Disclosure Limitation in OLAP

Inaugural-Dissertation zur Erlangung des akademischen Grades eines Doktors der Wirtschaftswissenschaften an der wirtschafts-wissenschaftlichen Fakultät der Universität Passau

vorgelegt von

Dipl.-Kfm. Christoph Lange

Passau

2011

Gutachter

Prof. Dr. Peter Kleinschmidt

Prof. Dr. Franz Lehner

Danksagung

Ich bedanke mich an dieser Stelle bei allen, die mich beim Verfassen dieser Arbeit unterstützt haben.

Mein besonderer Dank gilt Herrn Prof. Dr. Peter Kleinschmidt, der durch seine Betreuung das Entstehen dieser Arbeit erst ermöglicht hat. Mein besonderer Dank gilt auch Herrn Prof. Dr. Franz Lehner für die Übernahme des Zweitgutachtens.

INHALT

ABKÜRZUNGEN

aktual.	aktualisierte
ARBAC	Administrative Role-Based Access Control
bspw.	beispielsweise
BULA	Bundesland
bzgl.	bezüglich
csv	comma-separated values
DAC	Discretionary Access Control
DB	Datenbank
DBMS	Datenbankmanagementsystem
DSS	Decision Support System(s)
DW	Data Warehouse
DWS	Data Warehouse System
EIS	Executive Information System(s)
entspr.	entsprechend(e)
et al.	et alii *oder* et aliae *oder* et alia
hins.	hinsichtlich
Hrsg.	Herausgeber
iabst	Abstände zwischen interessensrelevanten Elementen einer Hierarchiestufe
IC	Inference Control (Inferenzkontrolle)
ICh	Inference Channel
iDIM	interessensrelevante Dimension
i.d.Regel	in der Regel
iHIER	interessensrelevante Hierarchie
iHS	interessensrelevante Hierarchiestufe
IP	Inference Problem
iRAD	Interessensradius
iSE	interessensrelevante Stufenelement
iSWP	Interessensschwerpunkt
IT	Informationstechnologie / Information Technology
Jg.	Jahrgang
km	Kilometer
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich

MAC	Mandatory Access Control
min	Minuten
MIS	Management Information System(s)
MIT	Massachusetts Institute of Technology
ms	Millisekunden
MLS	Multi-Level Secure [Database]
MSS	Management Support Systems
OLAP	On-Line Analytical Processing
OLTP	Online Transactional Processing
ORGA	Organisation
PRA	Permission-Role Assignment
REBE	Regierungsbezirk
RBAC	Role-Based Access Control
RRA	Role-Role Assignment
s	Sekunden
S.	Seite(n)
SDB	Statistical Database oder Statistische Datenbank
SoD	Separation of Duties
sog.	so genannt
STDT	Stadt
SQL	Structured Query Language
u.a.	unter anderem / unter anderen
überarb.	überarbeitete
UCC	SAP University Competence Center
URA	User-Role Assignment
uvm.	und viele mehr
Vgl.	vergleiche
vollst.	vollständig

TABELLEN

ABBILDUNGEN

1 EINLEITUNG

Die vorliegende Arbeit ist in einem ebenso wirtschaftlich bedeutenden[1] wie wissenschaftlich ergiebigen Gebiet der Informationstechnologie angesiedelt: „Business Intelligence“ (BI). Im Kern geht es bei BI-Anwendungen um die IT-getriebene Analyse sehr umfangreicher Datenbestände im Rahmen der Entscheidungsunterstützung. „OLAP“ (On-Line Analytical Processing) stellt hierfür das Basiskonzept zur Strukturierung und Analyse der Datenbestände aus Anwendersicht dar.

Die mit OLAP bearbeiteten Datenbestände können jedoch Informationen enthalten, die bestimmten Personen aus dem Anwenderkreis gerade nicht zugänglich gemacht werden sollen (sog. „sensible Informationen“). Damit ergibt sich ein Spannungsverhältnis zwischen dem eigentlichen Zweck von OLAP und BI (umfassende Informationsversorgung zur Unterstützung betrieblicher Entscheidungen) und der Gefahr, dabei sensible Informationen offen zu legen („Disclosure“). Ziel dieser Arbeit ist vor allem die Entwicklung von Mechanismen, die bei möglichst guter Informationsversorgung, die Gefahr von unerwünschter Offenlegung verringern („Disclosure Limitation“), wobei diese Mechanismen mit einem vertretbaren Aufwand realisierbar, also „praktisch anwendbar“ sein sollen.

Der erste Abschnitt beschreibt diejenigen Entwicklungen bei entscheidungsunterstützenden IT-Systemen, aus denen der Gegenstand dieser Arbeit entstanden ist. So wird das Thema dieser Arbeit zum einen in einen Kontext eingeordnet und zum anderen bereits gegen einige nahe liegende Themenbereiche abgegrenzt. Die Hinführung aus dem ersten Abschnitt 1.1 wird dann im zweiten aufgegriffen und verfeinert, um die wissenschaftliche Motivation der vorliegenden Arbeit zu erläutern. Abschnitt 1.2 schließt mit den abstrakten Zielsetzungen. Mit einer Beschreibung des Aufbaus der Arbeit in Abschnitt 1.3 schließt dieses Kapitel.[2]

---

1 Der Markt für BI-Software wächst stetig - im Jahr 2009 in Deutschland trotz gesamtwirtschaftlich angespannter Lage um 8% auf ein Volumen von 816 Millionen Euro bei ausschließlicher Berücksichtigung von Lizenz- und Wartungsumsätzen [vgl. BARC (2010)].

2 Im ersten Kapitel werden einige Begriffe des allgemeinen Sprachgebrauchs (bspw. „Information“) verwendet, für die im wissenschaftlichen Kontext - je nach Themengebiet und/oder Autor - unterschiedliche Definitionen vorliegen können. Zugunsten der Übersichtlichkeit wird an dieser Stelle jedoch auf definitorische Einschübe verzichtet, soweit diese nicht für eine thematische Verortung der Arbeit erforderlich sind. Alle grundlegenden Begriffe werden dann im Rahmen der folgenden Kapitel an jeweils geeigneter Stelle präzise abgegrenzt.

1.1 Einführung in Kontext und Gegenstand der Arbeit

Mit den ersten betrieblichen IT-Anwendungen in Unternehmen kam bereits Mitte der 1960er Jahre der Gedanke auf, die durch operative Systeme erzeugte Datenbasis zur Gewinnung planungsrelevanter Informationen über das gesamte Unternehmen nutzbar zu machen. Erste Umsetzungsversuche wurden im Rahmen so genannter „Management Information Systems" (MIS) unternommen.[3] Eine wesentliche Funktion von MIS war, Führungskräften eine Gesamtsicht auf das Unternehmen zu bieten, indem Daten aus operativen Systemen integriert und verdichtet zur Verfügung gestellt wurden.[4] Jedoch behinderten zunächst eine noch unzureichende IT-Infrastruktur (insbesondere im Hinblick auf die flexible Integration und Verarbeitung großer Datenmengen)[5], aber auch konzeptionelle Unzulänglichkeiten[6], eine zufrieden stellende Implementierung von MIS.[7] Nichtsdestoweniger wurde die vielfache Verwendung von Reports über aggregierte Geschäftsdaten in Tabellenform, wie sie auch heute in Unternehmen üblich ist, durch die MIS-Bewegung etabliert.

Die IT-getriebene Aufbereitung und Analyse großer Datenbestände zur Unterstützung dispositiver Entscheidungen wurde verbessert und erweitert, wobei die Schwerpunkte in der Zielsetzung dieser Weiterentwicklungen variieren. Zwei bekannte Konzepte sind „Decision Support Systems" (DSS)[8] und „Executive Information Systems" (EIS)[9].

DSS sollen die Abstraktion konkreter Planungsprobleme mit Hilfe von Modellen erleichtern und Methoden zu deren mathematisch-algorithmischer Lösung anbieten. DSS bedienen sich dazu inzwischen in hohem Maße Erkenntnissen aus dem Operations Research.[10] EIS hingegen betonen weniger die Algorithmik zur Problemlösung und mehr die geeigne-

---

3 Vgl. u.a. GLUCHOWSKI/GABRIEL/CHAMONI (2008), S. 55 für diesen und den vorangegangenen Satz

4 Vgl. u.a. CHAMONI/GLUCHOWSKI (1997, S. 152) für eine entspr. enge (Aufgaben-)Definition von MIS

5 Vgl. STAHLKNECHT (1995), S. 288

6 Vgl. bspw. RUSSEL (1967) für eine frühe kritische Betrachtung des Designs von MIS hins. deren Eignung zur Führungsunterstützung (Titel: „Management Misinformation Systems")

7 Vgl. bspw. CHAMONI/GLUCHOWSKI (2006), S. 6

8 Der Begriff DSS geht auf SCOTT MORTON zurück und wurde von GORRY/SCOTT MORTON (1971) geprägt. Vgl. dazu sowie für eine Darstellung der Entwicklungsgeschichte der verschiedenen DSS-Strömungen POWER (2008)

9 Als Initialpunkt des EIS-Konzepts wird der Beitrag „Chief executives define their own data needs" [ROCKART (1979)] betrachtet [vgl. bspw. TURBAN/WATSON (1989), S. 74–75]. Darin wird die Umsetzung des Konzepts „Kritischer Erfolgsfaktoren" im Rahmen eines Informationssystems vorgeschlagen.

10 Vgl. u.a. GLUCHOWSKI/GABRIEL/CHAMONI (2008), S. 63–65

te Darstellung der für die Unternehmensführung wirklich erheblichen Informationen.[11] Je nach Definition und Ausprägung ergänzen die angesprochenen drei Systemkategorien die Nutzbarmachung von Datenbeständen zur entscheidungsunterstützenden Informationsversorgung als tragendes Konzept durch weitere Funktionalität (insbesondere zur Verbesserung der Kommunikation im Unternehmen).[12] Für die vorliegende Arbeit ist jedoch lediglich der Kernaspekt – die Nutzbarmachung von Datenbeständen zur entscheidungsunterstützenden Informationsversorgung – von Interesse.

Kategorisierung und Definition von MIS, DSS und EIS variieren in der Literatur stark; zudem existieren zahlreiche Abwandlungen und Ergänzungen.[13] So werden EIS beispielsweise auch als datenfokussierte Strömung im Rahmen von DSS kategorisiert.[14] Eine genauere phänomenologische Betrachtung ist jedoch für eine Einordnung der vorliegenden Arbeit nicht notwendig.[15] Hierfür ist es hilfreicher, sich die grundlegenden und allen gemeinsamen Anforderungen für die unmittelbar mit der Datenaufbereitung und Datenauswertung befassten Bestandteile dieser Systeme zu vergegenwärtigen. Das diesen Anforderungen zugrunde liegende Ziel ist die IT-getriebene Informationsgewinnung aus großen Mengen quantitativer Daten, um damit Führungs- und Fachkräfte bei dispositiven Entscheidungen zu unterstützen. Die Anforderungen lassen sich grob wie folgt strukturieren.

---

11 Vgl. u.a. ebenda, S. 77 sowie TURBAN/WALLS (1995) für einen Überblick über die frühe Entwicklung des EIS-Konzepts

12 „the use of […] information technologies to support managers [... by...] teleconferencing, electronic data bases, and graphic workstations are all information technologies that are potentially useful for MSS." [SCOTT MORTON (1983), S. 5] MSS steht für Management Support Systems und kann hier als Überkategorie für MIS, DSS und EIS aufgefasst werden.

13 Vgl. OPPELT (1995, S. 9) für eine viel zitierte Systematisierung auch hier nicht genannter Konzepte; Der Begriff MIS umfasst nach dieser Interpretation alle anderen Konzepte als übergeordnete Kategorie. Eine andere Ordnung, in der MIS Spezialfall von EIS sind, schlägt bspw. CORNELIUS (1991) vor.

14 Vgl. bspw. POWER (2008, S. 128) für eine solche Sicht auf EIS

15 Vgl. u.a. SWIONTEK (1997, S. 55–153) für eine umfassende phänomenologische Darstellung sowie eine kritische Bewertung IT-getriebener Konzepte zur Führungsunterstützung bis Mitte der 1990er Jahre

Unternehmen verwenden zumeist mehrere IT-Systeme zur Durchführung des Geschäftsbetriebs (gewöhnlich ERP-Systeme). Die erste Anforderung besteht folglich darin, relevante Daten zur späteren Informationsgewinnung verfügbar zu machen und zu integrieren. Diese Daten müssen ggf. noch durch weitere Daten aus externen Quellen angereichert werden (Schicht I in Abbildung 1). Sollen bspw. die Verkaufszahlen eines Unternehmens analysiert werden, ist es ggf. nötig, sowohl die Verkaufsdaten der deutschen Zentrale als auch die im ERP-System der US-amerikanischen Niederlassung auszuwerten. Dabei müsste bspw. sichergestellt werden, dass derselbe Kunde, der in beiden Systemen geführt wird, bei der Analyse mit einer einzigen Identität auftritt. Um die eigene Verkaufsperformance beurteilen zu können, wäre in diesem Szenario der Zukauf von Daten über Marktwachstum und Marktvolumen in einzelnen Verkaufsregionen bei einem Marktforschungsinstitut denkbar. Die relevanten Daten müssen dann in eine für eine Analyse geeignete Struktur gebracht werden. Diese muss zum einen alle nötigen Daten zu den jeweils gewünschten Analysegegenständen (bspw. Verkaufsdaten des Unternehmens oder Qualitätskontrolle der Fertigungsprozesse) in einer geeigneten Struktur zusammenführen (vgl. Abbildung 1, Schicht II). Die letzte Schicht (Schicht III in Abbildung 1) dient dem Nutzer dann schließlich für die eigentliche Analysetätigkeit. Dazu müssen die Daten in geeigneter Weise dargestellt werden. Eine möglichst intuitive Veränderung der Betrachtungsperspektive durch eine ebenfalls intuitive Bereitstellung von Navigations- bzw. Analysemethoden sollte gewährleistet sein. Die Datenanalyse erfordert nicht nur bei augenfällig komplexen Analyseaufgaben (wie bspw. Analyseverfahren aus dem Operations Research) sondern bereits dann Berechnungen, wenn Daten in unterschiedlichem Detaillierungsgrad dargestellt werden sollen. Besonders zwischen den Schichten II und III ergeben sich Überschneidungen. Die Datenhaltung in

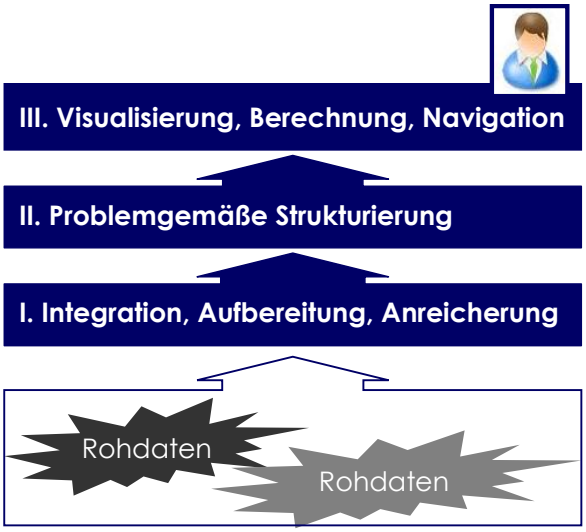


Abbildung 1: Anforderungen bzgl. Informationsgewinnung
Eigene Darstellung[16]

[16] Ähnliche Darstellungen finden sich naturgemäß in vielen Beiträgen zu Data Warehousing und OLAP, da beide Systemkategorien - wie im Weiteren beschrieben wird - Anforderungen dieses Schemas erfüllen.

Schicht II wird bis zu einem gewissen Maße den Analyseerfordernissen in Schicht III entsprechen müssen. Berechnungen von Daten mit verschiedenem Detaillierungsgrad können bereits in Schicht II erfolgen und dann nur noch durch Schicht III abgefragt werden. Die genaue Ausgestaltung ergibt sich durch die technische Implementierung. MIS, DSS und EIS lassen sich alle in diesem Schema abbilden und unterscheiden sich lediglich in der Schwerpunktsetzung. DSS bspw. legen einen verstärkten Fokus auf den Aspekt der „Berechnung".

Ab Mitte der 1990er Jahre nahm dann der Begriff „Business Intelligence" (BI) im eingangs beschriebenen Umfeld immer mehr Raum ein. HOWARD DRESNER wird die Einführung dieser Bezeichnung im modernen Kontext zugeschrieben, wobei die Wortschöpfung mit sehr ähnlichem Bedeutungshintergrund auf einen Beitrag von HANS LUHN (1958)[17] zurückgeht. DRESNER definiert BI in einem viel zitierten Interview wie folgt.

> "Business Intelligence (BI) is a conceptual umbrella. Underneath it are a variety of technologies that support end-user access to and analysis of quantitative information sources."[18]

Es existieren inzwischen zahlreiche Auffassungen, was unter dem Begriff BI zu verstehen ist. Beispielhaft sei hier folgende Definition von GLUCHOWSKI UND KEMPER zitiert.

> „Unter Business Intelligence wird ein integriertes IT-Gesamtkonzept verstanden, das für die unterschiedlichen Ausprägungen der Anforderungen an geeignete Systeme zur Entscheidungsunterstützung tragfähige und miteinander verknüpfte Lösungen anbietet."[19]

Dieser sehr allgemein gehaltenen Definition folgt im weiteren Verlauf des entspr. Beitrags eine Darstellung der Referenzarchitektur für BI-Anwendungen (siehe umseitige Abbildung 2), die dem hier in Abbildung 1 dargestellten Anforderungsschema entspricht. Alle weiteren gängigen Definitionen von BI beinhalten ebenfalls die in Abbildung 1 dargestellten Aspekte. Die vorliegende Arbeit setzt an der analyseorientierten Struktur der Daten an (vgl. Schicht II in Abbildung 1) und lässt sich somit in der Schnittmenge der unterschiedlichen Perspektiven auf BI verorten.

---

17 Vgl. LUHN (1958); LUHN beschreibt hier die funktionellen Anforderungen an ein Dokumentenmanagementsystem zur automatisierten bedarfsgerechten Informationsversorgung und betitelte dieses als „BI-System".

18 DRESNER (2001), S. 26

19 GLUCHOWSKI/KEMPER (2006)

Vor dem Hintergrund, dass die grundlegenden Anforderungen an BI mit denen der „Vorgängerkonzepte“ im Wesentlichen identisch sind, fällt der „Hype“[20], der sich um BI entwickelte und immer noch anhält, ins Auge. Dafür lassen sich Gründe anführen, die den folgenden drei Kategorien zugeordnet werden können und sich in ihrer Wirkung gegenseitig verstärken.

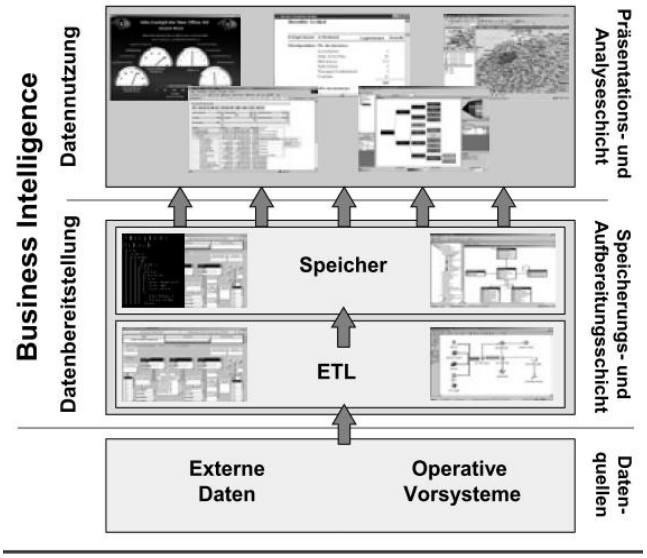


Abbildung 2: Business-Intelligence-Schichtenarchitektur
Vgl. GLUCHOWSKI/KEMPER (2006), S. 6

(1) Vermarktung des Begriffs BI in der Geschäftswelt
(2) Gestiegenes Bewusstsein für und Bedarf an Datenanalyse bei gewachsener Datenbasis
(3) Technische Weiterentwicklungen

zu (1). Unter die erste Kategorie fällt insbesondere die Neubenennung im Grunde bekannter Konzepte. Das Akronym MIS war und ist aufgrund nicht zufrieden stellender Realisierungen negativ konnotiert. Der Anspruch bei der Entwicklung dieser Systeme ging häufig weit über die oben formulierte Aufgabenstellung hinaus - bis hin zu einer sehr weitgehenden Automatisierung von Managementprozessen.[21] Gerade in Anbetracht dieser ambitionierten Zielsetzung gelten MIS aufgrund ihrer fundamentalen technischen Mängel allgemein als gescheitert[22]. Sie wurden bereits kurz nach ihrem Aufkommen heftig kritisiert, was sich an vielbeachteten Beiträgen wie dem 1972 veröffentlichten „The Myths of MIS“[23] zeigt. Der Begriff BI dagegen war unverbraucht. Den „BI-Hype“ hat wohl auch HOWARD DRESNER selbst - ab 1992 als Analyst bei der Gartner Group - verstärkt, indem er die Bedeutung von BI in Wirtschaft und Wissenschaft mit Nachdruck propagierte.[24] Sicher auch dadurch bedingt wurde „BI“ unspezifisch und inflationär zur werbewirksa-

[20] DRESNER (2002), S. 2–3; DRESNER schreibt hier in einer Zusammenfassung der Ergebnisse einer Marktstudie von Gartner „Lots of ‚Buzz' […] hype abounds in the BI software marketplace“.
[21] Vgl. SWIONTEK (1997), S. 65
[22] Vgl. u.a. GLUCHOWSKI/KEMPER (2006), S. 12
[23] MINTZBERG (1972)
[24] DRESNER gründete bspw. unter anderem die „Business Intelligence Research Community” und die „North American BI conference” [vgl. GARTNER (2005)].

men Benennung bestehender und neuer Produkte durch Beratungshäuser und Softwarehersteller verwendet.[25] Der eben beschriebene Zusammenhang hat einen großen Anteil an der Verbreitung des Themas BI, wurde jedoch durch zwei substanzielle Entwicklungen unterfüttert, welche die zweite Kategorie darstellen. Erst diese verstärkten die Verbreitung von BI in der Praxis sowie die wissenschaftliche Aufmerksamkeit für dieses Gebiet nachhaltig.

zu (2). Eine der beiden Entwicklungen manifestiert sich im insgesamt gestiegenen Bewusstsein für die Bedeutung von Information. Schlagworte wie „Informations-" und „Wissensgesellschaft" haben inzwischen unübersehbar Einzug in die Alltagssprache gehalten. Seit Mitte der 1990er Jahre wird bei der Begründung wirtschafts- und bildungspolitischer Maßnahmen auffallend oft auf „die Wissensgesellschaft" verwiesen.[26] Gleichzeitig kam in der deutschsprachigen wirtschaftswissenschaftlichen Literatur die Diskussion auf, ob die klassischen Gutenberg'schen Produktionsfaktoren um die „Ressource Information" zu ergänzen seien, wobei dabei meist auf die gestiegene Bedeutung der Information im Produktionsprozess verwiesen wurde.[27] Im betriebswirtschaftlichen Umfeld kann wohl auch das ungefähr zeitgleich aufblühende Interesse an Wissensmanagement-Systemen (gelegentlich ebenfalls als „Hype"[28] wahrgenommen) als Zeichen einer zunehmenden Sensibilisierung für eine effiziente Informationsversorgung von Managern im Sinne einer „wesentliche[n] Voraussetzung für Entscheidungen"[29] interpretiert werden.

Im Hinblick auf die Informationsgewinnung durch BI-Anwendungen haben die Ausweitung des E-Business, der Globalisierung und der IT-Unterstützung betriebswirtschaftlicher Prozesse parallel die verfügbare Datenbasis vergrößert. Gleichzeitig stieg die Komplexität unternehmerischer Entscheidungssituationen - genauso wie Anforderungen an die Transparenz und Fundierung betrieblicher Entscheidungsfindung[30]. Folglich wuchsen auch der Bedarf für und der Anspruch an die Funktionalität der inzwischen unter „BI"

---

25 MERTENS (2002), S. 2

26 Vgl. HEIDENREICH (2003), S. 25 für diesen und den vorangegangenen Satz

27 Vgl. STÜDEMANN (1993), S. 258; für eine Kategorisierung von Information als Produktionsfaktor wird bspw. bei HILDEBRAND (1995, S. 11) und PICOT (1989, S. 3), gegen eine solche bspw. bei BUSSE VON COLBE/LAßMANN (1990, S. 81) und EICHHORN (1996, S. 38), für eine kontextabhängige Kategorisierung bspw. bei BODE/ZELEWSKI (1992, S. 601) und KRCMAR (1996, S. 720) argumentiert.

28 PFEIFER ET AL. (2007), S. 287; vgl. auch PRUSAK (2001), S. 1002

29 LEHNER (2008), S. 6; vgl. S. 5 – 14 für einen Überblick über Gründe für und Reaktion auf die wachsenden Bedeutung von Information im Kontext des Wissensmanagements

30 Als Beispiele seien die Verpflichtung zum Risikomanagement für Banken gemäß BASEL II und Vorschriften für ein „Überwachungssystem" gemäß KonTraG angeführt.

firmierenden Konzepte. Nicht zuletzt führte dies zu einer Neuausrichtung bisheriger Lösungen – insbesondere hin zu einer stärkeren Anwenderorientierung.[31] Im Hinblick auf die Bedienbarkeit der Anwendungen („Usability") haben sich (mit dem breiteren Bedarf an Datenanalyse unter dem Begriff BI) daher auch zumindest in der praktischen Umsetzung der BI-Systeme bzw. BI-Frontends Entwicklungen vollzogen, die ggf. eine evolutorische Abgrenzung zu den Vorläufersystemen anhand des höheren Grads der Usability ermöglichen.

zu (3). Die dritte Kategorie fasst die technischen Gründe, die den „BI-Hype" stützen, zusammen. Der gestiegene Bedarf nach entsprechenden Lösungen und die stark gewachsene Datengrundlage trafen auf ein verbessertes technisches Vermögen. Gemeinsam mit dem stetigen Fortschritt in der Hardwaretechnik sind hier vor allem die Entwicklungen bzgl. der Integration und Analyse von großen Datenbeständen zu nennen, die seit Mitte der 1980er Jahre zu verzeichnen waren. Der Beitrag „An architecture for a business and information system"[32] (1988) von DEVLIN UND MURPHY gilt in diesem Zusammenhang als konzeptionell richtungweisend. INMON prägte dann 1990 für die dort vorgestellte IT-Anwendungskategorie den inzwischen gebräuchlichen Begriff „Data Warehouse" (DW).[33] Darunter versteht man „eine physische Datenbank, die eine integrierte Sicht auf beliebige Daten zu Analysezwecken ermöglicht"[34]. Grundsätzlich werden dazu Daten aus operativen Quellsystemen in ein DW repliziert, um dann integriert und in analysegerecht aufbereiteter Struktur dauerhaft mit einem Zeitbezug vorgehalten zu werden. Analog zur Nomenklatur bei Datenbanken(-Systemen)[35] wird auch hier der Begriff „Data Warehouse-System" (DWS) verwendet, um die Erweiterung um Komponenten des DW-Betriebs, also insbesondere solche zur Datenbeschaffung und -integration,[36] zu kennzeichnen. In Bezug auf das dargestellte Anforderungsschema setzen DWS also im Wesentlichen an der ersten Stufe (vgl. Abbildung 1) an.

Zur Verbreitung von BI hat noch eine andere Entwicklung beigetragen, die eine Innovation im Sinne der zweiten Stufe in Abbildung 1 darstellt: OLAP. Fast jede moderne BI-

---

31 Vgl. KEMPER/BAARS (2006), S. 8f. sowie GLUCHOWSKI/KEMPER (2006), S. 12 für diesen und die beiden vorangegangen Sätze

32 DEVLIN/MURPHY (1988)

33 Vgl. HUMMELTENBERG (2008), S. 11 und S.16 für diesen und die vorangegangenen beiden Sätze; der Begriff „Data Warehouse" wurde durch INMON in seiner Monographie „Building the Data Warehouse" [vgl. INMON (1990)] geprägt.

34 BAUER/GÜNZEL (2009b), S. 8

35 Vgl. bspw. KLEINSCHMIDT/RANK (2002)

36 BAUER/GÜNZEL (2009b), S. 8

Anwendung basiert auf diesem Konzept, für das CODD 1993 den Begriff „On-Line Analytical Processing“[37] prägte.[38] Mit OLAP bezeichnet man inzwischen - etwas vereinfacht ausgedrückt - eine Kategorie von Anwendungen, die eine benutzerfreundlich definierte ad-hoc Analyse von potentiell großen Datenbeständen zum Ziel haben. Wesentliches Gestaltungsparadigma von OLAP ist die multidimensionale Anordnung der Daten.[39]

> „Unter Multidimensionalität [in OLAP] ist hierbei eine bestimmte Form der logischen Anordnung quantitativer, betriebswirtschaftlicher Größen zu verstehen, die betriebswirtschaftlich relevantes Zahlenmaterial simultan entlang unterschiedlicher Klassen logisch zusammengehöriger Informationsobjekte aufgliedert und dadurch mit der naturgemäß mehrdimensionalen Problemsicht der Unternehmungsanalytiker weitgehend korrespondiert.“[40]

„Betriebswirtschaftlich relevantes Zahlenmaterial“ meint im Allgemeinen Kennzahlen wie etwa die Anzahl verkaufter Produkte. „Unterschiedliche Klassen von Informationsobjekten“ sind die sogenannten Dimensionen im Sinne von unterschiedlichen Sichtweisen auf diese Kennzahlen - also bspw. das verkaufte Produkt, der geographische Ort des Verkaufs (bspw. das Bundesland) sowie der Zeitraum, in dem der Verkauf stattgefunden hat (bspw. das Quartal). So würde in umseitiger Abbildung 3 die Kombination aus {Produkt = „P1“, Geographie = „HES“, Zeit = „Q1“} die Anzahl = „1“ liefern. Für jede Kombination der Ausprägungen der Dimensionen hält der multidimensional strukturierte Datenbestand (potentiell) eine Ausprägung der Kennzahl vor. Der hier nach drei Dimensionen beispielhaft strukturierte Datenbestand aus Kennzahlen nimmt so die Form eines „Würfels“ an. Von einem „Datenwürfel“ spricht man auch bei mehr als drei Dimensionen und auch angesichts der Tatsache, dass nicht alle Dimensionen gleich viele Ausprägungen umfassen müssen.

---

37 Vgl. CODD/CODD/SALLEY (1993)

38 Inzwischen wird OLAP häufig auf Basis der 1995 aufgestellten FASMI-Regeln definiert [vgl. PENDSE/CREETH (1995)].

39 „The key thing that all OLAP products have in common is multidimensionality.“ [PENDSE/CREETH (1995)]; vgl. dazu auch CODD/CODD/SALLEY (1993) sowie bspw. CHAMONI/GLUCHOWSKI/HAHNE (2005), S. 21

40 GLUCHOWSKI/GABRIEL/CHAMONI (2008), S. 144f.

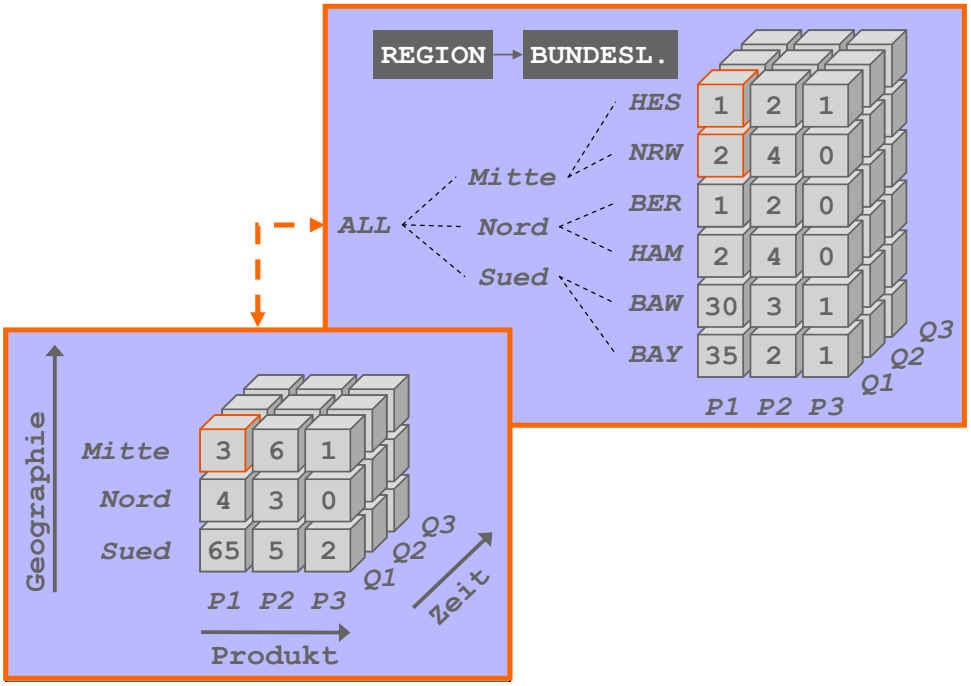


Abbildung 3: Einfacher Datenwürfel in granularer und aggregierter Perspektive
Eigene Darstellung

Als weiteres kennzeichnendes Merkmal der Multidimensionalität in OLAP stehen die Elemente einer Dimension meist in hierarchischer Ordnung zueinander, so dass Kennzahlen von unterschiedlichen Ebenen der Dimensionshierarchie aus betrachtet werden können.[41] In Abbildung 3 weist die Dimension „Geographie" eine Hierarchie von Regionen zugeordneten Bundesländern auf. Eine präzisere Darstellung der für diese Arbeit wichtigen Aspekte von OLAP erfolgt in Kapitel 2.

OLAP gilt als zentrales Element von Business Intelligence[42] und ist eines der am weitesten verbreiteten Werkzeuge zur Entscheidungsunterstützung[43].

41 Vgl. CODD/CODD/SALLEY (1993); PENDSE/CREETH (1995)

42 Vgl. GLUCHOWSKI (2001), S. 7, und Abbildung 4; hier wird OLAP gemeinsam mit MSS als „enges Verständnis" von BI aufgefasst.

43 Vgl. bspw. WANG/JAJODIA/WIJESEKERA (2004), S. 161

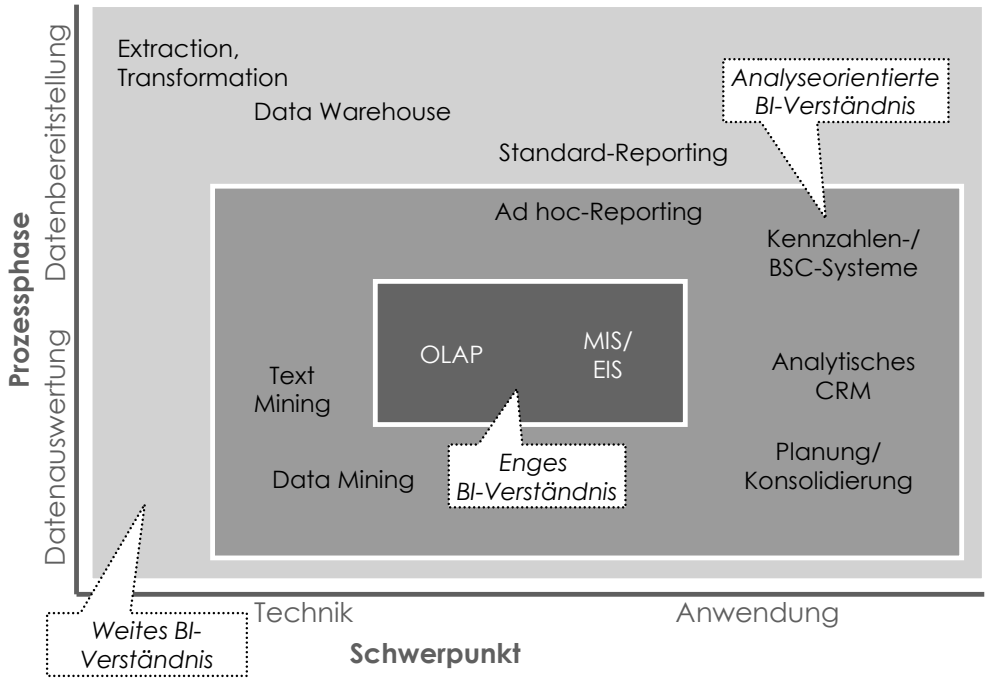


Abbildung 4: OLAP im Rahmen von BI
In Anlehnung an GLUCHOWSKI (2001), S. 7

Der BI-Gedanke setzt voraus, dass zunächst alle relevanten Daten zu einem Analysegegenstand integriert zur Verfügung gestellt werden - letztendlich meist in einem OLAP-Würfel. Gängige Praxis war und ist es noch häufig, einen OLAP-Würfel allen Nutzern ohne Einschränkung zur Verfügung zu stellen. Böswillige Anwender können so problemlos auch sensible Informationen in Erfahrung bringen. So enthält der Würfel aus Abbildung 3 für einen Mitarbeiter im Außendienst, dessen erfolgsabhängiger Gehaltsbestandteil wahrscheinlich im Wesentlichen von den Verkaufszahlen abhängt, wertvolle Informationen zur Steuerung der Maßnahmen im Sinne des Unternehmens in seinem Bereich. Allerdings ist er auch leicht in der Lage, aus den Verkaufszahlen seines Kollegen dessen variablen Gehaltsbestandteil abzuleiten, was kaum im Sinne des Unternehmens sein kann.

Vergleichbar mit der Situation in sozialen Netzen wie etwa Facebook, in denen ebenfalls zunächst die Möglichkeiten der leichten und individuell nutzbringenden Verbreitung von persönlichen Informationen sehr unbedacht verwendet wurden und datenschutzrechtliche Aspekte erst mit Verspätung stärker in den Vordergrund rückten, vollzieht sich auch im Umgang mit OLAP ein Wandel, den diese Arbeit unterstützen soll.

1.2 Motivation und Zielsetzung der Arbeit

Dem Autor ist aufgrund der Zusammenarbeit des Lehrstuhls für Wirtschaftsinformatik I (Prof. Dr. Peter Kleinschmidt, Universität Passau) mit zahlreichen Unternehmen bekannt, dass ein großer (Nachhol-)Bedarf bzgl. Disclosure Limitation im OLAP-Bereich herrscht. Falls überhaupt vorhanden, sind die eingesetzten Sicherheitsmechanismen rudimentär. Das Problem wird als äußerst heikel betrachtet, jedoch aus offensichtlichen Gründen möglichst nicht gegenüber Dritten thematisiert.[44] Die vorliegende Arbeit soll einen Beitrag leisten, Disclosure Limitation in OLAP der praktischen Anwendbarkeit näher zu bringen. Im Folgenden wird der Frage nachgegangen, warum sich die Ist-Situation wie beschrieben darstellt, da sich hieraus die im Anschluss beschriebenen Ziele der vorliegenden Arbeit ableiten.

Auf Aspekte der Datensicherheit bei OLAP wurde in der wissenschaftlichen Diskussion bereits früh hingewiesen. KIMBALL, der mit INMON zu den frühen Protagonisten der DWS-Idee gehört, formulierte bspw. in seinem Beitrag „Hackers, crackers, and spooks: ensuring that your data warehouse is secure" folgenden Gedanken.

> "A data warehouse, by its very nature, creates a security conflict. On the one hand, the goal of every data warehouse is to make valuable data accessible. […] On the other hand the world seems seems[*sic*] to be filled with hackers, crackers, and industrial spooks of various kinds […][45]

KIMBALL fokussiert in diesem Beitrag Sicherheitsprobleme über die ganze funktionelle Bandbreite eines OLAP-einschließenden DWS. Weniger explizit geht er auf die Gefahr der Offenlegung sensibler Daten im Rahmen der dedizierten Nutzer von OLAP-Anwendungen ein, erwähnt aber sehr wohl „curious employees who can't resist the temptation to explore" [46]. Somit umreißt KIMBALL bereits 1997 mit diesen beiden Bemerkungen das Feld, in dem diese Arbeit angesiedelt ist. Dass Disclosure Limitation in OLAP dennoch in Wissenschaft und Praxis wenig etabliert ist, rührt von einer Vielzahl von Gründen, die sich trotz Wirkungszusammenhängen grob in drei Kategorien gliedern lassen.

(1) Der immanente Konflikt zwischen Hauptfunktion von OLAP und Datensicherheit

---

44 Aus diesem Grund war eine belastbare Studie zur Analyse der Ist-Situation nicht möglich. Die weiteren Ausführungen im Rahmen dieses Abschnitts werden jedoch deutlich machen, dass ein Nachholbedarf auf diesem Gebiet unstrittig ist.

45 KIMBALL (1997), S. 14

46 ebenda

(2) Die Fokussierung auf die Verbesserung der Kernfunktionalität von OLAP

(3) Die Änderung des Anwenderkreises von OLAP

zu (1). Der erste Punkt deckt sich mit dem eingangs angeführten Zitat von Kimball, das noch stärker als auf DWS konkret auf OLAP zutrifft. OLAP soll Nutzern die Analyse großer Datenbestände ermöglichen. „Sicherheit durch Verstecken von Daten" steht daher ganz grundsätzlich im Konflikt zum eigentlichen Verwendungszweck. Darüber hinaus unterscheidet sich OLAP in der Art der Nutzung von anderen Informationssystemen. OLAP dient der explorativen Datenanalyse.[47] „Der Analysepfad […] ist vorab kaum vordefinierbar. Er entwickelt sich ad hoc während der Analyse aufgrund von spezifischen Datenkonstellationen."[48] In Anbetracht der Vielzahl verschiedener sinnvoller Möglichkeiten zur Exploration und Analyse der Daten und des entsprechend schwierig zu antizipierenden Analyseverlaufs stellt sich bei der Implementierung eines Sicherheitsmechanismus die Frage, welche Daten(bereiche) welchem Nutzer vorenthalten werden sollen, ohne eine sinnvolle „Exploration" zunichte zu machen. Vor allem dieses Charakteristikum der Verwendung von OLAP verhindert, dass Erkenntnisse aus verwandten Problemstellungen übertragen werden können. So wurde bspw. früh auf die Parallelen zwischen OLAP und Statistischen Datenbanken (SDB) hingewiesen.[49] Auch SDB stellen die Daten in einem multidimensionalen Raum dar. Allerdings unterscheiden sich die Art der Verwendung und der Nutzerkreis deutlich. Dies betrifft vor allem die Tatsache, dass statistische Produkte im Allgemeinen für alle Kunden nach denselben Anforderungen geschützt werden. So darf bspw. keiner der Kunden genaue Rückschlüsse auf private Daten einer eindeutig identifizierten natürlichen Person erlangen. Bei OLAP-Anwendungen hingegen kann die A-Priori-Eingrenzung der Explorationsmöglichkeiten zu einem schwerwiegenden Verlust an Informationsqualität bzw. dem Nutzen, den ein Unternehmen aus OLAP ziehen kann, führen.

zu (2). Am eigentlichen Zweck von OLAP orientierte sich - vor allem in den Anfangsjahren dieses Konzepts - auch der Fokus der Entwicklungsbemühungen in Wissenschaft und Praxis. Zur Gewährleistung einer effektiven Analysetätigkeit wurden vor allem an der Verbesserung der Performanz der OLAP-Anwendungen (Indizierung, Speichertechnologie etc.), aber auch an anderen diesem Ziel zuträglichen Eigenschaften wie bspw. der Vi-

47 Vgl. PRIEBE/PERNUL (2000), S. 33

48 OEHLER (2010), S. 349

49 Vgl. SHOSHANI (1997)

sualisierung der Daten gearbeitet. Da dem Analysezweck von OLAP nicht direkt zuträglich, blieb Disclosure Limitation in OLAP zumindest in der unternehmerischen Praxis weitestgehend unbeachtet. In der wissenschaftlichen Literatur existieren nicht viele Beiträge zu diesem Thema. Bei den vorliegenden Arbeiten handelt es sich jedoch zum Großteil um Veröffentlichungen, die rein (informations-)theoretischer Natur sind und sich „thematisch allein stehend" speziellen Aspekten des Disclosure Problems widmen, ohne die praktische Umsetzbarkeit zu berücksichtigen. Einige wenige Arbeiten haben hohe praktische Relevanz; dort formulierte Anforderungen wurden teils bereits als Funktionen in OLAP-Standardsoftware umgesetzt. Allerdings handelt es sich hierbei immer um relativ offensichtliche Aspekte, also bspw. der Forderung danach, einem Benutzer die Daten aus bestimmten Ästen des Hierarchiebaums vorenthalten zu können. Überlegungen zu einem mit vertretbarem Aufwand administrierbaren Sicherheitskonzept fehlen bis jetzt.

zu (3). Für die „Forschungs- und Implementierungslücke" bzgl. Disclosure Limitation in OLAP findet sich noch ein weiterer Grund in der Entwicklungsgeschichte des OLAP-Konzepts. Wie im vorangegangenen Abschnitt 1.1 erläutert, steht OLAP in einer Entwicklungslinie mit analytischen Informationssystemen, die sich im Wesentlichen an „Fach- und Führungskräfte" richteten. Auch für BI galt diese Nutzergruppe lange als ausschließliche Zielgruppe.[50] Geht man davon aus, dass dieser Personenkreis im Sinne des Unternehmens besonders vertrauenswürdig ist und insbesondere Mitglieder des gehobenen Managements ein berechtigtes Interesse an beinahe allen Daten des Unternehmens haben, scheinen Sicherheitsfragen tatsächlich vernachlässigbar. Allerdings lässt sich seit einigen Jahren der Trend beobachten, OLAP-Anwendungen zunehmend hierarchiestufenübergreifend in eine Vielzahl von Geschäftsprozessen einzubinden. Diese Entwicklung firmiert unter dem Titel „BI for the masses"[51] und wird von Softwareanbietern durch entsprechende Werkzeuge bspw. im Rahmen des Microsoft Project Gemini aufgegriffen.[52]

PRIEBE formuliert die Situation daher 2009 in sehr kritischem Ton wie folgt.

> "Traditionell erfolgt ein Zugriff [durch OLAP-Werkzeuge] auf ein Data Warehouse[53] ausschließlich von Anwendern des Managements oder Business-

[50] Vgl. GLUCHOWSKI/GABRIEL/CHAMONI (2008), S. 4f., TOTOK (2000), S. 49

[51] Vgl. GENTSCH (2008), S. 2 für diesen Teilsatz und den vorangegangenen Satz

[52] Vgl. HEWLETT-PACKARD (2009), S. 5

[53] PRIEBE spricht hier von „Zugriff auf ein Data Warehouse". Neben der Überschrift des etnspr. Abschnitts „Anwenderzugriff im Analysebereich" machen auch PRIEBES weiteren Ausführungen an dieser Stelle deutlich, dass er sich auf Anwendungen zur Datenanalyse - insbesondere OLAP - und damit nur mittelbar auf ein Data Warehouse bezieht.

> Analysten, was von Herstellern als Vorwand genutzt wurde, keine feingranularen Zugriffskontrollmechanismen zu implementieren. Diese Annahme trifft inzwischen allerdings nicht mehr zu. Der mögliche Kreis von Anwendern für Analysewerkzeuge mit Zugriff auf ein Data Warehouse wächst immer mehr bis hin zu Kunden und Partnern."[54]

Die Beobachtung, dass zunehmend auch Dritte, wie etwa Beratungsunternehmen ohne Betrachtung von Disclosure-Aspekten mit Daten aus OLAP-Systemen versorgt werden, wird von vielen geteilt[55] und erhöht den potentiellen Schaden aus Disclosure (im Vergleich zu Disclosure gegenüber Unternehmensangehörigen) in vielen Fällen erheblich. Die hier geäußerte Kritik an Softwareherstellern von OLAP-Produkten scheint allerdings etwas überspitzt. Die Möglichkeiten von OLAP-Software zur Implementierung von Disclosure Limitation-Mechanismen sind sicher noch nicht voll ausgereift, jedoch haben die Softwarehersteller hier erhebliche Verbesserungen eingeführt. SAP erweiterte bspw. mit der neuen Hauptversion der integrierten DWS- und OLAP-Softwarelösung SAP Netweaver BI 7.0 die Standardfunktionalität zur Implementierung eines Sicherheitskonzepts entscheidend. Dass diese softwareseitigen Möglichkeiten in der Praxis nicht ausreichend genutzt werden, liegt vor allem daran, dass noch keine praktikablen Konzepte und Algorithmen vorliegen, um mit diesen Einstellungsmöglichkeiten ein praktikables Disclosure Limitation System aufzubauen. Allerdings lässt sich die auf dedizierte OLAP-Anwendungen gemünzte Kritik auch auf die Systeme übertragen, in die OLAP im Zuge des oben beschriebenen Trends „BI for the masses" integriert wurde. So bietet das auf dem „Software-as-a-Service"-Gedanken beruhende mittelstandsorientierte ERP-System der SAP AG (SAP Business byDesign) zwar OLAP-Funktionalität, jedoch noch kein spezielles Sicherheitskonzept für diese Anwendungen (vgl. Abbildung 5).

---

54 PRIEBE (2009), S. 166

55 Vgl. bspw. WANG/JAJODIA/WIJESEKERA (2007), S. 2

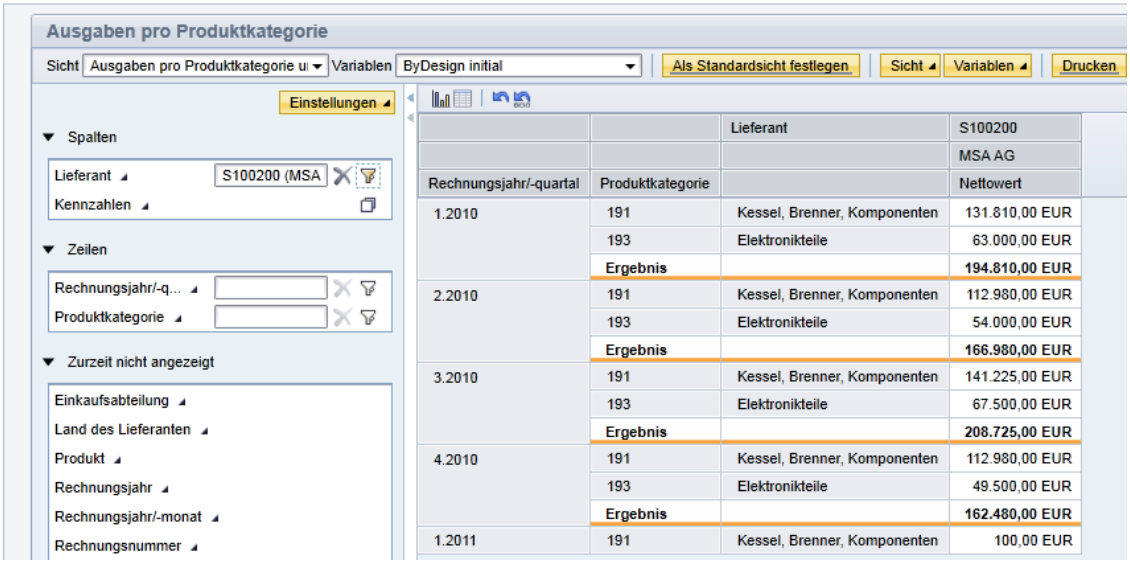


Abbildung 5: OLAP-Anwendung in SAP Business byDesign
Screenshot aus einer SAP Business byDesign-Instanz

Die Entwicklung eines Sicherheitssystems für OLAP, das den eben diskutierten Anforderungen genügt, ist folglich eine komplexe Aufgabe. Eine praktikable Lösung muss zusätzlich noch den Restriktionen genügen, welche durch die begrenzte Verfügbarkeit der (menschlichen) Ressourcen für die Administration des Sicherheitssystems entstehen.

Auf Basis der beschriebenen Situation ist das Globalziel der vorliegenden Arbeit, „Disclosure Limitation in OLAP“ der praktischen Umsetzung näher zu bringen. Es sollen daher insbesondere diejenigen Lücken in der bisherigen Forschungsarbeit geschlossen werden, die einem praktischen Einsatz noch im Wege stehen. Das Globalziel wird durch nachstehende vier aufeinander aufbauende Subziele erreicht. Die hier folgende abstrakte Beschreibung dieser Ziele wird in Abschnitt 1.3 konkretisiert.

Die für Disclosure Limitation in OLAP kritischen Faktoren - insbesondere im Hinblick auf den praktischen Einsatz - werden herausgearbeitet, da eine umfassende Analyse bisher nicht vorliegt. Es werden erstmalig in strukturierter Form Qualitätskriterien für OLAP auf diesem Gebiet abgebildet, so dass bisherige und zukünftige Ansätze zur Disclosure Limitation anhand dieser Kriterien analysiert und weiterentwickelt werden können. Diese Darstellung dient gleichzeitig als Unterstützung bei der zielorientierten Analyse von Verfahren der Disclosure Limitation in OLAP für den Einsatz in einem spezifischen Kontext.[56] Bestehende Lösungsansätze für Teilprobleme bei der „Disclosure Limitation in OLAP“ so-

[56] Neben der abstrakten Analyse des Erfüllungsgrades einzelner Verfahren hinsichtlich einer Menge von Zielkategorien ist ein Mapping auf das Zielsystem eines konkreten Unternehmens möglich.

wie relevante Arbeiten in angrenzenden Forschungsgebieten werden analysiert und hinsichtlich der herausgearbeiteten Faktoren kategorisiert. Basierend auf diesen drei Schritten wird ein Vorgehensmodell aufgebaut, das Schwachpunkte in der bisherigen Forschung bzgl. der Umsetzbarkeit von Disclosure Limitation adressiert und Lösungen dafür anbietet. Die praktische Anwendbarkeit dieses Vorgehensmodells wird durch eine beispielhafte Implementierung im SAP BI7.0 demonstriert.

1.3 Aufbau der Arbeit

Kapitel 2 führt in die für diese Arbeit grundlegenden Begriffe im Umfeld von DW und OLAP ein. Die Entstehung sowie grundlegende Eigenschaften von DW, OLAP und BI werden kurz beschrieben. Anschließend werden in Kapitel 3 Kriterien zur Evaluation der Qualität von OLAP aus den Anforderungen von Nutzern und Unternehmen abgeleitet. OLAP-Anwendungen befinden sich in einem Spannungsfeld zwischen dem Nutzen, der dem Unternehmen durch explorative Datenanalysen entsteht, der Sicherheit, welche sie bezüglich des unautorisierten Zugriffs auf geschäftsrelevante Daten bieten, und den Kosten, welche durch den Einsatz und die Administration entstehen. Die Trade-Offs zwischen diesen gegensätzlichen Anforderungen bilden die Grundlage zur Beurteilung der Lösungsansätze zu Disclosure Limitation hinsichtlich ihrer praktischen Einsetzbarkeit. Ein Evaluationsmodell wird theoretisch hergeleitet, welches in zwei (kompatiblen) Adaptionen die Bewertung von OLAP einerseits und von Disclosure Limitation-Verfahren in OLAP andererseits im Hinblick auf den Nutzen, welcher einem Unternehmen durch den Einsatz von OLAP bzw. von Schutzmechanismen entsteht, ermöglicht.

Kapitel 4 führt in das Themengebiet Disclosure Limitation ein, stellt die Ent- bzw. Weiterentwicklung von Ansätzen zur Zugriffs- und Inferenzkontrolle vor und diskutiert die jeweiligen Vor- und Nachteile der einzelnen Ansätze, die Raum für weitere Forschungsarbeit boten oder bieten. Da alle Ansätze (historisch bedingt) für völlig andere Technologien entwickelt wurden, ist ihre Anwendbarkeit für OLAP zu prüfen. Dies geschieht nicht nur im Hinblick auf die technische Machbarkeit der Implementierung, sondern auch unter Verwendung der in Kapitel 3 herausgearbeiteten Evaluationskriterien.

In Kapitel 5 werden Konzepte zur Zugriffs- und Inferenzkontrolle diskutiert, die speziell für den Einsatz in OLAP entwickelt wurden. Sie beruhen zum Teil auf „alten“ Konzepten, welche bereits in Kapitel 4 eingeführt wurden. Das Kapitel schließt mit einer Beurteilung der existierenden Lösungsansätze bezüglich der in Kapitel 3 erarbeiteten Kriterien

zur praktischen Anwendbarkeit und identifiziert Ansatzpunkte für Verbesserungen.

Auf Basis dieser Erkenntnisse wird in Kapitel 6 ein neuer Ansatz zur Lösung der identifizierten Probleme entwickelt. Er richtet sich an den in Kapitel 4 und 5 identifizierten Lücken und Schwachpunkten der bisher vorgeschlagenen Ansätze sowie den in Kapitel 3 hergeleiteten Unternehmensanforderungen aus. Hierbei steht die Forderung nach beherrschbarem administrativem Aufwand und Verständlichkeit des Ansatzes im Fokus: Hierdurch soll eine grundsätzliche Akzeptanz erreicht werden, welche eine praktische Anwendung überhaupt erst möglich und lohnend im Hinblick auf die identifizierten Trade-Offs macht. Der Ansatz wird beispielhaft in eine SAP Netweaver BI 7.0-Umgebung implementiert, um seine praktische Anwendbarkeit zu unterstreichen.

Kapitel 7 schließt mit einer zusammenfassenden Betrachtung des hier vorgestellten Ansatzes sowie des Evaluationsinstrumentes. Es werden Kernpunkte identifiziert, die im Hinblick auf die Weiterentwicklung des Ansatzes und die empirische Überprüfung des Evaluationsinstrumentes besonders wichtig sind und für weiterführende Forschungsarbeiten besonders viel versprechend scheinen.

2 GRUNDLEGENDE ASPEKTE DES ON-LINE ANALYTICAL PROCESSING

In diesem Kapitel werden der Begriff OLAP kurz eingeordnet sowie die für den weiteren Verlauf dieser Arbeit relevanten Aspekte präzisiert.[57] Für ein Berechtigungskonzept ist insbesondere das OLAP zugrunde liegende multidimensionale Datenmodell von Belang. Dieses unterteilt den Datenbestand in Ausschnitte („sicherheitsrelevante Objekte"), die für die Vergabe von Berechtigungen entscheidend sind. Zum Abschluss dieses Kapitels wird OLAP kurz in den Kontext von DWS und BI eingeordnet.

Dieses Kapitel beschränkt sich auf die für diese Arbeit relevanten Aspekte von OLAP. Für eine thematisch breit angelegte phänomenologische Betrachtung sei bspw. auf GLUCHOWSKI/GABRIEL/CHAMONI (2008), S. 143–190, für eine umfängliche Beschreibung technischer Fragestellungen bspw. auf THOMSEN (2002) verwiesen. Einen umfassenden Überblick von OLAP aus Perspektive von DWS findet sich u.a. in BAUER/GÜNZEL (2009a).

2.1 Begriffliche Einordnung

Der „Vater relationaler Datenbanksysteme", EDGAR F. CODD, schuf 1993 den Begriff OLAP. Er titulierte damit in Abgrenzung zu OLTP (On-Line Transactional Processing) ein Konzept zur intuitiven Datenanalyse. CODD beschrieb OLAP durch zwölf Anforderungen, die er später durch weitere ergänzte.[58] Das Konzept OLTP beschreibt den Vorgang der Abbildung des Verlaufs von Geschäftsprozessen mit betrieblichen Informationssysteme durch häufige, oft auch schreibende Zugriffe auf zweidimensional strukturierte Datenbestände (im Wesentlichen relationale Datenbanken). OLAP dagegen beschreibt das Konzept der flexiblen Analyse von Geschäftsdaten.[59]

Obwohl das OLAP-Konzept großen Widerhall fand, wurden die von CODD aufgestellten Kriterien im Einzelnen als wenig geeignet zur produktunspezifischen konzeptionellen

[57] Notwendigerweise ergeben sich dadurch vereinzelt Überscheidungen mit dem einleitenden Kapitel. Redundanzen werden zugunsten einer flüssigeren Lesbarkeit unkommentiert gelassen.

[58] THOMSEN (2002)

[59] Vgl. CODD/CODD/SALLEY (1993) für den gesamten Absatz

Beschreibung empfunden.[60] Daraufhin wurden von PENDSE/CREETH (1995) fünf Kriterien zur Beschreibung von OLAP vorgeschlagen, die sie unter dem Akronym „FASMI" (Fast Access of Shared Multidimensional Information) zusammenfassten. Die FASMI-Kriterien gelten inzwischen gemeinhin als geeigneter zur Beschreibung von OLAP im Vergleich zu den Regeln von CODD. Die Bestandteile von FASMI beschreiben PENDSE/CREETH (1995) im Einzelnen wie folgt.

- FAST. Die Antwortzeit auf Anfragen darf 20 Sekunden nicht übersteigen.
- ANALYSIS. Es muss ein ergonomisches und intuitives Analysewerkzeug, das vom Endanwender erweitert werden kann, zur Verfügung stehen.
- SHARED. Der gleichzeitige Zugriff durch mehrere Benutzer sowie die geltenden Zugriffsrechte müssen geregelt werden.
- MULTIDIMENSIONAL. Es muss eine multidimensionale Sicht (vgl. Abschnitt 2.2) auf die Daten möglich sein, unabhängig davon, welche physische Datenbank zu Grunde liegt.
- IINFORMATION. „Information" steht hier für die Performance des OLAP-Systems bei der zu bewältigenden Datenmenge.

