahl geeigneter Repräsentationsformen. Als Ergebnis entsteht ein operatives Entwurfsmodell, das im Gegensatz zum Expertisemodell implementierungsorientiert ist. Das Entwurfsmodell wird zusätzlich als Dokumentationsbasis zur Wartung und Pflege des WBS eingesetzt.

Auf Basis des Entwurfsmodells wird das WBS konstruiert. Das WBS kann als Werkzeugkasten bzw. Shell bezeichnet werden, der das IS-Sicherheitsmanagement unterstützt und hierfür Repräsentationsformalismen und spezifische Problemlösungsmethoden anbietet. In einem WBS kann eventuell die Wissensbasis ein gewisses Basiswissen enthalten, das angepasst und erweitert wird. Wenn ein WBS die wesentlichen Aspekte des IS-Sicherheitsmanagements beinhaltet, kann das WBS in die jeweilige Institution eingebettet werden.

Fachexperte und Knowledge Engineer
Im Rahmen des KE vertreten der Fachexperte und der Knowledge Engineer unterschiedliche Rollen. Da Fachexperten typischerweise keinen Überblick über Expertisemodelle, Problemlösungsmethoden und Entwicklungswerkzeuge haben, benötigen sie für die Konstruktion eines fachspezifischen Expertisemodells und für die Auswahl der Entwicklungswerkzeuge Unterstützung eines Knowledge Engineers. Nach der Überführung des Expertisemodells in ein maßgeschneidertes WBS ist es bei ausreichender Fähigkeit zur Selbstreflektion des Fachexperten durchaus möglich, dass Fachexperten das IS-Sicherheitswissen direkt eingeben und vor allem auch pflegen können[92]. Hierdurch wird die Gefahr verhindert, bei der Erstellung und Wartung der Wissensbasis von einem Knowledge Engineer abhängig zu sein. Dies hat Auswirkungen auf die Auswahl der Wissensrepräsentationsform des WBS, da der Fachexperte das IS-Sicherheitswissen direkt eingeben soll.

Zusammenfassend sollen bei der Arbeit die Sicht und die Anforderungen des Fachexperten für die Operationalisierung entscheidend sein und nicht die des Knowledge Engineers. Somit wird die Gefahr verringert, dass ein WBS auf Basis des Transferansatzes erstellt wird.

[92] Vgl. Puppe/Stoyan/Studer (2000), S. 616

2 Informationssystemsicherheits-Management

Die Durchdringung der Informationsverarbeitung in Institutionen und die daraus erwachsene Abhängigkeit von der IS-Sicherheit ist in den letzten Jahren angewachsen. Dadurch hat die Schaffung von IS-Sicherheit (kurz IS-Sicherheitsmanagement) sich in Institutionen zu einer Managementaufgabe entwickelt, welche klassische Aufgabenbereiche beinhaltet, wie z.B. Planung, Organisation, Entscheidung, Kontrolle, Kommunikation usw. In diesem Kapitel erfolgt zuerst eine begriffliche und inhaltliche Abgrenzung des Begriffs „Informationssystemsicherheit“ (kurz IS-Sicherheit), welcher das zentrale Tätigkeitsumfeld des IS-Sicherheitsmanagements beinhaltet.

Nutzenniveau von Information

Im Rahmen dieser Arbeit wird die Informationssicherheit wie folgt in unterschiedliche Ebenen differenziert.

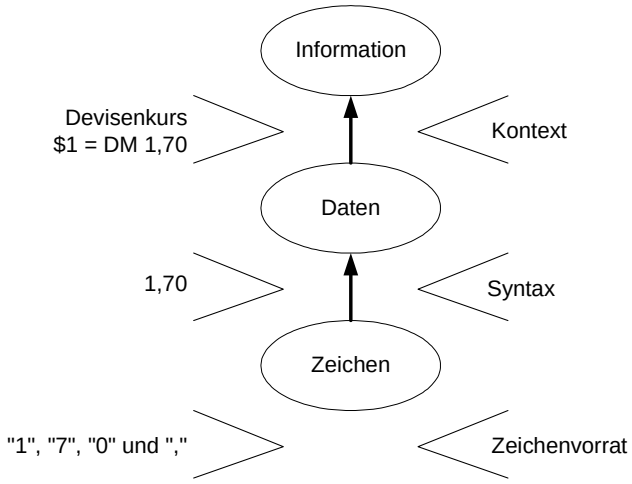


Abbildung 13: Abgrenzung von Information, Daten und Zeichen[93]

Auf der untersten Ebene sind die Grundelemente zur Informationsdarstellung in Form von Zeichen vorhanden. Durch Anwendung von festgelegten Regeln werden die Zeichen zu Daten konvertiert und erlangen eine Struktur (Syntax), besitzen aber keinen Bezug zu einem Kontext. Erst in einem bestimmten Kontext (Devisenkurs) erlangt die Zahl eine konkrete Bedeutung (Semantik). Für das Unternehmen und ebenfalls für die Konkurrenz entstehen aus den Daten Informationen, wenn ein Verwendungsnutzen zu erkennen ist; die „Sicherheit der Information“ erlangt an Bedeutung. Eine Information kann somit in einem unterschiedlichen Kontext individuell eine andere „Sicherheitsbedeutung“ erlangen.

Die Sicherheit von Informationen ist verbunden mit der Verwendungswirkung für den Benutzer. Wenn einerseits für eine Person die Information bekannt ist, jedoch diese keine Verwendung findet, dann ist die Information für diese Person nutzlos. Anderseits kann sie zum Wissenszuwachs (z.B. Lernen) oder als Entscheidungsgrundlage „verwendet“ werden. Dieses „kontextorientierte Nutzenniveau von Information“ hat als Bewertungsmaßstab für das „Si-

[93] Vgl. Krcmar (2000), S. 11

cherheitsniveau“ der Information eine entscheidende Bedeutung. Auf Basis dieser Sicht rückt das Sicherheitsbedürfnis für Informationen durch den Grad des Verwendungszwecks bzw. durch den Wirkungsgrad des Benutzers in den Vordergrund. So sind Informationen für einen Dieb nutzlose Daten, solange er nicht deren Bedeutung bzw. Wert erkennt und somit keine Verwendung für die Daten hat. Oder verliert ein Unternehmen Daten, für die es keine Verwendung gibt oder deren Bedeutung unbekannt ist, wird dieser Verlust als nicht besonders gravierend eingestuft oder gar nicht bemerkt (z.B. der häufig anzutreffende Datenfriedhof).

Daten- und Informationssystemsicherheit

Informationssysteme (IS) sind sozio-technische Systeme[94] mit menschlichen und technischen Komponenten (Mensch-Maschine-Beziehung), die als Ziel ein definiertes Informationsangebot bzw. eine definierte Informationsnachfrage decken sollen[95]. Sämtliche erforderliche Personen sowie eine Aufbau- und Ablauforganisation und technische Komponenten (Hard- und Software) bilden die Informationsinfrastruktur.

Die Sicherheit im Kontext der Begriffe „Information“ und „Informationssysteme“ wird in der Literatur mit facettenreichen Begriffsausprägungen beschrieben,. So werden die Begriffe Datenschutz, Datensicherheit, Informationssicherheit, Computersicherheit, Kommunikationssicherheit, Sicherheit der Informationsverarbeitung, Informationssicherung usw. im Kontext der sicheren Verarbeitung von computergestützten Informationssystemen verwendet[96]. Die Begriffsausprägungen werden häufig synonym verwendet, obwohl sie unterschiedliche Aspekte der Sicherheit im Kontext der Informationssysteme und -verarbeitung widerspiegeln[97].

In der folgenden Abbildung erfolgt die Abgrenzung der Sicherheitsbegriffe auf der Grundlage der Differenzierung zwischen Daten und Informationen[98]. Es wird deutlich, dass Aspekte der Teilmenge einen Bereich der Obermenge darstellen.

[94] „*Ein System ist eine geordnete Ganzheit von zueinander in Beziehung stehenden Elementen*.“ Stickel/Groffmann/Rau (1998), S. 696
[95] Vgl. Stickel/Groffmann/Rau (1998), S. 336
[96] Vgl. Pohl (1995), S. 105; Adam (1995), S. 31; Skoudis (1999) S. 453; Hare (1999b), S. 577; Röhm (2000), S. 18; BDSG (2001); Hepp (2001), S. 148 und Eckert (2001), S. 3
[97] Vgl. Kersten (1995), S. 12 und Horster/Kraaibeek (2000), S. 4
[98] Vgl. Abbildung 13: Abgrenzung von Information, Daten und Zeichen

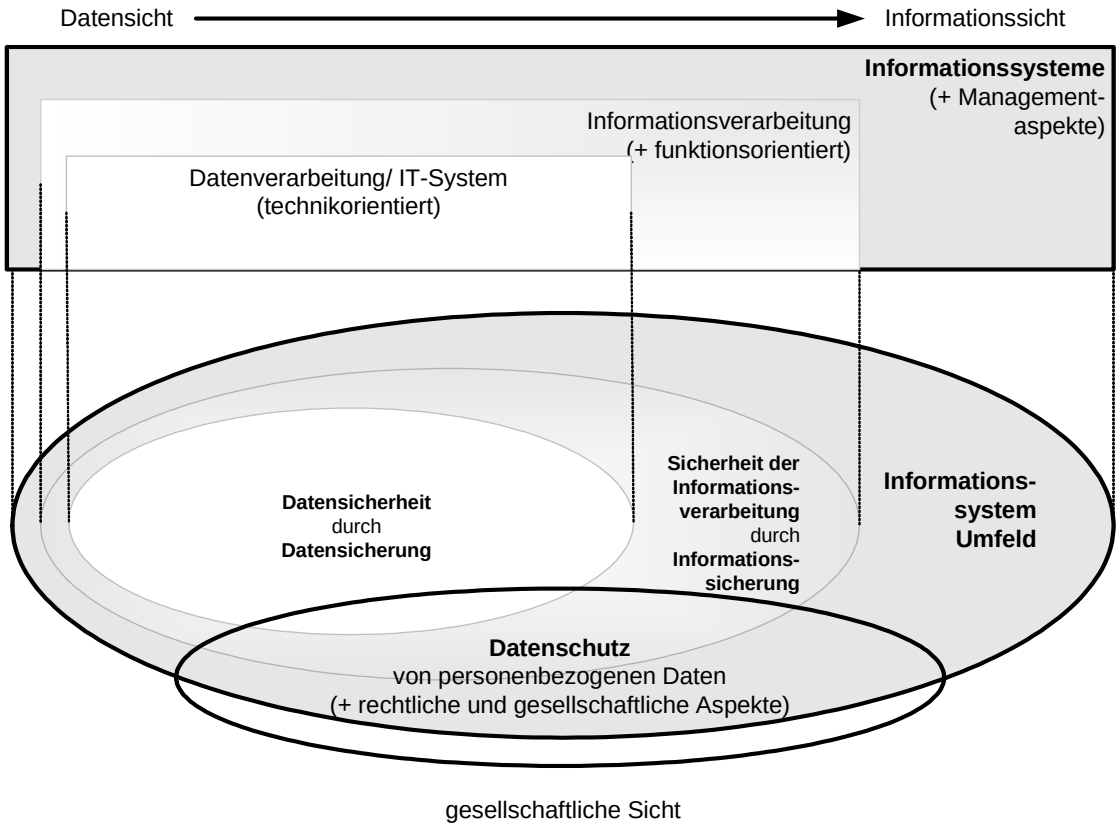


Abbildung 14: Übersicht und Abgrenzung der relevanten Sicherheitsbegriffe im Kontext von Informationssystemen

Datensicherheit und Datensicherung

Die Erfordernisse einer formalen Datenverarbeitung haben zu einer syntaktisch orientierten Auffassung von Daten geführt[99]. Somit ist die Datenverarbeitung ein weitgehend mechanischer Verarbeitungsprozess von Daten nach dem EVA-Prinzip. Dieser formale Prozess ist losgelöst von der Bedeutung des Dargestellten und hat einen vorwiegend automatisierten und maschinemäßigen Charakter.

Die Datensicherung aus Sicht der Informatik beinhaltet alle Maßnahmen und Einrichtungen, die die Datensicherheit herbeiführen oder erhalten, wie regelmäßige Sicherung der Daten (Backup) auf einem externen Datenträger[100]. Die Datensicherheit beschreibt den Zustand, in welchem Maße Daten gesichert sind[101]. Die Sicherheit der Datenverarbeitung bzw. die Datensicherheit hat als Ziel, den Verlust oder die Verfälschung von Daten durch technisch orientierte IT-Systeme zu verhindern. Die Datensicherheit beinhaltet zwei Ebenen, die in enger Abhängigkeit zueinander stehen. Es handelt sich um Systembestandteile der physischen Ebene (z.B. RAID-Systeme oder Streamer) sowie um Anwendungsdaten und Programme der logischen Ebene (z.B. Backup-Programme und deren Archivdaten).

[99] Vgl. Fleischhauer/Rouette (1989), S. 9
[100] Vgl. Locarek-Junge (1995), S. 89
[101] Vgl. Ehmann (1993), S. 72

Informationssicherung
Die Informationsverarbeitung (Verarbeitung, Speichern, Erfassen und Übertragen von Informationen)[102] berücksichtigt aufgabenspezifische Verwendungszusammenhänge. Dies bedeutet, dass aus Daten(verarbeitung) Informations(verarbeitung) entsteht, sobald ein Bezug zu einem Handlungskontext erfolgt[103]. So werden funktionale Maßnahmen eingesetzt, um einen kontext- bzw. personenbezogenen Zugang zu der Informationsverarbeitung herzustellen, wie z.B. Zugangsmaßnahmen (Identifikations- und Authentifizierungs-Verfahren) oder Verschlüsselungstechniken.

Informationssystemsicherheit und Informationssicherheit
Durch den Begriff „Informationssystemsicherheit" bzw. „IS-Sicherheit" werden über den funktionalen Charakter hinaus weitere Managementbereiche, wie z.B. organisatorische, personelle oder rechtliche Aspekte, abgedeckt[104]. So sind zur Schaffung von Informationssystemsicherheit zusätzliche Gestaltungsaspekte, wie z.B. die Erstellung von IS-Sicherheitszielen und IS-Sicherheitsstrategien, notwendig.

Der Begriff „Informationssicherheit" umfasst das vollständige Spektrum der Informationssystemsicherheit[105], wird aber in der Literatur aufgrund der teilweisen unsauberen Trennung zwischen Daten- und Informationsverarbeitung ausschließlich mit Aspekten der Datensicherheit in Verbindung gebracht[106]. Im Rahmen dieser Arbeit sind die Begriffe Informationssicherheit und Informationssystemsicherheit inhaltlich gleichgesetzt und werden synonym verwendet.

IT-Sicherheit (Datensicht) und IS-Sicherheit (Informationssicht)
In Anlehnung an die Datenverarbeitung und Informationsverarbeitung lassen sich die Begriffe

- IT-Sicherheit (**I**nformations**T**echnische-Sicherheit) und
- IS-Sicherheit (**I**nformations**S**ystem-Sicherheit)

differenzieren.

Durch die Orientierung auf die technischen Systeme (Hard- und Software) gelangt man zu dem Begriff IT-Systeme. Die Informations- und Sicherheitstechnologie stellt die Basistechnik und -verfahren zur sicheren Speicherung, Bearbeitung und Übermittlung von Informationen zur Verfügung. Zusätzlich ist ein politisches sowie aufbau- und ablauforientiertes Umfeld nötig, um ein „System" von Sicherheit zu gewährleisten, welches über die system-technischen Aspekte hinausgeht.

[102] Vgl. Stickel/Groffmann/Rau (1998), S. 340
[103] Vgl. Lenz (1991), S. 41 und Zilahi-Szabô (1998), S. 4
[104] Vgl. Schaurette (1999), S. 239
[105] Vgl. Lippold (1992), S. 913, Röhm (2000), S. 18, Hartmann/Karger (2001), S. 379 und Heinrich (2002), S. 279
[106] Vgl. Voßbein, J. (1999), S. 38

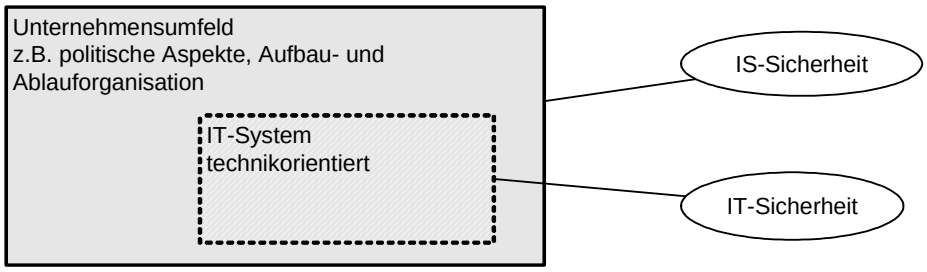


Abbildung 15: Abgrenzung von IT- und IS-Sicherheit[107]

Dies soll aber nicht darüber hinwegtäuschen, dass die IS-Sicherheit ohne die IT-Sicherheit sinnlos ist, da die Technik eine wesentliche Grundlage für die IS-Sicherheit darstellt. Vielmehr ist die IT-Sicherheit ein unverzichtbarer Bestandteil der IS-Sicherheit.

Datenschutz

Weitere Aspekte der IS-Sicherheit bilden Gesetze und Verordnungen, die insbesondere externe Anforderungen an die IS-Sicherheit darstellen[108]. So sind Institutionen in gewissem Rahmen durch Gesetze verpflichtet, den Datenschutz mit bestimmten Maßnahmen (Daten- und Informationssicherung) zu implementieren und aufrechtzuerhalten. Betroffen sind sensitive Daten von natürlichen Personen in der Art, dass durch deren Verarbeitung auf ihre Identität (der Personen) geschlossen werden kann. Der Datenschutz beinhaltet somit den Schutz von personenbezogenen Daten und erzielt aufgrund der steigenden Durchdringung von Informationstechnologien auf gesellschaftlicher und politischer Ebene ein immer größeres Interesse. Das Grundrecht bzw. Bürgerrecht in Bezug auf informationelle Selbstbestimmung ist in manchen Staaten sogar als Menschenrecht anerkannt[109]. Nicht vom Datenschutz abgedeckt sind Daten über

- juristische Personen (AG oder GmbH) oder
- reine Sachdaten (Patente oder Betriebsgeheimnisse)[110].

Der Datenschutz ist gesetzlich u.a. in dem BDSG[111] geregelt[112]. Ebenfalls andere Gesetze, wie z.B. die Telekommunikationsgesetze[113], beeinflussen den Datenschutz. Um den Datenschutz zu gewährleisten, sind neben rechtlichen Aspekten auch technische und organisatorische Aspekte der IS-Sicherheit von Bedeutung. Dies kommt u.a. in der Anlage zu §9 Satz 1 BDSG zum Ausdruck, die dafür sorgen soll, dass die Regelungen des Datenschutzes durch technische und organisatorische Maßnahmen praktisch umgesetzt werden[114]. Diese gesetzliche Forderung des Datenschutzes ist die Schnittmenge zwischen Datenschutz und IS-Sicherheit.

[107] Vgl. Kerster (1995), S. 72
[108] Vgl. Ziener (1997), S. 71
[109] Vgl. Tinnefeld/Ehmann (1998), S. 3
[110] Vgl. Ehmann (1993), S. 73 und Herbst (2001), S. 145
[111] BDSG = Bundesdatenschutzgesetz
[112] Vgl. Eckert (2001), S. 3
[113] Z.B. TDDSG (1997) oder TKG (1996)
[114] Vgl. Behrens (1997), S. 27-29. Behrens bezieht sich noch auf das alte BDSG (1997). Im BDSG (2001) wurden die „ alten“ 10 Gebote zu 8 Geboten „zusammengefasst“.

Roßnagel/Pfitzmann/Garstka (2001) haben umfangreiche Verbesserungsvorschläge für den Datenschutz erarbeitet, die als Ziel die Förderung datenschutzfreundlicher Technologien und die Stärkung der informationellen Selbstbestimmung beinhalten. Hierfür ist eine höhere Transparenz, Vermeidung des Personenbezugs, Zweckbindung der Datenverarbeitung, organisatorische Unterstützung des Datenschutzes und eine Stärkung der Betroffenenrechte nötig. Des Weiteren sollen Spezialregelungen bzgl. des Datenschutzes, die sich in anderen Gesetzen befinden, in einem „neuen" BDSG zusammengefasst werden und die Datenschutzgrundsätze sollten gleichermaßen auch für nicht öffentliche Bereiche gelten[115].

Ein weiteres Ziel - das durch das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein[116] (ULD SH) gefördert wird - ist, den Datenschutz zu einem Qualitätsmerkmal für Institutionen zu etablieren. Dieses Qualitätsmerkmal stellt einen Wettbewerbsvorteil für diese Institutionen dar und fördert somit auch datenschutzfreundliche Technologien[117].

2.1 Phasen des IS-Sicherheitsmanagements

Im Folgenden werden grundlegende Phasen des Managements der IS-Sicherheit diskutiert. Die Problemlösungsprozesse der IS-Sicherheitsstrategien des IS-Sicherheitsmanagements bilden einen Schwerpunkt des Kapitels, da sie die Grundlage für die Problemlösungsmethoden des KE darstellen.

Der Begriff „IS-Sicherheitsmanagement" wird in der Arbeit als „*…die Gesamtheit aller Aktivität zur geplanten und dauerhaften Gestaltung der Informationssicherheit in einem Unternehmen oder einer Behörde verstanden*"[118]. Der Gestaltungsprozess zur Schaffung von Informationssystemsicherheit bzw. des IS-Sicherheitsmanagements basiert auf der Grundlage der klassischen strategischen Planung und Organisationsplanung. Diese betriebswirtschaftlichen Phasenmodelle bilden abgegrenzte Teilphasen, welche die Zielbildung über die Analyse bis zur Umsetzung umfassen[119]. Die Phasen bzw. Aktivitäten des Sicherheitsmanagements lassen sich in folgende Bereiche differenzieren (Abbildung 16):

- Politisches Sicherheitsmanagement (Top Management)
  Festlegung der IS-Sicherheitspolitik und –ziele.
- Konzeptionelles Sicherheitsmanagement (Mittleres Management)
  Analyse und Bewertung der IS-Sicherheit unter Anwendung von IS-Sicherheitsstrategien und Entwicklung eines IS-Sicherheitskonzeptes.
- Operationelles Sicherheitsmanagement (Unteres Management)
  Umsetzung der IS-Sicherheitsmaßnahmen des IS-Sicherheitskonzeptes.
- IS-Kontrollmanagement.
  Kontrolle der vorhergehenden Phasen.

[115] Vgl. Roßnagel/Pfitzmann/Garstka (2001), S. 13-20
[116] Veröffentlicht im Internet, URL: http://www.datenschutzzentrum.de (Stand: 10.12.2002)
[117] Vgl. Wedde/Schröder (2001); IT-Prüfzeichen (2002); Voßbein, R. (2002), S. 7; Bäumler (2002); Schaar/Stutz (2002), S. 330; Datenschutzsiegel (2002) und Dambeck (2003), S. 32
[118] Konrad (1998), S. 46. Vgl. auch Oppliger (1997), S. 21
[119] Vgl. Welge/Al-Laham (1992), S. 44; Krüger (1992), S. 1579; Hentze/Brose/Kammel (1993), S. 65; Berger/Häntschel (1996), S. 38 und Bühner (1999), S. 19

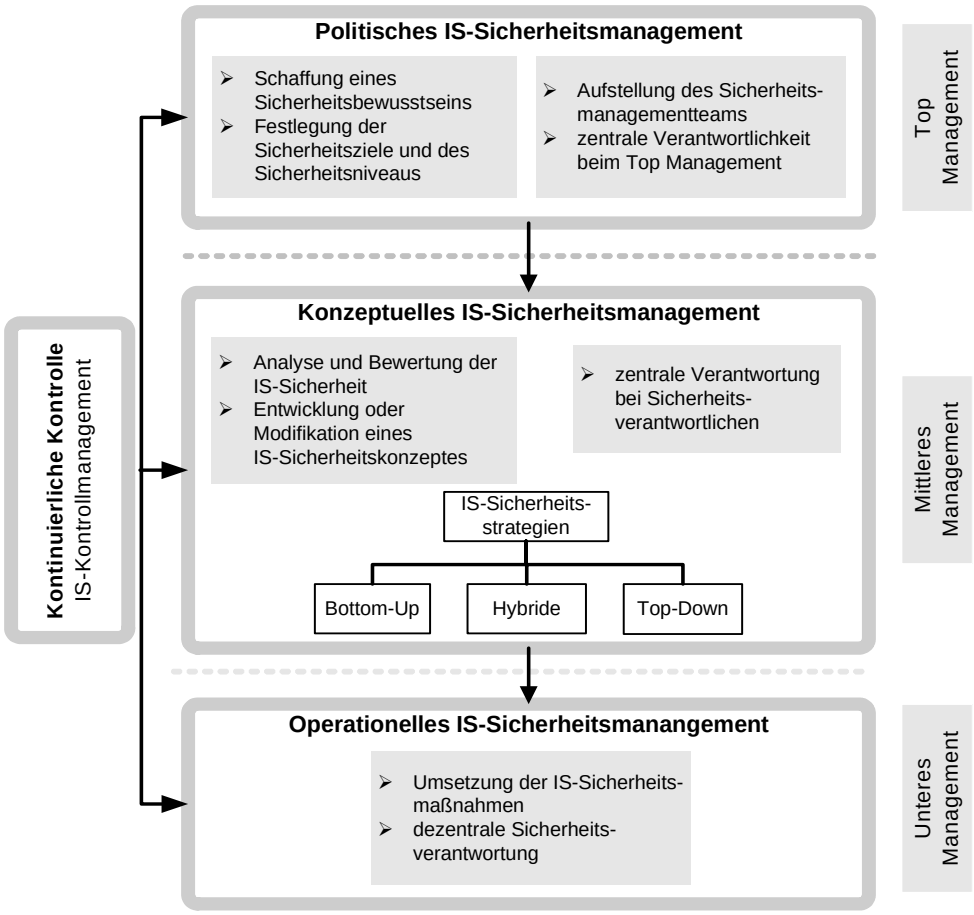


Abbildung 16: Phasen des Sicherheitsmanagements

Die IS-Sicherheitsstrategie ist das zentrale Instrument des IS-Sicherheitsmanagements, deren Ziele und Ergebnisse in einem IS-Sicherheitskonzept dokumentiert werden. Die IS-Sicherheitsstrategie dient zur Umsetzung der IS-Sicherheitspolitik und bildet die Grundlage für die Verwirklichung der IS-Sicherheit im Unternehmen. In der Operationalisierungsphase erfolgt das Umsetzen des IS-Sicherheitskonzeptes in konkrete Maßnahmen und deren Durchführung.

Das IS-Sicherheitsmanagement wird im Laufe der Zeit einer permanenten Kontrolle unterzogen, da die Systemlandschaft einer ständigen Veränderung unterworfen ist. So kann das IS-Sicherheitsmanagement nicht als „starres“ System angesehen werden, sondern es wird den aktuellen Gegebenheiten ständig angepasst. Aus diesem Grund ist die Einbeziehung einer kontinuierlichen Kontrolle bzw. einer IS-Sicherheitsrevision in der Ablauforganisation ein entscheidender Faktor für ein erfolgreiches IS-Sicherheitsmanagement[120].

[120] Vgl. Münch (1999), S. 355

2.2 IS-Sicherheitspolitik

Die IS-Sicherheitspolitik schafft die Grundlage für die IS-Sicherheit im Unternehmen und somit auch für das IS-Sicherheitskonzept[121]. Ohne IS-Sicherheitspolitik ist die Konzepterstellung ziellos und des Weiteren existiert kein Kontrollmaß für den Durchführungsgrad des IS-Sicherheitskonzeptes. Die Sicherheitspolitik ermittelt u.a. auf der Grundlage der Sicherheitsziele das benötigte Sicherheitsniveau, das eine Eingangsgröße für das IS-Sicherheitskonzept darstellt. Dafür ist in den meisten Fällen erst eine Sensibilisierung des Managements für die Sicherheitsproblematik notwendig. Im Hinblick auf den Einsatz eines WBS im Rahmen des IS-Sicherheitsmanagements stellt die IS-Sicherheitspolitik die Anforderungen an das zu entwickelnde WBS.

Die Schaffung der IS-Sicherheitspolitik umfasst folgende Inhalte:

- Schaffung eines Sicherheitsbewusstseins der Führungsebene als Voraussetzung für die Ermittlung des erforderlichen Sicherheitsniveaus.
- Bildung von Sicherheitszielen (z.B. Vertraulichkeit, Integrität und Verfügbarkeit).
- Bildung eines Sicherheitsmanagement-Teams und Vergabe der Verantwortung für die Erstellung und Realisierung des Sicherheitskonzepts.
- IS-Sicherheitspolitik ist auf einen längeren Zeitraum ausgelegt und sollte auch in der Gesamtpolitik des Unternehmens verankert werden.
- IS-Sicherheitspolitik besitzt einen hohen Abstraktionsgrad und soll Richtlinien für die weiteren Phasen darstellen, die dann konkretisiert werden.
- Es sind Umwelteinflüsse und der erforderliche Aufwand bzgl. der Umsetzung der IS-Sicherheitsziele in Relation zu den vorhandenen Ressourcen des Unternehmens für die IS-Sicherheitspolitik zu beachten.

Schaffung des Sicherheitsbewusstseins

Eine wesentliche Voraussetzung für eine erfolgreiche Schaffung von IS-Sicherheit ist die Sensibilisierung des Sicherheitsbewusstseins[122]. Dieses psychologische Problem wurde lange vernachlässigt und seine Bedeutung unterschätzt[123]. Grundsätzlich ist es erforderlich, auf allen Unternehmensstufen ein IS-Sicherheitsbewusstsein zu schaffen, jedoch primär auf der oberen Führungsebene. Die KES-Studie von 2002 belegt mittlerweile, dass das Problem bzgl. des mangelnden IS-Sicherheitsbewusstseins erkannt und als gravierend eingestuft worden ist[124].

[121] Vgl. Brandao (1996), S. 8
[122] Vgl. Hartmann/Karger (2001), S. 381
[123] Vgl. Voßbein, R. (1995b), S. 41 und Wehner (1995), S. 27
[124] Vgl. Voßbein, R./Voßbein, J. (2002a) und Voßbein, R./Voßbein, J. (2002b)

Welche Probleme behindern Sie am meisten bei der Verbesserung der ISi? (Mehrfachnennungen möglich)	
Basis der Prozentuierung	260
Es fehlt an Bewusstsein bei den Mitarbeitern	65%
Es fehlt an Bewusstsein beim mittleren Management	61%
Es fehlt an Bewusstsein und Unterstützung im Top-Management	50%
Es fehlt an Geld	46%
Es fehlt an Möglichkeiten zur Durchsetzung sicherheitsrelevanter Maßnahmen	38%
Es fehlen verfügbare und kompetente Mitarbeiter	37%
Die Kontrolle auf Einhaltung ist unzureichend	34%
Es fehlen die strategischen Grundlagen/ Gesamt-Konzepte	34%
Anwendungen sind nicht für ISI-Maßnahmen vorbereitet	22%
Es fehlen realisierbare (Teil-)Konzepte	21%
Die vorhandenen Konzepte werden nicht umgesetzt	20%
Es fehlen geeignete Methoden und Werkzeuge	18%
Es fehlen geeignete Produkte	12%
Es fehlt an praxisorientierten Sicherheitsberatern	10%
Sonstiges	6%
Keine	4%

Tabelle 1: Problembereiche zur Verbesserung der IS-Sicherheit[125]

Die Führungsebene übernimmt als originäre Aufgabe die Erreichung der Unternehmensziele. Somit hat diese Ebene in letzter Konsequenz auch die Verantwortung für die IS-Sicherheit zu tragen[126]. Des Weiteren besitzt nur die Führungsebene die Kompetenz einer globalen Sichtweise auf die Systemlandschaft, was die Voraussetzung für eine unternehmensinterne und -externe Sichtweise für die Abhängigkeit des Unternehmens von der Informationsverarbeitung und dem damit verbundenen IS-Sicherheitsproblem darstellt. Trotz dieser Notwendigkeit ist die Sensibilität der Unternehmensleitung für die IS-Sicherheit i.d.R. nicht stark ausgeprägt[127]. Dies dokumentiert die Studie, in der ermittelt worden ist, dass 57% der Unternehmen kein eigenes Budget für IS-Sicherheitsaufgaben bereitstellten und zum anderen, dass nur 20% des Top-Managements die IS-Sicherheit als vorrangiges Ziel betrachten[128].

Welchen Stellenwert hat die ISi für Ihr Top-Management?			
	1994	2000	2002
ISi ist ein vorrangiges Ziel der Informationsverarbeitung	16%	23%	20%
ISi ist ein gleichrangiges Ziel der Informationsverarbeitung	49%	46%	50%
ISi ist eher ein „lästiges Übel“	35%	30%	29%

Tabelle 2: Stellenwert der IS-Sicherheit beim Top-Management[129]

[125] Vgl. Voßbein, R./Voßbein, J. (2002b), S. 18
[126] Vgl. Stelzer (1993), S. 75; Jaspers (1997), S. 159; Plate (1997), S. 373; Konrad (1998), S. 39 und BSI-Grundschutzhandbuch (2000), Kapitel 1.1, S. 1
[127] Vgl. Stelzer (1993), S. 64 und Voßbein, J. (1999), S. 74-77
[128] Vgl. Budget (2001). Insgesamt wurden 431 Unternehmen befragt.
[129] Vgl. Voßbein, R./Voßbein, J. (2002a), S. 20

Deshalb ist es erforderlich, die Führungsebene für ihre Verantwortung gegenüber der Abhängigkeit von Informationssystemen und deren Sicherheit zu sensibilisieren. Diese Verantwortung drückt sich in den Sicherheitszielen, dem -niveau und deren Umsetzung aus. Es ist nicht zu erwarten, dass die ausführenden Ebenen des Unternehmens ein umfangreiches Sicherheitsbewusstsein entwickeln, wenn dieses nicht in der Führungsebene Vorrang hat[130]. Für eine erfolgreiche Durchsetzung der Sicherheitspolitik ist es erforderlich, dass von der Führungsebene die Initiative für die IS-Sicherheit ausgeht[131].

Ein WBS besitzt die Möglichkeit, die Sensibilität für die IS-Sicherheit zu schärfen, da einerseits die Schwachstellen, andererseits auch deren negative Konsequenzen für das Unternehmen aufgezeigt werden. Insbesondere wenn sich die Unternehmensleitung bewusst ist, dass sie für die aufgezeigten Konsequenzen die Verantwortung zu tragen hat, ist die Motivation zur Erstellung eines IS-Sicherheitskonzepts gewachsen.

Basissicherheitsziele

Bei der Erreichung der Unternehmensziele existieren im großen Umfang Interdependenzen zwischen Informationssystemen und deren Sicherheit. Die Abhängigkeiten zwischen Unternehmenszielen und Informationssystemen können aus zwei Sichten betrachtet werden[132]:

- Einerseits bilden die Unternehmensziele die Vorgaben oder den Rahmen für die Informationssysteme[133]. Davon werden die Sicherheitsziele abgeleitet und konkretisiert. Die Informationssysteme werden in diesem Fall an den Unternehmenszielen ausgerichtet (align). So bildet z.B. das Unternehmensziel „Einstieg in den E-Commerce“ Vorgaben für die Entwicklung und für den Betrieb von (neuen) Informationssystemen.
- Andererseits kann die Durchsetzung der Unternehmensziele erst durch den Einsatz von Informationssystemen möglich sein. Hierbei bilden die Informationssysteme die Voraussetzung für die Erreichung von Unternehmenszielen (enable). Dabei erlangt die Sicherheit von Informationssystemen einen entscheidenden Einfluss. Erst bei Erfüllung der Sicherheitsziele für Informationssysteme ist eine Durchsetzung der Unternehmensziele gewährleistet. Hierbei wird die Abhängigkeit der Unternehmensziele von den Informationssystemen und deren Sicherheit deutlich.

[130] Vgl. Brandao (1996), S. 9
[131] Vgl. Licht (1996), S. 22 und Grundschutzhandbuch (2000), Kapitel 1.1
[132] Vgl. Krcmar (2000), S. 203
[133] Vgl. Berger/Häntschel (1996), S. 39

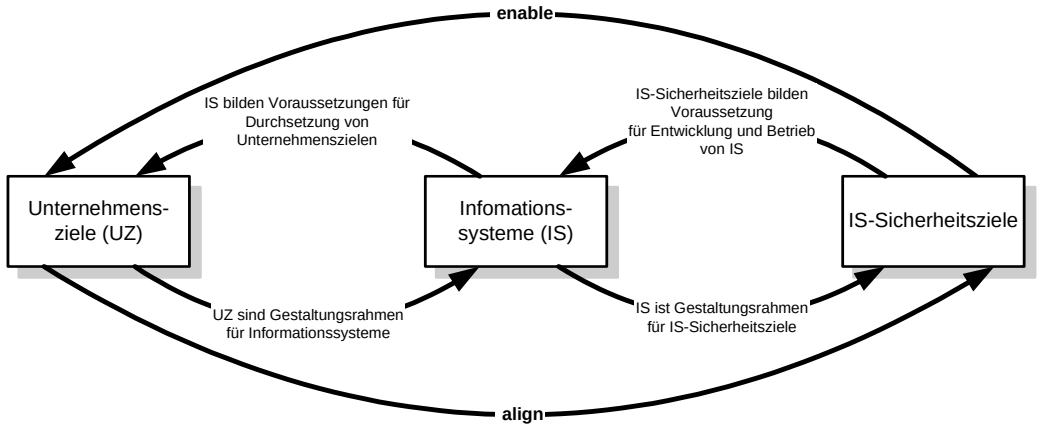


Abbildung 17: Zusammenhang zwischen Unternehmens- und Informationsziel[134]

Die komplementären Bereiche wie Unternehmensziele, Informationssysteme und IS-Sicherheit beeinflussen sich gegenseitig. So stellen die Unternehmensziele den Rahmen für die Informationssysteme dar, andererseits werden die Unternehmensziele erst durch Informationssysteme möglich. Diese Interdependenz wird auf die Sicherheitsziele erweitert, denn Sicherheitsziele dienen einerseits als Voraussetzungen für eine erfolgreiche Entwicklung und dem Betrieb von Informationssystemen, andererseits bilden die Informationssysteme den Gestaltungsrahmen für die Sicherheitsziele. Die Sichtweise der Interdependenz ist von dem jeweiligen Standpunkt (Unternehmensziel, Informationssystem oder IS-Sicherheit) abhängig. Dadurch entsteht ein logischer Zirkel, der nicht aufzulösen ist. Ein ähnliches Dilemma ist aus der Ziel-Planung bekannt. Dort sind Ziele einerseits Voraussetzung der Planung, andererseits Ergebnis der Planung[135].

In der Literatur und Praxis haben sich Vertraulichkeit, Integrität und Verfügbarkeit als Basissicherheitsziele der IS-Sicherheit herausgebildet[136]. Im Rahmen der Arbeit orientieren sich die Definitionen der Basissicherheitsziele an dem BSI-Grundschutzhandbuch:

- *„Vertraulichkeit soll sicherstellen, daß der Zugriff auf bestimmte Daten und Informationen nur berechtigten Benutzern ermöglicht wird.*
- *Integrität bezeichnet die Korrektheit, Manipulationsfreiheit und Unversehrtheit von Daten und Informationen.*
- *Verfügbarkeit charakterisiert ein IT-System, dessen Daten und Informationen, Prozesse und IT-Anwendungen zur rechten Zeit bereitstehen.*“[137]

Die Abhängigkeit von Informationssystemen scheint primär durch die Verfügbarkeit der Funktionalität determiniert zu sein. Dieser Eindruck wird durch die sehr schnellen Auswirkungen des Verlustes der Verfügbarkeit ausgelöst. Auf den zweiten Blick wird die Abhängig-

[134] Erweitert in Anlehnung an Krcmar (2000), S. 203
[135] Vgl. Hentze/Brose/Kammel (1992), S. 67
[136] Vgl. Baer (1995), S. 55; Kruth (1995), S. 54; Licht (1996), S. 22; Voßbein, R. (1997), S. 10; Schaurette (1999), S. 223; Peltier (1999), S. 197; Hammer (1999), S. 187; Kubicek (2001), S. 13 und Maczkowsky/Rost/Köhntopp (2001), S. 58
[137] BSI-Grundschutzhandbuch (2000), Kapitel 2.2, S. 5

keit der anderen Sicherheitsziele deutlich. Der Verlust der Verfügbarkeit und Integrität zieht eventuell einen Verlust der Vertraulichkeit nach sich. Dieser Zusammenhang wird in folgender Abbildung dargestellt.

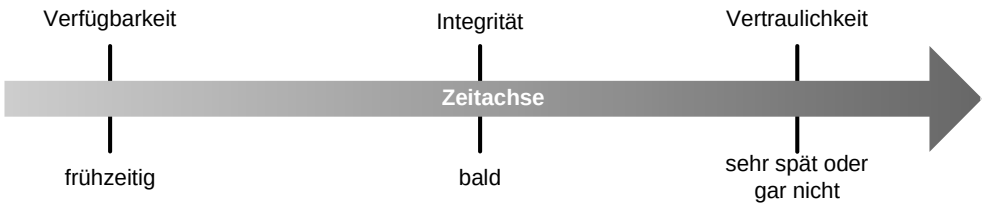


Abbildung 18: Zeitpunkt der Entdeckung des Verlustes eines Grundziels[138]

Somit bringt eine isolierte Sicht auf „ein" Basisziel nicht das gewünschte Ergebnis. Die Ziele kommen erst in ihrer Summe dem „Oberziel" eines sicheren Informationssystems näher. Das Oberziel eines „vollständigen sicheren" Informationssystems ist aber in den meisten Fällen nicht mit den zu erwartenden Kosten vereinbar; es muss ein Restrisiko in Kauf genommen werden[139]. Des Weiteren sollten bei den Anforderungen an die Sicherheit von Informationssystemen immer die Angemessenheit, Bedienungsfreundlichkeit und Verfügbarkeit der Maßnahmen in Betracht gezogen werden[140]. Andernfalls werden überzogene Sicherungsmaßnahmen die Akzeptanz des Informationssystems stark mindern.

In der Literatur werden häufig weitere Sicherheitsziele oder deren Erweiterung beschrieben, wie z.B. Vertraulichkeit oder Authentizität, die insbesondere in Verbindung mit der Kommunikationssicherheit und dem E-Commerce zu finden sind[141]. Es sind außerdem konträre Sicherheitsziele zwischen Partnern zu beachten, denn die beteiligten Partner können z.B. bei einer Transaktion unterschiedliche Sicherheitsziele verfolgen[142]. Inwieweit es sinnvoll ist, diese zusätzlichen Ziele zu berücksichtigen und auf gleicher Ebene wie Basisziele zu behandeln, ist von der jeweiligen Sichtweise abhängig, in der die IS-Sicherheit betrachtet wird.

Sicherheitsniveau

Im Rahmen der Sicherheitspolitik wird das gewünschte Sicherheitsniveau von der Unternehmensleitung festgelegt[143]. Das Sicherheitsniveau ist eine strategische Richtgröße bzw. eine langfristige Zielgröße des IS-Sicherheitsmanagements für die ganze Institution. Es kann als aggregierte Aussage der Sicherheitsziele aufgefasst werden, wobei das „stärkste" oder „höchste" Sicherheitsziel das Niveau bestimmt. So kann bei der Ausgestaltung des Sicherheitskonzepts das konkrete Sicherheitsniveau für die einzelnen Unternehmensbereiche kurz- oder langfristig differenzieren[144].

[138] Vgl. Kerster (1995), S. 78
[139] Vgl. Lippold (1992), S. 916
[140] Vgl. Fox (2001), S. 24
[141] Vgl. Kersten (1995), S. 77; RSD (1999), S. 23; Wolf (1999), S. 36-37; Röhrig/Knorr/Noser (2000), S. 500; Hennig (2001), S. 411 und Kubicek (2001), S. 13
[142] Vgl. Rannenberg (2000), S. 490
[143] Vgl. Pohl (1995), S. 114
[144] Z.B. wird im Rahmen des IT-Grundschutzhandbuchs die konkrete Ausgestaltung des Sicherheitsniveaus als „Schutzbedarf" bezeichnet. Als Ziel wird aber die Erreichung des angestrebten Sicherheitsniveaus für das ganze Unternehmen angenommen.

Das BSI[145] schlägt im IT-Grundschutzhandbuch folgende vier Sicherheitsniveaus vor:

Niveau: Maximal Der Schutz vertraulicher Informationen muss gewährleistet sein, um in sicherheitskritischen Bereichen strengen Vertraulichkeitsanforderungen zu genügen. (Vertraulichkeit) Die Informationen müssen im höchsten Maße korrekt sein. (Integrität) Die zentralen Aufgaben der Institution sind ohne IT-Einsatz nicht durchführbar. Knappe Reaktionszeiten für kritische Entscheidungen fordern ständige Präsenz der aktuellen Informationen, Ausfallzeiten sind nicht akzeptabel. (Verfügbarkeit) Insgesamt gilt: Der Ausfall der IT führt zum totalen Zusammenbruch der Institution oder hat schwerwiegende Folgen für breite gesellschaftliche oder wirtschaftliche Bereiche. (Abhängigkeitsgrad)
Niveau: Hoch Der Schutz vertraulicher Informationen muss hohen gesetzlichen Anforderungen genügen und in sicherheitskritischen Bereichen stärker ausgeprägt sein. Die verarbeiteten Informationen müssen korrekt sein, auftretende Fehler müssen erkennbar und vermeidbar sein. In zentralen Bereichen der Institution laufen zeitkritische Vorgänge oder es werden dort Massenaufgaben wahrgenommen, die ohne IT-Einsatz nicht zu erledigen sind; es können nur kurze Ausfallzeiten toleriert werden. Insgesamt gilt: Im Schadensfall tritt Handlungsunfähigkeit in zentralen Bereichen der Institution ein; Schäden haben erhebliche Beeinträchtigungen der Institution selbst oder betroffener Dritter zur Folge.
Niveau: Mittel Der Schutz von Informationen, die nur für den internen Gebrauch bestimmt sind, muss gewährleistet sein. Kleinere Fehler können toleriert werden, Fehler, die die Aufgabenerfüllung erheblich beeinträchtigen, müssen jedoch erkenn- oder vermeidbar sein. Längere Ausfallzeiten, die zu Terminüberschreitungen führen, sind nicht zu tolerieren. Insgesamt gilt: Schäden haben Beeinträchtigungen der Institution zur Folge.
Niveau: Niedrig Vertraulichkeit von Informationen ist nicht gefordert. Fehler können toleriert werden, solange sie die Erledigung der Aufgaben nicht völlig unmöglich machen. Dauernder Ausfall ist zu vermeiden, längere Ausfallzeiten sind jedoch hinnehmbar. Insgesamt gilt: Schäden haben nur eine unwesentliche Beeinträchtigung der Institution zur Folge.

Tabelle 3: Formen von Sicherheitsniveaus[146]

Es wird i.d.R. ein höchst mögliches Sicherheitsniveau angestrebt. Die Ernüchterung kommt bei dem Klarwerden der Konsequenzen des hohen Sicherheitsniveaus, das sich in einem finanziellen und personellen Aufwand widerspiegelt[147]. So ist bei der Bestimmung des Sicherheitsniveaus immer die Relation zwischen erwartetem Aufwand und den vorhandenen Ressourcen zu beachten. Eine nur geringe Steigerung des Sicherheitsniveaus kann zu einem sehr starken Anstieg des erforderlichen Aufwands führen.

Es lassen sich grob folgende Ressourcenklassen als Restriktionen für das Sicherheitsniveau differenzieren[148]:

- qualifiziertes Personal
- finanzielle Mittel, besonders bei größeren Investitionen in die IS-Sicherheit
- Verfahren und Produkte, um die IS-Sicherheit durchzusetzen
- Zeit, um die IS-Sicherheit zu realisieren.

[145] BSI = Bundesamt für Sicherheit in der Informationstechnik. Eine Übersicht der Historie und Struktur des BSI bietet Heuser (2000) an.
[146] Grundschutzhandbuch (2000), Kapitel 1.2, S. 6
[147] Vgl. Voßbein, J. (1999), S. 260
[148] Vgl. Lippold/Stelzer/Konrad (1992), S. 372

Eine sinnvolle Sicherheitszielsetzung ist nur zu erreichen, wenn die Sicherheitsziele in Verbindung mit dem ganzen Unternehmenszielsystem entwickelt[149] und in IS-Sicherheitsstrategien umgesetzt werden. Dieser Gesamtzusammenhang wird in der folgenden Abbildung dargestellt.

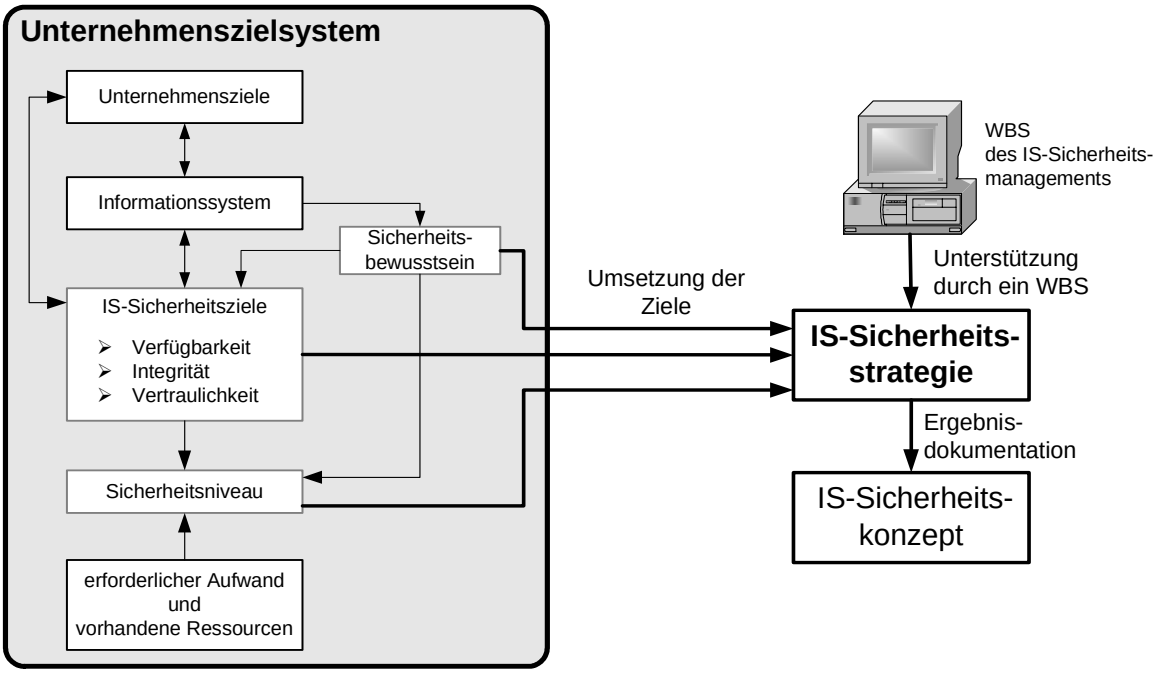


Abbildung 19: IS-Sicherheitsziele und -strategien

Die Ermittlung der IS-Sicherheitsziele selbst kann durch das WBS meist nur indirekt unterstützt werden, da die Zielbildung einen stark kognitiven Charakter aufweist und sehr viele „politische“ Einflussfaktoren besitzt. Eine Formalisierung der politischen Ebene ist deshalb nur bedingt möglich. Die Unterstützung kann z.B. durch Aufzeigen von erforderlichem Aufwand für ein bestimmtes Sicherheitsniveau erfolgen.

2.3 IS-Sicherheitsstrategien

Die Umsetzung des IS-Sicherheitsniveaus, -bewusstseins und der -ziele erfolgt durch die Auswahl und Ausgestaltung der IS-Sicherheitsstrategien. So existieren Strategien, die als Ziel ein hohes oder ein niedriges bis mittleres IS-Sicherheitsniveau haben. Das IS-Sicherheits-WBS unterstützt die jeweiligen IS-Sicherheitsstrategien, wodurch eine indirekte Umsetzung der IS-Sicherheitspolitik durch ein WBS erfolgt. Die Zielgrößen der Sicherheitspolitik werden als Eingangsgrößen für die IS-Sicherheitsstrategie interpretiert, deren Ergebnis das IS-Sicherheitskonzept ist. Das IS-Sicherheitskonzept ist wiederum die Ausgangsgröße für eine erfolgreiche Operationalisierung der IS-Sicherheit im Unternehmen. Die Ergebnisse des IS-Sicherheitskonzepts sind grob eine Darstellung des Sicherheitszustandes und eine Erläuterung bzw. Begründung der erforderlichen Umsetzungsmaßnahmen, um ein gewisses Sicherheitsniveau zu erreichen. Die IS-Sicherheitsstrategie umfasst grob folgende Teilphasen:

[149] Vgl. Stelzer (1993), S. 60

- Erhebung und Abbildung der relevanten IS-Sicherheitsaspekte
- Analyse und Bewertung des IS-Sicherheitszustandes
- Entwicklung erforderlicher Maßnahmen.

Hierfür lassen sich folgende generische IS-Sicherheitsstrategie-Ansätze unterscheiden[150]:

- Bottom-Up Ansatz
- Top-Down Ansatz.

2.3.1 Bottom-Up Ansatz

Die Bottom-Up Ansätze[151] zerlegen das Informationssystem in einzelne Bestandteile, um diese auf ihre Sicherheitsaspekte (z.B. Gefahren, Konsequenzen oder Risiken) zu untersuchen. Die Granularität der Zerlegung und Beschreibung ist u.a. von dem konkreten Analyseinstrument, dem -kontext, der -komplexität, der -methode und dem erwarteten Aufwand abhängig. Auf Basis der ermittelten und bewerteten Sicherheitsaspekte werden die erforderlichen Maßnahmen festgestellt. Bei diesem Ansatz ist es notwendig, dass Beziehungen zwischen den sicherheitsrelevanten Elementen sowie deren Abhängigkeiten dargestellt werden, damit das jeweilige Risiko bzw. der Risikograd ermittelt werden kann[152]. Eine häufig anzutreffende Ausprägungsform dieses atomistischen Ansatzes ist die Risikoanalyse, die in unterschiedlichen Formen existiert und im Kapitel 2.3.1.1 beschrieben wird.

Gefährdungsorientierter IS-Sicherheitsbegriff

Der Bottom-Up Ansatz ist durch den gefährdungsorientierten IS-Sicherheitsbegriff geprägt, da hier die Sicherheit über das Erkennen und Verhindern von Gefährdungen, Bedrohungen, Risiken oder die Beeinträchtigungen des jeweiligen Informationssystems definiert wird. Im Vordergrund dieser Begriffsabgrenzung stehen vor der Durchführung von Sicherungsmaßnahmen zuerst die Analyse und Darstellung der Risikofaktoren. Voraussetzung für den Bottom-Up Ansatz bildet somit eine detaillierte Modellierung von Sicherheitsaspekten des Informationssystems, womit individuelle Gefahren erkannt und sofort Gegenmaßnahmen entwickelt werden können. Hierdurch entsteht ein weitreichender reaktiver Bereich für die Institution, um auf negative Vorfälle zu reagieren.

[150] Vgl. Konrad (1998), S. 58; Voßbein, J. (1999), S. 233 und Gerber/Solms (2001), S. 582

[151] Die Begriffe Top-Down und Bottom-Up werden auch in der Systementwicklung als Entwicklungsstrategien (Top Down = schrittweise Verfeinerung bzw. Spezialisierung; Bottom-Up = schrittweise Verallgemeinerung bzw. Generalisierung) verwendet. Dies ist inhaltlich nicht vollständig mit den in der IS-Sicherheitskonzepterstellung verwendeten Top-Down und Bottom-Up Ansätzen gleichzusetzen, da diese z.T. andere Aspekte besitzen.

[152] Vgl. Stelzer (1995), S. 117 und Konrad (1998), S. 57

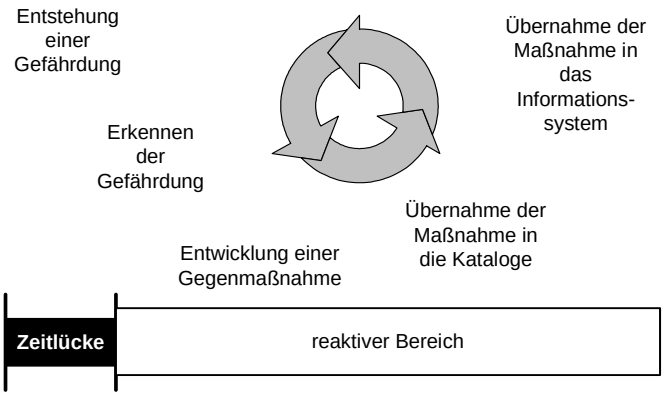


Abbildung 20: Zeitlücke beim gefährdungsbasierten Sicherheitsbegriff[153]

Der Nachteil entsteht durch die hohe erforderliche Komplexitätsbildung und dem damit verbundenen hohen Aufwand, da für jedes Informationssystem eine individuelle Analyse durchgeführt wird. Der Bottom-Up Ansatz ist somit in „reiner Form" meistens von theoretischem Charakter[154].

2.3.1.1 Risikoanalyse

Insbesondere in der USA hat die Risikoanalyse eine starke Verbreitung erfahren, da dort das National Bureau of Standard (NBS) 1979 verbindlich eine Richtlinie zur Durchführung der Risikoanalyse für Behörden entwickelt hat[155]. Es existieren verschiedene Ausprägungen von Risikoanalysen, die unterschiedliche Schwerpunkte auf die einzelnen Phasen setzen. Manche Autoren verstehen unter dem Begriff „Risikoanalyse" nur die Phase Risikobewertung[156] oder die Risikoerkennung in Form der Analyse der Wechselwirkungen von Schwachstellen und Bedrohungen[157]. Trotz der unterschiedlichen Ausgestaltungen lässt sich ein Rahmen für die Risikoanalyse strukturieren, die auf folgenden Phasen basiert. In der Arbeit beinhaltet der Begriff „Risikoanalyse" die Systemabgrenzung, Risikoerkennung, Risikobewertung und Risikobewältigung[158].

[153] Erweitert in Anlehnung an Voßbein, J (1999), S. 40
[154] Vgl. Kerster (1995), S. 84
[155] Vgl. Oppliger (1997), S. 22
[156] Vgl. Kerster (1995), S. 79 und Oppliger (1997), S. 24
[157] Vgl. Krallmann (1989), S. 35 und Heinrich (2002), S. 279
[158] Vgl. Stelzer (1995), S. 199 und Kyas (1996), S. 22

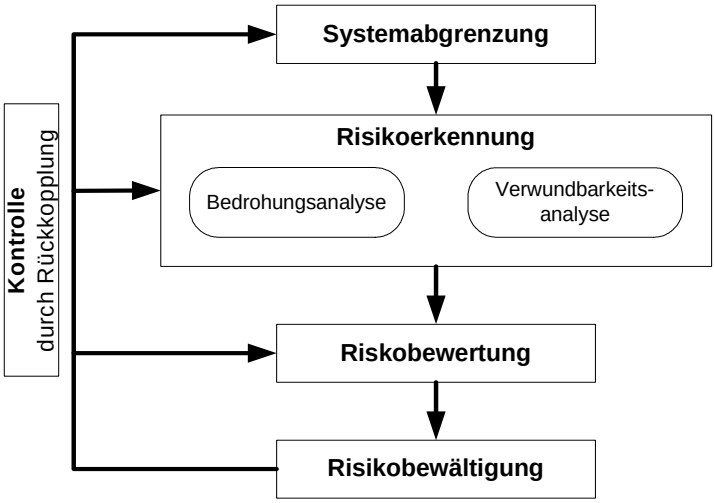


Abbildung 21: Vorgehensmodell der Risikoanalyse

In der Abbildung ist der iterative Prozess der Risikoanalyse beschrieben, wobei die Validierung bzw. Kontrolle der Phasen als Rückkopplung dargestellt wird. Zwischen den einzelnen Phasen besteht ein fließender Übergang; teilweise lassen sich die Phasen nicht eindeutig trennen.

Systemabgrenzung
In dieser Phase werden die sicherheitsrelevanten Aspekte der Elemente und Beziehungen der zu analysierenden Informationssysteme systematisch identifiziert, erfasst und dargestellt[159]. Der Detaillierungsgrad der Erhebung und Beschreibung kann den jeweiligen situativen Faktoren, wie Aufwand oder vorhandene Ressourcen, angepasst werden. Das Ergebnis der Erfassung und Beschreibung wird als Systemmodell[160] oder Strukturmodell[161] bezeichnet, das als Basis für die folgenden Phasen dient. Wenn ein sehr komplexes System entsteht, können die sicherheitsrelevanten Objekte eventuell nach Kriterien priorisiert werden. Die Ergebnisse des ersten Schrittes gehen meist fließend in den zweiten Schritt - die Risikoerkennung - über.

Risikoerkennung
Auf Basis des Systemmodells erfolgt mit der Bedrohungsanalyse und Verwundbarkeitsanalyse (oder Schwachstellenanalyse im engeren Sinne[162]) eine inhaltliche Beschreibung der Risiken. Die Bedrohungs- bzw. Gefährdungsanalyse dient der Ermittlung und Analyse von Bedrohungen bzw. Gefahren. Im Rahmen der Verwundbarkeitsanalyse werden Schwachstellen und Bedrohungen ermittelt und dem Systemmodell zugeordnet. Im Rahmen der Risikoerkennung werden nicht nur die Gefahrenquellen für die sicherheitsrelevanten Elemente identifiziert, sondern auch die Konsequenzen ermittelt und beschrieben. Wenn eine Gefahr vorhanden ist und sicherheitsrelevante Elemente Schwachstellen besitzen, ist von einem Risiko auszugehen. Der Risikograd wird in der folgenden Risikobewertung ermittelt.

[159] Vgl. Jung/Han/Suh (1999), S. 62
[160] Vgl. Oppliger (1997), S. 24
[161] Vgl. Stelzer (1993), S. 183
[162] Aufgrund der Begriffsverwirrung von Schwachstellenanalyse als eigenständiges Analyseinstrument und der Schwachstellenanalyse im engeren Sinne als Teil der Risikoerkennung wird der Begriff „Verwundbarkeitsanalyse“ verwendet.

Risikobewertung

Die Risikobewertung hat zur Aufgabe, das Ausmaß eines Risikos zu bestimmen (Risikograd) und in Relation zu anderen Risiken oder einem Risikomaßstab zu setzen. Kardinale Bewertungsverfahren - wie die Annualized Loss Expectancy (ALE) - beruhen auf formalen Berechnungsvorschriften, die als Variablen die Eintrittwahrscheinlichkeit und die erwartete Schadenshöhe einer Gefahr besitzen[163]. Hierbei besteht die Problematik, dass für dieses statistische Wissen eine umfangreiche Falldatenmenge benötigt wird, um eine Objektivität der Ergebnisse zu gewährleisten („Gesetz der großen Zahlen"). Diese Voraussetzung ist aber bei den benötigten Eintrittswahrscheinlichkeiten und den Schadenshöhen meist nicht gegeben. Es wird somit häufig auf subjektive Schätzungen zurückgegriffen, obwohl die Ergebnisse einer Risikoanalyse eine exakte Risikobewertung suggerieren[164]. Insbesondere die Ermittlungen von Risiken mit sehr großem (kleinem) Schadenpotential und geringer (hoher) Eintrittswahrscheinlichkeit ergeben häufig keine sinnvollen Ergebnisse. Um die oben aufgeführten gravierenden Probleme zu mildern, wurden die kardinalen Größen teilweise oder vollständig durch ordinale Größen ersetzt. Die Eintrittswahrscheinlichkeiten und Schadenshöhen werden zu Gruppen oder Klassen zusammengefügt, wobei der Grad der Detaillierung variieren kann. Die Risiken werden mit Hilfe von Listen oder Matrizen ermittelt und nicht mehr „exakt" errechnet.

Insgesamt wird bei der kardinalen und ordinalen Risikobewertung versucht, komplexe und schlecht strukturierte Problembereiche - wie die IS-Sicherheit - mit wohlstrukturierten Modellen zu beschreiben. Hierbei entsteht aber eine deutliche „Differenz" zwischen dem realen Problem und der Problembeschreibung.

Risikobewältigung und Kontrolle

In der Risikobewältigung erfolgt die schriftliche Fixierung der Ergebnisse der vorhergehenden Phasen und der erforderlichen Sicherheitsmaßnahmen in einem Sicherheitskonzept. Dabei handelt es sich nicht nur um die simple Aufzählung der Ergebnisse und Maßnahmen, sondern um die Beschreibung der Vorgehensweisen und Zusammenhänge für die folgende Umsetzung und Kontrolle. Dabei soll das Konzept einen Charakter eines Handbuches oder Pflichtenheftes besitzen. Die Risikobewältigung folgt häufig im folgenden Stufenverfahren.

[163] Risikograd = Eintrittswahrscheinlichkeit · erwartete Schadenshöhe. Vgl. BSI-IT-Sicherheitshandbuch (1992), S. 44; Baer (1995), S. 27 und Ozier (1999), S. 249

[164] Vgl. Theil (1995), S. 79-94; Pongratz (1996), S. 237; Ciechanowicz (1997), S. 224; Oppliger (1997), S. 25; Voßbein, J. (1999), S. 239 und Damm et al. (1999), S. 76

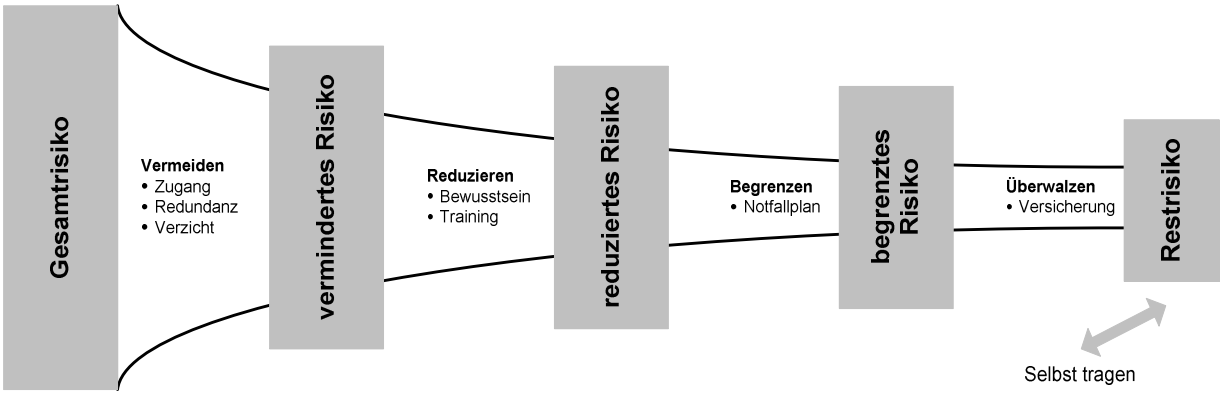


Abbildung 22: Stufenweise Risikobewältigung[165]

In Verbindung mit dem Risiko wird häufig der Begriff „Restrisiko“ verwendet, das als das Risiko bezeichnet wird, das nicht mehr durch Sicherungsmaßnahmen neutralisiert oder auf Versicherungen „überwälzt“ werden kann oder soll[166].

2.3.1.2 FMEA Verfahren[167]

Eine formalisierte Risikomethode ist das FMEA Verfahren, das Anfang der 80er Jahre als „Ausfalleffektanalyse“ (DIN 25448) genormt wurde und bis heute ständig weiterentwickelt wird. Die Methode wurde ursprünglich Anfang der 60er Jahre im Rahmen von Vorhaben der NASA entwickelt und ab den 80er Jahren insbesondere in der Automobilindustrie, Kerntechnik und Luft- und Raumfahrtechnik eingesetzt[168].

Die Zielrichtung der Methode ist ausgehend vom Betrachtungsgegenstand das Aufdecken und Bewerten von möglichen Fehlerquellen sowie deren Ursachen. Diese Methode wird hauptsächlich in technischen Bereichen eingesetzt, dient der Qualitätssicherung und ist aufgrund der Normierung in einem gewissen Grad formalisiert[169]. Die Risikoanalyse bezüglich der IS-Sicherheit kann als ein angepasstes und spezialisiertes FMEA-Verfahren angesehen werden. Die folgende Schablone für ein FMEA-Formblatt strukturiert den Grundaufbau der FMEA.

[165] Vgl. RSD (1999), S. 109
[166] Vgl. Kerster (1995), S. 84 und Heinrich (1999), S. 278
[167] Die Abkürzung FMEA wurde ins Deutsche als „Fehler-Möglichkeits- und Einflussanalyse“ übersetzt und steht auch für den englischen Ausdruck „Failure Mode und Effects Analysis“. Vgl. Müller/Tietjen (2000), S. 2
[168] Vgl. FQS (1994), S. 10
[169] Vgl. Müller/Tietjen (2000), S. 2-3

(1) **Stammdaten** Auswahl der Untersuchungsinhalte und organisatorische Vorbereitung der FMEA.		
(2) **Untersuchungs-gegenstand** Beschreibung und Strukturierung des Untersuchungs-gegenstandes bzgl. seiner Funktionen und seines Aufbaus.	(3) **Risikoanalyse** (Risikoerkennung und -bewertung) Fehlerbeschreibung des Untersu-chungsgegenstandes durch poten-tielle Fehlerfolge, potentielle Fehler-ursache und Erfassung von Schwachstellen. Danach Bewertung der Ergebnisse.	(4) **Risiko-minimierung** Ermittlung der Maßnahmen, um die Schwach-stellen des Unter-suchungsgegen-standes zu besei-tigen.

Tabelle 4: Schematischer Aufbau des FMEA-Formblattes[170]

Im Zusammenhang mit der FMEA sind folgende formalisierte Methoden von Bedeutung, die besonders die Risikoanalyse bzgl. der Fehlerwirkungen und deren Ursachen unterstützen[171]:

- Bei der Fehlerbaumanalyse (FTA[172]) nach DIN 25424 werden ausgehend von einem unerwünschten Zustand oder Ereignis des Systems (z.B. Ausfall) die dafür möglichen Ursachen ermittelt.
- Im Unterschied dazu werden bei der Ereignisablaufanalyse (EAT[173]) nach DIN 25419 ausgehend von einem Anfangsereignis bzw. einer Ursache die Folgewirkung (Konsequenz) bzw. Fehlerfortpflanzung und der Endzustand im System ermittelt.

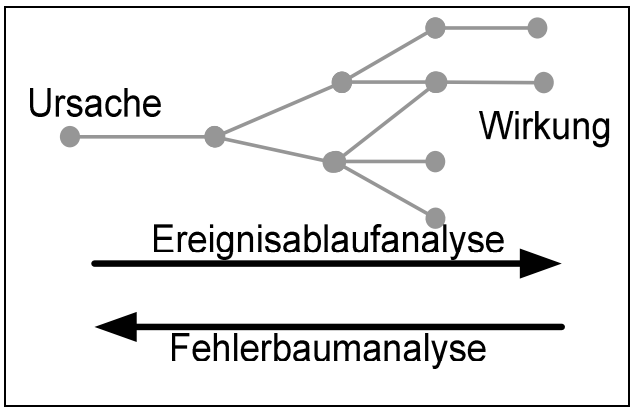


Abbildung 23: Gegenüberstellung der FTA und ETA

Die Analyse von kausalen Zusammenhängen kann in Form einer Baumstruktur abgebildet werden. Ausgehend von einer Ursache werden die Folgewirkungen in Form von Verzweigungen dargestellt. Voraussetzung für solch eine kausale Modellierung ist eine System- und Funktionsanalyse des Untersuchungsgegenstandes, z.B. eines Informationssystems. Es wird deutlich, dass ein möglichst detailliertes Systemmodell erforderlich ist, um die kausalen Abhängigkeiten zu modellieren.

[170] Vgl FQS (1994), S. 19 ff. und Müller/Tietjen (2000), S. 24 ff.
[171] Vgl. Theil (1995), S. 45-49
[172] Engl.: Fault Tree Analysis (FTA)
[173] Engl.: Event Tree Analysis (ETA)

2.3.2 Top-Down Ansatz

Die Motivation für den Top-Down Ansatz liegt in der fortlaufenden Durchdringung der Informationsverarbeitung und den veränderten Anforderungen an die IS-Sicherheit. Anfang der 60er Jahre bis zu den 80er Jahren hatten nur IT-Spezialisten Zugriff auf die computergestützte Informationsversorgung. Zudem wurde die computergestützte Verarbeitung in zentral abgeschlossenen Bereichen durchgeführt, so dass Sicherheitsinseln und isolierte Teilkonzepte ausreichen[174]. In der unteren Abbildung ist ein Beispiel für die typische Datenverarbeitung dieser Jahre dargestellt.

Abbildung 24: Beispiel einer Datenverarbeitung (IBM 702, 705) der 60er - bis 80er Jahre[175]

Die entstandenen Sicherheitsinseln und Teilkonzepte sind auf kleine Unternehmensbereiche (meist IV-Bereichen) und deren Infrastruktur beschränkt. Es existierten weitgehend proprietäre Insellösungen und physische Schutzmaßnahmen, wie z.B. stabile Zugangstüren oder Überwachungskameras, wobei diese Maßnahmen ausreichten, um ein hohes Maß an Sicherheit zu gewährleisten[176]. Zudem wurden meist bestehende Sicherheitsmaßnahmen des Herstellers integriert. Insgesamt lag kein planerisches und zielgerichtetes Handeln vor. Die Risikoanalyse als Bottom-Up Ansatz wurde im gleichen Zeitraum entwickelt. Diese versucht, die Infrastruktur durch Modelle abzubilden, um deren Risiken zu ermitteln und zu bewerten. Der Bottom-Up Ansatz war deshalb möglich, da alle Elemente des IS und Personen, die auf die Informationsverarbeitung Einfluss hatten, in einem sehr engen und überschaubaren Umfeld „greifbar" waren[177]. Gerber (2001) et al. bezeichnet diese Phase als „Computer-centric era".

Information-centric era

Die Anforderungen für die IS-Sicherheit haben sich ab der 80er Jahre durch die anhaltende quantitative und qualitative Durchdringung der Informationsverarbeitung verändert[178], wobei diese Phase als „Information-centric era" bezeichnet werden kann. Insgesamt gewinnt der Produktionsfaktor[179] und Wettbewerbsfaktor[180] „Information" für Institutionen immer mehr an Bedeutung[181]. Möglich geworden ist diese Weiterentwicklung der Informationsverarbeitung durch die rasant steigende Leistungsfähigkeit der Informationstechnologie bei gleichen

[174] Vgl. Voßbein, J. (1999), S. 219 und Horster/Kraaibeek (2000), S. 8
[175] Vgl. Becaulair (1968), S. 135
[176] Vgl. Solms (1996), S. 282
[177] Vgl. Scanlon (1999), S. 271
[178] Vgl. Voßbein, R. (1995a), S. 10-11
[179] Vgl. Krcmar (2000), S.13
[180] Vgl. Tinnefeld/Ehmann (1998), S. 3
[181] Vgl. Finne (2000), S. 234

oder sinkenden Preisen für die Technologie[182]. Mit dem Siegeszug des PC erfolgte eine Verteilung der Informationen und deren Verarbeitung auf viele Unternehmensbereiche; eine umfangreiche Anzahl von Mitarbeitern erlangte Zugriff auf die Informationsverarbeitung. Dies bezieht sich nicht nur auf die operative Ebene, sondern auch verstärkt auf die Managementaufgaben der taktischen und strategischen Ebenen, die eine hohe qualitative Problemlösungsunterstützung erwarten. Die Informationsverarbeitung ist nicht mehr auf einen bestimmten Unternehmensbereich eingegrenzt, zu dem nur ausgewählte Mitarbeiter Zugang haben. Des Weiteren sind die Komplexität und Vernetzung der Informationsverarbeitung in überhaus hohem Maße angestiegen[183]. Durch diese wachsende Integration der Informationsverarbeitung kann die Beeinträchtigung eines Teilsystems den Zusammenbruch des gesamten Systems zur Folge haben. Eine beschränkte Sicht auf „Insellösungen" ist nicht mehr möglich, sondern es muss das gesamte System betrachtet werden[184].

Durch die Kommunikation und der damit verbundenen Verlagerung wirtschaftlicher Aktivitäten auf die Informationsverarbeitung ist zusätzlich eine neue Dimension des Informationsaustausches über die Unternehmensgrenzen hinausgehend entstanden, die sich durch Dienstleistungen im Internet - wie z.B. durch Versandhandel, Dienstleistung und Auktionen[185] - manifestiert[186]. Hierdurch fordern nicht nur Systembetreiber und -hersteller Sicherheit, sondern auch deren Nutzer, da menschliche Kommunikation immer häufiger technisch vermittelt wird und diese Nutzer ihr Sicherheitsbedürfnis berücksichtigt haben wollen[187]. So sind „Verlässlichkeit" und „Fairness" Voraussetzungen für das Sicherheitsbedürfnis der Teilnehmer des elektronischen Handels. Der Anbieter wird keine Waren vertreiben, wenn keine sichere Bezahlung garantiert ist und der Nutzer des Angebots will, dass die Lieferung nach der Bezahlung garantiert ist[188]. Dies erfordert eine mehrseitige Sicherheit, wodurch unterschiedliche Sicherheitsansprüche gewährleistet werden sollen. „*Mehrseitige Sicherheit bedeutet die Berücksichtigung der Sicherheitsanforderungen aller beteiligten Parteien.*"[189] Nach Pfitzmann besitzt die mehrseitige IS-Sicherheit[190] folgende Grundsätze[191]:

- Jede Partei bzw. Teilnehmer hat sein besonderes Schutz-Ziel.
- Jede Partei bzw. Teilnehmer formuliert sein Schutz-Ziel.
- Sicherheitskonflikte werden erkannt und Kompromisse ausgehandelt.
- Jede Partei bzw. jeder Teilnehmer führt seine Schutz-Ziele innerhalb des ausgemachten Kompromisses durch.

Diesen neuen Anforderungen wird der Bottom-Up Ansatz nicht gerecht, da der Ansatz auf einer Abbildung der internen Infrastruktur basiert, um Risiken zu ermitteln und zu bewerten. Hierfür ist es erforderlich, dass die Infrastruktur „fassbar" ist, was aber wegen des Durchdringungs-, Integrations- und Komplexitätsgrades der Informationsverarbeitung in seiner Gänze

[182] Vgl. Weck (1995), S. 20
[183] Vgl. Murray (1999), S. 219
[184] Vgl. Voßbein, R. (1997), S. 14
[185] Vgl. Scanlon (1999), S. 272; Lepschies (2000), S. 2-4 und Brenner/Lux (2000)
[186] Vgl. Malley (2001), S. 363
[187] Vgl. Rannenberg (1998), S .19
[188] Vgl. Pernul/Röhm/Herrmann (1999), S. 2
[189] Rannenberg (1998), S. 24
[190] Engl.: Multilateral Security
[191] Vgl. Pfitzmann (2001), S. 165

nicht möglich ist. So wurden in den letzten Jahren allgemein akzeptierte IS-Sicherheitskriterienwerke entwickelt, um durch standardisierte Maßnahmen ein einheitliches IS-Sicherheitsniveau von Produkten und Institutionen zu gewährleisten[192]. Zudem erfordert die mehrseitige Sicherheit eine nach außen dokumentierte IS-Sicherheit, um sicherzustellen, dass die angebotene IS-Sicherheit den Sicherheitsansprüchen der Akteure genügt. Es sind folgende Anforderungen an Kriterien und Zertifizierung zu stellen[193]:

- Ein umfassender Bereich der IS-Sicherheit muss durch die Kriterien abgedeckt werden.
- Bei der Zertifizierung müssen die Interessen aller beteiligten Partner berücksichtigt werden.
- Die Prüfergebnisse müssen zugänglich und verständlich sein.

Zudem ist eine unabhängige Evaluation und Zertifizierung auf Basis von Kriterien die Grundlage für Vertrauen, denn Zertifikate vermitteln eine nach außen orientierte IS-Sicherheit[194]. Außerdem wird durch eine neutrale und unabhängige Instanz weitgehend gewährleistet, dass wertvolles Know-how, das während einer Zertifizierung benötigt wird, nicht in die Hände der Konkurrenz gelangt[195].

Die (Informations-)Gesellschaft stellt zusätzliche rechtliche Anforderungen bzgl. der Beherrschbarkeit und Sicherheit der Informationstechnik. Insbesondere der Anspruch auf informationelle Selbstbestimmung - manifestiert im Datenschutzgesetz - zeigt das gesellschaftliche Interesse an einer gesetzlichen Regelung. Der Datenschutz wird durch die oben genannten Veränderungen beeinflusst und muss Antworten auf die neu entstandenen Problemgebiete finden[196]. Ein Gütesiegel für datenschutzfreundliche Produkte auf Basis von Kriterien ist ein Ansatz, den Datenschutz einer Institution nach „außen“ zu dokumentierten. Ist die Bewertung der Evaluationsergebnisse erfolgreich, kann ein Zertifikat bzw. Gütesiegel vergeben werden. Das Zertifikat oder Gütesiegel ist ein nach außen dokumentiertes Datenschutzniveau und stellt ein Kaufkriterium bzw. einen Wettbewerbsvorteil dar[197].

Auch die Behörden verstärken ihre Initiativen, um internetfähige Dienstleistungen online bereitzustellen[198]. Diese Aktivitäten werden unter dem Begriff „E-Government“ zusammengefasst: „*Unter ‚Electronic Government’ (‚E-Government’) verstehen wir* [Bundesamt für Sicherheit in der Informationstechnik] *die Nutzung elektronischer Informations- und Kommunikationstechnik zur Einbeziehung des Kunden in das Handeln von Regierung und öffentlicher Verwaltung*.“[199] Als Kunden einer Behörde sind Bürger, Unternehmen und andere (Partner-) Behörden anzusehen. So verpflichtet sich die Initiative Bund-Online 2005, Dienstleitungen der Bundesverwaltung „online“ verfügbar zu machen. Bei der Realisierung von E-Government sind IS-Sicherheitsaspekte von entscheidender Bedeutung für den Erfolg von Online-Dienstleistungen[200]. Hierbei sind Funktionen, wie z.B. Identifikation, Authentisierung

[192] Vgl. Voßbein, R (1994b), S. 64
[193] Vgl. Rannenberg (1998), S. 26
[194] Vgl. Kersten (1997), S. 323
[195] Vgl. Mackenbrock (2001), S. 341
[196] Vgl. Haaz (1997), S. 33
[197] Vgl. Görtz (1997), S. 321; Röhrig/Knorr/Noser (2000), S. 499 und Diek (2002), S. 159
[198] Vgl. Traummüller/Lenk/Wimmer (2001), S. 381 und E-Government-Handbuch-Vortrag (2001)
[199] E-Government-Handbuch-Glossar (2002), S. 3
[200] Vgl. Dridi/Pernul/Sabol (2001), S. 406

oder Public-Key Verfahren, nötig, um ein hohes Maß an Sicherheit zu bieten. Das E-Government Handbuch bietet auf Basis der BSI-Grundschutzmaßnahmen verschiedene Vorschläge zum sicheren Internetauftritt bzgl. des E-Governments[201].

Durch den Top-Down Ansatz werden unternehmensunabhängig Kriterien aus unterschiedlichsten Bereichen auf die entsprechende Institution direkt angewendet, indem die vergleichbaren Kriterienbereiche ausgewählt werden. Im Gegensatz zu den Bottom-Up Ansätzen bieten die Top-Down Ansätze somit eine nach „außen" dokumentierte IS-Sicherheit, da der Ansatz auf anerkannten Kriterien basiert. Dies bedeutet, dass bei einer unabhängigen Evaluation die IS-Sicherheit zertifiziert werden kann. IS-Sicherheitskriterien sind daher eng verbunden mit der unabhängigen Evaluation und Zertifizierung von Systemen und Produkten[202]. Dieses Zertifikat kann durch „Kunden" oder „Bürger" wahrgenommen werden, die sich ein Bild über die IS-Sicherheit des „Gegenübers" machen können. Der Bottom-Up Ansatz dagegen ist ein Individualansatz, der nicht nach außen dokumentiert werden kann, da er nicht auf einer allgemein anerkannten Grundlage bzw. auf allgemein anerkannten Kriterien basiert[203].

Maßnahmenorientierter IS-Sicherheitsbegriff

Der Top-Down Ansatz ist durch den maßnahmenorientierten IS-Sicherheitsbegriff geprägt, da die Sicherheit von der Existenz und Anwendung der entsprechenden Maßnahmen-Kriterien abhängt. Hierbei wird auf eine detaillierte Dekomposition des Informationssystems - wie bei dem Bottom-Up Ansatz - weitgehend verzichtet. Es werden basierend auf IS-Sicherheitskriterien erforderliche Maßnahmen ermittelt. Der Ansatz beruht darauf, dass, wenn die erforderlichen Sicherungsmaßnahmen eingesetzt werden, von einem „zuverlässigen" Informationssystem ausgegangen werden kann. Werden Maßnahmen nicht vollständig und wirkungsvoll eingesetzt, ist von Sicherheitslücken bzw. Schwachstellen auszugehen[204]. Dabei ist der Grad von „Sicherheit" nur eine Richtgröße, da der Einfluss der Maßnahmen für die Sicherheit nicht zuverlässig determiniert werden kann[205]. Die IS-Sicherheits-Schwachstellenanalyse (SiSSA) ist eine Methode für diese Top-Down Vorgehensweise.

Ein Nachteil der maßnahmenorientierten Sichtweise liegt in dem geringen reaktiven Bereich, denn Maßnahmen werden häufig erst beim Auftauchen von Gefahren entwickelt und die schon bestehenden Maßnahmen können eventuell nicht vor den neuen Gefahren schützen. Es ist ersichtlich, dass in dieser „Zeitlücke" das Informationssystem der Gefahr schutzlos ausgesetzt ist. Dieser Zusammenhang wird in der folgenden Abbildung dargestellt.

[201] Vgl. E-Government-Handbuch-Internetauftritt (2002)
[202] Vgl. Winzler/Holbein (1996), S. 269
[203] Vgl. Solms (1996), S. 283
[204] Vgl. Stelzer (1993), S. 212 und Voßbein, J. (1999), S. 38 f.
[205] Eine Aussage, dass beim Fehlen von 10% der Maßnahmen eine Sicherheit von 90% gegeben ist, ist nicht möglich.

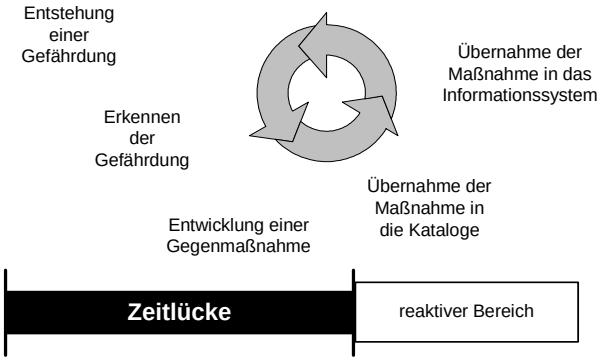


Abbildung 25: Zeitlücke beim maßnahmenbasierten Sicherheitsbegriff[206]

Aus diesem Grund ist ein umfassender und aktueller Maßnahmenkatalog entscheidend für die Anwendung des maßnahmenbasierten Sicherheitsbegriffs. Ansonsten entsteht schnell eine „Scheinsicherheit“ des Informationssystems. Es ist permanent zu prüfen, ob die standardisierten Maßnahmen für die jeweilige Institution ausreichen oder durch individuelle Maßnahmen ergänzt werden müssen.

2.3.2.1 IS-Sicherheitskriterien

In der Tabelle erfolgt eine Differenzierung der Kriterien nach folgender Struktur[207]:

- Das Kriterienwerk bezieht sich auf ein einzelnes Produkt bzw. auf eine Komponente oder die Sicht ist auf die Einsatzumgebung im Kontext des Gesamtsystems einer Institution gerichtet.
- Die Kriterien sind entweder auf technische oder auf nicht-sicherheitsrelevante (z.B. organisatorische) Aspekte fokussiert.

[206] Erweitert in Anlehnung an Voßbein, J (1999), S. 39
[207] Vgl. D21 (2001), S. 7. Eine ähnliche Struktur findet sich bei Eloff/Solms (2000b)[207]

systembezogen		BSI IT-Grundschutz (grundlegende Absicherung des Gesamtsystems)	ISO 13335 (Handreichungen für das IS-Sicherheitsmanagement)
			ISO 17799 („Best Practice Ansatz“ in der IS-Sicherheit)
			ISO 9000 (allgemeine Anforderungen an ein Qualitätsmanagementsystem)
			CobiT (Etablierung eines geeigneten Kontrollumfeldes)
produktbezogen	BSI Task Force (Maßnahmenkatalog für ein sicheres Internet)	Datenschutzaudit	
	ITSEC/ Common Criteria (technische Prüfkriterien für Produkte und Systeme)		
	NIST FIPS (Validierung von Krypto-Modulen)		
	ECMA E-COFC (Extended Commercially Oriented Functionality Class for Security Evaluation)		
	technisch		**nicht-technisch**

Tabelle 5: Differenzierte Zusammenstellung der Kriterienwerke[208]

Die Einteilung in produktorientierte und system- bzw. umgebungsorientierte Sicht zeigt die Extrempositionen für den Einsatz von Kriterien. Eine umfangreiche Verwendung von Kriterien erfolgt durch einen kombinierten bzw. ergänzenden Einsatz der erforderlichen Bestandteile von Kriterienwerken. So können z.B. einzelne Verfahren bzw. Prozesse in einer konkreten Einsatzumgebung mit Hilfe von systembezogenen Kriterien analysiert werden oder zertifizierte Produkte können eine Voraussetzung für eine sichere umgebungsorientierte Sicht bilden.

IT-Grundschutz bzw. IT-Baseline des BSI

Ziel des IT-Grundschutzes ist es, durch infrastrukturelle, organisatorische, personelle und technische Standard-Sicherheitsmaßnahmen ein mittleres Sicherheitsniveau für IT-Systeme aufzubauen, das auch für sensible Bereiche ausbaufähig ist. Zum Schutz der Infrastruktur sind Grundschutz- bzw. Baseline-Maßnahmen[209] häufig ausreichend, wenn es sich um standardisierte IT-Systeme handelt[210]. Das folgende Schichtmodell strukturiert die Maßnahmenbereiche.

[208] Erweitert in Anlehnung an D21 (2000), S. 7
[209] Vgl. Pongratz (1996), S. 233 und Schaurette (1999), S. 237 f.
[210] Vgl. Gerber/Solms (2001), S. 583

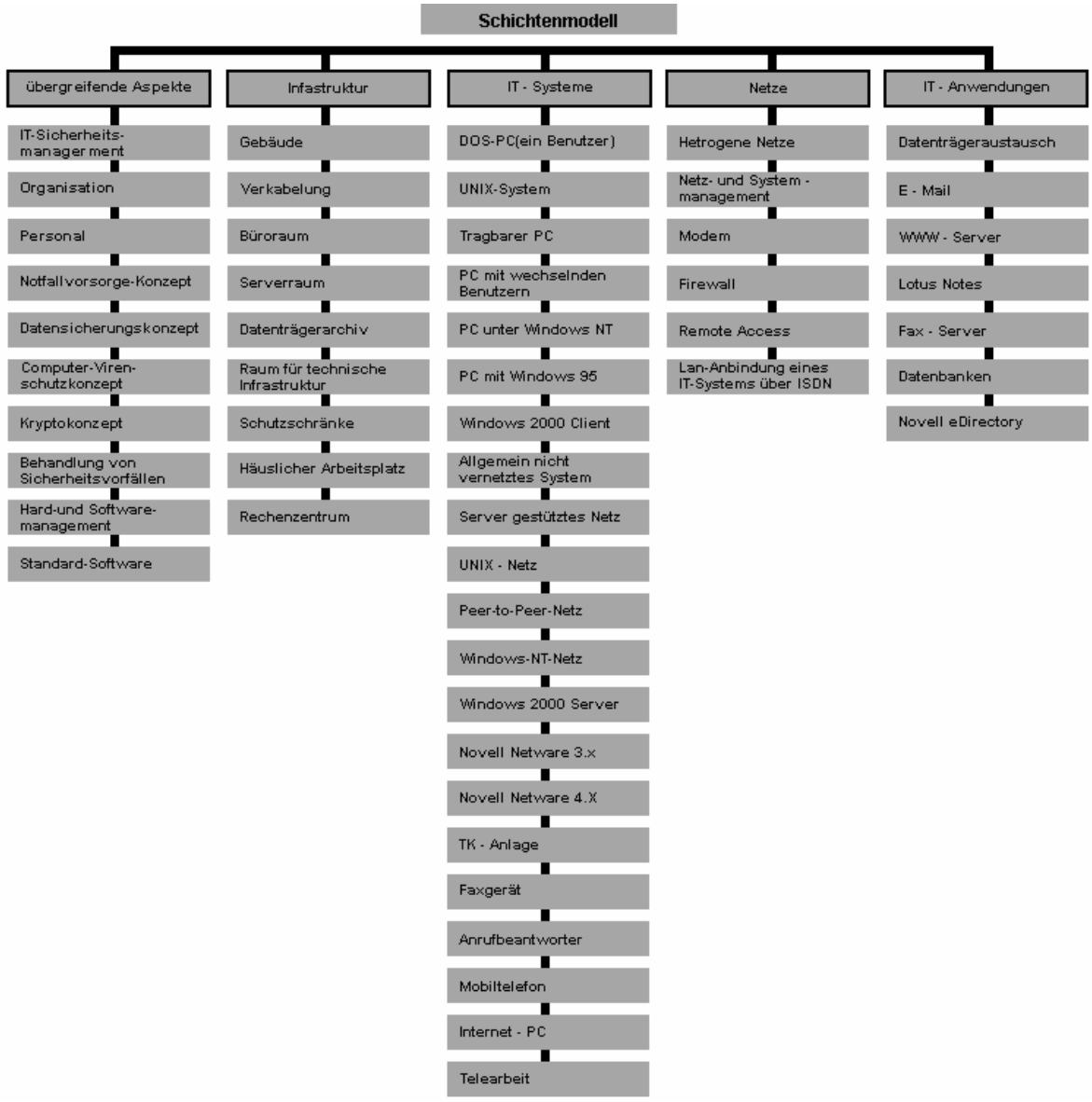


Abbildung 26: Schichtenmodell des BSI-Grundschutzhandbuchs[211]

Jedem IT-Baustein des Schichtenmodells sind mögliche Gefahren und Gegenmaßnahmen zugeordnet. Sind die geforderten Maßnahmen des Grundschutzes erfüllt, ist ein gewisses Maß an IS-Sicherheit vorhanden. Falls ein hoher Grad an IS-Sicherheit für die Bereiche der Infrastruktur benötigt wird, können die Risiken individuell ermittelt werden, um Maßnahmen anzupassen. Eine umfangreichere Beschreibung der Struktur und Anwendung des BSI-Grundschutzes erfolgt im Kapitel 2.3.3.

[211] Veröffentlicht im Internet, URL: http://www.bsi.de/gshb/deutsch/menue.htm (Stand: 10.12.2002)

BS 7799/ISO 17799 (Code of Practice (CoP))

Der CoP „*…entstand aus dem Bedürfnis von Handel und Industrie nach einfach einsetzbaren Sicherheitsstandards*“[212]. Dieser „Code of Practice“ wurde in mehreren Schritten in einen British Standard (BS) 7799 umgesetzt und im Jahre 2000 als internationaler Standard ISO/IEC 17799 veröffentlicht.

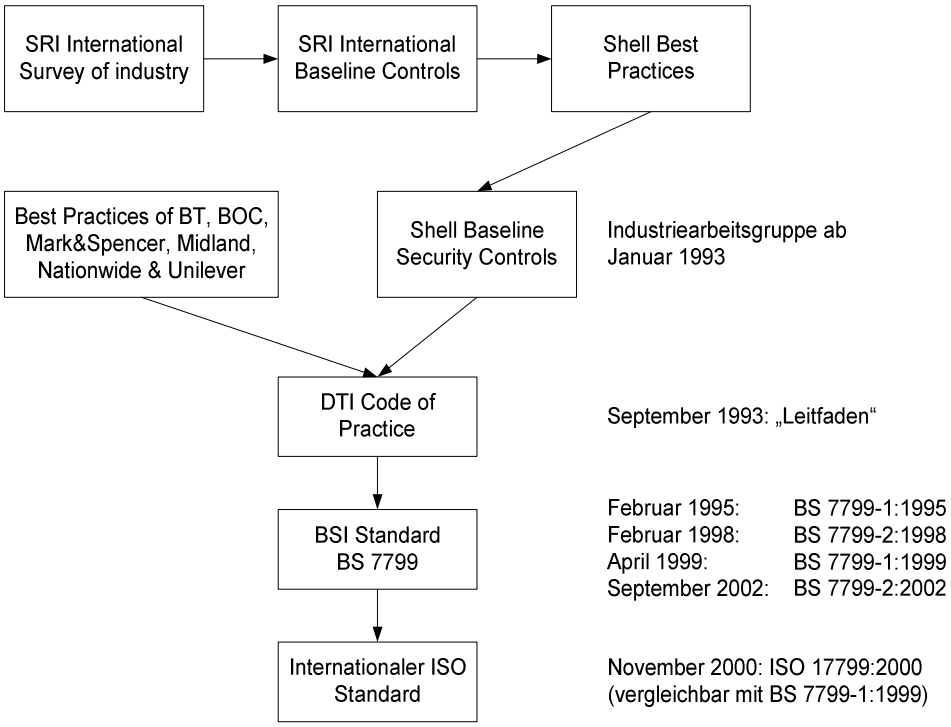


Abbildung 27: Entstehungsgeschichte des BS 7799/ISO 17799[213]

Der CoP bietet einen praxisorientierten und unternehmensunabhängigen Maßnahmenkatalog, der dem „Best Practice Ansatz“ in der IS-Sicherheit genügt. Es wird davon ausgegangen, dass sich in der Praxis eine Vielzahl von bewährten bzw. vorbildlichen „Praktiken“ bzw. Maßnahmen entwickelt hat, die die Grundlage für andere Institutionen darstellt[214]. Durch die pragmatische, praxis- und maßnahmenbezogene Vorgehensweise des CoP-Ansatzes liegt der Vorteil in der Umsetzbarkeit und der Einsparung von Kosten. Die Hauptanwendung beruht auf der Erstellung eines Sicherheitskonzeptes, was eine Studie vom Herbst 1997 der Information Systems Audit and Control Association (ISACA) belegt[215]. Ähnliches erreicht der Baseline Security Policy (BSP) Ansatz, der auch auf Basis von bewährten Management-„Regeln“ und Standard-Kriterien ein „Grundmaß“ an Sicherheit gewährleisten will[216].

[212] ISACA (1998), S. 7
[213] Aktualisiert in Anlehnung an ISACA (1998), S. 7 und Götze/TÜV (2002), S. 11
[214] Vgl. Konrad (1998) und Eloff/Solms (2000a), S. 250. Zieschang (2001) bietet z.B. ein Best Practice Ansatz für den IS-Sicherheitsbereich „E-Commerce“
[215] Vgl. ISACA (1998), S. 29
[216] Vgl. Gritzalis (1997), S. 713

Teil 1 der BS 7799[217] bzw. ISO 17799[218] beinhaltet einen Leitfaden zum Management von Informationssicherheit mit folgenden Maßnahmenbereichen:

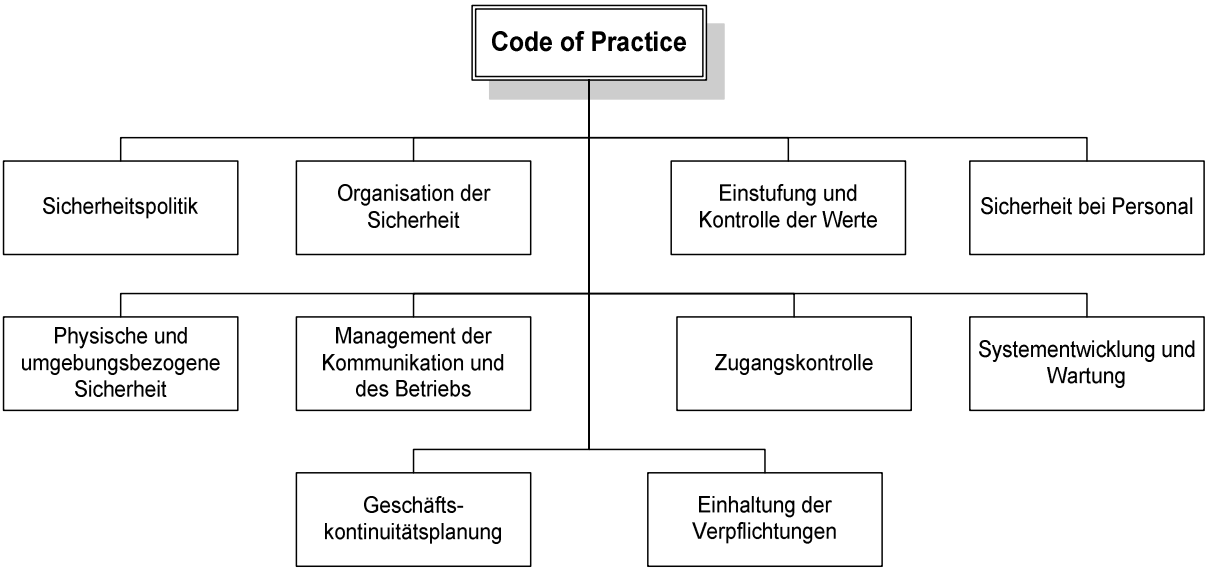


Abbildung 28: Struktur des BS 7799-1

Der zweite Teil des BS 7799 (BS 7799-2:1998[219]) dient zur Spezifikation eines „Information Security Management Systems“ und bildet eine Zertifizierungsgrundlage[220], wobei dieser Teil nicht in die ISO 17799:2000 eingegangen ist. Im September 2002 wurde ein überarbeiteter und aktualisierter BS 7799-2:2002[221] veröffentlicht, der hinsichtlich der ISO 9001:2000 harmoniert worden ist[222]. In der folgenden Tabelle erfolgt eine Gegenüberstellung der BS 7799-2:1998, BS 7799-2:2002 und ISO 9001:2000.

[217] Vgl. BS 7799-1 (1999)
[218] Vgl. ISO 17799 (2000)
[219] Vgl. BS 7799-2 (1998)
[220] Vgl. Eloff/Solms (2000a), S. 250 und c:cure (2002)
[221] Vgl. BS 7799-2 (2002)
[222] Vgl. c:cure (2002)

BS 7799-2:1999	BS 7799-2:2002	ISO 9001:2000
	0 Introduction	0 Introduction
1 Scope	1 Scope	1 Scope
	2 Normative references	2 Normative references
2 Terms and definitions	3 Terms and definitions	3 Terms and definitions
.	.	.
.	.	.
.	.	.
3 Information security management system requirements	4 Information Security management system	4 QMS requirements
3.1 General	4.1 General requirements	4.1 General requirements
3.2 Establishing a management framework	4.2 Establishing and managing the ISMS	
	4.2.1 Establish the ISMS	
3.3 Implementation	4.2.2 Implement and operate the ISMS	
	4.2.3 Monitor and review the ISMS	
	4.2.4 Maintain and improve the ISMS	
3.4 Documentation	4.3 Documentation requirements	4.2 Documentation requirements
	4.3.1 General	4.2.1 General
3.5 Document control	4.3.2 Control of documents	4.2.3 Control of documents
3.6 Records	4.3.3 Control of records	4.2.4 Control of records
-	5 Management responsibility	5 Management responsibility
-	5.1 Management commitment	5.1 Management commitment
-	5.2 Resource management	6 Resource management
-	6 Management review	5.6 Management review
-	6.1 General	5.6.1 General
-	6.2 Review input	5.6.2 Review input
-	6.3 Review output	5.6.3 Review output
-	6.4 Internal ISMS audits	8.2.2 Internal audits
-	7 ISMS improvement	8 Improvement
-	7.1 Continual improvement	8.5.1 Continual improvement
-	7.2 Corrective action	8.5.2 Corrective actions
-	7.3 Preventive action	8.5.3 Preventive actions
4 Detailed Controls	Annex A Control objectives and controls	
-	A.1 Introduction	
-	A.2 Guidance an best practice	
4.1 Security policy	A.3 Security policy	
4.2 Organisational security	A.4 Organisational security	
4.3 Asset classification and control	A.5 Asset classification and control	
4.4 Personnel security	A.6 Personnel security	
4.5 Physical and environmental	A.7 Physical and environmental security	
4.6 Communications and operations management	A.8 Communications and operations management	
4.7 Access control	A.9 Access control	
4.8 System development and	A.10 System development and maintenance	
-	Annex B Guidance on the use of the standard	
-	Annex C Correspondence between ISO 9001:2000, ISO 14001:1996 and BS 7799 Part 2:2002	Annex A Links between ISO 14001 and ISO 9001

Tabelle 6: Gegenüberstellung der BS 7799-2:1998, BS 7799-2:2002 und ISO 9001:2000[223]

Ziel der ISO 9000 Standard Serie[225] ist es, ein Prüfverfahren zu definieren, in dem Forderungen an ein Qualitätsmanagementsystem festgelegt werden. Das Prüfverfahren dient zur Darlegung des Qualitätsmanagements einer Organisation zur Erfüllung der Qualitätsforderungen der Kunden sowie der Beurteilung und Dokumentation durch interne und externe Stellen. Dieses Prüfverfahren lässt sich z.T. auf den IS-Sicherheitsbereich anwenden (siehe BS 7799-2:2002)[226].

[223] Vgl. Humphreys (2002), S. 7
[225] Vgl. ISO 9000 (2000)
[226] Vgl. Solms (1996), S. 284

ISO 13335

Die „Suite“ gibt Handreichungen für das IS-Sicherheitsmanagement, ohne bestimmte Lösungen zu erzwingen. Es besteht aus folgenden Bereichen: „Konzepte und Modelle der IT-Sicherheit“[227], „Managen und Planen von IT-Sicherheit“[228], „Techniken für das Management von IT-Sicherheit“[229], „Auswahl von Sicherheitsmaßnahmen“[230] und „Netzwerksicherheit“[231]. Die „General Management Guidelines for Information Security“ der ISO 13335 beschreibt einen fortlaufenden Sicherheitsmanagementprozess[232].

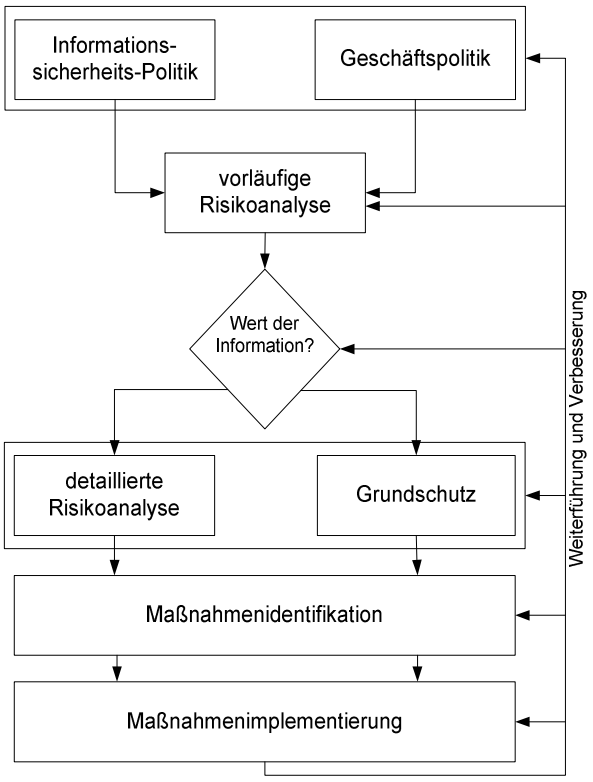


Abbildung 29: Informationsmanagement nach ISO 13335[233]

Ausgehend von der Informationssicherheits- und Geschäftspolitik wird für das zu untersuchende Informationssystem eine vorläufige Risikoanalyse durchgeführt, wobei die Wertbestimmung der Bestandteile des Informationssystems das Ziel darstellt. Aufgrund der „Wertbestimmung“ erfolgt für sensible Bereiche eine detaillierte Risikoanalyse und für die anderen Bereiche wird ein Grundschutz entwickelt. Auf Basis der Risikoanalyse und des Basisschutzes werden Maßnahmen identifiziert und implementiert.

Diese Vorgehensweise ist in dem BSI-Grundschutzhandbuch bzw. in der IT-Baseline zu finden, die auch als „Grundschutz+X“ bezeichnet wird, wobei X für eine zusätzliche IS-Sicherheitsanalyse (z.B. durch Risikoanalyse) steht. Hierbei erfolgt eine Wertbestimmung, die beim BSI- Grundschutzhandbuch als Schutzbedarfsfeststellung bezeichnet wird. Es folgt eine

[227] Vgl. ISO 13335-1 (1996)
[228] Vgl. ISO 13335-2 (1997)
[229] Vgl. ISO 13335-3 (1998)
[230] Vgl. ISO 13335-4 (2000)
[231] Vgl. ISO 13335-5 (2001)
[232] Vgl. Plate (1997), S. 370
[233] Vgl. RSD (1999), S. 28

Trennung in eine Risikoanalyse z.B. gemäß dem BSI-Sicherheitshandbuch oder dem Grundschutz z.B. bezüglich des BSI-Grundschutzhandbuches.

