Bundesamt für Sicherheit in der Informationstechnik

**Kommunikations- und Informationstechnik 2010 + 3**
neue Trends und Entwicklungen in
Technologie, Anwendungen und Sicherheit

Die vorliegende Studie wurde im Auftrag und in Zusammenarbeit mit dem Bundesamtes für Sicherheit in der Informationstechnik (BSI) in einer interdisziplinären Kooperation der Technischen Universität München und der Ludwig-Maximilians-Universität München sowie der Sirrix AG security technologies, Homburg/Saar, erstellt.

Die dieser Studie zugrunde liegende Expertenbefragung wurde im Herbst 2002 durchgeführt. Der vorliegende Bericht spiegelt ausschließlich die Meinungen der befragten Experten und Erkenntnisse aus der Literatur wider. Marken, Produktnamen, sowie Produktabbildungen und Logos werden nur zur Identifikation der Produkte verwendet und können eingetragene Marken der entsprechenden Hersteller sein. Verwendete Marken- und Produktnamen sind Handelsmarken, Warenzeichen oder eingetragene Warenzeichen der entsprechenden Inhaber.

Bundesamt für Sicherheit in der Informationstechnik

# Kommunikations- und Informationstechnik

# 2010 + 3

## neue Trends und Entwicklungen in Technologie, Anwendungen und Sicherheit

SecuMedia Verlag

Bibliografische Information der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.ddb.de abrufbar.

**ISBN 3–922746–48–9**

© 2003 Bundesamt für Sicherheit in der Informationstechnik–BSI,
Godesberger Allee 185–189, D–53175 Bonn
und SecuMedia Verlags–GmbH, Postfach 1234, D–55205 Ingelheim,
Tel. 06725/93040, Fax. 06725/5994, E-Mail info@secumedia.de

Alle Rechte vorbehalten. Nachdruck, auch auszugsweise, fotomechanische Wiedergabe, Speicherung oder Übermittlung durch elektronische Medien sowie Übersetzung nur mit schriftlicher Genehmigung des Bundesamtes für Sicherheit in der Informationstechnik–BSI, Godesberger Allee 183, D–53175 Bonn.

Grafik: Anneli Nau, Werner Halla, Klaudija Ćosić

Umschlaggestaltung: Conrad Schmitt, BSI

Layout: LaTeX & Markus Garschhammer, LMU

Herstellung: Schmidt & more Drucktechnik, Haagweg 44, 65462 Ginsheim-Gustavsburg

Printed in Germany

## Autoren und Experten

### Autoren

In die Erstellung dieser Studie waren eingebunden:

- ein Kooperationsteam der Lehrstühle

  Prof. Dr. Manfred Broy, Lehrstuhl für Programmiermethodik und verteilte Entwicklung, Technische Universität München,

  Prof. Dr. Heinz-Gerd Hegering, Lehrstuhl für Kommunikationssysteme und Systemprogrammierung, Ludwig-Maximilians-Universität München,

  Prof. Dr. Dres. h.c. Arnold Picot, Lehrstuhl für Betriebswirtschaftliche Informations- und Kommunikationsforschung, Ludwig-Maximilians-Universität München.
- Sirrix AG security technologies, Homburg/Saar.
- Bundesamt für Sicherheit in der Informationstechnik

Das interdisziplinäre Autorenteam bildeten

- Ammar Alkassar
- Markus Garschhammer
- Frank Gehring
- Patrick Keil
- Harald Kelter
- Ulrich M. Löwer
- Marcus Pankow
- Ahmad-Reza Sadeghi
- Michael Schiffers
- Markus Ullmann
- Sascha Vogel.

### Experten

Die Ergebnisse der vorliegenden Studie sind der kompetenten und ausführlichen Beantwortung zahlloser Fragen zu verdanken. Unser Dank gilt daher den 162 Damen und Herren, die an der empirischen Erhebung auf der Basis strukturierter Fragebögen teilgenommen haben:

Prof. Dr. Sebastian Abeck
Rüdiger Azone
Herbert Bartenschlager
Dr. Andreas Barth
Dr. Matthias Barth
Dr. Brigitte Bartsch-Spörl
Fritz Bauspieß
Hartmut van Bel
Nadine Berezak-Lazarus
Prof. Dr. Jörg Biethahn
Bernd-Christoph Bijok
Hubert Biskup
Hans Brandl
Dr. Matthias Bueger
Prof. Dr. Hans Ulrich Buhl
Rolf-Dieter Clavery

Prof. Dr. Stefan Conrad
Roland Cuny
Dr. Peter Daniel
Rainhard Degener
Ingo Demgensky
Mathias Duckeck
Helmut Duschinger
Prof. Dr. Jörg Eberspächer
Dr. Ralf Ebner
Klaus Eckert
Prof. Dr. Claudia Eckert
Gerd Eickelpasch
Dr. Rolf Engelbrecht
Dr. Hermann Englberger
Anton Enterrottacher
Prof. Erwin Fahr
Dr. Wolfgang Faisst
Ulrich Faisst
Frank Farnschläder
Dr. Hannes Federrath
Peter Fellinger
Prof. Dr. Herbert Fischer
Dr. Werner Flacke
Dr. Albert Fleischmann
Dirk Fox
Aiko Frank
Prof. Dr. Gerhard Frey
Peter Friedl
Alexander Frommelt
Dr. Arnd Gerns
Gerhard Geßler
Wolfgang Glock
Dr. Richard Göbel
Dr. Jan Göpfert
Dr. Klaus Georg Götzer
Felix Grabmeyer
Prof. Rüdiger Grimm
Prof. Eberhard Grötsch
Dr. Michael Gutzmann
Prof. Dr. Rudolf Haggenmüller
Peter Hammer
Marit Hansen
Prof. Dr. Johannes Heigert
Dr. Stephen Heilbronner
Prof. Dr. Thomas Hess
Dr. Karl F. Hettling
Dr. Axel Hoff
Stefan Holtel
Stefan Hotop
Dr. Frank Houdek
Dr. Reinhard Hund
Prof. Dr. Stefan Jablonski
Dr. Peter Jüttner
Prof. Dr. Firoz Kaderali
Dr. Jürgen Kazmeier
Wolfgang Killmann
Prof. Dr. Axel Lehmann
Dr. Thorsten Liebig
Dr. Harald Ließmann
Volkmar Lotz
Dr. Thomas Luckenbach
Hero Lüers
Ulrich Mahn
Prof. Dr. Matthias Maier
Prof. Dr. Christian Märtin
Prof. Dr. Dr. h.c. mult. Peter Mertens
Prof. Dr. Klaus Meyer-Wegener
Albert Mokler
Wolf-Rüdiger Moritz
Dr. Petra Morschheuser
Dr. Kathrin Möslein
Dr. Andreas Müller
Michael Müller-Haerendel
Günther Müller-Luschnat
Dr. Michael Nerb
Dr. Rahild Neuburger
Dr. Bernhard Neumair
Rudolf Neurath
Dr. Marcus Niggl
Thomas Ötinger
Thomas Ott
Prof. Dr. Helmut Partsch
Dirk Petershagen
Prof. Dr. Andreas Pfitzmann
Dr. Joachim Posegga
Dr. Günter G. Prockl
Dr. Stefan Pütz
Prof. Dr. Kai Rannenberg
Prof. Dr. Dr. h.c. Ralf Reichwald
Alfred Reß
Dr. Michael Rohloff
Dr. Thomas Ruf
Prof. Dr. Christoph Ruland
Dr. Bernhard Rumpe
Harald Rützel
Dr. Ralf Schäfer
Christian Scheer
Dr. Axel Schell
Helmut Scherzer
Stefan Schmale

Dr. Werner Schmidt
Prof. Dr. Gunther Schmidt
Dr. Gisela Schöpke
Prof. Dr. Matthias Schumann
Dr. Thomas Seidl
Hartmut Seifert
Dr. Robert Skerjanc
Prof. Dr. Bernd Skiera
Harry Sneed
Prof. Dr. Friedrich Sösemann
Klaus Steiner
Dr. Helmuth Steinheuer
Prof. Dr. Ralf Steinmetz
Prof. Dr. Peter Stöhr
Guido P. Supe
Dr. Michael Thiel
Dr. Ulf Timm
Thomas Tschersich
Roland Vogt
Prof. Dr. Reinhard Vossbein
Dr. Dirk Wacker
Dr. Klemens Waldhör
Prof. Dr. Rolf Weiber
Peter Weierich
Dr. Franz Weikmann
Florian Weiß
Dr. Günter Welsch
Dr. Réné Wies
Dr. Andreas Winzen
Gerhard Wolfstieg
Dr. Felix Wunderer
Dr. Thomas Zeggel
Uwe Zeithammer

13 weitere Teilnehmer wünschten eine anonyme Berücksichtigung ihrer Ergebnisse.

Viele Experten haben mehrere Fragebögen unterschiedlicher Themenkomplexe bearbeitet, daher basiert die Studie auf insgesamt 185 Fragebögen.

# Inhaltsverzeichnis

# Abbildungsverzeichnis

# 1 Vorwort

Liebe Leserinnen, Liebe Leser,

Vor Ihnen liegt der neue BSI-Trendreport, mit dem wir Sie - wie auch vor drei Jahren - über aktuelle Trends und Entwicklungen auf den Gebieten der Informations- und Kommunikationstechnik (IuK-Technik), sowie deren Sicherheitsaspekte informieren wollen.

Die Beobachtung der Technologieentwicklung auf diesen Gebieten sowie die Vorausschau auf die kurz-, mittel- und langfristige Zukunft ist für das BSI keine einmalige, sondern eine kontinuierliche Aufgabe. Nur mit diesem Wissen ist es dem BSI möglich, seine vielschichtigen Aufgaben - unter anderem die Untersuchung von Sicherheitsrisiken bei der Anwendung der Informations- und Kommunikationstechnik - zu erfüllen. Somit wird das BSI in die Lage versetzt, neue Technologien unter dem Gesichtspunkt neuer Bedrohungspotenziale zu analysieren und daraus Gegenmaßnahmen einzuleiten.

Der rasante Fortschritt – in den Materialwissenschaften, der Mikrosystemtechnik, der Computertechnik sowie das Zusammenwachsen von Kommunikations- und Informationstechnologie und der heutige Trend hin zum Pervasive- und Ubiquitous Computing – zeigt, dass trotz der derzeitigen Konjunkturkrise die Dynamik der Informations- und Kommunikationstechnologie dafür sorgen wird, dass auch in Zukunft diese Technologien eine führende Rolle bei der industriellen Globalisierung und Liberalisierung der Märkte spielen werden.

Das Jahr 2002, in dem die Experteninterviews für diese Studie stattfanden, war das schwierigste in der jüngsten Geschichte der Informations- und Kommunikationstechnik. Weltweit konnte die Branche nur noch um 1,2% zulegen. „In Deutschland lagen wir 2002 im Minus und für 2003 rechnen wir mit einer schwarzen Null - nicht mehr und nicht weniger", nach Menno Harms, Vizepräsident des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) zur CeBIT 2003 in Hannover.

Nach den überspannten Prognosen für die IuK-Technik in der Vergangenheit herrscht heute überwiegend Zurückhaltung. Diese orientieren sich jetzt am technisch Machbaren sowie nach den Verbraucherwünschen.

Da sich die erste Studie „Kommunikations- und Informationstechnik 2010: Trends in Technologie und Markt" innerhalb des Trendforums im BSI in der Umsetzung der Ergebnisse und dem strategischen Nutzen für staatliche Entscheidungsträger sowie für die Wirtschaft als sehr hilfreich erwiesen hat, wurde mit der jetzt aktualisierten Studie diese Reihe fortgesetzt und um den Bereich der IT-Sicherheit erweitert. Das alte Paradigma, wonach man IT-Sicherheit als funktional getrenntes Add-On aufgefaßt hat, ist nicht mehr haltbar.

Mit dem Eintritt in die vernetzte mobile Wirtschaft avanciert das Thema der IT-Sicherheit zur Grundvoraussetzung unternehmerischen Handelns und rückt heute immer stärker in den Fokus der Öffentlichkeit. Für Wirtschaftsunternehmen, aber auch für die Politik existiert hinsichtlich der künftigen Entwicklung in der IuK-Technik ein hoher Bedarf an Orientierungswissen, um zu einer optimalen Allokation beitragen zu können und somit strategisch bedeutsame Märkte zu erschließen.

Mit dieser Studie wird ein fundierter Blick in die Zukunft der IuK-Technik gewagt. Es ist möglich, bestimmte Entwicklungen einzuschätzen, diese zu diskutieren und anschließend Maßnahmen festzulegen, um bestehende Defizite zu beseitigen und so den verschärften Wettbewerb auf dem Weltmarkt begegnen zu können. Diese Studie liefert also nicht nur ein Bild von der Zukunft der IuK-Technik, sondern stellt eine Informationsgrundlage für notwendige Entscheidungen in der Gesellschaft, der Wirtschaft und in den Verwaltungen dar. Zusätzlich bietet diese Studie einen inter-

essanten Vergleich zu bereits getroffenen Prognosen aus der Vorgängerstudie.

Technisch versierte Leser finden hier detaillierte Beschreibungen und Prognosen über einzelne Technologien, dem interessierten Laien bietet die Studie viele Informationen über zukünftige Geschäftsmodelle, Anwendungen, Arbeitsformen und Auswirkungen der Technologien auf das tägliche Leben.

Bonn, im Mai 2003

Dr. Udo Helmbrecht

Präsident des Bundesamtes für Sicherheit in der Informationstechnik

## 2 Geleitwort

Der Bereich der Information und Kommunikation ist gekennzeichnet durch eine hohe Dynamik der Technologien und deren Märkte. Veränderungen sind zwar oft technologiegetrieben, resultieren aber – nicht zuletzt als Ergebnis technologischer Fortschritte – aus kontinuierlich neuen Anforderungen und Bedürfnissen der Märkte. So bestimmen heute beispielsweise drahtlose Netze und mobile Dienste die Diskussion in vielen Bereichen, während sich die Euphorie im Internet-Bereich gelegt hat. Was noch vor einigen Jahren als Zukunftstechnologie galt, wurde schon bald von anderen Konzepten überholt, denen vorher kaum jemand Beachtung schenkte. Diese Dynamik in Verbindung mit dem herrschenden Kostenbewusstsein bei Unternehmen wie bei öffentlichen Haushalten zwingt die Verantwortlichen, die zukünftigen Trends und Entwicklungen früh zu erkennen und ihre Strategien an diese Entwicklungen anzupassen. Gerade die öffentliche Verwaltung darf sich diesen Entwicklungen nicht entziehen, will sie ihre Aufgaben der Administration, Regulierung und Kontrolle weiterhin effizient erfüllen.

Für die Akzeptanz von Diensten und Technologien steigt die Bedeutung von Sicherheitseigenschaften, die in den letzten Jahren immer weiter in das Interesse der Marktteilnehmer gerückt sind. Gerade zu diesem Thema sind öffentliche Stellen und Unternehmen auf die Kenntnis aktuellster Entwicklungen angewiesen.

All diese Herausforderungen verlangen nach einer Untersuchung, die möglichst viele Facetten der IuK-Technik beleuchtet und diese in Verbindung mit ihren möglichen Anwendungen und Auswirkungen auf das private und berufliche Leben bringt. Die vorliegende Studie bietet diese umfassende Sichtweise, indem Experten aus verschiedenen Bereichen zur Zukunft der Informations- und Kommunikationstechnik und zu den resultierenden persönlichen, beruflichen und gesellschaftlichen Veränderungen befragt wurden.

Im Jahr 2000 wurde im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik (BSI) eine ähnliche Studie veröffentlicht. In allen Kapiteln gibt es thematische Verschiebungen zwischen den beiden Studien. Diese Veränderungen sind deshalb aufschlussreich, weil sie eine Rückschau auf die letzten Jahre und die seitdem zu beobachtenden Entwicklungen erlauben. Aus gesamtwirtschaftlicher Perspektive fällt diese Rückschau auf den ersten Blick nicht besonders positiv aus: die Ereignisse des 11. September 2001, ihre Folgen und die Bedenken vor einem Krieg im Nahen und Mittleren Osten haben zu einer tiefen Verunsicherung bei Unternehmen und Verbrauchern geführt. Gerade internationale Firmen, die die Trends im Hardware-, Telekommunikations- und Softwaremarkt mitbestimmen, reagieren mit Zurückhaltung bei ihren Investitionen. Darüber hinaus verhindert die gebremste Konjunktur, v.a. in den USA als dem größten Technologiemarkt, weiterhin ein Ansteigen der Ausgaben für Forschung und Entwicklung. Beim Vergleich der Ergebnisse der beiden Studien finden sich diese Entwicklungen wieder: in vielen Bereichen haben sich die Erwartungen hinsichtlich der Dauer bis zur Realisierung bestimmter Technologien und Anwendungen um mehrere Jahre nach hinten verschoben. Aus den Aussagen der befragten Experten wird aber auch deutlich, dass eine Vielzahl zukunftsträchtiger Entwicklungen diesen negativen Einflüssen entgegenwirkt. Gerade die in dieser Studie betrachteten Spitzentechnologien werden Innovationszyklen weiter verringern, neue Produkte ermöglichen und für Fortschritt in allen Wirtschaftsbereichen sorgen. Allerdings wird die Konkurrenz zwischen einzelnen Technologien, Konzepten und Produkten weiterhin hart bleiben. Hier bietet die Studie in zahlreichen Fällen schon jetzt Einschätzungen, welche Ergebnisse dieser Wettbewerb bringen wird.

Dabei wird nicht nur Wert auf die Beschreibung spezifischer Technologien ge-

legt, die an vielen Stellen zu einer intensiven und fachlich anspruchsvollen Diskussion zukunftsträchtiger Entwicklungen führt. Vielmehr soll der Leser diese einzelnen Ergebnisse in einen Gesamtkontext einreihen können. Dies wird insbesondere durch die Strukturierung in Technologiebereiche und Anwendungen sowie einer weiteren Detaillierung in Trends und Thesen gefördert. Damit ist diese Studie ein fundierter Beitrag zur Erfassung von Zukunftstrends und bietet eine Orientierung in dem schnelllebigen und weiter an Bedeutung gewinnenden Bereich der IuK–Technologie. Sie gibt Antworten auf Fragen, wie sich spezifische Informations- und Kommunikationstechnologien kurz-, mittel- und langfristig entwickeln werden. Die Ergebnisse sind eingehend begründet. Sie können in Folge dessen als Unterstützung für Strategieentscheidungen oder als Grundlage für die Ableitung von Handlungsempfehlungen herangezogen werden.

Die Herren Frank Gehring, Harald Kelter und Markus Ullmann begleiteten das Projekt von Seiten des Bundesamtes für Sicherheit in der Informationstechnik mit großem Einsatz. Markus Garschhammer, Patrick Keil, Ulrich Löwer, Marcus Pankow, Michael Schiffers und Sascha Vogel sowie Ammar Alkassar betrieben die Erstellung der Studie mit bewundernswertem Engagement und fachlichem Verständnis. Allen Genannten gilt unser Dank. Insbesondere möchten wir allen Experten, die in den verschiedenen Phasen wertvolle Beiträge in Interviews oder durch ihre Teilnahme an der Fragebogenaktion geliefert haben, unseren Dank aussprechen. Ohne sie wäre diese Studie in der vorliegenden Form nicht möglich gewesen. Für ihre Anmerkungen sind wir schon jetzt allen interessierten Lesern dankbar.

München, im Mai 2003

M. Broy, H.-G. Hegering, A.Picot


# 3 Zusammenfassung

Die vielfältigen und schnelllebigen Entwicklungen im Bereich der Information und Kommunikation erfordern von Unternehmen und öffentlichen Einrichtungen eine Abschätzung zukünftiger Trends. Diese werden weiterhin, daran besteht kein Zweifel, unsere Lebensweise, Ausbildung, Arbeit und Freizeit beeinflussen und verändern. Auf die Veränderungen vorbereitet zu sein und sie bewusst zu nutzen ist eine wichtige Voraussetzung für den Erfolg im (internationalen) Wettbewerb. Genauso wichtig ist das Wissen um künftige Entwicklungen für staatliche Regulierungs- und Aufsichtsbehörden, die die Rahmenbedingungen vorgeben und den Marktteilnehmern Hilfestellung bieten. Die dazu nötigen fundierten Prognosen über die Zukunft der Informations- und Kommunikationstechnik (IuK) in den nächsten zehn Jahren liefert diese Studie.

Zwischen 1990 und 2000 sind die Preise für PCs – qualitätsbereinigt – jährlich um 20% gesunken. Und Moore's Gesetz, das 1965 prognostizierte, dass die Zahl von Transistoren auf einem Micro-Chip in einem Zyklus von etwa 18 bis 24 Monaten verdoppelt wird, gilt auch noch nach über 35 Jahren. Dass immer intelligentere, leistungsfähigere und kleinere Computer zu immer weiter sinkenden Preisen angeboten werden konnten, war der Grundstein für die rasche Ausbreitung der IuK-Technologien in den letzten Jahren. Nicht nur im betriebswirtschaftlichen und im öffentlichen Umfeld schreitet diese Ausbreitung voran, sondern immer stärker auch in privaten Haushalten. Hier besteht noch großes Marktpotenzial, da beispielsweise in den USA die Ausgaben von privaten Haushalten für IuK-Güter (Computer, Software, Telekommunikationsausrüstung) nur ca. 7,5% der entsprechenden Ausgaben von Unternehmen erreichen. Die vorliegende Studie zeigt auch, dass sich gerade für den privaten Bereich umfassende intelligente Systeme entsprechend ausbreiten werden (Abschnitt 9).

Aber welche Technologien und Anwendungen werden sich in welchem Zeitraum durchsetzen? Diese Frage versucht die vorliegende Studie zu beantworten. Anhand von übergreifenden Trends (vgl. Kapitel 6), die langfristig alle Bereiche der IuK-Technologien bestimmen, werden die aktuellen und zukünftigen Entwicklungen dargestellt. Die Identifikation und Definition übergreifender Trends wie Integration und Standardisierung, Konvergenz oder Mobilität sind die Basis für das Erkennen und Einordnen dieser Entwicklungen. Um eine möglichst umfassende Sicht zu ermöglichen, wurden nicht nur die Technologiebereiche Rechnertechnik, Rechnernetze und -kommunikation, Softwaretechnik sowie Datenbanken und Wissensmanagement betrachtet, ein besonderes Augenmerk wurde auch auf die sich daraus ergebenden Anwendungen und die Veränderungen im Vergleich zur Vorgängerstudie [SETIK 00] gelegt. Allerdings muss man sich auch die Risiken und Bedrohungen des technischen Fortschritts bewusst machen und nicht nur für Unternehmen rücken Fragen der Sicherheit immer weiter in den Vordergrund. Deshalb nimmt dieses Themengebiet einen wichtigen Platz innerhalb der Studie ein.

Die folgenden Abschnitte beschreiben, welche spezifischen Trends in den jeweiligen Bereichen untersucht wurden und welche wesentlichen Ergebnisse dabei erzielt werden konnten.

## 3.1 IT-Sicherheit

Innerhalb des Sicherheitsbereiches werden Public-Key-Infrastrukturen, Anonymisierungsdienste, das Gebiet der Kryptographie, der Open-Source-Gedanke, zentrale Authentisierungsverfahren für Internet-Anwendungen und die Biometrie als zentrale Sicherheitstechnologien gesehen. Diese kommen immer wieder in verschiedenen Ausprägungen vor und spielen in vielen Bereichen der Sicherheit eine wichtige Rolle.

Eine der genannten Sicherheitstechnologien, die hier neben der Biometrie stellvertretend für den Bereich dieser zentralen Technololgien vorgestellt werden soll, ist erst in den vergangenen Jahren in den Mittelpunkt des Interesses gerückt und wird für viele zukünftige Dienste als elementar angesehen: Public-Key-Infrastrukturen (PKI), die bei der Ver- bzw. Entschlüsselung mit privaten und öffentlichen Schlüsseln arbeiten. Obwohl die Euphorie der vergangenen Jahre mittlerweile deutlich nachgelassen hat, wird mit einer baldigen Verbreitung gerechnet. Dabei wird sich der Einsatz von PKIs für Kommunikationsbeziehungen zwischen Behörden als erstes etablieren, gefolgt von Kommunikationsbeziehungen zwischen Unternehmen bzw. zwischen Unternehmen und Behörden. Im Bereich Kunde – Unternehmen und Bürger – Behörde wird mangels heute sichtbarer „Killerapplikationen" erst deutlich später mit dem Einsatz solcher Systeme gerechnet. Die im Rahmen von PKIs benötigten Verzeichnisdienste werden etwa zeitgleich verfügbar sein.

Zur Durchsetzung von PKI-Systemen spielt die Interoperabilität (Integration und Kommunikation verschiedener Systeme) eine wichtige Rolle. Hierzu gehören insbesondere die verwendeten Zertifikatsformate. Hier geht der Trend klar in Richtung der hierarchisch orientierten X.509v3-Zertifikate bzw. einem möglichen Nachfolger. PGP-Zertifikate, die eher an das Konzept des „Web of Trust" angelehnt sind, werden hingegen trotz der umfangreichen Fördermaßnahmen vornehmlich im privaten und akademischen Bereich verbleiben.

Mit der Verabschiedung des Signaturgesetzes 1997 (SigG) wurde der Begriff der „qualifizierten elektronischen Signatur" eingeführt. Dieser beschreibt die gesetzlichen Anforderungen an digitale Signaturen für den Einsatz in Bereichen, die üblicherweise der Schriftform bedürfen. Obwohl diese digitalen Signaturen für viele innovative Dienste, z.B. für rechtsverbindliche elektronische Vertragsabschlüsse, essentiell sind, kann mit deren weiten Verbreitung erst gegen Ende des Jahrzehnts gerechnet werden. Der Trend ist eindeutig und zeigt eine erhebliche Bedeutungszunahme qualifizierter elektronischer Signaturen auf. Die beiden anderen im SigG genannten Signaturarten, elektronische und fortgeschrittene elektronische Signatur, werden nur mittelfristig weiter an Bedeutung gewinnen.

Eine Sicherheitstechnologie, an die hohe Erwartungen gestellt werden, ist die Biometrie. Von biometrischen Verfahren erwartet man eine sichere Identifizierung von Personen. Kurz- und mittelfristig werden Anwendungsmöglichkeiten bei der Fingerabdruckerkennung gesehen, langfristig bietet die Gesichtserkennung die größten Perspektiven. Kaum eine Rolle wird hingegen die Iriserkennung spielen. Die Iriserkennung wird fast ausschließlich mit physikalischer Zugangskontrolle im Hochsicherheitsbereich (kritische Infrastrukturen wie Kernkraftwerke, militärische Anlagen) assoziiert. In diesen Bereichen ist die Akzeptanz höher, andere Anwendungen, z.B. Geldausgabe am Bankautomaten, werden auf absehbare Zeit keine Akzeptanz erfahren.

Ein grundsätzliches Problem aller biometrischen Identifikationsverfahren ist das Fehlen von Massenanwendungen. Die befragten Experten gehen davon aus, dass beispielsweise EC-Karten mit biometrischen Merkmalen als typische Massenanwendung mittelfristig nicht zu erwarten sind und dass die vollständige Ablösung anderer Authentisierungsmethoden bei Geschäftsprozessen überhaupt nicht stattfinden wird.

## 3.2 Rechnertechnik

Erst die Evolution und Revolution in der Mikroelektronik ermöglichten einige der grundlegenden Veränderungen innerhalb der Gesellschaft durch die Informations- und Kommunikationstechnologie während der letzten Jahrzehnte. Dies ist besonders auf die stetige Leistungssteigerung bei gleichzeitiger Miniaturisierung der Bausteine zurückzuführen. Im Kapitel Rechnertechnik wurde deshalb für diese Studie besonderer Wert auf die Teilbereiche Prozessortechnik, Speichertechnik, Mensch-Maschine-Kommunikation und Hochleistungsarchitekturen gelegt.

Die Studie bestätigt, dass für die Teilbereiche Prozessortechnik und Speichersysteme Moore's Gesetz, nach dem sich die Leistungsfähigkeit von Prozessoren etwa alle

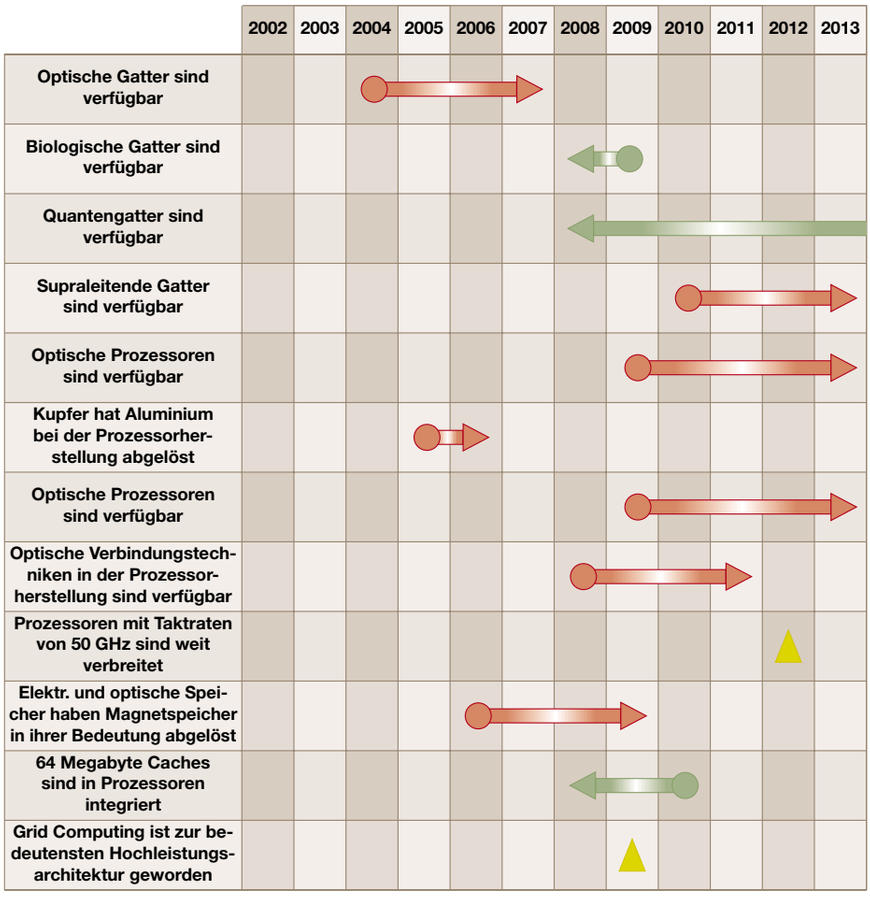



Abbildung 3.1: Verschiebungen ausgewählter Prognosen im Bereich Rechnertechnik

18 Monate verdoppelt, nach Meinung der befragten Experten auch für die nächsten zehn Jahre gelten wird. Damit wird langfristig ein Weg in eine Zukunft eröffnet, in der wir von spontan miteinander kommunizierenden Prozessoren umgeben sein werden, die aufgrund ihrer geringen Größe und ihrem niedrigen Preis selbst in Alltagsgegenstände integriert werden können. Die Vision einer ubiquitären Computerlandschaft wird damit Wirklichkeit.