Etwas konkreter wird eine Charakterisierung von OLAP in Abgrenzung zu OLTP, wie die folgende Tabelle 1 für Aspekte der Anwendung zeigt.

		Anwendung	
		OLTP	**OLAP**
I	Einsatzgebiet	Operatives Geschäft	Dispositive Aufgaben
II	Nutzerkreis	Sachbearbeiter	Mitarbeiter mit Führungsverantwortung
III	Nutzungsintensität	sehr häufig	gelegentlich
IV	Anzahl der Nutzer	sehr viele	wenige
V	Antwortzeiten	ms - s	s - min
VI	Arbeitsweise	sich wiederholende, definierte Abfragestatements	unplanbarer, spontaner, iterativer Analyseprozess

Tabelle 1: OLAP im Vergleich zu OLTP (Anwendung)
Zusammenfassung aus TOTOK (2000), S. 42; KEMPER/UNGER/MEHANNA (2006), S. 14; SCHINZER/BANGE/MERTENS (1999), S. 47 sowie BAUER/GÜNZEL (2009b), S. 10f.

[60] Vgl. CHAMONI/ZESCHAU (1996), S. 71; man unterstellte CODD, seine OLAP-Kriterien in erster Linie im Sinne des (damaligen) Unternehmens Arbor Software so formuliert zu haben, dass die OLAP-Kriterien der multidimensionalen Datenbank Essbase dieses Unternehmens gerecht wurden [vgl. bspw. PENDSE/CREETH (1995)].

Obwohl auch in aktuellen Veröffentlichungen[61] eine wie in Tabelle 1 dargestellte Charakterisierung vorgeschlagen wird, können die hier aufgeführten Unterschiede zwischen OLTP und OLAP inzwischen nur noch als „tendenziell" bezeichnet werden. Wie bereits in den einleitenden Abschnitten 1.1 und 1.2 belegt, haben sich bei OLAP-Anwendungen Nutzerkreis (II) und -anzahl (IV) denen von OLTP-Anwendungen angenähert („BI for the masses"). Durch eine stärkere Integration der OLAP-Funktionalitäten in operative Anwendungen verändert sich ebenfalls die Nutzungsintensität (III). Die Antwortzeit einer Abfrage auf große Datenbestände (im Rahmen von OLAP) wird tendenziell immer länger sein als die einer zumeist weit weniger Entitäten umfassende Datenbanktransaktion im Rahmen eines ERP-Systems (V). Antwortzeiten werden massiv durch die der OLAP-Anwendung zugrunde liegenden Datenbankanwendung beeinflusst. Aufgrund eines zunehmenden Trends zur Nutzung von sehr perfomanter DB-Technologie wie sog. In-Memory-Ansätzen[62], verringern sich jedoch auch die Antwortzeiten bei OLAP immer weiter (V). Immer noch klar zu unterscheiden ist dagegen die Arbeitsweise mit den unterschiedlichen Systemen (VI). Während die Arbeit mit OLTP-Systemen entlang von Geschäftsprozessen stark strukturiert und damit vorhersehbar erfolgt, dient OLAP einer explorativen Datenanalyse. Die zugrunde liegenden Abfragen sind entsprechend schwer vorhersehbar.[63]

Im Hinblick auf die zugrunde liegende Datenbasis findet man analog Charakterisierungen von OLAP in Abgrenzung zu OLTP (vgl. Tabelle 2).

61 Vgl. bspw. BAUER/GÜNZEL (2009b), S. 10f.

62 Beispiele hierfür sind das DBMS Cognos TM1 von IBM [vgl. bspw. KOLODZIEJ (2011)] oder auch die relativ junge Hama-Technologie der SAP AG.

63 Vgl. u.a. auch PRIEBE/PERNUL (2000), S. 33; OEHLER (2010), S. 349

		Datenbasis	
		OLTP	**OLAP**
I	Operationen	lesen/schreiben/löschen	nur lesender Zugriff
II	Datenquellen	eine	mehrere
III	Granularität	detailliert	aggregiert/abgeleitet
IV	Aktualisierung	durch laufende Geschäftsvorfälle	periodisch
V	Semantisches Modell	zweidimensional	multidimensional
VI	physische Datenbank	relational	relational/multidimensional

Tabelle 2: OLAP im Vergleich zu OLTP (Datenbasis)
Zusammenfassung aus TOTOK (2000), S. 42; KEMPER/UNGER/MEHANNA (2006), S. 14; SCHINZER/BANGE/MERTENS (1999), S. 47 sowie BAUER/GÜNZEL (2009b), S. 10f.

Auch hier kann man feststellen, dass die Unterscheidung weniger trennscharf ausfällt als die Literaturauswertung suggeriert. Auch in OLAP wird in manchen Szenarien schreibender Zugriff auf zu analysierende Datenstrukturen gewährt - so bspw. bei Planungs- und Budgetierungsvorgängen (vgl. Tabelle 2: I).[64] Ein Großteil der OLAP-Anwendungen wird jedoch vor allem im Sinne einer Überwachung bzw. eines Controllings eingesetzt, so dass es hier doch noch überwiegend um lesenden Zugriff geht. Die vorliegende Arbeit beschäftigt sich daher auch ausschließlich mit diesem Aspekt.

2.2 Multidimensionalität

Die Multidimensionalität ist das wesentliche Gestaltungsparadigma von OLAP.[65] Beim multidimensionalen Modell handelt es sich um ein semantisches (konzeptionelles) Datenmodell, mit dessen Hilfe ein Datenbestand in ein nach diesem Modell gestaltetes Schema (Datenwürfel) geordnet werden kann. Die Grundzüge des Modells sind inzwischen ebenso bekannt wie die des relationalen Datenbankmodells. Hier soll daher lediglich knapp im Sinne eines Überblicks und besonders im Hinblick auf die in Kapitel 6 verwendete Nomenklatur eine kurze Beschreibung erfolgen. Bei den Ausführungen in Kapitel 5 werden jeweils dafür geeignete Nomenklaturen verwendet. Auf speziellere Aspekte

[64] Bereits das SAP Business Warehouse 3 sieht spezielle Datenwürfel vor, die schreibenden Zugriff erlauben (sog. transaktionale InfoCubes).

[65] „The key thing that all OLAP products have in common is multidimensionality." [PENDSE/CREETH (1995)]; vgl. dazu auch CODD/CODD/SALLEY (1993) sowie bspw. CHAMONI/GLUCHOWSKI/HAHNE (2005), S. 21

von OALP wird dort im konkreten Zusammenhang eingegangen.

Die folgende Darstellung bezieht auf die im deutschen Sprachraum sehr verbreitete Beschreibung und Nomenklatur des multidimensionalen Modells in ALBRECHT/HARREN/SAPIA (2009). Für eine umfassendere Einführung mit sehr ähnlicher Nomenklatur sei auf DETERMANN (2002) oder auch auf GLUCHOWSKI (2011) verwiesen.

Zentrales Element des multidimensionalen Modells ist der Datenwürfel (vgl. dazu auch die einführenden Schilderungen in Abschnitt 1.1 und dort insbes. Abbildung 3), der Fakten enthält. Diese stellen zu analysierende quantitative Größen dar - meist betriebswirtschaftliche Kennzahlen, so dass der Begriff „Kennzahl" häufig synonym zum Begriff „Fakt" verwendet wird. Einen Überblick über strukturierende Elemente eines Datenwürfels und deren Zusammenhang findet sich in Abbildung 6 als Entity-Relationship-Schema.

Ein multidimensionaler Datenwürfel wird durch die zugehörigen Dimensionen aufgespannt. Die Kanten des Würfels stehen also für die Dimensionen (vgl. Abbildung 6: I).

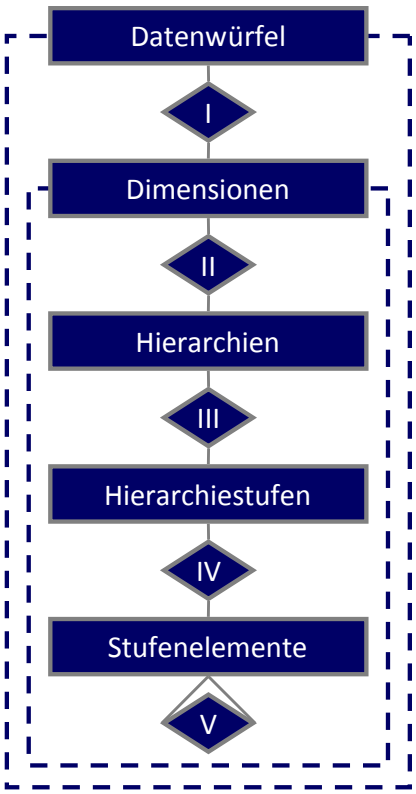


Abbildung 6: Datenwürfelstruktur
Eigene Darstellung

Dimensionen können Hierarchien (auch Klassifikationshierarchien genannt) enthalten (vgl. Abbildung 6). Im Allgemeinen sind dies balancierte Bäume, die in mehrere Hierarchiestufen (auch: Dimensionsstufen) unterteilt (vgl. HS1, HS2 und TOP in Abbildung 7), die Elemente der Dimension in eine Taxonomie bringen.

Meist werden nur die Blätter des Hierarchiebaums (vgl. Knoten 5-14 in Abbildung 7), also Ausprägungen der untersten Hierarchiestufe, als Dimensionselemente bezeichnet, nicht jedoch die Ausprägungen der darüber gelagerten Hierarchiestufen (vgl. Knoten 0-4 in Abbildung 7). In Kapitel 6 dieser Arbeit werden letztere und Dimensionselemente daher als „Hierarchiestufenelemente" oder kurz „Stufenelemente" bezeichnet. Als Hierarchie(-pfad) bezeichnet man exakt eine Ausprägung funktionaler Abhängigkeit zwischen den Hierarchiestufen (vgl. Abbildung 7: HS2 → HS1 → TOP). Es können jedoch mehrere „parallele" Hierarchien bzw. Hierarchiepfade in einer Dimension bestehen (vgl. Abbildung 7 in der Zeit-Dimension: Tag → Kalender-

woche → Jahr → TOP, Tag → Monat → TOP).

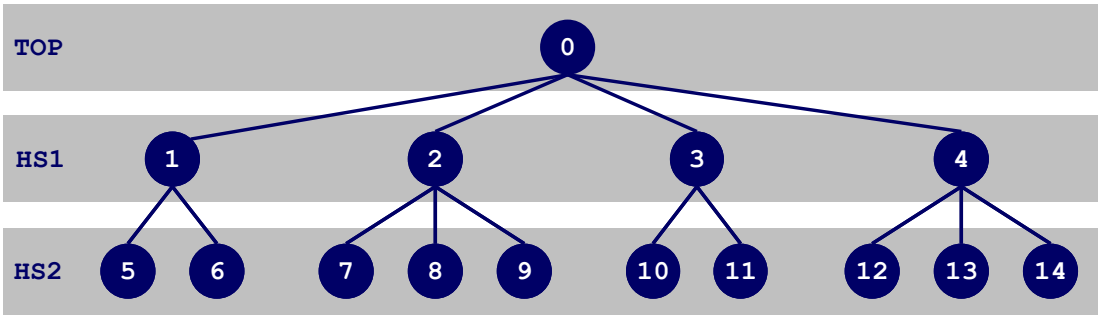


Abbildung 7: Beispielhafte unspezifische Hierarchie
Eigene Darstellung

Weniger geläufig ist der Begriff „Hierarchiestufencontainer". Mit ihm werden in Kapitel 6 entweder die Menge aller Stufenelemente einer Hierarchiestufe (bspw. in Abbildung 7 für HS1 die Element 1-4) oder die Kindknoten eines Stufenelements (bspw. in Abbildung 7 für Element 2 die Dimensionselemente 7-9) bezeichnet.

Die Dimensionsstufen entsprechen den einzelnen Aggregationsstufen der Dimensionen. Zwischen Stufenelementen derselben Stufe können Ordnungen bestehen (vgl. Abbildung 6: V). Tage in der Zeit-Dimension lassen sich bspw. in eine Kardinalskala ordnen.

Jedem Fakt und auch jeder Dimensionsstufe können Attribute zugeordnet werden. Diese entsprechen funktional abhängigen Attributen im Sinne des relationalen Modells und dienen der Beschreibung des jeweiligen Objekts von dem sie abhängig sind.

Neben den Strukturelementen wird das multidimensionale Modell durch Operationen gekennzeichnet, die sich an der Struktur eines Datenwürfels festmachen. „Die Navigation [im OLAP-Würfel] muss in jeder Richtung über alle Dimensionen hinweg möglich sein."[66] Die Navigationsoperationen bedingen Aggregationen oder Disaggregationen entlang der Hierarchiepfade. Die Art der Aggregation sollte bei der Modellierung des Datenwürfels in Abhängigkeit der Hierarchiestufen und der Stufenelemente frei bestimmbar sein. Die am häufigsten verwendete und wenig komplexe Aggregationsfunktion ist die Summenfunktion. Werden dagegen beispielsweise die finanzwirtschaftlichen Kennzahlen des externen Rechnungswesens im Rahmen eines Datenwürfels zur Konzernkonsolidierung verwaltet, muss nach wesentlich komplexeren Regeln - bspw. unter Berücksichtigung der Eliminierung von Binnenumsätzen - aggregiert werden können. (Im Rahmen der Inferenzkontrolle ist die Art der Aggregationsfunktion ein wesentlicher Faktor, wohingegen sie bei der

[66] TOTOK (2000), S. 62

Zugriffskontrolle kaum eine Rolle spielt.) Zugriff zu Bereichen eines Datenwürfels wird anhand der Strukturelemente (Hierarchiestufen) und/oder der Instanzen (Stufenelemente) sowie ihrer Kombinationen über verschiedene Dimensionen gegeben oder entzogen. (vgl. bspw. Abbildung 8. Berechtigte Stufenelemente und Fakten sind orange hinterlegt.)

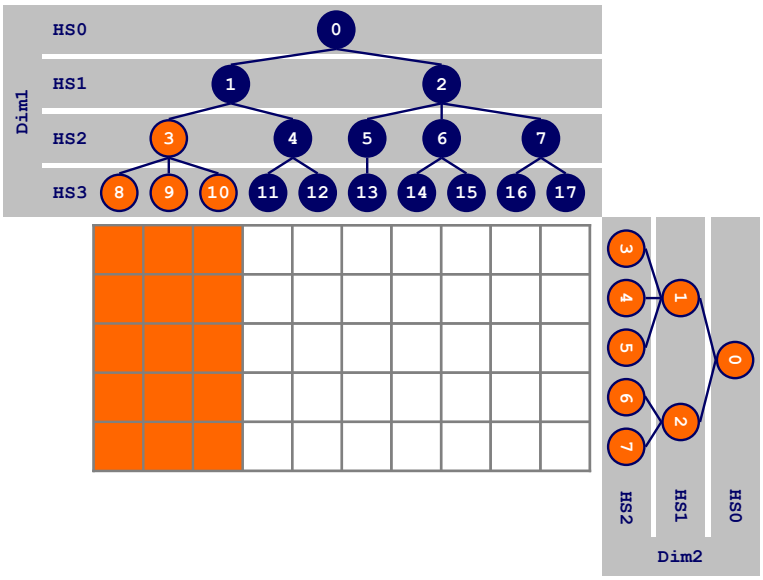


Abbildung 8: Beispielhafte Darstellung von Berechtigungen anhand von Hierarchien
Eigene Darstellung

Die wichtigsten vier Operationen in OLAP sind:

(1) *Slicing*. Slicing bezeichnet die Aggregation einer Dimension über ein Stufenelement, was de facto die Dimensionalität des betrachteten Datenwürfels im Moment der Betrachtung um eins reduziert. (Aus einem dreidimensionalen Würfel wird so eine Tabelle.)

(2) *Dicing*. Dicing bezeichnet die Einschränkung des Betrachtungsraums durch Bildung von echten Teilmengen bei den Stufenelementen mehrerer Dimensionen. Bildlich gesprochen entsteht so ein kleinerer Würfel.

(3) *Drill-Down*. Drill-Down bezeichnet die Ausgabe der Daten in höherer Granularität, indem die Daten auf Basis der Stufenelemente einer niedrigeren Hierarchiestufe betrachtet werden.

(4) *Roll-Up*. Roll-Up ist die komplementäre Operation zu Drill-Down. Die Daten werden aggregiert.

2.3 DWS und OLAP

INMON, der „Vater des DW-Gedankens", definierte DW wie folgt.

> „A data warehouse is a subject-oriented, integrated, nonvolatile, and time-variant collection of data in support of management's decisions."[67]

Dieser Definition entsprechend,

- orientiert sich ein DW an einer bestimmten betriebswirtschaftlichen Fragestellung („subject-oriented"),
- hält ein DW aus heterogenen Quellsystemen semantisch und syntaktisch zusammengeführte Daten vor („integrated"),
- ändert oder überschreibt ein DW die integrierten Daten nicht mehr („nonvolatile") sondern ergänzt lediglich weitere Daten,
- die bei ihrer Speicherung mit einem Zeitraumbezug („time-variant") versehen werden und
- dem Zweck der Entscheidungsunterstützung („Management Support") dienen.

Die Auffassungen über ein DWS gehen in der Literatur auseinander. Sie unterscheiden sich im Wesentlichen in der Frage, ob sich die Struktur der gespeicherten Daten in einem DW bereits hauptsächlich an den Erfordernissen der späteren Analyse durch den Endanwender, also letztendlich einer OLAP-Anwendung, orientiert oder davon unabhängig erfolgt. Letzterer Ansatz bedingt dann zwischen OLAP-Anwendung und DW eine technische Zwischenschicht, die die Daten so aufbereitet, dass OLAP-Abfragen ausreichend schnell beantwortet werden können. Die zweite, verbreitetere Sichtweise geht davon aus, dass die Art der Datenspeicherung eines DW dezidiert auf die Erfordernisse von OLAP ausgerichtet ist.

Im Gegensatz zu DWS, die die Bereitstellung der Datenbasis und - im Datenbanksinne - die logische Modellierung der Datenbestände betonen, nimmt OLAP den Blickwinkel des Anwenders ein (vgl. Stufe III in Abbildung 1). Das Konzept OLAP klammert dabei die technische Umsetzung im Hintergrund aus.[68] Häufig basiert eine OLAP-Anwendung jedoch auf einem DW, und analyseorientierte Datenhaltung im DW meint grundsätzlich eine an den Anforderungen von OLAP orientierte Strukturierung. Auch wenn OLAP nicht notwendigerweise auf einem DWS basiert, wird OLAP als integraler (analyseorientierter) Bestandteil eines DWS betrachtet. Daher wird der Begriff DW(S) gelegentlich

[67] INMON (2005), S. 21

[68] Vgl. PENDSE/CREETH (1995)

auch synonym mit OLAP verwendet, wenn OLAP als „integrales Frontend-Konzept eines DW“ betrachtet wird.[69] Für letztere Sichtweise auf DWS sei beispielhaft auf folgendes Zitat verwiesen.

> „[…] unter einem Data Warehouse [wird] ein unternehmensweites Konzept verstanden, dessen Ziel es ist, eine logisch zentrale, einheitliche und konsistente Datenbasis für die vielfältigen Anwendungen zur Unterstützung der analytischen Aufgaben von Fach- und Führungskräften aufzubauen, die losgelöst von den operativen Datenbanken betrieben wird.“[70]

In jedem Fall impliziert der DWS-Begriff jedoch die notwendige Funktionalität, um Daten für eine Analyse aufzubereiten. Diese wird im sog. ETL-Prozess (Extraction, Transformation, Loading) zusammengefasst. Im Rahmen von Kapitel 6 wird am Beispiel des SAP BI 7.0 auf diesen Prozess und die dementsprechende Referenzarchitektur eines DWS eingegangen, da hier die notwendigen Basisdaten für die beispielhafte Implementierung eines Zugriffskontrollmechanismus angesiedelt werden.

Im Zusammenhang von DWS und OLAP steht insbesondere die Frage nach der OLAP zugrunde liegenden Datenbanktechnologie (vgl. Abbildung 9).

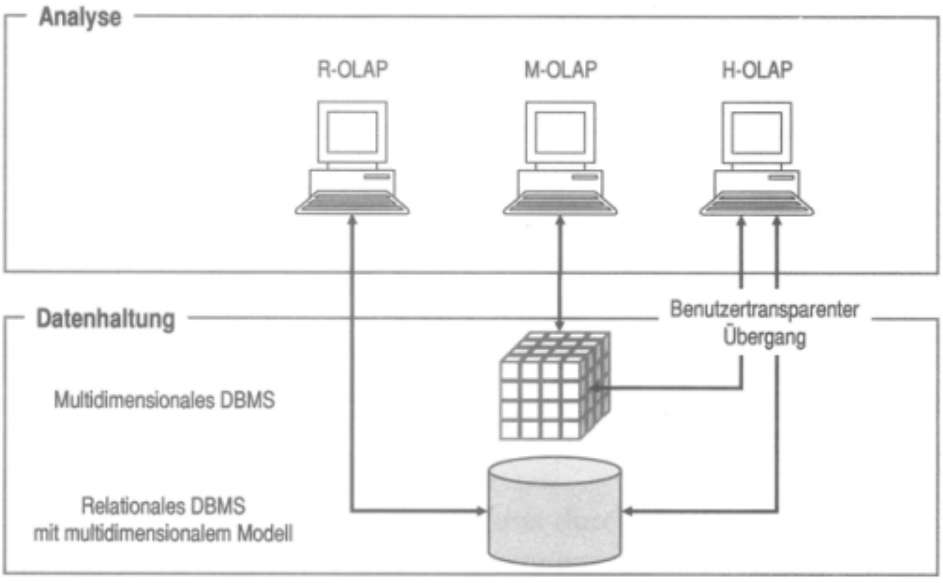


Abbildung 9: Alternative Datenbanken für OLAP
Vgl. (KEMPER/UNGER/MEHANNA (2006), S. 100)

Steht eine OLAP-Anwendung frei von einem DWS, werden aufgrund der Performanzvorteile inzwischen verstärkt multidimensionale Datenbanken verwendet (M-OLAP). Trotz des erwähnten Trends zur multidimensionalen Datenhaltung existieren weiterhin

[69] Vgl. bspw. DETERMANN (2002), S. 71
[70] CHAMONI/GLUCHOWSKI (2006), S. 12

etliche R-OLAP-Lösungen (bspw. das SAP BI 7.0, vgl. Abschnitt 6.3.1). Im Fall von R-OLAP muss jedoch eine sog. „R-OLAP-Engine“ die multidimensionalen Anfragen der OLAP-Anwendungen in relationale übersetzen.[71]

[71] Vgl. GLUCHOWSKI/CHAMONI (2010) für den gesamten Absatz sowie eine ausführliche Darstellung der Architekturkonzepte von OLAP.

3 ERFOLGSDIMENSIONEN VON OLAP

Im Folgenden werden die für den erfolgreichen Einsatz im betrieblichen Umfeld entscheidenden Anforderungen an OLAP erarbeitet. Insbesondere ist von Interesse, inwiefern Sicherheitsmechanismen zur Disclosure Limitation einen negativen Einfluss auf diese erfolgskritischen Faktoren haben.[72] Die Kenntnis dieser Wirkungszusammenhänge erlaubt erstens einen strukturierten Vergleich (vgl. Abschnitt 5.3) konzeptionell grundlegend verschiedener Verfahren hinsichtlich ihrer praktischen Einsetzbarkeit. Zweitens bildet sie die Basis für die zielorientierte Entwicklung praxistauglicher Verfahren zur Disclosure Limitation in OLAP (vgl. Kapitel 6).

Es ist intuitiv nachvollziehbar, dass zwischen dem Ausmaß der Erhöhung der Sicherheit durch die Implementierung eines Schutzmechanismus, den damit verbundenen Kosten und dem aus OLAP-Anwendungen realisierbaren Nutzen Trade-Offs bestehen. Beispielsweise zieht die Erfüllung der Forderung, ein Verfahren solle möglichst flexibel sein, eine Erhöhung der Implementierungskosten nach sich, ermöglicht jedoch auch eine fundierte Datenanalyse. Im Hinblick auf das Ziel dieser Arbeit, ein verwaltungstechnisch möglichst aufwandsarmes Verfahren zur Disclosure Limitation in OLAP zu entwickeln, das eine sinnvolle Balance zwischen Sicherheit und Nutzen bietet, ist ein genaues Verständnis dieser Trade-Offs von zentraler Bedeutung..

3.1 Sicherheit in OLAP-Anwendungen

Überlegungen im Hinblick auf die Entwicklung von Verfahren zur Sicherstellung der Vertraulichkeit öffentlich verfügbarer Zensus-Daten gab es bereits in den 1930er Jahren. Mit der Verwendung von SDB[73] zur Speicherung und Analyse ökonometrischer Daten verstärkten sich die Forschungsaktivitäten auf dem Gebiet der Datensicherheit.[74] In dem Maße, wie sich DBMS zur Speicherung großer Datenbestände im öffentlichen und betrieblichen Umfeld durchsetzten, wuchs das Interesse an Datensicherheit in Forschung wie Praxis weiter. Datensicherheit wird unter drei Aspekten diskutiert, denen auch OLAP-

[72] Zu restriktive Zugriffskontrollen beispielsweise können zu einer Senkung der Produktivität führen, wenn dadurch Informationen unzugänglich werden, welche die Mitarbeiter zur Erledigung ihrer Arbeitsaufgaben benötigen.

[73] Für eine genauere Begriffsklärung vgl. Abschnitt 4.3

[74] Vgl. u.a. ADAM/WORTHMANN (1989); DENNING/SCHLÖRER (1983)

Anwendungen[75], die auf diese Datenbestände zugreifen, prinzipiell genügen müssen:[76]

- Vertraulichkeit („confidentiality"): Schutz der Daten vor unautorisierten Lesezugriffen
- Integrität („integrity"): Schutz der Daten vor unautorisierten Schreibzugriffen
- Verfügbarkeit („availability"): Sicherstellung des Zugriffs auf Daten durch autorisierte Personen

Vertraulichkeit wiederum besitzt zwei Dimensionen, „confidentiality" und „privacy", die in der Literatur häufig synonym verwendet werden, sich jedoch genau genommen fundamental voneinander unterscheiden. „Confidentiality" bedeutet, dass der Zugriff auf Daten nur einem bestimmten Personenkreis gestattet wird. „Privacy" betrifft die Verwendung personenbezogener Daten. Die hierfür notwendigen Schutzmechanismen gehen über „confidentiality" hinaus, denn es muss sichergestellt werden, dass die Daten nur zu den Zwecken verwendet werden, denen die betreffende Person zugestimmt hat.[77]

Tabelle 3 gibt einen Überblick über die Kriterien, welche zur Beurteilung von SDB und OLAP-Anwendungen im Hinblick auf die Trade-Offs zwischen Sicherheit, Kosten und Nutzen herangezogen werden. Die Kategorie „Datenqualität" korrespondiert mit der in BERTINO/SANDHU (2005) geforderten Integrität; in OLAP-Anwendungen wird dieses Kriterium häufig vernachlässigt, da der lesende Zugriff im Fokus steht (vgl. Abschnitt 2.1).[78]

[75] Auch das FASMI-Kriterium „Shared" (vgl. Abschnitt 2.1) impliziert diese Anforderungen.

[76] Vgl. BERTINO/SANDHU (2005), S. 2 für die nachfolgende Aufzählung

[77] Vgl. ebenda, S. 2f. für den vorhergehenden Absatz

[78] Vgl. WANG/JAJODIA/WIJESEKERA (2007), S. 2f.

	Adam/Worthmann (1989)	Wang et al. (2007)
	SDB	***OLAP***
Flexibilität	✓	✓
	▪ Art und Anzahl der schützbaren Skalen ▪ Art und Anzahl der schützbaren Attribute ▪ Online-Einsatz	▪ Art der Aggregationen ▪ Externe Informationen ▪ Adaptierbarkeit
Datenqualität	✓	
	▪ Unverzerrtheit ▪ Präzision ▪ Konsistenz	
Sicherheit	✓	✓
	Inferenzen	▪ Direkte Zugriffe ▪ Inferenzen
Kosten	✓	✓
	▪Implementierung ▪Performanz ▪Usability	**Implementierung** **Performanz**
Verfügbarkeit		✓

Tabelle 3: Anforderungen an Sicherheitsmechanismen in SDB und OLAP
Eigene Darstellung[79]

Die Sicherheit von vertraulichen Daten kann auf zwei Arten kompromittiert werden. Erstens können unautorisierte Personen aufgrund fehlender Zugriffskontrollen direkten Zugang zu vertraulichen Daten erhalten. Zweitens können selbst bei funktionierenden Zugriffskontrollen unter Umständen Rückschlüsse (sog. Inferenzen) auf sensible Daten aus nicht vertraulichen Daten gezogen werden; beispielsweise durch unzureichende Anonymisierung persönlicher Daten.[80] Ein Überblick über verschiedene Arten von Disclosure sowie über gängige Verfahren zur Reduktion von Disclosure-Risiken findet sich in den Kapiteln 4 und 5.

Der folgende Abschnitt beleuchtet die mit dem Einsatz von OLAP-Anwendungen sowie der Implementierung von Sicherheitsmechanismen verbundenen Kosten genauer.

[79] Die fett gedruckten Kriterien werden von WANG/JAJODIA/WIJESEKERA (2007, S. 5) als separate Kriterien genannt. Aus Gründen der Übersichtlichkeit wurden sie in der Grafik in die entsprechenden Kategorien eingeordnet.

[80] Vgl. DALENIUS (1977)

3.2 Kosten von OLAP-Anwendungen

Hinsichtlich des Verwaltungs- und Wartungsaufwandes von DW gibt es eine Reihe von Einzelfallbeschreibungen wie bspw. von SHIN (2003). Diese sei hier exemplarisch angeführt, um die betriebswirtschaftliche Bedeutung von DW zu unterstreichen. Der Autor berichtet, dass die Betreuung des Data Warehouse (Rechteverwaltung, Aktualisierungen usw.) in einem Konzern mit 65.000 Mitarbeitern 20 IT-Mitarbeiter in Anspruch nahm. Die Einsparungen durch den Einsatz des DW betrugen jährlich 3,5 Millionen US-Dollar, während etwa 20 Millionen US-Dollar für DW-bezogene Ausgaben zwischen 1992 und 2002 zu verzeichnen waren.[81]

Belastbare, groß angelegte empirische Studien zu den Kosten von DW oder OLAP-Anwendungen existieren bisher nicht, so dass Schätzungen von Durchschnittswerten oder auch nur Intervallen jeder Basis entbehren würden. Aus diesem Grund wird im folgenden Verlauf der Arbeit darauf verzichtet, Vermutungen über die tatsächliche Höhe von Kosten und Kosteneinsparungspotenzialen vorzunehmen.

Einen Hinweis darauf, dass speziell auch die Implementierung und Administration von Sicherheitsmaßnahmen in DW von betriebswirtschaftlicher Bedeutung ist, liefert die Studie von O'CONNOR/LOOMIS (2010) zu den Auswirkungen von Datenschutzmechanismen, genauer des Zugriffskontrollverfahrens „Role-based Access Control" (RBAC)[82]. Die Autoren untersuchen die Effekte von RBAC auf die Kategorien Produktivität, Verwaltungsaufwand und effizientere Aufgabenerfüllung.[83] Sie schätzen, dass der Produktivitätsverlust von Mitarbeitern, denen unzureichende Zugriffsrechte auf DW eingeräumt wurden, durchschnittlich 42% beträgt, während die Mitarbeiter auf die Erteilung der entsprechenden Rechte warten.[84] Durch die Einführung von RBAC ließe sich der Produktivitätsverlust, welcher aus einer zu restriktiven Rechtevergabe und daraus resultierenden „Leerlaufzeiten" der Mitarbeiter entstehen kann, um etwa 300.000 US-Dollar pro Jahr senken (vgl. Tabelle 4: II). Der IT-Verwaltungsaufwand (vgl. Tabelle 4: I und III) ließe sich durch die Einführung eines effizienteren Rechteverwaltungssystems um durchschnittlich knapp 665.000 US-Dollar pro Jahr senken, während sich der Nutzen aus effizienterer Aufgaben-

81 Vgl. SHIN (2003), S. 157

82 Das allgemeine Konzept von RBAC wird in Abschnitt 4.2.4 und OLAP-spezifische Adaptionen in Abschnitt 5.1.2 vorgestellt.

83 Vgl. O'CONNOR/LOOMIS (2010), S. 67

84 Diese und alle folgenden Schätzungen beziehen sich auf Unternehmen mit etwa 10.000 Mitarbeitern.

erfüllung mit knapp 450.000 US-Dollar beziffern lässt (vgl. Tabelle 4: IV).[85]

		Zeiteinsparung	Durchschnittl. Stundenlohn	Kostenersparnis	**Gesamtersparnis**
		Pro Mitarbeiter	*US-Dollar*	*Pro Mitarbeiter*	***10.000 Mitarbeiter***
	Effizientere Rechtevergabe				
I	▶ Netzwerk- und Systemadministratoren	**0,035**	**68,20**	**2,38**	**23.800**
II	▶ Mitarbeiter im operativen Geschäft	**0,55**	**54,62**	**30,05**	**300.500**
	Effizientere Aktualisierung und Zertifizierung				
III	▶ IT-Mitarbeiter	**0,72**	**92,10**	**66,31**	**663.100**
IV	▶ Mitarbeiter im operativen Geschäft	**0,45**	**98,94**	**44,52**	**445.200**
	Gesamtnutzen			**143,26**	**1.432.600**

Tabelle 4: Gesamtnutzen aus RBAC
Vgl. O'CONNOR/LOOMIS (2010), S. 201

Eine RBAC-Implementierung kostet durchschnittlich über 2 Millionen US-Dollar.[86] Hieraus wird ersichtlich, dass die Implementierungskosten bei der Beurteilung der Auswirkungen von Schutzmechanismen auf den Unternehmensnutzen keinesfalls vernachlässigt werden dürfen. In OLAP-Anwendungen können – zusätzlich zu den Implementierungs- und Verwaltungskosten – durch zu restriktive Schutzmechanismen Opportunitätskosten verursacht werden, die aufgrund nicht erkannter Muster in den Daten und entsprechend unterlassener Maßnahmen (bspw. verkaufsfördernde Maßnahmen) entstehen (vgl. Tabelle 5). Im Rahmen dieser Arbeit wird von einem Versuch abgesehen, diese Kosten zu quantifizieren; es wird lediglich angenommen, dass sie mit zunehmender Restriktivität der Schutzmechanismen steigen.

Aktualisierungen	Implementierung
Rechteverwaltung	Opportunitätskosten
Kosten	

Tabelle 5: Kosten von DL in OLAP
Eigene Darstellung

[85] Vgl. O'CONNOR/LOOMIS (2010), S. 6–9 für den vorhergehenden Absatz
[86] ebenda, S. 18

3.3 Nutzeneffekte von OLAP-Anwendungen

Empirisch belegte positive Effekte des Einsatzes von DW in Unternehmen lassen sich grob in die folgenden Kategorien einordnen:

(1) Produktivitätssteigerung[87],
(2) Effizienzgewinn[88],
(3) Kostensenkung[89] sowie
(4) Produkt-/Dienstleistungs- und Prozessverbesserung[90]

In einer Untersuchung aus dem Jahr 1996 bspw. fand man bei 62 untersuchten DW-Implementierungen nach 3 Jahren einen durchschnittlichen ROI von etwa 400%.[91] Als Treiber dieser Verbesserungen werden verbesserte und verkürzte Entscheidungsprozesse aufgrund höherer Datenqualität und Datenintegration über heterogene (verteilte) Systeme angeführt (vgl. Tabelle 6).

OLAP-Anwendungen werden als strategische Analyseinstrumente insbesondere auch von Entscheidungsträgern auf höheren Hierarchieebenen (vgl. Abschnitt 2.1) eingesetzt, um (langfristige) Verbesserungspotenziale zu entdecken, d.h. die Qualität der strategischen Entscheidungen wird durch OLAP beeinflusst. Die Quantifizierung deren Auswirkungen auf den Unternehmenserfolg ermöglicht einen Rückschluss auf den organisatorischen Nutzen, den OLAP-Anwendungen stiften.

Ansatzpunkt ist folglich der einzelne Anwender (auf Management-Ebene), dessen Leistung und Entscheidungsverhalten durch OLAP-Anwendungen beeinflusst wird. Die kumulierten individuellen Effekte bilden die Basis zur Beurteilung des Einflusses von OLAP auf den organisatorischen Nettonutzen. Bisher gibt es entsprechende Untersuchungen lediglich auf Ebene von DW. Tabelle 6 gibt einen Überblick über die bereits empirisch nachgewiesenen Effekte des Einsatzes von DW-Technologien.

87 Vgl. SHIN (2003); SEDERA/GABLE (2004)
88 Vgl. WIXOM/WATSON (2001)
89 Vgl. SEDERA/GABLE (2004)
90 Vgl. WIXOM/WATSON (2001); SEDERA/GABLE (2004); HONG ET AL. (2006); XU/HWANG (2008)
91 IDC, zitiert nach WATSON/GOODHUE/WIXOM (2002), S. 491

Nettonutzen		Wixom/ Watson (2001)	Shin (2003)	Wixom/ Todd (2005)	Hong et al. (2006)
Organisatorisch	**Individuell**				
Kosten					
	Aufwandsärmere Umsetzung von Entscheidungen	✓			
Produktivität					
	Effizientere Umsetzung von Entscheidungen	✓			
	Individuelle Produktivität		✓	✓	
Leistungsqualität					
	Leistungsqualität		✓	✓	✓
	Entscheidungsqualität			✓	✓
Veränderung der Geschäftsprozesse					
	Veränderung der Arbeitsaufgaben	✓			

Tabelle 6: Vergleich der Operationalisierungen von Nettonutzen in Studien zu DW
Eigene Darstellung

Die Frage, welche Charakteristika den erfolgreichen Einsatz von OLAP-Anwendungen determinieren, wird im Folgenden aus Perspektive der Anwender diskutiert.

Die zentrale Anforderung der Nutzer an DW und datenbankbasierte Informationssysteme wie OLAP ist die Bereitstellung aller Daten, welche die Nutzer zur Erledigung ihrer Aufgaben in der Organisation benötigen.[92] Die Erfüllung dieser Anforderung lässt sich anhand der zur Verfügung gestellten Daten selbst (Daten- oder Informationsqualität) sowie der Art und Weise, wie sie zur Verfügung gestellt werden (Systemqualität), beurteilen.[93]

Zur Abbildung und Messung dieser Zusammenhänge wurde in den oben zitierten Studien das DeLone/McLean-Modell (vgl. Abbildung 10[94]) herangezogen. Es wurde ursprünglich für betriebliche IS im Allgemeinen entwickelt und ist (in seiner zweiten aktualisierten Version) vielfach empirisch belegt.[95]

92 Vgl. WANG/JAJODIA/WIJESEKERA (2007), S. 2
93 Vgl. DELONE/MCLEAN (2003)
94 Die blau hervorgehobenen Konstrukte werden im weiteren Verlauf dieses Kapitels genauer besprochen.
95 Vgl. ebenda

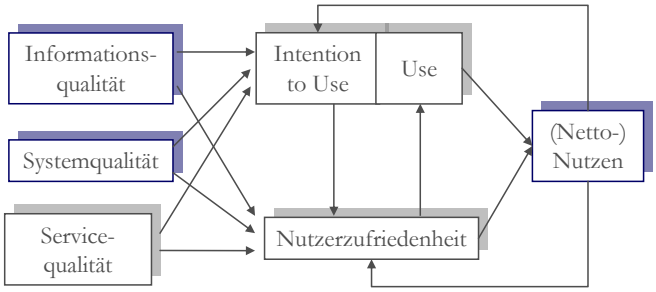


Abbildung 10: Aktualisiertes DeLone/McLean-Modell
Vgl. DELONE/MCLEAN (2003), S. 24

Die Konstrukte „Informationsqualität", „Systemqualität" [96] und „Servicequalität" beeinflussen die Nutzerzufriedenheit, die tatsächliche Nutzung des Systems („Use") sowie die Nutzungsabsicht („Intention to Use") und dadurch den Nutzen, der den Mitarbeitern durch den Einsatz des Systems entsteht.[97] Positive Nutzeneffekte, wie bspw. verbesserte Entscheidungsqualität[98], verstärken wiederum die Nutzung(sabsichten) sowie die Nutzerzufriedenheit.

Das Konstrukt „Servicequalität" wird im folgenden Verlauf der Arbeit nicht weiter betrachtet. Dies signalisiert keine Geringschätzung des Erfolgsbeitrages von IT-Services, sondern dient der besseren Fokussierung der systembezogenen Aspekte.[99] Eine Reintegration des Konstrukts in das Modell ist problemlos möglich.[100]

Eine systematische Herleitung von IS-Qualitätsfaktoren[101] aus der einschlägigen Literatur zur Messung der einzelnen Konstrukte des DeLone/McLean-Modells findet sich in NELSON/TODD/WIXOM (2005). Sie entwickeln insbesondere ein mehrdimensionales Verständnis[102] von Informationsqualität:[103]

- Die intrinsische Dimension beschreibt, inwiefern Informationen mit der Realität korrespondieren, die sie abbilden (Korrektheit).

---

96 Tabelle 7 gibt einen Überblick über die in einschlägigen Studien zum erfolgreichen Einsatz von DW verwendeten Operationalisierungen für Daten- und Systemqualität.

97 Vgl. bspw. DELONE/MCLEAN (2003) und GRGECIC/ROSENKRANZ (2010) für eine Diskussion der Operationalisierung der Konstrukte Nutzerzufriedenheit, „Use" und „Intention to Use"

98 Vgl. HONG ET AL. (2006)

99 Eine detaillierte Begründung für diese Entscheidung findet sich in Abschnitt 3.1.4.

100 Diese Vorgehensweise orientiert sich an der von WIXOM/TODD (2005, S. 91) vorgeschlagenen Messung des Erfolgsbeitrags von DW.

101 Vgl. NELSON/TODD/WIXOM (2005)

102 Das daraus abgeleitete Messinstrument erklärte in einer DW-Studie über 75% der Varianz von Informations- und Systemqualität, was darauf hindeutet, dass die zentralen Einflussfaktoren erfasst werden [vgl. ebenda, S. 214f.].

103 Vgl. ebenda, S. 202 für die folgende Aufzählung

- Die kontextuelle Dimension gibt Aufschluss über die aufgaben- und umfeldbezogene Relevanz von Informationen (Vollständigkeit, Aktualität).
- Die gegenständliche Dimension schließlich beschreibt, inwiefern die Darstellung von Informationen ihre Interpretierbarkeit und Verständlichkeit befördert (Präsentation).

	Wixom/ Watson (2001)	Shin (2003)	Wixom/ Todd (2005)	Hong et al. (2006)	
Informationsqualität					
Vollständigkeit	✓		✓		Lieferung aller notwendigen Informationen
Korrektheit	✓	✓	✓	✓	Korrektheit der Informationen
Konsistenz	✓	✓			Konsistenz der Informationen
Granularität		✓		✓	Detailliertheitsgrad der Informationen
Präsentation			✓	✓	Güte der Informationsdarstellung
Aktualität		✓	✓	✓	Aktualität der Informationen
Relevanz				✓	Relevanz der gelieferten Informationen bzgl. seiner Arbeitsaufgabe
Systemqualität					
Flexibilität	✓		✓		Anpassungsfähigkeit an Nutzeranforderungen
Integration	✓		✓		Datenintegration aus verschiedenen Quellen
Zugriffskontrolle		✓			Zugriff auf die für Arbeitsaufgaben benötigten Informationen
Auffindbarkeit		✓			Lokalisierbarkeit benötigter Informationen
Performanz		✓	✓	✓	zeitnahe Systemantwort auf Nutzeranfragen
Ease of Use		✓			Benutzerfreundlichkeit des Systems
Zuverlässigkeit			✓		Zuverlässigkeit der Systemoperationen
Verfügbarkeit		✓	✓	✓	Leichtigkeit des Zugriffes auf oder der Extraktion von Informationen

Tabelle 7: Vergleich der Operationalisierungen von Daten- und Systemqualität in Studien zu DW
Eigene Darstellung

Die für Nutzer von DW wichtigsten Kriterien sind nach dem aktuellen Stand der Forschung neben der Verfügbarkeit der relevanten Informationen somit Vollständigkeit, Korrektheit, Präsentation und Aktualität der Information sowie Flexibilität, Integration und Zuverlässigkeit des Systems.[104] Da die Mehrzahl der Nutzer über eine OLAP-Anwendung auf den Datenbestand eines DW (vgl. Abschnitt 2.1) zugreift, ist für die separate Beurteilung der OLAP-Anwendung eine Differenzierung zwischen der vom DW und der direkt von OLAP gelieferten Funktionalität notwendig. Im Folgenden werden die

[104] Vgl. WIXOM/TODD (2005)

einzelnen Kriterien hinsichtlich ihrer Relevanz zur Beurteilung von OLAP (vgl. FASMI-Kriterien in Abschnitt 2.1) eingeordnet und ein entsprechend adaptiertes Modell zur Messung der Erfolgswirkung von OLAP vorgeschlagen.

Zur Messung des Konstrukts „Systemqualität" werden die Faktoren Flexibilität, Performanz und Verfügbarkeit vorgeschlagen. Das Kriterium „Integration" ist zwar für OLAP-Anwendungen von Bedeutung, die auf verteilten Datenbeständen basieren[105]; die eigentliche Datenintegration (Transformation, Säuberung) geschieht jedoch i.d.Regel auf Ebene des DW. „Zuverlässigkeit" beschreibt die Ausfallsicherheit eines Systems. Hierfür bietet i.d.Regel ebenfalls das zugrunde liegende DW (bzw. das verwendete DBMS) Lösungen an (vgl. Abschnitt 2.3). Folglich sind diese Kriterien für die Beurteilung der Qualität von OLAP-Anwendungen nicht geeignet.

Hinsichtlich des Faktors „Verfügbarkeit" ist eine Begriffsklärung vorzunehmen. Er ist nach dem Verständnis der oben zitierten Studien ein systemimmanenter Usability-Aspekt, der die Intuitivität der Bedienung[106] beschreibt (vgl. Tabelle 7). Im Kontext der vorliegenden Arbeit steht die Forderung „[that] data should be readily available to legitimate users with sufficient privileges"[107] im Vordergrund. Dies ist durch die explorative Natur von OLAP-Anwendungen bedingt, zielt auf die Maximierung der Explorationsmöglichkeiten der Anwender und somit des (betrieblichen) Nutzens aus der Datenanalyse.

Die Flexibilität eines OLAP-Systems lässt sich u.a. an der Anzahl und Verschiedenheit von Aggregationsoperationen ablesen, welche den Nutzern zur Verfügung stehen (vgl. Abschnitt 2.2) und entsprechend verschiedenartige Möglichkeiten der Datenanalyse eröffnen. Außerdem wird sie determiniert durch die Leichtigkeit, mit der das System an (neue) Nutzeranforderungen angepasst[108] werden kann. Zusätzlich ist in OLAP auch der Faktor „Performanz" von Bedeutung, denn komplexe Aggregationsoperationen auf sehr großen Datenbeständen können Rechen- und Wartezeiten unzumutbar verlängern, wenn das System nicht laufzeitoptimiert ist. [109]

Im Hinblick auf das Konstrukt „Informationsqualität" einer OLAP-Anwendung sind die

---

[105] Vgl. WANG/JAJODIA/WIJESEKERA (2007), S. 5

[106] Mitunter beschreibt er auch die Datensicherung (Legacy-Systeme etc.), wenn die Benutzerfreundlichkeit separat bspw. durch „Ease of Use" abgebildet wird (vgl. Tabelle 7).

[107] WANG/JAJODIA/WIJESEKERA (2007), S. 5

[108] Dieser Aspekt entspricht teilweise dem FASMI-Kriterium „Analysis" (vgl. Abschnitt 2.1).

[109] Performanz entspricht dem FASMI-Kriterium „Fast". Der Einsatz immer performanterer DBMS-Technologien lässt dieses Kriterium relativ zu den anderen etwas an Bedeutung verlieren (vgl. Abschnitt 2.1).

Anforderungen verglichen mit DW (vgl. Tabelle 7) weitgehend identisch; es ist leicht nachvollziehbar, dass Anwender unabhängig vom verwendeten System erwarten, dass die vorgehaltenen bzw. zurück gelieferten Daten aktuell, vollständig, korrekt und konsistent sind. Die (physische) Speicherung und Aktualisierung der Daten unter Berücksichtigung dieser Aspekte geschieht zwar auf DW-Ebene, doch verschiedene Sicherheitsmechanismen auf OLAP-Ebene können dazu führen, dass diese Leistungskriterien beeinträchtigt werden (vgl. Abschnitt 3.4), weswegen sie auch im vorliegenden Modell berücksichtigt werden sollten. Speziell in OLAP ist die Granularität, in der die Daten vorgehalten werden bzw. abrufbar sind, von Bedeutung, da die Aussagekraft (und die Gefahr von Inferenzen) stark aggregierter Daten niedriger ist als die feingranularer Daten. Dies hat u.a. eine direkte Auswirkung auf die Datenanalysen, die darauf ausgeführt werden können. Tabelle 8 fasst die Anforderungen der Nutzer an OLAP zusammen.

Systemqualität	Informationsqualität
▶ **Flexibilität** ▪ Art der Aggregationen ▪ Adaptierbarkeit ▶ **Performanz** ▶ **Verfügbarkeit**	▶ **Vollständigkeit** ▶ **Korrektheit** ▶ **Konsistenz** ▶ **Granularität** ▶ **Aktualität** ▶ **Präsentation**

Tabelle 8: Nutzeranforderungen an Qualität von OLAP
Eigene Darstellung

Diese Kriterien entsprechen im Wesentlichen den FASMI-Kriterien (vgl. Abschnitt 2.1) bzw. dem Teil der FASMI-Kriterien, welche der Anwender wahrnehmen und evaluieren kann. Die Erfüllung dieser Anforderungen wirkt sich – über Nutzerzufriedenheit und Nutzung – direkt auf den individuellen Nutzen und folglich kumuliert auch auf den organisatorischen Nutzen aus OLAP aus.[110] Im Kontext der vorliegenden Arbeit ist von Interesse, inwiefern Mechanismen zur Disclosure Limitation die Erfüllung dieser Kriterien (und damit den erzielbaren Nutzen aus der OLAP-Anwendung) beeinträchtigen könnten. Eine diesbezügliche Beurteilung der verschiedenen Verfahren findet sich in Abschnitt 5.3. Im folgenden Abschnitt erfolgt eine genauere Betrachtung der Trade-Offs zwischen Sicherheit, Kosten und Nutzen, die mit der Implementierung von Schutzmechanismen in OLAP verbunden sind.

[110] Vgl. DELONE/MCLEAN (2003)

3.4 Trade-Offs durch Disclosure Limitation in OLAP

Da das DeLone/McLean-Modell (vgl. Abbildung 10) keine direkten Ansatzpunkte zur Untersuchung der Effekte von Sicherheitsmechanismen auf den Nutzen aus OLAP-Anwendungen bietet, wird an dieser Stelle eine Erweiterung um den Faktor „Sicherheit" vorgenommen. Dieser beschreibt, inwiefern unautorisierten Nutzern direkte Zugriffe oder Inferenzen auf geschäftskritische Daten möglich sind. Je schwieriger sich dies gestaltet, desto höher ist der Nutzen, welcher dem Unternehmen aus dem eingesetzten Verfahren entsteht.[111]

Es wird erwartet, dass sich in Abhängigkeit des implementierten Sicherheitsmechanismus Veränderungen in der wahrgenommenen System- und Informationsqualität zeigen, welche die Nutzerzufriedenheit sowie die Nutzungsabsicht beeinflussen. Der organisatorische (Netto-)Nutzen wird einerseits über diese Wirkungskette, andererseits (negativ) durch zusätzlichen Administrationsaufwand und (positiv) durch erhöhte Datensicherheit beeinflusst.

An dieser Stelle muss zwischen den technisch-administrativen und anwenderbezogenen Konsequenzen der Implementierung eines Sicherheitsmechanismus unterschieden werden. Beide Aspekte sind wichtig für eine umfassende Beurteilung der Vorteilhaftigkeit eines Verfahrens. Jedoch ist es höchst unwahrscheinlich, dass die Anwender den administrativen Aufwand korrekt einschätzen können. Umgekehrt ist nicht zu erwarten, dass den IT-Mitarbeitern die Implikationen der Restriktionen eines bestimmten Verfahrens auf die Nützlichkeit der OLAP-Anwendung vollständig bewusst sind bzw. dass vollständig antizipierbar ist, wie die Anwender auf neue Restriktionen reagieren. Es werden somit zwei Messmodelle benötigt (vgl. Abbildung 11), die getrennt voneinander den individuellen Nutzen aus der tatsächlichen Nutzung von OLAP-Anwendungen und den Aufwand für die Administration des Systems erfassen.

Die in Abbildung 11 postulierten Zusammenhänge werden im Folgenden näher erläutert und die potentiellen Auswirkungen der Implementierung eines Sicherheitsmechanismus auf die Indikatoren der einzelnen Konstrukte (vgl. Abbildung 12) diskutiert.

111 Zur Bezifferung des Nutzens können bspw. Schätzungen über die Höhe des potentiellen Schadens aus dem Bekanntwerden der zu schützenden Daten herangezogen werden.

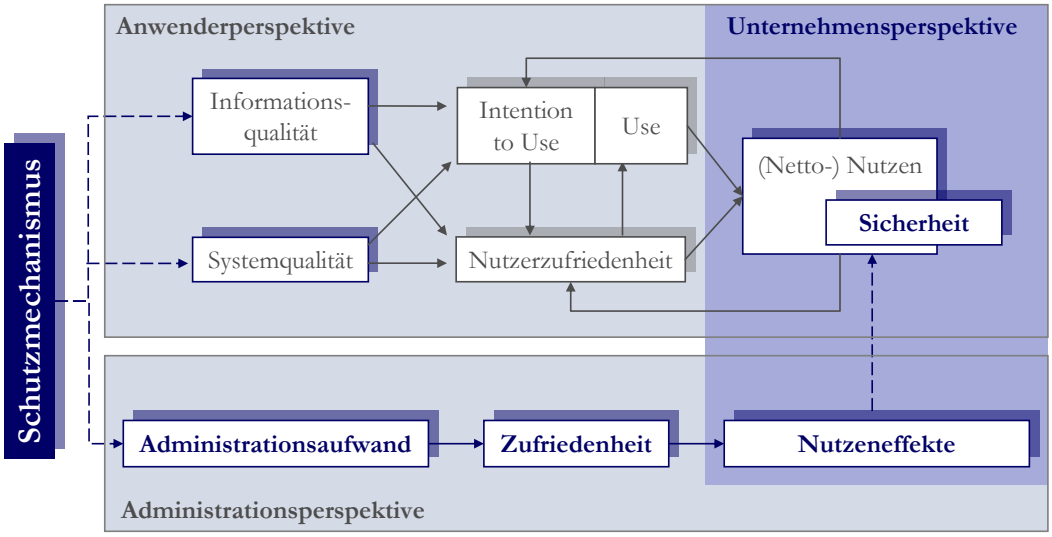


Abbildung 11: Effekte von Sicherheitsmechanismen im DeLone/McLean-Modell
Eigene Darstellung

Im Hinblick auf die Systemqualität ist eine Verschlechterung der Wahrnehmung aller drei Indikatoren möglich. Disclosure Limitation-Verfahren haben i.d.Regel negative Auswirkungen auf die Performanz, da zusätzlich zur eigentlichen Berechnung eine Zulässigkeitsprüfung zur Laufzeit erfolgt.[112] Manche Verfahren (vgl. Abschnitt 5) schränken die zulässigen Aggregationsoperationen ein, was den Faktor „Flexibilität" beeinflusst. Disclosure Limitation -Verfahren führen mitunter zu Zugriffsverboten auf Daten, welche der oder die Anwender zur Erledigung ihrer Arbeitsaufgaben benötigen. Diese Problematik ergibt sich beispielsweise dann, wenn ein Verfahren den organisatorischen Prozessen nicht hinreichend angepasst wurde, so dass die Zugriffsrechte nicht korrekt vergeben wurden.[113]

Bezüglich der Informationsqualität ist leicht ersichtlich, dass – beispielsweise durch unzureichende Zugriffsrechte – Vollständigkeit und Granularität beeinflusst werden können. Perturbationsbasierte Disclosure Limitation (vgl. Abschnitt 4.3.2) kann zu Einschränkungen der Konsistenz und Korrektheit von Daten führen, da hierbei die tatsächlichen Ausprägungen der Daten „verrauscht" werden und lediglich verteilungsbasierte statistische Kennzahlen keine Änderung erfahren. Die Aktualität der Daten kann indirekt von Disclosure Limitation beeinträchtigt werden, wenn sich die Aktualisierung der Daten bzw. der Zugriffsrechte als Folge der Implementierung eines Sicherheitsmechanismus schwierig und zeitaufwendig gestaltet und nur in relativ großen zeitlichen Abständen durchgeführt werden kann. Bezüglich der Präsentation der Daten sind keine Einschränkungen zu er-

[112] Vgl. Abschnitt 5.3
[113] Für Effekte auf Produktivität vgl. Abschnitt 3.2 bzw. O'CONNOR/LOOMIS (2010), S. 67

warten.

Erhöht sich der Administrationsaufwand für das OLAP-System durch die Implementierung eines Disclosure Limitation-Verfahrens, so wirkt sich dies auf die Effizienz und ggf. die Qualität der Arbeit der zuständigen IT-Mitarbeiter aus. Es wird angenommen, dass ähnliche Zusammenhänge wie für die Nutzerperspektive unterstellt werden können. Analog zum DeLone/McLean-Modell wird daher auf Administrationsseite die Zufriedenheit der zuständigen IT-Mitarbeiter in Abhängigkeit des Administrationsaufwandes für Aktualisierungen und Rechtevergabe modelliert. Eine Veränderung der Zufriedenheit der IT-Mitarbeiter mit dem System führt dann zu einer Veränderung von Effizienz und/oder Qualität der Arbeit, welche wiederum eine Dimension des organisatorischen Nettonutzens darstellt. „Intention to Use“ und „Use“ werden nicht in die Betrachtung aufgenommen, da angenommen wird, dass die Betreuung des Systems als Arbeitsaufgabe der IT-Mitarbeiter vertraglich geregelt ist.

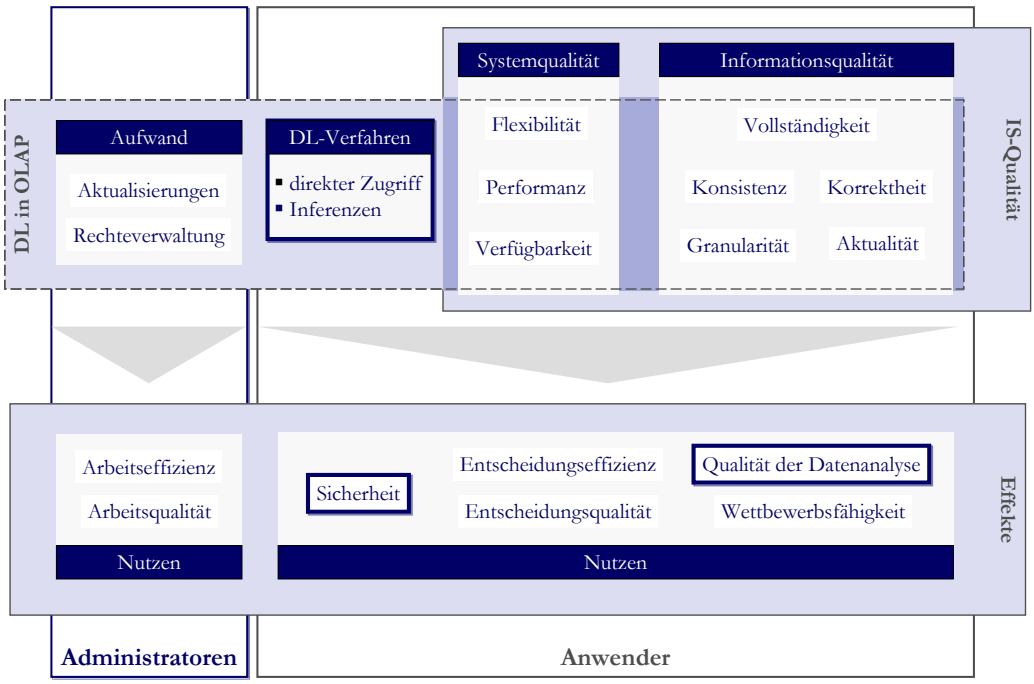


Abbildung 12: Indikatoren für Effekte von Disclosure Limitation auf den Nutzen aus OLAP
Eigene Darstellung

Das adaptierte Modell wird in Abschnitt 4.3 verwendet, um die potentiellen Auswirkungen von Disclosure Limitation, die für SDB vorgeschlagen wurde, für OLAP zu prüfen. Geeignete Verfahren werden in Abschnitt 5 diskutiert und anhand des eben entwickelten Modells in Abschnitt 5.3 hinsichtlich ihrer relativen Vor- und Nachteile diskutiert.