Common Criteria (CC)

Die CC-Evaluationskriterien beinhalten Prüfverfahren für sicherheitsrelevante Aspekte von IT-Produkten und IT-Systemen, die als Evaluationsgegenstände (EVG) bezeichnet werden. Die EVG können auf Basis der CC-Kriterien strukturiert untersucht werden, so dass die Ergebnisse nachvollziehbar sind. Die CC beschreibt zudem, wie für alle gängigen IT-Produkte bzw. -Systeme Prüfungen in Form von Schutzprofilen oder Sicherheitsvorgaben zusammengestellt werden können[234]. In der unteren Abbildung ist die Entstehungsgeschichte der CC dargestellt. Wie zu erkennen ist, wurde die CC von Kriterien aus unterschiedlichen Ländern beeinflusst, wie z.B. die TCSEC[235]/Orange Book (USA), ITSEC (Deutschland) und CTCPEC[236] (Kanada).

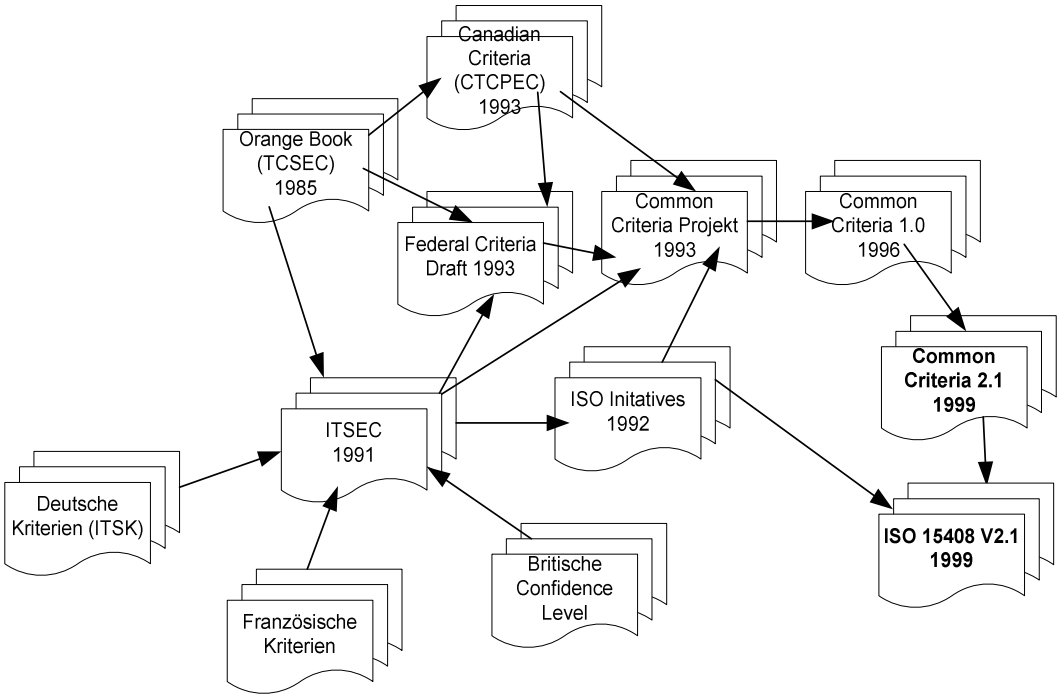


Abbildung 30: Übersicht zur Entstehungsgeschichte der Common Criteria (CC)[237]

Die CC ist in der Version 2.1 als eine internationale ISO 15408 verabschiedet worden[238], die auf den folgenden drei Teilen der CC basiert: „Einführung und allgemeines Modell“[239], „Funktionale Sicherheitsanforderungen“[240] und „Anforderungen an die Vertrauenswürdigkeit“[241]. In dem ersten Teil werden die CC allgemein und deren Anwendung beschrieben. Hierfür werden implementierungsunabhängige Schutzprofile (PP[242]) eingeführt, die Lösungen für Standard-Sicherheitsprobleme einer bestimmten Produktgruppe darstellen. Die Sicher-

[234] Vgl. Mackenbrock (1999), S. 94
[235] TCSEC = Trusted Computer Systems Evaluation Criteria
[236] CTCPEC = Canadian Trusted Computer Product Evaluation Criteria
[237] Erweitert in Anlehnung an http://www.commoncirteria.org/docs/origins.html (Stand: 10.12.2002)
[238] Vgl. ISO 15408-1 (1999), 15408-2 (1999) und 15408-3 (1999)
[239] Vgl. CC-Teil 1 (2000)/ ISO 15408-1 (1999)
[240] Vgl. CC-Teil 2 (2000)/ ISO 15408-2 (1999)
[241] Vgl. CC-Teil 3 (2000)/ ISO 15408-3 (1999)
[242] Engl.: Protection Profile

heitsvorgaben (ST[243]) dienen der Prüfung und Bewertung des konkreten EVG. Die ST für einen konkreten EVG können durch Verweis auf ein PP oder direkt auf Basis von funktionalen Vertrauenswürdigkeitskomponenten der CC erstellt werden.

Der zweite Teil der CC beschreibt Funktionalitätsanforderungen, die für einen EVG spezifiziert werden können. Für die Sicherheitsprotokollierung sind z.B. kryptographische Unterstützung, Schutz der Benutzerdaten, Zugriffskontrollpolitik, Authentisierung oder Identifikation zu nennen. Der dritte Teil der CC stellt Anforderungen an die Vertrauenswürdigkeit und beruht auf frühere Kriterien, wie die TCSEC oder ITSEC[244]. Die Anforderungen sind in Vertrauenswürdigkeitsklassen wie Konfigurationsmanagement, Auslieferung und Betrieb, Entwicklung, Testen oder Handbücher eingeteilt, die wiederum durch Vertrauenswürdigkeitsfamilien verfeinert werden. Für die Bewertung der Vertrauenswürdigkeit werden sieben Vertrauenswürdigkeitsstufen (EAL[245] 1-7) verwendet, die eine ansteigende Skala darstellen. Je höher die Vertrauenswürdigkeitsstufen sind, umso mehr Vertrauenswürdigkeitskomponenten sind erforderlich.

FIPS (Federal Information Processing Standards)[246]

Die von der NIST herausgegebenen FIPS haben die Validierung von Krypto-Modulen als Ziel. Da gewisse US-Regierungsstellen den Einsatz von FIPS-zertifizierten Produkten vorschreiben, stellen FIP-Standards auf dem US-Markt eine hohe Bedeutung dar. Vor allem folgende FIP-Standards sind von Relevanz[247]:

- FIPS 46-3 Data Encryption Standard (DES)[248]
- FIPS 186-2 Digital Signature Standard (DSS)[249]
- FIPS 180-1 Secure Hash Standard (SHA)[250]
- FIPS 197 Advanced Encryption Standard (AES)[251]

Bei den vier Standards handelt es sich wesentlich um Implementierungsstandards für kryptographische Algorithmen. Dagegen bilden die FIPS 140-1[252] und FIPS 140-2[253] einen Standard zur Evaluierung von Qualität und Stärke von kryptographisches Modulen (kurz: Krypto-Module), z.B. Hardware-Sicherheitsmodule. Im Jahre 1994 wurde die FIPS-1 veröffentlicht und mit der FIPS-2 wurde 2001 ein überarbeiteter und erweiterter Standard präsentiert[254]. Ein Krypto-Modul kann eine Hardware, Software, Firmware oder eine Kombination sein, welche kryptographische Algorithmen und optional eine Schlüsselgenerierung beinhaltet. Es besitzt definierte physische Eingangs- und Ausgangsports sowie logische Schnittstellen (Interfaces). Für jedes Krypto-Modul existieren rollenbasierte Authentifizierungen und für höhere Sicherheitsstufen identitätsbasierte Erweiterungen. Zusätzlich sollten Standarddienste, wie z.B. eine

[243] Engl.: Security Target
[244] Vgl. Mackenbrock (2001), S. 344
[245] Engl.: EAL = Evaluation Assurance Level
[246] Die Standards der FIPS sind unter der URL: http://csrc.nist.gov/publications/fips veröffentlicht.
[247] Vgl. Churley (2002), S. 75
[248] Vgl. FIPS 46-3 (1999)
[249] Vgl. FIPS 186-2 (2000)
[250] Vgl. FIPS 180-1 (1995)
[251] Vgl. FIPS 197 (2001)
[252] Vgl. FIPS 140-1 (1994)
[253] Vgl. FIPS 140-2 (2001)
[254] In Snouffer/Lee/Oldehoeft (2001) sind die wesentlichen Veränderungen der FIPS 140-2 erläutert.

Statusausgabe oder ein Selbsttest des Krypto-Moduls, angeboten werden. Abhängig von der Sicherheitsstufe des Krypto-Moduls sollten physische Sicherheitsaspekte, wie eine physische „Ummantelung“, die einen unerlaubten Zugriff wahrnehmbar macht oder ein automatisches Zurücksetzen von sicherheitsrelevanten Informationen, vorhanden sein. Als Sicherheitsvoraussetzung werden zusätzlich ausreichende Tests, Dokumentationen sowie Konfigurations- und Installationsunterstützungen vorausgesetzt. Die Krypto-Module sollten außerdem Angriffe „abschwächen“ können, die nicht während der Entwicklung bekannt waren. Die FIPS 140 beinhalten folgende Anforderungs- bzw. Sicherheitsstufen:

- Grundlegende Sicherheit (Sicherheitsstufe 1)
  Auf dieser Stufe werden die grundlegenden Anforderungen an ein Krypto-Modul festgelegt, die auch ein Mindestmaß an Sicherheit bieten. Diese Form der Sicherheit kann eingesetzt werden, wenn keine zusätzliche physisch-, netzwerk- oder administrationsorientierte Sicherheit verfügbar ist. Ein Beispiel für Produkte der Stufe 1 ist das „encryption board“ von PC, das aber keinen zusätzlichen physischen Schutz beinhaltet.
- Manipulationsnachweis durch physische Ummantelung (Sicherheitsstufe 2)
  Es wird zusätzlich eine physische „Ummantelung“ der Krypto-Module verlangt. Somit sind „physische Veränderungen“ erkennbar[255]. Es wird zudem eine rollenbasierte Authentifizierung verlangt, damit bestimmte sicherheitsrelevante Dienste angeboten werden können. Auch sollen die Anforderungen der CC an einen PP berücksichtigt werden[256] und die Vertrauenswürdigkeitsstufen 2 (EAL2) oder höher der CC erfüllt werden.
- Manipulationssicherheit: Das Modul wird gegenüber physischen Attacken aktiv geschützt (Sicherheitsstufe 3).
  Es werden zusätzliche physische Maßnahmen benötigt, die einen physischen Angriff erkennen und aktive Gegenmaßnahmen einleiten, wie z.B. die Zurücksetzung aller Klartext-CPS (zeroization). Die rollenbasierte Authentifizierung wird durch eine identitätsbasierte Authentifizierung ersetzt, die nur eindeutige identifizierte Benutzer autorisiert, eine spezifische Rolle einzunehmen. Zusätzlich müssen die Vertrauenswürdigkeitsstufen 3 (EAL3) oder höher der CC erfüllt werden.
- Erweiterte Manipulationssicherheit: Aktives Erkennen und Reagieren gegen Manipulationsversuche (Sicherheitsstufe 4).
  Zusätzlich werden Gefährdungen durch Umwelteinflüsse oder Veränderungen der Arbeitsumgebung, wie Spannung oder Temperatur, erkannt und geeignete Gegenmaßnahmen aktiviert. Level 4 Module können in Umgebungen eingesetzt werden, die sonst keinen physikalischen Schutz aufweisen. Zusätzlich müssen die Vertrauenswürdigkeitsstufen 4 (EAL4) oder höher der CC erfüllt werden.

CC-Kriterien und die folgende E-COFC decken im Vergleich zu den FIPS eine breitere Produktpalette sowie unterschiedlichere IS-Sicherheitsaspekte ab, wohingegen FIPS 140-2 auf die Evaluation von Krypto-Modulen spezialisiert ist.

[255] Die physischen Veränderungen können z.B. durch einen physischen Zugriff und einer physischen Manipulation an den Kryptographieschlüsseln und den kritischen Sicherheitsparametern (Critical Security Parameters = CPS) erfolgen.
[256] Vgl. CC-Teil 1 (2000), Anhang B, S. 43-48

E-COFC (Extended Commercially Oriented Functionality Class for Security Evaluation)

E-COFC bzw. ECMA-271 wird als kommerzieller IS-Sicherheits-Standard für vernetzte „Geschäftssysteme“ 1999 durch die European Computer Manufactures Association (ECMA) veröffentlicht und ist eine Erweiterung der 1993 veröffentlichten COFC bzw. ECMA-205. ECMA wurde 1961 gegründet und stellt einen Zusammenschluss von über 20 festen Mitgliedern, wie z.B. Apple, Dell, Hewlett Packard, IBM, Intel, Microsoft oder Sony und weiteren assoziierten und Not-for-profit Mitgliedern, wie z.B. AOL, Siemens, NIST, TU-Dresden, dar. Die Aufgabe der ECMS besteht in der Erstellung von Standards und technischen Reports für kommerzielle Informations- und Kommunikations-Technologien[257].

Das Ziel der E-COFC[258] besteht im sicheren Datenaustausch in einer kommerziellen Geschäftsumgebung, wobei die Evaluation von IT-Produkten auf Kriterien basiert, welche unabhängig von einer speziellen Hardware oder einer Softwareplattform erarbeitet worden sind. Hierbei wird zwischen den folgenden Sicherheitsklassen von kommerziellen Umgebungen unterschieden.

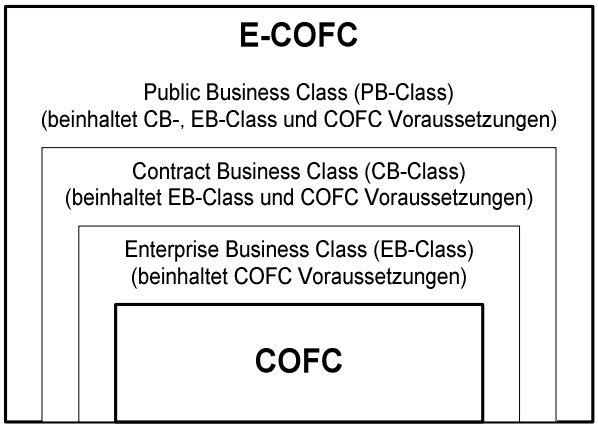


Abbildung 31: Hierarchische Klassen der E-COFC[259]

- Bei der EB-Klasse erfolgt die Kommunikation nur zwischen Mitarbeitern innerhalb einer Institution; somit ist auch nur eine Instanz verantwortlich für die Geschäftsvorgänge.
- Bei der CB-Klasse erfolgen Geschäftsvorgänge zwischen mehreren unabhängigen Institutionen, wobei eine geschlossene Nutzergruppe besteht, denn an der Kommunikation können nur Institutionen teilnehmen, die eine vorher definierte Form der Geschäftsvorgänge und Sicherheitsregeln akzeptieren.
- Bei der PB-Klasse existiert keine geschlossene Nutzergruppe mehr, da die Kommunikation in einer offenen Umgebung erfolgt. Diese Umgebung ist z.B. ein internetbasierter Marktplatz für den Handel verschiedener Güter oder die Bereitstellung internetbasierter Dienstleistungen.

Abhängig von der Sicherheitsklasse werden unterschiedliche Voraussetzungen bzgl. der IS-Sicherheit an den Evaluationsgegenstand gestellt. Die Kriterien für die aufbauenden Sicherheitsklassen werden in folgende Bereiche strukturiert:

[257] Es gibt über 335 ECMS-Standards und 85 technische Reports. URL: http://www.ecma.ch (Stand: 03.02.2003)
[258] Vgl. E-COFC (1999), S. 3
[259] Vgl. E-COFC (1999), S. 6

- Allgemeine kommerzielle Sicherheitsaspekte der jeweiligen Sicherheitsklassen.
- Gegenüberstellung von Gefahren und möglichen Gegenmaßnahmen (ähnlich wie bei dem BSI-Grundschutz) der jeweiligen Sicherheitsklasse.
- Funktional orientierte IS-Sicherheitsaspekte der jeweiligen Sicherheitsklasse, die eine Erweiterung des funktional orientierten IS-Sicherheitsstandards COFC bzw. ECMA-205 darstellen.

Task Force Sicheres Internet des BSI[260]

Die Aufgabe der Task Force ist die Erstellung eines Maßnahmenkatalogs für ein sicheres Internet. Insbesondere die Koordination von Maßnahmenkatalogen aus der Wissenschaft, Wirtschaft und aus Behörden ist die Aufgabe der Task Force. Anfang 2003 standen folgende Maßnahmenkataloge zur Verfügung:

- Empfehlung zum Schutz vor verteilten Denial of Service Angriffen im Internet[261].
- Empfehlungen zum Schutz vor Computer-Viren aus dem Internet, wobei die Empfehlungen insbesondere für den Schutz von Microsoft Windows- und Office-Produkten ausgelegt sind[262].

Die Maßnahmenkataloge bieten zunächst eine Einführung in die oben genannten Problembereiche und anschließend konkrete Maßnahmen-Empfehlungen an. Die Maßnahmen sind unterteilt in:

- Endanwender-Maßnahmen: Private Nutzer, die überwiegend Informationen aus dem Internet abrufen, um sie zu verarbeiten,
- Administratoren/Netzvermittler-Maßnahmen: Verwalter und Betreuer von Rechnern und Netz-Infrastrukturen,
- Software-Hersteller/Server-Betreiber-Maßnahmen: Hersteller von Betriebssystem- und Anwendungs-Programmen sowie Betreiber von Diensten im Internet (WWW-Server, DNS-Server usw.) und
- Inhalt-Anbieter Maßnahmen: Produzenten von redaktionellen Inhalten, die im WWW bereitgestellt werden.

CobiT (Control Objectives for Information and Related Technology)

CobiT[263] wurde durch die Information Systems Audit and Control Association (ISACA)[264] entwickelt, welche 1969 unter dem Namen EDP Auditors Foundation gegründet worden ist. ISACA ist heute eine weltweite Verbindung von ca. 24.000 IS-Fachleuten[265], die sich mit der Revision, Kontrolle und Sicherheit von der IS befassen[266]. CobiT ist ein Kontrollsystem für das IS-Management. Es dient der Erreichung und Sicherstellung von Geschäftszielen (unter den klassischen Sicherheitsanforderungen Vertraulichkeit, Integrität, Verfügbarkeit sowie

[260] Vgl. auch URL: http://www.bsi.de/taskforce/index.htm
[261] Vgl. Task-Force-DDoS (2000)
[262] Vgl. Task-Force-Virenschutz (2000)
[263] Ist seit 2000 als 3. Edition verfügbar. Vgl. Cobit (2001), Kapitel B
[264] Vgl. auch URL: http://www.isaca.org
[265] Stand 2001
[266] Vgl. Cobit (2001)

Wirtschaftlichkeit, Wirksamkeit, Einhaltung rechtlicher Erfordernisse und Zuverlässigkeit)[267]. Das CobiT-Framework basiert auf einem IT-Prozess, der 34 zentrale IT-Prozesse zu vier Domänen zusammenfasst. Durch die Umsetzung des CobiT-Frameworks soll unter Berücksichtigung der oben genannten Ziele eine Bereitstellung der Ressource „Information“ sichergestellt werden[268].

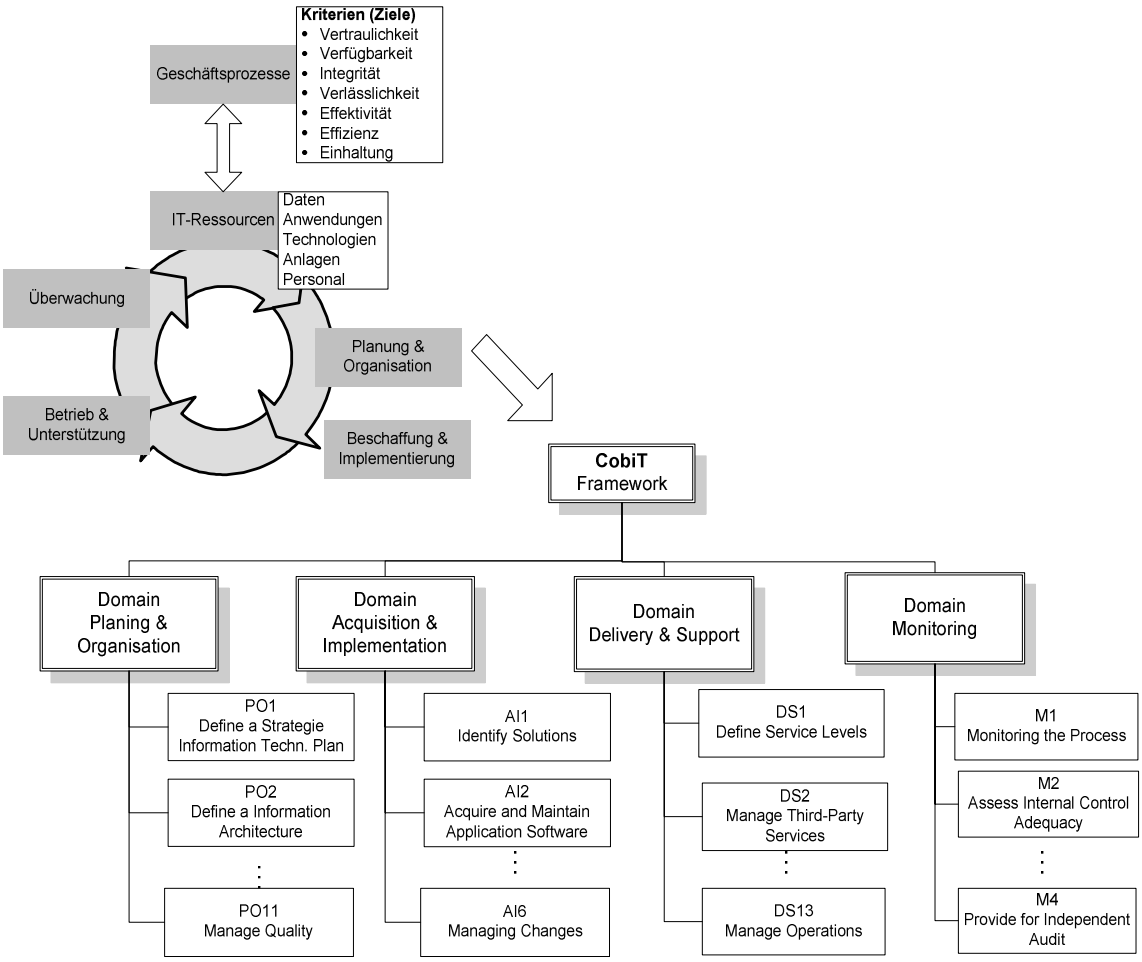


Abbildung 32: CobiT-Framework[269]

Zu jedem der 34 kritischen Prozesse (P01, P02, …, M4) werden zwischen 3 und 30 Kontrollziele zugeordnet[270], die über 30 nationale wie internationale Standards integrieren[271], wodurch ein hoher Abstraktionsgrad der Kontrollziele existiert. Hierdurch lässt sich die CobiT unabhängig auf unterschiedliche Plattformen und Geschäftsfelder anwenden. Insgesamt wird Co-

[267] Vgl. ISACA (1998), S. 13 und Eloff/Solms (2000a), S. 249
[268] Vgl. Junginger/Krcmar (2002), S. 363
[269] Vgl. Cobit (2001), Kapitel B
[270] Insgesamt 318 Kontrollziele in der 3. Edition 2000
[271] Z.B.: ITSEC, ISO 9000 und Common Criteria. Vgl. ISACA (1998), S. 16

biT überwiegend in der Revision von Kontrollzielen bzw. Sollvorgaben der IS-Sicherheit eingesetzt, wohingegen eine detaillierte Beschreibung von Sicherheitsmaßnahmen nicht unterstützt wird.

Gütesiegel/Produktaudit Schleswig-Holstein[272]

Das Ziel, den Datenschutz als Wettbewerbsvorteil zu etablieren[273], wird durch das Gütesiegel umgesetzt. Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein bescheinigt mit seinem Datenschutz-Gütesiegel *„…dem IT-Produkt, dass es mit den Vorschriften über den Datenschutz und die Datensicherheit vereinbar ist“*[274]. Nach dem LDSG SH (2000) sollen Behörden des Landes IT-Produkte[275] einsetzen, die ein Gütesiegel besitzen[276]. Nur in Ausnahmefällen dürfen nicht zertifizierte IT-Produkte in Behörden eingesetzt werden.

Eng damit ist das Datenschutz-Behördenaudit verbunden, wodurch das Datenschutzkonzept von Behörden in einem förmlichen Verfahren überprüft und bewertet wird. Voraussetzung für die Erteilung eines erfolgreichen Auditzeichens für die zu überprüfende Behörde ist der bevorzugte Einsatz von Produkten, welche ein Gütesiegel besitzen. Das Gütesiegel hat eine positive Wirkung auf die Vermarktung in der Privatwirtschaft, indem die zertifizierten IT-Produkte durch das Gütesiegel als datenschutzgerechte Produkte gekennzeichnet sind und somit als datenschutzfreundliche Produkte beworben werden können.

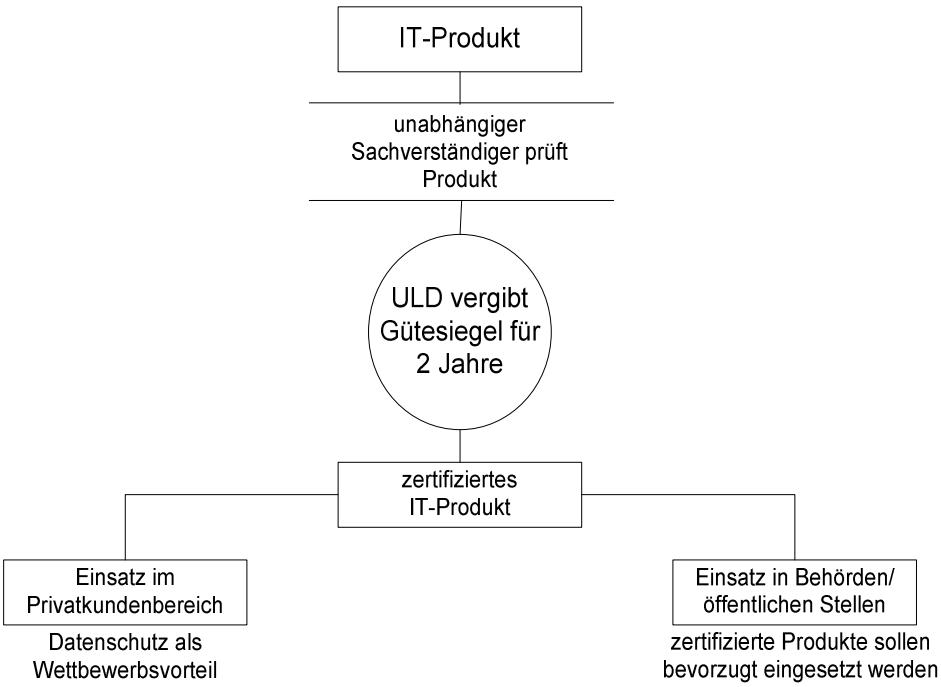


Abbildung 33: Das Gütesiegel-Verfahren[277]

Das Gütesiegel legt insbesondere auf Datenvermeidung/Datensparsamkeit, auf Datensicherheit/Revisionsfähigkeit der Datenverarbeitung und auf Gewährleistung der Rechte der Betroffenen Wert[278]. Hiefür wird der Anforderungskatalog in vier Komplex-Bereiche gruppiert[279]:

[272] Vgl. Datenschutzsiegel (2002)
[273] Vgl. Roßnagel (2000), S. 1 und Bäumler (2001)
[274] Datenschutz- Broschüre (2002), S. 5
[275] Der ULD SH versteht unter den zertifizierbaren IT-Produkten sowohl Hard- und Software als auch automatisierte Verfahren. Vgl. Datenschutz-Broschüre (2002), S. 11
[276] Vgl. §4 Abs. 2 LDSG SH (2000)
[277] Vgl. Datenschutz-Broschüre (2002), S. 10

- Grundsätzliche technische Ausgestaltung von IT-Produkten, wie z.B. Datensparsamkeit, frühzeitiges Löschen, Anonymisieren oder Pseudonymisieren von Daten sowie Transparenz und Produktbeschreibung.
- Zuverlässigkeit der Datenverarbeitung, wie z.B. Einwilligung, Sicherstellung der Zweckbindung sowie Löschung nach Wegfall des Erfordernisses.
- Technisch-organisatorische Maßnahmen, wie z.B. umfangreicher Schutz vor unbefugter Datenverarbeitung.
- Rechte der Betroffenen, wie z.B. Aufklärung und Benachrichtigung sowie vollständige Löschung.

Grundsätzlich ist eine bundesweite Einführung des Datenschutz-Gütesiegels zu erwarten, da andere Bundesländer, wie Brandenburg, Nordrhein-Westfalen und Mecklenburg-Vorpommern, den Einsatz von datenschutzfreundlichen Technologien durch Vorschriften fördern wollen. Zudem regelt das Bundesdatenschutzgesetz das Audit und Gütesiegel, wenn auch noch ein entsprechendes Ausführungsgesetz fehlt[280].

2.3.2.2 Sicherheits-Schwachstellenanalyse (SiSSA)

Die Sicherheits-Schwachstellenanalyse (kurz Schwachstellenanalyse[281] oder SiSSA) ist eine Weiterentwicklung und Anpassung der Schwachstellenanalysen aus der Organisationslehre. Die SiSSA unterstützt durch ihre Vorgehensweise den Top-Down Ansatz. Die SiSSA verwendet hierfür Kriterien, um mit deren Hilfe eine Analyse und Bewertung des Informationssystems hinsichtlich seiner Schwachstellen durchzuführen[282]. Des Weiteren können verschiedene Aspekte der IS-Sicherheit mit Hilfe der SiSSA evaluiert und zertifiziert werden. Die SiSSA ist nicht auf ein spezielles Kriterienwerk ausgelegt, sondern sie kann die unterschiedlichen Inhalte der jeweiligen Kriterienwerke transparent verarbeiten. Dadurch ist in einem gewissen Umfang eine Vergleichbarkeit zwischen Ergebnissen unterschiedlicher Kriterien möglich, was bei Methoden, die auf „ein“ Kriterienwerk ausgelegt sind, nur bedingt möglich ist[283]. Aufgrund der Top-Down Ausrichtung und der Verwendung von Kriterien lässt sich die Schwachstellenanalyse als eine standardisierte Methode für die ganze Institution bezeichnen, die an die individuellen Informationssystemstrukturen angepasst werden kann. Hierdurch können auch unternehmensindividuelle IS-Sicherheitsaspekte verarbeitet werden, was eine Anpassung an die Infrastruktur in einem gewissen Rahmen gestattet. Die SiSSA setzt folgende Aspekte des Top-Down Ansatzes um:

- Durch die Modularisierung können verschiedene Kriterienwerke und datenschutzorientierte Gesetze in Modulen strukturiert werden. So können unterschiedliche Bereiche der IS-Sicherheit und des Datenschutzes abgedeckt werden.

[278] Vgl. Hansen/Probst (2002), S. 167
[279] Vgl. Gütesiegel-Anforderungskatalog (2002)
[280] Vgl. §9a BDSG (2001) und Schaar/Stutz (2002), S. 330
[281] Die Phase Verwundbarkeitsanalyse der Risikoanalyse wird auch als „Schwachstellenanalyse“ bezeichnet, ist nicht mit der hier dargestellten SiSSA vergleichbar, da sie eine eigene Methode des IS-Sicherheitsmanagements ist.
[282] Vgl. Voßbein, R. (1994b), S. 64
[283] Vgl. Haar/Solms, R. (1993), S. 7

- Durch die Repräsentation der Kriterien mittels Fragebögen sind die Evaluation und die Ergebnisse transparent und zugänglich.
- Die Bewertung der Evaluationsergebnisse wird qualitativ und quantitativ unterstützt.
- Durch die offene Struktur und die einfache Erweiterung mit Hilfe von Individualkriterien können auch IS-Sicherheitsaspekte der einzelnen Unternehmen berücksichtigt werden.

Die Grundstruktur der SiSSA basiert auf Modulen, die flexibel erweitert werden können, um unterschiedliche Kriterienwerke zu repräsentieren und eine Anpassung an die unternehmensindividuellen Aspekte zu ermöglichen. Das Basismodul umfasst einen Querschnitt von verschiedenen Maßnahmenbereichen, die i.d.R. in jeder Institution benötigt werden. Die Spezialbereiche bauen auf dem Basismodul auf und beinhalten Maßnahmen für verschiedene Bereiche. Die Spezialbereiche können einen Querschnittscharakter für alle IS-Sicherheitsaspekte aufweisen (z.B. Datenschutz) oder nur bestimmte Funktionen (z.B. spezifische Identifikation und Authentifizierung) analysieren.

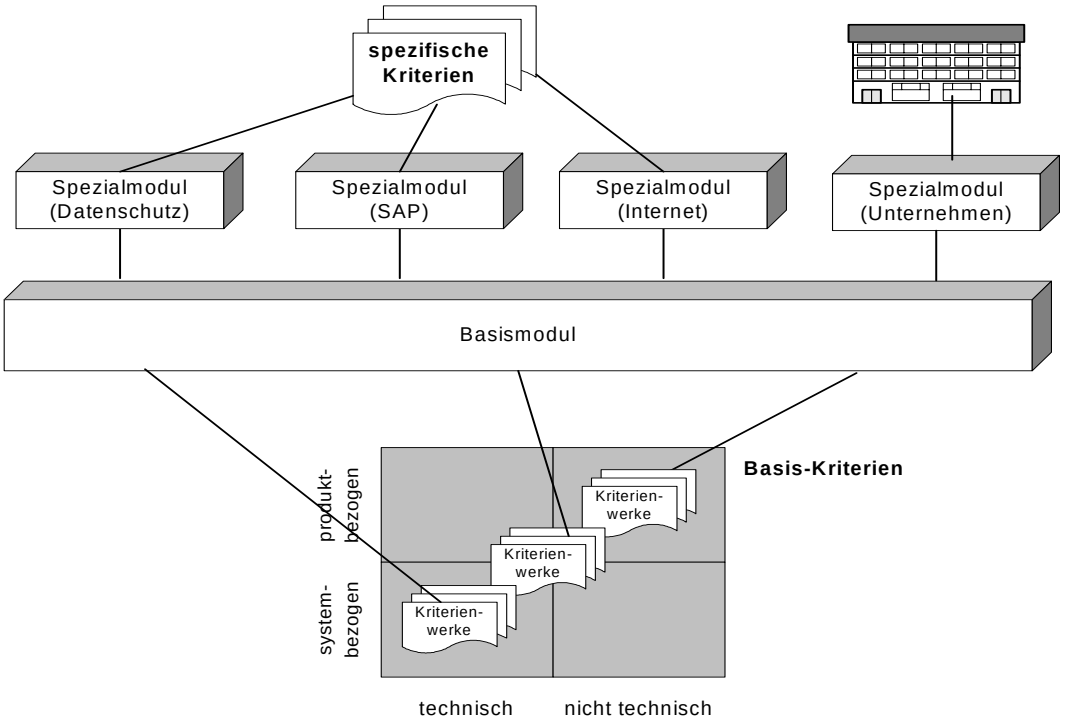


Abbildung 34: Modularer Aufbau der SiSSA

Eine Kombination von Kriterien ist sinnvoll, sofern weite Bereiche der IS-Sicherheit erfasst werden sollen. Die ISO 17799 und die CobiT decken Aspekte des Managements der IS-Sicherheit ab und stellen eher generische Maßnahmen bereit. Um diese mit konkreten Maßnahmen zu „füllen“, bietet sich z.B. das IT-Grundschutzhandbuch an[284]. Somit kann der IT-Grundschutz ein Standard-Niveau gewährleisten und besonders sensible Sicherheitsbereiche

[284] Vgl. Hange/Moritz (2002), S. 69

aufdecken. Diese können zusätzlich durch Common Criteria zertifizierte Produkte geschützt werden; datenschutzrechtliche Aspekte werden durch den Anforderungskatalog des ULD SH abgebildet[285].

Phasen der Sicherheitsschwachstellenanalyse

In der folgenden Abbildung sind die Phasen der Schwachstellenanalyse dargestellt.

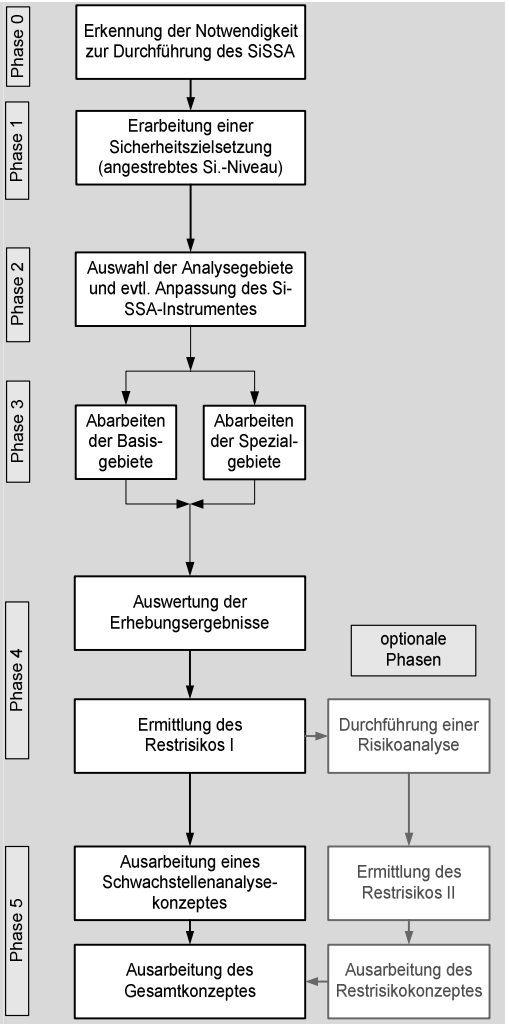
Phasen der SiSSA	
	Die Inhalte der Phasen 0 und 1 entsprechen der IS-Sicherheitspolitik. Das angestrebte Sicherheitsniveau kann in Anlehnung an die Niveaustufen des Grundschutzhandbuchs[286] übernommen werden und bildet Eingangsgrößen für die weiteren Phasen. In der Phase 2 werden auf Grund des modularen Aufbaus nur die relevanten Module ausgewählt. Eventuell werden diese an die individuellen Gegebenheiten angepasst. In Phase 3 erfolgt die Erhebung der Schwachstellen mit Hilfe der ausgewählten Basis- und Spezialmodule. Die Befragung erfolgt in Form von strukturierten Fragen, die z.B. aus einfachen Ja/Nein über Rating Fragen bis hin zu offenen Fragen bestehen können. Meist werden die relevanten Personen in einer Gruppe von einem Interviewer befragt. Als Ergebnis der Auswertung werden in der Phase 4 die Schwachstellen dargestellt. Grundsätzlich erfolgt die Auswertung der Schwachstellen durch die Gegenüberstellung von ermittelten und geforderten Maßnahmen. Aufgrund der fehlenden Maßnahmen werden Schwachstellen als Differenz eines Soll-Ist Vergleichs assoziiert. Aufgrund der Phase 4 wird nun ein Schwachstellenkonzept erarbeitet und daraus resultierend ein Maßnahmenkonzept, das die Schwachstellen beseitigen soll. Dabei ist die Abstimmung der Ergebnisse der Schwachstellenanalyse mit eventuell zusätzlich durchgeführten Risikoanalysen und anderen Sicherheitskonzepten zu berücksichtigen. Die verschiedenen Maßnahmen sind untereinander und mit anderen Konzepten abzustimmen.

Tabelle 7: Phasen der SiSSA[287]

Durchführung der SiSSA durch Fragenkataloge[288]

In der empirischen Sozialforschung wird zur Informationsgewinnung neben der Beobachtung[289] und der Inhaltsanalyse[290] häufig die Befragung eingesetzt. Bedingt durch eine Reihe von Anwendungsgebieten und eine hohe Flexibilität der einzelnen Befragungsmethoden ist

[285] Vgl. Hansen/Probst (2002)
[286] Vgl. Tabelle 3
[287] Vgl. Voßbein, J. (1999), S. 258
[288] Die Begriffe Fragenkatalog und Fragebogen werden im Rahmen der Arbeit synonym verwendet.
[289] Beobachten beinhaltet das systematische Erfassen, Festhalten und Deuten eines Verhaltens zum Zeitpunkt seines Geschehens. Vgl. Atteslander (1995), S. 87
[290] Die Inhaltsanalyse beschäftigt sich mit der Analyse eines vorgegebenen Inhalts (z.B. Text, Bild), um daraus einen Zusammenhang der Entstehung dieses Inhalts zu ermitteln. Vgl. Atteslander (1995), S. 238

eine beträchtliche Anzahl unterschiedlichster Befragungsformen entwickelt worden[291]. Im Rahmen der SiSSA erfolgt eine Befragung in Form eines strukturierten Interviews, dem ein Fragebogen zugrunde liegt. Das Interview wird durch den Interviewer aktiv geführt, wobei der Befragte z.T. die Möglichkeit hat, das Interview zu beeinflussen. Die Fragebögen können ebenfalls in elektronischer Form vorliegen, was eine Effizienz- und Flexibilitätssteigerung gegenüber der manuellen Erhebung und Auswertung beinhaltet. Die Vorteile liegen insbesondere in der automatischen Überwachung und Steuerung der Fragenreihenfolge, der automatischen Antwortkontrolle, der Vermeidung von Übertragungsfehlern, der Antwortzeitmessung und der Unterstützung verschiedener Sprachen[292]. Ein computergestützter Fragebogen verwendet häufig standardisierte geschlossene Fragen, die die Antwortmöglichkeiten vorgeben. Durch standardisiert gestaltete Fragen ist gewährleistet, dass die Erhebung objekt- und nicht personenbezogen erfolgt[293]. Offene Fragen werden zusätzlich verwendet, wenn der Befragte inhaltliche Aussagen tätigt, die nicht durch den Fragenkatalog abgedeckt sind.

Die folgende Abbildung zeigt den grundsätzlichen Aufbau eines computergestützten Fragebogensystems in Verbindung mit der SiSSA.

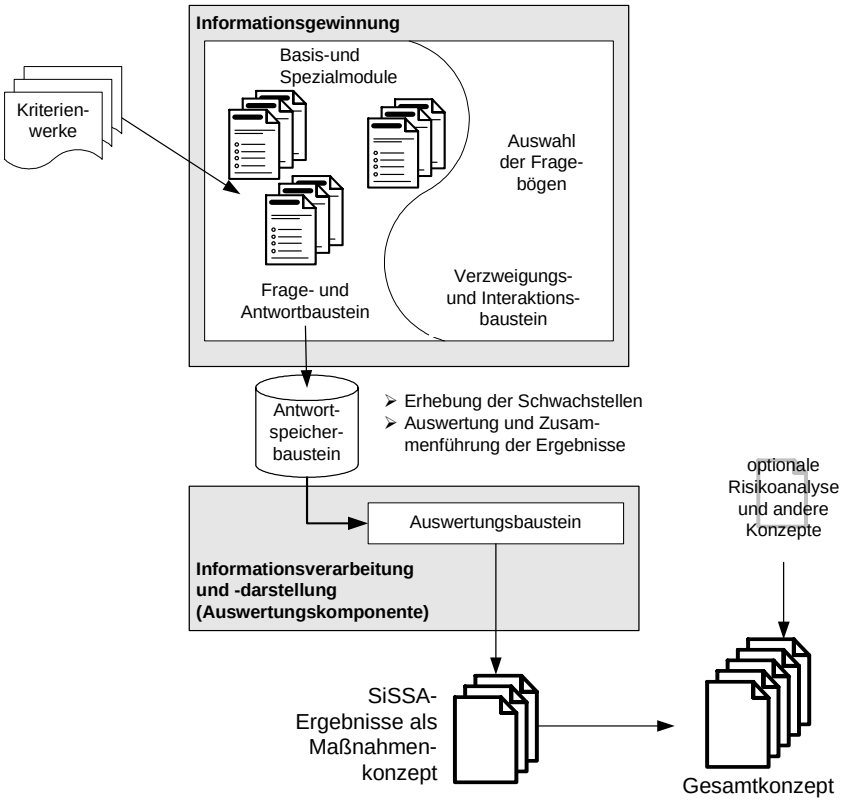


Abbildung 35: Computergestützte Vorgehensweise der SiSSA[294]

Der Kern eines computergestützten Fragebogensystems ist die Frage- und Antwortkomponente, die die Maßnahmenkriterien enthält. Sie beinhaltet den eigentlichen Fragebogen mit seinen Antwortmöglichkeiten. Die Verzweigungs- und Interaktionskomponente eines computergestützten Fragebogens soll dem Benutzer die Möglichkeit geben, manuell den Fragebogen an-

[291] Vgl. Koolwijk (1974), S. 15
[292] Vgl. Hoepner (1994), S. 174-176
[293] Vgl. Hoepner (1994), S. 7
[294] Angepasst und erweitert in Anlehnung an Möhrle (1997), S. 462

zupassen und zu navigieren. Aufgrund der engen Verknüpfung der Module ist es erforderlich, Redundanzen und Abhängigkeiten zwischen dem Basis- und Spezialmodul sowie zwischen Spezialmodulen bei der Erhebung zu berücksichtigen[295]. Es werden somit systembedingte Verzweigungen durchgeführt, um z.B. redundante oder nicht benötigte Fragen zu vermeiden. Die Antwortspeicherkomponente besitzt die Möglichkeit, die erhobenen Maßnahmen-Antworten so zu speichern und zu verwalten, dass eine spätere Auswertung problemlos möglich ist. Die Auswertung soll die erhobenen Maßnahmen in Form eines Berichtes automatisch zusammenzufassen, auswerten und anschließend entsprechend darstellen. Der Bericht enthält z.B. die fehlenden Maßnahmen auf Basis eines Soll-Ist Vergleichs und zusätzliche Maßnahmenempfehlungen.

2.3.3 Hybrider Ansatz

Einen hybriden Ansatz verbinden Teilaspekte des Bottom-Up und Top-Down Ansatzes. Der folgende Ansatz des BSI-Grundschutzes (IT-Grundschutzhandbuchs) ist ein Beispiel für einen hybriden Ansatz[296].

BSI-Grundschutzhandbuch bzw. IT-Baseline

Das BSI hat 1995 die erste Version des IT-Grundschutzhandbuchs[297] veröffentlicht, da das zuvor veröffentlichte IT-Sicherheitshandbuch in der Praxis Defizite in der Umsetzung erfahren hat. Der hohe Umsetzungsaufwand des Bottom-Up geprägten IT-Sicherheitshandbuchs hat das BSI veranlasst, eine Kombination der Top-Down und Bottom-Up Vorgehensweise in Form des IT-Grundschutzhandbuchs zu entwickeln[298]. Der Kern des IT-Grundschutzhandbuchs bildet das hybride IT-Sicherheitskonzept oder „Grundschutz + X“[299], was auf den General Management Guidelines for Information Security der ISO 13335 basiert[300]. Aufgrund einer zuvor durchgeführten Schutzbedarfsfeststellung der einzelnen IT-Anwendungen und IT-Systeme wird entschieden, ob diese nach dem IT-Grundschutz oder nach einer Risikoanalyse weiterbearbeitet werden sollen. Wenn ein niedriger bis mittlerer Schutzbedarf besteht, wird nach dem IT-Grundschutz weiter verfahren; existiert ein höherer Schutzbedarf, dann soll zusätzlich eine Risikoanalyse eingesetzt werden[301]. Im Folgenden werden die Schritte des BSI-Grundschutzes dargestellt.

---

[295] So kann die gleiche oder inhaltlich vergleichbare Frage X schon in Modul A gestellt worden sein, ist aber auch in Modul B enthalten. Oder durch eine Beantwortung einer Frage wird ein ganzer Frageblock überflüssig.
[296] Vgl. Junginger/Krcmar (2002), S. 361
[297] Das IT-Grundschutzhandbuch wird fortlaufend erweitert. Die aktuelle Version kann unter http://www.bsi.de (Stand: 10.12.2002) bezogen werden.
[298] Vgl. Weck (1995), S. 13-16
[299] X steht i.d.R. für Risikoanalyse
[300] Vgl. Abbildung 29: Informationsmanagement nach ISO 13335
[301] Vgl. BSI-Grundschutzhandbuch (2000), Kapitel 2.1, S. 2

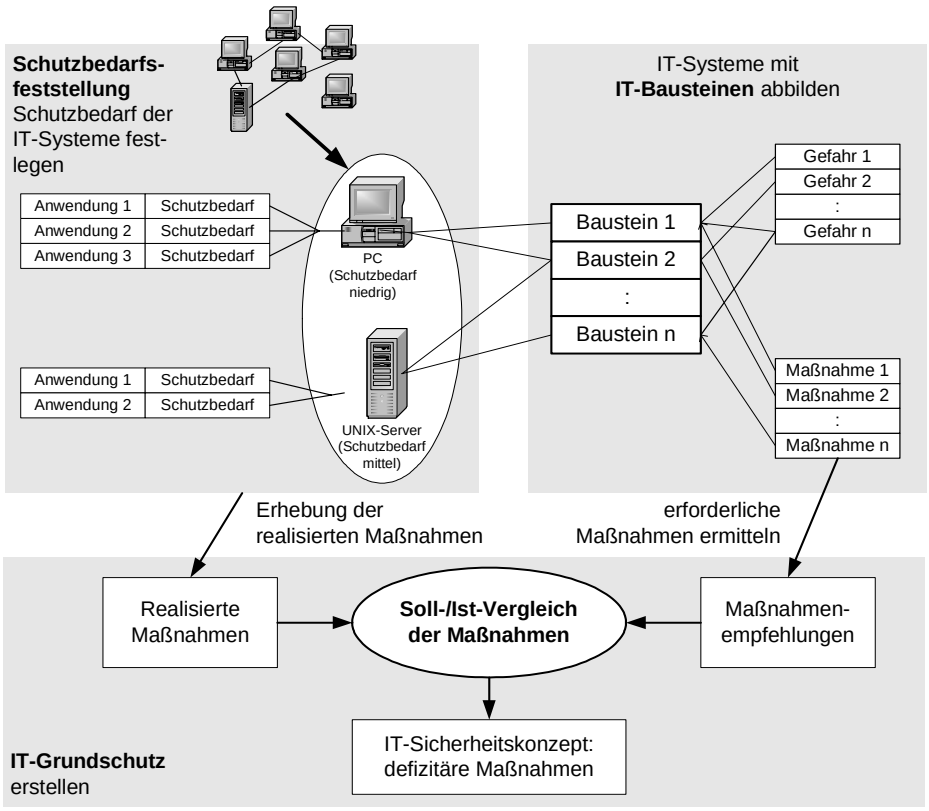


Abbildung 36: Zusammenhang zwischen IT-System, IT-Baustein, Maßnahmen und Gefahr

Schutzbedarfsermittlung (Schutzbedarfsfeststellung)

Zuerst werden alle vorhandenen und geplanten IT-Systeme erfasst, wobei gleichartige IT-Systeme aus Komplexitätsreduktionsgründen in Gruppen zusammengefasst werden. Anschließend werden die laufenden und geplanten IT-Anwendungen ermittelt und dargestellt. Die ermittelten IT-Anwendungen werden dem jeweiligen IT-System zugeordnet; i.d.R. besitzt jedes IT-System 1 bis n Anwendungen. Dabei werden die wichtigsten IT-Anwendungen und deren Informationen aufgrund ihres vorläufigen Schutzbedarfs vorsortiert. Für eine detaillierte Analyse des Schutzbedarfs werden die Schäden und deren Konsequenzen ermittelt, die bei Verlust von den drei Basiszielen (Vertraulichkeit, Integrität und Verfügbarkeit) je IT-System und IT-Anwendung auftreten können. Die erwarteten Schäden und ihre Konsequenzen werden in drei Schutzbedarfskategorien eingeteilt (niedrig bis mittel; hoch und sehr hoch). So sind bei niedrigem bis mittlerem Schutzbedarf die Konsequenzen begrenzt, wohingegen bei hohem bis sehr hohem Schutzbedarf die Konsequenzen beträchtlich sein können. Die Schäden der einzelnen IT-Anwendung, die jedes IT-System betreffen können, werden zusammengefasst und in ihrer Gesamtheit ermittelt. Es ist auf Abhängigkeiten und Kumulationseffekte der Schäden zu achten. Dabei wird nach dem Maximumprinzip verfahren, so dass der stärkste Schaden bzw. die stärkste Konsequenz für die Bestimmung des Schutzbedarfes ausschlaggebend ist. Besitzt ein IT-System niedrigen bis mittleren Schutzbedarf, so ist der IT-Grundschutz ausreichend. Bei höherem Schutzbedarf sollte zusätzlich eine Risikoanalyse durchgeführt werden.

Die Schutzbedarfsfeststellung ist Bottom-Up geprägt, da wie in der Risikoanalyse die Informationssysteme erst in ihre Einzelbestandteile zerlegt werden und dann für jedes einzelne IT-System der Schutzbedarf nach dem Maximumprinzip ermittelt wird. Das Ergebnis wird anschließend in Form einer Tabelle dargestellt, die für jedes IT-System den Schutzbedarf nach dem jeweiligen Sicherheitsbasisziel beschreibt[302].

IT-Grundschutz erstellen

Kern des Grundschutzhandbuchs bilden vordefinierte IT-Bausteine sowie ein Maßnahmen- und Gefährdungskatalog, wobei die IT-Bausteine in einem Schichtenmodell strukturiert sind[303]. Mit den IT-Bausteinen wird die zu analysierende Systemlandschaft durch „Standard-Bausteine" abgebildet. Mit den IT-Bausteinen sind Soll-Maßnahmen verknüpft, die durch eine direkte Anwendung einen Grundschutz erstellen können.

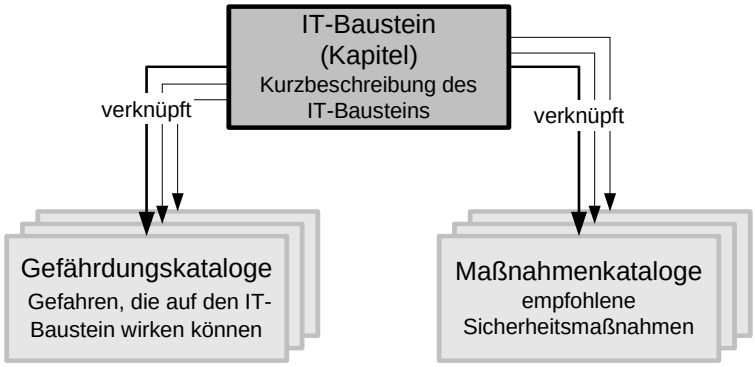


Abbildung 37: Grundstruktur von Bausteinen

Die den Bausteinen zugeordneten Gefahren und Maßnahmen sind in fünf Gefahrenklassen (z.B. höhere Gewalt oder technisches Versagen) bzw. sechs Maßnahmenklassen (z.B. Organisation oder Notfallversorgung) zusammengefasst und bei Bedarf mit dem jeweiligen Baustein verknüpft. In den Bausteinen wird zusätzlich auf Querverbindungen zu anderen Bausteinen hingewiesen, da diese teilweise übergreifende Eigenschaften (wie z.B. Organisation, Personal oder Datensicherungskonzepte) besitzen. Die Bausteine werden permanent durch das BSI aktualisiert und erweitert.

Es erfolgt ein Soll-Ist Vergleich der Grundschutz-Maßnahmen mit den vorhandenen Maßnahmen, was einer Top-Down Strategie entspricht. Die Differenz zwischen Soll- und Ist-Zustand beschreibt die umzusetzenden Maßnahmen, um einen IT-Grundschutz zu erreichen. Die ermittelten Maßnahmen sind teilweise als optional gekennzeichnet und sollten zudem priorisiert werden, insbesondere wenn die erforderlichen Ressourcen begrenzt sind, um eine Rangfolge der zu erfüllenden Maßnahmen aufzustellen.

Die Ergebnisse des IT-Grundschutzes und der eventuell durchgeführten Risikoanalyse werden zu einem IT-Sicherheitskonzept zusammengefügt. Das Sicherheitskonzept sollte die erarbeiteten Maßnahmen enthalten, aber auch Umsetzungs- und Kontrollkonzepte aufweisen. Als Ergebnis erhält der Sicherheitsverantwortliche eine Liste von Maßnahmen, deren Umsetzung

[302] Vgl. BSI-Grundschutzhandbuch (2000), Kapitel 2.2, S. 16
[303] Vgl. Abbildung 26: Schichtenmodell des BSI-Grundschutzhandbuchs

erforderlich ist, um ein mittleres Sicherheitsniveau zu erreichen. Das IT-Grundschutzhandbuch bietet vielfältige Umsetzungsbeispiele für das oben genannte Konzept, das in jedem Schritt dem Sicherheitsverantwortlichen mit praktischen Beispielen zur Seite steht[304].

Dieser Ansatz wurde seitens der Behörden und Unternehmen positiv angenommen, so dass ein Gütesiegel auf Basis des IT-Grundschutzes vergeben wird. Das Gütesiegel ist auf verschiedene Zielgruppen, wie z.B. Wirtschaftsunternehmen, E-Commerce-Anbieter oder Behörden, ausgelegt und soll nachweisen, dass die IS-Sicherheit nach dem IT-Grundschutz umgesetzt ist und aufrechterhalten wird[305]. Die IT-Grundschutz-Evaluation weist drei Ausprägungsstufen auf, d.h. von einer Selbsterklärung des Unternehmens bis hin zum IT-Grundschutz-Zertifikat, das durch eine unabhängige Instanz vergeben wird.

Die folgende Tabelle stellt die IS-Sicherheitsstrategien zusammenfassend dar.

[304] Vgl. BSI-Grundschutzhandbuch (2000), Kapitel 2.4 - 2.5
[305] Vgl. Münch/Niggemann (2001), S. 257

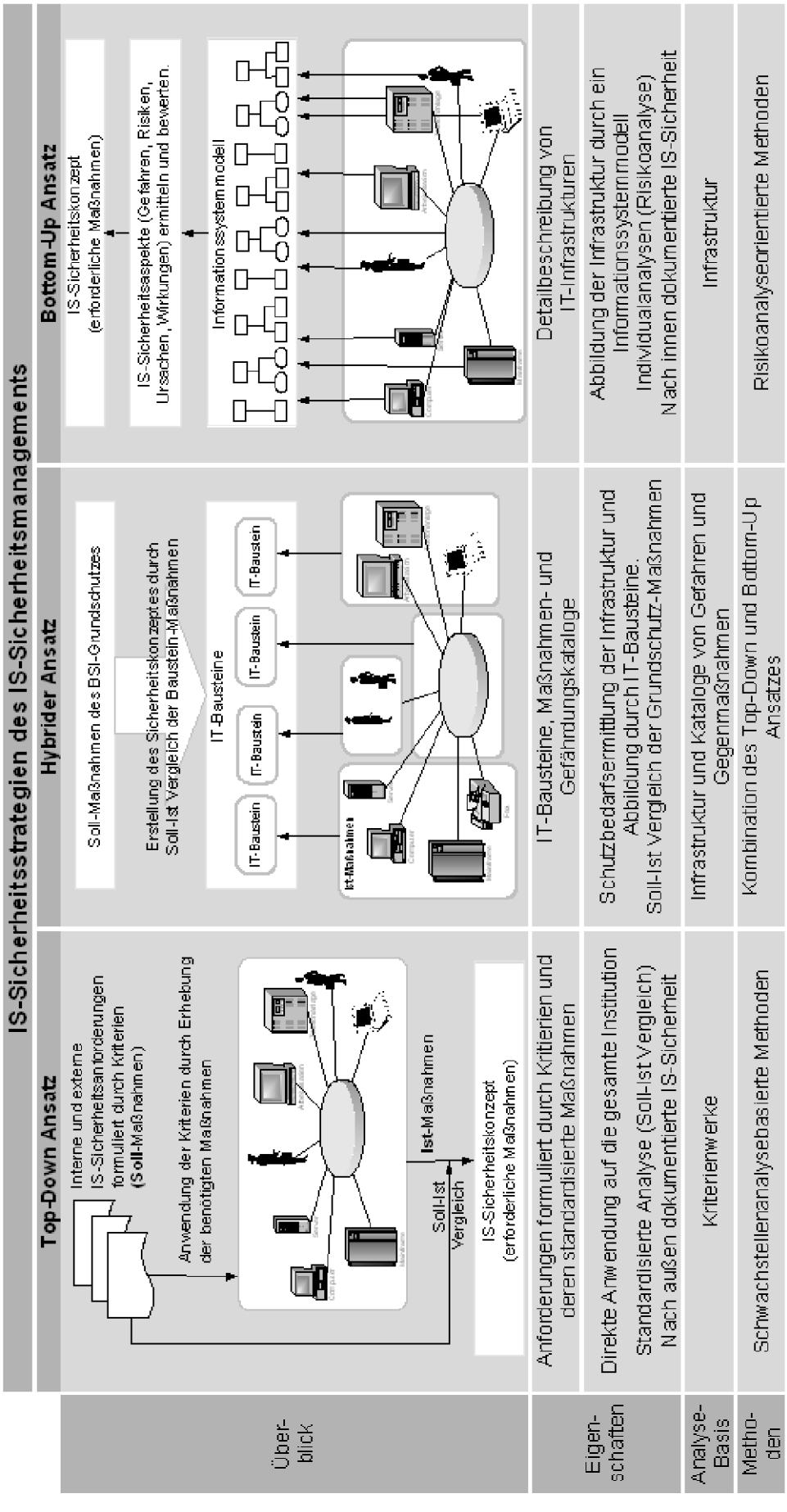


Tabelle 8: IS-Sicherheitsstrategien des IS-Sicherheitsmanagements

2.4 Integriertes IS-Sicherheitsmanagement

Im Folgenden bilden die vorgestellten Ansätze die Grundlage für ein integriertes IS-Sicherheitsmanagement, wobei folgende Vor- und Nachteile bedacht werden sollten. Der Bottom-Up Ansatz gewinnt sehr schnell an Komplexität, da für jedes einzelne Element oder Gruppe das jeweilige Risiko ermittelt werden muss. Dies schreckt vor einem wiederholten Einsatz oft ab. Aus diesem Grund wird häufig gefordert, den Bottom-Up Ansatz nur auf besonders kritische Bereiche einzugrenzen[306]. Die Durchführung des Top-Down Ansatzes durch die SiSSA erfordert einen geringeren Aufwand als die Risikoanalyse, da eine aufwendige individuelle Anpassung entfällt. Durch den relativen kostengünstigen Einsatz der SiSSA ist eine iterative Kontrollanalyse im Unternehmen leichter durchzusetzen als bei der aufwendigeren Risikoanalyse. Aufgrund der Standardisierung ist nicht ein so hohes Sicherheitsniveau wie bei der Risikoanalyse zu erreichen, es wird jedoch eine „Standard-Sicherheit“ bzw. Baseline-Sicherheit auf Basis von Kriterien ermöglicht. Hybride Verfahren verknüpfen Aspekte des Top-Down und Bottom-Up Ansatzes. Das BSI-Grundschutzkonzept ist ein Beispiel für ein hybrides Verfahren, das in Abhängigkeit des Schutzbedarfes der IT-Systeme für das weitere Vorgehen entweder den Top-Down Ansatz oder den Bottom-Up Ansatz einteilt. Wird ein niedriger bis mittlerer Schutzbedarf benötigt, so werden mit Hilfe von IT-Bausteinen Soll-Ist Vergleiche der benötigten Maßnahmen - vergleichbar mit dem Vorgehen des Top-Down Ansatzes - durchgeführt.

Mit einem kombinierten Einsatz der IS-Sicherheitsstrategieansätze erfolgt ein integriertes IS-Sicherheitsmanagement durch eine

- Breiten- und Tiefenanalyse sowie mittels einer
- präventiven und reaktiven Sichtweise.

Breiten- und Tiefenanalyse der IS-Sicherheit
Aufgrund des Top-Down Ansatzes können die einzelnen Unternehmensbereiche durch eine Breitensuche auf Schwachstellen hin untersucht werden, die durch Standard-Maßnahmen geschlossen werden können.

[306] Vgl. Stelzer (1995), S. 126

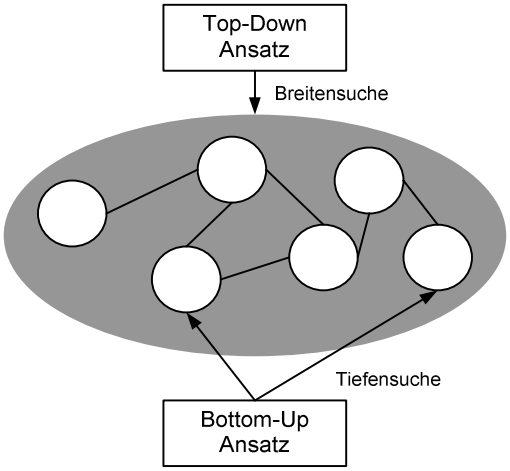


Abbildung 38: Breiten- und Tiefenanalyse

Der Top-Down Ansatz kann ebenfalls als Selektionsinstrument für hochsensible IS-Sicherheitsbereiche verwendet werden. Für die Bereiche, die ein sehr hohes IS-Sicherheitsniveau benötigen, kann der aufwendige Bottom-Up Ansatz in Form einer Tiefensuche angewandt werden. Es ist zu beachten, dass durch eine Priorisierung alle sicherheitsrelevanten Unternehmensbereiche bei der Analyse berücksichtigt werden. Diese integrierte Vorgehensweise entspricht den Rahmenkonzepten des IS-Sicherheitsmanagements der SiS-SA, dem BSI- Grundschutzhandbuch und dem Informationsmanagement nach ISO 13335.

Präventives und reaktives IS-Sicherheitsmanagement

Das beste IS-Sicherheitsmanagement ist das präventive, da negative Vorfälle erst gar nicht entstehen[307]. Aufgabe des präventiven IS-Sicherheitsmanagements ist die Ermittlung von fehlenden Maßnahmen und die vorausschauende Analyse eines negativen Vorfalls, um geeignete Maßnahmen einzusetzen. Im reaktiven Fall ist der negative Vorfall schon aufgetreten; das Ziel ist die Suche nach der Ursache dieses Vorfalls bzw. die Erklärung der negativen Konsequenz, um reaktiv adäquate Maßnahmen zu ergreifen. Da aber nicht alle sicherheitsrelevanten Aspekte antizipiert werden können, ermöglicht erst eine Integration des präventiven und reaktiven IS-Sicherheitsmanagements eine umfassende IS-Sicherheit. Dies bedeutet, dass einerseits präventiv IS-Sicherheitsaspekte berücksichtigt werden, um einen negativen Zustand in Form einer Konsequenz im Vorfeld „präventiv“ zu verhindern. Andererseits sollte auch die Möglichkeit bestehen, reaktiv auf negative Vorfälle zu reagieren. Im Folgenden werden deshalb die IS-Sicherheitsansätze mit einer präventiven und reaktiven Sichtweise erweitert.

Die Differenzierung zwischen dem präventiven und reaktiven IS-Sicherheitsmanagement existiert auch im CERT[308]-Ansatz, den das deutsche BSI durch den CERT-Bund im Jahre 2001 umgesetzt hat[309]. Der Bundesminister des Innern hat dessen Aufgaben wie folgt definiert: „*Seine* [CERT-Bund] *Aufgaben bestehen zum einen darin,* ***präventive*** *Sicherheitslücken in den Computersystemen des Bundes zu finden. Zum anderen wird das CERT-Bund in der Lage sein, rund um die Uhr, sieben Tage die Woche auf mögliche Gefährdungen oder Angriffe zu*

[307] Vgl. Mühlen (1995), S. 167
[308] CERT = Computer Emergency Response Team
[309] Das erste CERT-Team wurde durch die Defense Applied Research Projects Agency (DARPA) im Jahre 1988 gegründet, nachdem der Morris-Wurm 10 % der am Internet beteiligten Computer außer Betrieb setzte. Vgl. Hare (1999a), S. 553

reagieren *und kurzfristige Gegenmaßnahmen zu ergreifen*“[310]. Der CERT-Ansatz ist inhaltlich und strukturell in Anlehnung an RFC 2350 entstanden, wobei hier die Internet-Sicherheit im Vordergrund steht[311]. Ziel der Einrichtung des CERT-Bundes ist die Bereitstellung einer zentralen Anlaufstelle für präventive (Computer Security Incident Prevention) und reaktive Notfallsituationen (Computer Security Incident Response) in Bezug auf sicherheits- und verfügbarkeitsrelevante Vorfälle in Computer-Systemen (Computer-Notfälle)[312].

Auch größere Unternehmen und andere öffentliche Einrichtungen, wie z.B. Universitäten, betreiben CERT-Einrichtungen. Diese sind z.T. öffentlich zugänglich; insbesondere CERT-Einrichtungen von Unternehmen sind - im Unterschied zum CERT-Bund - nur für einen beschränkten Nutzerkreis zugänglich. Die notwendige Koordination zwischen den weltweit agierenden CERT-Einrichtungen erfolgt über das FIRST-Forum[313]. In der folgenden Tabelle werden wichtige deutsche CERT-Einrichtungen zusammengefasst.

Dienstleister	Cert Bund	D-Cert	DFN-Cert	FSC-Cert	IBM-ERS	RUS-Cert	S-Cert	Secu-Cert	Siemens-Cert	Telekom-Cert
Betreiber	BSI	T-Systems	DFN-Verein	Fujitsu Siemens	IBM	RZ Uni Stgt.	Spark.-Gruppe	Secunet	Siemens	Telekom
Interne Zwecke	P/R	P/R	P/R	P/R	P/R	P/R	P/R	P/R	P/R	P/R
Wirtschaft		P/R			P/R					
Öff. Verw. (Bund)	P/R	P/R			P/R					
Öff. Verw. (Land, Komm.)	P	P/R			P/R	P				
Banken und Versicherer		P/R			P/R		P/R Spark.			
Forschung und Lehre		P/R	P/R		P/R	P				

P = Präventiv; R = Reaktiv

Tabelle 9: Übersicht der deutschen CERT-Einrichtungen[314]

Die Notwendigkeit einer präventiven und reaktiven Sichtweise hat sich auch in dem Business Continuity Management (BCM) durchgesetzt. So hat sich seit Ende der 80er Jahre das Konzept des Business Continuity Managements entwickelt, das die Gewährleistung der Funktionsfähigkeit des „Business“ unter allen Umständen zum Ziel hat. Insbesondere das Ziel der Verfügbarkeit stand im Vordergrund. Hierbei waren und sind insbesondere Aspekte der IS-Sicherheit von Bedeutung, da immer mehr Geschäftstätigkeiten von computergestützten Informationssystemen und deren Sicherheit abhängen. Erste Realisierungsformen des BCM hatten überwiegend reaktive technische Implementierungen als Lösung anzubieten. Es wurde schnell erkannt, dass diese reaktive Sicht durch eine antizipative bzw. präventive Sichtweise der IS-Sicherheit zu ergänzen war. Zudem ist eine allein technisch orientierte Sichtweise nicht mehr ausreichend und wird durch zusätzliche organisatorische Aspekte der IS-Sicherheit, wie z.B. mittels Katastrophenpläne, ergänzt. Somit definiert das Business Continuity Institute das BCM wie folgt: “… *as the act of anticipating incidents which will affect mission critical function and processes for the organisation and ensuring that it responds to any incident in a planned and rehearsed manner whilst the business recovers.*”[315]

[310] Schily (2001)
[311] Vgl. Brownlee/Guttman (1998)
[312] Vgl. Teaminfo (2001), Kapitel 3.1
[313] FIRST = Forum of Incident Response and Security Teams. Für weitere Informationen: URL: http://www.first.org (Stand: 10.10.2002)
[314] Vgl. CERT-Einrichtungen (2002)
[315] Sharp (2002), S. XI

Dieses präventive und reaktive IS-Sicherheitsmanagement soll auf Top-Down und Bottom-Up Ansätze angewandt werden. Im Zusammenhang mit den IS-Sicherheitsstrategien ist

- die präventive Sicht auf eine Verhinderung von negativen Vorfällen ausgerichtet, wohingegen
- die reaktive Sicht erklärungsorientiert ausgerichtet ist, um Ursachen für negative Vorfälle zu ermitteln.

In der folgenden Abbildung werden die IS-Sicherheitsstrategien des integrierten IS-Sicherheitsmanagements zusammenhängend dargestellt. Hierbei dient die Schwachstellenanalyse zur standardisierten präventiven Aufdeckung und reaktiven Breitensuche von Schwachstellen. Durch das präventive Herleiten von Schwachstellen werden zukünftige negative Vorfälle verhindert, wohingegen bei aufgetretenen Vorfällen ermittelte Schwachstellen bzw. fehlende Maßnahmen eine Erklärung für diese Vorfälle bieten. Für eine umfassende Erklärung der Ursachen, die auch die gefährdenden Ereignisse umfasst, ist eine FMEA orientierte Risikoanalyse geeignet. Die FMEA erklärt einerseits reaktiv die Ursachen für einen negativen Vorfall. Anderseits können auch präventiv die Auswirkungen eines negativen Vorfalls (z.B. Auswirkungen von möglichen gefährdenden Ereignissen) antizipiert werden.

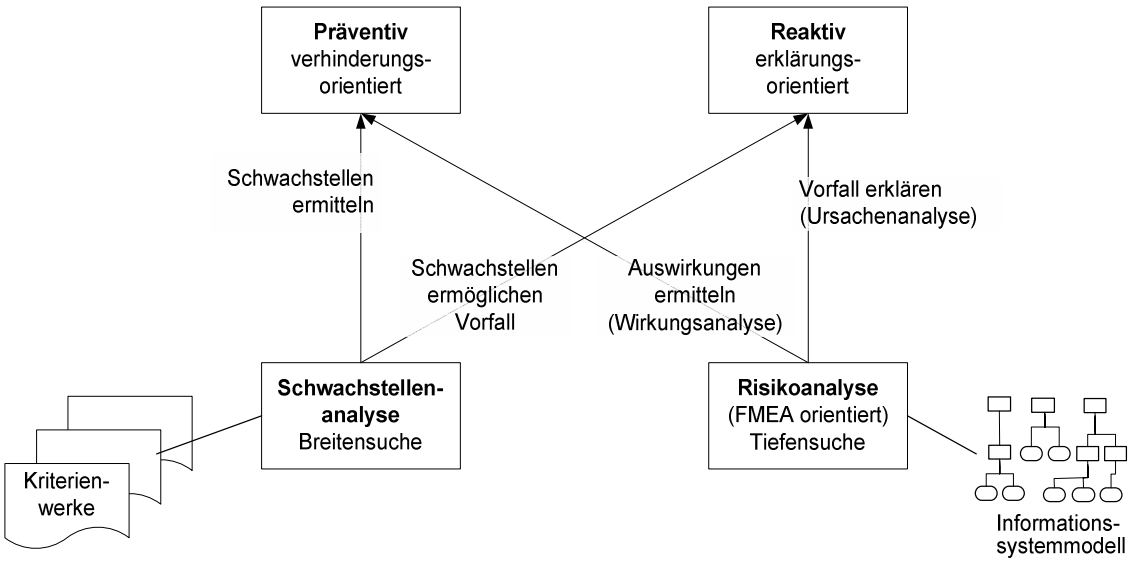


Abbildung 39: IS-Sicherheitsstrategien des integrierten IS-Sicherheitsmanagements

Die Schwachstellenanalyse basiert im Wesentlichen auf allgemein gültigen Kriterien, die Risikoanalyse beruht auf einem Modell des Informationssystems, das die unternehmensindividuelle Infrastruktur abbildet. Die folgende Tabelle fasst das integrierte IS-Sicherheitsmanagement zusammen.

	Top-Down	Bottom-Up
präventive Sichtweise	Die präventive Sichtweise wird in erster Linie durch die SiSSA unterstützt, da sie im Vorfeld Schwachstellen von Informationssystemen aufdeckt und entsprechende präventive Maßnahmen empfiehlt. Sie kann durch eine Breitenanalyse präventiv viele Bereiche der Institution abdecken, da standardisierte Module verwendet werden.	Für hochsensible Bereiche von Informationssystemen ist eine Tiefenanalyse in Form einer Ereignisablaufanalyse bzw. Wirkungsanalyse notwendig, um individuelle Sicherheitsaspekte zu berücksichtigen. Dies beinhaltet insbesondere die vorausschauende Analyse der Auswirkungen eines negativen Vorfalls.
reaktive Sichtweise	Die Schwachstellenanalyse ermöglicht eine Breitensuche von Schwachstellen, welche die negativen Vorfälle „ermöglicht“ haben. Hierbei wird davon ausgegangen, dass Informationssysteme, die keine Schwachstellen besitzen, Vorfälle verhindern können. Sind aber Schwachstellen ermittelt worden, ermöglichen diese, dass ein negativer Vorfall entsteht. Somit stellen Schwachstellen „indirekte“ Verdachtsursachen dar.	Eine „Erklärung“ des negativen Vorfalls erfolgt durch eine Ursachenanalyse. Die Ursachenanalyse kann auf Basis ihres Systemmodells kausale Erklärungen in Form von Ursache für den negativen Vorfall liefern. Auf Basis der Erklärungen können gezielter Maßnahmen eingesetzt werden. Kurzfristig werden korrigierende und rekonstruierende Maßnahmen eingesetzt, wobei die Ergebnisse auch zur längerfristigen Analyse von präventiven Maßnahmen dienen.

Tabelle 10: Kombiniertes IS-Sicherheitsmanagement

3 Expertisemodell

Das Expertisemodell beinhaltet die Konzepte und die Organisation der Problemlösungsprozesse des IS-Sicherheitsmanagements und wird in folgende Ebenen unterteilt:

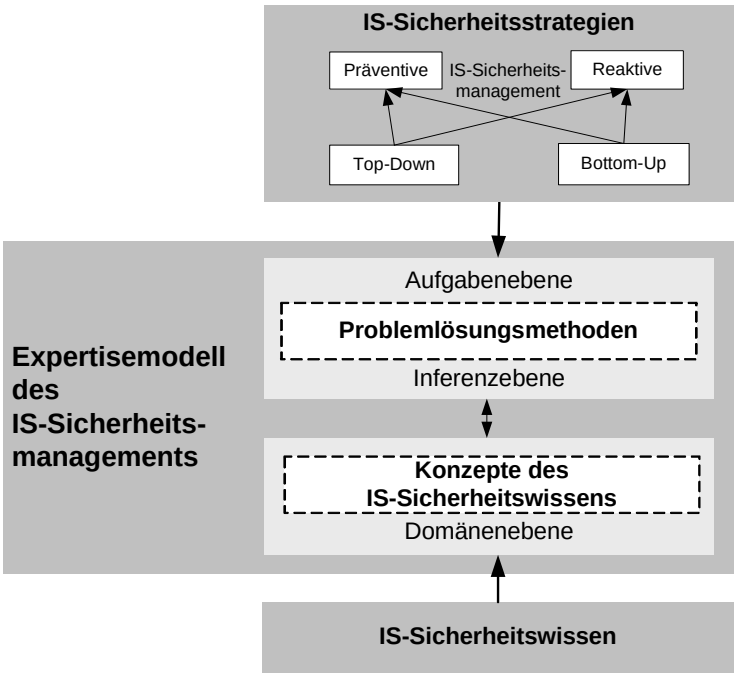


Abbildung 40: Zusammenfassende Darstellung des Expertisemodells

Die Aufgabenebene spezifiziert die Ziele der zu lösenden Aufgabe und deren generische Lösungsschritte. Ein Oberziel kann folglich die Etablierung eines gewissen IS-Sicherheitsniveaus mit Hilfe der Diagnose sein. Die Strategien des IS-Sicherheitsmanagements bilden die Grundlagen für die Aufgabenebene und somit die epistemologische Basis der Problemlösungsmethoden des Expertisemodells. Die Aufgabenebene wird durch tiefere Ebenen in Teilaufgaben und in Inferenzen zerlegt.

Die Inferenzebene beschreibt die Lösungsprozesse des IS-Sicherheitsmanagements mittels Inferenzen und Wissens-Rollen. Die Wissens-Rolle bildet die Verbindung zwischen der Domänen- und Problemlösungsmethode, wobei die Inferenz-Struktur in Abhängigkeit von der jeweiligen IS-Sicherheitsstrategie und deren Teilaufgaben variiert. Die Inferenz- und Aufgabenebene bilden zusammen die Problemlösungsmethoden; sie stellen dar, „wie“ die Domänenebene im Problemlösungsprozess verwendet wird.

Die Domänenebene spezifiziert Wissen über Konzepte des IS-Sicherheitsmanagements und deren Abhängigkeiten. Somit werden auf dieser Ebene grundlegende Konzepte, z.B. Schwachstellen oder Maßnahmen und deren Abhängigkeiten, abstrahiert dargestellt. Diese Konzepte bilden die Basis für die Konstruktion der Wissensbasis, die dann konkrete Instanzen der Konzepte beinhaltet. Eine Wissensbasis kann sinngemäß vereinfacht als „Container“ für Konzept-Instanzen gesehen werden.

Im folgenden Kapitel werden die Problemlösungsmethoden und die Konzepte des IS-Sicherheitswissens in einem Expertisemodell beschrieben. Zuerst erfolgt eine Übersicht der Erhebungsmethoden und Wissensquellen.

3.1 Wissensquellen

3.1.1 Erhebungsmethoden

Neben den folgenden Wissenserhebungsmethoden für Wissensquellen existiert eine Vielzahl anderer Erhebungsmethoden, die meist eine Weiterentwicklung bzw. Spezialisierung der folgenden Methoden darstellen[316]. Im Rahmen der Arbeit soll auf die drei am häufigsten verwendeten Methoden eingegangen werden[317]:

- Textanalyse
- strukturiertes und unstrukturiertes Interview
- Protokollanalyse

Textanalyse
Die Textanalyse ist geeignet, um in neue Domänen „einzusteigen“. Der Knowledge Engineer versucht, sich durch das Studium von einschlägiger Fachliteratur, Kriterien und Handbüchern einen Überblick zu verschaffen, um in einem späteren Interview gezielter Fragen stellen zu können. Die Textanalyse basiert auf schriftlichen Wissensquellen und dient somit der Ausarbeitung von Taxonomiewissen. Dabei können auch Strukturen und Konzepte der IS-Sicherheit ermittelt werden.

Interview
Das Interview stellt eine verbreitete Form der indirekten Wissenserhebung (Knowledge Engineer und IS-Sicherheitsexperte sind unterschiedliche Personen) dar. Beim unstrukturierten Interview gewinnt der Knowledge Engineer eine Übersicht über die Domäne, indem er den IS-Sicherheitsexperten befragt. Diese Interviewform ist ebenfalls für die Einstiegsphase in das Gesamtprojekt dienlich, um den Problemraum auf die wesentlichen Aspekte zu verkleinern. Beim strukturierten Interview werden dagegen gezielt Fragen gestellt, um detailliertes IS-Sicherheitswissen zu erlangen. Dafür kann entweder das unstrukturierte Interview oder eine vorgeschaltete Textanalyse als Interview-Grundlage nützlich sein. Durch ein fokussierendes Interview werden einzelne ausgewählte Aspekte tiefer durchdrungen, um z.B. gezielt Problemlösungsprozesse zu erheben.

Protokollanalyse
Um das Problemlösungswissen zu ermitteln, ist eine Protokollanalyse bzw. „Lautes Denken“ erforderlich. Im Gegensatz zur Textanalyse und zum Interview werden bei der Protokollanalyse vor allem Lösungsanweisungen erhoben. Hiermit soll das Problemlösungsverhalten eines IS-Sicherheitsexperten ermittelt werden, indem der Problemlösungsprozess mit Hilfe von „Lautem Denken“ verbal untersucht wird. Die Protokollanalyse stellt somit eine wichtige Ergänzung zum Interview dar.

[316] Siehe für weitere Erhebungsmethoden Lenz (1991), S. 183-197, Gabriel (1992), S. 210-222 und Schreiber et al. (2000), S. 187-214
[317] Vgl. Gabriel (1992), S. 208

Direkte oder indirekte Wissensakquisition
Bei den Erhebungsmethoden ist zu beachten, ob es sich um eine direkte oder indirekte Wissensakquisition handelt. Bei einer indirekten Erhebung ist i.d.R. ein Interview erforderlich. Bei der direkten Erhebung kann dies entfallen, da der Knowledge Engineer und der IS-Sicherheitsexperte die gleiche Person darstellen. Eine Zwischenstufe stellt die Interviewsituation dar, in der der Interviewer sich zwar als IS-Sicherheitsexperte erweist, jedoch nicht auf einem spezialisierten Bereich. Da sich hier zwei Experten gegenüberstehen (z.B. allgemeiner IS-Sicherheitsexperte und IS-Sicherheitsexperte im Bereich E-Commerce), entsteht eher eine „Konversation“ auf Expertenebene.

Zu Beginn des KE werden die vorhandenen Wissensquellen ermittelt und analysiert. Für das IS-Sicherheitsmanagement existieren folgende Wissensquellen-Kategorien:

- Implizites Erfahrungswissen (Menschliches Expertenwissen)
- Explizites Erfahrungswissen (IS-Sicherheitskriterien und weitere explizite Quellen)
- Explizites Vorschriftenwissen (Gesetzliche Vorschriften)

3.1.2 Implizites Erfahrungswissen

Implizites Expertenwissen ist in den „Köpfen“ von menschlichen Experten gespeichert und schwer formalisierbar, kommunizierbar und teilbar (Embodied Knowledge). Es beinhaltet subjektive Einsichten und ist tief in Handlungen und Erfahrungen von Individuen verankert, wie z.B. Ideale, Werte oder Gefühle. Dieses implizite Wissen beinhaltet Wissensstrategien in Form von unbewussten angewendeten Verhaltensregeln bzw. Problemlösungsmethoden, die für den Lösungsprozess entscheidend sind. Ein wesentlicher Bestandteil des WBS ist nicht „nur“ die Repräsentation des expliziten „offensichtlichen“ Wissens, sondern auch des impliziten „verborgenen“ Wissens.

Explizites Wissen ist um ein Vielfaches einfacher in eine Wissensbasis zu überführen als implizites Wissen, da der Vorgang der Explikation von implizitem, unstrukturiertem Wissen oft nur schwer oder gar nicht möglich ist (z.B. beim Allgemeinwissen). Aber gerade dieses implizite Wissen ist nötig, um die Problemlösungsprozesse zu repräsentieren[318]. Eine zentrale Aufgabe des KE ist die Überführung und Repräsentation des impliziten Problemlösungswissens des IS-Sicherheitsmanagements in explizite Problemlösungsmethoden von WBS.

[318] Vgl. Wolfertz (2001), S. 457

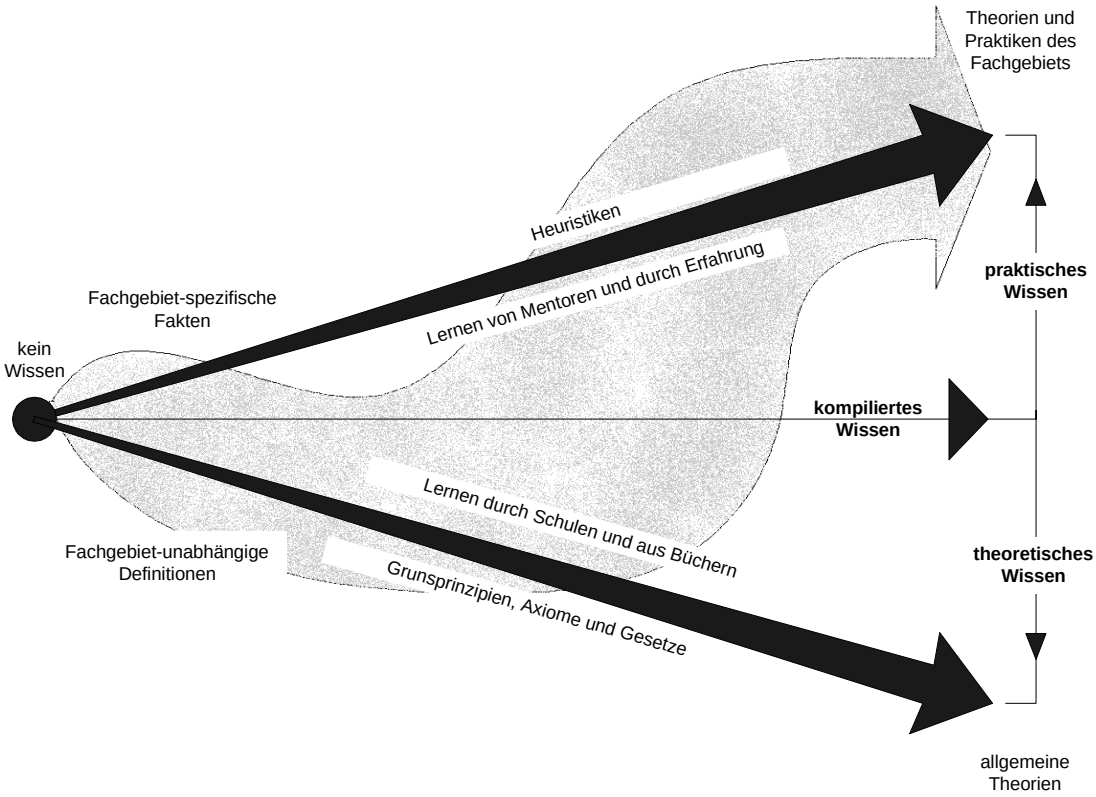


Abbildung 41: Modell des kompilierten Expertenwissens im Zeitablauf[319]

Die Herkunft und Struktur des menschlichen Expertenwissens lässt sich mit Hilfe einer Zeitachse darstellen. Grundsätzlich eignet sich das Individuum über einen Zeitraum schrittweise Wissen an, wobei folgende Unterscheidung erfolgt[320]:

- Theoretisches Wissen
  Im Laufe des Lebens erlernt ein Individuum zuerst in Schulen und durch Lesen von Lehrbüchern fachgebiet-unabhängiges Wissen, das als theoretisches Wissen oder Tiefenwissen bezeichnet wird[321]. Dieses Wissen liegt in Form von Definitionen, Axiomen und Gesetzmäßigkeiten vor und ist meist gut formalisierbar, strukturierbar und nachvollziehbar. Zudem ist theoretisches Wissen häufig in Form von „Basiswissen“ die Voraussetzung, um sich fachgebiet-spezifisches Wissen anzueignen.
- Praktisches Erfahrungswissen
  Fachgebiet-spezifische Probleme können dagegen alleinig mit theoretischem Wissen nicht gelöst werden, da der Lösungsraum für eine umfassende Problemlösungssuche zu groß ist. In seinem beruflichen Verlauf eignet sich ein Fachexperte zusätzlich fachgebiet-spezifisches Erfahrungswissen an, das als praktisches Wissen oder Oberflächenwissen bezeichnet wird; das praktische Wissen gewinnt im beruflichen Umfeld immer mehr an Bedeutung.

[319] Vgl. Harmon/King (1989), S. 38. Harmon/King bezeichnet das theoretische Wissen als Tiefenwissen und das praktische Wissen als Oberflächenwissen.
[320] Vgl. Harmon/King (1989), S 35 ff.
[321] Vgl. Thuy/Schnupp (1989), S. 63

Das praktische Wissen ermöglicht es dem Individuum, sich in einem Fachgebiet (z.B. IS-Sicherheit) schnell auf die wesentlichen Aspekte eines Problems zu konzentrieren und die Zusammenhänge zu erkennen[322]. Es beinhaltet häufig vages oder unvollständiges Wissen und wird meist durch Heuristiken und Daumenregeln beschrieben[323] und kann somit bei schlecht strukturierten Problemen eingesetzt werden. Das praktische Wissen ist für das Unternehmen - ebenfalls für den Experten selbst - ein sehr wertvolles Gut, das im Berufsleben z.T. unbewusst erworben wird und meist implizit im „Kopf" des Experten vorhanden ist. Dieses Expertenwissen macht „einen Berater zu einem Berater", da für einen Klienten gerade dieses Expertenwissen von Nutzen ist[324]. Die meisten wissensbasierten Systeme, die auf Expertenwissen ausgelegt sind, repräsentieren explizit das praktische Wissen, um es für eine konkrete Problemlösung verfügbar zu machen[325].

Es kann zusätzlich eine Differenzierung zwischen Wissen von Fortgeschrittenen und Experten erfolgen. Fortgeschrittene besitzen zwar ein fundiertes erlerntes Fachwissen, jedoch fehlt es an „praktischer" Erfahrung. Bei Absolventen eines Studienganges ist theoretisches Fachwissen vorhanden, das sie aber noch nicht angewandt haben. Der Experte, der z.T. über mehrere Jahrzehnte praktisches Problemlösungswissen entwickelt hat, verfügt vielleicht nicht über das umfangreiche aktuelle Fachwissen, kann aber durch seine „Intuition" praktische Probleme besser lösen als der „Theoretiker".

Allgemeinwissen

Die Repräsentation und Anwendung des Allgemeinwissens bzw. Weltwissens stellt eine besondere Problematik für das WBS dar. Das Allgemeinwissen hat keinen permanenten Bezug zu einem speziellen Aufgabenbereich, vielmehr wird aufgrund situations- und personenspezifischer Umstände entschieden, welche Bestandteile des Allgemeinwissens Verwendung finden. So ist z.B. zum Verstehen der Bedeutung von Begriffen oder Sätzen häufig zusätzliches Allgemeinwissen notwendig[326]. Dies macht deutlich, dass das komplette menschliche Allgemeinwissen durch das WBS jederzeit verfügbar sein muss, was (noch) nicht möglich ist[327].

Die negativen Auswirkungen dieses Problems sind bei der Problemlösung durch ein WBS als „Kliff- und Plateau Effekt" bekannt und bis heute nicht gelöst. So leisten WBS erfolgreiche Arbeit in eng eingegrenzten Aufgabengebieten, sobald aber das WBS nur geringfügig außerhalb seines Spezialgebietes angewandt wird, erfolgt ein sehr starker Kompetenzabbruch und das WBS liefert keine qualifizierte Lösung, da Allgemeinwissen fehlt[328]. Einen umfangreichen Versuch zur Modellierung von Allgemeinwissen bildet das Projekt „CYC", indem sehr viele Konzepte mit logischen Axiomen und Regeln formalisiert werden[329]. Pirlein (1995) bietet eine umfangreiche Übersicht von Commonsense Ontologien an, die eingesetzt werden können, um Allgemeinwissen abzubilden.

[322] Vgl. Harmon/King (1989), S 36
[323] Vgl. Thuy/Schnupp(1989), S. 65
[324] Vgl. Wolfertz (2001), S. 457
[325] Vgl. Puppe (1991), S. 189
[326] Siehe dazu das Beispiel in Strube et al. (2000), S. 50-52
[327] Vgl. Voß/Gutenschwager (2001), S. 355
[328] Vgl. Hoppe (1992), S. 22
[329] Vgl. Heller (1996), S. 23 und Fensel (2001), S. 15

3.1.3 Explizites Erfahrungswissen

Die Fachwissenschaften - wie die IS-Sicherheit - besitzen i.d.R. ein gut strukturiertes Begriffssystem, denn sie formulieren ihre Syntax und Semantik in ihrer Fachsprache. Somit bieten die Fachsprachen eine Grundlage für die explizite Normierung einer Domäne. Dies soll nicht darüber hinwegtäuschen, dass die Fachsprachen sich ständig in Bewegung und Diskussion befinden, wodurch eine endgültige Normierung nicht möglich ist. Trotz dieser Einschränkungen ist eine normierte Konzeptionalisierung und Formalisierung einer Fachwissenschaft-Domäne z.T. möglich[330].

IS-Sicherheitskriterien

Die IS-Sicherheitskriterien weisen den Charakter von allgemeinem anerkanntem und kompiliertem Erfahrungswissen auf und stellen somit das Ergebnis einer Normierung der Domäne IS-Sicherheit dar, welches in kommunizierbarer, verständlicher und strukturierter Form vorliegt (Disembodied Knowledge)[331]. Im Rahmen der Arbeit bilden die IS-Sicherheitskriterien eine wesentliche Grundlage für explizit repräsentiertes Erfahrungswissen.

Da Fachbegriffe der Kriterienwerke in expliziter und strukturierter Form (z.B. in Tabellen oder Listen) vorliegen, haben sie den Charakter eines Knowledge Dictionaries bzw. Glossars. Somit können Kriterien häufig direkt in ein elektronisches Glossar umgesetzt werden, was eine technische Repräsentation der Fachsprachen darstellt. Auch die Übernahme aus anderen Wissensquellen in ein Glossar wird erleichtert, da eine strukturierte Vorlage existiert.

Das Glossar beinhaltet aber nicht nur eine starre Auflistung der Fachbegriffe, sondern es kann auch zusätzlich Abhängigkeiten durch semantische Netze berücksichtigen. So wurden die semantischen Netze ursprünglich für die strukturierte Wissensbeschreibung entwickelt[332] und bieten die Möglichkeit, das Wissen in Netzstrukturen mit Hilfe von Kanten und Knoten abzubilden. Sie eignen sich besonders für die Abbildung einer stabilen Taxonomie oder der Sprachanalyse. Eine bewährte Methode zur Strukturierung von Fachausdrücken ist die Bildung von Netzen in Form von Hierarchien und Heterarchien, da sie eine verständliche und übersichtliche Darstellung bieten[333]. Die syntaktische und semantische Normierung bildet eine Zwischenstufe für die konzeptuelle Analyse und Repräsentation des IS-Sicherheitswissens.

Ein Beispiel für ein vernetztes Glossar bildet das Grundschutzhandbuch des BSI, das Grundschutz-Kriterien repräsentiert. Die Systembestandteile eines konkreten Informationssystems werden durch IT-Bausteine abgebildet, die mit einem Gefahren- und Maßnahmenkatalog verknüpft sind. Die Verknüpfungen werden durch Hyperlinks in einem HTML-Dokument realisiert. Die folgende Abbildung zeigt, wie das BSI-Grundschutzhandbuch mit Hilfe von HTML-Strukturen repräsentiert wird.

---

[330] Vgl. Puppe/Stoyan/Studer (2000), S. 601

[331] Der Konsens der Kriterien ist sicher nicht überall zu finden, aber durch die Legitimation durch nationale und internationale anerkannte Gremien ist ein gewisses Maß an Übereinkunft entstanden.

[332] Vgl. Lenz (1991), S. 233

[333] Vgl. Puppe et al. (1996), S. 78

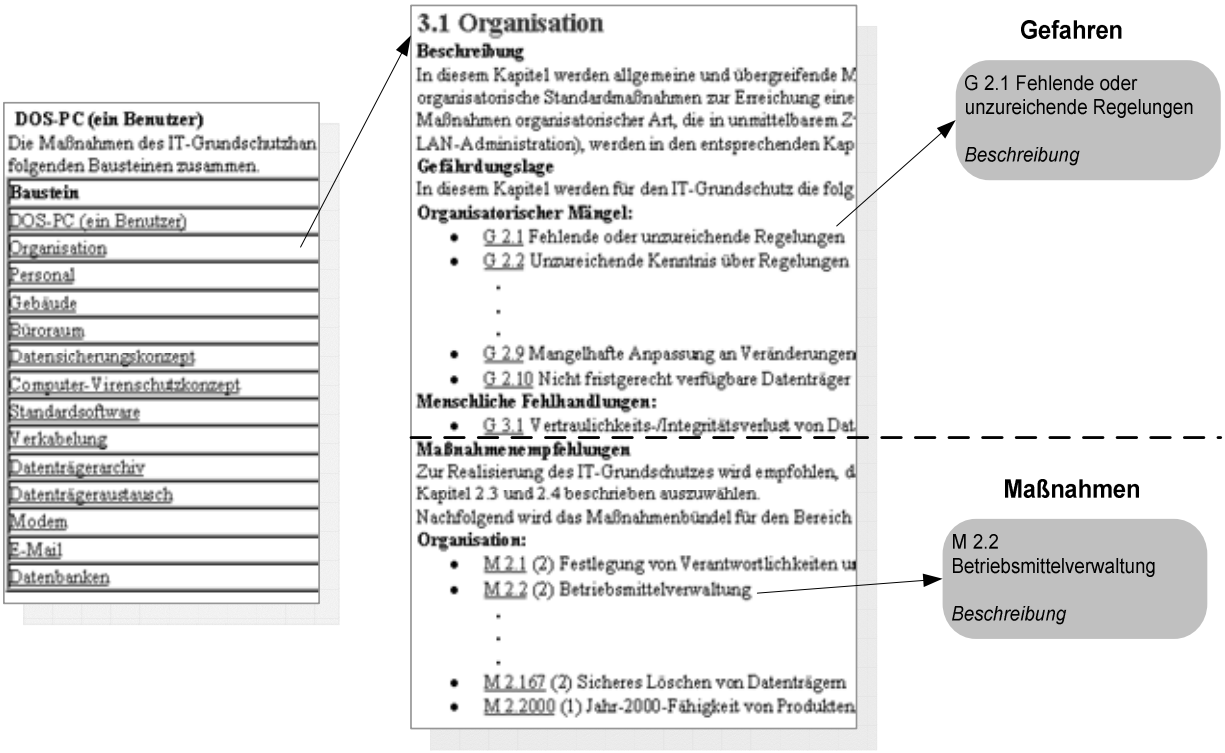


Abbildung 42: Aufbau des HTML-basierten BSI-Grundschutzhandbuchs

Weitere explizite Wissensquellen

Es existieren weitere schriftliche Wissensquellen in vielfältiger Ausprägung. In den schriftlichen Wissensquellen wird neben deklarativem Wissen (z.B. reine Begriffsdeklarationen) auch prozedurales Wissen in Form von Handlungsanweisungen repräsentiert. Bei diesen Wissensquellen ist nicht davon auszugehen, dass eine allgemein akzeptierte Fachsprache verwendet wird. In dem Bereich der IS-Sicherheit lassen sich grob folgende schriftliche Wissensquellenbereiche differenzieren:

- Fachwissen durch Fachzeitschriften
  Expertenwissen aus Fachzeitschriften, wie z.B. die KES oder DuD, wobei hier die Überführung dieses Expertenwissens in ein WBS auf Grund der Unstrukturiertheit (schriftliche Form) problematischer ist als bei Kriterienwerken. Dieses schriftliche Expertenwissen hat dafür den Vorteil, dass konkrete Handlungsanweisungen bzw. Heuristiken weitergegeben werden können.
- Unternehmenseigene IS-Sicherheitskonzepte
  Es hat sich in den letzten Jahrzehnten in der Praxis und in der Theorie ein vielfältiges IS-Sicherheitswissen über Strukturen, Abläufe und Problemlösungsstrategien in Institutionen herausgebildet, deren Resultate in IS-Sicherheitskonzepten dokumentiert sind. Die Problematik liegt in der Verfügbarkeit dieser IS- Sicherheitskonzepte und in der starken Verknüpfung mit der unternehmensindividuellen IS-Sicherheitsproblematik.

3.1.4 Explizites Vorschriftenwissen

Die Bereiche der gesetzlichen Regelungen haben einen Vorschriftencharakter und sind dem Bereich des Datenschutzes zuzurechnen. Dieses Vorschriftenwissen ist relevant für die Erstellung von IS-Sicherheitskonzepten, weil davon auszugehen ist, dass sich Institutionen an Gesetze halten wollen. Somit sollte das WBS auch in der Lage sein, Gesetzesverstöße aufzudecken und Lösungen anzubieten. Als relevante Gesetze sind in erster Linie das BDSG und die Bundesländerdatenschutzgesetze zu nennen. Aber auch andere Gesetze und Verordnungen besitzen Relevanz im Bereich Datenschutz, wie z.B. Teledienstedatenschutzgesetz (TDDSG)[334], Fernmeldeverkehr-Überwachungs-Verordnung (FÜV)[335], Entwurf eines Elektronischen Geschäftsverkehr-Gesetzes (EGG)[336], Entwurf einer Telekommunikations-Überwachungsverordnung (TKÜV)[337], Telekommunikations-Kundenschutzverordung (TKV)[338], Telekommunikations-Datenschutzverordnung (TDSV)[339], Teledienstgesetz (TDG)[340], Telekommunikationsgesetz (TKG)[341], Signaturgesetz (SigG)[342] und das Gesetz zur Kontrolle und Transparenz in Unternehmensbereichen (KonTraG)[343]. Europäische Vorschläge zum Schutz personenbezogener Daten[344] und andere bereichspezifische Gesetze, wie z.B. Steuergesetze, Strafgesetze oder ärztliche Schweigepflicht[345], sind zusätzlich zu berücksichtigen. Auch „ … *das Internet ist kein rechtsfreier Raum, wie viele in ihrer Begeisterung über das neue Medium anfangs glaubten. Dies zeigt sich insbesondere, wenn man die Rechtsbeziehungen zwischen Anbietern und Nutzern untersucht.*“[346] Das Internet beinhaltet Problembereiche bezüglich der Online-Verträge, des Verbraucherschutzes, der Gewährleistung/Haftung oder des Urheberrechts. Eine Übersicht von Problemstellungen bzgl. des Online-Rechts gibt es in Schwerdtfeger et al. (1999). Zudem sind bei den oben genannten Gesetzen auch deren Verknüpfungen zu beachten.

Die Umsetzung der gesetzlichen Regelungen steht in einem Interdependenzverhältnis mit den erforderlichen Maßnahmen. So können erst technische und organisatorische IS-Sicherheitsmaßnahmen eine Einhaltung der Gesetze gewährleisten. Andererseits geben die Gesetze Vorgaben für die zu entwickelnden Maßnahmen vor. Am folgenden Beispiel lässt sich die Verknüpfung zwischen den Bereichen darstellen:

---

[334] Vgl. TDDSG (1997)
[335] Vgl. FÜV (1995), § 9
[336] Vgl. EGG (2001), Zielsetzung
[337] Vgl. TKÜV (1998), § 9(1)
[338] Vgl. TKV (2002), § 6(2); § 13(3); § 14 und § 21
[339] Vgl. TDSV (2002)
[340] Vgl. TDG (2001), § 4 Abs. 4 Nr. 10
[341] Vgl. TKG (1996), § 12; § 15 und elfter Teil des Gesetzes
[342] Vgl. SigG (2001), § 14
[343] Aufgrund des in Kraft getretenen KonTraG (1998) wurde § 91 Abs. 2 Aktiengesetz (AktG) geändert, wodurch der Vorstand geeignete Maßnahmen zu treffen hat, um ein Überwachungssystem einzurichten, damit gefährdende Entwicklungen früh erkannt werden. Die Verletzung dieser Organisationspflicht kann zur Schadensersatzpflicht führen (§ 93 Abs. 2 AktG). Dieses Überwachungssystem beinhaltet die angemessene Gestaltung sicherer IS-Systeme als wesentlichen Teil einer Risikostrategie. Vgl. Risknews (2000), S. 3 und Voßbein (2001), S. 75
[344] Vgl. EG-Datenschutzvorschlag (1999)
[345] Vgl. Sienkiewicz (1994), S. 20-29 und Haaz (1997), S. 35
[346] Vgl. Schwerdtfeger (1999), S. 8

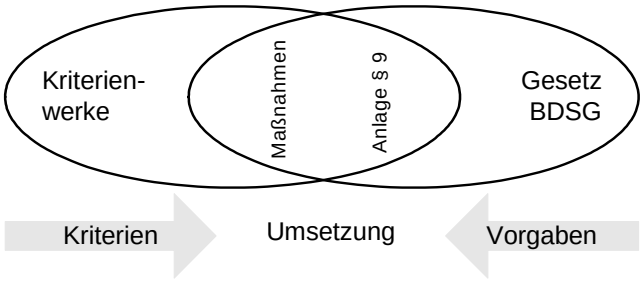


Abbildung 43: Interdependenzen zwischen Kriterien und Gesetzen

Das BDSG fordert in der Anlage zu § 9 Satz 1[347] die Umsetzung der Gesetze durch Maßnahmen[348]. Diese Maßnahmen können z.B. durch Kriterien gewährleistet werden.

Bei der Entwicklung von Informationssystemen sollten weitere datenschutzrechtliche Aspekte berücksichtigt werden. So werden in § 3a BDSG (2001) die Datenvermeidung und Datensparsamkeit[349] sowie der Gebrauch der Anonymisierung[350] und Pseudonymisierung[351] als Gestaltungsanforderung für Informationssysteme beschrieben[352].

3.2 Domänenmodell der IS-Sicherheitsstrategien

3.2.1 Ontologien

Eng verbunden mit der konzeptuellen Analyse und Konstruktion der IS-Sicherheitsdomäne sind die Ontologien, um eine Verteilung und Wiederverwendung von Wissen zu ermöglichen[353]. Im KE werden Ontologien eingesetzt, um den Aufbau von Domänenmodellen zu erleichtern und diese Modelle über verschiedene wissensbasierte Anwendungen hinweg zu vereinheitlichen[354]. Ontologien ermöglichen eine explizite Konzeptualisierung der Semantik einer Domäne durch folgende Punkte[355]:

- Die Spezifizierung von Ontologien ist aus syntaktischer und semantischer Sicht reichhaltiger als die traditionellen Datenbankansätze.
- Die Beschreibung von Domänenwissen durch Ontologien beinhaltet zusätzlich natürlichsprachliche Ausprägungsformen.
- Ontologien beinhalten „vereinheitlichte“ Ausdrücke (Terminologien), die einen Konsens für einen bestimmten Bereich besitzen, damit sie austauschbar sind.

---

[347] Vgl. BDSG (2001)
[348] Vgl. Behrens (1997), S. 27-29
[349] Siehe dazu auch „Datenschutzfreundliche Technologien“. Vgl. Gundermann (1999) und Ernestus (1999)
[350] „*Anonymisieren ist das Verändern personenbezogener Daten derart, daß die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.*“ § 6 BDSG (2001)
[351] „*Pseudonymisierung ist das Verändern personenbezogener Daten derart, daß die Einzelangaben über persönliche oder sachliche Verhältnisse ohne Nutzung der Zuordnungsfunktion nicht oder nur mit einem unverhältnismäßigen Aufwand einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.*“ Gundermann (1999), S. 146 und Vgl. § 6(a) BDSG (2001)
[352] Vgl. Gundermann (1999), S. 141
[353] Vgl. Chandrasekaran/Josephson/Benjamins (1999), S. 21
[354] Vgl. Puppe/Stoyan/Studer (2000), S. 622
[355] Vgl. Fensel (2001), S. 1

- Ontologien liefern eine Domänentheorie und nicht die Struktur eines „Datencontainers".