Nach fast 30-jähriger Tradition von Silizium und Transistorverbindungen aus Aluminium werden die physikalischen Grenzen im Material erreicht. In den Forschungslaboratorien der Prozessorhersteller wird deshalb schon seit längerem nach Alternativen zur heutigen Prozessortechnologie gesucht. Die Studie zeigt, dass Materialien auf Indium- und Germanium-Basis an der Schwelle zur serienmäßigen Verwendung stehen und dass sich auf Kupfer basierende Verbindungstechnologien zwischen Transistoren schon in den nächsten fünf Jahren durchsetzen werden. Optische Verbindungstechniken werden erst langfristig eine Rolle spielen. Alternative Prozessortechnologien, basierend auf optischen, biologischen oder Quanteneffekten, könnten Moore's Gesetz weitertragen, stecken aber noch in den Kinderschuhen. Eine allgemeine Verfügbarkeit optischer, biologischer und Quantengatter wird von den Experten zwar schon mittelfristig vorausgesagt, optische Prozessoren werden allerdings erst in zehn Jahren erwartet, biologische und Quantenprozessoren noch sehr viel später.

Aufgrund der zunehmenden Miniaturisierung und Integrationsdichte werden die Chips der nächsten zehn Jahre mit fast zehn Milliarden Transistoren bestückt sein und Gatterlängen unter zehn Nanometern (nm) besitzen, vorausgesetzt, die Halbleiterindustrie ist in der Lage, den bei diesem Chip-Design potenziell erhöhten

Stromverbrauch zu kontrollieren. Damit können Taktraten von einigen hundert GHz erreicht werden. Die Experten sind sich weitgehend einig, dass in spätestens zehn Jahren Taktraten von 50 GHz auf 128-Bit-Architekturen zum Standard geworden sind. Multiprozessor-Chips mit einem optimierten Strommanagement und einer alternativen Stromversorgung werden als komplementäres Konzept zur Leistungssteigerung nach Meinung der Experten schon mittelfristig zum Tragen kommen können. Greifen diese Ansätze, bleibt Moore's Gesetz auch für die nächsten zehn Jahre gültig.

Bei den Prozessorarchitekturen werden die heute noch üblichen 32-Bit-Architekturen schon mittelfristig durch 64-Bit-Architekturen abgelöst. Langfristig allerdings sehen die Experten eine Dominanz der 128-Bit-Architekturen.

Bei den Speichertechnologien zeigt sich weiterhin die hervorragende Bedeutung elektronischer Speicher, aber auch die zunehmende Relevanz optischer und biologischer Speicher gegenüber den heute verbreiteten magnetischen Speichern. Die nächsten zehn Jahre werden daher neben einer massiven Steigerung der Speicherkapazitäten vor allem durch die Einführung derartiger Speichermedien geprägt. Allein die Kapazitäten der über verschiedene Hierarchiestufen organisierten Cache-Speicher werden bis zum Ende dieses Jahrzehnts 60 Megabyte und bis zum Jahr 2013 etwa 300 Megabyte erreichen. Ähnliche Entwicklungen werden bei Hauptspeicherkapazitäten erwartet: Langfristig werden Desktops mit annähernd 100 Gigabyte Hauptspeicher ausgestattet, Server mit etwa 60 Terabyte und Hochleistungsrechner mit einem Viertel Petabyte.

Im Rahmen der Mensch-Maschine-Schnittstelle wird für die nächsten Jahre erwartet, dass die Eingabe von Information über Tastatur und Touchscreen kontinuierlich von Spracheingabe und Handschriftenerkennung abgelöst werden wird. Eine ähnliche Entwicklung wird bei der Darstellung von Informationen gesehen, wo die klassische Röhrentechnologie mehr und mehr durch Laser-Display-Technologien (LDT) ersetzt werden wird.

Parallel- und Hochleistungsrechner unterschiedlicher Architekturen werden zunehmend für immer komplexere Anwendungen benötigt. Ihre Leistungsgrenze werden sie auch in zehn Jahren nicht erreicht haben, trotz des Vorstoßes in den PetaFlop-Bereich. Da die klassischen Vektorrechner jedoch spürbar an ihre Grenzen stoßen, werden mittel- bis langfristig Cluster-Architekturen und Grid-Systeme an Bedeutung gewinnen, nicht nur im wissenschaftlichen Bereich. Untersucht wurden deshalb neben Speicherarchitekturkonzepten für Mehrprozessorsysteme auch Prozessorstrukturen von Parallelrechnern. Einige weitere interessante Aspekte, auf die in der Studie näher eingegangen wird, sind der Aufbau paralleler Systeme aus Standardkomponenten, die Parallelisierung von Desktop-Systemen und die langfristige Bedeutung von Ein-/Ausgabeperipherien. Es zeigt sich, dass bis zum Ende des Jahrzehnts Hochleistungssysteme auf der Basis von Standardprozessoren, massiv parallele Desktopsysteme und kommerziell eingesetzte Hochleistungsrechner eine wachsende Rolle spielen werden.

Der Vergleich mit der Vorgängerstudie zeigt hauptsächlich bei der Einschätzung der Verfügbarkeit von Bausteinen und Prozessoren sowie bei der Beurteilung optischer Technologien Prognoseverschiebungen. Die Verfügbarkeit optischer und supraleitender Gatter wird in dieser Studie sehr viel pessimistischer gesehen, während die Verfügbarkeit biologischer und Quantengatter optimistischer beurteilt wird. Die Verfügbarkeit optischer Prozessoren und optischer Verbindungstechniken in der Prozessorherstellung werden um etwa vier Jahre nach hinten korrigiert, während die Experten die Integration großer Cache-Speicher auf Prozessor-Chips in dieser Studie früher sehen. Die wesentlichen Prognoseverschiebungen und neuen Trends sind in Abbildung 3.1 zusammengefasst.

## 3.3 Rechnernetze und Kommunikation

Kommunikationsinfrastrukturen stellen die Basis für vielfältige Anwendungen der IuK-Technologie. Im Kapitel Netze und Kommunikation (8.2) werden die umfassenden Entwicklungen in diesem Bereich beleuchtet. Dabei wird sowohl auf die Weiterentwicklung bestehender Systeme als auch auf neu entstehende

Technologien eingegangen. Besonders der Austausch von Informationen wirft unterschiedlichste Fragestellungen bezüglich der Sicherheit in Kommunikationsnetzen auf, die ebenfalls in diesem Kapitel betrachtet werden. Allgemein läßt sich feststellen, dass die Experten in ihren Aussagen wesentlich pessimistischer geworden sind als in der Vorgängerstudie aus dem Jahr 2000 [SETIK 00]. Die Verschiebung von ausgewählten Prognosen zeigt Abbildung 3.2. Dabei wird deutlich, dass nur sehr wenige Vorhersagen aus dem Jahr 2000 eingehalten werden.

Die Betrachtung der Sicherheit im Internet zu Beginn des Kapitels zeigt, dass sich der Einsatz von Firewalls weiterhin verstärken wird. Dabei werden auch neuartige Konzepte wie dezentrale und Personal-Firewalls umgesetzt und zusätzliche Filterfunktionen wie Virenscanner mit in diese Sicherheits-Gateways integriert werden. Als Sicherheitsprotokoll wird sich mittelfristig IPSec (Internet Protocol Security) [IETF 99] durchsetzen, das langfristig zum festen Bestandteil von IPv6 werden wird. Bei Verfahren zur Datenanalyse erwarten die Experten, dass die derzeit vorherrschende Signaturerkennung langfristig von der Anomalieerkennung eingeholt wird. IDSe (Intrusion Detection System) werden als integrale Bestandteile von Sicherheits-Gateways weite Verbreitung finden. Ebenso werden mittelfristig IRS (Intrusion Response System) eingesetzt werden. Die Übertragung aktiver Inhalte wird in den nächsten Jahren sowohl durch Signieren als auch durch Protection Lists gesichert werden. Allerdings wird nicht erwartet, dass keine unsicheren Übertragungsverfahren mehr eingesetzt werden. Im Moment ist nach Aussage der Experten ein ungeprüftes Ausführen von aktiven Inhalten gängig, weil eine vollständige Sperrung des Zugriffs auf Inhalte dieser Art nicht durchsetzbar ist. Mittelfristig wird der Einsatz von Sandboxing-Technologien zur Kontrolle aktiver Inhalte erwartet. Ihre Prüfung wird durch Secure Proxies erfolgen.

Der bereits in der Vorgängerstudie im Jahr 2000 prognostizierte Trend zur Erhöhung der Übertragungsraten wird weiter anhalten. Beschränkungen werden eher durch den Markt und den Bedarf der Anwender als durch den Mangel an geeigneten Technologien erwartet. Langfristig wird sich, wie auch schon 2000 vorhergesagt, der Glasfaseranschluss bis zum Endgerät ebenso durchsetzen wie die Anbindung von Endsystemen mit hochratigen Übertragungstechniken. Bereits 2006 wird die drahtlose Vernetzung mit WLANs (Wireless LAN) weit verbreitet sein. Ebenso wird, wie bereits im Jahr 2000 (siehe Abbildung 3.2), vorhergesagt, dass asymmetrische Zugangstechnologien (wie xDSL [Hart 00]) mittelfristig symmetrische Technologien verdrängen werden, um dem gesteigerten Bandbreitenbedarf im Zugangsnetz gerecht zu werden. Als Zukunftstechnologie wrden sich photonische Netze [Detk 99] erst in zehn Jahren durchsetzen. Bei dieser Technologie ist die Veschiebung der Prognose gegnüber 2000 besonders auffallend (siehe Abbildung 3.2).

Die Vereinheitlichung der Kommunikationsinfrastrukturen bei gleichzeitig zunehmender Vernetzung wird weiter anhalten. IPv4 wird auf lange Sicht durch IPv6 abgelöst werden. Allerdings hat sich der Zeitpunkt für diese Ablösung gegenüber 2000 weiter verschoben (siehe Abbildung 3.2). Als Backbonetechnologie wird sich WDM (Wavelength Division Multiplexing) und damit IP over $\lambda$ (IP over lambda) [Ghan 00] durchsetzen. MPLS (Multi Protocol Label Switching) [Davi 00] wird nur eine Bedeutung als Übergangstechnologie beigemessen. Etablierte Technologien wie ATM (Asynchronous Transfer Mode) [Sieg 03], SDH (Synchronous Digita Hirarchy) oder ISDN (Integrated Services Digital Network) [Kanb 98] werden bereits innerhalb der nächsten fünf Jahre an Bedeutung verlieren. Gigabit-Ethernet wird das klassische Ethernet [Hanc 96] ablösen. Da die Experten neue Zugangstechniken erwarten, wird xDSL langsam an Bedeutung verlieren. DAB (Digital Audio Broadcasting) [DAB 03, Frey 97] und DVB (Digital Video Broadcasting) [DAB 03, PSF$^+$ 00] werden zukünftig ebenfalls zum Aufbau von Verteil- und Zugangsnetzen verwendet werden. UMTS (Universal Mobile Telecommunication System) [KAL$^+$ 01] und MobileIP werden sich langfristig zu Schlüsseltechnologien der Mobilkommunikation entwickeln. Bluetooth wird nur in „Nischen" Anwendung finden. UMTS und WLAN werden die bevorzugte Basis für IP-Kommunikation (Internet Protocol) [IETF 81] in drahtlosen Netzen bilden. DECT (Digital Enhanced Cordless Technologies) [Walk 98] und GPRS (General Packet

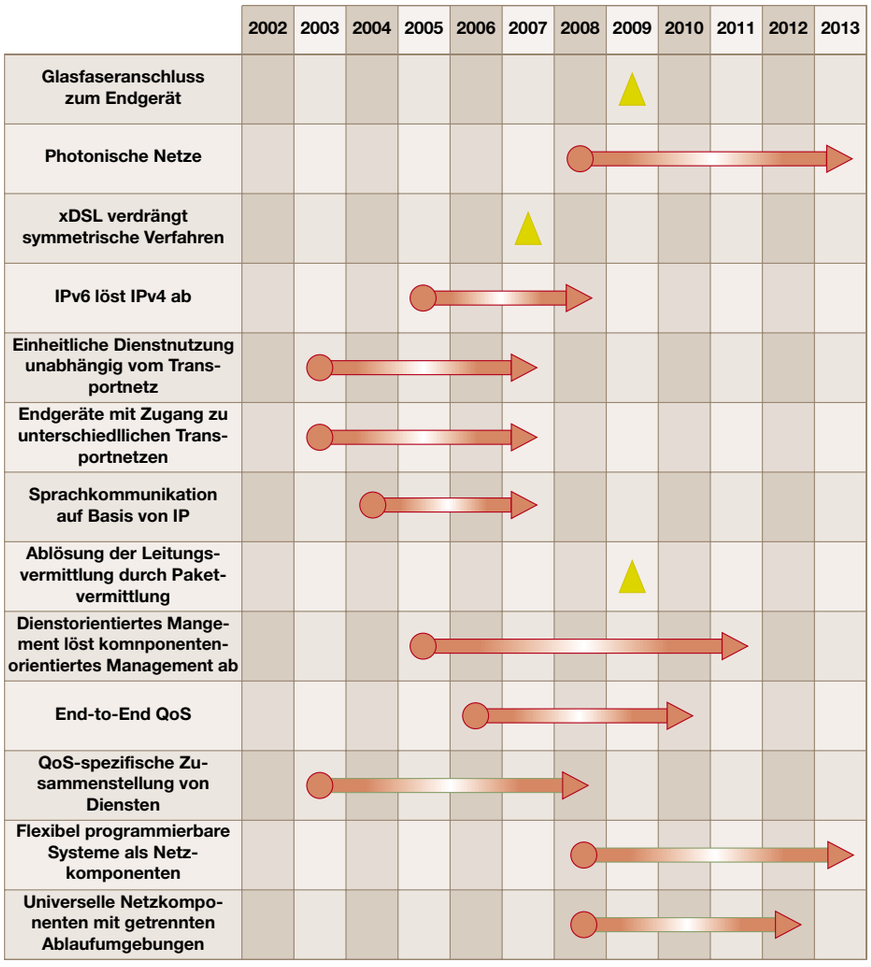



Abbildung 3.2: Verschiebungen ausgewählter Prognosen im Bereich Netze und Kommunikation

Radio Service) [HeSa 01] werden in den Hintergrund treten. MPLS und Wirespeed-Routing werden zwar als Technologien zur Durchsatzsteigerung von IP bedeutender als andere Technologien in diesem Umfeld, allerdings lässt sich auf Grund der wenig unterschiedlichen Wertungen der Experten keine deutliche Aussage über zukünftige Entwicklungen treffen. Mittelfristig sind MPLS-Netze weit verbreitet. Allerdings wird dabei auch auf lange Sicht kein durchgängiges MPLS-Netz entstehen. Der Zugang zu Datennetzen wird bald auch für Automobile und Haushaltsgeräte möglich sein. Beim Aufbau von Zugangsnetzen werden TV-Kabel-Netze in den nächsten zehn Jahren Stromnetze als Basisinfrastruktur zum Aufbau von Zugangsnetzen verdrängen.

Langfristig wird von einer gänzlichen Konvergenz der Netze und Endgeräte ausgegangen. In absehbarer Zeit, aber deutlich später als 2000 vorhergesagt (siehe Abbildung 3.2), wird ein einheitliches Dienstangebot unabhängig vom unterliegenden Transportnetz ebenso erwartet wie Endgeräte mit Zugang zu unterschiedlichen Transportnetzen. Ein einheitliches Transportnetz wird sich auch langfristig nicht etablieren. VoIP (Voice over IP) wird mit einer Dienstgüte, die mit der derzeitiger Sprachnetze vergleichbar ist, bald auch in Weitverkehrsnetzen verfügbar sein. Auch bei dieser Technologie hat sich die Prognose der Experten deutlich verschoben (vgl. Abbildung 3.2). Wie 2000 vorhergesagt (vgl. Abbildung 3.2), wird die paketvermittelnde Übertragung die leitungsvermittelnde Übertragung im Bereich der

Sprachübertragung auf Backbones und in Zugangsnetzen nur langfristig ablösen. In einigen Jahren werden fest installierte und mobile Endgeräte für Sprach- und Datenkommunikation weit verbreitet sein. Zwischen der Kommunikation im Festnetz und jener im Mobilnetz wird sich langfristig ein verhältnismäßiges Gleichgewicht einstellen. Das Verhältnis von Sprach- zu Datenkommunikation wird sich sowohl im Volumen als auch in den Umsätzen von einem deutlichen Übergewicht der Sprachkommunikation hin zu einem leichten Übergewicht der Datenkommunikation entwickeln.

Auch im Bereich der Dienstorientierung, der Erbringung von Dienstgüte und Nutzung von Dienstplattformen, hat sich gezeigt, dass die Experten gegenüber 2000 in ihren Einschätzung wesentlich pessimistischer wurden. Dienstorientiertes Management wir das komponentenbasierte Management nur langfristig ablösen. In diesem Fall hat sich die Prognose der Experten massiv verschoben (siehe Abbildung 3.2). Auf längere Zeit ermöglichen standardisierte Beschreibungstechniken Trading. Die Einschätzung über die Verfügbarkeit von End-to-End-Dienstgüte-Garantien im Internet hat sich verschoben (siehe Abbildung 3.2). Diese Garantien werden nach Meinung der Experten erst langfristig verfügbar. Eine Verschiebung ist ebenfalls bei der kundenspezifischen Zusammenstellung von Diensten aufgrund gewünschter Dienstgüten sichtbar (siehe Abbildung 3.2). Dennoch wird eine von mehreren Providern genutzte Dienstgütearchitektur verbreitet eingesetzt werden. Schnittstellen zur Dienstgüteüberwachung werden sich langfristig Jahren etablieren. Für Großkunden wird es dann auch die Möglichkeit geben, die Dienstgüte durch Managementeingriffe selbst zu beeinflussen. Als Mechanismus zur Bereitstellung garantierter Dienstgüten wird MPLS vorhergesagt. Zur Signalisierung von Dienstgüteanforderungen wird langfristig, wohl im selben Maß, wie es sich auch als Transportprotokoll durchsetzen wird, IPv6 verwendet werden. Bereits in einigen Jahren werden standardisierte Plattformen zur Implementierung und Erbringung von Diensten eingesetzt. Eine einheitliche API (Application Programmers Interface) für Dienstplattformen wird sich nur langsam etablieren.

Auch im Bereich der flexibel programmierbaren Netze sind die Einschätzungen gegenüber der Vorgängerstudie im Jahr 2000 deutlich pessimistischer geworden. Überlegungen nach der rein funktionalen Umsetzbarkeit sind hier komplexeren Fragestellungen des Managements und der Sicherheit (im Sinne von Security) gewichen. Dennoch werden VPNs (Virtual Private Network) auf Basis von IP bereits sehr bald eingesetzt. Flexibel programmierbare Systeme werden derzeitige Netzkomponenten nur sehr langfristig ersetzen. Hier hat sich wie beim Einsatz universeller Netzkomponenten, die für Benutzer getrennte Ablaufumgebungen zur Verfügung stellen, eine deutliche Korrektur der Prognose aus dem Jahr 2000 ergeben (siehe Abbildung 3.2). Mittelfristig werden von den Experten jedoch sichere und operable Systeme auf Basis mobiler Agenten ebenso erwartet wie die Umsetzung des Management-by-Delegation-Konzepts.

Mobile Computing [Roth 02] bietet als mittlerweile eigenständiger Bereich der Rechnerkommunikation enorme Entwicklungschancen, die auch mit der Einführung von UMTS verbunden werden. WLANs werden sich als öffentliches Zugangsnetz bereits kurzfristig verbreiten. Mittelfristig stehen auch mobilen Endgeräten hochratige (mindestens 10 MBit/s) Anbindungen, allerdings nicht exklusiv, zur Verfügung. Für mobile Benutzer ist es dann ebenfalls möglich, beliebige Dienste auf beliebigen mobilen Geräten zu nutzen (Mobilität des Gerätes). Ebenso können in einigen Jahren beliebige Dienste (neben Telefonie) auf mobilen Geräten genutzt werden. (Mobilität des Benutzers). Die Mobilität der Session, also die beliebige Unterbrechung und Wiederaufnahme der Dienstnutzung bei einem Wechsel des Endgeräts wird von den Experten nicht als vordringliche Fragestellung betrachtet. UMTS und WLAN setzen sich langfristig als Technologien für den drahtlosen Netzzugang durch. Als Anwendungsprotokoll in mobilen Netzen wird sich, ebenso wie im Festnetz HTML (Hyptertext Markup Language) [MuKe 01] durchsetzen. Langfristig werden drahtlose Netze der 4. Generation (4G) durch Weiterentwicklung der 3G-Techniken ebenso entstehen wie durch Konvergenz vorhandener Techniken (WLAN, Bluetooth, usw.). Die Notwendigkeit, auf Grund von Protesten aus der Bevölkerung beim Aufstellen neuer Sender

neue drahtlose Netze nur noch auf Basis bestehender Infrastrukturen (Größe und Lage von Funkzellen) zu nutzen, wird sich nach den Aussagen der Experten nicht ergeben. Sie erwarten, dass technische Probleme beim Einsatz des von CDMA (Code Devision Multiple Access) in UMTS-Netzen bereits in zwei Jahren gelöst sind, sagen die technische und organisatorische Trennung von Netz- und Dienstbetrieb in UMTS-Netzen allerdings erst für das Ende des Jahrzehnts voraus. Als Hintergrund-Infrastruktur für UMTS wird sich IP langfristig durchsetzen.

Besonders der Bereich des Mobile Computing wirft neue Sicherheitsfragestellungen auf. Die wichtigste neue Sicherheitseigenschaft in UMTS ist nach Ansicht der Experten die gegenseitige Authentifizierung sowie die Integritätsprüfung der übertragenen Daten. Die Umsetzung von Sicherheitsdiensten für UMTS auf Basis von TCP/IP (Transmission Control Protocol/Internet Protocol) [IETF 81] wird nicht erwartet. Bedrohungen durch das Einbringen von ausführbaren Inhalten mit Schadfunktion bzw. durch Ausspähen der übertragenen Daten werden zunehmen. Die Kopplung der UMTS-Netze mit dem Internet über Gateways schafft neue Bedrohungspotenziale. Vornehmlich werden Angriffe auf die UMTS-Netzwerkinfrastruktur über das Internet-Gateway z.B. durch DDoS-Angriffe (Distributed Denial of Service) erwartet. Sicherheitsschwächen von Funknetzen werden durch die Benutzer erfasst und in den Sicherheitsrichtlinien berücksichtigt werden. Eingebaute Sicherheitsfunktionen der standardisierten Wireless-Technologien werden zwar bereits kurzfristig von den Benutzern verwendet werden, bieten aber nach den Aussagen der Experten keinen wirksamen Schutz gegen böswillige Angreifer. Sicherheitsfunktionalitäten in den höheren Protokollschichten werden bereits kurzfristig bisherige Link-Sicherungskonzepte auf der Luftschnittstelle ersetzten. Als spezifische Bedrohungen für Wireless-Netze wird das Ausspähens der im Netzwerk kommunizierten Daten genannt, wie die mögliche spontane Vernetzung und DoS-Angriffe (Denial of Service) durch Störsender.

## 3.4 Datenbanken und Wissensmanagement

Die Repräsentation, Speicherung und Verarbeitung von Informationen ist Gegenstand dieses Technologiefeldes, das eine besondere Position im Umfeld von Informations- und Kommunikationstechnologien darstellt: nahezu keine Anwendung wird heute mehr entwickelt, ohne auf Datenbanktechnologien zurückzugreifen. Die Integration neuer Funktionen und Anwendungen in Datenbanksysteme, z.B. zur Lösung statistischer Probleme oder für CAD, führt auch zu einer Weiterentwicklung der bisher dominierenden Datenmodelle. Gleichzeitig verlangt der Markt nach Interoperabilität und Vernetzung von Datenbanken, damit mehrere Benutzer von verschiedenen Anwendungen aus auf die selbe Datenbank zugreifen können, oder um mit Hilfe verteilter Datenbanken dem steigenden Datenvolumen Herr zu werden. Dies setzt allerdings eine fortschreitende Vereinheitlichung von Schnittstellen und die Verwendung standardisierter Dateiformate voraus. Weitere Untersuchungsgegenstände im Bereich der Datenbanken sind Speichertechnologien, Datenbankarchitekturen, Abfragesprachen sowie Fragen der Datenanalyse sowie der Sicherheit in Datenbanken.

Im Kontext von Datenmodellierung wurde untersucht, wie sich die Bedeutung verschiedener Datenbanktechniken zukünftig entwickeln wird. Während heute relationale Modelle dominierend sind, ergeben sich v.a. durch immer komplexere Daten, z.B. im Multimedia-Bereich, neue Anforderungen. Deshalb wird erwartet, dass objektrelationale Datenmodelle relationale, aber auch rein objektorientierte Modelle ablösen werden. Von großer Bedeutung wird in den nächsten zehn Jahren v.a. die Integration von Funktionalität für ingenieurtechnische Anwendungen (z.B. Computer Aided Design) und zur Verarbeitung geographischer Daten sein. Aber auch deduktive Datenbanktechniken zur „Wissensgenerierung", die heute schon in den gängigsten Datenbanksystemen integriert aber noch nicht ausgereift sind, werden an Bedeutung gewinnen, z.B. im Customer Relationship Management oder für Navigationssysteme. Auch Verfahren zur Lösung statistischer Probleme wie evolu-

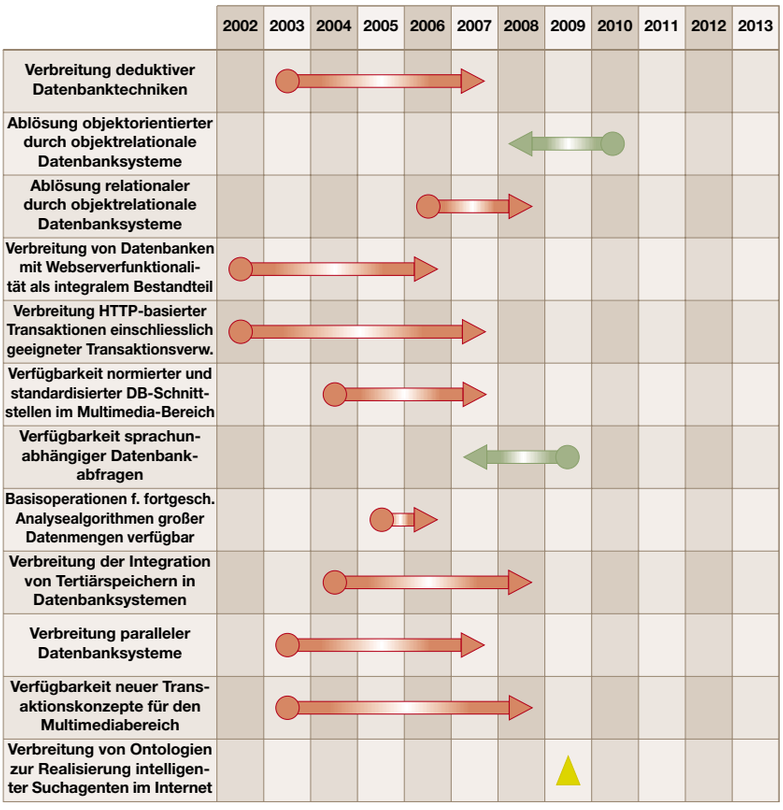



Abbildung 3.3: Verschiebungen ausgewählter Prognosen im Bereich Datenbanken und Wissensmanagement

tionäre Algorithmen oder neuronale Netze werden in Datenbanken integriert werden.

Anhand der Fragen zu Datenmodellierung lassen sich deutliche Verschiebungen in den Einschätzungen der Experten ablesen. Während sich in allen Themenbereichen zeigt, dass die Erwartungen der letzten Studie sehr optimistisch hinsichtlich der Dauer bis zum Eintreten bestimmter Entwicklungen waren, wird die Ablösung von objektorientierten durch objektrelationale Datenbanksysteme zwei Jahre früher erwartet als in der Studie 2000. Die Ablösung relationaler DBS dagegen wird später geschehen als vor drei Jahren angenommen. Um durchschnittlich ein bis zwei Jahre haben sich die Erwartungen der Experten nach hinten verschoben. Dabei muss beachtet werden, dass die Vorgängerstudie in der Zeit des Internet-Booms entstand, der auch für die dahinterliegenden Datenbanksysteme enorme Veränderungen bedeutet hat. Neben dem Abflauen dieser Euphorie muss auch die weltwirtschaftliche und weltpolitische Lage in Betracht gezogen werden. Gerade die Entwicklung neuer CRM- und Data-Warehouse-Anwendungen leidet unter dem Rückgang der Investitionen der Unternehmen, da diese Systeme für das operative Geschäft nicht unbedingt nötig sind. Einige der interessantesten Veränderungen zeigt Abbildung 3.3, wobei einige Themen der Vorgängerstudie nicht mehr in die Befragung aufgenommen wurden, da sie mittlerweile „state of the art" sind. Eine Reihe von Themen wurde dagegen erstmals oder ausführlicher behandelt, z.B. Fragen zu Ontologien. Die nächste Überarbeitung der Studie wird wiederum thematische Verschiebungen und Anpassungen nötig machen.

Die zunehmende Vernetzung von Systemen und Anwendungen bietet auch im Datenbankbereich völlig neue Möglichkeiten, z.B. im E-Commerce oder in Form des Supply Chain Management. Grundlage für die Vernetzung und Interoperabilität ist eine Vereinheitlichung von Schnittstel-

len und die Verfügbarkeit von Standard-Dateiformaten. Bei den Dateiformaten wird XML eine entscheidende Rolle spielen, während EDI in einigen Jahren kaum noch verwendet werden wird. Die Studie geht dabei auch schon auf potenzielle Nachfolger von XML ein. Schnelle Entwicklungen sind auch bei der Integration von Web-Funktionalität einschließlich moderner netzweiter Transaktionskonzepte zu beobachten. Einen weiteren Beitrag zur Interoperabilität, Bedienerfreundlichkeit und zunehmenden Internationalisierung von Datenbanken wird die Entwicklung sprachunabhängiger Datenbankabfragen leisten, die innerhalb der nächsten Jahre erfolgen wird. Weiterhin wurden die aufgrund der steigenden Vernetzung zunehmend an Bedeutung gewinnenden Fragen der Datensicherheit ebenfalls in die Untersuchungen einbezogen.

Bedingt durch die immer weiter fortschreitende Digitalisierung vieler Daten, aber auch durch die Integration multimedialer und ingenieurtechnischer Anwendungen wird das in Datenbanken verwaltetet Datenvolumen langfristig um jährlich ca. 50% wachsen. Dies verlangt zwangsläufig nach neuen Speichertechnologien. Welche hierbei in Frage kommen und inwieweit sie neue Datenbanktechniken ermöglichen werden, wird ebenfalls erläutert. Deutliche Performancesteigerung versprechen auch die Nutzung paralleler Datenbanksysteme sowie neue Index- und Zugriffstrukturen, die ebenfalls thematisiert werden.

Diese Diskussion schließt, als letzten Abschnitt des Kapitels Datenbanken, mögliche Weiterentwicklungen von Transaktionskonzepten und bestehenden Datenmodellen bzw. Datenbanksystemen sowie neue Konzepte für Datenbankabfragen ein. Bei der Gegenüberstellung der gängigsten Datenbanksysteme zeigt sich auch langfristig keine Änderung an der beherrschenden Marktstellung der Produkte Oracle, IBM DB2 und Microsoft SQL Server. Zwar werden Open-Source Datenbanksysteme wie MySQL an Bedeutung gewinnen, durch ihre immer noch geringere Funktionalität werden sie aber auch langfristig nur für kleinere Anwendungen Verwendung finden. Die vorherrschende Abfragesprache in kommerziellen Datenbanksystemen wird auch weiterhin SQL sein, auch wenn in den nächsten Jahren XML-basierte Abfragesprachen wie XQL und XSL an Bedeutung gewinnen. Diese Sprachen ermöglichen auch das Durchsuchen von Daten, die nicht in Tabellenform, sondern in beliebigen Dokumenten vorliegen.