4 GRUNDLEGENDE ASPEKTE VON DISCLOSURE

Der Umgang mit Daten und Informationen stellt jede Organisation vor das Problem, wie Datenschutz und Datenanalyse zu vereinbaren sind. Einerseits stecken rechtliche Vorschriften und die Notwendigkeit, sensible Organisationsdaten vor Zugriffen durch unautorisierte Personen zu schützen, enge Grenzen für den zulässigen Zugang zu und Umgang mit Daten. Speziell im Kontext von Datenbanken ergeben sich Trade-Offs zwischen dem bestmöglichen Schutz vertraulicher Daten vor dem Zugriff nicht berechtigter Nutzer, den Kosten des Einsatzes von Schutzmechanismen hinsichtlich Implementierungsaufwand und Effizienzverlusten bei Abfragen, sowie der Maximierung der Nützlichkeit von Abfragen (insbesondere Aggregationsoperationen) zur systematischen Datenanalyse (vgl. Abschnitt 3.4). Systematische Abfragen sind hierfür unabdingbar, gleichzeitig jedoch problematisch, da sie verwendet werden können, um Schutzmechanismen zur Anonymisierung oder Unterdrückung sensibler Daten zu unterlaufen (vgl. Abschnitt 4.3).[114]

Als Beispiel sei ein Versicherungsunternehmen genannt, das feststellen möchte, ob die Versicherten einer bestimmten Region die empfohlene FSME-Schutzimpfung regelmäßig vornehmen lassen. In dieser Region seien 500 Männer und eine Frau bei dem Unternehmen versichert. Erlaubt das Unternehmen nun die Aufschlüsselung der Daten nach „Leistungsart", „Jahr" und „Geschlecht", so ist dies für die 500 Männer unproblematisch. Die Frau jedoch kann eindeutig identifiziert werden. Selbst ohne die Möglichkeit, nach Geschlecht zu aggregieren, existieren Disclosure-Risiken. Die Aufschlüsselung der Daten nach Leistungsarten ist beispielsweise problematisch: Für die Leistungsart „Zahnärztliche Regeluntersuchung" ist eine Disclosure eher unwahrscheinlich; für die Leistungsart „Schwangerschaftsuntersuchung" jedoch kann direkt auf die Identität der Person rückgeschlossen werden, welche diese Leistung in Anspruch genommen hat.

Aus betrieblicher Perspektive ist es sehr wohl wünschenswert, solche Analysen durchzuführen, um bspw. Leistungsdefizite oder auch ein Überangebot in der Region aufzudecken. Methoden zur Lösung dieses Dilemmas werden in der Literatur unter dem Begriff „Statistical Disclosure Control" oder „Statistical Disclosure Limitation" diskutiert.[115]

---

[114] Vgl. WANG/JAJODIA/WIJESEKERA (2007), S. 2 und DALENIUS (1977), S. 429f. für diesen und die beiden vorhergehenden Sätze

[115] Vgl. ebenda, S. 429

Die Forschung zu diesem Thema untergliedert sich in zwei Themengebiete.[116] Die sog. „Access Control"-Literatur beschäftigt sich mit der Frage, wie die Vergabe von Lese- und ggf. Schreibrechten an Nutzer gestaltet werden kann. Entsprechende Konzepte zur Kontrolle des Zugriffs auf Daten werden in Abschnitt 4.2 vorgestellt. Abschnitt 4.3 gibt einen Überblick über die „Inference Control"-Literatur. Sie befasst sich mit der Problematik der Identifikation potentiell sicherheitsgefährdender Queries und der Entwicklung von Gegenmaßnahmen.

4.1 Begriffliche Einordnung

Das Problem der Disclosure wurde zunächst bezüglich der Veröffentlichung von Bevölkerungsstatistiken beschrieben und diskutiert. Auf diesen Anwendungsfall bezieht sich die Definition von DALENIUS, der dieses Thema als einer der Ersten auch in Bezug zu statistischen Datenbanken systematisch erforschte. Statistische Disclosure liegt ihm zufolge vor, „if the release of the statistics S makes it possible to determine the value D_K, more accurately than is possible without access to S".[117] Der Wert D_K beschreibt eine Eigenschaft eines Objektes O_K, das Bestandteil der Population O ist, für welche die Statistik S[118] erhoben wurde.[119] Disclosure kann sich somit auf folgende Arten äußern:

- Offenlegung der Identität. Beteiligt sich beispielsweise genau ein Vorstandsmitglied an einer Umfrage, welche eine Frage nach der Arbeitsposition des Antwortenden enthält, kann sein Fragebogen eindeutig identifiziert werden.
- Offenlegung bestimmter Attribute. Unvollständige Angaben des nun identifizierten Vorstandsmitgliedes zu seinem Familienstand könnten aus den Daten des Einwohnermeldeamtes oder des Standesamtes vervollständigt werden und zusätzliche Daten (z.B. Adresse) erfasst werden.
- Inferenzen. Beteiligen sich zwei Vorstandsmitglieder an einer Umfrage, können sie aus den nach Hierarchiestufe aggregierten Daten die Antworten des jeweils anderen ableiten (z.B. Einkommen).

---

116 Vgl. WANG/JAJODIA/WIJESEKERA (2007), S. 2f.

117 DALENIUS (1977), S. 433

118 Im Kontext von OLAP spricht man, dem betriebswirtschaftlichen Duktus folgend, statt von Statistiken von Kennzahlen („facts", vgl. Abschnitt 2.2). Aus Gründen der Einheitlichkeit und besseren Lesbarkeit der Arbeit wird im Folgenden ausschließlich der Begriff „Kennzahlen" verwendet.

119 Vgl. ebenda, S. 430-433 für den vorhergehenden Satz und die nachfolgende Aufzählung

4.2 Zugriff und Zugriffskontrolle in relationalen Datenbanken

Mit der Entstehung der ersten Dateimanagement- und Informationssysteme ergab sich die Frage, wie Zugriffskontrolle und -verwaltung organisiert werden sollten.[120] Für DBMS mussten spezielle Zugriffskontrollmodelle entwickelt werden, welche sich in Relationen[121], Attributen und Tupeln ausdrücken lassen, um sie dem logischen Datenmodell zuordnen zu können. Zudem muss ein effektiver DBMS-Sicherheitsmechanismus neben einer „name-based access control" auch „content-based access control" unterstützen, d.h. eine Berechtigungsprüfung auf das abgefragte Objekt ist sowohl anhand des Objektnamens als auch des Objektinhalts durchzuführen.[122] Im Folgenden werden die beiden Basiskonzepte der Zugriffsbeschränkung – Discretionary Access Control (DAC) und Mandatory Access Control (MAC) – kurz erläutert. Beide Konzepte beinhalten in ihren Grundformen kritische Sicherheitslücken. Insbesondere weisen sie eine hohe Anfälligkeit gegenüber trojanischen Pferden, d.h. unbemerkt vom Nutzer mit dessen Rechten ausgeführte schädliche Programme, und „covert channels" auf, d.h. die Verwendung von Programm- oder Systemkomponenten[123] zur unautorisierten Übertragung sensibler Informationen. Zudem verursachen DAC und MAC beträchtlichen Verwaltungsaufwand. Mit steigender Zahl der zu verwaltenden Objekte und Nutzer wurde die Lösung dieser Probleme drängender, und es wurden diverse DBMS-spezifische Erweiterungen der beiden Basismodelle entwickelt.

Abschnitt 4.2.3 stellt das von DENNING 1976 entwickelte MAC-basierte Lattice-Modell zur Identifikation und Eingrenzung unsicherer Informationsflüsse in (betrieblichen) Anwendungssystemen vor, das in den folgenden Jahrzehnten insbesondere für den Einsatz in Datenbanken immer wieder aufgegriffen und erweitert wurde. In Abschnitt 4.2.4 wird Role-Based Access Control (RBAC)[124] beschrieben, die mit dem Ziel der Verminderung des Verwaltungsaufwandes von Zugriffsrechten in Datenbanken bzw. Data Warehouses

120 Vgl. bspw. BELL/LAPADULA (1973b), GRIFFITHS/WADE (1976)

121 Dieses Kapitel fokussiert Sicherheitskonzepte in relationalen DBMS. Der überwiegende Teil der Forschung zu Sicherheit in DBMS wurde auf Basis relationaler DBMS durchgeführt. Für andere DBMS vgl. bspw. BERTINO/SANDHU (2005)

122 Vgl. ebenda

123 Vermutet ein Nutzer beispielsweise, dass ein geschütztes Objekt existiert und sendet eine entsprechende Query, so kann durch die Systemantwort „Access Denied" auf die Existenz dieses Objektes geschlossen werden (vgl. Abschnitt 4.2.2).

124 Vgl. O'CONNOR/LOOMIS (2010); BERTINO/SANDHU (2005), S. 7

entwickelt wurde.[125] Abschließend werden die Vor- und Nachteile der vorgestellten Ansätze hinsichtlich ihrer Anwendbarkeit auf OLAP in Abschnitt 4.2.5 verglichen und bewertet.

4.2.1 Discretionary Access Control

Auf DAC fußende Sicherheitsrichtlinien enthalten keine inhaltsbasierten Regeln zur Rechtevergabe, sondern funktionieren ausschließlich über nutzerbezogene Berechtigungen (vgl. Abbildung 13). Die einzelnen Ansätze von DAC unterscheiden sich hauptsächlich hinsichtlich der Objekte, für welche Berechtigungen vergeben werden können, sowie der Rechteverwaltung.

Das Basismodell der DAC in relationalen Datenbanken („System R“) beschränkte sich auf Tabellen und Views als zu schützende Objekte.[126] Spätere DAC-Ansätze erweiterten dieses Basismodell um andere Objekte wie z.B. Trigger oder Foreign-Key-Referenzierungen.[127] In den SQL-Dialekten ist das DAC-Konzept über die Befehle GRANT und REVOKE verankert.

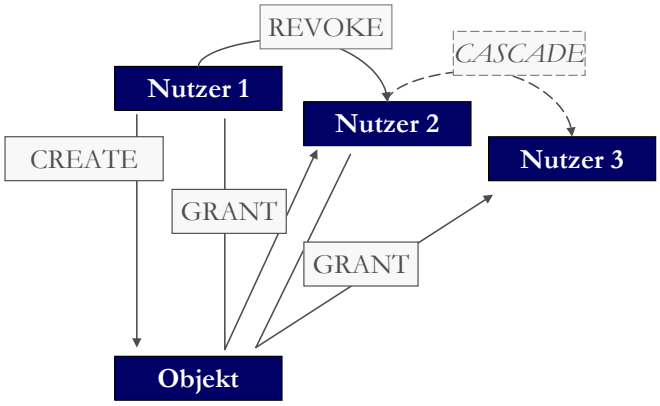


Abbildung 13: Beispiel für DAC
Eigene Darstellung

Werden die Rechte zentral verwaltet, so können lediglich wenige Superuser Berechtigungen erteilen und widerrufen. Das Gegenmodell ist die sog. „ownership administration“, in welcher der Ersteller oder „Besitzer“ eines Datenobjekts selbst anderen Benutzern die Berechtigung erteilen kann, Rechte auf dieses Objekt zu vergeben oder zu widerrufen (vgl. Abbildung 13). Einem Nutzer können Rechte eingeräumt werden, eine oder mehrere der

[125] Vgl. SANDHU ET AL. (1996), S. 39
[126] Vgl. GRIFFITHS/WADE (1976)
[127] Vgl. WIDOM/CERI (1996)

Operationen SELECT, INSERT, DELETE, UPDATE und DROP auf einem Objekt auszuführen. Innerhalb des Basismodells gilt eine „closed world policy", d.h. wenn einem Nutzer keine Rechte auf ein Objekt eingeräumt wurden, wird dies als Zugriffsverbot interpretiert. Da diese Vorgehensweise insofern problematisch ist, als sie nicht grundsätzlich verbietet, dass einem Nutzer bestimmte Rechte eingeräumt werden, wurde sie um das „denials-take-precedence"-Prinzip erweitert. Hier werden explizit Zugriffsverbote ausgesprochen, so dass die Erteilung des Zugriffsrechtes auf ein „verbotenes" Objekt unwirksam bleibt. Dieses Prinzip existiert in mehreren Abwandlungen.[128]

SANDHU (1993, S. 13f.) nennt als Hauptkritikpunkt die in DAC-Modellen mit dezentraler Berechtigungsvergabe fehlende Möglichkeit, das Kopieren von sensiblen Daten zu verhindern. Vergibt ein Nutzer das Leserecht an einem Objekt mit der Einschränkung, dass keine weiteren Autorisierungen auf dieses Objekt erfolgen dürfen,[129] kann der neu autorisierte Nutzer stattdessen die Daten in ein neues, von ihm selbst erstelltes Objekt kopieren („Copy-of-Private"[130]) und beliebigen anderen Nutzern Rechte darauf einräumen, ohne dass der ursprüngliche Besitzer dieser Daten dies verhindern kann oder überhaupt davon erfährt. Obwohl das DAC-Modell den Nutzern grundsätzlich Vertrauenswürdigkeit unterstellt, ist diese Lücke problematisch, da sie von Schad- bzw. Spionagesoftware genutzt werden kann.

Ein weiteres spezielles Problem der DAC ist die Abwicklung des Rechteentzugs. Wird einem Nutzer das Zugriffsrecht für ein Objekt entzogen, so werden im „System R" allen Nutzern, denen durch den vormalig Berechtigten Rechte am Objekt erteilt wurden, ebenfalls alle Rechte entzogen (CASCADE in Abbildung 13).[131] Im Unternehmensumfeld kann dieser Mechanismus zu Problemen führen, wenn Mitarbeiter ihre Positionen wechseln und damit „alte" Rechte verlieren. Wechselt bspw. ein Produktions-Bereichsleiter aus Deutschland in die USA, so verlieren alle Mitarbeiter des deutschen Produktionsbereiches, denen durch ihn Rechte auf Objekte des deutschen Produktionssystems erteilt wurden, diese Rechte und müssen neu autorisiert werden. Als Lösung wurden nicht-

128 Vgl. BERTINO/SANDHU (2005), S. 6

129 "Strict DAC" erlaubt keine weitere Propagation von Zugriffsrechten. "Liberal DAC" lockert diese Beschränkung beispielsweise in der Form des „one-level grant" (A räumt B das Leserecht samt dem Recht, C Lesezugriff zu gewähren, ein. C kann nun Lesezugriff erhalten, nicht aber das Recht, diese weiterzugeben.), welche beliebig zu „n-level-grants" erweitert werden könnten [vgl. OSBORN/SANDHU/MUNAWER (2000), S. 99f.].

130 SANDHU (1993), S. 14

131 Vgl. GRIFFITHS/WADE (1976), S. 247

kaskadierende Entzugsmechanismen sowie rollen- (vgl. Abschnitt 4.2.4) statt personenbezogene Rechtevergabe vorgeschlagen. DAC leidet insgesamt darunter, dass der Kontext, in dem Rechte vergeben werden, nicht abbildbar ist. Darunter fallen bspw. zeitliche oder aufgabenbezogene Rechte bzw. Einschränkungen der Rechte für einen Nutzer.[132]

4.2.2 Mandatory Access Control

Im Modell der MAC werden Objekten und Nutzern bzw. Subjekten[133] Sicherheitsstufen[134] zugewiesen (vgl. Abbildung 14).[135] Zugriffsrechte werden erteilt, wenn der Abgleich der Sicherheitsstufen bestimmte Bedingungen erfüllt. Die beiden zu erfüllenden Grundprinzipien des Basismodells von BELL/LAPADULA sind „no read-up" – auch „simple-security property" genannt – und „no write-down" – auch „star property" genannt.[136] „No write-down" bedeutet, dass Nutzer nur Objekte modifizieren können, deren Sicherheitslevel über ihrem eigenen liegt. Ein „top-secret"[137]-klassifizierter Nutzer darf bspw. keine Daten der Stufe „unclassified" anlegen oder ändern. Auf diese Weise soll verhindert werden, dass „top-secret"-Daten absichtlich oder auch versehentlich in ein „unclassified"-Objekt kopiert oder geschrieben werden.

---

132 Vgl. BERTINO/SANDHU (2005), S. 6 für diesen und den vorangegangenen Satz

133 In der Literatur werden mitunter sowohl der (menschliche) Nutzer als auch ein vom Nutzer angestoßener Prozess, der auf ein Objekt zugreift, als „Subjekt" bezeichnet. Die vorliegende Arbeit folgt aus Gründen der Verständlichkeit und konzeptionellen Klarheit BELL/LAPADULA (1973a, S. 11) und SANDHU (1993, S. 12) in ihrer strikten Trennung zwischen Nutzern und Prozessen (Subjekten).

134 BELL/LAPADULA (1973a, S.12) weisen Objekten „classification levels", Nutzern und Subjekten „clearance levels" zu.

135 Vgl. BELL/LAPADULA (1973a), S. 12f.; FERRAIOLO/KUHN (1992), S. 556

136 Vgl. BELL/LAPADULA (1973b), S. 14f.

137 In den folgenden Beispielen wird die von BELL/LAPADULA (1973b) exemplarisch eingeführte Unterscheidung in die vier Sicherheitskategorien „top secret", „secret", „classified" und „unclassified" verwendet. Die in diesem Abschnitt zitierten Ansätze können zwar eine Vielzahl von Sicherheitsstufen berücksichtigen, jedoch folgen die Autoren der jeweiligen Artikel bei der Konstruktion ihrer Beispiele dieser (einfachen) Klassifikation. Zur besseren Übersichtlichkeit und Vergleichbarkeit wird diese de-facto Konvention auch in der vorliegenden Arbeit beibehalten.

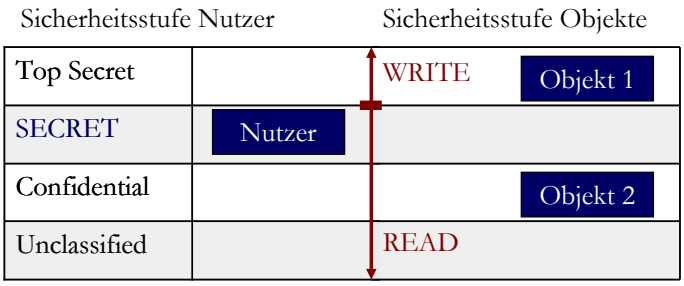


Abbildung 14: Beispiel für MAC
Eigene Darstellung

SANDHU argumentiert in Übereinstimmung mit dem DAC-Prinzip, menschlichen Nutzern sei grundsätzlich Vertrauen entgegenzubringen, so dass die „no write-down"-Regel hauptsächlich für Subjekte relevant sei, da diese Schadprogramme wie trojanische Pferde beinhalten könnten.[138] Weiterhin ergibt sich das Problem, dass „unclassified" Nutzer „top-secret"-Daten modifizieren oder sogar löschen können. Dies kann verhindert werden, indem Modifikationsrechte nur auf Objekte derselben Sicherheitsstufe wie die des Nutzers vergeben werden, oder indem Modifikationsrechte separat vergeben werden, so dass „append only" beispielsweise für Objekte höherer Sicherheitsstufen zulässig ist, „delete" und „create" jedoch unzulässig.[139] Dies eröffnet die Möglichkeit von „covert channels", indem durch die Verweigerung des Anlegens, Löschens oder der Bearbeitung eines Objektes der Nutzer Kenntnis von der Existenz eines schützenswerten Objektes erhält (vgl. auch die Ausführungen im folgenden Absatz und in Abschnitt 4.2.3).

Im Datenbankenumfeld führte die Implementierung von MAC zur Notwendigkeit, Mehrebenenmodelle in relationalen Datenbanken („multi-level secure databases", MLS) zu verwenden. LUNT ET AL. beschäftigen sich im Rahmen ihres „Sea View"-Modells ausführlich mit den damit einhergehenden Problemen, insbesondere der Polyinstanziierung.[140] Wird einem „unclassified" Nutzer bspw. nicht gestattet, einen Datensatz in einer Tabelle anzulegen, auf die er eigentlich Zugriff hat, so ist daraus erkenntlich, dass es einen Datensatz mit höherer Sicherheitsstufe gibt. Um diesen ungewollten Informationsfluss zu vermeiden, sollte dem Nutzer gestattet werden, einen „unclassified" Datensatz mit demselben Primärschlüssel anzulegen. Im ungünstigsten Fall könnte somit für jedes Tupel eine Instanziierung pro Sicherheitsstufe existieren.[141] Die eindeutige Identifizierung von

138 Vgl. SANDHU (1993), S. 14
139 Vgl. ebenda, S. 14f.
140 Vgl. LUNT ET AL. (1990)
141 Vgl. ebenda, S. 597

Datensätzen im „Sea View"-Modell geschieht somit über die Kombination von Primärschlüssel und Sicherheitsstufe.[142] Falls das zugrunde liegende Modell erlaubt, Tupel mit Attributen verschiedener Sicherheitsstufen auszustatten, kann die Polyinstanziierung über verschiedene Sicherheitsstufen Integritätsbedingungen verletzen. Da die Implementierung von Mechanismen, welche dies verhindern, äußerst aufwendig ist, fand diese MAC-Abwandlung wenig Resonanz in kommerziellen Lösungen.[143] Das „Sea View"-Modell wurde jedoch in der Forschung gut rezipiert und stetig weiterentwickelt. JAJODIA/SANDHU befassten sich mit der Problematik der massenhaften Generierung neuer Tupel nach Update-Operationen, welche aufgrund der Polyinstanziierung zur Sicherstellung der Datenintegrität notwendig sind.[144] SMITH/WINSLETT (1992) analysieren die MLS-Datenbankmodelle von LUNT ET AL. (1990) und JAJODIA/SANDHU (1991) und identifizieren als Hauptkritikpunkte die Beschränkung auf Syntax unter völliger Vernachlässigung der Semantik – „what exactly users at each [security] level believe to be the state of the world"[145] – und die syntaktische Mehrdeutigkeit der Entitätsdefinitionen.[146]

BYUN/BERTINO/LI (2005) schlagen eine MLS-Abwandlung vor, die Zugriffe nicht mit Hilfe von Sicherheitsstufen steuert, sondern mit zweckbasierten Zugriffsregeln („Purpose-based Access Control"). In diesem Modell werden für jedes Set an Daten „intendierte Zwecke" hinterlegt, für welche diese Daten verwendet werden dürfen. Zugriff auf die Daten wird nur erteilt, wenn die „intendierten Zwecke" den „Zugriffszweck" beinhalten, der bspw. mit einer Query auf diese Daten assoziiert ist. Zugriffsverbote für bestimmte Zwecke können explizit spezifiziert werden. Sowohl intendierte Zwecke als auch Zugriffszwecke können in einer Hierarchie hinterlegt werden.[147] Problematisch an diesem Modell ist die Abfrage des Zugriffszweckes. BYUN/BERTINO/LI (2005) stellen drei Mechanismen vor: Erstens könnte der Nutzer den Zugriffszweck explizit in seiner Query nennen, zweitens könnten bestimmte Anwendungen nur mit bestimmten Zugriffszwecken assoziiert sein, und drittens könnte der Zugriffszweck dynamisch aus dem aktuellen Systemkontext (anfragender Nutzer bzw. Anwendung, Dateninhalt, Anfragezeit etc.) bestimmt werden.[148] Die zweite Alternative ist nicht sinnvoll, wenn Anwendungen existie-

142 Vgl. ebenda, S. 598
143 Vgl. BERTINO/BONATTI/FERRARI (2001), S. 9
144 Vgl. JAJODIA/SANDHU (1991); JAJODIA ET AL. (2001)
145 SMITH/WINSLETT (1992), S. 205
146 Vgl. ebenda
147 Vgl. ebenda, S. 3f. für den vorhergehenden Absatz
148 Vgl. ebenda, S. 5

ren, die mit mehreren Zwecken assoziiert sind, so dass sich die gewünschte Zugriffsbeschränkung eigentlich erst aus der Kombination (Nutzer, Anwendung) ergibt. Die dritte Alternative setzt ein Mapping einer Vielzahl von Systeminformationen auf einzelne Zugriffszwecke voraus, das einen beträchtlichen Implementierungs- und Verwaltungsaufwand impliziert. BYUN/BERTINO/LI (2005) entwickeln daher eine SQL-Erweiterung für eine experimentelle Implementierung der ersten Möglichkeit.[149]

Einige kommerzielle DBMS implementieren heute MAC (ORACLE bspw. die sog. „Label-based Access Control", LBAC) in einer Form, welche die Zuordnung von Sicherheits-Labels zu Objekten und Subjekten ermöglicht und zumindest das erste Prinzip von MAC, die „simple security property", unterstützt.[150]

4.2.3 Lattice-based Access Control

Im Modell des Lattice-based Access Control (LAC) werden Informationsflüsse zwischen Sicherheitsklassen untersucht.[151] Wie im vorher beschriebenen Modell der MAC wird jedem Objekt eine Sicherheitsstufe zugeordnet. Zusätzlich wird für jede Sicherheitsstufe festgelegt, zu welchen anderen Sicherheitsstufen Informationsflüsse zulässig sind, und welche Sicherheitsstufe Objekte erhalten, die aus einer Kombination von Objekten mit verschiedenen Sicherheitsstufen hervorgehen.[152] Ein Lattice-Modell ist sicher, wenn keine mögliche Sequenz von Abfragen auf die zugrunde liegende Datenbank einen unzulässigen Informationsfluss zwischen zwei Objekten (bzw. Sicherheitsstufen) ermöglicht.[153]

SANDHU (1993) beschreibt den Informationsfluss in einem erweiterten BELL-LAPADULA-Modell (BLP, vgl. auch Abschnitt 4.2.3) im Rahmen eines Lattice-Modells. Das BLP besteht aus einer DAC-Matrix und einer MAC-Sicherheitsrichtlinie: Einem Nutzer wird nur dann gestattet, eine Operation auf einem Objekt auszuführen, wenn er sowohl durch DAC wie auch durch MAC dafür autorisiert ist, wobei beide MAC-Grundprinzipien greifen.[154] SANDHU lockert die Annahme, dass Sicherheitsstufen von Objekten nicht geändert werden können, indem er die neue Regel einführt, dass nur Heraufstufungen durch einen

149 Vgl. ebenda
150 Vgl. RJAIBI/BIRD (2004), S. 1011; BERTINO/SANDHU (2005), S. 10; BHATTI/GAO/LI (2008), S. 203
151 Vgl. DENNING (1976); SANDHU (1993), S. 10
152 Vgl. DENNING (1976), S. 236–238
153 Vgl. SANDHU (1993), S. 237
154 Vgl. ebenda, S. 14f. für diesen und die vorhergehenden beiden Sätze

Nutzer auf derselben Sicherheitsstufe wie das betreffende Objekt erlaubt sind.[155] So wird sichergestellt, dass Informationsfluss von „oben" nach „unten" stattfindet. Wäre es beispielsweise einem „top-secret"-Nutzer erlaubt, ein „unclassified"-Objekt anzulegen und später heraufzustufen, so hätten „unclassified"-Nutzer in der Zwischenzeit Zugriff auf „top-secret"-Informationen; allein das „Verschwinden" von Objekten aus der Sicht von „unclassified"-Nutzern bedeutet, dass „unclassified"-Nutzer um die Existenz von Objekten über ihrer Sicherheitsstufe wissen oder sogar deren Inhalt kennen. SMITH/WINSLETT sowie SANDHU weisen darauf hin, dass MAC in seiner Grundform für das „covert channel"-Problem keine Lösung bietet.[156]

SANDHU zeigt für das BLP (vgl. Abschnitt 4.2.2) sowie für das Biba-Modell, welches das zur Sicherung der Vertraulichkeit entwickelte BLP auf ein Modell der Integritätssicherung uminterpretiert, dass beide mit Hilfe eines einzigen Lattice-Modells abgebildet werden können.[157] Im BLP-Modell ist die zulässige Informationsflussrichtung von unten (Low Security, λ_L) nach oben (High Security, λ_H), um die Vertraulichkeit der klassifizierten Objekte zu schützen. Im Biba-Modell hingegen liegt der Fokus auf der Sicherstellung der Integrität der Daten, so dass sich die zulässige Informationsflussrichtung umkehrt (von oben ω_H nach unten ω_L).[158] Tabelle 9 zeigt die Äquivalenz beider Modelle.

Sicherheitsstufen der Objekte

Sicherheitsstufen der Benutzer	$\lambda_L\,\omega_L$	$\lambda_L\,\omega_H$	$\lambda_H\,\omega_L$	$\lambda_H\,\omega_H$
$\lambda_L\,\omega_L$	rw	r	w	↱
$\lambda_L\,\omega_H$	w	rw	w	w
$\lambda_H\,\omega_L$	r	r	rw	r
$\lambda_H\,\omega_H$	↱	r	w	rw

Tabelle 9: Lattice-Modell des BLP und Biba-Modells
SANDHU (1993), S. 16

Neben dem Mapping der Zugriffsrechte in Lattice-Modellen ist auch die Abbildung der Objekte möglich, auf welche die Nutzer zugreifen bzw. deren Zugriff beschränkt werden soll. In Abschnitt 4.3 wird ein Lattice-Modell einer (statistischen) Datenbank verwendet, um Inferenzkontrollmechanismen zu beschreiben. Abschnitt 5.1.1. stellt ein Lattice-

155 Vgl. ebenda, S. 15
156 Vgl. SMITH/WINSLETT (1992), S. 199f.; SANDHU (1993), S. 15
157 Vgl. SANDHU (1993), S. 14–17
158 Vgl. ebenda

Modell zur Access Control in OLAP vor, das in Abschnitt 5.2 als Basis und zur Illustration der dort erörterten Inferenzkontrollverfahren dient.

4.2.4 Rollenbasierte Zugriffsmodelle

Maßgeblich für die Entwicklung von RBAC in den 1990ern war zum einen der Mangel an geeigneten Sicherheitskonzepten speziell für private Unternehmen, um die Vertraulichkeit und Integrität ihrer Datenbestände zu schützen.[159] Gleichzeitig suchten viele Organisationen nach Mitteln, den stark steigenden administrativen Aufwand für das Management von Zugriffsrechten zu verringern.[160] RBAC wurde als Lösung beider Probleme vorgeschlagen. Im Basismodell der RBAC werden Zugriffsrechte an Rollen vergeben, denen wiederum die einzelnen Nutzer zugeordnet sind (vgl. Abbildung 15).[161] Die Vergabe und der Entzug von Rechten werden so wesentlich vereinfacht: Wechselt ein Nutzer beispielsweise den Arbeitsplatz, so wird seine Zuordnung zur „alten" Rolle widerrufen und ihm wird die „neue" Rolle zugeteilt. De Rolle ist (im Idealfall) genau das Bündel an Berechtigungen zugewiesen, welches der Nutzer für die Erledigung seiner Aufgaben in der Organisation benötigt. Die Zugriffsrechte werden aktiviert, wenn ein Nutzer (in einer oder mehreren Rollen) eine Session startet.[162] (OSBORN/SANDHU/MUNAWER (2000) zeigen, dass sowohl MAC als auch DAC durch RBAC abgebildet werden können.)

159 Vgl. FERRAIOLO/KUHN (1992), S. 555f.
160 Vgl. SANDHU ET AL. (1996), S. 2; FERRAIOLO/KUHN (1992), S. 555–558; OH/PARK (2001)
161 Vgl. SANDHU ET AL. (1996), S. 1
162 Vgl. BERTINO/SANDHU (2005), S. 8; SANDHU ET AL. (1996), S. 1f.

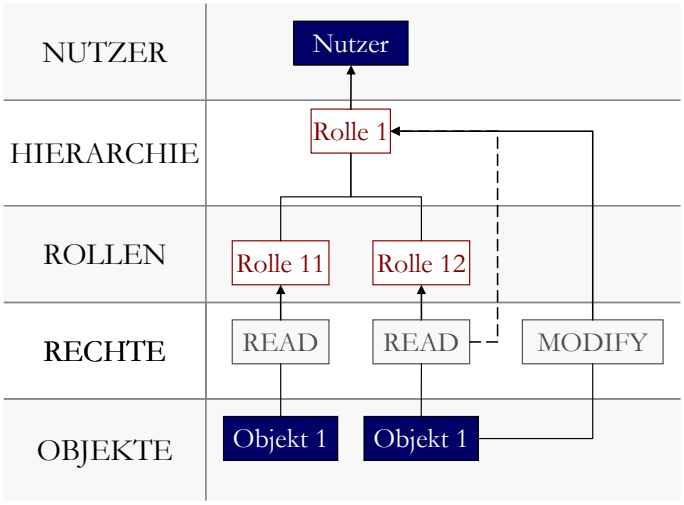


Abbildung 15: Beispiel für RBAC
Eigene Darstellung

RBAC unterstützt die Sicherheitsprinzipien „Least Privilege", „Separation of Duties" und „Data Abstraction". Das Prinzip „Least Privilege" bildet die Forderung ab, dass kein Nutzer mehr Rechte erhält als für die Erledigung seiner Aufgaben absolut notwendig ist, und kann über die Zuordnung „minimaler" Rechtebündel zu den einzelnen Rollen realisiert werden. „Data Abstraction" beschreibt die Möglichkeit, in RBAC Rechte für bestimmte Transaktionen statt für die reinen Schreib- und Leserechte des operativen Systems zu erteilen,[163] wie bspw. die abstrakte Berechtigung „Kunde anlegen" statt „Schreibzugriff auf Tabellen XYZ". „Separation of Duties" (SoD) bezeichnet die Forderung nach personell getrennten Zuständigkeiten, um Betrug zu verhindern. Für RBAC bedeutet dies, dass bestimmte Rollen nicht gleichzeitig denselben Personen zugeordnet werden dürfen. Statische SoD ist zwar relativ problemlos zu implementieren, erlegt den Nutzern eines Systems jedoch sehr starre Regeln auf, die realen organisatorischen Gegebenheiten nicht immer entsprechen. Dynamische SoD wird daher von den Anwendern präferiert, stellt aber eine größere Herausforderung dar, da sie nur zur Laufzeit möglich ist.[164] Will ein Unternehmen beispielsweise sicherstellen, dass Rabatte nur nach Abstimmung des lokalen Verkaufsleiters und des zuständigen Bereichsleiters im Verkauf gewährt werden, könnte statische SoD folgendermaßen aussehen: Der Rolle „Sales Manager" wird das Recht „Rabatt eintragen" und der Rolle „Division Manager" das Recht „Rabatt zustimmen" eingeräumt. Sofern der Bereichsleiter gleichzeitig auch seinen eigenen (lokalen) Verkaufsbereich besitzt, ist statische SoD für dieses Unternehmen unbrauchbar. Mittels dynamischer SoD

[163] Vgl. SANDHU ET AL. (1996), S. 3 für diesen und die vorangegangenen beiden Sätze
[164] Vgl. FERRAIOLO/KUHN (1992), S. 555–560 für diesen und die vorangegangenen beiden Sätze

hingegen könnte dafür gesorgt werden, dass der Bereichsleiter in seinen zwei Rollen die Transaktion nicht gleichzeitig anstoßen und genehmigen kann. Beispielsweise könnte die Zustimmungspflicht zur Rabattaktion an den stellvertretenden Bereichsleiter übergehen.[165] Eine ausführliche Diskussion von SoD in RBAC findet sich in KUHN (1997).

4.2.4.1 Erweiterungen von RBAC: Administration

SANDHU/BHAMIDIPATI/MUNAWER (1999) entwickelten „Administrative RBAC" (ARBAC97), um durch die Organisation der System- und Nutzerverwaltung auf Basis von RBAC-Prinzipien die Realisierung des ursprünglich intendierten Nutzens von RBAC - nämlich die Verringerung des Administrationsaufwandes - auch in komplexen Umgebungen sicherzustellen. ARBAC97 besteht aus drei Komponenten, welche den Zuständigkeitsbereich verschiedener Administratoren widerspiegeln sollen: URA97 („User-Role Assignment"), PRA97 („Permission-Role Assignment") und RRA („Role-Role Assignment").[166]

URA97 definiert die Zulässigkeit von GRANT- und REVOKE-Operationen in Abhängigkeit der Rolle eines Administrators neu – angenommen, dass eine Rollenhierarchie innerhalb der Administration besteht.[167] Würden diese Operationen lediglich nach DAC-Logik beschränkt, so wäre der für eine Rolle zuständige Administrator der Besitzer dieser Rolle und könnte sie beliebig vergeben und entziehen, ihr Rechte hinzufügen oder entziehen sowie ihren Platz in der Rollenhierarchie ändern.[168] Durch die Definition einer administrativen Rollenhierarchie, welche für „User-Role Assignments" zuständig ist, kann die Universalität der DAC-Rechte sinnvoll eingeschränkt und die Definition rollen- und nutzerbezogener Constraints vereinfacht werden.[169] Dies eliminiert den bei Administratoren besonders gravierenden Nachteil des kaskadierenden Rechteentzugs in DAC, da Berechtigungen nicht mehr direkt mit der Person des Administrators, sondern mit seiner Rolle verknüpft sind, welche auch bei einem Wechsel des Mitarbeiters ihre Berechtigungen zur Rechteerteilung behält.[170]

---

165 Vgl. SANDHU ET AL. (1996), S. 40; BERTINO/BONATTI/FERRARI (2001), S. 214
166 Vgl. SANDHU/BHAMIDIPATI/MUNAWER (1999), S. 107
167 Vgl. ebenda, S. 109-118
168 Vgl. ebenda, S. 110
169 Vgl. ebenda, S. 118f.
170 Vgl. ebenda, S. 118

Die zweite ARBAC97-Komponente, PRA97, wendet dieselbe Logik wie URA97 auf die Zuweisung von Berechtigungen zu Rollen an. Auch hier wird auf Basis der Rollenhierarchie in der (System-)Verwaltung festgelegt, welche (administrative) Rolle welche Berechtigungen an welche anderen Rollen vergeben darf.

Die dritte und letzte Komponente von ARBAC97 schließlich definiert die Zuordnung von Rollen untereinander. Zu diesem Zweck wird zwischen „abilities", „groups" und „UP-roles" („user and permission roles") unterschieden. „Abilities" beschreiben Mengen von Rechten, die einer Rolle in ihrer Gesamtheit zugeteilt werden müssen, damit die Nutzer dieser Rolle die ihnen zugedachten Aufgaben erledigen können. „Groups" sind das Gegenstück von „abilities" auf der Nutzerseite und beschreiben eine Menge von Nutzern, die einer Rolle gemeinsam zugeteilt werden. Durch die Definition solcher Rechtepakete und Nutzergruppen soll der Administrationsaufwand gesenkt werden.[171] Den „UP-Roles" schließlich können sowohl Rechte als auch Nutzer zugeteilt werden, d.h. sie bilden die eigentlichen Nutzer-Rechte-Beziehungen ab und sind somit das „Herzstück" von RRA97. Für „UP-Roles" wie für die anderen beiden Arten von Rollen können Hierarchien definiert werden, wobei die „UP-Roles" übergeordnete Hierarchieknoten darstellen, um eine widerspruchsfreie Abbildung von nutzer- und rechtebezogenen Rollen zu ermöglichen.[172]

Schon in den frühen Veröffentlichungen zu RBAC wurde darauf hingewiesen, dass eine Vielzahl von (zusätzlichen) Bedingungen mittels Restriktionen abgebildet werden können.[173] Die in Abschnitt 4.2.4.2 vorgestellten Erweiterungen von RBAC nutzen diese Möglichkeit, um den Arbeitskontext (z.B. Zeit oder Aufgaben), für welchen eine Rolle vergeben wird, in das Modell zu integrieren. Allerdings unterstützen die meisten kommerziellen Datenbanken lediglich die „flache" Version von RBAC, d.h. Modelle ohne Rollenhierarchien oder Restriktionen.[174]

4.2.4.2 Erweiterungen von RBAC: Berücksichtigung des Kontextes

Eine zeitbezogene Variation des RBAC ist unter der Abkürzung TRBAC bekannt (Temporal RBAC). Der Fokus liegt hier auf zeitlich bedingten Restriktionen, die in Form von Rollen-Triggern abgebildet werden. Diese können entweder periodisch zur (De-

171 Vgl. ebenda, S. 122 für den vorhergehenden Absatz
172 Vgl. ebenda, S. 123f. für diesen und den vorhergehenden Satz
173 Vgl. FERRAIOLO/KUHN (1992); SANDHU ET AL. (1996)
174 Vgl. BERTINO/SANDHU (2005), S. 8

)Aktivierung von Rollen führen oder bei der (De-)Aktivierung von Rollen ausgelöst werden, zwischen denen eine zeitliche Abhängigkeit existiert. Konflikte zwischen Triggern werden durch Prioritätsregeln gelöst.[175]

Trotz der Vereinfachung des Zugriffsrechte-Managements durch die Verwendung von Rollen als zentrale Bezugsobjekte ist der administrative Aufwand noch beträchtlich, wenn Änderungen der Daten-, Aufgaben- oder Unternehmensstruktur umgesetzt werden sollen. Mehrere Autoren schlagen daher ein aufgabenbezogenes RBAC („task-role-based access control", T-RBAC) vor, das die Rollen und Zugriffsrechte den einzelnen Aufgaben zuordnet.[176] OH/PARK argumentieren, dass sich durch den Wechsel des zentralen Bezugsobjektes der administrative Aufwand insofern verringere, als bei der Änderung oder Neueinführung einer Aufgabe automatisch allen zugeordneten Rollen die diesbezüglich definierten Zugriffsrechte zugeteilt werden. Die Aufgaben können wiederum nach ihren Charakteristika in verschiedene Klassen eingeteilt und Rollen verschiedener Hierarchiestufen zugeteilt werden, welche aufgabenbezogene Zugriffsrechte wiederum übergeordneten Rollen vererben können.[177] Um das Mapping der Unternehmensrealität auf T-RBAC zu vereinfachen und Implementierungs- sowie Administrationsaufwand weiter zu verringern, schlagen die Autoren einen mehrstufigen Modellierungsprozess unter Verwendung von Visualisierungstools vor.[178] Da T-RBAC allerdings die Identifikation aller Aufgaben in einem Unternehmen, die Zuordnung von Rechten zu diesen Aufgaben und zusätzlich von Aufgaben zu Rollen zu Nutzern verlangt, dürfte der Implementierungsaufwand bemerkenswert hoch sein. Möglicherweise auch wegen der mangelnden Unterstützung von Hierarchien (ein wesentlicher Bestandteil von T-RBAC) durch kommerzielle DBMS[179] ist dieser Ansatz bisher von geringer praktischer Relevanz.

4.2.5 Bewertung der Ansätze

Problematisch an DAC ist die unzureichende Absicherung der Daten gegen Angriffe und die unzureichenden Administrationsmöglichkeiten aufgrund der dezentralen Rechteverga-

175 Vgl. BERTINO/BONATTI/FERRARI (2001) für den vorhergehenden Absatz

176 Vgl. OH/PARK (2001), S. 923. In anderen Publikationen wurde eine ähnliche Variante aufgabenorientierter RBAC diskutiert; jedoch galt hierbei das Hauptaugenmerk der teamorientierten Zusammenarbeit [vgl. bspw. THOMAS (1997)].

177 Vgl. OH/PARK (2001), S. 925

178 Vgl. ebenda, S. 926f.

179 Vgl. BERTINO/SANDHU (2005), S. 8

be. Das von DAC implizierte Eigentum an Objekten liegt eigentlich beim Unternehmen und nicht beim Mitarbeiter, welcher die Daten angelegt hat.[180] MAC eliminiert diese Probleme; hier ist jedoch der hohe Aufwand problematisch, welcher bei der Administration der Sicherheitsrichtlinien entsteht, da sie für jeden Nutzer und jedes Objekt einzeln festgelegt werden müssen. Dies gilt insbesondere in dynamischen Umgebungen, in denen bspw. Nutzer den Arbeitsplatz oder das Aufgabenfeld häufig wechseln, Produktgruppen neu aufgenommen oder neue Kunden akquiriert werden. Das (ursprünglich im militärischen Umfeld entstandene) Konzept der Sicherheitsstufen in MAC findet oft keine einfache Entsprechung in der Unternehmenswelt.[181]

	Charakteristika	Hauptkritikpunkte
DAC		
	▶ Ownership-basiert ▶ Flexibel	▶ Niedriges Sicherheitslevel
MAC		
	▶ Verwaltungsbasiert ▶ Informationsflusskontrollen ▶ Sicherheitsstufen	▶ Niedrige Flexibilität ▶ Festlegung der Sicherheitsstufen schwierig
RBAC		
	▶ Policy-neutral ▶ Flexibel ▶ Hierarchien und Restriktionen ▶ Einfach implementierbar	▶ Unrealistisches Konzept der Rechtevererbung ▶ Keine Trennung von Aufgabe und Rolle ▶ Keine aktive Zugriffskontrolle

Tabelle 10: Vergleich von AC-Ansätzen
Eigene Darstellung nach OH/PARK (2001, S. 52)

Mit RBAC wurde ein Sicherheitskonzept entwickelt, das sowohl den kritischen Nachteil von DAC (mangelnde Absicherung gegen unzulässige Zugriffe) als auch den kritischen Nachteil von MAC (zu hoher administrativer Aufwand im Geschäftsumfeld) eliminieren sollte. Wie die empirischen Zahlen zu Akzeptanz von und Aufwandsreduktion durch RBAC[182] belegen, wurden diese Ziele teilweise erreicht. Auf gesamtwirtschaftlicher Ebene werden die Netto-Ersparnisse durch RBAC zwischen 1994 und 2009 auf 6 Milliarden US-Dollar geschätzt. 1992 hatten etwa 2,5% der befragten Unternehmen RBAC adaptiert, 2009 bereits über 40%.[183] Allerdings lässt sich an den Studienergebnisse gut erkennen, dass die Implementierung und Administration von RBAC immer noch mit beträchtlichen

180 Vgl. FERRAIOLO/KUHN (1992), S. 555–558
181 Vgl. ebenda
182 Vgl. O'CONNOR/LOOMIS (2010)
183 Vgl. ebenda, S. 77

Kosten verbunden sind und ein verbessertes Konzept zur RBAC-Administration vonnöten ist.[184]

OH/PARK (2001) stellen sowohl bei ARBAC als auch RBAC den fundamentalen Nachteil fest, dass Veränderungen in der Unternehmensstruktur oder dem Produktprogramm möglicherweise umfassende Änderungen im RBAC-Modell bedingen. Werden beispielsweise neue Produktlinien eingeführt, muss für jede Rolle festgelegt werden, inwiefern sie auf diese Produktlinie Zugriff haben soll, bzw. falls neue Rollen definiert werden, wie deren Beziehungen zu den bereits existierenden Rollen und ihr Platz in der Rollenhierarchie bestimmt sind.

4.2.6 Zuordnung der Berechtigungen

Die Frage, wie die Zuordnung von Zugriffsrechten zu Rollen oder Aufgaben tatsächlich durchgeführt werden sollte, wird i.d.Regel als „domänenspezifisch" bezeichnet und weitgehend offen gelassen. Ebenso ist die Automatisierung der Autorisierung von Nutzern oder Nutzergruppen für Abfragen in OLAP ein noch ungelöstes Problem.[185]

Unter der Annahme, dass Nutzer nur zu Abfragen berechtigt sein sollten, die sie im Kontext ihrer Arbeit benötigen, wird im folgenden Abschnitt die Frage diskutiert, wie sich der Arbeitskontext eines Nutzers so bestimmen lässt, dass der Verwaltungsaufwand für das Sicherheitskonzept im laufenden Betrieb möglichst niedrig ist. Für die in dieser Arbeit vorgeschlagene Lösung wird zunächst eine weitere Annahme getroffen: Der Arbeitskontext eines Nutzers lässt sich mittels der Dimensionen abbilden, welche im OLAP vorhanden sind. Beispielsweise könnte man den Arbeitskontext eines Sales Managers mit Produktgruppe und Region, für die er zuständig ist, beschreiben. Aus dieser Sichtweise ergibt sich die im Folgenden diskutierte Herausforderung, die „Position" eines Nutzers auf allen relevanten Dimension festzustellen, um ihm entsprechende Abfragen zu gestatten und andere, die „zu weit" von seinem Arbeitsgebiet entfernt sind, zu verbieten. Wollte der Sales Manager für „Laptops Deutschland" eines multinationalen Elektronikunternehmens beispielsweise eine Abfrage bezüglich des Gewinns im Bereich „Staubsauger Asien" absetzen, ergäben sich auf beiden Dimensionen relativ große Distanzen zwischen den Aus-

184 Vgl. ebenda, S. 67

185 Diese beiden Lücken weisen alle im Rahmen dieser Arbeit besprochenen Ansätze auf, mit Ausnahme von FUGKEAW/PIYAWIT/SEKPON (2009) [(vgl. Abschnitt 5.1.2)].

prägungen (Deutschland, Asien) und (Laptops, Staubsauger). Wollte unser Sales Manager hingegen die Absatzzahlen im Bereich „Tablet-PCs Deutschland“ oder „Desktop-Rechner Deutschland“ sehen, lägen die Ausprägungen einander näher. Ob die Anfrage gestattet würde, hinge noch davon ab, wie groß der Radius ist, innerhalb dessen der Sales Manager zur Ausführung von Abfragen berechtigt ist. Diese Festlegung ist sinnvollerweise in Abhängigkeit von den organisatorischen Gegebenheiten zu treffen. Ansätze zur Bestimmung dieses „Interessensbereiches“ sowie eine beispielhafte Implementierung dieses Ansatzes, welcher diese Mechanismen abbildet, werden in Kapitel 6 dargestellt.

4.3 Inferenzen und Inferenzkontrolle in Statistischen Datenbanken

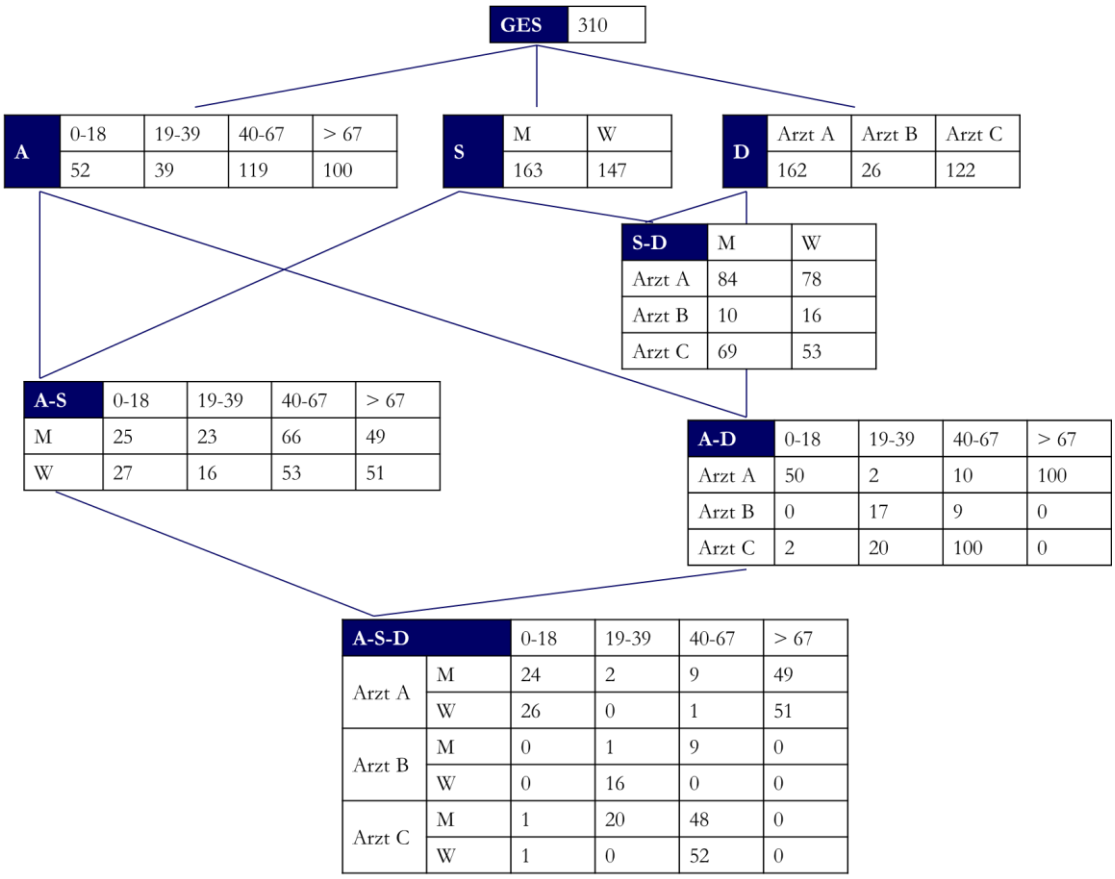
Statistische Datenbanken enthalten vornehmlich ökonometrische Daten und Zensus-Daten, die ursprünglich offline analysiert wurden; Hauptverwendungszweck von OLAP hingegen ist die interaktive Analyse von Geschäftsdaten, welche in der Regel in Data Warehouses vorgehalten werden.[186] Die im Folgenden erörterten Verfahren wurden ursprünglich für den Einsatz in statistischen Datenbanken entwickelt. Ihre Eignung für OLAP wird in Abschnitt 4.3.4 diskutiert. Abschnitt 5.2 stellt speziell für OLAP entwickelte Verfahren der Inferenzkontrolle vor.

DALENIUS schlug für die Verhinderung näherungweiser Disclosure in SDB aggregierte Zähldaten Restriktionen (vgl. Abschnitt 4.3.1) und Perturbationen (vgl. Abschnitt 4.3.2) als Lösungsmechanismen vor.[187] Restriktionsbasierte Mechanismen in SDB verhindern Inferenzen, indem unsichere Queries nicht ausgeführt werden bzw. ihr Ergebnis dem Nutzer nicht angezeigt wird. Perturbationsbasierte Methoden „verrauschen“ die zu schützenden Daten in einer Weise, dass die (statistischen) Kennzahlen der Population unverzerrt bleiben, Rückschlüsse auf die einzelnen Mitglieder der Population jedoch unmöglich gemacht werden.

Das Lattice-Modell des Informationsflusses in Datenbanken (vgl. Abschnitt 4.2.3) wird auch zur Beschreibung und Bewertung von Inferenzkontrollmechanismen herangezogen.

[186] Vgl. WANG/JAJODIA/WIJESEKERA (2007), S. 13
[187] Vgl. DALENIUS (1977), S. 441f.

Als Beispiel[188] ist in Tabelle 11 und Abbildung 16 die Datenbank eines Versicherungsunternehmens beschrieben, die für jeden Versicherten die Informationen (Alter AGE, Geschlecht SEX, Hausarzt DOC) enthält.



GES	310

A	0-18	19-39	40-67	> 67
	52	39	119	100

S	M	W
	163	147

D	Arzt A	Arzt B	Arzt C
	162	26	122

S-D	M	W
Arzt A	84	78
Arzt B	10	16
Arzt C	69	53

A-S	0-18	19-39	40-67	> 67
M	25	23	66	49
W	27	16	53	51

A-D	0-18	19-39	40-67	> 67
Arzt A	50	2	10	100
Arzt B	0	17	9	0
Arzt C	2	20	100	0

A-S-D		0-18	19-39	40-67	> 67
Arzt A	M	24	2	9	49
	W	26	0	1	51
Arzt B	M	0	1	9	0
	W	0	16	0	0
Arzt C	M	1	20	48	0
	W	1	0	52	0

Tabelle 11: Beispieltabellen im Lattice-Modell
Eigene Darstellung

Die höchste Dimension besitzt die Tabelle A-S-D, aus der durch Aggregationsoperationen (in diesem Fall SUM) über jeweils ein Attribut die drei zweidimensionalen Tabellen A-S, A-D und S-D errechnet werden können. Durch weitere Mikroaggregationen erhält man die drei eindimensionalen Tabellen A, S und D sowie die Tabelle GES der Dimension Null.

[188] Auf dieses an ADAM/WORTHMANN (1989, S. 524–553) angelehnte Beispiel zur Illustration von Inferenzkontrollmechanismen wird auch in den folgenden Abschnitten zurückgegriffen.

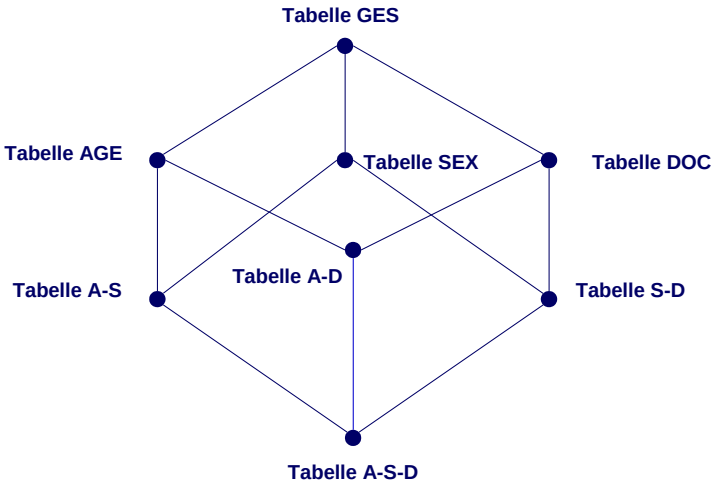


Abbildung 16: Beispielhafte Grafik des Lattice-Modells
Eigene Darstellung

Traditionell wird im Bereich SDB zwischen der Verwendung bzw. Veröffentlichung von Mikro- und Makrodaten unterschieden. Als Mikrodaten bezeichnet man eine Sammlung von Datensätzen, in der sich jeder Satz auf eine einzelne Entität bezieht.[189] Man geht mit Blick auf die Disclosure-Problematik davon aus, dass keine Attribute vorhanden sind, die einen direkten Rückschluss auf die zugehörige Entität zulassen. Die Gefahr der Zuordnung eines Datensatzes zu einer (bekannten) Entität besteht immer dann, wenn dieser Datensatz eine besonders seltene Ausprägung bei einem Attribut oder eine seltene Kombination von Ausprägungen der Attribute aufweist und dadurch ein indirekter Rückschluss möglich ist.[190] DALENIUS (1977, S. 433–435) unterscheidet statistische Disclosure hinsichtlich sechs Charakteristika:

- Art der Kennzahl S. Ist sie eine Mikro- oder Makro-Kennzahl?)
- Messskala, mit der S ausgedrückt wird. (z.B. Häufigkeiten)
- Direkt oder indirekt. Kann die Disclosure von D_K[191] direkt aus S abgelesen werden oder muss S zunächst in eine Kennzahl S' transformiert werden?
- Exakt oder näherungsweise. Kann der Wert von D^*_K exakt bestimmt werden oder kann lediglich das Intervall bzw. die Kategorie bestimmt werden, in die D^*_K fällt? Näherungsweise Disclosure kann weiterhin in „sicher" und „unsicher" unterschieden

[189] Vgl. DALENIUS (1977) S. 429f. für diesen und den vorhergehenden Satz
[190] Vgl. WILLENBORG/DE WAAL (1996), S. 4f. für diesen und die vorangegangenen beiden Sätze
[191] als D^*_K notiert, vgl. DALENIUS (1977), S. 434

werden, wobei unter „unsicher“ auch die probabilistische Approximation fällt: Hier wird die Wahrscheinlichkeit, mit der D^*_K in ein Intervall/eine Kategorie fällt, bestimmt.

- Extern oder intern. Ist es möglich, D^*_K zu berechnen, ohne Informationen über die Eigenschaft D^*_J eines anderen Objektes O_J desselben Sets (auf das sich S bezieht) zu besitzen, so spricht DALENIUS von externer Disclosure. Ist es hingegen möglich, bei Kenntnis von D^*_J zu einer besseren Approximation von D_K zu gelangen, so spricht man von interner Disclosure.
- S-basiert oder SxE-basiert. E bezeichnet „extra-objective data“[192], d.h. für den ursprünglichen Erhebungszweck unerhebliche und daher nicht explizit erfasste Daten.

Als Lösungsansätze für exakte Disclosure auf aggregierten (Makro-) Daten schlägt DALENIUS die Zusammenfassung schwach besetzter Klassen, die Verrauschung von Zellen sowie die Unterdrückung von Zellen vor.[193] Diese Ansätze werden im Folgenden kurz erläutert.

4.3.1 Restriktionsbasierte Inferenzkontrolle

Restriktionsbasierte Mechanismen in SDB verhindern Inferenzen, indem unsichere Queries nicht ausgeführt werden bzw. ihr Ergebnis dem Nutzer nicht angezeigt wird: Dem Nutzer werden also neben den sensiblen Daten weitere, an sich nicht-sensible Daten vorenthalten, deren Kenntnis jedoch Rückschlüsse auf den Inhalt der sensiblen Daten zuließe.[194] Hier ist ein Trade-Off zwischen den Forderungen „Sicherheit“ und „Zugänglichkeit“[195] oder auch „Disclosure Risk“ und „Data Utility“[196] direkt ersichtlich. Abbildung 17 veranschaulicht die Trade-Offs zwischen Kosten, Sicherheit und Zugänglichkeit für verschiedene Verfahren der Inferenzkontrolle.