Seit Anfang der 90er Jahre werden Ontologien in vielen Bereichen der KI-Forschung eingesetzt. Ontologie kann als „ *...an explicit specification of conceptualization*"[356] definiert werden. Die Konzeptualisierung besitzt die Identifikation von Konzepten und deren Beziehungen in einer Domäne bzw. kann als„*…eine abstrakte und vereinfachte Sichtweise auf Phänomene eines Realitätsausschnitts verstanden* [werden], *der für vorgegebene Erkenntniszwecke von Interesse ist.*"[357] Dies bedeutet, dass die Konzeptualisierung eine zweck- und auch subjektabhängige Auszeichnung der Realitätsaspekte darstellt. Die „Ontologie-Konzepte" bilden das Ergebnis der Konzeptualisierung ab. Sie werden als sprachliche Konstrukte ausgedrückt und stellen deshalb auch eine begriffliche bzw. natürlich-sprachliche Vorstrukturierung dar. Dies wird durch die Bereitstellung einer vordefinierten bzw. normierten Zusammenstellung von Begriffen einer Domäne erreicht. Ontologien werden deshalb als „wieder verwendbare" Begriffe (reusable terminologies[358]) bezeichnet.

Ontologien haben neben einer terminologischen und syntaktischen Dimension zudem auch eine semantische. Aus semiotischer Sicht erfolgt durch die Semantik eine Trennung zwischen dem Inhalt (Daten) und seiner Bedeutung[359]. Die Darstellung der Verwendung bzw. Bedeutung der natürlich-sprachlichen Ausdrücke innerhalb einer Ontologie erfolgt durch semantische Regeln. Die Regeln legen fest, wie aus expliziten natürlich-sprachlichen Ausdrücken das darin implizit enthaltene Wissen erschlossen wird bzw. wie die implizit „verborgenen" Aspekte explizit formuliert werden.

Die Spezifikation von Ontologien erfolgt durch vielfältige Beschreibungssprachen, die formalen Charakter besitzen, wobei eine explizite und formale Spezifikation von Ontologien tendenziell eine maschinell verarbeitende Sprache erfordert. Die formale explizite Darstellung der Konzepte orientiert sich an Beschreibungssprachen der Wissensrepräsentation, wie z.B. Frames mit Objekt-Attribut-Wert Strukturen[360]. Das Ziel der Spezifikation ist eine formalsprachliche Präzision der flexiblen natürlich-sprachlichen Konzeptualisierungsebene.

Der Widerspruch zwischen natürlich- und formal-sprachlicher Sicht der Ontologien löst sich infolge unterschiedlicher Ontologie-Ebenen auf. Auf der Ebene der Konzeptualisierung lassen Ontologien formal- und natürlich-sprachliche Ausdrücke zu, die die Grundlage der Spezifikationsebene bilden. Auf der Spezifikationsebene zeichnet sich somit eine Ontologie durch formale Semantik aus, die in der zugrunde liegenden Konzeptualisierung natürlich-sprachlich beschrieben wird. Hierdurch lässt sich eine formal-sprachliche Präzision auf der Spezifikationsebene mit natürlich-sprachlicher Ausdrucksreichhaltigkeit und -flexibilität auf der Konzeptionsebene kombinieren[361].

Eine weitere wesentliche Eigenschaft der Ontologie ist die geteilte (shared) Sicht auf eine Domäne: „*Ontologien stellen ein gemeinsames Verständnis einer Domäne zur Verfügung und ermöglichen so die zwischenmenschliche Kommunikation, aber auch die Kommunikation zwi-*

[356] Gruber (1993), S. 199
[357] Zelewski/Schütte/Siedentopf (2001), S. 187
[358] Vgl. Motta (1999), S. VII
[359] Vgl. Krcmar (2000), S. 13
[360] Vgl. Studer/Benjamins/Fensel (1998), S. 188
[361] Vgl. Zelewski/Schütte/Siedentopf (2001), S. 192

schen Anwendungssystemen und ihren Benutzern.“[362] Aus dieser Eigenschaft ergibt sich, dass Ontologien typischerweise in Kooperation zwischen mehreren Personen entwickelt werden mit dem Ziel einer Konsensfindung bei oftmals sehr unterschiedlichen Sichten auf eine Domäne[363]. Diese Ontologie-Eigenschaft wird auch als „ontological commitment“ bezeichnet[364]. Deshalb sind insbesondere Wissensquellen von Interesse, die ein weitgehendes gemeinsames normiertes Verständnis für die Domäne IS-Sicherheit beinhalten, wobei dies insbesondere bei Kriterienwerken der Fall ist.

Kriterienwerke sind z.T. als Standards[365] veröffentlicht[366], was zu einer „… *Vereinfachung der Durchführung von Transaktionen zwischen Akteuren bzw. zu einem einfachen Austausch von Informationen …*“[367] führt. Hierdurch erlangen Standards eine „extensionale Ausprägung“, was eine nach außen dokumentierte und kommunikationsfähige IS-Sicherheit ermöglicht. Hierbei sei die Problematik der gemeinsamen Verständigung erwähnt, denn der Konsens bzw. die Akzeptanz eines Standards kann in Abhängigkeit des jeweiligen Umfeldes variieren.

Um Ontologien für die IS-Sicherheit zu erstellen, ist eine Konzeptualisierung und Spezifikation der Domäne erforderlich. Das Ergebnis dieser „Wissensanalyse“ ist ein Domänenmodell von relevanten Konzepten mit ihren Eigenschaften und Abhängigkeiten, die auf ein „formales“ WBS überführt werden. Hierfür werden folgende Ausprägungsformen von Ontologien verwendet, die jeweils eine spezifische Rolle in dem Knowledge Engineering spielen[368]:

- Domänenontologien erfassen das Wissen einer bestimmten Domäne und sind somit nur für diese Domäne gültig. Diese Art der Ontologien bildet die Grundlage für das Domänenmodell des Expertisemodells.
- Repräsentationsontologien spezifizieren die Ausdrucksmöglichkeiten von Repräsentationssprachen. Diese Ontologien legen die Primitive von Wissensrepräsentationssprachen, wie z.B. durch Frames, Produktionsregeln und Fragenkataloge, fest.

Als weitere Ontologieformen werden häufig Aufgaben- und Methodenontologien genannt[369], wobei sich diese Formen der Ontologie im Konflikt mit den Wissens-Rollen der Problemlösungsmethoden befinden. Die Methodenontologien definieren die domänenunabhängigen Problemlösungskonzepte; durch die Aufgabenontologien werden die Begrifflichkeiten verschiedener Typen von Aufgaben definiert. Durch die gleichzeitige Verwendung von der Aufgaben- und Methodenontologien und Wissens-Rollen der Problemlösungsmethoden entsteht ein begrifflicher Konflikt, da die Ontologien und Wissens-Rollen zwar häufig die gleichen Bezeichnungen haben, sich aber auf unterschiedlichen Ebenen befinden. Dies wird durch folgende Aussage von van Heijst/Schreiber/Wielinga (1997) deutlich: „*In summary then, we believe that knowledge roles are integral components of PSMs* [PSM = Problem Solving Me-

[362] Puppe/Stoyan/Studer (2000), S. 622 und siehe auch Gruber (1993)
[363] Vgl. Richards/Simoff (2001), S. 122
[364] Vgl. Hesse (2002), S. 478
[365] Standards, die von einer Standardisierungsorganisation verabschiedet wurden, werden auch als Normen bezeichnet. Somit ist der Begriff „Norm“ eine Spezialisierung des Begriffs „Standard“ und wird im Rahmen der Arbeit synonym verwendet. Vgl. Buxmann/König (1998), S. 122
[366] Z.B. ISO 17799 oder ISO 15408
[367] Vgl. Buxmann/König (1998), S. 122
[368] Commonsense Ontologien werden im Rahmen der Arbeit nicht behandelt.
[369] Vgl. Guarino (1997)

thods]. *Although they often have the same names they can, not be replaced by ontological concepts because they are of another epistemological type.*"[370]

Konzepte des IS-Sicherheitsmanagements im Expertisemodell

Die IS-Sicherheits-Konzepte im Expertisemodell besitzen als Extension eine Menge von Realitätsausschnitten (Objekte), welche ähnliche Eigenschaften haben. Die Intension von IS-Sicherheits-Konzepten besteht in der natürlichen und semiformalen Beschreibung von IS-Sicherheitsaspekten auf einer epistemologischen Ebene. Dieser Aspekt findet sich auch in Konzeptklassen des objektorientierten Ansatzes wieder. Hierbei sind für die Arbeit folgende Unterschiede zu beachten:

- Konzepte beinhalten keine Methoden, Funktionen oder Operationen[371].
- Konzepte werden unabhängig von der Symbolebene auf der Wissensebene explizit beschrieben. Dies bedeutet, dass Konzepte eine abstraktere epistemologische Sichtweise besitzen als „formale" Klassen und Objekte.
- Konzepte können in semiformaler (z.B. Hypertext) oder sogar in natürlich sprachlicher Form beschrieben werden. Aber auch objektzentrierte Darstellungen, wie semantische oder inferentielle Netze, sind möglich. Umso formaler die Darstellung ist, desto leichter lässt sie sich später auf der Symbolebene repräsentieren.

Insgesamt werden durch das Expertisemodell die wesentlichen erkenntnistheoretischen Konzepte explizit formuliert. Die Konstruktion der Konzepte durch die typischen Wissensrepräsentationsformalismen, wie z.B. mittels Frames, Fragenkataloge oder Produktionsregeln, erfolgt erst auf der Symbolebene.

[370] Heijst/Schreiber/Wielinga (1997), S. 317
[371] Vgl. Schreiber et al (2000), S. 92

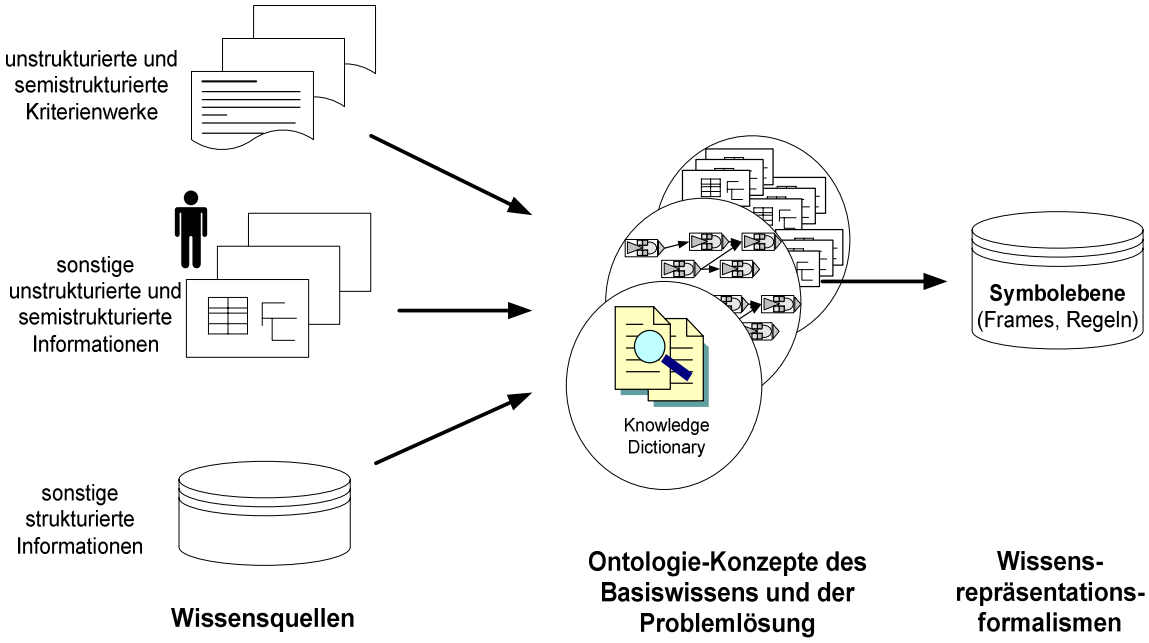


Abbildung 44: Zusammenhang zwischen Wissensquellen und Ontologie-Konzepten[372]

Die Ontologie-Konzepte[373] des Domänenmodells werden wie folgt unterteilt:

- Konzepte des Basiswissens enthalten die Fachterminologie und definitorisches Wissen über deren Beziehungen. Die Formalisierung ist meist unproblematisch, da diese z.B. durch Kriterien in expliziter und deklarativer Form vorliegt. Das Basiswissen soll möglichst unabhängig vom Problemlösungsprozess modelliert werden.
- Konzepte der Problemlösung[374] beinhalten die Grundlage für das Lösungswissen der spezifischen Problemlösungsprozesse. Diese Konzepte sind deshalb im Gegensatz zum Basiswissen eng mit dem Problemlösungsprozess verbunden. Die Repräsentation ist deutlich schwieriger als beim Basiswissen, da das Bewertungs- bzw. Lösungswissen häufig nur in impliziter Form vorhanden ist. Dies gilt insbesondere für das implizite IS-Sicherheitswissen.

[372] Erweitert in Anlehnung an Studer et al. (2000), Kapitel 2.3
[373] Ontologie-Konzepte werden im Folgenden als Konzepte bezeichnet.
[374] Die Begriffe „Problemlösungskonzepte“, „Lösungskonzepte“ und „Bewertungskonzepte“ werden in der Arbeit synonym verwendet.

Domänenwissen	
Konzepte des Basiswissens	**Konzepte der Problemlösung**
allgemeines in die „Breite“ ausgelegtes IS-Sicherheitswissen	spezifisches IS-Sicherheitswissen für Problemlösungsprozesse festlegen
unabhängig von dem Problemlösungsprozess	abhängig von dem Problemlösungsprozess
häufig schon in expliziter Form vorhanden	meist nur in impliziter Form vorhanden
definitorische natürlich-sprachliche und semi-formale Beschreibung	inferentielle natürlich-sprachliche und semi-formale Beschreibung
Explizierung durch Tabellen und Hierarchien	Explizierung durch semantische Regeln

Tabelle 11: Differenzierung zwischen Basis- und Problemlösungskonzepten

In dem folgenden Kapitel erfolgt eine Beschreibung der Basiskonzepte und Problemlösungskonzepte.

3.2.2 Basiskonzepte des IS-Sicherheitswissens

Sicherheitsrelevante Bereiche

Um die IS-Sicherheit und ihre Basiskonzepte unabhängig von einem speziellen Unternehmen zu strukturieren bzw. zu klassifizieren, werden sicherheitsrelevante Bereiche bzw. Ebenen verwendet. Stelzer (1993) hat zwischen den physischen, logischen, organisatorischen, rechtlich-wirtschaftlichen Ebenen differenziert[375]. Die physische Ebene fasst die sicherheitstechnisch relevanten Bereiche der Informationssysteme (z.B. Hardware, Datenspeicher, Netzwerk oder Gebäude) zusammen, wohingegen sich die logische Ebene auf sicherheitsrelevante Daten und Programme bezieht. In der organisatorischen und sozialen Ebene werden die organisatorischen Bereiche in Form von Aufbau- und Ablauforganisation strukturiert[376]. Für die IS-Sicherheit sind zusätzliche gesellschaftliche, organisatorische und rechtlich-wirtschaftliche Aspekte nötig, um das vollständige Spektrum der Sicherheit zu beschreiben[377].

Die Kriterienwerke strukturieren die IS-Sicherheitsaspekte in sicherheitsrelevante Bereiche, wobei verschiedene Ausprägungsformen in unterschiedlichen Detaillierungsgraden existieren. Das BSI-Grundschutzhandbuch verwendet ein Schichtenmodell, die BS 7799/ISO 17799 eine Kapitelstruktur, die CC eine Klassen- und Familienstruktur und das CobiT-Framework Domänen-Prozesse. Sicherheitsrelevante Kriterienwerk-Bereiche sind eine anwendungsorientierte und unternehmensunabhängige Strukturierung der IS-Sicherheit, denen Maßnahmen zugeordnet sind. Sind diese Maßnahmen vorhanden, ist davon auszugehen, dass der Bereich ein gewisses IS-Sicherheitsniveau besitzt. Hierdurch sind Kriterienwerke direkt auf das Informationssystem anzuwenden und unterstützen somit die Top-Down Strategie, denn die Bereiche sind so weit wie möglich unternehmens- und plattformunabhängig. Den Bereichen können auch andere Konzepte, wie z.B. Gefahren, zugeordnet werden.

Sicherheitsrelevante Elemente

„*Sicherheitsrelevante Elemente der Informationsverarbeitung sind alle Elemente, die durch Gefahren für die Informationsverarbeitung unmittelbar oder mittelbar beeinträchtigt werden können.*“[378] Sicherheitsrelevante Elemente versuchen somit das „reale“ unternehmensspezifische Informationssystem so präzise wie möglich in einem Informationssystemmodell abzu-

[375] Vgl. Stelzer (1993), S. 28
[376] Vgl. Krallmann (1989), S. 93 und Rupietta (1996), S. 57
[377] Vgl. Hartmann/Karger (2001), S. 379
[378] Stelzer (1993), S. 32

bilden. Dabei wird angenommen, dass die konkreten sicherheitsrelevanten Elemente „zu ermitteln“ bzw. „greifbar“ sind. Dies ist - wenn überhaupt - für IT-Systeme auf physischer und logischer Ebene möglich, wobei auch hier nur eine Approximation stattfindet.

Sicherheitsrelevante Elemente unterstützen somit den Bottom-Up orientierten Ansatz, da eine Abbildung der Informationsverarbeitung in Form eines spezifischen Informationssystemmodells des Unternehmens erfolgt. Dadurch wird ein möglichst realistisches Modell bzgl. der IS-Sicherheit des jeweiligen Informationssystems (nach)modelliert, das eine computergestützte automatisierte Verarbeitung der individuellen IS-Sicherheit ermöglicht.

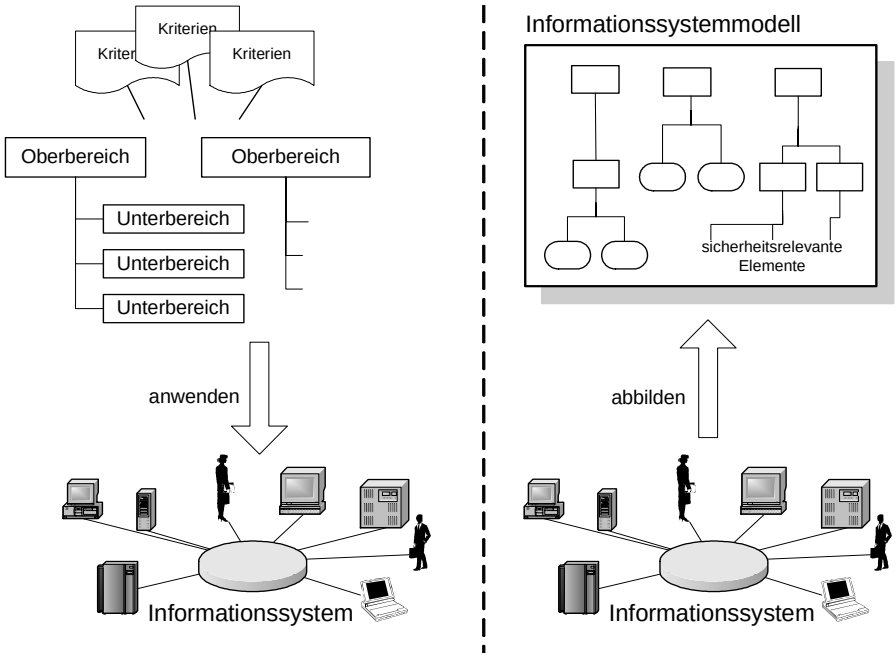


Abbildung 45: Unterschiede zwischen sicherheitsrelevanten Bereichen und Elementen

Eine Abgrenzung zwischen sicherheitsrelevanten Elementen und Bereichen ist nicht eindeutig möglich, denn es gibt Zwischenstufen, wie sie bei den hybriden Ansätzen anzutreffen sind. Die folgende Heuristik ist zur Differenzierung hilfreich:

- Erfolgt eine weitgehend allgemeine Sichtweise, die unabhängig von einem spezifischen Informationssystem ist, werden sicherheitsrelevante Bereiche verwendet. Bereiche werden insbesondere in der anwendungsorientierten Top-Down IS-Sicherheitsstrategie eingesetzt.
- Erfolgt eine konkrete Sichtweise auf ein spezifisches Informationssystem, ist von sicherheitsrelevanten Elementen auszugehen, welche in der abbildungsorientierten Bottom-Up IS-Sicherheitsstrategie Verwendung finden.

Gefahrenquellen und Gefahren (Bedrohungen)

Auf Basis von Gefahrenquellen entstehen Gefahren - anders ausgedrückt - die Gefahren lassen sich auf Gefahrenquellen zurückführen. Gefahrenquellen und deren Gefahren sind häufig nicht offensichtlich und verursachen erst bei ihrer Aktivierung negative Auswirkungen. Dies ist in den meisten Fällen ein zu später Zeitpunkt, um Schaden zu verhindern.

Gefahrenquellen können die Ursache für

- beabsichtigte Gefahren[379] oder
- für unbeabsichtigte bzw. zufällige Gefahren

sein.

Für die Auswahl einer geeigneten Maßnahme, um eine Gefahr zu verhindern oder zu reduzieren, ist die Kenntnis der Gefahr und ihrer Quelle bedeutend. So können bei bestimmten Gefahren - z.B. natürliche Quellen wie Sturm oder Erdbeben - nur detektivische und korrigierende Maßnahmen eingesetzt werden. Bei anderen Gefahren können zusätzlich präventive Maßnahmen verwendet werden. In der Abbildung können die grau unterlegten Gefahren im Ansatz bekämpft werden. Die anderen Gefahren befinden sich außerhalb des Wirkungsbereichs von einem Unternehmen und es können nur deren Auswirkungen bekämpft werden.

interne Quellen	Technik	Mensch (bewusst oder unbewusst)
externe Quellen	Natur/Umfeld	

Tabelle 12: Klassifikation von Gefahrenquellen[380]

Gefahrenquellen lassen sich zusätzlich in interne und externe Gefahrenquellen differenzieren. Der Mensch bildet eine interne (z.B. Mitarbeiter) und externe Gefahrenquelle (z.B. Hacker); er ist die einzige Gefahrenquelle, welche bewusst Schaden verursachen kann. Die meisten Schäden werden durch unbewusstes Handeln der Mitarbeiter, wie z.B. durch Fehlbedienung oder Nachlässigkeit, verursacht[381]. Gegen Gefahren technischer Herkunft kann ein Unternehmen am effektivsten Einfluss nehmen[382], da sie meist innerhalb des eigenen Einflussbereichs liegen. Dieser Einfluss ist aber zu relativieren, da die Informationssysteme eine hohe Komplexität und einen hohen Integrationsgrad besitzen.

In der Tabelle 13 erkennt man, dass vom Menschen die meisten Gefahren ausgehen[383]. Auf das Umfeld, insbesondere die Natur oder „höhere Gewalt“, kann das Unternehmen am wenigsten Einfluss nehmen. Es können nur die Auswirkungen bekämpft werden, da die Herkunft selbst nicht verhindert werden kann. Dafür treten Gefahrenquellen aus Natur und Umfeld am seltensten auf[384]. Es können neben der Natur weitere sehr schwer beeinflussbare Gefahren entstehen, wie z.B. unklare Gesetze, starke Einflussnahme von Regierungen, Terrorismus oder Krieg.

[379] In der Arbeit schließt der Begriff „Gefahren“ inhaltlich den Begriff „Bedrohungen“ mit ein.
[380] Vgl. Stelzer (1993), S. 30 und Voßbein, J (1999), S. 59
[381] Vgl. Voßbein, J. (1999), S. 65
[382] Vgl. Konrad (1998), S. 25
[383] Vgl. Britsch (1995), S. 124 und BSI-Grundschutzhandbuch (2000), Kapitel 2.3
[384] Siehe auch Britsch (1995), S. 124; Voßbein, J. (1999), S. 68 und BSI-Grundschutzhandbuch (2000), Kapitel 2.3

Welche dieser Gefahrenbereiche haben in Ihrem Haus in den vergangenen beiden Jahren tatsächlich zu mittleren bis größeren Beeinträchtigungen geführt?		
Basis der Prozentuierung		260
	Summe	Prozent
von Menschen direkt verursachte Gefahren	135	52 %
Irrtum und Nachlässigkeit eigener Mitarbeiter	79	30 %
unbeabsichtigter Fehler von Externen (z.B. Wartungstechnikern)	23	9%
Manipulation zum Zweck der Bereicherung	6	2%
unbefugte Kenntnisnahme, Informationsdiebstahl, Wirtschaftsspionage	16	6%
Sabotage	4	2%
Hacking (Vandalismus, Probing, Missbrauch, …)	21	8%
Malware (Viren, Würmer, Trojanische Pferde usw.)	64	25%
technische Defekte/Qualitätsmängel	85	33%
Hardware bedingt	38	15%
Software bedingt	50	19%
Mängel der Dokumentation	8	3%
höhere Gewalt (Feuer, Wasser usw.)	8	3%
Sonstige	17	7%

Tabelle 13: Gefahrenbereiche[385]

Gefährdendes Ereignis

Der Zustand des Einwirkens einer Gefahr auf ein sicherheitsrelevantes Element wird als „gefährdendes Ereignis“ bezeichnet. Hierbei wird unter einem Ereignis „*…eine Zustandsveränderung, für die es einen Ort und eine Zeitdauer oder einen Zeitpunkt gibt*“[386], verstanden. Die sicherheitsrelevanten Elemente werden mit Hilfe eines Informationssystemmodells abgebildet, die mit relevanten Gefahren aus einer Gefahrenliste ergänzt werden. Aus der Kombination der Gefahren mit dem sicherheitsrelevanten Element erfolgt die Beschreibung des gefährdenden Ereignisses.

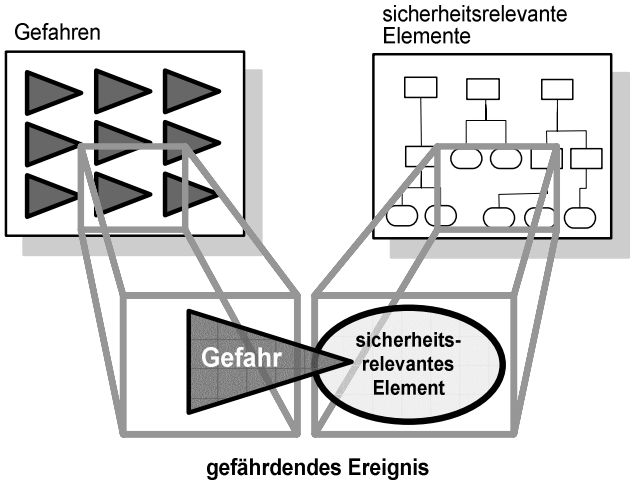


Abbildung 46: Gefährdendes Ereignis[387]

[385] Vgl. Voßbein, R./Voßbein, J. (2002a), S. 14
[386] Reimer (1991), S. 22
[387] Erweitert in Anlehnung an Konrad (1998), S. 188

Gefährdende Ereignisse bilden die Basis für eine kausale Beschreibung, mit deren Hilfe die Ursache in Form eines gefährdenden Ereignisses und deren Wirkung als Konsequenz dargestellt wird.

Konsequenzen
Die negativen Auswirkungen eines gefährdenden Ereignisses werden als Konsequenzen bezeichnet. Gefahren können mehrere Konsequenzen (z.B. Ausfall eines IT-Systems) verursachen, wobei der Verlust der Verfügbarkeit zuerst bemerkt wird. Als ein besonderes Problem stellt sich das rechtzeitige Erkennen von Konsequenzen heraus, deren Auswirkungen nicht sofort bemerkt werden, wie z.B. der Verlust an Integrität oder Vertraulichkeit. So werden diese Konsequenzen meist zu spät oder gar nicht erkannt.

Eine Konsequenz kann sich zu einer Gefahr für andere sicherheitsrelevante Elemente entwickeln. So besitzt ein Verlust der Verfügbarkeit einer Festplatte direkte Konsequenzen für die Verfügbarkeit des Systems. Diese Rückkopplung kann über mehrere Ebenen erfolgen und gewinnt dadurch eine hohe Komplexität. Ob eine negative Erscheinung eine Gefahr oder eine Konsequenz darstellt, ist von der jeweiligen Sichtweise abhängig. So ist z.B. für das sicherheitsrelevante Element A der negative Zustand Z eine Konsequenz, wohingegen für das sicherheitsrelevante Element B der negative Zustand Z eine Gefahr darstellt.

Schwachstellen
Damit eine Konsequenz überhaupt auftreten kann, ist eine Schwachstelle erforderlich. So wird eine Konsequenz erst durch eine Schwachstelle ermöglicht, wobei dies eine indirekte Verursachung darstellt, da erst gefährdende Ereignisse die Konsequenzen direkt verursachen. Eine offene Schwachstelle wird durch Maßnahmen geschlossen, wodurch eine Gefahr nicht mehr negativ auf ein sicherheitsrelevantes Element einwirken kann und somit keine Konsequenz entsteht. Für den Begriff Schwachstellen ergeben sich daraus folgende Sichtweisen[388]:

- Die Schwachstellen können als eine konkrete negative Eigenschaft bzw. Fehler in Elementen oder im Bereich von Informationssystemen interpretiert werden. Sie bilden somit erst die Voraussetzung, dass eine Gefahr an einem sicherheitsrelevanten Element wirksam wird. Diese Definition berücksichtigt die kausale Sichtweise der FMEA Risikoanalyse.
- Schwachstellen können auch durch das Fehlen von Sicherheitsmaßnahmen definiert werden. Wenn diese Maßnahmen fehlen oder diese ungenügend sind, kann eine Gefahr auf ein sicherheitsrelevantes Element negativ einwirken. Diese Definition bildet die Basis für die Problemlösung der Sicherheits-Schwachstellenanalyse und des IT-Grundschutzes nach dem BSI.

Die beiden Schwachstellendefinitionen schließen sich aber nicht gegenseitig aus. Denn beide Sichtweisen haben gemeinsam, dass für eine wirksame „Schließung“ der Schwachstellen adäquate Maßnahmen ergriffen werden müssen.

[388] Vgl. Stelzer (1993), S. 212 und Konrad (1998), S. 28

Maßnahmen

Um Gefahren und Schwachstellen zu vermindern oder gar zu verhindern, können Maßnahmen nach dem Wirkungszeitpunkt[389]

- präventiv
- detektivisch
- korrigierend (rekonstruierend)

differenziert werden.

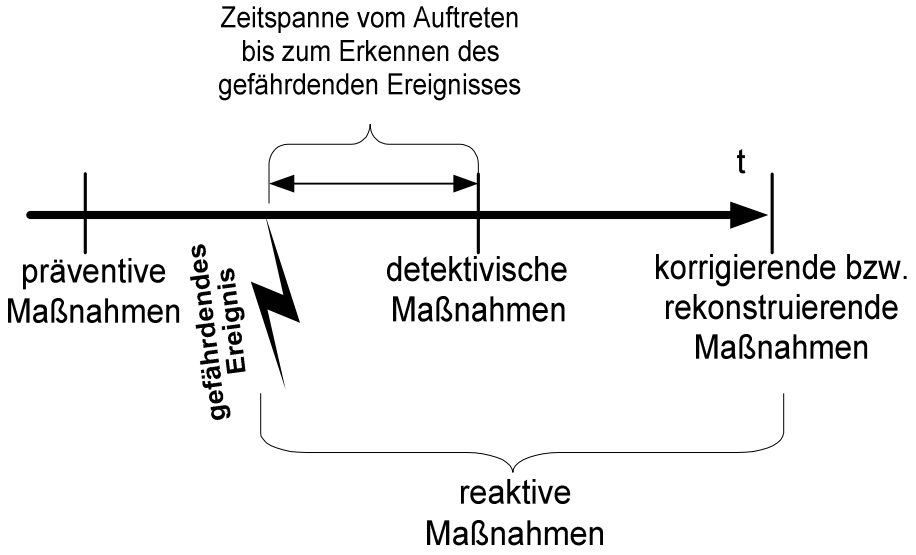


Abbildung 47: Wirkungszeitpunkte von Sicherungsmaßnahmen[390]

In der Abbildung ist der Wirkungszeitpunkt dargestellt, wobei präventive Maßnahmen die effektivsten sind, da sie ein gefährdendes Ereignis erst gar nicht aufkommen lassen. Dies erfordert, dass die Gefahrenquelle ausgeschaltet oder gemindert wird. Ein völliges Ausschalten der Gefahrenquelle im Bereich der Natur und des Menschen ist in den seltensten Fällen möglich. Aus diesem Grund sind Maßnahmen erforderlich, die reaktiv auf ein gefährdendes Ereignis bzw. dessen gefährdenden Zustand reagieren. Aber auch diese reaktiven Maßnahmen sollten im Vorfeld präventiv implementiert werden.

Detektivische Maßnahmen können im Gegensatz zu den präventiven Maßnahmen ein gefährdendes Ereignis bzw. Zustand nicht verhindern, sondern nur mit speziellen Indikatoren erkennen und eine Warnung ausgeben. Aufgrund der Warnung können automatische oder manuelle Aktionen initiiert werden. Detektivische Maßnahmen sind z.B. Rauchmelder oder Virenscanner. Inwieweit detektivische Maßnahmen das Auftreten eines gefährlichen Ereignisses sofort oder dies erst nach einem gewissen Zeitraum entdecken, ist von der Art der Verletzung und der Qualität des Indikators abhängig. So ist z.B. eine Verletzung der Verfügbarkeit schneller zu entdecken als der Verlust der Vertraulichkeit.

Erst im Zusammenspiel von detektivischen Maßnahmen mit darauf folgenden korrigierenden Maßnahmen werden die Gesamtmaßnahmen sinnvoll, da eine Warnung ohne Reaktion das Sicherheitsproblem nicht beseitigt. Insbesondere bei manuellen Aktionen durch den Men-

[389] Vgl. Voßbein, J (1999), S. 122
[390] Erweitert in Anlehnung an Voßbein, J. (1999), S. 122

schen sind diese durch zusätzliche aufbau- und ablauforganisatorische Regelungen zu flankieren[391]. So sollten bei einem erkannten Brand oder Wassereinbruch nach einem gewissen organisatorischen Ablaufplan, welcher die entsprechenden Schritte und Personen beinhaltet, Gegenmaßnahmen eingeleitet werden.

Korrigierende und rekonstruierende Maßnahmen sollen die negativen Folgen eines gefährdenden Ereignisses und den gefährdenden Zustand soweit wie möglich abschwächen. Typische Maßnahmen sind z.B. Backup oder ein Notfall- und Wiederanlaufplan[392]. Dabei sind die Reaktionszeit und die Güte der detektivischen Maßnahmen von entscheidender Bedeutung. Wird das gefährdende Ereignis schnell und vollständig erkannt und frühzeitig eine Warnung ausgegeben, ist ein schnelles Reagieren von korrigierenden Maßnahmen gegeben.

Korrigierende Maßnahmen haben einen reaktiven Charakter, wohingegen rekonstruierende Maßnahmen einen Wiederherstellungscharakter (z.B. in Form von Backup) besitzen. Korrigierende Maßnahmen versuchen direkte Konsequenzen, wie z.B. den Verlust der Verfügbarkeit, direkt zu mindern, wohingegen die rekonstruierenden Maßnahmen einen längeren Zeitraum benötigen. Eine eindeutige Abgrenzung von korrigierenden und rekonstruierenden Maßnahmen ist meist nicht möglich, da sie oft ineinander greifen.

Weitere verfeinerte Klassifikationen von Maßnahmen bieten z.B. das BSI-Grundschutzhandbuch[393] oder Krallmann[394]. Welche Detaillierungstiefe man wählt, ist von dem konkreten Umfeld und der Analysetiefe abhängig. Eine Kombination von Klassifikationskriterien in Form einer n-dimensionalen Matrix - z.B. physikalische Maßnahmen mit präventiver und reaktiver Dimension erweitert - kann eine detaillierte Differenzierung ermöglichen[395].

3.2.3 Problemlösungskonzepte der IS-Sicherheitsstrategien

Die Problemlösungskonzepte bilden in der Arbeit tendenziell die semantische Dimension von Ontologien auf einer natürlich-sprachlichen Ebene ab. Natürlich-sprachliche Abhängigkeitskonzepte legen die Grundstruktur von Inferenz-Regeln fest, indem sie mittels natürlich-sprachlicher Ausdrücke das implizite semantische Lösungswissen bzw. „Bedeutungswissen“ explizieren. Diese Abhängigkeitskonzepte ähneln den Inferenz-Regeln der formalen Logik hinsichtlich ihrer Fähigkeit, implizites Wissen zu explizieren. Die Abhängigkeitskonzepte werten aber zusätzlich Wissen über den Inhalt bzw. Bedeutung der natürlich-sprachlichen Ausdrücke aus. Für die Darstellung der Abhängigkeitskonzepte ist eine differenzierte Sicht auf die IS-Sicherheits-Domäne und die Problemlösungsprozesse der IS-Sicherheitsstrategien notwendig, da diese Abhängigkeitskonzepte die Schnittstelle zwischen der spezifischen Problemlösungsmethode des IS-Sicherheitsmanagements und dem Domänemodell bilden.

[391] Vgl. Schäfer (1995), S. 205
[392] Vgl. Schäfer (1995), S. 229
[393] Vgl. BSI-Grundschutzhandbuch (2000), Kapitel 2.3
[394] Vgl. Krallmann (1989), S. 52
[395] Vgl. Krallmann (1989), S. 85 ff.

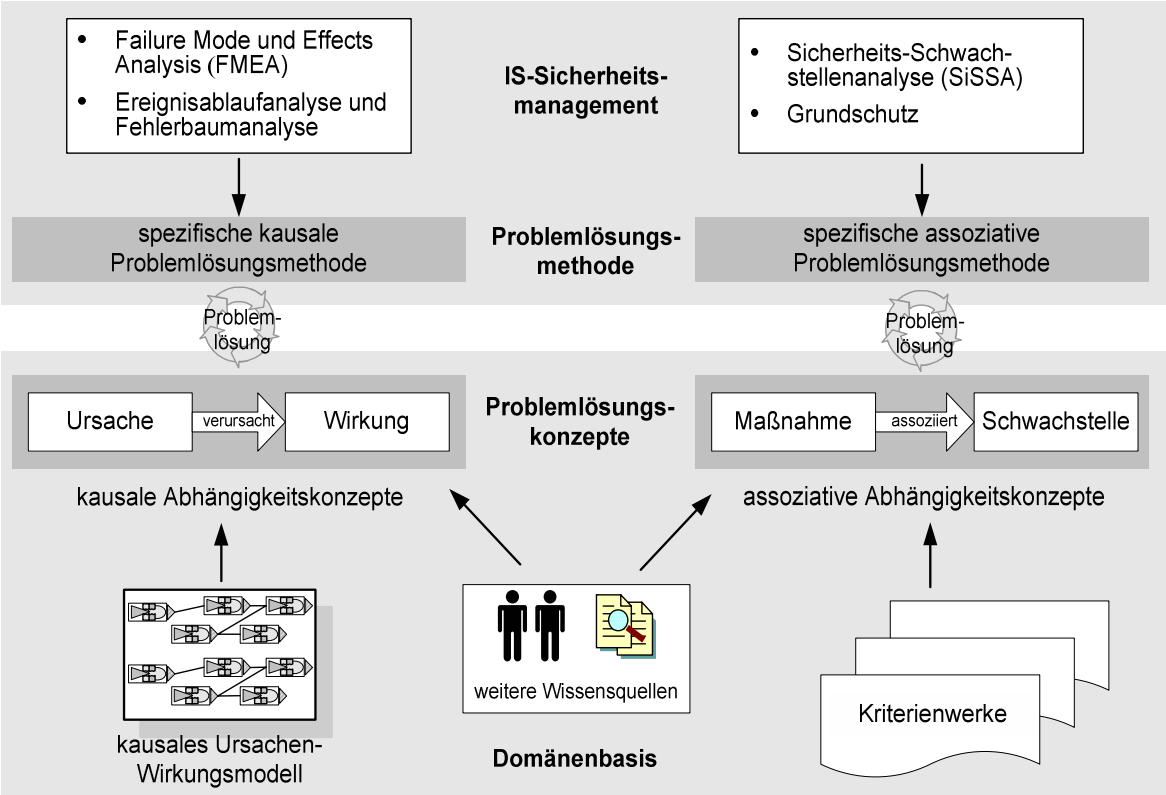


Abbildung 48: Problemlösungskonzepte

Die Problemlösungskonzepte des IS-Sicherheitsmanagements basieren auf folgenden kausalen und assoziativen Abhängigkeitskonzepten:

- Die kausalen Abhängigkeitskonzepte ermöglichen - ausgehend von einer Ursache - zuverlässig eine Wirkung vorauszusagen bzw. eine Wirkung durch eine Ursache zu erklären. Grundlage für diesen Problemlösungsprozess bilden die formalisierte FMEA und ein kausales Ursachen-Wirkungsmodell.
- Die assoziativen Abhängigkeitskonzepte ermöglichen - ausgehend von Maßnahmen - Schwachstellen zu ermitteln. Grundlage für diesen Problemlösungsprozess bilden die SiSSA und der Grundschutz, die allgemein gültige Kriterienwerke verwenden.

Auf diesen Abhängigkeitskonzepten werden ebenfalls andere Wissensquellen abgebildet, wobei hier insbesondere das individuelle kompilierte Expertenwissen angeführt werden soll. Das „zusätzliche“ individuelle menschliche Expertenwissen kann durch beide Abhängigkeitskonzepte formalisiert werden. Dabei ist zu beachten, ob zuverlässiges oder heuristisches Wissen vorliegt, da im ersten Fall das kausale und im zweiten Fall das assoziative Abhängigkeitskonzept vorzuziehen ist.

3.2.3.1 Kausale Abhängigkeitskonzepte

Die zentrale Aufgabe des kausalen Abhängigkeitskonzeptes ist, aus dem Verhalten und den Funktionen der Informationssysteme die entscheidenden kausalen sicherheitsrelevanten Abhängigkeiten zu extrahieren.

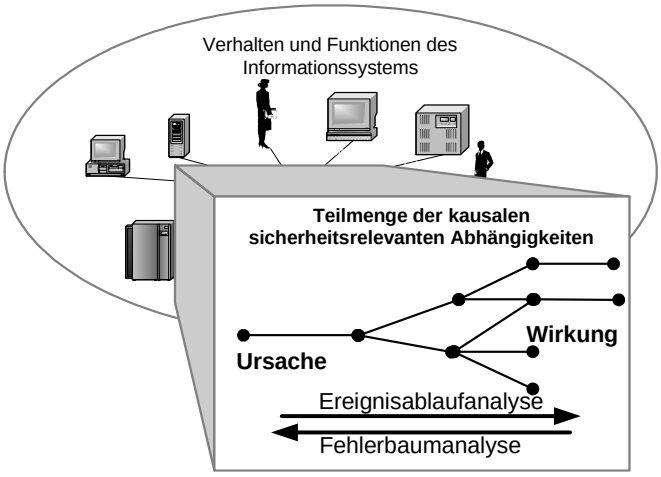


Abbildung 49: Teilmenge kausaler sicherheitsrelevanter Abhängigkeiten[396]

Diese sicherheitsrelevante Untermenge des Verhaltens und die Funktionen eines Informationssystems in Form eines Ursachen-Wirkungsmodells werden mittels des FMEA Verfahrens angewandt. FMEA ist eine formalisierte Methode, um

- ausgehend von einem unerwünschten Zustand oder Ereignis des Systems (z.B. Ausfall) die dafür möglichen Ursachen zu ermitteln (Fehlerbaumanalyse);
- ausgehend von einem Anfangsereignis bzw. einer Ursache die Folgewirkung bzw. Fehlerfortpflanzung sowie den Endzustand im System zu ermitteln (Ereignisablaufanalyse).

Kausales Ursachen-Wirkungs-Modell

Die Ursachen-Wirkungs-Kausalmodelle können durch Fischgräten-Diagramme, die nach seinem Erfinder auch als „Ishikawa-Diagramm“ bezeichnet werden, visualisiert werden. Die Kausalmodelle stellen die Interdependenzen in allgemeiner Form dar, die durch Belegung mit konkreten Werten eine Kausalkette bzw. Ursachen-Wirkungs-Zusammenhänge repräsentieren. In dem folgenden Beispiel können auf sicherheitsrelevante Elemente Gefahren (negative Ursachen) oder deren Gegenmaßnahmen (positive Ursachen) einwirken und zu einer negativen oder positiven Wirkung führen. Damit Ursachen-Wirkungsmodelle erfolgreich eingesetzt werden, ist zuverlässiges IS-Sicherheitswissen notwendig, damit eindeutige Rückschlüsse gezogen werden können. Bei technischen Systemen, welche gut verstanden sind, ist dies möglich, wobei man sich hier auf die wesentlichen IS-Sicherheitsfunktionen beschränkt.

[396] In Anlehnung an Konrad (1998), S. 179 und erweitert bzgl. eines Ursachen-Wirkungsmodells.

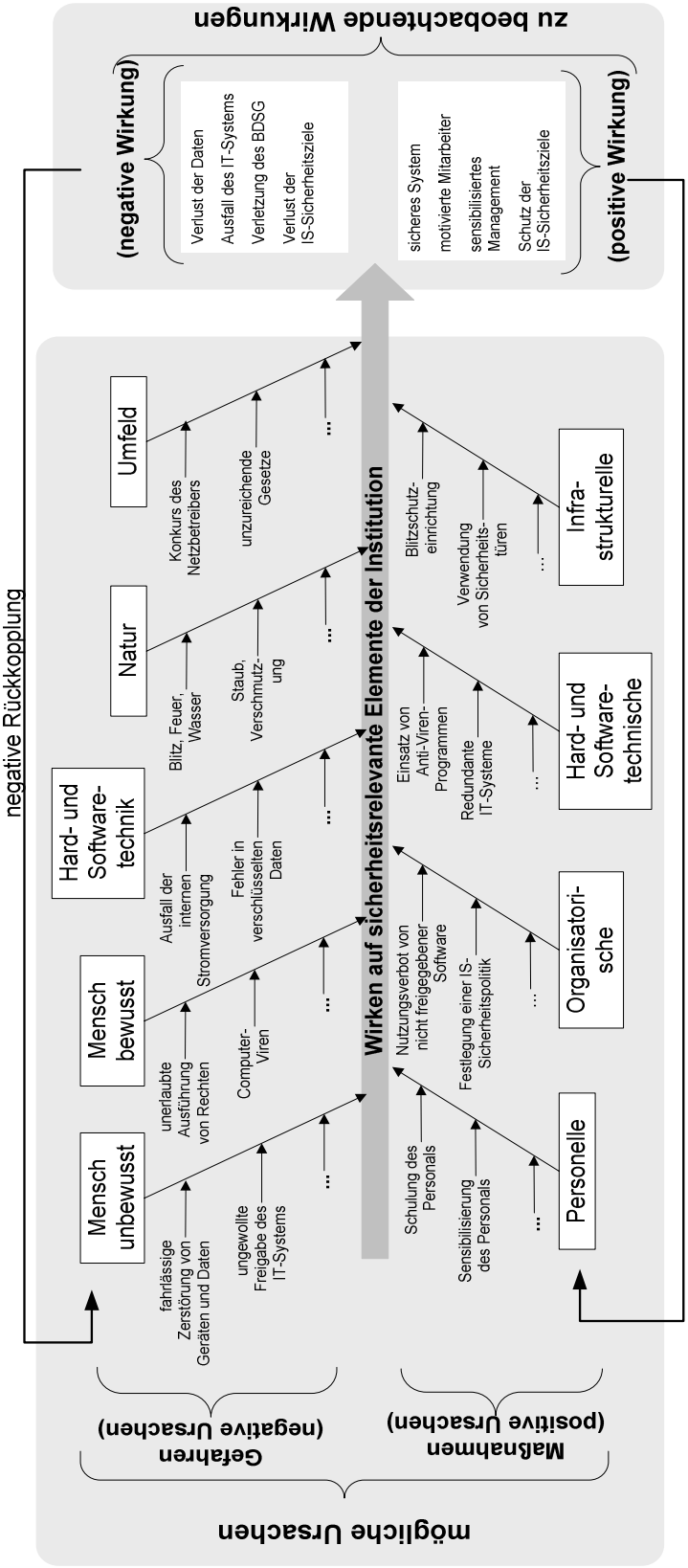


Abbildung 50: Fischgräten-Kausalmodell[397]

[397] In Anlehnung an Müller/Tietjen (2000), S. 49 und erweitert auf die IS-Sicherheitsproblematik

Kausalmodell des gefährdenden Ereignisses
In dem folgenden Kausalmodell wird die kausale Kette von der Gefahr über das gefährdende Ereignis bis zur Konsequenz dargestellt. Im Schaubild werden die Maßnahmen auf Basis des Wirkungszeitpunktes differenziert.

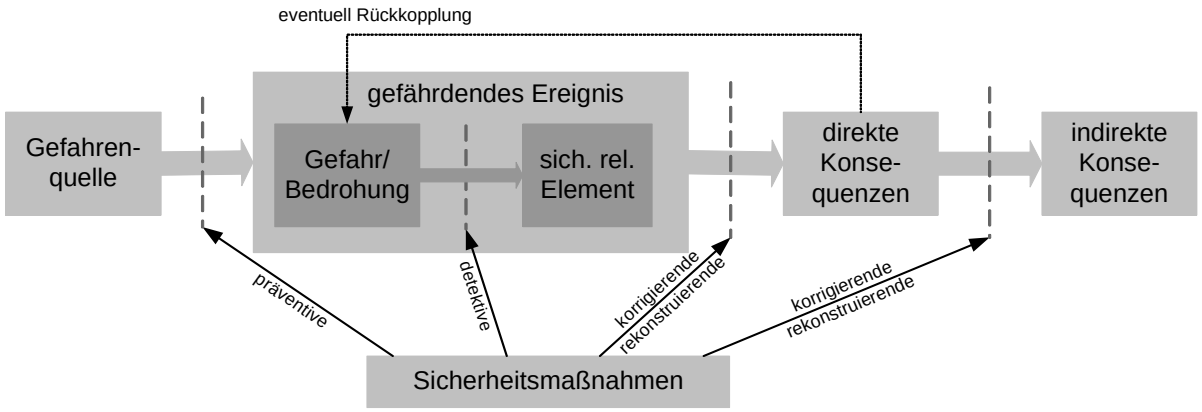


Abbildung 51: Kausalmodell des gefährdenden Ereignisses[398]

Durch diese Darstellung wird deutlich, dass Maßnahmen in unterschiedlichen Abschnitten des Kausalmodells realisiert werden, wobei eine Maßnahme am „Anfang“ des Kausalmodells positivere Wirkung aufweist als Maßnahmen am „Ende“ des Kausalmodells. Das Kausalmodell besitzt somit das Wissen, um die Konsequenzen eines gefährdenden Ereignisses vorherzusagen oder die Ursachen von Konsequenzen zu erklären. Durch die modellhafte Abbildung der Rückkopplungen wird die Komplexität der Beziehung zwischen den Sicherheitsaspekten deutlich. So kann die Konsequenz (Wirkung) eines gefährdenden Ereignisses wiederum eine Gefahr (Ursache) für andere sicherheitsrelevante Elemente darstellen.

3.2.3.2 Assoziative Abhängigkeitskonzepte

Eine andere Sichtweise hat das assoziative Abhängigkeitskonzept, das nicht auf dem Bottom-Up Ansatz basiert, sondern auf dem Top-Down Ansatz. Dies bedeutet, dass nicht ein Kausalmodell erstellt wird, welches auf einer individualisierten System- bzw. Funktionsanalyse basiert, sondern dass allgemein anerkannte Kriterien als kompiliertes Erfahrungswissen direkt auf die Institution angewandt werden. Es wird im Rahmen der SiSSA und des Grundschutzes durch assoziative Abhängigkeitskonzepte auf Schwachstellen geschlossen. Die Domänenbasis für assoziative Abhängigkeitskonzepte bilden die Kriterienwerke.

In der Abbildung 52 ist die Grundlage für den assoziativen Zusammenhang dargestellt. Für Gefahren existieren jeweils eine oder mehrere Maßnahmen. Wenn keine oder ungenügende relevante Maßnahmen vorhanden sind, enthalten die betroffenen sicherheitsrelevanten Bereiche Schwachstellen, sofern die Maßnahmen relevant sind. Andererseits können sicherheitsrelevante Elemente Schwachstellen in Form von negativen Eigenschaften bzw. Fehlern besitzen, welche auch durch Maßnahmen geschlossen werden können. In beiden Fällen ermöglicht

[398] Erweitert in Anlehnung an Stelzer (1993), S. 38

erst eine geöffnete Schwachstelle das „Durchschlagen“ einer Gefahr und somit das Entstehen einer negativen Konsequenz.

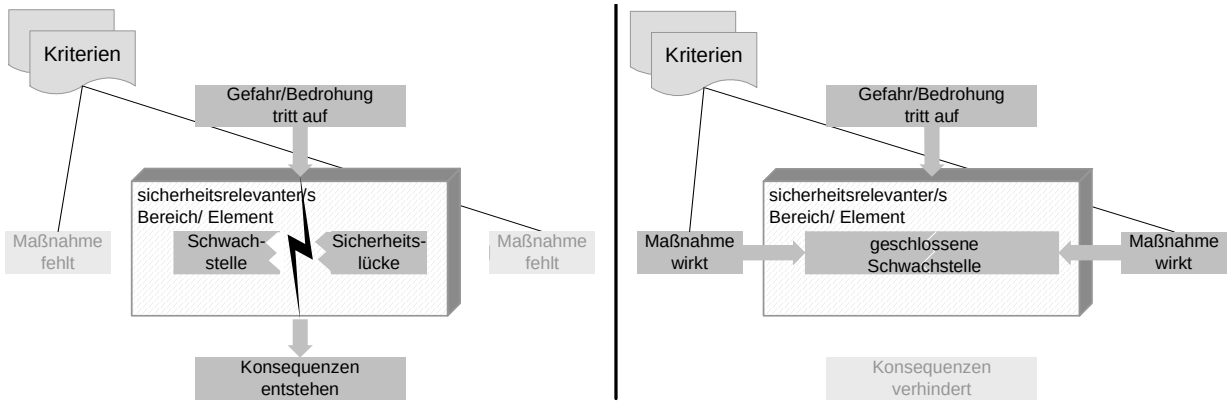


Abbildung 52: Assoziativer Maßnahmen-Schwachstellen Ansatz[399]

Die Grundlage bildet die Assoziation, dass durch fehlende oder nicht geeignete Maßnahmen auf Schwachstellen „gedeutet“ werden kann. Zusätzlich wird die Assoziation erweitert, indem Konsequenzen auf Schwachstellen deuten, da für die „Aktivierung“ einer Konsequenz eine Schwachstelle erforderlich ist. Um diese Schwachstelle zu schließen, werden die benötigten Maßnahmen eingesetzt.

Da meist eine vollständige Elimination der Gefahrenquelle nicht möglich ist, wie z.B. bei Menschen oder Umwelt, besteht somit fast immer eine potentielle Kombination aus Gefahren und sicherheitsrelevanten Elementen. Unter dem Aspekt von vorhandenen Maßnahmen ist dies nicht weiter bedrohlich, da durch eine „geschlossene“ Schwachstelle keine negative Konsequenz erfolgt und somit die Wahrscheinlichkeit des Auftreffens einer Gefahr nicht von Relevanz ist[400]. Auf Basis dieser Überlegung kann es ausreichend sein, die Schwachstellen zu identifizieren, ohne vorher eine komplexe Ursachen-Wirkungsanalyse der spezifischen IS-Sicherheitsumgebung im Rahmen einer Risikoanalyse zu erstellen. Zudem lassen sich auf der assoziativen Basis neben technischen auch organisatorische Schwachstellen identifizieren, die in Ursachen-Wirkungsmodellen nur unzureichend zu beschreiben sind.

[399] Erweitert in Anlehnung an Nosworthy (2000), S. 600
[400] Vgl. Kailay/Jarratt (1995), S. 457

3.2.3.3 Diagnostische Wissensarten der Abhängigkeitskonzepte

Im Folgenden werden die oben dargestellten Abhängigkeitskonzepte auf Wissensarten der Problemlösungsklasse „Diagnostik“ abgebildet. In der Diagnostik wird zwischen folgenden grundlegenden Wissensarten differenziert[401]:

- sicheres Wissen,
- statistisches und fallbasiertes Wissen,
- heuristisches (assoziatives) Wissen und
- modellbasiertes (kausales) Wissen.

Diese diagnostischen Wissensarten prägen die spätere Auswahl und Spezifikation der Problemlösungsmethoden. Das unten abgebildete Abhängigkeitsmodell stellt die assoziativen und kausalen Abhängigkeitskonzepte im Zusammenhang mit dem heuristischen und modellbasierten Diagnosewissen dar.

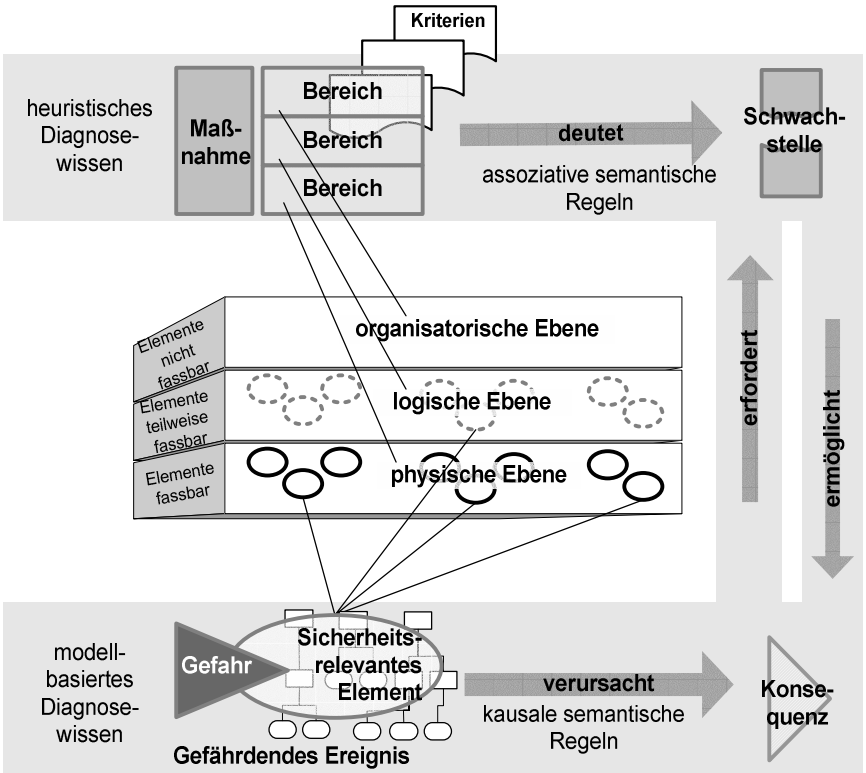


Abbildung 53: Integriertes kausales und assoziatives Abhängigkeitsmodell

Assoziative semantische Regeln (assoziatives Diagnosewissen)
Assoziatives Diagnosewissen und dessen semantische Regeln basieren auf heuristischem und kompiliertem Erfahrungswissen von IS-Sicherheitsexperten, welches durch Kriterien explizit dargestellt und somit in sicherheitsrelevanten Bereichen anwendungsorientiert repräsentiert wird. Dadurch ist dieser anwendungsorientierte Ansatz auf die Problembereiche direkt bzw. „universell“ einsetzbar, da der Ansatz deutlich schwächere Voraussetzungen hinsichtlich der Beschreibung eines konkreten Informationssystems besitzt als der kausale Ansatz. Es können

[401] Vgl. Puppe (1991), S. 80

auch übergeordnete sicherheitsrelevante Aspekte der organisatorischen und rechtlichen Ebene beschrieben werden. Diese Aspekte können für gewöhnlich nur unzureichend durch ein „konkretes“ Informationssystemmodell abgebildet werden.

Typisch für assoziative semantische Regeln ist, dass ausgehend von beobachteten Merkmalen auf Hypothesen (hin)gedeutet wird. Angewandt auf den anwendungsorientierten Top-Down Ansatz lässt sich folgende primäre assoziative semantische Regel darstellen:

***fehlende Maßnahmen* (Merkmal) deuten auf *Schwachstellen* (Hypothese)**

Die fehlenden Maßnahmen stellen die beobachteten Merkmale dar, die Schwachstelle beschreibt die Hypothese.

Kausale semantische Regeln (modellbasiertes Diagnosewissen)
Im Gegensatz zu dem assoziativen Ansatz basiert das modellbasierte Ursachen-Wirkungs-Diagnosewissen auf der Annahme, dass eine Ursache zuverlässig zu bestimmten Wirkungen führt. Die Abbildung 54 zeigt ein kausales Modell, das die kausalen Abhängigkeiten zwischen einem gefährdenden Ereignis (Gefahr trifft auf sicherheitsrelevantes Element) und der daraus resultierenden Konsequenz beschreibt.

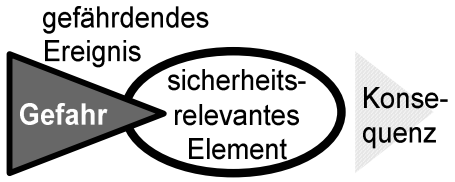


Abbildung 54: Kausales Modell des gefährdenden Ereignisses[402]

Der Detaillierungs- und Komplexitätsgrad der kausalen Modelle kann stark variieren, wobei insbesondere die Rückkopplungseffekte die Komplexität erhöhen. Bezeichnend für kausale semantische Regeln ist, dass bestimmte Ursachen (beobachtbare) Wirkungen verursachen bzw. bewirken. Angewandt auf den abbildungsorientierten Bottom-Up Ansatz lässt sich folgende primäre kausale semantische Regel darstellen:

***gefährdendes Ereignis*[403] (Ursache) verursacht *Konsequenz* (Wirkung)**

Das gefährdende Ereignis stellt die Ursache dar; die Konsequenz bildet die beobachtbare Wirkung ab.

Dieser Ansatz beschreibt die Kausalität des spezifischen Informationssystems möglichst realitätskonform. Deshalb werden als Beschreibungsgrundlage hauptsächlich „greifbare“ sicherheitsrelevante Elemente verwendet, was insbesondere auf der technisch physischen und logischen Ebene möglich ist. Insgesamt ist die Detaillierungstiefe beim kausalen Ansatz höher als beim assoziativen.

[402] Vgl. Konrad (1998), S. 200
[403] Gefährdendes Ereignis = Gefahr trifft auf sicherheitsrelevantes Element

Zusätzliche assoziative und kausale semantische Regeln

Zusätzliche Abhängigkeiten zwischen der Schwachstelle und Konsequenz werden durch weitere semantische Regeln beschrieben. Dadurch, dass eine Schwachstelle eine Konsequenz indirekt ermöglicht, erfordert eine Konsequenz eine Schwachstelle. Durch den assoziativen Bestandteil der Regel wird „gedeutet", dass eventuell eine Konsequenz entsteht, wenn eine offene Schwachstelle existiert. Hingegen werden Konsequenzen kausal durch Schwachstellen indirekt gegebenenfalls „ermöglicht" (verursacht).

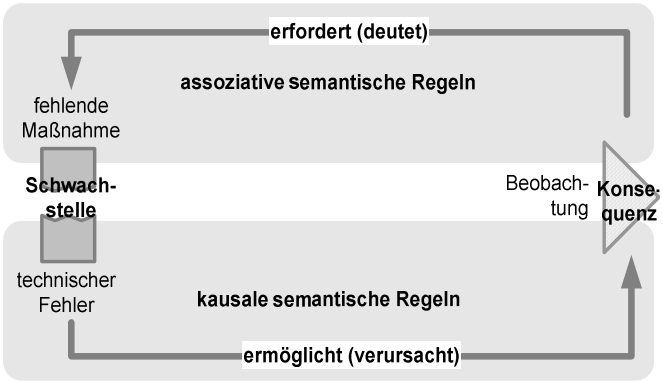


Abbildung 55: Sekundäre assoziative und kausale semantische Regeln

- Die assoziative Sicht geht von der Konsequenz aus, die auf eine mögliche „assoziative" Schwachstelle hindeutet:
  Konsequenz erfordert *(assoziative) Schwachstelle*.
  Dieses Abhängigkeitswissen beinhaltet nicht einen eindeutigen assoziativen Charakter, wie „fehlende Maßnahme deutet auf Schwachstelle", da Konsequenzen ihren Ursprung in der kausalen Darstellung besitzen. Deshalb wird diese Abhängigkeitsform als Ergänzung und nicht als Ersatz für die typische assoziative Abhängigkeit „*fehlende Maßnahmen* deutet auf *Schwachstellen"* verstanden.
- Die kausale Sicht geht von einer „kausalen" Schwachstelle aus, die eine Konsequenz ermöglicht (indirekt verursacht):
  (*kausale) Schwachstelle* ermöglicht *Konsequenz bzw. gefährdendes Ereignis*.
  Diese Schwachstelle ist in diesem Kontext als negative Eigenschaft (Fehler) eines sicherheitsrelevanten Elementes zu interpretieren. Dabei ist zu beachten, dass nicht eine eindeutige Kausalität wie bei der Abhängigkeit „*gefährdendes Ereignis* verursacht *Konsequenz*" besteht, da eine Schwachstelle die Konsequenz indirekt ermöglicht.

Die beiden sekundären semantischen Regeln „Konsequenz erfordert Schwachstelle" und „Schwachstelle ermöglicht Konsequenz" erhalten ihren assoziativen bzw. kausalen Charakter vor allem durch deren Verwendung in den Problemlösungsmethoden. So werden vorwiegend die assoziativen Abhängigkeitskonzepte in der heuristischen Klassifikation und die kausalen Abhängigkeitskonzepte in der modellbasierten Diagnose angewandt. In der Tabelle 14 sind die semantischen Regeln der Abhängigkeitskonzepte zusammengefasst.

	Merkmal		Lösung
assoziative semantische Regeln	*Maßnahme*	**deutet**	*assoziative Schwachstelle*
	Konsequenz	**erfordert**	
Wissensgrundlage	heuristisches Erfahrungswissen der IS-Sicherheit		

	Ursache		Wirkung
kausale semantische Regeln	*gefährdendes Ereignis*	**verursacht**	*Konsequenz*
	kausale Schwachstelle	**ermöglicht**	
Wissensgrundlage	zuverlässiges kausales modellorientiertes IS-Sicherheitswissen		

Tabelle 14: Übersicht der semantischen Regeln

Statistisches und fallbasiertes Diagnosewissen

Die statistischen Bewertungsansätze finden im Rahmen der Risikobewertung Anwendung, wobei hier Bewertungsprobleme bzgl. der Eingangsgrößen „Eintrittswahrscheinlichkeit“ und „Schadenshöhe“ bestehen[405]. Sollen komplexere statistische Ansätze - z.B. Bayes-Ansatz oder Dempster-Shafer Ansatz - benutzt werden, bestehen Vorbedingen, wie z.B. die Unabhängigkeit der Merkmale, die im Rahmen des IS-Sicherheitsmanagements meist nicht erfüllt werden können. Auf Grund der meist unzureichenden Voraussetzungen kann das statistische Diagnosewissen nur als Bewertungsergänzung dienen, wenn ausreichend zuverlässige Falldaten vorhanden sind.

Die fallbasierte Problemlösung beruht auf historischen Vorfällen. Da Fallwissen nicht auf wenige statistische Werte abstrahiert wird, behält das Wissen eine konkrete Fall-Eigenschaft[406]. Hierbei werden Beobachtungen mit historischen Fällen direkt verglichen, um bei einer gewissen Überschneidung die schon gewonnenen Ergebnisse des alten Falls zu verwenden[407]. Auch können durch eine Szenarioanalyse Fallbeispiele vorausschauend konstruiert werden, die dann mit Hilfe von historischen Vorfällen verglichen werden[408].

Durch eine Szenario-Analyse können mit Unterstützung von Fallbeispielen kausale Zusammenhänge exemplarisch dargestellt werden. Dabei werden nicht alle sicherheitsrelevanten Aspekte eines Unternehmens dargelegt, sondern nur die des Fallbeispiels. Ist eine Überschneidung der Voraussagen und der historischen Fälle vorhanden, so sind die Voraussagen als gefährlich zu bewerten. Insgesamt ist eine umfangreiche Erstellung und Erhaltung von IS-Sicherheit durch Fallbeispiele nicht möglich, da die Fälle nur auf sehr spezielle Bereiche beschränkt sind und sich nicht immer per Analogieschluss auf andere Fälle übertragen lassen[409].

Die folgende Tabelle stellt die Aspekte der jeweiligen Wissensarten und deren Anwendung in dem IS-Sicherheitsmanagement zusammenfassend dar.

[405] Das Bewertungsproblem wurde im Rahmen der Risikoanalyse diskutiert.
[406] Vgl. Weß (1996), S. 19
[407] Vgl. Puppe et al. (1996), S. 129 und Bartsch-Spörl/Lenz/Hübner (1999), S. 67
[408] Siehe zur Szenarioanalyse Sigesmund (1995)
[409] Vgl. Stelzer (1995), S. 122

		IS-Sicherheitsmanagement		
		Domänenbasis	Ziel der Problemlösung	Sicherheitsstrategie
Abhängigkeits-Konzepte	assoziatives Diagnosewissen	heuristisches Erfahrungswissen basierend auf Experten und Kriterien ⇒ anwendungsorientierter Ansatz	fehlende Maßnahmen ermitteln und deren Schwachstellen herleiten	SiSSA und Grundschutz (Top-Down Ansatz)
	kausales Diagnosewissen	Zuverlässiges Wissen basierend auf kausalen Systemmodellen ⇒ abbildungsorientierter Ansatz	Ermittlung von Gefahren und Erklärung von Konsequenzen	Risikoerkennung (Bottom-Up Ansatz) Risikobewertung
	statistisches Diagnosewissen	Wahrscheinlichkeiten und Schadenshöhen basierend auf statistischen Berechnungen	Bewertung von Risiken durch Eintrittswahrscheinlichkeiten und Schadenshöhen	
	fallorientiertes Diagnosewissen	Fallwissen basierend auf historischen Vorkommnissen und Lösungen	eine schon bestehende Lösung für das aktuelle Problem finden	Risiko- und Szenarioanalyse

Tabelle 15: Vergleich der IS-Sicherheitswissensarten[410]

Sicheres Diagnosewissen
Diese Form des Wissens kann eine Ergänzung zu anderen diagnostischen Wissensarten darstellen. Das sichere Wissen kann in Entscheidungsbäumen oder Entscheidungstabellen abgebildet werden, wodurch Lösungen direkt hergeleitet werden können. Typisch sind JA/Nein-Fragen, die die Knoten eines Entscheidungsbaums darstellen. Dadurch ist die Abbildung von sicherem Diagnosewissen im Gegensatz zu den anderen Wissensarten deutlich einfacher, da eine direkte Überführung dieses Wissens in eine Implementierungsform (Entscheidungsbäume oder -tabellen) möglich ist. Dieses Wissen kann für Bereiche des IS-Sicherheitsmanagements verwendet werden, wo eindeutige Regeln festgelegt werden können.

3.2.4 Schwachstellen-Kausalmodell

Eine Zusammenführung der kausalen und assoziativen Sicht in ein Schwachstellen-Kausalmodell ist häufig problematisch, da sicherheitsrelevante Bereiche (assoziative Sicht) und sicherheitsrelevante Elemente (kausale Sicht) auf unterschiedlichen Wissensarten bzw. -quellen basieren. So haben die sicherheitsrelevanten Bereiche mit ihren Maßnahmen und Schwachstellen ihren Ursprung in unternehmensunabhängigen Kriterien, während sicherheitsrelevante Elemente die kausale Infrastruktur einer Institution abbilden.

[410] Anlehnung an Puppe (1991), S. 81 und erweitert bzgl. des IS-Sicherheitsmanagements.

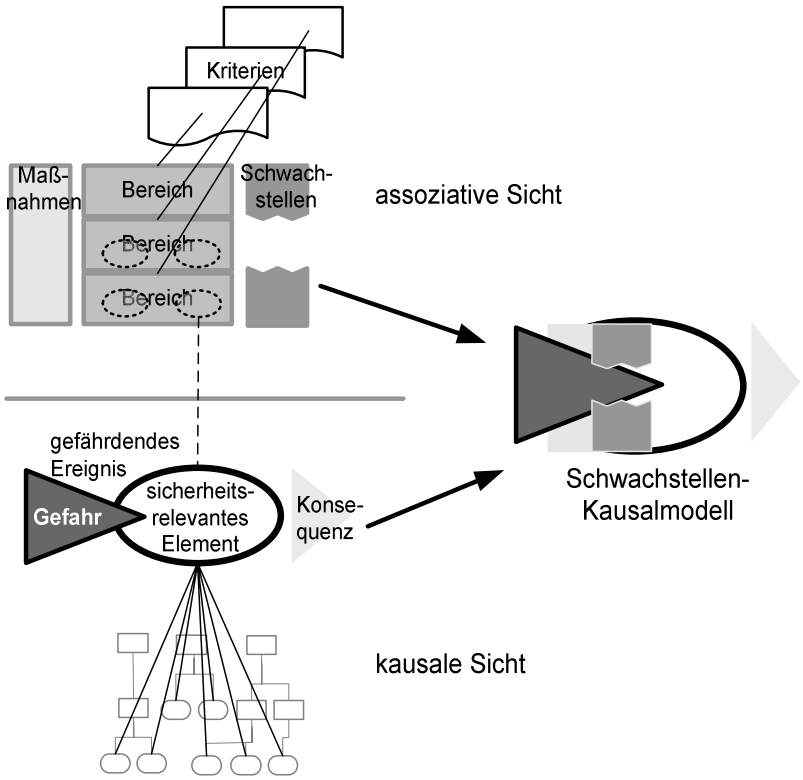


Abbildung 56: Schwachstellen-Kausalmodell

Das Schwachstellen-Kausalmodell dient der abstrakten Beschreibung von Zusammenhängen zwischen den Konzepten der assoziativen und kausalen Sicht. Eine Zusammenführung der assoziativen und kausalen Sicht ist nur möglich, wenn sich das sicherheitsrelevante Element im sicherheitsrelevanten Bereich „wieder findet“ und eine Kausalität sich präzise beschreiben lässt. Dann können die „assoziativen“ Schwachstellen als negative Eigenschaft in Form einer „kausalen“ Schwachstelle einem sicherheitsrelevanten Element zugeordnet werden und in einem kausalen Ursachen-Wirkungsmodell verwendet werden. Diese Schwachstellen besitzen meist einen technischen Bezug. Andere Schwachstellen, die sich nur durch das Fehlen von Maßnahmen darstellen lassen (z.B. im organisatorischen Bereich), können unzureichend oder gar nicht auf die kausale Sicht überführt werden.

Vernetzte Abhängigkeitskonzepte

Bisher wurden einfache Abhängigkeiten des Schwachstellen-Kausalmodells dargestellt. Das IS-Sicherheitswissen besteht jedoch z.T. aus „vernetzten“ Abhängigkeitskonzepten. Durch semantische Netze können die vernetzten Abhängigkeiten durch das „Fortpflanzen“ von Schwachstellen und Konsequenzen dargestellt werden.

Das Fortpflanzen einer Schwachstelle basiert darauf, dass ein fehlendes oder fehlerhaftes sicherheitsrelevantes Element eine (unzureichende) Maßnahme für ein anderes sicherheitsrelevantes Element darstellt. Zur Illustration dieser Abhängigkeit dient das folgende Beispiel: Um die Funktionsfähigkeit des technischen sicherheitsrelevanten Elementes „USV“ zu gewährleisten, ist die organisatorische Maßnahme „Wartungsintervalle überprüfen“ notwendig. Die USV bildet andererseits eine technische Maßnahme für Server. Werden nun die Wartungsintervalle für die USV nicht überprüft, entsteht eine Schwachstelle für die USV, da die Funktionsfähigkeit der USV nicht mehr gewährleistet ist. Dies stellt wiederum eine unzureichende technische Maßnahme (Schwachstelle) für den Server dar. Wenn die USV ausfällt, kann die

Verfügbarkeit des sicherheitsrelevanten Elements „Server“ bei einem Stromausfall nicht mehr gewährleistet werden.

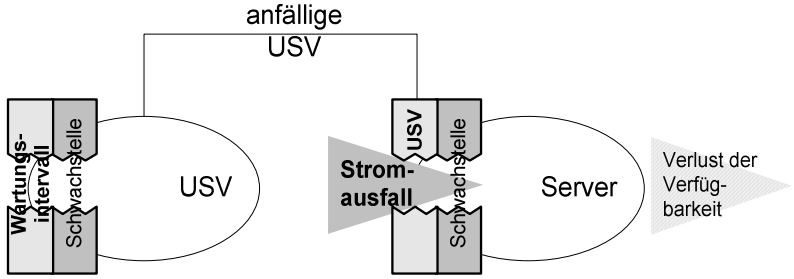


Abbildung 57: Fortpflanzung von technischen Schwachstellen

Die Fortpflanzung lässt sich als „Zustandsänderung“ von Basiskonzepten abbilden. Ein sicherheitsrelevantes Element mit einer Schwachstelle kann somit in einem anderen Kontext die fehlende oder unzureichende („anfällige“) Maßnahme darstellen.

Eine Fortpflanzung der Gefahren erfolgt durch Konsequenzen, da sich eine Konsequenz für ein anderes sicherheitsrelevantes Element zur Gefahr entwickeln kann. Bei dieser Form der Beschreibung stehen die kausalen Abhängigkeiten zwischen der Gefahr, dem sicherheitsrelevanten Element und der Konsequenz im Vordergrund.

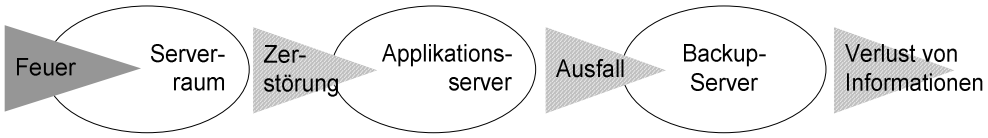


Abbildung 58: Beispiel einer einfachen und erweiterten kausalen Abhängigkeitskette

Auf der Ebene des kausalen Ursachen-Wirkungs-Wissens kann das Fortpflanzen der Konsequenzen auch als eine Zustandsänderung dargelegt werden. Dies bedeutet, dass eine Konsequenz eines Elementes eine Gefahr für ein anderes Element darstellt. Um komplexere Abhängigkeitsstrukturen aufzuzeigen, sind Heterarchien (oder multiple Hierarchien) notwendig. In der folgenden Abbildung ist ein komplexeres Beispiel für eine kombinierte assoziierte und kausale Darstellung dargelegt. Die Konzepte werden durch Knoten und die Zustandsänderungen durch Kanten dargestellt.

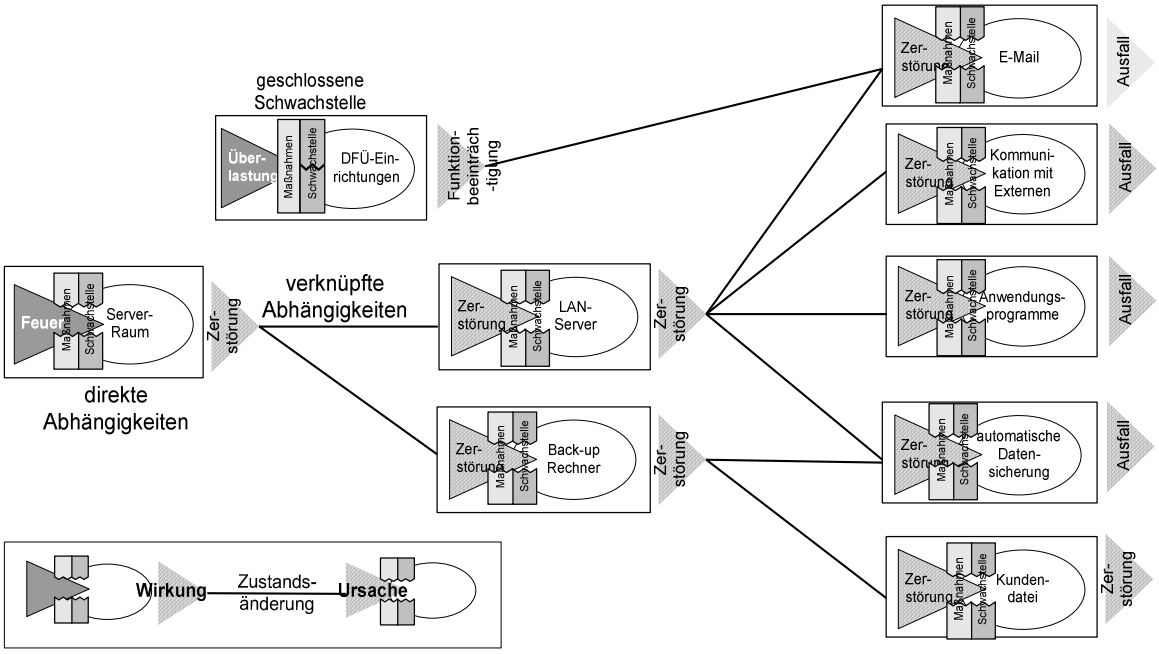


Abbildung 59: Beispiel von Zustandsänderungen

Die direkten Abhängigkeiten bestehen zwischen den Konzepten in einem Kontext (z.B. Raum oder System), wohingegen die verknüpften Abhängigkeiten eine Zustandsänderung des Konzeptes in Abhängigkeit des Kontexts nach sich ziehen. So ist die Konsequenz „Zerstörung“ im Kontext „Serverraum“ eine Gefahr im Kontext „LAN-Server“. Diese kausalen Zustandsänderungen werden insbesondere durch „greifbare“ technische Schwachstellen, Konsequenzen und gefährdende Elemente beschrieben, da diese eine zuverlässige und präzise Kausalität zulassen.

Andere Bereiche mit z.B. menschlichen oder organisatorischen Schwachstellen können nicht durch kausale Zustandsänderungen dargestellt werden, da sie als Grundlage heuristisches Wissen beinhalten. Aufgabe der Top-Down Strategie ist die Aufdeckung von möglichen Schwachstellen auf Basis von fehlenden Maßnahmen durch assoziatives Schließen und nicht die kausale Darstellung von Zustandsänderungen einer Schwachstelle oder Konsequenz.

3.3 Problemlösungsmethoden der Diagnose

Im Rahmen des KE beschreiben die Ontologien das Domänenwissen eines WBS und die Problemlösungsmethoden das Lösungsverhalten. Die Beschreibung von Lösungsprozessen der IS-Sicherheitsstrategien durch Problemlösungsmethoden erfolgt im Expertisemodell auf einer epistemologischen Ebene. Im Folgenden wird auf Problemlösungsmethoden der Diagnose eingegangen, welche die IS-Sicherheitsstrategien des Managements möglichst adäquat abbilden. In der unteren Abbildung erfolgt die Zerlegung der Diagnose in Aufgaben und Inferenzen.

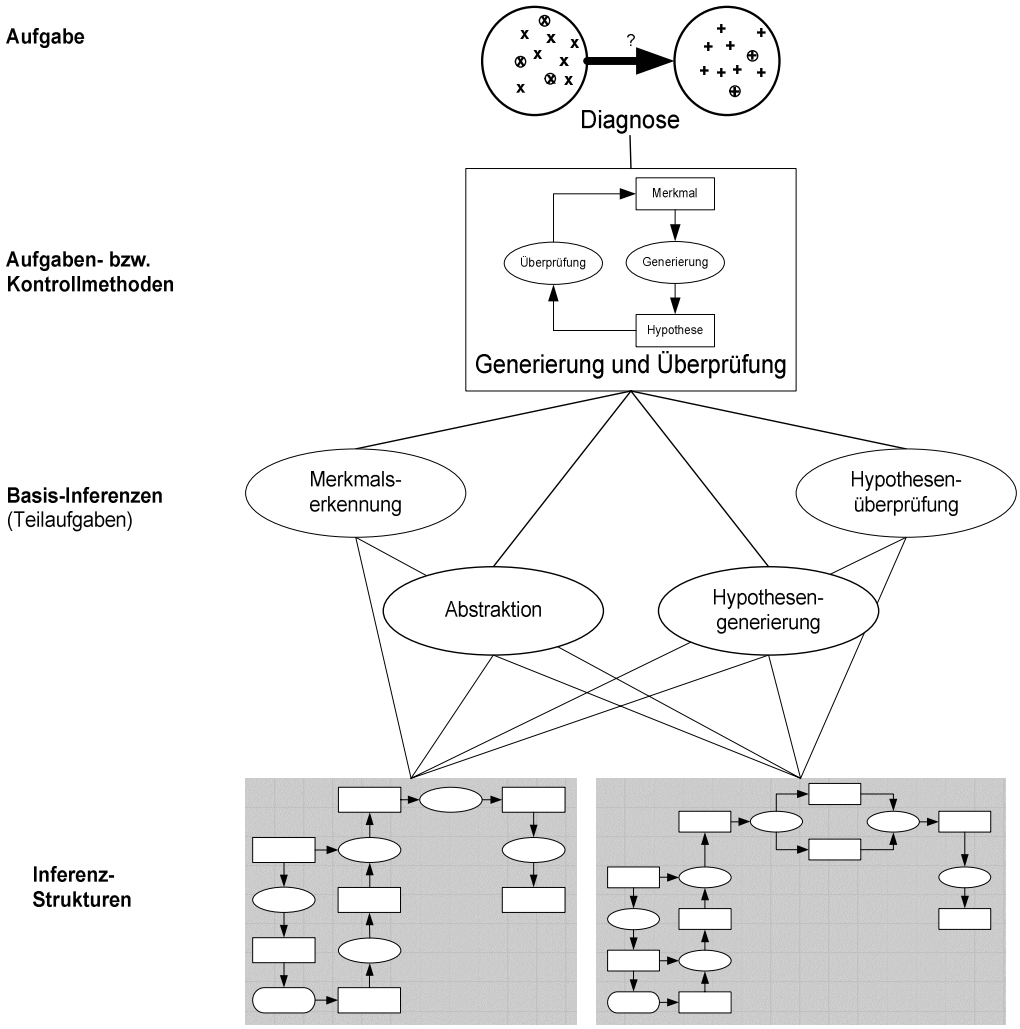


Abbildung 60: Übersicht der Bestandteile einer Diagnose-Problemlösungsmethode[411]

Als Erstes erfolgt die Beschreibung des Ziels der Diagnose; Lösungen werden auf Basis von Beobachtungen und Merkmalen hergeleitet (Beschreibung der Diagnoseaufgabe). Um dieses Ziel zu erreichen, werden auf einer domänenunabhängigen Ebene Kontrollstrukturen beschrieben, wie die Generate-and-Test oder Hypothesize-and-Test Strategie, die auf der Generierung von Hypothesen und deren Überprüfung basieren (generische Kontroll- bzw. Aufgabenmethoden zur Bewältigung der Diagnoseaufgabe)[412].

Die Kontrollmethoden werden in Teilaufgaben bzw. Basis-Inferenzen zerlegt, die wiederum in Inferenz-Strukturen aufgeteilt werden. Der Unterschied zwischen (Teil-)Aufgaben und der Inferenzebene besteht in der Verknüpfung mit dem Domänenmodell. Während die Aufgabenebene weitgehend unabhängig von dem Domänenmodell ist, besitzen Inferenz-Strukturen

[411] Vgl. Schreiber et al. (2000), S. 113
[412] Vgl. Schreiber et al. (2000), S. 112

durch Wissens-Rollen Schnittstellen zwischen der Problemlösung und der Domäne. Zusammenfassend enthalten Problemlösungsmethoden folgende wesentliche Bereiche:

- Aufgabenbeschreibung der Diagnose[413],
- Aufgaben- bzw. Kontrollmethoden sowie deren Basis-Inferenzen (Ovale) und
- Inferenz-Strukturen.

3.3.1 Kontroll- bzw. Aufgabenmethoden der Diagnose

Den ersten Bereich der Problemlösungsmethoden bilden die Kontroll- bzw. Aufgabenmethoden, die unabhängig von der jeweiligen Domäne beschrieben werden sollen. In den regelbasierten WBS der ersten Generationen existierten folgende „klassische“ Kontrollstrategien, die auch als schwache Problemlösungsmethoden bezeichnet werden:

- Vorwärtsverkettung: Ausgehend von beobachteten Merkmalen werden alle anwendungsbereite Regeln ausgewertet und Lösungen abgeleitet. Dabei können Ergebnisse entstehen, die wiederum durch weitere Regeln ausgewertet werden. Die Merkmalserhebung muss durch zusätzliches Wissen oder durch den Benutzer gesteuert werden. Da mehrere Regeln durch Daten aktiviert werden können, ist eine Konfliktstrategie notwendig, die bestimmt, welche Regel „feuert“. Diese Kontrollstrategie ist datengetrieben, da die Merkmale bekannt sind.
- Die Rückwärtsverkettung geht von einem Ziel - z.B. einer Wirkung in Form eines Ausfalls eines Servers - aus. Dabei werden alle Regeln interpretiert, die zum Erreichen des Zieles beitragen können. Diese Strategie eignet sich zum gezielten Erfragen von notwendigen Fakten, um weitere Regeln abzuleiten, damit schließlich die Ursache der erhobenen Wirkungen erklärt wird. Diese Auswertung wird auch als „zielgetriebenes“ Schließen bezeichnet.

Die alleinige Anwendung der beiden oben genannten vor- und rückwärtsorientierten Kontrollstrategien ist für die Diagnose unzureichend und wurde durch den Hypothesize-and-Test, Select-and-Test bzw. die Generate-and-Test Strategie Kontrollstrategien erweitert[414]. Bei dieser hypothetisch-deduktiven Vorgehensweise werden durch abduktives Zurückschließen von Beobachtungen (Merkmale) Verdachtshypothesen hergeleitet, zu deren Bestätigung oder Ausschluss gezielt deduktiv weitere Merkmale angefordert werden[415].

Die folgende Übersicht zeigt drei unterschiedliche Varianten der Generierung-und-Test Strategie, die sich z.B. bei Ärzten beobachten lassen. So werden aufgrund von erhobenen Merkmalen - wie z.B. erhöhte Temperatur und gerötete Haut - Verdachtshypothesen (z.B. Masern) aufgestellt. Um den Verdacht des Arztes zu bestätigen, werden gezielt zusätzliche Untersuchungen durchgeführt, die weitere Merkmale erkennen lassen, welche die Hypothese bestätigen oder widerlegen.

[413] Vgl. Kapitel 1 Einleitung
[414] Vgl. Schreiber (2000), S. 115 und Fensel (2000), S. 14
[415] Vgl. Puppe/Stoyan/Studer (2000), S. 619

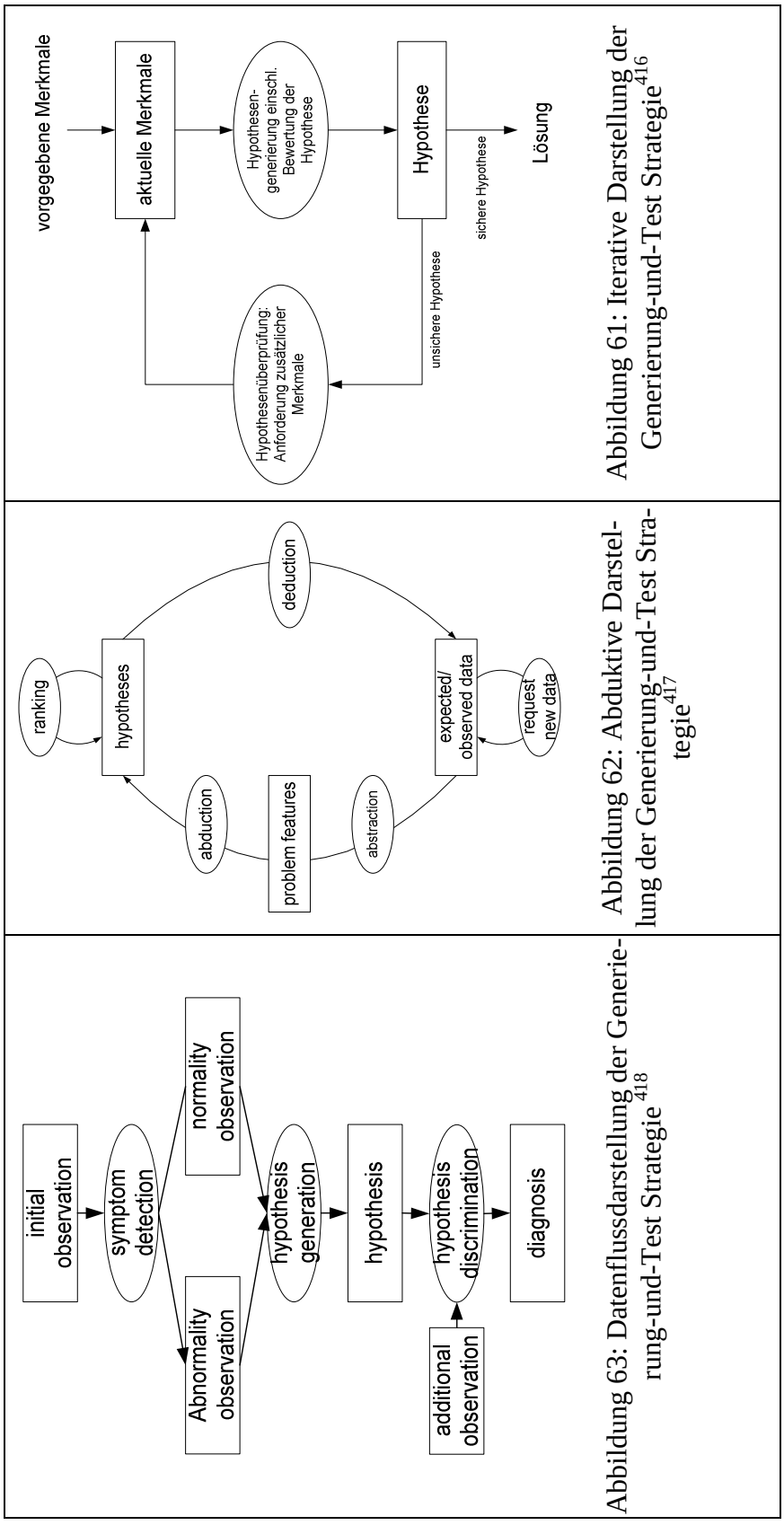


Abbildung 61: Iterative Darstellung der Generierung-und-Test Strategie[416]

Abbildung 62: Abduktive Darstellung der Generierung-und-Test Strategie[417]

Abbildung 63: Datenflussdarstellung der Generierung-und-Test Strategie[418]

[416] Vgl. Puppe/Stoyan/Studer (2000), S. 620
[417] Vgl. Heijst (1995), S. 14
[418] Vgl. Benjamins (1993), S. 49

3.3.2 Basis-Inferenzen der Diagnose

Es erfolgt eine Erläuterung der folgenden Basis-Inferenzen:

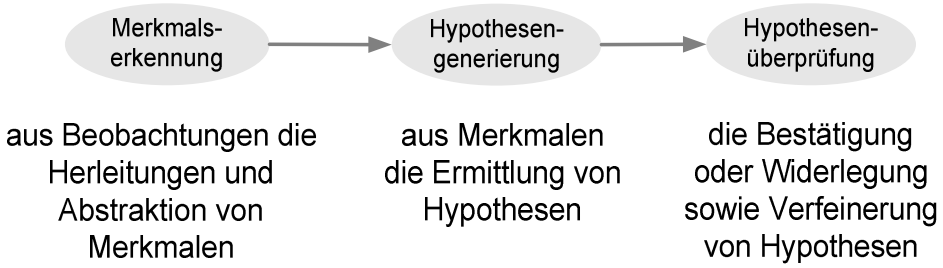


Abbildung 64: Basis-Inferenzen der Diagnose

3.3.2.1 Merkmalserkennung und Abstraktion

In der Merkmalserkennung werden die Beobachtungen abstrahiert, als Merkmale erkannt und eventuell in normale oder abnormale Merkmale differenziert. Die Erkennung kann direkt durch den Benutzer oder durch den Vergleich von beobachteten und erwarteten Merkmalen erfolgen. Wenn die Beobachtungen unmittelbar als abnormale Merkmale erkannt werden, ist der Vergleich nicht nötig.

Ein wichtiges Prinzip beim Umgang mit Unsicherheiten bei der Merkmalserkennung ist die schrittweise Abstraktion von Merkmalen. Durch die Abstraktion sollen Beobachtungen zu abstrahierten Merkmalen zusammengefasst werden, welche für das Schließen auf eine Lösung verwendet werden. Die Datenabstraktion lässt sich in folgende Bereiche differenzieren[419]:

- Durch arithmetische Berechnung (z.B. durch Berechnung des Risikograds).
- Abstraktion von quantitativen zu qualitativen Werten (Risikograd > 30% bedeutet hohes Risiko). Dieses Verfahren verlangt häufig eine linguistische Variable (z.B. niedrig, mittel und hoch), die z.B. durch die Fuzzy-Logik unterstützt wird. So kann z.B. bei mehr als drei Ausfällen eines Servers in einem Jahr von einem hohen Ausfallpotential des Servers „abstrahiert“ bzw. ausgegangen werden.
- Zusammenfassung bzw. Zuordnung von Einzelbeobachtungen zu (fach-)sprachlichen Abstraktionen aus der IS-Sicherheit.

3.3.2.2 Hypothesengenerierung

Die Abbildung der Merkmalsabstraktionen auf Lösungen bzw. Diagnosen ist eine zentrale Basis-Inferenz der Diagnostik. Im Rahmen der Hypothesengenerierung wird auf Basis der ermittelten Merkmale mit Hilfe von Problemlösungskonzepten auf Hypothesen geschlossen. Hierbei kann ein Merkmal mehrere Hypothesen besitzen (abduktives Schließen). Falls möglich, können Hypothesen nach einem oder mehreren Kriterien bewertet werden. Es wird die Lösung gewählt, die die höchste Gesamtbewertung auf Basis beobachteter Merkmale erzielt. Als Ergebnis entsteht ein Ranking, in welchem die Hypothesen nach der Schlussfähigkeit

[419] Vgl. Bamberger (1999), S. 28

bzw. Erklärungsfähigkeit oder z.B. deren Risikograd sortiert sind. Insgesamt ist die Verdachtsbewertung problematisch, da häufig auf unsichere empirische Daten oder subjektive Expertenmeinungen zurückgegriffen werden muss.

3.3.2.3 Hypothesenüberprüfung

Die Aufgabe der Hypothesenüberprüfung besteht darin, aus der Hypothesenmenge die richtigen Lösungen (Diagnosen) „herauszufiltern“. Auf Basis der Verdachts- bzw. Hypothesenbewertung werden zusätzliche Merkmale ausgewählt und erhoben, um die Hypothesen zu bestätigen oder zu verwerfen. Somit werden ausgehend von einer Hypothese zusätzliche Erklärungsmerkmale angefordert, welche die Hypothesen überprüfen. Diese zusätzlichen Merkmale generieren eventuell neue verfeinerte Hypothesen, die wiederum überprüft werden müssen. Hierbei ist auch der Erhebungsaufwand von zusätzlichen Merkmalen zu berücksichtigen.

Mit der Hypothesenüberprüfung schließt sich die Diagnose-Iteration. Insgesamt ist die Hypothesengenerierung und -überprüfung stark miteinander verknüpft. Eine eindeutige Trennung dieser Basis-Inferenzen ist häufig nicht möglich.

3.3.3 Abduktives und deduktives Schließen

Im Rahmen der Diagnose wird für die Beschreibung der Hypothesengenerierung und -überprüfung das abduktive und deduktive Schließen verwendet. Peirce hat 1932 folgende Schlussfolgerungen klassifiziert[420]:

- Deduktion
  Bei dem deduktiven Schließen werden aus allgemeinen Sachverhalten spezielle Aussagen abgeleitet. Mit den deduktiven Schlussfolgerungen ist die Vorstellung verbunden, dass es sich stets um wahre bzw. korrekte Schlussfolgerungen handelt und vom Allgemeinen auf das Spezielle schließt.
- Induktion
  Aus wiederholter Beobachtung von Einzelgegebenheiten können Regeln bzw. allgemeine Gesetzmäßigkeiten abgeleitet werden. Dieses induktive Schließen erfolgt z.B. beim „automatischen“ Lernen, ist aber nicht Bestandteil der Arbeit.
- Abduktion
  Bei der Abduktion erfolgt ein Zurückschließen von Beobachtungen auf Merkmale. Bei der Induktion und Abduktion ist - im Unterschied zu der Deduktion - das abgeleitete Wissen nicht notwendigerweise wahr oder korrekt bzw. unterliegt keiner logisch zwingenden Schlussfolgerung. So können die beobachteten Wirkungen auf vielen Ursachen basieren. Hierdurch besteht bei der Abduktion meist noch eine gewisse Unsicherheit.

Der grundsätzliche Problemlösungsprozess der Diagnose basiert auf dem abduktiven Zurückschließen von Beobachtungen, auf Lösungen bzw. Ursachen. Meist werden (unsichere) Verdachtshypothesen erzeugt, die mit zusätzlichen Merkmalen zu überprüfen und zu verfeinern sind. Die Überprüfung und Verfeinerung ist ein deduktiv orientiertes Schließen, da aus allgemeinen Verdachtshypothesen auf weitere speziellere Merkmale geschlossen wird, welche zur Überprüfung der Verdachtshypothesen dienen. Hierbei ist aber die Hypothesenüberprüfung

[420] Vgl. Peirce (1932) zit. nach Heijst (1995), S. 12 ff.

nicht ein deduktives Schließen im Sinne von stets wahren oder korrekten Schlussfolgerungen, sondern es soll die Orientierung vom Allgemeinen zum Speziellen darstellt werden. Dies bedeutet, dass die Deduktion eine Form des Voraussehens, der Vorausschau oder Voraussage (prediction) von weiteren möglichen Merkmalen ist, welche die Hypothese bestätigt oder widerlegt.

Am Beispiel der heuristischen Klassifikation soll das diagnostische abduktive und deduktive Schließen verdeutlicht werden.

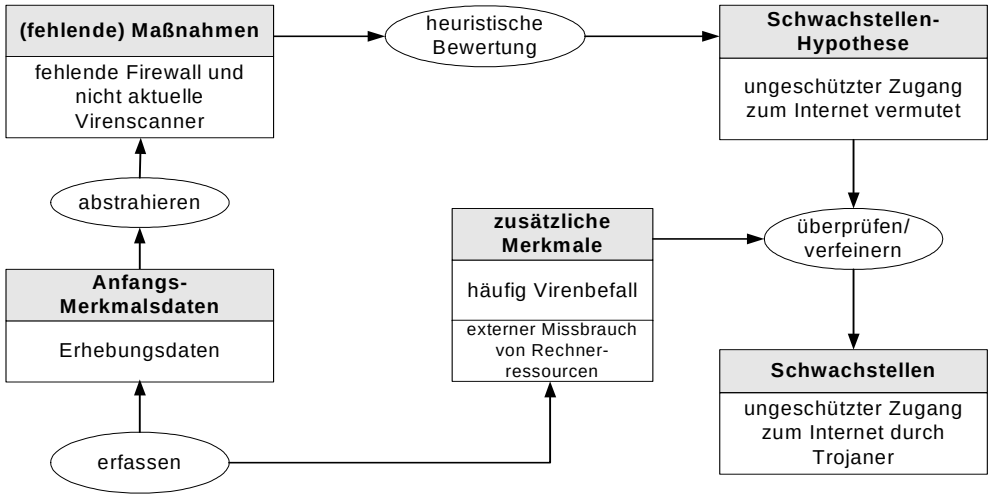


Abbildung 65: IS-Sicherheitsstrategie durch heuristische Klassifikation[421]

Ausgangspunkt für das abduktive Schließen bilden Merkmale oder Wirkungen, die durch die Merkmalserkennung erhoben und ermittelt worden sind. Hierfür werden erhobene Merkmalsdaten abstrahiert, so dass fehlende Maßnahmen erkannt werden (Merkmalserkennung). Die abduktive Hypothesengenerierung erfolgt für assoziative Abhängigkeitskonzepte durch das Schließen von erhobenen (fehlenden) Maßnahmen auf Schwachstellen-Hypothesen. Basierend auf assoziativem Abhängigkeitswissen ist abduktiv davon auszugehen, dass Schwachstellen im Zugang zum Internet vorhanden sind (Hypothesengenerierung)[422]. Ausgangspunkt für das deduktive Schließen bilden die Verdachtshypothesen, die durch die Hypothesengenerierung ermittelt worden sind. Auf Basis von Verdachtshypothesen werden zusätzliche „detaillierte“ Merkmale (z.B. weitere fehlende Maßnahmen oder Konsequenzen) ermittelt bzw. vorhergesagt, die zur Überprüfung der Verdachtshypothesen dienen (Hypothesenüberprüfung). Die Schwachstelle im Internetzugang wird z.B. durch zusätzlich ermittelte Merkmalskonsequenzen, wie häufiger Virenbefall oder externer Missbrauch von Rechnerressourcen, bestätigt und die Schwachstellen-Hypothese wird eventuell noch zusätzlich verfeinert.

[421] Erweitert in Anlehnung an Hoppe (1992), S. 78
[422] Für kausale Abhängigkeitskonzepte erfolgt ein Zurückschließen von Wirkungen (erhobenen Fehlzuständen) auf Ursachen, welche die Wirkungen verursacht bzw. ermöglicht haben.

3.3.4 Inferenz-Strukturen

Die nicht weiter zerlegbaren Bestandteile des Problemlösungswissens werden als Inferenzen bezeichnet und bilden den zweiten Bereich der Problemlösungsmethoden. Der grundlegende Prozess einer Inferenz ist durch Eingabe, Ausgabe und das für die Verarbeitung benötigte Lösungswissen gekennzeichnet. Zur Darstellung des Eingangs, Ausgangs und des benötigten Wissens einer Inferenz werden Wissens-Rollen verwendet. Wissens-Rollen bilden die Verbindung bzw. Schnittstelle zwischen Aufgabenwissen, Inferenzwissen und Domänenwissen. Es wird zwischen dynamischen und statischen Wissens-Rollen unterschieden[423]:

- Dynamische Wissens-Rollen bilden den Eingang und Ausgang einer Inferenz ab und nehmen unterschiedliche Konzepte der Domäne an.
- Statische Wissens-Rollen spezifizieren die Bereiche des domänenspezifischen Wissens, die für die Problemlösung benötigt werden. Sie verwenden die Problemlösungskonzepte (Abhängigkeitskonzepte[424]) und sind während des Problemlösungsprozesses weitgehend stabil.

Eine Kombination aus einzelnen Inferenzen und Wissens-Rollen wird zusammenfassend in einer Inferenz-Struktur abgebildet. In der folgenden Abbildung ist das Grundprinzip einer Inferenz abgebildet.

[423] Vgl. Speel et al. (2001), Kapitel 3.2
[424] Problemlösungskonzepte und Abhängigkeitskonzepte werden in der Arbeit synonym verwendet.

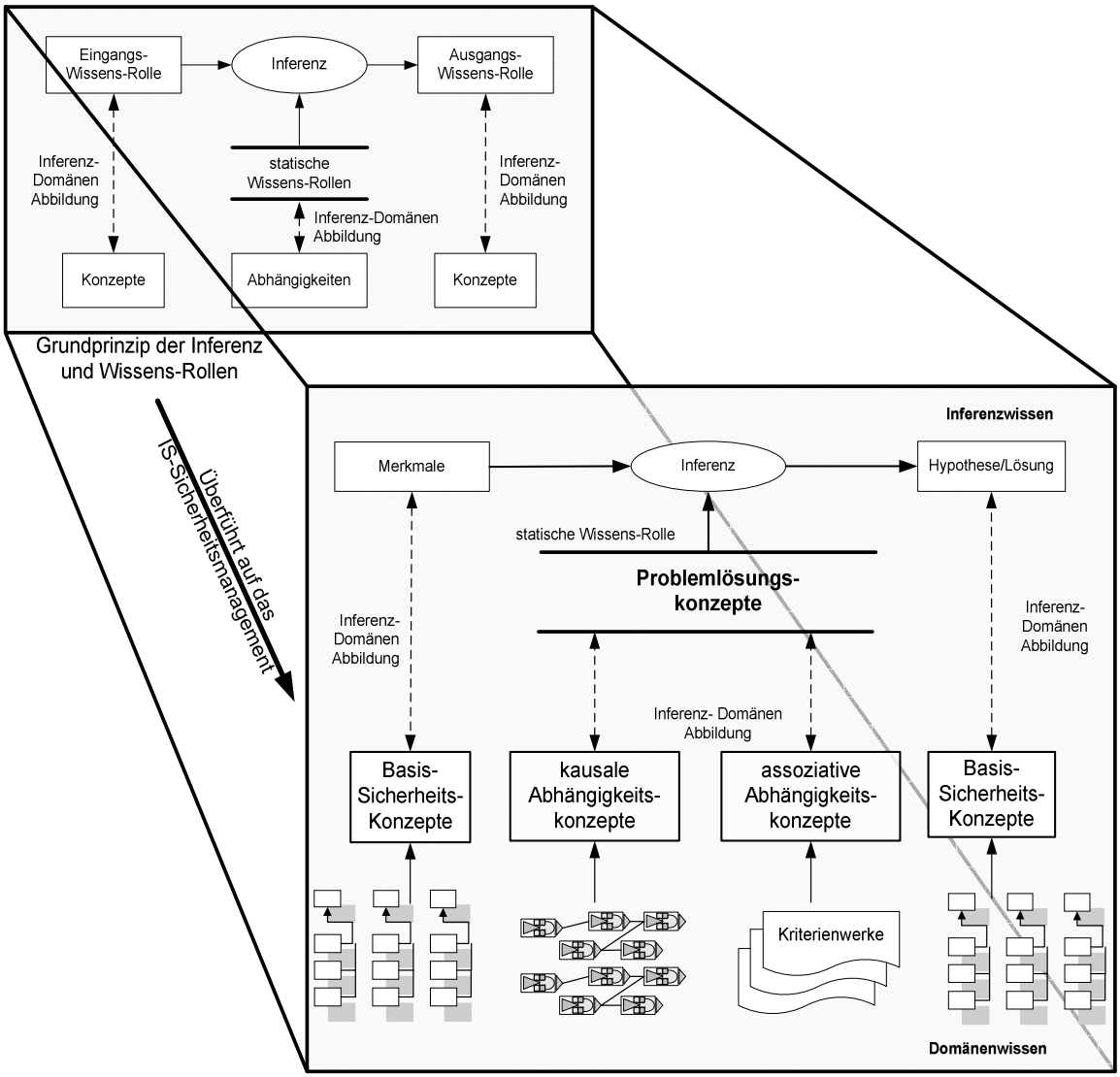


Abbildung 66: Grundprinzip der Inferenz und Wissens-Rollen

Die IS-Sicherheits-Konzepte bilden die Grundlage für die dynamischen Eingangs- und Ausgangswissens-Rollen. Die kausalen und assoziativen Abhängigkeitskonzepte dienen als statische Wissens-Rollen für die Inferenzen. Dieses Prinzip ist in der folgenden Abbildung am Beispiel des BSI-Grundschutzhandbuchs dargestellt.