Abschließend wird auf die Problematiken und möglichen Lösungen im Bereich der Sicherheit in Datenbanken eingegangen. Dabei zeigt sich, dass gerade im Datenbankbereich Sicherheit als sehr umfassendes Kriterium angesehen werden muss. Identifikation, Authentisierung und Zugriffskontrolle werden deshalb immer wichtiger werden. Die Entwicklung von umfassenden Sicherheitsarchitekturen wird aber eine bedeutende Aufgabe für alle Bereiche der Informations- und Kommunikationstechnik werden.

## 3.5 Softwaretechnik

Die Softwaretechnik wird in den kommenden Jahren noch verstärkt neuen Anforderungen gegenüber stehen. Diese schließen die Flexibilität und Dynamik von Systemen und Systemumgebungen und die Skalierbarkeit bei der Systemnutzung sowie die komplexen Informations- und Kommunikationsstrukturen mit ein.

Diese Anforderungen sind ohne neue Konzepte in der Softwaretechnik nicht realisierbar. Diese Konzepte betreffen unterschiedliche Bereiche des Softwareengineerings und reichen dabei von Fragen der Strukturierung von Architekturen über Komponenten oder Dienste bis hin zur Definition neuer Beschreibungstechniken sowie deren semantischen Fundierung, der Entwicklung neuer Entwicklungsparadigmen sowie der Definition präziser und dennoch praktikabler Vorgehensmodelle. Dabei steht insbesondere eine stärkere Automatisierung und Systematisierung des Entwicklungsprozesses im Zentrum der Diskussion.

Die Entwicklung verlangt insbesondere die Einführung neuer Modelle zur effizienten Entwicklung von vernetzten und flexiblen Systemen. Diese Systeme werden zunehnend in allen Bereichen des täglichen Lebens zu finden sein, wenn auch vielfach für den Endnutzer nicht unmittelbar sichtbar, wie beispielsweise elektronische Haussteuerungskomponenten oder Komponenten zur elektronischen Fahrzeugsteuerung. In diesem Zusammenhang ist

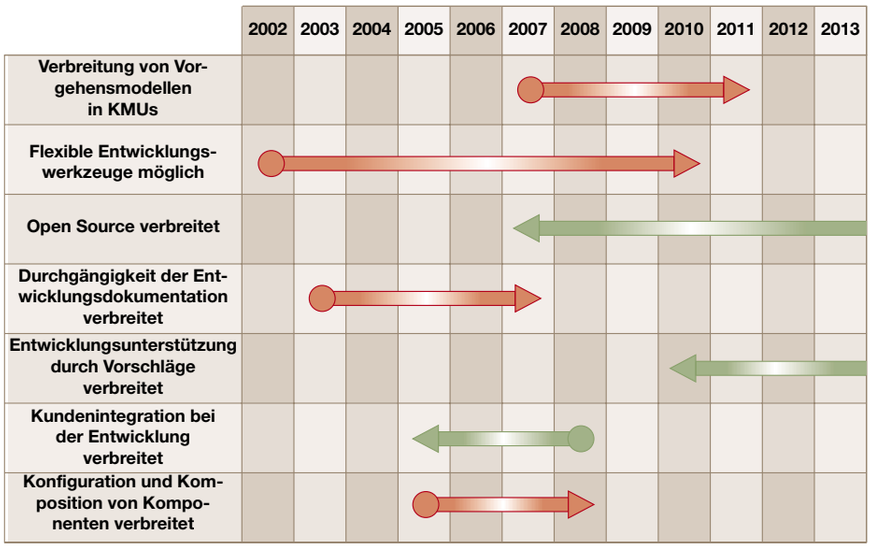



Abbildung 3.4: Verschiebungen ausgewählter Prognosen im Bereich Softwaretechnik

es sinnvoll, die Entwicklung von Software sehr abstrakt zu ermöglichen, um den Softwareingenieur von der zugrunde liegenden Technologie zu befreien, so dass dieser sich vorwiegend auf die Realisierung von Systemanforderungen konzentrieren kann.

Die Studie untersucht Technologien in den Forschungsbereichen Softwarearchitekturen und Kommunikationsmechanismen wie SunONE, .NET oder XML, Beschreibungstechniken wie SDL oder die etablierte objektorientierte UML oder Entwicklungsprozesse und Prozessdefinitionen wie Cleanroom, CMM oder (R)UP. Zusätzlich werden Systemanforderungen wie Reaktivität, Realzeitigkeit oder Mobilität ebenso wie unterschiedliche Systemklassen in den Bereichen Automotive, Telekommunikation oder Integrierte Gebäudesysteme detailliert diskutiert. Ferner wird untersucht, welche Werkzeugkonzepte wie beispielsweise Artisan, Ascet, Statemate oder UML/RT den Anforderungen der Zukunft in den angegebenen Systemklassen gewachsen sind.

Die bereits genannten Entwicklungen im Bereich der Softwaretechnik erfordern methodisch die Verbreitung immer leistungsfähigerer Entwicklungsumgebungen, damit Systeme mit den aufgezeigten Anforderungen auch künftig realisiert werden können. Dies setzt effizientere Entwicklungmethoden und neue Werkzeugkonzepte zur Entwicklung moderner dynamischer und mobiler Systeme voraus. Folgende Trends können exemplarisch beobachtet werden: zunächst ist ein Trend zur Vereinfachung und Leistungssteigerung von Software-Entwicklungsprozessen identifizierbar. Dieser basiert vorwiegend auf dem Bedeutungszuwachs von Komponenten- und Diensttechnologien, die eine modulare und strukturierte Entwicklung ermöglichen. Dadurch werden zudem Wiederverwendungspotenziale erhöht, was zu einer größeren Effizienz bei der Softwareentwicklung führt. Durch neue und leistungsstärkere Qualitätssicherungsverfahren im Bereich Testen und Verifikation sind darüber hinaus Potenziale bei der Reduktion von Fehlern zu erwarten.

Weiterhin ist abzusehen, dass der Trend zur Interoperabilität von Systemen zunehmend an Gewicht gewinnt. Hierzu zählt insbesondere die Selbstorganisation von Systembausteinen, die sich wie folgt charakterisieren lässt: Geschäftsreisende sind beispielsweise in der Lage, in Hotels oder Flughäfen die bestehende Infrastruktur mit ihren eigenen tragbaren Rechnern zu nutzen und zu bedienen. Die Integration und die Interoperabilität erfolgen dabei dynamisch zur Laufzeit und müssen nicht vom Nutzer mühsam konfiguriert werden.

Interoperabilität ist allerdings auch aus methodischer Sicht bei der Entwicklung von Bedeutung. In diesem Zusammenhang wurde evaluiert, welche Kriterien erfüllt sein müssen, damit eine weitere erfolgreiche Automatisierung des Entwicklungsprozesses möglich wird. Dazu gehören neben der Interoperabilität von Werkzeugen und Methoden auf Basis gemeinsamer Metamodelle auch die zunehmende Unterstützung von Prozessen durch Simulationen, Codegenerierung oder organisatorische Aspekte wie das Projektmanagement. Die Bedeutung dieses Trends wird bestätigt durch die Erwartung eines enormen Zuwachses des Automatisierungsgrades am Beispiel der Codegenerierung. In diesem Kontext zeigt sich die große Bedeutung von Technologien zur Unterstützung der Interoperabilität wie XML oder SOAP. Abgeschlossen wird die Betrachtung des Softwaretechnik-Bereiches mit einer Bewertung gängiger Entwicklungswerkzeuge, die in Zukunft als umfassende „Best-of-Everything-Werkzeuge" aus einzelnen Werkzeugen zusammengesetzt sein werden.

Die hohe Dynamik in der Entwicklung der angesprochenen Forschungsbereiche hat in den vergangenen Jahren dazu geführt, dass im Bereich Softwaretechnik zahlreiche Verschiebungen in der Einschätzung von Anwendungen, Technologien und Methoden zu beobachten sind. Alle signifikanten Veränderungen, die sich aus einem Vergleich zur Vorgängerstudie [SETIK 00] beobachten lassen, werden im Themenfeld Softwaretechnik diskutiert. Einige dieser Veränderungen sind in Abbildung 3.4 veranschaulicht und lassen sich wie folgt beschreiben: Die Integration von Vorgehensmodellen zur ingenieursmäßigen Entwicklung von Software in kleine und mittelständige Unternehmen wird sich nach Aussage der Experten weiter in die Zukunft verschieben. Flexible Entwicklungsumgebungen, welche eine metamodellbasierte Systementwicklung über die unterschiedlichen Entwicklungsphasen hinweg ermöglichen, verschieben sich ebenfalls deutlich in die Zukunft. Gleichermassen verhält es sich mit der Durchgängigkeit der Entwicklungsdokumentation oder neuen Paradigmen wie der Erstellung von Software über die Komposition und Konfiguration von Software-Komponenten. Deutlich optimistischer werden hingegen in diese Studie die Verbreitung von Open Source, die Entwicklungsunterstützung über Vorschläge und Simulationen sowie die Qualitätssicherung von Kundenanforderungen durch eine stärkere Einbindung von Kunden durch die Experten bewertet.

## 3.6 Anwendungen

Technologien und der sichere Umgang mit ihnen machen ohne praktische Anwendungen wenig Sinn. Allerdings wirken sich die hier untersuchten Technologien in derart vielen Bereichen aus, dass es unmöglich erscheint, alle denkbaren Anwendungsfelder in gleicher Tiefe zu analysieren. Auf Grund der großen Bedeutung liegt der Schwerpunkt dieser Studie auf Anwendungen im betriebswirtschaftlichen Umfeld und kann viele weitere Themen nur am Rande streifen, wie zum Beispiel Gesundheitswesen oder Verkehrstelematik.

Das Internet wird in den kommenden Jahren weiter an Bedeutung gewinnen. Viele Anwendungen im privaten Bereich werden in Zukunft über das Internet abgewickelt werden. Dem E-Commerce werden enorme Wachstumsraten zugesprochen. Es zeigt sich, dass das Internet vielfach zu einer Unterstützung traditioneller Geschäftsmodelle, nicht jedoch zu einer Ablösung derer führen wird. So nutzen es beispielsweise Bücherläden und Reisebüros als eine zusätzliche Kommunikations- und Handelsplattform. Auch werden in Zukunft Besuche von virtuellen Museen und realen Veranstaltungen im Internet zunehmen; doch können sie die Sinneseindrücke der realen Welt in absehbarer Zeit nicht vermitteln. Im geschäftlichen Bereich wird das Internet in allen Branchen an Bedeutung gewinnen. Es entwickelt sich zu der wesentlichen Infrastruktur für die Abwicklung von Geschäftsprozessen. Jedoch zeigt sich auch im B2B-Bereich, dass der persönliche Kontakt zwischen den Menschen nicht durch das Internet ersetzt werden kann. Die Möglichkeit, über das Internet neue Kunden sowie Zulieferer und Kooperationspartner zu finden, wird sich in Zukunft weiter entwickeln, doch müssen Verhandlungen mit den entsprechenden Entscheidungsträgern auch weiterhin persönlich geführt werden. E-Government wird in den kommenden Jahren einen Aufschwung erfahren. Dennoch waren die

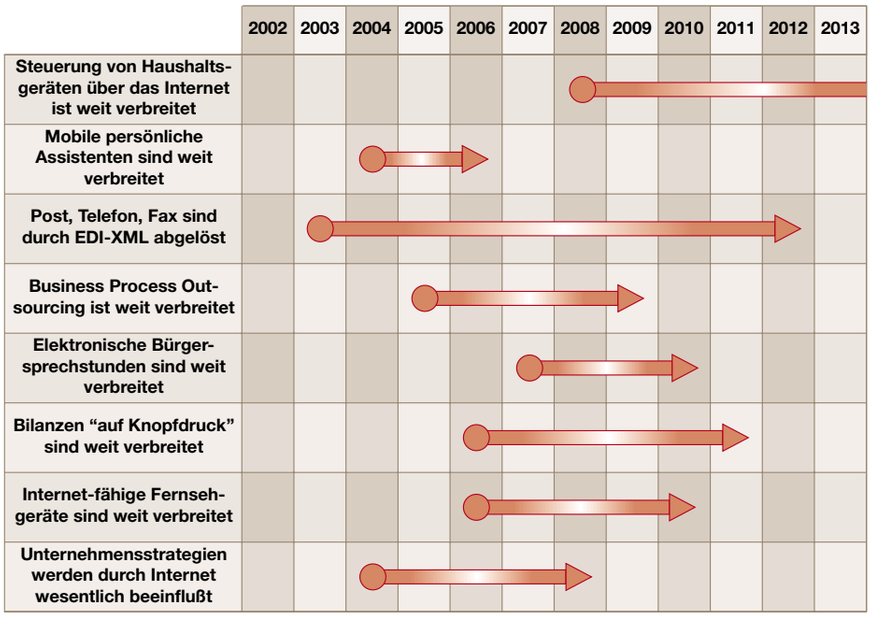



Abbildung 3.5: Verschiebungen ausgewählter Prognosen im Anwendungsbereich

Experten im Vergleich zur Vorgängerstudie zurückhaltender mit ihren Prognosen bezüglich der Entwicklungsgeschwindigkeit. Die weite Verbreitung von Aufgaben des E-Government wie elektronische Bürgersprechstunden, elektronische schwarze Bretter und elektronische Informationsveranstaltungen sehen sie statt in vier erst in sieben Jahren (vgl. Abbildung 3.5).

Schon heute verbreiten sich Micro-Chips und Netzwerktechnik in immer mehr Alltagsgegenständen. Sie ermöglichen die „intelligente" Vernetzung unterschiedlichster Geräte, ganzer Gebäude und Inneneinrichtungen. Die Einschätzung der Experten hinsichtlich der Steuerung von Haushaltsgeräten über das Internet hat sich gegenüber der Vorgängerstudie deutlich nach hinten verschoben: Sie erwarten eine weite Verbreitung dieser Anwendung nicht mehr innerhalb der nächsten zehn Jahre (vgl. Abbildung 3.5). Näher ist dagegen der breite Einsatz von zentralen Servern für den jederzeitigen Zugriff auf eigene Dateien, ebenso, wie multifunktionale und sehr einfach zu bedienende Endgeräte (z.B. PDAs (Personal Digital Assistant)).

Diese ermöglichen auch die Nutzung mobiler Dienste, deren Bedeutung in den nächsten Jahren weiter zunimmt, aber auf lange Sicht wohl stagnieren wird, da die Sprachtelefonie, trotz neuer Anwendungen wie ortsabhängigen Diensten und nachladbaren Softwaremodulen, weiterhin dominant bleiben wird. Zwei Jahre später als in der Studie 2000 prognostiziert, erwarten die Experten die weite Verbreitung mobiler persönlicher Assistenten (vgl. Abbildung 3.5). Obwohl langfristig eine mobile Geräteklasse (z.B. durch Konvergenz von Smartphones und PDAs) bei vielen alltäglichen Aufgaben elektronische Unterstützung bieten werden, ist in den nächsten zehn Jahren nicht zu erwarten, dass sie dabei Papier vollständig aus dem Alltag verdrängen.

Neben dem Einsatz zur persönlichen Kommunikation, unterstützen IuK-Systeme zunehmend das Management von Unternehmen durch Bereitstellung und Auswertung umfangreicher Informationsquellen. Aber auch in der Produktion spielt IuK-Technologie bei Simulationen, automatischen Fertigungsanlagen, kundenindividuellen Produkten und der Fernwartung weiterhin eine zunehmende Rolle. So ist zu erwarten, dass in spätestens zehn Jahren ein Großteil kritischer inner- und zwischenbetrieblicher Geschäftsprozesse voll automatisiert abläuft. Hinsichtlich der hier bedeutenden Schlüsseltechnologie XML (Extensible Markup Langua-

ge) [XML 99] sind die Experten aber gegenüber der letzten Studie deutlich pessimistischer, denn sie erwarten eine Ablösung von herkömmlichen Geschäftsverkehr durch EDI-XML erst 2012 (vgl. 3.5). Allerdings ist auch eindeutig, dass XML gegenüber alternativen Formaten dominieren und der darauf aufbauende ebXML-Standard EDIFACT ablösen wird. Für den geschäftlichen Einsatz wird er auch bedeutender als andere Web Services Standards werden. Bei der elektronischen Geschäftsabwicklung sind in den nächsten Jahren Supply Chain Management (SCM) und Customer Relationship Management (CRM) als die wichtigsten Bereiche zu sehen, gefolgt von ERP-Systemen und Data Warehousing, EDI und Web Services. Überraschenderweise spielt die in den letzten Jahren viel diskutierte EAI (Enterprise Application Integration) eine vergleichsweise geringe Rolle in der künftigen IuK-Systemlandschaft eines Unternehmens.

IuK-Systeme beeinflussen deutlich die Entwicklung von Organisationsstrukturen und führen zu einer weiteren Modularisierung und Spezialisierung von Unternehmen. In der Folge nehmen Telekooperationen zwischen Unternehmen weiter zu und Intermediäre wie Kooperationsbörsen, elektronische Marktplätze und neue Vertriebswege verändern alt bekannte Branchenstrukturen. Diese Entwicklungen führen zu zunehmend virtualisierten Unternehmen. Allerdings wird es erst in vielen Jahren weit verbreitet sein, über standardisierte Schnittstellen flexibel und schnell neue Unternehmensverbünde zusammenzusetzen. Ein heute bereits gut beobachtbarer Vorbote derartiger Entwicklungen ist das zunehmende Business Process Outsourcing, welches die Experten allerdings erst für 2009 als weit verbreitet einschätzen, eine Verschiebung gegenüber der Studie 2000 um vier Jahre (vgl. Abbildunng 3.5).

Die unterstützenden Möglichkeiten des Internets für traditionelle Geschäftsmodelle zeigen sich auch im Bankenbereich. Finanzdienstleister nutzen in fünf Jahren das Internet für Corporate-Finance-Aktivitäten. Sie treten gegenüber den Kunden als virtuelle Leistungsanbieter auf, um mit Hilfe von Partnerunternehmen sämtliche Dienstleistungen aus einer Hand anzubieten. Das Filialbanksystem wird aber nicht durch Online-Banking abgelöst werden. Ebenso wenig werden elektronische Zahlverfahren in Zukunft das Kleingeld in Zukunft ersetzen, obgleich sich ihr Stellenwert in den kommenden Jahren erhöhen wird. In sieben Jahren werden elektronische Zahlungssysteme für Kleinstbeträge weit verbreitet sein. Die Micropayment-Systeme nehmen ständig an Bedeutung zu und werden sich zusammen mit den Kreditkarten zu den wichtigsten Zahlverfahren entwickeln. In fünf Jahren, so prognostizieren die Experten über die künftigen Abrechnungsverfahren, wird das Leasen oder Mieten von Software weit verbreitet sein. In der Vorgängerstudie wurde eine Verbreitung von E-Reporting bereits in drei Jahren erwartet. Die Möglichkeit eines Unternehmens jederzeit Bilanzen automatisch zu generieren erwarten dagegen die Experten der vorliegenden Studie erst in acht Jahren (vgl. Abbildung 3.5).

Die Medien-, Informations- und Kommunikationsmärkte werden in Zukunft immer weiter konvergieren. Damit geht auch die Konvergenz der Endgeräte einher. So werden in sieben Jahren internetfähige Fernsehgeräte weit verbreitet sein. Die Experten der Studie 2000 hatten diese Entwicklung schon in drei Jahren erwartet (vgl. Abbildung 3.5). Internetfähige Fernsehgeräte führen jedoch nicht dazu, dass das klassische Fernsehen durch interaktives Fernsehen und Video-on-Demand abgelöst wird. Dagegen werden in sieben Jahren analoge Produktionsformen von Medieninhalten vollständig durch digitale Techniken ersetzt sein. Multimedia und Virtual Reality werden künftig für Weiterbildungsangebote, Produktpräsentation und Marketingaktivitäten eingesetzt werden. Allerdings erwarten die Experten nicht, dass virtuelle Räume wie digitale Wohnzimmer oder Fantasiewelten Verbreitung in der Freizeitgestaltung finden.

Fragen zu Rechtemanagement und Digital Rights Management (DRM)-Systemen sind in dieser Studie neu hinzugefügt worden. Es zeigt sich, dass die Verbreitung von DRM-Systemen von den Experten in naher Zukunft erwartet wird. Watermarkingverfahren werden nach Aussagen der Experten in drei Jahren weit verbreitet sein, die identitätsgebundene Nutzung von Content in fünf Jahren. Die Verankerung von DRM-Mechanismen in Betriebs-

systeme und Hardware wird in zehn bzw. sieben Jahren verbreitet sein. Die Experten haben jedoch die technische Wirksamkeit der Sicherheitssysteme äußerst kritisch diskutiert. Ein Umstand, der auch zu Hemmnissen bei der Verbreitung von Online-Wahlen führt. Zwar prognostizieren die Experten, dass in fünf Jahren sichere Verfahren für Online-Wahlen verfügbar sein werden, doch wird ein leichter Bedeutungszuwachs dieser Verfahren gerade für politische Wahlen erst in über zehn Jahren erwartet.

In der Vorgängerstudie haben die Experten erwartet, dass bereits in einem Jahr das Internet die strategische Unternehmensplanung weit verbreitet beeinflusst. In der vorliegenden Studie dagegen hat sich die Einschätzung der Experten um vier Jahre nach hinten verschoben (vgl. Abbildung 3.5). Die Entwicklungen in der Informations- und Kommunikationsindustrie wirken sich auch in Zukunft bedeutend auf die Entstehung neuer Geschäftsmodelle und Märkte aus und haben somit Einfluss auf die Unternehmensstrategie. Allerdings sind nach der anfänglichen Euphorie bei den Technologiewerten auf den Kapitalmärkten auch die Aussagen der Experten zu realistischeren Werten zurückgekehrt. Neue Märkte werden sich durch die Digitalisierung und den Trend zur Dienste- und Komponentenorientierung entwickeln. In drei Jahren wird es einen globalen Markt für spezialisierte Softwarekomponenten geben. Bereits in sechs Jahren halten es die Experten für denkbar, dass Geschäftsmodelle weit verbreitet aus einzelnen Komponenten realisiert werden. Dienstanbieter, Application Service Provider, werden in fünf Jahren weit verbreitet ihre Software zur Verfügung stellen. Ebenfalls in fünf Jahren wird der Handel mit personenbezogenen Daten weit verbreitet sein.

## 3.7 Technologische Meilensteine

Informations- und Kommunikationstechnologien sind vor dem Hintergrund der in der Studie diskutierten übergreifenden Trends rasanten Entwicklungen unterworfen. Die kurz-, mittel- und langfristigen Einschätzungen der Experten über zukünftige technologische Entwicklungen beziehen sich deshalb nicht nur auf die Beurteilung der Trends selbst, sondern gehen in vielen Bereichen auch in Detailprognosen. Die dabei von den Befragten identifizierten technologischen Meilensteine werden in den einzelnen Kapiteln abgeleitet. Einige dieser Meilensteine sind im Kapitel 10 auf einer Zeitskala über die nächsten zehn Jahre angeordnet.

# 4 Einleitung

In vielen Bereichen des täglichen Lebens, auch im privaten Bereich, ist eine immer weiter fortschreitende Verbreitung von Informations- und Kommunikationstechnologie zu beobachten. Die neu entstehenden Systeme und Anwendungen fordern und fördern wiederum Neu- und Weiterentwicklungen in den verschiedenen Technologiebereichen. Diese wechselseitige Beeinflussung führt zu einem hohen Innovationstempo in der gesamten IuK-Technik. Die schnellen Veränderungen bringen eine hohe Unsicherheit mit sich, denn je ungenauer die Vorstellungen von der zukünftige Entwicklung, desto höher ist das Risiko, beispielsweise bei Investitionsentscheidungen von Unternehmen. Prognosen spezifischer technologischer Entwicklungen in den Gebieten Information und Kommunikation und die Identifikation neuer Anwendungsgebiete sind unter diesen Voraussetzungen von ganz erheblicher Bedeutung. Wie schon die erste Auflage, die im Jahr 2000 erschien [SETIK 00], trägt die vorliegende erweiterte und vollständig überarbeitete Studie dieser Notwendigkeit Rechnung.

Die grundsätzliche Schwierigkeit bei der Identifikation und Diskussion von Zukunftstrends in den IuK-Technologien sind die verschiedenen Ebenen, auf denen sich diese Entwicklungen vollziehen; sie bedingen sich gegenseitig und dürfen deshalb nicht isoliert voneinander betrachtet werden: grundlegende Techniken wie Speicher, Netzen oder Displays bestimmen die Art und Verbreitung ihrer verschiedenen Anwendungen. Diese Anwendungen wiederum beeinflussen, oft unbemerkt, unser tägliches Leben in Arbeit und Freizeit. Die Kette von Einflüssen wirkt aber auch in die Gegenrichtung: neue Anforderungen an die Technik entstehen aufgrund neuer, spezifischer Produkte, deren Nachfrage oft genug ihren Ursprung in veränderten Lebensgewohnheiten hat. Somit sind neue Entwicklungen zum einen technologieinduziert, zum anderen werden sie durch Markt-Bedürfnisse vorangetrieben.

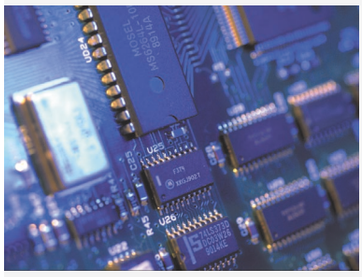
Aufgrund dieser Wechselwirkungen gliedert sich die Studie in einen Technologie- und einen Anwendungsteil. Der Technologieteil besteht aus den Teilbereichen Rechnertechnik, Rechnernetze und -kommunikation, Datenbanken und Wissensmanagement sowie Softwaretechnik. Der Anwendungsteil spannt den oben beschriebenen Bogen von spezifisch technikgetriebenen Entwicklungen, beispielsweise im Bereich der Mobiltelefonie, hin zu Veränderungen im sozialen und beruflichen Leben. Eine wichtige Rolle in der Informations- und Kommunikationstechnik haben in den letzten Jahren Fragen der Sicherheit bei Austausch und Verarbeitung von Informationen gespielt. Aufgrund der Bedeutung der Entwicklungen in diesem Bereich enthält die vorliegende Studie ein eigenständiges Kapitel IT–Sicherheit, das die aktuellen und zukünftigen Sicherheitstechnologien umfassend und detailliert zugleich diskutiert.

Diese zahlreichen Facetten der Informations– und Kommunikationstechnik müssen beleuchtet werden, um einzelne Entwicklungen in einen Gesamtkontext einordnen zu können. Um diesem Anspruch gerecht zu werden, muss eine solche Studie von einem interdisziplinär ausgerichteten Team erstellt werden, das Wissen und Erfahrung sowohl aus dem Bereich der Informatik als auch aus dem Bereich der Betriebs- und Volkswirtschaft einbringt. Durch die Kooperation des Bundesamtes für Sicherheit in der Informationstechnik mit der Technischen Universität München, der Ludwig-Maximilians-Universität München und der Sirrix AG, die nach Projektbeginn die Sicherheitsfragen (Kapitel 7 und Abschnitte 3.1, 8.2.1, 8.2.8 und 9.8) bearbeitete, ist diese Interdisziplinarität gegeben.

Eine nicht minder große Bedeutung für die Aussagekraft von Trendstudien hat die inhaltliche und methodische Fundierung. Da sich die Fortschritte bei den Technologien und ihren Anwendungen so

schnell und in so viele, teils gegenläufige Richtungen vollziehen, muss eine solche Untersuchung sehr viel Wissen bündeln. Die übergreifenden Trends wurden deshalb anhand zahlreicher Informationsquellen identifiziert. Experteninterviews, Workshops mit Unternehmen und akademischen Forschungsgruppen sowie umfassende Literaturarbeit erlaubten eine Konsolidierung der bestehenden Erkenntnisse. Die Evaluation der einzelnen Entwicklungen oblag schließlich einer Gruppe von 162 unabhängigen Experten. Bei der Gestaltung der Fragebögen wurde auf die Details einzelner spezifischer Technologien genauso Wert gelegt wie auf ihre Einordnung in einen Gesamtkontext. So kann ein umfassendes Bild von der Zukunft der Informations- und Kommunikationstechnik gezeichnet werden, weil Zusammenhänge, Querbezüge und die Triebkräfte der beschriebenen Entwicklungen identifiziert und erklärt werden können.

Das folgende Kapitel beschreibt detailliert das methodische Vorgehen, das zu den Ergebnissen führte, die in den Kapiteln 7 (IT-Sicherheit), 8 (Technologien) und 9 (Anwendungen) ausführlich erläutert werden. In Kapitel 6 werden die übergreifenden Trends vorgestellt, die für alle untersuchten Bereiche relevant sind und die die Einordnung einzelner Ergebnisse in einen Gesamtkontext erlauben.



# 5 Vorgehensweise

Ziele der vorliegenden Studie, wie schon der Vorgängerstudie des Jahres 2000 [SETIK 00], sind die Ermittlung und Beschreibung zukünftiger Entwicklungen in den Informations- und Kommunikationstechnologien der nächsten zehn Jahre. Dabei geht es ausschließlich um eine Evaluation von Technologieentwicklungen und deren Anwendungen, aber nicht um Marktprognosen für einzelne Technologien oder gar Unternehmen. Eine Ableitung von Marktchancen bestimmter Produkte oder Produktgruppen ist zwar anhand der Ergebnisse möglich, ist aber nicht der Anspruch der vorliegenden Studie.

Aufgrund des äusserst weit gefassten Untersuchungsgegenstands war es notwendig, in mehreren Schritten das Themengebiet zu strukturieren und in Teilbereiche zu gliedern. Die Themenbereiche Sicherheit, Technologien und Anwendungen stellen die gröbste Gliederungsebene dar. Der Technologiebereich selbst wurde weiterhin in die Kapitel Rechnertechnik, Rechnernetze, Datenbanken sowie Softwaretechnik gegliedert. In einem nächsten Schritt wurden anhand einer intensiven Literaturarbeit diejenigen Themenfelder identifiziert, die sich durch eine besondere Relevanz in den jeweiligen Teilen auszeichnen. Diese Themenfelder stellen die einzelnen Abschnitte in den Bereichen dar.

Die Strukturierung und Detaillierung einzelner Themenfelder erfolgte in einem iterativen Prozess zahlreicher Befragungen von Experten aus Wissenschaft und Praxis. Diese als Delphi-Verfahren bekannte Iteration von Interviews hatte zwei Ziele: zum einen wurden übergreifende Trends definiert, die für alle untersuchten Bereiche gelten, zum anderen wurden in jedem einzelnen Themengebiet spezifische Thesen formuliert, die eine detaillierte Analyse dieses Themenfeldes erlauben. Damit werden in jedem Bereich einzelne Trends untersucht, die einem oder mehreren übergreifenden Trends zugeordnet werden können. Das umfangreiche Delphi-Verfahren zur Generierung der Themen wurde gewählt, da Gruppenbewertungen aufgrund der größeren Informationsmenge qualitativ besser sind als individuelle Bewertungen. Jeder an diesem Verfahren teilnehmende Experte gibt dabei in der ersten Runde seine individuellen Prognosen ab, wird aber in den nachfolgenden Runden systematisch mit den Prognosen des gesamten Panels konfrontiert. [HSG 94] und andere Arbeiten zeigen, dass die Delphi-Methode als Prognoseverfahren für die Bewertung komplexer Themengebiete zu einer vergleichsweise hohen Ergebnisqualität führt. Dieses Verfahren wurde schon zur Erstellung der Studie 2000 [SETIK 00] verwendet. Die quantitativen Ergebnisse und die zahlreichen Anmerkungen der damals teilnehmenden Experten gaben ebenfalls wichtige Impulse bei der Auswahl der Themen und Thesen dieser Studie.