192 ebenda, S. 432
193 Vgl. ebenda, S. 441
194 Vgl. DENNING/SCHLÖRER (1983), S. 72
195 Vgl. BERTINO/SANDHU (2005), S. 2; WANG/JAJODIA/WIJESEKERA (2007), S. 5
196 Vgl. DUNCAN/KELLER-MCNULTY/STOKES (2004)

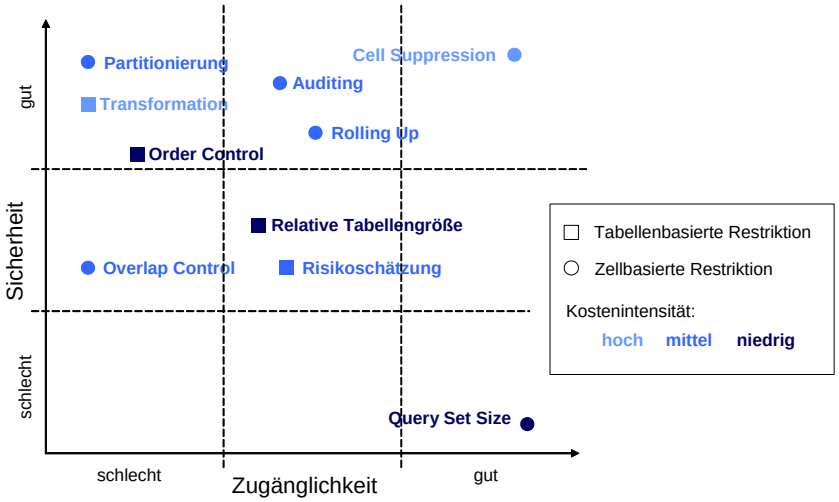


Abbildung 17: Trade-Offs verschiedener restriktionsbasierter Inferenzkontrollmechanismen
In Anlehnung an DENNING/SCHLÖRER *(1983), S. 78*

Ein erster Ansatzpunkt ist die Unterdrückung kompletter Tabellen, in denen sensible Zähldaten vorhanden sind. Im einfachsten Fall wird ein Parameter festgelegt, welcher die Anzahl an Attributen, d.h. die Dimensionalität der Ausgabetabelle, restringiert, welche durch eine Query zurückgeliefert werden darf.[197] Im Beispiel des Versicherungsunternehmens wäre bei der Festlegung der Dimensionalität 1 lediglich der Zugriff auf drei Tabellen erlaubt (vgl. Abbildung 18).

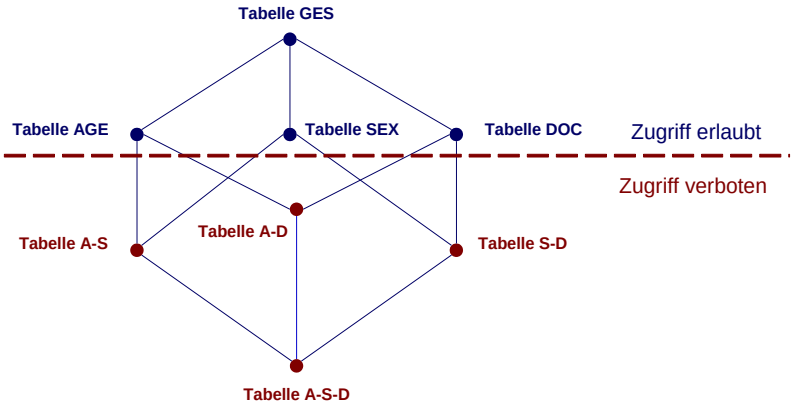


Abbildung 18: Tabellenbasierte Inferenzkontrolle
Eigene Darstellung

Da diese Maßnahme hinsichtlich der Implementierungskosten zwar vorteilhaft ist, jedoch offensichtlich unzureichend für eine signifikante Verringerung des Disclosure-Risikos in großen Tabellen, wurde die Größe der Tabelle als zusätzliches Kriterium für die Unterdrückung von Werten hinzugezogen: Eine Tabelle wird nur dann angezeigt, wenn die durchschnittliche Anzahl der zu aggregierenden Werte in jeder Zelle ein vorher festgeleg-

197 Vgl. DENNING/SCHLÖRER (1983), S. 72f.

tes Minimum übersteigt.[198] Die Datenbank des Versicherungsunternehmens enthält insgesamt 310 einzelne Einträge sowie drei Attribute (AGE, SEX, DOC) mit je (4, 2, 3) möglichen Ausprägungen. Angenommen, das Versicherungsunternehmen möchte nur Zugriffe auf Tabellen zulassen, deren durchschnittliche Besetzung pro Zelle 30 übersteigt, so werden folgende Tabellen für den Zugriff gesperrt (vgl. Abbildung 19):[199]

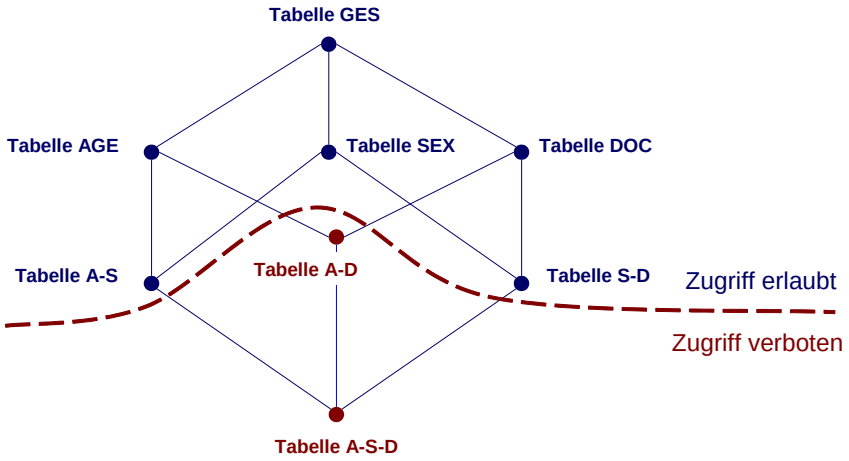


Abbildung 19: Tabellenbasierte Inferenzkontrolle II
Eigene Darstellung

Abgesehen davon, dass die Bestimmung eines geeigneten Wertes für den Restriktionsparameter schwierig ist, verhindert diese Methode auch keine Inferenzen in Tabellen mit ausreichend vielen Werten, und ist für andere Aggregationsoperationen als COUNT ungeeignet. Daher wurde die direkte Schätzung des Disclosure-Risikos auf Basis der Häufigkeitsverteilungen der Werte in der abgefragten Tabelle als Entscheidungsgrundlage für die Unterdrückung von Tabellen vorgeschlagen. Problematisch hierbei ist die Gleichbehandlung verschiedener Aggregationsoperationen, da diese einen unterschiedlich hohen Informationsgehalt haben: Beispielsweise ist eine Einschränkung der zulässigen Abfragen auf Basis des mit einer Zähloperation verknüpften Disclosure-Risiko für eine Summierungsoperation in der Regel nicht hinreichend restriktiv.[200] Möglichkeiten der Datentransformation wie die von DALENIUS/REISS vorgeschlagenen „Data Swaps“ in Kontingenztabellen[201] sind hauptsächlich für die Sicherung von Vertraulichkeit bei der Veröffentlichung von Mikrostatistiken außerhalb des Unternehmensumfeldes von Interesse, da die

198 Vgl. ebenda, S. 73

199 Das Verhältnis der Dimensionalität der Tabelle A-D (4*3) zur Größe der Datenbank (310) übersteigt den zulässigen Restriktionsparameter (0,039 > 0,033). Es ergeben sich durchschnittlich lediglich 25 Einträge pro Zelle statt der geforderten 30.

200 Vgl. ebenda, S. 73 für diesen und die vorhergehenden beiden Sätze

201 Vgl. DALENIUS/REISS (1982)

notwendige Modifikation der Basisdaten (Vertauschen mit z.B. zufällig generierten Werten, welche ungefähr dieselben statistischen Charakteristika aufweisen wie die Ursprungsdaten) für Geschäftsdaten nicht möglich ist.[202]

Da die Unterdrückung kompletter Tabellen zu einem starken Informationsverlust führt, werden Techniken bevorzugt, welche lediglich den Zugriff auf einzelne Zellen restringieren. Eine der ersten Entwicklungen auf diesem Gebiet basiert auf der Größe des Query Sets („Query Set Size Control") und soll Inferenzen verhindern, indem sehr große und sehr kleine[203] Ergebnismengen verboten werden.[204] Allerdings ist dieser Sicherheitsmechanismus relativ leicht mit sog. Trackern zu umgehen: Eine Menge von gerade ausreichend großen Queries, welche alle sensiblen Daten enthalten, wird abgegeben. Durch die Subtraktion der überflüssigen Daten voneinander erhält der Angreifer Zugriff auf die sensiblen Daten.[205]

Für das obige Beispiel wären – angenommen, die zulässige Query-Set-Größe sei auf 100 bis 210 Entitäten beschränkt[206] – Inferenzen mit folgenden Queries möglich, die das Set an weiblichen Versicherten als Tracker nutzen (vgl. Tabelle 12):

Q1	COUNT (sex = W)	**S1**	147
Q2	COUNT (sex = W AND (age = 35 AND sex = M AND doc = A))	**S2**	149
Q3	COUNT (sex = W AND (age = 35 AND sex = M AND doc = A AND leistungsart = Psychologische Behandlung))	**S3a**	147
		S3b	149

Tabelle 12: Beispielhafte Tracker-Abfragen
Eigene Darstellung

Q1 liefert das zulässige Set S1 zurück, Q2 das zulässige Set S2. Durch Subtraktion S2-S1 kann auf die Anzahl der von Arzt A behandelten Männer geschlossen werden. Liefert die zusätzliche Abfrage Q3 beispielsweise S3b zurück, so ist für beide Männer bekannt, dass sie eine psychologische Behandlung in Anspruch genommen haben (sog. negative Disclo-

202 Vgl. FIENBERG/MCINTYRE (2004), S. 520

203 Bei einer sog. "Single Query Attack" beispielsweise aggregiert ein Angreifer über eine Menge von Zellen, deren Wert er bereits kennt oder von der er weiß, dass sie (mit Ausnahme der geschützten Zelle) leer sind und kann so den Wert der geschützten Zelle inferieren [vgl. DENNING/SCHLÖRER (1983)].

204 Vgl. DENNING/SCHLÖRER (1983), S. 74

205 Vgl. ebenda

206 Für den Parameter K gilt $0 \leq K \leq L/2$, wobei L die Anzahl der Entitäten in der Datenbank beschreibt [vgl. DENNING/DENNING/SCHWARTZ (1979)]. Das zulässige Query-Set S wird durch $K \leq S \leq L\text{-}K$ beschränkt [vgl. HOFFMAN/MILLER (1970)].

sure).

Diesem Angriffsmechanismus soll durch die sog. „Overlap Control" begegnet werden, d.h. es werden nur Queries erlaubt, deren kombinierte Ergebnismengen keine Inferenzen ermöglichen.[207] Das Versicherungsunternehmen beispielsweise könnte die Inferenz dadurch verhindern, dass eine maximal zulässige Anzahl $r < 147$ überlappender Queries festgelegt wird. Query Sets S1 und S2, die 147 überlappende Entitäten enthalten, wären in diesem Fall unzulässig. Allerdings sinkt der Nutzen aus der Verwendung der SDB damit beträchtlich, da überlappende Queries häufig unabdingbar für die Analyse von Daten – bspw. die Überprüfung von Unterschiedshypothesen (Ausgaben für ärztliche Untersuchungen von Männern und Frauen bestimmter Altersgruppen im Unterschied zu den durchschnittlichen gesamten Ausgaben) – sind.

Audit-Modelle legen eine Query-Historie an und berechnen auf Basis der bereits abgefragten Daten, ob durch die aktuelle Query Inferenzen ermöglicht werden.[208] Das Verfahren „Audit-Expert"[209] basiert darauf, Tabellen zu linearen Gleichungssystemen umzuformen und mittels linearer Optimierung mögliche Inferenzen zu identifizieren (z.B. falls für einen unbekannten Wert nach Ausführung der Query lediglich eine zulässige Lösung existiert). Nachteile solcher Ansätze bestehen darin, dass nur exakte Inferenzen verhindert werden können, dass die Modelle typischerweise auf SUM-Aggregationen beschränkt sind, dass sie performanzbedingt nur auf relativ kleine Query-Sets angewendet werden können, und dass die Höhe des Informationsverlustes wesentlich von der Reihenfolge, in welcher die Queries gestellt werden, abhängt.[210]

Eine weitere Lösung für Inferenzkontrolle ist die sog. „Cell Suppression", die einzelne Zellen unterdrückt, wenn deren Veröffentlichung exakte oder näherungsweise Inferenzen ermöglicht.[211] Neben den Zellen, welche sensible Daten enthalten (sog. „primary compressions"), werden auch zusätzliche Zellen unterdrückt (sog. „complementary suppressions"). Nachteilig an dieser Lösung ist, dass die Auswirkungen dieser „complementary suppressions" auf den Informationsverlust gravierend sein können, und dass die Identifikation der zu unterdrückenden Zellen mit steigender Anzahl der Attribute immer schwie-

207 Vgl. ADAM/WORTHMANN (1989), S. 527
208 Vgl. CHIN/OZSOYOGLU (1982); MALVESTUTO/MEZZINI/MOSCARINI (2006)
209 Vgl. CHIN/OZSOYOGLU (1982)
210 Vgl. WANG/JAJODIA/WIJESEKERA (2007), S. 28–32
211 Vgl. COX (1980)

riger wird.[212] Zudem wurde diese Lösung für statische SDB entwickelt; je dynamischer eine Datenbank ist, desto häufiger müssen Neuberechnungen der zu unterdrückenden Zellen vorgenommen werden. ROBERTSON/ETHIER zeigen, dass Verfahren der Cell Suppression in zweierlei Hinsicht noch nicht hinreichend entwickelt sind: Die angewandten Unterdrückungsregeln sind häufig unzureichend, so dass sensible Informationen trotzdem veröffentlicht werden bzw. errechnet werden können. Gleichzeitig fehlt eine robuste Metrik, um den Informationsverlust durch Unterdrückung zu berechnen, so dass die relative Vorteilhaftigkeit verschiedener Unterdrückungsmuster kaum beurteilt werden kann.[213]

Das Versicherungsunternehmen beispielsweise könnte durch Cell Suppression Inferenzen verhindern, wenn es Tabelle A-D (AGE-DOC) veröffentlichen möchte. In Altersgruppe 0-18 beispielsweise hat Arzt C lediglich zwei Patienten. Durch eine einfache Abfrage auf die ungeschützte Tabelle A-S-D ist zu erfahren, dass ein Patient weiblich und ein Patient männlich ist. Ist einem Angreifer nun beispielsweise bekannt, dass einer der beiden Patienten eine schwangerschaftsbedingte Leistung in Anspruch genommen hat, ist die Zuordnung Patient-Leistung eindeutig möglich. Diese Information soll geschützt werden (vgl. Tabelle 13).

A-S-D		0-18	19-39	40-67	> 67
Arzt A	M	24	2	9	49
	W	26	0	**X**	51
Arzt B	M	0	**X**	9	0
	W	0	16	0	0
Arzt C	M	**X**	20	48	0
	W	**X**	0	52	0

Tabelle 13: Unsichere Cell Suppression auf Tabelle A-S-D
Eigene Darstellung

Es ist für einen Angreifer leicht ersichtlich, dass beide Zellen den Wert Eins enthalten, da weder Nullen noch Zweier unterdrückt werden und aus der Tabelle A-D hervorgeht, dass Arzt C zwei Patienten in dieser Altersgruppe hat. Zusätzlich müssen alle ähnlichen Konstellationen (Patienten von beiden Ärzten A und B in Altersgruppe 19-39; Patienten von Arzt A in Altersgruppe 40-67) ebenso unterdrückt werden wie alle weiteren kritischen altersbezogenen Daten (vgl. Tabelle 14).

[212] Vgl. DENNING/SCHLÖRER (1983), S. 75 für diesen und den vorhergehenden Satz
[213] Vgl. ROBERTSON/ETHIER (2006) für den vorhergehenden Absatz

A-S-D		0-18	19-39	40-67	> 67
Arzt A	M	**X**	**X**	**X**	49
	W	**X**	**X**	**X**	51
Arzt B	M	0	**X**	**X**	0
	W	0	**X**	**X**	0
Arzt C	M	**X**	**X**	48	0
	W	**X**	**X**	52	0

Tabelle 14: Sichere Cell Suppression auf Tabelle A-S-D
Eigene Darstellung

Eine andere Möglichkeit, Angreifer daran zu hindern, mit Eins besetzte Zellen zu identifizieren, ist die Zusammenfassung dieser Zellen mit anderen Zellen, welche Werte größer Eins enthalten.[214]

Als weitere A-Priori-Lösungen wurden Verfahren der Gruppierung (sog. „Rolling Up") und Partitionierung entwickelt. Gruppierungsverfahren verhindern Inferenzen durch die (hierarchisch strukturierte) Zusammenfassung von Attributen, z.B. durch eine Summierung sensibler und nicht-sensibler Daten, und das Verbot der Veröffentlichung der entsprechenden Mikrodaten.[215] Partitionierungsverfahren teilen die Daten auf Basis der Attribute in disjunkte Populationen, die mindestens zwei Objekte umfassen müssen. Populationen der Größe eins werden mit anderen Populationen zusammengefasst oder mit Dummy-Daten ergänzt. Abfragen sind nur auf diese Populationen oder auf Vereinigungen dieser Populationen erlaubt.[216]

Das Versicherungsunternehmen beispielsweise könnte auch durch Gruppierung Inferenzen verhindern, wenn es Tabelle A-D (AGE-DOC) veröffentlichen möchte (vgl. Tabelle 15).

214 Vgl. OZSOYOGLU/CHUNG (1986)
215 Vgl. DENNING/SCHLÖRER (1983), S. 76f.
216 Vgl. ebenda, S. 77

A-S-D		0-18	19-39	40-67	> 67
Arzt A	M	24	2	**10**	49
	W	26	0		51
Arzt B	M	0	**17**	9	0
	W	0		0	0
Arzt C	M	**2**	20	48	0
	W		0	52	0

Tabelle 15: Gruppierung auf Tabelle A-S-D
Eigene Darstellung

Aus Tabelle S-D (SEX-DOC) wird allerdings ersichtlich, dass Arzt C insgesamt 53 weibliche Patienten hat. Davon fallen 52 in die Altersgruppe 40-67 (vgl. Tabelle 16).

S-D	M	W
Arzt A	84	78
Arzt B	10	16
Arzt C	**122**	

Tabelle 16: Gruppierung auf Tabelle S-D
Eigene Darstellung

Um Inferenzen über die Tabelle S (SEX) zu verhindern, muss diese ebenfalls gruppiert werden, womit sie der Tabelle GES entspricht. Nach Gruppierung aller kritischen Attributkategorien können die Daten aus Abbildung 20[217] veröffentlicht werden.

[217] Alle gruppierten Attributwerte sind fett gekennzeichnet. Die effektiv ausgeblendeten Tabellen - der Inhalt von Tabelle A-S kann leicht aus Tabelle A errechnet werden - sind transparent kenntlich gemacht.

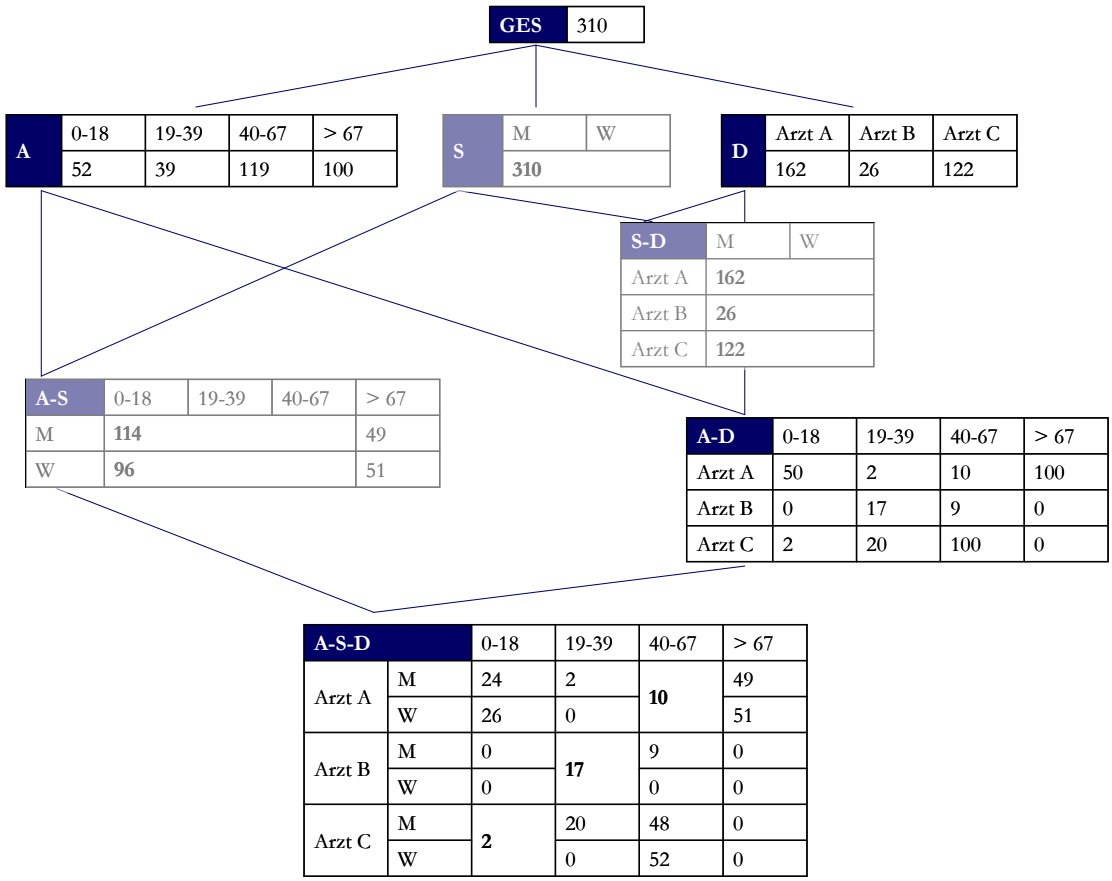


Abbildung 20: Gruppierung als Inferenzkontrollmechanismus
Eigene Darstellung

Ein Vergleich der Tabelle A-S-D nach Cell Suppression (vgl. Tabelle 14) und nach Gruppierung (vgl. Tabelle 15) zeigt, dass der Informationsverlust für das Versicherungsunternehmen auf der Stufe mit der geringsten Granularität wesentlich geringer ausfällt, wenn Gruppierung als Inferenzkontrollmechanismus gewählt wird. Auf den zweidimensionalen Tabellen jedoch ist der Informationsverlust bei Gruppierung erheblich, so dass hinsichtlich der möglichen Auswertungen, welche auf Basis der veröffentlichten Daten möglich sind, Cell Suppression der Vorzug zu geben ist.

4.3.2 Perturbationsbasierte Inferenzkontrolle

Perturbationsbasierte Methoden fügen den Datenstrukturen (Query-Ergebnissen oder den Quelldaten) Rauschen hinzu, um Inferenzen zu erschweren.[218] Auch perturbationsbasierte Methoden werden nach den Metriken Informationsverlust, Sicherheitsniveau und Implementierungskosten bzw. Performanzverlust beurteilt, wobei der Informationsverlust nun

[218] Vgl. DENNING/SCHLÖRER (1983), S. 77

nicht mehr anhand der Anzahl der unterdrückten Kennzahlen geschätzt wird, sondern anhand der Fehlervarianz in der perturbierten Kennzahl.[219] Die „Risk-Utility Confidentiality Map“ (vgl. Abbildung 21) illustriert den Trade-off zwischen dem Disclosure-Risiko und dem Informationsverlust für verschiedene Perturbationsverfahren.[220]

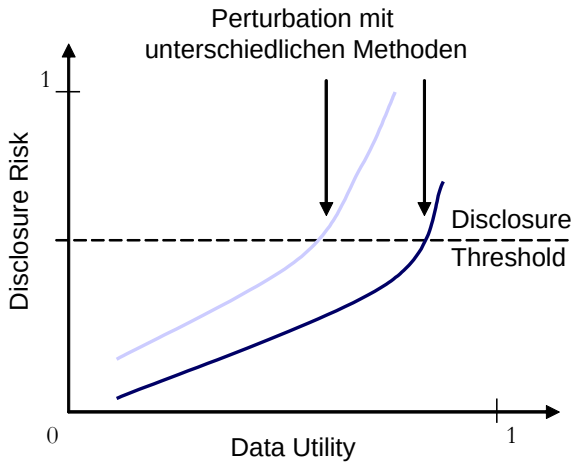


Abbildung 21: R-U Confidentiality Map
Eigene Darstellung nach DUNCAN/KELLER-MCNULTY/STOKES (2004)

Zwei weitere Kenngrößen sind bei der Beurteilung eines Perturbationsverfahrens von Interesse: Erstens sollte der Bias zwischen der „wahren“ Kennzahl und des Erwartungswertes ihrer perturbierten Schätzung möglichst klein sein, und zweitens sollten die Perturbationen nicht zu Inkonsistenzen in zurückgelieferten Kennzahlen führen. Neben dem unerwünschten Effekt, dass inkonsistente Ergebnisse die Verwendbarkeit der SDB stark einschränken, können sie Ansatzpunkte für Angreifer bilden, welche den Durchschnitt über eine Menge von Queries mit inkonsistenten Ergebnissen berechnen und so die „wahre“ Kennzahl schätzen können (sog. „Averaging“-Attacke).[221]

Datenbasierte Perturbation kann bspw. implementiert werden, indem eine Kennzahl nicht auf Basis des gesamten Query Sets, sondern einer Zufallsstichprobe aus dem Query Set berechnet wird. Da der Sampling-Fehler zufällig aus einer Verteilung mit Erwartungswert Null gezogen wird, ist das perturbierte Ergebnis insgesamt nicht verzerrt. Dies gilt allerdings nur für SUM-Operationen; zufällig perturbierte COUNT-Operationen können zu negativen Ergebnissen führen. Auch für andere Kennzahlen wie Korrelationskoeffizienten ist diese Methode ungeeignet. Es existieren Perturbationsverfahren sowohl für katego-

[219] Vgl. ADAM/WORTHMANN (1989), S. 534
[220] Vgl. DUNCAN/KELLER-MCNULTY/STOKES (2004)
[221] Vgl. bspw. DENNING/SCHLÖRER (1983), S. 77–80; ADAM/WORTHMANN (1989), S. 534f. für den vorhergehenden Absatz

riale wie für numerische Daten.[222]

Ergebnisbasierte Perturbation wird häufig mit Rundungsverfahren umgesetzt. Systematische Rundungsverfahren runden alle Kennzahlen auf einen festgelegten Parameter b oder auf ein festgelegtes Intervall. Der Einfachheit des Verfahrens steht der Nachteil gegenüber, dass sich potentiell viele Inkonsistenzen ergeben können.[223] In Tabelle 17 stimmt beispielsweise der in der Tabelle abgetragene gerundete Summenwert für die männlichen Patienten von Arzt A nicht mit der Summe der einzelnen gerundeten Werte überein. Allerdings würde eine Query auf diese Summe immer denselben Wert zurückliefern, so dass eine Averaging-Attacke wirkungslos bliebe. Das auf das Beispiel angewendete Verfahren berechnet sich mit Hilfe des Entscheidungsparameters $r = |C| \bmod b$[224]:

$$|C| = \begin{cases} |C| & \text{wenn } r = 0 \\ |C| - r & \text{wenn } r < (b+1)/2 \\ |C| + b - r & \text{wenn } r > (b+1)/2 \end{cases}$$

Zufälliges Runden verändert die Formel lediglich insofern, als Auf- bzw. Abrundung jeweils mit einer Wahrscheinlichkeit (in Abhängigkeit von r und b) versehen werden.[225]

A-S-D		0-18	19-39	40-67	> 67	♦
Arzt A	M	**25**	**5**	**10**	**50**	**85**
	W	**25**	0	**0**	**50**	**80**
Arzt B	M	0	**0**	**10**	0	10
	W	0	**15**	0	0	**15**
Arzt C	M	**0**	20	**50**	0	**70**
	W	**0**	0	**50**	0	**55**
♦		**50**	**40**	**120**	100	310

Tabelle 17: Systematische Rundung von Tabelle A-S-D (b=5)
Eigene Darstellung

Die Sicherheit des Rundens wird erhöht, wenn statt einzelner Werte gerundete Intervalle (sog. „Range Rounding“) berechnet und dem Nutzer zurückgeliefert werden. Eine sehr einfache Möglichkeit des systematischen Range Rounding (vgl. Tabelle 18) besteht darin, zunächst eine Rundung wie eben dargestellt durchzuführen; es wird jedoch immer auf den

222 Vgl. DENNING/SCHLÖRER (1983), S. 77 für den vorhergehenden Absatz
223 Vgl. ADAM/WORTHMANN (1989), S. 542f. für diesen und die vorhergehenden beiden Sätze
224 Vgl. ebenda für diesen und den vorhergehenden Satz
225 Vgl. ebenda, S. 542

niedrigeren Wert gerundet. Anschließend wird der Rundungsparameter addiert und 1 subtrahiert, um die obere Intervallgrenze zu errechnen. Hierfür könnten beliebig komplizierte Funktionen verwendet werden.[226]

A-S-D		0-18	19-39	40-67	> 67	♦
Arzt A	M	[20,24]	[0,4]	[5,9]	[45,49]	[80,84]
	W	[25,29]	[0,4]	[0,4]	[50,54]	[75,79]
Arzt B	M	[0,4]	[0,4]	[5,9]	[0,4]	[10,14]
	W	[0,4]	[15,19]	[0,4]	[0,4]	[15,19]
Arzt C	M	[0,4]	[20,24]	[45,49]	[0,4]	[65,69]
	W	[0,4]	[0,4]	[50,54]	[0,4]	[50,54]
♦		[50,54]	[35,39]	[115,119]	[100,104]	[310,314]

Tabelle 18: Systematische Range-Rundung von Tabelle A-S-D
Eigene Darstellung

Eine Rundungsmethode, welche das Problem der inkonsistenten Randsummen löst, ist das kontrollierte Runden („Controlled Rounding"). Die Rundung der Zellwerte erfolgt – wie im Fall der systematischen Rundung – zu einem bestimmten Parameter. Die gerundeten Werte und Randsummen werden mit Hilfe iterativer Verfahren (im Falle höherdimensionaler Tabellen bspw. Simulated Annealing oder Mixed Integer Programming) bestimmt, so dass eine Summierung über die gerundeten Zellwerte den Randsummen entspricht.[227]

Weitere Methoden der ergebnisbasierten Perturbation umfassen beispielsweise die „Varying Output Perturbation"[228], welche auf Basis von summierten Zufallsvariablen die Ergebniswerte der Query perturbieren. In variierenden Abständen werden neue Zufallsvariablen gezogen, so dass aufeinander folgende Ziehungen hoch miteinander korrelieren und eine sehr große Anzahl an Queries notwendig ist, bis ein Angreifer aus den Differenzen zwischen den Ergebnissen Inferenzen ableiten kann.[229]

4.3.3 Gaps

Einen bisher wenig untersuchten Spezialfall von Inferenzen stellen Wertebereichslücken, so genannte „Gaps", dar. Ist die Domäne einer Kennzahl vom Typ Integer, kann auf Ba-

226 Vgl. DENNING/SCHLÖRER (1983), S. 80
227 Vgl. WILLENBORG/DE WAAL (2001), S. 225–239 für den vorhergehenden Absatz
228 Vgl. BECK (1980)
229 Vgl. ADAM/WORTHMANN (1989)

sis der veröffentlichten Daten deren potentieller Wert in einer unterdrückten Würfelzelle ggf. auf bestimmte Wertebereiche (oder bestimmte einzelne Werte) im Rahmen eines größeren Intervalls geschätzt werden. Die Wertebereiche (oder die einzelnen Werte), die zwischen diesen Schätzwerten liegen und für die angegriffene Würfelzelle ausgeschlossen werden können, bezeichnet man als „Gaps". Alle bekannten Untersuchungen zu Gaps beziehen sich auf die ausschließliche Offenlegung von Aggregaten. Der Begriff Gap hat seinen Ursprung darin, dass im SDB-Bereich Schätzintervalle eines Angreifers auch für Daten des Typs Integer mit linearen Programmen approximiert werden, da das eigentliche Problem, also die Bestimmung exakter Wertebereiche für eine ganzzahlige Variable, im Allgemeinen NP-schwer ist. Innerhalb der approximierten oberen und unteren Schranken liegen dann ggf. Gaps, die ein Schätzintervall von vermeintlich ausreichender Größe inakzeptabel verkleinern können.[230]

Als sehr anschauliches Beispiel sei hier die Veröffentlichung von Unternehmensdaten genannt, die einen (überraschend) präzisen Rückschluss auf die Basisdaten zulassen. Ein Unternehmen legt offen, dass trotz schwerer Krise ¾ seiner Verkaufseinheiten im Inland (absolute Anzahl v_{I+}) und ⅓ seiner Verkaufseinheiten im Ausland (absolute Anzahl v_{A+}) profitabel gearbeitet haben. Es ist weiterhin bekannt, dass das Unternehmen 29 Verkaufsorganisationen umfasst.

$$\begin{pmatrix} v_{I+} & v_{A+} \\ v_{I-} & v_{A-} \end{pmatrix};\ \frac{v_{I+}}{v_{**}} = \frac{3}{4}\ ;\ \frac{v_{A+}}{v_{**}} = \frac{1}{3}\ ;\ v_{**} = 29$$

Schätzt man nun den möglichen Wertebereich für die absolute Anzahl der Verkaufsorganisationen im Inland, die profitabel gearbeitet haben (v_{I+}), mittels eines linearen Programms, erhält man das Ergebnis $0 \leq v_{I+} \leq 21{,}75$. Angesichts von nur 29 Verkaufsorganisationen insgesamt ist dies im Hinblick auf die Sicherheit vermutlich ein akzeptables Schätzintervall. Eine genauere Schätzung mittels eines linearen ganzzahligen Optimierungsproblems liefert das präzisere Ergebnis $6 \leq v_{I+} \leq 15$ und damit ein Intervall der Breite 9, was ebenfalls vermutlich annehmbar wäre.

Abbildung 22: Beispiel für Gaps bzgl. v_{I+}
Eigene Darstellung

Tatsächlich kann jedoch mit Methoden des Integer Programmings berechnet und auf-

[230] Vgl. SULLIVANT (2005), S. 787 für diesen und die beiden vorangegangenen Sätze

grund der kleinen Zahlen hier leicht nachvollzogen werden, dass v_{I+} nur zwei Werte annehmen kann, so dass gilt $v_{I+} \in \{6, 15\}$.

$$\begin{pmatrix} v_{I+} & v_{A+} \\ v_{I-} & v_{A-} \end{pmatrix} = \begin{pmatrix} 6 & 7 \\ 2 & 14 \end{pmatrix} \textit{ oder } \begin{pmatrix} 15 & 3 \\ 5 & 6 \end{pmatrix}$$

Alle anderen Werte lassen sich entsprechend erschließen. Es ergeben sich auf Basis der veröffentlichten Daten demnach nur die zwei oben dargestellten Varianten für die zugrunde liegende Matrix.

4.3.4 Bewertung der Ansätze

Der Einsatz von Audit-Modellen in OLAP ist aus drei Gründen kritisch zu sehen. Erstens ist die Anzahl möglicher Queries i.d.Regel so groß, dass die Berechnung möglicher Inferenzen durch potentiell folgende Queries die Performanz des Systems unzumutbar einschränkt. Zweitens hängt die Zulässigkeit von Abfragen von der Query-Historie ab, so dass ein Nutzer, der mit der „falschen" Query anfängt, möglicherweise eine starke Einschränkung seiner Ergebnismengen hinnehmen muss. Falls die Query-Historie nicht permanent gespeichert wird[231], kann der Fall eintreten, dass ein Nutzer die Daten, die er vor Löschung der Query-Historie (z.B. am Vortag) noch sehen durfte, aufgrund eines anderen Verlaufes seiner neu angelegten Query-Historie nicht mehr sehen darf. Neben der dadurch bedingten schlechteren Usability des OLAP-Systems ergibt sich hier die Möglichkeit für einen Angreifer, nach Löschung der Query-Historie die für eine Inferenz noch fehlende (nunmehr erlaubte) Query bzw. Query-Sequenz auszuführen. Drittens ergibt sich speziell in OLAP-Systemen eine sinnvolle Query-Folge häufig erst auf Grundlage der Erkenntnisse aus den vorherigen Queries. Der sich ergebende Analysefluss wird durch Audit-Modelle i.d.Regel verhindert.[232] Stellt beispielsweise ein Analyst des Versicherungsunternehmens fest, dass einer der Ärzte in der Region nur einen einzigen Patientenbesuch zu verzeichnen hat, so müsste die Query, welche Leistungsarten dieser Arzt anbietet, verboten werden, wenn der Analyst vorher bereits die Verteilung der Patienten nach Geschlecht auf die einzelnen Ärzte in der Region abgefragt hatte und das Ergebnis dieser Query „eine weibliche Patientin" war: Damit könnte sich eine Zuordnung der weiblichen

[231] Diese Alternative ist nicht zu empfehlen, da sie die Flexibilität und Interaktivität des OLAP-Systems entweder unzumutbar einschränkt oder zu sehr lockeren Restriktionen im Audit Expert führen muss, was wiederum zu einer schlechten Absicherung des Systems führt.

[232] Vgl. WANG/JAJODIA/WIJESEKERA (2007), S. 44

Patientin zu der Leistungsart „schwangerschaftsbezogene Leistungen“ herstellen lassen.

Beim Einsatz intervallbasierter Inferenzkontrollmechanismen in OLAP bestehen folgende Disclosure-Risiken:[233]

- Die Existenz eines Wertes kann abgeleitet werden, wenn die untere Grenze größer Null ist.
- Die untere Grenze für einen Wert kann zu Upward-Disclosure führen.
- Analog kann die obere Grenze für einen Wert Downward-Disclosure ermöglichen.
- Approximative Disclosure ist möglich, wenn das Intervall klein genug gewählt wird.

Das grundsätzliche Problem pertubationsbasierter Inferenzkontrollmechanismen liegt darin, dass Nutzer in OLAP im Unterschied zu Anwendern statistischer strukturentdeckender Verfahren (z.B. zur Klassifikation oder Mustererkennung) weniger auf Basis von Verteilungen arbeiten, sondern häufiger Aggregationsoperationen auf großen, überlappenden Wertemengen ausführen.[234] Während die aus der Perturbation der Einzelwerte resultierende Ergebnisungenauigkeit möglicherweise für den Anwender in SDB oder von Data Mining-Verfahren unkritisch ist, kann sie die Nützlichkeit von OLAP durch die Beeinträchtigung der Korrektheit und Konsistenz der Daten unzumutbar einschränken und sogar zu (geschäftskritischen) Fehlentscheidungen führen (vgl. Kapitel 3). Aus diesem Grund werden perturbationsbasierte Verfahren im Weiteren nicht betrachtet.

[233] Vgl. KEMPER/UNGER/MEHANNA (2006), S. 92

[234] Vgl. WANG/JAJODIA/WIJESEKERA (2007), S. 22

5 DISCLOSURE IN OLAP

Zwei eminent wichtige Ansätze zur Disclosure Limitation in OLAP sind Zugriffskontrolle und Inferenzkontrolle.[235] In Abschnitt 4.2 wurden verschiedene Konzepte der Zugriffskontrolle in Datenbanken diskutiert. Diese Konzepte müssen für die Anwendung in OLAP adaptiert werden: Die „klassischen" Zugriffskontrollmechanismen für Datenbanken implizieren ein „flaches" Datenmodell, wohingegen OLAP ein multidimensionales Cube-Modell zugrunde liegt (vgl. Abschnitt 2.2), d.h. dass sinnvolle neue Autorisierungsobjekte definiert werden müssen.[236] Zudem ist in OLAP meist nur die Leseberechtigung von Interesse, wohingegen in Datenbanken mindestens zwischen Berechtigungen für Lese- und Schreiboperationen unterschieden werden muss (vgl. Abschnitt 2.1). Eine weitere OLAP-spezifische Anforderung ist die Schnelligkeit, mit der das System die Antwort auf eine Query zurückliefert (vgl. Abschnitt 2.1). Für Offline-Anwendung entwickelte Inferenzkontrollverfahren sind daher in der Regel eher ungeeignet für den Einsatz in OLAP; dies gilt auch für Verfahren, deren Rechenzeiten proportional zum Query Set wachsen.[237]

Im Unterschied zu Data Mining, welches bereits ein regel- oder musterbasiertes Modell des zu untersuchenden Realitätsausschnitts enthält, ist OLAP ein in diesem Sinn modellfreies Analysetool. Sowohl die Abfragen als auch die Interpretation der Ergebnisse hängen völlig vom Anwender ab. Diesem sollte somit große Freiheiten eingeräumt werden, um die Erkennung (neuer) Muster in den im OLAP hinterlegten Daten zu ermöglichen.[238] Die meisten Inferenzkontrollmechanismen aus dem SDB-Umfeld jedoch implizieren eine Kenntnis der „wichtigen" Zusammenhänge zwischen den Daten bzw. der „wichtigen" Kennzahlen, da in den SDB in der Regel Datensammlungen (bspw. Zensus-Daten) mit relativ gut beschreibbaren Analysezielen enthalten sind. Disclosure-Risiko und Informationsverlust können unter diesen Annahmen sinnvoller bestimmt und gegeneinander abgewogen werden als für den Fall, dass das Analyseziel noch unbekannt ist. Die Vorteilhaftigkeit vieler Inferenzkontrollverfahren in OLAP kann im einzelnen Anwendungsfall kaum eingeschätzt werden. Zudem zielen Inferenzkontrollmechanismen genau auf die Verhinderung systematischer Queries mit „unbekanntem Ziel", so dass der Informationsverlust schnell unzumutbar groß wird. Aus diesen beiden Gründen – dem zu erwartenden

235 Vgl. WANG/JAJODIA/WIJESEKERA (2007), S. 3
236 Vgl. ebenda, S. 123
237 Vgl. ebenda, S. 53
238 Vgl. ebenda, S. 13f. für den vorhergehenden Absatz

Performanzverlust und dem schlecht abschätzbaren Informationsverlust – sind die meisten für SDB entwickelten Verfahren nicht auf OLAP anwendbar. In Abschnitt 5.2 werden Mechanismen vorgestellt, die speziell für Inferenzkontrolle in OLAP entwickelt wurden.

5.1 Zugriff und Zugriffskontrolle in OLAP

In Analogie zu Kapitel 4 erfolgt in Abschnitt 5.1 zunächst eine Beschreibung von für OLAP geeigneten Zugriffskontrollmechanismen. Inferenzkontrollmechanismen in OLAP werden in Abschnitt 5.2 vorgestellt. Eine abschließende Bewertung von Zugriffs- und Inferenzkontrollverfahren erfolgt in Abschnitt 5.3.

5.1.1 Lattice-based Access Control in OLAP

Ziel des Ansatzes von WANG/JAJODIA/WIJESEKERA (2007) ist eine effiziente Integration von Zugriffskontrolle und Inferenzkontrolle: Auf Basis der Logik des Lattice-Modells wird zunächst ein Verfahren zur flexiblen Spezifikation von Schutzobjekten entwickelt, das anschließend als Grundlage für die Identifikation unsicherer Queries dient, so dass durch eine offline festgelegte Beschränkung der zulässigen Queries Inferenzen eliminiert werden können.[239] Die AC-Komponente dieses Ansatzes sowie ihre Weiterentwicklung[240] (durch dieselben Autoren) werden im Folgenden dargestellt. Die Beschreibung des ursprünglich vorgeschlagenen Inferenzkontrollmechanismus sowie seiner Weiterentwicklung „Query-driven Inference Control“[241] findet sich in den Abschnitten 5.2.3 und 5.2.4.

Grundlage dieses Konzeptes ist das Lattice-Modell von DENNING sowie dessen Weiterentwicklungen.[242] WANG/JAJODIA/WIJESEKERA (2007) treffen die Annahme, dass die Dimensionen (mindestens partiell) hierarchisch geordnet sind, um auf dieser Basis sog. „Dependency Lattices“ definieren zu können.[243] Beispielsweise hat das Versicherungsunternehmen in seiner Datenbank über die letzten Jahre Informationen zu den Patientenausgaben für Arztbesuche in verschiedenen Ländern gesammelt, so dass sich das Schema der Basistabelle als (Quartal, Patient, Ausgabe) ergibt. Die Dimensionen „Zeit“ und

239 Vgl. WANG/JAJODIA/WIJESEKERA (2007), S. 119-145
240 Vgl. ebenda, S. 147-167
241 Vgl. ebenda
242 Vgl. DENNING (1976); HARINARAYAN/RAJARAMAN/ULLMAN (1996); SANDHU (1993)
243 Vgl. WANG/JAJODIA/WIJESEKERA (2007), S. 120–122

„Länder“ sind entsprechend geordnet, d.h. sie implizieren die darauf sinnvoll anwendbaren Aggregationsoperationen bereits. Durch entsprechende hierarchische Aggregationen der Basistabelle können die Cuboiden des „Dependency-Lattice“ (vgl. Abbildung 23) erstellt werden. Leere Zellen implizieren, dass dem Nutzer bzw. Angreifer der Inhalt dieser Zellen aufgrund von externen Informationen bereits bekannt ist. Im Unterschied zu anderen Modellen der Inferenzkontrolle[244] werden als „Kennzahlen“ grundsätzlich nur die sensiblen numerischen Attribute bezeichnet.[245]

Wie im ursprünglichen Lattice-Modell[246] auch besteht eine Autorisierung aus dem Tripel (Objekt, Subjekt, Operation), wobei die Annahmen getroffen werden, dass für die Sicherung der Vertraulichkeit in OLAP Beschränkungen der Leserechte ausreichend sind und dass Subjekte sich nicht-kooperativ verhalten (d.h. keine Inferenzen durch Kollusion).[247]

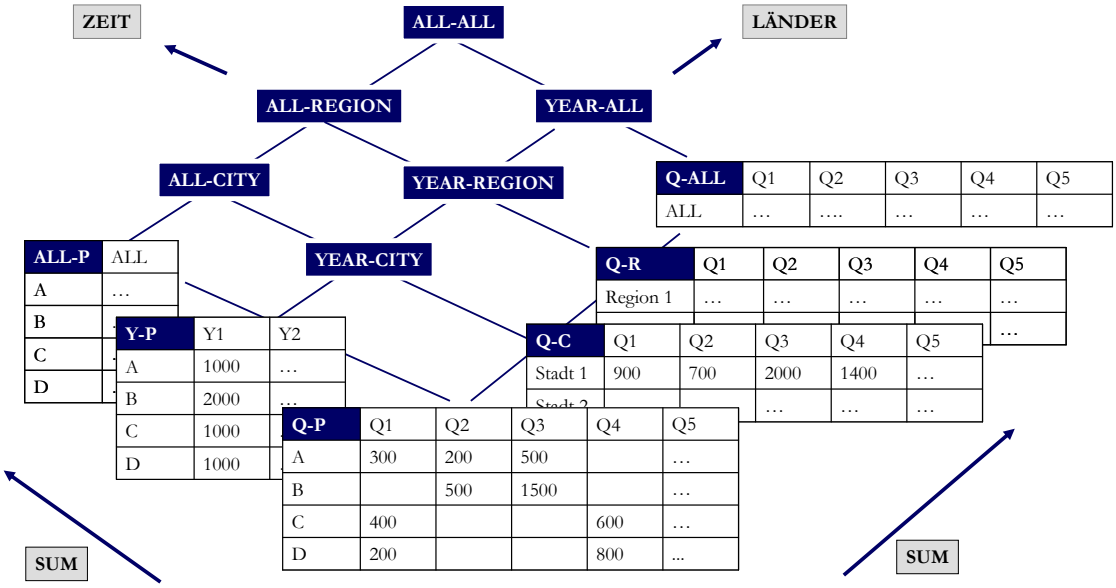


Abbildung 23: Beispiel eines Dependency-Lattice
In Anlehnung an WANG/JAJODIA/WIJESEKERA (2007), S. 121

Die Autorisierungsobjekte in OLAP unterscheiden sich grundlegend von den Objekten in Lattice-Modellen auf (flachen) relationalen Modellen: Neben Core Cuboids können Aggregations-Cuboids, Slices, Hierarchiestufen usw. sensible Daten enthalten und als Autorisierungsobjekte definiert werden.[248] Das Versicherungsunternehmen muss aus rechtlichen Gründen bspw. sicherstellen, dass seine Analysten keinen Zugriff auf die Ausgaben der

244 Vgl. Abschnitte 5.2.1 und 5.2.2
245 Vgl. WANG/JAJODIA/WIJESEKERA (2007), S. 122 für die beiden vorhergehenden Sätze
246 Vgl. DENNING (1976)
247 Vgl. WANG/JAJODIA/WIJESEKERA (2007), S. 123
248 Vgl. ebenda, S. 123

einzelnen Patienten pro Quartal haben. Zusätzlich kann der Analysezeitraum etwa auf Jahr 1 beschränkt werden. Abbildung 24 zeigt, dass hierfür u.a. der Zugriff auf vier Cuboids verboten werden muss.[249]

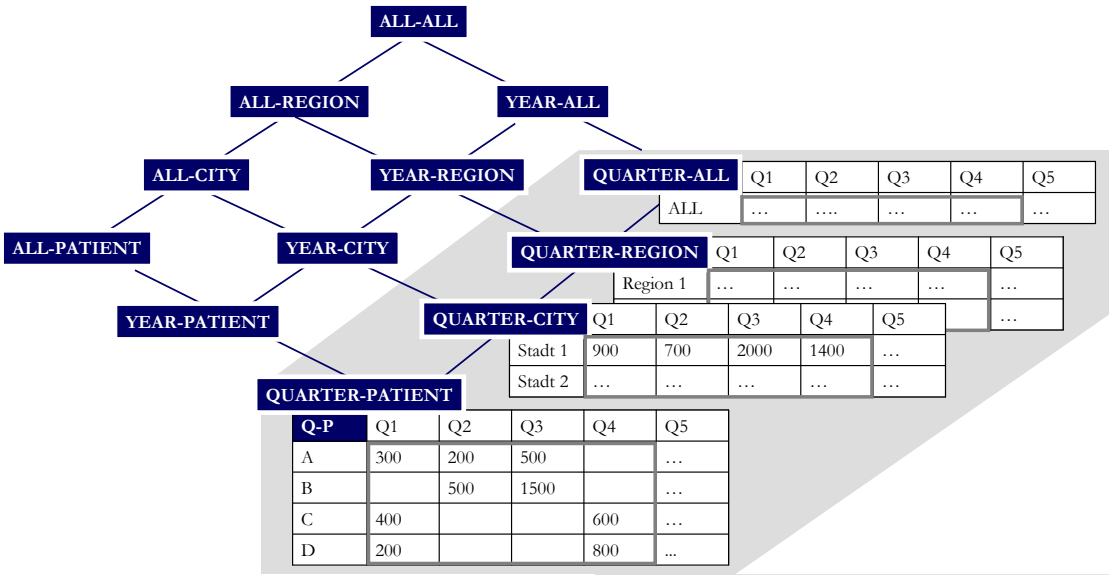


Abbildung 24: Beispielhafte Autorisierung im Dependency-Lattice
Eigene Darstellung

Zur Vereinfachung der Administration der Lattice-based AC können Level- und Slice-Spezifikationen vorgenommen werden, welche für das vorliegende Beispiel „Below(<QUARTER, ALL>)“ respektive „Slice({<q, p>: q ∈ QUARTER, p ∈ PATIENT, q ≥ Q5})“ lauten würden. Damit sind alle dem Cuboid <QUARTER, ALL> untergeordneten Cuboids inklusive ihm selbst sowie Slices auf den Zeitraum nach Jahr 1 verboten. l-Spezifikationen entsprechen vertikalen Partitionierungen, s-Spezifikationen horizontalen Partitionierungen des Data Cube.[250] Jedes Autorisierungsobjekt wird durch mindestens ein Paar von l- und s-Spezifikationen beschrieben.[251] Falls mehrere Autorisierungsobjekte desselben Cuboids, Slices etc. enthalten, gilt die jeweils striktere Autorisierungsvorschrift, wenn ein Nutzer eine Query darauf ausführen möchte.[252]

In den Termini des ursprünglichen Lattice-Modells ausgedrückt, verhindern „Below“-Restriktionen, dass Nutzer auf geschützte Zellen zugreifen, deren Sicherheitsstufe über ihrer eigenen liegt. Im Modell von WANG/JAJODIA/WIJESEKERA (2007) wird ein Objekt,

249 Die in den folgenden Kapiteln zur Erläuterung der Disclosure-Problematik in OLAP angeführten Beispiele sind an WANG/JAJODIA/WIJESEKERA (2007) entnommen und adaptiert.

250 Vgl. WANG/JAJODIA/WIJESEKERA (2007), S. 124f. für diesen und den vorhergehenden Satz

251 Vgl. ebenda, S. 126

252 Es gilt eine open policy, d.h. Zugriff auf ein Objekt wird nur gestattet, falls kein Verbot existiert [vgl. ebenda, S. 125f.].

das von einem anderen abhängt, als dessen Vorgänger („ancestor“) bezeichnet; das abhängige Objekt heißt entsprechend Nachfolger („descendant“).[253] In Abbildung 24 ist beispielsweise der Cuboid QUARTER-PATIENT Vorgänger von QUARTER-CITY, und ALL-ALL ist ein Nachfolger von ALL-REGION. Vorgänger haben i.d.Regel höhere Sicherheitsstufen als Nachfolger, da sie granularere Daten enthalten und entsprechend anfälliger für Inferenzen sind.

WANG/JAJODIA/WIJESEKERA (2007) zeigen zwar, dass es nicht notwendig ist, die Schnittmengen und Randzellen der Slices als separate Autorisierungsobjekte zu verwalten,[254] doch schon die Umformulierung aller existierenden Berechtigungen in Mengen von OLAP-Sicherheitsobjekten (Slices, Cubiods, Data Cubes) ist eine komplexe Aufgabe. Die Autoren weisen zwar darauf hin, dass die explizite Definition von Zugangsberechtigungen nicht unbedingt notwendig sei: Würde das Lattice-Modell mit einem Inferenzkontrollmechanismus gekoppelt, bspw. „SeCube“ (vgl. Abschnitt 5.2.3), könnten Zugriffsrechte implizit abgebildet werden.[255] Allerdings bedingt SeCube eine statische Definition der zulässigen Queries, eine Einschränkung, welche die Autoren selbst als kritisch betrachten.[256] Die Frage, ob eine effiziente Administration der Sicherheitsobjekte, Sicherheitsstufen sowie der Berechtigungen möglich ist, wird nicht diskutiert.[257] Der Implementierungs- und Aktualisierungsaufwand für das Lattice-Modell ist vermutlich beträchtlich.

5.1.2 RBAC in OLAP

FUGKEAW ET AL. entwickeln ein RBAC-basiertes Zugriffskonzept für OLAP auf verteilten Datenbanken.[258] Es besteht aus fünf Komponenten: den lokalen Data-Warehouse-Sicherheitsrichtlinien, Nutzern, Rollen(-hierarchien), Zugriffsrechten und DW-Autorisierungsrichtlinien. Die Rollenhierarchien und Rollenberechtigungen werden in den lokalen DW definiert. Die Zugriffsrechte auf die Daten werden in Autorisierungstabellen gespeichert, die für jede Rolle die Zugriffsrechte für jede Dimensions- und Faktenzelle enthält. Tabelle 19 zeigt ein Beispiel für verschiedene Rechtebündel einiger Rollengruppen, die auf OLAP-Daten zugreifen, welche aus dem Data Warehouse 1 stammen.

253 Vgl. ebenda, S. 122
254 Vgl. ebenda, S. 125
255 Vgl. ebenda, S. 130-140
256 Vgl. ebenda, S. 147-151
257 Vgl. ebenda, S. 147f.
258 Vgl. FUGKEAW/PIYAWIT/SEKPON (2009)

DWID	GroupID	ZEIT Year	ZEIT Quarter	LÄNDER City	LÄNDER Regions	PATIENT Name	FACT Ausgaben
1	1(Controlling)	Y	Y	Y	Y	N	Y
1	2(Analyst)	Y	N	Y	Y	N	Y
1	3(Accounting)	Y	Y	N	N	Y	Y

Tabelle 19: Beispielhafte Autorisierungstabelle für DW1
Eigene Darstellung nach FUGKEAW/MANPANPANICH/JUNTAPREMJITT (2008)

In diesem Modell müssen DW-übergreifende zusätzliche Restriktionen, die in den ursprünglichen, lokalen Rollenbeschreibungen nicht vorgesehen sind, im Autorisierungskonzept auf OLAP-Ebene separat und wenn nötig für jede Dimension und Rolle einzeln eingetragen werden.[259] Die vorgeschlagene Methode kann dadurch auf existierenden DW aufsetzen, ohne Veränderungen in den lokalen Rollen- und Berechtigungskonzepten vornehmen zu müssen. Bei der Einführung eines regionalen Controllings könnte beispielsweise das DW-Rechtekonzept aus Tabelle 19 unverändert bleiben und lediglich auf OLAP-Ebene eine Verschärfung der Zugriffsberechtigung auf die Dimension LÄNDER spezifiziert werden. So wird ein direkter Eingriff in die DW-Berechtigungsstruktur vermieden, der außer auf DW1 auch auf anderen DW Veränderungen notwendig machen könnte.

Voraussetzung für den Einsatz dieses Modells ist ein funktionierendes Rollenkonzept auf DW-Ebene sowie eine konsistente Definition der zusätzlichen Zugriffsrechte auf OLAP-Ebene; die Spezifizierung der Zugriffsrechte wird nicht thematisiert.[260] Dieses Modell enthält keine Mechanismen zur Inferenzkontrolle. Der Implementierungsaufwand wird insofern reduziert, als keine Veränderungen in den DW-Berechtigungsstrukturen notwendig sind; jedoch ist die konsistente Spezifikation zusätzlicher Rechte auf OLAP-Ebene sicherlich keine triviale Aufgabe. Vorteil dieser Vorgehensweise ist die feine Granularität, mit der die Rechte vergeben werden können, so dass Flexibilität des und Nutzen aus dem OLAP-System maximiert werden.

SOLER ET AL. (2008) stellen als Teil der DW-Entwicklung ein Vorgehensmodell für die Identifikation und Modellierung von Sicherheitsanforderungen vor. Sie unterscheiden zwischen informationsbezogenen und Quality-of-Service-Anforderungen an DW-Design, worunter sie Sicherheitsaspekte wie vor allem das Zugangsberechtigungskonzept fassen. Nachteile ihres Modells sind der extrem hohe Detaillierungsgrad, mit dem die informati-

[259] Vgl. ebenda
[260] Vgl. ebenda

onsbezogenen Anforderungen erfasst werden müssen. Um den Informationsbedarf und die Zugangsberechtigungen eines Nutzers zu erfassen, müssen die Sicherheitsebenen (Rolle, „compartment", Sicherheitslevel) sowie die individuellen Ziele und die dafür relevanten Kontexte und Geschäftsprozesse jedes Nutzers festgelegt werden. Dies zieht einen hohen Änderungsbedarf nach sich, da bei jeder inhaltlichen oder personellen Veränderung unter den Zugriffsberechtigten das Modell angepasst werden muss. Die empfohlene Vorgehensweise bei der Identifikation der Ziele und sicherheitsrelevanten Aspekte ist sehr generisch gehalten.[261]

5.2 Inferenzen und Inferenzkontrolle in OLAP

In diesem Abschnitt werden neuere Ansätze zur Inferenzkontrolle vorgestellt, welche unter Berücksichtigung der Bedürfnisse der Anwender speziell für den Einsatz in OLAP entwickelt wurden.

5.2.1 Kardinalitätsbasierte Inferenzkontrolle in OLAP

WANG/JAJODIA/WIJESEKERA (2007) entwickeln ein kardinalitätsbasiertes Verfahren zur Inferenzkontrolle von sog. „skeleton queries"[262], die sich ausschließlich auf ganze Zeilen oder Spalten eines Data Cubes oder eines Core Cuboids beziehen.[263] Sie zeigen, dass bei der Identifizierung von Inferenzen sowohl die Kardinalitäten der Cuboids als auch die Anzahl der leeren Zellen im Data Cube ausschlaggebend für die Kompromittierbarkeit des Data Cube sind.[264]

Aus Gründen der Performanz und des Speicherplatzbedarfes wird meist nicht der komplette Data Cube materialisiert, sondern lediglich ein Core Cuboid, aus dem die anderen Tabellen errechnet werden können.[265] Die Auswirkungen vollständiger Materialisierung lassen sich erahnen, wenn man den vollständig materialisierten dreidimensionalen Data Cube des Versicherungsunternehmens betrachtet (vgl. Tabelle 20) und mit dem Core

261 Vgl. SOLER ET AL. (2008)

262 Im Gegensatz dazu erlauben Range Queries auf multidimensionalen Tabellen die Einschränkung des Suchbereichs auf Sequenzen, d.h. sie führen eine partielle Aggregation von Zeilen oder Spalten durch [vgl. WANG/JAJODIA/WIJESEKERA (2007), S. 38f.].