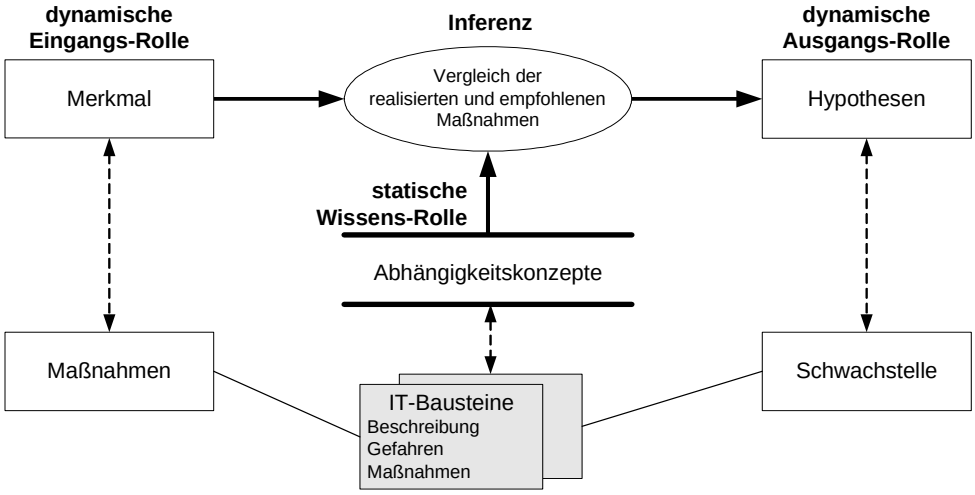


Abbildung 67: Grundprinzip der Inferenz und Wissens-Rollen am Beispiel des BSI-Grundschutzhandbuchs

Die IT-Bausteine bilden das Domänen-Wissen in Form des BSI-Grundschutzes ab und werden auf Wissens-Rollen überführt. Auf der dynamischen Wissens-Rolle „Merkmale“ werden erhobene Maßnahmen abgebildet; auf der dynamischen Wissens-Rolle „Hypothese“ werden Schwachstellen abgebildet. Die statische Wissens-Rolle „Lösungskonzepte“ beinhaltet das Abhängigkeits- bzw. Lösungswissen zwischen defizitären Maßnahmen und Schwachstellen. Die Problemlösungsmethode besteht in diesem Beispiel aus einer „Soll-Ist Vergleich“ Inferenz der realisierten Maßnahmen (Merkmale) und Maßnahmenempfehlungen.

3.4 Problemlösungsansätze für IS-Sicherheitsstrategien

Ein zentrales Problem des Knowledge Engineerings ist das „Knowledge Interaction Problem“, welches die Abbildung des Domänenwissens auf das Problemlösungswissen und umgekehrt beinhaltet.

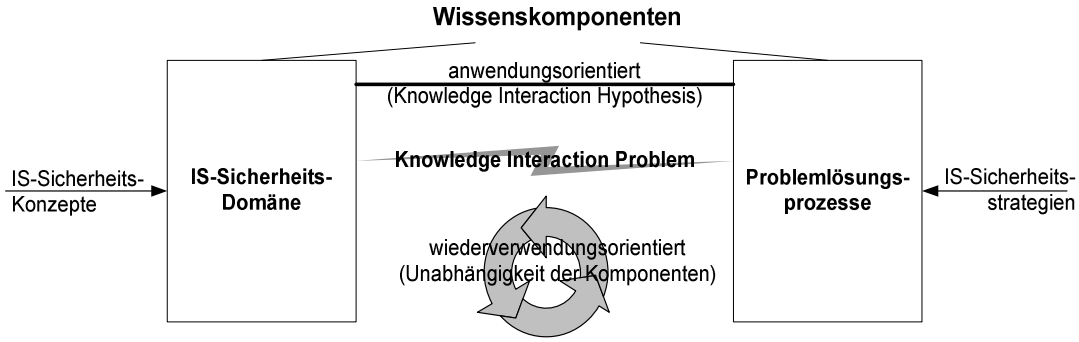


Abbildung 68: Knowledge interaction problem

Die Abbildung lässt sich durch folgende Extrempositionen beschreiben[425]:

- Durch die Unabhängigkeit der beiden Wissenskomponenten (Domäne und Problemlösung) ist eine Wiederverwendung (reuse) der jeweiligen Wissenskomponenten möglich. Somit können unterschiedliche Problemlösungsprozesse des IS-Sicherheitsmanagements eine Repräsentation der IS-Sicherheitsdomäne verwenden. Mehrere Ausprägungsformen einer IS-Sicherheitsrepräsentation können durch einen Problemlösungsprozess angewandt werden. Diese Unabhängigkeit wird z.B. durch den KADS-Ansatz gefordert, wobei die vollständige Wiederverwendung durch die „Relative Interaction Hypothesis“ relativiert wird[426]. So bestehen in gewissem Umfang Abhängigkeiten bzw. Anforderungen zwischen Repräsentationen und Problemlösungsmethoden der Problemlösungsprozesse, so dass keine „vollständige“ Wiederverwendung der beiden Bereiche besteht.
- Dem Extrem der Unabhängigkeit stehen die „Strong Knowledge Interaction Hypothesis“ orientierten Ansätze entgegen. Diese Ansätze sind anwendungsorientiert (usability), da im Wesentlichen nur die passende Problemlösungsmethode des IS-Sicherheitsmanagements ausgewählt wird und die Wissensrepräsentation des Domänenmodells bzw. der IS-Sicherheitskonzepte vordefiniert ist[427]. Diese Ansätze besagen, dass die Repräsentation einer Domäne durch die Problemlösungsmethode determiniert wird bzw. der Akquisitionsprozess des Domänenwissens durch die Problemlösungsmethode bestimmt wird[428]. Die Problemlösungsmethoden, welche durch eine Wissensart (z.B. sicheres, heuristisches oder modellbasiertes Wissen) spezialisiert bzw. bestimmt werden, werden als starke Problemlösungsmethoden bezeichnet[429].

[425] Vgl. Motta (1999), S. 40
[426] Vgl. Studer/Benjamins/Fensel (1998), S. 170
[427] Vgl. Angele/Fensel/Studer (1998), S. 173
[428] Vgl. Bylander/Chandrasekaran (1988), S. 67 und Reynaud/Tort (1997), S. 340
[429] Vgl. Puppe (1996), S. 6

Es wäre aber von Interesse, ein anwendungsorientiertes Domänenmodell zu besitzen, welches auf unterschiedliche Problemlösungsmethoden multifunktional angewandt werden kann[430]. Mit Hilfe von „multifunktionalen Problemlösungsmethoden“ wird im Folgenden ein Kompromiss zwischen einem anwendungs- und wiederverwendungsorientierten Ansatz entwickelt, der beide Extrempositionen vereinigt. Grundlage dafür bilden die IS-Sicherheitsstrategien, welche durch multifunktionale Problemlösungsmethoden beschrieben werden. Diese Methoden berücksichtigen in einem gewissen Rahmen auch eine Wiederverwendung der Domänen-Konzepte und Problemlösungsmethoden. Die folgende Abbildung stellt einen Zusammenhang zwischen Basis-Inferenzen, Domänen-Konzepten und Inferenz-Strukturen der folgenden Kapitel dar. Hierfür werden zunächst die anwendungsorientierten Basis-Inferenzen beschrieben, die im Weiteren um multifunktionale Inferenz-Strukturen erweitert werden.

[430] Vgl. Motta (1999)

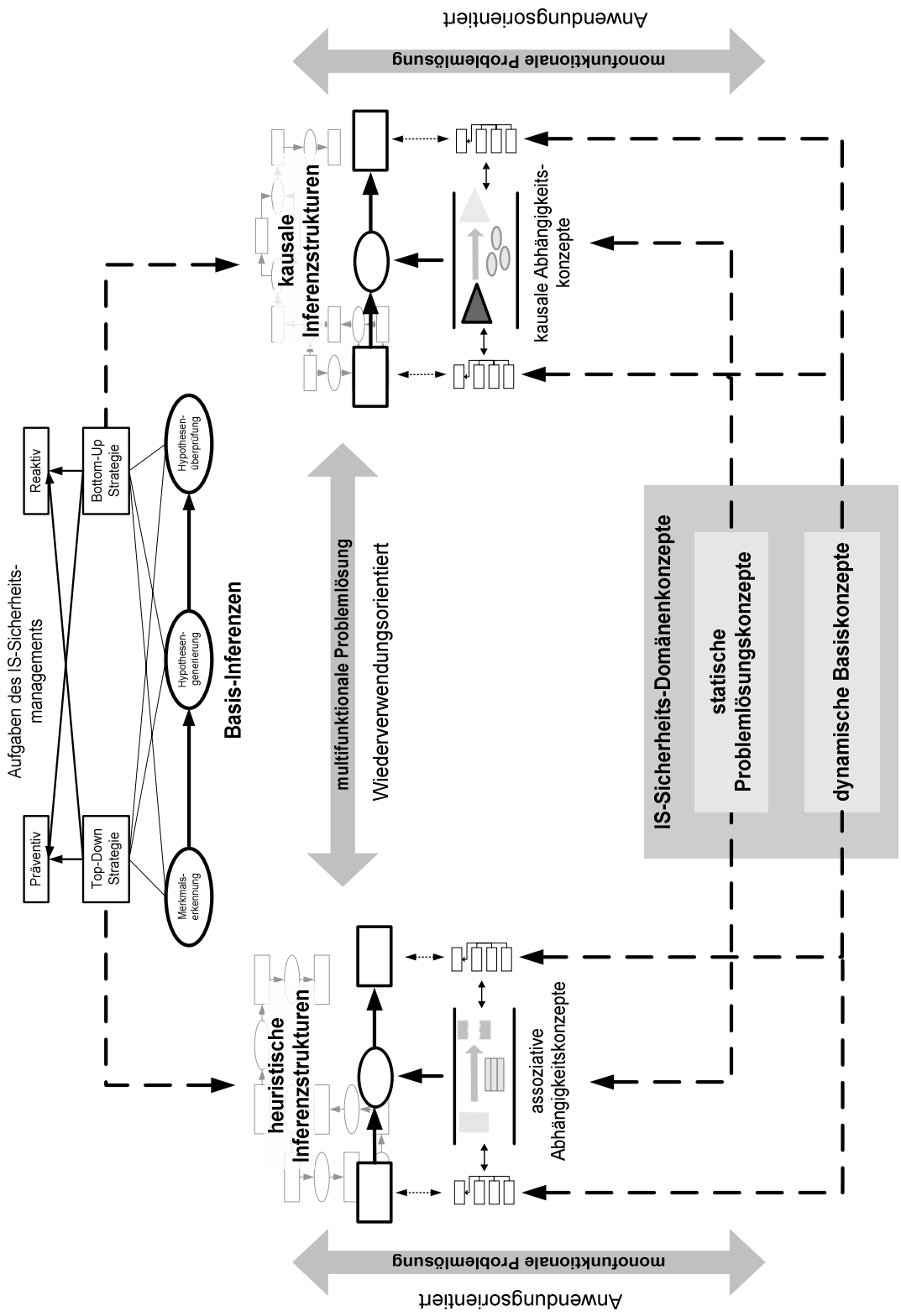


Abbildung 69: Mono- und multifunktionales Domänen- und Problemlösungsmodell

3.4.1 IS-Sicherheits-Domänenkonzepte

Die Basis- und Problemlösungskonzepte aus Kapitel 3.2.2 und Kapitel 3.2.3 werden im Folgenden erweitert.

3.4.1.1 Dynamische Basiskonzepte

Die Basiskonzepte enthalten das dynamische Domänenwissen, das für die meisten Problemlösungsmethoden benötigt wird. Deshalb erfolgt die Beschreibung möglichst unabhängig von spezifischen Problemlösungsmethoden (im Gegensatz zu den Problemlösungskonzepten). Das Basiswissen enthält vor allem formalisierte und normierte Fachausdrücke, wie Maßnahmen, Schwachstellen, Gefahren, Konsequenzen usw. Die Strukturierung der Basis-Konzepte erfolgt häufig mit Hilfe von Hierarchien. Diese Basiskonzepte werden auf dynamische Eingangs- und Ausgangs-Wissens-Rollen überführt.

3.4.1.2 Anwendungsorientierte statische Problemlösungskonzepte

Abhängigkeitsmodelle
Die Konzepte der Abhängigkeitsmodelle werden von den spezifischen Abhängigkeitskonzepten zu deren jeweiligen Problemlösung verwendet, indem sie in deren statische Wissens-Rollen überführt werden. Da diese spezifischen Abhängigkeitskonzepte die Problemlösung entscheidend prägen, werden die Abhängigkeitskonzepte als spezifische Problemlösungskonzepte bezeichnet. Für die Arbeit sind folgende Abhängigkeitskonzepte von Bedeutung[431]:

- Heuristische Abhängigkeitskonzepte der Art „*Merkmal deutet auf Hypothese/Lösung*“, die auf assoziativem und heuristischem Erfahrungswissen basieren.
- Kausale Abhängigkeitskonzepte der Art „*Ursache (Hypothese, Lösung) verursacht Wirkung (Merkmal)*“, die auf Systemmodellen beruhen, bei denen Ursachen zuverlässig bestimmte Wirkungen hervorrufen.

Überführung von funktionalen Modellen auf kausale Abhängigkeitskonzepte
Für die modellorientierte Diagnose können neben kausalen Systemmodellen auch

- funktionale Systemmodelle und
- verhaltensorientierte Systemmodelle

als Grundlage dienen.

Für ein Funktionsmodell ist ein gut verstandenes Systemmodell nötig, das den Normalzustand und Fehlzustand von einzelnen Komponenten darstellen kann. Ein funktionales Modell ist meist komplexer als ein kausales Modell, da es zusätzlich detaillierte funktionale Zusammenhänge beschreibt, wobei die Komponenten nur streng lokale Auswirkungen besitzen dürfen. Die Begriffe „Komponenten“ und „Materialien“ werden abstrakt verwendet, wobei die Komponenten meist feste Objekte mit vorhersagbarem Verhalten darstellen und Materialien passive „Verbindungen“ zwischen Komponenten aufzeigen, so dass sie als Verbindungstypen bezeichnet werden[432].

[431] Vgl. Puppe et al. (1996), S. 117
[432] Vgl. Struss (2000), S. 442

Bei verhaltensorientierten Modellen wird auch von einem gut verstandenen Modell ausgegangen, welches aber zusätzlich das „No-Function-in-Structure“ Prinzip besitzt[433]. Dies bedeutet, dass die Modelle keine Voraussetzung für einen bestimmten Kontext besitzen. Somit „muss“ das vollständige Verhalten für einen beliebigen Kontext modelliert werden. Bei den funktionalen und insbesondere bei verhaltensorientierten Modellen entsteht sehr schnell eine hohe Komplexität, besonders wenn komplexe „Informationssysteme“ abgebildet werden. Aus diesem Grund wird das Problemlösungsverhalten der verhaltensorientierten und funktionalen Modelle auf kausale Modelle überführt. Die funktionalen Anhängigkeiten werden somit durch kausale Ursachen- und Wirkungs-Abhängigkeitskonzepte repräsentiert.

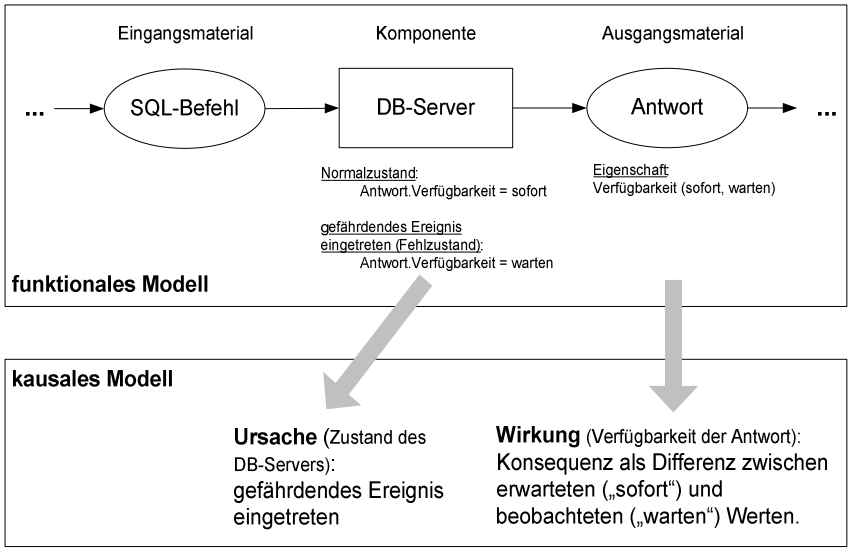


Abbildung 70: Überführung eines funktionalen Modells in ein kausales Modell

Die Überführung des funktionalen Modells in ein kausales Modell geschieht durch folgende Zuordnungen[434]:

- In einem funktionalen Modell entspricht jede Diskrepanz zwischen dem zu erwartenden (z.B. normale Zugriffszeit für Informationen) und dem tatsächlich beobachteten Wert (z.B. langsame Zugriffszeit für Informationen) einem Merkmal (Wirkung).
- Jeder abnorme Fehlzustand entspricht einer Komponente einer Lösung (Ursache). Die Zustände (Normal- oder Fehlzustand) ergeben das Verhalten der Komponente und können in Form von Regeln beschrieben werden (WENN ein gefährdendes Ereignis eingetreten ist; DANN ist die Antwort nicht verfügbar). Auf Basis der Merkmale lassen sich Rückschlüsse auf die Komponente vornehmen, die die Fehler verursacht.

[433] Vgl. Struss (2000), S. 450
[434] Puppe et al. (1996), S. 123

Manifestierendes Modell
Die manifestierenden Modelle werden für die Hypothesenüberprüfung verwendet. Ziel hierbei ist, auf Basis einer Hypothese bzw. einer Ursache zusätzliche Merkmale zu ermitteln, die die Hypothese bzw. Ursache überprüfen bzw. verfeinern. Im Unterschied zu der Hypothesengenerierung wird dieses Wissen nur aktiviert bzw. benötigt, wenn die betreffende Hypothese auch verdächtigt wird. Deshalb haben diese zusätzlichen Merkmale den Charakter einer detaillierten Nachfrage für einen ermittelten Verdacht.

Wie bei der Hypothesengenerierung ist zwischen assoziativen und kausalen manifestierenden Modellen zu unterscheiden.

- In den assoziativen manifestierenden Modellen wird festgelegt, welche weitere vermutete (fehlende) Maßnahme die Schwachstellen-Hypothese bestätigen oder widerlegen könnte.
- In den kausalen manifestierenden Modellen wird festgelegt, welche weitere Konsequenz das vermutete gefährdende Ereignis[435] erklären oder widerlegen könnte.

Hierarchische Modelle
Die hierarchischen Modelle werden für die heuristische Hypothesengenerierung und Hypothesenüberprüfung (hierarchische Klassifikation) verwendet. Sie können als eine Spezialisierung des assoziativen Abhängigkeitskonzepts interpretiert werden. Dies bedeutet, dass auf Basis des hierarchischen Abhängigkeitswissens zwischen den Basiskonzepten Verdachtshypothesen ermittelt werden. Um z.B. eine Schwachstelle zu beschreiben, können in Form einer Hierarchie mehrere Maßnahmen und Konsequenzen zusammengefasst werden. Fehlen die Maßnahmen und werden Konsequenzen beobachtet, so kann auf eine Schwachstelle gedeutet werden. Für die hierarchische Hypothesengenerierung und -überprüfung wird häufig die „Establish-Refine“ Strategie verwendet, welche im Kapitel 3.4.2.2 erläutert wird.

Vorgabenmodelle
Die Vorgabenmodelle werden vor allem in der Merkmalserkennung eingesetzt, um z.B. eine Beobachtung auch als Konsequenz zu „erkennen“ oder als eine fehlende Maßnahme zu identifizieren. Im Rahmen der Merkmalserkennung werden Vorgaben mit Beobachtungen verglichen, um auf Basis der Vergleichsergebnisse die Merkmale und Wirkungen zu abstrahieren. Dabei lassen sich folgende Vorgabenbereiche unterscheiden:

- Maßnahmen-Vorgaben
  Es wird auf Basis von erforderlichen Soll-Maßnahmen durch Vergleiche der erhobenen Maßnahmen auf fehlende Maßnahmen geschlossen.
- Zustands-Vorgaben
  Auf Basis von Fehl- und Normalzustand wird im Vergleich mit den erhobenen Zuständen auf Konsequenzen geschlossen.

[435] Gefährdendes Ereignis = Gefahr trifft auf sicherheitsrelevantes Element.

Die Tabelle 16 stellt Basis- und Problemlösungskonzepte zusammenhängend dar.

dynamische Basiskonzepte	
Darstellung der wesentlichen Fachterminologien und deren definitorischen Beziehungen.	
Grundlage für dynamische Eingangs- und Ausgangs-Wissens-Rollen	
statische Problemlösungskonzepte	
Abhängigkeitsmodelle	
assoziative Konzepte	fehlende Maßnahme deutet auf Schwachstelle/ Konsequenz erfordert Schwachstelle
kausale Konzepte	gefährdendes Ereignis verursacht Konsequenz/ Schwachstelle ermöglicht Konsequenz
Grundlage für Hypothesengenerierung	
manifestierende Modelle	
assoziative Konzepte	Schwachstellen lassen weitere fehlende Maßnahmen oder erfassbare Konsequenzen vermuten
kausale Konzepte	gefährdende Ereignisse und kausale Schwachstellen sagen weitere Konsequenzen voraus
Grundlage für Hypothesenüberprüfung	
hierarchische Modelle	
Spezialisierung der assoziativen Abhängigkeitskonzepte auf hierarchische Beziehungen	
Grundlage für hierarchische Hypothesengenerierung und -überprüfung	
Vorgabenmodelle	
Soll-Maßnahmen	Erkennung von fehlenden Maßnahmen
Fehl- bzw. Normalzu-stände	Erkennung von Konsequenzen
Grundlage für Merkmalserkennung	

Tabelle 16: Multifunktionale IS-Sicherheits-Domäne

3.4.2 Anwendungsorientierte Basis-Inferenzen der IS-Sicherheitsstrategien

In dem folgenden Kapitel folgt die Überführung der IS-Sicherheitsstrategien auf anwendungsorientierte Basis-Inferenzen der Diagnose.

- Bei den Top-Down Strategien wird präventiv auf Basis von Merkmalen in Form von erhobenen fehlenden Maßnahmen und reaktiv in Form von beobachteten Konsequenzen auf Schwachstellen-Hypothesen assoziativ geschlossen, welche eventuell durch weitere Merkmale bestätigt oder verfeinert werden.
- Durch die Bottom-Up Strategien wird reaktiv ausgehend von beobachteten Wirkungen in Form von Konsequenzen auf deren Ursachen-Hypothesen (gefährdende Ereignisse und kausale Schwachstellen) geschlossen, welche die Wirkungen kausal erklären. Die Ursachen werden eventuell durch weitere Beobachtungen (Wirkungen) bestätigt oder verfeinert. Präventiv wird ausgehend von gefährdenden Ereignissen deren mögliche Konsequenzen vorausschauend ermittelt.

Zusammenfassend lässt sich die reaktive und präventive Sichtweise auf dem Schwachstellen-Kausalmodell abbilden. Durch die präventive Sichtweise werden basierend auf fehlende Maßnahmen die Schwachstellen geschlossen, um Konsequenzen zu verhindern. Reaktiv werden aufgetretene Konsequenzen durch deren Ursachen erklärt.

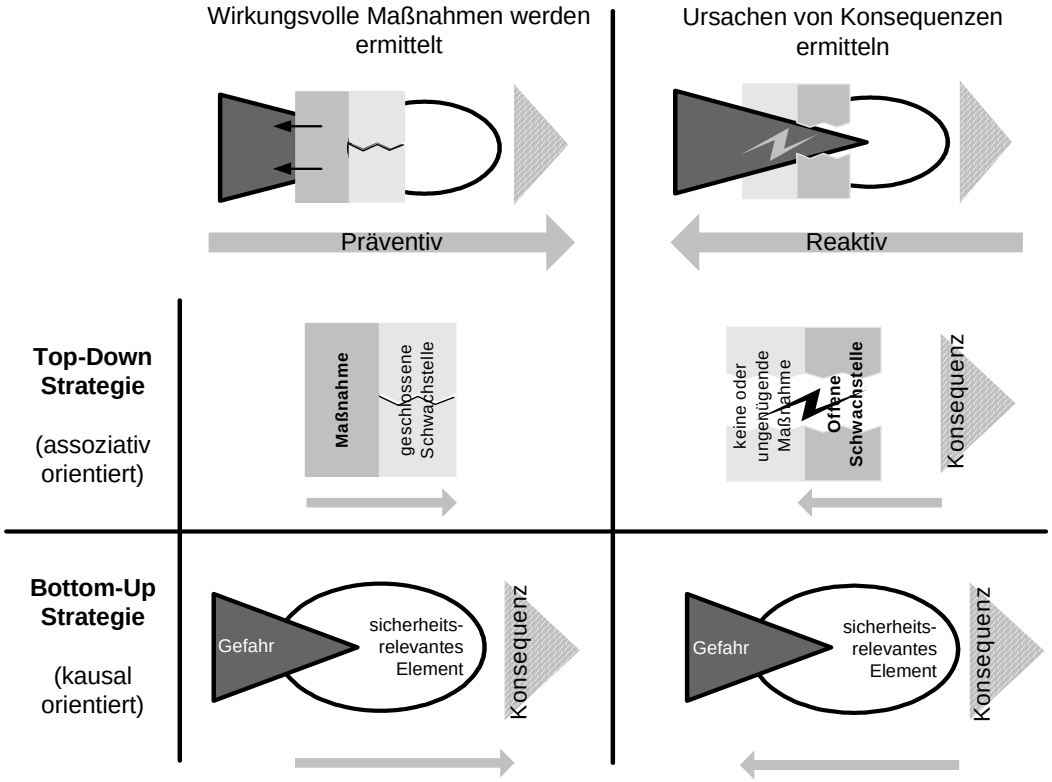


Abbildung 71: Reaktive und präventive Sichtweise des Schwachstellen-Kausalmodells

Die folgende Abbildung stellt zusammenhängend die benötigten Problemlösungskonzepte in Verbindung mit den IS-Sicherheits-Problemlösungsmethoden dar. Diese spezifischen Problemlösungsmethoden (heuristische Klassifikation und modellbasierte Diagnose) werden als starke Problemlösungsmethoden bezeichnet, da sie im Gegensatz zu den schwachen Problemlösungsmethoden (einfache Vorwärts- und Rückwärtsverkettung) auf Angaben des spezifischen Abhängigkeitswissens (assoziative oder kausale Anhängigkeitskonzepte) basieren.

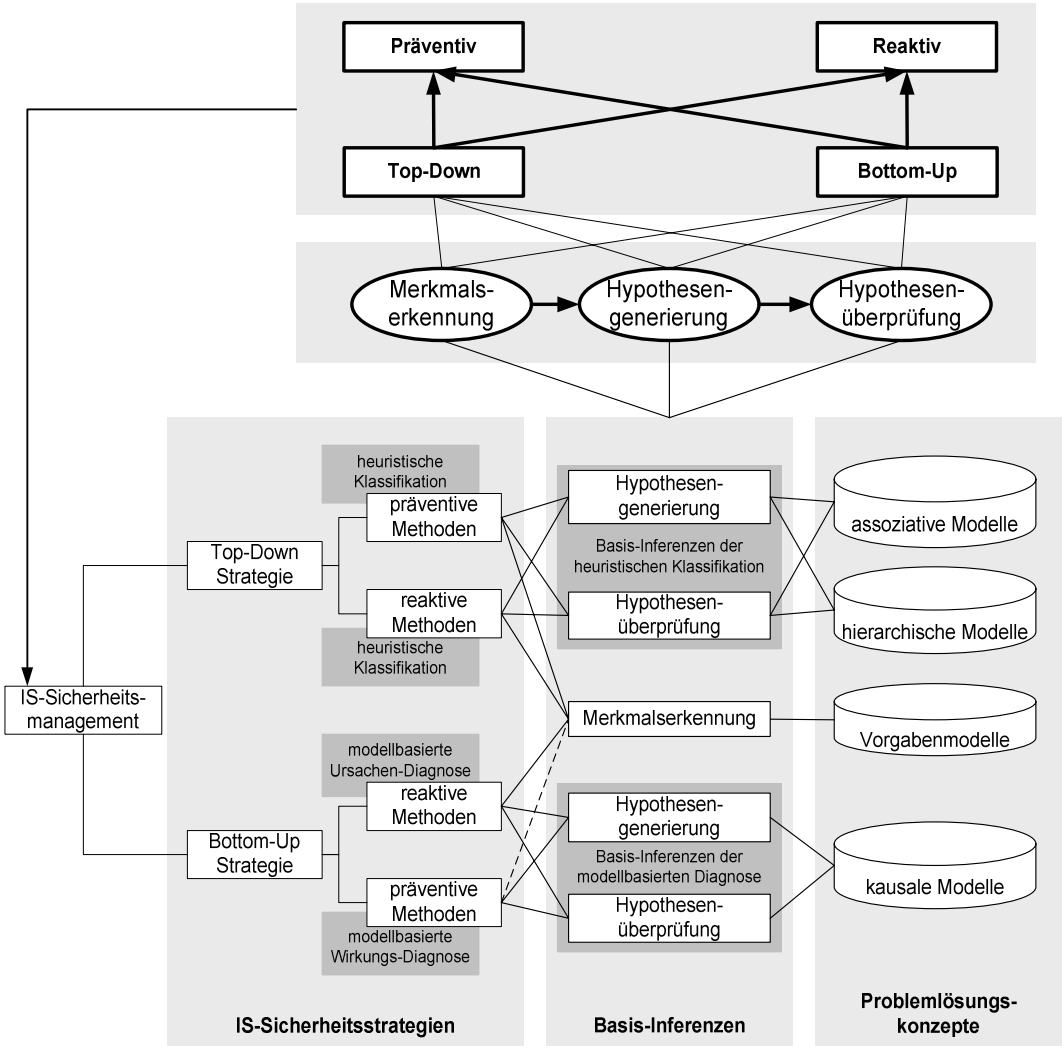


Abbildung 72: Anwendungsorientierte IS-Sicherheits-Problemlösungsmethoden

Die Basis-Inferenz „Merkmalserkennung“ basiert auf Vorgabenmodellen und wird für Problemlösungsmethoden der IS-Sicherheitsstrategien - bis auf ein präventives Bottom-Up - in gleicher Form verwendet. Die präventive Bottom-Up Strategie, die auf einer Vorhersage von möglichen gefährdenden Ereignissen basiert, benötigt zur Hypothesengenerierung keine „klassische“ Merkmalserkennung, da sie auf „angenommenen Ursachen“ beruht und nicht auf erhobenen Merkmalen, wie z.B. Wirkungen. Für eine Überprüfung der vorhergesagten Hypothesen können Merkmale erhoben werden, welche die vorhergesagten Hypothesen bestätigen oder widerlegen.

Die anwendungsorientierte Hypothesengenerierung und -überprüfung basiert auf unterschiedlichen Problemlösungskonzepten. Es erfolgt

- die heuristische Top-Down Hypothesengenerierung und -überprüfung auf assoziativen und hierarchischen Problemlösungskonzepten,
- die modellbasierte Bottom-Up Hypothesengenerierung und -überprüfung gründet sich dagegen auf kausale Problemlösungskonzepte.

Durch Auswahl der IS-Sicherheitsstrategie werden entsprechende Problemlösungsmethoden und deren spezifische Problemlösungskonzepte durch das anwendungsspezifische WBS angeboten, um darauf basierend ein WBS zu konfigurieren. Dies hat den Vorteil, dass IS-Sicherheitsexperten ein WBS ohne Hilfe eines Knowledge Engineerings erstellen können, da die Problemlösungsmethode und deren Wissensrepräsentation schon vorgegeben sind. Der IS-Sicherheitsexperte wählt eine oder mehrere Problemlösungsmethoden aus und erzeugt „nur“ Instanzen der Basis- und Problemlösungskonzepte, um die Wissensbasis zu „füllen“.

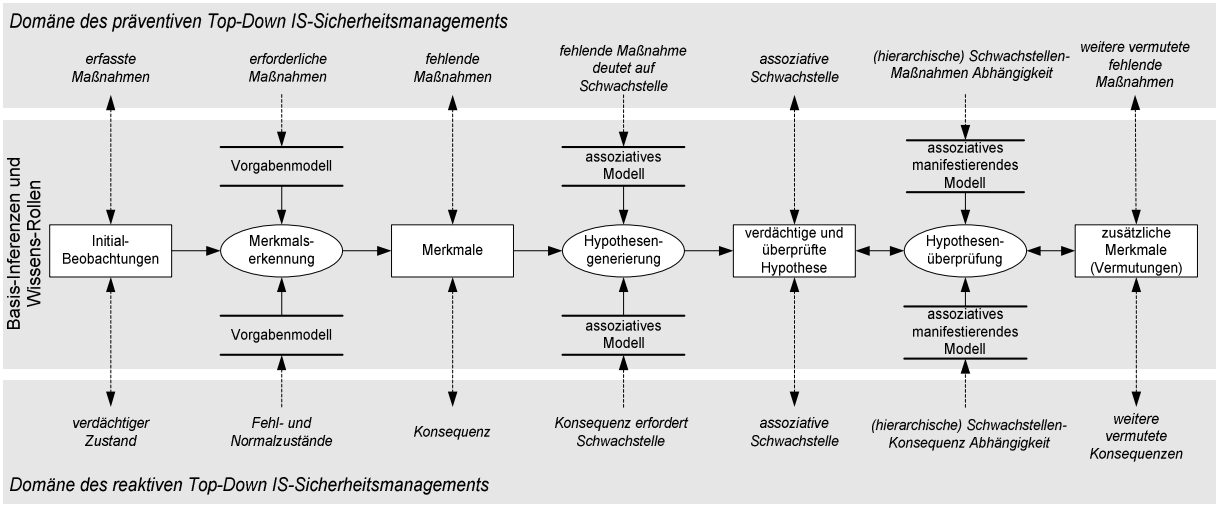
3.4.2.1 Heuristische Klassifikation

Im Folgenden erfolgt eine Zusammenstellung der Überführung der Basiskonzepte des reaktiven und präventiven Top-Down IS-Sicherheitsmanagements auf die Wissens-Rollen der spezifischen Problemlösungsmethoden der

- reaktiven und
- präventiven

heuristischen Klassifikation.

Basis-Inferenzen der präventiven Top-Down Strategie			
Ziel	Präventiv sollen basierend auf fehlenden Maßnahmen mögliche Schwachstellen vorausschauend aufgedeckt werden, um im Vorfeld Gefahren abzuwehren.		
Eingang	Maßnahmen (Merkmale)		
Ausgang	Schwachstellen (Hypothesen)		
Merkmalserkennung		**Hypothesengenerierung**	**Hypothesenüberprüfung**
Fehlende Maßnahmen abstrahieren und erkennen		Aufdeckung von möglichen Schwachstellen	Verdachts-Schwachstellen sind durch weitere Maßnahmen zu überprüfen



Beobachtete Fehlzustände (Wirkungen) abstrahieren und als Konsequenzen erkennen	Aufdeckung von möglichen Schwachstellen, die für das Auftreten der Konsequenzen erforderlich sind	Verdachts-Schwachstellen sind durch weitere Konsequenzen zu überprüfen und einzugrenzen
Merkmalserkennung	**Hypothesengenerierung**	**Hypothesenüberprüfung**

Eingang	Konsequenzen (Merkmale)
Ausgang	Schwachstellen (Hypothesen)
Ziel	Reaktiv wird von beobachteten Konsequenzen auf Schwachstellen gedeutet, die für die Konsequenzen erforderlich sind.
Basis-Inferenzen der reaktiven Top-Down Strategie	

Abbildung 73: Überführung des reaktiven und präventiven Top-Down IS-Sicherheitsmanagements auf die heuristische Klassifikation

Die Merkmalserkennung erfolgt durch Vergleich eines Vorgabenmodells und den abstrahierten Beobachtungen. Auf Grund der Interpretation des Vergleichsresultats können Merkmale erkannt werden.

- Präventiv besteht das Vorgabenmodell aus erforderlichen Maßnahmen, die häufig in Kriterienwerken repräsentiert werden.
- Reaktiv sind vorgegebene Fehl- und Normalzustände in dem Vorgabenmodell repräsentiert.

Die Strategie der heuristischen Hypothesengenerierung und -überprüfung setzt sich aus dem assoziativen Schließen von Merkmalen auf Hypothesen und deren Verfeinerung zusammen. Dabei wird abduktiv von Merkmalen auf Hypothesen geschlossen (Hypothesengenerierung); diese Hypothesen werden durch deduktiv ermittelte zusätzliche Merkmale überprüft und verfeinert (Hypothesenüberprüfung).

- Präventiv wird bei der Hypothesengenerierung ausgehend von fehlenden Maßnahmen auf Schwachstellen gefolgert, wohingegen bei der
- reaktiven Hypothesengenerierung von beobachteten Konsequenzen auf Schwachstellen geschlossen wird.

Das Ziel der anschließenden Hypothesenüberprüfung ist das Überprüfen und Verfeinern von Schwachstellen-Hypothesen durch weitere vermutete Merkmale, wie z.B. Maßnahmen und/oder Konsequenzen. Hierbei kann ein Iterationsprozess entstehen, da eventuell neue Schwachstellen ermittelt werden und weitere Merkmale zur Überprüfung notwendig sind.

Die Hypothesenüberprüfung kann mit Hilfe der Rückwärtsverkettung erfolgen, wobei ausgehend von Verdachtshypothesen alle Regeln ausgewertet werden, welche zur Erreichung bzw. Überprüfung der Schwachstelle (Ziel) beitragen können. Falls Vorbedingungen in den Regeln unbekannt sind, werden diese rekursiv als Unterziele (verknüpfte Schwachstelle) hergeleitet oder vom Benutzer erfragt. Diese Form der Hypothesenüberprüfung hat den Nachteil, dass die Anforderung zusätzlicher Merkmale implizit in den Regeln zur Hypothesengenerierung enthalten ist, was zuverlässiges kausales Wissen voraussetzt. Dies ist bei der Top-Down Problemlösung meist nicht vorhanden und somit ist eine erforderliche rückwärtsverkettete Tiefensuche nicht möglich. Deshalb ist es sinnvoll, das assoziative Wissen zur Überprüfung einer Hypothese explizit durch ein manifestierendes Modell getrennt vom Hypothesengenerierungs-Wissen abzubilden[436].

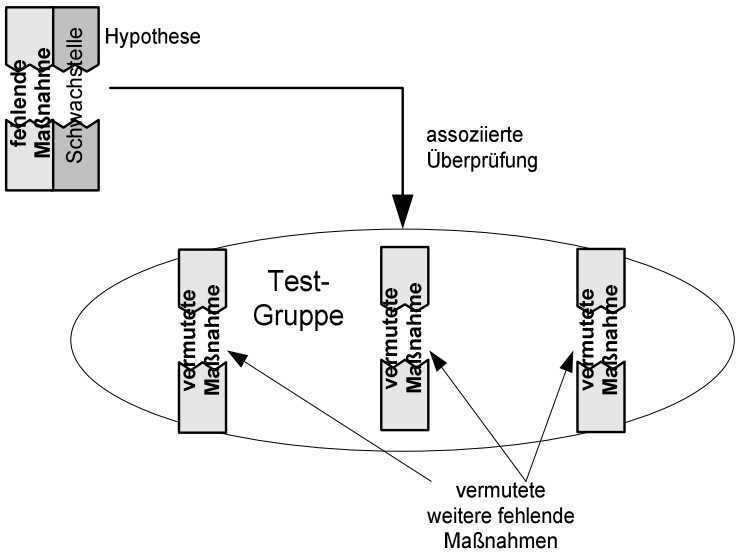


Abbildung 74: Manifestierende Test-Gruppen

Hierzu werden zur Überprüfung notwendige vermutete fehlende Maßnahmen zu Gruppen (Tests) zusammengefasst bzw. assoziiert, damit diese auch im jeweiligen Kontext zusammenhängend erfragt werden. Hierbei werden bei den Generierungs-und-Test Zyklen immer nur die Überprüfungs-Merkmale ausgewählt, die zur Überprüfung notwendig sind. Erst wenn die Schwachstelle verdächtigt wird, werden die „Überprüfungs-Maßnahmen“ aktiviert. Diesen Überprüfungs-Gruppen kann eventuell das Kosten-Nutzen-Wissen hinzugefügt werden, um den Aufwand der zusätzlichen Erhebung und dessen Nutzen abzuschätzen.

[436] Vgl. Puppe (1991), S. 79

3.4.2.2 Establish-Refine Strategie (hierarchische Klassifikation)

Für die Überprüfung und Verfeinerung von Schwachstellen ist es besonders hilfreich, wenn Abhängigkeiten zwischen Schwachstellen und Maßnahmen zusätzlich durch hierarchische Modelle abgebildet werden können. Die vermuteten fehlenden Maßnahmen und Schwachstellen können dann übersichtlich strukturiert werden und die Establish-Refine Strategie angewandt werden. Ferner kann für die Hypothesengenerierung und -überprüfung das gleiche Domänenmodell verwendet werden, wenn die Abhängigkeitskonzepte in hierarchischen Strukturen vorliegen.

Die Establish-Refine Strategie ist ein Spezialfall der Generierungs-und-Test Strategie und basiert auf hierarchischen Schwachstellen-Maßnahmen-Abhängigkeiten. Eine verdächtigte Schwachstelle (A) wird durch zusätzliche Maßnahmen (1 und 2) bestätigt bzw. etabliert und eventuell werden weitere Schwachstellen (B und C) verdächtigt, die wiederum durch zusätzliche Maßnahmen bestätigt werden können. Durch diese hierarchische Überprüfung werden die Schwachstellen immer mehr verfeinert. Diese Vorgehensweise entspricht hierarchischen Test-Gruppen, denen Verdachts-Schwachstellen zugeordnet sind.

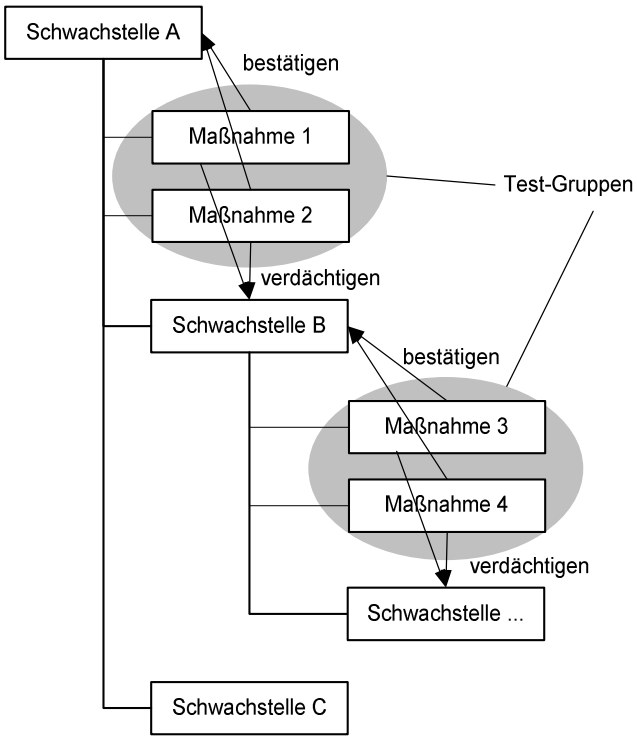


Abbildung 75: Beispiel einer Schwachstellenhierarchie und ihre Anwendung durch die Establish-Refine Strategie

Um eine komplexere Hypothesenüberprüfung innerhalb der Establish-Refine Strategie zu erreichen, kann die Überprüfung mit manifestierenden Test-Gruppen kombiniert werden.

3.4.2.3 Modellbasierte Diagnose

Bei der modellbasierten Diagnose wird zwischen der Wirkungs- und Ursachenanalyse unterschieden.

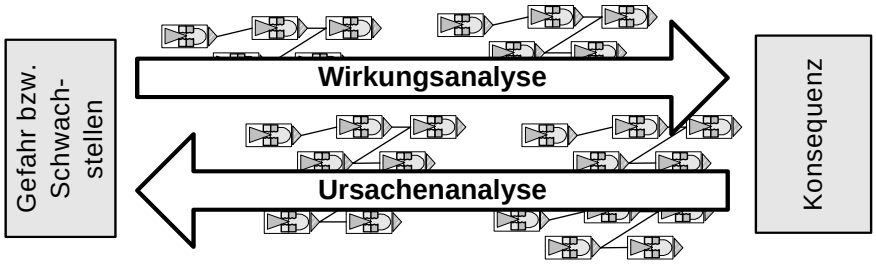


Abbildung 76: Wirkungs- und Ursachenanalyse

Diese beiden Analysemethoden werden ebenfalls in der FMEA angewendet, wobei sie hier als Fehlerbaumanalyse (nach DIN 25424) und Ereignisablaufanalyse (nach DIN 25419) bezeichnet werden. Die Fehlerbaumanalyse kann inhaltlich mit der Ursachenanalyse und die Ereignisablaufanalyse mit der Wirkungsanalyse gleichgesetzt werden[437]. Beide Analyseformen basieren auf Systemmodellen, wobei insbesondere deren kausale Abhängigkeitskonzepte von Bedeutung sind.

Im Folgenden erfolgt eine Zusammenstellung der Überführung der Basiskonzepte des Bottom-Up IS-Sicherheitsmanagements auf die Wissens-Rollen der spezifischen Problemlösungsmethode „modellbasierte Diagnose“.

3.4.2.3.1 Reaktive Ursachen-Problemlösung

Die Ursachenanalyse versucht - ausgehend von einem potentiellen Fehlzustand (Konsequenz) - dessen mögliche Ursache zu analysieren. Dadurch ist es möglich, den Entstehungspfad des Schadens (Konsequenz) bis zur Quelle hin zu untersuchen. Die Ursachenanalyse hat einen reaktiven Charakter, da Fehlzustände aufgetreten sind und deren Ursprung erklärt werden soll[438].

[437] Vgl. Müller/Tietjen (2000), S. 53
[438] Vgl. Stelzer (1993), S. 218

Basis-Inferenzen der reaktiven modellbasierten Diagnose		
Ziel	Reaktiv werden aufgetretene Konsequenzen durch Ursachen in Form von gefährdenden Ereignissen und kausalen Schwachstellen erklärt. Die reaktiven Schwachstellen ermöglichen die beobachteten Konsequenzen. Somit stellen Schwachstellen indirekte Verdachtsursachen dar[439], wohingegen gefährdende Ereignisse direkte Verdachtsursachen darstellen.	
Eingang	Konsequenzen (Wirkungen)	
Ausgang	Gefährdende Ereignisse und kausale Schwachstellen (Ursachen)	
Merkmalserkennung	**Hypothesengenerierung**	**Hypothesenüberprüfung**
beobachtete Fehlzustände (Wirkungen) abstrahieren und als Konsequenzen erkennen	gefährdendes Ereignis und Schwachstelle werden als Erklärung für die Konsequenzen ermittelt	Vorhersage von weiteren Konsequenzen, um die Verdachtsursachen zu überprüfen
Der reaktive Bottom-Up Ansatz basiert auf kausalem Abhängigkeitswissen. Hiermit ist eine Tiefenanalyse bzw. -suche für bestimmte Ursachen möglich.		

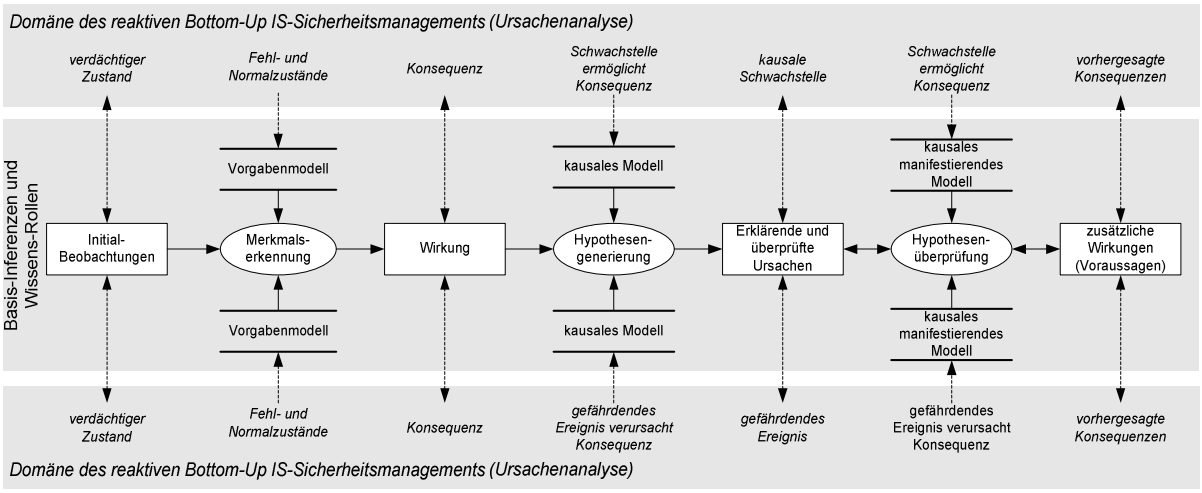


Abbildung 77: Überführung des reaktiven Bottom-Up IS-Sicherheitsmanagements auf die modellbasierte Diagnose

Die Merkmalserkennung erfolgt durch das Vergleichen von erhobenen Zuständen mit Fehl- und Normalzuständen aus dem Vorgabenmodell. Für die Ursachenanalyse eignet sich die überdeckende Hypothesengenerierung und deren -überprüfungen. Ziel der überdeckenden Diagnose ist die abduktive Ermittlung von Ursachen, welche die beobachteten Wirkungen (am besten) erklären bzw. überdecken. Im Rahmen der überdeckenden Hypothesengenerierung wird ausgehend von beobachteten Konsequenzen „überdeckend" auf deren Ursachen in Form von gefährdenden Ereignissen geschlossen. In der Hypothesenüberprüfung werden für die ermittelten Ursachen deduktiv weitere Wirkungen vorausgesagt, welche die Ursachen zusätzlich erklären oder überprüfen können.

Die Ursachen und Wirkungen können zu komplexen kausalen Modellen verknüpft werden, wobei die Verknüpfung durch Zustandsänderungen einer Konsequenz hin zu einer Gefahr für ein anderes gefährdendes Ereignis dargestellt wird. Hierdurch können weitere verknüpfte Ursachen bzw. die Ursprungs-Konsequenzen oder die Gefahr ermittelt werden, die letztlich für die beobachteten Konsequenzen verantwortlich sind. Durch die Hypothesengenerierung werden eventuell Ursprungs-Konsequenzen ermittelt, welche Ausgangs-Konsequenzen indirekt bestätigen. Diese Strategie entspricht einer rückwärtsverketteten Tiefensuche.

[439] Hierbei wird davon ausgegangen, dass ein sicherheitsrelevanter Bereich, der keine Schwachstellen besitzt, Gefahren erfolgreich abwehren kann und somit keine Konsequenz erzeugen kann. Sind aber Bereiche mit Schwachstellen ermittelt worden, ermöglichen diese, dass eine negative Wirkung in Form einer Konsequenz entsteht. Vgl. Nosworthy (2000), S. 599

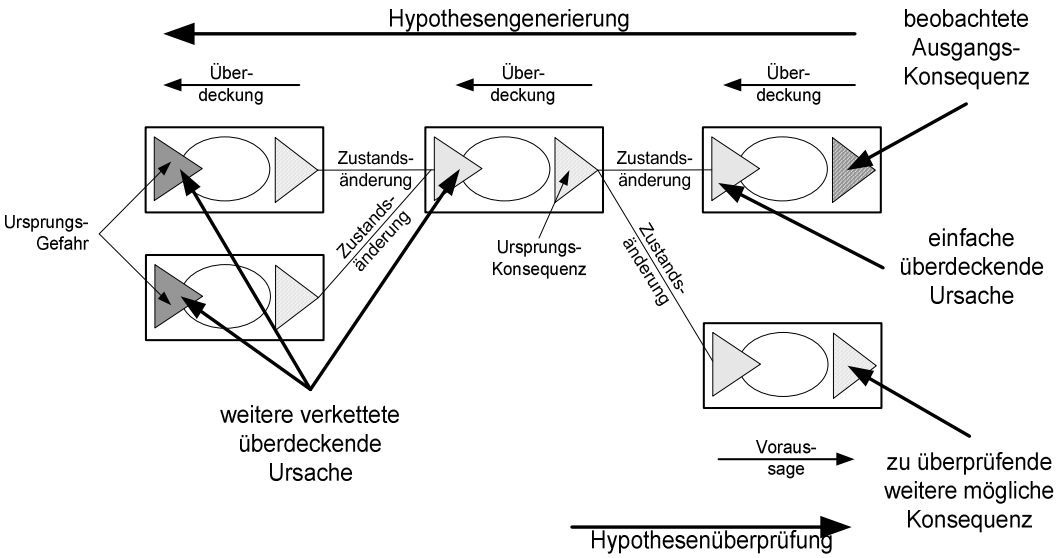


Abbildung 78: Hypothesengenerierung und -überprüfung mit Hilfe von kausalen Modellen

Zusätzlich können durch Hypothesenüberprüfung mögliche Konsequenzen vorhergesagt bzw. vermutet werden, die noch nicht erhoben worden sind. Falls die vermuteten Konsequenzen beobachtet werden, bestätigen sie die Ursachen-Konsequenz oder Gefahr und somit indirekt die Ausgangs-Konsequenz. Bei der Hypothesengenerierung und -überprüfung können neben den gefährdenden Ereignissen auch kausale Schwachstellen ermittelt werden, wobei die Schwachstellen die Ursachen indirekt ermöglichen. Hierbei ist zu beachten, dass den sicherheitsrelevanten Elementen die „kausalen“ Schwachstellen zuverlässig als technische Fehler zugeordnet werden müssen.

Für die Hypothesengenerierung und -überprüfung kann das gleiche kausale Domänenmodell verwendet werden. Der Umgang mit Mehrfachlösungen und Rückkopplungen erschwert die Hypothesengenerierung und -überprüfung in hohem Maße. Deshalb wird für den Umgang dieser komplexen Problemstellungen häufig auf Heuristiken zurückgegriffen und die Auswahl bei mehreren Verdachts-Ursachen dem Benutzer überlassen[440].

3.4.2.3.2 Präventive Wirkungs-Problemlösung

Die präventive Wirkungsanalyse besitzt nicht die charakteristische hypothetisch-deduktive Vorgehensweise der Problemklasse „Diagnose“, in welcher aus erhobenen Wirkungen auf Ursachen geschlossen wird (und die Ursachen deduktiv überprüft und verfeinert werden). Die Wirkungsanalyse ist eher der Problemklasse „Simulation“ zuzuordnen, die als Aufgabe die Vorhersage von Auswirkungen von bestimmten Annahmen auf ein System hat. Übertragen auf die Begrifflichkeit der modellorientierten Diagnose wird ausgehend von Ursachen (Hypothesen) auf deren Wirkungen (Merkmale) geschlossen.

[440] Vgl. Puppe et al. (1996), S. 119

Obwohl die Wirkungsanalyse nicht unmittelbar der Problemklasse Diagnostik zugeordnet wird, soll die Problemlösung der Wirkungsanalyse im Rahmen der Diagnostik beschrieben werden. Von Bedeutung ist, dass nicht ein „typisches“ und in den meisten Fällen komplexes Simulationsmodell verwendet wird, sondern ein kausales „Simulationsmodell“ der Diagnose. Hierbei ist anzumerken, dass während der Hypothesenüberprüfung der modellbasierten Diagnose schon eine vereinfachte Form der Simulation stattfindet, in welcher auf Basis von Verdachts-Ursachen weitere Wirkungen (Merkmale) vorhergesagt bzw. simuliert werden, um die Ursachen zu überprüfen.

Im Folgenden verwendet die „kausale“ Simulation die kausalen Abhängigkeitskonzepte der modellbasierten Hypothesengenerierung und -überprüfung. Hiermit können zwar nicht die gleichen Verhaltenszustände wie bei „klassischen“ Simulationsmodellen generiert werden, aber für eine Wirkungssimulation mit einem experimentellen Charakter reichen die kausalen Abhängigkeitskonzepte aus. Somit können durch Annahme in Form von gefährdenden Ereignissen deren Auswirkungen bzw. Konsequenzen betrachtet werden. Deshalb kann die Wirkungsanalyse auch als „Lernmittel“ der IS-Sicherheit bzw. als vorausschauende (präventive) Problemlösung bezeichnet werden. Auch dient die präventive Problemlösung zur Unterstützung der Szenario-Technik, die einen vorausschauenden Charakter besitzt[441]. Hierfür wird ein Szenario von Schwachstellen, Gefahren und sicherheitsrelevanten Elementen angenommen, um deren Konsequenzen zu antizipieren.

Eine Hypothesenüberprüfung kann erfolgen, wenn für die angenommenen Ursachen und vorausgesagten Wirkungen vergleichbare historische Fälle ermittelt werden können. Die ähnlichsten historischen Ursachen und Wirkungen können erstens die Voraussage bestätigen und zweitens eventuell Lösungsvorschläge enthalten, um die vorhergesagte Konsequenz zu verhindern. Hierfür werden die bekannten Vergleichsfälle in einer Datenbank gespeichert, in der die wesentlichen Merkmale eines Falls - wie z.B. Konsequenzen, Gefahren, sicherheitsrelevante Elemente und Schwachstellen - repräsentiert sind. Die „klassische“ Merkmalserkennung im Rahmen der Hypothesengenerierung entfällt, da Merkmale bzw. Wirkungen durch die Wirkungsanalyse angenommen und nicht durch Beobachtungen ermittelt werden.

[441] Vgl. Sigesmund (1995), S. 128

Basis-Inferenzen der präventiven modellbasierten Diagnose	
Ziel	Ausgehend von gefährdenden Ereignissen und kausalen Schwachstellen werden präventiv deren Konsequenzen (Wirkungen) vorhergesagt bzw. simuliert.
Eingang	angenommene gefährdende Ereignisse und Schwachstellen (Ursachen)
Ausgang	vorhergesagte Konsequenzen (Wirkungen)

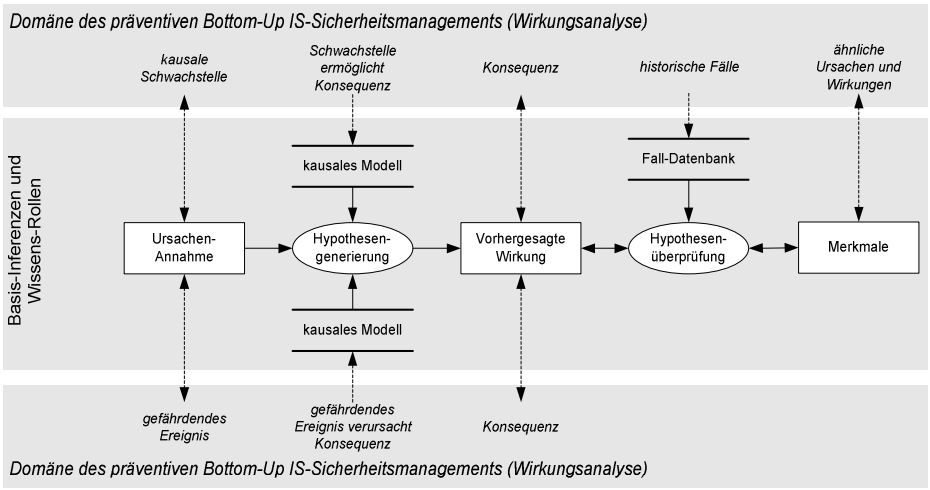


Abbildung 79: Überführung des präventiven Bottom-Up IS-Sicherheitsmanagements auf die modellbasierte Diagnose

Die „kausale“ Simulation versucht, ausgehend von gefährdenden Ereignissen und kausalen Schwachstellen, deren Wirkungen in Form von Konsequenzen abzuleiten. Diese Konsequenzen können sich wiederum auf sicherheitsrelevante Elemente auswirken, so dass durch iterative Verfolgung der Konsequenzen ein inferentielles Netz in Form eines Baumes entsteht.

3.4.3 Wiederverwendungsorientierte Basis-Inferenzen der IS-Sicherheitsstrategien

Die Inferenzen der anwendungsorientierten Problemlösungsmethoden besitzen weitgehend eine monofunktionale Ausprägung. Die monofunktionale Ausprägung wird durch die Anforderungen der heuristischen Klassifikation und der modellorientierten Diagnose bestimmt. Um die Wiederverwendung der einzelnen Inferenz-Strukturen zu erreichen, sollten die spezifischen Problemlösungsmethoden miteinander kombiniert werden können. So besitzen die assoziativen Problemlösungsmethoden die Stärken im Erkennen von fehlenden Maßnahmen und deren Schwachstellen. Modellorientierte Problemlösungsmethoden haben dagegen ihre Leistungsfähigkeit in der Erklärung von Konsequenzen oder Ermittlung von Wirkungen.

Für den Erklärungsaspekt ist ein möglichst zuverlässiges Wissen auf Basis von kausalen Systemmodellen nötig. Deshalb sinkt die Attraktivität für die überdeckende Diagnose beträchtlich, wenn die kausalen Abhängigkeiten überwiegend unsicher sind. In diesem Fall kann heuristisches Wissen verwendet werden, um für den gesamten Umfang der Informationssysteme Verdachtsdiagnosen aufzustellen (Breitenanalyse). Nur bestimmte sicherheitskritische Teilbereiche werden mit Hilfe kausaler Inferenz-Strukturen abgebildet (Tiefenanalyse). Der Vorteil liegt in der Kombination von unterschiedlichen Wissensformen und Inferenz-Strukturen. Des Weiteren ist der Aufwand vergleichsweise geringer, einer heuristischen Wissensbasis überdeckendes kausales Wissen hinzuzufügen (oder umgekehrt), als eine komplett neue kausale oder

assoziative Wissensbasis aufzubauen[442]. So kann es sinnvoll sein, eventuell beide Formalismen gleichzeitig zu repräsentieren. Wie im Folgenden gezeigt wird, besitzen heuristische und modellorientierte Inferenz-Strukturen Überschneidungen, die für ein kombiniertes Problemlösungs-Szenario verwendet werden können.

Inferenz-Templates

Ziel des folgenden Abschnittes ist es, eine Wiederverwendbarkeit und Kombination der Inferenz-Strukturen und Wissens-Rollen zu erreichen. Die Grundlage für die individuelle Anpassung der Inferenz-Strukturen an die IS-Sicherheitsstrategien bilden Inferenz-Schablonen bzw. Templates, welche die Inferenz-Strukturen und Wissens-Rollen auf einer Ebene zwischen den Basis-Inferenzen der Diagnose und Inferenzen der IS-Sicherheitsstrategien abbilden. Hierbei werden zuerst die Aspekte der Domänenebene weitgehend vernachlässigt, wobei die Templates schnell mit den Anforderungen an das Wissen der Domänenebene - insbesondere durch Abhängigkeitskonzepte - ergänzt werden können.

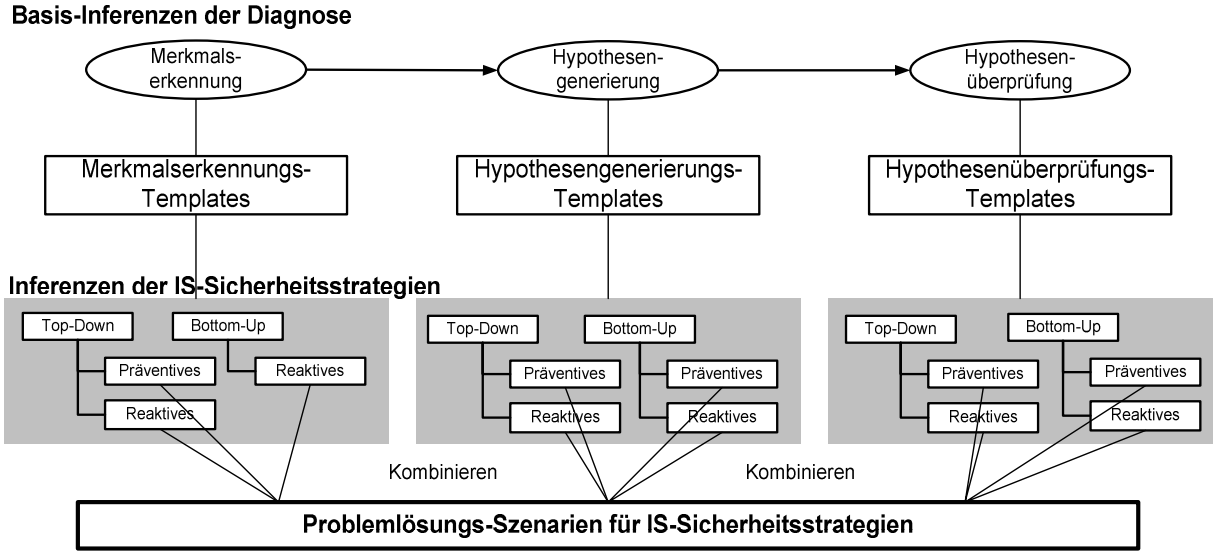
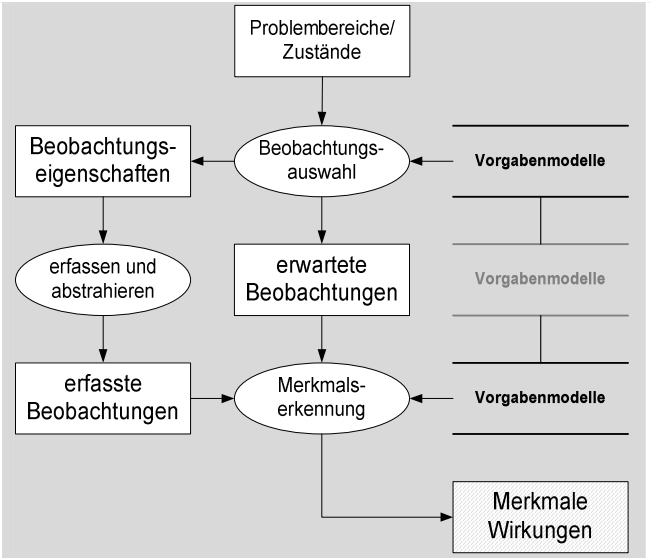


Abbildung 80: Zusammenhang zwischen Inferenz-Templates und Problemlösungsmethoden der IS-Sicherheitsstrategien

Die Templates sind unabhängig von dem spezifischen Anhängigkeits- bzw. Problemlösungskonzept oder der Domänenbasis einer IS-Sicherheitsstrategie; sie haben aber schon die wesentlichen gemeinsamen Inferenz-Strukturen der IS-Sicherheitsstrategien-Problemlösungsmethoden. Durch Kombination der Templates entstehen zusammengesetzte Problemlösungsmethoden, die als Problemlösungs-Szenarien bezeichnet werden. Bei Veränderungen der Templates ist darauf zu achten, dass die Schnittstellen der Wissens-Rollen erhalten bleiben. Die folgende Abbildung stellt die Templates dar.

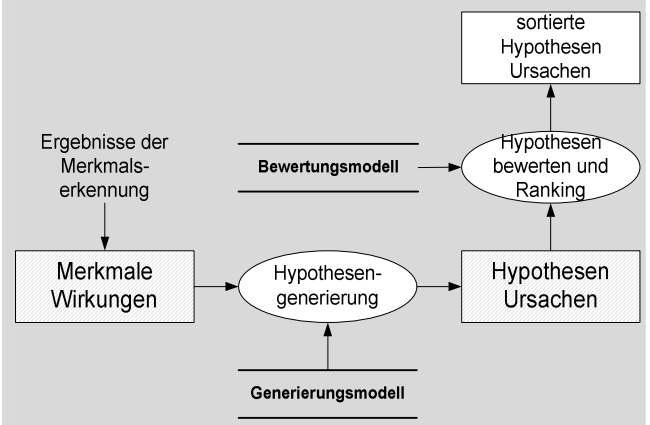
[442] Vgl. Puppe et al. (1996), S. 120

Templates der Basis-Inferenzen für die IS-Sicherheitsstrategien



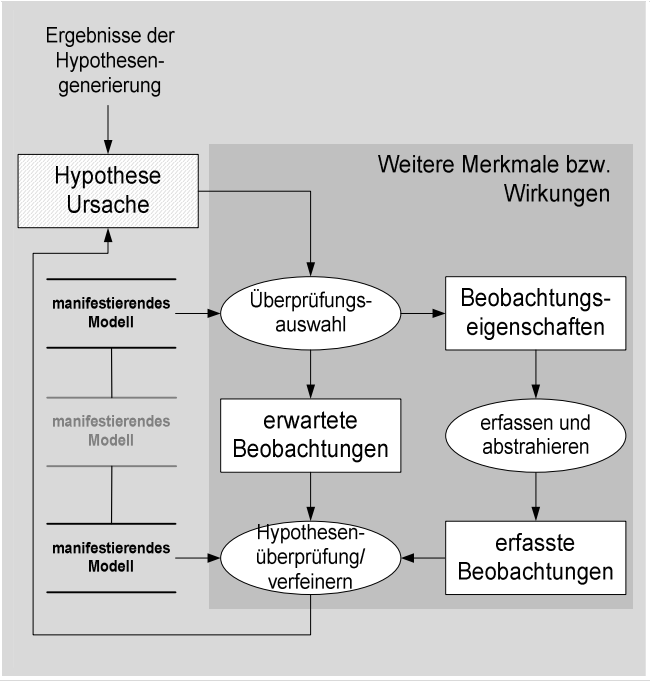
Merkmalserkennung

In der **Beobachtungsauswahl** werden die erwarteten Beobachtungen und Beobachtungseigenschaften festgelegt.
Im Rahmen der **Merkmalserkennung** werden die erfassten und abstrahierten Beobachtungen mit den erwarteten Beobachtungen verglichen. Auf Basis des Resultates werden die Merkmale bzw. Wirkungen festgelegt.
Die **Vorgabenmodelle** für die Beobachtungsauswahl sowie die Merkmalserkennung können zu einem Modell zusammengefasst oder getrennt erstellt werden.



Hypothesenauswahl

Aus den Merkmalen bzw. Wirkungen werden durch die **Hypothesengenerierung** basierend auf einem Generierungsmodell Hypothesen bzw. Ursachen abgeleitet.
Diese können im Rahmen der **Verdachts- bzw. Hypothesenbewertung** eventuell zusätzlich bewertet oder gerankt werden.



Hypothesenüberprüfung

In der **Überprüfungsauswahl** werden die erwarteten Beobachtungen und Beobachtungseigenschaften von weiteren Merkmalen oder Wirkungen festgelegt, welche Hypothesen bzw. Ursachen überprüfen sollen. Die Überprüfungsauswahl basiert auf manifestierenden Modellen.
Die **Hypothesenüberprüfung** erfolgt ähnlich der Merkmalserkennung durch Vergleich der erfassten und abstrahierten Beobachtungen mit den erwarteten Beobachtungen. Auf Basis des Resultates werden die Hypothesen bzw. Ursachen bestätigt oder widerlegt. Durch Überprüfung können eventuell zusätzliche (verfeinerte) Hypothesen bzw. Ursachen ermittelt werden.
Die **manifestierenden Modelle** für die Überprüfungsauswahl und Hypothesenüberprüfung können zu einem Modell zusammengefasst oder getrennt erstellt werden.

Abbildung 81: Templates der Basis-Inferenzen für die IS-Sicherheitsstrategien

Die Templates bieten den Vorteil der Flexibilität und Individualisierung der Inferenz-Strukturen, da diese unabhängig von der spezifischen IS-Sicherheitsstrategie erweitert oder verändert werden und schnell mit dem benötigten kausalen und heuristischen Domänenwissen erweitert werden können. Die mit kausalen und heuristischen Domänenwissen spezifisierten Templates besitzen dann wieder einen anwendungsorientierten Charakter. In der folgenden Abbildung werden die Inferenz-Templates auf die Inferenzen der spezifischen Problemlösungsmethoden von IS-Sicherheitsstrategien überführt und die Anforderungen an die Domänenebene beschrieben. Hierbei werden dynamische und statische Wissens-Rollen der Templates durch konkrete Basis- und Problemlösungskonzepte der IS-Sicherheitsstrategien abgebildet.

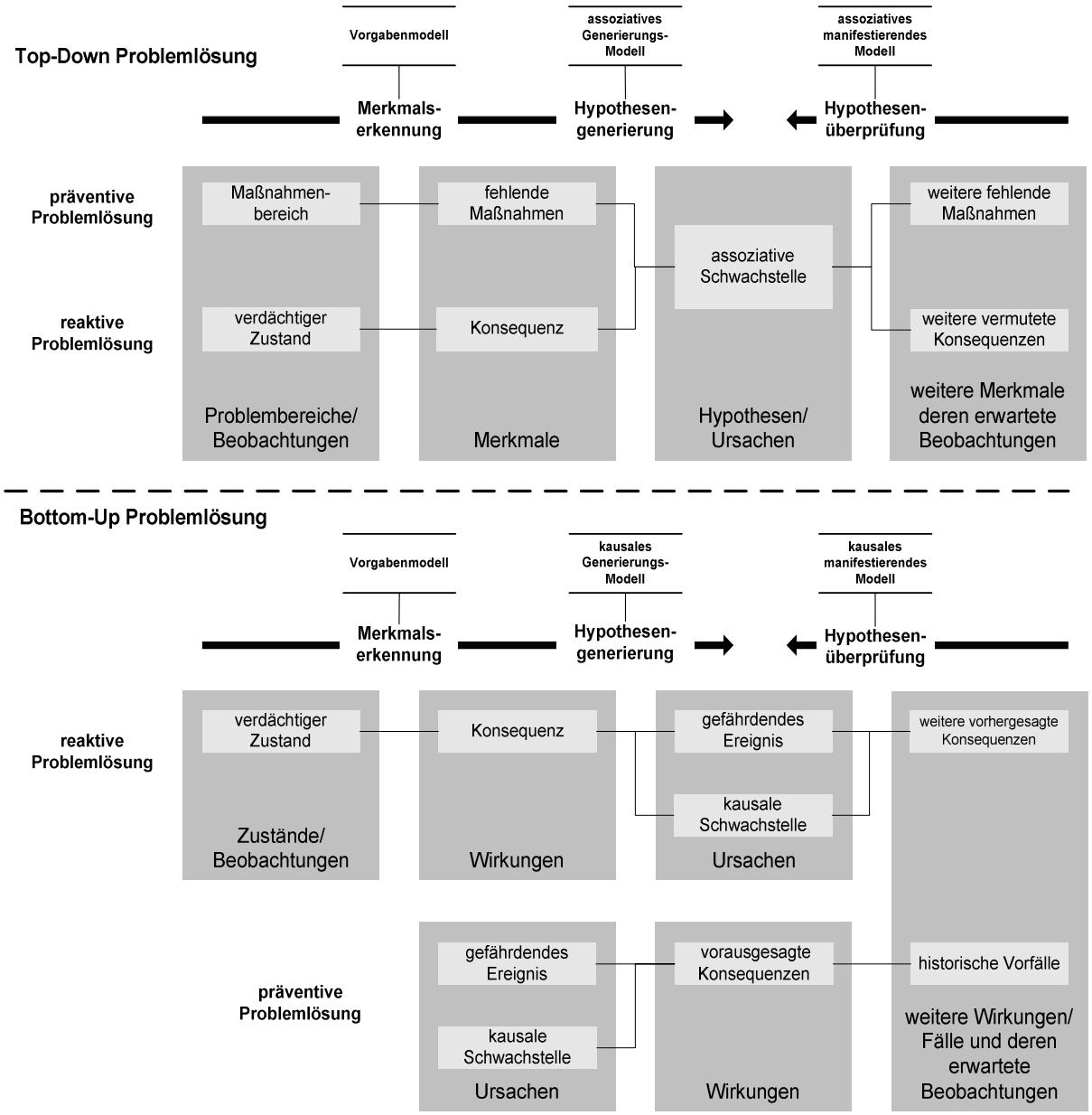


Abbildung 82: Überführung der Top-Down und Bottom-Up Problemlösung auf die Basis-Inferenz Templates

Die Merkmalserkennung für die Top-Down und Bottom-Up Problemlösung erfolgt in ähnlicher Form. So wird bei der Merkmalserkennung keine Unterscheidung zwischen Top-Down und Bottom-Up durchgeführt, sondern nur zwischen präventiver und reaktiver Merkmalserkennung. Für die präventive Bottom-Up Problemlösung wird keine Merkmalserkennung benötigt, da Ursachen als Merkmals-Annahmen in eine Simulations-Problemlösung eingehen. Für die weitere Hypothesengenerierung und -überprüfung ist eine differenziertere Unterscheidung zwischen Top-Down und Bottom-Up Problemlösung erforderlich.

Durch die Top-Down Problemlösung werden überwiegend assoziative Schwachstellen aufgedeckt, die auf fehlenden Maßnahmen basieren. Die Unterscheidung zwischen reaktiver und präventiver Sicht erfolgt im Wesentlichen durch die unterschiedliche Überführung der IS-Sicherheits-Konzepte auf die Wissens-Rollen. Die Basis-Inferenzen der Problemlösungen Hypothesengenerierung (Merkmal deutet auf Lösung) und ebenso die Hypothesenüberprüfung (Überprüfung der Lösung durch weitere Merkmale) bleiben bei reaktiver und präventiver Sicht gleich. Das Konzept „Schwachstelle“ bildet die Verbindung zwischen der reaktiven und präventiven Sicht.

In der Bottom-Up Problemlösung wird die unterschiedliche Problemlösungsrichtung durch die reaktive und präventive Sicht bestimmt. In der reaktiven Sicht werden ausgehend von Konsequenzen deren Ursachen überdeckend ermittelt. Zur Überprüfung der Verdachts-Ursachen werden weitere vermutete Konsequenzen auf Basis des kausalen Modells festgestellt. Dagegen werden bei der präventiven Sicht ausgehend von Ursachen-Annahmen deren Wirkungen in Form von Hypothesen-Konsequenzen simuliert, womit die präventive Sicht einen vorausschauenden Charakter besitzt. Eine präventive Überprüfung erfolgt nicht auf Basis des kausalen Modells, sondern durch den Vergleich der Voraussagen z.B. mit historischen Vorfällen bzw. erhobenen Konsequenzen.

In der Top-Down Problemlösung ist - im Gegensatz zu den kausalen Modellen der Bottom-Up Problemlösung - kein kausales Ursachen-Wirkungsmodell der konkreten Systeme notwendig. So können auch Schwachstellen ohne Einsatz eines komplexen Ursachen-Wirkungsmodells ermittelt werden. Durch die Bottom-Up Problemlösung können im Gegensatz zu der Top-Down Problemlösung insbesondere technisch kausale Schwachstellen ermittelt werden, wenn die Kausalität in ein Ursachen-Wirkungsmodell überführt werden kann. Dieses Ursachen-Wirkungsmodell bildet ein konkretes - meist technisches - Informationssystem ab, um die kausalen sicherheitsrelevanten Aspekte abzubilden.

Im Anhang A ist das „Mapping“ bzw. die Überführung konkreter Domänen-Konzepte auf die generischen Templates dargestellt. Hierbei wird gezeigt, wie heuristische und modellbasierte Diagnosen durch die Erweiterung der Inferenz-Templates mit konkretem Domänenwissen beschrieben werden können.

Problemlösungs-Szenarien

Durch Kombination der Basis-Inferenzen können Problemlösungs-Szenarien entwickelt werden, die zusammengesetzte Problemlösungsstrategien auf einer epistemologischen Ebene beschreiben. So besteht bei den reaktiven Top-Down oder Bottom-Up Problemlösungen die Problematik, dass Schwachstellen ermittelt werden, aber nicht die benötigten Maßnahmen, um diese Schwachstellen zu schließen. Hier kann eine zusätzliche Maßnahmen-Suche die erforderlichen Maßnahmen ermitteln.

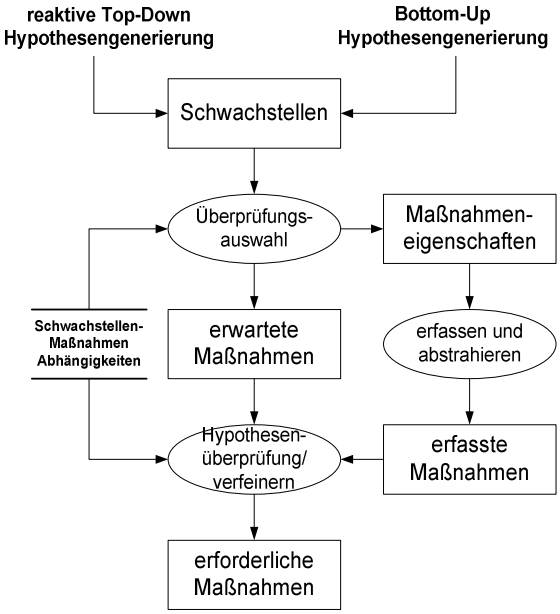
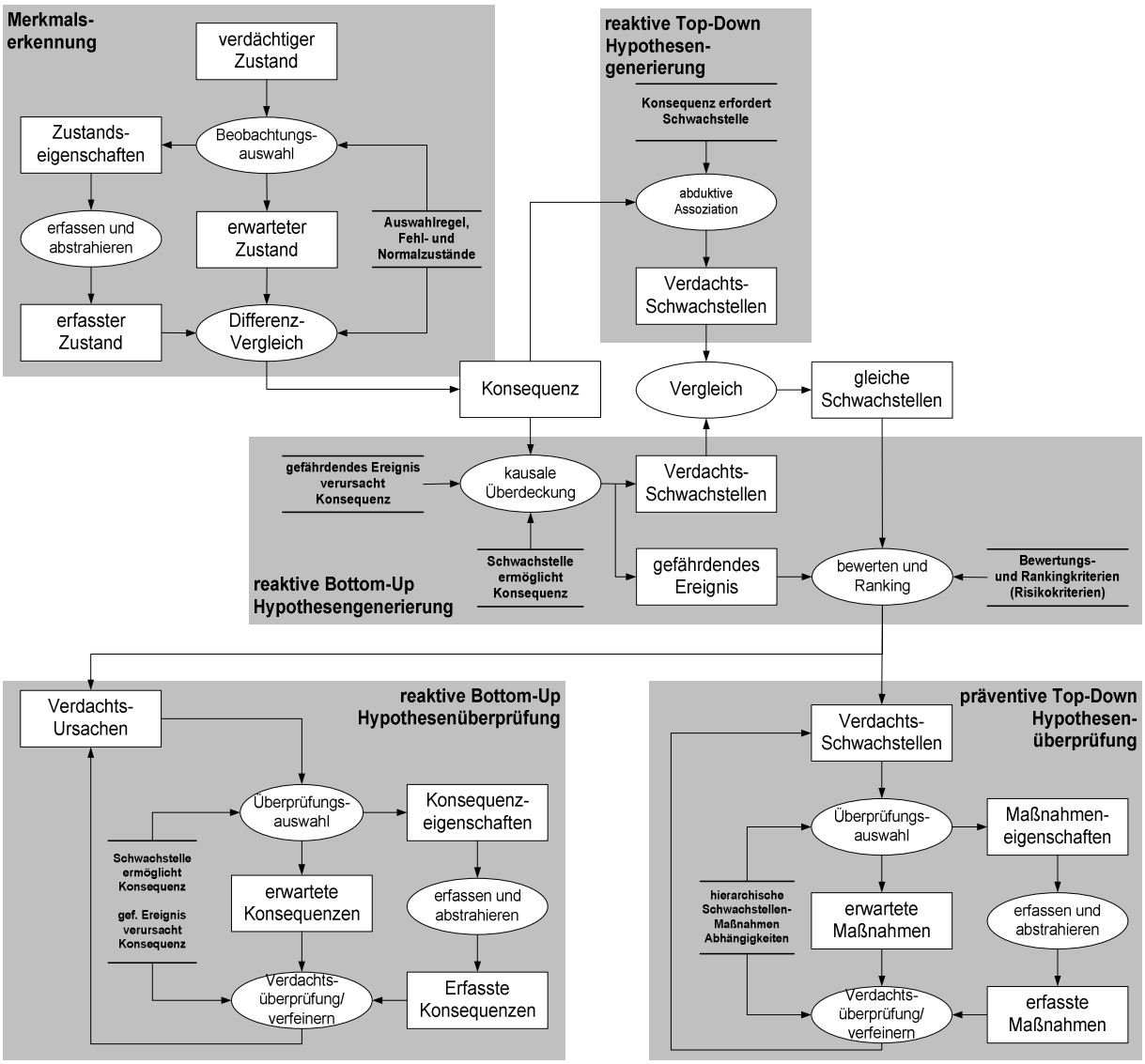


Abbildung 83: Präventive Top-Down Hypothesenüberprüfung als Maßnahmen-Suche

Diese zusätzliche Maßnahmen-Suche kann durch eine hinzugefügte präventive Top-Down Hypothesenüberprüfung erfolgen, die für die ermittelten Schwachstellen nach erforderlichen Maßnahmen sucht.

In dem folgenden Beispiel ist ein umfangreicheres Problemlösungs-Szenario dargestellt. Durch die kombinierte Hypothesengenerierung werden assoziative und kausale Verdachts-Schwachstellen ermittelt. Es werden nur die Schwachstellen weiter überprüft, die in beiden Hypothesengenerierungen ermittelt worden sind.



Basis-Inferenzen	Inferenz-Strukturen
Merkmalserkennung	reaktiver Bottom-Up
Hypothesengenerierung	reaktiver Bottom-Up und Top-Down
	zusätzlicher Vergleich der Verdachts-Schwachstellen
Hypothesenüberprüfung	reaktiver Bottom-Up und präventiver Top-Down

Abbildung 84: Gleichzeitige Problemlösung der Bottom-Up und Top-Down IS-Sicherheitsstrategien

In dem obigen Problemlösungs-Szenario werden nur gleiche Verdachts-Schwachstellen betrachtet. Die Hypothesenüberprüfung der Ursachen erfolgt einerseits Bottom-Up orientiert, um durch weitere vermutete Konsequenzen die Ursachen zu überprüfen. Andererseits werden durch die präventive Top-Down Hypothesenüberprüfung fehlende Maßnahmen ermittelt, um Schwachstellen zu überprüfen. Zugleich werden Maßnahmen gewonnen, damit die ermittelten Schwachstellen geschlossen werden können.

In dem Anhang B wurden umfangreiche Szenarien konstruiert, um den multifunktionalen Charakter der Templates darzustellen. Es wird zudem gezeigt, wie umfangreiche monofunktionale Problemlösungsmethoden ebenfalls durch Inferenz-Templates dargestellt werden können.

4 Entwurfsmodell

Die Repräsentation von „menschlichem“ Wissen kann als symbolische Rekonstruktion von Wissen in einer Wissensrepräsentationssprache verstanden werden[443]. Dies bedeutet, Wissen wird in adäquaten formalorientierten Sprachen repräsentiert bzw. die Wissensrepräsentation ist eine operationale Umsetzung der Wissensebene in eine Symbolebene[444]. Puppe/Stoyan/Studer (2000) bezeichnen die Formalisierung als „... *eine Tätigkeit, bei der eine natürlich-sprachliche Beschreibung der Welt (oder eines Weltausschnitts) in eine formal-sprachliche Beschreibung überführt wird*“[445], wobei für die Arbeit das Management der IS-Sicherheit den zu formalisierenden Weltausschnitt darstellt. Das Entwurfsmodell formalisiert die Repräsentationsformen und Problemlösungsmethoden und bildet die Grundlage für die folgende Implementierung des WBS. Hier liegt ein Problem in der Abgrenzung zwischen formalem Entwurfsmodell und der „eigentlichen“ Implementierung. Das formale Entwurfsmodell soll aber prinzipiell einen höheren Abstraktionsgrad besitzen als die Repräsentation auf der Implementierungsebene.

Adäquatheit der Wissensrepräsentation

Um Kriterien für die Auswahl einer Wissensrepräsentation und Problemlösung zu ermitteln, ist deren Adäquatheit bezüglich der Umsetzung des abzubildenden Problembereichs von Bedeutung. Mit der Adäquatheit einer Repräsentation wird die Übereinstimmung zwischen der Wissensrepräsentation und dem zu repräsentierenden Anwendungsbereich bezeichnet[446]. In der folgenden Abbildung werden Kriterien für die Bewertung der adäquaten Wissensrepräsentation dargestellt.

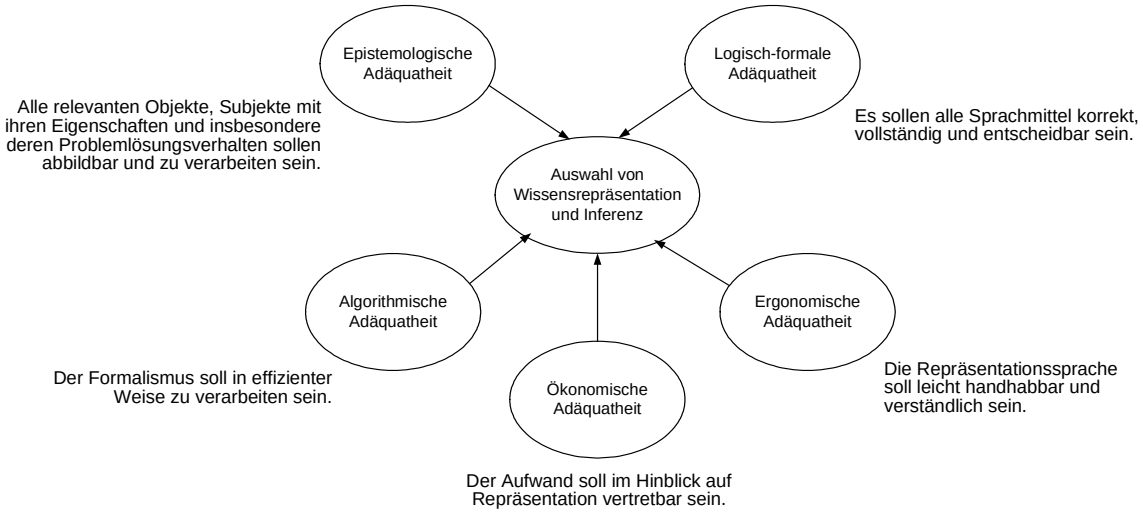


Abbildung 85: Adäquatheit der Wissensrepräsentation[447]

[443] Vgl. Schefe (1986), S. 25
[444] Vgl. Frick (1998), S. 101
[445] Puppe/Stoyan/Studer (2000), S. 600
[446] Vgl. Gabriel (1992), S. 98
[447] Vgl. Lenz (1991), S. 55 und Haun (2000), S. 40-42

Die Repräsentation der IS-Sicherheit soll im Idealfall alle Kriterien erfüllen. Dies ist in der Realität mit den zeitlich und wirtschaftlich begrenzten Ressourcen i.d.R. nicht möglich. Die verschiedenen Kriterien stehen also z.T. miteinander in Konkurrenz. Ist das eine Kriterium erfüllt, so können andere Kriterien in ihrer Ausprägung geschwächt werden. So stehen insbesondere die ergonomischen und ökonomischen Kriterien in Konkurrenz zu den epistemologischen und logisch-formalen Kriterien. Es existiert nicht „die eine" Form der Wissensrepräsentation, um das Wissen der verschiedenen Problemgebiete darzustellen. Es ist vielmehr erforderlich, ein ausgeglichenes Verhältnis zwischen der Problemstellung, dem Nutzerkreis und dem Erstellungs- und Pflegeaufwand der Wissensbasis zu finden. Dies äußert sich in einer geeigneten Kombination aus Repräsentationsformen und Problemlösungsverfahren. Daraus ergibt sich ein Kompromiss der oben angeführten Kriterien[448].

Es sind noch andere Einflussfaktoren, wie z.B. die Vorkenntnisse des Konstrukteurs der Wissensbasis oder die Möglichkeit der direkten Wissenseingabe eines Fachexperten, von Bedeutung. Auch werden häufig Repräsentationsformen zu hybriden Sprachen zusammengeführt, wobei eine Kopplung von frame- und regelbasierten orientierten Formalismen anzutreffen ist[449].

Konstruktionsadäquanz

Der Grundsatz der Konstruktionsadäquanz fokussiert die problemangemessene Nachvollziehbarkeit der Modellkonstruktion. Die Konstruktionsadäquanz bringt zum Ausdruck, dass Modelle immer aus einer bestimmten Perspektive bzw. einem bestimmten Standpunkt heraus entwickelt werden. Dabei stellt sich die Frage, wie angemessen diese Perspektive ist. Somit ist einerseits der Ausgangspunkt der Modellkonstruktion entscheidend, anderseits, wie die Repräsentation des Problems mit Hilfe einer Sprache vorzunehmen ist. Hierbei entstehen konfliktäre Verhältnisse zwischen Modellnutzer und dem Modellersteller[450].

Dieses Modellierungsverhältnis bzw. das Zusammenwirken erfolgt im Rahmen des KE zwischen Fachexperten und dem Knowledge Engineer. Da Fachexperten typischerweise keinen Überblick über Methoden und Techniken des KE besitzen, benötigen sie bei der Konstruktion eines fachspezifischen Expertisemodells und der Auswahl der Entwicklungswerkzeuge die Unterstützung eines Knowledge Engineers. Anders verhält sich die Problematik bei der Eingabe und Wartung des spezifischen IS-Sicherheitswissens sowie bei der Konfiguration des WBS an die jeweilige Situation. Hier sollte die Wissenseingabe direkt durch den Fachexperten erfolgen, ohne dass ein Knowledge Engineer benötigt wird. Diese Vorgehensweise besitzt folgende Motivation:

- Bei der indirekten Wissenseingabe durch den Knowledge Engineer besteht eine fachliche Distanz zwischen Fachexperten (domänenorientiert) und dem Knowledge Engineer (systemorientiert), was sich in vielfältigen Missverständnissen äußern kann. Hierdurch wird der Aufwand einer Wissenseingabe erheblich erhöht. Die Gefahr einer (ungewollten) Verfälschung des Expertenwissens durch den Knowledge Engineer ist gegeben. Dieses Problem wird auch „Knowledge Engineering bottleneck" genannt[451].

[448] Vgl. Kurbel (1992), S. 36
[449] Vgl. Primio (1993) und Dodenhöft (1995)
[450] Vgl. Schütte (1998), S. 114
[451] Vgl. Kurbel (1992), S. 70

- Zudem ist der IS-Sicherheitsexperte von einem hochbezahlten Knowledge Engineer abhängig, was wiederum zu ökonomischen Problemen in der späteren Erweiterung und Pflege des WBS führt, wenn dies ausschließlich durch einen Knowledge Engineer erfolgt.

Programmierer und auch der Knowledge Engineer sind gewöhnt, ihre Programme bzw. Repräsentationssprachen in Form von vorgegebener und formaler Syntax (Programmcode) einzugeben. Bei der direkten Wissenseingabe werden aber Fachexperten und der Knowledge Engineer in einer Person vereint. Für eine solche direkte Form der Wissenseingabe durch einen Fachexperten ist eine Repräsentationssprache erforderlich, welche die Ausdrucksformen des Fachexperten unterstützt. Visuelle Repräsentationssprachen unterstützen die direkte Wissenseingabe durch einen (IS-Sicherheits-)Fachexperten, sind aber nicht auf einen „formalen" Knowledge Engineer ausgerichtet[452]. Jedoch ist der Grad an grafischer Unterstützung stark von der Komplexität bzw. von dem Umfang der Syntax abhängig. Grundsätzlich gilt: Je eingeschränkter die Syntax, desto mehr grafische Unterstützung ist möglich[453].

Diese anwenderfreundlichen und visuellen Repräsentationssprachen und deren WBS haben insgesamt den Vorteil einer problemorientierten Wissensakquisition ohne Berücksichtigung eines kostenintensiven Knowledge Engineers. Sie sind aber nur auf ein begrenztes Aufgabengebiet ausgelegt und besitzen nicht die Universalität bzw. Problemunabhängigkeit von formalen Sprachen, wie z.B. Prolog oder Lisp. Da im Rahmen der Arbeit der Fachexperte „sein" und anderes IS-Sicherheitswissen direkt in ein WBS eingeben und warten soll, sind Repräsentationssprachen erforderlich, welche ohne oder mit geringen Programmierkenntnissen zu beherrschen sind. So hat ein IS-Sicherheitsexperte nicht die zeitlichen Ressourcen, sich in eine formale Repräsentationssprache einzuarbeiten; er achtet eher auf die ergonomische Praktikabilität bzw. Anwendbarkeit und die ökonomischen Aspekte.

4.1 Formalisierungsgrundlage für sicherheitsrelevante Konzepte

Das in einer Wissensbasis befindliche IS-Sicherheitswissen stellt eine Art Referenzmodell dar[454]. Schütte definiert ein Referenzmodell als „*… das Ergebnis einer Konstruktion eines Modellierers, der für Anwendungssystem- und Organisationsgestalter Informationen über allgemeingültige zu modellierende Elemente eines Systems zu einer Zeit als Empfehlungen mit einer Sprache deklariert, so daß ein Bezugspunkt für ein Informationssystem geschaffen wird*."[455] Die Wissensbasis für das IS-Sicherheitsmanagement stellt somit einen Bezugspunkt zum unternehmensspezifischen IS-Sicherheitswissen dar, da sie eine Menge von Anwendungsfällen manifestieren kann.

Referenzmodelle besitzen wie Ontologien eine semantische Dimension, wobei Referenzmodelle zusätzlich eine normative Semantik aufweisen und somit eine empfehlenswerte Konzeptualisierung einer Domäne spezifizieren. Die Spezifikation der Referenzmodelle erfolgt durch eine Kombination aus natürlich- und formal-sprachlichen Mitteln, wohingegen die Spezifizierung von Ontologien tendenziell durch formale Sprachen erfolgt. Auch werden Referenzmodelle für eine bestimmte Domäne entwickelt (hier IS-Sicherheitsmanagement) und entspre-

[452] Vgl. Gappa (1995), S. 4
[453] Vgl. Puppe et al. (1996), S. 70
[454] Vgl. Schütte (1998), S. 81
[455] Schütte (1998), S. 69

chen bzgl. des jeweiligen Betrachtungsspektrums somit den Domänen-Ontologien. Ontologien werden dagegen auch für weitere Gegenstandsbereiche wie Commonsense-, Aufgaben oder Methoden-Ontologien verwendet[456].

Auf Grundlage der IS-Sicherheitsstrategien werden an das Referenzmodell und an das darauf basierende WBS unterschiedliche Anforderungen gestellt. Bei dem Bottom-Up Ansatz steht die Konkretisierung von IS-Sicherheits-Referenzmodellen in unternehmensspezifischen Systemmodellen durch objektorientierte Techniken im Vordergrund. Ausgangspunkt sind Klassenhierarchien, die dem konkreten Problem angepasst werden. Als Ergebnis entsteht ein objektorientiertes Systemmodell, das die spezifische „IS-Sicherheit" der konkreten Institution beschreibt und die Grundlage für ein IS-Sicherheitskonzept darstellt.

Bei dem Top-Down Ansatz erfolgt dagegen die direkte Anwendung von IS-Sicherheitskriterien durch wissensbasierte Fragenkataloge bzw. Expertisesysteme[457] und deren Antworttexten, welche einen Empfehlungs- oder Sollcharakter darstellen. „*Kern von Expertisesystemen ist das Textkonzept, in dem vorformulierte Lückentexte mit Platzhaltern (Textvaribalen) für Textpassagen oder Zahlen enthalten sind, die meist abhängig von der Datenlage* [hier Antworten der Fragen] *regelbasiert eingefügt werden.*"[458] Wissensbasierte Fragen bzw. Checklisten[459] können im Rahmen von wissensbasierten Fragenkatalogen bzw. Expertisesystemen eingesetzt werden, welche eine Variante von WBS darstellen[460].

Expertenwissen wird im Beratungs- und Prüfbereich eingesetzt, wobei hier das Erkennen von Schwachstellen im Vordergrund steht[461]. Hierfür werden Expertisesysteme seit vielen Jahren[462] erfolgreich in betriebswirtschaftlichen Problemstellungen verwendet. Die Expertisesysteme können somit als ein Werkzeug der wissensbasierten Diagnose für den betriebswirtschaftlichen Bereich interpretiert werden. Als Beispiel ist das Expertisesystem „Unternehmensreport" der DATEV zu nennen, das bei den meisten deutschen Steuerberatern eingesetzt wird[463]. Insgesamt werden bei Prüfungen - wie bei einer Jahresabschlussanalyse oder bei Rechts- und Sicherheitsfragen - häufig Expertisesysteme angewandt[464].

Die folgende Abbildung erstellt eine Übersicht der grundsätzlichen Operationalisierungsmöglichkeiten abhängig von den IS-Sicherheitsstrategien.

[456] Vgl. Zelewski/Schütte/Siedentopf (2001), S. 194
[457] Die Begriffe „wissensbasierte Fragenkatalog-Systeme" und „Expertisesystem" werden im Rahmen der Arbeit synonym verwendet.
[458] Mertens (2001), S. 197
[459] Checklisten bestehen im Rahmen der Arbeit überwiegend aus einfachen Ja/Nein Fragen.
[460] Vgl. Puppe/Stoyan/Studer (2000), S. 630
[461] Vgl. Heinrich (2002), S. 528
[462] Schon 1989 beschreibt Mertens (1989) viele Anwendungsbeispiele für Expertisesysteme.
[463] Vgl. Haase et al. (1995), S. 57
[464] Vgl. Mertens/Borkowski/Geis (1993), S. 287

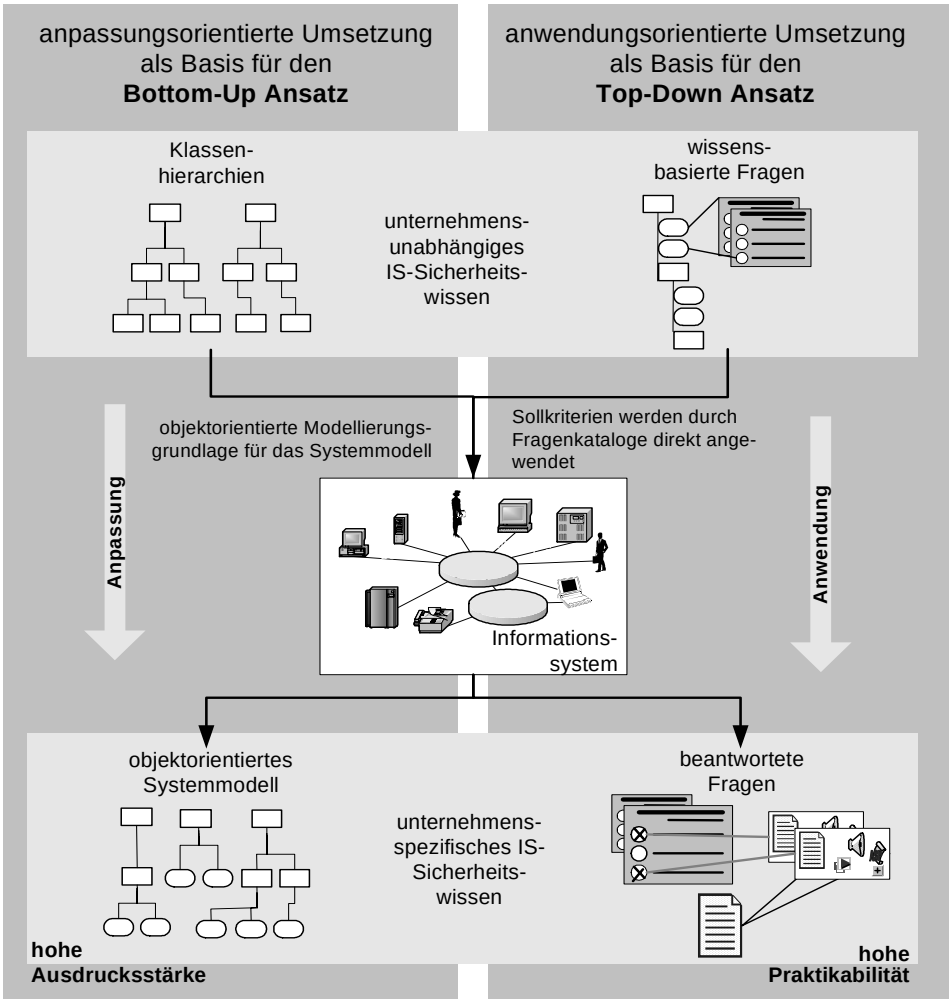


Abbildung 86: Objektorientierte und fragenorientierte Formalisierung

Beiden Repräsentationsformalismen ist gemeinsam, dass sie auf einer Objekt-Attribut-Wert Struktur basieren. Objekte stehen für Gegenstände oder Begriffe (z.B. aus dem IS-Sicherheitsbereich), deren Eigenschaften in Form von Attributen beschrieben werden. Die Eigenschaften können Werte annehmen, die den Ausprägungen der Attribute entsprechen.

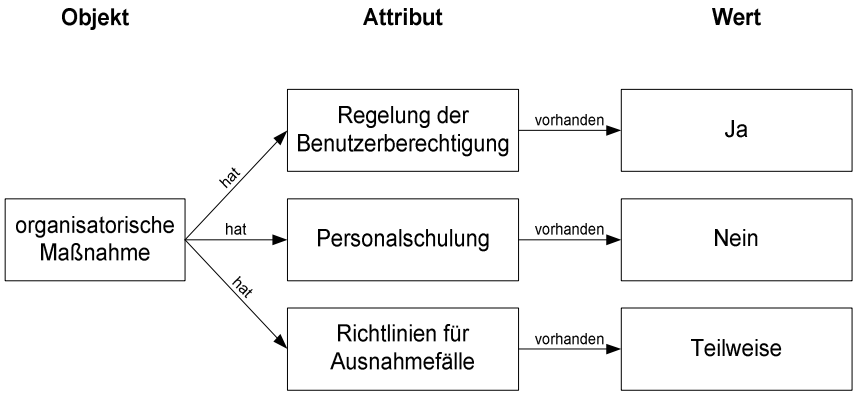


Abbildung 87: Einfache Objekt-Attribut-Wert Struktur

In der Abbildung 88 ist ein Beispiel für eine Objekt-Attribut-Wert Struktur. Es werden organisatorische Maßnahmen durch drei Attribute beschrieben, welche Werte wie „vorhanden“, „nicht vorhanden“ oder „teilweise vorhanden“ annehmen. Auch Fragen können Objekte, Attribute und deren Werte repräsentieren, indem Fragen Antwortmöglichkeiten zugeordnet werden. Diese Antwortmöglichkeiten können Werte annehmen, wodurch Fragen zugleich einen Merkmalsindikator darstellten. Der Unterschied zwischen den beiden Darstellungsformen (Fragenkataloge und objektorientierte Strukturen) erfolgt in der Ausdrucksstärke und der Praktikabilität bei der Überführung des unternehmensunabhängigen IS-Sicherheitswissens in unternehmensspezifisches Wissen. In der folgenden Abbildung wird eine Einordnung von wissensbasierten Fragenkatalogen in Wissensrepräsentationsformalismen dargestellt.