Das Resultat der Interviews und der parallel dazu durchgeführten Literaturarbeit waren übergreifende Trends und - für die jeweiligen Teilbereiche der Studie - spezifische Themenfelder und Thesen. Zur Validierung der Thesen wurde schließlich eine Fragebogenaktion durchgeführt. Mit diesem Vorgehen entstand keine von bestehenden Erkenntnissen losgelöste Studie, sondern es gelang, bestehendes Wissen umfassend zu nutzen und dieses im Rahmen einer Trendabschätzung zu bewerten.

Die Ausprägungen der übergreifenden Trends innerhalb der einzelnen Technologiefelder werden in jedem Kapitel anhand einer Grafik verdeutlicht. Abbildung 5.1 zeigt, am Beispiel des Themenbereiches Softwaretechnik, welche übergreifenden Trends relevant sind und welche Ausprägungen in Form spezifischer Trends sie dort besitzen.

Interessant sind in dieser Studie vor allem die Verschiebungen der Ausprägungen und der Relevanz einzelner übergreifender Trends im Vergleich zur Vorgänger-

studie. Viele der dort untersuchten Thesen und spezifischen Trends wurden auch in der vorliegenden Studie wieder thematisiert werden, um die damaligen Prognosen vergleichen und daraus Rückschlüsse auf die Entwicklungen während der letzten drei Jahre ziehen zu können. Wann immer innerhalb der Texte auf die „Vorgängerstudie", „Studie 2000" oder „letzte Studie" verwiesen wird, werden Ergebnisse und Prognosen aus [SETIK 00] referenziert. Um die Expertenerwartungen nicht zu beeinflussen oder gar zu verzerren, wurde den Befragten die Vorgängerstudie nicht explizit zur Verfügung gestellt.

Der nachfolgende Abschnitt beschreibt, welche Bereiche als wesentlich für den Informations- und Kommunikationsbereich ermittelt wurden. Daran anschließend wird die Methodik beschrieben, die bei der Strukturierung der Bereiche in Trends sowie bei der Identifikation der Thesen angewendet wurde. Abschließend wird dargestellt, wie bei der Befragung vorgegangen wurde, um die aufgestellten Thesen zu evaluieren und wie die Auswertung der Antworten erfolgte.

## 5.1 Auswahl der untersuchten Themenbereiche

Technischer Fortschritt resultiert nie allein aus der Existenz neuer technologischer Möglichkeiten. Denn technologische Innovationen sind nur ein Treiber des Fortschritts *(*Technology-Push*)*, die zweite unbedingt nötige Kraft sind neue Bedürfnisse des Marktes *(*Market-Pull*)*. Abbildung 5.2 illustriert diese Wechselwirkungen. So löste die Anwendung neuer Technologien immer wieder weitere technologische und organisatorische Innovationen aus. Dieser Kreislauf, verbunden mit dem nahezu exponentiellen Wachstum der Informations- und Kommunikationstechnologien, führt zu einem Spiraleffekt, der dramatische Änderungen in Wirtschaft, Gesellschaft und Politik hervorrufen kann [Nefi 01]. Drei Gründe sprechen dafür, dass der Spiraleffekt technologisch induzierter und marktgetriebener Entwicklungen auch weiter anhalten wird:


Abbildung 5.2: Wechselseitige Beeinflussung von Markt und Technologien

- Die untersuchten und im folgenden beschriebenen Technologiebereiche bringen weiterhin in atemberaubenden Tempo neue Entwicklungen, die bestehende Anwendungen schneller, einfacher und preiswerter machen.
- Die Nachfrage nach neuen oder weiterentwickelten Anwendungen in Unternehmen, Haushalten und allen Bereichen des Lebens ist weiter ungebrochen.
- Schon bestehende Technologien sind noch nicht von allen potenziellen Anwendern übernommen worden.

Denn entgegen dem schnellen Innovationstempo ist die technologische Ausbreitung relativ langsam. [GrYo 97] schätzen, dass es ca. 15 Jahre dauert, bis eine neue Technologie von 50% der Unternehmen eingesetzt wird.

Gerade die Auswirkungen der IuK-Technologien auf Politik und Gesellschaft werden oft unterschätzt. Aber es lässt sich beispielsweise eine hohe negative Korrelation zwischen dem Einsatz von IT in Unternehmen und dem Anteil von Routinearbeiten nachweisen [ALM 01]. [DDT 97] zeigen, dass Fabriken, die neue Informationstechnologien früher einführen, höher qualifizierte Arbeiter und Manager besitzen. Die Politik ist aufgerufen, hier die wichtigen Weichenstellungen vorzunehmen. Dies ist v.a. in der Wirtschaftspolitik nötig, immerhin ist die Produktivität im IT-Sektor in Deutschland immer noch um ca. 40% niedriger als in den USA [OECD 00]. Eine detaillierte Analyse der Wechselwirkungen zwischen Gesellschaft, Wirtschaft und

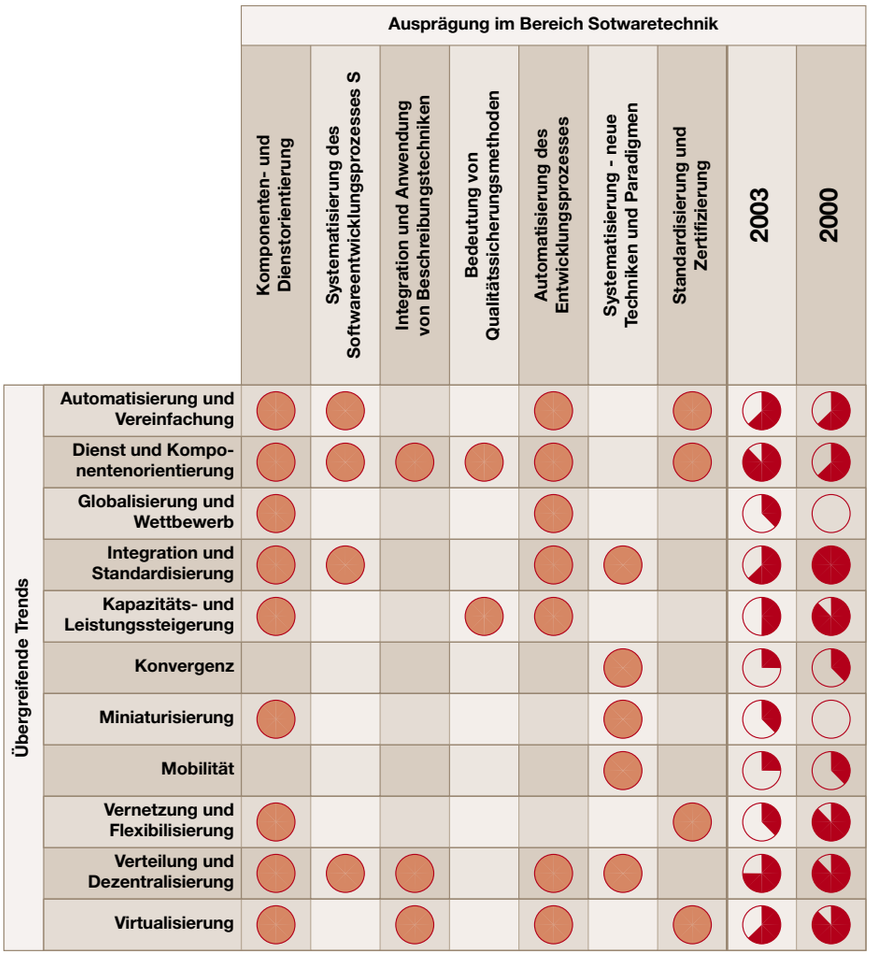



Abbildung 5.1: Verbindung von übergreifenden und spezifischen Trends am Beispiel des Technologiebereiches Softwaretechnik

Staat ist nahezu unmöglich. Deshalb wurden im Rahmen dieser Studie spezifische Bereiche ausgewählt, für die die wichtigsten Technologie- und Anwendungstrends aufgezeigt wurden.

Die rasante Entwicklung der Rechnertechnik hat in den vergangenen Jahren zu einem deutlichen Anstieg der Leistungsfähigkeit von Prozessoren und anderen Hardware-Bauteilen geführt. Die entsprechende Miniaturisierung ermöglichte den Einsatz von Kleinstcomputern in immer neuen Gebieten, z.B. in der Medizin. Parallel dazu stieg die Interoperabilität und die Vernetzung der Rechner. Dies spiegelt sich insbesondere im Internet wider, das mittlerweile weltweit von 500 Millionen Menschen genutzt wird [Bund 02]. Das Wachstum der Bedeutung und des Inhalts dieses Mediums scheint auf absehbare Zeit kein Ende zu nehmen, täglich werden schätzungsweise sieben Millionen neue Seiten eingestellt [Medi 02]. Aus diesem Grund ist ein besonderes Augenmerk auf Technologien im Bereich der Vernetzung und Kommunikation der Rechner zu legen. Hier ergeben sich durch die Entwicklung und den mittlerweile breiten Einsatz drahtloser Netze neue Möglichkeiten, aber auch neue Sicherheitsrisiken. Die steigende Vernetzung führte in kurzer Zeit zu Technologien, die es erlauben, auf weltweit verteilte, heterogene Informationen multimedial zuzugreifen. Dies führte wiederum zu einer Reihe von Innovationen im Bereich der Kommunikations- und Datenbanktechnologien. Somit bestand die Möglichkeit, weltweit verteilte Informationen zu erhalten und diese zu verarbeiten. Verbunden mit diesem technologischen Fortschritt hat

sich die Komplexität der zu entwickelnden Systeme erhöht. Neue oder stark an Bedeutung gewinnende Anforderungen wie Mobilität, z.B. für PDAs (Personal Digital Assistants), Verteilung oder Echtzeitfähigkeit, wie bei Steuerungssoftware für Maschinen, werden an die Systeme gestellt. Dies führt zu einem steigenden Bedarf an Methoden und Techniken zur strukturierten und systematisierten Entwicklung dieser Systeme. Parallel zu diesen technologischen Entwicklungen hat eine Sensibilisierung für sicherheitsrelevante Themen stattgefunden. Dabei darf Sicherheit nicht nur als Bestandteil einzelner Anwendungen gesehen werden, sondern muss als umfassende und übergreifende Aufgabe gesehen werden, die die Zukunft der Märkte für Informations- und Kommunikationstechnologie mitbestimmen wird.

Diese technischen Entwicklungen wirken sich auch auf die Unternehmen und das Arbeitsleben aus. So hat beispielsweise das Internet zu einer Vielzahl neuer Arbeitsfelder geführt. Der Nutzen des Internet für die Industrie steigt weiterhin enorm an, wobei die Erhöhung der Bandbreiten und die netzweite Verarbeitung von Multimedia-Daten Katalysatoren dieses Wachstums sind. Auch neue Geschäftsmodelle auf Basis mobiler Dienste sowie neue Organisationsstrukturen und Arbeitsformen werden die Geschäftswelt in Zukunft bewegen.

Um ein umfassendes Bild der Wechselwirkungen zwischen den Informations- und Kommunikationstechnologien und den Anwendungsfeldern zu zeichnen, wurde die Studie zunächst in einen Sicherheits-, einen Technologie- und einen Anwendungsbereich gegliedert. Der Technologiebereich beinhaltet dabei die Kapitel Rechnertechnik, Rechnernetze und -kommunikation, Datenbanken und Wissensmanagement und Softwaretechnik. Dabei wird auf die Wirkungszusammenhänge zwischen den technologischen Entwicklungen und spezifischen Anwendungen genauso Wert gelegt wie auf die Beschreibung bestehender und beobachtbarer Trends.

## 5.2 Ermittlung und Einschätzung von Trends und Thesen

Im Rahmen des oben beschriebenen Vorgehens wurden zunächst übergreifende Trends identifiziert, d.h. allgemeine Entwicklungen, die in vielen Bereichen der Informations- und Kommunikationstechnologien wiederzufinden sind. In den einzelnen Bereichen wurde dann wiederum nach konkreten Ausprägungen dieser globalen Trends gesucht, was zu einer Vielzahl weiterer Trends und Thesen führte. Die erarbeiteten übergreifenden Trends werden in Abschnitt 6 im einzelnen dargestellt. Darüber hinaus wird am Beginn jedes Kapitels gezeigt, in welchen Teilbereichen Ausprägungen bestimmter übergreifender Trends identifiziert werden können. Somit dienen diese Trends nicht nur als Ausgangspunkt für das methodische Vorgehen, sondern auch als „roter Faden" durch die Studie und erleichtern die Einordnung einzelner Ergebnisse in einen Gesamtkontext.

Die einzelnen Ergebnisse innerhalb der Studie schließlich sind das Resultat einer breit angelegten Fragebogenaktion bei Experten der jeweiligen Fachbereiche. Insgesamt wurden für die vorliegende Studie im Bereich IT-Sicherheit ca. 70 und für den Bereich der Technologieprognose etwa 120 Experten befragt. Durchschnittlich sind die in Fragebogenform vorgelegten Trends und Thesen dabei aufgrund des breiten Themenspektrums von jeweils ca. 40 Experten bewertet worden. Dabei wurden den Fragen zur zeitlichen Einschätzung der Entwicklungen sowie zur Einschätzung der Bedeutung bestimmter Konzepte oder Produkte in den nächsten zehn Jahren gestellt, um die ermittelten Trends und Thesen zu validieren. Die in der vorliegenden Studie beschriebenen Zukunftseinschätzungen beruhen somit auf vier wesentlichen Säulen:

- Literaturrecherche
- Expertengespräche
- Ergebnisse der Studie 2000 [SETIK 00]
- Fragebogenaktion

Die Experten, die bei der Entstehung der Studie mitgewirkt haben, stammen etwa zu gleichen Teilen aus dem wissenschaftlichen Umfeld und der Wirtschaft.

Die befragten Experten aus der Wirtschaft sind in Beratungsunternehmen, bei IT-Dienstleistern und in der Industrie (vorwiegend in den Branchen Telekommunikation, Automotive, Fertigungs- und Halbleiterindustrie) tätig. Die befragten Experten aus dem wissenschaftlichen Umfeld arbeiten sowohl an Hochschulen als auch in wissenschaftlichen Einrichtungen im Bereich der Informatik, der Betriebswirtschaft und der Elektrotechnik.

### 5.2.1 Auswertung der Fragebögen

Der Aufbau der Fragebögen ist so gestaltet, dass zeitliche Abschätzungen zur Entwicklung spezifischer Themen gegeben werden. Zu jeder dieser Fragen werden aber auch korrespondierende Aussagen über Anwendungsgebiete, notwendige Technologien oder sonstige Kommentare verlangt. Daher wurde die Auswertung der Fragebögen in zwei Phasen vorgenommen:

- **quantitative Auswertung**: Bei jeder Frage sollten quantitative Aussagen getroffen werden, z.B. bezüglich des zu erwartenden Zeithorizonts bis zum Eintreffen einer These oder bezüglich der Einschätzung der Bedeutung einer Aussage zu bestimmten Zeitpunkten. Dazu wurde ein System von Fragetypen entwickelt, die mit verschiedenen statistischen Methoden ausgewertet wurden.
- **qualitative Auswertung**: Zu jeder Frage war ausreichend Platz vorgesehen, so dass die befragten Experten qualitative Aussagen treffen und Kommentare abgeben konnten. Diese Anmerkungen wurden in die Diskussion der Ergebnisse integriert.

Zur Auswertung und graphischen Aufbereitung der quantitativen Daten wurden statistische Methoden verwendet, die im Folgenden detailliert beschrieben werden.

### 5.2.2 Statistische Methoden

Zur Darstellung der quantitativen Ergebnisse der Auswertung wurden Boxplots und Trendlinien verwendet. Aufgrund der geeigneten Auswahl der Experten wurde auf eine Gewichtung der Expertenmeinungen in Abhängigkeit von der individuellen Vertrautheit mit dem jeweiligen Fachgebiet verzichtet. Die folgende Beschreibung der angewandten statistischen Analyseverfahren gliedert sich nach den drei Fragetypen, die im Fragebogen verwendet wurden.

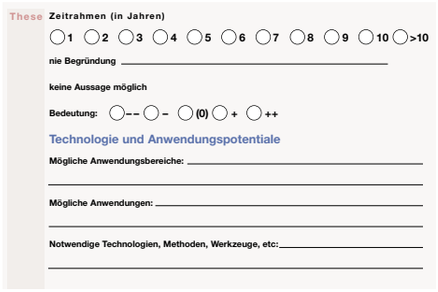



Abbildung 5.3: Fragenschema von Typ 1-Fragen

#### 5.2.2.1 Typ 1-Frage (Bewertung einer These)

Typ 1-Fragen ermöglichten es den Befragten, ein Zeitintervall anzugeben, in dem erwartet wird, dass die gegebene These erstmals zutreffen wird. Die möglichen Zeitintervalle reichten hierbei von „heute" bis zu einem Zeitpunkt in zehn Jahren. Darüber hinaus war es möglich anzugeben, dass die These erst in mehr als zehn Jahren zutreffen bzw. die These niemals zutreffen wird (vgl. Abbildung 5.3).

Zur Veranschaulichung und Analyse der hier erzielten Ergebnisse wurden Boxplot-Diagramme gewählt (siehe Abbildung 5.4). Durch einen Boxplot wird die Verteilung der Daten in einem bestimmten Wertebereich analysiert. Dazu werden die in den Fragebögen genannten Werte der Größe nach sortiert und damit in eine Rangfolge gebracht. Entlang der Werteachse wird ein Rechteck (Box) gezeichnet, dessen Inhalte wie folgt bestimmt werden: Der Median, der durch den mittleren senkrechten Strich innerhalb der Box gekennzeichnet ist, wird dadurch bestimmt, dass genau 50 Prozent der genannten Werte unterhalb und 50 Prozent oberhalb dieser Nennung liegen. Damit besitzt der Median den „mittleren Rang", der in dieser Studie auch häufig mit als Durchschnitt bezeichnet wird. Beispielsweise ist das bei einer

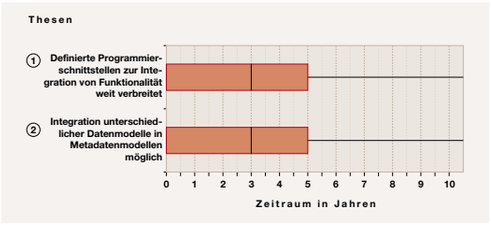



Abbildung 5.4: Boxplot zur Darstellung der Ergebnisse von Typ 1-Fragen

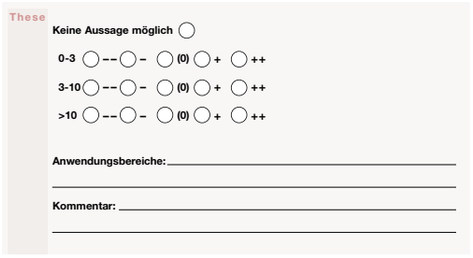



Abbildung 5.5: Fragenschema von Typ 2-Fragen

Stichprobe mit 100 unterschiedlichen Elementen das Element mit Rang 51. Für die untere Grenze wird ein Element so aus der Rangfolge ausgewählt, daß noch 25 Prozent aller Werte unter diesem Wert liegen. Entsprechend wird die Obergrenze so gewählt, daß noch 25 Prozent aller Werte über der gewählten Grenze liegen, im Beispiel also das Element mit der Rangnummer 75. Die Grenzen der Boxen werden als 25 Prozent- bzw. 75 Prozent-Quantil bezeichnet. Damit entsteht eine Box, die durch ihre Ausdehnung und Lage anzeigt, in welchem Wertebereich 50 Prozent der Daten liegen [Sach 88].

Aus der Breite der Box ist leicht erkennbar, wie stark die angegebenen Daten divergieren. Je breiter die Box, desto uneiniger waren sich die Befragten. Die Lage des Medians relativ zu den Grenzen der Box gibt an, wie stark die Verteilung der Daten von der symmetrischen Normalverteilung abweicht. Die Streuung der Nennungen lsst sich auch an den sogenannten Whiskern ablesen. Diese sind durch die Endpunkte der schwarzen Linien auf beiden Seiten der Boxen gekennzeichnet und stellen die 5 Prozent- und 95 Prozent-Quantile dar.

Alle Boxplots verwenden, wie die Fragebögen auch, eine Zeitskala von 0 bis 10 Jahren. Somit kann es vorkommen, dass Boxen nur „angeschnitten" oder auch gar nicht sichtbar sind. Dadurch wird verdeutlicht, dass der von den Experten angegebene Zeitraum bzw. ein oder mehrere Quartile außerhalb des gegeben Zeitrahmens liegen.

Wurden in einem Teilbereich mehrere Typ 1-Fragen gestellt, so wurden die sich aus den Antworten ergebenden Boxplots in ein Diagramm aufgenommen. Damit ist der direkte Vergleich von Teilaussagen möglich. Um die Zuordnung von im Text genannten Ergebnissen zu einzelnen Boxplots zu vereinfachen, werden die Boxen innerhalb eines Diagrammes nummeriert. Die Referenzierung auf eine Box wird im Text mit eingekreisten Zahlen (z.B. ①) vorgenommen.

#### 5.2.2.2 Typ 2-Frage (Bewertung einer Bedeutung)

Bei dieser Art der Fragestellung sollte angegeben werden, welche Bedeutung einer gegebenen Technologie innerhalb der nächsten drei Jahre, innerhalb der nächsten drei bis zehn Jahre sowie in mehr als zehn Jahren beigemessen wird. Hierzu standen insgesamt fünf Bedeutungsklassen von „- -" (sehr geringe Bedeutung) bis „++" (sehr große Bedeutung) zur Verfügung (vgl. Abbildung 5.5).

Zur Veranschaulichung der hierbei erzielten Ergebnisse wurde folgendermaßen vorgegangen: In jedem Zeitintervall wurde der Mittelwert aller eingegangenen Antworten bestimmt. Hierzu wurden der Bedeutungsklasse „- -" ein Wert von -2 zugeordnet, der Bedeutungsklasse „0" ein Wert von 0 und der Bedeutungsklasse „++" ein Wert von +2. Für „-" bzw. „+" ergeben sich entsprechend die Werte „-1" bzw. „+1". Somit war es möglich, das arithmetische Mittel der eingegangenen Antworten zu bestimmen und in einem Koordinatensystem einzutragen. Die Werte für die drei Zeitintervalle wurden mittels Spline-Interpolation miteinander verbunden. Spline-Funktionen bilden gleitende Durchschnitte und sorgen so für eine Glättung der Werte, sodass sich der langfristige Trend der Bedeutung einer speziellen

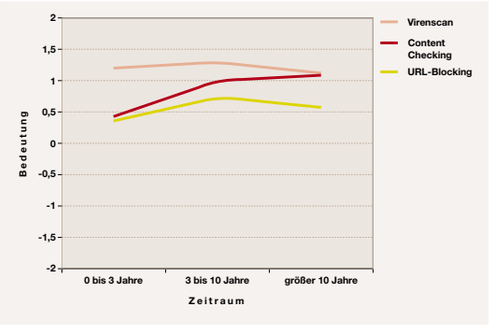



Abbildung 5.6: Trendlinien zur Veranschaulichung der Ergebnisse von Typ 2-Fragen

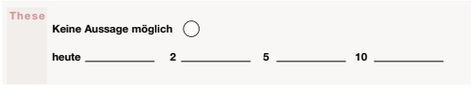



Abbildung 5.7: Fragenschema von Typ 3-Fragen

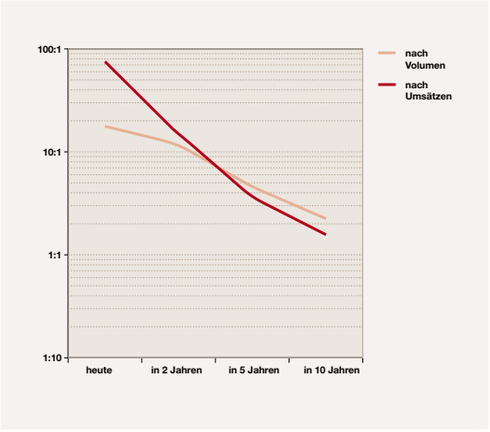



Abbildung 5.8: Trendlinien zur Veranschaulichung der Ergebnisse von Typ 3-Fragen

Technologie erkennen lässt (siehe Abbildung 5.6). Bei Fragen, bei denen mehrere vergleichbare Technologien zur Auswahl standen, wurden deren jeweilige Trendkurven in einem Koordinatensystem zusammengefasst, um die relative Bedeutung der einzelnen Technologien zueinander darzustellen.

#### 5.2.2.3 Typ 3-Frage (Frage nach Zahlenwerten)

Fragen dieser Art dienten dazu, eine quantitative Einschätzung einer bestimmten Entwicklung „heute", in zwei, in fünf und in zehn Jahren zu erhalten (vgl. Abbildung 5.7). Dabei wurde nach absoluten Werten gefragt, wie beispielsweise den verwendeten Bandbreiten. Um schließlich stabilere Aussagen zu erhalten, wurden aus den absoluten Werten die Zuwächse ermittelt, so dass auf relative und somit stabilere Größen zurückgegriffen werden konnte. Die relativierten Werte wurden schließlich über Splines miteinander verbunden, was eine einfache und intuitive grafische Darstellung ermöglicht (vgl. Abbildung 5.8).

#### 5.2.2.4 Typ 4-Frage (Frage nach Zuordnungen)

Über diese Art der Fragestellung kann eine Zuordnung getroffen werden zwischen unterschiedlichen Betrachtungsmerkmalen. Wie in der Abbildung 5.9 dargestellt wird, kann beispielsweise evaluiert werden, welche der auf der Ordinatenachse angetragenen Technologien in den auf derAbszissenachse angegebenen Entwicklungsphasen der Softwareerstellung besonders geeignet sind. Die Zuordnung der Werte auf der Abszisse und der Ordinate ermöglicht die Darstellung der Ergebnisse in einer Matrix.

Bei dieser Art der Fragestellung konnten die befragten Experten jeweils angeben, ob eine dieser Zuordnungen zutrifft oder nicht. Die Ergebnisse in den jeweiligen Feldern der Matrix ergaben sich schließlich aus dem Quotienten der Werte der angegebenen und aller möglichen Zuordnungen. Das zu diesem Ergebnistyp gehörende Fragenschema entspricht im Wesentlichen der gezeigten Ergebnismatrix, wobei statt der jeweiligen Ergebnisse Platzhalter vorhanden sind, um die spezifische Zuordnung zu markieren.

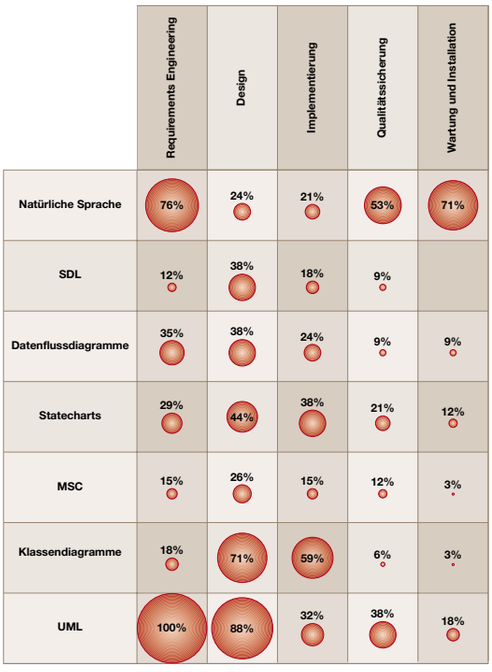


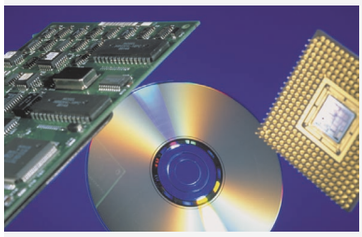

Abbildung 5.9: Häufigkeiten zur Veranschaulichung der Ergebnisse von Typ 4-Fragen

## 5.3 Hinweise für den Leser

In den folgenden Kapiteln und Abschnitten werden eine Reihe von Abkürzungen verwendet. Diese werden bei der ersten Nennung pro Kapitel aufgelöst und danach als bekannt vorausgesetzt. Im Glossar findet sich in den meisten Fällen auch eine kurze Erklärung.

Um die Lesbarkeit der Studie zu erhöhen, werden nicht alle Thesen mit der Vorgängerstudie [SETIK 00] verglichen. Dieser Vergleich findet nur dann statt, wenn sich die Thesen auch tatsächlich vergleichen lassen oder sich sinnvolle Aussagen aus dem Vergleich ableiten lassen (wenn es sich z.B. um einen neuen Trend handelt). In der Zusammenfassung (Kapitel 3) ist zu jedem Abschnitt eine Grafik mit den wichtigsten Verschiebungen relativ zur Vorgängerstudie eingefügt. Dabei ist eine Verschiebung rot gekennzeichnet, wenn die Experten durchschnittlich von einem späteren Eintreffen der Entwicklung ausgehen. Eine gelbe Markierung kennzeichnet eine stabile Prognose. Wenn die Experten durchschnittlich von einer optimistischeren Entwicklung ausgehen, wird dies durch einen grünen Pfeil dargestellt.

Jedes Kapitel enthält in der Einleitung eine Tabelle über die Ausprägungen der übergreifenden Trends (siehe Kapitel 6) im jeweiligen Themenbereich und wie diese mit den themenspezifischen Trends in dieser und der Vorgängerstudie korrelieren (siehe z.B. Abbildung 5.1). Der Füllungsgrad der Kreisgrafiken, die in den jeweils zusammenfassenden Spalten (Spaltentitel 2000 und 2003) zu finden sind, dient dazu, diesen Zusammenhang für die beiden Studien darzustellen: Je mehr Segmente des Diagramms ausgefüllt sind, desto mehr übergreifende Trends beeinflussen die jeweilige These im Themenbereich. Aus den direkten Vergleichen beider Kreisdiagramme lassen sich dann entsprechende Verschiebungen ableiten. So ist beispielsweise aus Abbildung 5.1 ersichtlich, dass Dienst- und Komponentenorientierung als übergreifender Trend im Themenfeld Softwaretechnik an Einfluß gewonnen haben und Miniaturisierung als neuer Trend identifiziert werden kann.



# 6 Übergreifende Trends

Informations- und Kommunikationstechnologien spielen in immer mehr Bereichen des täglichen Lebens eine große Rolle. Allerdings erschwert die hohe Innovationsgeschwindigkeit die Erstellung treffender Aussagen über ihre weitere Entwicklung und künftige Bedeutung. Für viele strategische Entscheidungen ist es aber unabdingbar, zumindest „Eckpfeiler" für die Zukunft zu skizzieren, um verschiedene Szenarien erstellen zu können. Durch alle spezifischen Trends in den Sicherheits-, Technologie- und Anwendungsbereichen dieser Studie, ziehen sich übergreifende Trends, die im weiteren als derartige Eckpfeiler dienen, um als Analyseraster einen vergleichenden Überblick über die spezifischen Trends zu ermöglichen. Zur Identifizierung dieser Trends dienten insbesondere Experteninterviews, ergänzt um weitere Literaturrecherchen.