263 Vgl. ebenda, S. 38

264 Vgl. ebenda, S. 35-38

265 Vgl. ebenda, S. 17

Cuboid Tabelle (AGE, SEX, DOC) in Tabelle 11 vergleicht.[266]

	AGE	SEX	DOC	GES
GES	ALL	ALL	ALL	310
ALL, SEX, ALL	ALL	M	ALL	163
	ALL	W	ALL	147
AGE, ALL, ALL	0-18	ALL	ALL	52
	19-39	ALL	ALL	39
	40-67	ALL	ALL	119…
	> 67	ALL	ALL	100
ALL, ALL, DOC	ALL	ALL	A	162
	ALL	ALL	B	26
	ALL	ALL	C	122
ALL, SEX, DOC	ALL	M	A	84
	ALL	W	A	78
	ALL	M	B	10
	ALL	W	B	16
	ALL	M	C	69
	ALL	W	C	53
AGE, ALL, DOC	0-18	ALL	A	50
	0-18	ALL	B	0
	0-18	ALL	C	2
	19-39	ALL	A	2
	19-39	ALL	B	17
	19-39	ALL	C	20
	40-67	ALL	A	10
	40-67	ALL	B	9
	40-67	ALL	C	100
	> 67	ALL	A	100
	> 67	ALL	B	0
	> 67	ALL	C	0

	AGE	SEX	DOC	GES
AGE, SEX, ALL	0-18	M	ALL	25
	0-18	W	ALL	27
	19-39	M	ALL	23
	19-39	W	ALL	16
	40-67	M	ALL	66
	40-67	W	ALL	53
	> 67	M	ALL	49
	> 67	W	ALL	51
AGE, SEX, DOC	0-18	M	A	24
	0-18	W	A	26
	0-18	M	B	0
	0-18	W	B	0
	0-18	M	C	1
	0-18	W	C	1
	19-39	M	A	2
	19-39	W	A	0
	19-39	M	B	1
	19-39	W	B	16
	19-39	M	C	20
	19-39	W	C	0
	40-67	M	A	9
	40-67	W	A	1
	40-67	M	B	9
	40-67	W	B	0
	40-67	M	C	48
	40-67	W	C	52
	> 67	M	A	49
	> 67	W	A	51
	> 67	M	B	0
	> 67	W	B	0
	> 67	M	C	0
	> 67	W	C	0

Tabelle 20: Dreidimensionaler Data Cube
Eigene Darstellung

Das Lattice-Modell (vgl. Abschnitt 4.2.3 und Abschnitt 5.1.1) kann zur besseren und sparsameren Visualisierung des Data Cube eingesetzt werden (vgl. Abbildung 25).

[266] Die für diesen und die folgenden Abschnitte verwendeten Beispiele sind an WANG/JAJODIA/WIJESEKERA (2007) angelehnt.

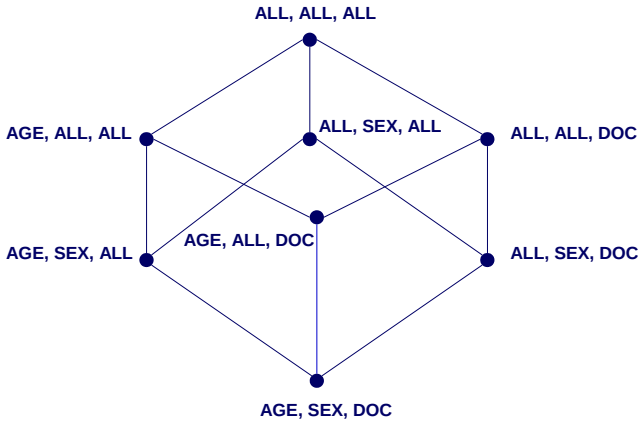


Abbildung 25: Beispiel eines Lattice
Eigene Darstellung nach ADAM/WORTHMANN (1989), S. 524

Ein Cube ist umso sicherer, je weniger leere Zellen er enthält (leere Zellen repräsentieren Werte, die ein Angreifer aufgrund von externen Informationen kennt). Eine untere Grenze existiert für die maximale Anzahl an leeren Zellen für jeden beliebigen sicheren Cube.[267] Angenommen, die Versicherung möchte die noch unbekannten Information „Ausgaben pro Patient pro Jahr" schützen. Die Patienten (A-D) werden in den Spalten des Cubes in Tabelle 21 abgetragen, die Jahre (2007-2010) in den Zeilen.

	A	B	C	D	♦
2007	?	?	?		5000
2008		?	?		6500
2009	?			?	4500
2010	?			?	4000
♦	7500	4000	4000	4500	20000

Tabelle 21: Beispielhafter Data Cube
Eigene Darstellung nach WANG/JAJODIA/WIJESEKERA (2007), S. 54

Ziel der im Anschluss beschriebenen Umformulierungen ist es, eine binäre Aggregationsmatrix zu erhalten, auf Basis derer dann mögliche Inferenzen für den Data Cube identifiziert werden und sichere Schwellwerte für die Kardinalitäten der Core Cuboids berechnet werden.[268]

Zunächst wird der Data Cube zu einem Core Cuboid umformuliert, indem in jede Zelle das entsprechende Dimensionstupel eingetragen wird. Für jeden Core Cuboid muss gelten, dass jede (Integer-)Ausprägung jeder Dimension in mindestens einem Tupel enthalten ist (vgl. Tabelle 22); der Full Core Cuboid entspricht dem kartesischen Produkt aller

[267] Vgl. WANG/JAJODIA/WIJESEKERA (2007), S. 53-89
[268] Vgl. ebenda, S. 62-76

Dimensionen des zugrunde liegenden Data Cubes.[269]

	1	2	3	4
1	(1,1)	(1,2)	(1,3)	
2		(2,2)	(2,3)	
3	(3,1)			(3,4)
4	(4,1)			(4,4)

Tabelle 22: Beispielhafter Core Cuboid
Eigene Darstellung nach WANG/JAJODIA/WIJESEKERA (2007), S. 59

Ein Slice auf die erste Dimension dieses Core Cuboids würde die Patientenausgaben im Jahr 2007 liefern. Jeder Dimension kann nun der *-Wert hinzugefügt werden, wodurch eine sog. „augmentierte Dimension“[270] entsteht, die auch andere Werte (*-Elemente) als Integer enthält. Vektoren mit j *-Elementen heißen j*-Aggregationsvektor und die Zusammenfassung aller j*-Aggregationsvektoren, welche ein *-Element an derselben Stelle haben, heißt j*-Aggregations-Cuboid. Dieses Konzept ist interessant, da es erlaubt, *-Elemente in Vektoren mit beliebigen Integern im Core Cuboid zu matchen, so dass die „matched“ Tupel das Aggregationsset des Vektors bilden.[271] Für das Versicherungsunternehmen ergibt sich ein neuer Core Cuboid (vgl. Tabelle 23). Das Aggregations-Set (1,*) besteht beispielsweise aus den Tupeln {(1,1), (1,2), (1,3)} und der einzige 2-*-Aggregations-Cuboid ist (*,*).

	1	2	3	4	*
1	(1,1)	(1,2)	(1,3)		(1,*)
2		(2,2)	(2,3)		(2,*)
3	(3,1)			(3,4)	(3,*)
4	(4,1)			(4,4)	(4,*)
*	(*,1)	(*,2)	(*,3)	(*,4)	(*,*)

Tabelle 23: Beispielhafter Aggregations-Cuboid
Eigene Darstellung nach WANG/JAJODIA/WIJESEKERA (2007), S. 60

Aus dem Core Cuboid und den Aggregations-Cuboids wird nun die Aggregationsmatrix M erstellt. Hierzu werden die Tupel des Core Cuboid zeilenweise absteigend sortiert und die Aggregations-Cuboiden aufsteigend nach Anzahl ihrer *-Elemente und der Indizes ihrer *-Elemente (vgl. Tabelle 24).[272]

269 Vgl. WANG/JAJODIA/WIJESEKERA (2007), S. 57f.
270 Vgl. ebenda, S. 58
271 Vgl. ebenda, S. 58-60 für den vorherigen Absatz
272 Vgl. ebenda, S. 61

Position	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Core Cuboid	(1,1)	(1,2)	(1,3)			(2,2)	(2,3)		(3,1)			(3,4)	(4,1)			(4,4)
Aggregations-Cuboid	(1,*)	(2,*)	(3,*)	(4,*)	(*,1)	(*,2)	(*,3)	(*,4)								

Tabelle 24: Sortierung der Cuboids für Aggregationsmatrix
Eigene Darstellung

Die Aggregationsmatrix wird gebildet, indem an den besetzten Stellen 1 eingetragen wird, sonst 0 (vgl. Tabelle 25).[273] Für die Aggregationsmatrix kann nun relativ einfach die Gefahr durch Inferenzen bestimmt werden, indem Sequenzen von zulässigen elementaren Zeilenoperationen daraufhin überprüft werden, ob sie einen Einheitsvektor in irgendeiner Zeile liefern.[274]

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	1	1													
2						1	1									
3									1			1				
4													1			1
5	1								1				1			
6		1				1										
7			1			1										
8								1				1				1

Tabelle 25: Aggregationsmatrix
Eigene Darstellung nach WANG/JAJODIA/WIJESEKERA (2007), S. 62

WANG/JAJODIA/WIJESEKERA (2007) sprechen von trivialer Kompromittierung des Data Cubes, wenn einer der Aggregationsvektoren alleine den Cube kompromittiert, d.h. wenn er eine Aggregation über nur ein Tupel ausführt.[275] Nicht-triviale Kompromittierung liegt vor, wenn M zunächst umgeformt[276] werden muss, wie es auch im hier dargestellten Beispiel der Fall ist (vgl. Tabelle 26). Die Matrix bzw. der Core Cuboid wird durch das Set an (1,*)-Aggregations-Cuboids kompromittiert (vgl. Zeile 1 in Tabelle 26); genauer gesagt ist das erste Tupel im Core Cuboid kompromittiert.

273 Aufgrund der besseren Übersichtlichkeit wurden alle Werte gleich 0 hier nicht eingetragen.
274 Vgl. WANG/JAJODIA/WIJESEKERA (2007), S. 62
275 Vgl. ebenda, S. 62f.
276 Vgl. CHIN/OZSOYOGLU (1982)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1															
2		1					-1									
3			1				1									
4						1	1									
5									1							-1
6												1				1
7													1			1
8																

Tabelle 26: Nicht-triviale Kompromittierung der Aggregationsmatrix
Eigene Darstellung nach WANG/JAJODIA/WIJESEKERA (2007), S. 63

WANG/JAJODIA/WIJESEKERA (2007) beweisen, dass für voll besetzte Core Cubes triviale Kompromittierung unmöglich ist. Ebenso liefern sie eine untere (dimensionsabhängige) Grenze[277] für die Anzahl der Tupel, welche ein Core Cuboid mindestens enthalten muss, um gegen triviale Kompromittierung geschützt zu sein.[278]

Nicht-triviale Kompromittierung ist für vollständig besetzte Core Cuboids bzw. für den zugrunde liegenden Data Cube unmöglich.[279] Ein hinreichend großer Data Cube kann nicht-trivial kompromittiert werden, wenn die Anzahl der fehlenden Tupel groß genug ist, d.h. wenn sie mindestens so groß ist, dass die Aggregations-Cuboids der zwei kleinsten Dimensionen für nicht-triviale Kompromittierung verwendet werden können.[280]

Auf Basis dieser Ergebnisse schlagen WANG/JAJODIA/WIJESEKERA (2007) ein Drei-Schichten-Modell der Inferenzkontrolle vor, das zwischen der Daten- und der Query-Schicht eine Aggregationsschicht enthält, in welcher die zulässigen sicheren Aggregationsoperationen gespeichert sind.[281] Vorteile dieser Architektur sind erstens die Lokalisierbarkeit von Inferenzen, welche durch eine entsprechende Partitionierung der Daten möglicherweise eliminiert werden können, zweitens die Senkung des Inputs in den Kontrollmechanismus (lediglich die gewünschte Aggregationsoperation), und drittens die Reduktion des Performanzverlustes durch Inferenzkontrolle, da die zulässigen Aggregationsoperationen weitgehend offline berechnet werden können.[282]

---

277 $|C_{Core}| < 2^{k-1} \cdot \max(d_1, \ldots, d_k)$ wobei der k-dimensionale Cuboid C_{Core} die Dimensionen $D_1, \ldots, D_k$ enthält. Für das hier angeführte Beispiel ergibt sich eine untere Grenze der Tupelzahl von 12.

278 Vgl. WANG/JAJODIA/WIJESEKERA (2007), S. 66–78

279 Vgl. ebenda, S. 68f.

280 Vgl. ebenda, S. 71-76

281 Vgl. ebenda, S. 76-86

282 Vgl. ebenda, S. 79f.

Nachteile der kardinalitätsbasierten Inferenzkontrolle[283] sind die Ermöglichung von Inferenzen durch nicht in der Aggregationsschicht hinterlegte Subqueries und die Einschränkung auf „skeleton queries“ sowie (bedingt durch den Einsatz des Audit Experts[284] als Identifikationsverfahren für Inferenzen) auf das Auffinden exakter Inferenzen durch einfache Aggregationsoperationen wie SUM. Die Annahme, dass alle Dimensionen eine sinnvolle Hierarchie enthalten, wird lediglich im Kontext kategorialer Daten diskutiert, für welche eine beliebige Ordnung festgelegt werden kann, um dichter besetzte Partitionen zu erhalten.[285] Möglicherweise gibt es jedoch unerkannte sinnvolle Hierarchien in den Daten, die durch Partitionierung zerstört werden (z.B. Produktähnlichkeiten). Die Annahme, dass anhand der Datenstrukturen bzw. der Dimensionshierarchien prinzipiell die relevantesten Queries herausgefiltert werden können,[286] ist zwar intuitiv nachvollziehbar, wird jedoch nicht begründet oder nachgewiesen. Die Partitionierung der Daten (z.B. zu niedrige Granularität der Dimension „Zeit“[287]) kann dazu führen, dass manche Analysen unmöglich werden, obwohl sie eigentlich einen hohen Nutzen hätten. Schließlich sind die Bedingungen für die Kompromittierbarkeit von Data Cubes hinreichend, aber nicht notwendig; bei Überschreiten der oberen Grenze für die zulässige Zahl an leeren Zellen können keine Aussagen über mögliche Inferenzen mehr gemacht werden.[288]

5.2.2 Paritätsbasierte Inferenzkontrolle in OLAP

WANG/JAJODIA/WIJESEKERA (2007) schlagen vor, Nutzern lediglich geradzahlige multidimensionale Range Queries (MDR) zu gestatten, um Inferenzen (auf den ungeraden Wert 1) durch die Bildung von Vereinigungen und Schnittmengen der Ergebnismengen zulässiger SUM-Queries zu erschweren. Dazu zeigen WANG/JAJODIA/WIJESEKERA (2007), dass die Menge aller geradzahligen MDR nur dann keine Inferenzen gestattet, wenn dies für eine spezifische Menge an Zweiersummen gilt. Für den Fall der ungeradzahligen MDR existiert eine geringe Anzahl an geradzahligen MDR, deren Ergebnis um genau 1 vom Ergebnis der (unzulässigen) ungeradzahligen MDR abweicht, so dass

283 Vgl. WANG/JAJODIA/WIJESEKERA (2007), S. 53–86
284 Vgl. CHIN/OZSOYOGLU (1982)
285 Vgl. WANG/JAJODIA/WIJESEKERA (2007), S. 84f.
286 Vgl. ebenda, S. 77
287 Vgl. ebenda, S. 63f.
288 Vgl. ebenda, S. 91

diese näherungsweise beantwortet werden kann.[289]

Ein Core Cuboid des Versicherungsunternehmens gibt Aufschluss über die Veränderung der Patientenausgaben für ärztliche Behandlungen (vgl. Tabelle 27). Selbst wenn ein direkter Zugriff auf die Inhalte der Zellen nicht zulässig ist, können die exakten Werte doch leicht errechnet werden, wenn ungeradzahlige MDR erlaubt sind.

	A	B	C	D
2009	2000	1000	-500	
2010		500	-2000	1000

Tabelle 27: Beispielhafter Data Cube zur Illustration von MDR
Eigene Darstellung

Die Veränderung der Ausgaben von Patient A in 2009 entspricht der Summierung einer einelementigen Spalte. Durch Subtraktion der Query Sets S2a und S2b voneinander kann die Veränderung der Ausgaben von Patient A in 2009 ebenfalls leicht errechnet werden (vgl. Tabelle 28), so dass in diesem Fall selbst geradzahlige MDR problematisch sind.

Q1	SUM (patient = A AND year FROM 2009 TO 2010)	S1	2000
Q2a	SUM ((patient = B AND year = 2009), (patient = C AND year =2009))	S2a	500
Q2b	SUM ((patient = A AND year = 2009), (patient = C AND year =2009))	S2b	1500

Tabelle 28: Beispiele für Inferenzen aus MDR
Eigene Darstellung

Kompromittierbarkeit bedeutet in diesem Fall, dass beliebige Queries einelementige Ergebnismengen des Core Cuboids zurückliefern, womit sowohl das zurückgelieferte Tupel als auch der Core Cuboid insgesamt kompromittiert sind.[290] Queries bzw. ihre Ergebnismengen können (beinahe analog zu Abschnitt 5.2.1) in einer binären Inzidenzmatrix abgebildet werden.

[289] Vgl. WANG/JAJODIA/WIJESEKERA (2007), S. 92 für die beiden vorhergehenden Sätze
[290] Vgl. ebenda, S. 94-97

MDR Queries q*	
q*((1,1),(2,4))	{(1,1),(1,2),(1,3),(2,2),(2,3),(2,4)}
q*((1,1,),(1,2))	{(1,1),(1,2)}
q*((1,2),(1,3))	{(1,2),(1,3)}
q*((1,2),(2,2))	{(1,2),(2,2)}
q*((2,3),(2,4))	{(2,3),(2,4)}

Tabelle 29: Positionsbestimmung in der Inzidenzmatrix
In Anlehnung an WANG/JAJODIA/WIJESEKERA (2007), S. 9)

Eine einfache Zeilenoperation auf die Inzidenzmatrix in Tabelle 30 liefert die Inzidenzmatrix der Query {(1,2)} als [0,1,0,0,0,0] und somit den Nachweis, dass das Tupel kompromittiert ist.

	1	2	3	4	5	6
1	1	1	1	1	1	1
2	1	1				
3		1	1			
4		1		1		
5					1	1

Tabelle 30: Inzidenzmatrix eines kompromittierten Cuboids
In Anlehung an WANG/JAJODIA/WIJESEKERA (2007), S. 97

WANG/JAJODIA/WIJESEKERA (2007) zeigen, dass die Leistungsfähigkeit von Query Set Size Control, Overlap Control sowie des Audit Expert (vgl. Abschnitt 4.3.1) nicht steigt, wenn der Nutzer auf MDR beschränkt wird.[291] Außerdem ist es nicht möglich, durch die Anwendung dieser Verfahren in Kombination mit der Beschränkung auf MDR Inferenzen zu verhindern. WANG/JAJODIA/WIJESEKERA (2007) schlagen daher vor, spezifische Zweiersummen zu bilden, indem die letzten beiden aufeinander folgenden Tupel zweier ungeradzahliger Ergebnismengen zu zusätzlichen Zweiersummen addiert werden.[292] Anschließend zeigen die Autoren, dass diese Vorgehensweise dazu führt, dass in geringerer Zeit als mit dem Benchmark Audit Expert eine Menge an sicheren MDR-Queries für einen Data Cube berechnet werden kann.[293] Die Zweiersummen können in einem sog.

[291] Vgl. ebenda, S. 97-99
[292] Vgl. ebenda, S. 104
[293] Vgl. ebenda, S. 103-107

QDT-Graphen abgebildet werden, der keine Zyklen ungerader Länge enthält, wenn die Menge der Zweiersummen sicher ist.[294] Wie aus Abbildung 26 ersichtlich, sind die Zweiersummen für den Core Cuboid des Versicherungsunternehmens nicht sicher.

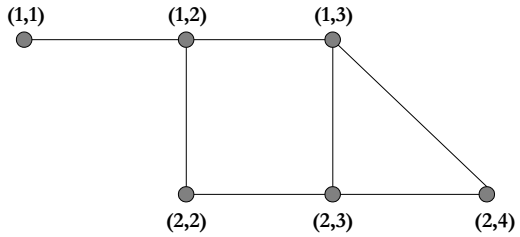


Abbildung 26: Beispielhafter QDT-Graph
WANG/JAJODIA/WIJESEKERA (2007), S. 109

WANG/JAJODIA/WIJESEKERA (2007) diskutieren die Integration der paritätsbasierten Inferenzkontrolle in ihr Drei-Schichten-Modell (vgl. Abschnitt 5.2.1) und stellen fest, dass dieses Verfahren aufgrund der Zulässigkeit von MDR eine Vielzahl von Operationen (Slicing, Dicing, Roll-up, Drill-Down) ermöglicht, wodurch die Nützlichkeit des OLAP-Systems für Analysezwecke deutlich erhöht wird. Zudem können auch einige Queries aus unsicheren MDR-Sets beantwortet werden und die Bedingungen zur Identifizierung sicherer MDRs sind sowohl hinreichend als auch notwendig. Allerdings sind die verwendbaren Aggregationsoperationen auch hier im Prinzip auf SUM-Queries beschränkt, und das Verfahren ist anfällig für komplexe Inferenzen.[295]

5.2.3 SeCube

WANG/JAJODIA/WIJESEKERA (2007) schlagen eine statische und eine dynamische Variante (vgl. Abschnitt 5.2.4) der Kontrolle von multidimensionalen Inferenzen (m-d Inferenzen) vor. Die statische Variante „SeCube“ führt die Inferenzkontrolle offline durch und setzt die so identifizierten Restriktionen anschließend online mit den Mechanismen der Zugriffskontrolle durch, d.h. bei jeder Query erfolgt eine Autorisierungsprüfung nur auf Autorisierungsobjekten, die bereits frei von Inferenzen sind.[296] Das Verfahren „SeCube“ basiert auf der Überlegung, dass die Annahmen des „detect-then-remove“-Ansatzes unrealistisch sind, da eine vollständige Enumeration aller möglichen oder auch nur der

[294] Vgl. WANG/JAJODIA/WIJESEKERA (2007), S. 107-110
[295] Vgl. ebenda, S. 116 für den vorhergehenden Absatz
[296] Vgl. ebenda, S. 119-145

schwerwiegendsten Inferenzen unter realistischen Bedingungen unmöglich ist.[297] Zunächst werden einige für das Verständnis der beiden Verfahren zentrale Begriffe geklärt.

Die BELOW-Restriktionen aus dem Lattice-Modell (vgl. Abschnitt 5.1.1) verhindern, dass aus den Vorgänger-Cuboiden Rückschlüsse auf geschützte Zellen der Nachfolger-Cuboide gezogen werden.[298] Der umgekehrte Fall erfordert den Einsatz eines Inferenzkontrollmechanismus.[299] Die ungeschützten Zellen oder Cuboide, welche eine Inferenz ermöglichen, werden als Quelle („source") bezeichnet und die geschützten Zellen oder Cuboide, deren Wert errechnet werden soll, als Ziel („target").[300] Für sog. 1-d (eindimensionale) Inferenzen, welche einer Single Query Attack (vgl. Abschnitt 4.3.1) ähneln, schlagen WANG/JAJODIA/WIJESEKERA (2007) vor, jede Quelle auf Inferenzen bzgl. ihrer Vorgänger im Ziel-Cuboid zu überprüfen. Im Falle von m-d Inferenzen ist die Prozedur notwendigerweise etwas komplizierter, denn unterschiedliche Aggregationsoperationen können zu unterschiedlichen Inferenzen führen und müssen separat untersucht werden.[301]

Die Beziehung zwischen 1-d und m-d Inferenzen wird folgendermaßen beschrieben:

> „m-d inference is the complement of 1-d inference in the sense that the intersection of the source with any single cuboid does not cause an inference, but the source does."[302]

Könnte der Analyst des Versicherungsunternehmens bspw. nur den Cuboid QUARTER-CITY (Q-C) sehen und verfügte er über die externe Information, dass B im dritten Quartal dreimal so viel für Arztbesuche ausgegeben hat wie A, könnte er den Wert beider Zellen <Q3, A> und <Q3, B> inferieren (vgl. Abbildung 27).[303] Hier liegt eine einfache 1-d Inferenz vor.

---

297 Häufige Annahmen betreffen die Einschränkung der zulässigen Aggregationsoperationen auf SUM, die Abwesenheit externer Informationen über einzelne Zellen oder Zusammenhänge zwischen den Cuboiden und die zu grobe Festlegung der Schutzkriterien [vgl. WANG/JAJODIA/WIJESEKERA (2007), S. 127].

298 Vgl. ebenda, S. 125f.

299 Vgl. ebenda, S. 127-143

300 Vgl. ebenda, S. 126f.

301 Vgl. ebenda, S. 128

302 ebenda, S. 128

303 Die leeren Zellen werden als dem Angreifer bekannt angenommen.

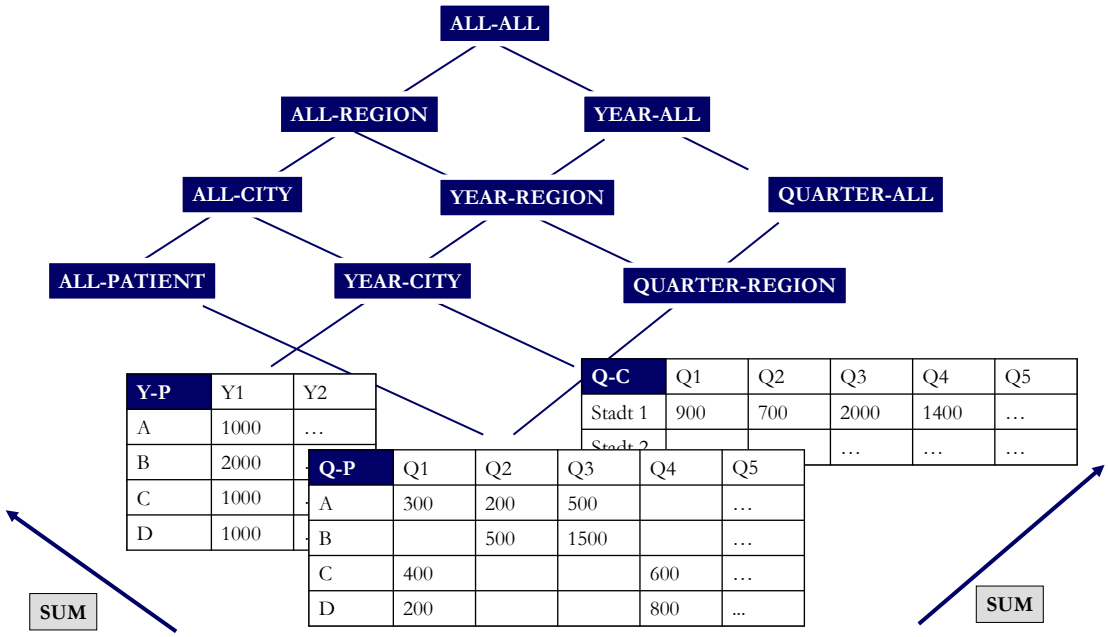


Abbildung 27: Beispiel für 1-d und m-d Inferenzen
In Anlehnung an WANG/JAJODIA/WIJESEKERA (2007), S. 121

m-d Inferenzen sind schwieriger zu entdecken, insbesondere wenn sie durch die Anwendung verschiedener Aggregationsoperationen ausgelöst werden. Als erstes Beispiel (nur SUM-Operationen seien erlaubt) sei hier angenommen, dass der Versicherungsanalyst Zugriff auf die Cuboide <QUARTER, CITY> und <YEAR., PATIENT> hat, jedoch keine externen Informationen über die relativen Ausgaben der Patienten mehr besitzt. Der Analyst kann jedoch auch in diesem Fall auf einfache Weise den Wert der Zelle <Q1, A> inferieren (vgl. Tabelle 31).

Q1	SUM ((year = Y1 AND patient = A) , (year = Y1 AND patient = B))	**S1**	3000
Q2a	SUM((quarter = 2 AND city = Stadt 1), (quarter = 3 AND city = Stadt 2))	**S2a**	2700
Q2b	S1 – S2a	**S2b**	300

Tabelle 31: Beispiel für m-d Inferenzen durch SUM-Queries
Eigene Darstellung

Im zweiten Beispiel sei die (unrealistische) Annahme aufgegeben, dass der Analyst ausschließlich SUM-Operationen durchführen darf. Ihm seien nun auch MAX und MIN erlaubt. Das Dependency Lattice muss also um die Aggregations-Cuboide MAX und MIN erweitert werden (vgl. Abbildung 28). Der Analyst verfügt über keine externen Informationen bzgl. des Inhalts von <QUARTER, PATIENT>, jedoch hat er bereits durch MAX-Aggregationen den Wert von <Q3, B> inferiert.

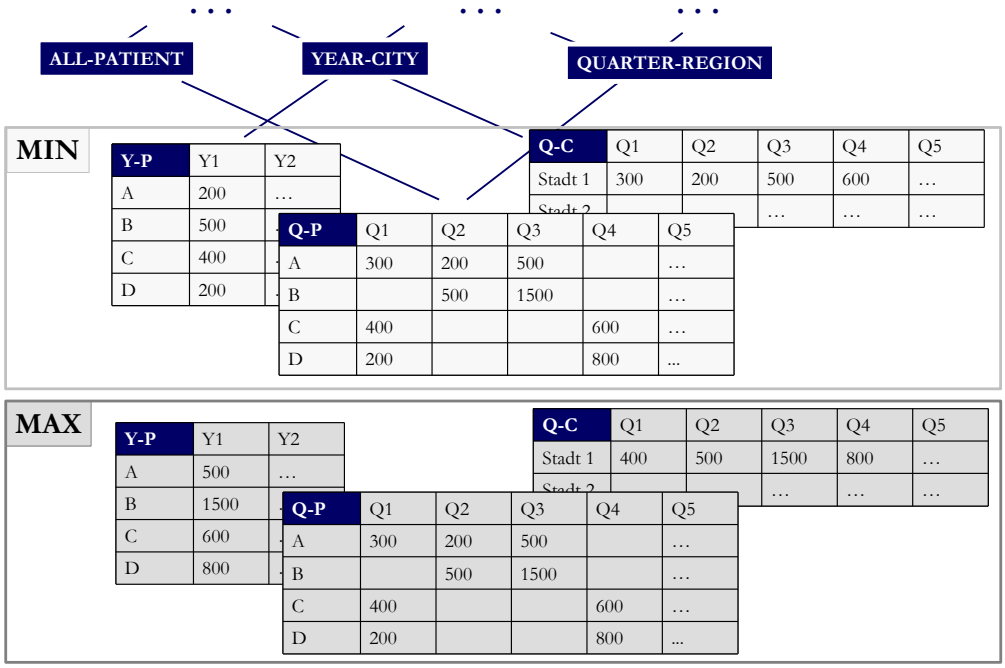


Abbildung 28: Beispielhafte Erweiterung des Lattice um MAX und MIN
Eigene Darstellung

Aus den Operationen MAX, MIN und SUM für Patient B erfährt der Analyst die Höhe der restlichen Ausgaben von B in Jahr 1 (vgl. Tabelle 32). Er weiß nun, dass die Ausgaben von B in Q1, Q2 oder Q4 500 betrugen und in den übrigen beiden Quartalen 0.

Q1a	MAX (year = Y1 AND patient = B)	**S1a**	1500
Q1b	MIN (year = Y1 AND patient = B)	**S1b**	500
Q1c	SUM (year = Y1 AND patient = B)	**S1c**	2000
➡	{<Q1, B>, <Q2, B>, <Q4, B>}		{0, 0, 500}; {0, 500, 0}; {500, 0, 0}

Tabelle 32: Inferenzen durch kombinierte Aggregationsoperationen, Schritt 1
Eigene Darstellung

Um festzustellen, in welchem Quartal B die Ausgabe 500 getätigt hat, muss der Analyst einige zusätzliche Queries an <QUARTER, CITY> stellen (vgl. Tabelle 33). Aus den Ergebnissen ist ersichtlich, dass nur in Q2 eine Ausgabe von 500 getätigt wurde. Somit hat der Analyst die Arztausgaben von B in Jahr Y1 vollständig inferiert und kann auch die restlichen Zellen von <QUARTER, PATIENT> ableiten.

Q2a-c	MAX / MIN / SUM (quarter = Q1 AND city = Stadt 1)	S2a-c	400 / 200 / 900
Q3a-c	MAX / MIN / SUM (quarter = Q2 AND city = Stadt 1)	S3a-c	500 / 200 / 700
Q4a-c	MAX / MIN / SUM (quarter = Q4 AND city = Stadt 1)	S4a-c	800 / 400 / 1400

<Q1, ?>	{?, ?, 200, 400}; {?, 200, ?, 400}; . . .; {200, 400, ?, ?}
<Q2, ?>	{0, 0, 500, 200}; {0, 500, 0, 200}; . . .; {500, 200, 0, 0}
<Q4, ?>	{0, 0, 600, 800}; {0, 600, 0, 800}; . . .; {600, 800, 0, 0}

Tabelle 33: Inferenzen durch kombinierte Aggregationsoperationen, Schritt 2
Eigene Darstellung

Zu diesen Überlegungen lassen sich zwei Beobachtungen machen, welche als Ausgangspunkte für die Bestimmung der „sicheren" Objekte dienen: Objekte, welche mit dem Zielobjekt nicht verglichen werden können (d.h. in keiner Abhängigkeitsbeziehung stehen) können vernachlässigt werden, da nur Nachfolger Inferenzen auf das Zielobjekt verursachen können. Nachfolger von Objekten aus der Quelle (d.h. den ungeschützten Objekten) sind ebenfalls irrelevant, da sie lediglich redundante Informationen enthalten.[304] Die zu analysierenden Objekte (vgl. Abbildung 29) reduzieren sich beispielsweise für den geschützten Cuboiden <1,2,1> aus BELOW(S_l) mit S_l = {<1,1,2>, <1,2,1>} auf die sog. Basis(S_l, <1,2,1>) = {<1,2,2> , <2,2,1>}.

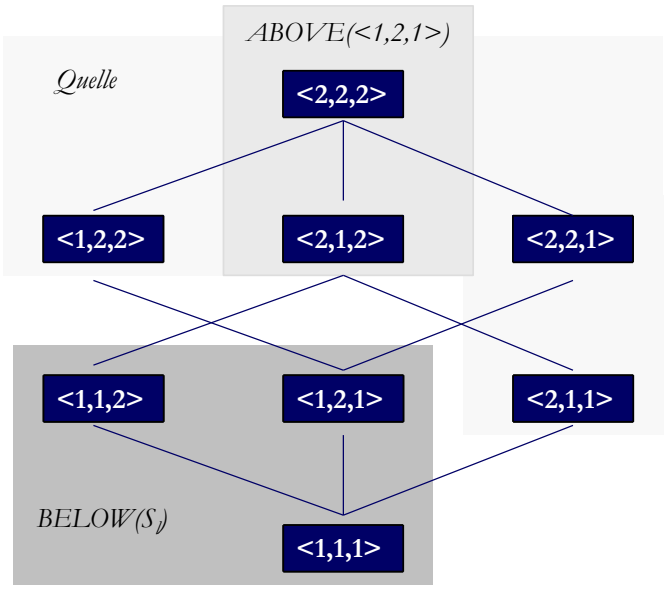


Abbildung 29: Beispiel für eine Basis für m-d Inferenzen
In Anlehnung an WANG/JAJODIA/WIJESEKERA (2007), S. 132

Wenn die Basis mehr als ein Objekt enthält, sind Inferenzen möglich; umgekehrt ist das

[304] Vgl. WANG/JAJODIA/WIJESEKERA (2007), S. 132f. für diesen und die beiden vorhergehenden Sätze

zu einer einelementigen Basis gehörende Cuboid-Set inferenzfrei. Zur Verhinderung von Inferenzen kann folglich eine inferenzfreie Untermenge der Quelle auf Basis genau eines ungeschützten Objekts („root“) konstruiert werden, der vom Zielobjekt abhängig ist. Dieses Objekt sowie alle seine Nachfolger stellen – als Ergebnis der Funktion ABOVE() – das inferenzfreie Set für das Ziel dar.[305]

Ob ein inferenzfreies Set für den Core Cuboid <1,1,1> aus Abbildung 29 existiert, kann nun geprüft werden. Der Root-Cuboid ist der ungeschützte Cuboid <2,1,1>, für den ABOVE(<2,1,1>) = {<2,1,2>, <2,2,2>}. Da Basis(ABOVE(<2,1,1>), <1,1,1>) = {<2,1,1>}, ist das Set inferenzfrei bzgl. <1,1,1>.

Der Zugriff auf alle Cuboiden, die nicht in einem sog. „answerable set“, d.h. einem inferenzfreien Root-Set, enthalten sind, wird restringiert.[306] In Abbildung 30 können bspw. die Cuboiden <ALL, PATIENT> oder <QUARTER, ALL> als Roots für die zu schützenden Objekte in BELOW(<YEAR, REGION>) gewählt werden. Die „answerable sets“ sind respektive {<ALL, ALL>, <ALL, REGION>, <ALL, CITY>, <ALL, PATIENT>} und {<ALL, ALL>, <YEAR, ALL>, <QUARTER, ALL>}.

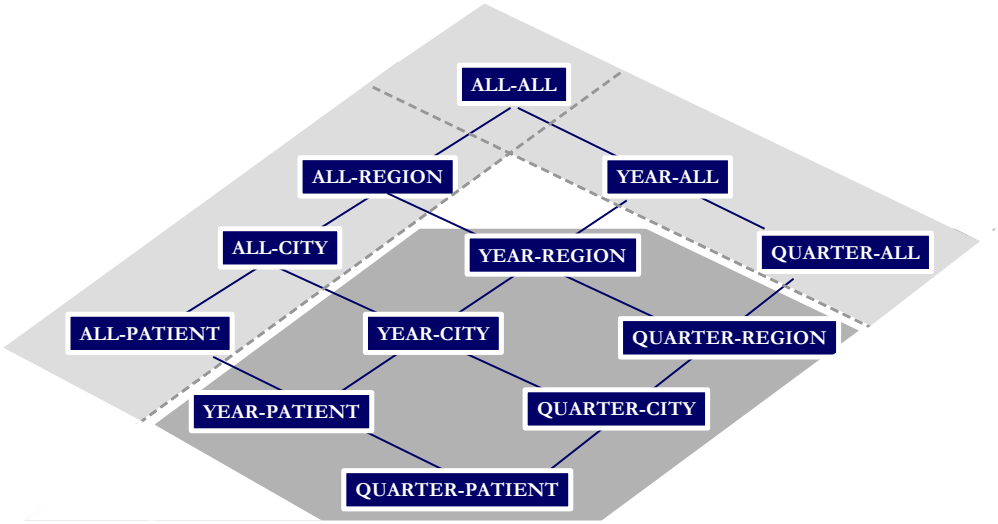


Abbildung 30: Beispielhafte Darstellung alternativer Roots
Eigene Darstellung nach WANG/JAJODIA/WIJESEKERA (2007), S. 151

Da SeCube die Inferenzberechnungen offline durchführt, wird die Online-Performanz des OLAP-Systems dadurch kaum beeinträchtigt. Allerdings kann die Dauer der Berechnung der Inferenzen für große Datenmengen selbst für ein Offline-System problematisch sein, da sie durch die Anzahl an Level- und Slice-Spezifikationen, die Größe des Data

[305] Vgl. WANG/JAJODIA/WIJESEKERA (2007), S. 133f. für den vorhergehenden Absatz
[306] Vgl. ebenda, S. 150

Cube und die Größe des Dependency Lattice determiniert wird. [307] Zudem ist das Verfahren statisch, d.h. die (inferenzbedingte) Zulässigkeit von Queries passt sich nicht dynamisch an das Nutzerverhalten an, wodurch die Analysemöglichkeiten und folglich die Nützlichkeit des OLAP-Systems eingeschränkt werden.[308]

5.2.4 Query-basierte Inferenzkontrolle in OLAP

WANG/JAJODIA/WIJESEKERA (2007) entwickeln für das in Abschnitt 5.1.1 vorgestellte Lattice-Modell zur Disclosure Control in OLAP einen query-basierten Inferenzkontrollmechanismus, dessen Funktionalität der des Audit Expert[309] (vgl. Abschnitt 4.3.1) ähnelt und eine Weiterentwicklung des Verfahrens SeCube (vgl. Abschnitt 5.2.4) darstellt.[310] Ziel ist eine dynamische Online-Inferenzkontrolle, bei der statt Query-Historien lediglich Autorisierungsobjekte gespeichert werden.[311]

Dies bedingt eine Änderung des SeCube-Algorithmus, da nun die Berechnung inferenzfreier Sets bzw. zulässiger Queries nicht mehr ex ante offline erfolgen kann. Statt des inferenzfreien Subsets wird nun ein inferenzfreies Superset auf Basis eines Root-Objekts für die auszuführende Query berechnet.[312]

Abbildung 31 zeigt das Set ABOVE(S_q) für die Query S_q = {<2,2,1,2>, <2,2,2,1>}, und den zu schützenden Cuboiden <1,2,1,1>. Es soll geprüft werden, ob Queries auf die beiden angefragten Cuboiden zulässig sind. Dies erfolgt über die Herleitung (vgl. Abschnitt 5.2.3) des zum Root-Cuboiden C_r gehörigen Supersets ABOVE(C_r). Dieses lässt keine Inferenzen auf den zu schützenden Cuboiden zu; die Query ist sicher.

307 Vgl. WANG/JAJODIA/WIJESEKERA (2007), S. 143f. für diesen und den vorhergehenden Satz
308 Vgl. ebenda, S. 147f.
309 Vgl. CHIN/OZSOYOGLU (1982)
310 Vgl. WANG/JAJODIA/WIJESEKERA (2007), S. 147–167
311 Vgl. ebenda, S. 166
312 Vgl. ebenda, S. 152-156

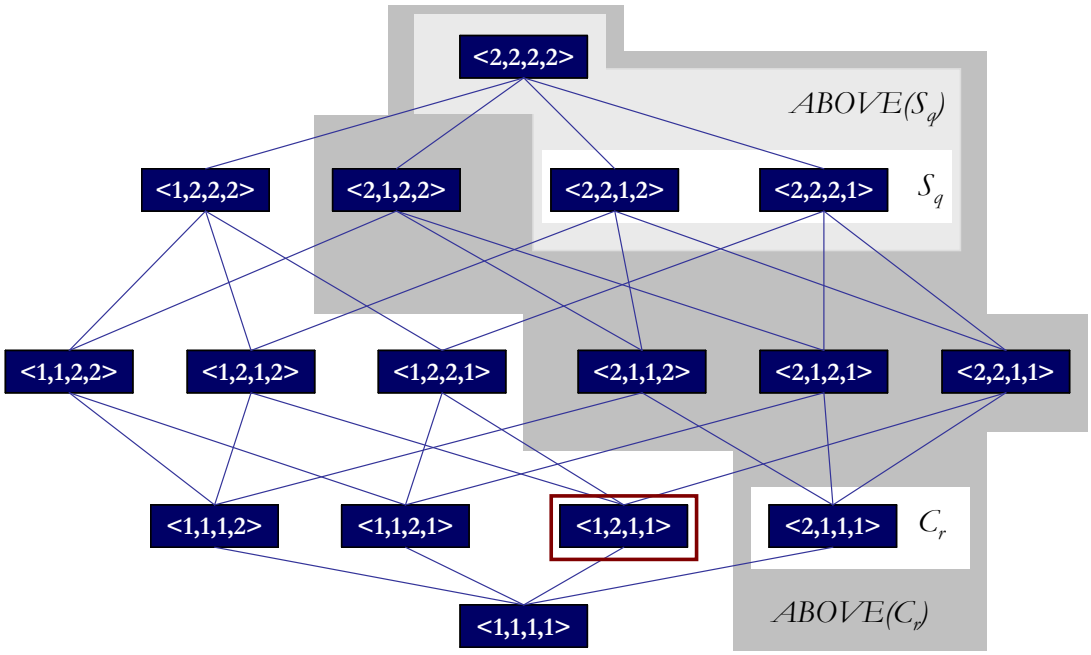


Abbildung 31: Beispielhafte Darstellung eines inferenzfreien Sets
WANG/JAJODIA/WIJESEKERA (2007), S. 152

WANG/JAJODIA/WIJESEKERA (2007, S. 153–156) weisen nach, dass m-d inferenzfreie Sets nur existieren, wenn der zu schützende Cuboid kein Nachfolger des Root-Cuboiden der Query ist. Abbildung 32 zeigt diesen Fall beispielhaft für den zu schützenden Cuboiden <2,1,1,2> und die Query S_q = {<2,1,2,2>, <2,2,1,2>, <2,2,2,1>}. Wird die Query zugelassen, sind durch die zurückgelieferten Cuboiden <2,1,2,2> und <2,2,1,2> Inferenzen auf den Cuboiden <2,1,1,2> möglich.

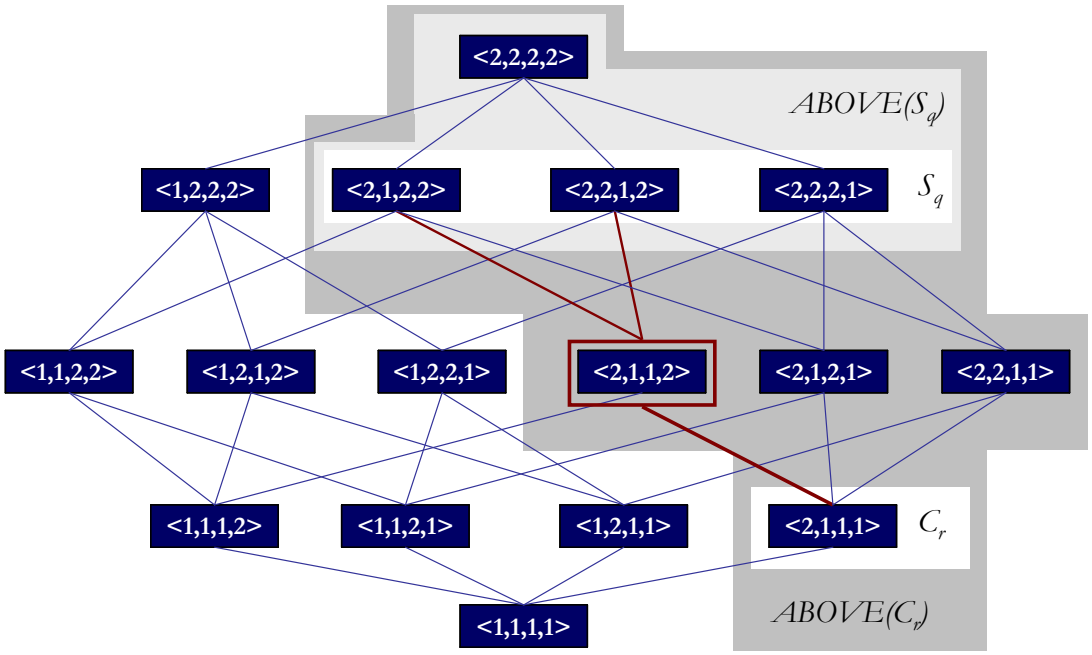


Abbildung 32: Beispielhafte Darstellung von m-d Inferenzen auf Cuboid-Ebene
WANG/JAJODIA/WIJESEKERA (2007), S. 152

Diese Erkenntnis gilt auch auf Slice-Ebene; das sog. „inferierbare Set" einer Query wird nun durch die Kombination des oder der angefragten Cuboiden S_q und des angefragten Slices r_q determiniert. Es enthält alle Zellen, welche durch m-d Inferenzen betroffen sind, d.h. alle Zellen außerhalb des inferierbaren Sets sind sicher. Es muss also die Sicherheit der Schnittmenge des Slices und des Cuboiden, d.h. die überlappenden Zellen, geprüft werden. [313] Für mehrere Slices ergibt sich das inferierbare Set folglich aus der Schnittmenge der Slices mit den Cuboiden aus ABOVE(C_r).[314]

Abbildung 33 illustriert dies am Beispiel zweier Slices r_1 und r_2 und zweier angefragter Cuboiden S_1 = {<QUARTER, PATIENT>} und S_2 = {<YEAR>, <PATIENT>}. Überlappungen der Slices ergeben sich bspw. für <Y1, A>, d.h. die Schnittmenge (r_1, S_2) ∩ (r_2, S_2) ist nicht leer. Offensichtlich ermöglicht diese Query eine Inferenz auf <Q4, Stadt1>. Die Schnittmenge (r_1, S_1) ∩ (r_2, S_1) ist leer, d.h. diese Query ist sicher.

[313] Vgl. WANG/JAJODIA/WIJESEKERA (2007), S. 154-156 für diesen und die beiden vorhergehenden Sätze

[314] Vgl. ebenda, S. 159

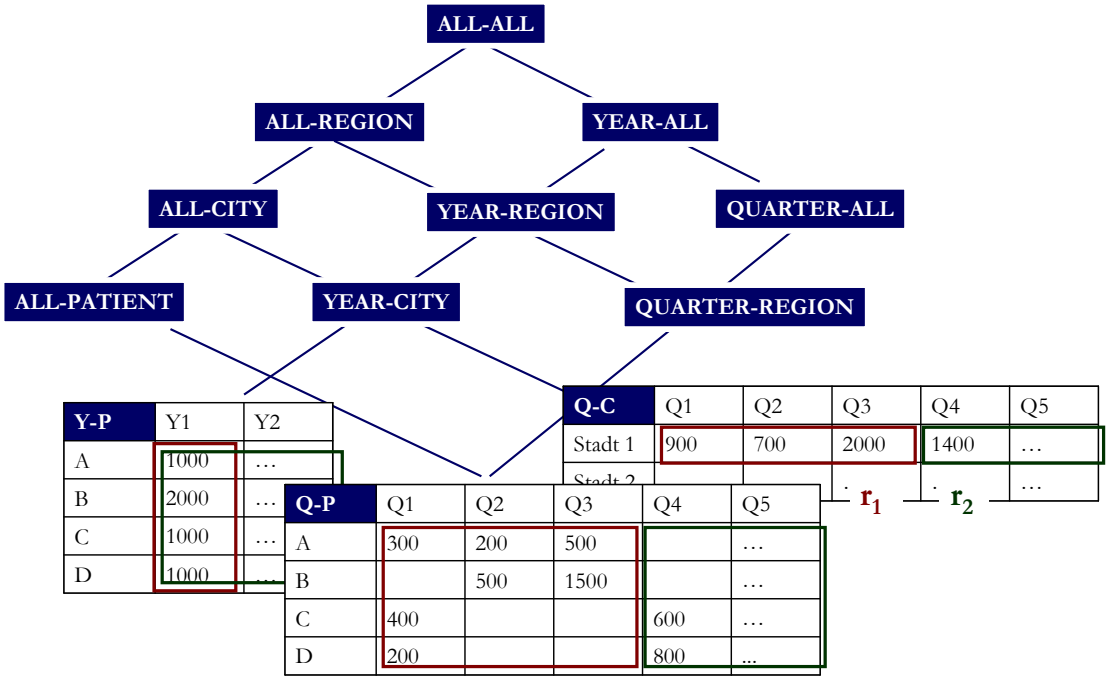


Abbildung 33: Beispielhafte Darstellung von m-d Inferenzen auf Slice-Ebene
WANG/JAJODIA/WIJESEKERA (2007), S. 152

Zur Autorisierung von Queries werden für den Nutzer zwei Relationen R_o und R_q gebildet, die das Autorisierungsobjekt (die Query) und das inferierbare Set des Nutzers als Projektionen auf den Core Cuboid enthalten. Somit kann für jede Zelle t des Core Cuboid ermittelt werden, ob $R_q(t)$ ein Vorgänger eines Cuboiden aus $R_o(t)$ ist. Wenn dies der Fall ist, so überlappen sich das Autorisierungsobjekt und das inferierbare Set, d.h. die Query sollte nicht beantwortet werden.[315] Anstatt einer Query-Historie werden folglich für jeden Nutzer die beiden Relationen gespeichert und aktualisiert, d.h. wenn ein neues Objekt in den Data Cube eingefügt wird, wird eine neue Berechnung des inferierbaren Sets durchgeführt und geprüft, ob sichere Queries auf das neue Objekt möglich sind.[316]

5.3 Bewertung der Lösungsansätze

Die Vorteile und Nachteile der hier behandelten Lösungsansätze zu Zugriffs- und Inferenzkontrolle in OLAP können anhand des in Kapitel 3 erarbeiteten Modells hinsichtlich ihrer Erfüllungsgrade bzgl. der einzelnen Anforderungskriterien und ihrer Auswirkungen auf den (betrieblichen) Nutzen analysiert werden, welcher durch ihre Anwendung entsteht. Grundsätzlich ist eine Verschlechterung des Erfüllungsgrades der Anforderungen

315 Vgl. WANG/JAJODIA/WIJESEKERA (2007), S. 161 für den vorhergehenden Absatz
316 Vgl. ebenda, S. 161-165

zu erwarten; je nach Verfahren werden einzelne Kriterien jedoch weniger stark beeinträchtigt. Die Stärke der einzelnen Effekte ist sehr von der Implementierung der Sicherheitsmechanismen sowie dem betrieblichen Umfeld, bspw. den Geschäftsprozessen und der Klarheit der Aufgabendefinitionen, abhängig. Die im Rahmen dieser Arbeit erarbeitete Darstellungs- und Vergleichsform (vgl. Abschnitt 3.4) ermöglicht eine strukturierte Beschreibung jedes beliebigen Zugriffs- und Inferenzkontrollmechanismus und seine Beurteilung hinsichtlich eines unternehmensspezifisch festlegbaren Zielsystems.

Tabelle 34 gibt einen Überblick über die relativen Vor- und Nachteile der in den Abschnitten 5.1 und 5.2 besprochenen Verfahren.[317] Die Einschätzung der Verfahren bzgl. der einzelnen Kriterien wird im Anschluss diskutiert.

	Lattice-based AC	RBAC	K-IC	P-IC	SeCube	Q-IC
Systemqualität						
▸ **Flexibilität**						
▸ **Performanz**						
▸ **Verfügbarkeit**						
Informationsqualität						
▸ **Vollständigkeit**						
▸ **Korrektheit**						
▸ **Konsistenz**						
▸ **Granularität**						
▸ **Aktualität**						
Nutzen – Anwender						
▸ **Qualität der Datenanalyse**						
▸ **Sicherheit**						
Administrationsaufwand						
▸ **Rechteverwaltung**						
▸ **Aktualisierungen**						
Nutzen – Administratoren						
▸ **Arbeitseffizienz**						

Tabelle 34: Vergleich verschiedener Verfahren zur Disclosure Limitation in OLAP
Eigene Darstellung

Die beiden Verfahren Lattice-based Access Control und RBAC adressieren Möglichkeiten der expliziten Zuweisung von Rechten zu Objekten, während umgekehrt die Inferenzkontrollverfahren Zugriffsrechte implizit festlegen bzw. einschränken.

[317] Rote Markierungen stellen eine dezidierte Verschlechterung der Kriterien dar, rot gestreifte Kriterien eine im Vergleich dazu geringere Verschlechterung. Analog sind die grünen Markierungen zu verstehen. Weiße Kästchen bedeuten, dass die Kriterien kaum oder gar nicht beeinträchtigt werden.

WANG/JAJODIA/WIJESEKERA (2007) plädieren daher für eine Kombination zweier Verfahren (Lattice-based Access Control und SeCube oder query-basierte Inferenzkontrolle, vgl. Abschnitt 5.1.1) und die Abbildung von Zugriffsrechten über Autorisierungsobjekte im Rahmen der Inferenzkontrolle (vgl. Abschnitt 5.2.3). Dies bedingt jedoch einen signifikanten Performanzverlust, wie aus Tabelle 35 hervorgeht. Insbesondere für SeCube ist die Komplexität der Berechnung bemerkenswert: Im schlechtesten Fall wird sie von der Anzahl der Spezifikationen (die auf Slice- und Cuboid-Ebene festgelegt werden), der Größe des Data Cube und der Größe des Dependency Lattice bestimmt. Dies ist für sehr große Datenbestände eine prohibitiv lange Berechnungszeit – insbesondere bei Berücksichtigung regelmäßiger Aktualisierungen des Data Cube.

Die Berechnung erfolgt sowohl bei SeCube wie im Audit-Modell[318], kardinalitätsbasierter und paritätsbasierter Inferenzkontrolle offline, um die vom Anwender wahrgenommene Verzögerung zu minimieren. Query-basierte Inferenzkontrolle hingegen wird online vorgenommen, was zu einem höheren Performanzverlust führt, da alle Zellen der Schnittmenge zwischen dem angefragten Slice und dem Core Cuboid überprüft werden müssen (vgl. Tabelle 35).

[318] Dieses Modell von CHIN/OZSOYOGLU (1982) wird häufig als „Benchmark“ für neu entwickelte Inferenzkontrollverfahren herangezogen [vgl. bspw. WANG/JAJODIA/WIJESEKERA (2007)] und daher der Vollständigkeit halber mit aufgeführt.

Verfahren	Performanz
Audit-Modell	
	▶ Berechnung der Inferenzen in $O(m^2n)$, mit m, n = Dimensionen der Aggregationsmatrix
Kardinalitätsbasierte IC	
	▶ Partitionierung des Cube in $O(n^S)$, mit S= Aggregationsvektoren und S = Kardinalität des Core Cuboids ▶ Berechnung der Inferenzen in O(n)
Paritätsbasierte IC	
	▶ Berechnung der inferenzfreien geradzahlingen MDR-Queries in O(mn), mit m = Queries
SeCube (IC)	
	▶ Offline-Berechnung bis zu maximal $O((r+S) \cdot \|C\| \cdot \|Lat\|)$, mit r, S = Spezifikationen und und C = Größe des Data Cube und Lat = Größe des Dependency Lattice ▶ Online-Verzögerung für Inferenzkontrolle $O(\|S\| \cdot k)$, mit S = angefragte Zellen und k = Dimensionen von C_{core} ▶ Speicherbedarf pro Nutzer $O(\|C_{core}\| \cdot k)$
Query-basierte IC	
	▶ Autorisierung einer Query in O(n) mit $n = \|Slice(r) \cap C_{core}\|$ ▶ Speicherbedarf pro Nutzer $O(\|C_{core}\|)$

Tabelle 35: Bewertung der Performanz von IC-Mechanismen in OLAP
Eigene Darstellung

Die ersten drei Verfahren bestimmen die Zulässigkeit einer Query auf Basis der Query-Historie des Nutzers, während die beiden letzten Verfahren statt der Queries die Menge an Zellen speichern, auf die der Nutzer noch zugreifen darf. Dies ist im Fall von SeCube das „answerable set“ und im Fall von query-basierter Inferenzkontrolle das „inferable set“ (vgl. Abschnitte 5.2.3 und 5.2.4). Das zulässige Set an Queries muss dann nicht mehr bekannt und gespeichert sein, sondern kann in Abhängigkeit der tatsächlichen Nutzung bestimmt werden (vgl. Tabelle 36).

Flexibilität und Verfügbarkeit	KIC	PIC	SeCube	QIC
▶Offline (statisch)	✓	✓	✓	
▶Pfadabhängige Zulässigkeit von Queries	✓	✓	✓	✓
▶A-Priori-Festlegung zulässiger Queries	✓	✓		
▶ Beschränkung auf Skeleton Queries	✓			
▶ Verbot kompletter Cubes bei gefährdeten Zellen	✓			
▶Beschränkung auf geradzahlige MDR		✓		
▶ Komplizierte Level- und Slice-Spezifikation			✓	✓

Tabelle 36: Bewertung der Flexibilität und Verfügbarkeit bei IC-Mechanismen in OLAP
Eigene Darstellung

In allen Fällen kann dies jedoch zu einer massiven Verschlechterung der Datenversorgung einzelner Nutzer führen, wenn Queries in einer „ungeschickten" Reihenfolge gestellt werden. „Ungeschickt" meint in diesem Zusammenhang, dass ein Nutzer die hinter allen auf Auditing basierenden Modellen stehende Annahme verletzt, dass Queries nach absteigender Wichtigkeit an das System gestellt werden. Trifft diese Annahme zu, ist der Informationsverlust aus nicht mehr zulässigen Queries theoretisch akzeptabel. Sie ist allerdings in höchstem Maße unrealistisch, wenn man bedenkt, dass OLAP-Anwendungen zur Datenexploration verwendet werden und der Nutzer a priori häufig nicht weiß bzw. wissen kann, welche Queries am wichtigsten sind. Der aus nicht mehr zulässigen Queries resultierende Informationsverlust kann daher – anders als in den theoretischen Modellen angenommen – beträchtlich sein. Auch der Administrationsaufwand kann negativ beeinflusst werden: Erhält ein Nutzer nicht die für seine Arbeit notwendigen Informationen (und weiß aber vielleicht auf Basis früherer Queries, dass diese existieren), so wird er um Löschung seiner Query-Historie oder zumindest um die entsprechende Erweiterung seiner Zugriffsrechte bitten. Dies impliziert – falls eine konsistente Erweiterung der Zugriffsrechte überhaupt möglich ist – eine Neuberechnung der zulässigen Queries bzw. Sets. Diese Vorgehensweise unterliefe auch den Zweck eines Inferenzkontrollmechanismus, da auf genau die Informationen Zugriff gewährt würde, die vorher aus Sicherheitsgründen gesperrt waren.