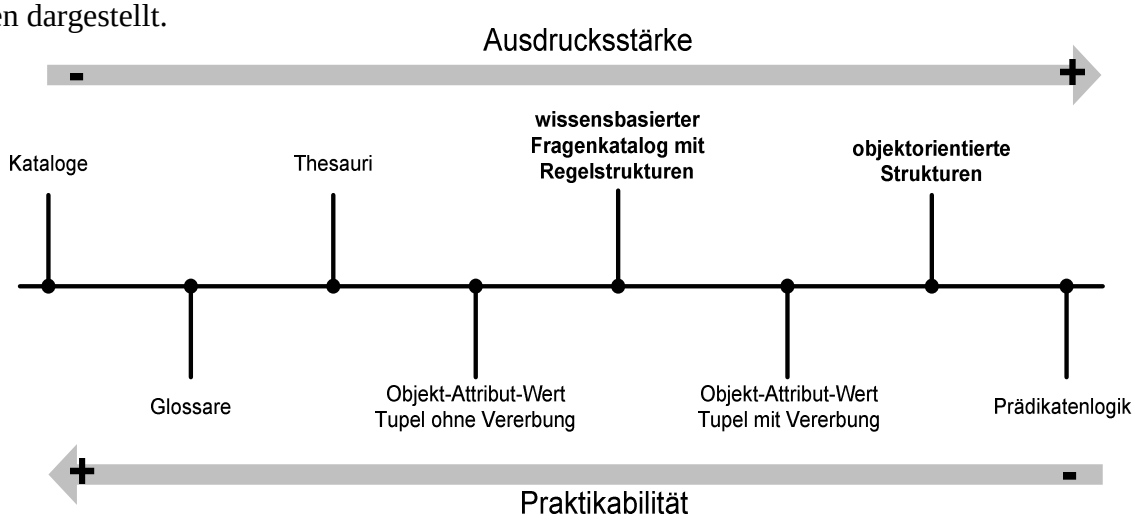


Abbildung 88: Praktikabilität und Ausdrucksstärke[465]

[465] Vgl. Erweitert in Anlehnung an Volz (2001), Folie 4

Bei der Überführung in ein unternehmensspezifisches IS-Sicherheitsmodell werden folgende unterschiedliche Vorgehensweisen bzw. folgende Umsetzungen angewandt:

- Anpassungsorientiert: Klassenhierarchien und deren Instanzen bzw. Objekte bilden durch ihre Objekt-Attribut-Wert Struktur weitgehend unternehmensunabhängige sicherheitsrelevante Aspekte ab. Die Anpassungsorientierung ist möglich, da durch Klassen und Objekte formale Modelle repräsentiert werden können, welche eine hohe Ausdrucksstärke besitzen[466]. Die angepassten Klassen (z.B. durch Vererbung) und deren Instanzen repräsentieren das unternehmensspezifische Wissen.
- Anwendungsorientiert: Wissensbasierte Fragenkataloge enthalten eine hohe Praktikabilität, da eine direkte Anwendung und Wissenseingabe möglich ist. Diese Form der Wissensrepräsentation besitzt hingegen nicht die Möglichkeiten einer Spezialisierung oder Vererbung, die in der objektorientierten Formalisierung verwendet werden. Fragen wenden ihre Objekt-Attribut-Wert Struktur direkt an, um sicherheitsrelevante Aspekte des Informationssystems zu erheben. Fragen besitzen Antwortmöglichkeiten, die eine bestimmte Antwort bzw. einen bestimmten Wert annehmen können. Die beantworteten Fragen entsprechen dem unternehmensspezifischen Wissen, die durch Antworttexte ausgedrückt werden. Die Antworttexte ermöglichen eine Textgenerierung, wobei die Dokumente zusätzlich weitere dynamische Objekte, wie Grafiken oder XML basierte Dokumente, besitzen können.

4.1.1 Anpassungsorientierte Überführung

Das Referenzmodell ist ein abstrahierter IS-Sicherheitsspezifischer „Modelltyp“ bzw. Bezugspunkt, aus dem durch Konkretisierung „konkrete“ angepasste unternehmensspezifische Systemmodelle erstellt werden[467]. Diese Vorgehensweise wird bei dem Bottom-Up Ansatz angewandt, indem ein Referenzmodell im Kontext der IS-Sicherheit als Modellierungsgrundlage für die unternehmensspezifische Risikoanalyse verwendet wird.

Im Rahmen der Risikoanalyse werden häufig objektorientierte Wissensrepräsentationen verwendet, wie z.B. beim Konzept zur Risikoanalyse von Stelzer[468], beim Simulationsmodell der Risikoanalyse von Konrad[469] oder bei der workflowbasierten Risikoanalyse von Thoben[470]. Objektorientierte Wissensrepräsentationen folgen Paradigmen, die mit der objektorientierten Programmierung verwandt sind und auf dem Prinzip des abstrakten Datentyps basieren. Die grundlegenden Elemente der objektorientierten Wissensrepräsentation sind Klassen und deren Instanzen, die als Objekte bezeichnet werden. Eine Klasse ist ein abstrakter Datentyp oder eine Art „Schablone“ für ein Objekt, die die Eigenschaften und Verhaltensweisen der künftigen Objekte in Form von Attributen und Methoden bereitstellt. Durch den Vorgang der Instanziierung werden aus den Klassen Objekte (Instanzen) gebildet. Die Objekte können ihre Eigenschaften kapseln und kommunizieren mit ihrer „Außenwelt“ und untereinander mit Hil-

[466] Vgl. Volz (2001)
[467] Vgl. Zelewski/Schütte/Siedentopf (2001), S. 194
[468] Vgl. Stelzer (1993)
[469] Vgl. Konrad (1998)
[470] Vgl. Thoben (2000)

fe von Nachrichten. Über Schnittstellen können interne Methoden des Objekts aktiviert werden, die eine bestimmte Reaktion bewirken. Die Klassen werden in hierarchischen Vererbungsstrukturen bzw. semantischen Netzen dargestellt, wobei die Oberklasse der Unterklasse ihre Eigenschaften und Verhaltensweisen vererbt[471].

Klassen und Objekte können durch die Unified Modeling Language (UML-Notation) grafisch beschrieben werden. In der folgenden Tabelle ist die UML-Notation im Vergleich mit dem datenorientierten Entity-Relationship-Model (ERM-Notation) dargestellt. Beide Methoden haben sich als Standardnotation durchgesetzt; es existiert eine Vielzahl von computergestützten grafischen Werkzeugen für deren Darstellung.

UML	ERM	UML	ERM
Objekt ein Objekt	**Entität** *(entity)*	Assoziation Klasse 1 — Klasse 2	**Beziehung , Assoziation** *(relationship type)* Typ — Typ
Klasse Klasse / Attribut / Operation()	**Entitätstyp** *(entity type)* Entitätstyp	Kardinalität 0..1 / * / 1 / 1..*	Kardinalität, Komplexität, Stetigkeit 1 — M / 1 — M
Attribut	**Attribut** Entitätstyp — Attribut Attribut		
Attributtyp	Wertebereich, Domäne, Wertetypen *(domain, value-set)* Attribut	Aggregation Aggregat / Teil	**Aggregation** *ist-Teil-von-Beziehung* part of
—	Schlüsselattribut		
Verbindung *(link)* zwischen Objekten :Klasse 1 — :Klasse 2	**Beziehung** *(relationship)*	Vererbung	**Vererbung** *ist-ein-Beziehung* is-a

Tabelle 17: Vergleich der UML- und ERM-Notation[472]

Die Anpassung bzw. Konkretisierung kann durch eine Spezialisierung der Referenzklassen auf die unternehmensspezifischen IS-Sicherheitsaspekte erfolgen. Die Klassen dienen als „Schablone“ für konkrete Objekte (Instanzen). Ein Objekt ist z.B. eine konkrete Gefahr, Konsequenz oder ein sicherheitsrelevantes Element des spezifischen Unternehmens. Das Ergebnis ist ein Systemmodell der sicherheitsrelevanten Aspekte des unternehmensspezifischen Informationssystems.

4.1.2 Anwendungsorientierte Überführung

Anhand der folgenden Abbildung werden die grundsätzlichen Probleme einer Überführung des Referenzmodells in ein unternehmensspezifisches Informationsmodell bzw. Systemmodell dargestellt.

[471] Semantische Netze stammen ursprünglich aus dem Bereich der KI und wurden dort zum Verständnis und zur Verarbeitung natürlicher Sprache eingesetzt. Vgl. Ralfs (1995), S. 34

[472] Verkürzt in Anlehnung an Balzert (2001), S. 225-226

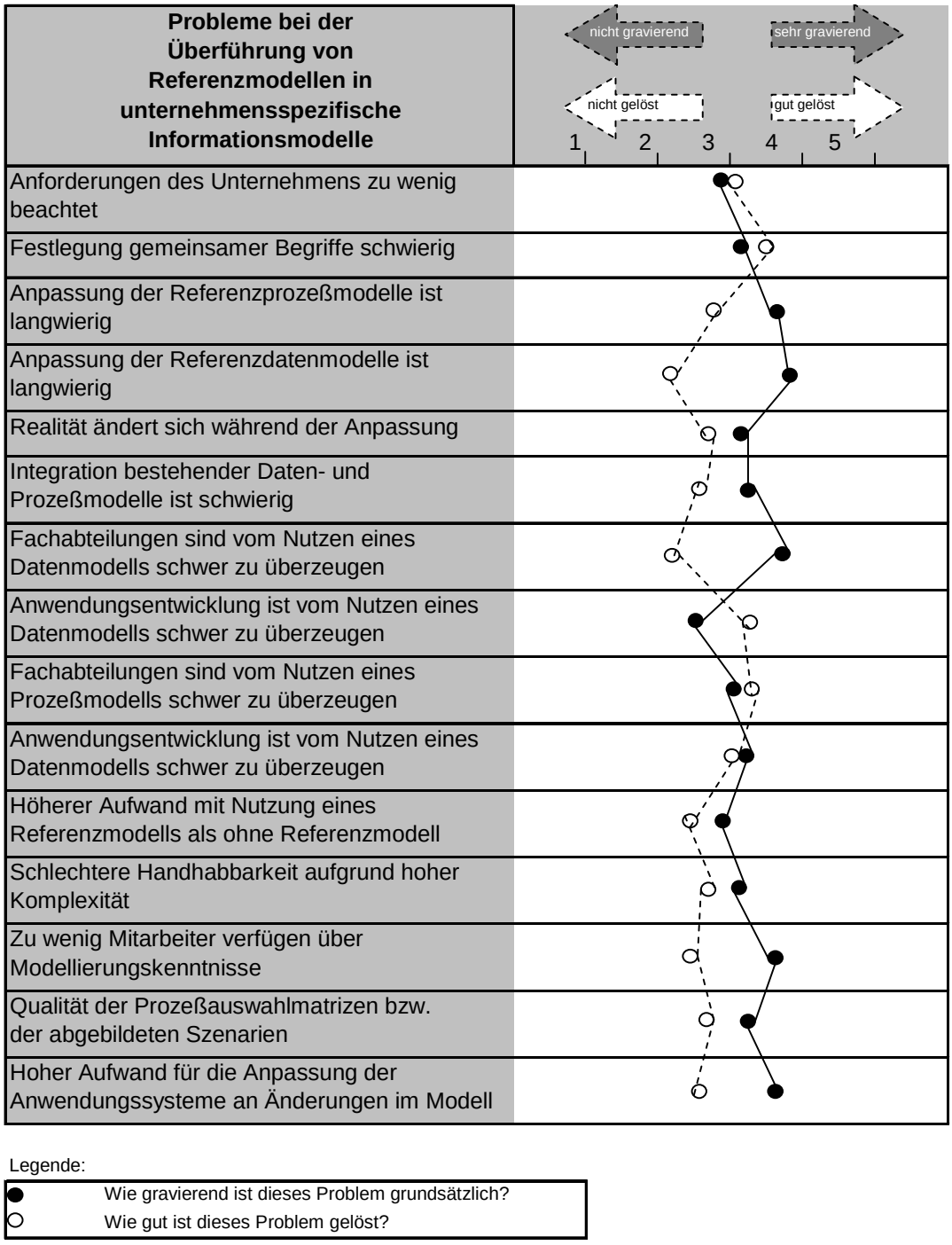


Abbildung 89: Probleme bei der Überführung von Referenzmodellen in unternehmensspezifische Informationsmodelle[473]

Insbesondere die langwierige Anpassung des Referenzmodells in unternehmensspezifische Systemmodelle stellt einen wesentlichen Aufwand bei der Erstellung und Wartung des IS-Sicherheitswissens dar. In Verbindung mit der Überführung tauchen zusätzliche Problembereiche auf, die z.T. aus der Risikoanalyse bekannt sind.

- Für die Spezialisierung müssen die sicherheitsrelevanten Aspekte, insbesondere die Elemente, identifiziert und „fassbar“ sein. Dies ist aber nur in beschränktem Maße bei bestimmten Bereichen - wie Teilbereiche der Infrastruktur - möglich.

[473] Vgl. Schütte (1998), S. 79

- Solange standardisierte Elemente, wie Standard-PC, Betriebssysteme oder Standardsoftware vorhanden sind, ist eine direkte Vererbung und Instanziierung möglich. Sollen „individualisierte Elemente“ beschrieben werden, werden spezialisierte oder gar neue Klassen benötigt, die über die Referenzklassen hinausgehen; dies kann eine umfangreiche Anpassung erfordern. Bei geringer Anpassung der Referenzklassen ist dies in einem gewissen Rahmen durch den Fachexperten möglich, bei umfangreicheren Anpassungen ist eine Unterstützung durch einen Knowledge Engineer erforderlich. Hiermit ist eine direkte Wartung des WBS durch einen IS-Sicherheitsexperten stark eingeschränkt.

Dies führt zu der Überlegung, dass Repräsentationsformen angewandt werden, die

- eine direkte Wissenseingabe des IS-Sicherheitswissens durch den Fachexperten und
- eine direkte Anwendung bzw. Nutzung des repräsentierten IS-Sicherheitswissens auf ein konkretes IS-Sicherheitsproblem

ermöglichen.

Diese anwendungsorientierte Sicht verlangt eine direkt anwendbare Wissensrepräsentationssprache, die sich ohne wesentlichen Anpassungsaufwand auf die sicherheitsrelevanten Aspekte des Informationssystems überführen lässt, was insbesondere ökonomische Vorteile in sich birgt. Der Nachteil der direkten Wissenseingabe und Anwendung besteht im Verlust der syntaktischen und semantischen Präzisierung der Repräsentationssprache gegenüber einer formalen Sprache.

Des Weiteren ist diese praktikabilitätsorientierte Umsetzung eine wesentliche Voraussetzung für den Top-Down Ansatz des IS-Sicherheitsmanagements. Bei diesem Ansatz werden unternehmens-unabhängige Kriterienwerke direkt auf das unternehmensspezifische Informationssystem angewendet. Eine Anpassung erfolgt durch Auswahl der benötigten sicherheitsrelevanten Bereiche. Diese Anpassung ist aber nicht so umfangreich wie bei einem unternehmensspezifischen Systemmodell. Die direkte Wissenseingabe und direkte Nutzung bzw. Anwendung der Wissensrepräsentation wird im Weiteren durch wissensbasierte Fragenkataloge erreicht.

4.2 Wissensbasierte Fragenkataloge

Grundsätzlich gilt zugespitzt für einen Fragenkatalog[474]: „*… nicht der Interviewer, der Fragebogen muß schlau sein.*“[475] Insbesondere für die Erfassung von Beobachtungen und für eine strukturierte Ergebnisausgabe in Form eines Statusberichtes sind computergestützte Fragebögen geeignet. Die wissensbasierten Fragenkataloge der Arbeit stellen eine wissensbasierte Erweiterung von computergestützten Fragenkatalogen dar, denn bei konventionellen Fragenkatalogen bzw. Checklisten ist das Lösungswissen noch implizit in Fragen und Antworten enthalten. Der Ergebnis-Statusbericht eines computergestützten Fragenkatalogs stellt zwar eine gute Arbeitsgrundlage dar, aber die eigentliche Problemlösung erfolgt immer noch durch den Fachexperten.

[474] Die Begriffe „Fragenkatalog“ und „Fragebogen“ werden synonym verwendet.
[475] Schmidtchen (1962), S. 9 zit. nach Hoepner (1994), S. 6

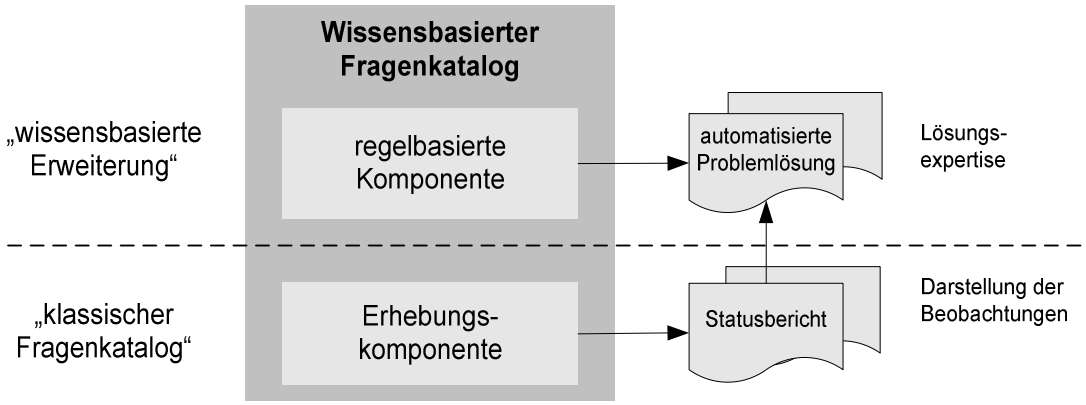


Abbildung 90: Grundstruktur eines wissensbasierten Fragenkatalogs

Die wissensbasierte Regelerweiterung der Fragenkataloge ermöglicht zusätzlich die Repräsentation von Abhängigkeitskonzepten basierend auf unterschiedlichen Fragenkatalog-Regeln, wodurch die Problemlösungen explizit beschrieben und angewendet werden können. Hierdurch kann das WBS „selbstständig“ auf Basis der Erhebung eine spezifische Problemlösung durchführen und ein IS-Sicherheitskonzept erstellen, wobei die Ergebnisse des Statusberichtes in die Lösungsexpertise einfließen. Hierbei ist aber zu beachten, dass diese Lösungsexpertise zwar eine deutlich höhere „Lösungsqualität“ als ein konventioneller Statusbericht hat, aber trotzdem durch einen Fachexperten überarbeitet werden muss. Eine vollständige Ersetzung des Fachexperten durch ein WBS ist (noch) nicht möglich.

In der folgenden Abbildung ist das Grundprinzip eines wissensbasierten Fragenkatalogs mit Hilfe der UML-Notation dargestellt.

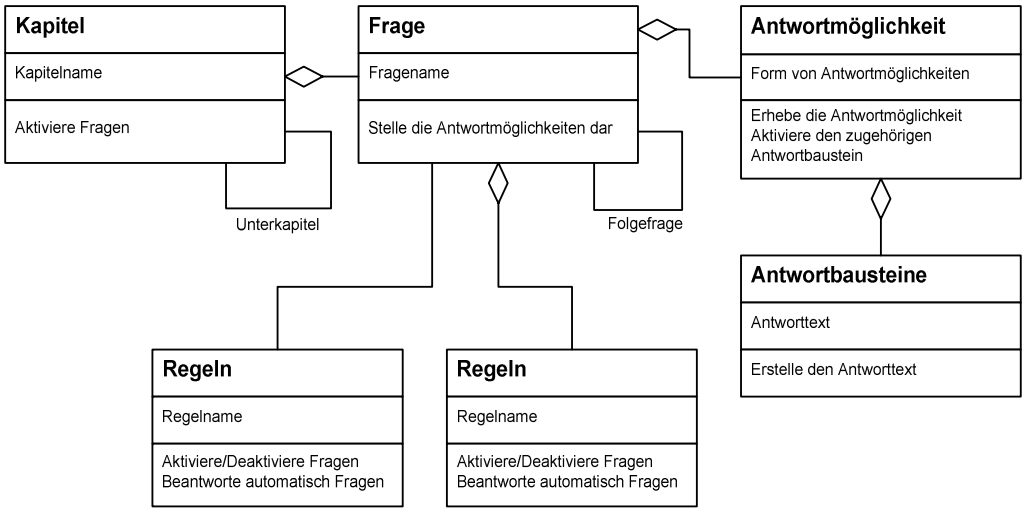


Abbildung 91: Wissensbasierter Fragenkatalog in UML-Notation

Kapitel sind in Oberkapitel und Unterkapitel strukturiert und enthalten Fragen. Die Kapiteleigenschaften werden durch Attribute (z.B. durch einen eindeutigen Kapitelnamen) beschrieben. Die Frage besitzt einen eindeutigen Namen, einen Fragetext und zugeordnete Antwortmöglichkeiten, wodurch die Antworten erhoben werden. Die Antwortmöglichkeiten enthalten Antwortbausteine, welche Antworttexte erzeugen können. Regeln dienen der automatisierten Steuerung der Befragung und der Problemlösungsunterstützung. Regeln sind entweder Teil

einer Frage (aggregiert) - sie sind direkt mit einer Frage verbunden - oder Regeln werden unabhängig von Fragen repräsentiert. Diese unabhängigen Regeln können komplexere Abhängigkeiten zwischen Fragen beschreiben als die aggregierten Regeln.

Das Vererbungs- Instanziierungsprinzip wird durch Fragenkataloge nicht unterstützt. Es können zwar Fragen auf Basis einer Schablone erstellt werden, welche aber nur eine „Kopiervorlage“ für die Frage- und Antwortstruktur darstellt. Eine Vererbung von Eigenschaften und Methoden, wie bei der objektorientierten Repräsentation, ist bei Fragenkatalogen nicht möglich. Hierdurch sind die Beschreibungsmöglichkeiten von computergestützten Fragenkatalogen nicht so umfangreich wie bei der objektorientierten Repräsentation. Dafür ist eine anwendungsorientierte Umsetzung, Wartung und Pflege zu realisieren, so dass ein Fachexperte direkte und eigenständige Veränderungen in der Wissensbasis vornehmen kann. Eine Beschreibung der Abhängigkeitskonzepte erfolgt durch natürlich-sprachliche Regeln.

In der Arbeit sollen auch Aspekte des Bottom-Up Ansatzes auf Kapitel- und Fragestrukturen überführt werden. Aufgrund der eingeschränkten syntaktischen und semantischen Möglichkeiten gegenüber objektorientierten Formalismen erfolgt lediglich eine Überführung der kausalen Abhängigkeiten zwischen den Konzepten. Andere Abhängigkeiten, insbesondere Beziehungen zwischen den sicherheitsrelevanten Elementen, werden nicht berücksichtigt.

Ein wissensbasierter Fragenkatalog lässt sich grob in zwei Bereiche einteilen:

- Kapitel-, Fragen- und Antwortstrukturen,
  die sich zur Erhebung von Beobachtungen und zur Strukturierung der Basiskonzepte eignen und
- Fragenkatalogregeln,
  die sich zur Steuerung der Befragung und zur Beschreibung der Abhängigkeitskonzepte eignen.

4.2.1 Kapitel- und Fragestruktur

Die Kapitel dienen der Strukturierung des Problemgebiets und repräsentieren sicherheitsrelevante Bereiche, die durch Unterkapitel verfeinert werden. Durch die Kapitel- und Fragestruktur ist zudem der Befragungspfad vorgegeben, da vom Oberkapitel aus die Fragen der Unterkapitel gemäß der Kapitelstruktur nacheinander abgearbeitet werden. Bei Fragenkatalogen ist grundsätzlich zwischen den

- unternehmensunabhängigen Fragen (Merkmalsindikatoren) und
- deren unternehmensspezifischen Antworten (erhobene Merkmale) zu unterscheiden.

Das unternehmensunabhängige IS-Sicherheitswissen ist in den Inhalten, der Struktur und den Abhängigkeiten zwischen den Fragen repräsentiert, wohingegen die beantworteten Fragen bzw. das Ergebnis der Befragung das unternehmensabhängige bzw. -spezifische IS-Sicherheitswissen darstellen. Eine Anpassung des Fragenkatalogs an die Unternehmensstruktur ist ein Zwischenschritt zur Anwendung des Fragenkatalogs. Dieser Zusammenhang ist in der folgenden Abbildung dargestellt.

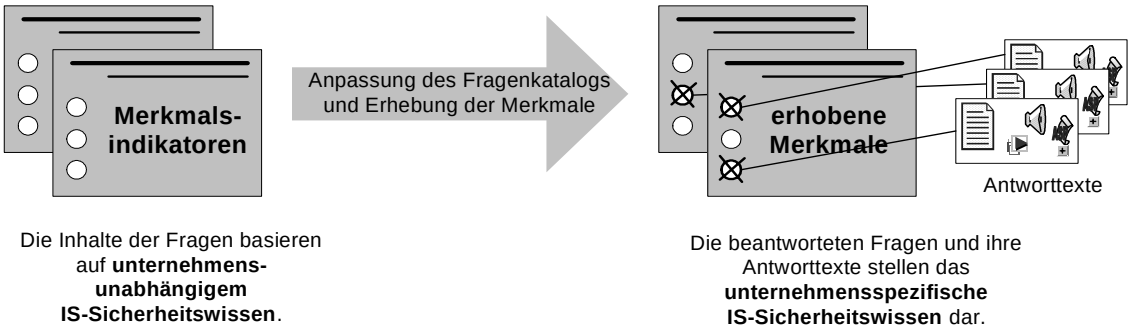


Abbildung 92: Repräsentation von IS-Sicherheitswissen in Fragenkatalogen

Typen von Antwortmöglichkeiten

Fragen abstrahieren Merkmale und sind gleichzeitig Merkmalsindikatoren, die konkrete Merkmalswerte ermitteln. Die Antwortmöglichkeiten sind von den Antworttypen abhängig. Diese Typen werden in folgende Kategorien eingeteilt[476], wobei sie auch miteinander kombiniert und weiter spezialisiert werden können:

- Identifikationstyp
  Fragen nach „wer“, „wo“, „wann“, „wie viele“ oder „welche“. Diese Frage kann als offene Frage (beliebiger Text kann eingegeben werden; z.B. bestimmte Angaben: der Name einer Person) oder geschlossene Frage dargestellt werden (die Frage bietet eine endliche Zahl an Alternativen an, z.B. Betriebssysteme).
- Selektionstyp/Alternativfrage
  Eine Frage dieses Typs stellt dem Befragten mehrere Antwortmöglichkeiten zur Verfügung, aus denen dieser eine oder mehrere Alternativen auswählen bzw. selektieren kann. Bei der Auswahl von alternativen Antwortmöglichkeiten können mehrere Alternativen markiert werden, wohingegen bei selektiven Antwortmöglichkeiten nur eine Alternative ausgewählt werden kann.
- Ja/Nein-Typ
  Eine Ja/Nein-Frage ist ein häufig verwendeter Spezialtyp von Selektionsfragen und besitzt als Antwort einen binären Wert.

[476] Vgl. Atteslander (1995), S. 180 ff.

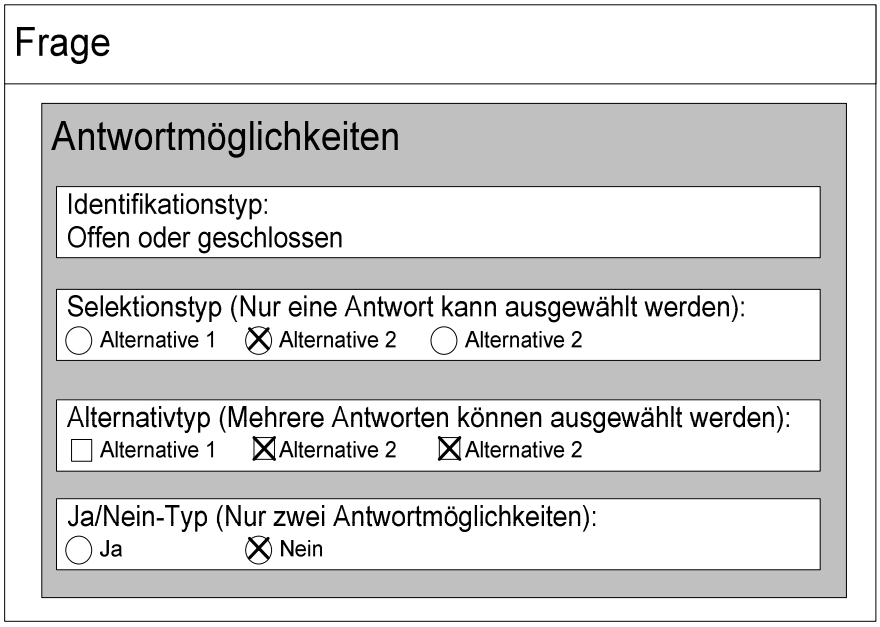


Abbildung 93: Antworttypen einer Frage

Zustandsformen von Fragen

Eine Frage besitzt vor der Befragung einen Zustand, der sich während der Frage dynamisch verändern kann. Diese Zustandsveränderung der Fragen erfolgt entweder offen für den Benutzer oder ist verdeckt durch das System. Offene Fragen können durch den Benutzer beantwortet werden oder dem Benutzer werden schon während der Erhebung z.B. automatisch beantwortete Fragen präsentiert. Verdeckte Fragen bleiben dem Benutzer während der Erhebung verborgen und werden durch das System automatisch bzw. autonom beantwortet.

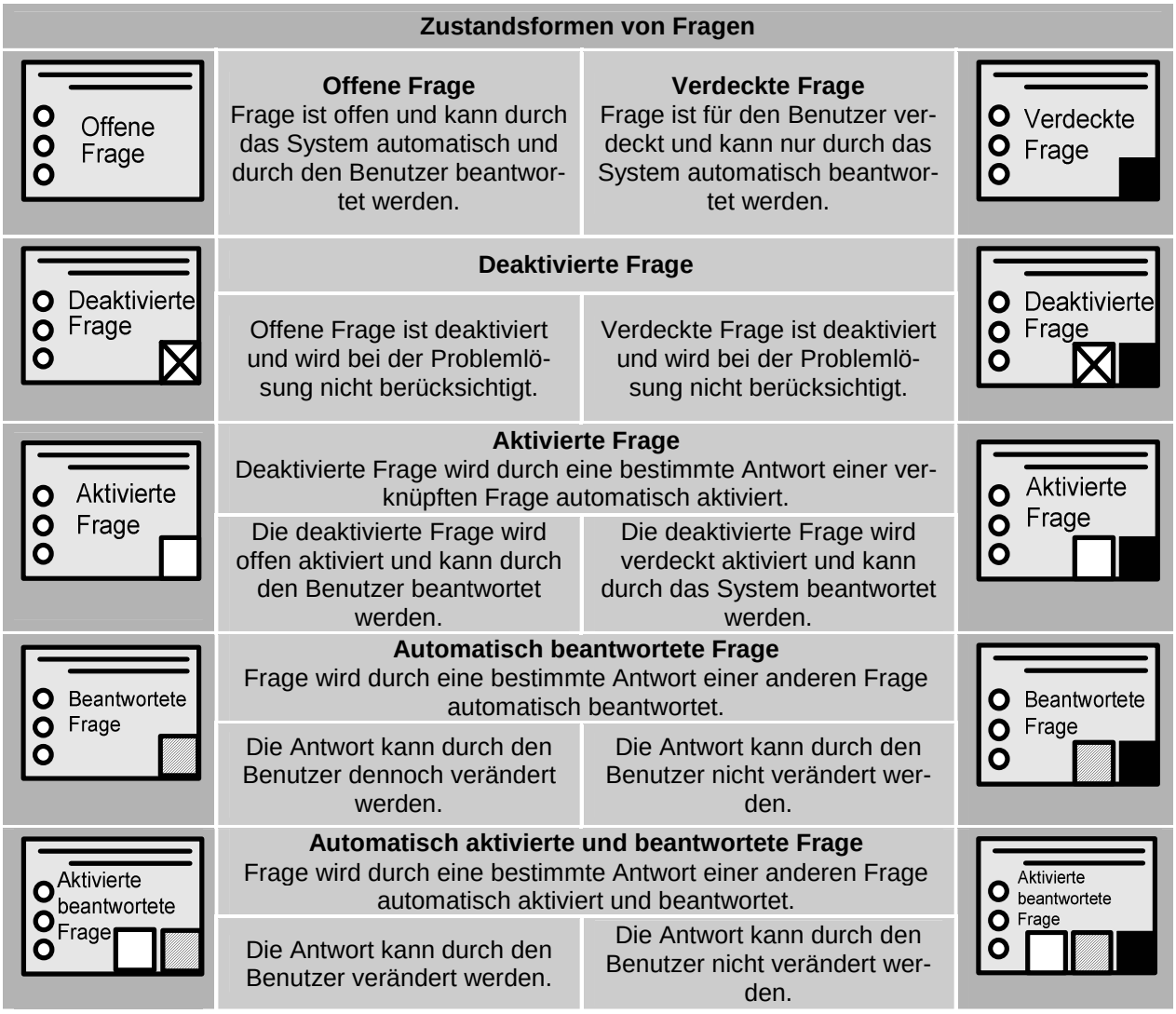


Abbildung 94: Zustandsformen von Fragen

4.2.2 Qualitative und quantitative Auswertung von Fragenkatalogen

Die direkte Auswertung ist eine wesentliche Funktion eines computergestützten Fragenkatalogs, in der automatisch ein Statusbericht der Erhebung erstellt wird. Hierbei lässt sich die qualitative Auswertung von der ergänzenden quantitativen Auswertung unterscheiden.

4.2.2.1 Qualitative Auswertung von Fragenkatalogen

Die Antwortbausteine dienen zur Darstellung von Antwortmerkmalen, wie z.B. die Darstellung von fehlenden Maßnahmen oder Konsequenzen. Hierfür ist jede Antwortmöglichkeit mit einem Antwortbaustein verbunden. So sind bei einer binären Antwortmöglichkeit zwei Antwortbausteine verknüpft. Ist die Antwortmöglichkeit A bzw. B (Antwort) angeklickt, wird „Antwortbausteine_angeklickt“ aktiviert. Ist die Antwortmöglichkeit nicht angeklickt, wird „Antwortbausteine_nicht_angeklickt“ aktiviert. Alle Antwortbausteine einer Frage werden zu einer Antwortgruppe zusammengefasst.

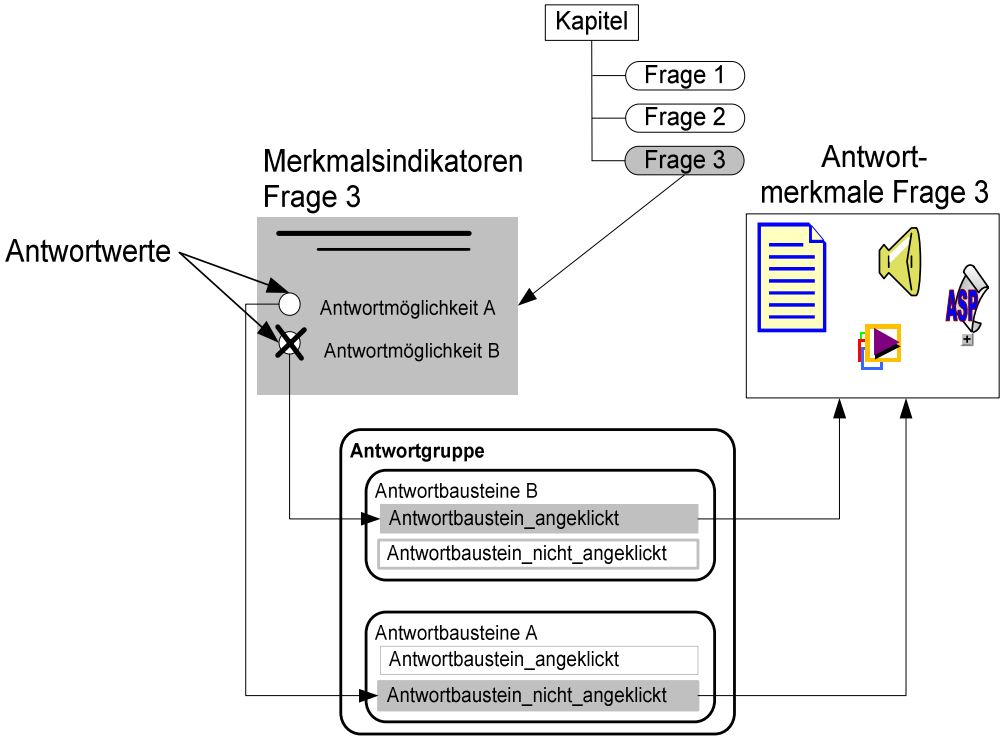


Abbildung 95: Verknüpfung zwischen Merkmalsindikator und Antwortmerkmal

Antwortbausteine sind häufig Textbausteine, die zu einem Statusbericht der Erhebung zusammengefasst werden können. Antwortbausteine können zudem aktive Objekte darstellen, wie z.B. Grafiken, Videoclips oder kleine Programme. Das Antwortmerkmal einer Frage setzt sich aus mehreren Antwortbausteinen zusammen, die zu einem aktiven Dokument zusammengefasst werden.

4.2.2.2 Quantitative Auswertung von Fragenkatalogen

Die oben erläuterte Antwortstruktur ermöglicht eine qualitative Auswertung. Es folgt eine quantitative Ergänzung, wobei die quantitativen Auswertungen die qualitative Auswertung nicht ersetzen, sondern „ergänzen“ sollen. Die Grundstruktur der Erweiterung ist in der folgenden Abbildung dargestellt.

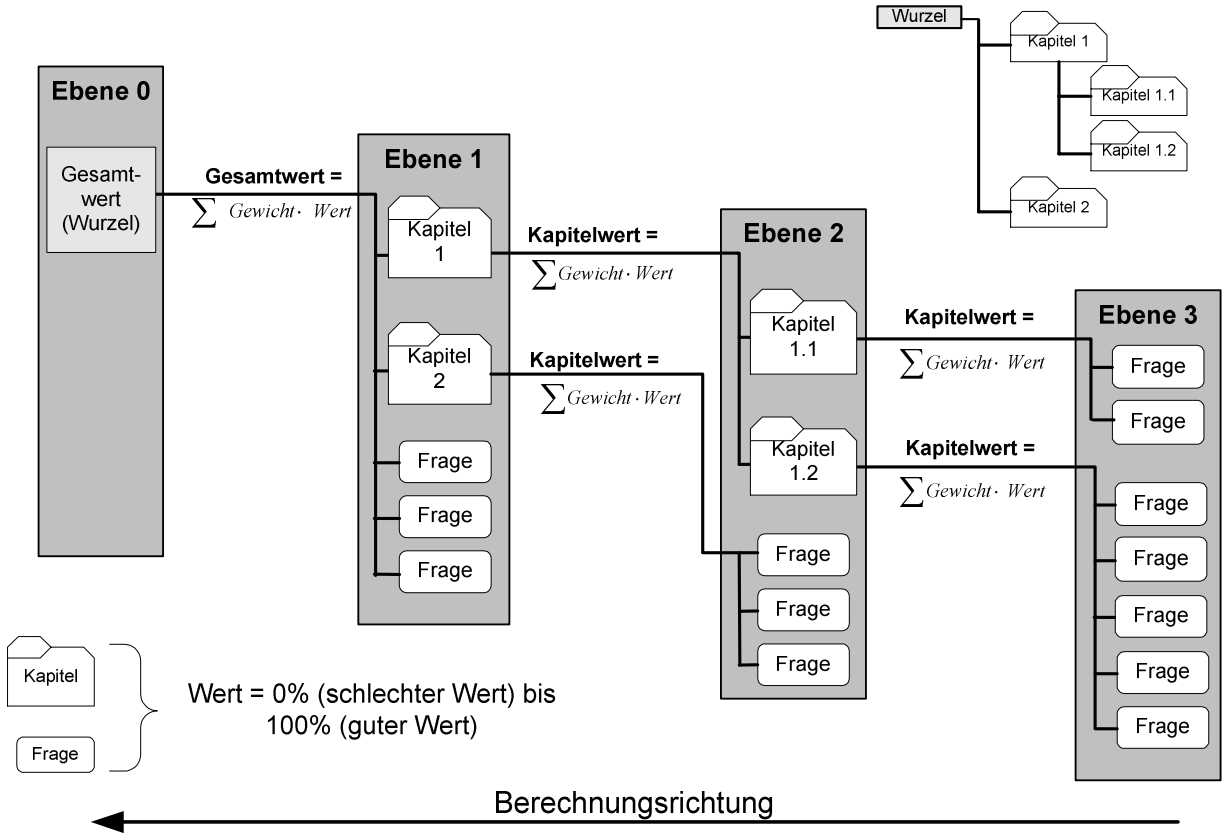


Abbildung 96: Rekursive Berechnung von Kapitel- und Fragenwerten

Jede quantifizierbare Antwortmöglichkeit kann einen Wert annehmen. Die Antwortwerte jeder Frage werden addiert und wie folgt zusätzlich zu einem Fragenwert von 0% bis 100% gewichtet.

Gewichtungsalternativen von Fragenwerten	
$\frac{\text{aktueller Antwortwert}}{\text{maximaler Antwortwert}} = Fragenwert$	$\frac{\sum_{1}^{\text{Anzahl der beantworteten Antwortmöglichkeiten}} \text{Werte beantworteter Kontrollelemente}}{\sum_{1}^{\text{Alle Antwortmöglichkeiten}} \text{Werte der Kontrollelemente}} = Fragenwert$
Bei selektiven Antwortmöglichkeiten kann nur eine Alternative ausgewählt werden.	Bei alternativen Antwortmöglichkeiten können mehrere Alternativen ausgewählt werden.

Tabelle 18: Gewichtungsberechnung von Fragenwerten

Die Fragenwerte einer Ebene können gewichtet zu einem Kapitelwert zusammengefasst werden. Die Kapitelwerte der unteren Ebenen werden rekursiv zu einem Kapitelwert (Wurzelwert) vereint, wobei auch die Kapitelwerte jeweils gewichtet werden. Da die Fragen- und Kapitelwerte zwischen 0% und 100% gewichtet sind, können Grenzen eingeführt werden, um Aussagen über die Werte zu tätigen. Im Folgenden werden zwei Grenzen eingefügt, um in Anlehnung von Ampelfarben die Werte zu beurteilen.

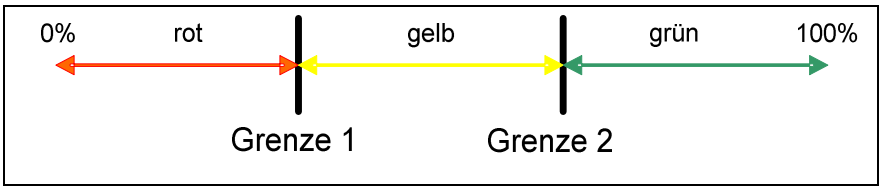


Abbildung 97: Fragen- und Kapitelgrenzen

So besitzen Fragen- und Kapitelwerte, die sich im roten Bereich befinden, eine besondere Aufmerksamkeit, da hier z.B. eine Maßnahme fehlt. Gelb könnte bedeuten, dass zwar Maßnahmen existieren, diese aber eventuell durch weitere Maßnahmen zu ergänzen sind. Fragen und Kapitel im grünen Bereich beinhalten die erforderlichen Maßnahmen.

4.2.3 Regelbasierte Erweiterung des Fragenkatalogs

Der Statusbericht stellt zwar eine wesentliche Grundlage für den IS-Sicherheitsexperten dar, wird aber durch regelbasierte Problemlösungskomponenten erweitert. Regeln werden in vielen Formen als Repräsentationsform verwendet, weil sie eine vertraute Wissensdarstellung repräsentieren. Die Aufteilung des Wissens in viele kleine eigenständige „Wissensstücke“ macht die Wissensbasis modular, aber auch unübersichtlich. Die Regeln haben folgende Grundstruktur:

WENN Vorbedingungen DANN Nachbedingungen

Gleichung 1: Prinzip einer Regel

Die Ausprägung der Vorbedingungen und Nachbedingungen ist abhängig, ob assoziative und kausale Regeln in einer Wissensbasis gespeichert sind. Zudem haben die unterschiedlichen Problemlösungsmethoden Auswirkung auf die unterschiedliche Aktivierung der Vor- oder Nachbedingungen einer Regel.

Die Wissensbasis besteht aus Fragenkatalogen und zugehörigen Regeln, die eine Umsetzung der Basis- und Problemlösungskonzepte darstellen. Die Basiskonzepte werden möglichst unabhängig von den Problemlösungskonzepten und somit von dem späteren Problemlösungsprozess formalisiert. Die „Füllung“ der assoziativen Wissensbasis erfolgt durch standardisierte Maßnahmen-Kriterien, wohingegen die kausale Wissensbasis auf möglichst individualisierten Ursachen-Wirkungs-Zusammenhängen beruht.

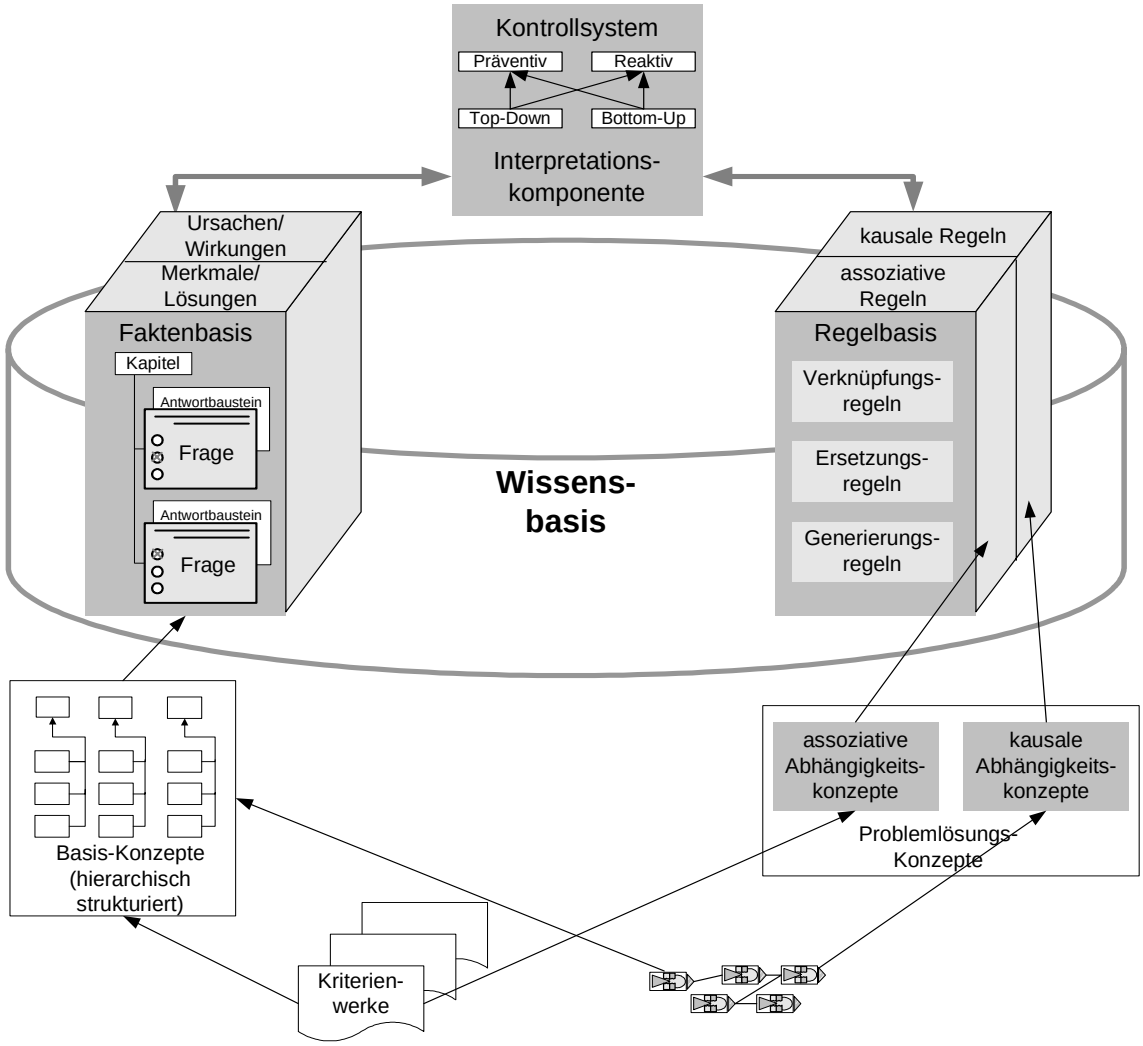


Abbildung 98: Komponenten eines Produktionssystems

Die Wissensbasis des Fragenkatalogs besteht im Kern aus folgenden Bestandteilen:

- Die Faktenbasis besitzt
  - statische Fakten in Form von Fragen sowie Antwortstrukturen als Platzhalter für
  - dynamische Fakten in Form von Antworten.
- Die Regelbasis speichert folgende Fragenkatalog-Regeln:
  - Verknüpfungsregeln dienen der automatischen Steuerung der Befragung und der automatischen Zustandsveränderung von Fragen.
  - Ersetzungsregeln dienen der automatischen Beantwortung von Fragen.
  - Generierungsregeln dienen einer komplexen Problemlösung.
- Das Kontrollsystem entscheidet, welche IS-Sicherheitsstrategie angewandt wird.
- Die Interpretationskomponente, welche die unterschiedlichen Regelformen auswertet. Die Interpretationskomponente hat den Charakter eines Regelinterpreters.

In der folgenden Abbildung ist eine Zusammenstellung der Ausprägungsformen von Fragenkatalog-Regeln dargestellt.

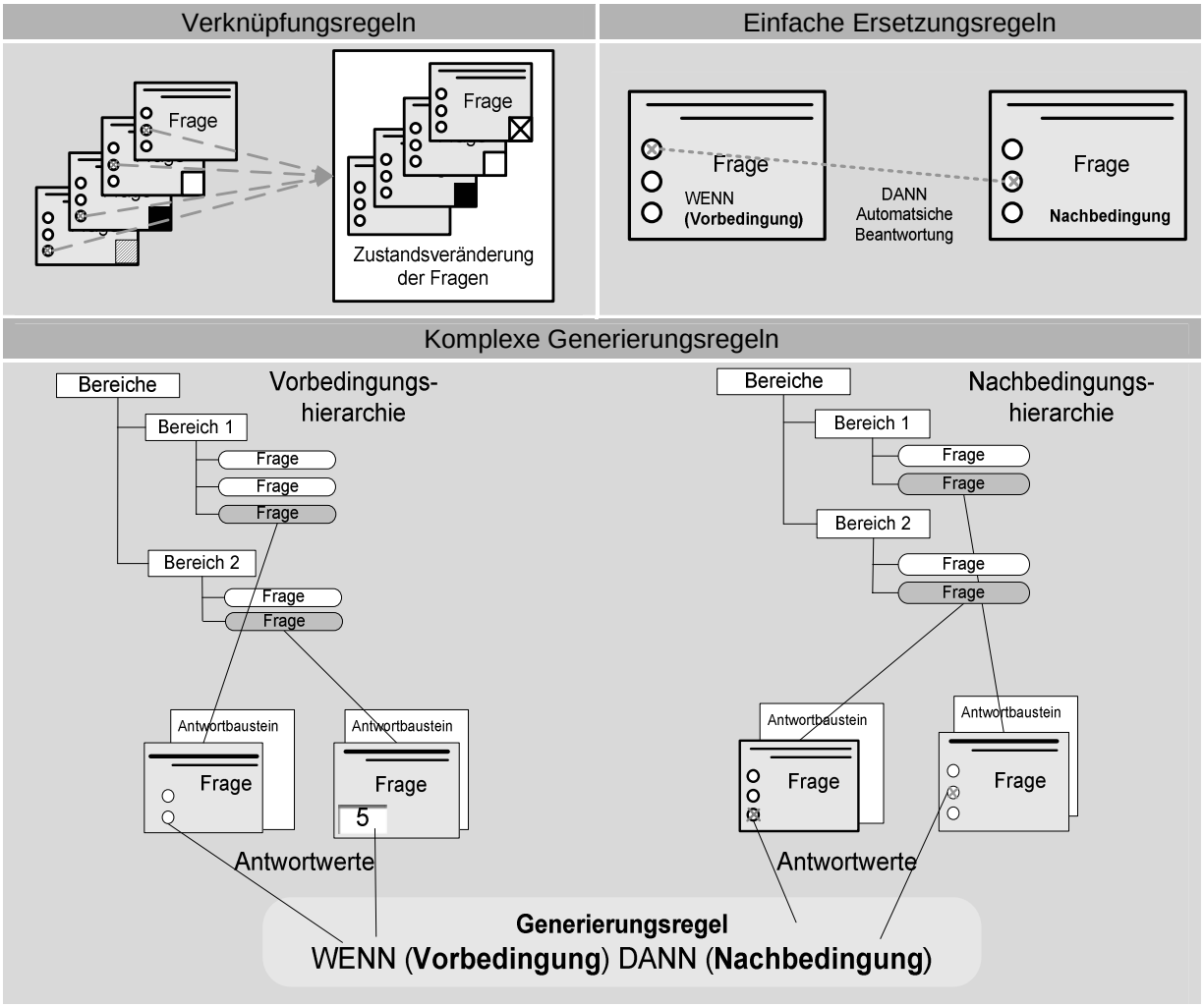


Abbildung 99: Überblick der Ausprägungsformen von Produktionsregeln für wissensbasierte Fragenkataloge

4.2.3.1 Verknüpfungsregeln

Die Verknüpfungsregeln haben die Aufgabe, den Zustand der verknüpften Fragen durch das System automatisch zu verändern. So kann auf Grund einer bestimmten Beantwortung z.B. eine Frage aktiviert oder deaktiviert werden. Die aktive Veränderung der Abfragerichtung erfolgt auf Grund eines bestimmten Antwortwertes, welcher veranlasst, dass Fragen übersprungen werden. Die Verknüpfungsregeln können insbesondere für die gezielte Erhebung und Hypothesenüberprüfung zusätzlich benötigte Fragen aktivieren und nicht benötigte Fragen deaktivieren.

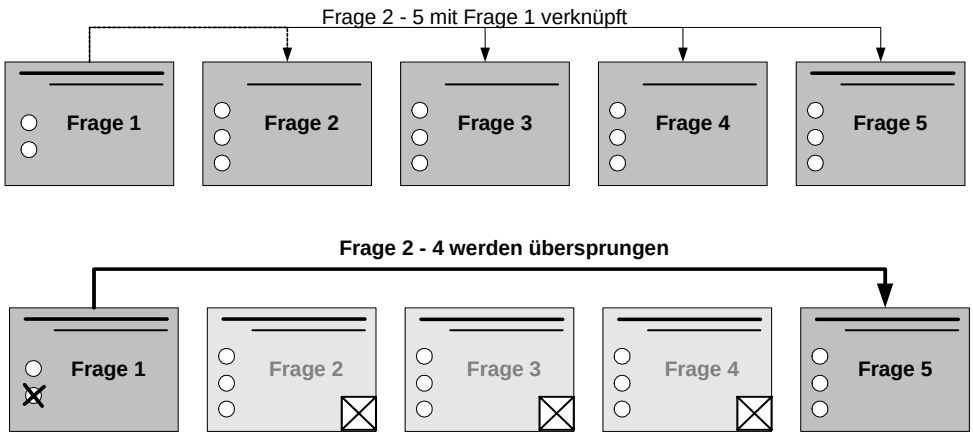


Abbildung 100: Automatische Ablaufsteuerung

Die Ursprungsfrage (Frage 1) ermittelt, ob z.B. ein sicherheitsrelevantes Element im Unternehmen überhaupt existiert oder welches IS-Sicherheitsniveau benötigt wird. Aufgrund der Beantwortung der Ursprungsfragen werden dann gezielt Fragen (Fragen 2-4) als nicht relevant markiert und übersprungen, da sie z.B. für eine Überprüfung nicht benötigt werden[477].

4.2.3.2 Ersetzungsregeln

Die Ersetzungsregeln dienen der automatischen Beantwortung von Fragen durch das System. Eine Ersetzungsregel verändert durch ihre automatische Beantwortung zusätzlich den Zustand einer Frage auf „Beantwortet“. Die automatisch beantwortete Frage kann für den Benutzer verdeckt beantwortet werden oder in Form einer offenen beantworteten Frage (Vorschlagsbeantwortung), wobei die Vorschlagsantworten durch den Benutzer revidiert werden können. So besitzen verdeckte Fragen den Charakter einer sicheren Lösung, dagegen stellen offene Fragen einen Vorschlag dar, der durch den Benutzer bestätigt oder widerlegt werden kann.

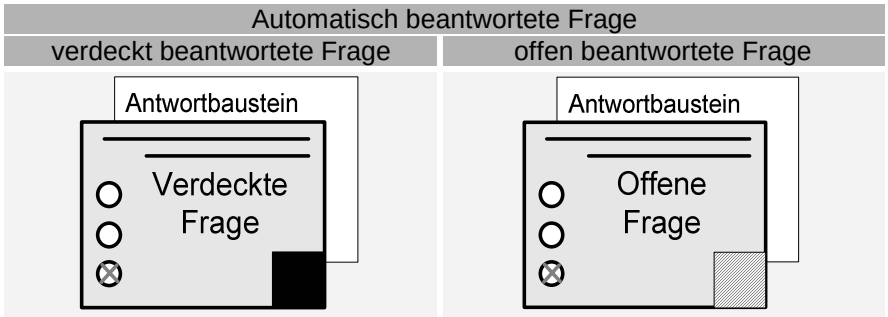


Abbildung 101: Formen automatisch beantworteter Fragen

[477] Eine weitere Möglichkeit der Erhebungssteuerung bietet das direkte Anspringen von Fragen aufgrund einer bestimmten Antwort der Ursprungsfrage. Auf Basis der Antwort von Frage 1 werden die Frage 5 und eventuelle weitere Fragen direkt angesprungen. Problem sind die zusätzlich erforderlichen Rücksprungbedingungen, welche durch weitere Regeln anzugeben sind.

4.2.3.3 Generierungsregeln

Die Generierungsregeln besitzen ähnliche Funktionen wie die Ersetzungsregeln, werden aber von den Fragen getrennt repräsentiert. Dies bedeutet, dass die Ersetzungsregeln in eine Frage „eingebettet“ und mit deren Antwortmöglichkeiten direkt verknüpft sind, wohingegen die Generierungsregeln getrennt von den Fragen repräsentiert werden. Fragen können wie Ersetzungsregeln durch Generierungsregeln automatisch offen oder verdeckt beantwortet werden,

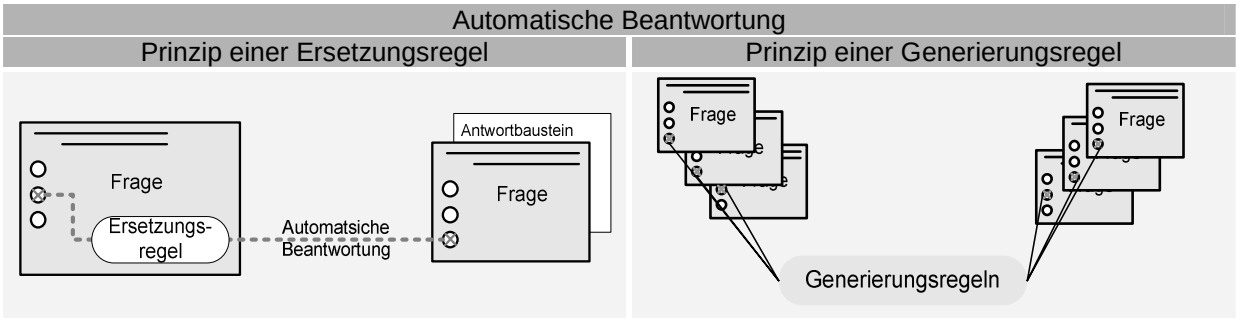


Abbildung 102: Prinzip der automatischen Beantwortung

Bei Generierungsregeln werden mehrere Antworten von Fragen zu einer Vorbedingung zusammengefasst. Mehrere automatische Beantwortungen bilden die Nachbedingungen. Um Generierungsregeln zu verknüpfen, können Ergebnisse von Generierungsregeln in die Vorbedingungen anderer Generierungsregeln als logische Aussage eingebunden werden. Die Aufgabe der Generierungsregeln besteht insbesondere darin, komplexe Zusammenhänge zu beschreiben.

Zusammenhang zwischen Komplexität und Anzahl der Regeln

Regeln sind modular aufgebaut und können unabhängig von anderen Regeln und der Faktenbasis hinzugefügt oder entfernt werden. Durch diese Modularität gewinnt der Kontrollfluss bei einer geringen Anzahl von Regeln sehr schnell eine hohe Komplexität. Schwächen liegen deshalb besonders in der Ineffizienz bei großen Wissensbasen, die zu komplexen und umfangreichen Regelstrukturen führen. Aus diesem Grund ist eine stufenweise Erstellung einer Regel-Wissensbasis möglich. Die Grundausrichtung besteht darin, viele einfache Verknüpfungsregeln und wenige komplexe Generierungsregeln anzugeben.

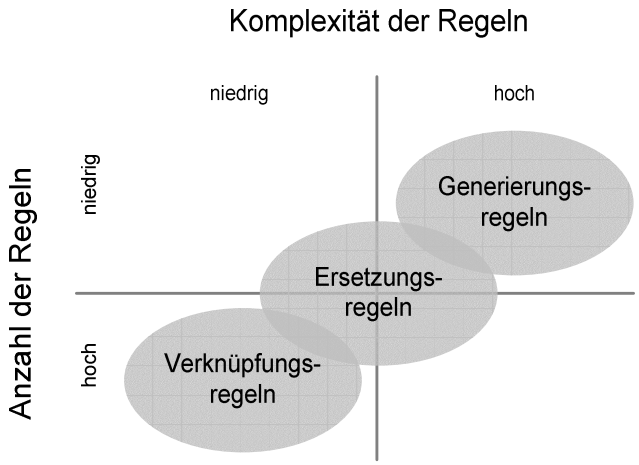


Abbildung 103: Zusammenhang zwischen Komplexität und Anzahl der Regeln

Auf der ersten Stufe werden nur Frage- und Antwortstrukturen repräsentiert, die zwar sehr schnell zu erstellen sind, jedoch für eine umfangreiche Problemlösung nicht ausreichen. Mit Verknüpfungsregeln sind eine automatische Erhebungssteuerung und eine einfache Problemlösung möglich. Durch den einfachen Aufbau von Verknüpfungsregeln kann eine hohe Anzahl dieses Regeltyps repräsentiert werden. Für eine umfangreiche Problemlösung sind Ersetzungs- und Generierungsregeln notwendig, wobei insbesondere bei Generierungsregeln deren Komplexität gegenüber Verknüpfungsregeln deutlich zunimmt. Ersetzungs- und Generierungsregeln sollten deshalb in einer geringeren Anzahl repräsentiert werden.

Erhebungs- und Auswertungssicht von Fragenkatalogen

In der folgenden Abbildung sind die Komponenten eines wissensbasierten Fragenkatalogs aus einer Erhebungs- und Auswertungssicht dargestellt. Ein fragenkatalogbasiertes WBS sollte eine getrennte Sichtweise auf die Erhebung und die Auswertung besitzen, denn Verknüpfungs-, Ersetzungs- und Generierungsregeln beeinflussen z.T. gemeinsam die Erhebungssteuerung und die Auswertung. Zwar sind somit die Bereiche Erhebung und Auswertung eng miteinander verbunden, aber für die Konstruktion eines fragenkatalogbasierten WBS und einer flexiblen Auswertung ist eine Trennung der beiden Sichtweisen hilfreich.

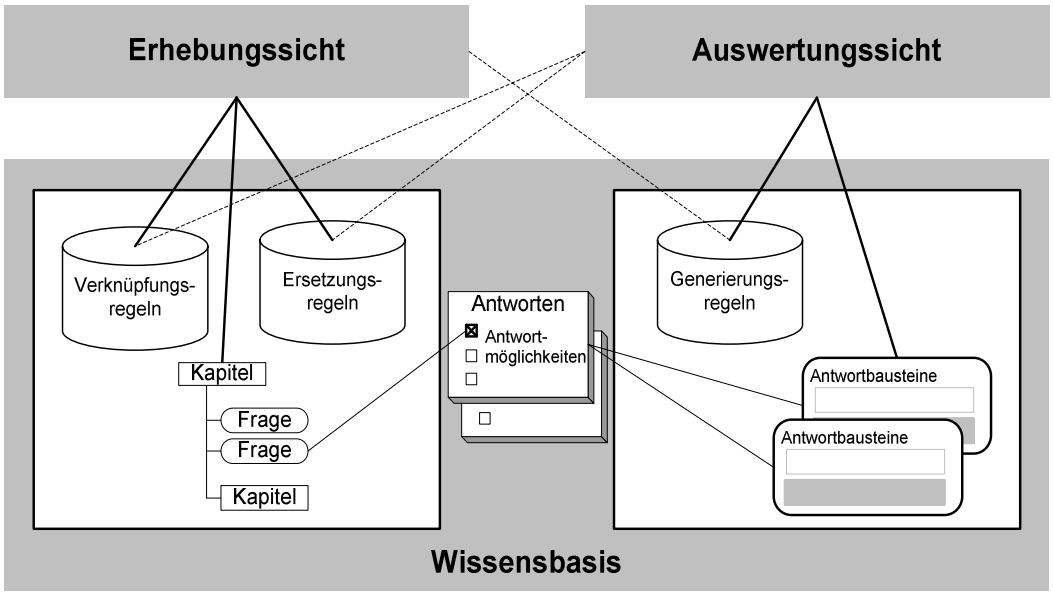


Abbildung 104: Erhebungs- und Auswertungssicht eines wissensbasierten Fragenkatalogs

Die Fragenkatalogstruktur beeinflusst primär die Erhebungssteuerung, wobei diese zusätzlich durch Verknüpfungs- und Ersetzungsregeln automatisiert werden kann. Durch die einfache Struktur von Verknüpfungsregeln und deren enger Kopplung mit dem Fragenkatalog sind diese zur Erhebungssteuerung besonders geeignet. Zusätzlich dienen Ersetzungsregeln der automatischen Beantwortung von Fragen während der Erhebung. Generierungsregeln können zwar die Erhebung beeinflussen, sollten aber durch ihre Struktur nur bei komplexen Steuerungsproblemen eingesetzt werden. Durch einen alleinigen Einsatz von Generierungsregeln bei der Erhebung würde schnell eine nicht mehr überschaubare „Steuerungskomplexität“ entstehen.

Grundsätzlich basiert die Auswertungssicht auf den Antworten und der Auswertung der Antwortbausteine. Die Auswertungssicht ist somit primär abhängig von der Struktur des Fragenkatalogs und deren Antwortbausteine. Für eine von der Fragenkatalogstruktur unabhängige Auswertung sind die Generierungsregeln geeignet, da sie von dem Fragenkatalog getrennt repräsentiert werden. Die Auswertungssicht sollte aber auch die Beeinflussung der Ergebnisse durch Verknüpfungs- und Ersetzungsregeln explizit darstellen, denn diese Regeln beeinflussen durch deren Erhebungssteuerung indirekt die Auswertungsergebnisse. So ist es für die Erklärung der Ergebnisse hilfreich, wenn die übersprungenen oder automatisch beantworteten Fragen im Auswertungsbericht besonders berücksichtigt werden.

4.2.4 Repräsentationserweiterung für unsicheres und vages Wissen

Die Stärken von Regelsystemen liegen in der natürlichen Wissensbeschreibung von Expertenwissen und in einer offenen Struktur, die sich durch Kopplung anderer Repräsentationsformen - wie unsicheres oder vages Wissen - erweitern lässt. So besitzt das Expertenwissen

einen gewissen Grad an nicht sicherem Wissen. Das nicht sichere Wissen wird in zwei Ausprägungsformen differenziert[478]:

- unsicheres, stochastisches oder probabilistisches Wissen und
- unscharfes oder vages Wissen.

4.2.4.1 Unsicheres, stochastisches oder probabilistisches Wissen

Wissen, das sich nicht mit vollständiger Korrektheit darstellen lässt, also nicht deterministisch ist, wird mit Wahrscheinlichkeiten bewertet. Die Darstellung von unsicherem Wissen kann wie folgt beschrieben werden:

- Theorem von Bayes
- Konfidenzfaktoren

Theorem von Bayes

Ein Ansatz, um unsicheres Wissen durch bedingte Wahrscheinlichkeiten darzustellen, ist das Theorem von Bayes. Der Bayes´sche Ansatz basiert auf der folgenden Gleichung:

$$P(D \mid S) = \frac{P(S \mid D) \cdot P(D)}{P(S)} = \frac{\text{kausale Wahrscheinlichkeit} \cdot \text{Grundrate}}{\text{Wahrscheinlichkeit des Symptoms}} = \text{diagnostische Wahrscheinlichkeit}$$

Darstellung mit mehreren Symptomen :

$$P_r(D_i \mid S_1 \wedge \ldots \wedge S_m) = \frac{P(D_i) \cdot P(S_1 \mid D_i) \cdot \ldots \cdot P(S_m \mid D_i)}{\sum_{j=1}^{n} P(D_j) \cdot P(S_1 \mid D_j) \cdot \ldots \cdot P(S_m \mid D_j)}$$

$S_1,\ldots,S_m$	unabhängige Symptome bzw. Merkmale
$D_1,\ldots,D_j$	wechselseitige ausschließende Diagnosen bzw. Lösungen
Grundrate	Wahrscheinlichkeit der Diagnose ohne Berücksichtigung des Symptoms

Gleichung 2: Theorem von Bayes[479]

P(D|S) stellt die bedingte Wahrscheinlichkeit dar, wenn das Symptom vorliegt. *P(S|D)* ist die Wahrscheinlichkeit des Symptoms bei der jeweiligen Diagnose. *P(S)* ist die Wahrscheinlichkeit, mit der das Symptom vorliegt. *P(D)* ist die Grundrate. Neben dem grundsätzlichen Problem der Ermittlung von Wahrscheinlichkeiten[480], das schon bzgl. der Risikobewertung diskutiert worden ist, bergen die folgenden Voraussetzungen des Bayes'schen Ansatzes vielfältige Probleme für den Einsatz in der Praxis[481]:

- Diagnosen schließen sich gegenseitig aus und sind vollständig anzugeben,
- Unabhängigkeit der Merkmale,

[478] Vgl. Engelmann (1990), S. 187 und Gabriel (1992), S. 44 ff.
[479] Vgl. Spies (1993), S. 39 und Bamberger (1999), S. 33
[480] Vgl. Frank (1988), S. 62
[481] Vgl. Altenkrüger (1992), S.82 und Bamberger (1999), S. 32

- ausreichende Anzahl an Fällen pro Lösung,
- eine vollständige Darstellung aller Wahrscheinlichkeiten führt zu einer kombinatorischen Explosion.

Konfidenzfaktoren

Das regelbasierte System Mycin, das in dem Bereich der Medizin eingesetzt wird, verwendet Sicherheits- oder Konfidenz- bzw. Gewissheitsfaktoren[482] (cf), um die Gewissheit des Arztes zu berücksichtigen[483]. Hierbei werden einerseits Wahrscheinlichkeiten angegeben, mit welcher Wahrscheinlichkeit die vorliegenden Symptome auf eine Krankheit hindeuten (WENN Symptom S, DANN Krankheit K), anderseits wird angegeben, wie hoch die subjektive Wahrscheinlichkeit ist, dass die unterstellte Krankheit auch beim Fehlen des betrachteten Symptoms vorliegt (WENN Symptom S fehlt, DANN Krankheit K)[484].

Innerhalb der Regeln dürfen die Symptome miteinander korrelieren, die Regeln als Ganzes müssen aber unabhängig sein. Die Forderung der Unabhängigkeit der Regeln ist ein Hauptkritikpunkt des Mycin-Systems[485]. Allgemein ist in der Herkunft, Ermittlung und Aufbereitung von Wahrscheinlichkeiten und Konfidenzfaktoren, die auf stochastischem Wissen basieren, eine zentrale Schwachstelle der Methoden. Wenn diese Werte im großen Umfang auf subjektiven Erwartungswerten oder Durchschnittswerten basieren, ist dies problematisch. Auch eine statistisch einwandfreie Erhebung von Wahrscheinlichkeiten wird mit steigender Zahl der zu untersuchenden Aussagen immer aufwendiger.

4.2.4.2 Unscharfes oder vages Wissen

Fuzzy-Logik (Rechnen mit unscharfen Mengen)

Häufig ist Expertenwissen nicht exakt und an der natürlichen Sprache des Menschen ausgelegt. Aus diesem Grund wird diese Form als sprachliche oder linguistische Unsicherheit bezeichnet[486]. So sind Aussagen wie „wir besitzen hohe Ausfallsicherheit“ oder „wir haben ein umfangreiches Netzwerk“ nicht mit den konventionellen Repräsentationssprachen realisierbar, denn die scharfe und zwei elementige Menge (wahr, falsch) der klassischen Logik stößt schnell an ihre Grenzen. Hier bietet die mehrwertige oder Fuzzy Logik Möglichkeiten, welche aus einer Erweiterung der klassischen Mengentheorie besteht, dieses Wissen darzustellen. Mit Fuzzy Control Systemen, die seit Ende der 80er Jahre erfolgreich z.B. in Haushaltsanwendungen (Waschmaschinen, Mikrowellen-Öfen oder Video-Kameras) eingesetzt werden[487], ist es möglich, eine wissensbasierte Unsicherheitsverarbeitung zu unterstützen. Damit wird linguistisch formuliertes Wissen repräsentiert[488].

Im Gegensatz zur traditionellen Logik wird bei der Fuzzy-Logik die Zugehörigkeit eines Objektes zu mehreren Mengen durch eine bestimmte Wahrscheinlichkeit festgelegt. So kann bei der traditionellen Logik das Element A nur zur Menge X oder Menge Y gehören. Mit Hilfe

[482] Engl.: certainty factors
[483] Vgl. Kurbel (1992), S. 33. Konfidenzfaktoren werden auch als „Gewissheitsfaktoren“ bezeichnet. Vgl. auch Spies (1993), S. 49
[484] Vgl. Frank (1988), S. 57
[485] Vgl. Puppe (1991), S. 52
[486] Vgl. Zimmermann (1997), S. 4
[487] Vgl. Schulte (1993), S. 11
[488] Vgl. Lelke (1999), S. 3

von graduellen Zugehörigkeitsfunktionen kann bei der Fuzzy-Logik das Objekt A mit einer gewissen Wahrscheinlichkeit zur Menge X und Menge Y gehören. Die unscharfen Mengen, z.B. linguistische Variablen, können mit Operatoren wie Vereinigung, Durchschnitt oder Negation verarbeitet werden. Linguistische Variablen besitzen als Ausprägungen Worte oder Ausdrücke der natürlichen Sprache. So kann der Grad an „Vertraulichkeit“ durch eine linguistische Variable mit den Werten hoch, mittel oder niedrig beschrieben werden[489]. Unsicheres Wissen kann in Kombination von Regeln und Fuzzy-Technik abgebildet werden, wobei Prämissen und Konklusion als linguistische Variable repräsentiert werden. Dies hat den Vorteil, dass eine bewährte und verbreitete Repräsentationsform eine Erweiterung mit neuen Repräsentationstechniken findet. Anhand des unten dargestellten Beispiels soll die grundsätzliche Funktionsweise eines Fuzzy-Controllers dargestellt werden.

Die Wissensbasis besteht aus drei Regeln, wobei die Prämissen (Datenmenge, Beanspruchung der Festplatte) und die Konklusion (Risiko des Verlustes an Verfügbarkeit) aus linguistischen Variable bestehen:

- Regel 1: WENN Datenmenge = gering UND Beanspruchung der Festplatte = niedrig DANN Risiko = niedrig
- Regel 2: WENN Datenmenge = mittel UND Beanspruchung der Festplatte = mittel DANN Risiko = mittel
- Regel 3: WENN Datenmenge = hoch UND Beanspruchung der Festplatte = mittel DANN Risiko = hoch

[489] Vgl. Schönberg/Thoben (1999), S. 51

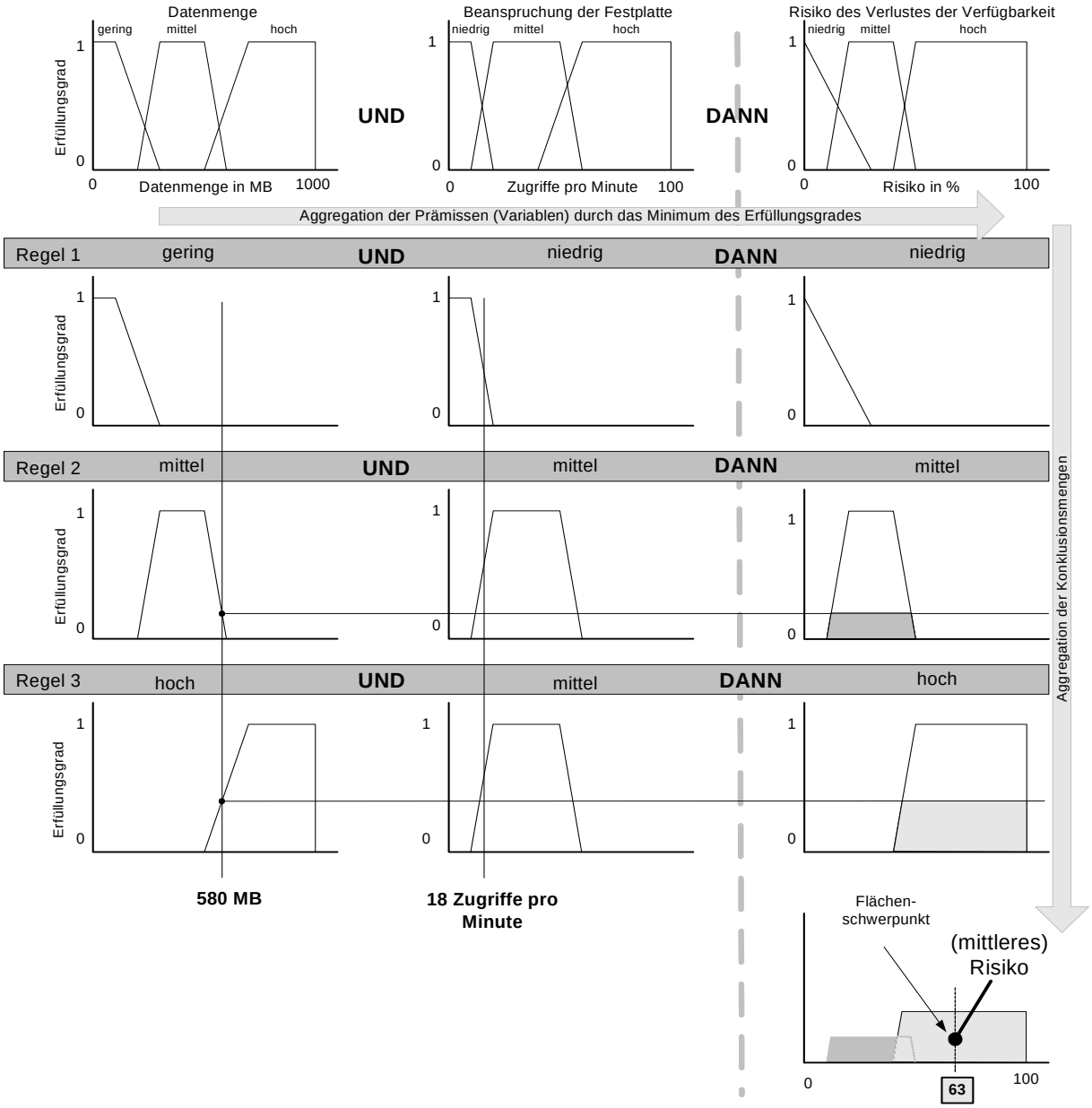


Abbildung 105: Prinzip des Fuzzy-Controllers am Beispiel der IS-Sicherheit[490]

Wie in der Abbildung dargestellt, ergeben sich die Werte „niedrig“, „mittel“ und „hoch“ als Kontinuum und überschneiden sich. Die Variable „Datenmenge“ wird mit dem gespeicherten Datenvolumen in MB bestimmt und die Variable „Beanspruchung der Festplatte“ wird mit Hilfe der Zugriffe pro Minute angegeben.

[490] Erweitert in Anlehnung an Spies (1993), S. 247 ff. Vgl. auch Lelke (1999), S. 106

Die Vorgehensweise des Fuzzy-Controllers, welcher das unsichere Wissen verarbeitet, lässt sich in den folgenden Schritten beschreiben[491]:

1. Fuzzyfizierung
   Im ersten Schritt erfolgt die Umwandlung der Eingangswerte (hier 580 MB und 18 Zugriffe pro Tag) in einen unscharfen Zustand. Hierzu wird die Zugehörigkeit des exakten Wertes zu der entsprechenden linguistischen Variablen bestimmt.
2. Inferenz
   Im ersten Teilschritt der Inferenz erfolgt die Aggregation der unscharfen Prämissen zu einem gesamten Erfüllungsgrad der Regel. In dem Beispiel existieren nur UND-Verknüpfungen zwischen den Prämissen, so dass als Aggregationsoperatoren das Minimum der einzelnen Erfüllungsgrade der Prämissen angenommen wird.
   So ist z.B. bei der zweiten Regel der Erfüllungsgrad der ersten Prämissen (Datenmenge) niedriger als der der zweiten Prämissen (Beanspruchung der Festplatte). Aus diesem Grund wird der Erfüllungsgrad der ersten Variablen verwendet. Wenn eine ODER-Verknüpfung vorliegt, wird das Maximum des Erfüllungsgrades als Aggregationsoperator angewandt.
   Im zweiten Teilschritt (Implikation) wird aufgrund des ermittelten Erfüllungsgrades die zugehörige Konklusion (hier das Risiko) für die jeweilige Regel ermittelt. Der ermittelte Erfüllungsgrad (hier Minimum) bildet den Grad der jeweiligen Konklusion ab.
   Im dritten Teilschritt werden die einzelnen Konklusionsmengen aggregiert. Als Ergebnis entsteht eine Vereinigung der Konklusionsmengen zu einer unscharfen Ergebnismenge.
3. Defuzzyfizierung
   Aus dem ermittelten unscharfen Inferenz-Ergebnis in Form der vereinigten Menge ist wieder ein scharfes Ergebnis zu ermitteln. Dabei wird häufig der Flächenschwerpunkt der Menge (wie im unteren Beispiel) oder der Mittelwert der Maximalwerte verwendet. Der ermittelte Wert (im Beispiel 63) kann wiederum in einen linguistischen Wert umgewandelt werden. So können auf einer Skala die Risikowerte 1 bis 100 in „niedrig“, „mittel“ und „hoch“ aufgeteilt werden. Im Beispiel wäre der Wert zwischen „mittel“ und „hoch“ einzustufen.

Obwohl mit wenigen quantitativen Regeln und sinnvoller Festlegung von Zugehörigkeitsfunktionen der Problembereich abgebildet wird, ist i.d.R. eine umfangreichere Anzahl an redundanzfreien Regeln erforderlich, um verwertbare Ergebnisse zu erlangen[492]. Die Komplexität eines solchen Modells wird analog zu der Repräsentation traditioneller Produktionsregeln sehr schnell unübersichtlich. Des Weiteren ist die Entwicklung von den Zugehörigkeitsfunktionen, insbesondere in den Maximum- und Minimumbereichen, nicht unproblematisch. I.d.R werden lineare Funktionen verwendet, da die Berechnung der Flächeninhalte meist durch ein Integral erfolgt; dies stellt bei nicht linearen Funktionen ein z.T. sehr komplexes Problem dar.

Vereinfachte Fuzzy-Logik

De Ru/Eloff (1996) bestimmen ohne Verwendung von linguistischen Variablen aus drei unscharfen Mengen (Festplattenalter, Zugriffsgrad, Mitarbeiterzufriedenheit) einen Risikofaktor. Bei der Berechnung des Risikos verzichten sie auf einen Teil der Fuzzyfizierung, da keine linguistischen Variablen verwendet werden. Die unscharfen Werte werden hier direkt von

[491] Vgl. Zimmermann (1993), S. 93 ff.
[492] Vgl. Spies (1993), S. 247

Eingangsgrößen (Festplattenalter = 10; Risikofaktor = 832) abgeleitet. Eine Zuordnung zu entsprechenden linguistischen Variablen entfällt. Eine Verknüpfung mehrerer unscharfer Mengen erfolgt durch Addition der jeweiligen Risikofaktoren, wie z.B. der Zugriffsgrad und die Mitarbeiterzufriedenheit.

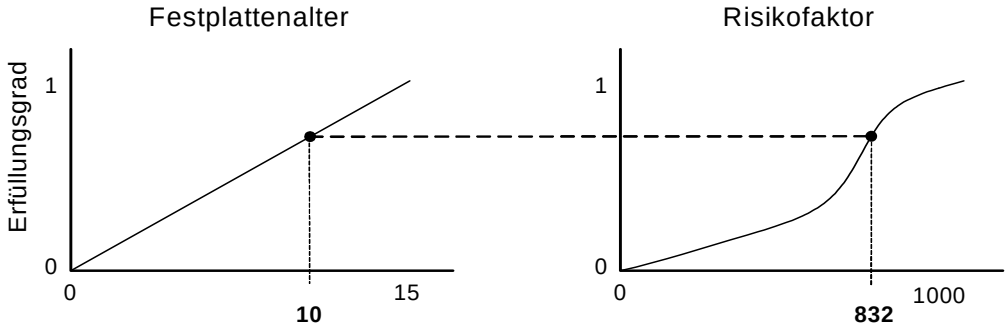


Abbildung 106: Vereinfachtes Fuzzy-Modell[493]

Dieses vereinfachte Vorgehen hat den Nachteil, dass bei der Regelerstellung auf linguistische Variablen verzichtet wird. So kann zwar die Aussage beschrieben werden, dass bei einer steigenden Lebensdauer einer Festplatte das Risiko steigt, jedoch die linguistischen Ausdrücke wie „gering“ bis „hoch“ werden nicht verwendet. Zur Abbildung von wenigen Variablen und Regeln ist dieses vereinfachte Fuzzy-Modell geeignet. Das vereinfachte Fuzzy-Modell kann aber nicht komplexe aggregierte Regeln darstellen.

4.3 Überführung der Basis-Inferenzen der IS-Sicherheitsstrategien auf das fragenkatalogorientierte Entwurfsmodell

Es folgt eine Anwendung des fragenkatalogorientierten Entwurfsmodells bzgl. der Basis-Inferenzen der IS-Sicherheitsstrategien. Hierfür werden die Basis-Inferenzen aus dem Expertisemodell durch das fragenkatalogorientierte Entwurfsmodell umgesetzt.

[493] Vgl. Ru/Eloff (1996), S. 246

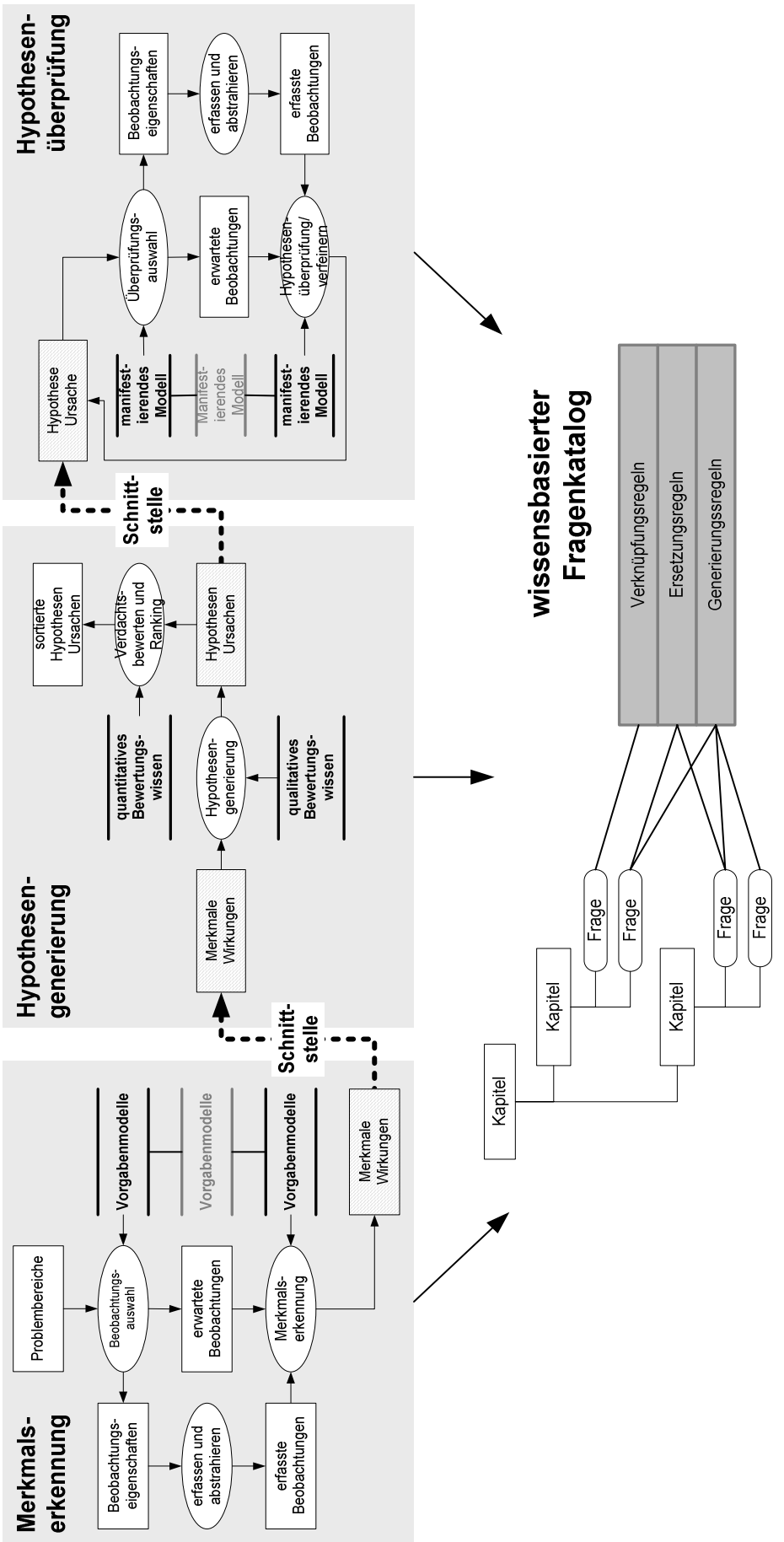


Abbildung 107: Überführung der Basis-Inferenzen auf das fragenkatalogorientierte Entwurfsmodell

4.3.1 Merkmalserkennung

Die eigentliche Differenzierung der Merkmalerkennung erfolgt durch unterschiedliche Vorgabenmodelle.

- Das Vorgabenmodell besteht aus erforderlichen Maßnahmen, die zum Erkennen von fehlenden Maßnahmen dienen.
- Das Vorgabenmodell wird zum Erkennen von vermuteten Zuständen als Wirkung verwendet.

Die Merkmalserkennung wird des Weiteren in der Beobachtungsauswahl sowie Erfassung und Abstraktion getrennt.

Beobachtungsauswahl
Die Grundstruktur der Beobachtungsauswahl wird primär durch die Kapitel- und ihrer Fragenstruktur vorgeben. Zusätzlich werden Verknüpfungsregeln hinzugefügt, um ausgewählte Bereiche zu aktivieren oder zu deaktivieren. Diese Grobauswahl des Problembereichs erfolgt durch Beantwortung von Auswahlfragen, welche ganze Problembereiche aktivieren oder deaktivieren. Die „Frage“ hat zudem die Aufgabe eines Merkmalsindikators. Die Antwortmöglichkeiten einer Frage (z.B. offene Fragen oder Alternativ-Frage) können bestimmte Beobachtungseigenschaften festlegen.

Erfassung und Abstraktion
Die Erfassung von Beobachtungen erfolgt durch Beantwortung der Antwortmöglichkeiten. Auf Basis des Antwortwertes resultiert die Abstraktion durch Aktivierung des Antwortbausteins, welcher mit dem Antwortwert verknüpft ist. Durch Antwortbausteine werden die Beobachtungen dargestellt. Es werden die erwarteten und erfassten Merkmale (Antwortbausteine) in einem Statusbericht zusammenfassend aufgezeigt. Wenn das erwartete Resultat (angeklickte Merkmal) gleich/ungleich ist, wird angezeigt, dass

- die geforderte Maßnahme (Merkmal) vorhanden/nicht vorhanden ist
- oder eine Konsequenz (Wirkung) besteht/nicht besteht.

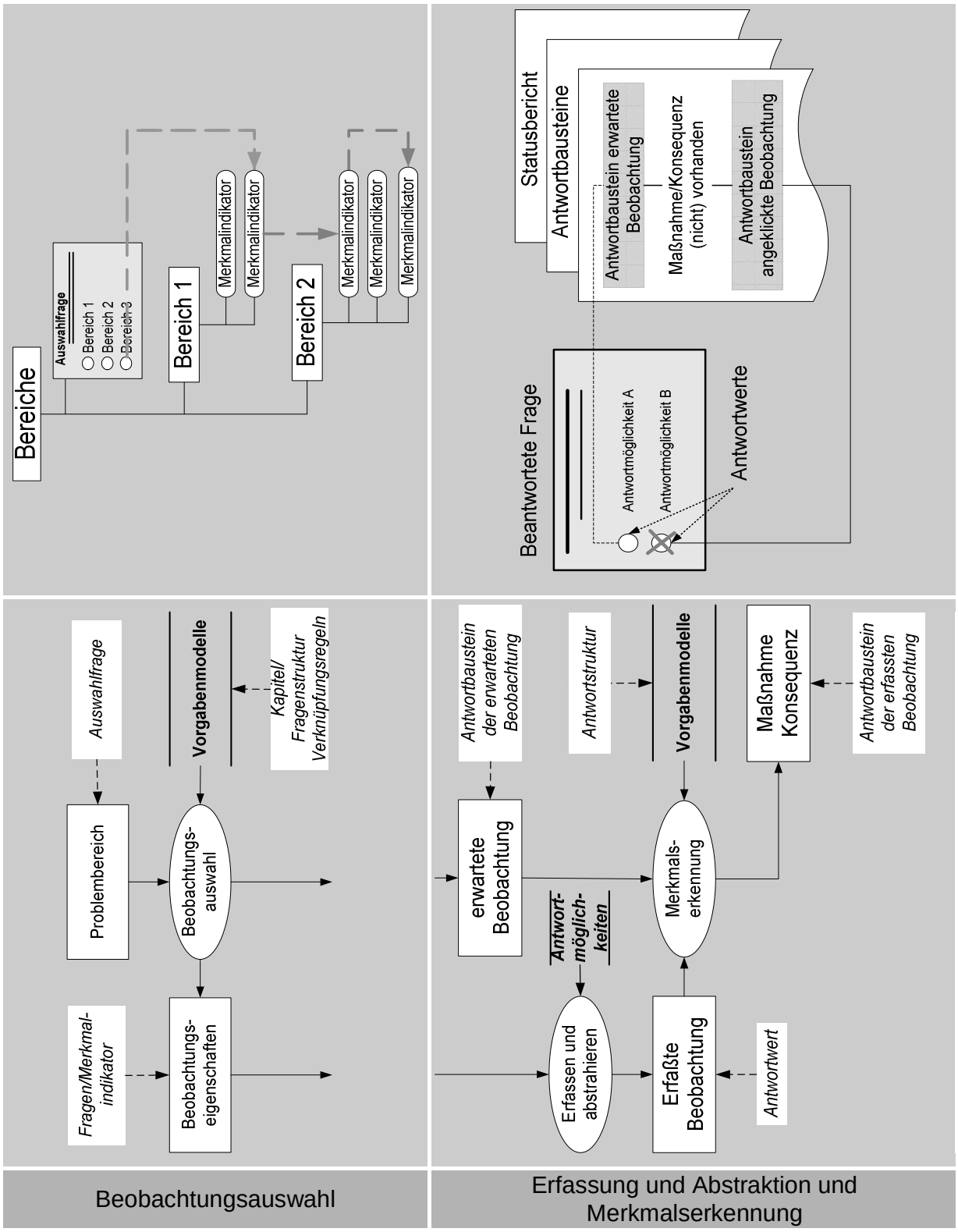


Abbildung 108: Beobachtungsauswahl und Merkmalserkennung

4.3.2 Hypothesengenerierung und -überprüfung

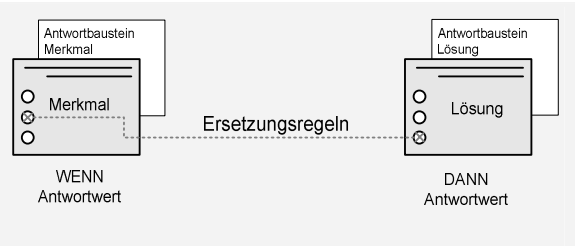
Bei der Hypothesengenerierung und -überprüfung ist eine differenzierte Überführung der IS-Sicherheitsstrategien auf die Fragenkataloge und deren Regeln erforderlich. Im Rahmen der Arbeit werden Problemlösungskonzepte durch folgende Ausprägungsformen beschrieben:

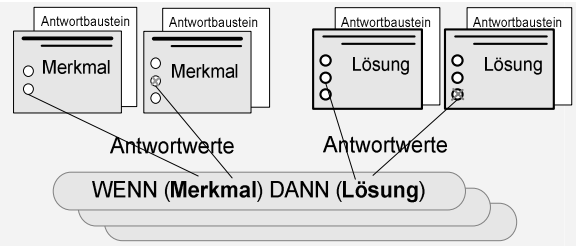
- Heuristische Regeln besitzen die Form „Merkmale deutet auf Lösung“, wohingegen
- kausale Regeln durch „Ursache (Lösung) verursacht Wirkung (Merkmal)“ gekennzeichnet sind.

Die folgende Tabelle stellt die Überführung der assoziativen und kausalen Abhängigkeitsformen in Regeln dar.

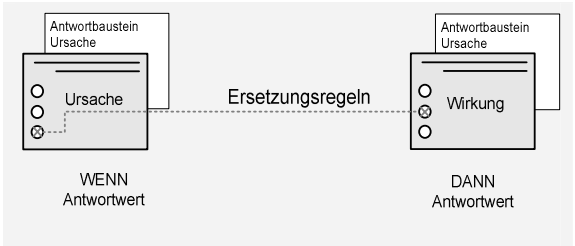
Problemlösungskonzepte					
assoziative Abhängigkeiten			kausale Abhängigkeiten		
Merkmal	deutet auf	Lösung	Ursache	verursacht	Wirkung
Maßnahme fehlt	deutet auf	Schwachstelle	gefährdendes Ereignis	verursacht	Konsequenz
Konsequenz	erfordert		Schwachstelle	ermöglicht	
Überführt ⇓ in assoziative Regeln			Überführt ⇓ in kausale Regeln		
WENN	Vorbedingung	DANN	Nachbedingung	WENN	Vorbedingung	DANN	Nachbedingung
	Maßnahme fehlt		Schwachstelle		Gefahr UND Element[494]		Konsequenz
	Konsequenz				Schwachstelle		

Überführt in assoziative Ersetzungs- und Generierungsregeln





Überführt in kausale Ersetzungs- und Generierungsregeln



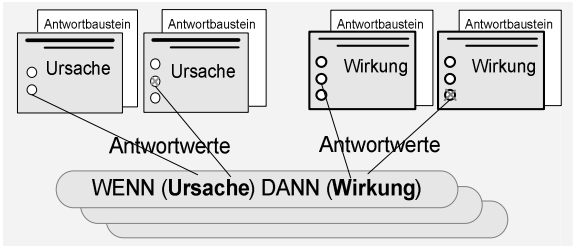


Tabelle 19: Überführung der Problemlösungskonzepte in Regeln

Kausale Regeln lassen sich einfacher angeben, weil das Kausalitätsprinzip direkt (vorwärtsorientiert) beschrieben werden kann. Dafür ist die Auswertung bei kausalen Regeln schwieriger, da die Regeln im Gegensatz zu den assoziativen nicht direkt anwendbar sind[495]. Dies rührt daher, dass bei einer reaktiven Bottom-Up Strategie von beobachteten Konsequenzen überdeckend (rückwärtsorientiert) auf deren Ursachen geschlossen wird. Die Anwendung der Problemlösungskonzepte auf die IS-Sicherheitsstrategien wird durch das Kontrollsystem festgelegt. Hierbei wird insbesondere die Interpretationskomponente gesteuert, die wiederum festlegt, wie die Regeln abgearbeitet werden.

[494] Das gefährdende Ereignis wird durch eine UND-Verknüpfung zwischen Gefahr und sicherheitsrelevantem Element abgebildet.
[495] Vgl. Puppe et al. (1996), S. 117

4.3.2.1 Top-Down Problemlösung

Die Top-Down Problemlösungskonzepte werden mit Hilfe von Produktionsregeln dargestellt. „*Unter einer Produktionsregel versteht man eine mit einer Vorbedingung versehene Aktion. Die Aktion gilt als ausführbar, wenn die Vorbedingung erfüllt ist*“[496]. Die Vorbedingungen beziehen sich auf eine Faktenbasis, z.B. auf erhobene Antwortwerte. Diese Systeme werden auch häufig als Produktionssysteme bezeichnet, da die Regeln ausgehend von Ursprungsfakten neues Wissen in Form von neuen Fakten produzieren. Auch wenn Parallelen zwischen Produktionsregeln und Implikationen aus der Prädikatenlogik bestehen - da Regeln als „*prozedurale interpretierbare prädikatenlogische Implikationen*“[497] bezeichnet werden können - sollte beachtet werden, dass Aktionen Handlungsanweisungen darstellen, die sich ganz anders verhalten können als ein logisches Kalkül, das „nur“ einen Wahrheitswert annehmen kann[498].

Prämissen und Konklusionen von Produktionsregeln können logische Ausdrücke ähnlich der Prädikatenlogik sein, wobei Konklusionen auch Aktionen bzw. Handlungen - wie z.B. weitere Merkmale erheben - beinhalten können. Eine Regel „Prämisse DANN Konklusion“ wird wie folgt interpretiert: Wenn die Prämisse erfüllt ist, dann wird die Konklusion oder eine Aktion ausgeführt[499]. In dieser Vorgehensweise werden auf Grund von erhobenen Beobachtungen (Maßnahmen und Konsequenzen) Konklusionen (Schwachstellen) abgeleitet, wenn die Vorbedingungen erfüllt sind. Prämissen können als Vorbedingungen aufgefasst werden und mit Konjunktionen (Und-Verbindungen) oder Disjunktionen (Oder-Verbindungen) erweitert werden. Regeln können zudem über Konklusion miteinander verknüpft werden und bilden somit eine Ableitungskette bzw. ein inferentielles Netz.

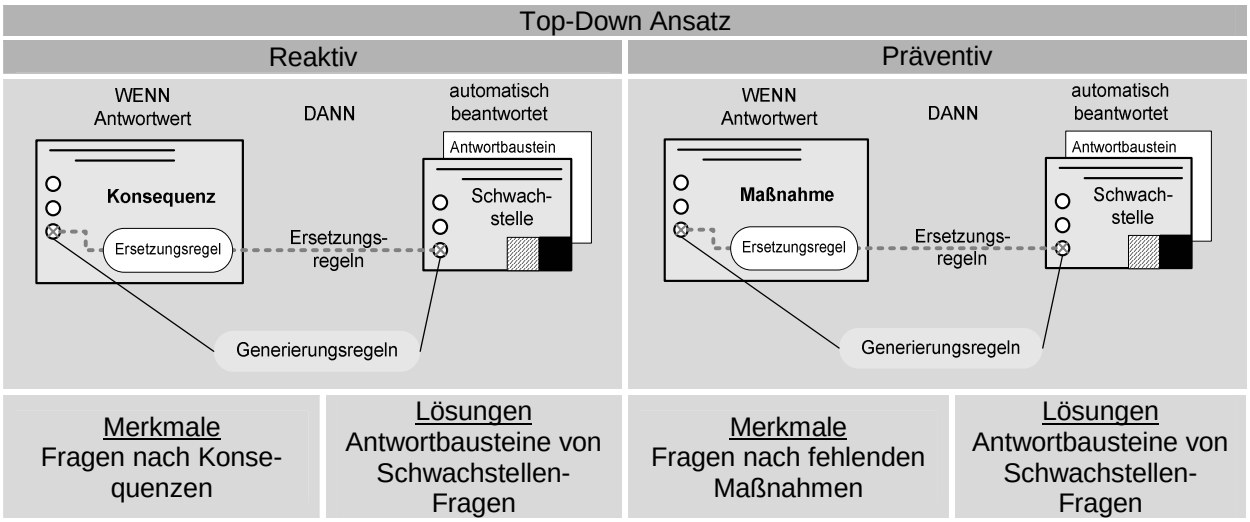


Abbildung 109: Reaktive und präventive Top-Down Regeln

Die Differenzierung zwischen reaktiver und präventiver Top-Down IS-Sicherheitsstrategie erfolgt in der Aktivierung bzw. Deaktivierung der zu erhebenden Merkmale. Bei der reaktiven Sichtweise werden beobachtete Konsequenzen (Konsequenz-Frage) erhoben, wohingegen bei

[496] Reimer (1991), S. 55
[497] Altenkrüger (1992), S. 7
[498] Vgl. Reimer (1991), S. 55 und Altenkrüger (1992), S. 22
[499] Vgl. Kurbel (1992), S. 47

der präventiven Sichtweise fehlende Maßnahmen (Maßnahmen-Frage) erhoben werden. Hierbei erfolgt die Auswertung der Regeln in ähnlicher Art, wobei die Vorbedingungen in Abhängigkeit der präventiven und reaktiven Problemlösung variieren. Eine parallele reaktive und präventive Strategie ist von Vorteil, da die Ermittlung beider Merkmalsformen die Problemlösung erhöhen kann.

4.3.2.1.1 Direkte Hypothesengenerierung und Verdachtsbewertung

Die direkte Assoziation erfolgt in entsprechender Weise wie bei der Merkmalserkennung, wobei hier nicht nur die erhobenen Beobachtungen dokumentiert werden, sondern bei einer fehlenden Maßnahme die zusätzliche Schwachstelle direkt zugeordnet wird. Hierfür werden die Maßnahmen-Antwortbausteine mit Schwachstellen erweitert. Diese Zuordnung ist einfach anzugeben, da keine zusätzlichen Ersetzungsregeln notwendig sind; sie ist aber schnell begrenzt durch die einfache Repräsentation. So kann nicht dargestellt werden, ob vorhandene Maßnahmen durch fehlende Maßnahmen ersetzt werden oder zusätzlich ermittelte Konsequenzen Verdachts-Schwachstellen verstärken können.

Bei der Verdachtsbewertung und -ranking werden durch eine „rekursive Hochrechnung“ der Kapitel-, Fragen- und Antwortwerte z.B. Schwachstellen gewichtet. So können die Schwachstellen durch gewichtete Frageergebnisse (rot, gelb, grün) sortiert werden. Die Kapitel bilden die bewerteten Problembereiche ab. Diese Form der rekursiven Verdachtsbewertung kann zur Bewertung der folgenden Hypothesen und Ursachen angewandt werden.

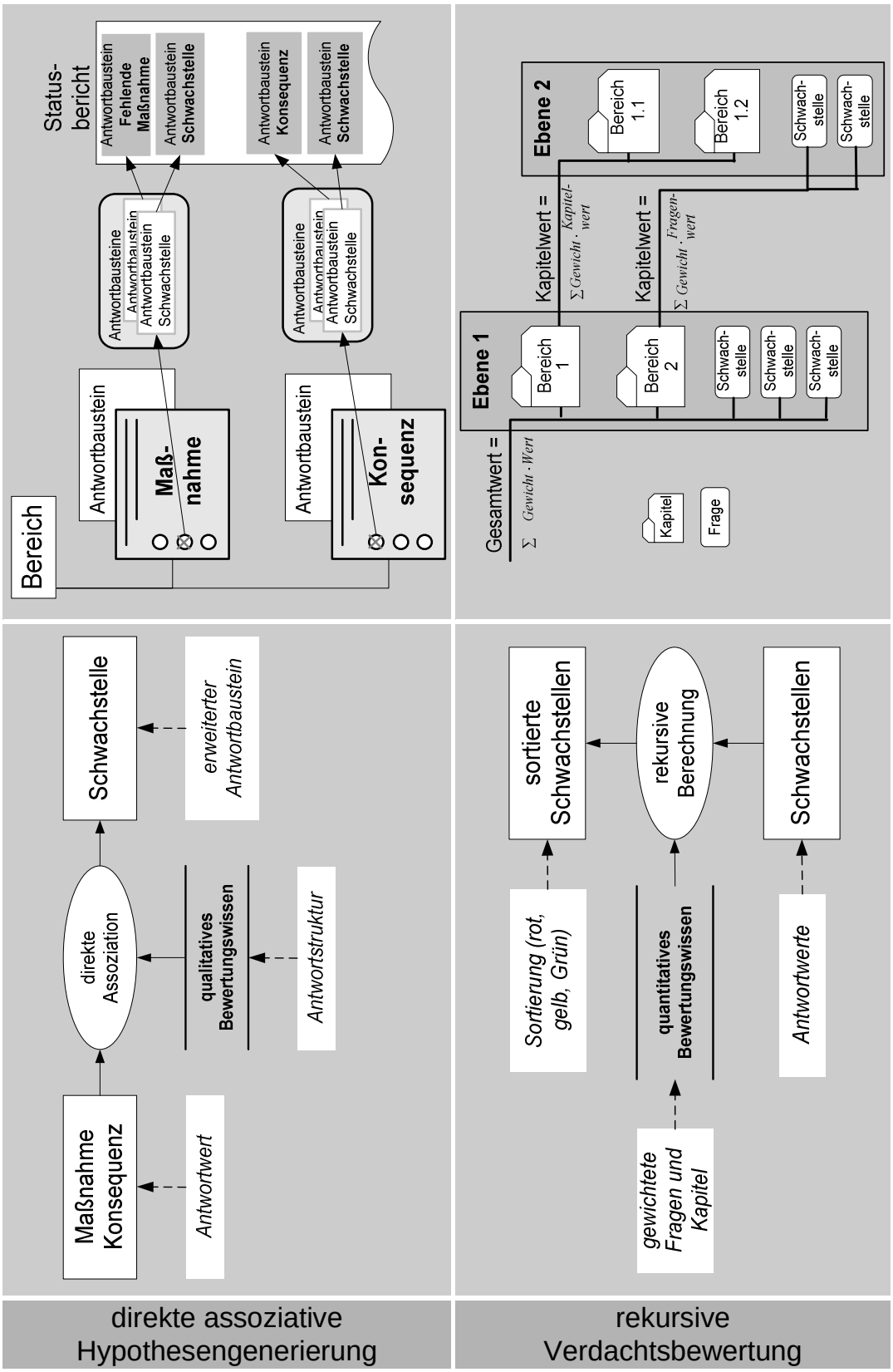


Abbildung 110: Direkte Top-Down Hypothesengenerierung und Verdachtsbewertung

4.3.2.1.2 Hierarchische Hypothesengenerierung und -überprüfung

Hierarchisch verknüpfte Assoziationen werden durch hierarchische Kapitel- und Fragestrukturen sowie durch zusätzliche assoziative Ersetzungsregeln dargestellt. Hiermit wird die Establish-Refine Strategie auf Fragenkataloge angewendet. Aufgrund von Antwortwerten werden verknüpfte Fragen durch Ersetzungsregeln automatisch beantwortet. Dabei werden Verdachts-Schwachstellen durch automatisch beantwortete Fragen und deren Antwortbaustein dargestellt.