Der Beginn eines jeden Teilbereiches beschreibt kurz, in welchen spezifischen Trends sich die übergreifenden Trends auswirken. Eine Tabelle fasst die Ausprägungen grafisch zusammen und hebt besonders die Unterschiede zu der Vorgängerstudie hervor [SETIK 00]. In Kapitel 10 aggregiert eine Übersichtstabelle die einzelnen Tabellen und zeigt damit auf, wie sich die übergreifenden Trends insgesamt verändert haben. Eine genaue Beschreibung dieser übergreifenden Trends geben die folgenden Abschnitte.

## 6.1 Automatisierung und Vereinfachung

Die Automatisierung dient der Arbeitserleichterung des Menschen durch Einsatz eines Automaten. Einem definierten Programm folgend, verarbeitet ein Automat selbstständig Inputs und transformiert diesen in Outputs. Das Streben nach Effizienzsteigerung und somit die Schaffung von Wettbewerbsvorteilen ist ein marktwirtschaftlicher Grundsatz.

Gerade in der Fertigungsindustrie haben Automaten seit vielen Jahren zur Arbeitserleichterung und Rationalisierung geführt. In der Informations- und Kommunikationsindustrie lässt sich der übergreifende Trend der Automatisierung aus zwei Perspektiven betrachten. Zum einen soll die Automatisierung der Informations- und Kommunikationsindustrie dazu dienen, der ansteigenden Komplexität in der Softwareentwicklung entgegenzuwirken; es wird nach einer Automatisierung in der Entwicklung von Softwaresystemen gesucht. Außerdem zeigt sich im Softwarebereich eine Entwicklung hin zur Vereinfachung von Benutzerschnittstellen. Zum anderen werden Softwareprogramme entwickelt, welche die Automatisierung in den verschiedensten Bereichen der Wirtschaft und der Gesellschaft ermöglichen, wie dies beispielsweise an den Entwicklungen im Knowledge Management oder Data Mining zu erkennen ist.

## 6.2 Dienst- und Komponentenorientierung

Abstraktion ist die verallgemeinernde, zusammenfassende Darstellung eines Sachverhalts ohne Berücksichtigung von Einzelheiten. Um die Komplexität heutiger Informations- und Kommunikationssysteme durchdringen zu können, zerlegt man sie in Teilsysteme unterschiedlicher Abstraktionsebenen. Die verschiedenen Ebenen werden Schichten genannt. Jedes Teilsystem einer Schicht stellt über festgelegte Schnittstellen definierte Dienste zur Verfügung. Die Implementierung einzelner Schichten kann durch Komponenten erfolgen. Komponenten sind Teile eines Ganzen, in denen Prozesse, Daten und Steuerinformationen gekapselt sind. Sie sind eine Konkretisierung von Diensten und bieten ihre Funktionen über Schnittstellen an.

Dieser Trend zeigt sich zum Beispiel bei Telekommunikationsanwendungen. Kommunikations-Infrastrukturen können

aus Hardware-Komponenten verschiedener Hersteller zusammengesetzt werden. Ihr Zusammenspiel wird über die definierten Schnittstellen sichergestellt. Die Infrastrukturen bilden die Basis-Schicht. Darauf setzen Middleware-Technologien auf, die eine Nutzung von Komponenten auf der Anwendungs-Schicht ermöglichen.

Auch in der Softwaretechnik wird die Schichtenbildung und Abstraktion angewandt. Eine Gliederung in unterschiedliche Prozessphasen ermöglicht die Abstraktion von technischen Anforderungen in der Analysephase. Erst in der Designphase werden schließlich technische Details integriert und die Softwarearchitektur erstellt. Moderne objektorientierte Programmiersprachen unterstützen die Entwicklung von Komponenten und Diensten. Ein Anwendungsbeispiel der Dienstorientierung ist die Entwicklung der Web Services. Versehen mit einer definierten Schnittstelle bieten Unternehmen eine Dienstleistung über das Internet an. Der Trend in der Softwareentwicklung geht zur Komponentenorientierung. Sie ermöglicht die Mehrfachverwendung eines Programmcodes, der einem definierten Zweck dient. Eine neue Anwendung kann so aus bereits implementierten Komponenten einfach und schnell zusammengesetzt werden.

## 6.3 Globalisierung und Wettbewerb

Die Informations- und Kommunikationstechniken ermöglichen durch einheitliche Standards bei der Sprach- und Datenübermittlung eine Globalisierung von Informationen. Durch sie wird die zunehmende Vernetzung von Unternehmen unterschiedlicher Branchen und auf unterschiedlichen Wertschöpfungsstufen ermöglicht. Die Unternehmen agieren über das Internet auf globalen Märkten und stehen mit globalen Konkurrenten im Wettbewerb.

Im Bereich der Softwaretechnik findet ein zunehmender Wettbewerb statt. Konkurrierende, proprietäre Technologien entstehen, was zu einem intensiven Wettbewerb insbesondere im Bereich der Definition von Standards führt. Die Öffnung der Telekommunikationsmärkte ist ein weiteres Beispiel dafür, wie verstärkter Wettbewerb zu einer Verbesserung des Dienstangebots bei gleichzeitig sinkenden Preisen führen kann.

## 6.4 Integration und Standardisierung

Integration ist das Zusammenfügen von Teilen zu einer Einheit. Die Standardisierung ist die Vereinheitlichung nach bestimmten Mustern. Der Trend zu Integration und Standardisierung zeigt sich in vielen technologischen Bereichen. Beispielsweise sind Backbone-Netze in der Lage, verschiedene lokale Netze zusammenzuführen. Die Datenintegration ist ein weiteres Beispiel: Unternehmensdaten werden einheitlich erfasst und gespeichert, um sie verschiedenen Anwendungen zur gemeinsamen Nutzung zur Verfügung zu stellen. Die Integration von Daten über Unternehmensgrenzen hinweg erfolgt zum Großteil über standardisierte Schnittstellen, wie EDI oder XML. Zudem erleichtert die Standardisierung in vielen Bereichen die Lösung von Problemstellungen. So könnten beispielsweise Geschäftsprozesse in Form von standardisierten Softwarekomponenten angeboten werden, in denen das jeweilige verfügbare Branchenwissen integriert ist. SAP/R3 ist ein gutes Beispiel für diesen Trend.

## 6.5 Kapazitäts- und Leistungssteigerung

Leistung stellt ein bestimmtes Ergebnis ins Verhältnis zum notwendigen Aufwand (meist Zeit) und dient als wesentlicher Parameter zur Bewertung von Alternativen. Großen Einfluss auf die Leistung eines Systems hat die zur Verfügung stehende Kapazität. Sowohl Leistungfähigkeit, als auch Kapazität vieler Technologien sind in den letzten Jahrzehnten kontinuierlich stark angestiegen. In immer kürzeren Entwicklungszeiten werden Prozessoren mit höheren Taktfrequenzen und größeren Caches entwickelt. Bussysteme erhöhen zunehmend die Kommunikationsmöglichkeiten zwischen den Hardwarebauteilen. Festplatten, Arbeitsspeicher und andere Medien mit schnelleren Zugriffszeiten und regelmäßig größeren Kapazitäten entstehen. Hinzu kommt die wachsende Parallelisierung und Verteilung in den unterschiedlichsten Berei-

chen. Die Verknüpfung mehrerer Systeme ermöglicht einfache Leistungssteigerungen auf der Basis vorhandender Technologien und Kapazitäten. Vergleichbares lässt sich im betriebswirtschaftlichen Umfeld beobachten. Unternehmenskooperationen ermöglichen einzelnen Unternehmen auf die Kapazitäten anderer zurückzugreifen und damit die eigene Leistungsfähigkeit z.B. durch Parallelisierung von Geschäftsprozessen oder Angebote neuer Produktmerkmale zu steigern. Es ist bisher nicht abzusehen, dass dieser fundamentale Trend der Kapazitäts- und Leistungssteigerung nachlässt, da die Grenzen etablierter Technologien und Konzepte durch kontinuierliche Innovation überwunden werden können.

## 6.6 Konvergenz

Konvergenz ist die Annäherung von Elementen aus vormals getrennten Bereichen. In dieser Studie wird unter Konvergenz die Vereinigung der Medien-, Informations- und Telekommunikationsindustrie verstanden. Ihre Technologien, Wertschöpfungsketten und Märkte wachsen zusammen. Die Digitalisierung ermöglicht ein hohes Maß an Konvergenz. Beispiele dafür sind die Verbindung von Mobilfunk- und Festnetzen zu hybriden Kommunikationsnetzen. Personal Computer und Fernsehgeräte konvergieren zu internetfähigen Fernsehgeräten. Informationen lassen sich über die unterschiedlichsten Medien übertragen. Die Konvergenz hat weitreichende gesellschaftliche, politische und wirtschaftliche Auswirkungen.

## 6.7 Miniaturisierung

Miniaturisierung bezeichnet die Verkleinerung technischer Bauteile und ist Voraussetzung für höhere Kapazität und Leistung auf immer kleinerem Raum. Besonders im Bereich der Prozessortechnik spielt Miniaturisierung eine bedeutende Rolle. Dort ist eine ständige Erhöhung der Integrationsdichte von Schaltungen zu beobachten. Auch im Bereich eingebetteter Systeme und mobiler Endgeräte (wie Mobiletelefone oder Personal Digital Assistants) ist die Miniaturisierung als wesentlicher Treiber für weitere Entwicklungen zu betrachten. Allerdings bremsen hier physikalische Grenzen. So scheinen Transistoren langsam die kleinst möglichen Abmessungen zu erreichen, während manche Mobiltelefone heute schon auf Grund ihrer kleinen Tasten kaum noch zu bedienen sind und dank höherer Leistung und kleinerer Akkus kürzere Laufzeiten aufweisen. Auswege bietet die Entwicklung neuer Ansätze wie Nanoröhren, Sprachbedienung, energiesparende Displays und kompakte Brennstoffzellen.

## 6.8 Mobilität

Mobilität bedeutet Beweglichkeit. Miniaturisierung und drahtlose Technologien wie Wireless LAN und Mobilfunk überwinden die Ortsgebundenheit elektronischer Medien und ermöglichen somit ihren Einsatz an jedem Ort und zu jedem Zeitpunkt. Innerhalb von Kommunikationsnetzen gewinnt mobile Software an Bedeutung, die sich zur Durchführung ihrer Aufgabe auf die jeweils notwendigen Systeme bewegt. Sowohl den geschäftlichen Bereich, als auch das Privatleben haben diese Entwicklungen in den letzten Jahren nachhaltig (Stichworte Mobiles Büro und Telearbeit) verändert und werden dies voraussichtlich auch die nächsten Jahre weiter tun. So sind hier inzwischen Entwicklungen eingetreten, die im Rahmen der Vorgängerstudie erst erahnt werden konnten (z.B. die überraschend weite Verbreitung von Mobiltelefonen und dem Kurznachrichtendienst SMS).

## 6.9 Vernetzung und Flexibilisierung

Vernetzung ist die relationale Verbindung einzelner Elemente zu einem größeren Gesamtsystem. Wesentliche Voraussetzung sind Schnittstellenstandards zur Kommunikation zwischen den Elementen (siehe Abschnitt 6.2). Eine entscheidende Folge ist das Erreichen größerer Flexibilität durch das Nutzen der jeweils besten im Netz verfügbaren Ressourcen. Zur Implementierung immer leistungsfähigerer und breitflächig vernetzter Kommunikationsinfrastrukturen bilden LAN/WAN-Standards wie WDM, ISDN oder DSL die technischen Grundlagen. IP und seine Weiterentwicklung IPv6 ermöglichen die flexible Verbindung der unterschiedlichsten Übertragungstechnologien. Darauf setzen

dann Protokolle wie HTTP oder SOAP zur losen Koppelung verschiedenster Anwendungen auf. Ähnliche Vernetzung bei gleichzeitiger Flexibilisierung findet auch zwischen Unternehmen statt und ermöglicht zum einen die Konzentration auf strategische Kernkompetenzen und zum anderen die Nutzung komplementärer Ressourcen. Vernetzung und Flexibilisierung nehmen in vielen Bereichen weiter zu und erfassen auch immer stärker das tägliche Leben, wie z.B. die Koppelung von Mobiltelefon, Personal Computer, Personal Digital Assistants und Unterhaltungselektronik.

## 6.10 Verteilung und Dezentralisierung

Dezentralisierung bezeichnet die logische und oft auch räumliche Unterteilung eines Gesamtsystems in weitgehend autonome Teile, welche aber gemeinsam bestimmte Zwecke erfüllen. Technische Systeme mit starker Dezentralisierung der Einzelkompenenten werden meist als verteilte Systeme bezeichnet. In Zusammenhang mit der oben behandelten Vernetzung ermöglicht die Verteilung Kapazitäts- und Leistungssteigerung entweder durch die Koppelung identischer Systeme (z.B. Rechencluster) oder durch die Verbindung hoch spezialisierter Systeme (Trennung von Datenbank- und Applikationsservern). Neuere Entwicklungen im Bereich der Softwaretechnik wie Web Services und mobiler Code verstärken diesen Trend. Ähnliches gilt für Organisationen, in denen starre, zentral gesteuerte Hierarchien zunehmend von dezentralen Kompetenzzentren verdrängt werden, die je nach Aufgabe ihre Ressourcen in flexibel zusammengesetze Projektteams einbringen.

## 6.11 Virtualisierung

Der Grundgedanke der Virtualisierung bezieht sich auf Objekte, die nicht real bzw. nicht physisch, aber ihrer Möglichkeiten bzw. ihrer Funktionen nach vorhanden sind. Demnach ist Virtualität immer im Zusammenhang mit Objekten zu betrachten. Die Ausprägungen virtueller Objekte sind vielfältig. Ein bekanntes Beispiel aus der Informationstechnik stellt der virtuelle Arbeitsspeicher dar, dessen Funktionalität der von RAM-Bausteinen entspricht, obwohl sich dahinter tatsächlich andere physischem Medien wie Festplatten oder gar Bandspeicher verbergen können. Dieses Prinzip findet sich auch bei virtuellen Unternehmen, die weder Aufbau- noch Ablauforganisation realer Unternehmen umfassen, aber dennoch aus der Sicht des Kunden wie reale Unternehmen am Markt agieren und oft sogar überlegene Leistungen anbieten können.

# 7 IT-Sicherheit

## 7.1 Grundbegriffe

Information und die damit verbundene Informations- und Kommunikationstechnologie sind zu wichtigen Säulen unserer Gesellschaft geworden. Informations- und Kommunikationstechnik sind Technologien zur Kodierung, Speicherung, Verarbeitung und Übertragung der Information in Form von Daten [Goll 99]. Die zunehmende Abhängigkeit unserer Gesellschaft von IT-Systemen stellt uns immer mehr vor neue Herausforderungen hinsichtlich ihrer Korrektheit und Sicherheit.

In den letzten Jahrzehnten haben die Anforderungen zum Schutz dieser Systeme sowohl im geschäftlichen als auch im privaten Bereich große Änderungen erfahren. Automatische Werkzeuge und Maßnahmen wurden erforderlich, um sicherheitskritische Daten und Prozesse auf Rechnern und Mehrbenutzersystemen vor unbefugtem Zugriff, Ausspähung, Verfälschung und Manipulation zu schützen und um für einen korrekten Systemablauf zu sorgen. Folglich fasst man diese Schutzmaßnahmen unter dem Oberbegriff Rechnersicherheit zusammen. Die Entstehung der Kommunikationsnetzwerke und -infrastrukturen mit heterogenen Rechnersystemen sowie die Einführung und Verbreitung verteilter Systeme und Anwendungen erforderte weitere Maßnahmen zum Schutz der Daten während der Übertragung sowie der involvierten Rechnersysteme und der von ihnen angebotenen Dienste. Diese Schutzmaßnahmen werden häufig unter Netzwerksicherheit zusammengefasst. Hinzu kommt, dass in komplexen IT-Systemen mit verteiltem und dynamischem Charakter (wie z.B. dem Internet) verschiedene Parteien (Organisationen und Personen, Programme und Maschinen) interagieren, die unterschiedliche Interessen haben und sich gegenseitig nur minimal vertrauen oder sogar völlig misstrauen. Sie können sich auf verschiedene Art und Weise angreifen, z.B. durch abhören, stören, täuschen oder außer Betrieb setzen. Hierbei werden Maßnahmen benötigt, welche die Sicherheitsanforderungen der einzelnen beteiligten Parteien auf einem sinnvollen Niveau erfüllen[1]. Dies wird auch als mehrseitige Sicherheit bezeichnet. In Wirklichkeit existieren keine klaren Grenzen zwischen den genannten Formen von Sicherheit. IT-Sicherheit ist ein recht allgemeiner Begriff, der in verschiedenen Zusammenhängen verwendet wird. Sie ist das Fachgebiet, das sich im Allgemeinen mit allen genannten Aspekten beschäftigt. Für sichere und korrekt funktionierende IT-Systeme müssen je nach Komplexität und Sicherheitsanforderungen unterschiedliche Maßnahmen ergriffen werden. In der Praxis hat man es häufig mit vernetzten Systemen zu tun, die an offene und unsichere Umgebungen wie das Internet angeschlossen und somit automatisch Angriffen von außen ausgesetzt sind. Diese können jedoch auch von innerhalb des jeweiligen Systems stammen. Die Hauptaufgabe der IT-Sicherheit besteht darin, solchen Bedrohungen kontinuierlich durch entsprechende Schutzmaßnahmen entgegenzuwirken, um eventuellen Schäden vorzubeugen. Diese Aufgabe ist vielfältig und berührt neben vielen verschiedenen organisatorischen und personellen Aspekten auch ein breites Spektrum technischer Aspekte aus unterschiedlichen Disziplinen. Dazu gehören u.a. der Einsatz von kryptographischen Verfahren und Protokollen, sicheren Betriebssystemen, Sicherheits-Gateways, Intrusion-Detection-Systemen und Software-Engineering bei der Erstellung von Anwendungen.

[1] Ein Beispiel hierfür ist der elektronische Handel über das Internet. In diesem Zusammenhang hat jede der beteiligten Parteien eigene Interessen, die auch gegensätzlich sein können. Beispielsweise möchten Kunden ihre Händler authentisieren, ihre Kaufdaten vertraulich halten, anonym bleiben und signierte Quittungen von Händlern bekommen. Händler hingegen möchten Kunden authentisieren, mehr über ihre Kaufinteressen erfahren und rechtsgültige Verträge über den Kauf bekommen.

Die folgenden Kapitel sollen einen kurzen Überblick der auf IT-Systeme einwirkenden Bedrohungen gewähren, mögliche Verfahren zur Abschätzung eines Risikopotenzials benennen sowie ausgewählte technische Maßnahmen zur Schutzzielerreichung vorstellen.

### 7.1.1 Bedrohungen der IT-Sicherheit

Unter der Bezeichnung Angriff werden bösartige Versuche zusammengefasst, die vor allem die Intention haben, Schutzziele und die jeweiligen Sicherheitsrichtlinien des Systems zu verletzen. In diesem Kontext fallen häufig die Begriffe Schwachstellen und Bedrohungen. Schwachstellen bezeichnen die verwundbaren Stellen eines Systems, über welche die Sicherheitsmaßnahmen des Systems umgangen bzw. überlistet werden können. Sie können durch mangelhafte Nutzung, Entwürfe oder Implementierungen entstehen. Solche Schwachstellen können aber auch von physischen Charakteristika eines Systems abhängen, wie z.B. Robustheit gegen Diebstahl, Stromausfall und Naturkatastrophen. Die Angriffsmöglichkeiten und sich potenziell daraus ergebende Nachteile, Verluste und Schäden stellen die Bedrohungen für dieses System dar.

Grundsätzlich ist zwischen aktiven und passiven Angriffen zu unterscheiden. Passive Angriffe beschränken sich auf Informationsgewinnung durch Ausspähung und Beobachtung eines Systems. Beispiele sind Abhören der Kommunikationskanäle (Telefon oder Datenkanäle) oder Verkehrsanalyse in Netzwerken. Bei aktiven Angriffen hingegen versucht der Angreifer durch aktives Eingreifen oder Interaktion mit dem Angriffsziel, Information zu gewinnen oder sie zu manipulieren, in ein System einzudringen, es zu korrumpieren, zu stören oder sogar außer Betrieb zu setzen. Aktive Angriffe sind wesentlich mächtiger als passive, erfordern jedoch meist auch mehr Aufwand durch den Angreifer. Einige Beispiele aktiver Angriffe sind Maskierungsangriffe, Replay- und Denial-of-Service-Angriff.

Die Bedrohungen und Angriffsmöglichkeiten auf IT-Systeme werden durch ihre Anbindung an offene Umgebungen verschärft. Die geschäftliche und private Nutzung des für alle öffentlich zugänglichen Internets hat in den letzten Jahren rapide zugenommen. Immer mehr Dienste und Geschäftsmodelle werden von der realen physikalischen Welt mehr oder weniger erfolgreich in die elektronische Welt übertragen, um die Vorteile und Möglichkeiten der Informationstechnik wie globale Erreichbarkeit, Skalierbarkeit, Geschwindigkeit und Automatisierung verteilter Berechnungen nutzen zu können. Hinzu kommen auch fortgeschrittene Geschäftsmodelle wie elektronische Zahlungssysteme und Auktionen. Die Kommunikation und die Nutzung dieser Dienste über eine offene Umgebung wie das Internet birgt jedoch auch Gefahren und Bedrohungen in sich, etwa gezielten Missbrauch, Betrug und kriminelle Handlungen wie das Ausspähen persönlicher und geschäftlicher Geheimnisse sowie die Zerstörung der Daten und die Lahmlegung der Rechnersysteme.

Zu den speziellen Bedrohungen gegen IT-Systeme gehört die sog. Malware. Dies sind i.a. Programme, die bestimmte bösartige Funktionen unbemerkt ausführen. Beispiele für Malware sind Trojaner und Viren [Denn 90, Rubi 01]:

Ein Trojaner ist eine versteckte Routine, die in einem harmlos erscheinenden Programm verborgen ist. Durch Ausführen des Programms wird der Trojaner auf dem betroffenen System unbemerkt im Hintergrund ausgeführt. Das Ziel hierbei ist es, Daten auszuspähen, zu manipulieren oder zu zerstören. Voraussetzung ist allerdings, dass das den Trojaner enthaltende Programm zuvor auf einem IT-System installiert wird. Charakteristisch für Trojaner ist die Einrichtung eines permanenten Zugangs zu dem betroffenen System, auch Hintertür genannt, über die der Angreifer unbemerkt Zugang zum System erhalten kann.

Ein Virus ist eine in einem Programm versteckte Routine mit der Fähigkeit, sich zu reproduzieren. Das erste Computervirus wird Leonard Adleman (auch einer der RSA Autoren) zugesprochen [Cohe 87]. Es kann durch Übertragung über Netzwerke andere Systeme befallen und infiltrieren. Nebst der Fortpflanzung besitzt ein Virus üblicherweise weitere Funktionen, die ausgeführt werden und Schaden anrichten können. Dies bezeichnet man auch als Zeitbombe bzw. logische Bombe. Eng

verwandt mit Viren sind die sog. Würmer, die sich reproduzieren und die Kopien über Netzwerke verteilen. Würmer können unterschiedliche Verbreitungsstrategien haben. Einige Beispiele für Viren und Würmer sind Melisa, Morris, CIH Chernobyl und I LOVE YOU (siehe http://www.f-secure.com/v-descs/). Es existieren verschiedene Typen von Trojanern, Viren und Würmern, die für unterschiedliche Systeme konstruiert sind und unterschiedliche Ziele verfolgen (siehe z.B. [Rubi 01]). Manche von ihnen zeigen potenzielle Bedrohungen auf, während andere bereits große Schäden verursacht haben.

Eine weitere spezielle Klasse der Bedrohungen gegen IT-Systeme sind Buffer Overflows [Alep 96, CWP+ 99], die auf die Schwachstellen von Programmen und Betriebsystemen durch mangelhaften Umgang mit der Speicherverwaltung zurückzuführen sind. Diese Nachlässigkeit kann von einem Angreifer geschickt ausgenutzt werden, um ein Programm in einem übergelaufenen Puffer zu platzieren und auszuführen.

Beispiele für weitere Angriffe sind Maskierung (Spoofing), Replay [Stal 98, MvOV 97, Rubi 01], Denial-of-Service (DoS) [ZCC 00, MVS 01] und Scanning [Fyod 97, SHM 02]. In einem Maskierungsangriff gibt eine Partei eine falsche Identität an, beispielsweise spielt der Angreifer eine falsche Email- bzw. Server-Identität (z.B. IP-Adresse) vor. Für einen Replay-Angriff werden Nachrichten einer Kommunikationssitzung (z.B. Autorisierung) aufgenommen und später entweder ganz oder in Teilen verwendet, um diese Sitzung zu simulieren. Denial-of-Service ist ein Angriff gegen die Verfügbarkeit der Ressourcen und Dienste eines IT-Systems mit dem Ziel, diese zu blockieren und somit regulären Benutzern keinen Zugriff mehr zu ermöglichen. Beispielsweise sendet der Angreifer eine große Zahl von Anfragen an ein ausgewähltes System, um die Nutzung des Systems durch Überlastung zu verhindern. Eine spezielle Form der DoS-Angriffe ist Distributed-Denial-of-Service (DDoS) [Cris 00, HoWe 01, MVS 01]. Dabei wird der zur Blockade führende Angriff nicht nur von einem einzelnen Angriffsrechner ausgeführt, sondern von mehreren gleichzeitig. Dadurch wird sowohl der Angriff verstärkt als auch die Einleitung der Gegenmaßnahmen erschwert, da diese auf mehrere Quellen angewendet werden müssen. Scanning-Techniken (z.B. Portscanning) werden eingesetzt, um Informationen über ein Netzwerk und dessen interne Struktur zu gewinnen, z.B. welche Netzadressen von Rechnern in Gebrauch sind oder wie die Netzwerktopographie aussieht. Häufig wird versucht, diese Aufgaben zu automatisieren.

Die Klassifizierung verschiedener Angriffe trägt sowohl zum besseren Verständnis existierender Systeme als auch zum effektiveren Entwurf zukünftiger Systeme bei. Versuche in diesem Zusammenhang werden beispielsweise in [LiJo 97, LBMC 94] beschrieben.

### 7.1.2 Methodische Vorgehensweise

Um einen gewünschten und angemessenen Sicherheitsgrad für das zugrunde liegende IT-System zu erreichen und diesen aufrecht zu erhalten, ist eine geplante und strukturierte Vorgehensweise erforderlich. Hierbei ist insbesondere zu berücksichtigen, dass die Komplexität der IT-Systeme und ihre Sicherheitsanforderungen sich kontinuierlich verändern. Die wesentlichen Aspekte dieser Vorgehensweise bestehen aus der Risikoanalyse und der Erstellung einer geeigneten Sicherheitsstrategie. In diesem Zusammenhang werden die relevanten Schutzziele identifiziert und präzise formuliert. Weiterhin werden die zu schützenden Werte (Geschäftsprozesse, Rechner bzw. Rechnersysteme, Daten, physikalische Verbindungen usw.) sowie mögliche Bedrohungen mit ihrer Gewichtung kategorisiert. Dadurch können potenzielle Schäden und damit verbundene Kosten abgeschätzt und der Schutzbedarf für die Werte relativ zu den Schutzzielen bestimmt werden. Die Ergebnisse dieser Analysen bilden eine wichtige Grundlage für die Definition und Festlegung entsprechender Maßnahmen und Sicherheitsstrategien, die über rein technische Maßnahmen hinausgehen.

Zur methodischen Vorgehensweise zur Schaffung der IT-Sicherheit existieren bereits verschiedene Ansätze. Beispiele für etablierte Methoden sind Common Criteria [Comm 99], das IT-Grundschutzhandbuch des BSI [BSI 01] und die britische Norm BS 7799.

### 7.1.2.1 Schutzziele

Die Sicherheitsanforderungen an ein IT-System bzw. dessen Schutzziele hängen von dem jeweiligen System ab und können beliebig kompliziert werden. Zur Klassifikation und Gruppierung wesentlicher Schutzziele gibt es unterschiedliche Ansätze [RPM 97, FePf 00, PSWW 00, PoSt 01]. Die klassischen Schutzziele sind Vertraulichkeit, Integrität und Verfügbarkeit.

- Vertraulichkeit bezeichnet das Ziel, unautorisierte Gewinnung von Information zu verhindern. Beispielsweise sollen sowohl die lokalen als auch die in der Übertragung befindlichen Daten vor Unbefugten verborgen bleiben.
- Unter Integrität versteht man das Ziel, unautorisierte und unbemerkte Modifikation von Information nicht zuzulassen. Beispielsweise werden empfangene Nachrichten auf ihre Integrität geprüft.
- Unter Verfügbarkeit versteht man, dass Ressourcen und Dienste zur Verfügung stehen sollen, wenn dies von (befugten) Parteien gewünscht wird.

Andere häufig explizit genannte Schutzziele sind

- Authentizität: Damit wird die Echtheitseigenschaft bezeichnet. Für eine Nachricht bedeutet dies die Integrität der Nachrichtenquelle. Beispielsweise ist ein Dokument authentisch, wenn sein erklärter Autor auch der tatsächliche Autor ist. In ähnlicher Weise ist eine vorgebliche Partei authentisch, wenn die erklärte Identität und die tatsächliche Identität übereinstimmen. Beispielsweise soll in einer Kommunikation garantiert sein, dass der Kommunikationspartner wirklich derjenige ist, für den er sich ausgibt. Das bezieht sich auf den Verbindungsaufbau, aber auch auf die darauf folgende Kommunikation.
- Anonymität: Eine Partei kann Ressourcen und Dienste nutzen ohne ihre Identität preisgeben zu müssen[2]. Beispielsweise wünschen die Kunden, ihre elektronischen Zahlungen anonym tätigen zu können, um die Erstellung von Kaufprofilen zu verhindern.
- Nichtabstreitbarkeit: Die Ausführung einer Aktion soll nicht abgestritten werden können. Beispielswiese soll der Empfänger bzw. der Sender einer Nachricht gegenüber einer dritten ehrlichen Partei den Empfang bzw. das Senden dieser Daten beweisen können. Dies ist besonders im Kontext des elektronischen Handels wichtig.

Einige Schutzziele fallen entweder unter die drei klassischen oder können aus ihren Kombinationen definiert werden. Beispielsweise kann man die Anonymität, wie oben definiert, bei der Vertraulichkeit einordnen oder Nichtabstreitbarkeit als Verfügbarkeit und Integrität bestimmter Metainformationen (Identität des Senders, Empfangsbestätigung und Identität des Empfängers) definieren.

### 7.1.2.2 Maßnahmendefinition

Die Sicherheitsstrategie für ein IT-System definiert organisatorische, personelle und technische Maßnahmen, die zur Erreichung der gesetzten Schutzziele erforderlich sind. Organisatorische Maßnahmen beinhalten u.a. die Definition und die Festlegung sicherheitsrelevanter Verantwortlichkeiten, die Schaffung von Regeln für erlaubten Zugang und Zugriff und Initiierbarkeit von Aktionen (beispielsweise müssen mindestens zwei von vier Geschäftsführern eine sicherheitskritische Aktion autorisieren), die Methoden zur Erreichung der Schutzziele (z.B. Risikoanalysemethoden), zur Evaluierung von technischen Realisierungen der Sicherheitsstrategien, zur Integration neuer Sicherheitsaspekte und zur Durchführung von Umstrukturierungsprozessen.