Weitere Einschränkungen der Flexibilität ergeben hinsichtlich der zulässigen Aggregationsoperationen (hier schneiden kardinalitäts- und paritätsbasierte Inferenzkontrolle am schlechtesten ab) und der Genauigkeit, mit der Autorisierungsobjekte spezifiziert werden

können. Kardinalitätsbasierte Inferenzkontrolle ermöglicht lediglich eine Sicherung von Skeleton Queries, was eine noch gravierendere Einschränkung bedeutet als die Restriktion auf geradzahlige MDR Queries bei paritätsbasierter Inferenzkontrolle. Kardinalitätsbasierte Inferenzkontrolle kann zudem die Unterdrückung kompletter Cubes verursachen, in denen sich gefährdete Zellen befinden. Die anderen drei Verfahren ermöglichen eine zielgenauere Limitation von Inferenzen, indem bspw. nur der Zugriff auf Slices mit gefährdeten Zellen verboten wird. Allerdings resultiert daraus insbesondere für SeCube und query-basierte Inferenzkontrolle der Nachteil, dass die Spezifikation der Autorisierungsobjekte hochgradig kompliziert ist: Sie muss für jeden Slice und jeden Level erfolgen. Im Hinblick auf die Implementierung und Verwaltung der Autorisierungsobjekte und ebenso der Subjekte bzw. der Nutzer, denen Zugriff auf bestimmte Objekte gewährt werden soll, erscheint die Praktikabilität dieser Ansätze höchst zweifelhaft. Die Anzahl von und die Abhängigkeiten zwischen Slices und Cuboiden sind bei großen Datenbeständen astronomisch hoch. Dies verlangt neben hoher Expertise bzgl. der Modellierung des OLAP-Systems sowie der mathematischen Funktionsweise des Inferenzkontrollmechanismus ein tiefgehendes Verständnis der Geschäftsprozesse sowie der daraus resultierenden Zugriffsrechtestruktur. Falls durch die Festlegung bzw. Aktualisierung der Zugriffsrechte, d.h. der Autorisierungsobjekte für einen Nutzer, Inferenzen entstehen und zur Sicherstellung der Verfügbarkeit der notwendigen Daten zusätzliche Adaptionen und Dokumentationen erfolgen müssen, dürfte der Administrationsaufwand prohibitiv ansteigen.

Im Hinblick auf die Informationsqualität werden lediglich die Kriterien Korrektheit und Konsistenz von keinem der Verfahren beeinträchtigt. Die Kriterien Vollständigkeit und Granularität werden von den kardinalitäts- und paritätsbasierten Verfahren am stärksten eingeschränkt, da sie erstens nur bestimmte Aggregationsoperationen zulassen und zweitens a priori ein Set an zulässigen Queries bestimmen. SeCube und query-basierte Inferenzkontrolle erlauben eine vollständigere Sicht - wegen des Wegfalls der Beschränkung der verwendbaren Aggregationsoperationen und im Falle von query-basierter Inferenzkontrolle der dynamischen Bestimmung zulässiger Queries. Bei Zugriffskontrollverfahren ist der Erfüllungsgrad dieses Kriteriums stark von der konkreten Ausgestaltung der Rechte abhängig. In Abgrenzung vom Kriterium der Verfügbarkeit werden dem Nutzer keine Daten vorenthalten, welche für seine Arbeit notwendig sind, sondern lediglich zusätzliche bzw. detailliertere Daten, welche er zur vollständigen bzw. genaueren Analyse einer Situation bzw. eines Musters in den Daten benötigt. Diese Wirkung ist in gewissem Maße allerdings durchaus intendiert; Zugang zu feingranularen Daten für eine umfassende Analy-

se kann auch die (nicht gewünschte) Kenntnis des Core Cuboids oder weiterer geschützter Objekte bedingen.

Die Aktualität der Daten ist bei allen fünf Ansätzen potentiell problematisch. Hier ist zwischen der Aktualisierung der Daten ohne Änderung der zugrunde liegenden Datenstruktur (bspw. Update der aktuellen Geschäftszahlen) und mit Änderung der Datenstruktur aufgrund einer Veränderung der Datenbasis (bspw. Integration eines zusätzlichen DW) oder organisatorischer Veränderungen zu unterscheiden. Im ersten Fall schneiden die Zugriffskontrollverfahren besser ab, da keine Respezifizierung der Zugriffsrechte vonnöten ist, während für die Inferenzkontrollverfahren eine Neuberechnung der potentiellen Inferenzen erforderlich ist. Der zweite Fall ist für beide Arten von Verfahren schwierig zu lösen, da er eine Neudefinition von Zugriffsrechten bedingt bzw. zusätzlich potentielle Inferenzen identifiziert werden müssen. Insgesamt schneiden die Inferenzkontrollmechanismen hinsichtlich dieses Kriteriums schlechter ab.

Auf Basis dieser Überlegungen lässt sich vermuten, dass die Qualität der Datenanalyse bei kardinalitäts- oder paritätsbasierter Inferenzkontrolle am meisten leidet, da Flexibilität, Verfügbarkeit und Informationsqualität stark eingeschränkt werden. Der geringste negative Einfluss wird für die Verfahren der Zugriffskontrolle erwartet, da sie den geringsten Effekt auf Flexibilität (angenommen, dass die Rechtedefinition nicht außergewöhnlich restriktiv erfolgt) und Performanz besitzen. Hinsichtlich ihrer Performanz schneiden SeCube und query-basierte Inferenzkontrolle am schlechtesten ab.

Aus der Perspektive der Administratoren eines OLAP-Systems und des Sicherheitsmechanismus ist RBAC hinsichtlich der Verwaltung der Rechte und des Updates von Daten am positivsten zu beurteilen (vgl. Tabelle 37[319]).

[319] Rot markierte Einträge signalisieren eine mögliche, jedoch aufwendige Änderung. Leere Zellen weisen darauf hin, dass das jeweilige Verfahren eine Aktion nicht vorsieht. Blau markierte Einträge signalisieren Änderungen, für welche das jeweilige Verfahren explizit gute Leistungsfähigkeit aufweist (vgl. die relevanten Abschnitte in Kapitel 5).

Rechteverwaltung	Lattice	RBAC	KIC	PIC	SeCube	QIC
▶ Vergabe von Rechten	✓	✓	✓	✓	✓	✓
▶ Entzug von Rechten	✓	✓				
▶ Bündelung von Rechten		✓				
▶ Änderung der Rechtestrukturen	✓	✓	✓	✓	✓	✓
▶ Level- und Slice-Spezifikation	✓	✓			✓	✓
Aktualisierung	**Lattice**	**RBAC**	**KIC**	**PIC**	**SeCube**	**QIC**
▶ Update der Daten	✓	✓	✓	✓	✓	✓
▶ Änderung der Datenstruktur (Integration)	✓	✓	✓	✓	✓	✓
▶ Änderung der Datenstruktur (organisatorisch)	✓	✓	✓	✓	✓	✓

Tabelle 37: Bewertung der Administrierbarkeit von OLAP mit IC-Mechanismen
Eigene Darstellung

Zwar erfordert der Einsatz von RBAC einen hohen Aufwand bei Änderungen der Rechtestrukturen oder der organisatorisch bedingten Datenstrukturen, jedoch sind Vergabe und Entzug von Rechten durch ihre Bündelung in Rollen relativ einfach möglich. Alle anderen Verfahren sind sehr viel schwieriger zu administrieren, da für jedes Autorisierungsobjekt separat Rechte festgelegt bzw. entzogen werden müssen (für SeCube bspw. auf Level- und Slice-Ebene). Eine Änderung der Rechtestrukturen verursacht hier demgemäß einen sehr hohen Aufwand. Ähnliches gilt für das Update der Datenbasis. Die query-basierte Inferenzkontrolle ist neben den Zugriffskontrollverfahren (bei denen sich kaum Komplikationen ergeben) am besten in der Lage, damit umzugehen, da sie ein dynamisches Verfahren ist und Inferenzen auf neue Daten zur Laufzeit erst bei tatsächlichen Abfragen auf diese Daten identifiziert werden müssen. Für die kardinalitäts- und paritätsbasierte Inferenzkontrolle hingegen muss die Menge der zulässigen Queries erweitert werden, d.h. eine Neuberechnung der Partitionierung bzw. der geradzahligen MDR Queries ist notwendig. Da SeCube ein statisches Verfahren ist, muss auch hier (offline) eine Neuberechnung der Inferenzen stattfinden. Im Hinblick auf die Änderung von Datenstrukturen schneidet kein Verfahren gut ab. In dem Maße wie Änderungen der bestehenden Rechtestrukturen durch Änderungen der Datenstrukturen notwendig werden, ist der damit verbundene Aufwand bei allen Ansätzen sehr hoch. In RBAC müssen bestehende Rechtebündel und Rechtehierarchien neu definiert bzw. erweitert werden. Lattice-based Access Control, SeCube und query-basierte Inferenzkontrolle bedingen eine Respe-

zifierung auf Level- und Slice-Basis. Kardinalitätsbasierte und paritätsbasierte Inferenzkontrolle erfordern eine völlige Neuberechnung der zulässigen Queries.

Im Hinblick auf die Sicherheit, welche die einzelnen Verfahren ermöglichen, ist hierbei der Verlust der „alten" Query-Historien respektive der „answerable sets" (SeCube) oder inferierbaren Sets problematisch. Deren Verwendbarkeit kann mit dem Ausmaß der Änderungen in den Datenstrukturen so stark sinken, dass eine Löschung unumgänglich ist. Tatsächlich hat der Nutzer jedoch noch Kenntnis über den Wert der vor Änderung der Datenstruktur abgefragten Daten. Die Veränderung von Datenstrukturen kann somit Inferenzen ermöglichen, die vom Kontrollmechanismus völlig unerkannt bleiben. Werden die Historien vorgehalten, kann der Fall eintreten, dass innerhalb der neuen Strukturen kaum noch Daten für einen Nutzer sichtbar werden, da sie Inferenzen hinsichtlich der früher durchgeführten Abfragen und Aggregationen verursachen könnten. SeCube und query-basierte Inferenzkontrolle ermöglichen zwar theoretisch das größte Maß an Sicherheit (Verhinderung von m-d Inferenzen bei einer Vielzahl von Aggregationsoperationen), jedoch gilt dies praktisch nur eingeschränkt bei einer Neuimplementierung bzw. für den Fall, dass bekannt ist, welche Zellen des Data Cubes einem Nutzer bereits bekannt sind. Diese Einschränkung gilt auch für kardinalitäts- und paritätsbasierte Inferenzkontrolle.

Insgesamt bietet somit Zugriffskontrolle auf Basis von RBAC das aufwandsärmste Verfahren, während SeCube und query-basierte Inferenzkontrolle hinsichtlich des Sicherheitslevels am besten abschneiden. Allerdings gilt dies vornehmlich auf theoretischer Ebene; die oben diskutierten Nachteile bzgl. Implementierungs- und Administrationsaufwand schränken die Umsetzbarkeit dieser Verfahren so stark ein, dass sie für den Einsatz in der betrieblichen Praxis kaum anwendbar sind. Kardinalitäts- und paritätsbasierte Inferenzkontrolle bieten aufgrund der Beschränkung auf bestimmte Queries nur ein geringes Maß an Sicherheit, das den nicht unbeträchtlichen Implementierungs- und Verwaltungsaufwand sowie die Verschlechterung der Qualität der Datenanalysen kaum rechtfertigt.

Abschließend lassen sich folgende Forderungen an ein praktikables Verfahren zu Disclosure Limitation formulieren:

- Flexible Rechteverwaltung. Vergabe, Entzug und Änderung von Rechten muss mit möglichst geringem Aufwand möglich sein.
- Automatisierung der Spezifizierung von Rechten. Die Berechnung der zugelassenen Zellen, Slices und Cuboiden muss möglichst ohne Eingreifen der Administratoren möglich sein.

- Passgenaue Rechte für explorative Datenanalyse. Spezifizierung und Vergabe von Rechten muss unter Berücksichtigung der explorativen Natur von OLAP-Anwendungen erfolgen.
- Inkrementelle Erweiterung in einem abgestuften Genehmigungsverfahren. Sollten sich Zugriffsrechte als zu restriktiv erweisen oder Updates der Daten erfolgen, muss eine entsprechende Adaption der Rechte möglichst aufwandsarm möglich sein, ohne die Sicherheit schwerwiegend zu beeinträchtigen.
- Adaptierbarkeit an neue Datenstrukturen. Sollten Veränderungen der Datenstrukturen erfolgen, sollte keine Neudefinition der Rechtestruktur notwendig werden.

6 ZUGRIFFSKONTROLLE AUF BASIS VON INTERESSENSSCHWERPUNKTEN

In diesem Kapitel wird in Abschnitt 6.1 ein eigener Ansatz der Zugriffskontrolle für OLAP vorgestellt. Abschnitt 6.2 diskutiert verschiedene Alternativen zur Ausgestaltung des Ansatzes hinsichtlich der Bestimmung des Arbeitskontextes der Anwender. Die Implementierung einer möglichen Umsetzung erfolgt in einem bewusst übersichtlich gehaltenen Beispiel im Rahmen eines SAP BI 7.0-System in Abschnitt 6.3.

6.1 Beschreibung des Ansatzes

Zunächst werden die grundlegenden Überlegungen hinter dem hier vorgestellten Ansatz dargestellt (vgl. Abschnitt 6.1.1). Im Anschluss wird das Vorgehensmodell zur Schaffung einer Zugriffskontrolle auf Basis von Interessensschwerpunkten auf Fachkonzeptebene beschrieben (vgl. Abschnitt 6.1.2).[320] Es folgt eine kurze Bewertung des Ansatzes (vgl. Abschnitt 6.1.3).

.

6.1.1 Grundlegende Idee

In Abschnitt 1.2 wurde dargelegt, dass sowohl Zugriffs- als auch Inferenzkontrolle in OLAP in der Praxis stark vernachlässigt wird. In Abschnitt 5.3 wurden mögliche Gründe dafür aus der Analyse vorliegender Konzepte abgeleitet. Am schwersten wiegt offenbar der enorme administrative Aufwand, der sich durch eine differenzierte Zugriffskontrolle ergibt - sei es lediglich als sehr granulare Festlegung von Zugriffsrechten, um den Nutzer auf die für ihn wirklich relevanten Teile des Datenwürfels zu beschränken oder als Teil eines Inferenzkontrollmechanismus. Es scheint daher besonders lohnend, Ansätze zu entwickeln, die eine möglichst sinnvoll differenzierte – im Sinne der Berücksichtigung des Arbeitskontextes der Nutzer – und automatisierbare Zuteilung von Berechtigungsobjekten zu Nutzern oder Nutzergruppen ermöglichen. (Im Weiteren wird immer von Nutzergruppen die Rede sein, wobei dies auch einzelne Nutzer sein können. So wird im Implementierungsbeispiel der einfacheren Übersicht halber mit einzelnen Nutzern gearbeitet.)

[320] Es wird darauf verzichtet, den Ansatz formal mathematisch auszudrücken, da er sich aufgrund seiner Einfachheit auch ohne den Rückgriff auf solch eine Darstellungsweise präzise beschreiben lässt.

Es wurde in Kapitel 5 deutlich, dass die komplexe Implementierung präziser Inferenzkontrollmechanismen in OLAP gerade auch deshalb ein praktisch kaum zu bewältigendes Ausmaß annimmt, weil - anders als bei SDB - die notwendigen Einstellungen des Sicherheitssystems für eine Vielzahl von Nutzergruppen vorgenommen werden müssen. Häufig werden sich zudem die Restriktionen durch eine Inferenzkontrolle und eine wünschenswert sinnvolle explorative Datenanalyse durch den Nutzer nicht in Einklang bringen lassen, da die existierenden Inferenzkontrollmechanismen für OLAP keine Abwägung zwischen dem Nutzen eines (aggregierten oder nicht aggregierten) Zellwertes für die Analyse und dem Schaden durch eventuelle Inferenzen durch dessen Offenlegung vorsehen. Dieses Thema ist auch in SDB noch nicht wirklich überzeugend gelöst worden[321] und ist aufgrund des explorativen, schwer vorhersehbaren Charakters der Datenanalyse in OLAP in diesem Bereich offensichtlich (neben dem Administrationsaufwand) ein weiteres Kernhindernis für die praktische Anwendbarkeit von Inferenzkontrollmechanismen. Darüber hinaus stellt sich die Frage, ob eine präzise Inferenzkontrolle - abgesehen von absolut sicherheitskritischen Bereichen - in einer großen Anzahl von Einsatzszenarien von OLAP-Anwendungen überhaupt notwendig ist. Wenn bspw. ein Unternehmen einer Unternehmensberatung einen OLAP-Zugriff auf Teile seiner Umsatz- und Kostendaten gibt, wird es weniger um den Schutz von Einzelwerten gehen. Das Sicherheitsinteresse des Unternehmen wird vielmehr darin bestehen, dass nicht externe „curious employees who can't resist the temptation to explore" [322] (vgl. Abschnitt 1.2) ein zu komplettes Bild des Unternehmens erhalten.

Selbst in Bereichen, in denen Inferenzkontrolle nicht notwendig ist, besteht somit Bedarf an Zugriffskontrolle. Dies ergibt sich aus der Tatsache, dass sich der Anwenderkreis von OLAP-Anwendungen stark ausgeweitet hat - insbesondere durch die immer stärker werdende Integration in ERP-Anwendungen. (vgl. Abschnitt 1.2) Waren OLAP-Anwendungen früher dem höheren Management vorbehalten, greifen jetzt auch vermehrt Sachbearbeiter auf solche Anwendungen zu.[323] Für das höhere Management sind Zugriffskontrollen aufgrund ihrer Befugnisse und ihres berechtigten Interesse an allen Unternehmensbelangen kaum sinnvoll. Hier macht ggf. eine Zugriffsbeschränkung hinsichtlich sehr granularer Werte Sinn. Anders verhält es sich bei Mitarbeitern niedrigerer Hie-

321 Vgl. WILLENBORG/DE WAAL (2001), S. 96f.
322 KIMBALL (1997), S. 14
323 Vgl. PRIEBE (2009), S. 166

rarchiestufen, die OLAP-Anwendungen zur Analyse eines wesentlich kleineren Interessensbereichs verwenden sollten. Der Sachbearbeiter, der für ein bestimmtes Produkt zuständig ist, soll ausschließlich in diesem Umfeld analysieren.

Vor dem Hintergrund dieser Ausführungen stellt sich also folgende Frage: Wie kann man für Benutzer automatisch den Datenbereich bestimmen, der für ihre Analyse notwendig ist, ohne sie für unverhältnismäßig große Bereiche der Würfelstruktur zu berechtigen bzw. in einem unverhältnismäßig großem Aufwand nach sorgfältiger Evaluierung der relevanten Daten pro Nutzergruppe eine sehr große Anzahl kleinster Würfelbereiche „manuell" zuweisen zu müssen.

Diese Anforderungen berücksichtigt der vorgestellte Ansatz, indem ein oder mehrere Interessensschwerpunkte (iSWP) pro Nutzergruppe bestimmt werden. Ein Interessensschwerpunkt entspricht einem bestimmten Hierarchiestufenelement.

Bestehende Ansätze der Disclosure Limitation in OLAP, beruhen meist auf der Zuweisung von Teilbereichen eines Datenwürfels, die durch einen Teil eines Hierarchiebaums eingegrenzt werden. So wird der Zugriff auf alle Daten erlaubt, die einem bestimmten Hierarchiestufenelement und den untergeordneten Hierarchiestufenelementen zugeordnet sind. Dies ist naheliegend, da die einem Hierarchiestufenelement untergeordneten Elemente in einem Sinnzusammenhang in Bezug auf OLAP-spezifische Analysen stehen. Allerdings ergibt sich diese Sinnhaftigkeit vor allem im Rahmen der Navigation, also im Rahmen einer dynamischen Analysetätigkeit. Hier bieten Hierarchien dem Anwender die Möglichkeit, seine Analyse zunächst mit reduzierter Komplexität/Granularität zu beginnen und dann insbesondere durch Drill-Downs detailliertere Nachforschungen anzustellen. Oft genügt die Einteilung einer Hierarchie schlicht bestimmten organisatorischen Gegebenheiten des Unternehmens, bspw. die geographische Einteilung in Verkaufsgebiete. Gerade an diesem Beispiel zeigt sich deutlich, dass eine Vergabe der Zugriffrechte (ausschließlich) auf Basis der Hierarchie wenig Sinn macht. Ein Sachbearbeiter, der für eine Stadt (iSWP in der Dimension Region) in einem Verkaufsgebiet zuständig ist, kann in einer OLAP-Datenanalyse nur dann sinnvoll arbeiten, wenn er die Kennzahlen, die „seiner Stadt" zugeordnet sind, mit den Kennzahlen ins Verhältnis setzen kann, die zu Städten gehören, die entweder aufgrund ihrer Situation vergleichbar sind oder deren Kennzahlenentwicklung in einem Zusammenhang zu denen „seiner Stadt" stehen. In diesem einfachen Fall wären für den Sachbearbeiter die Kennzahlen der Städte in der unmittelbaren Umgebung „seiner Stadt" von Interesse - unabhängig davon, ob sie im gleichen Hierarchiecontainer liegen oder nicht. Damit Zugriffe auf Elemente „in der Nähe" von iSWP

automatisch bestimmt werden können, wird hier die Aufstellung einer Abstandsmatrix für Elemente auf einer auszuwählenden Hierarchiestufe der für iSWP geeigneten Dimensionen vorgeschlagen.

Da sich der Nutzerkreis von OLAP-Anwendung inzwischen über die komplette Unternehmenshierarchie erstreckt,[324] sollte auch die hierarchische Position eines OLAP-Anwenders (neben seiner Nutzergruppe(n)) Berücksichtigung finden. Hier liegt es nahe, über eine Art „Radius um den oder die Interessensschwerpunkt(e)“ (Interessensradien) zu regeln, welche Hierarchiestufenelemente im „Umkreis“ berechtigt werden sollen (Interessensbereich).

6.1.2 Modellbeschreibung

Es wird davon ausgegangen,

(1) dass bereits eine Datenwürfelinstanz vorliegt, die alle Daten beinhaltet,
(2) dass die Nutzer(gruppen) dieses Datenwürfels bereits bestimmt wurden und
(3) dass die Nutzergruppen ggf. bereits in Hierarchieebenen untergliedert wurden

Es geht nun darum, die Zugriffsobjekte pro Nutzergruppe und Hierarchielevel festzulegen. Aus dem vorangegangenen Absatz lassen sich bereits alle Schritte ableiten, die für eine Modellierung der erforderlichen Daten für eine Zugriffskontrolle auf Basis von iSWP erforderlich sind und in Tabelle 38 stichpunktartig dargelegt wurden.

[324] Vgl. PRIEBE (2009), S. 166

iSWP-Vorgehensschritte (Basisdaten)	
1	Bestimmung der Dimensionen (iDIM) bzw. Hierarchien (iHIER), für die Interessensschwerpunkte (iSWP) festgelegt werden sollen.[325]
2	Bestimmung der Hierarchiestufe (iHS), auf der die iSWP festgelegt und zwischen deren Stufenelementen die Abstände bestimmt werden sollen, pro iHIER. Daraus ergeben sich die relevanten Stufenelemente (iSE).
3	Bestimmung der Abstände (iabst) zwischen den iSE derselben iHS.
4	Bestimmung der Interessensradien (iRAD bzw.) pro Nutzergruppe (NUTZ), Stufe in der Organisation (ORGA) und iHS.
5	Bestimmung der Interessensschwerpunkte (iSWP) pro Nutzergruppe und iHS.

Tabelle 38: Bestimmung der Interessensschwerpunkte
Eigene Darstellung

Aus diesem Vorgehen ergibt sich das folgende Datenschema als Entity-Relationship-Schema modelliert (vgl. Abbildung 34). Es wird realistischer Weise von einer eindeutigen Zuordnung iSE → iHS → iHIER ausgegangen.

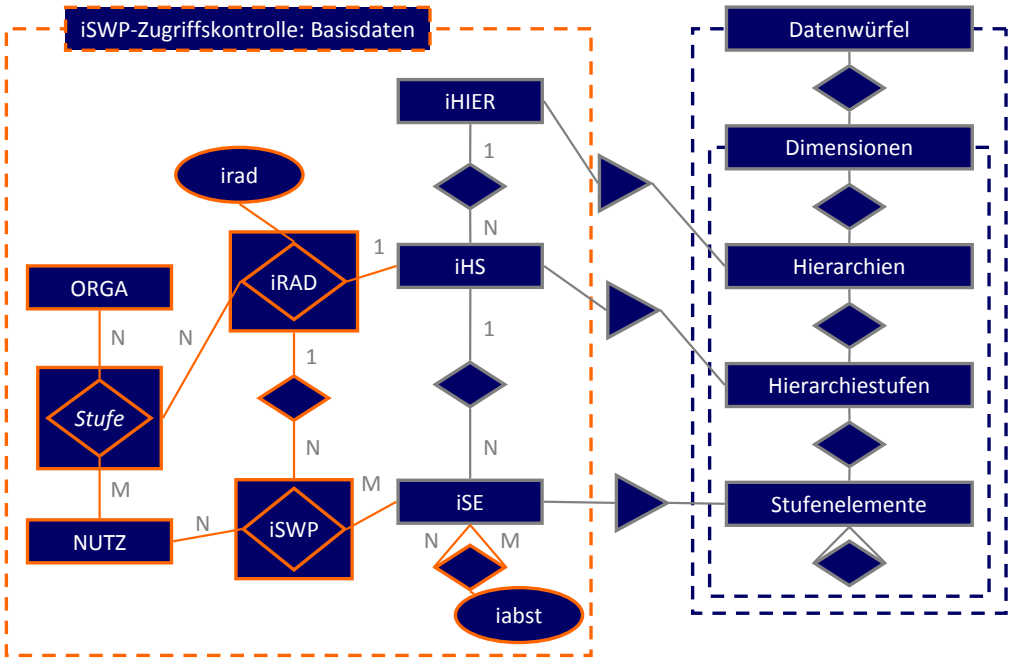


Abbildung 34: Basisdaten des iSWP-Ansatzes
Eigene Darstellung

zu Schritt 2: Bestimmung der Hierarchiestufe. Grundsätzlich kann jede Hierarchiestufe für iHS gewählt werden, wobei hier nur die unterste Stufe diskutiert werden soll, da diese Ein-

[325] Präziser handelt es sich um eine spezielle Hierarchie (mit nur einem Hierarchiepfad) einer Dimension. Hier wird davon ausgegangen, dass nur eine Hierarchie mit nur einem Pfad pro Dimension vorliegt. Da die Berechnung der Interessensbereiche auf Basis der Stufenelemente einer Stufe eines Hierarchiepfads erfolgt, werden alle anderen Hierarchiepfade, die diese Stufenelemente umfassen, abgedeckt.

schränkung auch für die empirische Untersuchung des Modells (vgl. Kapitel 7) vorgesehen ist. Dies hat zwei nahe liegende Gründe. Zum einen erhält man nur dann eine feingranulare Zugriffskontrolle, wenn Abstandsmaße und Interessensschwerpunkte auf sehr tiefer Hierarchieebene angeordnet sind. Wären sie auf einer hohen Ebene angeordnet, müsste man festlegen, ob die untergeordneten Knoten der zugelassenen Stufenelemente im Umkreis der iSWP ebenfalls für den entspr. Nutzer freigegeben werden sollten. Bejahte man dies prinzipiell, hätte er Zugriff auf alle untergeordneten Knoten und man würde die Idee der an Interessensschwerpunkten ausgerichteten Datenpräsentation ad absurdum führen. iSWP und iRAD nehmen jedoch eine implizite Abbildung der Berechtigung auf Hierarchieknotenebene vor. Nutzer sollten alle Elemente einer Hierarchieebene sehen, wenn diese für ihre Arbeitsaufgaben (Arbeitskontext) relevant sind. Nutzergruppen mit einer höheren hierarchischen Position in der Organisation wird sinnvollerweise ein großer Radius zugewiesen, so dass alle Elemente für sie sichtbar sind. Für Nutzergruppen auf niedrigeren hierarchischen Ebenen (der Organisation) ist dies grds. nicht wünschenswert. Gehören jedoch alle Elemente einer Hierarchieebene zum Arbeitskontext einer Nutzergruppe, d.h. sind die Abstände zwischen iSWP und den Elementen gering, so befinden sie sich innerhalb des Interessensradius. Es wäre auch eine Kombination der iSWP mit explizit (manuell) eingetragenen Berechtigungen möglich, so dass die Nutzergruppen Zugang zu der Vereinigungsmenge der jeweils zugänglichen Daten erhalten würde. Da hierbei jedoch wiederum hoher Administrations- und Aktualisierungsaufwand entsteht (neben einer Minderung der Sicherheit) und somit dem Ziel des hier vorgeschlagenen Ansatzes entgegensteht, wird diese Möglichkeit im Folgenden nicht betrachtet.

Ein weiterer Grund, iHS als granularste Ebene zu wählen, liegt darin, dass sich Abstandsmaße verlässlicher zwischen konkreten Objekten bestimmen lassen als zwischen (abstrakteren) Klassifikationen dieser Objekte, da durch die Generalisierung auf höheren Hierarchieebenen Attribute zur Abstandsmaßbildung verloren gehen.

Die Systematik des Modells würde grds. auch die Einführung unterschiedlicher Hierarchiestufen für iSWP und iabst erlauben. Allerdings geht so viel von der intuitiven Verständlichkeit es Modells verloren, was im Sinne einer praktikablen Disclosure Limitation für OLAP nicht sinnvoll scheint. In der folgenden Abbildung 35 wurde die niedrigste Hierarchiestufe für iHS gewählt.

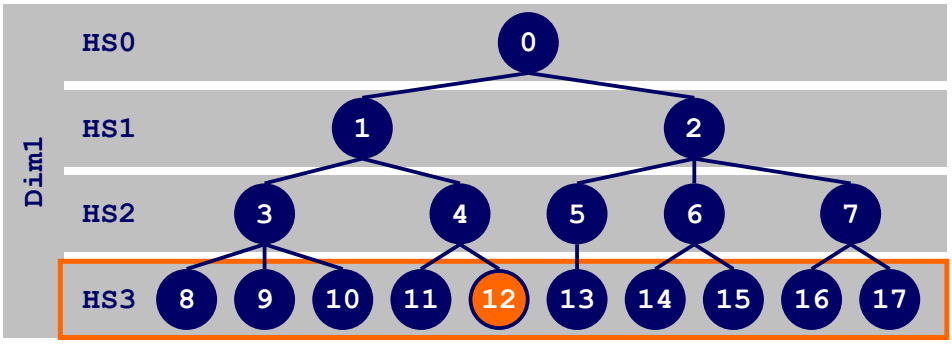


Abbildung 35: Hierarchiestufe (iHS) für Abstände und Interessensschwerpunkte
Eigene Darstellung

zu Schritt 3: Bestimmung der Abstände. Dies ist der aufwendigste Schritt des Verfahrens, wenn nicht bereits ein Abstandsmaß intuitiv einleuchtend ist und die entsprechenden Werte verfügbar sind. Es ist festzuhalten, dass in den meisten Fällen die Abstände zwischen denselben beiden Stufenelementen in Abhängigkeit der Richtung variieren werden.

zu Schritt 4: Bestimmung der Interessensradien. Der Radius dient dazu, den Zugriff für Stufenelemente einer iHS für eine Nutzergruppe in Abhängigkeit ihrer Stufe in der Organisationshierarchie zu bestimmen. Der Begriff „Radius“ ist hier etwas unpräzise, da er triangulläre Abstände impliziert und diese im Falle der Abstände (iabst) nicht gegeben sein müssen. Im Falle von räumlichen Distanzen (Luftlinie) liegen diese vor, aber schon bei der Berücksichtigung von Distanzen über das Straßennetz sind sie nicht mehr gegeben, da die Entfernung zwischen zwei Orten in Abhängigkeit der Richtung variiert. Ob ein Stufenelement im Interessenraum liegt, bemisst sich ausschließlich an dem Abstand vom aktuell geprüften iSWP.

zu Schritt 5: Bestimmung der Interessensschwerpunkte. Die Bestimmung der Interessensschwerpunkte pro Nutzergruppe erfolgt anhand des fachlichen Aufgabengebiets, das mit der entsprechenden Gruppe verbunden ist. Die Bestimmung mehrerer Interessensschwerpunkte ist sinnvoll und muss schon deshalb möglich sein, weil ein Nutzer ggf. mehreren Nutzergruppen angehört und sich die für ihn einsehbaren Bestandteile des Würfels als Vereinigungsmenge ergeben. In obiger Abbildung 35 wurde beispielhaft der Knoten 12 gewählt.

Die Bestimmung der Berechtigungsobjekte ist auf Basis der Kenntnis des Datenmodells intuitiv verständlich. Sie beruht auf einem Vergleich des Abstands (iabst) zwischen einem iSWP und allen anderen Stufenelementen auf der entspr. iHS mit dem Interessensradius (iRAD) des gerade betrachteten Nutzers.

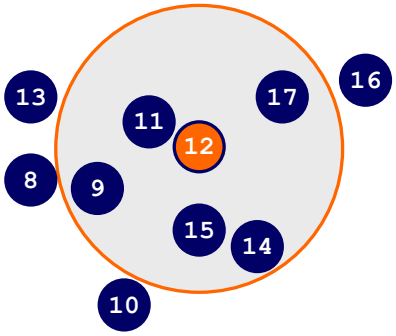


Abbildung 36: Beispielhafte Darstellung des Interessensradius bei iSWP 12
Eigene Darstellung

Liegt ein Stufenelement im Radius, erhält der Nutzer entspr. Zugriff auf die zugeordneten Datenelemente (vgl. Abbildung 36). Hieraus ergäbe sich folgende Sicht auf einen beispielhaften Datenbestand (vgl. Abbildung 37).

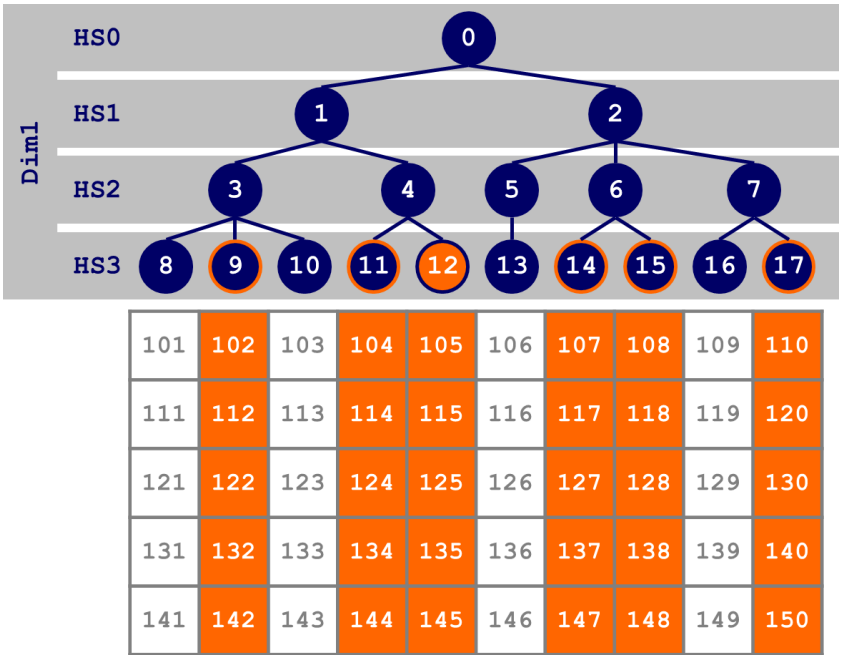


Abbildung 37: Beispielhafte Darstellung eines Interessenraums
Eigene Darstellung

6.1.3 Bewertung des Ansatzes

Der vorgeschlagene Ansatz besitzt im Vergleich zu den in Kapitel 5 beschriebenen Ansätzen einige klar erkennbare Vorteile.

(1) Intuitive Verständlichkeit

Der Ansatz ist intuitiv verständlich, wodurch die Implementier- und Wartbarkeit auf Administratorenseite gewährleistet sein und zudem keine Akzeptanzprobleme durch ein „ab-

schreckendes Komplexitätsniveau“ aufgebaut werden sollte.

(2) Minderung des administrativen Aufwands

Der administrative Aufwand wird im Vergleich zur „manuellen“ Freigabe vieler einzelner Hierarchiestufenelemente pro Nutzergruppe erheblich vermindert. Die Festlegung von ggf. nur einem Element (Interessensschwerpunkt) pro Dimension und Nutzergruppe steht hier der manuellen Bestimmung aller Elemente des Interessenraums gegenüber. Man mag als Argument anführen, dass die „interessanten Elemente“ durch eine manuelle Bestimmung sinnvoller und passgenauer ausgewählt werden könnten. Allerdings impliziert diese Vorgehensweise aufwendige Extraktion und Kodifizierung von Expertenwissen in den jeweiligen Fachgebieten bzw. Geschäftsbereichen, für welche die OLAP-Anwendung Daten enthält.

Zur Minderung des administrativen Aufwands trägt auch die Tatsache bei, dass sich unterschiedliche hierarchische Stellungen der Nutzer einfach über die Größe ihres Interessenradius abbilden lassen und sich so automatisch in den Zugriffsmöglichkeiten niederschlagen.

(3) Anpassbarkeit bzgl. des zu veröffentlichenden Datenbestands

Der Ansatz lässt sich sehr gut anpassen, wenn der Sicherheitspolitik des Unternehmens nach zu große Datenmengen veröffentlicht werden oder - im konträren Fall - keine sinnvollen explorativen Analysen möglich sind, da der Datenbestand nicht ausreichend umfassend oder granular ist. Über eine Anpassung des Radius können solche Probleme für jede Benutzergruppe separat gelöst werden. Auf Ebene aller Benutzergruppen lässt sich dies durch eine Veränderung der Abstände im Rahmen einer iHS um den gleichen Faktor verwirklichen. Sollen hochkritische Bereiche des Würfels unbedingt ein- bzw. ausgeblendet werden, kann notfalls deren Abstand in der Abstandsmatrix nachträglich angepasst werden. Ein Orientierungswert dafür ist der kleinste bzw. größte vergebene Interessensradius.

Neben diesen aus Sicht des Autors sachlich überwiegenden Vorteilen ergeben sich einige Nachteile bzw. Schwierigkeiten bei der Umsetzung dieses Ansatzes.

(1) Akzeptanzprobleme

Akzeptanzprobleme sind nicht auszuschließen, wenn sicherheitsrelevante Einstellungen automatisiert auf Basis einer Heuristik durchgeführt werden. Es bleibt aber festzuhalten, dass man dann eine andere geeignete und praktikable Lösung für Disclosure Limitation in

OLAP finden muss. Der vorgeschlagene Ansatz bietet natürlich keine echte Inferenzkontrolle und könnte auch deswegen nicht akzeptiert werden. Dies scheint in Anbetracht der Tatsache, dass Berichte über praktisch angewandte Inferenzkontrolle in OLAP-Anwendungen bis jetzt nicht bekannt sind, allerdings ein wenig stichhaltiges Argument zu sein.

(2) Aufwand der Abstandsmatrixbestimmung

Einen relativ hohen Aufwand verursacht die Bestimmung der Abstandsmatrix, wenn nicht - wie im Falle von räumlichen Distanzen - ein im Analysezusammenhang sinnvolles Abstandsmaß bereits vorhanden und die entspr. Daten mit wenig Aufwand zu beschaffen sind. Für die automatisierte Bestimmung von Abständen werden in Abschnitt 6.2 verschiedene Ansätze diskutiert. Der Vorteil einer Abstandsmatrix liegt vor allem darin, dass sie im entsprechenden Dimensionszusammenhang in mehreren Datenwürfeln verwendet werden kann. Es sind grds. auch Fälle vorstellbar, wo der Sinnzusammenhang des Abstandsmaßes ausschließlich für einen speziellen Datenwürfel gilt. Diese Konstellation würde höheren Aufwand verursachen, da dann mehrere Abstandsmatrizen gebildet werden müssen. Dieser Spezialfall wird im Folgenden jedoch nicht weiter besprochen, sondern zunächst die Praktikabilität des Grundkonzeptes in Abschnitt 6.3 unter Beweis gestellt.

(3) Inkonsistenzen bei der Aggregation

Der vorgestellte Mechanismus bedingt, dass in vielen Hierarchiestufencontainern nicht auf alle Elemente zugegriffen werden kann. Bei einem Roll-Up werden Aggregationen daher zu anderen Ergebnissen führen als wenn der Datenwürfel komplett abrufbar wäre. Dem Benutzer muss dies in jedem Fall bei den entsprechenden Operationen als Hinweis kenntlich gemacht werden. Die „richtigen“ aggregierten Werte (aus dem eigentlichen Datenwürfel) zusätzlich anzugeben, verbietet sich offensichtlich aufgrund der zusätzlichen Gefahr von Inferenzen. Zudem würde man dem Nutzer automatisch große Teile der Struktur ab der Hierarchiestufe über der iHS offen legen, da er für eine Anzeige des korrekten Aggregats nur einen untergeordneten Knoten in seinem Interessensraum haben müsste.

6.2 Bestimmung von Abstandsmaßen

Zunächst ist es notwendig, den Arbeitskontext jedes Nutzers oder jeder Nutzergruppe zu

bestimmen. Hierzu werden die Nutzer auf den verschiedenen Dimensionen verortet. Für Dimensionen mit Kardinalskalen ist dies einfach möglich; die Herausforderung besteht in der Bestimmung der Ähnlichkeiten bzw. Distanzen zwischen den einzelnen Elementen in nominal skalierten Dimensionen. Zusätzlich ist zu beachten, dass in DW und OLAP auch hierarchisch geordnete Daten vorgehalten und analysiert werden.

Ein Verfahren zur Bestimmung des Arbeitskontextes bzw. „Interessenschwerpunkts" eines Nutzers oder einer Nutzergruppe muss somit folgende Herausforderungen bewältigen können:

- Verarbeitung verschieden skalierter Dimensionen, insbesondere nominalskalierter Dimensionen
- Verarbeitung heterogener Datenbestände
- Verarbeitung hierarchisch geordneter Daten

In den folgenden Abschnitten werden verschiedene Ansätze zur Distanzbestimmung in nominalskalierten Dimensionen mit hierarchischer Ordnung am Beispiel von Produkten und Produktgruppen diskutiert, da letztere ein zentrales Bezugsobjekt vieler betrieblicher OLAP-Anwendungen darstellen (vgl. Abschnitt 2.2.1).

Zur Bestimmung der Distanzen in OLAP-Datenwürfeln können drei Ansatzpunkte gewählt werden. Erstens können die strukturierten Dimensionseigenschaften, d.h. die Produktattribute und ihre jeweiligen Ausprägungen, verwendet werden, um Distanzen zwischen Produkten und Produktgruppen zu berechnen (vgl. Abschnitt 6.2.1). Zweitens können sie auf Basis der quantitativen Zellinhalte empirisch-explorativ bestimmt werden, bspw. durch die Analyse des Käuferverhaltens (vgl. Abschnitt 6.2.2). Drittens ist die Berechnung der Distanzen durch eine Exploration des Dokumenten- und Datenbestandes außerhalb des Data Cube möglich, um eine möglichst passgenaue (im Sinne einer zu den tatsächlichen organisatorischen Strukturen und Prozesse passende) Abbildung der Produktdistanzen zu erhalten (vgl. Abschnitt 6.2.3).

6.2.1 Strukturierte Dimensionseigenschaften

Zur Identifizierung aller relevanten Dimensionseigenschaften können Taxonomien her-

angezogen werden. Im europäischen Raum sind die CE-Richtlinien[326] die wichtigste Taxonomie, da sie als Instrument für die staatenübergreifende Harmonisierung von Produkten sowie für die Festlegung juristisch zwingender Sicherheitsrichtlinien für Produkte dienen. Die Richtlinien definieren Produkt-Taxonomien anhand technischer und verwendungszweckbezogener Attribute. Lebensmittel sind beispielsweise in Verordnung (EG) Nr. 178/2002 definiert als „alle Stoffe oder Erzeugnisse, die dazu bestimmt sind oder von denen nach vernünftigem Ermessen erwartet werden kann, dass sie in verarbeitetem, teilweise verarbeitetem oder unverarbeitetem Zustand von Menschen aufgenommen werden".[327] Nachteil der CE-Richtlinien ist, dass sie keine Attributkataloge zur vollständigen Beschreibung von Produkten beinhalten. Diese Normierungslücke füllen attributbasierte Klassifizierungssysteme wie bspw. der eCl@ss-Standard[328], der zur Erleichterung der elektronischen Abwicklung von Geschäftsprozessen und Führung von Warenwirtschaftssystemen entwickelt wurde.[329] Die Klassifikationslogik von eCl@ss wird als „identitätsorientiert"[330] beschrieben. Alle Produkte bzw. Produktgruppen werden in maximal 4 Hierarchieebenen untergliedert, wobei lediglich der untersten Hierarchieebene Attribute zugeordnet werden. Die höheren Hierarchieebenen „dienen vorzugsweise als ordnungslogisches und sprachliches Strukturierungshilfsmittel"[331], denen keine Attribute zugeordnet werden. Jedes Produkt unterscheidet sich von jedem anderen Produkt in mindestens einer Attributausprägung.[332] Im Vergleich zu anderen Systemen ist eCl@ss ein „lebendiges" Artefakt, das regelmäßig und substanziell erweitert und auf einen neuen Stand gebracht wird.[333] Allerdings leidet es unter einem Ungleichgewicht der in den verschiedenen Produktgruppen hinterlegten Anzahl von Produkten und des Detaillierungsgrades ihrer Beschreibung.[334] Nur etwa die Hälfte der Produktklassen wurde 2007 durch ein Merkmalsset beschrieben.[335] Ein weiterer Nachteil ist die hohe Überschneidungsfreiheit der zur Klassi-

326 Eine Sammlung aller Richtlinien ist bei ROEHLING (2011) zu finden. Die einzelnen Richtlinien treten mit Veröffentlichung im Amtsblatt der EG in Kraft [vgl. EUR-Lex].

327 EG Nr. 178/2002, S. 1

328 Für einen Überblick vgl. HEPP/LEUKEL/SCHMITZ (2007)

329 Vgl. ECL@SS E.V. (2006)

330 ebenda, S. 2

331 ebenda, S. 2

332 Vgl. ebenda für diesen und die beiden vorhergehenden drei Sätze

333 Vgl. HEPP/LEUKEL/SCHMITZ (2007), S. 101–105

334 Vgl. ebenda, S. 100

335 Vgl. ebenda, S. 110

fizierung verwendeten Attribute, von denen im Jahr 2007[336] lediglich 50% für die Beschreibung von 2 oder mehr Produkten herangezogen wurde.[337] Im Hinblick auf die Verwendung für den hier vorgeschlagenen Ansatz ist das Fehlen von (mathematischen) Ansatzpunkten zur Berechnung der Distanzen zwischen den Produkten bzw. zwischen den nominalskalierten Attributausprägungen kritisch. eCl@ss müsste folglich um die Möglichkeit erweitert werden, Attributausprägungen zu normalisieren, zu gewichten und zu aggregieren, um eine Distanzbestimmung vornehmen zu können.

Diese Überlegung verfolgen bspw. JIAO ET AL. (2007) im Rahmen einer unternehmensspezifischen Taxonomie ohne Normcharakter. Die Autoren entwickeln ein Verfahren zur attributbasierten Ähnlichkeitsbestimmung zwischen Produktkomponenten, welches als Basis für effizientere Variantenkonfiguration dient. Jede Komponente muss in einer Textdatei mit ihren Attributen und/oder Bestandteilen beschrieben werden. Die Attribute werden aus den Textdateien extrahiert und ihre Auftrittshäufigkeiten berechnet. Anschließend wird die relative Wichtigkeit berechnet, die ein Attribut für die Beschreibung einer Komponente besitzt. Die Summe der Ähnlichkeiten zwischen den gewichteten Komponentenattributen (berechnet als Differenz ihrer minimalen und maximalen Ausprägungen) ergibt die Ähnlichkeit zwischen zwei Komponenten.[338] Problematisch hierbei ist erstens die Bestimmung von Ähnlichkeiten nominaler Attributausprägungen; JIAO ET AL. schlagen vor, Expertenurteile dafür heranzuziehen oder aber identische Ausprägungen gleich 1 und unterschiedliche Ausprägungen gleich 0 zu setzen.[339] Zweitens empfehlen die Autoren, die Ähnlichkeitsmaße zwischen Rohmaterialien und Zwischenerzeugnisse zu gewichten „based on domain knowledge“[340] [sic], was eine weitere Quelle für Inkonsistenzen darstellt und den Aufwand für die Implementierung ihres Ansatzes weiter erhöht. Diese Tatsachen in Verbindung mit der Annahme, dass jede Komponente korrekt, vollständig und in identischem Format beschrieben ist, schränkt die praktische Anwendbarkeit dieser und ähnlicher Ansätze[341] zur Bestimmung von Interessensschwerpunkten (vgl. Abschnitt 6.1) stark

336 Das aktuelle Release 7.0 ist im Vergleich zum Release 5.1 von 2007 laut eCl@ss ein „vollkommen überarbeitetes Release mit einer verbesserten [...] Struktur“ [vgl. ECL@SS E.V.]. Insofern mag die Kritik aus dem Jahr 2007 nicht mehr im selben Ausmaß zutreffen; es ist jedoch unwahrscheinlich, dass alle Kritikpunkte ausgeräumt wurden. Leider existiert keine Neuauflage der Vergleichsstudie von HEPP/LEUKEL/SCHMITZ (2007).

337 Vgl. HEPP/LEUKEL/SCHMITZ (2007), S. 99

338 Vgl. JIAO ET AL. (2007), S. 871f. für diesen und die drei vorhergehenden Sätze

339 Vgl. ebenda, S. 872

340 ebenda

341 Für einen Überblick vgl. bspw. JIAO/SIDDIQUE/SIMPSON (2006)

ein.

6.2.2 Quantitative Zellinhalte des Data Cube

CHEN/LYNCH stellen fest:

> „Whenever a large amount of information is collected and captured in a database, important domain knowledge also resides there.“[342]

Die im Data Cube vorgehaltenen Daten implizieren somit möglicherweise bereits die Distanzen zwischen den Produkten und Produktgruppen. Die Klassifikation ließe sich in diesem Fall durch die Extraktion des domänenspezifischen Wissens aus dem Data Cube effizienter gestalten als durch die Erhebung und Kodifizierung von Expertenwissen. Zur Illustrierung der Distanzbestimmung zwischen Produkten anhand der Zellinhalte des Data Cube stelle man sich einen dreidimensionalen Data Cube mit den Verkaufszahlen eines Produktes in den letzten Jahren an verschiedene Kunden oder Kundengruppen vor. Der Vertrieb sei produktorientiert ausgerichtet. Aus absatzpolitischer Sicht ist es sinnvoll, das Kaufverhalten von Kunden zu analysieren, um daraus die Attraktivität anderer (zusätzlicher) Produkte für diese Kunden abzuleiten. Eine flexibel und dynamisch gestaltete Zugriffskontrolle sollte dem für ein Produkt zuständigen Vertriebsmanager also Zugriff auf Kunden gewähren, welche „sein“ Produkt noch nicht gekauft haben, für die es aber wahrscheinlich attraktiv wäre. Ein anderes Szenario ergibt sich bspw. bei regionaler Vertriebsorganisation aus der Analyse des Verlaufes der Verkaufszahlen. Im Falle eines Absatzrückgangs wäre es für den zuständigen Mitarbeiter von Interesse zu erfahren, ob dieser lediglich in seinem Verkaufsgebiet geschieht oder auch angrenzende Gebiete betrifft. So könnten bspw. (interne) Kannibalisierungseffekte von Werbeaktionen oder (extern verursachte) Marktanteilsverluste identifiziert werden (vgl. Abschnitt 6.3).

DAS/MANNILA (2000) bspw. schlagen für kategoriale Datenbanken (z.B. „market basket“ eines Supermarkts) ein kontextbasiertes Verfahren vor. Die Datenbanken enthalten die Informationen, welcher Kunde (Zeile) welches Produkte (Spalte) kauft oder nutzt. Die Autoren fassen die Spalteninformationen als Sample von Häufigkeitsverteilungen auf und berechnen die Produktähnlichkeiten als Ähnlichkeiten zwischen den Häufigkeitsverteilungen. DAS/MANNILA (2000) entwickeln einen iterativen Lösungsalgorithmus als System nichtlinearer Gleichungen, dessen Ergebnisse folgende Fragen beantworten: „Wie hoch

[342] CHEN/LYNCH (1992), S. 885

ist die Wahrscheinlichkeit, dass ein Konsument von Produkt A auch mit Produkt B zufrieden wäre?“ und davon abgeleitet „Wie ähnlich sind sich Produkte A und B?“ oder, anders formuliert, die Distanz zwischen den Produkten A und B.

Weitere Analysemethoden finden sich auf dem Gebiet der Empfehlungssysteme, deren am weitesten verbreitete Verfahren „content-based“[343] und „collaborative filtering“[344] sind. In „content-based“ Empfehlungssystemen werden die Attributausprägungen von Produkten mit den Präferenzen eines Kunden für die einzelnen Attribute verglichen und die Differenzen aggregiert. Aus der Distanz eines Produktes zu den Kundenpräferenzen errechnet sich die Wahrscheinlichkeit, dass das Produkt für einen bestimmten Kunden interessant ist. Die Berechnung der Distanzen kann mit einer Vielzahl von Algorithmen vorgenommen werden, bspw. Clustering-Algorithmen.[345] Allerdings bedingt dieses Verfahren ebenso wie die in Abschnitt 6.2.1 angesprochenen Ansätze eine detaillierte Dokumentation der Produktattribute und – zusätzlich – der Nutzerprofile. Diesen Nachteil besitzt das „collaborative filtering“ nicht. Hier werden die Empfehlungen für einen Kunden auf Basis seines Kaufverhaltens und des Kaufverhaltens anderer, ihm ähnlicher Kunden, generiert.[346] „Collaborative filtering“ leidet allerdings unter dem sog. „cold start“-Problem: es ist nur einsetzbar, wenn möglichst weit reichende Kaufhistorien möglichst vieler Nutzer vorliegen. Je größer die Anzahl der Produkte ist, für die Empfehlungen abgegeben werden sollen, desto schwächer besetzt ist die Käufer-Produkt-Matrix, was zu Laufzeitproblemen und sinkender Präzision bei der Ähnlichkeitsberechnung führt.[347] Geringe Ähnlichkeiten zwischen den Produkten haben negative Auswirkungen auf die Qualität der Empfehlungen, da sich die Verallgemeinerung von Präferenzen über verschiedene Produktgruppen auf Basis der Kaufhistorie schwierig gestaltet.[348] Um diese Schwäche zu überwinden, wurden in den letzten Jahren diverse Erweiterungen vorgeschlagen, wie z.B. die Integration von Kontextinformationen (bspw. Suchmuster, Keywords), um so die rein auf Kundenverhalten basierende Ähnlichkeitsberechnung zu komplementieren.[349] SCHUSTER/JUCHHEIM/SCHILL (2010) bspw. schlagen Verfahren auf Basis von k-means Clus-

343 Vgl. ADOMAVICIUS/TUZHILIN (2005), S. 735–737

344 Vgl. ebenda, S. 737-740

345 Vgl. ebenda

346 Vgl. ebenda, S. 737f. für die vorhergehenden beiden Sätze

347 Vgl. ebenda, S. 740 für die vorhergehenden beiden Sätze

348 Vgl. ebenda, S. 739f. für die vorhergehenden beiden Sätze

349 Vgl. ebenda, S. 743-747 für einen Überblick über weitere Vorschläge zur Erweiterung der Funktionalität von Empfehlungssystemen

tering und Produkthierarchiebäumen vor, das öffentlich zugängliche Daten im Internet nutzt, um Beziehungen zwischen Produkten zu identifizieren. Die Art der Beziehung wird dazu genutzt, zwischen Komplementärprodukten und Produkten aus derselben Produktgruppe zu unterscheiden und so bessere Empfehlungen zu generieren.

Für die vorliegende Arbeit sind diese Ansätze insbesondere zur Überprüfung der Lage der Interessensschwerpunkte und des Interessensradius interessant. Sie können – wie eingangs angemerkt – bspw. Hinweise darauf geben, auf welchen Radius ein Interessensgebiet ausgedehnt werden sollte, um die Qualität absatzpolitischer Entscheidungen zu verbessern.

6.2.3 Dokument- und Datenbestand außerhalb des Data Cube

Klassifikationsmuster spiegeln sich auch in betrieblichen Dokumenten sowie im Internet bspw. in Form von Seitenstrukturen (bspw. Verlinkungen, Keywords) und online verfügbaren Dokumenten wieder, welche von Experten angelegt und verwaltet werden. Der dritte Ansatz zur Distanzbestimmung beruht daher auf der explorativen Analyse kodifizierten domänenspezifischen Wissens. Ansätze zur Mustererkennung und Klassifizierung in verschiedenen Umgebungen finden sich unter den Schlagworten „Web Mining", „Data Mining", „Text Mining", „Knowledge Discovery in Databases" u.v.m. Für einen Überblick über verschiedene Algorithmen und Ansätze sei bspw. auf LIU (2007) und KOLODZIEJ (2011) verwiesen.

CHEN/LYNCH bspw. schlagen folgende Vorgehensweise vor:

> "[To use an] algorithmic approach to the generation of a robust knowledge base based on statistical correlation analysis of the semantics (knowledge) embedded in the documents of real, textual databases"[350]

Ziel ist die automatische Generierung von Thesauri, die als semantische Netzwerke dargestellt werden, deren Knoten die Begriffe und deren Kantengewichte die Stärke des Zusammenhangs abbilden. Die Autoren vergleichen einen Cosinus-basierten Algorithmus mit einem Clustering-Algorithmus hinsichtlich seiner Leistungsfähigkeit, wobei sie insbesondere auf die verfahrensbedingten Unterschiede bei der Kantengewichtung eingehen. Der normalisierte Cosinus geht von symmetrischen gleich gewichteten Kanten zwischen zwei Knoten aus, wohingegen mit dem Clustering-Algorithmus asymmetrische und unter-

[350] CHEN/LYNCH (1992), S. 886

schiedlich gewichtete Kanten abgebildet werden können.[351] Ihre Ergebnisse weisen darauf hin, dass die Berücksichtigung asymmetrischer Verbindungen zu wesentlich besseren semantischen Netzwerken führt und die Unterstützung von (menschlichen) Experten durch solche Algorithmen die Qualität der Klassifizierung wesentlich verbessert.[352]

Auf Basis dieser und anderer Arbeiten zu semantischen Netzen entwickelten ZHAO/KUMAR/STOHR (2000) ein Modell zur Erstellung eines „organizational concept space". Dieser besteht aus einer Interessensmatrix und einem Ähnlichkeitsnetzwerk. In der Matrix wird für jeden Mitarbeiter mit einem Wert zwischen 0 und 1 beschrieben, wie intensiv er sich für jeden Begriff bzw. jedes Thema interessiert. Die Begriffe bzw. Themen werden in einem gerichteten Netzwerk gespeichert, das zwei Arten von Knoten enthält: Stammknoten, welche Sets von semantisch ähnlichen Begriffen enthalten, und Blätter, welche einzelne Begriffe abbilden. Die Kantengewichte bilden die Stärke des Zusammenhangs zwischen Stammknoten bzw. die Zugehörigkeit eines Blatt(knoten)s zu einem Stammknoten ab.[353] Durch das Matching zwischen Mitarbeiterinteressen und den Begriffen im Ähnlichkeitsnetzwerk soll der Informationsbedarf der Mitarbeiter in einer Organisation determiniert und die Verteilung von Informationen verbessert werden. Die Problematik der Interessensfeststellung und der Aktualisierung der Basisdaten bleibt jedoch ungelöst; die Autoren weisen selbst darauf hin, dass die Verwaltung der Interessensmatrix und des Ähnlichkeitsnetzwerkes vermutlich prohibitiv hohe Kosten verursachen würden.[354] ROUSSINOV/ZHAO (2003) entwickeln diese Idee weiter zur Methode der „Context Sensitive Similarity Discovery", die sie zur Reduzierung des Information Overload bspw. bei Dokument-Retrieval oder E-Mail-Filtern vorschlagen. Sie verwenden das Konzept des „organizational concept space", um den als Ähnlichkeitsmaß zwischen Dokumenten herangezogene Cosinus entsprechend des (organisatorischen) Kontextes zu gewichten und so die Präzision des Clustering-Algorithmus zu verbessern, welcher zur Identifizierung der Themenschwerpunkte verwendet wurde.[355] Das Verfahren wurde im Kontext eines Brainstorming-Meetings experimentell getestet, um meeting-bezogene Nachrichten zu klassifizieren. Es zeigte, verglichen mit manuell erstellten Klassifikationen, gute Ergebnis-

351 Vgl. CHEN/LYNCH (1992), S. 887 für diesen und die vorhergehenden beiden Sätze
352 Vgl. ebenda, S. 895f.
353 Vgl. ZHAO/KUMAR/STOHR (2000), S. 3 für diesen und die vorhergehenden beiden Sätze
354 Vgl. ebenda, S. 6 für diesen und den vorhergehenden Satz
355 Vgl. ROUSSINOV/ZHAO (2003), S. 157f.

se hinsichtlich der Konsistenz und der Präzision der Einordnung.[356] Allerdings klammerten die Autoren die Interessensmatrix, d.h. die Mitarbeiterperspektive, und somit einen wesentlichen Teil des Originalbeitrags von ZHAO/KUMAR/STOHR (2000) aus ihren Betrachtungen aus.[357]

Die Normalisierte Google-Distanz (NGD) ist Ergebnis von Bemühungen zur Entwicklung eines parameterfreien, kontextunabhängig einsetzbaren Verfahrens zur Berechnung der semantischen Nähe zwischen zwei Termen auf Basis der Häufigkeit ihres gemeinsamen Vorkommens in Dokumenten (vgl. Abbildung 38). Die Grundidee dieses Verfahrens ist ähnlich dem der Latenten Semantischen Analyse (LSA). Jedoch kann LSA aufgrund der großen Menge an notwendigen Matrixoperationen nicht dazu verwendet werden, ähnlich große Korpi zu durchsuchen wie dies bei Verwendung der NGD möglich ist.[358] Zudem ist LSA nicht parameterfrei: Ähnlichkeiten zwischen Termen und Dokumenten werden im k-dimensionalen Raum berechnet, wobei k frei festlegbar ist. Ein exaktes Verfahren zur Bestimmung des optimalen Wertes von k in einem bestimmten Setting gibt es nicht.[359]

Abbildung 38: Normalisierte Google-Distanz
CILIBRASI/VITANYI (2007), S. 374

f(x) steht für die Anzahl der Hits, welche eine Suchanfrage nach dem Term x zurückliefert. *f(x, y)* enthält die Anzahl der Hits, die eine Suchanfrage nach den beiden Termen x und y liefert. N ist die Gesamtzahl der Dokumente, welche der Korpus enthält.[360] CILIBRASI/VITANYI (2007) verwendeten als Ausgangsszenario die Durchsuchung des gesamten Webs mit der Suchmaschine Google. LINDSEY ET AL. (2007) zeigten in einem Vergleich der Leistungsfähigkeit der NGD mit Pointwise Mutual Interest[361] auf verschiedenen Dokumentkorpi, dass NGD eindeutig überlegen ist. Neben dem Vergleich der beiden Verfahren lag das Erkenntnisinteresse von LINDSEY ET AL. auch darin, verschiedene Korpi auf ihre Eignung zur Berechnung von semantischer Nähe zu untersuchen. Prob-

356 Vgl. ROUSSINOV/ZHAO, S. 160f.
357 Vgl. ROUSSINOV/ZHAO (2003), S. 152
358 Vgl. CILIBRASI/VITANYI (2007), S. 382
359 Vgl. BRADFORD (2008), S. 154f. für die beiden vorhergehenden Sätze
360 Vgl. CILIBRASI/VITANYI (2007), S. 374
361 Pointwise Mutual Interest wird berechnet als Logarithmus der Wahrscheinlichkeit, dass zwei Terme innerhalb eines Textfensters gefunden werden, dividiert durch die multiplizierten Wahrscheinlichkeiten, die beiden Terme separat zu finden [vgl. TURNEY (2001)].

lemfelder identifizieren sie hier hinsichtlich der Aktualität des Korpus, inhaltlicher Verzerrung durch Sampling-Entscheidungen, zu hoher oder zu geringer Strukturiertheit der Texte (z.B. Wörterbücher oder Internetforen) sowie des Umfangs des Korpus.[362] Allerdings gehen sie nicht detailliert darauf ein, inwiefern die Eigenschaften der Korpi die Vorteilhaftigkeit verschiedener Verfahren beeinträchtigen könnten.