Eine einfache hierarchische Hypothesenüberprüfung kann durch offene, automatisch beantwortete Schwachstellen-Fragen erfolgen. Die Verdachts-Schwachstellen werden durch beantwortete Maßnahmen- und Konsequenz-Fragen aktiviert. Diese aktivierten Verdachts-Schwachstellen werden bei offenen Fragen dem Benutzer präsentiert, der dann den Verdacht bestätigen oder durch Aktivierung einer anderen Antwortmöglichkeit revidieren kann. Es ist aber auch möglich, die Verdachts-Schwachstellen durch Antwortbausteine von verdeckten Fragen ohne Bestätigungsmöglichkeit herzuleiten[500]. Aufgrund der engen Verknüpfung zwischen der Hypothesengenerierung und der folgenden Überprüfung ist eine eindeutige Trennung der beiden Basis-Inferenzen nicht möglich.

Bei einer komplexeren hierarchischen Hypothesenüberprüfung werden ausgehend von Verdachts-Schwachstellen durch Verknüpfungsregeln zusätzliche Überprüfungsmerkmale in Form von Maßnahmen- und Konsequenzfragen aktiviert, welche sich in einer tieferen Hierarchiestufe befinden. Die „Verdachts-Überprüfungsfragen“ werden in Überprüfungsbereichen (Tests) zusammengefasst. Die Erfassung, Abstraktion und Merkmalserkennung erfolgt vergleichbar zu der Merkmalserhebung. Zur Hypothesenüberprüfung wird basierend auf den Antwortwerten die Verdachts-Schwachstelle durch Ersetzungsregeln automatisch bestätigt oder widerlegt. Bei der Überprüfung werden eventuell zusätzlich „verfeinerte“ Schwachstellen ermittelt, welche wiederum durch zusätzliche Merkmale überprüft werden können usw.

[500] In der Abbildung sind beide Varianten (verdeckte und offene Beantwortung) dargestellt.

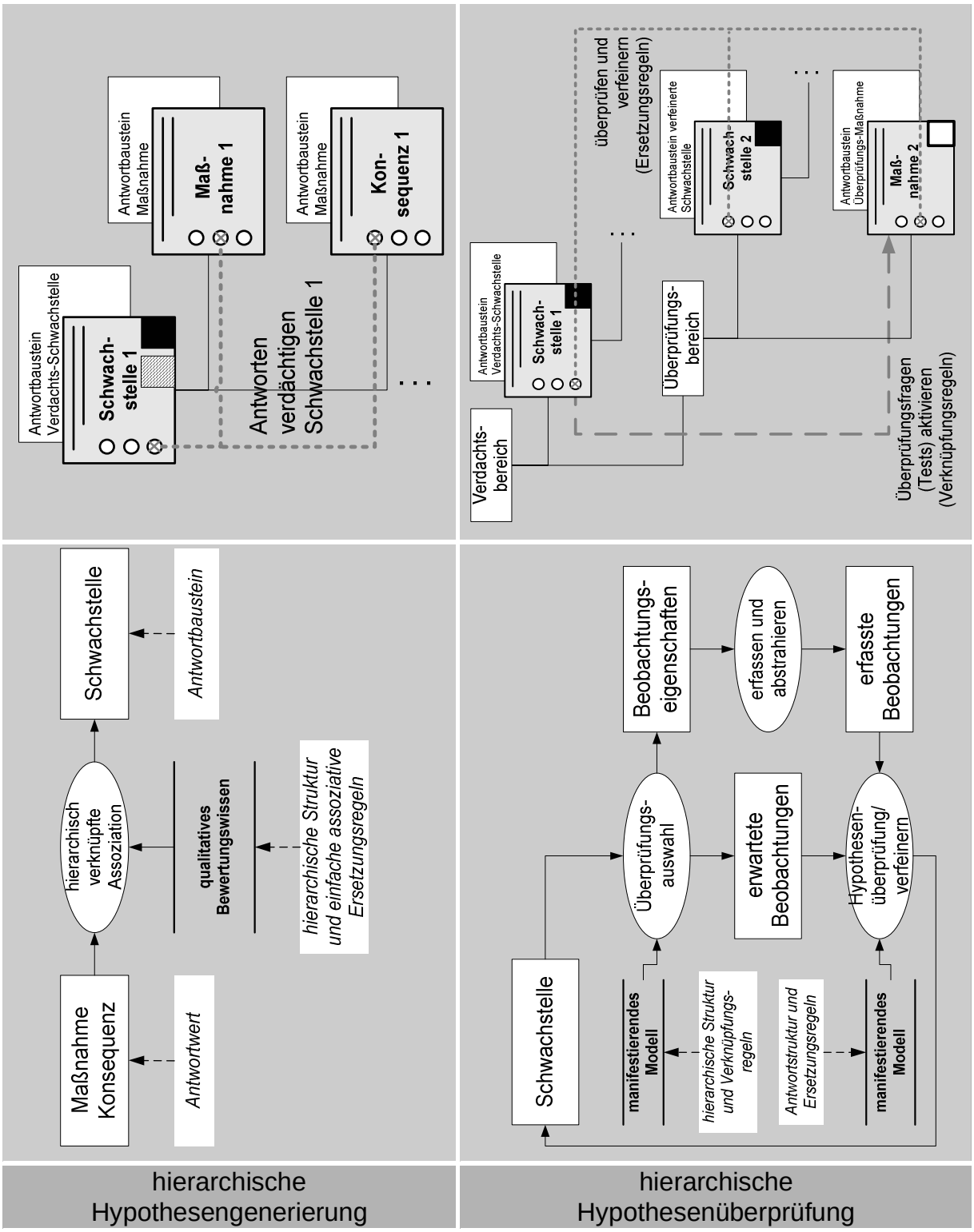


Abbildung 111: Hierarchische Top Down Hypothesengenerierung und -überprüfung

4.3.2.1.3 Komplexe Hypothesengenerierung und -überprüfung

Die komplex verknüpften Assoziationen basieren auf Generierungsregeln. Hierfür werden zwei getrennte Merkmals- und Verdachtshierarchien erstellt, deren Verknüpfung über komplexe Generierungsregeln erfolgt. Im folgenden Beispiel werden verschiedene Antwortwerte und eventuell vorhergehende logische Aussagen (Konklusionen) als Vorbedingungen (Prä-

missen) abgebildet. Diese Prämissen können zu komplexen Prämissenverknüpfungen zusammengefasst werden. Falls die Ersatzregel „feuert“, werden verdeckte Fragen automatisch beantwortet und deren Antwortbausteine werden aktiviert. Das Ergebnis der Generierungsregeln (Konklusion) kann wiederum in anderen Regel-Vorbedingungen als Prämisse verwendet werden und die verknüpften Regeln aktivieren.

Bei der komplexen Hypothesenüberprüfung werden ausgehend von der Verdachts-Schwachstelle zunächst durch Verknüpfungsregeln zusätzliche Merkmalsfragen zur Überprüfung aktiviert. Die Erfassung, Abstraktion und Merkmalserkennung erfolgt vergleichbar zu der Merkmalserhebung. Wenn die Vorbedingung der Überprüfungsregel „feuert“, wird die Verdachts-Schwachstelle durch eine Generierungsregel bestätigt oder widerlegt. Bei der Überprüfung können zudem neue Schwachstellen ermittelt werden, die eine Verfeinerung der zu überprüfenden Schwachstelle darstellen.

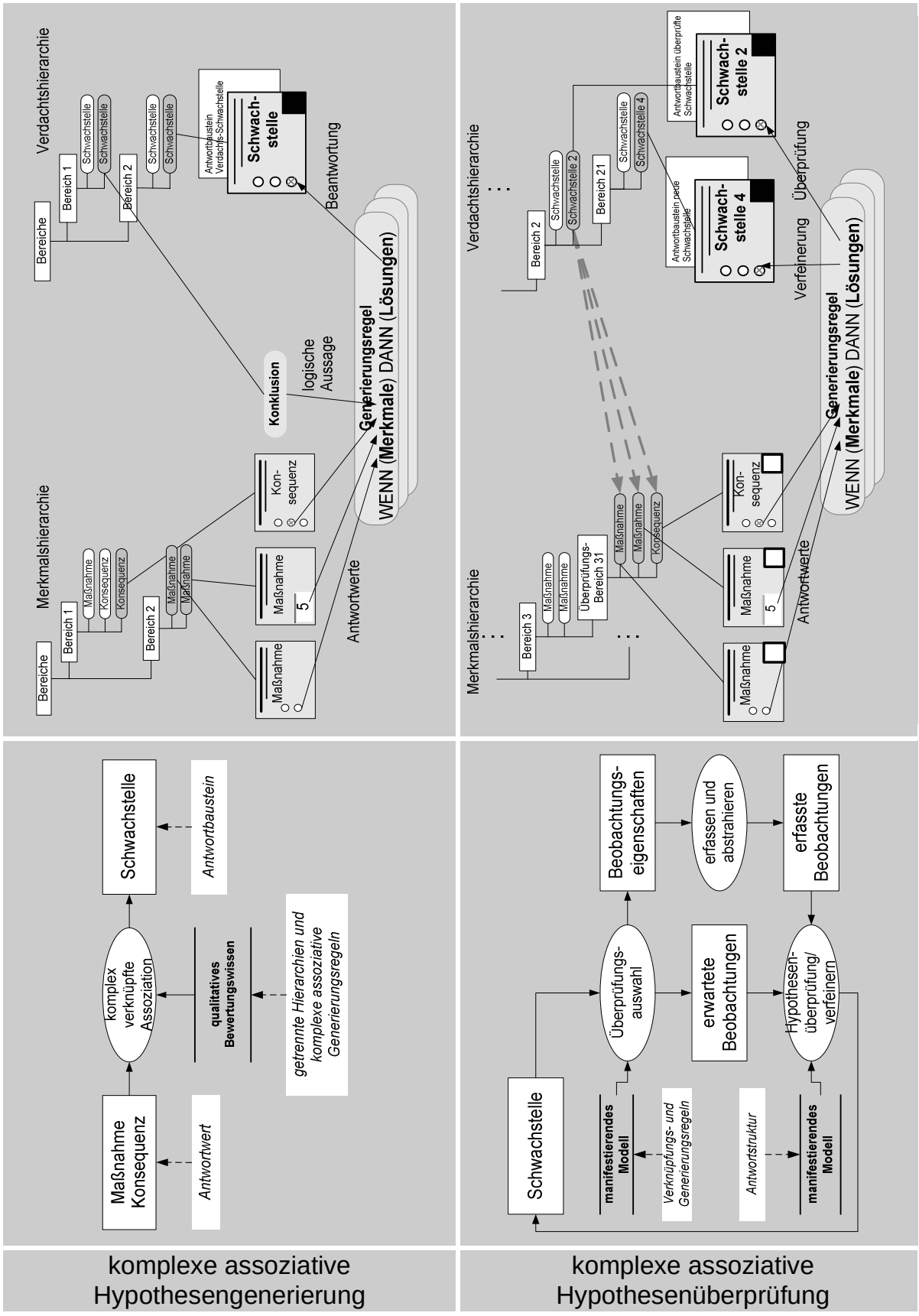


Abbildung 112: Komplexe Top-Down Hypothesengenerierung und -überprüfung

4.3.2.2 Bottom-Up Problemlösung

Mit Hilfe der Ersetzungs- und Generierungsregeln wird das Kausalitätsprinzip des Bottom-Up Ansatzes in wissensbasierte Fragenkataloge überführt. Die Ursachen (Element und Gefahr) können zu einer „gefährdenden Ereignis-Frage“ zusammengefasst und zusätzlich durch „kausale Schwachstellen“ erweitert werden. Die Zustandsänderungen von Konsequenzen in Gefahren für andere sicherheitsrelevante Elemente[501] werden mit Ersetzungs- und Generierungsregeln abgebildet. Prinzipiell lassen sich mit Ersetzungsregeln einfache kausale Abhängigkeiten und Zustandsänderungen erstellen. Für komplexe kausale Zusammenhänge und Zustandsänderungen sollten Generierungsregeln verwendet werden.

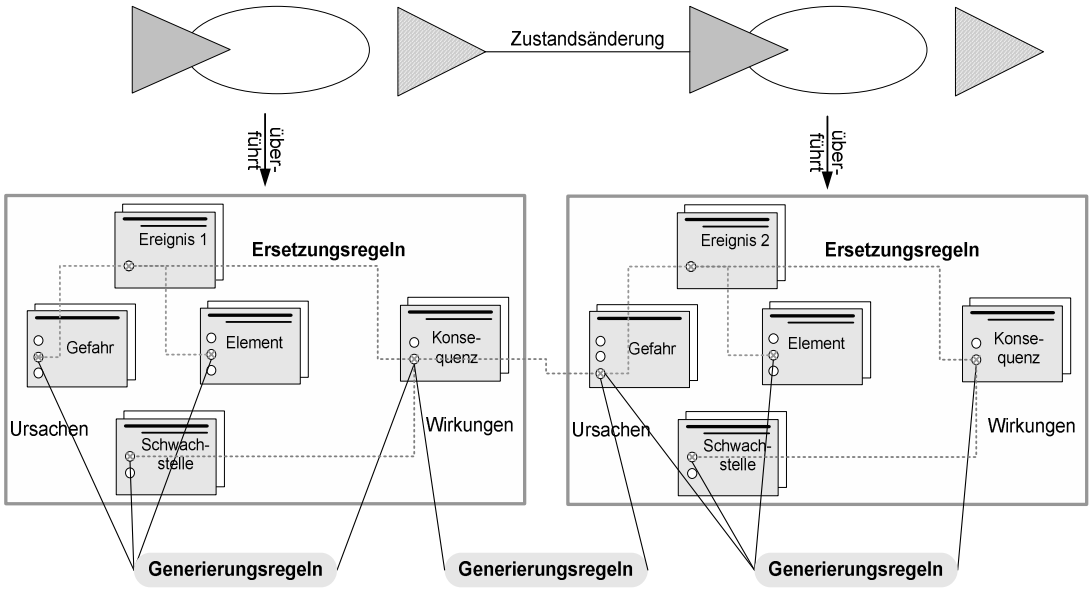


Abbildung 113: Abbildung des Kausalitätsprinzips

Folgend wird auf die explizite Darstellung von kausalen Schwachstellen verzichtet, da die daraus entstehende Kausalität - ähnlich wie bei „gefährdendes Ereignis“ - durch Ersetzungs- und Generierungsregeln überführt wird.

In den Bottom-Up Strategien erfolgt die Differenzierung der reaktiven und präventiven Sicht durch die Interpretationsrichtung der Regeln. Es wird bei der reaktiven Sichtweise ausgehend von erhobenen Konsequenzen rückwärtsorientiert auf Ursachen in Form von überdeckenden gefährdenden Ereignissen (Gefahren und Elementen) und kausalen Schwachstellen geschlossen. Ausgangspunkt ist die Konklusion der Regeln, welche die beobachteten Konsequenzen darstellen. Es wird versucht, die Regeln und somit die Ursachen (Vorbedingungen) zu finden, die am besten die Konsequenzen (Wirkungen) überdecken bzw. erklären. Bei der präventiven Sichtweise werden dagegen Konsequenzen ausgehend von angenommenen Ursachen vorwärtsorientiert vorausgesagt bzw. kausal simuliert.

[501] Im Beispiel ist aus Sicht von Ereignis 2 die Konsequenz von Ereignis 1 eine Gefahr für Ereignis 2.

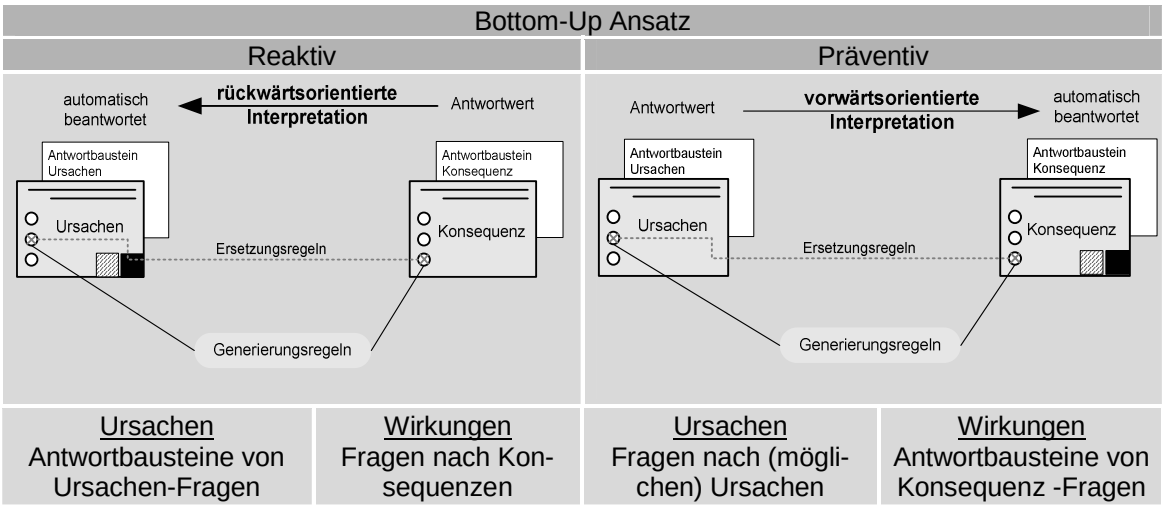


Abbildung 114: Reaktive und präventive Bottom-Up Regeln

Hierbei wird - basierend auf den gleichen Domänen-Basiskonzepten - die präventive und reaktive Problemlösung und ihre jeweiligen Problemlösungskonzepte durch unterschiedliche Aktivierung und Auswertung der Regeln repräsentiert. Eine parallele reaktive und präventive Strategie ist von Vorteil, da die Ermittlung beider Merkmalsformen die Problemlösung erhöhen kann.

4.3.2.2.1 Reaktive Bottom-Up Hypothesengenerierung und -überprüfung

Hypothesengenerierung und -überprüfung basierend auf Ersetzungsregeln
Die nachfolgende Abbildung von gefährdenden Ereignissen und deren Zustandsänderungen dient als Grundlage für die folgende Hypothesengenerierung und -überprüfung.

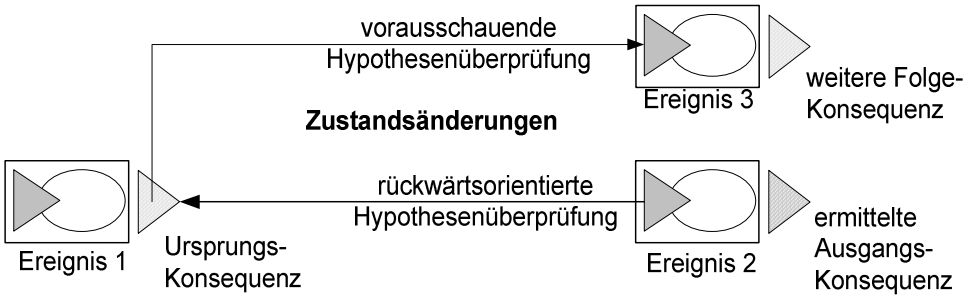


Abbildung 115: Zustandsänderungen

Bei der reaktiven Hypothesengenerierung erfolgt ausgehend von der ermittelten Konsequenz rückwärtsorientiert die Herleitung der überdeckenden Ursachen. Eine einfache Hypothesenüberprüfung kann durch „offene automatisch beantwortete“ Ursachen-Fragen erfolgen. Dieser generierte Verdacht wird dem Benutzer präsentiert, der den Verdacht bestätigt oder durch Aktivierung einer anderen Antwortmöglichkeit diesen widerlegt. Aufgrund der engen Verknüpfung zwischen Hypothesengenerierung und der folgenden Überprüfung ist eine eindeutige Trennung der beiden Inferenzen nicht möglich.

In der rückwärtsorientierten Hypothesenüberprüfung werden weitere Ursprungs-Konsequenz-Fragen aktiviert, welche nicht in der Merkmalserkennung berücksichtigt worden sind. Diese Überprüfung erfolgt mit Hilfe von Ersetzungsregeln, die die Zustandsänderung von Konsequenzen[502] repräsentiert. Hierbei werden die zusätzlichen Konsequenzen rückwärtsorientiert ausgewählt und beantwortet (Konsequenz von Ereignis 1). Diese Ursprungs-Konsequenz bestätigt oder widerlegt somit indirekt deren Folge- und beobachteten Konsequenzen.

Um mögliche Folge-Konsequenzen zur Hypothesenüberprüfung zu erhalten, werden weitere vermutete oder mögliche Folge-Konsequenzen vorausgesagt (Konsequenz von Ereignis 3), die noch nicht erhoben worden sind. Dies entspricht einer vorwärtsorientierten Überprüfungsauswahl bzw. Voraussage von möglichen Konsequenzen, welche auch indirekt die Ursprungs-Konsequenz bestätigen oder widerlegen können. Die eigentliche Überprüfung erfolgt durch die Beantwortung der zusätzlichen Konsequenz-Fragen und durch die automatische Beantwortung der Ursprungs-Konsequenzen.

[502] Konsequenzen können wiederum Gefahren für weitere sicherheitsrelevante Elemente darstellen.

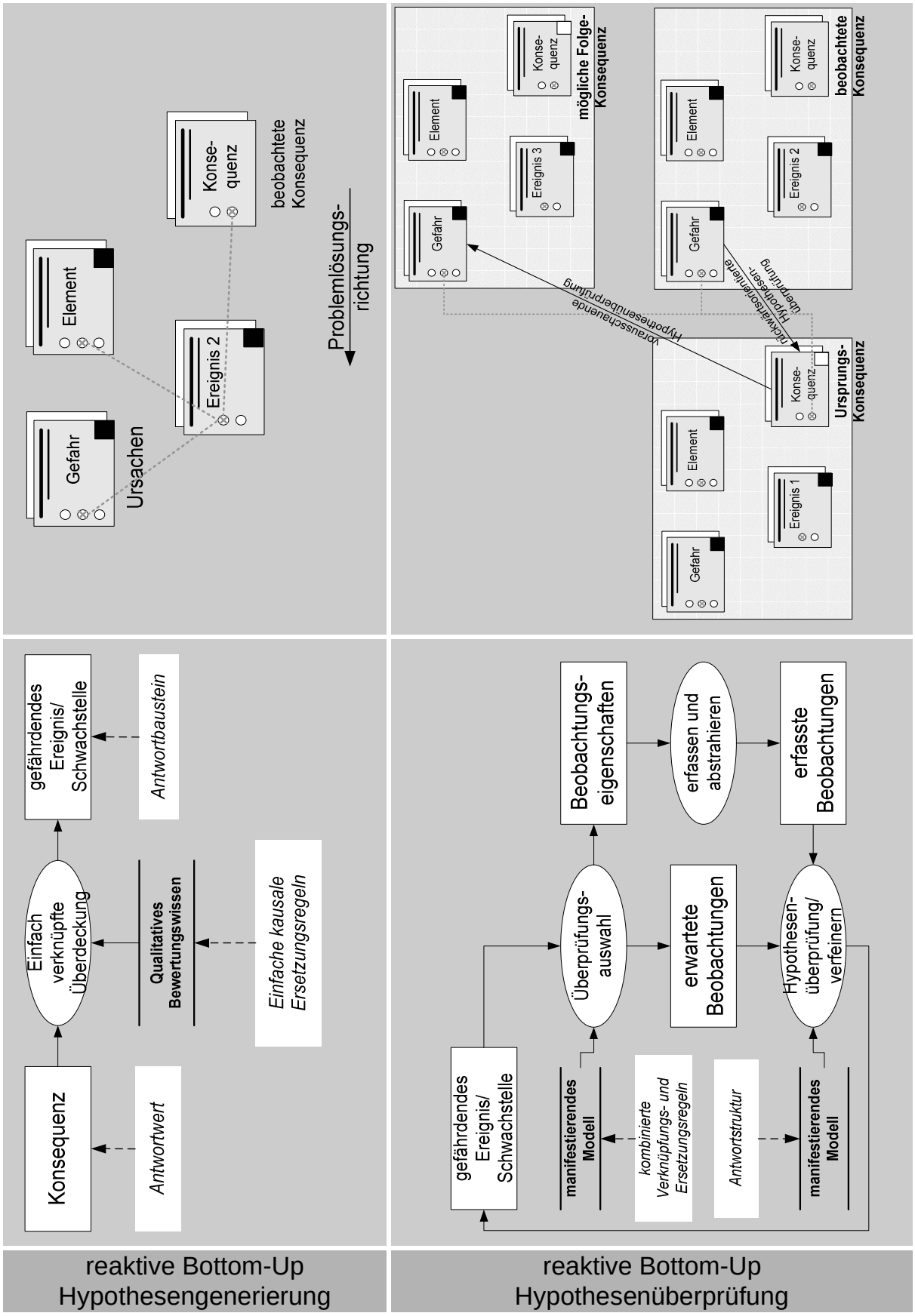


Abbildung 116: Reaktive Bottom-Up Hypothesengenerierung und -überprüfung basierend auf Ersetzungsregeln

Hypothesengenerierung und -überprüfung basierend auf Generierungsregeln
Ausgehend von den ermittelten Konsequenzen können die Generierungsregeln ableiten, welche Ursachen eine Konsequenz überdeckt bzw. erklärt. Überdeckend bedeutet, dass die Generierungsregeln und ihre Ursachen (Vorbedingungen) ausgewählt werden, welche die beobachteten Konsequenzen erklären können. Hierbei kann es zu Mehrfachlösungen kommen, welche dann durch den Benutzer nachzuprüfen sind. Zur Strukturierungshilfe werden die jeweiligen Ursachen eines Ereignisses zusammengefasst. Ist die Vorbedingung erfüllt, ist von einem gefährdenden Ereignis auszugehen.

In der Hypothesengenerierung werden Ursprungs-Konsequenzen, welche in der Merkmalserkennung noch nicht berücksichtigt worden sind, rückwärtsorientiert aktiviert und erhoben. Zur Darstellung von Zustandsänderungen der Konsequenzen werden die logischen Ergebnisse (Konklusionen) in den Vorbedingungen anderer Generierungsregeln als Ursachen verwendet. Die Ursprungs-Konsequenzen bestätigen oder widerlegen somit indirekt deren Folge- bzw. beobachtete Konsequenzen. Um auch weitere mögliche Folge-Konsequenzen zur Hypothesenüberprüfung zu erhalten, werden denkbare Folge-Konsequenzen durch eine vorwärtsorientierte Überprüfungsauswahl der Generierungsregeln vorausgesagt.

Es ist offensichtlich, dass schon bei einer geringen Verknüpfungstiefe der Generierungsregeln die Komplexität sehr schnell ansteigt, besonders wenn Ursprungs- und Folge-Konsequenzen gleichzeitig auftreten. Die damit verbundene indirekte Überprüfung der beobachteten Konsequenz ist dann nicht mehr nachvollziehbar durchzuführen. Aus diesem Grund ist die aufwendige Hypothesenüberprüfung basierend auf komplexen Zustandsänderungen nur auf sensible Sicherheitsbereiche anzuwenden.

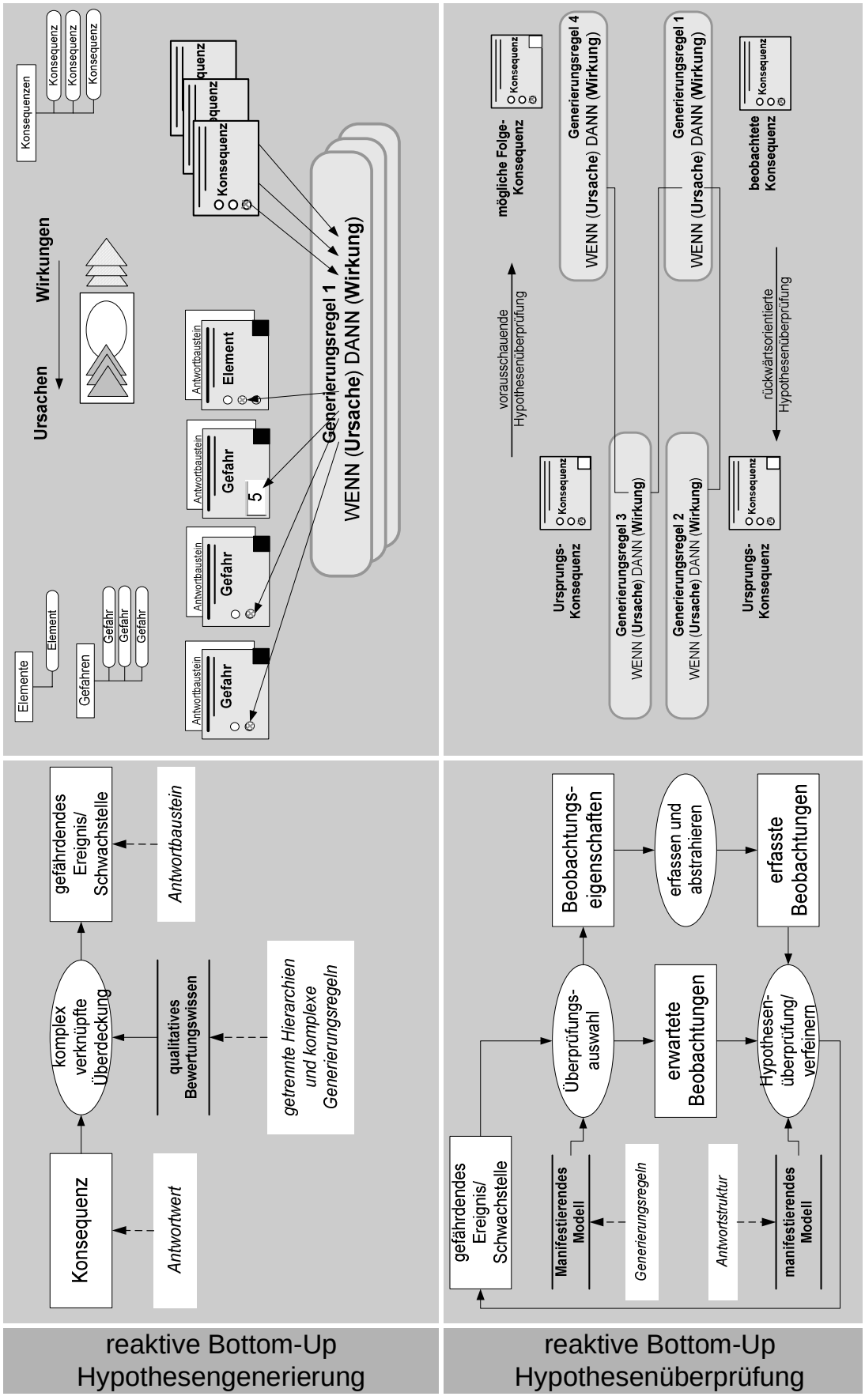


Abbildung 117: Reaktive Bottom-Up Hypothesengenerierung und -überprüfung basierend auf Generierungsregeln

4.3.2.2.2 Präventive Bottom-Up Hypothesengenerierung

Die präventive Hypothesengenerierung basiert auf den gleichen Ersetzungs- und Generierungsregeln der reaktiven Hypothesengenerierung. Die konsequente vorwärtsorientierte Anwendung der Ersetzungs- und Generierungsregeln erlaubt eine kausale Simulation. Ausgehend von angenommenen Ursachen werden deren Konsequenzen vorhergesagt, wobei auch Zustandsänderungen von Konsequenzen berücksichtigt werden können.

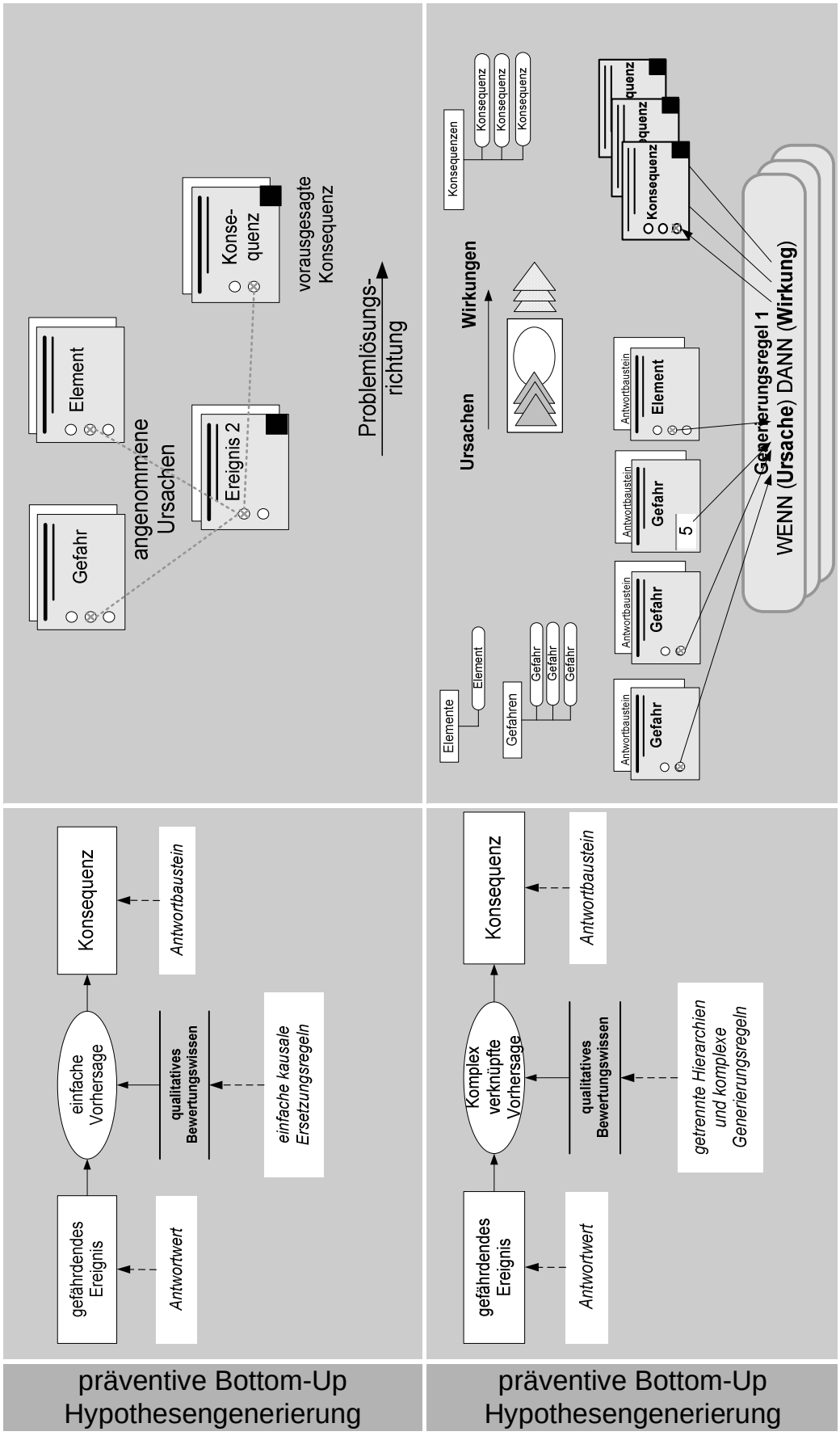


Abbildung 118: Präventive Bottom-Up Hypothesengenerierung

5 Implementierung

Die Implementierung des WBS ist als eine Umsetzung des formalen Entwurfsmodells anzusehen, wobei diese Transformation einen fließenden Übergang des Expertisemodells auf der Wissensebene hin zur Implementierung auf der Symbolebene darstellt. Im Rahmen des KE wird neben dem Begriff „wissensbasiertes System“ auch häufig „Expertensystem“[503] verwendet, wobei eine eindeutige Abgrenzung der Begriffe aufgrund eines „babylonischen Sprachwirrwarrs“ in der Literatur nicht existiert[504]. Diese „Systeme“ lassen sich als informationsverarbeitende Automaten auffassen, die sich wie folgt dadurch auszeichnen, dass:

- *„… der Benutzer den Automaten beauftragen kann, ein Problem zu bewältigen, ohne hierbei zu beschreiben, wie der Automat bei seiner Problembewältigung vorgehen soll (externer Aspekt der non-prozeduralen oder deklarativen Benutzeroberfläche);*
- *der Automat bei seiner Problembewältigung Wissen aus dem betroffenen Problembereich anwendet, das in einer separaten Wissensbasis explizit dargestellt wird (interner Aspekt der Wissensbasierung).“* [505]

In dieser Arbeit werden die Begriffe „wissensbasiertes System“ und „Expertensystem“ basierend auf Kurbels Definitionen wie folgt verwendet:

- ein wissensbasiertes System ist *„... ein Softwaresystem, bei dem das Fachwissen über ein Anwendungsgebiet (‚Domain knowledge’) explizit und unabhängig vom allgemeinen Problemlösungswissen dargestellt wird“* [506] und
- ein Expertensystem ist *„... ein Programm, das in einem eng abgegrenzten Anwendungsbereich die spezifische Problemlösungsfähigkeit eines menschlichen Experten zumindest annähernd erreicht oder übertrifft.“*[507]

Das „wissensbasierte System“ wird in der Arbeit als wissensbasiertes Werkzeug für ein Expertensystem verstanden. Hierdurch wird die softwaretechnologische Ebene mit der expliziten Beschreibung des Wissens in den Vordergrund gestellt[508]. Es ist zu beachten, dass nicht das „eine“ WBS existiert, das mit seinen Repräsentationsformalismen alle Formen von Domänen und deren Wissen verarbeiten kann. Dies wäre ein Versuch, ein GPS nach dem Transferansatz zu entwickeln, bei dem das Problemlösungsverhalten durch vorgegebene Repräsentationsformen bestimmt wird. Vielmehr wird in der Arbeit ausgehend vom Expertisemodell ein geeignetes WBS konstruiert, wobei das Entwurfsmodell eine Zwischenstufe darstellt.

---

[503] XPS = Expertensystem
[504] Vgl. Curth/Bölscher/Raschke (1991), S. 21; Hoppe (1992), S. 6; Bachem (1994), S. 15-18 und Wolfertz (2001), S. 457
[505] Zelewski (1989), S. 16
[506] Kurbel (1991) S. 18
[507] Kurbel (1991) S. 22
[508] Vgl. Kurbel (1992), S. 26

In der folgenden Tabelle werden die wesentlichen Hauptunterscheidungsmerkmale zwischen konventionellen und wissensbasierten Systemen dargestellt. Es ist zu beachten, dass es sich um eine sehr grobe Einteilung handelt; es existiert ein breites Kontinuum zwischen den zwei Extremen.

	Konventionelle Systeme	Wissensbasierte Systeme
Struktur der Wissensbasis und Problemlösungskomponente	Wissensbasis und Problemlösungskomponente sind miteinander verzahnt.	Wissensbasis und Problemlösungskomponente sind weitgehend getrennt.
Form der Problemlösung	Formale, mechanische Algorithmen und Daten sind die Grundlage der Problemlösung. Nur der Programmierer kann die Problemlösung erklären.	Symbolische Repräsentationsformen und „intelligente" Inferenz sind die Grundlage der Problemlösung. Das WBS kann den Problemlösungsprozess erklären (Erklärungskomponente)
Struktur der zu behandelnden Probleme und Wissensformen	Wohl strukturierte Problembereiche meist quantitativer („Number-crunching") Art. Homogen strukturierte Wissenseinheiten. Komplexität entsteht durch Umfang der Massendaten.	Semi- bis schlecht strukturierte Problembereiche. Heterogen strukturierte Wissenseinheiten. Komplexität entsteht durch Reichhaltigkeit der Wissensstrukturen.

Tabelle 20: Zusammenfassung der Unterschiede zwischen konventioneller Datenverarbeitung und WBS[509]

„Wenngleich Expertensysteme meist wissensbasiert konstruiert werden, so liegen die Begriffe doch auf unterschiedlichen Ebenen."[511] Für den Benutzer ist es unerheblich, ob das XPS intern auf wissensbasierten Techniken beruht oder eine „konventionell" programmierte Software darstellt. Entscheidend für die Einordnung eines computergestützten Informationssystems als Expertensystem ist sein nach außen dokumentiertes Problemlösungsverhalten - ähnlich einem menschlichen Experten - für eine bestimmte Domäne[512]. Des Weiteren wird nicht verlangt, ein adäquates kognitives Modell eines Experten zu erschaffen, sondern es wird ein künstliches System „konstruiert", welches angewandt auf einen beschränkten Aufgabenbereich „ähnliche" Resultate erzeugt wie der menschliche Experte.

Da XPS häufig auf Basis von WBS konstruiert werden und somit die Architektur und Problemlösung des WBS übernommen wird, verwischt häufig in der Praxis die Differenzierung zwischen den beiden Systemen, so dass in der Praxis nur noch „ein" System gesehen wird. So haben manche Autoren die Auffassung, dass der Begriff „Expertensystem" in WBS aufgehen sollte[513]. Somit wäre keine differenzierte Bezeichnung zwischen dem Werkzeug bzw. WBS und deren Ergebnisse bzw. XPS möglich. In der Arbeit wird zwischen den beiden Begriffen unterschieden, wobei die Differenzierung z.T. fließend ist. Im Weiteren wird davon ausgegangen, dass ein XPS auf wissensbasierten Techniken beruht.

[509] Vgl. Schönebeck (1994), S. 22 und Hansen/Neumann (2001), S. 471
[511] Kurbel (1992), S. 26
[512] Vgl. Kurbel (1991) S. 26 und Güldenberg (1997), S. 165
[513] Vgl. Busch et al. (1994), S. 4 und Schreiber et al. (2000) S. 6

Einordnung von XPS in Management Support Systeme

MSS[514] werden als Oberbegriff für alle Einsatzformen von Datenverarbeitungs-, Informations- und Kommunikationstechnologien zur Unterstützung des gesamten Unterstützungsspektrums von Managern verstanden[515]. Zusammenfassend lassen sich die Management Support Systeme in drei Gruppen unterteilen:

	Ausprägung und Management Support Systeme
Data Support	Hierunter wird die reine Bereitstellung von Informationen verstanden. Technologisch gesehen wird der Data Support durch Datenbank- und Kommunikationstechnologie realisiert. Schon 1968 hat Ackoff auf die Problematik hingewiesen, dass es nicht zu wenig, sondern eine „Informationsflut" im Unternehmen existiert[516]. Die damaligen MSS waren nicht in der Lage, dem Management ein wirkungsvolles computergestütztes Werkzeug zu bieten[517]. Aus diesen Problembereichen sind die modernen MIS und weitere Formen von MSS entstanden. Moderne MIS zeichnet sich durch einfach ergonomisch gestaltete Benutzeroberflächen aus. Diese Unterstützungsklasse basiert auf Standardfunktionen, die meist in Form von Verknüpfungs- und Verdichtungsoperatoren angeboten werden. In diese Klasse von MSS fallen die Management Information Systems (MIS) und für die Führungsebene vor allem die Executive Information Systems (EIS).
Decision Support	Bei dieser Unterstützungsklasse werden konkrete Entscheidungsprozesse, wie Einzel- oder Gruppenentscheidungen, unterstützt. Decision Support basiert auf computergestützten Methoden und Modellen, die vom Entscheidungsvorbereiter auf das konkrete Entscheidungsmodell angewandt werden. In diese Klassen lassen sich die Decision Support Systems (EUS[518]) einordnen.
Executive Support	Es werden nicht bestimmte Entscheidungen betrachtet, sondern sie sind auf die Entscheidungsträger oder -gruppen und auf den benötigten Informationsbedarf ausgerichtet. Diese Unterstützungsklasse verlangt eine arbeitsplatzindividuelle Kombination aus Data und Decision Support. Diese Systeme oder Konzepte werden als Executive Support Systems (ESS) bezeichnet.

Tabelle 21: Unterstützungsarten für den Manager[519]

Die Funktionen von MSS lassen sich auf Grund der vorhergehenden Betrachtungen in zwei Hauptbereiche einteilen[520]:

- Der informationsorientierte Bereich (durch MIS und EIS) besitzt den Schwerpunkt in der Bereitstellung und Präsentation von internen und externen Informationen.
- Der entscheidungsorientierte Bereich (durch EUS) unterstützt die Phasen des Entscheidungsprozesses.

[514] MSS = Management Support Systeme
[515] Vgl. Gluchowski/Gabriel/Chamoni (1997), S. 65
[516] Vgl. Ackoff (1968)
[517] Vgl. Werner (1992), S. 36
[518] Da das Akronym DSS schon für „Digital Signature Standard" verwendet wird, wird in der Arbeit die deutsche Abkürzung EUS = Entscheidungsunterstützendes System statt für Decision Support Systems =DSS verwendet.
[519] Vgl. Frick (1997), S. 41 und Krallmann (2001), S. 287. Die einzelnen Systeme folgen auch einer historischen Dimension, wobei die frühen Systeme (Dispositions- und Administrationssysteme und MIS, 50er bis 70er Jahre) auf der unteren Ebene und die modernen Systeme (EUS und EIS, 80er bis heute) auf der oberen Ebene zu finden sind. Vgl. Dressler (1997), S. 36 und Alex (1998), S. 29
[520] Vgl. Piechota (1993), S. 85 und Alex (1998), S. 45

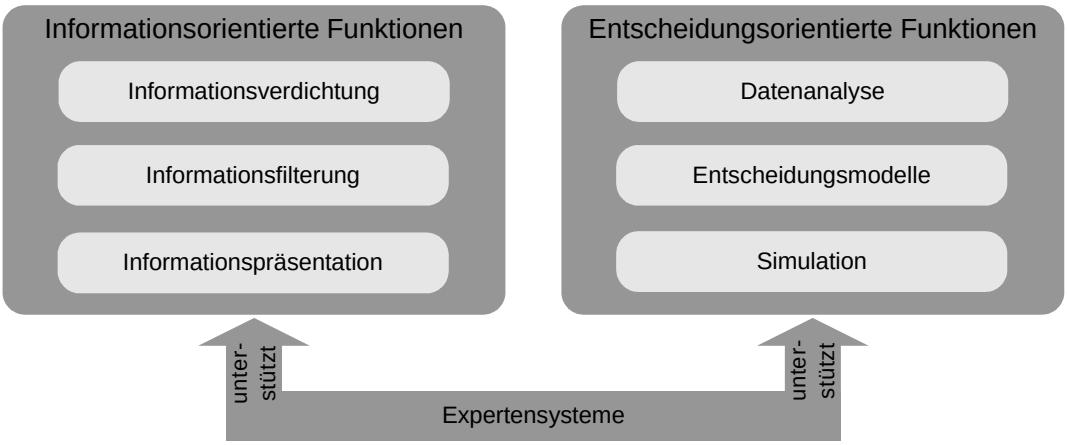


Abbildung 119: Informations- und entscheidungsorientierte Systeme[521]

XPS dienen auch der Entscheidungsvorbereitung und Informationsdarstellung für das IS-Sicherheitsmanagement und können im betriebswirtschaftlichen Bereich[522] somit als ein Management Support System (MSS) bezeichnet werden. Diese zentrale Aufgabe der Entscheidungsunterstützung eines XPS wird durch die empirische Studie von Martin/Subramanian/Yaverbaum (1996) belegt. Auf die Frage, welcher Nutzen von XPS für das Unternehmen zu erwarten ist, ergaben sich die folgenden zusammengefassten Ergebnisse[523]:

- schnellere Entscheidungsunterstützung
- Verbesserung der Produktivität
- Verbesserung der Entscheidungsqualität.

Ein XPS kann ebenfalls eine zusätzliche informationsorientierte Unterstützung anbieten, die vor allem eine verbesserte und gezielte Informationssuche und –analyse als Ziel hat[524].

Eine Differenzierung zwischen XPS und klassischen MSS erfolgt in der Problemlösung und Wissensrepräsentation auf Basis von wissensbasierten Techniken aus der KI, wobei hier die Anwendung von Heuristiken eine entscheidende Rolle innehat. Klassische EUS verwenden zur Problemlösung vorwiegend quantitative Methoden aus dem Bereich der klassischen Datenanalyse (z.B. Operations Research, Statistik und Tabellenkalkulation). Im Unterschied zu EUS besitzen die XPS zusätzlich eine flexible und leistungsfähigere Problemlösungsstrategie, die eine unterschiedliche Bewertung von Alternativen ermöglicht[525]. Eine eindeutige Unterscheidung ist nicht möglich, da wissensbasierte Techniken in modernen MSS immer mehr aufgehen bzw. miteinander gekoppelt werden[526]. Eine besondere Leistungssteigerung wird im Bereich der Entscheidungsunterstützung durch die Ergänzung von EUS durch wissensbasierte Techniken erreicht[527].

[521] In Anlehnung an Alex (1998), S. 47 und Piechota (1993), S. 85
[522] Vgl. Borkowski (2001), S. 193
[523] Vgl. Martin/Subramanian/Yaverbaum (1996), S. 56
[524] Vgl. Gluchowski/Gabriel/Chamoni (1997), S. 256
[525] Vgl. Weißenfluh (1990), S. 176 und Kurbel (1992), S. 171
[526] Vgl. Busch et al. (1994), S.4; Gluchowski/Gabriel/Chamoni (1997) und S. 258 ff.; McNurlin/Sprague (1998), S. 440 und Voß/Gutenschwager (2001), S. 357
[527] Vgl. Werner (1992), S. 142 und McNurlin/Sprague (1998), S. 436

5.1 Architektur und Komponenten von wissensbasierten Systemen

Das Architekturmodell beschreibt in einer abstrakten Form den Aufbau eines wissensbasierten Systems. Für WBS bilden

- die Wissensbasis,
- das Wissenserwerbssystem und
- das Wissensnutzungssystem

den Kern des Systems. Ist die Wissensbasis mit spezifischen Domänenwissen „gefüllt“ und besitzt somit spezifische Problemlösungsfähigkeit, kann von einem XPS gesprochen werden.

In der folgenden Abbildung sind die Komponenten eines WBS zusammenfassend dargestellt.

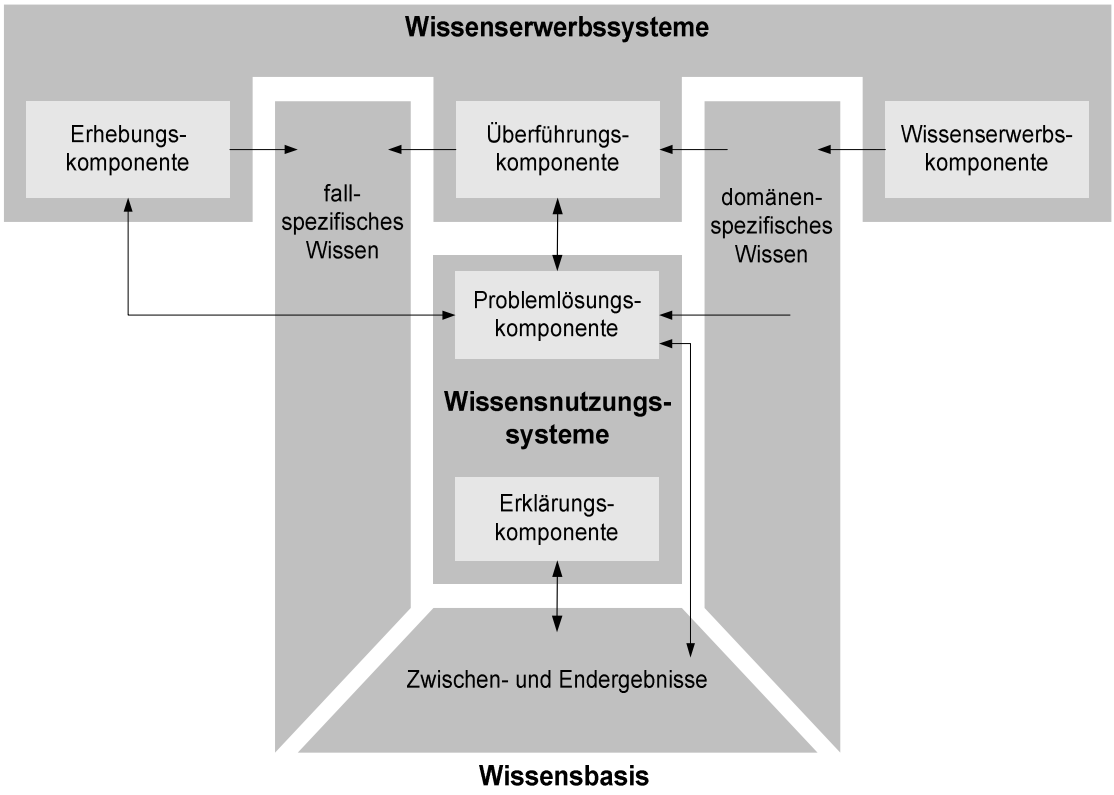


Abbildung 120: Architektur eines wissensbasierten Systems[528]

Erst durch die reibungslose Zusammenarbeit der einzelnen Komponenten kann ein effizientes System entstehen. Es ist von Relevanz, nicht jede Komponente isoliert zu betrachten, sondern auch die Beziehungen zwischen den einzelnen Komponenten zu berücksichtigen. In einem realen System können die logisch getrennten Komponenten zu einem Programm zusammengefasst werden.

[528] Erweitert in Anlehnung an Puppe (1991), S. 13 und Beierle/Kern-Isberner (2000), S. 18

Wissensbasis
Die Wissensbasis besitzt fall- und domänenorientiertes Wissen, das auf Basis der Herkunft differenziert werden kann[529]:

- Domänenspezifisches Wissen (z.B. IS-Sicherheitswissen) wird mit Hilfe der Wissenserwerbskomponente akquiriert. Es repräsentiert das Wissen über ein jeweiliges Aufgabengebiet (z.B. IS-Sicherheit), das auf ein konkretes Problem angewandt wird.
- Das fallspezifische Wissen ist domänenspezifisches Wissen, das an institutionsindividuelle Aspekte angepasst bzw. überführt worden ist. Das angepasste Wissen wird mit fallspezifischen Angaben über ein konkretes Problem ergänzt, die mit Hilfe der Interviewkomponente erhoben werden.
- Zwischen- und Endergebnisse ergeben die abgeleitete Problemlösung basierend auf dem domänen- und fallspezifischen Wissen.

In diesem Zusammenhang wird auch vom dynamischen und statischen Wissen gesprochen. So wird das domänenspezifische Wissen während des Inferenz-Prozesses weitgehend nicht verändert und besitzt deshalb eine statische Form[530], wohingegen das fallspezifische Wissen dynamisch ermittelt wird. Die Zwischenergebnisse haben eine dynamische Natur, da sie situationsbedingt abgeleitet werden[531].

Wissenserwerbssysteme
Die Qualität eines WBS und der Erfolg im praktischen Einsatz werden entscheidend durch den Aufbau der Wissensbasis und ihrer Unterstützung durch die Wissenserwerbskomponente geprägt[532]. Insbesondere die direkte Wissenseingabe und Wartung durch einen Fachexperten ohne Unterstützung eines Knowledge Engineers ist ein Ansatz, um Experten aktiv in die Entwicklung und Nutzung von WBS langfristig einzubinden[533]. Es lassen sich folgende Wissenserwerbssysteme differenzieren:

- Die Wissenserwerbskomponente ermöglicht primär den Aufbau und die Erweiterung des Domänenwissens unter Verwendung von adäquaten Formalismen der Wissensrepräsentation. Es handelt sich i.d.R. um intelligente und eventuell grafische Editoren, die eine syntaktische und semantische Prüfung der Eingaben vornehmen und die Erstellung von Abhängigkeiten der Wissenselemente ermöglichen.
- Die Überführungskomponente ermöglicht, das Domänenwissen an eine spezifische Institution anzupassen. Der Überführungsgrad kann in Abhängigkeit der jeweiligen Repräsentationsform variieren. So werden bei einem wissensbasierten Fragenkatalog die benötigten Bereiche mit geringem Anpassungsaufwand direkt angewendet, wohingegen die Anpassung bei objektorientierten Systemmodellen an ein konkretes Informationssystem umfangreicher ist.
- Die Erhebungskomponente bildet die Schnittstelle für den Dialog zwischen Endbenutzern mit dem System. Durch die Interviewkomponente werden Informationen über einen be-

[529] Vgl. Puppe (1991), S. 12
[530] Es ist zu beachten, dass domänenspezifisches Wissen nur während des Inferenz-Prozesses in statischer Form vorliegt. Domänenspezifisches Wissen kann während der Wissenserwerbs- und Wartungsphase verändert werden und besitzt somit auch eine dynamische Komponente.
[531] Vgl. Gabriel (1992), S. 41
[532] Vgl. Kirchhoff (1994), S. 2 ff.
[533] Vgl. Puppe/Stoyan/Studer (2000), S. 616

stimmten Problemfall erhoben bzw. erfragt. Insbesondere wenn es sich um keinen versierten Computerexperten handelt, ist es erforderlich, dass sich die Interviewkomponente intuitiv bedienen lässt und eine umfangreiche Hilfeleistung anbietet. Bei der Erhebungskomponente steht die Dialoggestaltung - wie Fenstertechnik, maus-sensitive Dialogsteuerung in Verbindung mit pop-up/pull-down -Menüs usw. - im Vordergrund.

Wissensnutzungssysteme
Die Wissensnutzungssysteme werten das domänen- und fallspezifische Wissen aus und steuern dessen Auswertung. Das Nutzungssystem ist eng mit der Erhebungs- und Überführungskomponente verbunden. Im klassischen Sinn besitzt die Problemlösungskomponente eine Interpretationsaufgabe des Domänen- und Fallwissens, wie z.B. durch Vorwärts- und Rückwärtsstrategien in der Auswertung von Regeln. Die Problemlösungskomponente in modernen Systemen repräsentiert zudem einen bestimmten Problemlösungstypen und dessen Problemlösungsstrategien. Die Komponente bestimmt somit auch Aufgabenziele der Problemlösung, z.B. einer Diagnoseaufgabe.

Die Erklärungskomponente leistet die Rekonstruktion und Darstellung der Schlussfolgerungsprozesse der Problemlösungskomponente für Benutzer und Experten. Diese Komponente hat einen optionalen Charakter, ist aber für die Akzeptanz des Expertensystems von entscheidender Bedeutung. Der Benutzer soll immer in der Lage sein, die Ergebnisse und Zwischenergebnisse nachzuvollziehen und auch überprüfen zu können[534].

5.2 Vorstellung von ausgewählten Realisierungsmöglichkeiten

In Stelzer (1993), Münch (1995), Ozier (1999) und Thoben (2000) werden mehrere beratungsunterstützende Werkzeuge für die IS-Sicherheit genannt und z.T. diskutiert. Die quantitativ orientierten Werkzeuge unterstützen meist Risikoanalysemodelle, die sich auf monetäre und andere kardinale Werte beschränken. Diese Werkzeuge unterstützen meist quantitative Methoden der klassischen Datenanalyse und lassen sich dem „klassischen“ MSS oder dem „Number-cruncher“ System zuordnen. Die qualitativen Werkzeuge basieren auf computergestützten bzw. konventionellen Fragebögen, die sich häufig auf einfach strukturierte Ja/Nein-Fragen beschränken. Hierbei stellen die Ergebnisse zwar eine Arbeitsgrundlage dar, die eigentliche Problemlösung erfolgt aber weiterhin durch den Fachexperten[535]. Die meisten Werkzeuge, die Stelzer (1993) und Thoben (2000) untersucht haben, stammen aus der zweiten Hälfte der 80er Jahre und können z.T. nicht als WBS bzw. XPS bezeichnet werden, da sie nicht auf wissensbasierten Techniken des KE basieren[536]. Im Folgenden werden weitere Werkzeuge exemplarisch vorgestellt, welche die Ansätze des IS-Sicherheitsmanagements unterstützen.

[534] Vgl. Gabriel (1992), S. 74f.; Kurbel (1992), S. 29 und Mertens/Borkowski/Geis (1993), S. 4
[535] Vgl. Kapitel 1.2
[536] Vgl. Stelzer (1993), S. 150

RAMeX[537]

RAMeX[538] ist ein Prototyp für ein Expertensystem zur Unterstützung der Risikoanalyse. Die Wissensbasis besteht im Wesentlichen aus den Risikofaktoren: sicherheitsrelevantes Element[539], Gefahrentyp[540], Gefahrenquelle[541], Schwachstelle[542] und Gegenmaßnahme[543] sowie Assoziationen zwischen den Risikofaktoren. Zuerst erfolgt eine Erhebung der sicherheitsrelevanten Elemente und Gefahren (Gefahrentypen und Gefahrenquellen) bezüglich der zu analysierenden Institution. Auf Basis der erhobenen Informationen wird im Folgenden die Institution auf mögliche Schwachstellen hin untersucht. Die folgende Abbildung ist ein Beispiel für eine Zuordnung eines sicherheitsrelevanten Elementes der Gefahren und Schwachstellen.

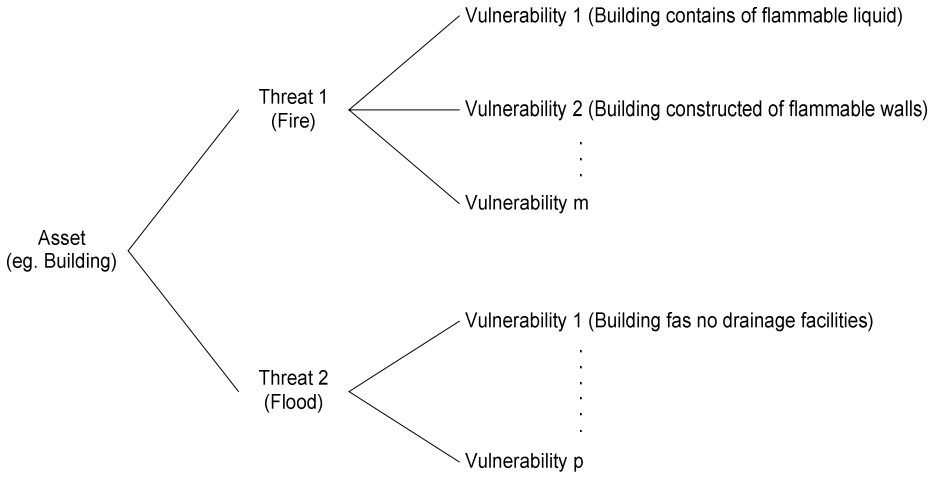


Abbildung 121: Zuordnung zwischen einem sicherheitsrelevanten Element, der Gefahren und Schwachstellen[544]

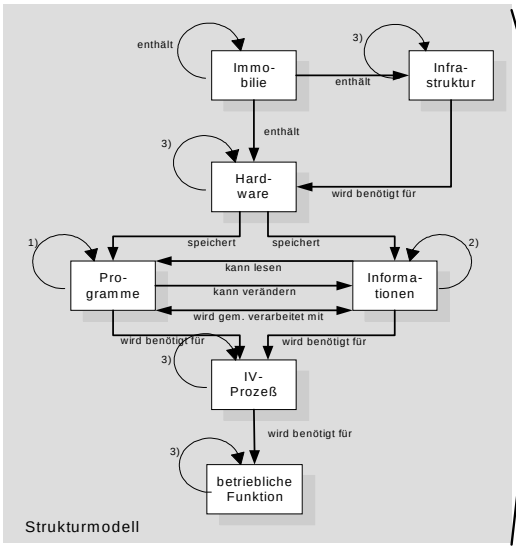
Werden die Schwachstellen für die zu untersuchende Institution als zu „vernachlässigen" eingestuft bzw. bewertet, werden die Risikofaktoren nicht weiter betrachtet. Sind die Schwachstellen für die Institution von Interesse, so werden diese qualitativ bewertet (very low, low, medium, high und very high). Der Bewertung liegen z.B. der Verlust von Verkäufen, Verlust von Kundenzufriedenheit oder Reputationsverlust zugrunde. In welcher Form die Bewertung durchgeführt werden soll, wird nicht weiter beschrieben. Werden durch den Benutzer die vorhandenen Maßnahmen als ausreichend für die ermittelten Schwachstellen eingeschätzt, so werden die entsprechenden Risikofaktoren nicht weiter betrachtet. Sind keine oder ungenügende Gegenmaßnahmen vorhanden, erfolgt für die Risikofaktoren eine qualitative Abschätzung der zu erwartenden Konsequenzen. Im letzten Schritt werden die benötigten Gegenmaßnahmen zur Verhinderung der Konsequenzen abgeschätzt. In einem Ergebnisreport wird der IS-Sicherheitsstatus der Organisation bzgl. der Risikofaktoren ausgegeben und es werden Vorschläge für Gegenmaßnahmen und deren Implementierung angeboten.

[537] Vgl. Kailay/Jarratt (1995)
[538] RAMeX = Risk Analysis and Management eXpert system
[539] Engl.: Asset
[540] Engl.: Threat Type
[541] Engl.: Threat Source
[542] Engl.: Vulnerability
[543] Engl.: Countermeasure
[544] Vgl. Kailay/Jarratt (1995), S. 457

Der RAMeX-Prototyp wurde mit dem regelbasierten Expertensystem-Shell Crystal[545] erstellt. Die Inferenz-Einheit verfügt über eine vorwärts- und rückwärtsorientierte Verarbeitung der Regeln, wodurch eine datengetriebene Analyse und eine zielgetriebene Analyse der Regeln möglich ist. Es existiert eine Schnittstelle für den Knowledge Engineer (Crystal Environment), der die Wissensbasis mit den Risikofaktoren und deren Regeln auffüllt sowie eine Benutzerschnittstelle, die auf einer strukturierten Befragung der relevanten Daten basiert.

Ansatz von Stelzer

Ein Konzept einer kombinierten objektorientierten und regelbasierten Wissensrepräsentation von IS-Sicherheitswissen wird in der Dissertation von Stelzer (1993) vorgestellt. Im Objektmodell werden Gefahren, sicherheitsrelevante Elemente und gefährdende Ereignisse mit Hilfe von Objekten und deren Attributen und Methoden dargestellt. Die Objekte werden in Form von Instanzen aus Klassen gebildet. So kann das Objekt „PC“ aus der Klasse „Hardware“ oder das Objekt „Anwendungssoftware“ aus der Klasse „Software“ instanziiert werden. Die folgende Tabelle basiert auf dem Konzept von Stelzer und stellt einen Ausschnitt für benötigte Objekte einer objektorientierten Wissensrepräsentation dar.



Aspekte der Realwelt	Darstellung im System	Attribute	Quellen der Attributwerte
Gefahren	Objekte	Name	im System vorgegeben
		Gefahrenquellen	im System vorgegeben
		betroffene Elementklassen	im System vorgegeben
sicherheits-relevante Elemente	Objekte	identifizierende Attribute	Benutzereingabe
		Beziehungsattribute	Benutzereingabe
		relevante Gefahren	im System vorgegeben
		realisierte Sicherungs-maßnahmen	Benutzereingabe
		bekannte Schwachstellen	Benutzereingabe
gefährdende Ereignisse	Objekte	aktuelle Gefahr	Ermittlung durch das System
		identifizierende Attribute und Klassen des betroffenen Systems	Ermittlung durch das System
		realisierte Sicherungs-maßnahmen	Ermittlung durch das System
		bekannte Schwachstellen	Ermittlung durch das System
		primäre Konsequenzen	Ermittlung durch das System

Abbildung 122: Objektmodell nach Stelzer[546]

Im Objektmodell werden

- Gefahren, sicherheitsrelevante Elemente und gefährdende Ereignisse als Objekte repräsentiert und
- Schwachstellen, Maßnahmen und Konsequenzen als deren Attribute und Methoden dargestellt.

[545] Vertrieben durch Intelligent Environments Ltd. (UK)
[546] Verkürzte Darstellung aus Stelzer (1993), S. 207 und S. 214

Eine eindeutige Zuordnungsvorschrift der Konzepte als Objekt oder Attribut kann nicht abschließend definiert werden. So können z.B. Maßnahmen oder Konsequenzen in Form von Attributen einem sicherheitsrelevanten Element zugeordnet oder als eigenständige Objekte repräsentiert werden. Stelzer hat in seiner Arbeit die Vor- und Nachteile der Zuordnung von den jeweiligen IS-Sicherheitskonzepten als Objekte oder Attribute beschrieben.

Das Konzept von Stelzer besitzt die wesentlichen Merkmale einer „klassischen" Systemabgrenzung und Risikoerkennung im Rahmen einer Risikoanalyse. Durch ein Strukturmodell erfolgt eine „Systemabgrenzung" des zu analysierenden Informationssystems. Das Strukturmodell repräsentiert die sicherheitsrelevanten Elemente und deren Beziehungen (z.B. „ist Teil von" oder „ist gespeichert auf") und bildet somit die Basis für das Gefährdungsmodell. Mit Hilfe der Gefährdungsanalyse wird die Risikoerkennung durch Wirkungs- und Ursachenanalyse unterstützt. Die Risikobewertung im klassischen Sinne wird durch den Ansatz nicht unterstützt[547].

Das Konzept wurde teilweise in dem Beratungsunterstützungssystem NASYS (früher ASIS) von Siemens-Nixdorf AG umgesetzt, wobei wichtige Aspekte des Konzepts, wie z.B. die Visualisierung von Objekten, nicht berücksichtigt wurden[548].

GPOOS

Eine Weiterentwicklung des Ansatzes von Stelzer bildet die simulationsbasierte Risikoanalyse GPOOS[549] von Konrad (1998). GPOOS hat als Inhalt die semi-formale Modellierung und inkrementelle Simulation sicherheitsrelevanter Zusammenhänge sowie die explizite Einbeziehung von Geschäftsprozessen in Verbindung mit einer visualisierten Darstellung des Untersuchungsmodells und Simulationsergebnisses. GPOOS wurde in ein prototypisches Simulationswerkzeug (SIMSI[550]) umgesetzt, welches auf Microsoft Visual Basic basiert. Dieses Simulationsmodell bzw. das Werkzeug unterstützt die Risikoanalyse in Verbindung mit Geschäftsprozessen, indem das Verhalten eines Systems auf Risiken bzw. Bedrohungen und den Einsatz von Maßnahmen simuliert wird. Auch hier wurde die Risikobewertung nur unzureichend unterstützt, was ein grundsätzliches Problem von wissensbasierten Risikoanalysetools ist[551].

TRAW

Eine weitere wissensbasierte Risikoanalyse für workflowbasierte Anwendungssysteme hat Thoben (2000) realisiert. Das zentrale Ziel von TRAW[552] ist, das Risiko-Management mit der Entwicklung workflowbasierter Anwendungssysteme zu koppeln, um somit einen Aufbau von sicheren workflowbasierten Anwendungssystemen zu unterstützen[553]. Ein System-Metamodell definiert ein konkretes Systemmodell durch Systemelementtypen und beschreibenden Attributtypen, das selbst die Basis für die Modellierung eines spezifischen Anwendungssystems darstellt. Das Systemmodell wird in ein konkretes Anwendungssystem überführt, indem konkrete Systemelemente, Sicherheitsmechanismen sowie deren Beziehungen festgelegt werden.

---

[547] Vgl. Stelzer (1993), S. 321
[548] Vgl. Konrad (1998), S. 131
[549] GPOOS = Geschäftsprozeß-orientiertes Simulations-System
[550] SIMSI = SIMulation von InformationsSIcherheit
[551] Vgl. Damm et al. (1999), S. 76
[552] TRAW = Knowledge Based Threat and Risk Analysis of Workflow-Bases Applications
[553] Vgl. Thoben (2000), S. 271

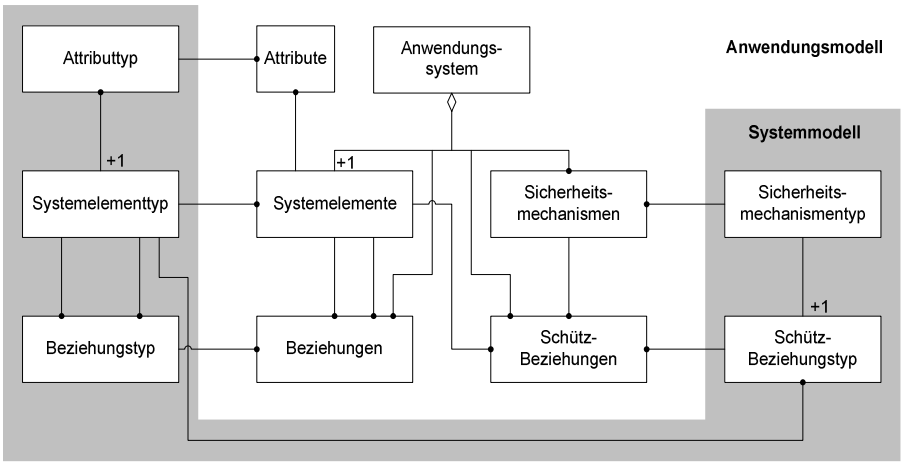


Abbildung 123:System-Metamodell[554]

Für die Risikoanalyse wird ein Risikomodell verwendet, das z.T. auf dem Systemmodell beruht. Im Risikomodell werden zusätzlich sicherheitsspezifische Aspekte berücksichtigt, welche nötig sind, um eine konkrete Risikoanalyse durchzuführen. In der folgenden Abbildung sind das Risikomodell und eine zusätzliche Beispielextension angegeben.

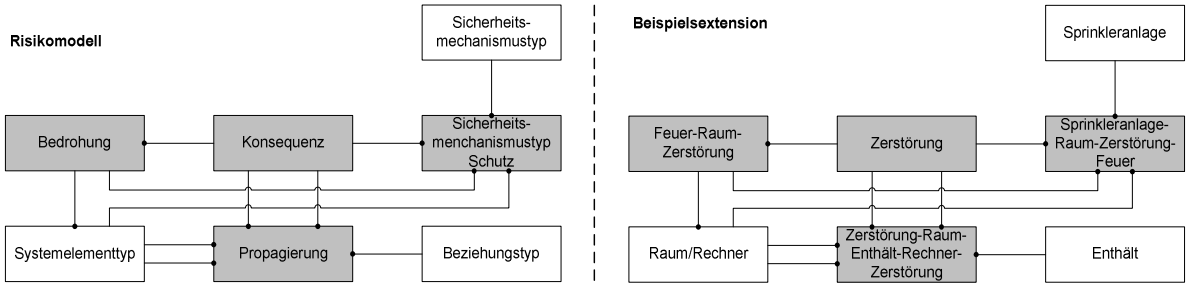


Abbildung 124: Risikomodell und Beispielsextension[555]

Anhand des Konzepts wurde das Werkzeug TRAW^T entwickelt, das dem Anwender ermöglicht, Systemmodelle von Anwendungssystemen grafisch zu modellieren sowie Sicherheitsanforderungen zu spezifizieren. Das Systemmodell wird durch die grafischen Meta-Editoren ILOG Views und ASSUME erstellt. Basierend auf dem Systemmodell und den Sicherheitsanforderungen können Analysen durchgeführt werden. Die struktur- und ablauflogikorientierten Sicherheitsanforderungen wurden mit Hilfe von BinProlog umgesetzt, wobei der Hauptteil des Werkzeugs durch die Programmiersprache C++ implementiert worden ist. Zusätzlich ermöglicht das Werkzeug unscharfe Risikobewertungen mit Hilfe der Fuzzy-Technologie, welche durch die Fuzzy-Bibliothek StarFLIP++ implementiert worden ist. Zur Datenhaltung wird das Oracle DBMS verwendet.

[554] Vgl. Thoben (2000), S. 117
[555] Vgl. Thoben (2000), S. 155 und S. 156

RSD-Expertensystem

An der Universität Zürich wurde im Rahmen des Projektes SINUS[556] ein XPS zur Unterstützung der sicheren Nutzung von Online-Diensten entwickelt. Das XPS soll die Entwicklung einer Internet-Sicherheitskonzeption unterstützen, die auf einem Rapid Secure Development Konzept (RSD) basiert. Das RSD-Konzept umfasst folgende fünf Prozessschritte[557]:

- Nutzungskonzeption: Ermittlung der funktionalen Anforderungen durch Szenarien.
- Dienstauswahl: Ermittlung der Dienste und Protokolle, die für die Anforderungen benötigt werden.
- Risikoanalyse: Basierend auf den Nutzungsszenarien und den ermittelten Online-Diensten werden Bedrohungen und Schwachstellen hergeleitet.
- Maßnahmen: Ermittlung von geeigneten Maßnahmen, um vor Risiken zu schützen.
- Realisierung: Gestaltung und Einsatz der erforderlichen Maßnahmen.

Für jede Phase des RSD wurde ein Frame entwickelt, das wiederum die oben beschriebenen Objekte (wie Gefahr oder Dienste) beinhaltet. Die Gemeinsamkeiten von Szenarien, Diensten, Gefahren, Gegenmaßnahmen und Realisierungsmaßnahmen werden als Frame zusammengefasst. Jede Phase kann erst begonnen werden, wenn die vorhergehende beendet ist, wobei der konkrete Endzustand einer Phase mit Hilfe von LISP-Funktionen ermittelt wird. Das Expertensystem verfügt darüber hinaus über eine Erklärungskomponente für jede Phase.

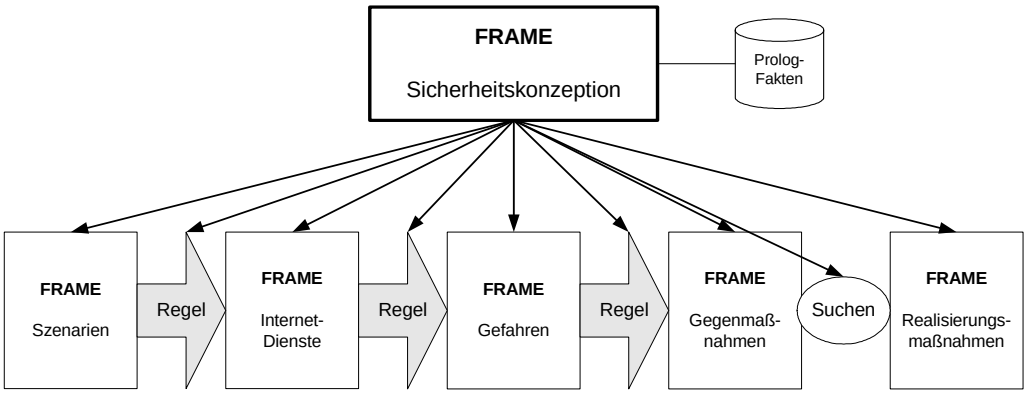


Abbildung 125: Phasen des RSD[558]

Alle Objekte werden zu Beginn einer Überprüfung instanziiert. Die benötigten Objekte werden anschließend durch den Benutzer oder das System nach Bedarf der Situation referenziert bzw. aktiviert. Die Aktivierung der Instanzen - sowie das Wissen, das beschreibt, durch welche Ursprungsinstanz die Aktivierung erfolgte - wird in einer Prolog-Faktenbasis dokumentiert.

Die Risikoanalyse und -bewertung basiert auf einer kardinalen Risikobewertung, indem der Vermögenswert mit der Häufigkeit des Schadeneintritts multipliziert wird. Die Bestimmung der Vermögenswerte wird nicht durch das Expertensystem unterstützt, sondern es werden

[556] SINUS = Sichere Nutzung von Online-Diensten. Projektinformationen veröffentlicht im Internet, URL: http://www.ifi.unizh.ch/ikm/SINUS/publications.html (Stand: 10.12.2002)
[557] RSD (1999), S. 48-49
[558] Vgl. RSD (1999), S. 48 und S. 148

schon ermittelte Werte vorausgesetzt. Als Ergebnis werden die Risiken der einzelnen Dienste berechnet, die in Relation zueinander in einer Matrix gesetzt werden. Auf den Achsen sind jeweils der Vermögenswert und die Häufigkeit des Schadeneintritts skaliert. Die Wahrscheinlichkeiten basieren auf Studien von Cohen, des DoD (Departement of Defense) und AIFCW (Air Force Information Warface Center)[559]. Diese Angaben werden aber von den Entwicklern kritisch bewertet[560].

Für die Implementierung des RSD-Expertensystems wurde das EMA-XPS der Universität Wuppertal verwendet. Das hybride EMA-XPS ist ein frei verfügbares grafisches Expertensystemwerkzeug. Es ergänzt die hybride wissensverarbeitende Sprache Babylon[561] der Gesellschaft für Mathematik und Datenverarbeitung (GMD), um eine grafische Oberfläche auf der Basis von X-Windows zu erstellen. Babylon wurde auf Basis der KI-Sprache CommonLISP entwickelt.

Case-Based Reasoning

Jung/Han/Suh (1999) haben ein Case-Based Reasoning (CBR) auf Basis der Risikoanalyse entwickelt. Hierfür wurde der CBR-Prozess für die Risikoanalyse angepasst, indem das menschliche „Nachdenken“ durch die Funktionen „Erinnern“, „Anwenden“ und „Lernen“ beschrieben wird. Durch die Erinnerungsfunktion werden auf Basis eines aktuellen Falles ähnliche Fälle in der Wissensbasis gesucht. Falls entsprechende Fälle gefunden werden, können deren Lösungen möglicherweise für den aktuellen Fall angewandt werden. Durch die Lernfunktion wird die Wissensbasis um weitere (neue) Fälle und deren Lösungen erweitert.

[559] Vgl. Damm et al. (1999), S. 67-68
[560] Vgl. Damm et al. (1999), S. 74
[561] BABYLON wurde von Primio (1993) beschrieben.

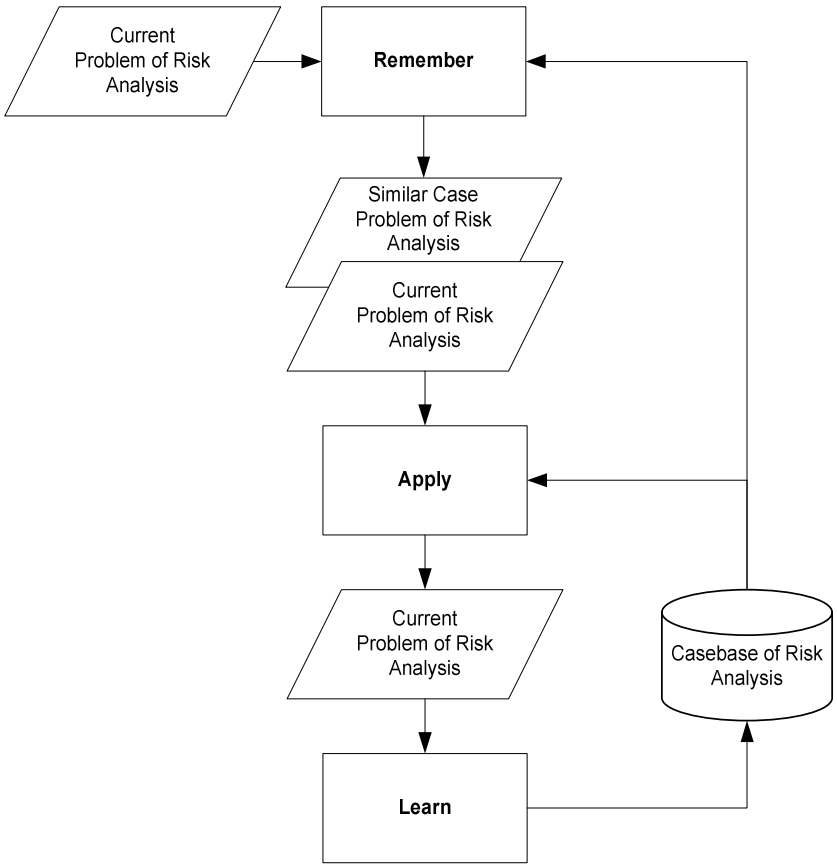


Abbildung 126: CBR-Prozess angepasst an die Risikoanalyse[562]

Die Risikoanalyse wurde weiterhin für den Bereich Electronic Commerce erweitert, so dass auch das CBR-System auf diesen Problembereich anzuwenden ist. Durch das System werden aktuelle Vorfälle mit historischen Vorfällen verglichen und falls Überschneidungen existieren, können die schon vorhandenen Lösungen des „alten" Falls verwendet werden. Hierfür ist es nötig, historische und aktuelle Fälle in einer Wissensbasis zu repräsentieren. Für den Vergleich zwischen historischen und aktuellen Fällen wird das Klassifikationsverfahren „single linkage" bzw. „nearest neighbour" aus der numerischen Taxonomie verwendet[563].

Durch den Problemlösungsvorgang mit Eingabe von neuen Vorfällen und deren Vergleich mit alten Vorfällen werden die wesentlichen Merkmale eines neuen Vorfalles in der Wissensbasis gespeichert und können wiederum für spätere Auswertungen verwendet werden. Die sicherheitsrelevanten Aspekte bzw. Merkmale der Vorfälle, die schon aus der Risikoanalyse bekannt sind und mit Aspekten des Electronic Commerce erweitert worden sind, werden durch Regeln und Frames repräsentiert.

Common Criteria[564]-Toolbox (CC-Toolbox)

Die Toolbox unterstützt einen automatisierten Prozess, um IT-Sicherheitserfordernisse in Verbindung mit der Common Criteria zu identifizieren. Dies ist insbesondere bei der Ermittlung von Schutzprofilen (Protection Profile = PP) für die zu erstellende Software-Produktentwicklung nützlich. Schutzprofile auf Basis von CC-Kriterien bieten eine anerkannte Lösung zuzüglich Erklärungen für Standard-Sicherheitsprobleme einer Produktgruppe. Sie

[562] Vgl. Jung/Han/Suh (1999), S. 65
[563] Vgl. dazu auch Opitz (1980), S. 87 ff.
[564] Vgl. CC-Teil 1 (2000); CC-Teil 2 (2000) und CC-Teil 3 (2000)

sind zunächst implementierungsunabhängig, können aber durch die daraus ableitbaren Sicherheitsvorgaben (Security Target = ST) auf einen konkreten Evaluationsgegenstand (EVG) zugeschnitten werden. Damit können beispielsweise Wirtschafts- und andere Interessensverbände ihre Vorstellungen und Bedürfnisse bezüglich der Sicherheit bestimmter IT-Produktgruppen (z.B. Firewalls, Chipkartenanwendungen) in Form von Schutzprofilen ausdrücken und weltweite Standards setzen[565].

Durch die CC-Toolbox werden Berichte von Sicherheitserfordernissen basierend auf den Vorgaben der CC erstellt. Es werden allgemeine PP-Berichte (Schutzprofilberichte) erstellt, welche eine implementierungsunabhängige Menge von Sicherheitsanforderungen darstellen. Sicherheitsvorgaben eines ST-Berichtes enthalten angepasste und implementierungsabhängige Sicherheitsanforderungen für einen konkreten EVG. Hierbei lässt sich ein PP-Bericht leicht in einen ST-Bericht überführen, da beide Berichtsformen auf dem gleichen Berichtsmodell basieren. In der folgenden Abbildung ist die Grundstruktur der Berichte dargestellt.

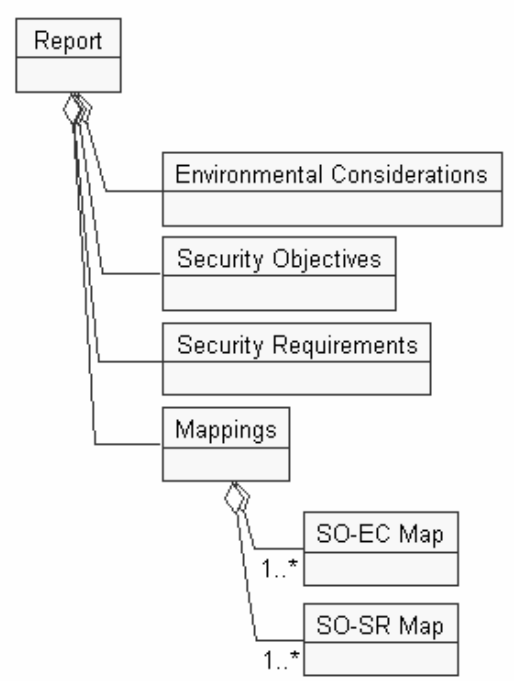


Abbildung 127: Grundstruktur der Berichte[566]

Sicherheitsumgebung (Environmental Considerations): In diesem Teil des Schutzprofils sollen die Sicherheitsaspekte der beabsichtigten Einsatzumgebung und die erwartete Art der Nutzung des EVG beschrieben werden. In einem Schutzprofil werden die Annahmen, die Bedrohungen und die organisatorische Sicherheitspolitik (also die Sicherheitsumgebung) den angestrebten Sicherheitszielen (Security Objectives) gegenübergestellt. Dieser Zusammenhang (Security Objectives und Environmental Considerations) wird durch ein SO-EC Map abgebildet.

Sicherheitsziele (Security Objective): Die Sicherheitsziele des EVG sollen in ihrer Einsatzumgebung definiert werden. Die Sicherheitsziele müssen detaillierte Angaben darüber machen, wie den Bedrohungen entgegengewirkt werden soll bzw. wie die Sicherheitspolitik er-

[565] Vgl. CC-Kurz (2001)
[566] Vgl. CC-Tool-User Manual, Kapitel Introduction

füllt werden soll. Für eine relevante Bedrohung bzw. für jede Sicherheitspolitik wird mindestens ein Sicherheitsziel empfohlen. Um die Definition der Sicherheitsumgebung zu unterstützen, werden vordefinierte Politiken, Bedrohungen, Annahmen und Sicherheitsziele (Predefined Data) in der CC-Toolbox mitgeliefert. Die Erhebung der erforderlichen Informationen erfolgt durch Interview-Fragen.

Sicherheitsanforderungen (Security Requirements): Hier werden die Anforderungen an die Funktionalität und an die Vertrauenswürdigkeit definiert, denen der EVG genügen muss, damit die Sicherheitsziele erfüllt werden. Es wird zunächst auf die Anforderungen der CC zurückgegriffen. Bei Bedarf können auch Anforderungen frei formuliert werden. Der Zusammenhang zwischen Security Objective und Security Requirements wird durch die SO-SR Map abgebildet.

Die CC-Toolbox wurde durch das Unternehmen Sparta für die National Security Agency (NIST) mit der Programmsprache Java entwickelt und ist kostenlos erhältlich[567].

BSI Tool IT-Grundschutz

Auf Basis des BSI-Grundschutzhandbuchs wurde durch die CSC Ploenzke AG ein BSI Tool IT-Grundschutz (kurz: BSI Tool) entwickelt, das die Erstellung eines Grundschutzkonzepts unterstützen soll[568]. Dieses Tool wurde in Java implementiert und besitzt Interbase Server 5.0 als Datenbank. Das Tool unterstützt alle Phasen des IT-Grundschutzhandbuchs von der Schutzbedarfsfeststellung bis zur Konzepterstellung. Das Tool bietet die Möglichkeit, gleichzeitig mehrere Sicherheitskonzepte zu verwalten. In der folgenden Tabelle ist zusammenfassend dargestellt, wie die einzelnen Funktionen des IT-Grundschutzhandbuchs durch das Tool unterstützt werden.

[567] Die CC-Toolbox kann unter der URL: http://niap.nist.gov/tools/cctool.html (Stand: 10.10.2002) bezogen werden.

[568] Informationen zum BSI Tool wird unter der URL: http://www.bsi.gstool/index.htm (Stand: 10.10.2002) veröffentlicht.

BSI-Grundschutzhandbuch	BSI Tool IT-Grundschutz
Erfassen der IT-Systeme	Eintragen der IT-Systeme in einen Hierarchiebaum.
Erfassen der Anwendungen	Zuordnung der Anwendungen zu IT-Systemen.
Schutzbedarf der Anwendung	Detaillierten Schutzbedarf der Anwendungen eintragen.
Schutzbedarf des IT-Systems	Automatische Erzeugung des Schutzbedarfs für das IT-System nach dem Maximumprinzip; Möglichkeit der manuellen Änderung.
Grundschutz der Risikoanalyse	Durch die farbige Kennzeichnung der IT-Systeme mit hohem oder sehr hohem Schutzbedarf bzw. dem Einsatz eines entsprechenden Filters werden IT-Systeme, die eine Risikoanalyse benötigen, hervorgehoben oder ausgeblendet.
Maßnahmen ermitteln	Die vorgesehenen Maßnahmen werden den IT- Systemen automatisch zugeordnet.
Redundanzen und Verknüpfungen feststellen	Durch übergeordnete Komponenten können übergeordnete Strukturen abgebildet werden. Durch Verweise auf Bausteine anderer IT-Systeme oder übergeordnete Komponenten werden Redundanzen aufgelöst.
Soll-/Ist-Vergleich	Zu jeder bearbeitenden Maßnahme werden die Bearbeitungsdaten aufgenommen, Berichte unterstützen die Erfassung des Ist-Zustandes.
Maßnahmenkatalog	Über Berichte wird die Zusammenstellung der noch zu realisierenden Maßnahmen unterstützt.
Aufsetzen des Sicherheitsmanagements	Zu den Bearbeitungsdaten der Maßnahmen gehören auch die Verantwortlichkeiten, denen durch entsprechende Berichte Aufgaben zugeteilt werden.

Tabelle 22: Übersicht der unterstützten Funktionen betreffend des BSI-Grundschutzhandbuchs durch das BSI-Tool[569]

Durch das BSI-Tool werden das Sicherheitswissen und die Problemlösung des BSI-Grundschutzhandbuchs auf ein computergestütztes System übertragen. Die erfassten IT-Systeme werden von vordefinierten IT-System Typen abgeleitet und durch einen Hierarchiebaum strukturiert. Den IT-System Typen sind bereits die erforderlichen Maßnahmen zugeordnet, die analog zu dem IT-Grundschutzhandbuch zu Bausteinen zusammengefasst werden, wobei ein IT-System mehrere Bausteine beinhalten kann. Da im Sicherheitskonzept redundante Maßnahmen auftauchen (ein Baustein ist in mehreren IT-Systemen vertreten), werden diese Bausteine mit Hilfe von „übergeordneten Komponenten“ verwaltet. Es besteht auch die Möglichkeit, nachträglich benutzerdefinierte IT-System Typen und Bausteine zu erstellen. Jedem IT-System können zusätzlich Informationen über seinen Standort, dessen Vernetzung und den Benutzer angegeben werden. Den IT-Systemen werden Anwendungen zugeordnet, wobei als Anwendung die Fachaufgabe und nicht das Programm angesehen wird. Für die Anwendungen wird der Schutzbedarf (von niedrig bis sehr hoch) ermittelt, wobei dieser auch manuell eingegeben werden kann.

[569] Vgl. BSI-Tool Benutzerhandbuch (1999), S. 10

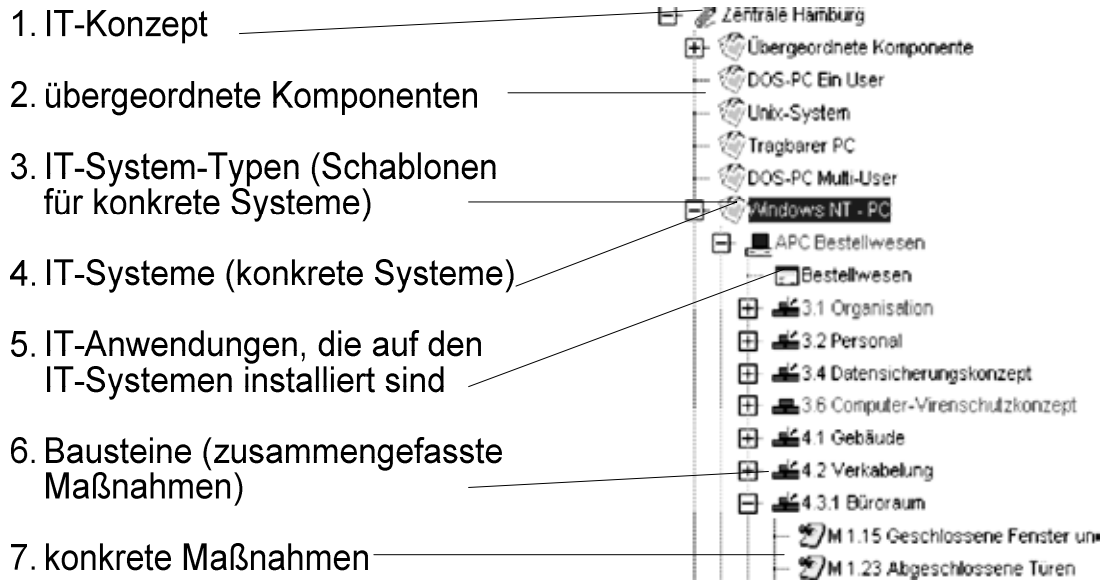


Abbildung 128: Grundstruktur des BSI Grundschutz Tools

Die eigentliche Problemlösung erfolgt mittels der Top-Down Strategie, d.h. durch einen Soll-Ist Vergleich von erforderlichen Maßnahmen der Bausteine mit vorhandenen Maßnahmen. Die Maßnahmen werden durch computergestützte Fragebögen erhoben, wobei eine benutzerdefinierte Änderung des Fragelayouts nicht möglich ist. Das Vergleichsergebnis wird in Form eines HTML-Maßnahmenberichts dargestellt, wobei in dem Maßnahmenbericht auch der Status der Maßnahmenumsetzung und die verantwortlichen Personen notiert sind. So ist eine permanente Kontrolle über den Fortschritt der Maßnahmen gegeben.

IT-Security Tool basierend auf TOSCANA[570]

Das folgende IT-Security Tool basiert auf TOSCANA, welches ein computergestütztes System für die konzeptuelle Analyse und Erkundung von Daten darstellt. So wurden über 30 konzeptuelle Informationssysteme im Bereich des Rechts, der Dokumentenrecherche oder der Analyse von Flugereignissen implementiert[571]. TOSCANA wurde durch die Technische Universität Darmstadt entwickelt. Durch NAVICON, Gesellschaft für begriffliche Wissensverarbeitung mbH und r^3 Security Engineering AG wurde TOSCANA der IS-Sicherheitsmanagementproblematik angepasst. Im Rahmen von TOSCANA wird ein Konzept durch dessen

- Extension, welche die Menge der Objekte, die zum Konzept gehören, darstellt und
- Intension, die die Eigenschaften des Konzeptes angibt,

beschrieben[572].

Für die Beschreibung der Konzepte wird das Tripel (G, M, I) verwendet. G steht für eine Menge von Objekten, M für eine Menge von Attributen und I stellt die Relationen dar. Diese Beschreibungsform wurde auf das BSI-Grundschutzhandbuch übertragen, indem durch G eine Menge von Gefahren eines sicherheitsrelevanten Objektes und durch M eine Menge von zu-

[570] Vgl. Becker et al. (2000)
[571] Vgl. Stumme (1999), S. 275
[572] Vgl. dazu auch Reimer (1991), S. 17

gehörigen Maßnahmen abgebildet wird. Für eine Visualisierung der Relationen dient eine skalierbare Gitterdarstellung des Konzeptes, die eine Navigation der Datenbasis erlaubt. Dies wird erreicht, indem jeder Knoten des Gitters wiederum eine weitere Gitterstellung beinhalten kann, womit eine skalierbare Kombination von Konzepten möglich ist. So kann für eine Maßnahme, die einen Knoten darstellt, eine verfeinerte Darstellung angeboten werden.

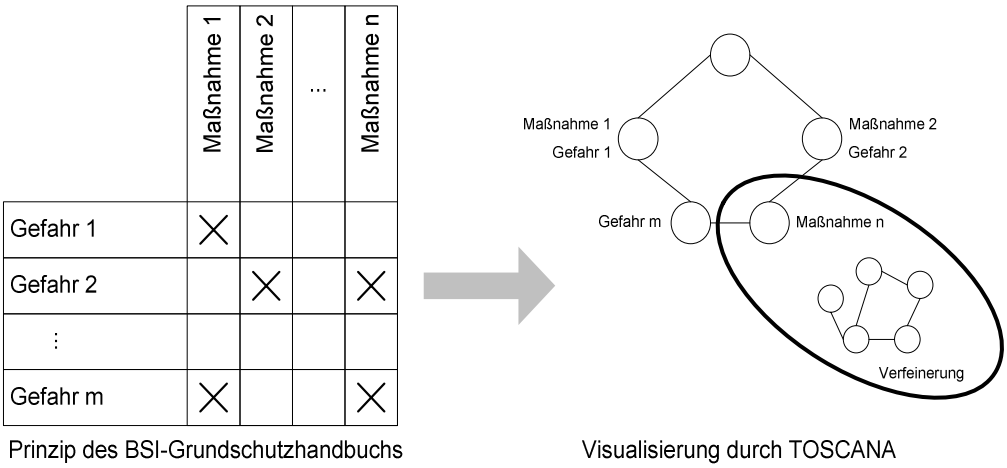


Abbildung 129: Visualisierung des BSI-Grundschutzhandbuchs durch TOSCANA

In dem Tool wird zwischen einem unternehmensunabhängigen Gefahren- und Maßnahmenkatalog einerseits und einer unternehmensabhängigen Strukturanalyse anderseits unterschieden. Auf Basis der Strukturanalyse werden notwendige Maßnahmen im Rahmen einer Checkliste erhoben. Die Maßnahmen werden durch das Tool in „Schlüsselmaßnahmen", die unbedingt notwendig sind und „Nicht-Schlüsselmaßnahmen", differenziert. Hierdurch soll erreicht werden, dass besonders relevante Maßnahmen zuerst analysiert werden. Die fehlenden Maßnahmen können durch verfeinerte Konzepte stufenweise tiefer gehend analysiert werden, was eine weiterführende Maßnahmensuche und Gefahrenanalyse unterstützt.

Datenschutz-Werkzeuge

Der DSB-Supporter[573] ist ein Software-Tool, das die gesetzlichen Aspekte des Datenschutzes in Form einer HTML-Struktur wiedergibt. Das Tool ist für Datenschutzberater ausgelegt und soll die innerbehördliche bzw. innerbetriebliche Mitarbeiterschulung unterstützen. Das Tool besitzt einen „Werkzeugkasten", der insbesondere Maßnahmen- und Checklisten enthält, um schützenswerte Bereiche einer Behörde oder eines Unternehmens aus Sicht des Datenschutzes zu überprüfen. Des Weiteren gibt es den „Schulungsbereich", der die Erstellung von Schulungsfolien unterstützt. Das Tool stellt eine „Bibliothek" zur Verfügung, in der die relevanten Gesetze (z.B. BDSG oder Telekommunikationsgesetze) gespeichert sind.

Ein weiteres Tool, das den Datenschutzbeauftragen unterstützen soll, ist das HMI-DSBtool[574]. Zentraler Bereich des Tools ist eine Geräte- und Dateiregisterfunktion. Durch diese Funktion können die wesentlichen Geräte- und Dateispezifikationen gespeichert werden. Zusätzlich ist

[573] Dieses Programm wurde durch die MEDIENHAFEN Dortmund mit Unterstützung der CAREMACHINE entwickelt. Weitere Informationen unter der Adresse http://www.caremachine.de (Stand: 10.12.2002)
[574] Hersteller: Herweg & Müthlein IT-Management GmbH, 50226 Frechen

eine Sammlung der relevanten Rechtsvorschriften und Gerichtsentscheidungen durch eine Retrieval-Funktion verfügbar; Mahndaten können durch eine Adressdatenbank verwaltet werden[575].

Zusammenfassung

In der folgenden Abbildung werden die vorgestellten computergestützten IS-Sicherheitsmanagement-Werkzeuge auf Basis

- der IS-Sicherheitsstrategien und
- der Überführungsstrategien[576]

differenziert.

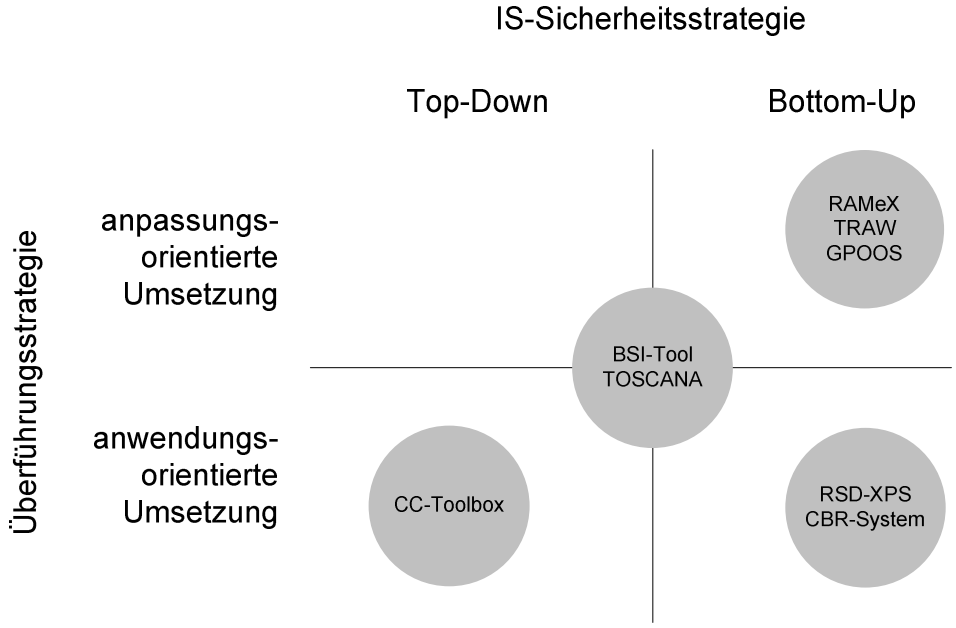


Abbildung 130: Vergleich der Realisierungen

Die Bottom-Up Strategie-Werkzeuge RAMeX, TRAW und GPOOS werden hauptsächlich in der Phase „Systemabgrenzung“ und „Risikoerkennung“ eingesetzt, wobei TRAW auch für die Risikobewertung verwendet werden kann. Die Werkzeuge können flexibel mit Wissen aus unterschiedlichen IS-Sicherheitsaspekten erweitert werden. Durch die Repräsentation des wieder verwendbaren IS-Sicherheitswissens soll eine Strukturierung bzw. Komplexitätsreduktion der Systemabgrenzung und Anpassung des Sicherheitsexpertenwissens im Rahmen der Risikoerkennung erreicht werden.

Das RSD-XPS und das CBR-System sind zwar risikoanalyseorientiert, jedoch auf ein spezifisches Problemgebiet (Online-Dienste) bzw. spezifische Fälle ausgerichtet und somit direkt anwendbar. Die Flexibilität der oben genannten Werkzeuge ist durch die Spezialisierung verloren gegangen. Das RSD-XPS - basierend auf dem SINUS-Konzept - stellt ein fertiges XPS für die Auswahl von Online-Diensten dar. Somit ist das XPS auf ein beschränktes Anwendungsgebiet ausgelegt und kann nicht als Werkzeug für andere IS-Sicherheitsaspekte verwendet werden. Da alle Objekte zu Beginn einer Überprüfung instanziiert sind, kann es sofort angewendet werden. Eine Erweiterung und Pflege des XPS für einen IS-Sicherheitsexperten

[575] Vgl. Jaspers (1997), S. 160-167
[576] Überführung des unternehmensunabhängigen Domänenwissens auf das fallspezifische Wissen.

ist ohne Kenntnisse in der KI-Sprache Babylon nicht möglich. Auch das CBR-System ermöglicht eine direkte Anwendung, indem für einen konkreten Fall auf historisch ähnliche Vorfälle und deren Lösungen zugegriffen wird, ohne dass eine Anpassung im Rahmen einer Systemabgrenzung erforderlich ist.

Das BSI Tool wie auch TOSCANA als hybrider Ansatz verlangen im ersten Schritt die Auswahl und Anpassung der vordefinierten IT-Systeme, denen zusätzlich IT-Bausteine zugeordnet sind. Im zweiten Schritt werden computergestützte Fragebögen angewandt, um realisierte Maßnahmen mit den erforderlichen Maßnahmen der jeweiligen IT-Bausteine zu vergleichen. TOSCANA bietet zudem eine skalierbare Visualisierung der Grundschutz-Konzepte und deren Abhängigkeiten. Die Differenz zwischen realisierten und erforderlichen Maßnahmen bildet die Basis für den Ergebnisbericht.

Bei der CC-Toolbox werden auf Basis von ermittelten IS-Sicherheitszielen Anforderungen festgestellt. Hierbei werden die IS-Sicherheitsziele durch Erhebung der Einsatzumgebung definiert. Das BSI-Tool und die CC-Toolbox haben gemeinsam, dass sie nur „ihr“ Kriterienwerk repräsentieren bzw. Aspekte anderer Kriterienwerke oder des Datenschutzes können nur sehr bedingt hinzugefügt werden. So ist die Möglichkeit zur Erweiterung und Anpassung der Wissensbasis mit anderen Kriterienwerken sehr eingeschränkt.

Die Datenschutz-Werkzeuge sind nicht in die Abbildung 130 eindeutig einzuordnen, da sie hauptsächlich Retrieval-Funktionen für Gesetze sowie Geräte- und Dateispezifikationen unterstützen. Des Weiteren sind sie für den Problembereich „Datenschutz“ ausgelegt, was eine umfassendere Anwendung nur bedingt ermöglicht.

Überführungsaufwand aufgrund der IS-Sicherheitsstrategie

Bei dem Entwicklungsaufwand einer Wissensbasis sind nicht nur die Erstellungskosten des domänenspezifischen IS-Sicherheitswissens zu berücksichtigen, sondern auch deren Anpassungsaufwand für eine bestimmte Institution. Der Überführungsaufwand kann den Erstellungsaufwand des domänenspezifischen IS-Sicherheitswissens im Laufe der Anwendungsdauer übertreffen.