Personelle Maßnahmen erstrecken sich über die gesamte Dienstzeit der Mitarbeiter und beinhalten u.a. Aspekte

[2] In diesem Kontext können auch weitere Eigenschaften wie Pseudonymität oder Unverkettbarkeit betrachtet werden. Pseudonymität bedeutet, dass die Identität verborgen bleibt, aber ein Fehlverhalten trotzdem nachweisbar auf die entsprechende Partei zurückgeführt werden kann. Unverkettbarkeit bedeutet, dass verschiedene Aktionen einer Partei nicht in Verbindung gebracht werden können (siehe auch [PfKö 00].

wie sicherheitsrelevante Verhaltensrichtlinien und Verpflichtung der Mitarbeiter zu deren Einhaltung, Vertretungsregelungen und Schulungen. Abhängig von den zu garantierenden Schutzzielen und den zu schützenden Werten werden verschiedene technische Maßnahmen benötigt. Diese betreffen u.a. physische Sicherheit, Zugriffskontrollmechanismen, kryptographische Verfahren und Protokolle, Sicherheits-Gateways und Intrusion Detection Systeme. Im Folgenden wird auf einige ausgewählte technische Maßnahmen eingegangen.

### 7.1.3 Ausgewählte technische Maßnahmen

#### 7.1.3.1 Verschlüsselung

Verschlüsselung ist, abstrakt betrachtet, eine Transformation, die Klartexte (Originaldaten) in Schüsseltexte transformiert mit dem Ziel, Vertraulichkeit zu erreichen. Allerdings ist zu beachten, dass Verschlüsselungsverfahren keine Integrität garantieren sollen. Zur Rücktransformation der Schlüsseltexte benötigt man den geheimen Schlüssel. Die Komponenten eines Verschlüsselungssystems sind Algorithmen zur Schlüsselgenerierung und zur Ver- bzw. Entschlüsselung. Gegen Verschlüsselungssysteme gibt es verschiedene Angriffstypen [MvOV 97]. Informationstheoretische Sicherheit bei einem Verschlüsselungsverfahren bedeutet, dass auch ein allmächtiger Angreifer anhand des beobachteten Schlüsseltextes keine Information über den Klartext gewinnen kann. Diese Verfahren werden auch „perfekt sicher" genannt. Man unterscheidet zwischen symmetrischen und asymmetrischen Verschlüsselungssystemen.

Symmetrische Verschlüsselungsverfahren verwenden denselben Schlüssel zur Ver- und Entschlüsselung. Das bekannteste dieser Verfahren ist das One-time pad. Es bietet informationstheoretische Sicherheit, ist jedoch praktisch kaum einsetzbar, da der Schlüssel mindestens so lang sein muss wie der zu verschlüsselnde Klartext. Andere bekannte symmetrische Verschlüsselungssysteme sind der Data Encryption Standard (DES) [Nati 77] und das davon abgeleitete Verfahren Triple-DES. Hierbei wird der Klartext drei mal hintereinander mit drei verschiedenen Schlüsseln chiffriert. Damit soll die Schlüssellänge im Vergleich zur DES-Schlüssellänge (56 Bit) größer werden, um einen höheren Sicherheitsgrad zu erreichen. DES gehört zu den sog. Blockchiffren [Knud 98], die dadurch charakterisiert sind, dass sie Nachrichtenblöcke fester Länge (z.B. 64 Bit) verarbeiten. Das Grundprinzip von DES besteht aus Wiederholungen von mehreren Runden, die sich durch die jeweils verwendeten Teilschlüssel unterscheiden, wobei die Teilschlüssel aus dem Hauptschlüssel abgeleitet werden. Diese beiden Verfahren waren oft Gegenstand analytischer [MvOV 97] und experimenteller[3] Angriffe [Schn 96, MvOV 97]. Für DES und alle vergleichbaren Systeme gibt es keine Sicherheitsbeweise oder Reduktionen auf mathematisch schwere Probleme. Das Design solcher Verfahren erfordert die Berücksichtigung aller bekannten Angriffe. Weitere bekannte Verfahren sind IDEA [LaMa 90] und die DES Nachfolgechiffre Advanced Encryption Standard (AES) [Nati 01]. Um aus Chiffren, wie z.B. DES, ein Verschlüsselungssystem für lange Nachrichten zu erhalten, werden die sog. Betriebsarten eingesetzt [MvOV 97]. Grob ausgedrückt sollen die Betriebsarten aus einer Blockchiffre eine Stromchiffre erzeugen, wobei sie im Gegensatz zum One-time Pad immer den gleichen Schlüssel, nämlich den der Blockchiffre, verwenden.

Wichtige kryptoanalytische Methoden zur Untersuchung symmetrischer Chiffren sind die lineare und die differentielle Kryptoanalyse [BiSh 93, Mats 94] und die sog. Korrelationsangriffe (Correlation Attacks) [MeSt 89].

Asymmetrische Verschlüsselungssysteme verwenden statt eines einzigen Schlüssels ein Schlüsselpaar, bestehend aus einem öffentlichen Schlüssel (public key) und einem geheimen Schlüssel (secret key, private key). Der öffentliche Schlüssel wird zur Verschlüsselung und der geheime zur Entschlüsselung verwendet. Für vertrauliche Kommunikation verschlüsselt der Sender die Nachricht mit dem öffentlichen Schlüssel des Empfängers. Das bekannteste asymmetrische Verschlüsselungsverfahren ist das RSA-Verfahren [RSA 78], das nach seinen Erfindern Ronald L. Rivest, Adi Shamir

[3] Siehe auch http://www.eff.org/descracker.html

und Leonard M. Adleman benannt wurde. Es verwendet eine sog. Einwegpermutation (one-way permutation) mit Falltür (trapdoor). Informell ist dies eine Einwegfunktion[4], die mit vertretbarem Aufwand schwer umzukehren ist, es sei denn, man besitzt eine zusätzliche (geheime) Information, nämlich die Falltür. Diese geheime Information ist der private Schlüssel. RSA ist bisher der Gegenstand von vielen analytischen und experimentellen Untersuchungen gewesen [Bone 99]. Die Sicherheit von RSA beruht vor allem auf der Faktorisierungsannahme. Ein weiteres bekanntes Verschlüsselungsverfahren ist das ElGamal-System [ElGa 85], dessen Sicherheit auf der Annahme basiert, dass in gewissen algebraischen Strukturen der diskrete Logarithmus mit vertretbarem Aufwand nicht zu lösen ist. RSA und ElGamal sind relativ effiziente Verfahren, aber nicht beweisbar sicher. Beweisbar sichere asymmetrische Verschlüsselungsverfahren waren lange Zeit nur ein Gegenstand der theoretischen Kryptographie, da es keine effizienten Systeme gab, die gegen alle Angriffstypen sicher waren. Der erste Durchbruch kam mit dem Cramer-Shoup Verfahren [Crypto98b]. Asymmetrische Verschlüsselungsverfahren können keine informationstheoretische Sicherheit bieten, denn ein informationstheoretischer Angreifer kann den privaten Schlüssel aus dem öffentlichen berechnen.

#### 7.1.3.2 Symmetrische Authentikation

Ziel der symmetrischen Authentikation ist die Integrität und Authentizität von Nachrichten. Die entsprechenden Verfahren werden manchmal Authentikationscode (Message Authentication Code, MAC) genannt. Zur Erzeugung und Überprüfung eines Authentikationscodes wird der gleiche Schlüssel verwendet. Es gibt verschiedene Angriffstypen auf Authentikationscodes [MvOV 97]. Informationstheoretische und effiziente symmetrische Authentikation ist möglich, da im Gegensatz zur informationstheoretisch sicheren Verschlüsselung das Problem der Schlüssellänge ein geringeres ist [WeCa 79]. Gewisse Betriebsarten der Blockchiffren [MvOV 97] und Hashfunktionen [Tsud 92, Crypto96] können für symmetrische Authentikation eingesetzt werden.

#### 7.1.3.3 Digitale Signaturen

Durch zunehmende Nutzung digitaler Medien im privaten und geschäftlichen Bereich werden immer mehr elektronische Transaktionen abgewickelt, die neue administrative, rechtliche und sicherheitstechnische Anforderungen an zugrunde liegende elektronische Systeme stellen. In diesem Kontext spielt eine der wichtigsten Klassen kryptographischer Primitive, die digitale Signatur, eine bedeutende Rolle, da sie die handschriftliche Unterschrift ersetzen und neben der Rechtssicherheit auch mehr Sicherheit gegen Fälschung bieten soll. Ein digitales Signatursystem stellt eine asymmetrische Authentikation dar mit dem Ziel, Nichtabstreitbarkeit zu erreichen, wodurch Dispute vor einer dritten Partei ermöglicht werden. Diese Eigenschaft kann man jedoch mit symmetrischer Authentikation nicht gewährleisten, da sie keine Unterscheidung zwischen den Parteien zulässt, die einen gemeinsamen geheimen Schlüssel besitzen.

Signaturverfahren bestehen aus Algorithmen zur Schlüsselgenerierung, Signaturerzeugung und Verifikation der Signatur. Zum Signieren wird der geheime Signierschlüssel und zur Verifikation der Signatur der öffentliche Verifikationsschlüssel verwendet. Dazu müssen die öffentlichen Verifikationsschlüssel authentisch und konsistent verteilt werden. Es gibt verschiedene Angriffstypen gegen Signatursysteme [MvOV 97, Pfit 96]. Bekannte Signatursysteme sind RSA [RSA 78], ElGamal [ElGa 85], Schnorr [Schn 91] und der Digital Signature Standard (DSS) [Nati 91], dem der auf ElGamal basierende Digital Signature Algorithm (DSA) zugrunde liegt. Das DSA Signatursystem wurde im Jahre 1991 vom National Institute of Standards and Technology (NIST) vorgeschlagen. Die Variante für elliptische Kurven heißt ECDSA. Die Sicherheit dieses Systems beruht auf der Schwierigkeit, diskrete Logarith-

[4] Einwegfunktionen gehören zu den fundamentalsten kryptographischen Primitiven in der komplexitätstheoretischen Kryptographie. Informell hat eine Funktion die Einwegeigenschaft, wenn der Funktionswert für alle Eingaben effizient zu berechnen ist, aber die Umkehrung mit vertretbarem Aufwand nicht möglich sein soll. Derzeit ist es nicht bekannt, ob solche Funktionen existieren. Es gibt jedoch sinnvolle Kandidaten, deren Einwegeigenschaft stark vermutet wird (siehe [Gold 01] für eine formale Betrachtung).

men auf elliptischen Kurven zu lösen. Die Sicherheit von DSS beruht auf der DL-Annahme in verschiedenen algebraischen Strukturen.

Die Sicherheit der genannten Systeme basiert auf heuristischen Argumenten. Die meisten beweisbar sicheren Signatursysteme sind ineffizient und werden deshalb in der Praxis nicht eingesetzt [GMR 88, Crypto94]. Ein neueres Signatursystem in [CrSh 99] bietet jedoch beweisbare Sicherheit mit durchaus guter Effizienz.

Die Sicherheit der meisten asymmetrischen Systeme beruht auf zahlentheoretischen Annahmen wie Faktorisierung und DL, wobei die DL-basierten Annahmen die größere Rolle spielen [SaSt 01] für eine Analyse von DL-Annahmen). Es gibt jedoch auch Vorschläge für asymmetrische Systeme, deren Sicherheit andere mathematische Probleme zugrunde liegen, d.h. die nicht zahlentheoretisch basiert sind. Diese sind beispielsweise Probleme aus der Codierungstheorie [McEl 87] und der Algebra und Kombinatorik [Kobl 98]. Eine andere Entwicklung zum Entwurf neuer Kryptosysteme setzt auf die Probleme in sog. Gittern, die eigentlich zu kryptoanalytischen Zwecken eingesetzt werden. Ein Beispiel für ein solches System ist NTRU [ANTS 98c].

### 7.1.4 Sicherheits-Gateway

Ein Sicherheits-Gateway, auch Firewall genannt, ist ein System bestehend aus Hardware- und Softwarekomponenten, das den Übergang zwischen zwei Rechnernetzen absichert. In der Praxis wird ein Sicherheits-Gateway meistens eingesetzt, um ein als sicher geltendes lokales Netzwerk gegen Angriffe aus anderen Netzen, vor allem dem Internet, zu schützen. Ein Sicherheits-Gateway realisiert die festgelegten Sicherheitsstrategien wie beispielsweise Zugriffskontrolle und Authentikation. Hierbei wird sämtlicher Datenverkehr durch das Gateway geleitet, um unerlaubte Zugriffe und schädliche Programme abzufangen. Beispielsweise können die Daten nach Viren abgesucht werden (Virenscan) oder es können Antworten auf Anfragen eines Benutzers an Server außerhalb des lokalen Netzes untersucht werden, um diese zu blockieren (URL-Blocking). Nur die zu den Sicherheitsrichtlinien konformen Datenpakete werden weitergeleitet. Bei Sicherheits-Gatways unterscheidet man zwischen den Gateway-Typen Paketfilter und Proxies [ZCC 00].

Häufig verwendete Schutzmaßnahmen innerhalb eines Gateway sind Paketfilter. Dieser Typ ist auf den OSI-Schichten 3 und 4 angesiedelt. Hier findet eine Überprüfung und Filterung der Datenpakete nach den festgelegten Sicherheitsregeln statt. Für ein an das Internet angebundenes Netzwerk bedeutet dies, dass die IP- bzw. TCP-Pakete untersucht werden. Dabei wird normalerweise nur der Header eines Pakets untersucht, obwohl Sicherheits-Gateways auch den restlichen Inhalt der Pakete untersuchen könnten. Dieser Header enthält u.a. Quell- und Zieladresse, d.h. Angabe zum Herkunfts- und Bestimmungsort der Daten. Weisen diese irgendwelche Unregelmäßigkeiten auf, z.B. könnten die Pakete von einem unautorisierten Rechner gesendet worden sein, so werden sie blockiert und erreichen das geschützte Rechnernetz nicht.

Proxy-Dienste sind spezialisierte Applikationen oder Serverprogramme, die als Stellvertreter für Benutzer zwischen ihnen und anderen Servern agieren. Die Idee bei einem Proxy-Gateway (circuit-level Gateway) besteht darin, die direkte TCP- (UDP-) Verbindung zwischen der Client-Software auf der Seite des lokalen Netzwerks und dem Server auf der Internetseite (und umgekehrt) zu unterbinden. Ein Proxy-Gateway arbeitet auf der Transportschicht des OSI-Modells. Einen Schritt weiter geht der Applikationsfilter (application-level Gateway). Diese Komponente arbeitet auf der Applikationsschicht des OSI-Modells. Im Gegensatz zum Proxy-Gateway hat es Informationen über die zu filternden Applikationen. Beispielsweise kann sie die in Applikationsprotokollen verwendeten Befehle interpretieren. Ein FTP-Proxy kann bei der Untersuchung der Nutzdaten feststellen, ob diese die Kommandos GET oder PUT beinhalten oder unzulässige aktive Inhalte, d.h. Programmcodes (z.B. Java), die z.B. in einem Webbrowser oder Email-Programm ausgeführt werden und dabei auf Systemressourcen zugreifen können.

Jede der genannten Varianten von Sicherheits-Gatways hat eigene Nach- bzw. Vorteile. Weiterhin gibt es verschiedene Möglichkeiten, ein Sicherheits-Gateway aufzubauen, wobei die ge-

eignete Architektur von den jeweiligen Sicherheitsrichtlinien abhängt [ZCC 00]. Den Sicherheits-Gateways sind jedoch auch Grenzen gesetzt. Beispielsweise bieten sie keinen Schutz gegen betrügerische Insider[5] oder Netzwerkverbindungen, die nicht durch sie eingeleitet werden. Abhilfe sollen hier die sog. Distributed Firewalls leisten [Bell 99]. Weiterhin können sie keinen vollständigen Schutz vor Computerviren oder Trojanern gewährleisten. Hierfür müsste ein Sicherheits-Gateway nicht nur alle Pakete eines Programms erkennen, sondern auch dessen Veränderung durch Viren. Dies ist jedoch eine schwierige Aufgabe. Weiterhin können Viren u.a. durch die Nutzung verschiedener Komprimierungs- und Codierungsverfahren unentdeckt das Sicherheits-Gateway passieren. Schwachstellen können auch durch die mangelhafte Konfiguration eines Sicherheits-Gateway auftreten.

#### 7.1.4.1 Intrusion Detection

Eine andere, häufig Sicherheits-Gateways ergänzende, Sicherheitsmaßnahme ist der Einsatz von Intrusion Detection Systemen. Der Begriff Intrusion stellt einen Oberbegriff für alle Handlungen dar, welche die Sicherheitsrichtlinien eines IT-Systems zu kompromittieren versuchen [Axel 00b]. Das Ziel der Intrusion Detection Systeme (IDS) ist es, die sicherheitsrelevanten Aktionen im System zu überwachen bzw. zu protokollieren, Verletzungsversuche zu erkennen und zu analysieren, Warnmeldungen auszugeben oder geeignete Gegenmaßnahmen automatisch durchzuführen (Intrusion Response System, IRS). Zur Analyse der protokollierten Daten und Aktivitäten (Auditdaten) verfolgen IDS im Wesentlichen zwei Ansätze. Diese sind Anomalie- und Signaturerkennung. Die Anomalieerkennung führt die Verletzung der Sicherheitsrichtlinien auf atypisches Benutzerverhalten zurück. Hierbei nimmt man an, dass Benutzer eine Art Verhaltensmuster bei der Benutzung des Systems aufweisen, und dass dieses Verhalten mit statistischen Methoden beschreibbar ist. Allerdings ist vor allem der Begriff „normales" Verhalten in der Praxis schwer erfassbar und hängt von verschiedenen Faktoren ab. Insbesondere können häufig falsche Fehlermeldungen auftreten. Weiterhin variieren Benutzer ihr Verhalten und somit müssen auch Anomalien entsprechend angepasst werden, wodurch die Gefahr besteht, dass betrügerische Benutzer die Anomalieerkennung systematisch an das sicherheitsverletzende Verhalten „gewöhnen".

Die Signaturerkennung vergleicht die Beschreibung bekannter Verhaltensmuster (z.B. hypothetischer Angriffsszenarien) mit den überwachten Daten und Aktivitäten. Allerdings liegt die Schwierigkeit darin, das Angreiferverhalten bzw. die minimalen Gemeinsamkeiten bestimmter Angriffe aus einer Angriffsklasse genau zu spezifizieren oder noch unbekannte Angriffe zu erkennen. Eine detaillierte Klassifikation und Taxonomie von IDS befindet sich beispielsweise in [Axel 00b, McHu 01, ADD+ 01]. Grenzen und Probleme dieser Systeme werden in [Axel 00a, PtNe 98] diskutiert.

## 7.2 Grundsätzliche Aspekte

Innerhalb dieses Abschnitts werden Fragen zu grundsätzlichen Aspekten der IT-Sicherheit behandelt. Im Vordergrund stehen hier nicht Sicherheitstechnologien, sondern Methoden zur Erstellung von IT-Sicherheitskonzepten sowie zur Messung und Bewertung von IT-Sicherheit. Weiterhin wird nach der Akzeptanz von IT-Sicherheit bei Behörden, Bürgern und in der Wirtschaft und Industrie gefragt [AdSa 01].

### 7.2.1 Bedrohungen

IT-Sicherheit befasst sich neben der Benennung von Maßnahmen zur Erzeugung von IT-Sicherheit in einem vorgegebenen IT-System vor allem mit der Analyse von auf die einzusetzende IT einwirkenden Bedrohungen. In diesem Kon-

[5] Hier kann die sog. Tunneltechnik (Tunneling) verwendet werden, um die Sicherheitsrichtlinien des Sicherheits-Gateway zu umgehen. Das Konzept des Tunneling erlaubt die Einbettung von Datenverkehr beliebiger Protokolle in einem anderen Protokoll. Hierbei werden die Datenpakete gekapselt in einen „Umschlag" eingepackt, mit dem Zweck, sie transparent zu transportieren. Die gekapselten Daten werden dann beim Empfänger interpretiert. Da der Datenstrom verschlüsselt werden kann, erlaubt Tunneling, ein lokales Netzwerk über eine beliebige Entfernung virtuell auszudehnen. Dies wird beispielsweise von SSH verwendet, um Port-Verbindungen von einem Rechner zum anderen durch einen sicheren Kanal (Tunnel) weiterzuleiten (port forwarding).

text geben die Befragten eine Abschätzung der zukünftigen Bedrohungslage für IT-Nutzer und IT einsetzende Institutionen anhand ihrer Einschätzung zu Denial-of-Service Angriffen, zum Ausspähen vertraulicher Daten sowie zu böswilliger Software (z.B. „Trojaner") wieder.

## Ergebnisse

Bei der Abschätzung der Bedrohungslage durch Distributed-Denial-of-Service-Angriffe (DDoS) auf Institutionen geht die überwiegende Mehrzahl der Befragten davon aus, dass diese nie weit verbreitet sein werden (siehe Abbildung 7.1, ①). DDoS-Angriffe sind Angriffe gegen die Verfügbarkeit, bei denen das „Opfer"-System nicht von einem einzelnen Rechner angegriffen und in seiner Funktion behindert wird, sondern gleichzeitig durch viele verschiedene Rechner angegriffen wird. Bei diesen Rechnern hat meist der Angreifer selbst die Kontrolle übernommen, z.B. durch ein eingebrachtes Schadprogramm.

So wird kein ausreichender wirtschaftlicher oder finanzieller Vorteil für potenzielle Angreifer gesehen. Lediglich kriegerische bzw. terroristische Beweggründe könnten eine ausreichende Motivation für solche Angriffe bieten. Der „sportliche Reiz", den die Angriffe zu Beginn hatten, wird nach Einschätzung der Befragten zunehmend an Bedeutung verlieren. Zukünftig wird daher eine größere Gefahr durch organisierte Angriffe mit staatsfeindlichem bzw. terroristischem Hintergrund erwartet als durch so genannte „Skript-Kiddies". Allerdings sehen über ein Viertel der Befragten eine Verbreitung innerhalb der nächsten zwei Jahre als gegeben an. So existieren einfache und weit verbreitete Werkzeuge zur Durchführung von DDoS-Angriffen, deren Verbreitung nicht aufzuhalten ist. Nach Ansicht der Experten sind DDoS-Angriffe heute schon wirksam zu bekämpfen. Es wird davon ausgegangen, dass in den nächsten Jahren Rechner standardmäßig mit Tools zur Erkennung und Abwehr solcher Angriffe ausgestattet sein werden, so dass diese in Zukunft nur in Einzelfällen wirksam und erfolgreich sein werden.

Ähnlich wird die Bedrohungslage bezüglich der missbräuchlichen Nutzung von IT-Systemen privater Nutzer zum Zweck der Durchführung von Denial-of-Service-Angriffen eingeschätzt (siehe Abbildung 7.1, ②). Zusätzliches Gefahrenpotenzial ergibt sich durch die Zunahme breitbandiger Internet-Zugänge für Privatnutzer wie z.B. DSL und den dauerhaften Online-Betrieb privat genutzter IT-Systeme. Viele der Befragten sind der Meinung, dass das Schutzniveau von Privatsystemen zunehmen wird und dass das Bewusstsein über die Abhängigkeiten von einer funktionierenden IT steigt und dies zu einer stärkeren Eigenverantwortlichkeit der Privatnutzer führen wird. Parallel werden verbesserte Möglichkeiten zum Schutz des privaten Rechners vor Missbrauch, insbesondere durch Standardsoftware, entwickelt. Ein wichtiger Faktor zukünftiger Maßnahmen gegen DDoS-Angriffe wird in Betriebssystemen mit verbesserten Sicherheitsmechanismen gesehen.

Betrachtet man die prognostizierte Bedeutung der Angriffe in Abbildung 7.2, so sieht man, dass dem Ausspähen von Unternehmensnetzen mit dem Ziel der unbefugten Kenntnisnahme von Unternehmensdaten die höchste Bedeutung über die nächsten zehn Jahre beigemessen wird. Klassische Ziele sind die (internationale) Wirtschaftsspionage (Technologie- und Know-How-Diebstahl) und die Erlangung von Wettbewerbsvorteilen (z.B. Ausschreibungen, Verträge und Preisinformationen). Als gefährdet werden nahezu alle Unternehmensbereiche genannt, wobei Forschungs- und Entwicklungsabteilungen am stärksten bedroht sind. Die Gefährdung ist auf keine Wirtschaftssparte beschränkt, sondern schließt alle wichtigen Industrie- und Dienstleistungssektoren ein. Die größte Gefährdung wird in Unternehmen mit großen werthaltigen Entwicklungsbereichen (Pharma, Automobilindustrie, Softwareentwicklung) gesehen.

Die Befragten werten in diesem Zusammenhang die Beteiligung fremder Nachrichtendienste bei der Technologiespionage als sehr problematisch und weisen auf den Schaden hin, der der heimischen Wirtschaft dadurch entsteht [Euro 01]. Der leichte Rückgang in der erwarteten Bedrohung im Zeitraum von fünf bis zehn Jahren wird mit dem zunehmendem Sicherheitsbewusstsein und dem dadurch höheren Aufwand für Angriffe erklärt.

DISTRIBUTED-DENIAL-OF-SERVICE-ANGRIFFE: werden auch in Zukunft nur vereinzelt auftreten. Der wirtschaftliche und finanzielle Anreiz scheint für Angreifer zu gering.

WIRTSCHAFTSSPIONAGE: Dem Ausspähen von Unternehmensnetzen wird auch weiterhin die größte Bedeutung beigemessen.

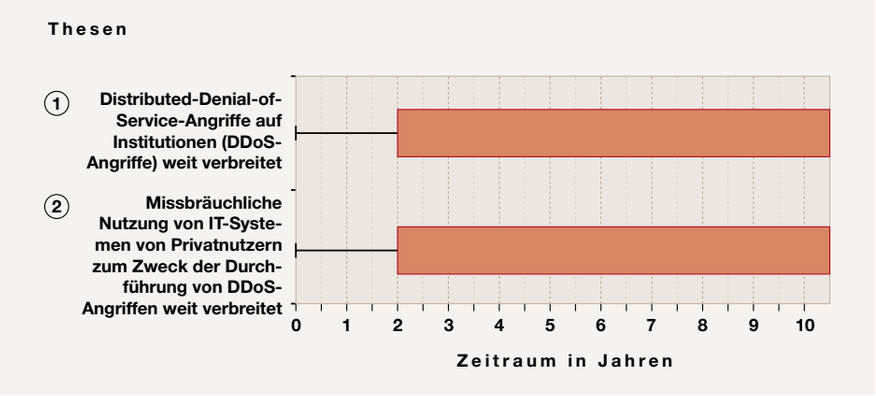



Abbildung 7.1: Ergebnisse der Thesen zu Distributed-Denial-of-Service-Angriffen

TROJANISCHE PFERDE: Die derzeit größte Gefährdung geht von Programmen mit Schadfunktion wie Viren, Trojanern oder Dialer-Programmen aus. Allerdings wird diese Bedrohung über die nächsten Jahre sinken.

SCHUTZFUNKTIONEN IN ZUKÜNFTIGEN BETRIEBSSYSTEMEN: Derartige Funktionen gelten als wichtiger Baustein für die Verbesserung der Systemsicherheit.

Eine stetig steigende Bedeutung (ausgehend von einem niedrigeren Niveau) wird dem Ausspähen von privater IT mit dem Ziel der unbefugten Kenntnisnahme persönlicher Daten beigemessen. Dabei stehen neben Daten mit vertraulichem Charakter vor allem Finanzdaten im Vordergrund. Lukratives Ziel für potenzielle Angreifer ist beispielsweise der Kreditkartenbetrug oder auch das Erpressungspotenzial abgehörter Informationen. Die Sicherheit privater IT gewinnt vor dem Hintergrund zunehmender Vermischung privater und geschäftlicher Aktivitäten auf dem gleichen Rechner zunehmend an Bedeutung.

Die derzeit größte Bedeutung wird der Gefährdung durch das in Umlauf bringen von Programmen mit Schadfunktionen wie Computerviren, trojanische Pferde oder Dialer-Programmen beigemessen. Faktoren sind neben der leicht möglichen Verbreitung von böswilliger Software durch einen hohen Grad der Vernetzung die große Wirkung, die diese mit verhältnismäßig geringen Mitteln erzielen. Langfristig wird allerdings von einem Sinken der Bedrohung ausgegangen.

Im Bereich des kommerziellen IT-Einsatzes, also bei Unternehmen und in der öffentlichen Verwaltung, werden die Ziele solcher Angriffe vor allem in der Beschaffung von Informationen, in der gezielten Sabotage, aber auch in der Befriedigung von Spieltrieb gesehen. Oftmals dient die Einbringung von Code der Vorbereitung und Unterstützung (Enabler) vieler Arten von Angriffen (DDoS, Spionage, Hacking). Für die betroffenen Institutionen ist nicht nur der mögliche finanzielle Schaden und der Arbeitsaufwand zur Behebung von Bedeutung, sondern zunehmend auch der dadurch resultierende Image-Schaden. Diese Einschätzung wird auch durch die Ergebnisse der KES-Studie [VoVo 02] untermauert, in der dem Imageverlust die größte Bedeutung bei der Risikobewertung beigemessen wird.

Insgesamt wird von einer rückläufigen Gefährdung aufgrund verbesserter, unternehmensweiter Sicherheitskonzepte ausgegangen, die sich in den Institutionen weiter etablieren. Viel wird in diesem Zusammenhang von verbesserten Schutzfunktionen in zukünftigen Betriebssystemen erwartet [PRS+ 01, StSa 03] und von Sicherheitsinitiativen wie Microsoft's Palladium [Manf 02], die mittlerweile in "Next-Generation Secure Computing Base" (NGSCB) umbenannt wurde, und der Trusted Computing Platform Alliance (TCPA). TCPA [TCPA 03] ist ein Zusammenschluss von Hardware- und Softwareherstellern und wurde von IBM, Intel, Microsoft, Infineon, National und Atmel mit dem vorrangigen Ziel initiiert, eine vertrauenswürdige Sicherheitsplattform in Hardware für zukünftige Systeme zu spezifizieren.

Im Bereich der privat genutzten IT wird die Gefährdung durch Schadprogramme weiterhin eine bedeutende Rolle spielen. Die Sicherheitssensibilisierung ist bei privaten IT-Nutzern noch zu wenig ausgeprägt, obwohl die privaten IT-Systeme zunehmend für sensible Aufgaben genutzt werden.