Der Einsatz von NGD auf dem Korpus betrieblicher Dokumente könnte im Rahmen des hier vorgeschlagenen Ansatzes herangezogen werden, um Distanzen zwischen Objekten und Interessensschwerpunkten auf Dimensionen zu berechnen, für die weder attributbasierte Verfahren noch explorative Datenanalysen geeignet sind bzw. einen unzumutbar hohen Aufwand für Implementierung und Aktualisierung verursachen würden.

6.2.4 Diskussion der Bestimmung der Abstandsmaße

Ursprünglich wurden die in Abschnitt 6.2.1 vorgestellten attributbasierten Ansätze im Produktionsbereich zur technischen Beschreibung von Produkten, ihrer Funktionsweise, ihren Bestandteilen und ihrem Einsatzzweck verwendet. Zu den hierdurch verfolgten unternehmerischen Zielen gehören bspw. die effizientere Gestaltung von Produktionsprozessen, die produktionstechnisch sinnvolle Modularisierung von Produkten zur Umsetzung von Mass Customization und die Verbesserung des Variantenmanagements.[363] Diese Attributorientierung findet sich auch in vielen Ansätzen der Konsumenten- und Marktforschung (vgl. Abschnitt 6.2.2), wo die Zusammenfassung von Produkten in Produktgruppen es ermöglicht, die Wahrnehmung von Marken und Produkten durch Konsumenten zu erfassen, um ihre Absatzpolitik dementsprechend zu optimieren. Schwierigkeiten ergeben sich jedoch bei der Integration produktions- und konsumentenorientierter Produktbeschreibungen, da Beschreibungen und relative Wichtigkeiten der Attribute häufig voneinander abweichen. Produktionsorientierte Ansätze schließen neben den Bestandteilen und Eigenschaften, mit denen ein Produkt beschrieben werden kann, häufig auch die zur Herstellung notwendigen Produktionsschritte in die Ähnlichkeitsbetrachtung mit ein.[364] Konsumentenorientierte Ansätze wiederum fokussieren die von Kunden wahrgenommenen Eigenschaften eines Produktes ohne Berücksichtigung solcher Strukturen[365],

362 Vgl. LINDSEY ET AL. (2007), S. 2f.
363 Vgl. JIAO/SIDDIQUE/SIMPSON (2006); KOLODZIEJ (2011)
364 Vgl. bspw. JIAO ET AL. (2007) ; JIAO/SIDDIQUE/SIMPSON (2006)
365 Vgl. bspw. ADOMAVICIUS/TUZHILIN (2005)

wie bspw. in katalogbasierten Online-Shopping-Umgebungen.[366]

Inkonsistente Produktbeschreibungen verursachen insbesondere beim Austausch von Produktdaten in der Supply Chain Probleme, weshalb Initiativen wie eCl@ss sich zum Ziel gesetzt haben, normierte Produktbeschreibungen zu entwickeln (vgl. Abschnitt 6.2.1). Die Aggregation von Daten über verschiedene Quellsysteme wird durch die Verwendung standardisierter Produktbeschreibungen und Produkthierarchien wesentlich vereinfacht. Es stellt sich allerdings das Problem, dass für staatlich schwach regulierte Branchen – im Gegensatz zu stark regulierten Branchen wie z.B. die Pharmazeutika-Herstellung – häufig keine Standards existieren bzw. vorhandene Standards auf hohem Abstraktionsniveau formuliert sind. Ein weiteres Problem ergibt sich daraus, dass Produkte, welche keine oder nur wenige Attribute teilen, kaum verglichen werden können. Die in eCl@ss vorhandenen Produktbeschreibungen bspw. weisen eine hohe Überschneidungsfreiheit hinsichtlich der verwendeten Attribute auf.[367] Insbesondere in diesen Fällen ist anzuzweifeln, ob die Implementierung eines der bisher existierenden Standards für jedes Unternehmen die beste Lösung (i. S. von sinnvoller Geschäftsprozessunterstützung) wäre. Die Eigenentwicklung von Taxonomien jedoch verursacht i.d.Regel hohen Aufwand für die Extraktion und Strukturierung des domänenspezifischen Wissens[368], für die Restrukturierung von Datenbeständen und deren (langfristige) Aktualisierung sowie Probleme im Hinblick auf die Kompatibilität mit den Taxonomien der Geschäftspartner in der Supply Chain. Im Hinblick auf die mathematische Berechnung der Unterschiedlichkeit zwischen Produkten besteht jedoch selbst bei Vorliegen einer vollständigen Klassifizierung noch die Frage, wie die Distanzen zwischen nominal skalierten Attributen und ihren Ausprägungen zu ermitteln sind. Lösungsvorschläge für diese Problematik liefern die in Abschnitt 6.2.3 besprochenen Ansätze.

Ziel dieser Ansätze ist die Entwicklung möglichst flexibel anwendbarer Verfahren zur Distanzberechnung, um in empirischen Datenbeständen sinnvolle (Klassifikations-) Muster zu entdecken. Der letztendlich sinnstiftende Anwendungszweck (wie Absatz- oder Produktionsoptimierung) fließt bspw. über Parameterkonfigurationen oder die Hinterlegung von Ontologien in die Verfahren ein.[369] Im Hinblick auf die Bestimmung der Interessensschwerpunkte ist der Ansatz von ZHAO/KUMAR/STOHR (2000) interessant, da er

366 Vgl. bspw. AGRAWAL/SRIKANT (2001)
367 Vgl. HEPP/LEUKEL/SCHMITZ (2007), S. 99
368 Vgl. CILIBRASI/VITANYI (2005), S. 370f.
369 Vgl. bspw. ebenda

(zumindest konzeptionell) die Interessen der Mitarbeiter berücksichtigt. Der Anwendungskontext seiner Arbeit (Klassifizierung von Nachrichten zur Vermeidung von Information Overload) ist zwar ein anderer, jedoch ist die Herangehensweise der Grundidee des in dieser Arbeit vorgestellten Ansatzes nicht unähnlich. Neben der Klassifizierung der Objekte, seien es Nachrichten oder Daten (Query-Resultate), soll der Informationsbedarf der Mitarbeiter bzw. Nutzer festgestellt werden. Stimmt die „Lage" der Interessensschwerpunkte der Nutzer mit den „Koordinaten" der Objekte überein, d.h. sind die Objekte für die Erledigung ihrer Arbeit relevant, so erhält der Nutzer die Nachricht bzw. Zugriff auf das Objekt. Im Unterschied zu ZHAO/KUMAR/STOHR (2000) soll das „Koordinatensystem" kein Themengebiet abbilden, sondern eine multidimensionale Beschreibung des Interessensschwerpunkts der Mitarbeiter ermöglichen. Die vorgeschlagene Vorgehensweise, eine Zahl zwischen 0 und 1 zur Signalisierung des Interesses an einem Thema bzw. Objekt zu verwenden,[370] ist jedoch nicht zu empfehlen. Erstens ist damit lediglich eine ordinale Skalierung möglich und zweitens entsteht durch die statische Natur der Interessensmatrix von ZHAO/KUMAR/STOHR (2000) ein hoher Aktualisierungsaufwand. Änderungen in der Organisation oder Umwelt bedingen jedoch ggf. eine Anpassung der Interessensschwerpunkte und somit der Zugriffsrechte, so dass eine flexible, dynamische Festlegung der Interessensschwerpunkte vonnöten ist. Die Anpassungen sollten weitgehend automatisch erfolgen können, um den Administrationsaufwand auf eine vertretbare Höhe zu begrenzen.

Die Erhebung und schriftliche bzw. konzeptionelle Fixierung von domänenspezifischem Wissen zur Festlegung, Aktualisierung und Überprüfung der Objektklassen und der Interessensschwerpunkte bzw. der entsprechenden Zugriffsrechte verursachen beträchtlichen Aufwand. Empirische Untersuchungen über den Erhebungsaufwand domänenspezifischen Wissens existieren kaum.

Eine Ausnahme stellt die Studie von O'CONNOR/LOOMIS (2010) dar, in welcher die Kosten geschätzt werden, die durch die Extraktion domänenspezifischen Wissens zum Zwecke der unternehmensgerechten Definition der Rollen und der Zuordnung von Nutzern bzw. Berechtigung zu den Rollen im Rahmen der Implementierung von RBAC entstehen (vgl. Abschnitt 3.2). Dies betrifft vor allem die Mitarbeiter des operativen Bereiches, welche ihr Wissen um organisatorische Prozesse, Strukturen und Verantwortungsbereiche

[370] Vgl. ZHAO/KUMAR/STOHR (2000)

explizieren und den für die Implementierung von RBAC zuständigen Mitarbeitern verständlich machen müssen.[371] Allein die Kosten im operativen Bereich beziffern O'CONNOR/LOOMIS (2010) für ein Unternehmen mit 10.000 Mitarbeitern mit durchschnittlich über 1,3 Millionen US-Dollar (vgl. Tabelle 39). Dieser Aufwand entsteht, obwohl RBAC ein relativ gut beschriebenes Instrument ist, für dessen Implementierung bereits standardisierte Prozesse und Produkte vorliegen.[372]

	Zeitaufwand	Durchschnittl. Stundenlohn	Kosten	**Gesamtkosten**
	Pro Mitarbeiter	*US-Dollar*	*Pro Mitarbeiter*	***10.000 Mitarbeiter***
▶ IT-Bereich	**0,75**	**92,10**	**69,37**	**693.700**
▶ Operativer Bereich	**1,34**	**98,94**	**132,28**	**1.322.800**
▶ Sonstige Kosten			**39,36**	**393.600**
▶ Jährliche Wartungskosten			**1,47**	**14.700**
Gesamtkosten			**241,01**	**2.410.000**

Tabelle 39: Schätzung der Implementierungskosten von RBAC
Eigene Darstellung nach O'CONNOR/LOOMIS (2010), S. 18

Zur Klassifizierung der Produkte bzw. Produktgruppen wird – sofern keine Taxonomie vorhanden und der Aufbau einer Taxonomie nicht möglich oder wirtschaftlich sinnvoll ist – die Verwendung eines Verfahren aus dem Data Mining befürwortet. Um den Implementierungs- und Aktualisierungsaufwand zu minimieren, scheint ein parameterfreies und zumindest teilautomatisierbares Verfahren am sinnvollsten. Im Hinblick auf den zu verwendenden Korpus liegt es nahe anzunehmen, dass das in einem Unternehmen verfügbare domänenspezifische Wissen sich in den Dokumenten und Datenbeständen in hinreichend genauer Form widerspiegelt, um auf dieser Basis Ähnlichkeiten zwischen Objekten zu bestimmen. Sollte eine entsprechende Datenbasis im Unternehmen nicht vorhanden sein, so könnte – in Abhängigkeit vom relevanten Kontext – ein webbasierter Korpus durchsucht werden (bspw. ein Expertenportal mit relevanter Fachliteratur und Diskussionsforen oder die Webshops, in denen die Produkte vertrieben werden). Denkbar wäre es auch, dass nur die Bestände des Dokumentenmanagementsystems oder Informationssys-

[371] Die durchschnittliche Implementierungszeit für ein RBAC-basiertes AC-System betrug 18 Monate. O'Connor/Loomis (2010, S. 18) schlüsselten die durchschnittlichen Implementierungskosten pro Mitarbeiter nach Kostenarten bzw. Verwendungszweck auf und stellten fest, dass Kosten für die Definition von Rollen, die Zuordnung von Berechtigungen und Rollen sowie die Implementierung der neuen AC das Fünffache der restlichen Kosten (Software-Lizenzen etc.) betrugen.

[372] Vgl. ebenda

tems eines bestimmten Funktionsbereiches herangezogen werden, um speziell für diesen Bereich des Unternehmens Produktähnlichkeiten zu berechnen. Zur paarweisen Ähnlichkeitsbestimmung zwischen Objekten könnte bspw. die NGD herangezogen werden, welche wie die meisten Verfahren des IR auf der Berechnung und Normalisierung der „term co-occurrences" beruht.[373] Ein mögliches Anwendungsszenario wäre die Kombination dieses Verfahrens mit explorativen Analysen der entsprechenden quantitativen Zellinhalte im Absatzbereich. Die externe Umwelt (Kundenverhalten) und die interne Perspektive (Arbeitsbereiche, Prozesse, Verantwortlichkeiten) könnten somit hinsichtlich ihrer Übereinstimmung geprüft werden. Auf dieser Basis könnten Lage und Radius der Interessensschwerpunkte im Hinblick auf mehrere Unternehmensziele (Absatz, Effizienz) optimiert werden.

6.3 Beispielhafte Implementierung in SAP BI 7.0

Die beispielhafte Implementierung soll im Wesentlichen deutlich machen, dass ein Sicherheitsmechanismus auf Basis des eben vorgeschlagenen Konzepts in SAP BI 7.0 mit sehr geringem Aufwand implementierbar ist. (SAP BI 7.0 gehört zu den in Deutschland am häufigsten verwendete OLAP-/DWS-Produkten.)[374] Das Beispiel ist bewusst übersichtlich gehalten. Die Implementierung beinhaltet alle Strukturen für die Kernfunktionalität des oben vorgeschlagenen Sicherheitsmechanismus bzgl. einer Dimension. Für den Produktivbetrieb sollte die Implementierung selbstverständlich um ergonomische Benutzerschnittstellen für Administratoren erweitert werden. Die für die Nachvollziehbarkeit der Implementierung notwendigen produktspezifischen Aspekte des SAP BI 7.0 werden an den entsprechenden Stellen erläutert, wobei hier keine technisch präzise Spezifikation sondern ein Überblick über den Verwendungszweck einzelner Designelemente des SAP BW 7.0 gegeben werden soll. So erfolgt auch die Beschreibung der Implementierung im Wesentlichen auf konzeptionellem Niveau, ohne technische Details zu thematisieren.[375]

Für eine ausführlichere Einführung zu SAP NetWeaver BI 7.0 sei insbesondere auf den „Leitfaden SAP BW 7"[376] sowie auf „Datawarehousing mit SAP BW 7"[377] und die SAP

373 Vgl. CILIBRASI/VITANYI (2007)

374 Vgl. BARC (2010)

375 Der Autor gibt gerne auf Anfrage eine genaue technische Dokumentation der Implementierung und alle notwendigen Daten zum Aufbau des Beispiels.

376 JÜTTNER ET AL. (2010)

Online-Dokumentation SAP (2010) verwiesen.[378] Umfangreiche Erläuterungen der Möglichkeiten, in SAP BI ab der Version 7.0 Zugriffskontrollmechanismen zu integrieren, finden sich in JOHN/KIENER (2010). An diesen Quellen orientieren sich auch die folgenden Beschreibungen von technologischen Aspekten, die nicht im Einzelnen zitiert werden, da diese nur den Charakter einer technischen Dokumentation haben.

6.3.1 Verwendete Komponenten des SAP BI 7.0

SAP BI 7.0 (eigentl. SAP NetWeaver BI 7.0) stellt die integrierte Softwarelösung der SAP AG für BI-Anwendungen dar und beinhaltet umfangreiche Funktionalität zu Data Warehousing und OLAP.[379]

Das im Rahmen dieser Arbeit verwendete System SAP NetWeaver BI 7.0 wurde durch das SAP University Competence Center (UCC) Magdeburg für gemeinsame Forschungsarbeiten von Prof. Dr. Robert Weismantel (ehem. Universität Magdeburg)[380] und Prof. Dr. Peter Kleinschmidt zur Verfügung gestellt. Es basiert auf der Plattform SAP NetWeaver 2004s. Das zugrunde liegende DBMS ist die „Oracle Database“ in der Version 10.2.0.2.0.

Der Funktionsumfang eines SAP BI 7.0-System wird meist anhand der folgenden drei Schichten kategorisiert.[381]

(1) Extraktionsschicht
(2) Data Warehouse (oder Business Warehouse)
(3) Data Analysis

zu (1) Extraktionsschicht. Die Extraktionsschicht bezeichnet im Wesentlichen die Quellsysteme. Für die Extraktionsschicht stellt das Data Warehouse Funktionalitäten zur Replikation von Daten in das BW zur Verfügung. Dazu gehören Schnittstellen zu unterschiedli-

377 MEHRWALD (2007)

378 Aufgrund der Entwicklungshistorie des SAP NetWeaver BI 7.0 [vgl. bspw. SINGU/VARADARAJAN (2009)] wird häufig synonym die Bezeichnung „SAP Business Warehouse 7“ oder „SAP BW 7“ verwendet. Auch das Kürzel BW schließt alle OLAP-spezifischen Komponenten mit ein. [vgl. JOHN/KIENER (2010), S. 34]

379 Vgl. SAP (2011)

380 Zu Beginn der Forschungskooperation zwischen Prof. Dr. Peter Kleinschmidt und Prof. Dr. Robert Weismantel hatte letzterer den Lehrstuhl für Mathematische Optimierung an der Otto-von-Guericke Universität Magdeburg. Daher sind Objekte im verwendeten SAP NetWeaver BI 7.0 häufig unter „Magdeburg“ und/oder „Weismantel“ eingeordnet. Inzwischen wechselte Prof. Dr. Robert Weismantel an das Institut für Operations Research an der Eidgenössischen Technischen Hochschule Zürich (ETHZ).

381 Vgl. MEHRWALD (2007), S. 7

chen Quellen, wie bspw. SAP (ERP-)Quellsystemen, ausgewählten DBMS und flachen (Text-)Dateien. In der beispielhaften Implementierung werden alle Daten aus flachen Dateien extrahiert.[382] Die Daten werden per Extraktion aus der Quelle in den Eingangsbereich der Data Warehouse-Schicht geladen.

zu (2) Data Warehouse. Die Funktionalität der Data Warehouse-Schicht lässt sich wiederum in einem Schichtenmodell ordnen, wie es in Abbildung 39 dargestellt wird. Die Daten „fließen", während sie entsprechend angepasst werden, „von unten nach oben" bis sie im Rahmen des Data Mart Layer in eine BW-spezifische multidimensionale Struktur gebracht werden.

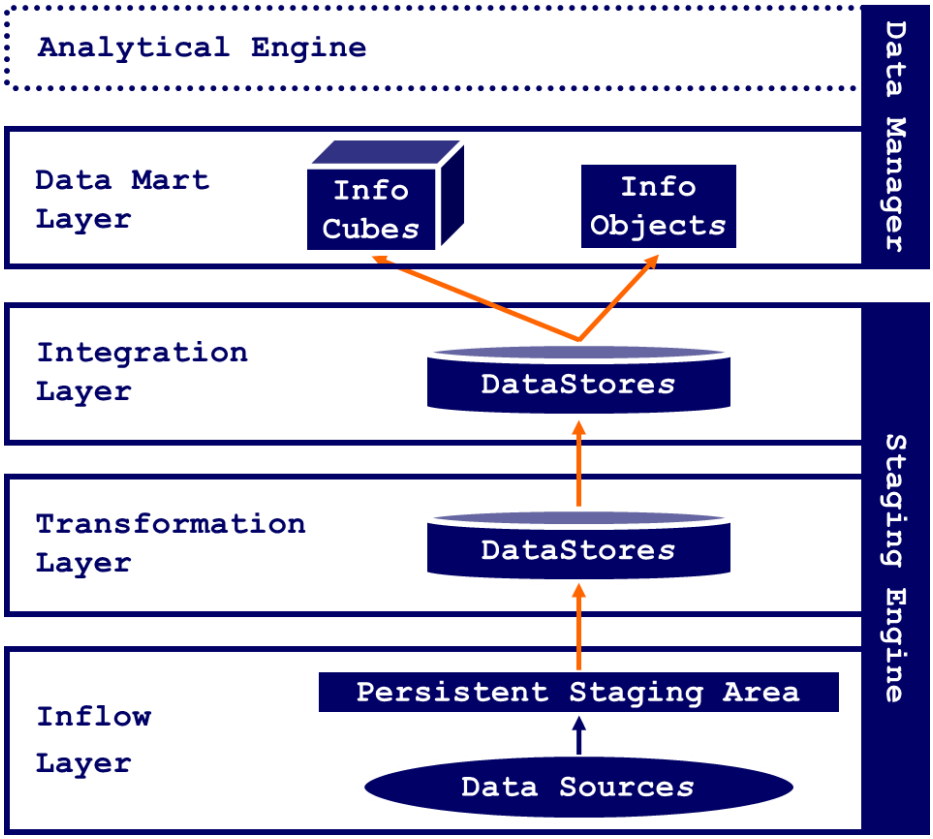


Abbildung 39: Referenzarchitektur der Data Warehouse-Schicht im SAP BI 7.0
In Anlehnung an JÜTTNER ET AL. (2010), S. 132

Die einzelnen Schichten sind dem Data Manager oder der Staging Engine zuzuordnen. Die Staging Engine umfasst Funktionen zur schrittweisen Aufbereitung der Daten aus den Quellsystemen im Sinne der Transformationsschicht (vgl. Abschnitt 2.3). Die Verbin-

[382] Für das Ziel der beispielhaften Implementierung ist die Art und Anbindung der Datenquellen nicht erheblich. Dennoch ist die Extraktion aus flachen Dateien aufgrund der sehr schnellen Datenübertragung in das SAP BI 7.0 sowie aufgrund des häufig sehr hohen Aufwands für die Einrichtung von Extraktionsmechanismen zu Systemen anderer Anbieter in der Praxis durchaus verbreitet.

dung zwischen Extraktionsschicht und DW bildet der sog. Inflow Layer. Dort werden die Daten aus den Quellsystemen zunächst unverändert in die Persistent Staging Area geladen. Der Ladevorgang orientiert sich an der sog. DataSource, die eine Strukturbeschreibung der Quelldaten in Form eines Relationenschemas darstellt. Wie die Extraktionsschicht ist der Inflow Layer für die beispielhafte Implementierung nicht von großem Belang, da weniger die Herkunft der Daten als deren Verarbeitung im Rahmen des SAP BI 7.0 interessiert.

Eine Harmonisierung (und ggf. Filterung) der Daten erfolgt im sog. Transformation Layer. Im Allgemeinen werden Daten für eine quellsystemunabhängige, persistente und integrierte Datenhaltung im Integration Layer transformiert und gespeichert. Das SAP BW 7.0 macht keine architektonischen Vorgaben für die Ausgestaltung dieser beiden Schichten und stellt mehrere Möglichkeiten bereit, Daten im Veränderungsprozess zwischenzuspeichern. In obiger Grafik finden sind beispielhaft sog. DataStores. Ein DataStore ist im Wesentlichen eine flexibel gestaltbare (relationale) Tabelle, die als Tabellenattribute Elemente des BW-spezifischen Datenmodells (sog. InfoObjects, s.u.) aus dem Data Mart Layer verwendet. Neben DataStores lassen sich hier u.a. auch sog. InfoSources einordnen, die lediglich eine Datenstrukturbeschreibung darstellen, an die die „durchfließenden Daten“ angepasst werden.[383]

Die orangefarbenen Linien in Abbildung 39 symbolisieren sog. Transformationen. Transformationen sind Regeln, die das Mapping der Daten beim Übergang von einer in die nächste Struktur bestimmen. Transformationen bieten darüber hinaus umfangreiche Funktionalitäten zur Veränderung und Anreicherung der Daten im Moment des Übergangs.

Der Data Manager dient der Präsentation der Daten (z.B. im Rahmen von OLAP) zur eigentlichen Auswertung. Im Data Mart Layer erfolgt daher eine Überführung der zur späteren Auswertung bestimmten Daten in BW-spezifische Datenstrukturen. Die homogenisierten, granularen Daten des Integration Layers sollen im Data Mart Layer anwendungsspezifisch aufbereitet werden.

Das SAP BI 7.0 verwendet das ROLAP-Konzept (vgl. Abschnitt 2.3) in Form einer Erweiterung des sog. Star-Schemas zur relationalen Umsetzung multidimensionaler Schema-

[383] Anders als die DataStores sieht die InfoSource keine physische Datenhaltung vor.

ta[384], die über ein SAP BW-spezifisches multidimensionales Modell definiert wurden. Die relationale Abbildung muss hier nicht weiter thematisiert werden, jedoch werden für das Beispiel relevante Elemente des SAP BW-spezifischen Datenmodells im Folgenden kurz vorgestellt, da diese für die Berechtigungsverwaltung im SAP BI 7.0 Ansatzpunkte darstellen.

InfoObjects sind die kleinsten Modellelemente im SAP BW 7.0. Man unterscheidet verschiedene Typen von InfoObjects (vgl. Abbildung 40). Merkmale beschreiben bestimmte betriebswirtschaftliche Sachverhalte und regeln, nach welchen Bezugsgrößen Kennzahlen gruppiert werden können. Sie dienen als Strukturbeschreibung (Datentyp etc.) für Dimensionselemente und gleichzeitig als Datencontainer für konkrete Ausprägungen des Merkmals. (Das SAP BW 7.0 setzt so ein Stammdatenkonzept um, das berücksichtigt, dass Zusammenstellungen und ggf. Hierarchisierungen von Dimensionsmerkmalen in mehreren Analyseumgebungen - sprich: InfoCubes - verwandt werden können.) Bei Kennzahlen handelt es sich ausschließlich um eine Strukturbeschreibung für Faktenwerte (Datentyp, etc.), die den Inhalt der Würfelzellen darstellen. Kennzahlen vom Typ Betrag bzw. Menge werden automatisch eine Einheit, die im gleichlautenden systemeigenen Merkmal vorgehalten wird, zugeordnet. Weitere systemseitig vorgegebene Merkmale sind die Zeitmerkmale (z.B. Kalendertag, Kalenderjahr/Monat), die jedoch grundsätzlich die gleiche Aufgabe wie die bereits eingeführten Merkmale haben.

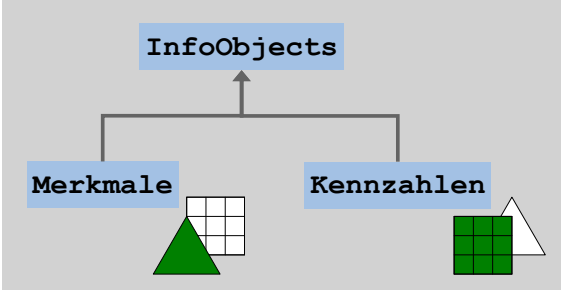


Abbildung 40: SAP InfoObjects
Eigene Darstellung

[384] Das erweiterte Starschema der SAP sieht pro Merkmal ergänzende sog. „Stammdatentabellen“ vor, die jeweils von einem Schlüsselattribut eines Merkmals (sog. S-IDs) in den Dimensionstabellen referenziert werden. In diesen Stammdatentabellen befinden sich im Wesentlichen Informationen zu Ausprägungen (originäre Schlüssel) sowie zugehörigen Attributen, Texten und Hierarchien des jeweiligen Merkmals. Diese Tabellen werden unabhängig vom jeweiligen InfoCube vorgehalten und können so - im Sinne eines Stammdatenkonzepts - in mehreren Kontexten (InfoCubes, DataStores) verwendet werden.

Merkmale (vgl. Abbildung 41) können für die enthaltenen Ausprägungen die Speicherung von Texten, Attributen und (externe) Hierarchien vorsehen. Attribute sind zugeordnete Merkmale, die vom eigentlichen Merkmal funktional abhängig sind. Externe Hierarchien ordnen die Ausprägungen des Merkmals (Dimensionselemente) in eine Hierarchie, wobei übergeordnete Hierarchieknoten bzw. die entspr. Hierarchiestufen andere Merkmale referenzieren können.

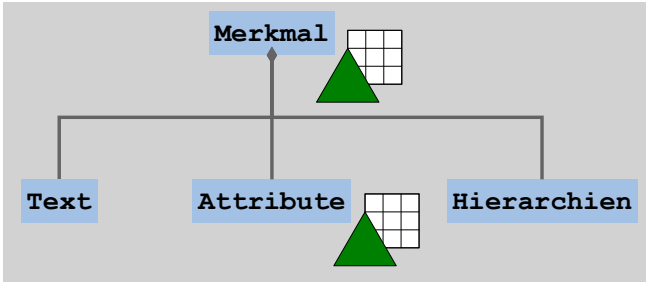


Abbildung 41: SAP Merkmal
Eigene Darstellung

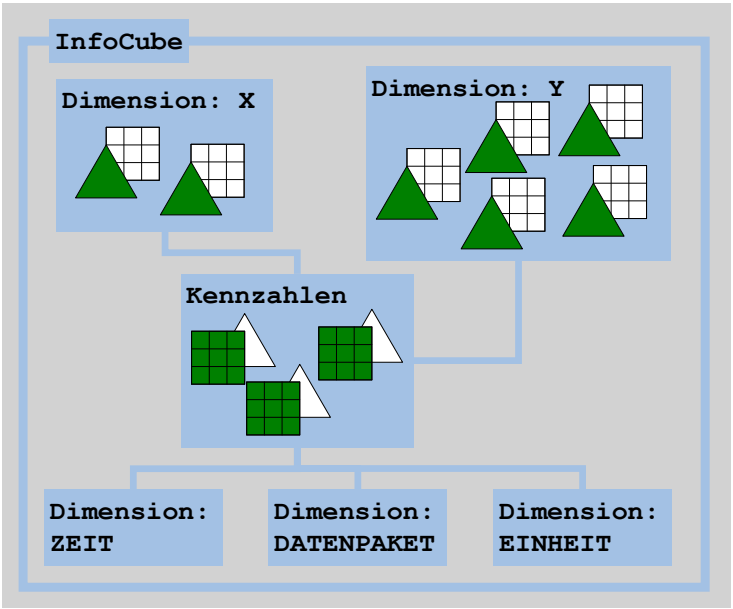


Abbildung 42: SAP InfoCube
Eigene Darstellung

InfoCubes (vgl. Abbildung 42) stellen die SAP BW-spezifische Adaption der multidimensionalen Datenwürfel dar. Sie speichern in sich geschlossene Datenbestände und bestehen aus einer oder mehreren Kennzahlen sowie mehreren Merkmalen, die das Gerüst des Würfels aufspannen und frei bestimmbaren Dimensionen[385] zugeordnet werden. Die Dimensionen Zeit und Einheit sind systemseitig vorgegeben und beinhalten entspr. Merkmale. Ebenfalls systemseitig vorgegeben ist die Dimension Datenpaket, deren enthaltene

[385] SAP-Dimensionen dienen lediglich als Container für Merkmale, die aus Performanzgründen zwar in funktionaler Abhängigkeit stehen sollten, es technisch jedoch nicht müssen. Sie entsprechen daher nicht der Definition aus Abschnitt 2.2.

Merkmale im Wesentlichen der Zuordnung der Daten im InfoCube dienen. In einen InfoCube werden also in die durch die Merkmale festgelegten Zellen die Ausprägungen der Kennzahlen geschrieben.

Bzgl. Abbildung 39 bleibt noch anzumerken, dass hier jedes Designelement (DataStore, InfoObject, InfoCube) in jeder Schicht aus Gründen der Übersichtlichkeit nur einmal auftaucht; zwischen Designelementen unterschiedlicher Schichten sind jedoch durchaus N:M-Beziehungen üblich.

Als oberste Schicht des Data Managers übernimmt die Analytical Engine die Funktion der R-OLAP-Engine (vgl. Abschnitt 2.3) und setzt die Abfragen des zugreifenden Analysetools um.

zu (3) Data Analysis. Für die Datenanalyse können SAP-eigene Analysetools oder Tools von Drittanbietern verwendet werden. Hier wird der SAP-eigene BEx Web Analyzer verwendet, der über den BEx API (Business Explorer Application Programming Interface) auf die Analytical Engine (OLAP Prozessor) zugreift.

Mit Hilfe des Query Designers werden Abfragen, sog. SAP-Queries, auf entspr. BW-Elementen (hier: InfoCube) definiert. Diese Queries regeln hauptsächlich Umfang, Granularität und Design des angezeigten Datenbestandes.

6.3.2 Beschreibung des Beispielszenarios

Wir gehen von einem einfachen Unternehmen aus, das (drei) hochwertige Fahrradtypen über ausgewählte Fachgeschäfte verkauft. Einige Mitarbeiter der Verkaufsabteilung sind im Außendienst für den Verkauf in jeweils einer bestimmten Stadt zuständig. (Im Weiteren werden sie als „Außendienstler“ bezeichnet.)

Den Außendienstlern soll durch den InfoCube „Verkaufs-Cube“ (vgl. Abbildung 43) ein OLAP-basiertes Controlling ihrer Verkaufszahlen ermöglicht werden. Der Würfel enthält dazu die Dimensionen „Produkt“, „Region“ und „Zeit“ sowie die Kennzahl „Anzahl verkaufter Produkte“. Die Zeit-Dimension ist mit den Merkmalen „Kalendertag“ und „Kalenderjahr / Monat“ gefüllt. Die Dimension „Produkt“ beinhaltet

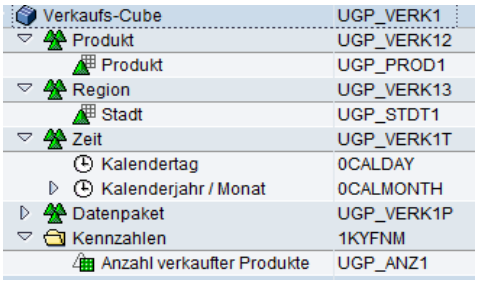


Abbildung 43: Datenmodell des Verkauf-Cubes Screenshotausschnitt aus dem SAP BI 7.0

nur das gleichlautende Merkmal. Da nur der Verkauf von drei Produkten dargestellt wird, kann hier auf eine Hierarchie verzichtet werden. Anders verhält es sich bei dem Merkmal „Stadt", das in die Dimension „Region" eingeordnet wurde (vgl. Abbildung 44).

Das Unternehmen ist in Nordrhein-Westfalen, Bayern und Oberösterreich aktiv. Es hat die Regionen, in der es seine Außendienstler tätigt sind, in eine dem Merkmal „Stadt" zugeordnete Hierarchie untergliedert, die die Dimensionsstufen „Stadt" → „Bundesland" → „Regierungsbezirk" → „Land" umfasst. (Für das Bundesland „Oberösterreich" wurden analog zu den deutschen Regierungsbezirken historische Viertel zur Einteilung verwendet.)

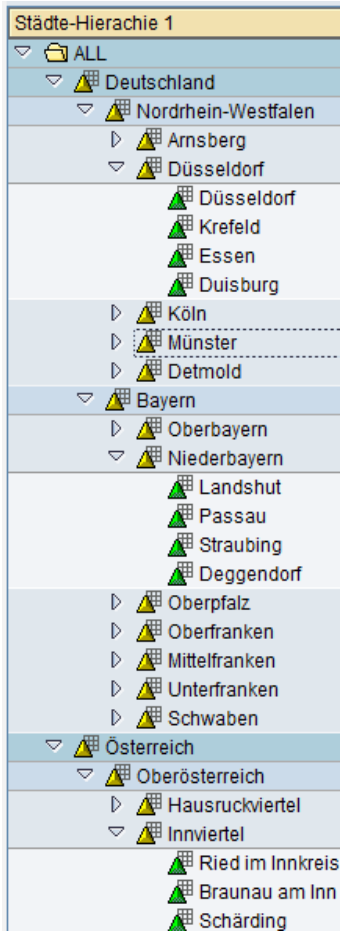


Abbildung 44: Hierarchie des Merkmals Stadt
Ausschnitt eines Screenshots aus SAP BI 7.0

Ein wesentlicher Anteil des Gehalts der Außendienstler ist erfolgsabhängig. Insofern lassen die Verkaufszahlen in einer Stadt einen Rückschluss auf die Höhe des Gehalts des entspr. Außendienstlers zu. Es ist daher sicher nicht wünschenswert, dass Außendienstler die Verkaufszahlen aller ihrer Kollegen einsehen können. Auf der anderen Seite sollten sie in der Lage sein, Änderungen der Verkaufszahlen in ihrem Verantwortungsbereich sinnvoll in einen Kontext setzen zu können.

Der Außendienstler für die Stadt Passau sollte sicher auf die entsprechenden Verkaufszahlen Zugriff haben. Er sollte jedoch auch in der Lage sein, Entwicklungen seiner eigenen Verkaufszahlen mit denen der umliegenden Städte, die für Passauer Kunden in Reichweite liegen, ins Verhältnis zu setzen.

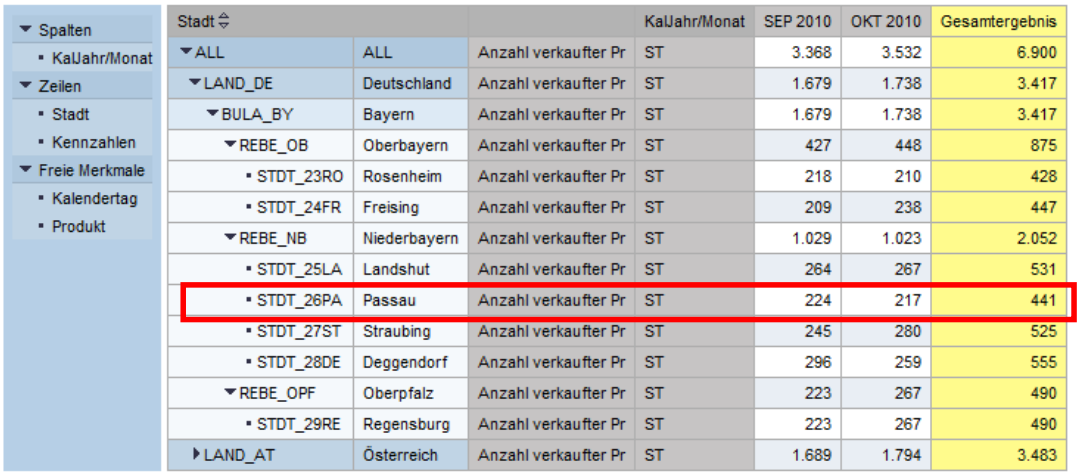
Ein Vorgehen anhand der vorgestellten Ansätze würde bedingen, dass ein Administrator für jeden Verkaufsmitarbeiter im granularsten Fall für jede einzelne Stadt festlegen müsste, ob der entspr. Außendienstler Zugriff auf die dortigen Verkaufszahlen haben soll. In einem Szenario realistischer Größenordnung ist dieses Vorgehen im Hinblick auf den administrativen Aufwand kaum machbar. Es wäre jedoch denkbar, dass man Automatis-

men vorsieht, die einem Außendienstler auf Basis „seiner" Stadt unter Rückgriff auf die Städtehierarchie Zugriff auf bspw. alle Städte des entspr. Regierungsbezirks, Bundeslands oder gar Lands erlauben. Gerade hier zeigt sich die Schwäche einer Hierarchie zur Festlegung, welche Bereiche eines Datenwürfels analysiert werden dürfen. Eine sinnvolle, explorative Datenanalyse erfordert auch Zugriff auf Daten der Städte, die in einem relativ engen Abstand zu der „interessanten Stadt" liegen. Eine Bestimmung des zugänglichen Datenaussschnitts anhand der Grenzen von Hierarchien, in diesem Fall also regionale Grenzen, sind mindestens für Städte, die im geographischen Randbereich eines Hierarchiestufencontainers liegen, nicht sinnvoll.

Das Unternehmen hat daher entschieden, die Berechtigungen für Außendienstler anhand von Interessensschwerpunkten zu vergeben, die hier naheliegender Weise durch jeweils eine Stadt pro Außendienstler festgemacht werden. Die für einen Außendienstler relevanten Städte werden dann anhand seines Interessenradius und den Abständen zwischen den Städten bestimmt. Beide Parameter beziehen sich auf die Entfernung der Städte über das Straßennetz. Die Abstände zwischen den Städten lassen sich bspw. - wie hier geschehen - durch das Programm Microsoft MapPoint Europa 2011 (mit dem Plugin MPMileCharter) berechnen und automatisch in eine Textdatei extrahieren, die dann in das SAP BW übertragen werden kann.[386] Der Außendienstler für Passau, aus dessen Perspektive nun mit dem SAP BEx Web Analyzer eine einfache Analyse demonstriert wird, hat den Interessensradius 100 (entspr. 100 km) und soll im Weiteren als Herr Maier bezeichnet werden.

Zunächst betrachtet Herr Maier alle deutschen Städte mit kumulierten Verkaufszahlen für September. Ihm fällt auf, dass trotz seiner vermehrten verkaufsfördernden Maßnahmen die Verkaufszahlen für die Stadt Passau zurückgegangen sind. Insgesamt ergibt sich jedoch ein uneinheitliches Bild der ihm zugänglichen Verkaufszahlen in deutschen Städten (vgl. Abbildung 45).

[386] In diesem Beispiel wurden die Zahlen zunächst in eine Datenbanktabelle (PostgreSQL 9.0) in From einer Abstandsmatrix geschrieben und dann mittels einer einfachen PL/pgSQL-Prozedur in eine Tabelle des Schemas (VON_STADT, BIS_STADT, ENTFERNUNG) geschrieben, um sie so leichter in das SAP BW übertragen zu können.



- Spalten
  - KalJahr/Monat
- Zeilen
  - Stadt
  - Kennzahlen
- Freie Merkmale
  - Kalendertag
  - Produkt

Stadt			KalJahr/Monat	SEP 2010	OKT 2010	Gesamtergebnis
ALL	ALL	Anzahl verkaufter Pr	ST	3.368	3.532	6.900
LAND_DE	Deutschland	Anzahl verkaufter Pr	ST	1.679	1.738	3.417
BULA_BY	Bayern	Anzahl verkaufter Pr	ST	1.679	1.738	3.417
REBE_OB	Oberbayern	Anzahl verkaufter Pr	ST	427	448	875
STDT_23RO	Rosenheim	Anzahl verkaufter Pr	ST	218	210	428
STDT_24FR	Freising	Anzahl verkaufter Pr	ST	209	238	447
REBE_NB	Niederbayern	Anzahl verkaufter Pr	ST	1.029	1.023	2.052
STDT_25LA	Landshut	Anzahl verkaufter Pr	ST	264	267	531
STDT_26PA	Passau	Anzahl verkaufter Pr	ST	224	217	441
STDT_27ST	Straubing	Anzahl verkaufter Pr	ST	245	280	525
STDT_28DE	Deggendorf	Anzahl verkaufter Pr	ST	296	259	555
REBE_OPF	Oberpfalz	Anzahl verkaufter Pr	ST	223	267	490
STDT_29RE	Regensburg	Anzahl verkaufter Pr	ST	223	267	490
LAND_AT	Österreich	Anzahl verkaufter Pr	ST	1.689	1.794	3.483

Abbildung 45: SAP BEx Web Analyzer - Städte im Umkreis Passaus (D)
Ausschnitt eines Screenshots aus dem SAP BEx Web Analyzer

Maier prüft daraufhin die Städte in Oberösterreich, auf die er Zugriff hat. Sofort fällt ihm ins Auge, dass die Verkaufszahlen in Schärding im Oktober rapide gestiegen sind (vgl. Abbildung 46).

- Spalten
  - KalJahr/Monat
- Zeilen
  - Stadt
  - Kennzahlen
- Freie Merkmale
  - Kalendertag
  - Produkt

Stadt			KalJahr/Monat	SEP 2010	OKT 2010	Gesamtergebnis
ALL	ALL	Anzahl verkaufter Pr	ST	3.368	3.532	6.900
LAND_DE	Deutschland	Anzahl verkaufter Pr	ST	1.679	1.738	3.417
LAND_AT	Österreich	Anzahl verkaufter Pr	ST	1.689	1.794	3.483
BULA_OO	Oberösterreich	Anzahl verkaufter Pr	ST	1.689	1.794	3.483
REBE_HAU	Hausruckviertel	Anzahl verkaufter Pr	ST	965	985	1.950
STDT_69WE	Wels	Anzahl verkaufter Pr	ST	228	246	474
STDT_70GR	Grieskirchen	Anzahl verkaufter Pr	ST	262	270	532
STDT_71VO	Vöcklabruck	Anzahl verkaufter Pr	ST	257	258	515
STDT_72AL	Alkoven	Anzahl verkaufter Pr	ST	218	211	429
REBE_INN	Innviertel	Anzahl verkaufter Pr	ST	724	809	1.533
STDT_73RI	Ried im Innkreis	Anzahl verkaufter Pr	ST	270	238	508
STDT_74BR	Braunau am Inn	Anzahl verkaufter Pr	ST	269	227	496
STDT_75SC	Schärding	Anzahl verkaufter Pr	ST	185	344	529

Abbildung 46: SAP BEx Web Analyzer - Städte im Umkreis Passaus (AT)
Ausschnitt eines Screenshots aus dem SAP BEx Web Analyzer

Ein anschließender Drill Down auf Einzelproduktebene - gefiltert nach Passau und Schärding (Dice) - ergibt (vgl. Abbildung 47), dass der Verkauf des Produkts MountainBike in Schärding im Oktober sprunghaft angestiegen und gleichzeitig in Passau rapide gefallen ist. Grund hierfür könnte bspw. ein sehr gutes Sonderangebot in Schärding sein, das auch in Passau bekannt (gemacht) wurde und für interessierte Kunden den Weg von Passau nach Schärding lohnend machte.

Stadt		Produkt			KalJahr/Monat	SEP 2010	OKT 2010	Gesamtergebnis
Gesamtergebnis				Anzahl verkaufter Pr	ST	409	561	970
STDT_26PA	Passau	PROD_MO	MountainBike	Anzahl verkaufter Pr	ST	67	16	83
		PROD_RA	RacingBike	Anzahl verkaufter Pr	ST	76	93	169
		PROD_ST	StreetBike	Anzahl verkaufter Pr	ST	81	108	189
		Ergebnis		Anzahl verkaufter Pr	ST	224	217	441
STDT_75SC	Schärding	PROD_MO	MountainBike	Anzahl verkaufter Pr	ST	60	133	193
		PROD_RA	RacingBike	Anzahl verkaufter Pr	ST	52	97	149
		PROD_ST	StreetBike	Anzahl verkaufter Pr	ST	73	114	187
		Ergebnis		Anzahl verkaufter Pr	ST	185	344	529

Abbildung 47: SAP BEx Web Analyzer - Drill Down & Dice zu Passau und Schärding
Ausschnitt eines Screenshots aus dem SAP BEx Web Analyzer

Wären die Berechtigungen auf Basis des Hierarchiebaums vergeben worden, hätte Herr Maier nur von dieser Konstellation erfahren, wenn er eine Berechtigung auf der Hierarchiestufe „Land“ für Deutschland und Österreich bis auf die Ebene der Städte erhalten hätte. Dies würde aber auch bedeuten, dass Herr Maier die Verkaufszahlen seines Kollegen, der für Duisburg zuständig ist, hätte einsehen können. Verkaufsaktionen in Duisburg beeinflussen aber wahrscheinlich kaum das Passauer Geschäft, und so würde das Unternehmen unnötigerweise eine Inferenz auf das Gehalt des Duisburger Kollegen in Kauf nehmen.

6.3.3 Implementierung in SAP BI 7.0

Die Implementierung des Sicherheitsmechanismus fügt sich in das in Abschnitt 6.3.1 beschriebene Schichten-Modell aus Transformation, Integration sowie Data Mart Layer ein. Als OLAP-Anwendung dient - wie aus dem vorangegangenen Abschnitt deutlich geworden - der Web Analyzer, der für alle Außendienstler über die gleiche BEx Query mit Daten versorgt wird.

Ausgangspunkt des Beispiels ist der InfoCube „Verkaufs-Cube“. Der InfoCube enthält alle potentiell relevanten Daten. Die Einschränkungen auf die relevanten Städte pro Außendienstler werden durch die genannte Query vorgenommen.

Eine schematische Darstellung der Implementierung findet sich in Abbildung 48, wobei hier der Sicherheitsmechanismus bei Aufrufen der Query noch nicht dargestellt wird. (Dieser Aspekt findet sich in Abbildung 49.) Hier wird lediglich gezeigt, wie Abstandsmatrix und Interessensschwerpunkte pro Außendienstler im Rahmen des SAP BW Daten- und Datenflussmodells integriert und daraus zugriffsrelevante Informationen generiert werden können.

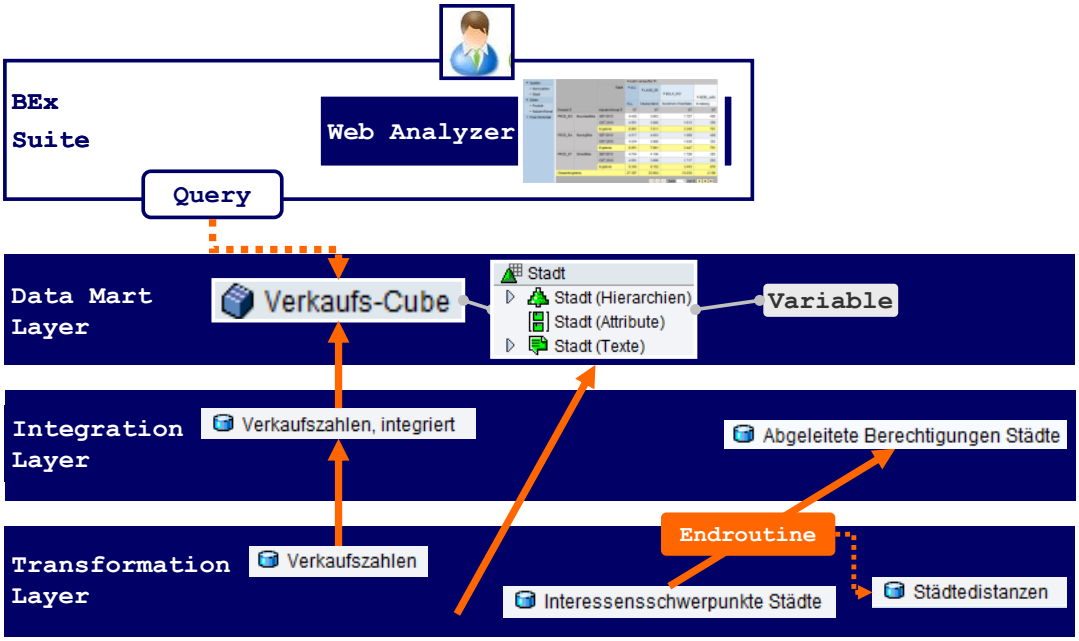


Abbildung 48: Implementierung von Interessensschwerpunkten in SAP BI 7
Eigene Darstellung (Symbole für InfoObects, DataStores und InfoCube sind Screenshots aus dem SAP BI 7.0 entnommen. Ebenfalls einem Screenshot entnommen ist die kleine Tabelle des Web Analyzers.)

Der Verkaufs-Cube wird über zwei DataStore-Objekte mit Daten gefüllt. Dem Verkaufs-Cube zugeordnet ist das Merkmal Stadt, das unter anderem mit einer externen Hierarchie versehen ist, deren Hierarchiestufen bzw. -knoten mit Ausprägungen der Merkmale „Land“, „Bundesland“ und „Regierungsbezirk“ gebildet werden.[387]

Das DataStore-Objekt „Interessensschwerpunkte Städte“ entspricht einer Tabelle mit dem Tabellenschema (Benutzer, Stadt, Radius), die jeweils einem InfoObject entsprechen. Bei Stadt handelt es sich um das auch im Verkaufs-Cube enthaltene InfoObject. USER wurde als Merkmal angelegt und beinhaltet SAP BI-Nutzer. Radius wurde als Kennzahl zur Aufnahme des Interessenradius definiert. Das DataStore-Objekt umfasst also genauso viele Zeilen, wie Benutzer gepflegt werden.

Das DataStore-Objekt „Städtedistanzen“ entspricht einer Tabelle mit dem Tabellenschema (Stadt_von, Stadt_bis, Distanz). Die für dieses InfoObject angelegten Merkmale (hier: Tabellenschlüsselattribute) referenzieren das Merkmal Stadt. Die Distanz wird analog zum Radius in einer Kennzahl festgehalten. Jeder Datensatz speichert die Distanz zwischen einer Stadt und einer anderen, so dass die Tabelle eine komplette Städtematrix mit der

[387] In der Version 7.0 des SAP BW kann eine externe Hierarchie ausschließlich über eine InfoSource angelegt werden. Die Hierarchie basiert auf einem in das BW geladenes Textfile, das in csv-Fomat den Inhalt einer Tabelle mit rekursiver Fremdschlüsselbeziehung zur Abbildung einer nicht überlappenden Hierarchie zwischen den Datensätzen (bzw. Knoten) beinhaltet. Jeder Knoten ist darin eindeutig einem übergeordneten zugeordnet.

Zeilenanzahl $|\text{Stadt}|^2$ abbildet.

Im DataStore-Objekt „Abgeleitete Berechtigungen Städte“ mit dem Tabellenschema (Stadt, Benutzer) werden die zulässigen Städte pro BW-Benutzer festgehalten, wobei jede Zeile eine zulässige Benutzer-Stadt-Kombination angibt. Dieses DataStore-Objekt wird über eine von „Interessensschwerpunkte Städte“ ausgehende Transformation mit Daten gefüllt. Im Rahmen dieser Transformation ist eine Endroutine (ABAP-Programm) definiert, die für jeden Benutzer aus „Interessensschwerpunkte Städte“ und jeder Stadt_bis aus „Städtedistanzen“, die innerhalb des Radius zum Interessensschwerpunkt (sprich Stadt aus „Interessensschwerpunkte Städte“) liegt, einen entsprechenden Datensatz in den Datentransfer integriert.

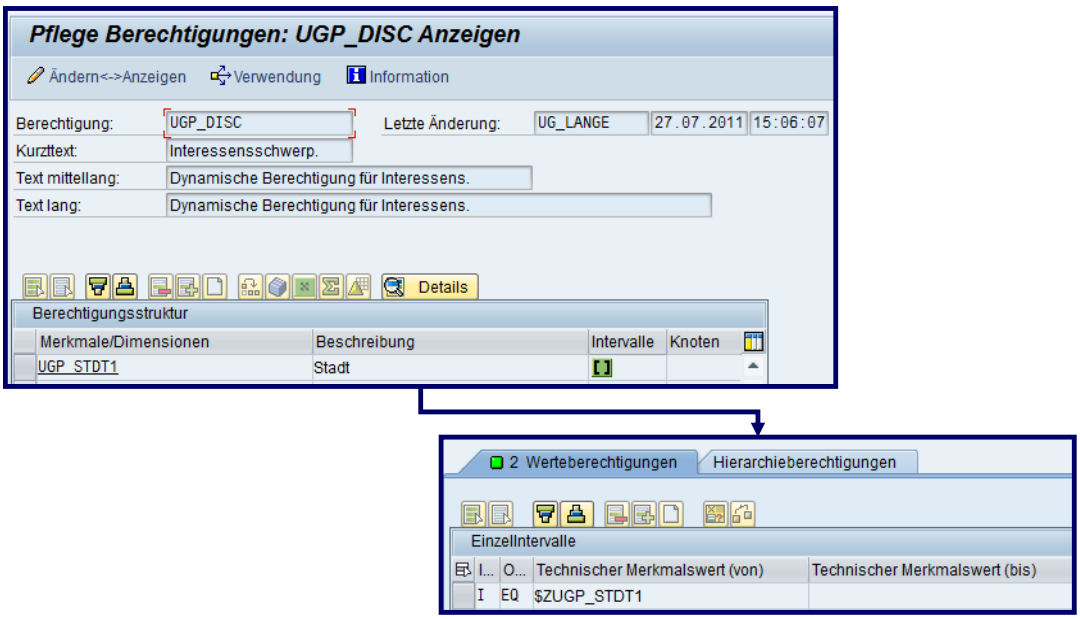


Abbildung 49: Berechtigung für das Merkmal Stadt (Intervall durch Variable)
Ausschnitte zweier Screenshots aus dem SAP BI 7.0

Weiterhin wurde das Merkmal Stadt als „berechtigungsrelevant“ gekennzeichnet. In der Ausgestaltung der Berechtigung (vgl. Abbildung 49) wurde festgelegt, dass die anzuzeigenden Merkmalsausprägungen (entspr. dem angezeigten Werte-„Intervall“) über eine „OLAP-Variable“ ($ZUGP_STDT1) bestimmt werden. Im Ergebnis heißt dies, dass unter dem Merkmal Stadt lediglich solche Ausprägungen angezeigt werden, die bei Zugriff auf die Merkmalsinformationen in der entsprechenden Variable vorhanden sind. (Eine OLAP-Variable kann mehrere Werte enthalten.) Eine Füllung der Variablen wird dynamisch bei Ausführung der entsprechenden Query vorgenommen. Bei der Definition der Query wurde eine Merkmalseinschränkung für das Merkmal Stadt anhand dieser Variablen vorgesehen (vgl. Abbildung 50).

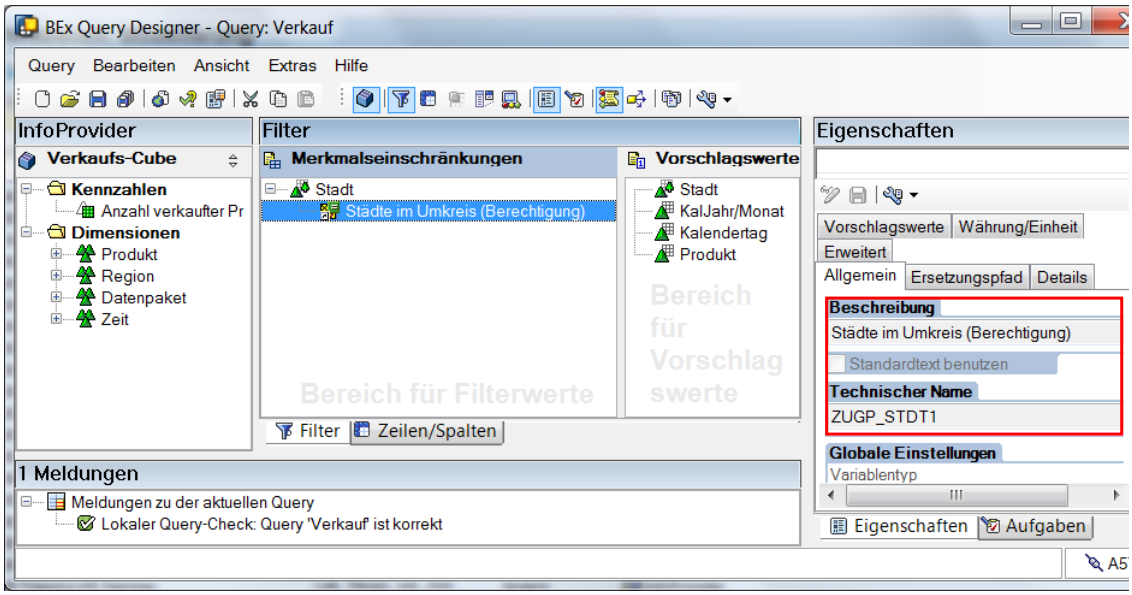


Abbildung 50: SAP BEx Query Designer - Query Verkauf (Screenshot)
Ausschnitt eines Screenshots aus dem SAP BEx Query Designer

Bei Ausführung der Query greift der in Abbildung 51 dargestellte Mechanismus.