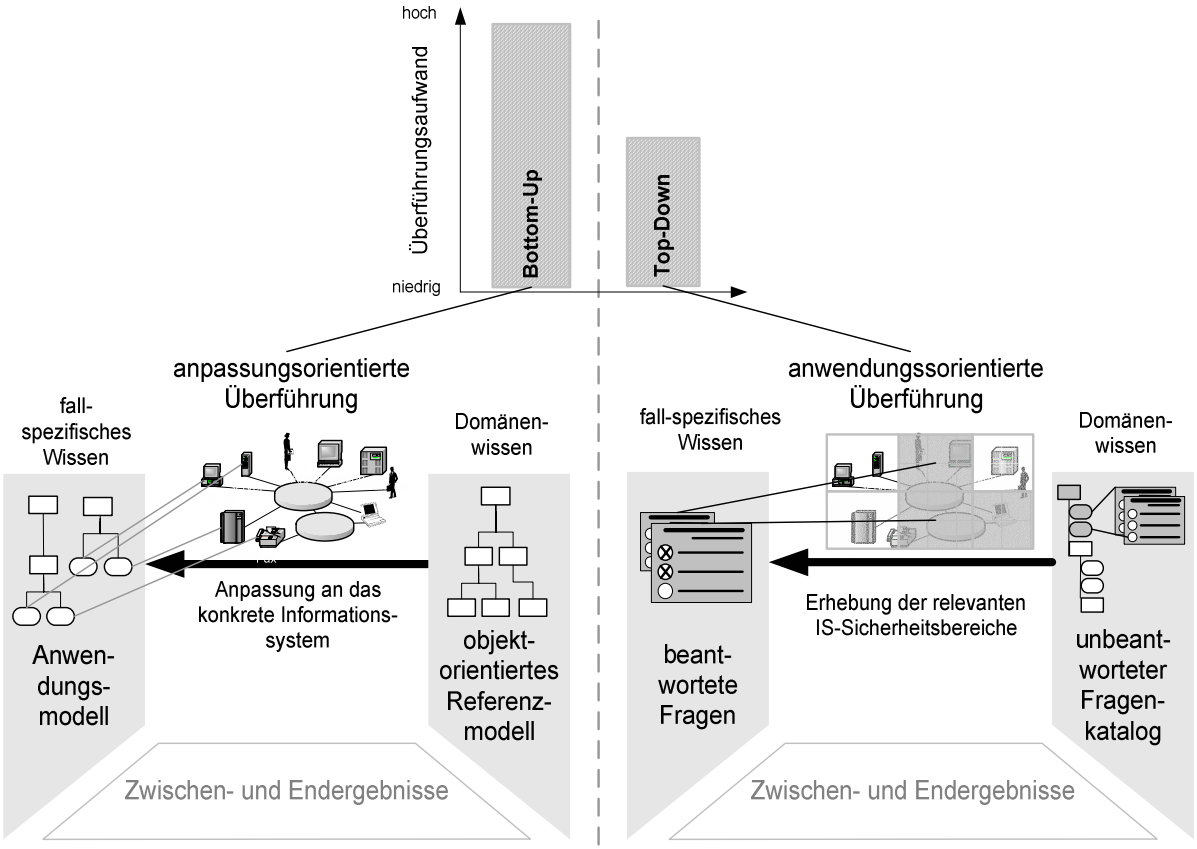


Abbildung 131: Anpassungs- und anwendungsorientierte Überführung

Die Strategiewahl zur Erzeugung von IS-Sicherheit beeinflusst den Überführungsaufwand des domänenspezifischen IS-Sicherheitswissens auf das fallspezifische IS-Sicherheitswissen. Der Aufwand bei dem Bottom-Up Ansatz ist höher als bei den Top-Down Ansätzen, da eine präzise Nachbildung von individuellen IS-Sicherheitsaspekten - meist durch objektorientierte Techniken - nötig ist. Dafür ist durch die detaillierte Konstruktion eine individualisierte Tiefenanalyse für die überführten Bereiche möglich.

Das Domänenmodell des Top-Down Ansatzes wird dagegen direkt auf die Institution angewendet und beinhaltet somit einen geringen Überführungsaufwand, denn das fallspezifische Wissen wird mit Hilfe von Fragenkatalogen erhoben, deren Antworten als Grundlage für die Problemlösung dienen. Es ist somit nur eine grobe Anpassung an die spezielle Unternehmenssituation zu erwarten, da hier keine Modellierung der unternehmensspezifischen Infrastruktur nötig ist, wodurch auch eine Breitanalyse für alle Bereiche ermöglicht wird.

5.3 Prototypische Realisierung einer Diagnose-Shell zur Erstellung von wissensbasierten Fragenkatalogen

Bei Wissenssystemlösungen soll die Balance zwischen dem Formalisierungsgrad des repräsentierten Wissens und dem damit verbundenen Erhebungsaufwand einerseits und dem erreichten Nutzen anderseits beachtet werden[577]. Bottom-Up geprägte Systeme besitzen einen hohen Formalisierungsgrad des IS-Sicherheitswissens sowie eine individuelle Anpassung an die unternehmensorientierte IS-Struktur. Der damit verbundene hohe Aufwand ist nur in besonders sensiblen IS-Bereichen gerechtfertigt, wenn zudem das IS-Sicherheitswissen präzise formuliert werden kann. Die Top-Down Systeme dagegen orientieren sich an der Anwendbarkeit des verfügbaren IS-Sicherheitswissens, wobei der Anpassungsgrad an die individuelle IS-Struktur nicht so hoch ist wie bei den Bottom-Up Systemen. Im Rahmen dieser Arbeit ist das WBS auf den Top-Down Ansatz ausgerichtet, wobei auch kausale Aspekte der Bottom-Up Problemlösung berücksichtigt werden. Hierfür wird ein Diagnosesystem auf Basis des Entwurfsmodells entwickelt. Es besteht eine Formalisierung des IS-Sicherheitswissens durch wissensbasierte Fragenkataloge, wobei der Formalisierungsgrad niedriger ist als bei Bottom-Up geprägten Systemen.

Historisch gesehen haben Diagnosesysteme den Ursprung in technischen Anwendungen, sind aber auch in der Medizin stark vertreten[579]. Diagnosesysteme werden teilweise unterschiedlich definiert und z.T. als Expertisesysteme bezeichnet[580]. So besitzen für Kurbel Diagnosesysteme nur die Möglichkeiten, Fehler zu erkennen; sie bieten aber keine Lösung. Systeme, die gleichzeitig eine Lösung anbieten, bezeichnet Kurbel als „Systeme zur Fehleranalyse und -behebung“[581]. Im Rahmen dieser Arbeit soll den wissensbasierten Diagnosesystemen neben der Fehlererkennung auch die Lösungskomponente zugeordnet werden. Mindestvoraussetzung hierfür ist die Festlegung auf den Problemlösungstyp Diagnose.

Ausprägungsformen von WBS

Für die Konstruktion von Diagnose-Expertensystemen haben sich historisch gesehen folgende Ausprägungsformen von WBS entwickelt:

- Zuerst wurden KI-Sprachen für eine implementierungsnahe Ebene entwickelt, die auf den Knowledge Engineer ausgerichtet waren.
- Später wurden WBS im Zusammenhang mit dem Modellierungsansatz als konfigurierbare Shells konstruiert, welche die abstraktere Wissensebene des Fachexperten als Grundlage besitzen und die direkte Wissenseingabe unterstützen.

KI-Sprachen sind in den Anfangsjahren der Künstlichen Intelligenz entstanden, wobei zwischen funktionalen Sprachen (z.B. LISP) und logischen Sprachen (z.B. PROLOG) zu unterscheiden ist. Wissensverarbeitungssprachen (z.B. KEE, OPS5, KAPPA oder SMART Elements) verbinden KI-Sprachansätze z.T. mit höheren Programmiersprachen. Sie stellen vordefinierte Ausdrucksmittel der Wissensrepräsentation (z.B. Produktionsregeln oder Frames) und

[577] Vgl. Staab et al. (2001), S. 27
[579] Z.B. zählt das bekannte XPS „Mycin“ zu den medizinischen Diagnosesystemen. Vgl. Kurbel (1992), S. 139
[580] Vgl. Stickel/Groffmann/Rau (1998), S. 261
[581] Vgl. Kurbel (1992), S. 141

Inferenz-Strategien zur Verfügung und liegen auf einer sehr implementierungsnahen Ebene, wodurch eine Kluft zwischen dem Knowledge Engineer und Experten entsteht. So sind bei KI-Sprachen die Realisierungsmöglichkeiten flexibel, jedoch ist der Realisierungsaufwand durch die indirekte Wissenseingabe hoch.

Diese KI-Sprachen bergen des Weiteren eine Abhängigkeit des Fachexperten von dem Knowledge Engineer in sich. Durch die wachsende Aktualitätsproblematik innerhalb der Informationstechnologie besitzt diese Abhängigkeit negative Auswirkungen auf die Pflege und Wartung der Wissensbasis. Das wissensbasierte Diagnosesystem des IS-Sicherheitswissens benötigt eine ständige Aktualisierung und Wartung des IS-Sicherheitswissens. Dies ist nur durch die Verbindung des Fachexperten und Knowledge Engineers in einer Person wirtschaftlich zu rechtfertigen, denn für ein Unternehmen ist es vorteilhaft, wenn ein Fachexperte nach geringer Einarbeitungszeit die Wissensbasis selbstständig pflegen kann, ohne sich die Fähigkeiten eines Knowledge Engineers anzueignen.

Erfolg versprechend ist deshalb die Entwicklung von wissensbasierten Shells, welche auf der direkten Wissenseingabe basieren. Somit wird primär die Wissensrepräsentation und Problemlösung durch die Operationalisierung des Expertisemodells bestimmt und nicht durch die formale Repräsentationsform einer KI-Sprache. Infolgedessen ist es möglich, problemspezifische Werkzeuge bzw. Shells zu erstellen, welche auf spezifischen (z.B. heuristischen oder modellbasierten) Problemlösungsmethoden basieren[582]. Die interne Struktur der Wissensbasis wird in eine „Fachexperten-Sprache“ abstrahiert, was einem Experten nach kurzer Einarbeitungszeit erlaubt, spezifische Expertensysteme selbstständig zu konstruieren[583].

Nachteil dieser Shells ist die Problemspezifizierung, wodurch der Einsatzbereich eingeschränkt ist. Hieraufhin wurden Shells mit konfigurierbaren Problemlösungsmethoden entwickelt, welche eine höhere Flexibilität haben, um sich an spezifische Probleme anzupassen. Auf Basis einer konfigurierbaren Shell können Fachexperten anwendungsorientiert Expertensysteme intuitiv erstellen und warten.

[582] Vgl. Schönebeck (1994), S. 23
[583] Vgl. Puppe (1996), S. 169

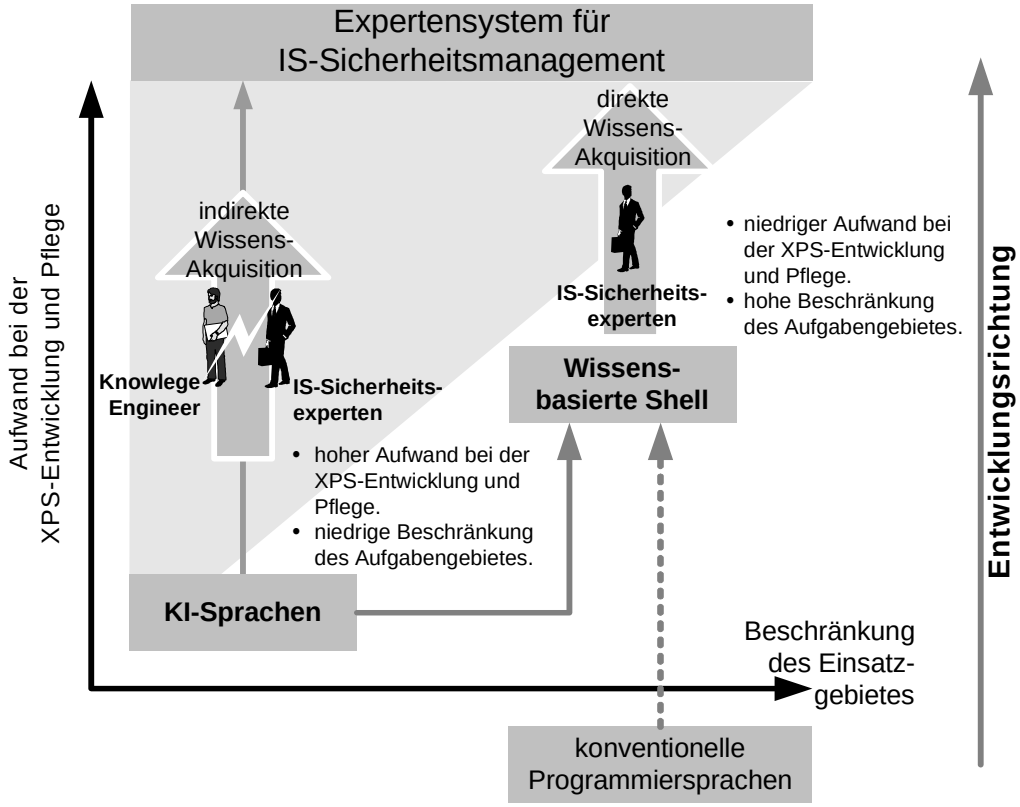


Abbildung 132: Zusammenhang zwischen Aufwand und Einsatzgebiet von WBS

Inwieweit ein WBS selbst auf Basis einer KI-Sprache oder eines anderen WBS entwickelt worden ist, hängt von der jeweiligen Sichtweise ab. WBS können aber auch ohne Einsatz von KI-Sprachen in konventionelle Programmiersprachen (z.B. C++, Pascal oder Java) implementiert werden.

Diagnose-Shell für das IS-Sicherheitsmanagement

Die Implementierung der prototypischen Diagnose-Shell des IS-Sicherheitsmanagements basiert auf dem Expertisemodell des IS-Sicherheitsmanagements und dem Entwurfsmodell des wissensbasierten Fragenkatalogs dieser Arbeit. Das WBS sollte möglichst viele Aspekte des Expertisemodells repräsentieren können, wobei primär eine anwendungsorientierte Top-Down Strategie unterstützt wird. Unabhängig von einem speziellen Kriterienwerk können durch das WBS Inhalte unterschiedlicher Kriterienwerke und Aspekte des Datenschutzes verarbeitet werden. Es können aber auch unternehmensindividuelle IS-Sicherheitsaspekte eingegeben und verarbeitet werden, sowie kausale Zusammenhänge repräsentiert werden, um einen Bottom-Up Ansatz zu unterstützen, wobei nicht die gleiche Abbildungsqualität der vorwiegend Bottom-Up geprägten Systeme, wie z.B. TRAW oder GOOPS, erreicht wird.

Die Diagnose-Shell besitzt den Charakter eines wieder verwendbaren Werkzeugkastens basierend auf wissensbasierten Fragenkatalogen, der die unterschiedlichen IS-Sicherheitsstrategien zur Erstellung eines IS-Sicherheitskonzepts unterstützt und sich somit an die jeweilige Institution und deren IS-Sicherheitspolitik anpasst. Auf Basis der ausgewählten IS-Sicherheitsstrategie werden aus der Diagnose-Shell die Problemlösungsmethoden und die benötigten IS-Sicherheitswissensbestandteile ausgewählt.

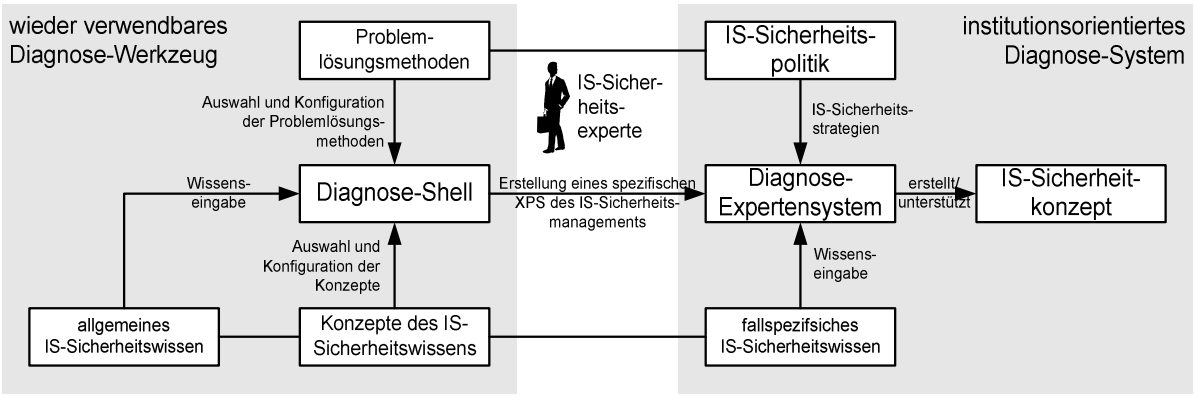


Abbildung 133: Anwendung einer wieder verwendbaren Diagnose-Shell

Durch die Diagnose-Shell kann der IS-Sicherheitsexperte selbstständig mit geringem Überführungsaufwand angepasste Diagnose-XPS erstellen und Inhalte von vielfältigen Kriterienwerken und Aspekten des Datenschutzes durch wissensbasierte Fragenkataloge repräsentieren, ohne die Hilfe eines Knowledge Engineers zu beanspruchen. Denn die IS-Sicherheitspolitik und der IS-Sicherheitsexperte sollen primär das IS-Sicherheitsniveau für die Institution bestimmen und nicht die „Fähigkeiten“ des Knowledge Engineers. Dies erfolgt durch

- direkte Wissenseingabe und -pflege von IS-Sicherheitswissen durch einen IS-Sicherheitsexperten,
- direkte Anwendung und Anpassung der Problemlösungsmethoden und des IS-Sicherheitswissens auf die konkrete Problemstellung durch ein spezifisches Diagnose-XPS,
- Unterstützung der präventiven und reaktiven Top-Down und Bottom-Up Strategie,
- Unabhängigkeit von speziellen Kriterienwerken (z.B. CC oder BSI-Grundschutz) und konkreten Institutionsformen (z.B. Unternehmen oder Behörden).

Die Arbeit des Fachexperten beinhaltet im Idealfall nur noch die Aktivierung und Konfiguration der benötigten Problemlösungsmethoden sowie „Füllung“ der Wissensbasis mit benötigtem IS-Sicherheitswissen. Das daraus entstandene Diagnose-XPS ist auf die jeweilige Institution ausgerichtet und kann die Erstellung von unternehmensindividuellen IS-Sicherheitskonzepten unterstützen.

Architektur der prototypischen Diagnose-Shell

Die Architektur der prototypischen Diagnose-Shell zur Erstellung eines wissensbasierten Fragenkatalogs ist in der folgenden Abbildung dargestellt.

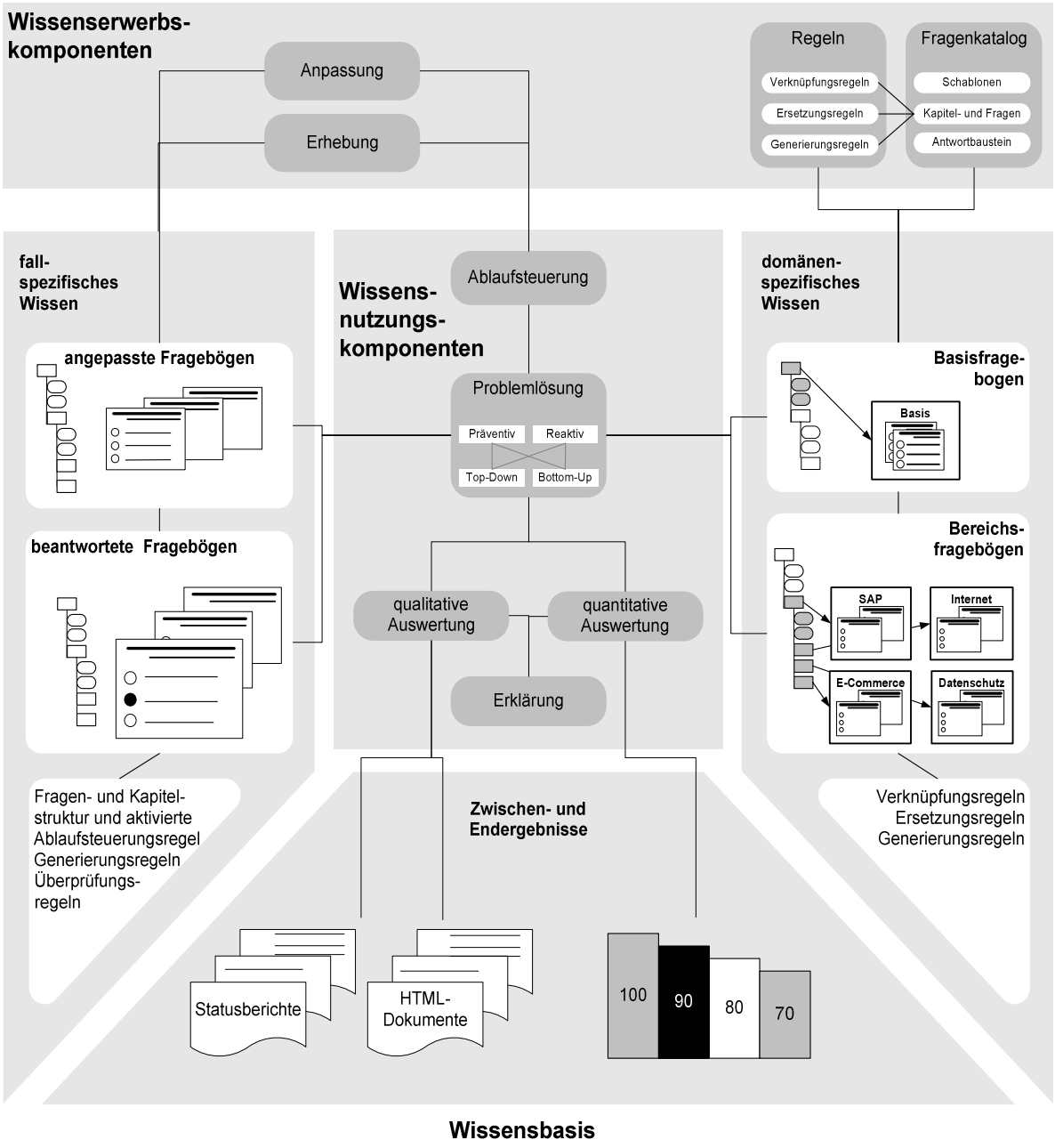


Abbildung 134: Architektur der Diagnose-Shell zur Erstellung von wissensbasierten Fragenkatalogen

Das WBS zur Erstellung wissensbasierter Fragenkataloge wird durch verschiedene Module realisiert, die miteinander verknüpft sind. Diese Module können eigenständige Programme oder Teile eines gesamten Programmpakets darstellen, wobei diese Module vielfältige Interdependenzen besitzen. Bei der folgenden Betrachtung der Module des WBS ist eine Unterscheidung zwischen domänenspezifischer und fallspezifischer Sicht nötig.

- Bei der Konstruktion des domänenspezifischen IS-Sicherheitswissens in Form von Fragenkatalogen wird versucht, einen möglichst großen Bereich des IS-Sicherheitsmanagements abzudecken.
- Aus fallspezifischer Sicht wird dieses umfangreiche Wissen auf den konkreten Fall überführt und die erforderlichen Informationen erhoben.

- Für die Wissensnutzung werden beide Bereiche - domänen- und fallspezifisches Wissen - benötigt, um Zwischen- und Endergebnisse zu erlangen.

Es folgt eine Beschreibung der Realisierung, bei der z.T. mehrere Module zu einem Programmpaket zusammengefasst wurden.

5.3.1 Wissenserwerbskomponenten

In Anlehnung an computergestützte Fragenkataloge lassen sich Anforderungen an einen wissensbasierten Fragenkatalog herleiten[584]. Insgesamt soll durch die Wissenserwerbskomponente die Umsetzung der folgenden Anforderungen ohne Programmierkenntnis möglich sein.

- Die optionalen Einstiegs- und Ausstiegsfragen haben die Aufgabe, den Befragten in die Befragung einzuführen bzw. einen abschließenden Überblick über die Befragung zu geben.[585].
- Im Rahmen der Gestaltung des Fragenkatalogs sind der Inhalt, die Anzahl und die Reihenfolge der Fragen festzulegen. Fragen des gleichen Themengebietes werden zu einem Komplex zusammengefasst; sensitive und „heikle“ Fragen sollten erst am Schluss einer Befragung auftreten. Die Fragen sollten einen einheitlichen graphischen Aufbau besitzen.
- Es sollten Ausstrahlungs- und Plazierungseffekte vermieden werden, d.h. der Befragte stützt seine Antwort nicht nur auf die aktuellen, sondern ggf. auch auf bereits zuvor gestellte Fragen.
- Die Einstreuung von Auswahlfragen soll verhindern, dass überflüssige Fragen in einem bestimmten Zusammenhang gestellt werden. Somit soll einer möglichen Ermüdung des Befragten vorgebeugt werden.

Schablonengenerator

Mit dem Schablonengenerator ist der Experte in der Lage, Schablonen zu erstellen, die als Vorlage für die Fragen dienen. Er bietet damit die Möglichkeit, unterschiedliche Fragetypen zu entwerfen. Hierdurch wird die Erstellung von standardisierten Fragenkatalogen unterstützt, da alle Fragen auf den gleichen Schablonen bzw. Fragetypen basieren, wie z.B. Ja/Nein- oder Rating-Fragen. Der Vorteil ist, dass die Fragen bei der Befragung auf dem gleichen Layout beruhen und die Flexibilität eines variablen Fragenlayouts bei der Fragenerstellung gleichzeitig erhalten bleibt.

[584] Vgl. Koolwijk (1974), S. 41; Roth (1995), S. 153; Stier (1996), S. 184
[585] Vgl. Möhrle/Hoffmann (1994), S. 244

Abbildung 135: Beispiel einer Schablone

Die Schablone kann unterschiedliche Dialog- und Bezeichnungsobjekte besitzen, wobei die Bezeichnung bei dem konkreten Fragenkatalog mit konkreten Werten belegt wird.

Kapitel- und Fragengenerator

Die Grundlage des wissensbasierten Fragenkatalogs bilden Kapitel und deren Fragen, welche Objekt-Attribut-Wert Strukturen repräsentieren. Durch den Kapitel- und Fragengenerator werden die einzelnen Fragen entwickelt und zu einem Gesamtkatalog zusammengefasst. Die Struktur der Kataloge wird mit Hilfe eines Kapitelbaums erzeugt, indem zusammengehörige Fragen zu Kapiteln zusammengefasst werden. Die Entwicklung der Kapitelstruktur wird durch Oberkapitel und deren Unterkapitel unterstützt. Zusätzlich sind Antwortbausteine, die zur Auswertung benötigt werden, einzugeben. Die Gesamtheit der erstellten Kapitel und Fragen bilden den Fragenkatalog. Zur groben Anpassung des Fragenkatalogs an die jeweilige Problemstellung werden i.d.R. vollständige Kapitel hinzugefügt oder gelöscht, wobei dieses Basis- oder Spezialgebieten entspricht. Eine verfeinerte spezifische Anpassung erfolgt z.B. durch Verknüpfungsregeln.

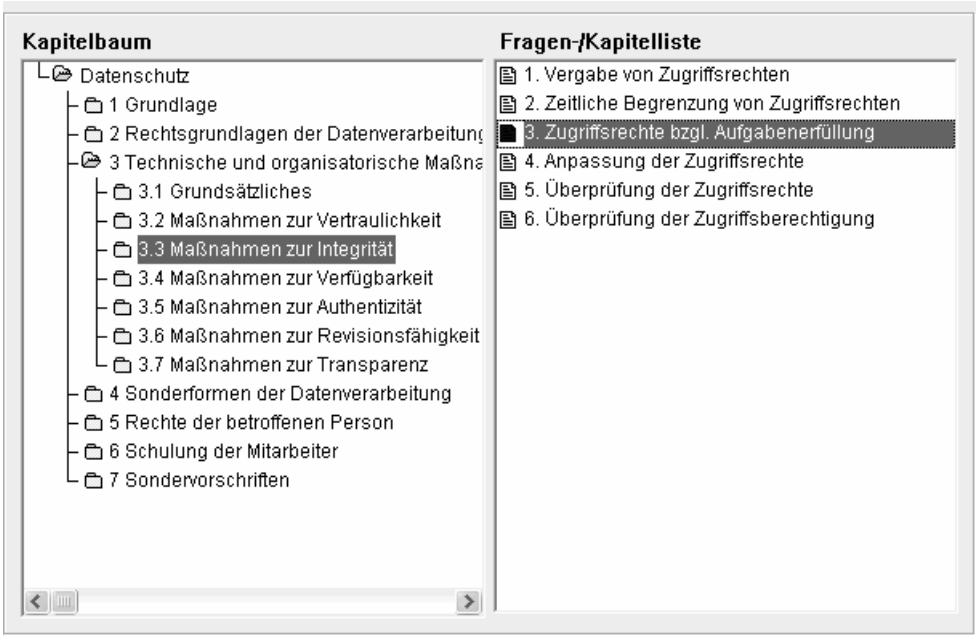


Abbildung 136: Beispiel einer Kapitelstruktur

Die Kapitel dienen erstens zur Strukturierung bzw. Abstrahierung des Problemgebiets. Es existieren Oberkapitel, die zu Unterkapiteln verfeinert bzw. spezialisiert werden. Zweitens beschreibt die Kapitelstruktur die grundlegende Abfragerichtung der Merkmalserhebung. Diese starre Abfragerichtung kann entweder durch verknüpfte Fragen automatisch (durch das System) geändert werden oder der Benutzer ändert manuell die Abfragereihenfolge.

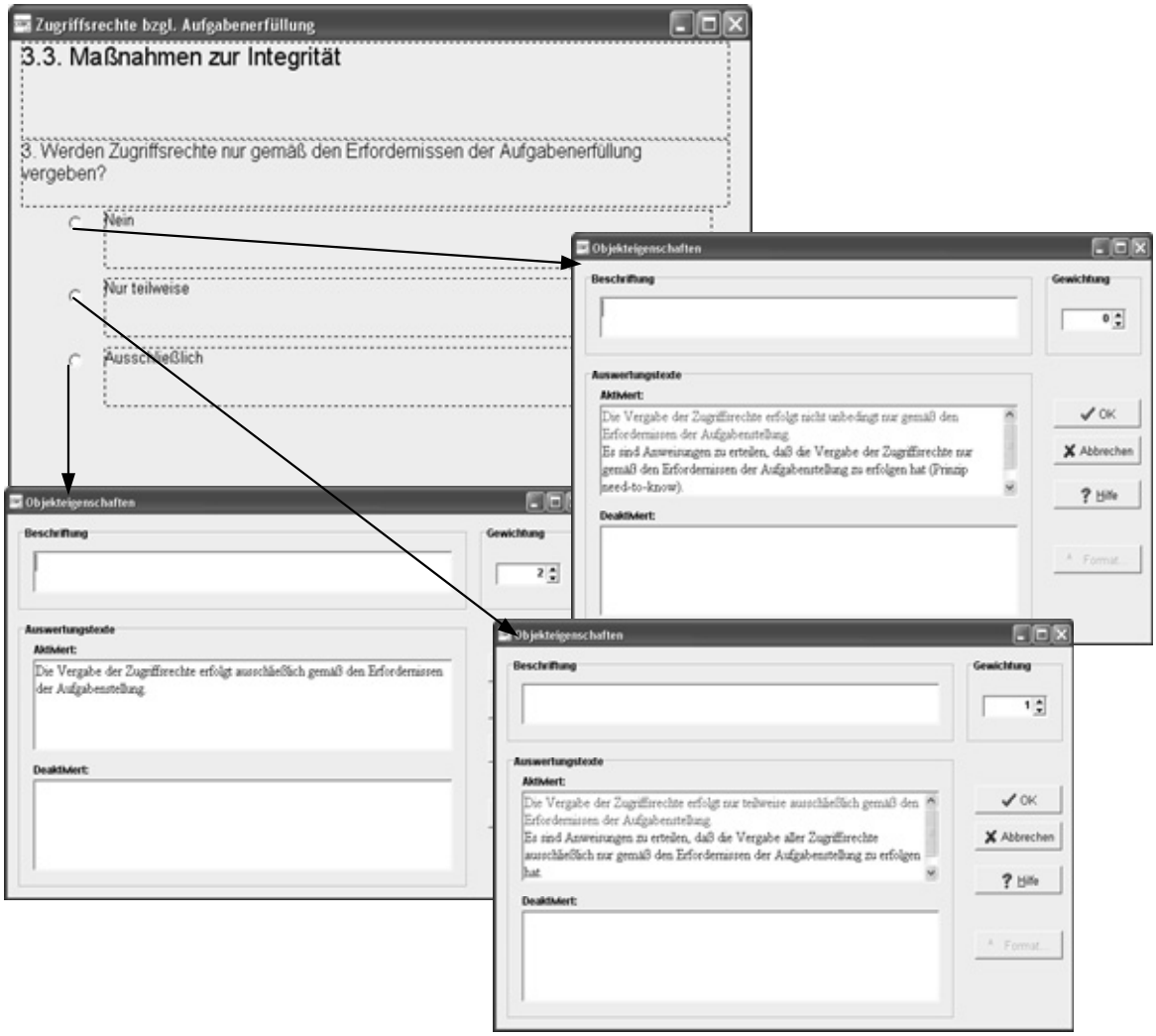


Abbildung 137: Beispiel einer Frage mit Antwortbausteinen

Fragen abstrahieren Merkmale, für die bei einer Befragung konkrete Merkmalswerte ermittelt werden. Die Fragen dienen gleichzeitig der Erhebung von Beobachtungen und als Merkmalsindikatoren für z.B. vorhandene oder nicht vorhandene Maßnahmen. Dafür stehen verschiedene Fragetypen wie Alternative- oder Ja/Nein-Fragen zur Verfügung. Die Fragetypen können auch miteinander kombiniert werden.

Jede einzelne Antwortmöglichkeit wird entweder mit Ja (angeklickt) oder Nein (nicht angeklickt) markiert. Entsprechend der binären Ausprägung der einzelnen Antwortmöglichkeit sind zwei Antworttexte (für Ja oder Nein) mit der jeweiligen Antwort verbunden. Bei der späteren Auswertung wird der jeweilige Antworttext ausgegeben. Da der Antworttext unterschiedliche Inhalte besitzen kann, werden diese durch Textfarben unterschieden. Zu jeder Antwortmöglichkeit kann noch ein Gewichtungsfaktor angegeben werden, der bei einer quantitativen Auswertung verwendet wird.

Basierend auf dem Entwurfsmodell werden folgende Fragenkatalog-Regeln verwendet, um Abhängigkeiten zwischen den Fragen herzustellen.

Verknüpfungsregelgenerator

Verknüpfungsregeln werden zur Ablaufsteuerung und verfeinerten Anpassung des Fragenkatalogs bei einer konkreten Situation angewandt. So werden für die jeweiligen IS-Sicherheitsstrategien eventuell nur gewisse Bereiche der Fragen benötigt. Ist z.B. eine präventive Top-Down Strategie gewünscht, so werden vor allem Maßnahmen erhoben oder nicht benötigte Sicherheitsbereiche einer Institution werden nicht berücksichtigt.

Die Anpassung an eine konkrete Situation ist eng mit dem Erhebungs-Tool und den Verknüpfungsregeln verbunden, da durch Auswahlfragen und -regeln die benötigten IS-Sicherheitsbereiche des Katalogs ermittelt werden. Aufgrund der Antworten werden durch Verknüpfungsregeln ganze Kapitel aktiviert oder deaktiviert bzw. übersprungen. Aufgrund des einfachen Aufbaus der Verknüpfungsregeln können umfangreiche Teilbereiche innerhalb der Kapitel übersprungen werden, um so eine differenziertere Anpassung zu erlangen. Diese Verknüpfungsregeln haben Einfluss auf die Problemlösung, da eventuell auf Grund einer bestimmten Antwort Fragen ausgelassen und diese bei der Auswertung ignoriert werden. Durch den Aufbau von Verknüpfungsregeln können viele einfache Abhängigkeiten repräsentiert werden; für komplexe Abhängigkeiten ist diese Form von Regeln nicht geeignet.

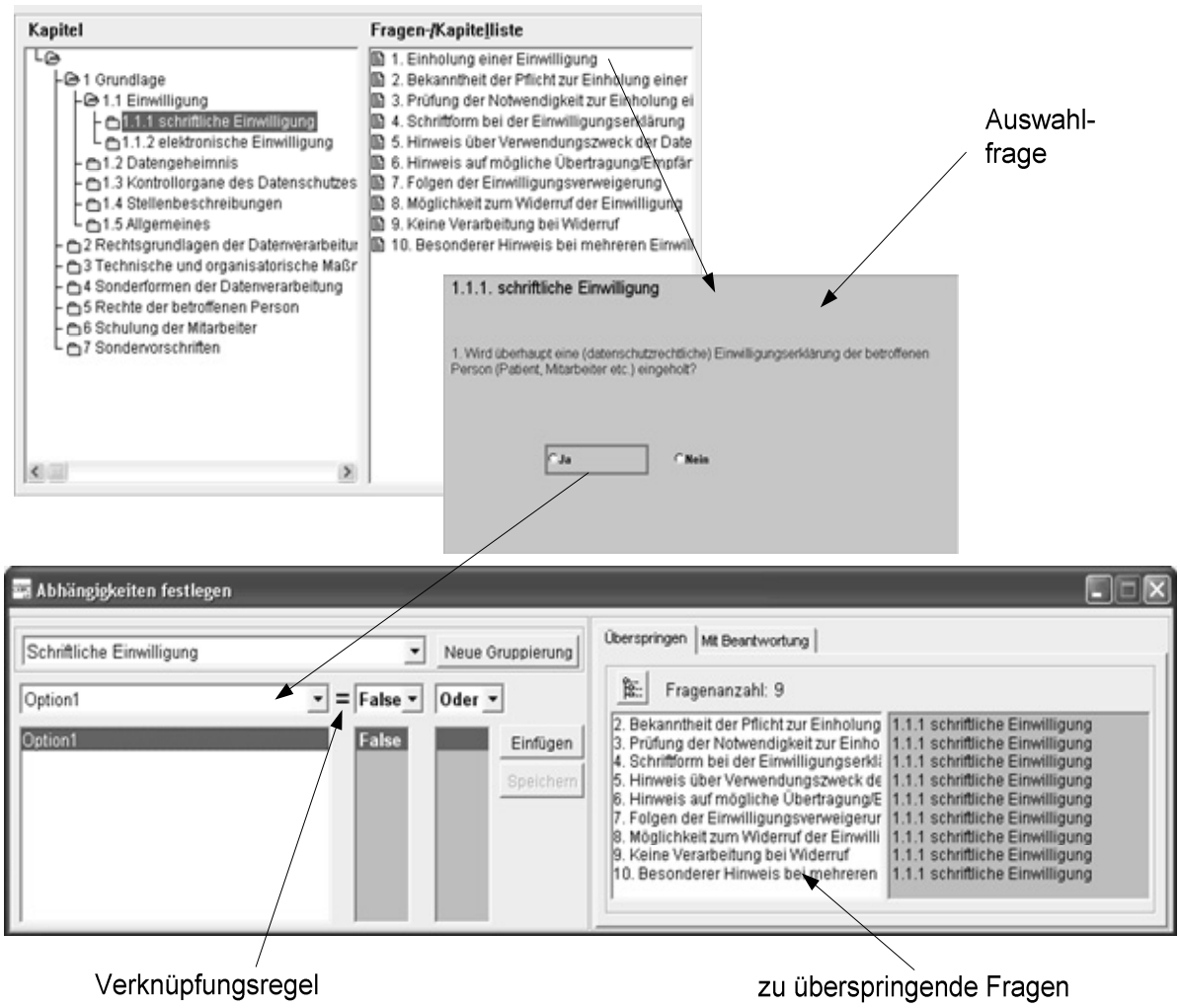


Abbildung 138: Beispiel einer Anpassungsfrage in Verbindung mit Verknüpfungsregeln

In obiger Abbildung ist ein Beispiel für eine Verknüpfungsregel aufgezeigt, die direkt der Auswahlfrage zugeordnet ist. Ausgehend von einem Antwortobjekt einer Auswahlfrage - z.B. Optionskästchen 1 (Option1) - können die „zu überspringenden Fragen“ definiert werden. Zur Strukturierung können die Regeln zu Gruppen zusammengefasst werden.

Ersetzungsregelgenerator

Ersetzungsregeln sind ähnlich den Verknüpfungsregeln einer Auswahlfrage direkt zugeordnet, können aber zusätzlich andere Fragen automatisch (und verdeckt) beantworten. Sie dienen somit primär einer einfachen Hypothesengenerierung und -überprüfung.

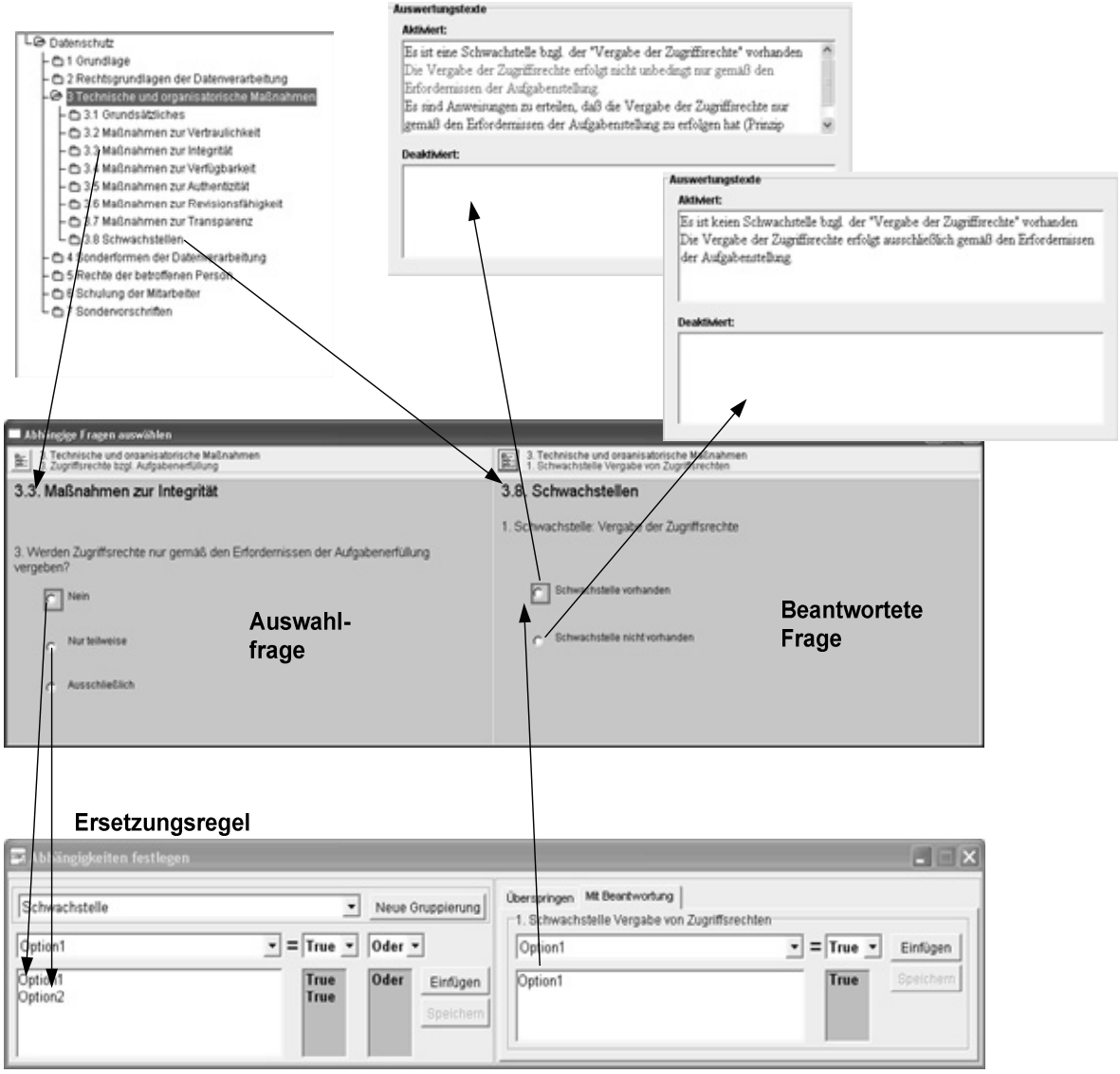


Abbildung 139: Beispiel für Ersetzungsregeln

Dieses Beispiel zeigt, wie durch Ersetzungsregeln, durch erhobene (fehlende) Maßnahmen und durch automatische Beantwortung von Fragen, Schwachstellen ermittelt werden. Im Gegensatz zu dem Beispiel aus Abbildung 137 können hier mehrere Fragen verknüpft werden. Hierdurch ist eine spätere Aufhebung der Schwachstellen durch eine andere erhobene und vorhandene Maßnahme möglich.

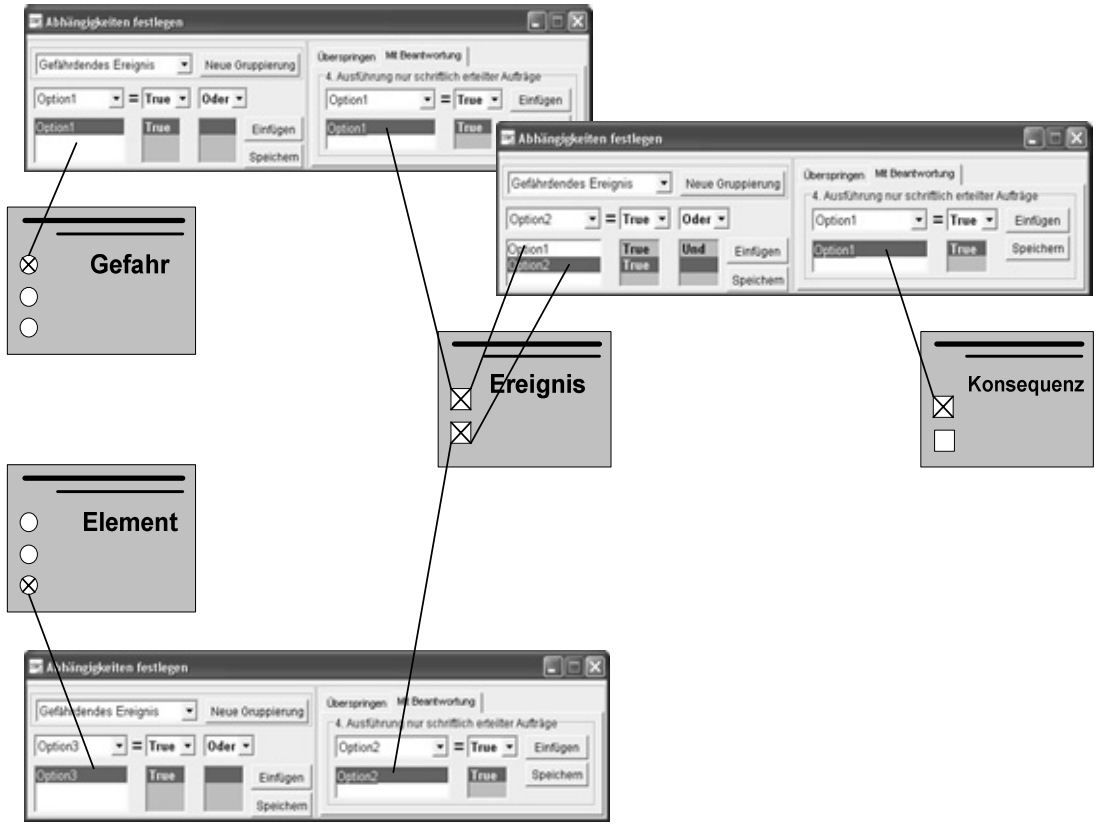


Abbildung 140: Kausale Ersetzungsregeln

Mit Ersetzungsregeln ist es möglich, einfache kausale Zusammenhänge durch zusammengesetzte Ersetzungsregeln darzustellen. In der Abbildung ist die Grundstruktur dargelegt, wobei auf eine Ereignisfrage verzichtet werden kann, wenn die Konsequenz-Frage direkt durch Gefahr- und Element-Ersetzungsregeln beantwortet wird.

Es ist zu beachten, dass diese Darstellungsform bei komplexeren Kausaldarstellungen schnell an die Grenzen stößt. So können kausale Abhängigkeiten in Form von Konsequenz, die wiederum als Eingangsgefahr für ein anderes gefährdendes Ereignis dient, mit dieser Repräsentationsform nur begrenzt dargestellt werden. Aus diesem Grund sollten kausale Regeln durch Generierungsregeln repräsentiert werden.

Generierungsregelgenerator

Die Generierungsregeln besitzen eine höhere Flexibilität gegenüber den Verknüpfungs- und Ersetzungsregeln und können somit komplexe Abhängigkeiten repräsentieren; dafür werden sie schnell unübersichtlich. Generierungsregeln sind nicht an eine bestimmte Auswahlfrage gebunden, sondern werden unabhängig von Fragen repräsentiert.

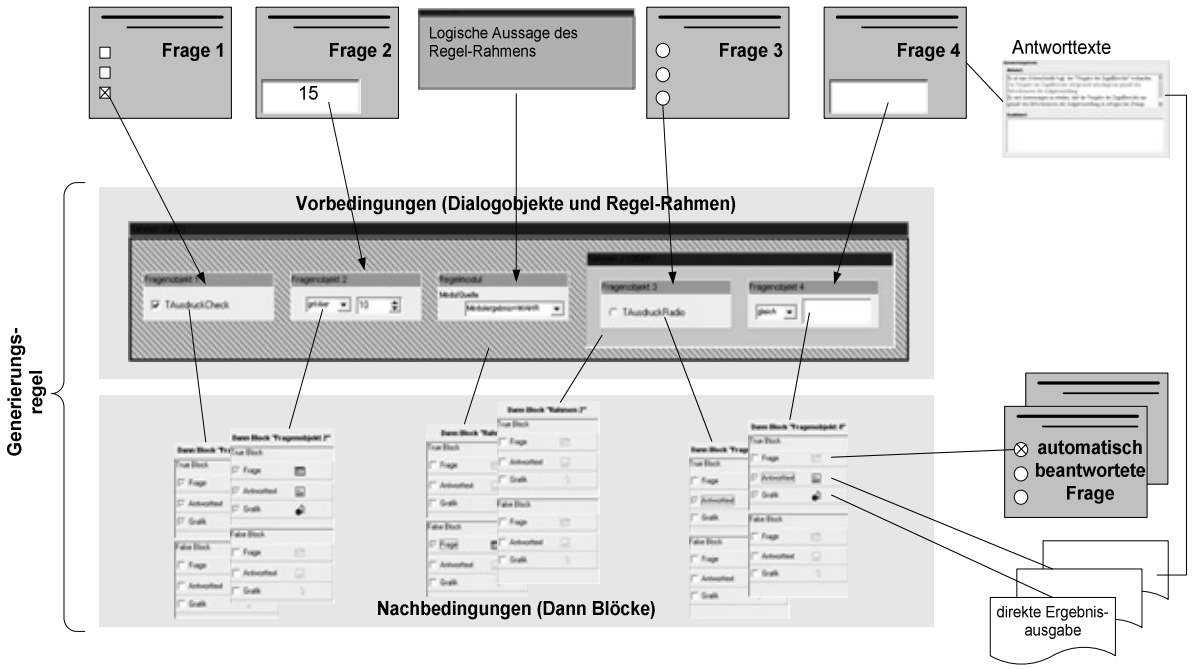


Abbildung 141: Grundstruktur einer Generierungsregel

Die Generierungsregel besteht aus einer Vorbedingung und einer Nachbedingung. Die Quelle der Vorbedingung bilden die Antwortwerte der Dialogobjekte. So ist bei einem Selektions- oder Alternativobjekt eine „Wahr/Falsch“ Vorbedingungseigenschaft ausreichend, wohingegen bei Texteingaben weitere Vorbedingungseigenschaften, wie z.B. „gleich“, „ungleich“, „kleiner“ oder „größer“, möglich sind. Die Vorbedingungen werden durch Verknüpfungsoperatoren, wie z.B. Konjunktionen oder Disjunktionen, zu Regel-Rahmen zusammengefasst. Logische Aussagen von Regel-Rahmen können auch als Vorbedingung für andere Generierungsregeln verwendet werden.

Aufgrund der Vorbedingung, die entweder erfüllt oder nicht erfüllt ist, kann eine Nachbedingung in Form eines Dann-Blocks aktiviert werden. Der Dann-Block besteht aus einem True-Block (Vorbedingung erfüllt) und einem False-Block (Vorbedingung nicht erfüllt). Ähnlich wie bei den Ersetzungsregeln können andere Fragen automatisch (verdeckt) beantwortet werden, aber auch andere „direkte“ Aktionen, wie z.B. Antworttexte oder „Grafiken ausgeben“, ausgeführt werden. Es können zudem schon bestehende Antworttexte von Schwachstellen-Fragen mit dem entsprechenden Dann-Block verknüpft werden. Generierungsregeln bieten durch den flexiblen Dann-Block eine Schnittstelle zu unformalen und semiformalen Dokumenten an, wie z.B. Kriteriendokumente oder relevante Gesetzesabschnitte.

Rahmen können wiederum Rahmen besitzen, wodurch eine Strukturierung bzw. Klammerung entsteht. Hierfür wird folgende hierarchische Darstellung verwendet. Mit Hilfe des Regel-Rahmens können somit komplexe Regeln entwickelt werden.

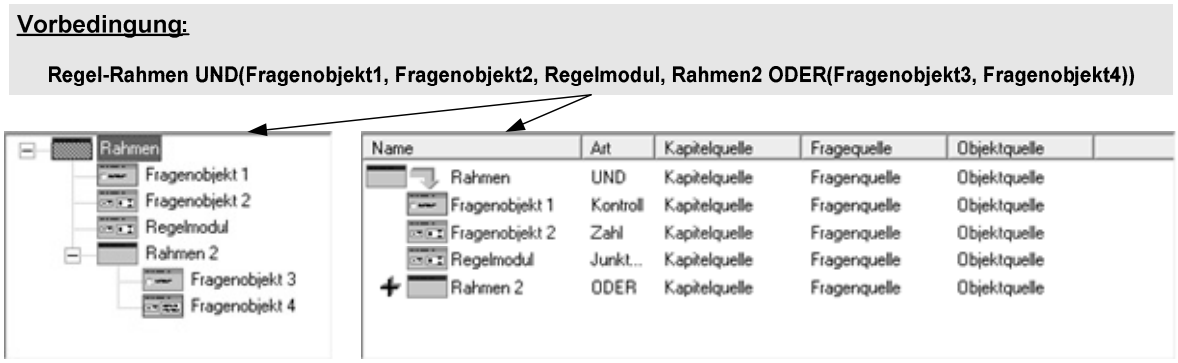


Abbildung 142: Hierarchische Darstellung der Modul-Rahmen

Durch die Auswertung der Generierungsregeln können direkte sowie komplexe Schwachstellen ermittelt werden. Die Antworten der „Maßnahmen-Fragen“ oder „Konsequenzen-Fragen“ werden hierfür als Merkmale interpretiert. Die jeweiligen Merkmale sind mit „Dann-Blöcken“ verknüpft, die „direkte“ Diagnosen bzw. Schwachstellen darstellen. Mehrere Merkmale können mit Hilfe von Verknüpfungsoperatoren zu einem Regel-Rahmen zusammengefasst werden. Die Ergebnisse der „Dann-Blöcke“ stellen die direkten Schwachstellen dar.

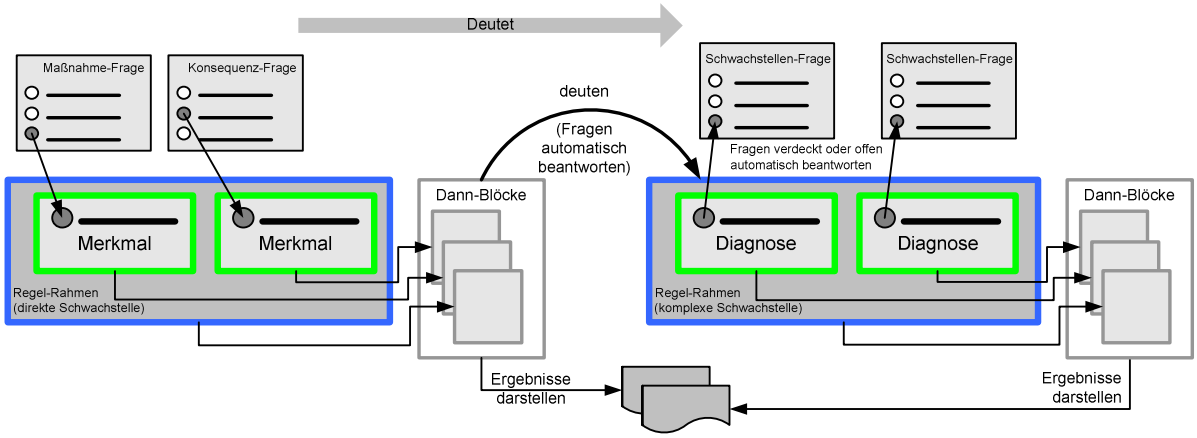


Abbildung 143: Generierungsregeln für assoziative Schwachstellen

Für komplexe Schwachstellen werden verknüpfte Generierungsregeln ausgewertet. Die „Dann-Blöcke“ sind zu diesem Zweck mit einem anderen Regel-Rahmen verknüpft. Bei der Aktivierung des zugehörigen Regel-Rahmens (Diagnose) wird der Regel-Rahmen erfüllt bzw. als „wahr“ angenommen. Die verbundenen Schwachstellen-Fragen können somit entweder „verdeckt“ oder „offen“ automatisch beantwortet werden.

Für Diagnosen, die weitere Test-Merkmale benötigen, werden Test-Fragen aktiviert. Die Aktivierung der Test-Fragen erfolgt über „Dann-Blöcke“. Die zusätzlichen Test-Fragen sind entweder weitere Maßnahmen-Fragen oder Konsequenzen-Fragen, die in einem Regel-Rahmen

(Test-Bereich) zusammengefasst werden. Auf Basis der Test-Merkmale werden einerseits die verdächtigen Schwachstellen bestätigt oder widerlegt, anderseits werden eventuell zusätzlich verfeinerte Schwachstellen abgeleitet.

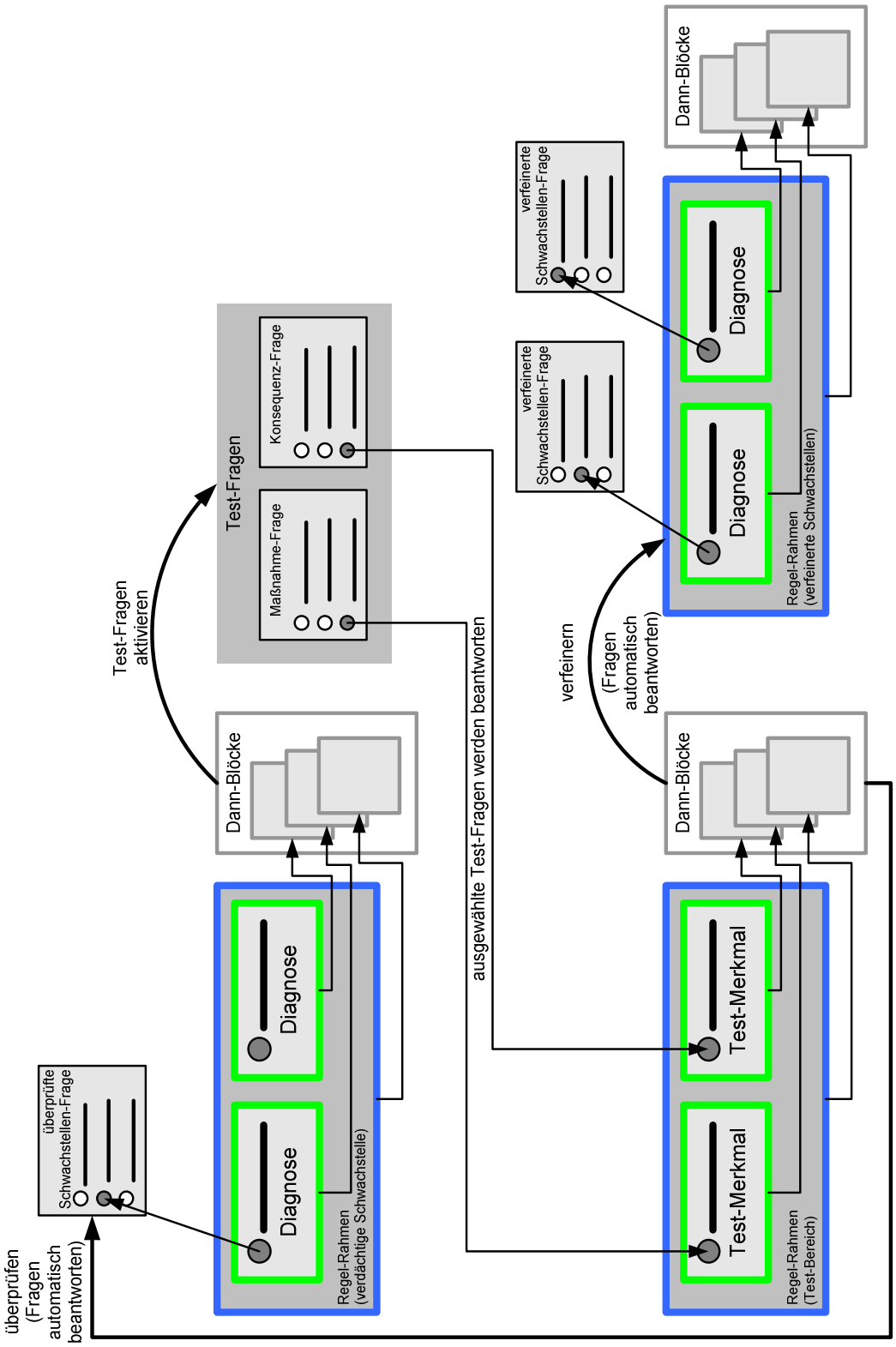


Abbildung 144: Tests mit Hilfe von Generierungsregeln

Die Repräsentation der kausalen Abhängigkeiten zwischen gefährdenden Ereignissen und deren Konsequenzen mit Hilfe von Generierungsregeln können für eine Wirkungs- und Ursachenanalyse verwendet werden. Hierfür werden mögliche Gefahren und sicherheitsrelevante Elemente mit Hilfe eines Regel-Rahmens zusammengefasst. Dieser Regel-Rahmen entspricht einem gefährdenden Ereignis. Bei einer Wirkungsanalyse werden die entsprechenden Regel-Rahmen als erfüllt bzw. als „wahr“ angenommen und die verknüpften Konsequenz-Fragen automatisch beantwortet. Diese Vorgehensweise entspricht einer vorwärtsorientierten Vorhersage.

Im Rahmen der Ursachenanalyse können die Generierungsregeln nicht direkt angewandt werden. Somit werden die gefährdenden Ereignisse (Ursachen) gemäß der Generierungsregeln „ausgewählt“, die die erhobenen Konsequenzen (Wirkungen) erklären bzw. überdecken. Des Weiteren werden die zugehörigen Gefahren- und gefährdenden Element-Fragen automatisch beantwortet. Diese Vorgehensweise entspricht einer rückwärtsorientierten Überdeckung.

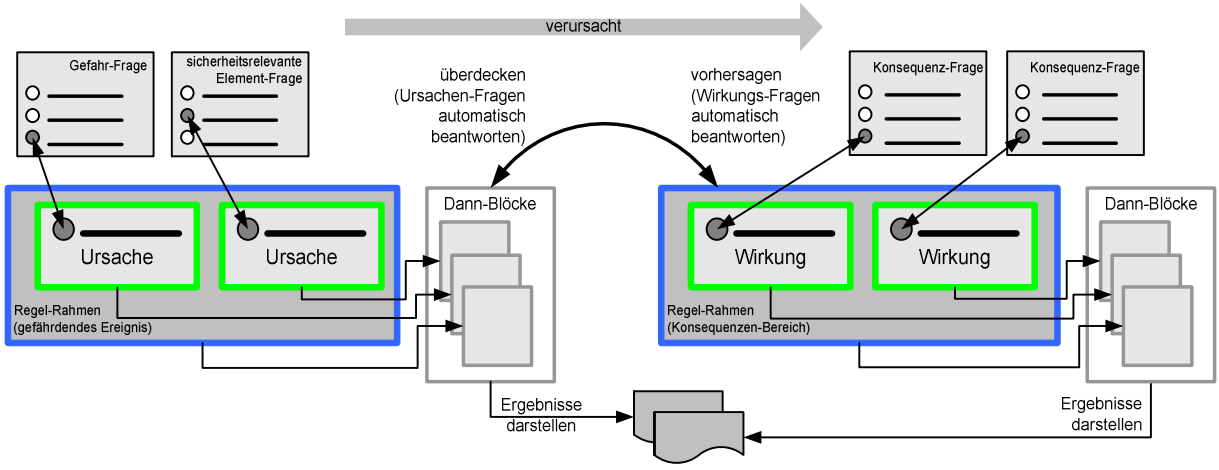


Abbildung 145: Generierungsregeln für kausale Ursachen-Wirkungen

Eine Überprüfung von Wirkungen und Ursachen erfolgt durch weitere verknüpfte Wirkungen und Ursachen. Somit können Folge-Konsequenzen und Ursprungs-Ursachen ermittelt werden. Hierbei ist zu beachten, dass eine Gefahr (Ursache) in einem anderem Kontext eine Konsequenz (Wirkung) darstellen kann. Eine Konsequenz-Frage (Wirkung) kann somit in einem anderen Regel-Rahmen als eine Ursache interpretiert werden. Das Ergebnis eines Regel-Rahmens (zusammengesetzter Konsequenzen-Bereich oder ein zusammengesetzter Ursachen-Bereich) kann in einem anderen Regel-Rahmen verwendet werden. Mit einer iterativen Überdeckung sind die Ursprungs-Ursachen darstellbar und mit einer iterativen Vorhersage die Folge-Konsequenzen.

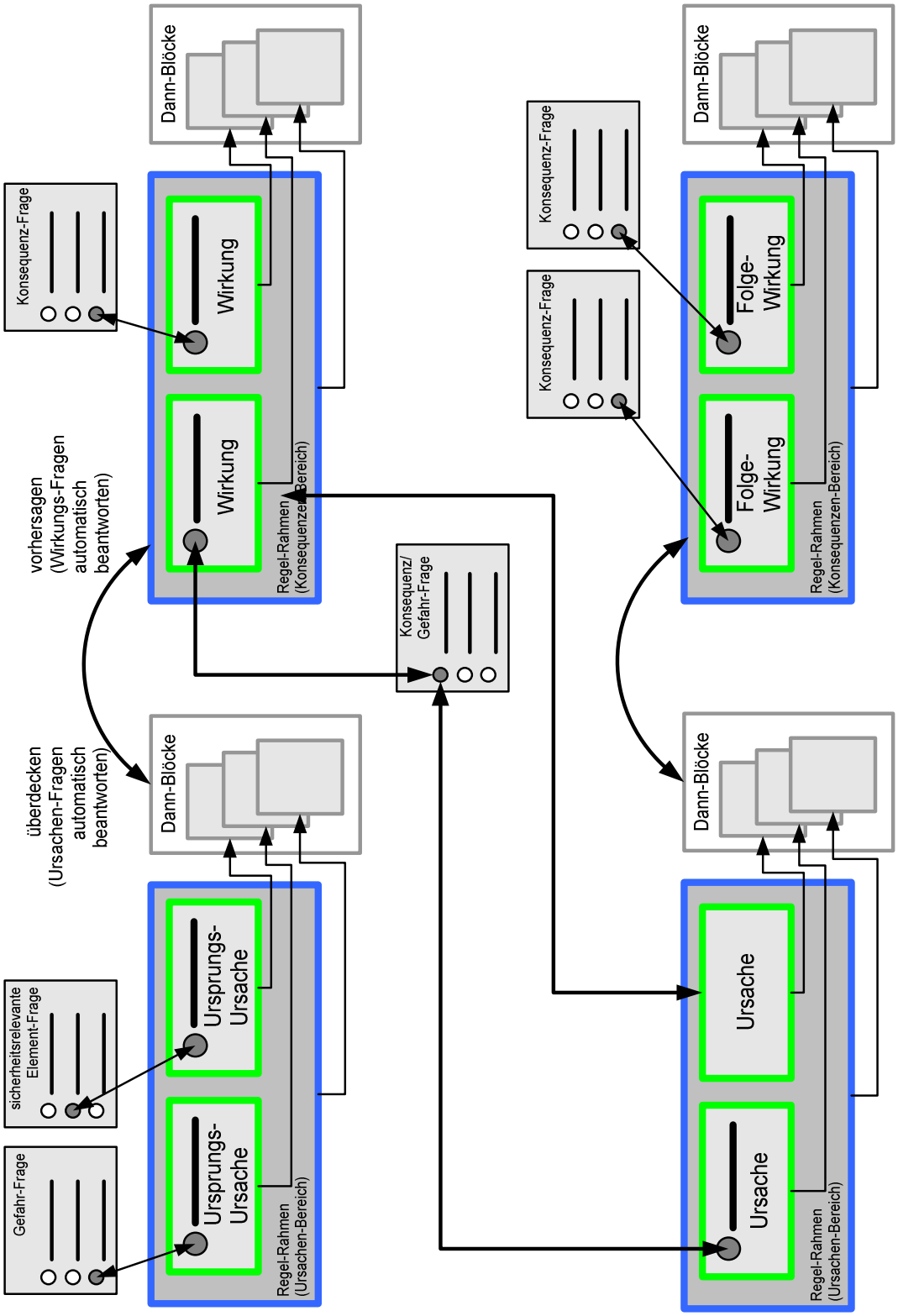


Abbildung 146: Überprüfung der Wirkungen und Ursachen

Erfassungstool

Bei einer wissensbasierten Frage ist zwischen externem Verhalten (Interviewer) und interner Sicht (Aufbau der Wissensbasis) zu unterscheiden. Die interne Struktur wird durch den Schablonen- und Fragengenerator sowie durch „Generatoren“ zur Regel-Erstellung bestimmt; das Erfassungstool stellt für den Interviewer die externe Sicht dar. Für den Interviewer besitzt die Software-Ergonomie während der Befragung und Auswertung eine hohe Relevanz, so dass sich der Interviewer nur noch auf die Erfassung beschränkt. Dies betrifft die einheitliche Darstellung der Fragen, die individuelle Steuerbarkeit der Fragenabfolge oder die komfortable Beantwortung der Fragen durch eine grafische Oberfläche. Weiterhin erhält der Interviewer während der Befragung zu den einzelnen Fragen Hilfestellung in Form eines Glossars. Die Abbildung zeigt eine Frage im Erfassungstool und die wesentlichen Funktionen. Systemfunktionen wie Anmeldung, Beendigung oder Drucken werden nicht weiter erläutert.

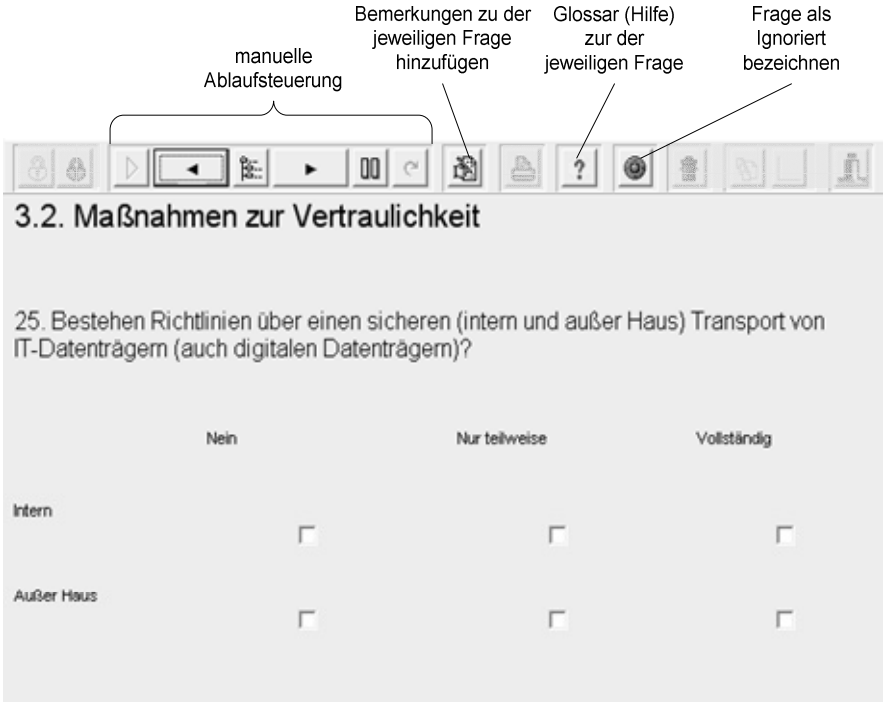


Abbildung 147: Beispiel einer Frage im Erfassungstool

Der Grundverlauf des Interviews wird durch die Kapitel- und Fragenstruktur und durch die Interpretation der Regel bestimmt. Das Erfassungstool ist somit eng mit der Ablaufsteuerung, die die automatische Auswahl von Fragen steuert, verbunden. Es sind auch manuelle bzw. benutzerbedingte Sprünge innerhalb des Fragenkatalogs möglich, wenn zusätzliche Informationen bei der Befragung auftauchen, die eine Richtungsänderung erzwingen. Der Benutzer hat auch die Möglichkeit, manuell Fragen zu ignorieren. Diese Fragen fließen nicht in die Auswertung ein, wodurch der Interviewer die Problemlösung direkt beeinflussen kann.

5.3.2 Wissensnutzungskomponente

Die Wissensnutzungskomponente hat folgende Aufgaben, welche durch vielfältige Interdependenzen geprägt sind:

- Festlegung der IS-Sicherheitsstrategie
- Ablaufsteuerung der Anpassung und Erhebung
- Hypothesengenerierung und -überprüfung
- qualitative und quantitative Auswertung
- Erklärung der Ergebnisse.

Problemlösungsgenerator
Dieser Bereich nimmt eine zentrale Stellung innerhalb der Wissensnutzungskomponenten ein, da es das domänen- und fallspezifische Wissen auswertet. Das Problemlösungsmodul legt das Problemlösungsverhalten durch Konfiguration der jeweiligen Problemlösungsmethode fest, die die IS-Sicherheitsstrategie repräsentiert. Auf Basis der IS- Problemlösungsmethode wird festgelegt,

- welche Fragen ausgewählt und erhoben werden,
- welche Regeln für die Hypothesengenerierung und -überprüfung aktiviert und
- in welcher Form diese interpretiert werden.

Die Auswahl der Fragen sowie die Aktivierung und Interpretation der Regeln wurde im Entwurfsmodell explizit beschrieben.

Aus klassischer Sicht erfolgt durch den Problemlösungsgenerator die Interpretation der Regeln auf Basis der gewonnenen Fakten bzw. Antworten der Fragen. Die Verknüpfungsregeln sowie die assoziativen Ersetzungs- und Generierungsregeln können direkt angewandt werden, wohingegen bei der überdeckenden Diagnose die rückwärtsorientierte Interpretation der kausalen Ersetzungs- und Generierungsregeln schwieriger ist. Die Interpretation bestimmt wiederum die Ablaufsteuerung des Erfassungstools, wodurch das Erfassungstool den expliziten Ausdruck der Hypothesengenerierung und -überprüfung darstellt.

Quantitative und qualitative Auswertung
Bei der Erhebung wird der angepasste Fragenkatalog beantwortet. Nach Beendigung erfolgt eine quantitative und qualitative Auswertung. Die qualitative Auswertung bietet durch Antwortbausteine Möglichkeiten, um Lösungen darzustellen. Hierdurch können auf einer ersten Auswertungsstufe Statusberichte erzeugt werden. Die Statusberichte basieren auf einem RTF-Dokument, das in Fließtextform oder tabellarischer Form die ermittelten Beobachtungen sowie hergeleitete Merkmale und Lösungen darstellt. Um Beobachtungen, Merkmale und Lösungen auch optisch differenziert darzustellen, können die Ergebnisse frei formatiert werden (z.B. Schriftfarbe, -größe oder -art). Insgesamt besitzt der Statusbericht den Charakter einer vorstrukturierten Arbeitsgrundlage für ein Sicherheitskonzept, das z.B. Schwachstellen und erforderliche Maßnahmen in Textform wiedergibt. Bemerkungen, die während der Erhebung vermerkt worden sind, werden zusätzlich ausgegeben.

Um eine differenziertere qualitative Auswertung zu erlangen, werden die assoziativen und kausalen Abhängigkeiten explizit in einem Dokument abgebildet, um auch den Lösungsprozess nachzuvollziehen. Hierfür werden HTML-Dokumente verwendet, welche auf Verknüpfungen der Antwortbausteine basieren und somit eine Strukturierung bieten. Somit besitzt das Dokument gleichzeitig ein Erklärungsmodul, da z.B. Schwachstellen mit deren fehlenden Maßnahmen einerseits oder Wirkungen mit deren Ursachen anderseits verknüpft sind. In der Abbildung wird die Grundstruktur für die HTML-Darstellung einer präventiven Top-Down und reaktiven Bottom-Up Problemlösung dargelegt.

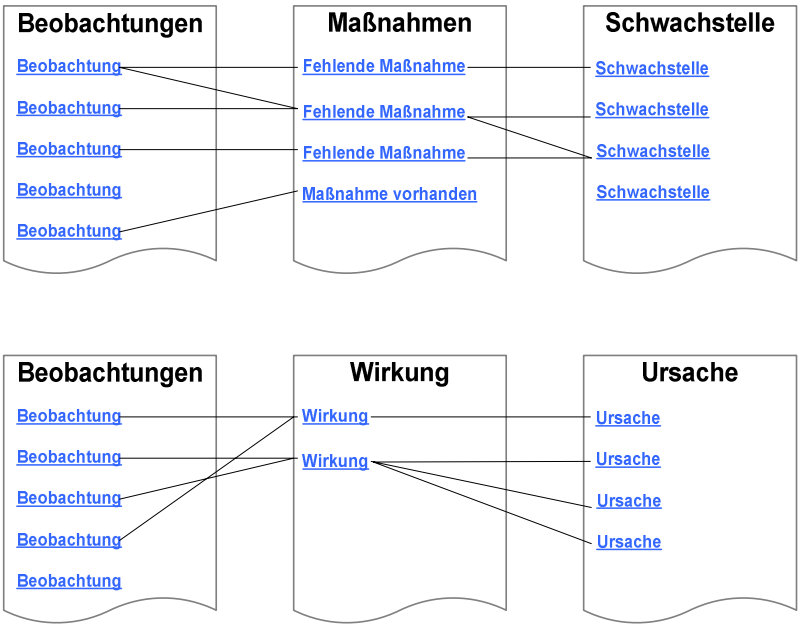


Abbildung 148: Auswertung durch HTML-Dokumente

Eine quantitative Auswertungserweiterung erfolgt durch Ermittlung von quantitativen Werten für die jeweiligen Fragen. Werden die Fragen in Kapitel und Unterkapitel strukturiert, kann für das jeweilige Kapitel auch ein Kapitelwert ermittelt werden, wobei zusätzlich eine Gewichtung der Fragen innerhalb des Kapitels erfolgt, wodurch brisantere Fragen höher gewichtet werden. Besteht eine Kapitelstruktur, so können wiederum die (Unter-)Kapitelwerte gewichtet und zu einem relativen Kapitelwert rekursive summiert werden. Diese ermittelten Werte können auf einer Skala (z.B. 1...100) normiert und als Indikatoren für potentiell sicherheitsrelevante Aspekte verwendet werden[586]. Die ermittelten Werte sind als Warnsignal für eine Abweichung von dem Soll-Wert gedacht - ähnlich der Ampeldarstellung. Eine feinere Einteilung, die mehr als drei Werte aufweist, ist nicht sinnvoll, da nur eine Tendenz aufgezeigt werden soll[587].

[586] So kann z.B. der Wert zwischen den Grenzen [1...33] „Schwachstelle existiert“, zwischen [34...66] „akzeptable Schwachstelle“ und zwischen [67..100] „keine Schwachstelle“ bedeuten.
[587] Ein ähnliches quantitatives Bewertungsmodell für den Datenschutz wird in Königshofen (1997) beschrieben.

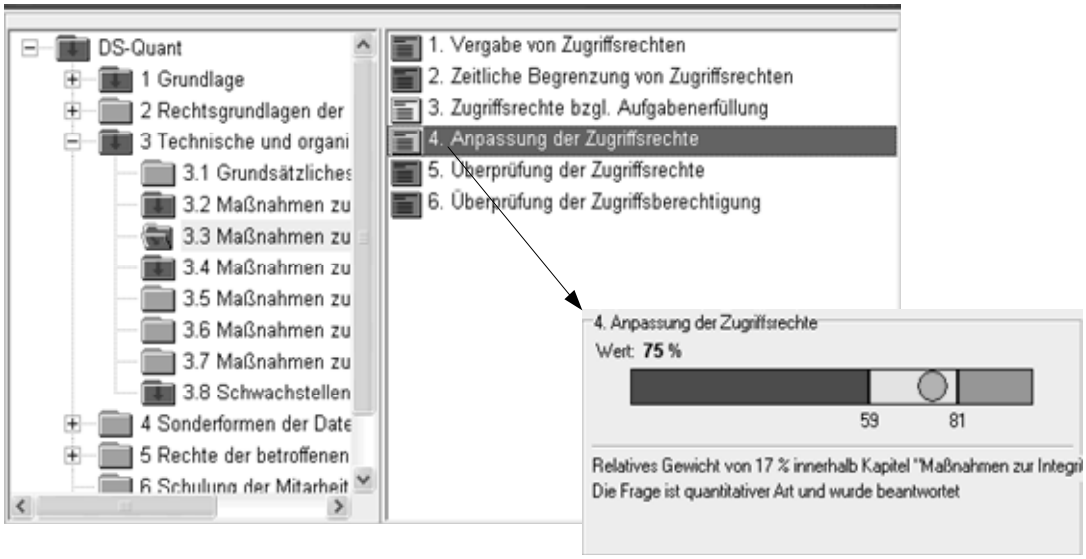


Abbildung 149: Beispiel einer quantitativen Auswertung

In der Abbildung ist ein Beispiel für die quantitative Auswertung dargestellt. Es wird ersichtlich, dass sich die Quantifizierung rekursiv an der Kapitelstruktur orientiert, was eine Erklärungskomponente in sich birgt, da die Wertberechnung nachvollziehbar ist.

Die Methoden der quantitativen Art besitzen das grundlegende Problem, dass versucht wird, auf ein schlecht strukturiertes Problem ein wohl strukturiertes bzw. allgemeingültiges Modell anzuwenden. Die qualitative Auswertung bietet dagegen komplexere Möglichkeiten, um Lösungen darzustellen. Deshalb dient die quantitative Auswertung als Ergänzung und nicht als Ersatz für die qualitative Problemlösung.

5.3.3 Bewertung der Realisierung

Die vorgestellte Realisierung stellt eine prototypische Operationalisierung des Expertisemodells dar. Wie bei dem Entwurfsmodell steht die Umsetzung des Top-Down Ansatzes mit Hilfe eines wissensbasierten Fragenkatalogs im Vordergrund. Dies beinhaltet insbesondere die Repräsentation vom heuristischen Erfahrungswissen und deren assoziativen Abhängigkeitskonzepten. Der Prototyp ermöglicht durch seine offene Struktur die Repräsentation von mehreren Kriterienwerken und Datenschutzaspekten. Somit ist der Prototyp unabhängig von einem Kriterienwerk. Zudem lassen sich institutionsindividuelle IS-Sicherheitsaspekte hinzufügen. Dieses umfangreiche IS-Sicherheitswissen kann direkt auf eine IS-Sicherheitsproblemstellung angewendet werden.

Mit den unterschiedlichen Ausprägungsformen von wissensbasierten Fragenkatalog-Regeln ist es möglich, die Basis-Inferenzen Merkmalserkennung, Hypothesengenerierung und Hypothesenüberprüfung der heuristische Klassifikation bzw. Diagnose zu unterstützen. Für eine einfache direkte Merkmalserkennung und Hypothesengenerierung sind Verknüpfungsregeln ausreichend, die sich durch ihren einfachen Aufbau auszeichnen. Zudem sind Verknüpfungsregeln eng mit der Erhebungssteuerung verknüpft. Um umfangreichere Hypothesengenerierungen und -überprüfungen zu konstruieren, können ergänzend Ersetzungsregeln verwendet

werden. Eine komplexe Hypothesengenerierung und -überprüfung ist mit den Generierungsregeln erreichbar, die sich durch eine getrennte Repräsentation von Regeln und Fragen auszeichnen.

Um die qualitativen Ergebnisse einer IS-Sicherheitsanalyse mit quantitativen Aussagen zu ergänzen, unterstützt der Prototyp eine rekursive Auswertung von gewichteten Kapitel- und Fragenwerten. Dies ermöglicht die Repräsentation von quantitativem Bewertungswissen.

Durch die Generierungsregeln ist eine Repräsentation von kausalen Abhängigkeiten möglich, die eine modellbasierte Diagnose unterstützen. Aber auf Grund einer schnell zunehmenden Komplexität bei umfangreichen Generierungsregeln sind nur einfache kausale Abhängigkeiten zu beschreiben. Für umfangreiche Bottom-Up orientierte Ursachen- und Wirkungsanalysen ist eine kausale Erweiterung des wissensbasierten Fragenkatalogs denkbar, die auf den Konzepten von Stelzer (1993), Konrad (1998) und Thoben (2000) basiert. Hierbei kann der wissensbasierte Fragenkatalog die Aufgabe einer intelligent gesteuerten Erhebung und Ausgabe für eine modellbasierte Diagnose übernehmen.

Eine weitere sinnvolle Ergänzung würde eine fallbasierte Problemlösung darstellen, die basierend auf historischen Vorfällen und aktuell erhobenen Merkmalen eventuell schon erarbeitete Lösungen anbieten kann. Auf statistische Ergänzungen in Form einer klassischen Risikobewertung wurde verzichtet, da deren notwendigen Voraussetzungen meist nicht gegeben sind und dadurch Aussagen einer statistischen Auswertung problematisch sind.

6 Schlussbetrachtung

6.1 Zusammenfassung

Die Wissensnutzung des IS-Sicherheitswissens im Rahmen des IS-Sicherheitsmanagements stand im Mittelpunkt der Arbeit. Hierfür wurden Methoden des Knowledge Engineerings verwendet, um die IS-Sicherheitsstrategien durch Problemlösungsmethoden zu beschreiben. Das benötigte IS-Sicherheitswissen wird durch IS-Sicherheitskonzepte repräsentiert. Als Ergebnisse der Arbeit sind Modelle auf unterschiedlichen Abstraktionsstufen entwickelt worden. Deren Ergebnisse sind in einen wissensbasierten Diagnose-Prototyp eingeflossen, der zur Unterstützung des IS-Sicherheitsmanagements dient.

Grundlage für den Entwicklungsprozess bildeten wissensbasierte Modellierungsansätze, die vor der Operationalisierung die Konstruktion eines epistemologischen Expertisemodells auf der Wissensebene erfordern. Hierfür wurde im ersten Kapitel ein Entwicklungsrahmen für das Knowledge Engineering des IS-Sicherheitsmanagements entwickelt. Dieser stellt auch gleichzeitig den Grundaufbau der Arbeit dar. Das IS-Sicherheitsmanagement bildet den Rahmen für die Wissensakquisition. Als Ergebnis der Wissensakquisition werden Problemlösungen und Konzepte durch ein epistemologisches Expertisemodell auf einer Wissensebene beschrieben. Dies geschieht unabhängig von einer konkreten Repräsentationsform. Das Expertisemodell stellt die Schnittstelle zu der Wissensoperationalisierung dar. Die Wissensoperationalisierung beinhaltet als Ergebnis ein Entwurfsmodell und darauf basierend ein Diagnose-WBS für das IS-Sicherheitsmanagement. Nach der Konstruktion des WBS soll der Fachexperte weitgehend unabhängig von einem Knowledge Engineer das IS-Sicherheitswissen direkt eingeben, pflegen und nutzen können.

Im zweiten Kapitel wurden zuerst die begrifflichen und inhaltlichen Grundlagen für das IS-Sicherheitsmanagement geschaffen, wobei insbesondere die Beschreibung der IS-Sicherheitsstrategien fokussiert ist. Hierfür wurde ein Phasenmodell des IS-Sicherheitsmanagements entwickelt, das die wesentlichen Schritte zur Schaffung von IS-Sicherheit beschreibt, aber auch den Rahmen für die IS-Sicherheitsziele und die IS-Sicherheitsstrategien vorgibt. Die wesentlichen Aspekte der IS-Sicherheitsstrategien werden durch ein deskriptives Modell des integrierten IS-Sicherheitsmanagements aufgezeigt. Die Beschreibung der IS-Sicherheitsstrategie bildet die Grundlage für die Problemlösungsmethoden des Expertisemodells und dessen Operationalisierung.

Die IS-Sicherheitsstrategien wurden in dieser Arbeit in Top-Down und Bottom-Up Ansätze eingeteilt, die unterschiedliche Eigenschaften und Anforderungen besitzen. Der Top-Down Ansatz beruht auf der direkten Anwendung von unternehmensunabhängigen IS-Sicherheitskriterien auf einem Informationssystem, wohingegen der Bottom-Up Ansatz das unternehmensindividuelle Informationssystem durch ein Systemmodell abbildet, um dann darauf kausale Ursachen-Wirkungsmodelle anzuwenden. Die beiden IS-Sicherheitsstrategien wurden durch eine verhinderungsorientiert präventive und erklärungsorientiert reaktive

Sichtweise für die IS-Sicherheit erweitert. Die präventive Sichtweise ermöglicht, fehlende Maßnahmen im Vorfeld zu ermitteln. Die reaktive Sichtweise erlaubt, adäquat auf schon eingetretene gefährdende Ereignisse zu reagieren.

Im dritten Kapitel sind die IS-Sicherheitsstrategien durch diagnostische Problemlösungen und die dafür benötigten IS-Sicherheitskonzepte in einem Expertisemodell weitgehend unabhängig von einer späteren Operationalisierung beschrieben. Hierfür wurden zuerst die wesentlichen Erhebungsmethoden dargestellt und Wissensquellen identifiziert, wobei insbesondere das implizite Expertenwissen, die expliziten IS-Sicherheitskriterien und das Vorschriftenwissen für die Arbeit von Bedeutung sind. Das Expertisemodell besteht aus der Aufgaben-, Inferenz und Domänenebene, in der die Domänenebene die IS-Sicherheitskonzepte des IS-Sicherheitsmanagements darstellt. Es wird zwischen Basiskonzepten, wie z.B. Schwachstellen, Gefahren oder Konsequenzen sowie kausalen und assoziativen Abhängigkeits- bzw. Problemlösungskonzepten, unterschieden. Die Basiskonzepte werden weitgehend unabhängig von einer Problemlösungsmethode beschrieben, wohingegen die Problemlösungskonzepte der Domänenebene eng mit der Aufgaben- und Inferenzebene verknüpft sind, denn

- der Top-Down Ansatz verwendet heuristische Problemlösungsmethoden auf Basis von assoziativen und hierarchischen Problemlösungskonzepten;
- der Bottom-Up Ansatz verwendet modellbasierte Problemlösungsmethoden auf Basis von kausalen Problemlösungskonzepten.

Die Problemlösungsmethode wird durch die Aufgabenebene und Inferenzebene des Expertisemodells beschrieben. Die Aufgabenebene des Expertisemodells stellt das Ziel sowie die generischen Lösungsschritte der diagnostischen Problemlösung dar. Auf einer Inferenzebene werden die konkreten Problemlösungsmethoden durch Wissens-Rollen und Inferenzen spezifiziert. Das Expertisemodell bietet monofunktionale Problemlösungsmethoden an, die stark von den Problemlösungskonzepten abhängig sind. Dies hat den Vorteil, dass der Wissensakquisitionsprozess weitgehend durch die jeweilige Problemlösungsmethode gesteuert wird. Um auch eine flexible Kombination der IS-Sicherheitsstrategien zu erreichen, wurde das Expertisemodell durch multifunktionale Templates erweitert. Die Templates beschreiben die wesentlichen Aspekte der Inferenz-Strukturen der IS-Sicherheitsstrategien weitgehend unabhängig von den spezifischen Problemlösungs- bzw. Abhängigkeitskonzepten. Die Templates können jedoch wiederum nachträglich mit den benötigten Abhängigkeitskonzepten ergänzt werden. Hierdurch lassen sich durch die Kombination von unterschiedlichen IS-Sicherheitsstrategien umfangreiche Problemlösungs-Szenarien auf einer Wissensebene aufzeigen.

Im vierten Kapitel wurden verschiedene Repräsentationsformen als Basis für eine Operationalisierung vorgestellt, die entweder auf einer anpassungsorientierten oder anwendungsorientierten Überführung des unternehmensunabhängigen IS-Sicherheitswissens basieren. Durch die anpassungsorientierte Überführung können unternehmensindividuell objektorientierte Systemmodelle der Systemlandschaft konstruiert werden, die eine kausale Ursachen- und Wirkungsanalyse unterstützen. Diese modellbasierte Diagnose wird insbesondere bei dem Bottom-Up Ansatz verwendet. Die anwendungsorientierte Überführung beruht dagegen auf Fragenkatalogen, die eine direkte Wissenseingabe und Wissensnutzung des IS-Sicherheitswissens durch einen IS-Sicherheitsexperten ermöglichen.

Im vierten Kapitel wurde ein Entwurfsmodell auf Basis von wissensbasierten Fragenkatalogen und Regeln entwickelt, das insbesondere den Top-Down Ansatz unterstützt. In einem gewissen Rahmen können aber auch kausale Abhängigkeiten beschrieben werden.

Im fünften Kapitel wurden zuerst die wesentlichen Komponenten eines WBS erörtert und vorhandene computergestützte Werkzeuge für das IS-Sicherheitsmanagement vorgestellt. Die vorgestellten Werkzeuge stammen entweder aus dem wissenschaftlichen Umfeld und stellen meist prototypische Realisierungen dar oder sie sind im praktischen Umfeld entstanden. Die Werkzeuge wurden in eine Top-Down oder Bottom-Up Strategieunterstützung sowie in eine anpassungs- oder anwendungsorientierte Überführungsstrategie des unternehmensunabhängigen IS-Sicherheitswissens eingeordnet. Zum Abschluss des Kapitels wurden die Architektur und Komponenten einer konkreten prototypischen Implementierung eines Diagnose-WBS beschrieben. Das Diagnose-WBS besitzt die Eigenschaft eines wieder verwendbaren wissensbasierten Werkzeuges (Shell), das unterschiedliche „Füllungen“ durch wissensbasierte Fragenkataloge repräsentieren kann.

6.2 Bewertung

Im Rahmen der Arbeit wurden unterschiedliche Modelle entwickelt, die die Ergebnisse der jeweiligen Hauptkapitel widerspiegeln. Hierbei bauen die Ergebnismodelle einerseits aufeinander auf, wobei sie anderseits in sich abgeschlossen sind, so dass sie z.T. unabhängig voneinander verwendet werden können.

IS-Sicherheitsstrategien des IS-Sicherheitsmanagements
Das Phasenmodell des IS-Sicherheitsmanagements beschreibt zuerst unabhängig von einer konkreten wissensbasierten Unterstützung den Rahmen zur Schaffung der IS-Sicherheit. Den zentralen Aspekt der Arbeit bilden die IS-Sicherheitsstrategien, die zur Umsetzung des Sicherheitsniveaus und der IS-Sicherheitsziele dienen und die Basis der Problemlösungsmethoden bilden. Zur Beschreibung der wesentlichen Eigenschaften und Anforderungen von konkreten IS-Sicherheitsstrategien wird ein deskriptives Modell der IS-Sicherheitsstrategien entwickelt, das auf Top-Down und Bottom-Up Ansätzen basiert. Das Modell wird durch eine reaktive und präventive Sichtweise erweitert, um ein weites Spektrum des IS-Sicherheitsmanagements zu beschreiben. Durch die Klassifikation der IS-Sicherheitsstrategien werden die Voraussetzungen zur Auswahl der geeigneten diagnostischen Problemlösung geschaffen, die sowohl die Basis für die Konzepte als auch die Problemlösungsmethoden des Expertisemodells darstellen.

Expertisemodell des IS-Sicherheitsmanagements
Basierend auf dem Modell der IS-Sicherheitsstrategien des integrierten IS-Sicherheitsmanagements werden die Problemlösungsmethoden und das benötigte IS-Sicherheitswissen in einem Expertisemodell des IS-Sicherheitsmanagements beschrieben. Das Expertisemodell bildet somit den zentralen Aspekt des modellorientierten Knowledge Engineerings, da auf einer epistemologischen Ebene Problemlösungsprozesse und das Domänenwissen beschrieben werden. Hiermit wird im Gegensatz zu dem Transferansatz die Entwicklung des WBS durch das Expertisemodell bestimmt und nicht durch schon bestehende Repräsentationsformen. Durch die Unabhängigkeit des Modells von einer Symbolebene können Problemlösungen der IS-Sicherheitsstrategien einerseits unabhängig von einer konkreten Operationalisierung dargestellt werden, anderseits können schon Anforderungen einer Operationalisierung der Domänenbasis und Problemlösung aufgezeigt werden.

Um eine von der Domänenbasis unabhängige Darstellung der Problemlösung der IS-Sicherheitsstrategien zu erlangen, werden Templates eingeführt. Diese beschreiben in einem ersten Schritt gemeinsame diagnostische Problemlösungsschritte der IS-Sicherheitsstrategien unabhängig von einer Domänenebene. Die Template-Strukturen können zudem aber wiederum schnell mit dem jeweiligen benötigten Domänenwissen und deren Abhängigkeitskonzepten erweitert werden. Des Weiteren können die Templates durch ihre Schnittstellen flexibel umfangreiche Problemlösungsszenarien von kombinierten IS-Sicherheitsstrategien beschreiben. Das Expertisemodell stellt insgesamt eine Schnittstelle zu der Operationalisierung dar, um die konzeptuelle Lücke zwischen der Akquisition des IS-Sicherheitsmanagements auf der Wissensebene und deren Operationalisierung auf der Symbolebene zu verringern.

Entwurfsmodell für das Diagnose-WBS

Die Konstruktion des Entwurfsmodells erfolgt unter der Prämisse einer direkten Wissenseingabe und Wissensnutzung durch einen IS-Sicherheitsfachexperten ohne zusätzliche Hilfe eines Knowledge Engineers. Durch Fragenkataloge und Regelstrukturen können Kriterienwerke, die die Basis für den Top-Down Ansatz bilden, adäquat und anwendungsorientiert abgebildet sowie direkt genutzt werden. Durch die regelbasierte Erweiterung können zudem Abhängigkeiten dargestellt werden, die jedoch nicht die gleiche Abbildungsqualität von kausalen Systemmodellen erreichen.

Am Ende des Kapitels wird erläutert, wie die diagnostischen Basis-Inferenzen (Merkmalserkennung, Hypothesengenerierung und -überprüfung) der jeweiligen IS-Sicherheitsstrategien des Expertisemodells auf das fragenkatalogorientierte Entwurfsmodell überführt werden. Das Entwurfsmodell bietet zusammenfassend eine konzeptuelle Grundlage für die spätere Implementierung von Fragenkatalogen durch ein WBS. Das Entwurfsmodell kann des Weiteren zur zusätzlichen Dokumentation im Rahmen einer Wartung und Pflege der fragenkatalogorientierten Wissensbasis eingesetzt werden.

Prototypische Implementierung des Diagnose-WBS

Eine Vorläuferversion des fragenkatalogorientierten Diagnose-WBS wird erfolgreich in der Berater-Praxis eingesetzt und besitzt mittlerweile unterschiedliche „Füllungen“ mit mehreren tausend Fragen und umfangreichen Regelstrukturen, die eine Analyse der IS-Sicherheit - basierend z.B. auf der BS 7799 und dem Datenschutz - unterstützt. Das Diagnose-WBS liefert qualitative sowie ergänzende quantitative Berichte, die eine umfassende Arbeitsgrundlage für ein IS-Sicherheitskonzept darstellen. Die direkte Wissenseingabe wird durch das WBS praktiziert, und zwar durch einen IS-Sicherheitsexperten ohne Unterstützung eines Knowledge Engineers. Dies ermöglicht eine anwendungsorientierte Umsetzung von IS-Sicherheitskriterien und unterstützt somit die wesentlichen Aspekte des Top-Down Ansatzes. Eine Umsetzung des Bottom-Up Ansatzes ist in der vorliegenden Version nur in Ansätzen möglich, da die Konstruktion eines umfangreichen individualisierten Systemmodells nicht möglich ist. Hierbei sei aber auf die Diskussion der meist fehlenden Voraussetzungen eines Bottom-Up Ansatzes und auf den folgenden Ausblick hingewiesen.

6.3 Ausblick

Das fragenkatalogorientierte Diagnose-WBS soll im Folgenden in einem erweiterten Rahmen von IT-basierten Wissensmanagementlösungen betrachtet werden. Es lassen sich hierfür folgende Aspekte unterscheiden[588]:

- Dokumentenorientierte Ansätze, die auf Basis impliziter und expliziter Klassifikation einer Dokumentensammlung deren Inhalte zugänglich machen.
- Wissensbasiert systemorientierte Ansätze[589], die das Wissen in einer formalisierten Form bereitstellen, um eine computergestützte automatische Verarbeitung zu unterstützen.

Bei den Ansätzen sollte die Ausgewogenheit zwischen Aufwand der Formalisierung des Wissens und dem zu erreichenden Nutzen einer Formalisierung beachtet werden. Sonst entsteht ein zu hoher Konstruktions- und Wartungsaufwand[590]. Ein Kompromiss zwischen Anwendbarkeit und formaler Abbildung erfolgte in der Arbeit durch die semiformale Repräsentation mit Hilfe von wissensbasierten Fragenkatalogen.

Ist ein hoher Abbildungsaufwand für bestimmte Bereiche, die z.B. ein sehr hohes Sicherheitsniveau benötigen, gerechtfertigt, bietet sich eine Erweiterung des fragenkatalogbasierten WBS in Form von objektorientierten Systemmodellen an. Diese Modelle ermöglichen eine umfangreiche modellbasierte und unternehmensindividuelle Ursachen-Wirkungs-Diagnose.

Es ist auch eine wenig bis nicht formale Repräsentationserweiterung für Dokumente in unstrukturierter bis strukturierter Textform (z.B. HTML-Dokumente) denkbar, so dass ein umfangreicher und direkter Zugriff auf unstrukturierte Wissensquellen möglich ist. Hierbei steht insbesondere der Wissenszugriff basierend auf Information Retrieval Funktionen im Vordergrund. Diese Funktionen unterstützen eine verknüpfte Recherche z.B. von mehreren Kriterienwerken und Gesetzestexten.

[588] Vgl. Staab et al. (2001), S. 27
[589] Staab et al. (2001) nennen diesen Ansatz „Expertensystemorientierte Ansätze“.
[590] Z.B. umfangreiche Abbildung einer konkreten Informationssystemstruktur und deren sicherheitsrelevanten Abhängigkeiten.

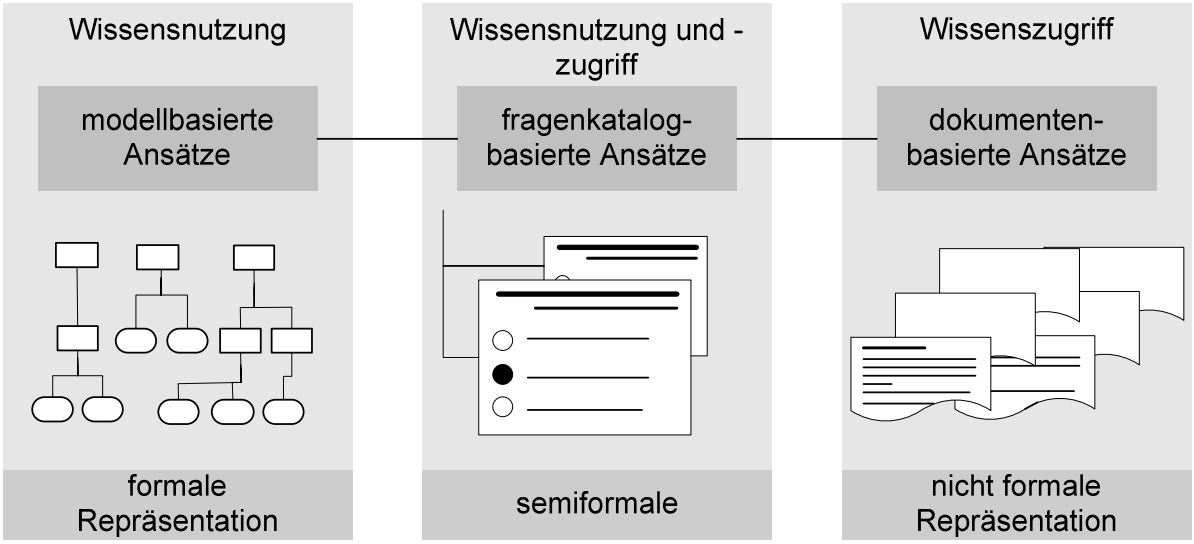


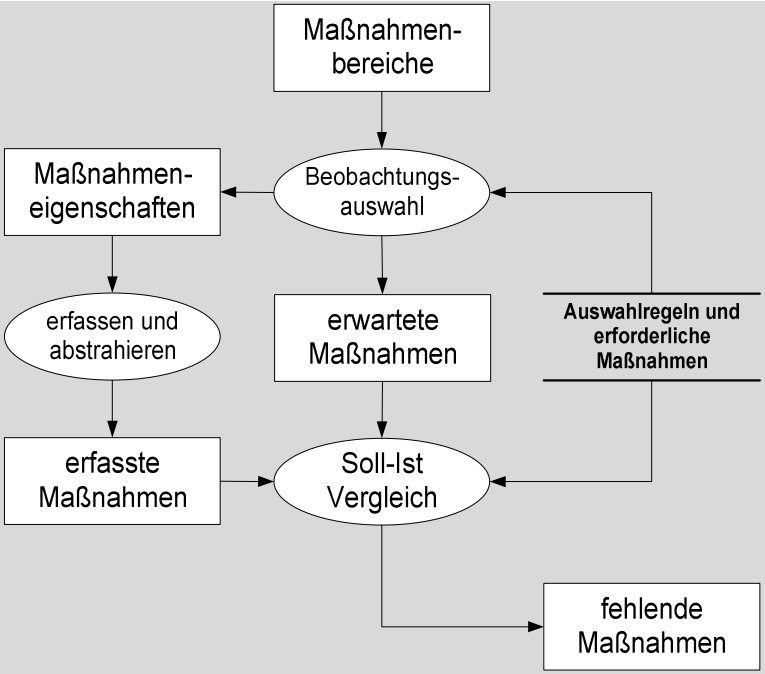
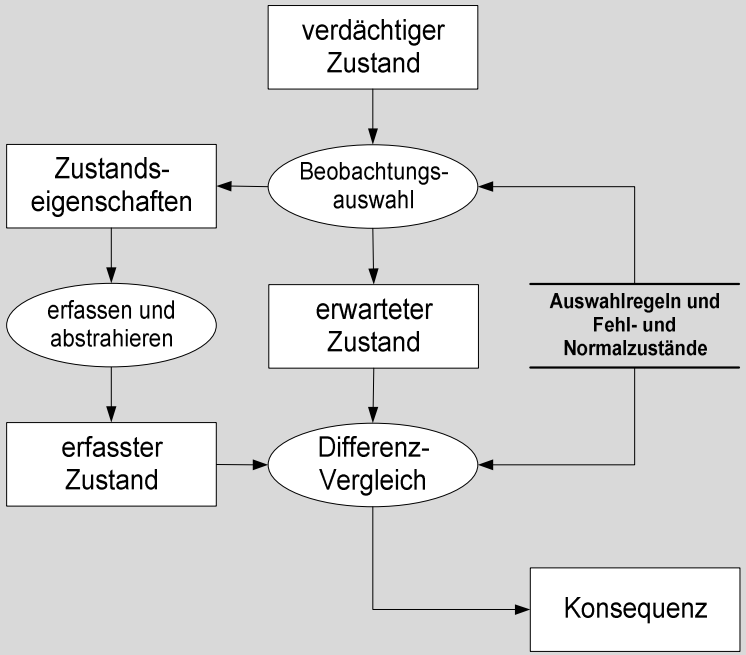
Abbildung 150: Erweiterung des fragenkatalogbasierten Ansatzes um einen modellbasierten und dokumentenbasierten Ansatz

Wissensbasierte Fragenkataloge können somit dahingehend erweitert werden, dass sie eine Verknüpfung zu Systemmodellen und Textdokumenten aufweisen. Hierbei sind folgende Vorteile zu erwarten:

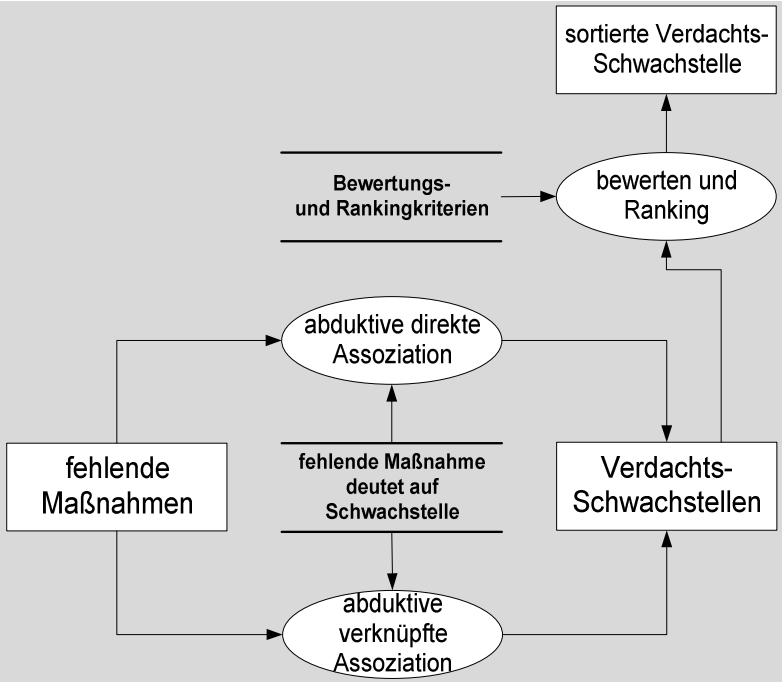
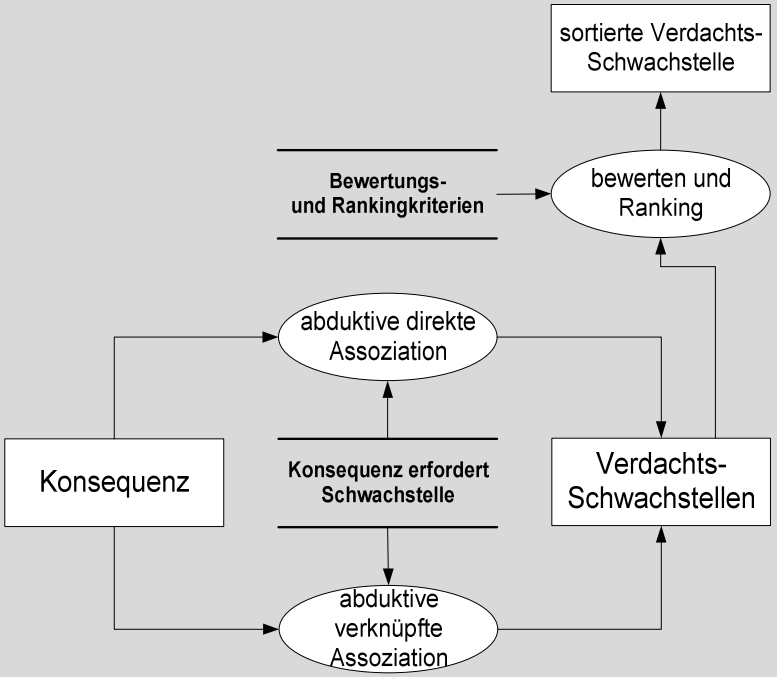
- So könnten die durch Fragenkataloge erhobenen Informationen in ein Systemmodell einfließen. Ergebnisse einer modellbasiert kausalen Diagnose können zudem als automatisiert erzeugte Ursachen- oder Wirkungsantworten in einem Fragenkatalog verarbeitet werden.
- Um die Ergebnisse einer fragenkatalogorientierten Diagnose zu untermauern, könnten Textpassagen direkt aus Kriterienwerken und Gesetzestexten in den Ergebnisbericht eingefügt werden. Zudem könnten Referenzen auf weitere Quellen „hinweisen“, um für eine tiefergehende Analyse einen direkten Zugang zu den adäquaten Wissensquellen zu verschaffen.