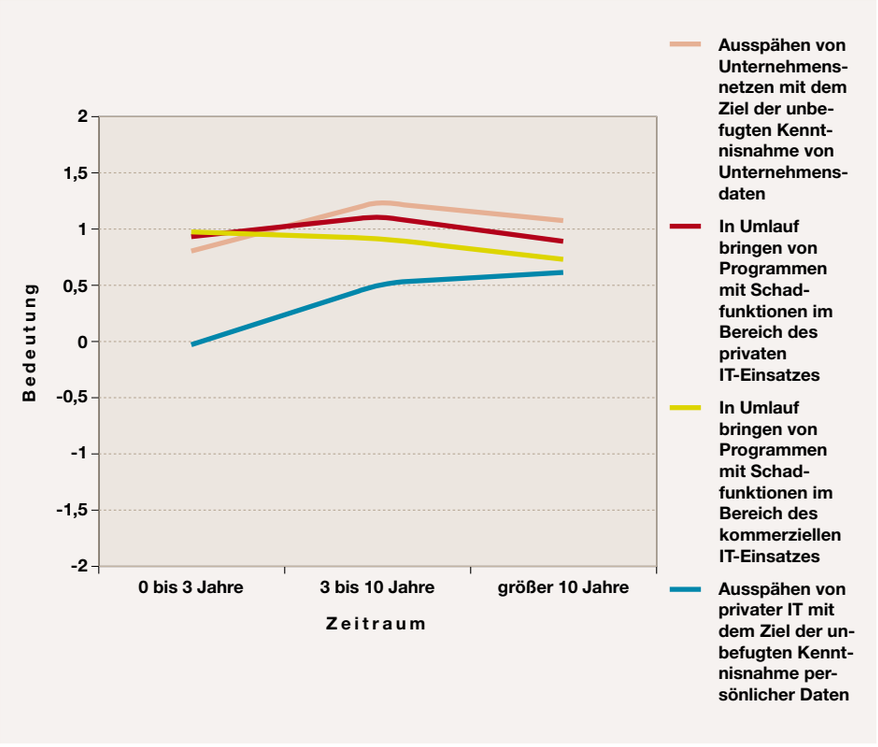



Abbildung 7.2: Bedeutung unterschiedlicher Angriffe auf Unternehmensnetzwerke und private IT

Neben möglichen finanziellen Schäden durch Betrugssoftware (wie z.B. beim elektronischen Kauf oder durch Erschleichen von Leistungen durch Dialer-Programme) ist für den privaten Nutzer der Zeitaufwand zum Beheben der Schäden bedeutsam und hat negative Auswirkungen auf die Akzeptanz von IT-Systemen im Allgemeinen.

## Zusammenfassung

Insgesamt kommt die Mehrzahl der Experten in ihrer Bewertung zur überraschenden Einschätzung, dass langfristig der tatsächliche Grad der Bedrohung rückläufig sein wird. Dies wird im Wesentlichen durch verbesserte Techniken zur Abwehr und durch die zunehmende Sensibilität beim Nutzer - sowohl im kommerziellen als auch im privaten Bereich - begründet. Zusammenfassend kann man festhalten:

- Distributed-Denial-of-Service-Angriffe auf Institutionen sowie die missbräuchliche Nutzung von IT-Systemen pivater Nutzer zum Zweck der Durchführung von Denial-of-Service-Angriffen werden weiterhin nur vereinzelt auftreten.

- Dem Ausspähen von Unternehmensnetzen wird über die nächsten zehn Jahre die höchste Bedeutung beigemessen. Für das Ausspähen privater IT wird hingegen die geringste, allerdings stetig steigende Bedeutung erwartet.

- Die derzeit größte Bedeutung hat nach Ansicht der Befragten das Einbringen von Schadprogrammen im kommerziellen und privaten Bereich. Allerdings wird von einem kontinuierlichen Bedeutungsverlust bis 2013 ausgegangen.

### 7.2.2 Methodik-Trends

Zum Erreichen von umfassender IT-Sicherheit haben sich verschiedene Methoden, mit zum Teil unterschiedlichen Vorgehensweisen, etabliert. Im folgenden Abschnitt bewerten die Experten die vier wichtigsten Methoden in ihrer prognostizierten Entwickung sowie deren eigenen Einsatz.

Die älteste betrachtete Methodik setzt ein analytisches Vorgehens voraus, wie es im IT-Sicherheitshandbuch des BSI [BSI 92] dargestellt ist. Dieses Verfahren basiert u.a. auf einer formellen Risikoabschätzung (Risikoanalyse) und ist daher bei umfassenden Sicherheitsanalysen mit erheblichem Aufwand verbunden, wenn es undifferenziert auf alle IT-Anwendungen angewandt wird.

Für IT-Anwender, deren zu schützende IT-Systeme und Informationen höchstens einen mittleren Schutzbedarf (gemäß Kapitel 2 in [BSI 01]) haben, empfiehlt sich die Anwendung des IT-Grundschutzhandbuches [BSI 01]. Das IT-Grundschutzhandbuch enthält pauschale Maßnahmenempfehlungen, die für den mittleren Schutzbedarf hinreichend sind. Seine modulare Struktur ermöglicht die Nachbildung von IT-Systemen durch die Zusammensetzung verschiedener Bausteine. Diese Bausteine enthalten die als wahrscheinlich angenommenen Gefährdungen und die dagegen empfohlenen Maßnahmen. Auf Grundlage des IT-Grundschutzes ist die Durchführung eines Basis-Sicherheits-Checks in Form von Checklisten möglich.

Die Common Criteria for Information Technology Security Evaluation (CC) [Comm 99] bzw. in ihrer deutschen Bezeichnung „Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik" sind eine international anerkannte Basis für die Beschreibung von IT-Sicherheit. Sie sind 1998 unter Beteiligung Deutschlands, Frankreichs, Großbritanniens, Kanadas, der Niederlande und der USA abschließend fertiggestellt worden und mittlerweile im ISO-Standard 15408 standardisiert. Sie sind für die Bewertung der Sicherheitseigenschaften praktisch aller informationstechnischen Produkte und Systeme geeignet. Die Kriterien stellen eine Möglichkeit bereit, flexibel IT-Sicherheitsanforderungen zu beschreiben und Ergebnisse von IT-Sicherheitsevaluierungen grenzüberschreitend anzuerkennen

Der aus der britischen Norm BSI7799 (Code of Practice for Information Security Management des British Standards Institute) entstandene internationale Standard ISO/IEC 17799 [ISO 17799] definiert Standards zum Aufbau eines Managementsystems für die Sicherheit von Informationstechnologie. Die Philosophie des Standards sieht keine Forderung nach konkreten Maßnahmen vor, sondern lediglich eine Auflistung von Aspekten, die zu beachten sind. Die Liste der Aspekte kann (und soll) systemspezifisch erweitert werden, denn BSI7799 erhebt keinen Anspruch auf Vollständigkeit. Im Folgenden sind die Ergebnisse der Befragung zur Verbreitung dieser unterschiedlichen Methoden erläutert.

#### Ergebnisse

Bei der Bewertung probabilistischer Methoden wie dem IT-Sicherheitshandbuch des BSI ist eine große Diskrepanz der Expertenmeinungen festzustellen. Wie in Abbildung 7.3, ① ersichtlich ist, rechnet sogar ein Viertel der Befragten damit, dass diese Methode überhaupt nicht zum Einsatz kommen wird. Obwohl als Zielgruppen Bereiche mit hoher Bedrohung bzw. hohen objektiven oder subjektiven Schutzanforderungen wie Behörden und staatliche (auch privatisierte) Einrichtungen sowie Banken und Versicherungen gesehen werden, können probabilistische Methoden wie das IT-Sicherheitshandbuch auch für kleine und mittlere Unternehmen (KMUs) ohne ausgebildete Sicherheitsfachleute interessant werden. Derzeit wird die Methodik, die vielfach noch unbekannt ist, als zu aufwendig für kleinere Unternehmen angesehen.

Das IT-Grundschutzhandbuch des BSI wird nach Ansicht der Befragten etwas früher, in etwa drei Jahren, an übergeordneter Bedeutung gewinnen (siehe Abbildung 7.3. ②). Aber auch hier sieht etwa ein Viertel keine zukünftige Rolle der Methodik. Derzeit werden Haupteinsatzbereiche in Behörden und öffentlichen Institutionen gesehen. Grundsätzlich ist der Einsatz

in allen Bereichen sinnvoll. Zukünftig wird der Einsatz insbesondere für KMU's und Unternehmen/Institutionen, die zu dem Zeitpunkt noch keine Sicherheitsrichtlinien erarbeitet haben, als interessant angesehen, da das Grundschutzhandbuch unmittelbar anwendbar ist und das Schutzniveau ohne konzeptionelle Vorphase erhöht. Weiterhin wird die Verbreitung der Methodik durch die Akkreditierung von Prüfern durch das BSI (Grundschutzaudit) erleichtert. Viele der Befragten sehen im IT-Grundschutzhandbuch einen mittelfristigen Quasistandard, obgleich dieser nur Minimalanforderungen durchsetzt. Als problematisch wird die schnelle Veralterung angesehen, die die Gefahr birgt, aktuelle Entwicklungen nicht angemessen zu berücksichtigen.

Die Verbreitung der Bewertung und Prüfung der Sicherheit in der Informationstechnik nach den Kriterien der Common Criteria wird durch die Befragten unterschiedlich gesehen (siehe Abbildung 7.3, ③). Einerseits vertritt ein Teil der Experten die Meinung, dass die Methodik zu generisch und theoretisch und damit zu aufwendig und zu teuer ist. Darüber hinaus verfügten Einzelproduktbetrachtungen über wenig Relevanz. Skeptisch wird grundsätzlich die statische Analyse dynamischer Systeme gesehen und die damit verbundene Problematik des Versionswechsels. Auch der Bewertung großer komplexer Systemen nach CC wird aufgrund des Aufwandes als derzeit nicht rentabel angesehen. So sehen einige Experten die Zukunft der CC nur in wenigen regulierten Bereichen.

Andererseits wird eine weite Verbreitung innerhalb der nächsten fünf Jahre erwartet und auf den dringenden Bedarf zertifizierter Produkte und die Notwendigkeit zur internationalen Vergleichbarkeit von Sicherheitsprodukten hingewiesen. Schon heute ist der Einsatz zertifizierter Produkte im Bereich qualifizierter elektronischer Signaturen gesetzlich vorgeschrieben, eine Ausweitung auf Produktentwicklungen im Hochsicherheitsbreich, bei kritischen Infrastrukturen und der Einsatz bei elektronischen Geschäftsprozessen wird zeitnah erwartet. Darüberhinaus wird die Methodik als Voraussetzung zur verlässlichen Kopplung heterogener Systeme benötigt. Die bisher aufgeführten Methoden werden überwiegend als zu generisch und zu theoretisch angesehen. Darüber hinaus erfordere die Individualität und Komplexität der Systeme tiefergehende Betrachtungen.

Der Management-orientierte Standard ISO 17799 ist im Vergleich zu anderen Berwertungsmethodiken deutlich weniger bekannt. Anwendungsbereiche werden bei großen und globalen Konzernen gesehen, insbesondere bei der Analyse und Bewertung komplexer IT-Systeme. Obwohl die Mehrzahl der Befragten bereits eine weite internationale Verbreitung als gegeben betrachtet und für viele Dienstleister eine Referenz auf anerkannte Standards und Zertifikate wichtig ist, erwartet man keine Durchsetzung des Standards in Deutschland (Abbildung 7.3, ④).

Die weite Verbreitung der Gütesiegel und Zertifikate zur Bestätigung eines bestehenden IT-Sicherheitsniveaus wird von der Mehrheit der Experten in fünf Jahren erwartet (siehe Abbildung 7.3, ⑤). Viele der Befragten sind allerdings skeptisch, was die Verbreitung über den Bereich hinaus angeht, in denen Zertifikate vorgeschrieben sind. Mögliche Hinderungsgründe hierfür werden vor allem im Aufwand und in den Kosten solcher Zertifizierungen gesehen. Die Akzeptanz solcher Zertifikate setzt voraus, dass es für Anbieter und Verbraucher einheitliche und transparente Bewertungsrichtlinien gibt. So wird erwartet, dass sich der „Markt" für Zertifikate und Gütesiegel in den nächsten acht Jahren bereinigt haben wird. Zertifikate werden nach Ansicht der Experten die Rolle eines Qualitätssiegels für Hersteller einnehmen, vergleichbar dem GS-Zeichen oder Bewertungen der Stiftung Warentest, und bilden damit einem vertrauenswürdigen Nachweis des Sicherheitsniveaus. Interessant wird auch die Integration in bestehende Unternehmenszertifizierungen wie beispielsweise ISO 9000 gesehen. Unterstützt wird dies durch die Forderung, bei Unternehmensrevisionen den Zustand der IT-Sicherheit in die Bewertungen mit aufzunehmen.

Neben der Einschätzung verschiedener Methoden gaben die Befragten an, welche der im vorigenen Abschnitt behandelten Methoden zur Erzeugung und Bewertung von IT-Sicherheit von ihnen zukünftig selbst eingesetzt werden und innerhalb welchen Zeitrahmens sie den Einsatz der jeweiligen Methode beabsichtigen.

QUASISTANDARD: Das IT-Grundschutzhandbuch wird bereits in 3 Jahren weit verbreitet sein.

GÜTESIEGEL UND ZERTIFIKATE: Diese werden zur Bestätigung eines bestehenden IT-Sicherheitsniveaus mehrheitlich in 5 Jahren erwartet. Der Markt für solche Zertifikate wird sich in etwa 8 Jahren bereinigt haben.

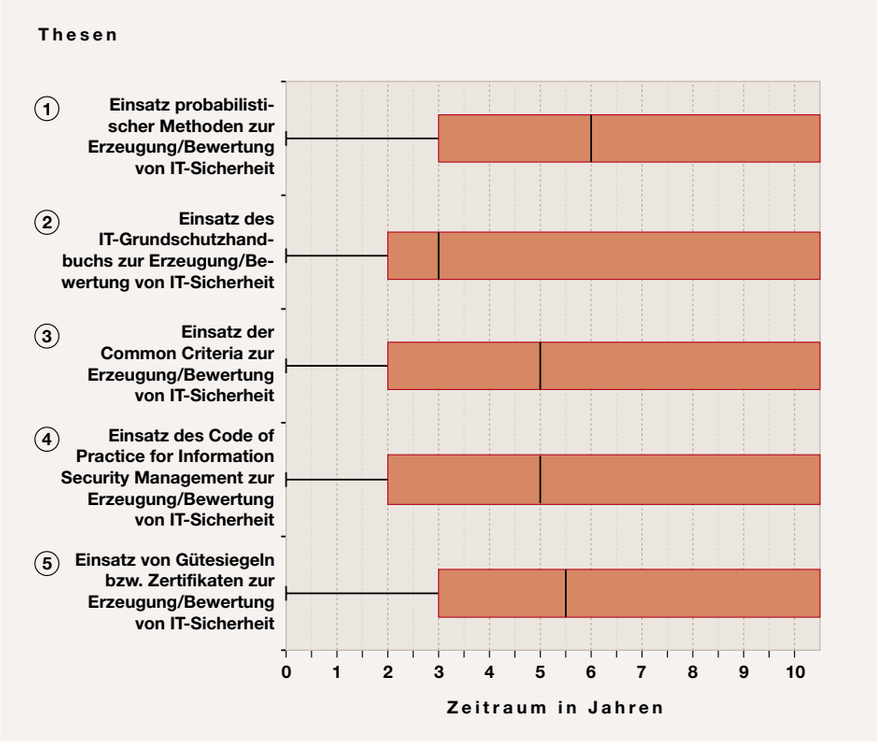



Abbildung 7.3: Ergebnisse der Thesen zu Methoden für die Erzeugung und Bewertung von IT-Sicherheit

Bei der Frage nach einem Zeitrahmen für den eigenen Einsatz der Methoden differieren die Angaben der Befragten. Wie in Abbildung 7.4 ersichtlich, gibt jeweils die Mehrheit der Befragten an, die jeweilige Methodik innerhalb der nächsten zwei bis drei Jahre einsetzen zu wollen. Jeweils ein Viertel der Befragten plant jedoch keinen Einsatz der jeweiligen Methodik. Lediglich die CC-Methodik wird nach Abbildung 7.4, ③ von der Mehrheit der Befragten bereits eingesetzt. Das Ergebnis erscheint ist im Hinblick auf die allgemeine Verbreitung der genannten Methoden ungewöhnlich, ist allerdings durch den speziellen Personenkreis der Befragten begründet.

Das IT-Sicherheitshandbuch und das IT-Grundschutzhandbuch werden vornehmlich zur Erstellung von IT-Sicherheitskonzepten und zur Analyse und Bewertung kompletter IT-Systeme eingesetzt. Das IT-Grundschutzhandbuch wird hauptsächlich im und für den Behördenbereich und zur Basisschutzermittlung bzgl. technischer und organisatorischer Maßnahmen verwendet, beispielsweise zum Sicherheitscheck bestehender Systeme und zur Grundschutz-Evaluierung und -zertifizierung. Diejenigen Befragten, die nach eigenen Angaben die Methodik des IT-Sicherheitshandbuchs bzw. des IT-Grundschutzhandbuchs nicht einsetzen wollen, begründeten dies vor allem mit der mangelnden internationalen Verbreitung der Methoden.

Die Common-Criteria-Methodik wird vor allem im E-Commerce Bereich und im Umfeld von Banken und Versicherungen für die Evaluierung und Zertifizierung von eigenen Produkten eingesetzt. Insbesondere global ausgerichtete Unternehmen greifen auf die CC als internationalen Standard zurück. Diejenigen, die diese Methodik nicht einsetzen wollen, verweisen auf den erheblichen Aufwand des Verfahrens und die damit verzögerte Produkteinführung, „Time to Market“, für neue Produkte.

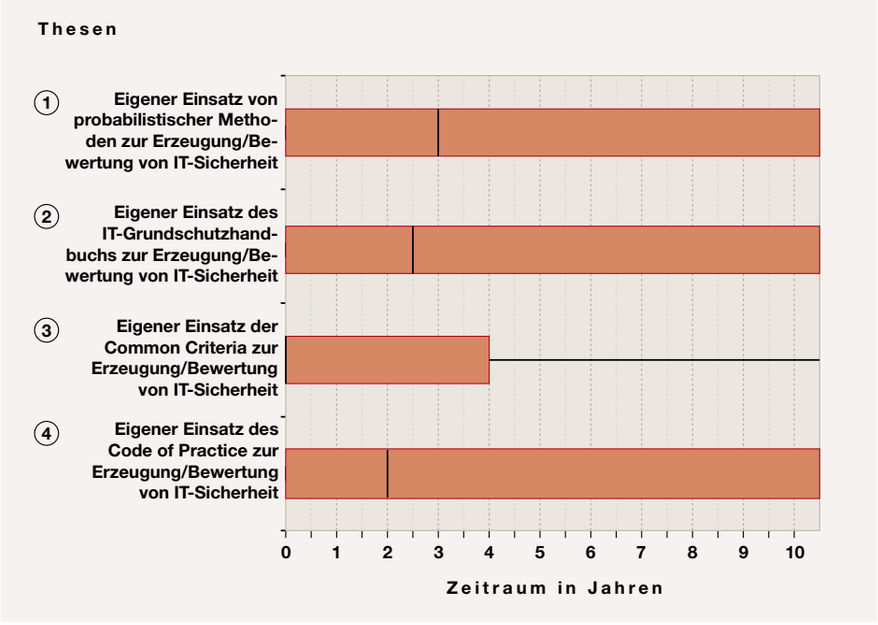



Abbildung 7.4: Ergebnisse der Thesen zum eigenen Einsatz verschiedener Methoden zur Bewertung und Erzeugung von IT-Sicherheit

### Zusammenfassung

Bei der Bewertung der Methodik-Trends gehen die Meinungen der Experten zum Teil erheblich auseinander. Während jeweils ein Teil der Befragten von keiner nennenswerten Verbreitung bzw. von keinem eigenen Einsatz der jeweiligen Methodik ausgeht, erstellt die Mehrheit der Befragten eine positive Prognose.

- Bei allen genannten Methoden sieht jeweils eine Mehrheit der Experten zwischen 2006 und 2009 eine Bedeutungszunahme.
- Die weite Verbreitung von Zertifikaten und Gütesiegeln zur Bestätigung eines bestehenden Sicherheitsniveaus wird hingegen einhellig bis 2008 erwartet, insbesondere im regulierten Bereichen.
- Die meisten der Befragten planen bis 2006 den eigenen Einsatz der jeweiligen Methodik, während jeweils über ein Viertel die Methodik überhaupt nicht einsetzen will. Lediglich die CC wird bereits überwiegend eingesetzt.

## 7.2.3 Akzeptanz und Status der IT-Sicherheit

Eine wichtige Voraussetzung für die Etablierung von IT-Sicherheit ist die Akzeptanz der Maßnahmen durch die Benutzer. Neben der bestehenden und erwarteten Sicherheitssensibilisierung spielt dabei auch die Abwägung der Benutzer zwischen Sicherheit und Funktionalität eine wichtige Rolle. In diesem Kontext werden im nächsten Abschnitt die Einschätzung der befragten Experten zur IT-Sicherheit in Behörden, in der Industrie sowie in der privaten IT-Nutzung betrachtet.

### Ergebnisse

Im Rahmen der Analyse von Akzeptanz und Status der IT-Sicherheit wurde gefragt, in wie weit IT-Sicherheit von den Beschäftigten der Behörden und öffentlichen Einrichtungen als notwendig und sinnvoll angesehen wird und ob durch die Behördenleitung veranlasste IT-Sicherheitsmaßnahmen von den Beschäftigten akzeptiert und gewissenhaft umgesetzt werden. Die Mehrzahl der Experten betrachtet diesen Zustand in etwa fünf Jahren als erreicht. (Abbildung 7.5, ①).

Abweichend davon erwartet rund ein Viertel der Experten, dass dieser Zustand nicht in absehbarer Zeit erreicht wird. Zum einen sei die Situation noch nicht reif und es seien „noch einige Skandale nötig", zum anderen wird darauf verwiesen, dass dies mit Blick auf die üblichen Anforderungen zum Teil nicht zu vermitteln und zum Teil vermittelbar, aber nicht zu erreichen sei. Vielfach werden Maßnahmen als notwendig und sinnvoll erkannt, eine gewissenhafte Umsetzung erscheint jedoch nahezu unmöglich. Insbesondere werden zu wenig natürliche Anreize für die Mitarbeiter gesehen. Ausnahmen hiervon sind hochsensible Bereiche, in denen Sicherheit traditionell eine große Rolle spielt und mit viel Aufwand aufrechterhalten wird, z.B. im Verteidigungsbereich.

SITUATION NOCH NICHT REIF: Viele der Befragten bleiben bzgl. ihrer Einschätzung der Akzeptanz von IT-Sicherheit skeptisch. Die Mehrheit erwartet jedoch eine Sensibilisierung innerhalb von 5 Jahren.

Die Sicherheitsorganisation wird nach Ansicht der Befragten in knapp vier Jahren integraler Bestandteil der Behördenorganisation sein (Abbildung 7.5, ②). Vereinzelt wurde die Prognose geäußert, dass die Sicherheitsorganisation verstärkt ausgelagert wird. Die verbleibenden Funktionen und Aufgaben werden dann in bestehende Strukturen eingebettet und nur ausnahmsweise als eigene Organisationsbestandteile sichtbar sein. Bereits in drei Jahren wird die Sicherheitstechnik ein integraler Bestandteil der in der Behörde verwendeten Informationstechnik sein (Abbildung 7.5, ③).

IN BESTEHENDE STRUKTUREN EINGEBETTET: Nur ausnahmsweise dürfte die Sicherheitsorganisation als eigener Organisationsbestandteil sichtbar werden.

MODETHEMA SICHERHEIT: Viele sehen im derzeitigen Medieninteresse nur eine vorübergehende Erscheinung.

Bei den Unternehmen wird die Sicherheitssensibilisierung zeitnaher gesehen. So erwarten die Experten, dass die IT-Sicherheit von den Beschäftigten der Unternehmen bereits in drei Jahren als notwendig und sinnvoll angesehen wird (Abbildung 7.5, ④). Durch die Unternehmensleitung veranlasste IT-Sicherheitsmaßnahmen würden dann von den Beschäftigten akzeptiert und gewissenhaft umgesetzt werden. Einige sehen allerdings einen ungelösten und inhärenten Interessenskonflikt zwischen den Beschäftigten und der IT-Sicherheit. Auch die Bequemlichkeit wird oft als Grund für diese Einschätzung genannt, so dass rund ein Viertel nicht mit einer Akzeptanz durch die Beschäftigten rechnet.

FEHLENDES PROBLEMBEWUSSTSEIN: Die eigene Gefährdung wird insbesondere im Privatbereich zu niedrig eingestuft.

NEUGIERDE UND BEQUEMLICHKEIT: verleiten oftmals zu unvorsichtigem Handeln.

In drei Jahren wird nach Ansicht der Experten die Sicherheitsorganisation ein integraler Bestandteil der Unternehmensorganisation sein (Abbildung 7.5, ⑤). Es wird davon ausgegangen, dass in zwei Jahren die Sicherheitstechnik ein integraler Bestandteil der im Unternehmen verwendeten Informationstechnik sein wird; obgleich sich dies schwieriger gestalten dürfte, da es die Umgestaltung z.B. von Abnahmeprozessen erfordert, die häufig unter starkem zeitlichen Druck stehen (Abbildung 7.5, ⑥).

SCHUTZMECHANISMEN: Viele Nutzer verbinden nach wie vor lediglich Anti-Viren-Software mit Schutzmechanismen.

Zur Einschätzung des Bewusstseins beim Bürger wurde abgefragt, wann beim privaten Einsatz von Informationstechnik sicherheitsbezogene Produkteigenschaften ein Entscheidungskriterium beim Kauf sein werden. Die Mehrzahl der Experten geht davon aus, dass dies in etwa vier Jahren der Fall sein wird (Abbildung 7.5, ⑦). Das steigende Sicherheitsinteresse wird teilweise auch auf das Medieninteresse zurückgeführt und birgt die Gefahr, als Modethema Sicherheit wieder aus dem öffentlichen Interesse zu verschwinden. Einige der Befragten kritisieren insbesondere ein fehlendes Problembewusstsein: Das subjektive, persönliche Risiko wird als nicht hoch eingestuft. Damit erhält die Sicherheit, im Vergleich zur Funktionalität, nicht den nötigen Stellenwert.

Darüber hinaus wurden die Experten nach ihrer Einschätzung gefragt, ob zur Gewährleistung von Sicherheitsfunktionen Einschränkungen der Funktionalität hingenommen werden. Dies würde beispielsweise bedeuten, dass der private Internetnutzer eine Seite, die er sich nur unter Verwendung aktiver Inhalte ansehen kann, nicht besuchen wird. Die Experten gehen überwiegend davon aus, dass derartige Einschränkungen nie akzeptiert würden (Abbildung 7.5, ⑧). Neugierde und Bequemlichkeit verleiten oftmals zu unvorsichtigem Handeln. So wird erwartet, dass der Benutzer versuchen wird, die Risiken zu minimieren und trotzdem auf die gewünschten Information zuzugreifen. Lediglich ein Viertel der Befragten erwarten innerhalb von fünf Jahren eine andere Entwicklung.

Abbildung 7.6 zeigt die Bedeutung der Sicherheitseigenschaften für den privaten Einsatz. Aus der Grafik ist erkennbar, dass die Bedeutung der Eigenschaften Betriebsstabilität, Zuverlässigkeit und Fehlerfreiheit sowie das Vorhandensein von Schutzmechanismen gegen unbefugte Manipulation in den nächsten drei Jahren ansteigen wird und auf einem hohen Niveau über die nächsten zehn Jahre ver-

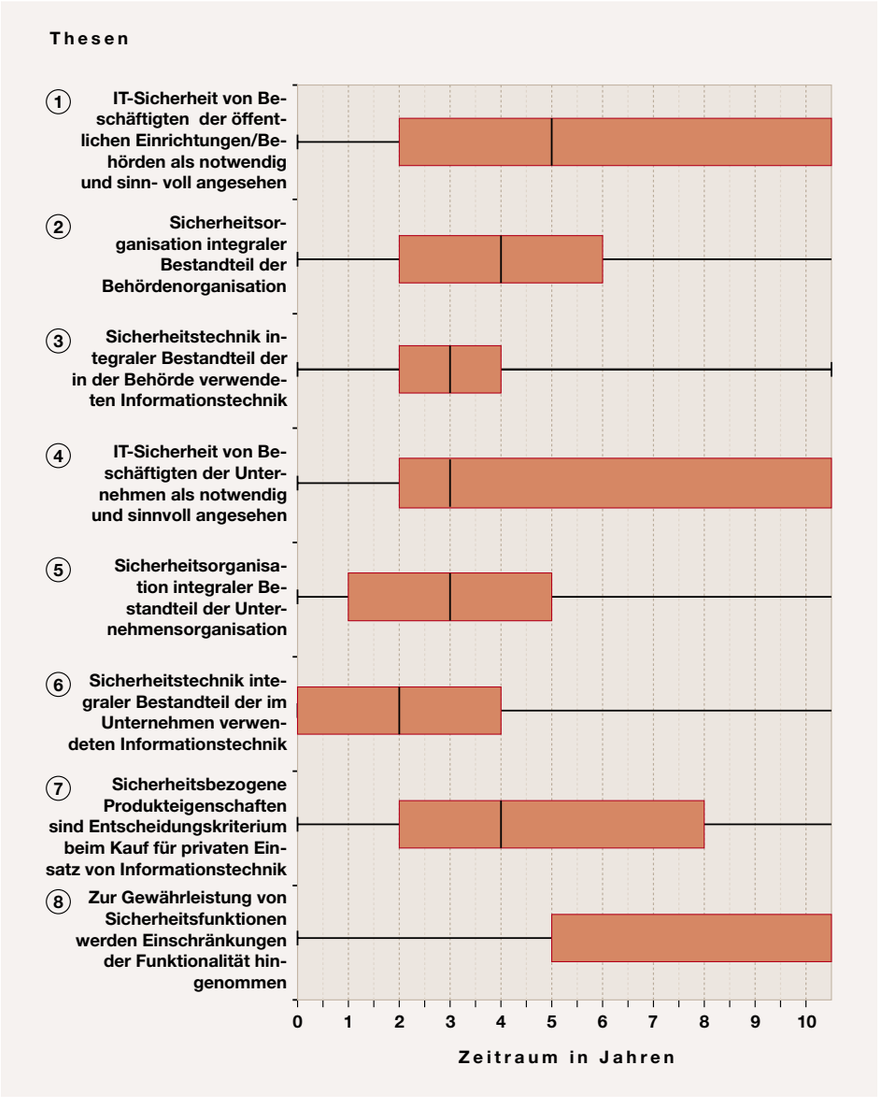



Abbildung 7.5: Ergebnisse der Thesen zur Akzeptanz von IT-Sicherheit in öffentlichen Einrichtungen, Unternehmen und bei den Bürgern

bleibt. Dabei wird die derzeitige Bedeutung von Schutzmechanismen gegen unbefugte Manipulation am geringsten eingeschätzt. Die Zuverlässigkeit der Betriebsstabilität und Fehlerfreiheit wird in rechtsverbindlichen Bereichen und solchen mit finanziellen Folgen, sowie insbesondere im Hinblick auf zukünftige Anwendungen in integrierten Gebäudesystemen [IGS 01], bei denen verschiedene Haushaltsgeräte und -systeme miteinander kommunizieren, als wichtig erachtet.

Allerdings ist derzeit die Sensibilität, auch aufgrund geringerer Medienverbreitung der Schadenswirkung, nicht so offenkundig wie bei böswilligen Angriffen. Eine gewisse Anzahl an Fehlern wird immer toleriert. Diese Schwelle wird allerdings nach Ansicht der Experten sinken, Nachbesserungen für teuer gekaufte Software werden dann nur noch selten akzeptiert werden. Dagegen steigt die Sensibilität im Bereich der Schutzmechanismen gegen unbefugte Manipulation deutlich stärker. Insbesondere werden die Mechanismen nach ersten persönlichen Schäden eingesetzt werden. Problematisch ist jedoch, dass viele Nutzer nach wie vor mit Schutzmaßnahmen lediglich Antiviren-Software verbinden.