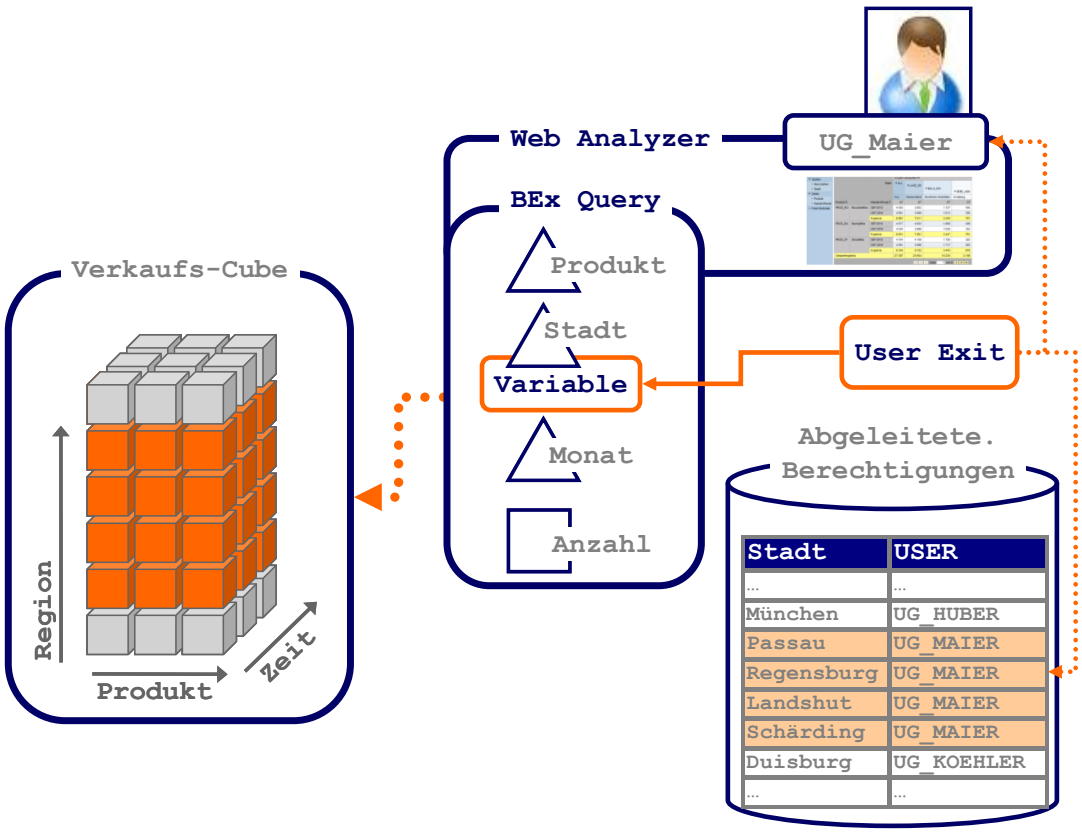


Abbildung 51: SAP BEx Query Designer - Query Verkauf (Verarbeitung)
Eigene Darstellung

Wird die Query aufgerufen, wurde festgelegt, dass automatisch auch ein User Exit (ABAP-Programm) ausgeführt wird. Dieser füllt anhand des Benutzernamens des aufrufenden Benutzers aus dem DataStore-Objekt „Abgeleitete Berechtigungen Städte“ die

Variable mit den für diesen Benutzer zulässigen Städten, so dass sich für diesen Benutzer nur eine ausschnitthafte Sicht auf den Verkaufs-InfoCube ergibt.

Die vorgestellte Implementierung bedingt nur eine äußerst geringe Beeinflussung der Performanz, da nur vor der eigentlichen Analysetätigkeit einmal beim Ausführen der Query eine sehr einfache Datenbankabfrage zur Füllung der OLAP-Variable durchzuführen ist.

Im Sinne des Stammdatenkonzepts der Merkmale können auch die berechtigungsrelevanten Informationen zu Interessensschwerpunkten in den DataStores pro Merkmal in unterschiedlichen InfoCubes verwendet werden und so den administrativen Aufwand eines Berechtigungsmechanismus erheblich reduzieren.

Die Implementierung ist bewusst einfach gehalten, lässt sich aber über die angesprochenen Berechtigungsmöglichkeiten in SAP BI 7.0 flexibel erweitern. Da auf jeden einzelnen Hierarchieknoten Berechtigungen vergeben werden können, ließe sich mit relativ geringem Implementierungsaufwand diese Lösung auch so erweitern, dass jeder Benutzer mindestens auf alle Städte des Bundeslands, in dem sein Interessensschwerpunkt liegt, zugreifen könnte.

Die Angabe mehrerer Interessensschwerpunkte (entspr. mehreren Städten) pro Benutzer ist schon in dieser Implementierung möglich. Auch auf andere Merkmale (bspw. Produkt) des Info-Cubes ließe sich die Lösung problemlos ausweiten. Hierzu sollten jeweils analog zu den Strukturen für das Merkmal Stadt drei DataStore-Objekte angelegt werden.

Im Rahmen dieses Beispiels wurde jedoch noch kein Mechanismus implementiert, der dem Benutzer zeigt, bei welchen Hierarchieknoten ihm nur eine Teilmenge der untergeordneten Städte gezeigt wird. Dies wäre insofern sinnvoll, da die Aggregationsfunktion (hier: Summe der Verkaufszahlen) auf Ebene von Regierungsbezirken, Bundesländern und Ländern pro Nutzer im Regelfall zu unterschiedlichen Ergebnissen führt.

7 FAZIT

Diese Arbeit leistet in zweifacher Hinsicht einen Beitrag zur Forschung auf dem Gebiet von Disclosure Limitation in OLAP. Zur Erreichung des Hauptziels, Disclosure Limitation in OLAP der praktischen Anwendbarkeit näher zu bringen, wurde erstens ein kontextbasiertes, leicht administrierbares Verfahren zur Spezifizierung und Aktualisierung von Zugriffsrechten in OLAP-Anwendungen entwickelt. Zweitens wurde ein Modell zur Evaluation von OLAP-Anwendungen und von Sicherheitsmechanismen in OLAP-Anwendungen erarbeitet. Die Erkenntnisbeiträge der vorliegenden Arbeit werden im Folgenden zusammengefasst. Abschließend werden Ansatzpunkte zur Weiterentwicklung und empirischen Überprüfung der in dieser Arbeit vorgeschlagenen Konzepte aufgezeigt.

7.1 Zusammenfassung

Kontextbasierte Zugriffskontrollmechanismen werden auf den mit OLAP verwandten Gebieten Data Warehousing und DBMS zwar schon seit Jahren diskutiert, besitzen jedoch aufgrund ihres geringen Reifegrades nach wie vor geringe praktische Relevanz. Ansätze zur Inferenzkontrolle werden beinahe ausschließlich auf konzeptionell-mathematischer Ebene (weiter) entwickelt und haben bis heute keinen Weg in kommerzielle OLAP-Anwendungen gefunden. Diese Verfahren zeichnen sich dadurch aus, dass ein Zugewinn an (Daten-) Sicherheit mit einem unzumutbar hohen Anstieg der Administrationskosten bzw. Einschränkung der Nutzbarkeit von OLAP verbunden ist. Implementierungs- und Administrationsaufwand entsteht insbesondere bei der Definition von Autorisierungsobjekten, der Rechteverwaltung und der Aktualisierung von Datenbeständen. Die Einschränkung der Nutzbarkeit kann, je nach Verfahren, verschiedene Ursachen haben. Die Möglichkeiten der explorativen Datenanalyse werden besonders stark durch Verfahren beschnitten, welche nur wenige Aggregationsoperationen zulassen und/oder bei denen mit jeder neuen Query die Anzahl unterdrückter bzw. „verbotener“ Zellen zunimmt und dem Nutzer dadurch immer weniger zusätzliche Daten zur Verfügung stehen. Manche Verfahren bedingen im Falle von Aggregationen über große Datenbestände so viele Sicherheitsüberprüfungen, dass die Rechenzeit für die Beantwortung solcher Queries in einem für den produktiven Betrieb unzumutbaren Ausmaß ansteigt.

Nach Meinung des Autors ist die Inferenzkontrolle ein hochinteressantes und mathematisch gut entwickeltes Forschungsgebiet, doch sind die Hürden für die praktische Anwen-

dung der Ansätze (noch) zu hoch. Im Unterschied dazu lassen sich Zugriffskontrollmechanismen relativ leicht implementieren und sind bereits in kommerziellen Standardlösungen integriert. Zum jetzigen Stand der Forschung werden daher zu erwartender Impact und Relevanz der Entwicklung eines verbesserten Verfahrens zur Rechteverwaltung und Zugriffskontrolle höher eingeschätzt.

In dieser Arbeit wird erstmals ein Verfahren entwickelt, das den Arbeitskontext (Interessensschwerpunkte und Interessensradius) der OLAP-Anwender direkt mit den vorhandenen Daten verknüpft. Diese Herangehensweise eröffnet die Möglichkeit, Zugriffsrechte dynamisch zu identifizieren und ihre Vergabe teilweise zu automatisieren. Die Festlegung eines Interessensradius und anschließende Berechnung der Distanzen zwischen Dimensionselementen und Interessensschwerpunkten determinieren die Zugriffsrechte des jeweiligen Nutzers auf die korrespondierenden Werte im Data Cube. Das Verfahren muss flexibel genug sein, um auch nominal skalierte Dimensionen mit hierarchischen Ordnungen in die Berechnung des Interessensschwerpunkts mit einbeziehen zu können. Hierfür wird der Einsatz eines parameterfreien Data-Mining-Verfahrens für sinnvoll gehalten, welches auf Basis von Dokumentenanalyse und semantischer Klassifikation die Zusammenhänge zwischen Dimensionselementen verschiedener Hierarchiestufen abbildet. Bei einer Datenbestandsänderung errechnet das Data-Mining-Verfahren dann automatisch die neuen Distanzen, so dass im Falle der Verringerung der Distanz eines Objektes zu einem Interessensschwerpunkt sofort ersichtlich wird, ob dieses nun innerhalb des Interessensradius liegt. In diesem Fall müssen die Zugriffsrechte entsprechend angepasst werden. OLAP-Anwendern werden nun automatisch, ohne dass eine aufwendige Neustrukturierung und Vergabe von Rechten erfolgen muss, die Daten mit der höchsten Relevanz angezeigt. Ist es aus organisatorischen Gründen nicht erwünscht, diesen Vorgang zu automatisieren, könnte ein Genehmigungsverfahren implementiert werden (vgl. Abschnitt 7.2). Die initiale Festlegung der Interessensschwerpunkte geschieht (zum jetzigen Stand der Entwicklung des Verfahrens) durch die Administratoren in Zusammenarbeit mit Mitarbeitern aus den Fachbereichen. Eine erste beispielhafte Implementierung in SAP BI7.0 zeigt, dass dieser Ansatz im Vergleich zum „konventionellen“ Verfahren flexibler ist und den Nutzen aus der OLAP-basierten Datenanalyse beträchtlich steigert. Die Festlegung von Interessensschwerpunkten pro Anwender und die dynamische Aktualisierung der Zugriffsrechte senken den Verwaltungsaufwand erheblich.

Der zweite Beitrag, welchen diese Arbeit leistet, ist die Erarbeitung eines Evaluationsinstruments für OLAP-Anwendungen. Es existieren keine empirisch überprüften Erkennt-

nisse über die Auswirkungen von Sicherheitsmechanismen auf die Qualität der Datenanalysen oder auf den organisatorischen Nutzen aus dem Einsatz von OLAP. Untersuchungen der Qualität und des Erfolges von DW vernachlässigen den Aspekt der Datensicherheit ebenfalls, obwohl er in DW im Vergleich zu anderen betrieblichen IS von herausragender Bedeutung ist. Der betriebswirtschaftliche Schaden aus der missbräuchlichen Nutzung von Geschäftsdaten kann den Nutzen eines DW erheblich mindern. Somit wird eine entscheidende Erfolgskomponente von DW ausgeblendet, nämlich die notwendige Balance zwischen Nutzerfreundlichkeit bzw. betrieblichem Nutzen (wie verbesserten Prozessen oder Wettbewerbsfähigkeit) und Sicherheit. Eine sicherheitstechnisch absolut notwendige Zugriffsbeschränkung etwa kann durchaus zu einer Reduktion der Nutzerfreundlichkeit des DW führen; so lange jedoch der erwartete Schaden aus der Nichtbeschränkung größer ist als durch die Einschränkung der Nutzerfreundlichkeit, ist diese in Kauf zu nehmen. Ein vor allem auf der Nutzerperspektive basierendes Erfolgsmodell ist somit für die Analyse von DW bzw. OLAP ungeeignet.

Diese Forschungslücke erschwert die Beurteilung bestehender Verfahren hinsichtlich ihrer relativen Vorteilhaftigkeit im produktiven Betrieb sowie die Ableitung fundierter Handlungsempfehlungen für Design und Weiterentwicklung von OLAP in theoretischer wie praktischer Hinsicht. In dieser Arbeit wird erstmals ein Modell zur Untersuchung des Einflusses von Sicherheitsmechanismen auf die Qualität von OLAP-Anwendungen vorgeschlagen. Eine Adaption des theoretisch und empirisch gut fundierten DeLone/McLean-Modells ermöglicht die Beurteilung der Qualität von OLAP-Anwendungen aus Perspektive der Anwender, der Administratoren und Unternehmen. Daraus wird auch ein erster konzeptioneller Vorschlag zur Beantwortung der Frage, wie die Benutzerfreundlichkeit einer OLAP-Anwendung unter Berücksichtigung von Sicherheitsaspekten gemessen werden könnte, entwickelt.

Die theoretisch hergeleiteten Evaluationskriterien bilden eine sinnvolle Grundlage für zukünftige empirische Untersuchung der Qualität von OLAP-Systemen; zusätzlichen Nutzen stiftet das Modell durch die explizite Einbeziehung von Wirkungszusammenhängen zwischen einzelnen Sicherheitsmechanismen und den Modellfaktoren. Es existieren noch keine empirischen Untersuchungen der Auswirkungen verschiedener Sicherheitsrichtlinien auf einzelne Kriterien bzw. von „akzeptablen“ Verschlechterungen der Beurteilung der einzelnen Kriterien, die als Leitlinien für die Ausgestaltung der Sicherheitsmechanismen im OLAP-Designprozess verwendet werden könnten. Nach einer Adaptierung des Messinstruments (diese wird in Abschnitt 7.2 kurz diskutiert) könnte ein empirischer

Test der in dieser Arbeit vermuteten Zusammenhänge wertvolle Hinweise für eine nutzer- und nutzungsfreundliche Gestaltung der Sicherheit von OLAP liefern.

7.2 Forschungsbedarf und Trends

Das vorgeschlagene Verfahren bietet einige interessante Ansatzpunkte für weiterführende Forschungsarbeit. Die grundsätzliche Funktionalität wurde bereits beispielhaft implementiert und erzielte gute Ergebnisse. Jedoch steht ein empirischer Test zur Prüfung des Umfangs der vermuteten Reduktion des Implementierungs- und Administrationsaufwandes noch aus. Auch die Erforschung der Kompatibilität mit anderen Sicherheitsmechanismen bzw. der Leichtigkeit einer Migration von einem Sicherheitskonzept zu dem hier vorgeschlagenen scheint viel versprechend. Beispielsweise dürfte die Existenz eines Rollenkonzepts den Aufwand zur Erstdefinition der Interessensschwerpunkte wesentlich verringern. Eine Integration von RBAC und dem hier vorgeschlagenen Ansatz scheint insofern besonders attraktiv. Zur Weiterentwicklung des Konzeptes wird weitere Forschungsarbeit den Interessensschwerpunkten und der Distanzmessung gewidmet sein. Neben dem hier erörterten Verfahren NGD, das aufgrund der Einfachheit seiner Anwendung, seiner Parameterfreiheit und der guten Resultate in bisherigen Vergleichsuntersuchungen vielversprechend erscheint, wäre der Einsatz anderer Verfahren denkbar. Auch die Wahl des „idealen“ Korpus zur Distanzbestimmung ist noch systematisch zu untersuchen. Wie in Abschnitt 7.1 angesprochen, könnte die automatische Vergabe bzw. Aktualisierung von Zugriffsrechten auf Skepsis der Anwender stoßen. Die Entwicklung und Integration eines effizienten Genehmigungsverfahrens wäre für die Akzeptanz und praktische Anwendbarkeit des vorgeschlagenen Ansatzes sicherlich förderlich.

Im Hinblick auf das in Abschnitt 3.4 speziell zur Beurteilung von Disclosure Limitation in OLAP entwickelte Modell besteht noch Forschungsbedarf hinsichtlich der empirischen Überprüfung. Die im DeLone/McLean-Modell enthaltenen Zusammenhänge wurden bereits für eine Reihe von betrieblichen IS empirisch validiert, so dass eine hohe Aussagekraft der hier vorgeschlagenen Adaption angenommen wird. Da jedoch die hier vorgeschlagenen Änderungen mangels empirischer Forschung zum Thema Nutzerzufriedenheit und Erfolgswirkungen von OLAP weitgehend theoriegeleitet erfolgen, ist eine Prüfung des Modells anzuraten. Bisher gestaltete sich die Durchführung umfassender empirischer Untersuchungen aus mehreren Gründen schwierig.

Erstens zeigen sich Unternehmen sehr zurückhaltend im Hinblick auf die Beteiligung an

Studien im Themengebiet „Erfolg von BI“ und insbesondere „Sicherheit im Rahmen von BI“. Es wird vermutet, dass dies hauptsächlich darin begründet liegt, dass die Unternehmen einerseits die Herausgabe geschäftskritischer Informationen vermeiden wollten und andererseits den dafür notwendigen Aufwand scheuten. Das hier vorgeschlagene Modell ist unter diesen Gesichtspunkten besonders attraktiv für Forscher, denn es verlangt weder die Angabe detaillierter Informationen über die Ausgestaltung der BI-Funktion noch über die technische Implementierung oder gar bezüglich der Ergebnisse der Datenanalysen. Die Durchführung einer solchen Studie erfordert lediglich ein Minimum an Zeit und Aufwand seitens des Unternehmens: Ein großer Teil der Messinstrumente für die hier diskutierten Konstrukte wurden in früheren Studien bereits validiert und auf eine sehr kleine Zahl an Items pro Konstrukt reduziert, so dass der für die Beantwortung des resultierenden Fragebogens notwendige zeitliche Aufwand pro Mitarbeiter gering ist.

Zweitens gestaltet sich die Bezifferung des Nutzens aus OLAP schwierig, insbesondere im Hinblick auf die Schätzung der Höhe der Opportunitätskosten aus der Nichterkennung von Mustern in den Daten. Auch die direkte Zurechnung von Effekten auf strategische Kategorien wie „Wettbewerbsfähigkeit“ oder „Steigerung des Marktanteils“ zu OLAP-Anwendungen ist keine einfache Aufgabe. Hierfür bietet das adaptierte DeLone/McLean-Modell allerdings einen Ansatzpunkt, denn der individuell realisierbare Nutzen aus OLAP ist etwas leichter messbar und kann dazu herangezogen werden, entsprechende Schätzungen auf organisatorischer Ebene zu unterfüttern und zu überprüfen.

Speziell die empirische Untersuchung der Auswirkungen von Verfahren zur Disclosure Limitation auf den durch OLAP-Anwendungen erzielbaren Nutzen für Unternehmen ist besonders interessant, gestaltet sich jedoch schwierig. Die Durchführung einer Feldstudie zum aktuellen Zeitpunkt ist überhaupt nur auf dem Gebiet „Zugriffskontrolle“ sinnvoll, da Verfahren zur Inferenzkontrolle – wie in Abschnitt 4 erläutert – aufgrund der Komplexität und schwierigen Umsetzbarkeit praktisch (noch) nicht relevant sind. Die Prüfung der Effekte von Zugriffskontrollmechanismen kann in einer Studie mit Zwei-Zeitpunkt-Messung (vor und nach der Implementierung) erfolgen. Auch hier wird die größte Herausforderung vermutlich die Akquirierung einer ausreichend großen Zahl an teilnehmenden Unternehmen sein. Daher scheint die Überprüfung des Modells im Rahmen einer Vollerhebung (d.h. die Befragung aller OLAP-Anwender) in einigen ausgesuchten Unternehmen aus praktischer Sicht am vielversprechendsten, wenn auch hinsichtlich der Generalisierbarkeit der Ergebnisse aus theoretischer Sicht nicht völlig zufrieden stellend.

Im Hinblick auf die vorgeschlagenen Anpassungen am DeLone/McLean-Modell bzw.

dessen DW-bezogenen Versionen ist aus konzeptioneller Sicht die hier vorliegende Fokussierung auf Disclosure Limitation zu betonen. Eine ganzheitliche Beurteilung der Erfolgswirkung von OLAP-Anwendungen bedingt die Prüfung des gesamten DeLone/McLean-Modells einschließlich des hier vernachlässigten Konstrukts „Servicequalität" und der Dimensionen „Präsentation", „Integration" und „Zuverlässigkeit" (vgl. Abschnitt 3). Hinsichtlich der Operationalisierung der im adaptierten Modell enthaltenen Konstrukte (insbesondere „Informationsqualität" und „Systemqualität") besteht noch Forschungsbedarf. Es wird erwartet, dass die in Abschnitt 3.4 vorgeschlagenen Indikatoren für Informations- und Systemqualität einen hohen Erklärungsgehalt hinsichtlich dieser beiden Dimensionen aufweisen werden, da sie auf einem bewährten Messinstrument beruhen. Die zur Messung verwendeten Indikatoren sowie deren Items sollten aufgrund des neuen Einsatzfeldes trotzdem in einer Vorstudie getestet und ggf. ergänzt werden. Trotz der zu erwartenden Schwierigkeiten bei der Datenerhebung erscheint eine empirische Untersuchung äußerst lohnend, da dann erstmals sowohl theoretisch wie auch empirisch fundierte Kriterien zum Design von OLAP-Anwendungen abgeleitet werden sowie die Stärke der Auswirkungen von Disclosure Limitation auf Qualität und Erfolg von OLAP geschätzt werden können.

QUELLEN

ADAM/WORTHMANN (1989)
Adam, Nabil / Worthmann, John C.: Security-control methods for statistical databases: a comparative study; in: ACM Computing Surveys; Jg. 21 (1989); Nr. 4; S. 515–556

ADOMAVICIUS/TUZHILIN (2005)
Adomavicius, Gediminas / Tuzhilin, Alexander: Toward the next generation of recommender systems: a survey of the state-of-the-art and possible extensions; in: IEEE Transactions on Knowledge and Data Engineering; Jg. 17 (2005); Nr. 6; S. 734–749

AGRAWAL/SRIKANT (2001)
Agrawal, Rakesh / Srikant, Ramakrishnan: On integrating catalogues; in: Proceedings of the tenth international conference on World Wide Web - WWW '01; Hrsg.: Shen, Vincent Y. 2001; S. 603–612

ALBRECHT/HARREN/SAPIA (2009)
Albrecht, Jens / Harren, Arne / Sapia, Carsten: Logische Modellierung; in: Data-Warehouse-Systeme - Architektur, Entwicklung, Anwendung; Hrsg.: Bauer, Andreas / Günzel, Holger; 3. überarb. und aktual. Aufl.; Heidelberg 2009; S. 186–199

BARC (2010)
Barc: Business-Intelligence-Softwaremarkt Deutschland 2009; Research Note; Business Application Research Center - BARC GmbH (verantw. Inst.); 2010 *(letzte Akt.)*; URL: http://www.barc.de/fileadmin/images/main/PDFs/BARC_Marktzahlen_2009.pdf *(zuletzt gepr. am 12.06.2011)*

BAUER/GÜNZEL (2009a)
Bauer, Andreas; Günzel, Holger (Hrsg.): Data-Warehouse-Systeme - Architektur, Entwicklung, Anwendung; 3. überarb. und aktual. Aufl.; Heidelberg 2009

BAUER/GÜNZEL (2009b)
Bauer, Andreas / Günzel, Holger: Begriffliche Einordnung; in: Data-Warehouse-Systeme - Architektur, Entwicklung, Anwendung; Hrsg: Bauer, Andreas / Günzel, Holger; 3. überarb. und aktual. Aufl.; Heidelberg 2009; S. 6–10

BECK (1980)
Beck, Leland L.: A security mechanism for statistical database; in: ACM Transactions on Database Systems; Jg. 5 (1980); S. 316–338

BELL/LAPADULA (1973a)
Bell, Elliott / LaPadula, Leonard: Secure Computer Systems: A Mathematical Model; Technical Report (Nr. 2547 Vol. II); MITRE (Hrsg. und verantw. Inst.); 1973 *(letzte Akt.)*

BELL/LAPADULA (1973b)
Bell, Elliott / LaPadula, Leonard: Secure Computer Systems: Mathematical Foundations; Technical Report (Nr. 2547 Vol. I); MITRE (Hrsg. und verantw. Inst.); 1973 *(letzte Akt.)*

BERTINO/SANDHU (2005)
Bertino, Elisa / Sandhu, Ravi: Database security - concepts, approaches, and challenges; in: IEEE Transactions on Dependable and Secure Computing; Jg. 2 (2005); Nr. 1; S. 2–19

BERTINO/BONATTI/FERRARI (2001)
Bertino, Elisa / Bonatti, Piero / Ferrari, Elena: TRBAC: A temporal role-based access control model; in: ACM Transactions on Information and System Security; Jg. 4 (2001); Nr. 3; S. 191–233

BHATTI/GAO/LI (2008)
Bhatti, Rafae / Gao, Dengfang / Li, Wen-Syan: Enabling policy-based access control in BI applications; in: Data & Knowledge Engineering; Jg. 66 (2008); Nr. 2; S. 199–222

BODE/ZELEWSKI (1992)
Bode, Jürgen / Zelewski, Stefan: Die Produktion von Dienstleistungen - Ansätze zu einer Produktionswirtschaftslehre der Dienstleistungen?; in: BFuP (Betriebswirtschaftliche Forschung und Praxis); Jg. 44 (1992); Nr. 6; S. 594–607

BRADFORD (2008)
Bradford, Roger B.: An empirical study of required dimensionality for large-scale latent semantic indexing applications; in: Proceeding of the 17th ACM conference on Information and knowledge management; Napa Valley 2008; S. 153–162

BUSSE VON COLBE/LAßMANN (1990)
Busse von Colbe, Walther / Laßmann, Gert: Betriebswirtschaftstheorie; 3., durchges. Aufl.; Berlin, Heidelberg 1990

BYUN/BERTINO/LI (2005)
Byun, Ji-Won; Bertino, Elisa; Li, Ninghui (Hrsg.) (2005): Purpose based access control of complex data for privacy protection, in: Proceedings of the tenth ACM symposium on Access control models and technologies; Stockholm 2005; S. 102–110

CHAMONI/GLUCHOWSKI/HAHNE (2005)
Chamoni, Peter / Gluchowski, Peter / Hahne, Michael: Business Information Warehouse; Berlin, Heidelberg 2005

CHAMONI/ZESCHAU (1996)
Chamoni, Peter / Zeschau, Dietmar: Management-Support-Systems und Data-Warehousing; in: Das Data-Warehouse-Konzept; Hrsg.: Mucksch, Harry / Behme, Wolfgang; Wiesbaden 1996; S. 47–83

CHAMONI/GLUCHOWSKI (1997)
Chamoni, Peter / Gluchowski, Peter: On-Line Analytical Processing (OLAP); in: Das Data-Warehouse- Konzept: Architektur - Datenmodelle - Anwendungen; Hrsg.: Mucksch, Harry / Behme, Wolfgang; 2 Aufl.; Wiesbaden 1997

CHAMONI/GLUCHOWSKI (2006)
Chamoni, Peter / Gluchowski, Peter: Analytische Informationssysteme — Einordnung und Überblick; in: Analytische Informationssysteme; Hrsg.: Chamoni, Peter / Gluchowski, Peter; 3. Aufl.; Berlin, Heidelberg 2006; S. 3–22

CHEN/LYNCH (1992)
Chen, Hsinchun / Lynch, Kevin J.: Automatic construction of networks of concepts characterizing document databases; in: IEEE Transactions on Systems, Man and Cybernetics; Jg. 22 (1992); Nr. 5; S. 885–902

CHIN/OZSOYOGLU (1982)
Chin, Francis Y. L. / Ozsoyoglu, G.: Auditing and Inference Control in Statistical Databases; in: IEEE Transactions on Software Engineering; Jg. 8 (1982); Nr. 6; S. 574–582

CILIBRASI/VITANYI (2005)
Cilibrasi, Rudi L. / Vitanyi, Paul M.B: Clustering by Compression; in: IEEE Transactions on Information Theory; Jg. 51 (2005); Nr. 4; S. 1523–1545

CILIBRASI/VITANYI (2007)
Cilibrasi, Rudi L. / Vitanyi, Paul M. B.: The Google Similarity Distance; in: IEEE Transactions on Knowledge and Data Engineering; Jg. 19 (2007); S. 370–383

CODD/CODD/SALLEY (1993)
Codd, Edgar F. / Codd, Sally B. / Salley, Clinch T.: Providing OLAP to User-Analysts: An IT Mandate; Codd & Associates (verantw. Inst.); 1993 *(letzte Akt.)*

CORNELIUS (1991)
Cornelius, Martin: Die Implementierung einer offenen Entwicklungsumgebung für ein Executive-Informationssystem; in: Beilagen zur 2. DGOR-Fachtagung Planungssprachen und Führungsinformationssysteme; Hrsg.: Hummeltenberg, Wilhelm / Chamoni, Peter; Bad Homburg 1991

COX (1980)
Cox, Lawrence H.: Suppression Methodology and Statistical Disclosure Control; in: Journal of the American Statistical Association; Jg. 75 (1980); Nr. 370; S. 377–385

DALENIUS (1977)
Dalenius, Tore: Towards a methodology for statistical disclosure control; in: Statistik Tidskrift; Jg. 15, (1977); Nr. 429-444; S. 429–444

DALENIUS/REISS (1982)
Dalenius, Tore / Reiss, Steven P.: Data-swapping: A technique for disclosure control; in: Journal of Statistical Planning and Inference (1982); Nr. 6; S. 73–85

DAS/MANNILA (2000)
Das, Gautam / Mannila, Heikki: Context-Based Similarity Measures for Categorical Databases; in: Lecture Notes in Computer Science; Hrsg.: Zighed, Djamel A. / Komorowski, Jan / Żytkow, Jan; Berlin, Heidelberg 2000; S. 201–210

DELONE/MCLEAN (2003)
DeLone, William / McLean, Ephraim: The DeLone and McLean Model of Information Systems Success: A Ten-Year Update; in: Journal of Management Information Systems; Jg. 19 (2003); S. 9–30

DENNING (1976)
Denning, Dorothy: A lattice model of secure information flow; in: Communications of the ACM; Jg. 19 (1976); S. 236–243

DENNING/DENNING/SCHWARTZ (1979)
Denning, Dorothy / Denning, Peter J. / Schwartz, Mayer D.: The tracker: a threat to statistical database security; in: ACM Transactions on Database Systems; Jg. 4 (1979); Nr. 1; S. 76–96

DENNING/SCHLÖRER (1983)
Denning, Dorothy / Schlörer, Jan: Inference Controls for Statistical Databases; in: Computer; Jg. 16 (1983); S. 69–82

DETERMANN (2002)
Determann, Lorenz: Modellierung analytischer Informationssysteme: Ein Konzept zur multidimensionalen Datenstrukturierung; Wiesbaden 2002

DEVLIN/MURPHY (1988)
Devlin, Barry A. / Murphy, Paul T.: An architecture for a business and information system; in: IBM Systems Journal; Jg. 27 (1988); S. 60–80

DRESNER (2001)
Dresner, Howard: Gartner Group's HOWARD DRESNER, Interview by David Baum; in: Information Builders Magazine; Jg. 11 (2001); Nr. 2; S. 26–28

DRESNER (2002)
Dresner, Howard: Gartner's 2002 BI Market Study: How Do You Stack Up?; Research (Nr. AV-18-5277); Gartner Inc. (verantw. Inst.); 2002 *(letzte Akt.)*

DUNCAN/KELLER-MCNULTY/STOKES (2004)
Duncan, George T. / Keller-MCnulty, Sallie A. / Stokes, S. Lynne: Database Security and Confidentiality: Examining Disclosure Risk vs. Data Utility through the R-U Confidentiality Map; National Institute of Statistical Sciences (verantw. Inst.); 2004 *(letzte Akt.)*; URL: http://www.niss.org/announcements/NISSFactSheet200809-Final.pdf *(zuletzt gepr. am 27.11.2008)*

ECL@SS
eCl@ss e.V.: eCl@ss Release 7.0; URL: http://www.eclassdownload.com/catalog/product_info.php?cPath=61_62&products_id=88 *(zuletzt gepr. am 15.07.2011)*

ECL@SS (2006)
eCl@ss e.V.: Grundsatzleitlinie des eCl@ss e.V., Köln.; eCl@ss e.V. *(Hrsg.)* ; URL: http://www.eclass.de/user/documents/grundsatzleitlinie_2006_12_06.pdf *(zuletzt gepr. am 25.06.2011)*

EG (verantw. Inst.) (2002): VERORDNUNG (EG) Nr. 178/2002 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 28. Januar 2002 zur Festlegung der allgemeinen Grundsätze und Anforderungen des Lebensmittelrechts, zur Errichtung der Europäischen Behörde für Lebensmittelsicherheit und zur Festlegung von Verfahren zur Lebensmittelsicherheit. (EG) Nr. 178/2002, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002R0178:20060428:DE:PDF; in: Amtsblatt der Europäischen Gemeinschaft; 2002 *(letzte Akt.)*.

EICHHORN (1996)
Eichhorn, Peter: Entwurf für ein neues Faktorsystem; in: Umweltorientierte Marktwirtschaft; Hrsg.: Eichhorn, Peter; Wiesbaden 1996; S. 37–46

EUR-Lex
EUR-Lex. Amtsblatt der Europäischen Union; URL: http://eur-lex.europa.eu/JOIndex.do?ihmlang=de *(zuletzt gepr. am 15.07.2011)*.

FERRAIOLO/KUHN (1992)
Ferraiolo, David / Kuhn, Richard: Role-Based Access Control; in: Proceedings of the 15th NIST-NCSC National Computer Security Conference; Hrsg.: National Institute of Standards and Technology 1992; S. 554–563

FIENBERG/MCINTYRE (2004)
Fienberg, Stephen E. / McIntyre, Julie: Data Swapping: Variations on a Theme by Dalenius and Reiss; in: Lecture Notes in Computer Science; Hrsg.: Kanade, Takeo / Kittler, Josef / Kleinberg, Jon M. / Mattern, Friedemann / Mitchell, John C. / Naor, Moni / Nierstrasz, Oscar / Pandu Rangan, C. / Steffen, Bernhard / Sudan, Madhu / Terzopoulos, Demetri / Tygar, Doug / Vardi, Moshe Y. / Weikum, Gerhard / Domingo-Ferrer, Josep / Torra, Vicenç; Berlin, Heidelberg 2004; S. 14–29

FUGKEAW/PIYAWIT/SEKPON (2009)
Fugkeaw, Somchart / Piyawit, Manpanpanich / Sekpon, Juntapremjitt: A-COLD: Access Control of Web OLAP over Multi-data Warehouse; in: Proceedings of the The Forth International Conference on Availability, Reliability and Security; Hrsg.: IEEE Computer Society; Los Alamitos, California, USA 2009; S. 469–474

FUGKEAW/MANPANPANICH/JUNTAPREMJITT (2008)
Fugkeaw, Somchart / Manpanpanich, Piyawit / Juntapremjitt, Sekpon: Securing Web OLAP Based on RBAC Model; in: International Conference on Advanced Computer Theory and Engineering; Jg. 0 (2008); S. 778–782

GARTNER (2005)
Gartner: The Gartner Fellows: Howard Dresner's Biography; Gartner, Inc (verantw. Inst.); 2005 *(letzte Akt.)*; URL: http://www.gartner.com/research/fellows/asset_79427_1175.jsp *(zuletzt gepr. am 23.06.2011)*

GENTSCH (2008)
Gentsch, Peter: Business Intelligence for better decisions; 30.10.2008 *(letzte Akt.)*; URL: http://www.intelligence-group.com/downloads/BI-for-better-decisions.pdf *(zuletzt gepr. am 11.08.2009)*

GLUCHOWSKI (2001)
Gluchowski, Peter: Business Intelligence. Konzepte, Technologien und Einsatzbereiche; in: HMD - Praxis der Wirtschaftsinformatik; Jg. 38 (2001); Nr. 222; S. 5–15

GLUCHOWSKI (2011)
Gluchowski, Peter: Grundstrukturen multidimensionaler Datenmodelle; in: BI-Spektrum; Jg. 5 (2011); Nr. 1; S. 31–34

GLUCHOWSKI/CHAMONI (2010)
Gluchowski, Peter / Chamoni, Peter: Entwicklungslinien und Architekturkonzepte des On-Line Analytical Processing; in: Analytische Informationssysteme - Business Intelligence-Technologien und -Anwendungen; Hrsg.: Chamoni, Peter / Gluchowski, Peter; 4., vollst. überarb. Aufl.; Berlin, Heidelberg 2010; S. 144–176

GLUCHOWSKI/GABRIEL/CHAMONI (2008)
Gluchowski, Peter / Gabriel, Roland / Chamoni, Peter: Management Support Systeme und Business Intelligence: Computergestützte Informationssysteme für Fach- und Führungskräfte; 2 Aufl. 2008

GLUCHOWSKI/KEMPER (2006)
Gluchowski, Peter / Kemper, Hans-Georg: Quo Vadis Business Intelligence?; in: BI-Spektrum; Jg. 1 (2006); Nr. 1; S. 12–19

GORRY/SCOTT MORTON (1971)
Gorry, G. Anthony / Scott Morton, Michael S.: A Framework for Management Information Systems; in: Sloan Management Review; Jg. 13 (1971); Nr. 1; S. 55–70

GRGECIC/ROSENKRANZ (2010)
Grgecic, Daniel / Rosenkranz, Christoph: Rethinking the Concept of IT Use; in: DIGIT 2010 Proceedings; Hrsg.: Diffusion Interest Group In Information Technology; St. Louis 2010; Paper 9

GRIFFITHS/WADE (1976)
Griffiths, Patricia P. / Wade, Bradford W.: An authorization mechanism for a relational database system; in: ACM Transactions on Database Systems; Jg. 1 (1976); Nr. 3; S. 242–255

HARINARAYAN/RAJARAMAN/ULLMAN (1996)
Harinarayan, Venky / Rajaraman, Anand / Ullman, Jeffrey D.: Implementing Data Cubes Efficiently; in: Proceedings of the 1996 ACM SIGMOD International Conference on Management of Data; Hrsg.: Jagadish, H.V / Mumick, Inderpal Singh 1996; S. 205–216

HEIDENREICH (2003)
Heidenreich, Martin: Die Debatte um die Wissensgesellschaft; in: Wissenschaft in der Wissensgesellschaft; Hrsg.: Schulz-Schaeffer, Ingo / Böschen, Stefan; Opladen 2003; S. 25–54

HEPP/LEUKEL/SCHMITZ (2007)
Hepp, Martin / Leukel, Joerg / Schmitz, Volker: A quantitative analysis of product categorization standards: content, coverage, and maintenance of eCl@ss, UNSPSC, eOTD, and the RosettaNet Technical Dictionary; in: Knowledge and Information Systems; Jg. 13 (2007); Nr. 1; S. 77–114

HEWLETT-PACKARD (2009)
Hewlett-Packard: Top 10 trends in Business Intelligence for 2009; 2009 *(letzte Akt.)*; URL: http://h20195.www2.hp.com/V2/GetPDF.aspx/4AA1-8346ENA.pdf *(zuletzt gepr. am 15.06.2011)*

HILDEBRAND (1995)
Hildebrand, Knut: Gestaltung und Einführung des Informationsmanagements: Organisation, Architektur und Planung; Berlin 1995

HOFFMAN/MILLER (1970)
Hoffman, L. J. / Miller, W. F.: Getting a personal dossier from a statistical data bank; in: Datamation; Jg. 16 (1970); Nr. 5; S. 74–75

HONG ET AL. (2006)
Hong, Soongoo / Katerattanakul, Pairin / Hong, Suk-Ki / Cao, Qing: Usage And Perceived Impact Of Data Warehouses: A Study In Korean Financial Companies; in: International Journal of Information Technology & Decision Making; Jg. 5 (2006); Nr. 2; S. 297

HUMMELTENBERG (2008)
Hummeltenberg, Wilhelm: 50 Jahre Business Intelligence-Systeme; Ausgewählte Publikationen; Universität Hamburg (verantw. Inst.); 2008 *(letzte Akt.)*; URL: http://www.uni-hamburg.de/fachbereiche-einrichtungen/fb03/iwi-ii/Ausgewaehlte_Publikationen_/W.%20Hummeltenberg%20-%2050%20Jahre%20Business%20Intelligence-Systeme.pdf *(zuletzt gepr. am 23.06.2001)*

INMON (1990)
Inmon, William H.: Building the Data Warehouse; New York 1990

INMON (2005)
Inmon, William H.: Building the data warehouse; 4. Aufl.; Indianapolis 2005

JAJODIA/SANDHU (1991)
Jajodia, Sushil / Sandhu, Ravi S. (Hrsg.) (1991): Towards a Multilevel Secure Relational Data Model 1991

JAJODIA ET AL. (2001)
Jajodia, Sushil / Samarati, Pierangela / Sapino, Maria Luisa / Subrahmanian, V. S.: Flexible support for multiple access control policies; in: ACM Transactions on Database Systems; Jg. 26 (2001); S. 214–260

JIAO ET AL. (2007)
Jiao, Jianxin / Zhang, Lianfeng / Pokharel, Shaligram / He, Zhen: Identifying generic routings for product families based on text mining and tree matching; in: Decision Support Systems; Jg. 43 (2007); Nr. 3; S. 866–883

JIAO/SIDDIQUE/SIMPSON (2006)
Jiao, Roger Jianxin / Siddique, Zahed / Simpson, Timothy W.: Product Platform and Product Family Design; New York 2006

JOHN/KIENER (2010)
John, Peter / Kiener, Peter: Berechtigungen in SAP NetWeaver BW; Bonn, Boston 2010

JÜTTNER ET AL. (2010)
Jüttner, Andreas / Corell, Helen / Fleischer, Katrin / Mehrwald, Christian: Leitfaden SAP® BW 7; 1 Aufl.; Heidelberg 2010

KEMPER/UNGER/MEHANNA (2006)
Kemper, Hans-Georg / Unger, Carsten / Mehanna, Walid: Business Intelligence - Grundlagen und praktische Anwendungen; 2., erg. Aufl.; Wiesbaden 2006

KEMPER/BAARS (2006)
Kemper, Hans-Georg / Baars, Henning: Business Intelligence und Competitive Intelligence - IT-basierte Managementunterstützung und markt-/wettbewerbsorientierte Anwendungen; in: Praxis der Wirtschaftsinformatik; Jg. 247 (2006)

KIMBALL (1997)
Kimball, Ralph: Hackers, crackers, and spooks: ensuring that your data warehouse is secure; in: DBMS; Jg. 10 (1997); Nr. 4; S. 14–16

KLEINSCHMIDT/RANK (2002)
Kleinschmidt, Peter / Rank, Christian: Relationale Datenbanksysteme: Eine praktische Einführung; 2., überarb. u. erw. Aufl.; Berlin 2002

KOLODZIEJ (2011)
Kolodziej, Christian: Was taugt der In-Memory-Ansatz?; in: BI-Spektrum; Jg. 6 (2011); Nr. 2; S. 37–40

KRCMAR (1996)
Krcmar, Helmut: Informationsproduktion; in: Handwörterbuch der Produktionswirtschaft; Hrsg.: Kern, W. / Schröder, Hans-Horst / Weber, Jürgen; 2., völlig neu gestaltete Aufl.; Stuttgart 1996; S. 717–727

KUHN (1997)
Kuhn, Richard: Mutual exclusion of roles as a means of implementing separation of duty in role-based access control systems; in: Proceedings of the second ACM workshop on Role-based access control - RBAC '97; Hrsg.: Youman, Charles / Coyne, Edward / Jaeger, Trent 1997; S. 23–30

LEHNER (2008)

Lehner, Franz: Wissensmanagement: Grundlagen, Methoden und technische Unterstützung; 2 Aufl.; München, Wien 2008

LINDSEY ET AL. (2007)

Lindsey, Robert / Veksler, Vladislav D. / Grintsvayg, Alex / Gray, Wayne D.: Be wary of what your computer reads: The effects of corpus selection on measuring semantic relatedness; in: 8th International Conference of Cognitive Modeling ICCM 2007; Hrsg.: Lewis, Richard / Polk, Thad / Laird, John; Ann Arbor 2007; S. 1–6

LIU (2007)
Liu, Bing: Web Data Mining; New York 2007

LUHN (1958)
Luhn, Hans P.: A Business Intelligence System; in: IBM Journal of Research and Development; Jg. 2 (1958); Nr. 4; S. 314–319

LUNT ET AL. (1990)
Lunt, Teresa F. / Denning, Dorothy E. / Schell, Roger R. / Heckman, Mark / Shockley, William R.: The SeaView Security Model; in: IEEE Transactions on Software Engineering (1990); S. 593–607

MALVESTUTO/MEZZINI/MOSCARINI (2006)
Malvestuto, Francesco / Mezzini, Mauro / Moscarini, Marina: Auditing sum-queries to make a statistical database secure; in: ACM Transactions on Information and System Security; Jg. 9 (2006); Nr. 1; S. 31–60

MEHRWALD (2007)
Mehrwald, Christian: Datawarehousing mit SAP BW 7 - BI in SAP NetWeaver 2004s - Architektur, Konzeption, Implementierung; 4., vollst. überarb. und erw. Aufl.; Heidelberg 2007

MERTENS (2002)
Mertens, Peter: Business Intelligence - ein Überblick; Arbeitspapier (Nr. 2/2002); Universität Erlangen-Nürnberg (verantw. Inst.); 2002 *(letzte Akt.)*

MINTZBERG (1972)
Mintzberg, Henry: The Myths of MIS; in: California Management Review; Jg. XV (1972); Nr. 1; S. 92–97

MUKSCH/BEHME (1996)

Mucksch, Harry / Behme, Wolfgang (Hrsg.): Das Data-Warehouse-Konzept; Wiesbaden 1996

NELSON/TODD/WIXOM (2005)

Nelson, R. Ryan / Todd, Peter A. / Wixom, Barbara H.: Antecedents of Information and System Quality: An Empirical Examination Within the Context of Data Warehousing; in: Journal of Management Information Systems; Jg. 21 (2005); S. 199 - 235

O'CONNOR/LOOMIS (2010)

O'Connor, Alan C. / Loomis, Ross J.: 2010 Economic Analysis of Role-Based Access Control - Final Report; RTI Project (Nr. 0211876); National Institute of Standards and Technology (verantw. Inst.); 2010 *(letzte Akt.)*; URL: http://csrc.nist.gov/groups/SNS/rbac/documents/20101219_RBAC2_Final_Report.pdf *(zuletzt gepr. am 10.0.6.2011)*

OEHLER (2010)

Oehler, Karsten: Unterstützung von Planung, Forecasting und Budgetierung durch IT-Systeme; in: Analytische Informationssysteme - Business Intelligence-Technologien und -Anwendungen; Hrsg.: Chamoni, Peter / Gluchowski, Peter; 4., vollst. überarb.; Berlin, Heidelberg 2010

OH/PARK (2001)

Oh, Sejong / Park, Seog: An Improved Administration Method on Role-Based Access Control in the Enterprise Environment; in: Journal of Information Science and Engineering; Jg. 17 (2001); Nr. 6; S. 921–944

OPPELT (1995)

Oppelt, Ulrich G.: Computerunterstützung für das Management; München, Wien 1995

OSBORN/SANDHU/MUNAWER (2000)

Osborn, Sylvia / Sandhu, Ravi / Munawer, Qamar: Configuring role-based access control to enforce mandatory and discretionary access control policies; in: ACM Transactions on Information and System Security; Jg. 3 (2000); Nr. 2; S. 85–106

OZSOYOGLU/CHUNG (1986)

Ozsoyoglu, G. / Chung, J.: Information Information loss in the lattice model of summary tables due to cell suppression; in: Proceedings of the IEEE Symposium on Security and Privacy; Oakland, CA, USA 1986; S. 75–83

PENDSE/CREETH (1995)

Pendse, Nigel / Creeth, Richard: What is OLAP?; 13.02.2008 *(letzte Akt.)*; URL: http://www.olapreport.com/fasmi.htm, inzwischen unter http://www.bi-verdict.com/fileadmin/dl_temp/a74140bc700a0e9f88f3cc3eb88dc3ea/fasmi.htm *(zuletzt gepr. am 21.02.2011)*

PFEIFER ET AL. (2007)
Pfeifer, Tilo / Schmitt, Robert / Betzold, Mark / Krippner, Daniel: Wissensmanagement; in: Masing Handbuch Qualitätsmanagement; Hrsg.: Schmitt, Robert / Pfeifer, Tilo; 5 Aufl.; München, Wien 2007; S. 285–308

PICOT (1989)
Picot, Arnold: Der Produktionsfaktor Information in der Unternehmensführung; in: Thexis; Jg. 6 (1989); Nr. 4; S. 3–9

POWER (2008)
Power, Daniel J.: Handbook of Decision Support Systems: A Historical Overview; Berlin, Heidelberg 2008; S. 121–140

PRIEBE (2009)
Priebe, Torsten: Sicherheit; in: Data-Warehouse-Systeme - Architektur, Entwicklung, Anwendung; Hrsg.: Bauer, Andreas / Günzel, Holger; 3. überarb. und aktual. Aufl.; Heidelberg 2009; S. 159–167

PRIEBE/PERNUL (2000)
Priebe, Torsten / Pernul, Günther: Towards OLAP security design –- survey and research issues; in: DOLAP '00: Proceedings of the 3rd ACM international workshop on Data warehousing and OLAP; Hrsg.: ACM 2000; S. 33–40

PRUSAK (2001)
Prusak, Larry: Where Did Knowledge Management Come From?; in: IBM Systems Journal; Jg. 40 (2001); Nr. 4; S. 1002–1007

RJAIBI/BIRD (2004)
Rjaibi, Walid / Bird, Paul: A Multi-Purpose Implementation of Mandatory Access Control in Relational Database Management Systems; in: (e)Proceedings of the Thirtieth International Conference on Very Large Data Bases, Toronto, Canada, August 31 - September 3 2004; Hrsg.: Nascimento, Mario A. / Özsu, M. Tamer / Kossmann, Donald / Miller, Renée J. / Blakeley, José A. / Schiefer, K. Bernhard 2004; S. 1010–1020

ROBERTSON/ETHIER (2006)
Robertson, Dale A. / Ethier, Richard: Cell Suppression: Experience and Theory; in: Lecture Notes in Computer Science; Hrsg.: Domingo-Ferrer, Josep; Berlin, Heidelberg 2006; S. 8–20

ROCKART (1979)
Rockart, John F.: Chief executives define their own data needs; in: Harvard Business Review; Jg. 57 (1979); Nr. 2; S. 81–93

ROEHLING (2011)
Roehling, Carsten: CE-Richtlinien; Ingenieurgesellschaft für Technik-Kommunikation GmbH (verantw. Inst.); 13.07.2011 *(letzte Akt.)*; URL: http://www.ce-richtlinien.eu/richtlinien/All_PS.html *(zuletzt gepr. am 15.07.2011)*

ROUSSINOV/ZHAO (2003)
Roussinov, Dmitri / Zhao, J. Leon: Automatic discovery of similarity relationships through Web mining; in: Decision Support Systems; Jg. 35 (2003); S. 149–166

RUSSEL (1967)
Russel, L. Ackoff: Management Misinformation Systems; in: Management Science; Jg. 14 (1967); Nr. 4; S. B147-B156

SANDHU (1993)
Sandhu, Ravi: Lattice-based access control models; in: Computer; Jg. 26 (1993); Nr. 11; S. 9–19

SANDHU ET AL. (1996)
Sandhu, Ravi / Coyne, Edward / Feinstein, H.L / Youman, Charles: Role-based access control models; in: Computer; Jg. 29 (1996); Nr. 2; S. 38–47

SANDHU/BHAMIDIPATI/MUNAWER (1999)
Sandhu, Ravi / Bhamidipati, Venkata / Munawer, Qamar: The ARBAC97 model for role-based administration of roles; in: ACM Transactions on Information and System Security; Jg. 2 (1999); Nr. 1; S. 105–135

SAP (2010)
SAP: SAP-Bibliothek - Business Intelligence; 16.12.2010 *(letzte Akt.)*; URL: http://help.sap.com/saphelp_nw70/helpdata/DE/43/87277bb4303b5be10000000a422035/frameset.htm *(zuletzt gepr. am 27.06.2011)*

SAP (2011)
SAP: SAP Deutschland - Komponenten & Werkzeuge von SAP NetWeaver: SAP NetWeaver Business Intelligence; SAP AG (verantw. Inst.); 26.06.2011 *(letzte Akt.)*; URL: http://www.sap.com/germany/plattform/netweaver/components/businessintelligence/index.epx *(zuletzt gepr. am 26.06.2011)*

SCHINZER/BANGE/MERTENS (1999)
Schinzer, Heiko D. / Bange, Carsten / Mertens, Holger: Data warehouse und data mining - Marktführende Produkte im Vergleich; 2., völlig überarb. und erw. Aufl.; München 1999

SCHUSTER/JUCHHEIM/SCHILL (2010)
Schuster, Daniel / Juchheim, Till M. / Schill, Alexander: Finding and Classifying Product Relationships using Information from the Public Web; in: ICEIS 2010 - Proceedings of the 12th International Conference on Enterprise Information Systems; Hrsg.: ICEIS; Funchal, Madeira 2010; S. 300–309

SCOTT MORTON (1983)
Scott Morton, Michael S.: State of the Art of Research in Management; Working Paper CISR (Nr. 107); Massachusetts Institute of Technology, Center for Information Systems Research (verantw. Inst.); 1983 *(letzte Akt.)*

SEDERA/GABLE (2004)
Sedera, Darshana / Gable, Guy: A Factor and Structural Equation Analysis of the Enterprise Systems Success Measurement Model; in: Proceedings of the TwentyFifth International Conference on Information Systems; Hrsg.: DeGross, J.I; New York 2004; S. 449–464

SHIN (2003)
Shin, Bongsik: An Exploratory Investigation of System Success Factors in Data Warehousing; in: Journal of the Association for Information Systems; Jg. 4 (2003); Nr. 6; S. 141–170

SHOSHANI (1997)
Shoshani, Arie: OLAP and statistical databases: similarities and differences; in: Proceedings of the sixteenth ACM SIGACT-SIGMOD-SIGART symposium on Principles of database systems; Hrsg.: ACM 1997; S. 185–196

SINGU/VARADARAJAN (2009)
Singu, Chandiraban / Varadarajan, Arun: Overview of SAP History and BW-BI Evolution; SAP AG (verantw. Inst.); SAP Community Network Wiki - SAP NetWeaver Business Warehouse; 26.11.2009 *(letzte Akt.)*; URL: http://wiki.sdn.sap.com/wiki/display/BI/Overview+of+SAP+History+and+BW-BI+Evolution *(zuletzt gepr. am 27.06.2011)*

SMITH/WINSLETT (1992)
Smith, Kenneth / Winslett, Marianne (Hrsg.): Entity Modeling in the MLS Relational Model; San Francisco 1992

SOLER ET AL. (2008)
Soler, Emilio / Veronika Stefanov / Mazon, Jose-Norberto / Juan Trujillo / Fernandez-Medina, Eduardo / Piattini, Mario: Towards Comprehensive Requirement Analysis for Data Warehouses: Considering Security Requirements; in: Third International Conference on Availability, Reliability and Security 2008; S. 104–111

STAHLKNECHT (1995)
Stahlknecht, Peter: Einführung in die Wirtschaftsinformatik; 7. Aufl.; Berlin, Heidelberg 1995

STÜDEMANN (1993)
Stüdemann, Klaus: Allgemeine Betriebswirtschaftslehre; 3. Aufl.; München, Wien 1993

SULLIVANT (2005)
Sullivant, Seth: Small Contingency Tables with Large Gaps; in: SIAM Journal on Discrete Mathematics; Jg. 18 (2005); S. 787–793

SWIONTEK (1997)
Swiontek, Jürgen: Realität und Versprechen von Führungsunterstützungssystemen. Dissertation; Frankfurt a. M. 1997

THOMAS (1997)
Thomas, Roshan K.: Team-based access control (TMAC): a primitive for applying role-based access controls in collaborative environments; in: RBAC '97 Proceedings of the second ACM workshop on Role-based access control; New York 1997; S. 13-19

THOMSEN (2002)
Thomsen, Erik: OLAP solutions - Building multidimensional information systems; 2. Aufl.; New York et al. 2002

TOTOK (2000)
Totok, Andreas: Modellierung von OLAP- und Data-Warehouse-Systemen. Dissertation; Technische Universität Braunschweig (verantw. Inst.); Braunschweig 2000

TURBAN/WATSON (1989)
Turban, Efraim / Watson, Hugh J.: Integrating Expert Systems, Executive Information Systems and Decision Support Systems; in: Transactions of the 9th International Conference on Decision Support Systems (DSS-89); Hrsg.: Widmeyer, George R. 1989; S. 74–82

TURBAN/WALLS (1995)
Turban, Efraim / Walls, Joseph G.: Executive information systems – a special issue; in: Decision Support Systems; Jg. 14 (1995); Nr. 2; S. 85–88

TURNEY (2001)
Turney, Peter D.: Mining the Web for Synonyms: PMI-IR versus LSA on TOEFL; in: Proceedings of the Twelfth European Conference on Machine Learning (ECML-2001); Hrsg.: Raedt, Luc de / Flach, Peter A. / Turney, Peter D. 2001; S. 491–502

WANG/JAJODIA/WIJESEKERA (2007)
Wang, Lingyu / Jajodia, Sushil / Wijesekera, Duminda: Preserving Privacy in On-Line Analytical Processing; New York 2007

WANG/JAJODIA/WIJESEKERA (2004)
Wang, Lingyu / Jajodia, Sushil / Wijesekera, Duminda: Securing OLAP data cubes against privacy breaches; in: Proceedings of the 2004 IEEE Symposium on Security and Privacy; Hrsg.: IEEE Computer Society 2004; S. 161–175

WATSON/GOODHUE/WIXOM (2002)
Watson, Hugh J. / Goodhue, Dale L. / Wixom, Barbara H.: The benefits of data warehousing: why some organizations realize exceptional payoffs; in: Information & Management; Jg. 39 (2002); Nr. 6; S. 491–502

WIDOM/CERI (1996)
Widom, John / Ceri, Stephano (Hrsg.): Active Database Systems - Triggers and Rules for Advanced Database Processing; Berlin 1996

WILLENBORG/DE WAAL (1996)
Willenborg, Leon / Waal, Ton de: Statistic Disclosure Control in Practice; New York 1996

WILLENBORG/DE WAAL (2001)
Willenborg, Leon / Waal, Ton de: Elements of Statistical Disclosure Control; New York 2001

WIXOM/WATSON (2001)
Wixom, Barbara H. / Watson, Hugh J.: An Empirical Investigation of the Factors Affecting Data Warehousing Success; in: MIS Quarterly; Jg. 25 (2001); Nr. 1; S. 17–41

WIXOM/TODD (2005)
Wixom, Barbara H. / Todd, Peter A.: A Theoretical Integration of User Satisfaction and Technology Acceptance; in: Information Systems Research; Jg. 16 (2005); Nr. 1; S. 85–102

XU/HWANG (2008)
Xu, Hongjiang / Hwang, Mark I.: A Structural Model of Data Warehousing Success; in: Journal of Computer Information Systems; Jg. 44 (2008); Nr. 1; S. 48–56

YU ET AL. (2006)
Yu, Philip S. / Tsotras, Vassilis; Fox, Edward, et al. (Hrsg.): Proceedings of the 15th ACM international conference on Information and knowledge management - CIKM '06; New York 2006

ZHAO/KUMAR/ STOHR (2000)
Zhao, J. Leon / Kumar, Akhil / Stohr, Edward A.: A Dynamic Grouping Technique for Distributing Codified-Knowledge in Large Organizations; in: Proceedings of the 10th Workshop on Information Technology and Systems 2000; S. 1–6