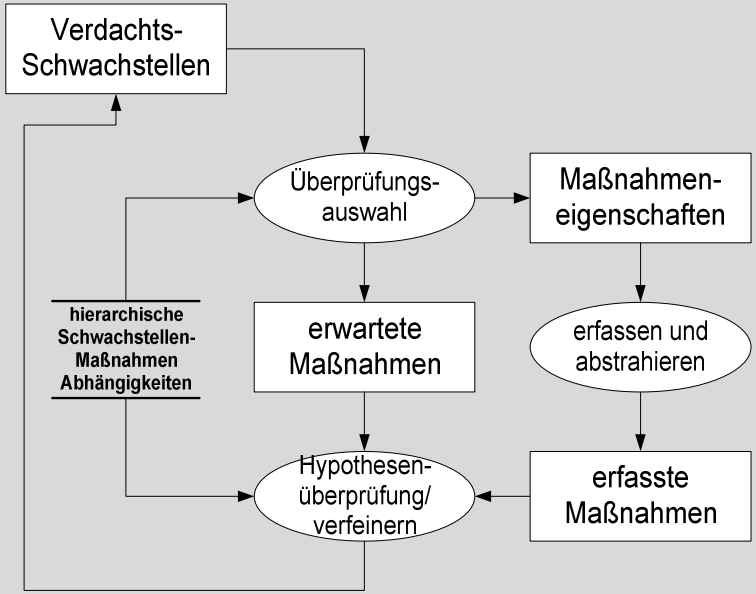
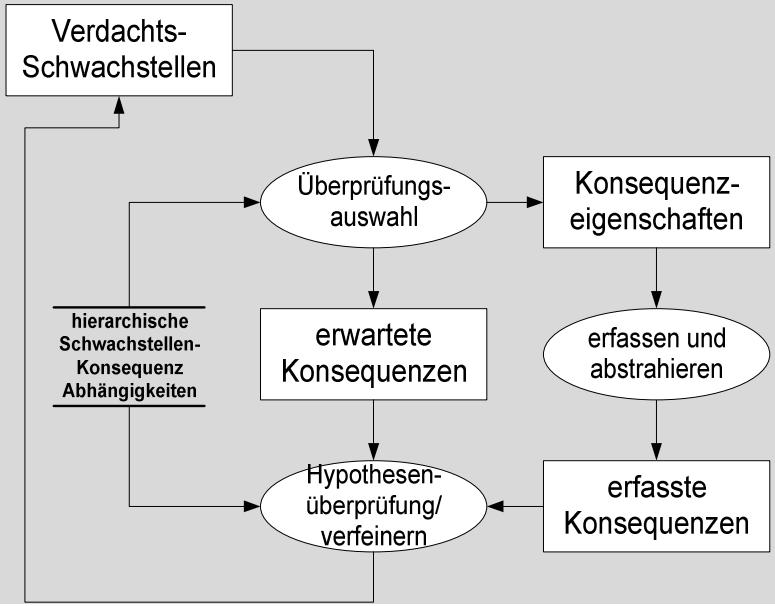
Anhang A

Basis-Inferenzen der IS-Sicherheitsstrategien

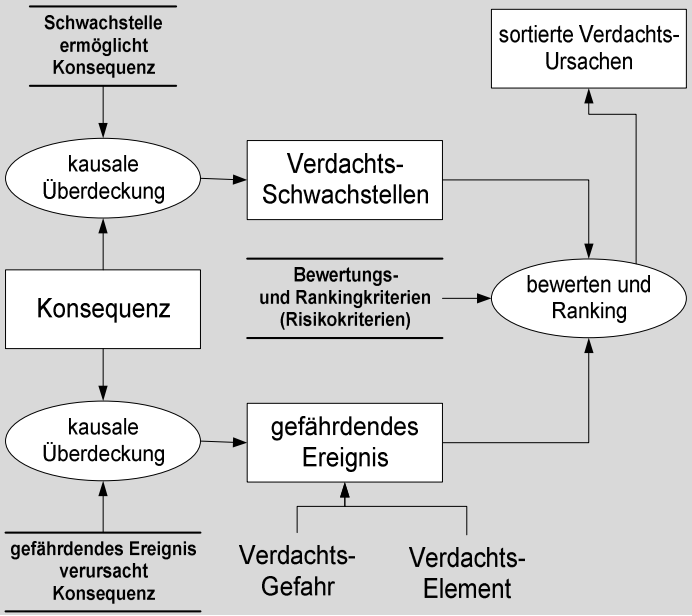
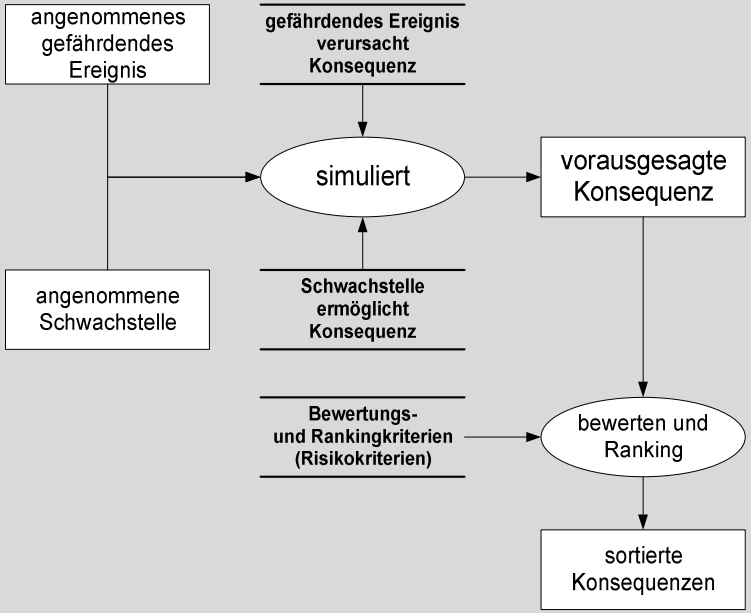
Merkmalserkennung	
Präventiv	Reaktiv
	
Eingang: Maßnahmenbereich Ausgang: fehlende Maßnahmen Statisch: Auswahlregeln und erforderliche Maßnahmen Ziele: Ausgehend von Maßnahmenbereichen, die Ermittlung von fehlenden Maßnahmen In der Beobachtungsauswahl werden auf Basis von Maßnahmenbereichen erwartete Maßnahmen und deren Eigenschaften ermittelt. Die Maßnahmenwerte werden erhoben und zu erfassten Maßnahmen abstrahiert. Die Merkmalserkennung erfolgt durch einen Soll-Ist Vergleich erfasster Maßnahmen mit erwarteten Maßnahmen. Falls eine Differenz vorliegt, ist von einer fehlenden Maßnahme auszugehen.	Eingang: verdächtiger Zustand Ausgang: Konsequenz Statisch: Auswahlregeln und vorgegebene Fehl- und Normalzustände Ziel: Erkennen, ob ein verdächtiger Zustand einer Konsequenz (Fehlzustand) oder dem Normalzustand entspricht. In der Beobachtungsauswahl werden auf Basis von verdächtigen Zuständen erwartete Zustandseigenschaften ermittelt. Die Zustandswerte werden erhoben und zu erfassten Zuständen abstrahiert. Die Merkmalserkennung erfolgt durch einen Vergleich erfasster Zustände mit erwarteten Fehl- oder Normalzuständen. Auf Basis des Differenzergebnisses wird einerseits von einer Konsequenz ausgegangen oder anderseits liegt keine Konsequenz vor.

Top-Down Hypothesengenerierung

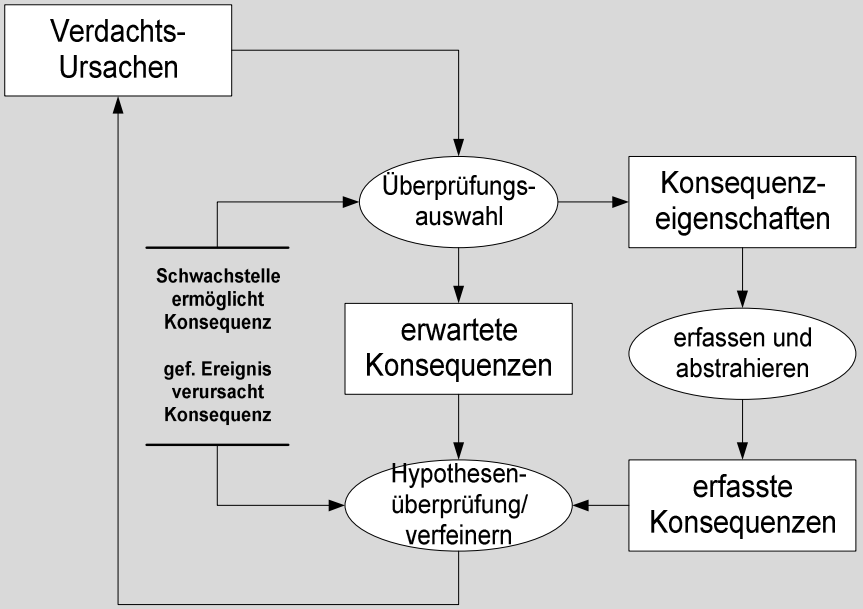
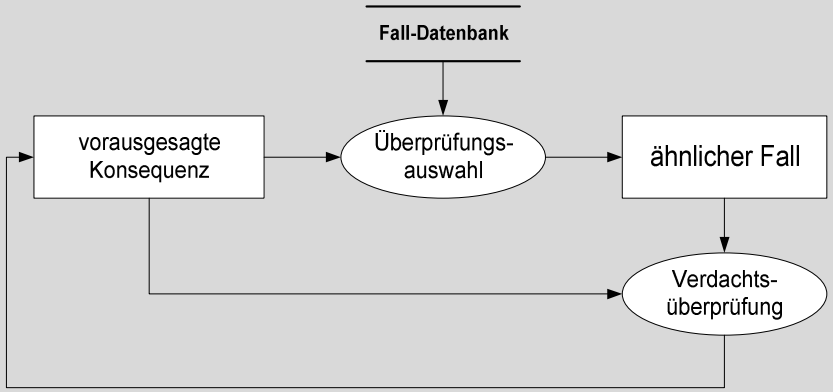
Präventiv	Reaktiv
	
Eingang: fehlende Maßnahmen Ausgang: Verdachts-Schwachstellen (sortiert) Statisch: Maßnahmen-Schwachstellen Assoziation (und Bewertungskriterien) Ziele: Ausgehend von fehlenden Maßnahmen werden Schwachstellen assoziiert. Auf Basis von fehlenden Maßnahmen werden Verdachts-Schwachstellen assoziiert (fehlende Maßnahmen deuten auf Schwachstellen). Dies kann durch eine direkte Maßnahmen-Schwachstellen Assoziation erfolgen oder durch eine Verknüpfung mehrerer Maßnahmen mit der Schwachstelle. Falls zuverlässige Bewertungs- und Rankingkriterien vorliegen, können die Schwachstellen nach diesen Kriterien sortiert werden.	Eingang: Konsequenz Ausgang: Verdachts-Schwachstellen (sortiert) Statisch: Konsequenz-Schwachstellen Assoziation (und Bewertungskriterien) Ziele: Ausgehend von Konsequenzen wird auf Schwachstellen assoziiert. Auf Basis von Konsequenzen werden Verdachts-Schwachstellen assoziiert (Eine aufgetretene Konsequenz erfordert Schwachstellen). Dies kann durch eine direkte Konsequenzen-Schwachstellen Assoziation erfolgen oder durch Verknüpfung mehrerer Konsequenzen mit der Schwachstelle. Falls zuverlässige Bewertungs- und Rankingkriterien vorliegen, können die Schwachstellen nach diesen Kriterien sortiert werden.

Top-Down Hypothesenüberprüfung	
Präventiv	Reaktiv
	
Eingang: Verdachts-Schwachstellen/weitere erwartete fehlende Maßnahmen Ausgang: überprüfte und verfeinerte Verdachts-Schwachstellen Statisch: (hierarchische) Schwachstellen-Maßnahmen Abhängigkeiten Ziele: weitere vermutete Maßnahmen dienen zur Überprüfung und Verfeinerung der Schwachstellen. In der Überprüfungsauswahl werden auf Basis von Verdachts-Schwachstellen weitere assoziierte erwartete fehlende Maßnahmen und deren Eigenschaften ermittelt. Die Maßnahmenwerte werden erhoben und zu erfassten Maßnahmen abstrahiert. Die Hypothesenüberprüfung erfolgt durch einen Soll-Ist Vergleich erfasster Maßnahmen mit erwarteten Maßnahmen. Falls eine Differenz vorliegt, wird die Verdachts-Schwachstelle bestätigt oder verfeinert. Können die Schwachstellen-Maßnahmen Abhängigkeiten durch Hierarchiestrukturen abgebildet werden, so ist eine Hypothesenüberprüfung basierend auf der „Establish Refine Strategie“ möglich.	Eingang: Verdachts-Schwachstellen/weitere erwartete Konsequenzen Ausgang: überprüfte und verfeinerte Verdachts-Schwachstellen Statisch: (hierarchische) Schwachstellen-Konsequenzen Abhängigkeiten Ziele: weitere vermutete Konsequenzen dienen zur Überprüfung und Verfeinerung der Schwachstellen In der Überprüfungsauswahl werden auf Basis von Verdachts-Schwachstellen weitere assoziierte erwartete Konsequenzen und deren Eigenschaften ermittelt. Die Konsequenzwerte werden erhoben und zu erfassten Konsequenzen abstrahiert. Die Hypothesenüberprüfung erfolgt durch einen Soll-Ist Vergleich erfasster Konsequenzen mit erwarteten Konsequenzen. Falls eine Übereinstimmung vorliegt, wird die Verdachts-Schwachstelle bestätigt oder verfeinert. Können die Schwachstellen-Konsequenzen Abhängigkeiten durch Hierarchiestrukturen abgebildet werden, so ist eine Hypothesenüberprüfung basierend auf der „Establish Refine Strategie“ möglich.

Bottom-Up Hypothesengenerierung

Reaktiv (Ursachenanalyse)	Präventiv (Wirkungsanalyse)
	
Eingang: Konsequenz Ausgang: Verdachts-Ursachen (sortierte Schwachstellen und gefährdendes Ereignis) Statisch: kausale Ursachen-Wirkungs-Abhängigkeiten Ziel: Ausgehend von Konsequenzen werden Schwachstellen und gefährdende Ereignisse hergeleitet, welche die Konsequenz kausal erklären. Auf Basis von erkannten Konsequenzen werden durch eine überdeckende Diagnose mögliche Ursachen hergeleitet, welche die Konsequenzen erklären (gefährdende Ereignisse) und ermöglichen (Schwachstelle). Falls zuverlässige Bewertungs- und Rankingkriterien (z.B. Risikokriterien) vorliegen, können die Schwachstellen und gefährdende Ereignisse nach diesen Kriterien sortiert werden.	Eingang: angenommenes gefährdendes Ereignis und angenommene Schwachstellen Ausgang: vorausgesagte Konsequenzen (sortierte) Statisch: kausale Wirkungs-Ursachen Abhängigkeiten Ziel: Ausgehend von angenommenen gefährdenden Ereignissen und Schwachstellen werden deren Konsequenzen „kausal“ simuliert. Falls zuverlässige Bewertungs- und Rankingkriterien (z.B. Risikokriterien) vorliegen, können die Konsequenzen nach diesen Kriterien sortiert werden.

Bottom-Up Hypothesenüberprüfung

Reaktiv (Ursachenanalyse)	Präventiv (Wirkungsanalyse)
	
Eingang: Verdachts-Ursachen (Verdachts-Schwachstellen und gefährdende Ereignisse)/weitere erwartete Konsequenzen Ausgang: überprüfte und verfeinerte Verdachts-Ursachen Statisch: kausale Ursachen-Wirkungs-Abhängigkeiten Ziele: Basierend auf Verdachts-Ursachen werden weitere Konsequenzen vorhergesagt. Das Resultat dient zur Überprüfung und Verfeinerung der Verdachts-Ursachen. Für die ermittelten Verdachts-Ursachen werden weitere kausale Konsequenzen und deren Eigenschaften vorausgesagt. Diese vermuteten Konsequenzen werden erfasst (Beobachtungen) und mit den Vermutungen verglichen. Auf Basis des Resultates können die Verdachts-Ursachen überprüft werden. Bei der Überprüfung entstehen eventuell neue Ursachen, welche die Verdachts-Ursachen verfeinern können.	Eingang: vorausgesagte Konsequenzen Ausgang: überprüfte Konsequenzen Statisch: Fall-Datenbank Ziele: Überprüfung, ob Fälle mit den vorausgesagten Konsequenzen übereinstimmen. Für die vorausgesagten Konsequenzen werden ähnliche Fälle gesucht, wobei auch die angenommenen Ursachen als Such-Merkmale verwendet werden. Sind ähnliche Fälle gefunden, wird überprüft, ob in der Vergangenheit bei den angenommenen Ursachen auch die vorausgesagten Konsequenzen eingetreten sind. Umgekehrt können für die Konsequenzen die jeweiligen Ursachen verifiziert werden. Falls Ursachen und deren Konsequenzen in der Vergangenheit aufgetreten sind, können die simulierten Vorhersagen als plausible eingestuft werden.

Anhang B

Problemlösungs-Szenarien

Monofunktionale Problemlösungs-Szenarien

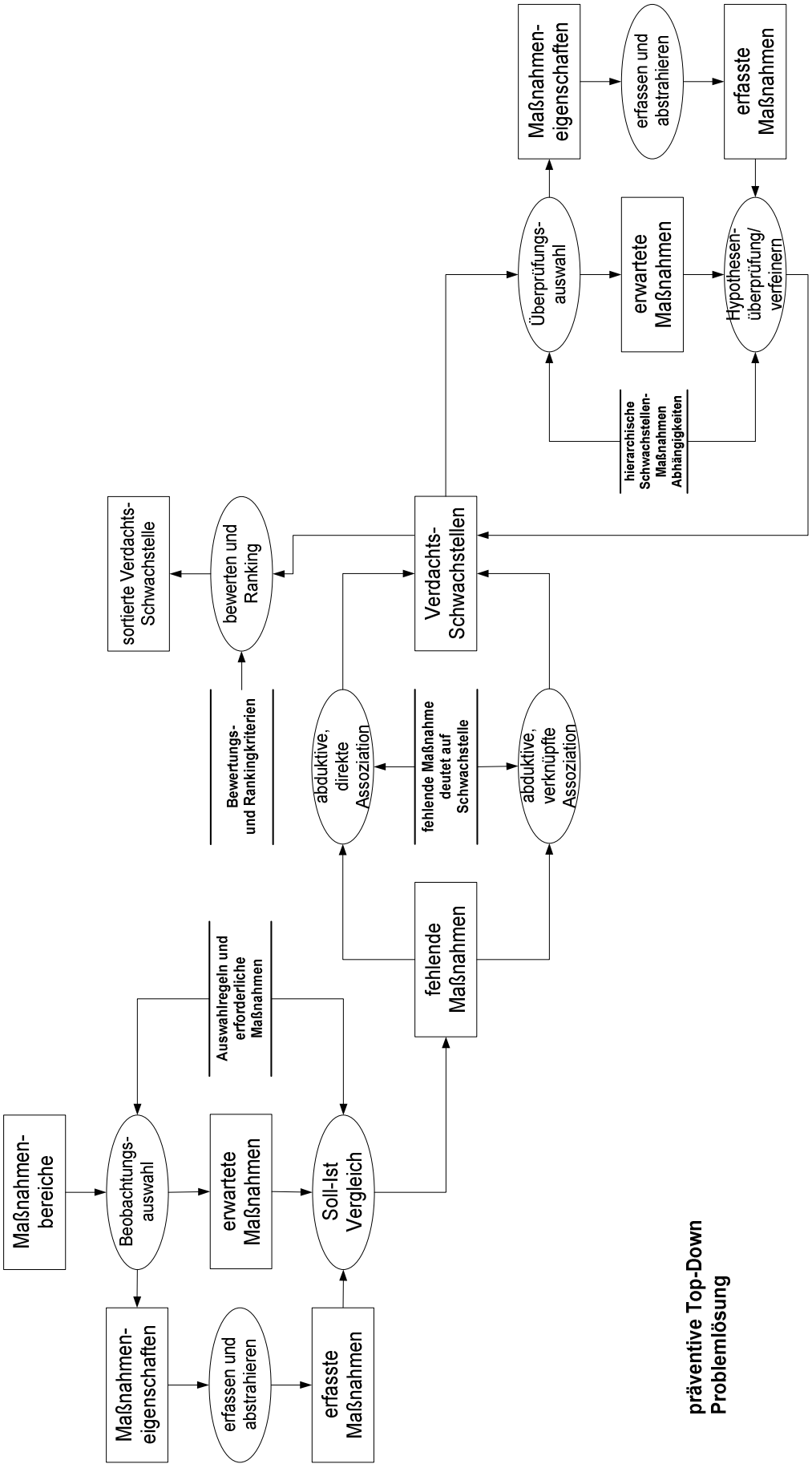
An den folgenden Szenarien soll dargestellt werden, in welcher Form monofunktionale Problemlösungen durch „monofunktionale“ Problemlösungs-Szenarien dargestellt werden.

- Als erstes erfolgt ein präventives IS-Sicherheitsmanagement, das auf dem Top-Down Ansatz basiert.

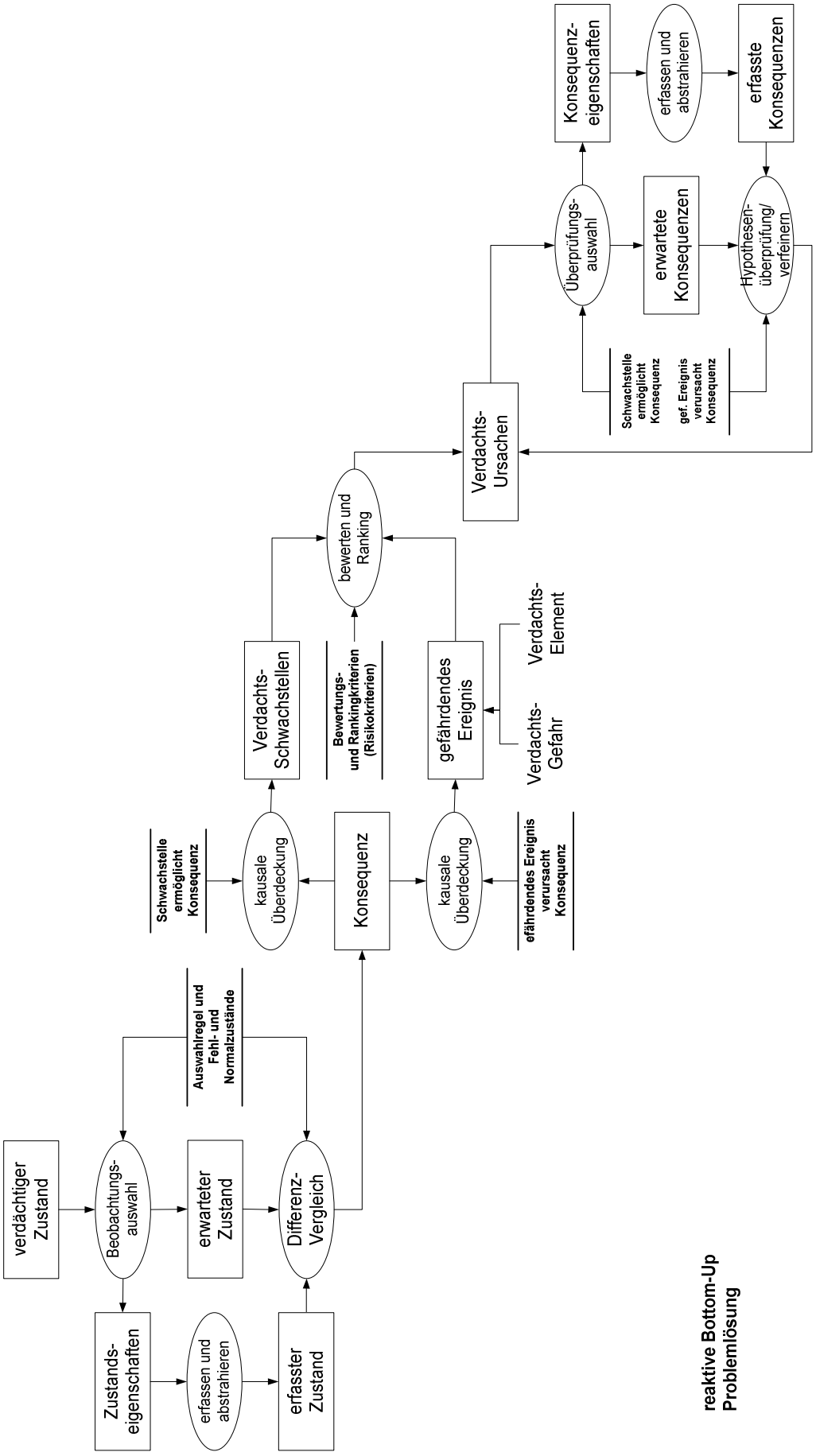
Basis-Inferenzen	Inferenz-Strukturen
Merkmalserkennung	präventiver Top-Down
Hypothesengenerierung	präventiver Top-Down
Hypothesenüberprüfung	präventiver Top-Down

- Eine weitere monofunktionale Problemlösung stellt das reaktive IS-Sicherheitsmanagement basierend auf dem Bottom-Up Ansatz dar.

Basis-Inferenzen	Inferenz-Strukturen
Merkmalserkennung	reaktiver Bottom-Up
Hypothesengenerierung	reaktiver Bottom-Up
Hypothesenüberprüfung	reaktiver Bottom-Up



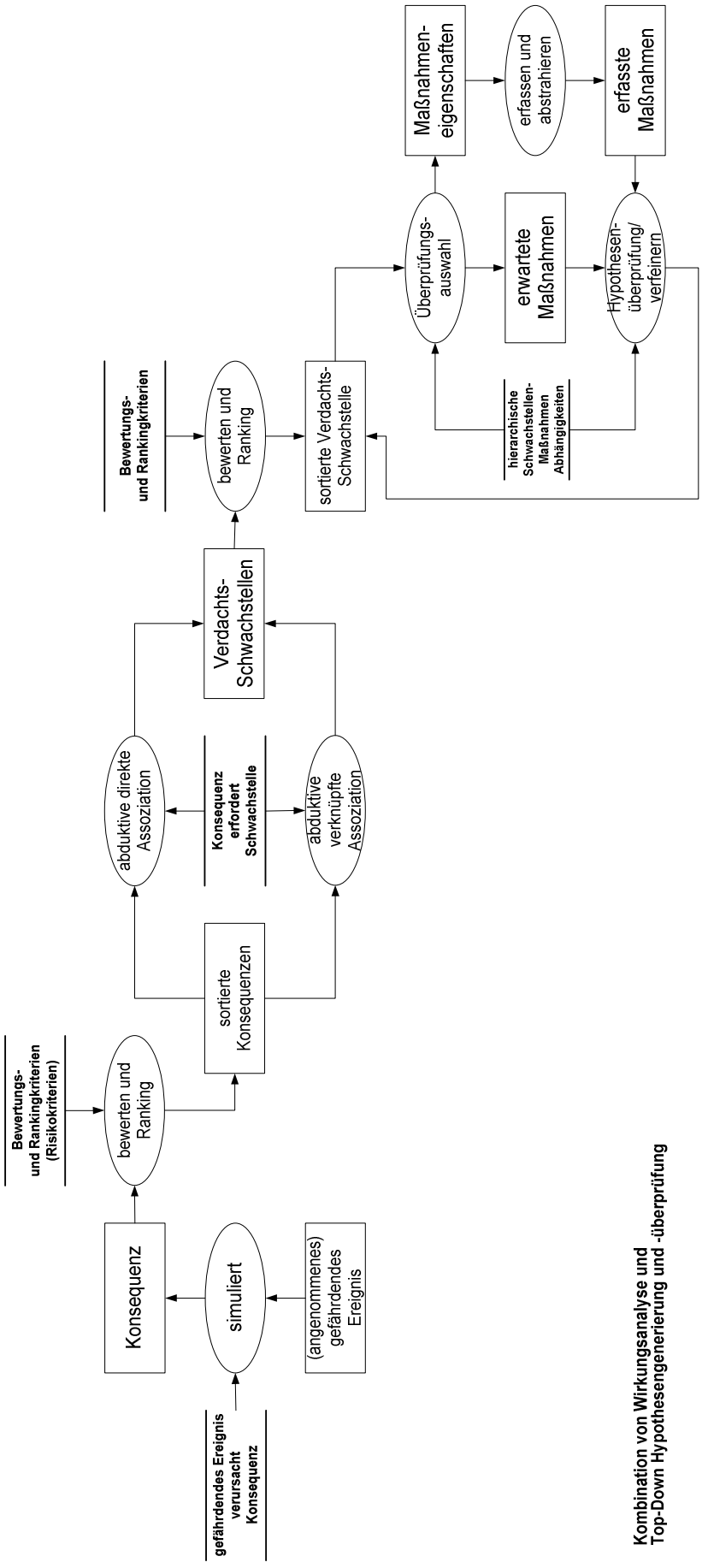
präventive Top-Down Problemlösung


verdächtiger Zustand
Beobachtungs-auswahl
Zustands-eigenschaften
erfassen und abstrahieren
erfasster Zustand
Auswahlregel und Fehl- und Normalzustände
erwarteter Zustand
Differenz-Vergleich
Schwachstelle ermöglicht Konsequenz
kausale Überdeckung
Konsequenz
kausale Überdeckung
efährdendes Ereignis verursacht Konsequenz
Verdachts-Schwachstellen
Bewertungs- und Rankingkriterien (Risikokriterien)
gefährdendes Ereignis
Verdachts-Element
Verdachts-Gefahr
bewerten und Ranking
Verdachts-Ursachen
Überprüfungs-auswahl
Schwachstelle ermöglicht Konsequenz
gef. Ereignis verursacht Konsequenz
erwartete Konsequenzen
Hypothesen-überprüfung/ verfeinern
Konsequenz-eigenschaften
erfassen und abstrahieren
erfasste Konsequenzen
reaktive Bottom-Up Problemlösung

Multifunktionale Problemlösungs-Szenarien

Neben den monofunktionalen Problemlösungs-Szenarien können die Basis-Inferenzen und IS-Sicherheitsstrategien in vielfältiger Form „multifunktional“ kombiniert werden. In dem folgenden Beispiel werden durch eine Wirkungsanalyse Konsequenzen simuliert. Für die Konsequenzen werden durch reaktive Top-Down Hypothesengenerierungen deren Verdachts-Schwachstellen assoziiert. Anschließend erfolgt eine Top-Down Hypothesenüberprüfung der ermittelten Schwachstellen.

Basis-Inferenzen	Inferenz-Strukturen
Hypothesengenerierung	Präventiver Bottom-Up und reaktiver Top-Down
Hypothesenüberprüfung	präventiver Top-Down



Kombination von Wirkungsanalyse und Top-Down Hypothesengenerierung und -überprüfung

Literaturverzeichnis

Ackoff (1968)
Ackoff, R. L.: Management Misinformation Systems. In: Management Science, Vol. 14(4), 1968, pp. 147-156

Adam (1995)
Adam, U.: Einführung in die Datensicherheit, Würzburg 1995

Alex (1998)
Alex, B.: Künstliche neuronale Netze in Management-Informationssystemen, Wiesbaden 1998

Altenkrüger (1992)
Altenkrüger, D.: Wissensbasierte Systeme, Braunschweig/Wiesbaden 1992

Angele/Fensel/Studer (1998)
Angele, J./Fensel, D./Studer, R.: Vorgehensmodelle für die Entwicklung wissensbasierter Systeme. In: Kneuper, R./ Müller-Luschnat, G./Oberweis, A. (Hrsg.): Vorgehensmodelle für die betriebliche Anwendungsentwicklung. Teubner-Reihe: Wirtschaftsinformatik, Ehrenberg, D./Seibt, D./Stucky, W. (Hrsg.) Stuttgart/Leipzig 1998, S. 168-188

Atteslander (1995)
Atteslander, P.: Methoden der empirischen Sozialforschung, 8. Aufl., Berlin/New York 1995

Bachem (1994)
Bachem, J.: Vorgehensmodelle für die Entwicklung wissensbasierter Systeme. Reihe: Wirtschaftsinformatik, Band 11, Seibt, D./Derigs, W./Mellis, W. (Hrsg.), Bergisch Gladbach/Köln 1994

Baer (1995)
Baer, R.: Informatik-Sicherheit - Konzept und Vorgehen. In: Pohl, H./Weck, G. (Hrsg.): Handbuch 2: Managementaufgaben im Bereich der Informationssicherheit, München/Wien 1995, S. 25-101

Balzert (2001)
Balzert, H.: Lehrbuch der Software-Technik. Software-Entwicklung, 2. Aufl., Heidelberg/Berlin 2001

Bamberger (1999)
Bamberger, S.: Verteiltes Problemlösen mit wissensbasierten Diagnosesystemen, Sankt Augustin 1999

Bartsch-Spörl/Lenz/Hübner (1999)
Bartsch-Spörl, B./Lenz, M./Hübner, A.: Case-Based Reasoning - Survey and Future Directions. In: Puppe, F. (Eds.): XPS-99: Knowledge-Based Systems. 5th Biannual German Conference on Knowledge-Based Systems, Würzburg (Germany), March 3-5 1999, Proceedings. Berlin u.a. 1999, pp. 67-89

Bäumler (2001)
Bäumler, H.: Datenschutz als Wettbewerbsvorteil. Eröffnungsrede anläßlich der Sommerakademie 2001, Kiel 2001. Veröffentlicht im Internet: URL: http://www.datenschutzzentrum.de/somak/somak01/sak01bau.htm#Inhalt (Stand: 10.10.2002)

Bäumler (2002)
Bäumler, H.: Der Konkurrenz einen Schritt voraus. In: Bäumler, H/Mutius, A. von (Hrsg.): Datenschutz als Wettbewerbsvorteil. DuD-Fachbeiträge: Pfitzmann, A./Reimer, H./Rihaczek, K./Roßnagel, A. (Hrsg.), Braunschweig/Wiesbaden 2002, S. 1-11

BDSG (1997)
Bundesdatenschutzgesetz (BDSG), vom 20. Dezember 1990, zuletzt geändert durch Art. 2 Abs. 5 des Begleitgesetzes zum Telekommunikationsgesetz vom 17. Dezember 1997. Veröffentlicht im Internet: URL: http://www.netlaw.de/gesetze/bdsg_alt.htm (Stand: 10.10.2002)

BDSG (2001)
Bundesdatenschutzgesetz (BDSG), vom 20. Dezember 1990, zuletzt geändert durch Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze vom 18. Mai 2001. Veröffentlicht im Internet: URL: http://www.netlaw.de/gesetze/bdsg.htm (Stand: 10.10.2002)

Becaulair (1968)
Becaulair, W. de: Rechnen mit Maschinen, Braunschweig 1968

Becker et al. (2000)
Becker, K./Stumme, G./Wille, R./Wille, U./Zickwolff, M.: Conceptual Information Systems Discussed through an IT-Security Tool. In: Dieng, R./Corby, O. (Eds.): Knowledge Engineering and Knowledge Management. 12th International Conference, EKAW 2000 in Juan-les-Pins (France), October 2-6, Proceedings. Lecture Notes in Artificial Intelligence (LNAI 1937), Berlin u.a. 2000, pp. 252-365

Behrens (1997)
Behrens, J.: Aufgaben des DSB und ihre Veränderungen durch Vernetzung und verteilte Systeme. In: Voßbein, R. (Hrsg.): Die Organisation der Arbeit des betrieblichen Datenschutzbeauftragten, Frechen 1997, S. 9-24

Beierle/Kern-Isberner (2000)
Beierle, C./Kern-Isberner, G.: Methoden wissensbasierter Systeme, Braunschweig/Wiesbaden 2000

Benjamins (1993)
Benjamins, V.R.: Problem solving methods for diagnosis, Amsterdam 1993

Benjamins (1995)
Benjamins, V.R.: Problem solving methods for diagnosis and their Role in Knowledge Acquisition. In: International Journal of Expert Systems, Vol 8(2), 1995, pp. 93-120

Berger/Häntschel (1996)
Berger, W. W./Häntschel, I.: Erfolgreiches Sicherheitsmanagement - Eine Fallstudie. In: Bauknecht, K./Karagiannis, D./Teufel, S. (Hrsg.): Sicherheit in Informationssystemen. Beiträge der Fachtagung SIS'96 in Wien vom 21-22 März 1996. Zürich 1996, S. 37-52

Borkowski (2001)
Borkowski, V.: Expertensystem, Anwendung in der Betriebswirtschaft. In: Mertens, P. (Hrsg.): Lexikon der Wirtschaftsinformatik, 4. Aufl., Berlin u.a. 2001, S. 193-195

Borndorff-Eccarius (1998)
Borndorff-Eccarius, S.: Rechnergestützte Wissensakquisition für wissensbasierte Diagnosesysteme im Bereich dynamischer technischer Systeme, Sankt Augustin 1998

Brandao (1996)
Brandao, R. P.: IT-Sicherheitskultur im Unternehmen. In: Bauknecht, K./Karagiannis, D./Teufel, S. (Hrsg.): Sicherheit in Informationssystemen. Beiträge der Fachtagung SIS'96 in Wien vom 21-22 März 1996. Zürich 1996, S. 1-20

Brenner/Lux (2000)
Brenner, W./Lux, A.: Virtual Purchasing. Die Revolution im Einkauf. Leinfelden-Echterdingen 2000

Britsch (1995)
Britsch, W.: Personelle Sicherheit in Unternehmen. In: Pohl, H./Weck, G. (Hrsg.): Handbuch 2: Managementaufgaben im Bereich der Informationssicherheit, München/Wien 1995, S. 121-164

Brownlee/Guttman (1998)
Brownlee, N./Guttman, E.: Expectations for Computer Security Incident Response (Internet Best Current Practice), o. O. 1998. Veröffentlicht im Internet: URL: http://www.ietf.org/rfc/rfc2350.txt (Stand:10.12.2002)

BS 7799-1 (1999)
British Standard Institution: BS 7799-1:1999: Information Security Management - Part 1: Code of practice for information security management, London 1999

BS 7799-2 (1998)
British Standard Institution: BS 7799-2:1998: Information Security Management - Part 2: Specification for information security management systems, London 1998

BS 7799-2 (2002)
British Standard Institution: BS 7799-2:2002: Information Security Management - Specification with guidance for use, London 2002

BSI-Grundschutzhandbuch (2000)
Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): IT-Grundschutzhandbuch, CD-ROM-Version, o. O. 2000

BSI-IT-Sicherheitshandbuch (1992)
Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): IT-Sicherheitshandbuch. Handbuch für die sichere Anwendung der Informationstechnik, Version 1.0, Bonn 1992

BSI-Tool Benutzerhandbuch (1999)
Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): BSI Tool IT-Grundschutz Benutzerhandbuch, Version 2.0, Bonn 1999

Budget (2001)
O. V.: Wurde ein Budget für IT-Sicherheitsaufgaben aufgestellt? In: Computer-Zeitung, 31. Jg. (2001) H. 12, S. 1

Bühner (1999)
Bühner, R.: Betriebswirtschaftliche Organisationslehre, 9. Aufl., München/Wien 1999

Busch et al. (1994)
Busch, B./Herrmann, T./Just, K./Rittenbruch, M.: Systeme für Experten statt Expertensysteme, Sankt Augustin 1994

Buxmann/König (1998)
Buxmann, P./König, W.: Das Standardisierungsproblem: Zur ökonomischen Auswahl von Standards in Informationssystemen. In: Wirtschaftsinformatik, 40. Jg. (1998) H. 2, S. 122-129

Bylander/Chandrasekaran (1988)
Bylander, T./Chandrasekaran, B.: Generic tasks for knowledge-based reasoning: the „right“ level of abstraction for knowledge acquisition. In: Gains, B./Boose, J. (Ed.): Knowledge Acquisition for Knowledge-based Systems, London u.a., 1988, S. 65-77

c:cure (2002)
c:cure: BS 7799 History: BS 7799-2-Information Security Management Systems. Veröffentlicht im Internet: URL: http://www.c-cure.org/7799history.htm (Stand: 15.01.2003)

CC-Kurz (2001)
Bundesamt für Sicherheit in der Informationstechnik: BSI-Kurzinformationen zu aktuellen Themen der IT-Sicherheit „Common Criteria (ISO/IEC 15408)“, Bonn 2001. Veröffentlicht im Internet: URL: http://www.bsi.de/literat/faltbl/ppschutz.html (Stand: 10.10.2002)

CC-Teil 1 (2000)
Bundesamt für Sicherheit in der Informationstechnik: Common Criteria: Teil 1: Einführung und allgemeines Modell. Deutsches Übersetzung der Common Criteria - Gemeinsame Kriterien, PDF-Version 2.1, am 29.09.2000 im Bundesanzeiger bekannt gemacht. Veröffentlicht im Internet: URL: http://www.bsi.de/cc/cc1_21.pdf (Stand:10.12.2002)

CC-Teil 2 (2000)
Bundesamt für Sicherheit in der Informationstechnik: Common Criteria: Teil 2: Funktionale Sicherheitsanforderungen. Deutsches Übersetzung der Common Criteria - Gemeinsame Kriterien, PDF-Version 2.1, am 29.09.2000 im Bundesanzeiger bekannt gemacht. Veröffentlicht im Internet: URL: http://www.bsi.de/cc/cc2_21.pdf (Stand:10.12.2002)

CC-Teil 3 (2000)
Bundesamt für Sicherheit in der Informationstechnik: Common Criteria: Teil 3: Anforderungen an die Vertrauenswürdigkeit. Deutsches Übersetzung der Common Criteria - Gemeinsame Kriterien, PDF-Version 2.1, am 29.09.2000 im Bundesanzeiger bekannt gemacht. Veröffentlicht im Internet: URL: http://www.bsi.de/cc/cc3_21.pdf (Stand:10.12.2002)

CC-Tool-User Manual
National Institute of Standards and Technology: CC-Toolbox: User's Manual, Version 6.0f. Veröffentlicht im Internet: URL: http://niap.nist.gov/tools/CCTB60f-Documentation/UsersGuide/UsersManual_FrameSet.html cctool.html (Stand: 10.10.2002)

CERT-Einrichtung (2002)
O. V.: Sicherheitsexperten suchen Kunden im Mittelstand. In: Computer-Zeitung, 32. Jg. (2002) H. 7, S. 17

Chandrasekaran (1986)
Chandrasekaran, B.: Generic Tasks in Knowledge-based Reasoning: High-level Building Blocks for Expert System Design. In: IEEE Expert, Vol. 1(3), 1986, pp. 23-30

Chandrasekaran/Johnson/Smith (1992)
Chandrasekaran, B./Johnson, T. R./Smith, J. W.: Task Structure Analysis for Knowledge Modeling. In: Communications of the ACM, Vol. 35(9), 1992, pp. 124-137

Chandrasekaran/Josephson/Benjamins (1999)
Chandrasekaran, B./Josephson, J. R./Benjamins, V. R.: What are Ontologies, and why do we need them. In: IEEE Intelligent Systems, Vol. 14(1), 1999, pp. 20-26

Churley (2002)
Churley, A.: FIPS: US-Standards für Informationssicherheit. In: KES, o. Jg. (2002) H. 1, S. 75-76

Ciechanowicz (1997)
Ciechanowicz, Z.: Risk analysis: requirements, conflicts and problems. In: Computers & Security, Vol. 16(3), 1997, pp. 223-232

Clancey (1985)
Clancey, W. J.: Heuristic Classification. In: Artificial Intelligence, Vol. 27(3), 1985, pp. 289-350

Cobit (2001)
Information Systems Audit and Control Association (ISACA): CobiT 3rd edition, Zürich 2001. Veröffentlicht im Internet: URL: http://www.isaca.ch/download/cobit/cobit_broschuere_2001.pdf (Stand: 15.01.2003)

Curth/Bölscher/Raschke (1991)
Curth, M. A./Bölscher, A./Raschke, B.: Entwicklung von Expertensystemen, München/Wien 1991

D21 (2001)
Arbeitsgruppe 5 der Initiative D21: Sicherheit und Vertrauen im Internet: IT-Sicherheitskriterien im Vergleich, o. O. 12/2001. Veröffentlicht im Internet: URL: http://www.initiativeD21/arbeitsgruppen/5sicherheit/leitfaden.pdf (Stand: 10.12.2002)

Dambeck (2003)
Dambeck, H.: Datenschutz-TÜV. In: Magazin für Computertechnik (c't), o. Jg. (2003) H. 1, S. 32

Damm et al. (1999)
Damm, D./Schlienger, T./Teufel, S./Weidner, H.: RSD-XPS - Ein Expertensystem für die Internet-Sicherheitskonzeption. In: Röhm, A./Fox, D./Grimm, R./Schoder, D. (Hrsg.): Sicherheit und Electronic Commerce. DuD-Fachbeiträge: Pfitzmann, A./Reimer, H./Rihaczek, K./Roßnagel, A. (Hrsg.), Braunschweig/Wiesbaden 1999, S. 63-77

Datenschutz-Broschüre (2002)
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: Welche Vorteile bringen mir Datenschutz-Behördenaudit & Datenschutz-Gütesiegel?, Kiel 2002. Veröffentlicht im Internet: URL: http://www.datenschutzzentrum.de/download/audsieeu.pdf (Stand: 10.10.2002)

Datenschutzsiegel (2002)
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: Das schleswig-holsteinische Datenschutzgütesiegel, Version 1.0, o. O. 2002. Veröffentlicht im Internet: URL: http://www.datenschutzzentrum.de/download/dssiegel.pdf (Stand: 10.10.2002)

Diek (2002)
Diek, A. C.: Gütesiegel nach dem schleswig-holsteinischen Landesdatenschutzgesetz. In: Bäumler, H/Mutius, A. von (Hrsg.): Datenschutz als Wettbewerbsvorteil. DuD-Fachbeiträge: Pfitzmann, A./Reimer, H./Rihaczek, K./Roßnagel, A. (Hrsg.), Braunschweig/Wiesbaden 2002, S. 157-162

Dodenhöft (1995)
Dodenhöft, D.: Hybride Wissensrepräsentation durch enge Kopplung eines frame- und regelbasierten Formalismus, München 1995

Dressler (1997)
Dressler, M.: Modellbasierte Navigationsstrategien in Executive Support Systems, Wiesbaden 1997

Dridi/Pernul/Sabol (2001)
Dridi, F./Pernul, G./Sabol, T.: The Webocracy Project: Overview and Security Aspects. In: Schnurr, H.-P./Staab, S./Studer, R./Stumme, G./Sure, Y. (Hrsg.): Professionelles Wissensmanagement: Erfahrungen und Visionen, Aachen 2001, S. 401-408

Eckert (2001)
Eckert, C.: IT-Sicherheit, München/Wien 2001

E-COFC (1999)
European Computer Manufactures Association: Extended Commercially Oriented Functionality Class for Security Evaluation (E-COFC). Standard ECMA-271, PDF-Version, Genf 1999. Veröffentlicht im Internet: URL: http://www.ecma.ch (Stand: 10.10.2002)

EG-Datenschutzvorschlag (1999)
Kommission der Europäischen Gemeinschaft: Vorschlag für eine Verordnung des europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, 99/0153 (COD), Brüssel 1999. Veröffentlicht im Internet: URL:
http://www.europarl.eu.int/dg2/hearings/pdf/20000222/libe/framework/eplegs/regulation/en/default.pdf (Stand: 10.10.2002)

EGG (2001)
Entwurf eines Gesetzes über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (Elektronischer Geschäftsverkehr-Gesetz - EGG), Stand 17.05.2001. Veröffentlicht im Internet: URL: http://dip.bundestag.de/btd/14/060/1406098.pdf (Stand: 10.12.2002)

E-Government-Handbuch-Glossar (2002)
Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): E-Government-Handbuch, Online-Version. Modul: Glossar, Bonn 2002. Veröffentlicht im Internet: URL: http://www.bsi.bund.de/fachtheme/gov/download/6_EGloss.pdf (Stand: 10.10.2002)

E-Government-Handbuch-Internetauftritt (2002)
Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): E-Government-Handbuch, Online-Version. Modul: Sicherer Internetauftritt im E-Government, Bonn 2002. Veröffentlicht im Internet: URL: http://www.bsi.bund.de/fachtheme/gov/download/4_IntAuf.pdf (Stand: 10.10.2002)

E-Government-Handbuch-Vortrag (2001)
Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): E-Government-Handbuch - Online-Version. Präsentation: E-Government in unserer Behörde, Bonn 2002. Veröffentlicht im Internet: URL: http://www.bsi.bund.de/fachtheme/gov/download/6_Folien.ppt (Stand: 10.10.2002)

Ehmann (1993)
Ehmann, E.: Rechtliche Aspekte in Einführung in die Informationssicherheit. In: Pohl, H./Weck, G. (Hrsg.): Handbuch 1: Einführung in die Informationssicherheit, München/Wien 1993, S. 52-84

Eloff/Solms (2000a)
Eloff, M. M./Solms, S.H. von.: Information Security Management: A Hierarchical Framework for Various Approaches. In: Computers & Security, Vol. 19(3), 2000, pp. 243-256

Eloff/Solms (2000b)
Eloff, M. M./Solms, S.H. von.: Information Security Management: An Approach to Combine Process Certification And Product Evaluation. In: Computers & Security, Vol. 19(3), 2000, pp. 698-709

Engelmann (1990)
Engelmann, R.: Integration nicht-sicheres Wissen in Expertensysteme. In: Ehrenberg, D./Krallmann, H./Rieger, B. (Hrsg.): Wissensbasierte Systeme in der Betriebswirtschaft . Reihe: Betriebliche Informations- und Kommunikationssysteme, Band 15, Krallmann, H. (Hrsg.). Berlin 1990, S. 185-196

Ernestus (1999)
Ernestus, W.: Datenschutzfreundliche Technologien. In: BSI (Hrsg.): IT-Sicherheit ohne Grenzen? Tagungsband: 6. Deutscher IT-Sicherheitskongreß des BSI, Ingelheim 1999, S. 151-162

Fensel (2000)
Fensel, D.: Problem-Solving Methods. Lecture Notes in Artificial Intelligence (LNAI 1791), Berlin u.a. 2000

Fensel (2001)
Fensel, D.: Ontologies: A Silver Bullet for Knowledge Management and Electronic Commerce, Berlin u.a 2000

Fink/Schneidereit/Voß (2001)
Fink, A./Schneidereit, G./Voß, S.: Grundlagen der Wirtschaftsinformatik, Heidelberg 2001

Finne (2000)
Finne, T.: Information Systems Risk Management: Key Concepts and Business Processes. In: Computer & Security, Vol. 19(3), 2000, pp. 234-242

FIPS 140-1 (1994)
U.S. Department Of Commerce/ National Institute of Standards and Technology: FIPS 140-1: Security Requirements for Cryptographic Modules, Gaithersburg 1994. Veröffentlicht im Internet: URL: http://csrc.nist.gov/publications/fips/fips140-1/fips1401.pdf (Stand: 10.10.2002)

FIPS 180-1 (1995)
U.S. Department Of Commerce/ National Institute of Standards and Technology: FIPS 180-1: Secure Hash Standard, Gaithersburg 1995. Veröffentlicht im Internet: URL: http://csrc.nist.gov/publications/fips/fips180-1/fip180-1.pdf (Stand: 10.10.2002)

FIPS 180-1 (1995)
U.S. Department Of Commerce/ National Institute of Standards and Technology: FIPS 180-1: Secure Hash Standard, Gaithersburg 1995. Veröffentlicht im Internet: URL: http://csrc.nist.gov/publications/fips/fips180-1/fip180-1.pdf (Stand: 10.10.2002)

FIPS 186-2 (2000)
U.S. Department Of Commerce/ National Institute of Standards and Technology: FIPS 186-2: Digital Signature Standard (DSS), Gaithersburg 2000. Veröffentlicht im Internet: URL: http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf (Stand: 10.10.2002)

FIPS 197 (2001)
U.S. Department Of Commerce/ National Institute of Standards and Technology: FIPS 197: Announcing the Advanced Encryption Standard (AES), Gaithersburg 2001. Veröffentlicht im Internet: URL: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf (Stand: 10.10.2002)

FIPS 46-3 (1999)
U.S. Department Of Commerce/ National Institute of Standards and Technology: FIPS 46-3: Data Encryption Standard (DES), Gaithersburg 1999. Veröffentlicht im Internet: URL: http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf (Stand: 10.10.2002)

Fleischhauer/Rouette (1989)
Fleischhauer, P./Rouette, L.: Wissen, Information und Daten. In: Computermagazin Wissen, Sonderheft Informationsstrategie, o. Jg. (1989) H. 101, S. 8-9

Fox (2001)
Fox, d.: E-Mail-Sicherheit: Kriterien, Standards und Lösungen. In: BSI (Hrsg.): 2001 - Odyssee im Cyberspace? Sicherheit im Internet! Tagungsband: 7. Deutschen IT-Sicherheitskongreß des BSI 2001, Ingelheim 2001, S. 23-40

FQS (1994)
Forschungsgemeinschaft Qualitätssicherung e.V. (FQS): Forschungsprojekt: Rechnergestützte, wissensbasierte Erstellung von Fehlermöglichkeits- und Einflußanalysen (FMEA), FQS-Schrift 85-02, Frankfurt a. M./Berlin 1994

Frank (1988)
Frank, U.: Expertensysteme: Neue Automatisierungspotentiale im Büro- und Verwaltungsbereich?, Wiesbaden 1988

Frick (1998)
Frick, D.: Die Akquisition betriebswirtschaftlichen Wissens zum Aufbau von wissensbasierten Entscheidungsunterstützungssystemen, Frankfurt a. M. u.a. 1998

FÜV (1995)
Verordnung über die technische Umsetzung von Überwachungsmaßnahmen des Fernmeldeverkehrs in Fernmeldeanlagen, die für den öffentlichen Verkehr bestimmt sind (Fernmeldeverkehr-Überwachungs-Verordnung - FÜV), vom 18.05.1995. Veröffentlicht im Internet: URL: http://www.netlaw.de/gesetze/fuev.htm (Stand: 10.10.2002)

Gabriel (1992)
Gabriel, R.: Wissensbasierte Systeme in der betrieblichen Praxis, London u.a. 1992

Gappa (1995)
Gappa, U.: Grafische Wissensakquisitionssysteme und ihre Generierung, Sank Augustin 1995

Gerber/Solms (2001)
Gerber, M./Solms, R. von: From Risk Analysis to Security Requirements. In: Computers & Security, Vol. 20(7), 2001, pp. 577-584

Gluchowski/Gabriel/Chamoni (1997)
Gluchowski, P./Gabriel R./Chamoni, P.: Management Support Systeme, Berlin u.a. 1997

Görtz (1997)
Görtz, H.: Sicherheitszertifizierung aus unterschiedlicher Sicht. In: BSI (Hrsg.): Mit Sicherheit in die Informationsgesellschaft. Tagungsband: 5. Deutscher IT-Sicherheitskongreß des BSI, Ingelheim 1997, S. 321-322

Görz/Wachsmuth (2000)
Görz, G/Wachsmuth, I.: Einleitung. In: Görz, G./Rollinger, C.-R./Schneeberger, J. (Hrsg.): Handbuch der Künstlichen Intelligenz, 3. Aufl., München/Wien 2000, S. 1-16

Götze/TÜV (2002)
Götze, S/TÜV Informationstechnik GmbH.: Zertifizierung von Sicherheitsmanagement-systemen nach BS7799. Vortrag. TÜViT Zertifizierungstag, o. O. 6.6.2002. Veröffentlicht im Internet: URL: http://www.secure.trusted.site.de/download/veranstaltungen/ZertTag/ZertTag_2002_BS7799.pdf (Stand: 10.12.2002)

Gritzalis (1997)
Gritzalis, D.: A baseline security policy for distributed healthcare information systems. In Computers & Security, Vol. 16 (8), 1997, pp. 709-719

Gruber (1993)
Gruber, T. R.: A translation approach to portable ontology specifications. In: Knowledge Acquisition, Vol 5(2), 1993, pp. 199-220

Guarino (1997)
Guarino, N.: Understanding, Building, And Using Ontologies. In: International Journal of Human and Computer Studies, Vol. 46(2-3), 1997, pp. 293-310

Güldenberg (1997)
Güldenberg, S.: Wissensmanagement und Wissenscontrolling in lernenden Organisationen, Wiesbaden 1997

Gundermann (1999)
Gundermann, L.: Datenschutzfreundliche Technologien in den Datenschutzgesetzen der 3. Generation. In: BSI (Hrsg.): IT-Sicherheit ohne Grenzen? Tagungsband: 6. Deutscher IT-Sicherheitskongreß des BSI, Ingelheim 1999, S. 137-149

Gütesiegel-Anforderungskatalog (2002)
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: Anforderungskatalog, Version 1.0a vom 24.4.2002, Kiel 2002. Veröffentlicht im Internet: URL: http://www.datenschutzzentrum.de/download/anford.pdf (Stand: 10.10.2002)

Haase et al. (1995)
Haase, M./Krehl, H./Heidecker, P./Mertens, P.: Unternehmensreport II - ein umfassender Ansatz zur wissensbasierten Unternehmensanalyse. In: Künstliche Intelligenz, 9. Jg. (1995) H. 5, S. 56-62

Haar/Solms, R. (1993)
Haar, H. van de/Solms, R. von: A Tool for Information Security Management. In: Information Management & Computer Security, Vol 1(1), 1993, pp. 4-10

Haaz (1997)
Haaz, H.: Das Anforderungsprofil des betrieblichen Datenschutzbeauftragten. In: Voßbein, R. (Hrsg.): Die Organisation der Arbeit des betrieblichen Datenschutzbeauftragten, Frechen 1997, S. 33-45

Hammer (1999)
Hammer, V.: Verletzlichkeitsreduzierende Technikgestaltung. Methodische Grundlagen für die Anforderungsanalyse. In: Baumgart, R./Rannenberg, K./Wähner, D./Weck, G. (Hrsg.): Verläßliche Informationssysteme. DuD-Fachbeiträge: Pfitzmann, A./Reimer, H./Rihaczek, K./Roßnagel, A. (Hrsg.), Braunschweig/Wiesbaden 1999, S. 187-202

Hange/Moritz (2002)
Hange, M./Moritz, W.-R.: IT-Sicherheitskriterien im Vergleich. In: KES, o. Jg. (2002) H. 1, S. 68-70

Hansen/Neumann (2001)
Hansen, H.R./Neumann, G.: Wirtschaftsinformatik I, 8. Aufl., Stuttgart 2001

Hansen/Probst (2002)
Hansen, M./Probst, T.: Datenschutzsiegel aus technischer Sicht: Bewertungskriterien des schleswig-holsteinischen Datenschutzgütesiegels. In: Bäumler, H/Mutius, A. von (Hrsg.): Datenschutz als Wettbewerbsvorteil. DuD-Fachbeiträge: Pfitzmann, A./Reimer, H./Rihaczek, K./Roßnagel, A. (Hrsg.), Braunschweig/Wiesbaden 2002, S. 162-179

Hare (1999a)
Hare, C.: CIRT: Responding to Attack. In: Tipton, H. F./Krause, M. (Eds.): Information Security Management Handbook, 4th ed., Boca Raton u.a. 1999, pp. 549-568

Hare (1999b)
Hare, C.: Improving Network-Level Security Through Real-time Monitoring and Intrusion Detection. In: Tipton, H. F./Krause, M. (Eds.): Information Security Management Handbook, 4th ed., Boca Raton u.a. 1999, pp. 569-595

Harmon/King (1989)
Harmon. P./King, D.: Expertensysteme in der Praxis, 3. Aufl., München/Wien 1989

Hartmann/Karger (2001)
Hartmann, A./Karger, P.: Sicherheitskompetenz - ein häufig vergessener Baustein der Informationsgesellschaft. In: BSI (Hrsg.): 2001 - Odyssee im Cyberspace? Sicherheit im Internet! Tagungsband: 7. Deutschen IT-Sicherheitskongreß des BSI 2001, Ingelheim 2001, S. 377 - 390

Haun (2000)
Haun, M.: Wissensbasierte Systeme, Renningen 2000

Heijst (1995)
Heijst, G. van: The Role of Ontologies in Knowledge Engineering, Amsterdam 1995

Heijst/Schreiber/Wielinga (1997)
Heijst, G. van/Schreiber, A. Th./Wielinga, B. J.: Roles are not classes: a reply to Nicola Guarino. In: International Journal of Human Computer Studies, Vol 46(2/3), 1997, pp. 311-318

Heinrich (2001)
Heinrich, L. H.: Wirtschaftsinformatik, 2. Aufl., München/Wien 2001

Heinrich (2002)
Heinrich, L. H.: Informationsmanagement, 7. Aufl., München/Wien 2002

Heller (1995)
Heller, B.: Modularisierung und Fokussierung erweiterbarer komplexer Wissensbasen auf der Basis von Kompetenzeinheiten, Sankt Augustin 1996

Hennig (2001)
Hennig, A.: Sicherheit in der Informationstechnik. In: Mertens, P. (Hrsg.): Lexikon der Wirtschaftsinformatik, 4. Aufl., Berlin u.a. 2001, S. 411-412

Hentze/Brose/Kammel (1993)
Hentze, J./Brose, P./Kammel, A.: Unternehmensplanung, 2. Aufl., Bern/Stuttgart/Wien 1993

Hepp (2001)
Hepp, M.: Datensicherheit. In: Mertens, P. (Hrsg.): Lexikon der Wirtschaftsinformatik, 4. Aufl., Berlin u.a. 2001, S. 148-150

Herbst (2001)
Herbst, T.: Datenschutz. In: Mertens, P. (Hrsg.): Lexikon der Wirtschaftsinformatik, 4. Aufl., Berlin u.a. 2001, S. 145-146

Herrmann (1997)
Herrmann, J.: Maschinelles Lernen und Wissensbasierte Systeme, Berlin u.a. 1997

Hesse (2002)
Hesse, W.: Ontologie(n). In: Informatik Spektrum, 25. Jg. (2002) H. 6, S. 477-480

Heuser (2000)
Heuser, A.: Das Bundesamt für Sicherheit in der Informationstechnik (BSI) - Aufgaben und Selbstverständnis. In: Geiger, G. (Hrsg.): Sicherheit der Informationsgesellschaft, Baden-Baden 2000, S. 108-116

Hoepner (1994)
Hoepner, G.: Computereinsatz bei Befragung, Wiesbaden 1994

Hoppe (1992)
Hoppe, U.: Methoden des Knowledge Engineering, Wiesbaden 1992

Horster/Kraaibeek (2000)
Horster, P./Kraaibeek, P.: Grundlegende Aspekte der Systemsicherheit in Systemsicherheit. In: Horster, P. (Hrsg.): Systemsicherheit. DuD-Fachbeiträge: Pfitzmann, A./Reimer, H./Rihaczek, K./Roßnagel, A. (Hrsg.), Braunschweig/Wiesbaden 2000, S. 1-18

Humphreys (2002)
Humphreys, T.: The Newly Revised Part 2 of BS 7799, o. O. 2002. Veröffentlicht im Internet: URL: http://www.gammassl.co.uk/bs7799/The%20Newly%20Revised%20Part%202%20of%20BS%207799ver3a.pdf (Stand: 15.01.2003)

ISACA (1998)
Information Systems Audit and Control Association: CoP, COBIT, Marion, IT-Grundschutzhandbuch - vier Methoden im Vergleich, Zürich 1998. Veröffentlicht im Internet: URL: http://www.isaca.ch/download/igcop/igcop_broschuere.pdf (Stand: 15.01.2003)

ISO 13335-1 (1996)
International Organization for Standardization/International Electrotechnical Commission: ISO/IEC TR 13335-1:1996: Information technology - Guidelines for the management of IT Security - Part 1: Concepts and models for IT Security, Genf 1996

ISO 13335-2 (1997)
International Organization for Standardization/International Electrotechnical Commission: ISO/IEC TR 13335-2:1997: Information technology - Guidelines for the management of IT Security - Part 2: Managing and planning IT Security, Genf 1997

ISO 13335-3 (1998)
International Organization for Standardization/International Electrotechnical Commission: ISO/IEC TR 13335-3:1998: Information technology - Guidelines for the management of IT Security - Part 3: Techniques for the management of IT Security, Genf 1998

ISO 13335-4 (2000)
International Organization for Standardization/International Electrotechnical Commission: ISO/IEC TR 13335-4:2000: Information technology - Guidelines for the management of IT Security - Part 4: Selection of safeguards, Genf 2000

ISO 13335-5 (2001)
International Organization for Standardization/International Electrotechnical Commission: ISO/IEC TR 13335-5:2001: Information technology - Guidelines for the management of IT Security - Part 5: Management guidance on network security, Genf 2001

ISO 15408-1 (1999)
International Organization for Standardization/International Electrotechnical Commission: ISO/IEC 15408-1:1999: Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model, Genf 1999

ISO 15408-2 (1999)
International Organization for Standardization/International Electrotechnical Commission: ISO/IEC 15408-2:1999: Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements, Genf 1999

ISO 15408-3 (1999)
International Organization for Standardization/International Electrotechnical Commission: ISO/IEC 15408-3:1999: Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements, Genf 1999

ISO 17799 (2000)
International Organization for Standardization/International Electrotechnical Commission: ISO/IEC 17799:2000: Information technology - Code of practice for information security management, Genf 2000

ISO 9000 (2000)
International Organization for Standardization: ISO 9000:2000: Quality Management Systems - Fundamentals and vocabulary, Genf 2000

IT-Prüfzeichen (2002)
O. V.: Prüfzeichen: IT-Sicherheit wird offiziell besiegelt. In: Computer-Zeitung, 32. Jg. (2002) H. 7, S. 1

Jaspers (1997)
Jaspers, J.: Organisatorische Hilfen und Tools zur Erleichterung der Arbeit des betrieblichen Datenschutzbeauftragten. In: Voßbein, R. (Hrsg.): Die Organisation der Arbeit des betrieblichen Datenschutzbeauftragten, Frechen 1997, S. 159-169

Jung/Han/Suh (1999)
Jung, C./Han, I./Suh, B.: Risk Analysis for Electronic Commerce Using Case-Based Reasoning. In: International Journal of Intelligent Systems in Accounting, Finance & Management, Vol. 8, 1999, pp. 61-73

Junginger/Krcmar (2002)
Junginger, M./ Krcmar, H.: IT-Risk-Management. In: WISU, o. Jg. (2002) H. 3, S. 360-368

Kailay/Jarratt (1995)
Kailay, M. P./Jarratt, P.: RAMeX: A prototype expert system for computer security risk analysis and management. In Computers & Security, Vol. 14(5), 1995, S. 449-463

Karger (1999)
Karger, P.: IT-Sicherheitsbewußtsein kommunizieren - Ein Weg gegen Irrtum und Nachlässigkeit. In: BSI (Hrsg.): Zur Didaktik der IT-Sicherheit, Ingelheim 1999, S. 153-171

Kersten (1997)
Kersten, H.: Sicherheitszertifizierung- Stand und Perspektiven. In: BSI (Hrsg.): Mit Sicherheit in die Informationsgesellschaft. Tagungsband: 5. Deutscher IT-Sicherheitskongreß des BSI, Ingelheim 1997, S. 323-324

Kerster (1995)
Kerster, H.: Sicherheit in der Informationstechnik, 2. Aufl., München/Wien 1995

Kimmel/Vetter (2001)
Kimmel, M./Vetter, A.: Einbruch im Auftrag: Eine Toolbox für Penetrationstests. In: BSI (Hrsg.): 2001 - Odyssee im Cyberspace? Sicherheit im Internet! Tagungsband: 7. Deutschen IT-Sicherheitskongreß des BSI 2001, Ingelheim 2001, S. 73-86

Kingston (1998)
Kingston, J. K C.: Designing knowledge based systems: the CommonKADS design model. In: Knowledge-Based Systems, Vol. 11(5-6), 1998, pp. 311-319

Kirchhoff (1994)
Kirchhoff, S.: Abbildungsqualität von wissensbasierten Systeme. Reihe: Wirtschaftsinformatik, Band 13, Seibt, D./Derigs, U./Mellis, W. (Hrsg.), Bergisch Gladbach/Köln 1994

Königshofen (1997)
Königshofen, T.: Die Arbeit des Konzern-DSB. In: Voßbein, R. (Hrsg.): Die Organisation der Arbeit des betrieblichen Datenschutzbeauftragten, Frechen 1997, S. 99-119

Konrad (1998)
Konrad, P.: Geschäftsprozeß-orientierte Simulation der Informationssicherheit. Reihe: Wirtschaftsinformatik, Band 20, Seibt, D./Derigs, U./Mellis, W. (Hrsg.), Lohmar/Köln 1998

Koolwijk (1974)
Koolwijk, J. van: Erhebungsmethoden: Die Befragung. In: Koolwijk, J. van/Wieken-Mayser, M. (Hrsg.): Techniken der empirischen Sozialforschung, Band 4, München/Wien 1974

Krallmann (1989)
Krallmann, H.: EDV-Sicherheitsmanagement. Integrierte Sicherheitskonzepte für betriebliche Informations- und Kommunikationssysteme, Berlin 1989

Krallmann (2001)
Krallmann, H.: Management Support Systeme (MSS). In: Mertens, P. (Hrsg.): Lexikon der Wirtschaftsinformatik, 4. Aufl., Berlin u.a. 2001, S. 287-288

Krcmar (2000)
Krcmar, H.: Informationsmanagement, 2. Aufl., Berlin u.a. 2000

Krüger (1992)
Krüger, W.: Organisationsmethodik. In: Frese, E. (Hrsg.): Handwörterbuch der Organisation, 3. Aufl., Stuttgart 1992, S. 1572-1588

Kruth (1995)
Kruth, W.: Probleme und Lösungen in unterschiedlichen Systemstrukturen. In: Voßbein, R. (Hrsg.): Handbuch 3: Organisation sicherer Informationsverarbeitungssysteme, München/Wien 1995, S. 53-99

Kubicek (2001)
Kubicek, H.: Die digitale Signatur zwischen Bürger und Verwaltung - Erleichterung oder Erschwernis? In: BSI (Hrsg.): 2001 - Odyssee im Cyberspace? Sicherheit im Internet! Tagungsband: 7. Deutschen IT-Sicherheitskongreß des BSI 2001, Ingelheim 2001, S. 11 - 22

Kurbel (1992)
Kurbel, K.: Entwicklung und Einsatz von Expertensystemen, 2. Aufl., Berlin u.a. 1992

Kyas (1996)
Kyas, O.: Sicherheit im Internet, Bergheim 1996

LDSG SH (2000)
Schleswig-holsteinisches Gesetz zum Schutze personenbezogener Informationen, vom 09.02.2000. Veröffentlicht im Internet: URL: http://www.datenschutzzentrum.de//material/recht/ldsh-neu/ldsg-neu.htm (Stand: 10.12.2002)

Lelke (1999)
Lelke, B.: Erklärungen in Fuzzy Expertensysteme, Aachen 1999

Lenz (1991)
Lenz , A.: Knowledge Engineering für betriebliche Expertensysteme, Wiesbaden 1991

Lepschies (2000)
Lepschies, G.: E-Commerce und Hackerschutz, 2. Aufl.. DuD-Fachbeiträge: Pfitzmann, A./Reimer, H./Rihaczek, K./Roßnagel, A. (Hrsg.), Braunschweig/Wiesbaden 2000

Licht (1996)
Licht, R.: Aufbau und Arbeitsweise einer Informationssicherheits (IS)-Organiation in einem Unternehmen oder einer Behörde. In: Bauknecht, K./Karagiannis, D./Teufel, S. (Hrsg.): Sicherheit in Informationssystemen. Beiträge der Fachtagung SIS'96 in Wien vom 21-22 März 1996. Zürich 1996, S. 22-36

Lippold (1992)
Lippold, H.: Informationssicherheit. In: Frese, E. (Hrsg.): Handwörterbuch der Organisation, 3. Aufl., Stuttgart 1992, S. 912-922

Lippold/Stelzer/Konrad (1992)
Lippold, H./Stelzer, D./Konrad, P.: Sicherheitskonzepte und ihre Verknüpfung mit Sicherheitsstrategie und Sicherheitsmanagement. In: Wirtschaftsinformatik, 34. Jg. (1992) H. 4, S. 367-377

Locarek-Junge (1995)
Locarek-Junge, H.: Probleme und Lösungen in PC-orientierten Konfigurationen. In: Voßbein, R. (Hrsg.): Handbuch 3: Organisation sicherer Informationsverarbeitungssysteme, München/Wien 1995, S. 81-99

Mackenbrock (1999)
Mackenbrock, M.: Common Criteria - Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik. In: BSI (Hrsg.): IT-Sicherheit ohne Grenzen? Tagungsband: 6. Deutscher IT-Sicherheitskongreß des BSI, Ingelheim 1999, S. 93-105

Mackenbrock (2001)
Mackenbrock, M.: Common Criteria Zertifizierung und Schutzprofile - Ein Angebot für IT-Anwender. In: BSI (Hrsg.): 2001 - Odyssee im Cyberspace? Sicherheit im Internet! Tagungsband des 7. Deutschen IT-Sicherheitskongreß des BSI 2001, Ingelheim 2001, S. 341-350

Maczkowsky/Rost/Köhntopp (2001)
Maczkowsky, R./Rost, R./Köhntopp, K.: Die Internet-Anbindung des virtuellen Datenschutzbüros - Open Source und innovative Internet-Konzepte in der Verwaltung. In: BSI (Hrsg.): 2001 - Odyssee im Cyberspace? Sicherheit im Internet! Tagungsband: 7. Deutschen IT-Sicherheitskongreß des BSI 2001, Ingelheim 2001, S. 57-71

Malley (2001)
Malley, J.: Internet-Kriminalität: Rahmenbedingungen zur Prävention aus polizeilicher Sicht. In: BSI (Hrsg.): 2001 - Odyssee im Cyberspace? Sicherheit im Internet! Tagungsband: 7. Deutschen IT-Sicherheitskongreß des BSI 2001, Ingelheim 2001, S. 363-367

Marcus (1998)
Marcus S. (Eds.): Automating Knowledge Acquisition for Expert Systems, Boston/Dordrecht/London 1988

Martin/Subramanian/Yaverbaum (1996)
Martin, B./Subramanian, G./Yaverbaum, G.: Benefits from expert systems: An exploratory investigation. In: Expert Systems with Applications, Vol 11(1), 1996, pp. 53-58

McNurlin/Sprague (1998)
McNurlin, B. C./Sprague, R.H.: Information Systems Management in Practice, 5th ed., New Jersey 1998

Mertens (1989)
Mertens, P.: Expertisesystem als Variante der Expertensysteme zur Führungsinformation. In: zfbf, 41. Jg. (1989) H. 10, S. 835-854

Mertens (2001)
Mertens, P.: Expertisesystem: In: Mertens, P. (Hrsg.): Lexikon der Wirtschaftsinformatik, 4. Aufl., Berlin u.a. 2001, S. 197

Mertens/Borkowski/Geis (1993)
Mertens, P./Borkowski, V./Geis, W.: Betriebliche Expertensystem-Anwendungen, 3. Aufl., Berlin u.a. 1993

Möhrle (1997)
Möhrle, M. G.: Ein Computerunterstützter Dialogfragebogen (CUDiF) in praktischer Erprobung. In: Wirtschaftsinformatik, 39. Jg. (1997) H. 5, S. 461-467

Möhrle/Hoffmann (1994)
Möhrle, M. G./Hoffmann, W.: Interaktives Erheben von Informationen im computerunterstützten Dialogfragebogen. In: Wirtschaftsinformatik, 36. Jg. (1994) H. 3, S. 243-251

Motta (1999)
Motta, E.: Reusable Components for Knowledge Modelling, Amsterdam u.a. 1999

Mühlen (1995)
Mühlen, R.A.H. von: Planung sicherer Rechenzentren. In: Pohl, H./Weck, G. (Hrsg.): Handbuch 2: Managementaufgaben im Bereich der Informationssicherheit, München/Wien 1995, S. 165-201

Müller/Tietjen (2000)
Müller, D. H./Tietjen, T.: FMEA-Praxis, München/Wien 2000

Münch (1995)
Münch, P.: Tools und PC-unterstützte Instrumente. In: Voßbein, R. (Hrsg.): Handbuch 3: Organisation sicherer Informationsverarbeitungssysteme, München/Wien 1995, S. 289-303

Münch (1999)
Münch, I.: Sicherheitsrevision - Praktische Erfahrungen des BSI und theoretische Ansätze. In: BSI (Hrsg.): IT-Sicherheit ohne Grenzen? Tagungsband: 6. Deutscher IT-Sicherheitskongreß des BSI, Ingelheim 1999, S. 355-360

Münch/Niggemann (2001)
Münch, I./Niggemann, H.: Messbare IT-Sicherheit - das IT-Grundschutz-Zertifikat. In: BSI (Hrsg.): 2001 - Odyssee im Cyberspace? Sicherheit im Internet! Tagungsband: 7. Deutschen IT-Sicherheitskongreß des BSI 2001, Ingelheim 2001, S. 257-267

Murray (1999)
Murray, W. H.: Enterprise Security Architecture. In: Tipton, H. F./Krause, M. (Eds.): Information Security Management Handbook, 4th ed., Boca Raton u.a. 1999, pp. 215-230

Newell (1982)
Newell, A.: The Knowledge Level. In: Artificial Intelligence, Vol. 18(1), 1982, pp. 87-127

Nosworthy (2000)
Nosworthy, J. D.: A practical Risk Analysis approach: Managing BCM Risk. In: Computers & Security, Vol. 19 (7), 2001, pp. 596-614

Oppliger (1997)
Oppliger, R.: IT-Sicherheit Grundlagen und Umsetzung in der Praxis, Braunschweig/Wiesbaden 1997

Opitz (1999)
Opitz, O.: Numerische Taxonomie. Reihe Betriebswirtschaftslehre: Grundwissen der Ökonomik, Bea, F. X./Dichtl, E./Schweitzer, M. (Hrsg.), Stuttgart/New York 1980

Ozier (1999)
Ozier, W.: Risk Analysis and Assessment. In: Tipton, H. F./Krause, M. (Eds.): Information Security Management Handbook, 4th ed., Boca Raton u.a. 1999, pp. 247-285

Peirce (1932)
Peirce, C. S.: Collected Papers of Charles Saunders Peirce, Vol. 2, Element of Logic, Cambridge 1932

Peltier (1999)
Peltier, T.: Security Awareness Program. In: Tipton, H. F./Krause, M. (Eds.): Information Security Management Handbook, 4th ed., Boca Raton u.a. 1999, pp. 197-212

Pernul/Röhm/Herrmann (1999)
Pernul, G./Röhm, A. W./Herrmann, G.: Trust for Electronic Commerce Transactions. In: Eder, J./Rozman, I./Welzer, T. (Eds.): Advances in Databases and Information Systems. 3th East-European Conference, ADBIS'99 in Maribor (Slovenia), September 13-16, Proceedings. Berlin u.a. 1999, pp. 1-13

Petzel (1996)
Petzel, E.: Management der Informationssicherheit, Weiden/Regensburg 1996

Pfeifer/Rothenfluh (1994)
Pfeifer, R./Rothenfluh, T.: Trends in der Artificial Intelligence - Anmerkungen zur Situation in der Schweiz. In: Coy, W./Cyranek, G. (Hrsg.): Die maschinelle Kunst des Denkens, Braunschweig/Wiesbaden 1994, S. 41-56

Pfitzmann (2001)
Pfitzmann, A.: Datenschutzfreundliche Techniken als Beitrag zur Mehrseitigen Sicherheit. In: BSI (Hrsg.): 2001 - Odyssee im Cyberspace? Sicherheit im Internet! Tagungsband: 7. Deutschen IT-Sicherheitskongreß des BSI 2001, Ingelheim 2001, S. 165-180

Piechota (1993)
Piechota, S.: DV-Unterstützung des Controllings mit Hilfe von Führungsinformationssystemen. In: Behme, W., Schimmelpfeng, K. (Hrsg.): Führungsinformationssysteme, Wiesbaden 1993, S. 83-103

Pirlein (1995)
Pirlein, T.: Wiederverwendung von Commonsense Ontologien im Knowledge Engineering, Sank Augustin 1995

Plate (1997)
Plate, A.: IT-Sicherheitsmanagement in der internationalen Standardisierung. In: BSI (Hrsg.): Mit Sicherheit in die Informationsgesellschaft. Tagungsband: 5. Deutscher IT-Sicherheitskongreß des BSI, Ingelheim 1997, S. 369-376

Poeck/Gappa (1993)
Poeck, K./Gappa, U.: Making Role-Limiting Shells more flexible. In: Aussenac, N./Boy, G./Gaines, B./Linster, M./Ganascia, J.-G./ Kodratoff, Y. (Eds.): Knowledge Acquisition for Knowledge-Based Systems. Lecture Notes in Artificial Intelligence (LNAI 723), Berlin u.a. 1993, pp.103-122

Pohl (1995)
Pohl, H.: Verantwortung und Aufgaben des IV-Sicherheitsbeauftragten. In: Pohl, H./Weck, G. (Herg.): Handbuch 2: Managementaufgaben im Bereich der Informationssicherheit, München/Wien 1995, S. 103-120

Pongratz (1996)
Pongratz, M.: Verfahren zur Risikoanalyse in der Informatik-Revision. In: Bauknecht, K./Karagiannis, D./Teufel, S. (Hrsg.): Sicherheit in Informationssystemen. Beiträge der Fachtagung SIS'96 in Wien vom 21-22 März 1996. Zürich 1996, S. 229-249

Preece et al.(2001)
Preece, A./Flett, A./Sleeman, D./Curry, D./Meany, N./Perry, P.: Better Knowledge Management through Knowledge Engineering. In: IEEE Intelligent Systems, Vol. 16(1), 2001, pp. 36-43

Primio (1993)
Primio, F. di: Hybride Wissensverarbeitung. Am Beispiel von BABYLON, Wiesbaden 1993

Puppe (1990)
Puppe, F.: Problemlösungsmethoden in Expertensystemen. Studienreihe: Informatik, Brauer, W./Goos, G. (Hrsg.), Berlin u.a. 1990

Puppe (1991)
Puppe, F.: Einführung in Expertensystem, 2. Aufl., Studienreihe: Informatik, Brauer, W./Goos, G. (Hrsg.), Berlin u.a. 1991

Puppe (1998)
Puppe, F.: Knowledge reuse among diagnostic problem-solving methods in the Shell-Kit D3. In: International Journal of Human-Computer Studies, Vol. 49(4), 1998, pp. 627-649

Puppe et al. (1996)
Puppe, F./Gappa, U./Poeck, K./Bamberger, S.: Wissensbasierte Diagnose- und Informationssysteme, Berlin/Heidelberg 1996

Puppe/Stoyan/Studer (2000)
Puppe, F./Stoyan, H./Studer, R.: Knowledge Engineering. In: Görz, G./Rollinger, C.-R./Schneeberger, J. (Hrsg.): Handbuch der Künstlichen Intelligenz, 3. Aufl., München/Wien 2000, S. 599-641

Ralfs (1995)
Ralfs, D.: Wissensbasierte Konfiguration von Modellen für Informationssysteme, Aachen 1995

Rannenberg (1998)
Rannenberg, K.: Zertifizierung mehrseitiger IT-Sicherheit. Kriterien und organisatorische Rahmenbedingungen. Braunschweig/Wiesbaden 1998

Rannenberg (2000)
Rannenberg, K.: Mehrseitige Sicherheit - Schutz für Unternehmen und ihre Partner im Internet. In: Wirtschaftsinformatik, 42. Jg. (2000) H. 6, S. 489-499

Reimer (1991)
Reimer, U: Einführung in die Wissensrepräsentation. Reihe: Leitfäden der angewandten Informatik, Appelrath, H.-J./Zürich, L. R./Stucky, W. (Hrsg.), Stuttgart 1991

Reynaud/Tort (1997)
Reynaud, C./Tort, F.: Using explicit ontologies to create problem solving methods. In: International Journal of Human-Computer Studies, Vol. 46(2-3), 1997, pp. 339-364

Richards/Simoff (2001)
Richards, D./Simoff, S. J.: Design ontology in context - a situated cognition approach to conceptual modelling. In: Artificial Intelligence in Engineering, Vol. 15(2), 2001, pp. 121-136

Risknews (2000)
o. V.: KonTraG - Gesetzlich verordnetes RM? In: Risknews, o. Jg. (2000) H. 7, S. 2-6. Veröffentlicht im Internet: URL: http://www.risknet.de/Data/Risknews07_2000.pdf (Stand: 10.12.2002)

Röhm (2000)
Röhm, A. W.: Sicherheit offener Elektronischer Märkte. Reihe: Electronic Commerce, Band 4, Szyperski, N./Schmid, B. F./Scheer, A.-W./Pernul, G./Klein, S. (Hrsg.), Lohmar/Köln 2000

Röhrig/Knorr/Noser (2000)
Röhrig, S./Knorr, K./Noser, H.: Sicherheit von E-Business-Anwendungen - Struktur und Quantifizierung. In: Wirtschaftsinformatik, 42. Jg. (2000) H. 6, S. 499-507

Roßnagel (2000)
Roßnagel, A.: Datenschutzaudit. DuD-Fachbeiträge: Pfitzmann, A./Reimer, H./Rihaczek, K./Roßnagel, A. (Hrsg.), Braunschweig/Wiesbaden 2000

Roßnagel/Pfitzmann/Garstka (2001)
Roßnagel, A./Pfitzmann, A./Garstka, H.: Modernisierung des Datenschutzrechtes. Gutachten im Auftrag des Bundesministeriums des Innern, Berlin 2001.

Roth (1995)
Roth, E.: Sozialwissenschaftliche Methoden: Lehr- und Handbuch für Forschung und Praxis. Erwin Roth (Hrsg.), 4. Aufl., München 1995

RSD (1999)
Damm, D./Kirsch, P./Schlienger, T./Teufel, S./Weidner, H./Zurfluh, U.: Rapid Secure Development. Ein Verfahren zur Definition eines Internet-Sicherheitskonzepts. Projektbericht SINUS - Sichere Nutzung von Online-Diensten. Universität Zürich - Institut für Informatik 1999. Veröffentlicht im Internet: URL: http://www.ifi.unizh.ch/ikm/SINUS/publications.html (Stand: 10.12.2002)

Ru/Eloff (1996)
Ru, W. G. de/Eloff, J. H. P.: Risk analysis modelling with the use of fuzzy logic. In Computer & Security Vol. 15(3), 1996, pp. 239-248

Rupietta (1996)
Rupietta, W.: Ein Modell zur organisationsbestimmten Verwaltung von Zugriffsrechen. In: Bauknecht, K./Karagiannis, D./Teufel, S. (Hrsg.): Sicherheit in Informationssystemen. Beiträge der Fachtagung SIS'96 in Wien vom 21-22 März 1996, Zürich 1996, S. 53-67

Scanlon (1999)
Scanlon, S.: World Wide Web Application Security. In: Tipton, H. F./Krause, M. (Eds.): Information Security Management Handbook, 4th ed., Volume 2, Boca Raton u.a. 1999, pp. 271-289
In: KES, o. Jg. (2002) H. 1, S. 68-70

Schäfer (1995)
Schäfer, G.: Sicherheitsgewinn durch ablauforganisatorische Lösungen. In: Voßbein, R. (Hrsg.): Handbuch 3: Organisation sicherer Informationsverarbeitungssysteme, München/Wien 1995, S.128-139

Schaar/Stutz (2002)
Schaar, P./Stutz, O.: Datenschutz-Gütesiegel für Online-Dienstleistungen. In: DuD, 26 Jg. (2002) H. 6, S. 330-334

Schaurette (1999)
Schaurette, K. M.: The Building Blocks of Information Security. In: Tipton, H. F./Krause, M. (Eds.): Information Security Management Handbook, 4th ed., Volume 2, Boca Raton u.a. 1999, pp. 221-240

Scheer (1998)
Scheer, A.-W.: Wirtschaftsinformatik. Referenzmodelle für industrielle Geschäftsprozesse, 7. Aufl., Berlin u.a. 1998

Schefe (1986)
Schefe, P.: Künstliche Intelligenz - Überblick und Grundlagen, Mannheim 1986

Scherdtfeger (1999)
Schwerdtfeger, A.: Probleme und Fragen zum Vertragsrecht. In: Scherdtfeger, A./Evertz, S./Kreuzer, P. A./Peschel-Mehner, A./Poeck, T.: Cyberlaw, Wiesbaden 1999, S. 7-30

Scherdtfeger et al. (1999)
Scherdtfeger, A./Evertz, S./Kreuzer, P. A./Peschel-Mehner, A./Poeck, T.: Cyberlaw, Wiesbaden 1999

Schily (2001)
Schily, O. (Bundesminister des Innern): Kongress „Effizienter Staat“, o. O. Februar 2001. Veröffentlicht im Internet: URL: http://www.bsi.de/certbund/index.html (Stand: 10.12.2002)

Schmidtchen (1962)
Schmidtchen, G.: Der Anwendungsbereich betriebssoziologischer Umfragen, Bern 1962

Schönberg/Thoben (1999)
Schönberg, A./Thoben, W.: Ein unscharfes Bewertungskonzept für die Bedrohungs- und Risikoanalyse Workflow-basierter Anwendungen. In: Röhm, A./Fox, D./Grimm, R./Schoder, D. (Hrsg.): Sicherheit und Electronic Commerce. DuD-Fachbeiträge: Pfitzmann, A./Reimer, H./Rihaczek, K./Roßnagel, A. (Hrsg.), Braunschweig/Wiesbaden 1999, S. 47-62

Schönebeck (1994)
Schönebeck, H.: Finanzmanagement auf Basis von Expertensystemen. Schriftenreihe: Controlling, Band 4, Serfling, K. (Hrsg.), Ludwigsburg/Berlin 1994

Schreiber et al. (2000)
Schreiber, G./Akkermans, H./Anjewierden, A./de Hoog, R./Shadbolt, N./Van de Velde, W./Wielinga, B.: Knowledge Engineering and Management, Cambridge u.a. 2000

Schulte (1993)
Schulte, U.: Einführung in Fuzzy-Logik, München 1993

Schütte (1998)
Schütte, R.: Grundsätze ordnungsmäßiger Referenzmodellierung, Wiesbaden 1998

Schwarzer/Krcmar (1996)
Schwarzer, B./Krcmar, H.: Wirtschaftsinformatik. Grundzüge der betrieblichen Datenverarbeitung, Stuttgart 1996

Servatius (1991)
Servatius, K.: Empirische Forschung und Expertensysteme, Frankfurt a. M. u.a. 1991

Sharp (2002)
Sharp, J.: Introduction. The Development of Business Continuity Management. In: Wieczorek, M./Naujoks, U./Bartlett, B. (Eds.): Business Continuity, Berlin u.a. 2002, S. IX-XII

Sienkiewicz (1994)
Sienkiewicz, B. S.: Computersicherheit, Bonn u.a. 1994

SigG (2001)
Gesetz zur digitalen Signatur (Signaturgesetz - SigG), vom 01.05.2001. Veröffentlicht im Internet: URL: http://www.netlaw.de/gesetze/sigg.htm (Stand: 10.12.2002)

Sigesmund (1995)
Sigesmund, M.: Konzepte auf der Basis von Szenario-Studien. In: Voßbein, R. (Hrsg.): Handbuch 3: Organisation sicherer Informationsverarbeitungssysteme, München/Wien 1995, S. 128-139

Skoudis (1999)
Skoudis, E.: Hacker Tools and Techniques. In: Tipton, H. F./Krause, M. (Eds.): Information Security Management Handbook, 4th ed., Volume 2, Boca Raton u.a. 1999, pp. 453-474

Snouffer/Lee/Oldehoeft (2001)
Snouffer, R./Lee, A./Oldehoeft, A.: A Comparison of Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2, NIST Special Publication 800-29, Gaithersburg 2001. Veröffentlicht im Internet: URL: http://csrc.nist.gov/publications/nistpubs/800-29/sp800-29,pdf (Stand: 10.10.2002)

Sobirey (1999)
Sobirey, M.: Datenschutzorientiertes Intrusion Detection. DuD-Fachbeiträge: Pfitzmann, A./Reimer, H./Rihaczek, K./Roßnagel, A. (Hrsg.), Braunschweig/Wiesbaden 1999

Solms (1996)
Solms, R. von: Information Security Management: The Second Generation. In: Computers & Security, Vol. 15(4), 1996, pp. 281-288

Speel et al. (2001)
Speel, P-H./Schreiber, A. Th./Joolingen, W. van/Heijst, G. van/Beijer, G. J.: Conceptual Modelling for Knowledge-Based Systems. In: Encyclopedia of Computer Science and Technology, New York 2001, nnb. Veröffentlicht im Internet: URL: http://www.swi.psy.uva.nl/usr/schreiber/home.html (Stand: 10.12.2002)

Spies (1993)
Spies, M.: Unsicheres Wissen. Wahrscheinlichkeit, Fuzzy-Logik, neuronale Netze und menschliches Denken, Heidelberg/Berlin/Oxford 1993

Staab et al. (2001)
Staab, S./Schnurr, H.-P./Studer, R./Sure, Y.: Knowledge Processes and Ontologies. In: IEEE Intelligent Systems, Vol. 16(1), 2001, pp. 26-34

Stelzer (1993)
Stelzer, D.: Sicherheitsstrategien in der Informationsverarbeitung - Ein wissensbasiertes, objektorientiertes System für die Risikoanalyse, Wiesbaden 1993

Stelzer (1995)
Stelzer, D.: Konzepte auf der Basis von Risikoanalysen. In: Voßbein, R. (Hrsg.): Handbuch 3: Organisation sicherer Informationsverarbeitungssysteme, München/Wien 1995, S. 115-128

Stickel/Groffmann/Rau (1998)
Stickel, E/Groffmann, H.-D./Rau, K.-H. (Hrsg.): Gabler Wirtschaftsinformatik Lexikon, Wiesbaden 1998

Stier (1996)
Stier, W.: Empirische Forschungsmethoden, Berlin u.a. 1996

Strube et al. (2000)
Strube, G./Habel, C./Konieczny, L./Hemforth, B.: Kognition. In: Görz, G./Rollinger, C.-R./Schneeberger, J. (Hrsg.): Handbuch der Künstlichen Intelligenz, 3. Aufl., München/Wien 2000, S. 19-72

Struss (2000)
Struss, P.: Modellbasierte Systeme und qualitative Modellierung. In: Görz, G./Rollinger, C.-R./Schneeberger, J. (Hrsg.): Handbuch der Künstlichen Intelligenz, 3. Aufl., München/Wien 2000, S. 431-490

Studer et al. (2000)
Studer, R./Decker, S./Fensel, D./Staab, S.: Situation and Perspective of Knowledge Engineering. In: Cuena, J./Demazeau, Y./Garcia, A./Treur, J. (Eds.): Knowledge Engineering and Agent Technologies, IOS Series on Frontiers in Artificial Intelligence and Application, Vol. 52, Amsterdam 2000, nnb. Veröffentlicht im Internet: URL: http://www.aifb.uni-karlsruhe.de/FormschungsgruppeIWBS/Publications/pub2000.html (Stand: 10.12.2002)

Studer/Benjamins/Fensel (1998)
Studer, R./Benjamins, V. R./Fensel, D.: Knowledge Engineering: Principles and methods. In: Data & Knowledge Engineering, Vol. 25(1-2), 1998, pp. 161-197

Stumme (1999)
Stumme, G.: Acquiring Expert Knowledge for the Design of Conceptual Information Systems. In: Fensel, D./Studer, R. (Eds.): Knowledge Acquisition, Modeling and Management. 11th European Workshop, EKAW 1999 in Dagstuhl Castle (Germany), May 26-29, Proceedings. Lecture Notes in Artificial Intelligence (LNAI 1621), Berlin u.a. 1999, pp. 275-290

Task-Force-DDoS (2000)
Bundesamt für Sicherheit in der Informationstechnik: Empfehlungen zum Schutz vor verteilten Denial of Service-Angriffen im Internet, Version 1.1a vom 20.06.2000, o. O. 2000. Veröffentlicht im Internet: URL: http://www.bsi.de/taskforce/ddos.htm (Stand: 10.12.2002)

Task-Force-Virenschutz (2000)
Bundesamt für Sicherheit in der Informationstechnik: Empfehlungen zum Schutz vor Computer-Viren aus dem Internet, Version 1.0 vom 18.05.2000, o. O. 2000. Veröffentlicht im Internet: URL: http://www.bsi.de/taskforce/viren.htm (Stand: 10.12.2002)

TDDSG (1997)
Gesetz über den Datenschutz bei Telediensten (Teledienstedatenschutzgesetz -TDDSG), vom 01.08.1997. Veröffentlicht im Internet: URL: http://www.netlaw.de/gesetze/tddsg.htm (Stand: 10.12.2002)

TDG (2001)
Teledienstgesetz (TDG), vom 14.12.2001. Veröffentlicht im Internet: URL: http://www.netlaw.de/gesetze/tkg_1.htm und http://www.netlaw.de/gesetze/tdg.htm (Stand: 10.12.2002)

TDSV (2002)
Telekommunikations-Datenschutzverordnung (TDSV), vom 18. Dezember 2000. Veröffentlicht im Internet: URL: http://www.netlaw.de/gesetze/tdsv.htm (Stand: 10.12.2002)

Teaminfo (2001)
Bundesamt für Sicherheit in der Informationstechnik: CERT-Bund: Teaminfo, Version 1.0, Bonn 2001. Veröffentlicht im Internet: URL: http://www.bsi.de/certbund/teaminfo/cb2350de.htm (Stand: 10.12.2002)

Theil (1995)
Theil, M.: Risikomanagement für Informationssysteme. Schriftenreihe: Forschungsergebnisse der Wirtschaftsuniversität Wien, Wien 1995

Thoben (2000)
Thoben, W.: Wissensbasierte Bedrohungs- und Risikoanalyse Workflow-basierter Anwendungssysteme. Teubner-Reihe: Wirtschaftsinformatik, Ehrenberg, D./Seibt, D./Stucky, W. (Hrsg.), Stuttgart/Leipzig/Wiesbaden 2000

Thuy/Schnupp (1989)
Thuy, N.H.C./Schnupp, P.: Wissensverarbeitung und Expertensysteme. Reihe: Handbuch der Informatik, Band 6.1, Endres, A./Krallmann, H./Schnupp, P. (Hrsg.), München/Wien 1989

Tinnefeld/Ehmann (1998)
Tinnefeld, M.-T./Ehmann, E.: Einführung in das Datenschutzrecht, 3. Aufl., München/Wien 1998

TKG (1996)
Telekommunikationsgesetz (TKG), vom 25.06.1996. Veröffentlicht im Internet: URL: http://www.netlaw.de/gesetze/tkg_1.htm und http://www.netlaw.de/gesetze/tkg_2.htm (Stand: 10.12.2002)

TKÜV (1998)
Entwurf einer Verordnung über die technische und organisatorische Umsetzung von Überwachungsmaßnahmen in der Telekommunikation (Telekommunikations-Überwachungsverordnung - TKÜV), Stand 11.05.1998. Veröffentlicht im Internet: URL: http://www.digital-law.net/papers/TKUEV.html (Stand: 10.12.2002)

TKV (2002)
Telekommunikations-Kundenschutzverordnung (TKV), vom 01.01.1998. Veröffentlicht im Internet: URL: http://www.netlaw.de/gesetze/tkv.htm (Stand: 10.12.2002)

Traummüller/Lenk/Wimmer (2001)
Traummüller, R./Lenk, K./Wimmer, M.: Wissensmanagement und E-Government. In: Schnurr, H.-P./Staab, S./Studer, R./Stumme, G./Sure, Y. (Hrsg.): Professionelles Wissensmanagement: Erfahrungen und Visionen, Aachen 2001, S. 381-392

Turban/Aronson (1998)
Turban, E/Aronson, J. E.: Decision Support Systems and Intelligent Systems, 5th ed., New Jersey 1998

Volz (2001)
Volz, R.: Eine kleine Einführung in Ontologien. Vortragsfolien zum Workshop: Begriffliche Formalisierung von Prozessen und Systemen an der TU Dresden vom 2. November 2001. Veröffentlicht im Internet: URL: http://math.tu-dresden.de/~rudolph/Dresden_Workshop.ppt (Stand: 10.12.2002)

Voß/Gutenschwager (2001)
Voß, S./Gutenschwager, K.: Informationsmanagement, Berlin u.a. 2001

Voßbein, J. (1999)
Voßbein, J.: Integrierte Sicherheitskonzeptionen für Unternehmen, Ingelheim 1999

Voßbein, R. (1994a)
Voßbein, R.: Schwachstellenanalyse - Ersatz oder Ergänzung von Risikoanalyse? (I). In: KES, o. Jg. (1994) H. 1, S. 34-40

Voßbein, R. (1994b)
Voßbein, R.: Schwachstellenanalyse - Ersatz oder Ergänzung von Risikoanalyse? (II). In: KES, o. Jg. (1994) H. 2 , S. 64-69

Voßbein, R. (1995a)
Voßbein, R.: Organisation der IT-Sicherheit: Probleme und Lösungen. In: Voßbein, R. (Hrsg.): Handbuch 3: Organisation sicherer Informationsverarbeitungssysteme, München/Wien 1995, S. 9-24

Voßbein, R. (1995b)
Voßbein, R.: IT-Sicherheit: Management-Verantwortung und Akzeptanzprobleme. In: Voßbein, R. (Hrsg.): Handbuch 3: Organisation sicherer Informationsverarbeitungssysteme, München/Wien 1995, S. 41-52

Voßbein, R. (1997)
Voßbein, R.: Der Datenschutzbeauftragte - Berufliche Endstation oder Entwicklungsposition? In: Voßbein, R. (Hrsg.): Die Organisation der Arbeit des betrieblichen Datenschutzbeauftragten, Frechen 1997, S. 9-24

Voßbein, R. (2001)
Voßbein, R.: Höhere Systemsicherheit durch Zertifikate. In: KES, o. Jg. (2001) H. 1, S. 74-75

Voßbein, R. (2002)
Voßbein, R.: Datenschutz-Controlling, Ingelheim 2002

Voßbein, R./Voßbein, J. (2002a)
Voßbein, R./Voßbein, J.: Lagebericht zur IT-Sicherheit (1). KES/KPMG-Sicherheitsstudie 2002. In: KES, o. Jg. (2002) H. 3, S. 14-23

Voßbein, R./Voßbein, J. (2002b)
Voßbein, R./Voßbein, J.: Lagebericht zur IT-Sicherheit (2). KES/KPMG-Sicherheitsstudie 2002. In: KES, o. Jg. (2002) H. 4, S. 16-24

Walter (1991)
Walter, B.: Datenbankkonzepte für Wissensbasierte Systeme, IBM Deutschland: Wissenschaftliches Zentrum: Institut für Wissensbasierte Systeme, Trier 1991

Weck (1995)
Weck, G.: Planung und Realisierung der Informationssicherheit. In: Pohl, H./Weck, G. (Hrsg.): Handbuch 2: Managementaufgaben im Bereich der Informationssicherheit, München/Wien 1995, S. 9-24

Wedde/Schröder (2001)
Wedde, P./Schröder, L. (Hrsg.): Das Gütesiegel für Qualität im betrieblichen Datenschutz (Quid!), Frankfurt a. M. 2001

Wedekind et al. (1998)
Wedekind, H./Görz, G./Kötter, R./Inhetveen, R.: Modellierung, Simulation, Visualisierung: Zu aktuellen Aufgaben der Informatik. In: Informatik-Spektrum, 21. Jg. (1998) H. 5, S. 265-272

Wehner (1995)
Wehner, T.: Sichere Systeme als Einstellungs- und Bewußtseinsproblem. In: Voßbein, R. (Hrsg.): Handbuch 3: Organisation sicherer Informationsverarbeitungssysteme, München/Wien 1995, S. 25-40

Weissenfluh (1990)
Weissenfluh, A. von.: Expertensysteme. Berner betriebswirtschaftliche Schriften, Band 5, Griese, J./Kühn, R. (Hrsg.), Bern/Stuttgart 1990

Welge/Al-Laham (1992)
Welge, M. K./Al-Laham, A.: Planung. Prozesse - Strategien - Maßnahmen, Wiesbaden 1992

Werner (1992)
Werner, L.: Entscheidungsunterstützungssysteme, Heidelberg 1992

Weß (1996)
Weß, S.: Fallbasiertes Problemlösen in wissensbasierten Systemen zur Entscheidungsunterstützung und Diagnostik, Sankt Augustin 1996

Winzler/Holbein (1996)
Winzler, S./Holbein, R.: Verfahren zur Auswahl von zertifizierten IT-Systemen unter dem Aspekt der Wirtschaftlichkeit. In: Bauknecht, K./Karagiannis, D./Teufel, S. (Hrsg.): Sicherheit in Informationssystemen. Beiträge der Fachtagung SIS'96 in Wien vom 21-22 März 1996. Zürich 1996, S. 269-289

Wolf (1999)
Wolf, G.: Generische, attributierte Aktionsklassen für mehrseitig sichere, verteilte Anwendungen. In: Röhm, A./Fox, D./Grimm, R./Schoder, D. (Hrsg.): Sicherheit und Electronic Commerce. DuD-Fachbeiträge: Pfitzmann, A./Reimer, H./Rihaczek, K./Roßnagel, A. (Hrsg.), Braunschweig/Wiesbaden 1999, S. 31-46

Wolfertz (2001)
Wolfertz, K.: Wissensmanagement bei Beratern mit Fuzzy Systems. In: Wirtschaftsinformatik, 43. Jg. (2001) H. 5, S. 457-466

Zelewski (1989)
Zelewski, S.: Einsatz von Expertensystemen in den Unternehmen, Ehningen bei Böblingen 1989

Zelewski/Schütte/Siedentopf (2001)
Zelewski, S./Schütte, R./Siedentopf, J.: Ontologien zur Repräsentation von Domänen. In: Schreyögg, G. (Hrsg.): Wissen in Unternehmen, Berlin 2001, S. 183-221

Ziener (1997)
Ziener, K.: Betrieblicher Datenschutzbeauftragter und DV-Revisor - Kooperation oder Gegensätze?. In: Voßbein, R. (Hrsg.): Die Organisation der Arbeit des betrieblichen Datenschutzbeauftragten, Frechen 1997, S. 69-98

Zieschang (2001)
Zieschang, T.: Security Engineering im E-Commerce: Best Practice und Standardsicherheitsmaßnahmen. In: BSI (Hrsg.): 2001 - Odyssee im Cyberspace? Sicherheit im Internet! Tagungsband: 7. Deutschen IT-Sicherheitskongreß des BSI 2001, Ingelheim 2001, S. 211-225

Zilahi-Szabô (1998)
Zilahi-Szabô, M.G.: Grundzüge der Wirtschaftsinformatik, München/Wien 1998

Zimmermann (1993)
Zimmermann, H.-J.: Fuzzy Technologien Prinzipien, Werkzeuge, Potentiale. Düsseldorf 1993