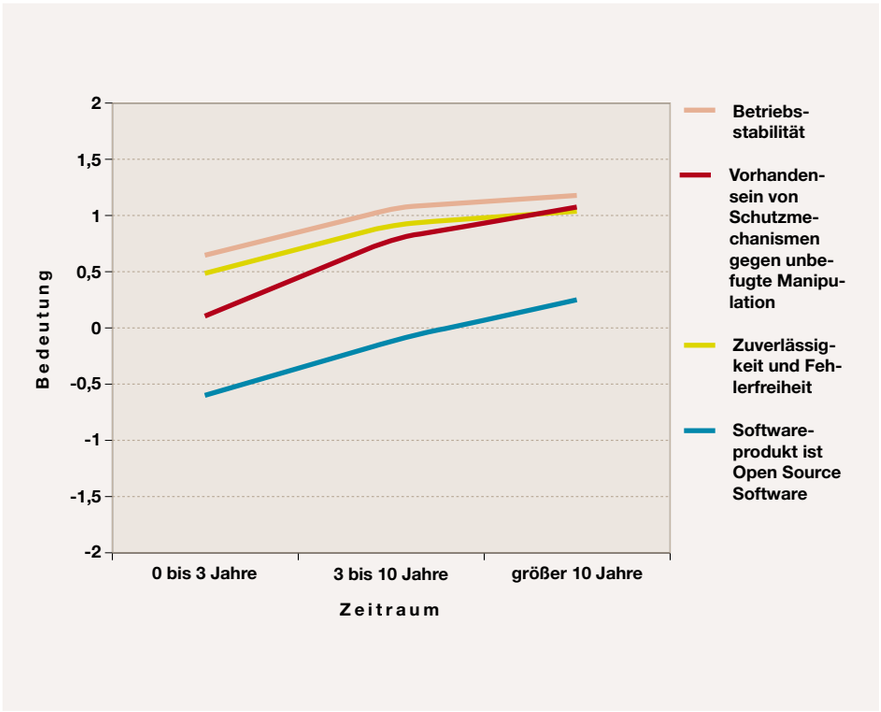



Abbildung 7.6: Bedeutung unterschiedlicher Sicherheitseigenschaften beim privaten Einsatz von IT

Eine Eigenschaft, die seit einigen Jahren verstärkt als Paradigma zum verfügbar machen von Sicherheit eingebracht wird, erwächst aus dem Open-Source-Konzept. Dieses kann dazu dienen, das Vertrauen des Benutzers gegenüber dem Hersteller in die Software zu erhöhen. Open Source ist kein alleiniges Allheilmittel für Sicherheit [Neum 00, KKP 00]. So ist die Offenlegung des Quellcodes nur so gut, wie ihn auch tatsächlich Fachkundige analysieren, ihre Resultate veröffentlichen und nicht im Sinn haben, gefundene Fehler für Angriffe auszunutzen. Derzeit ist es weitestgehend dem Zufall überlassen, welcher Quellcode von der Internet-Community evaluiert wird und wie schnell und gut die Fehler behoben werden [Send 01]. Weiterhin bewirkt die prinzipiell als positiv einzustufende Änderungsmöglichkeit durch den Anwender, dass sich bei ihm durch bereitgestellte Patches sicherheitsbedenkliche Fehler einschleichen können und es Angreifern leichter möglich ist, direkt vor der Übersetzung trojanische Pferde in den offengelegten Code einzubauen [CERT 02b]. Das Konzept wird als Sicherheitseigenschaft derzeit weniger bedeutend eingestuft. Allerdings wird erwartet, dass die Bedeutung über die nächsten zehn Jahre deutlich zunehmen wird. Als Einsatzbereiche werden vor allem Behörden und wissenschaftliche Einrichtungen gesehen, sowie Anwendungen mit Sicherheitsfunktionen. Für die Masse der privaten Nutzer wird allerdings keine Relevanz erwartet.

## Zusammenfassung

Die Experten äussern zum Teil sehr unterschiedliche Erwartungen bezüglich der Akzeptanz von IT-Sicherheit durch die Benutzer sowohl im behördlichen als auch im industriellen Bereich. Während eine Mehrzahl der Befragten eine vergleichsweise zeitnahe Sensibilisierung der Mitarbeiter und Angestellten sieht, glauben viele nicht an eine gewissenhafte Beachtung von IT-Sicherheitsrichtlinien. Zusammenfassed kann man feststellen:

- Sowohl im behördlichen als auch im industriellen Bereich erwartet die Mehrzahl der Befragten eine zeitnahe Sensibilisierung. Gleichzeitig er-

wartet eine große Zahl der Befragten überhaupt keine Zunahme der Sensibilisierung in Fragen der IT-Sicherheit in dem betrachteten Zeitraum.

- Die Integration der Sicherheitsorganisation in die Behörden- bzw. Unternehmensorganisation sowie die Integration der Sicherheitstechnik in die jeweilige Informationstechnik wird bis 2007 erwartet.

- Bei der Bewertung der Akzeptanz privater Nutzer gehen die Befragten davon aus, dass bis 2007 sicherheitsbezogene Produkteigenschaften Entscheidungsrelevanz erlangen. Dagegen wird nicht erwartet, dass in absehbarer Zeit Einschränkungen in der Funktionalität zur Gewährleistung von Sicherheitsfunktionen hingenommen werden.

## 7.3 Ausgewählte Sicherheitstechnologien

Im folgenden Abschnitt finden sich Bewertungen und Einschätzungen zu Sicherheitstechnologien, die nicht nur für sich alleine stehen, sondern in verschiedenen Ausprägungen innerhalb anderer Technologiebereiche immer wieder auftauchen. Um eine redundante Behandlung zu vermeiden, werden solche ausgewählten Sicherheitstechnologien an dieser Stelle gesammelt betrachtet.

### 7.3.1 Public-Key Infrastrukturen

Bei PKIs (Public Key Infrastructure) handelt es sich um Sicherheitsinfrastrukturen, die es den Benutzern eines grundsätzlich nicht gesicherten öffentlichen Netzes erlauben, sicher Daten durch die Benutzung eines asymmetrischen kryptographischen Verfahrens sowie eines zugehörigen Schlüsselpaares (public and private key) auszutauschen. Mögliche Dienste von Public-Key-Infrastrukturen können Schlüsselgenerierung, Identifizierung und Registrierung von Anwendern, Zertifizierung, Sperrung von Zertifikaten sowie das Unterhalten eines Verzeichnisdienstes zur Abfrage von Zertifikaten und Sperrlisten sein.

#### 7.3.1.1 Einsatzfelder von Public-Key-Infrastrukturen

**Ergebnisse**

Die Befragten erwarten, dass PKI-Infrastrukturen bei Kommunikationsvorgängen zwischen Unternehmen in drei Jahren weit verbreitet sein werden (siehe Abbildung 7.7, ①). Deren Einführung ist nach Ansicht der Experten für neue Anwendungen, die auf der Public-Key-Technologie aufsetzen, unverzichtbar; bis dahin sollte sich eine vernünftige Infrastruktur gebildet haben. Anwendungspotenziale werden beispielsweise in der elektronischen Rechnungsabwicklung (Bill presentment & payment), in sicheren elektronischen Liefer- und Leistungsbeziehungen sowie in den hierzu notwendigen Finanztransaktionen gesehen. Aber auch der Schutz der bisherigen Anwendungen, die (interne und externe) Kommunikation und Führung, sowie alle Verfahren mit Ende-zu-Ende Sicherheitsbedarf, beispielsweise das Verschlüsseln und Signieren der E-Mail-Kommunikation, gelten als potenzielle Anwendungsfelder.

PKI-INFRASTRUKTUREN BEI KOMMUNIKATIONSVORGÄNGEN ZWISCHEN UNTERNEHMEN: PKI-Systeme für B2B und B2G-Anwendungen werden in 3 Jahren, bei G2G-Anwendungen bereits in 2 Jahren erwartet.

BUSINESS-TO-CONSUMER: PKI-Systeme mit Beziehungen zum Endverbraucher werden frühestens in 5 Jahren erwartet. Die Experten vermissen Killerapplikationen.

Die aus diesen Technologieansätzen resultierenden Potenziale sind effizientere Prozesse mit weniger Zentralisierung, mehr Ausfallsicherheit, Kostenersparnis, schnellere und sichere Kommunikation zwischen Unternehmen und die eindeutige Identifizierung der Partner mit Nichtabstreitbarkeit von Transaktionen. Auch erhofft man sich eine raschere Entwicklung des B2B (Business-to-Business)-Geschäfts über das Internet und die Möglichkeit, sämtliche Geschäftsprozesse auf IT-Basis abwickeln zu können, bis hin zu interessanten Innovationen wie der Automatisierung von Vertrags(vor-)verhandlungen für Routineanwendungen. Der Hauptgrund für den bisher unzureichenden Einsatz der bereits vorhandenen Unternehmens-PKIs ist deren mangelnde Interoperabilität untereinander. Hier wird auf die europäischen Standardisierungsbemühungen hingewiesen [Sche 02b], von denen erwartet wird, dass sie ab Mitte 2003 greifen werden.

Frühestens in fünf Jahren erwarten die Befragten die weite Verbreitung von Public-Key-Infrastrukturen bei Kommunikationsvorgängen zwischen Unternehmen und Kunden (Business-to-Consumer). Hinder-

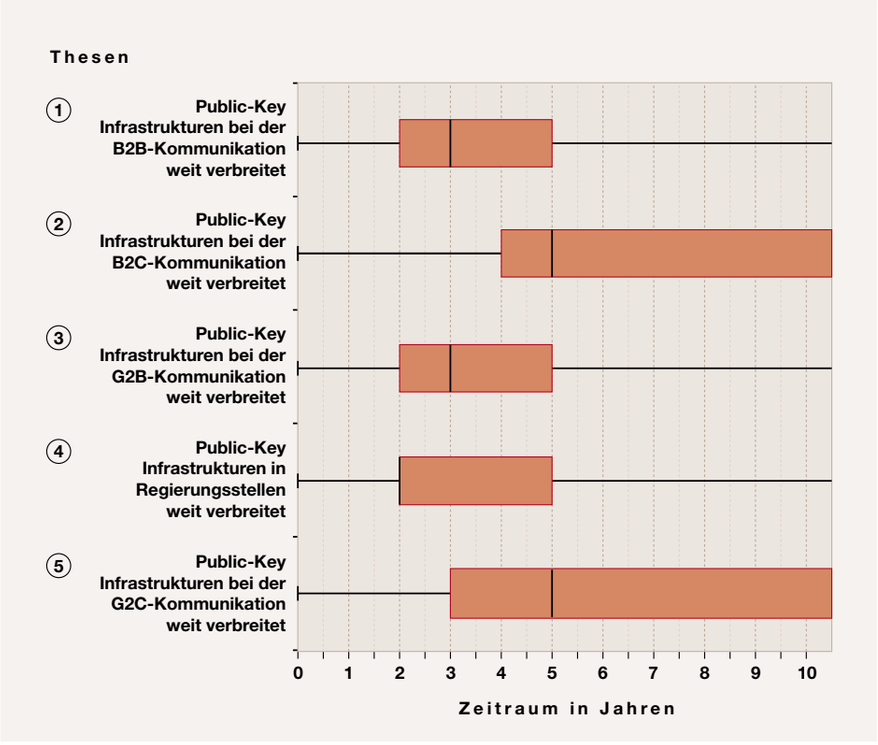



Abbildung 7.7: Ergebnisse der Thesen zu den Einsatzfeldern von Public-Key-Infrastrukturen

nisse, die bis dahin noch ausgeräumt werden müssen, sind beispielsweise die Senkung der Kosten des PKI-Einsatzes und die Senkung der Infrastrukturkosten des Kunden („Wer übernimmt die Kosten für Karten/Lesegeräte, Zertifizierung?", etc.). Viele Experten vertreten die Ansicht, dass eine weitere öffentliche Förderung zur Einführung der Infrastruktur nötig sein wird. Neue Technologiepotenziale ergeben sich im Bereich des E-Commerce beispielsweise beim Geldtransfer, im elektronischen Handel und dem fairen Austausch von (digitalen) Gütern (Fair Exchange [ABWP+ 00]), sowie generell für rechtsverbindliche Transaktionen und deren Nichtabstreitbarkeit. Beim Fair Exchange wird das Problem behandelt, in welcher Reihenfolge Güter geliefert und Zahlungen getätigt werden. Dies ist insbesondere zwischen Handelspartnern mit eingeschränktem gegenseitigem Vertrauen nötig. Über die finanzorientierten Anwendungen hinaus ergeben sich Potenziale bei der Datenübertragung und zum Schutz von Kundenkontakten. Allerdings wird vielfach festgestellt, dass die sogenannte „Killer"-Applikation für die Einführung der PKI-Funktionen beim Kunden noch fehlt. Darüber hinaus existieren etablierte proprietäre Verfahren wie z.B. PIN/TAN für eine Vielzahl von Anwendungen. Daher erwartet ein Teil der Befragten eine weite Verbreitung nicht vor zehn Jahren (siehe Abbildung 7.7, ②).

In drei Jahren wird die weite Verbreitung von Public-Key-Infrastrukturen in Kommunikationsbeziehungen zwischen Regierungsstellen und Unternehmen (G2B (Government-to-Business)) erwartet (Abbildung 7.7, ③). Dies ermöglicht zahlreiche neue Anwendungen, beispielsweise die elektronische Abwicklung von Genehmigungsverfahren oder Steuererklärungen, allgemeinen Schriftverkehr, Bescheinigungen sowie viele Transaktionen. Weiterhin ist die Verbreitung von PKIs Voraussetzung für elektronische Beschaffungs- und Vergabeverfahren, das so genannte „E-Procurement". Ein automatisierter Datenaustausch könnte bei Geschäftsprozessen mit Behörden hilfreich sein. Im Bereich der sicheren elektronischen Kommunikation erhofft man sich den elektronischen Austausch von im Rahmen des staatlichen Geheimschutzes

eingestuften Dokumenten. Die Potenziale der Technologieansätze sind groß: Ermöglicht wird eine digitale, medienbruchfreie Aktenbearbeitung mit Rationalisierungen in der Verwaltung und der Industrie sowie einer erheblichen Beschleunigung in der Vorgangsbearbeitung.

Abbildung 7.7, ④ zeigt die Einschätzung der Experten bezüglich Public-Key-Infrastrukturen bei Kommunikationsbeziehungen zwischen Regierungsstellen (G2G (Government-to-Government)). Hier wird davon ausgegangen, dass diese frühestens in zwei Jahren weit verbreitet sein werden. Potenziale werden im Austausch sensibler Daten und Dokumente, bei Ermittlungsbehörden und der Bundeswehr, sowie zur Rationalisierung des allgemeinen und verbindlichen Schriftverkehrs gesehen. Klärungsbedarf wird noch im Bereich der Interoperabilität sowie in organisatorischen Fragen, z.B. in der Vertreter-Frage, gesehen. Viele der Befragten sehen noch Hindernisse auf politischer Entscheidungsebene, beispielsweise bei der Klärung von Zuständigkeiten und bei der Überwindung rechtlicher und bürokratischer Hemmnisse.

Die Experten erwarten, dass Public-Key-Infrastrukturen bei Kommunikationsbeziehungen zwischen Regierungsstellen und Bürgern (G2C (Government-to-Citizen)) in etwa fünf Jahren weit verbreitet sein werden (siehe Abbildung 7.7, ⑤). Hier wird ein großes Potenzial für zahlreiche neue Anwendungen gesehen, z.B. Genehmigungsverfahren, elektronische Anträge, elektronischer Ausweis (Bürgerkarte), sämtliche Transaktionen wie Wohnsitzummeldung, Führerscheinausstellung etc. Die Experten sehen Möglichkeiten für erhebliche Einsparungen in Ämtern und für die Bürger, d.h. eine Verwaltungsvereinfachung und -rationalisierung. Darüber hinaus werden neue Möglichkeiten eröffnet, wie elektronische Abstimmungen und die automatische Mautabführung (z.B. durch die digitale Signaturim Mautsystem), sowie die Übertragung von persönlichen Daten (z.B. im Gesundheitswesen) über öffentliche Netze realisiert werden können. Skeptisch sind einige der Befragten hinsichtlich der hohen Investitionskosten und dem kurzfristig unsicheren Return on Investment (ROI).

### Zusammenfassung

Die befragten Experten erwarten im Wesentlichen in allen Anwendungsszenarien eine zeitnahe Verbreitung des Einsatzes von Public-Key Infrastrukturen. Die prognostizierten Zeiten sind allerdings vor dem Hintergrund bereits seit Jahren laufender und zum Teil sehr aufwendiger PKI-Projekte eher ernüchternd, spiegeln aber eine realistische Abschätzung der mittelfristigen praktischen Verbreitung solcher Systeme wieder.

- PKI-Systeme für B2B-Anwendungen werden bis 2006 weit verbreitet sein. Im gleichen Zeitraum werden PKI-Systeme für G2B-Anwendungen Verbreitung finden.
- Die Befragten erwarten hingegen, dass PKIs für Beziehungen zum Endverbraucher wie B2C (Business-to-Consumer) bzw. G2C frühestens 2008 etabliert sein werden. Die Experten bemängeln, dass noch keine „Killer-Applikation" in Sicht ist.
- Bereits für 2005 werden trotz politischer und organisatorischer Hemmnisse PKIs für Kommunikationsbeziehungen zwischen Behörden erwartet.

### 7.3.1.2 Zertifikatsformate

Eine elementare Rolle bei der Durchsetzung von Public-Key-Infrastukturen und deren Bewertung spielt die Interoperabiliät der verwendeten Systeme und damit die verfügbaren Zertifikatsformate. Zwei Zertifikatsformate haben sich in den vergangenen Jahren herauskristallisiert: Zum einen das hierarchisch orientierte X.509-Format in der derzeit aktuellen Version 3 [CCITT 88], das auch Grundlage der im SigG [Deut 99] vorgesehenen qualifizierten Digitalen Signatur ist.

Daneben hat sich, vor allem im Bereich der privaten Kommunikation, das PGP-Zertifikatsformat (Pretty Good Privacy) etabliert [Zimm 95], das auf dem Prinzip des so genannten „Web-of-Trust" beruht. Im Gegensatz zum hierarchischen Ansatz, bei dem die Regulierungsbehörde für Post und Telekommunikation (RegTP) die Root-Zertifizierungsstelle darstellt, sind die PGP-Zertifikate grundsätzlich auf der gleichen

Stufe. Der Benutzer selbst entscheidet, welchen Vertrauensgrad er den Ausstellern entgegen bringen möchte.

### Ergebnisse

ZERTIFIKATSFORMATE: X.509 wird sich gegenüber dem PGP-Format weiter durchsetzen.

Bei der Bewertung der Bedeutung dieser beiden Zertifikatsformate gehen die Befragten, wie in Abbildung 7.8 ersichtlich, davon aus, dass X.509v3 über die nächsten drei Jahre (auf einem konstant hohen Niveau) weiterhin wichtigstes Format bleiben wird, obwohl es noch erhebliche Interoperabilitäts-Schwierigkeiten gibt. Danach wird erwartet, dass neue Formate zunehmend X.509v3 ablösen werden. Anders beim PGP-Zertifikat. Hier sehen die Befragten vor allem einen Einsatz im Privatbereich, bei kleinen Unternehmen sowie im Hochschulbereich und gehen davon aus, dass innerhalb der nächsten zehn Jahre der Standard erheblich an Bedeutung verlieren und mittelfristig im insgesamt besser spezifizierten X.509 migrieren wird. Die zukünftige Bedeutung wird auch vom Erfolg von GnuPG und openPGP abhängen, die derzeit u.a. durch das Bundesministerium für Wirtschaft und Arbeit stark gefördert werden.

#### 7.3.1.1 PKIs für qualifizierte elektronische Signaturen

Bei den vorhergehenden Fragestellungen wurde nicht zwischen Public-Key-Infrastrukturen für elektronische Signaturen, fortgeschrittene elektronische Signaturen und qualifizierte elektronische Signaturen unterschieden. Innerhalb des Gesetzes über Rahmenbedingungen für elektronische Signaturen, kurz Signaturgesetz [Deut 99], wird diese Unterteilung jedoch durchgeführt.

Fortgeschrittene elektronische Signaturen sind ausschließlich dem Unterzeichner zugeordnet. Sie ermöglichen seine Identifizierung und werden mit Mitteln erstellt, die er unter seiner alleinigen Kontrolle halten kann und die so mit den Daten verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann. Im Gegensatz zu elektronischen Signaturen werden an fortgeschrittene elektronische Signaturen technische und organisatorische Anforderungen gestellt, um die Voraussetzung dafür zu schaffen, dass rechtliche Folgen an diese Art von Signaturen geknüpft werden können.

Eine wichtige Rolle spielen die qualifizierten elektronischen Signaturen, die weitergehende Anforderungen erfüllen müssen als die fortgeschrittenen. Nur mit ihnen wird die Abgabe von rechtsverbindlichen Erklärungen möglich sein, die die Anforderung der Schriftform erfüllen müssen. Innerhalb dieses Abschnitts wird auf die Einschätzung der Verfügbarkeit und Verbreitung elektronischer Signaturen durch Experten eingegangen.

### Ergebnisse

Public-Key-Infrastrukturen zur Behandlung qualifizierter elektronischer Signaturen, die für rechtsverbindliche elektronische Transaktionen essentiell sind, werden nach Ansicht der Befragten in sechs Jahren weit verbreitet sein (siehe Abbildung 7.9, ①). Etwa ein Viertel der Befragten sehen eine weite Verbreitung nicht vor zehn Jahren. Für diese Zeitspanne werden vor allem die hohen Anforderungen und der organisatorische Aufwand als Begründung aufgeführt. Einige Experten sehen durch diesen „Perfektionswillen" die Realisierung gebremst.

Der Einsatz qualifizierter elektronischer Signaturen wird noch lange mit rechtlichen Problemen verbunden sein (Identifikationsbeweis), insbesondere aufgrund der nach wie vor unsicheren IT-Infrastruktur wie Betriebssysteme und Hardwareschutz. In jedem Fall wird eine aktive Rolle der Politik, wie sie bei Bund Online 2005 erfolgt, als essentiell für die mittelfristige Durchsetzung der qualifizierten elektronischen Signatur gesehen. Trotz des Rückschlags durch den Rückzug großer Anbieter wie „SignTrust" aus dem PKI-Geschäft wird eine positive Entwicklung erwartet.

In Abbildung 7.10 ist die Bewertung der zukünftigen Bedeutung elektronischer Signaturen nach der Definition des Signaturgesetztes ersichtlich. Die elektronische Signatur wird demnach nach einem mittelfristigen Ansteigen wieder an Bedeutung verlieren. Die rechtsverbindliche Authentizität der Daten wird zunehmend wichtiger werden. Weiterhin wird die elektronische Signatur in privater und geschäftlicher Korrespondenz mit geringem Trans-


Abbildung 7.8: Bedeutung unterschiedlicher Zertifikatsformate

QUALIFIZIERTE ELEKTRONISCHE SIGNATUREN: Die derzeit dominierenden elektronischen Signaturen werden mittelfristig durch fortgeschrittene und langfristig durch qualifizierte elektronische Signaturen ersetzt werden.

aktionswert und auf der technischen Infrastrukturebene, z.B. bei VPN's, eine Rolle spielen.

Die fortgeschrittene elektronische Signatur wird parallel zur elektronischen in den nächsten drei Jahren an Bedeutung gewinnen und auf einem hohen Niveau über die nächsten zehn Jahre verbleiben. Danach wird erwartet, dass die fortgeschrittene elektronische Signatur von der qualifizierten abgelöst wird. Anwendungsbereiche werden in Finanztransaktionen geringer Höhe, einfachen Rechtsgeschäften mit Nichtabstreitbarkeit, E-Mail-Kommunikation sowie in Bereichen ohne hohe Anforderungen an die Schriftform gesehen.

Die Bedeutung der qualifizierten elektronischen Signatur wird derzeit am geringsten eingestuft, wird in den nächsten zehn Jahren aber erheblich an Bedeutung gewinnen. Als ausschlaggebend für die bisher zögerliche Verbreitung wird der Bedarf zusätzlicher Hardware sowie die Unsicherheiten bzgl. stabiler Rahmenbedingungen mit Blick auf die neuen EU-Richtlinien gesehen. Kritisiert wird, dass von der Industrie kaum Impulse zur Verbreitung der qualifizierten elektronischen Signatur ausgehen.

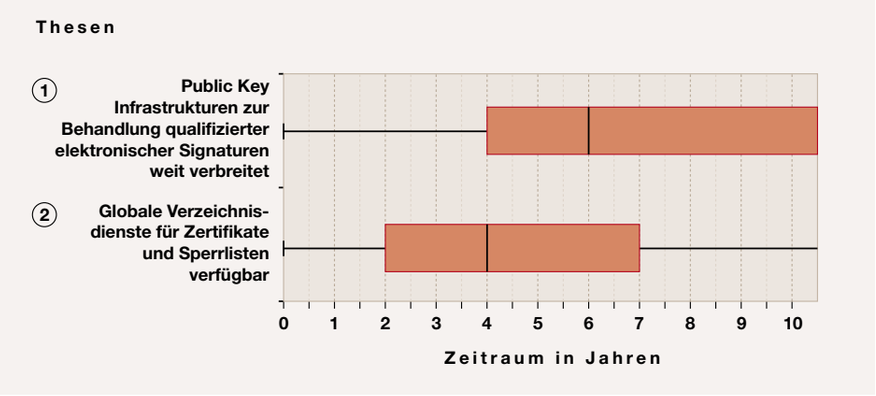
Die Experten versprechen sich durch qualifizierte elektronische Signaturen zahlreiche neue Anwendungsmöglichkeiten, insbesondere den Bereichen E-Commerceund E-Government. Potenzielle Anwendungsmöglichkeiten ergeben sich für elektronische Finanztransaktionen und Vertragsabschlüsse in großer Höhe und für die Abwicklung von verbindlichen Rechtsgeschäften. In vielen Bereichen wird die Technologie die manuelle Unterschrift ersetzen.

## Zusammenfassung

Insgesamt erwarten die Experten eine Bedeutungszunahme aller Ausprägungen von elektonischen Signaturen. Die Auswertung zeigt allerdings auch, dass die für viele Anwendungen wichtige qualifizierte elektronische Signatur heute keinerlei Rolle spielt. Ein Fazit ist auch, dass sich mittelfristig ein Standard für die technische Ausgestaltung der Zertifikate etablieren wird.

- Bei der Bewertung der Standards erwarten die Experten, dass sich mittelfristig das X509v3-Format gegenüber PGPdurchsetzen wird.

- Die derzeit dominierende elektronische Signatur wird mittelfristig durch die fortgeschrittene und langfristig durch die qualifizierte elektronische Signatur abgelöst werden.




GLOBALE VERZEICHNISDIENSTE: für Zertifikate und Sperrlisten werden in 4 Jahren verfügbar sein.

Abbildung 7.9: Ergebnisse der Thesen zu Signaturen und Verzeichnisdiensten

### 7.3.1.2 Verzeichnisdienste

Eine wichtige Technologiekomponente bei Public-Key-Infrastrukturen sind Verzeichnisdienste zur Verbreitung von Zertifikaten und Sperrlisten. Sperrlisten identifizieren dabei zurückgezogene bzw. nicht mehr gültige Zertifikate. Verzeichnisdienste müssen Mindestanforderungen bezüglich der Integrität und Verfügbarkeit garantieren. Globale Verzeichnisdienste sind dabei solche Verzeichnisdienste, die grundsätzlich nicht nur geschlossene Benutzergruppen abbilden, also etwa die Nutzer einer bestimmten PKI, sondern über mehrere Public-Key-Infrastrukturen hinweg nutzbar sind.

#### Ergebnisse

Die Befragten erwarten, dass globale Verzeichnisdienste für Zertifikate und Sperrlisten in spätestens vier Jahren verfügbar sein werden (siehe Abbildung 7.9, ②). Auf diesem Weg müssen nach Ansicht der Experten weiterhin Einzelverzeichnisdienste zusammengeführt und datenschutzrechtliche Fragen aufgelöst werden. Zukünftig werden dabei verbesserte Anwendungspotenziale für die Sicherheit in offenen Netzen gesehen. Hierzu zählt vor allem das Ermöglichen von verschlüsselten Ad-Hoc-Kommunikationsverbindungen (ad-hoc Networking).

In Abbildung 7.11 ist die Einschätzung der Befragten bzgl. der Bedeutung aktueller Standards und Produktlösungen für Verzeichnisdienste über die nächsten zehn Jahre aufgezeichnet. Betrachtet werden dabei der LDAP-Standard (Lightweight Directory Access Protocol), spezifiziert in RFC 1777, 2251, 2256, 2307, Active Directory von Microsoft sowie NDS (Novell Directory Services) von Novell.

Alle drei Verfahren werden nach Einschätzung der Experten über die nächsten zehn Jahre an Bedeutung verlieren, bei gleich bleibender Rangfolge in der Bedeutung: LDAP wird weiterhin der wichtigste Verzeichnisdienst-Standard bleiben, gefolgt von Active Directory, das in den nächsten drei Jahren sogar etwas an Bedeutung gewinnen wird und danach NDS, das im gleichen Zeitraum deutlich und am stärksten abfällt. Begründet wird diese Einschätzung mit der Korrelation zum erwarteten Verbreitungsrückgang von Novell-Umgebungen. Für VPNwird ein breites Anwendungsgebiet gesehen, insbesondere aufgrund der Herstellerunabhängigkeit und der einfachen technischen Struktur. Microsoft Active Directory wird unterschiedlich bewertet. Zum einen wird die Verbreitung durch die Verknüpfung mit den Betriebssystemen und den zugehörigen Diensten von Microsoft gefördert, zum anderen wird die Abhängigkeit von einem Quasi-Monopolisten als gefährlich eingestuft. Bei den Produktlösungen wird vor allem DirX der Siemens AG eine nennenswerte Bedeutung, insbesondere für Großunternehmen, beigemessen.

Eine zunehmende Bedeutung sehen die Befragten in der Ende-zu-Ende-Sicherheit vor dem Hintergrund der Interoperabi-

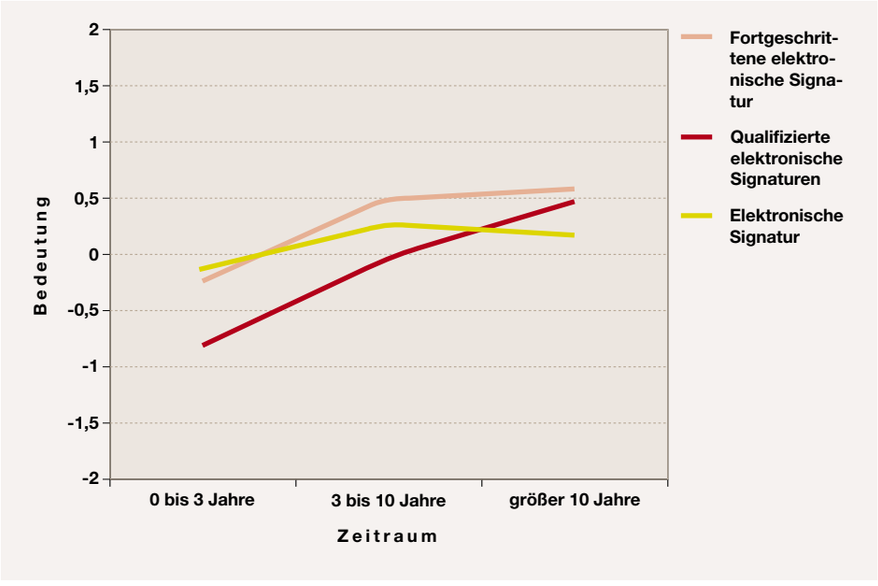



Abbildung 7.10: Bedeutung verschiedener Signaturarten

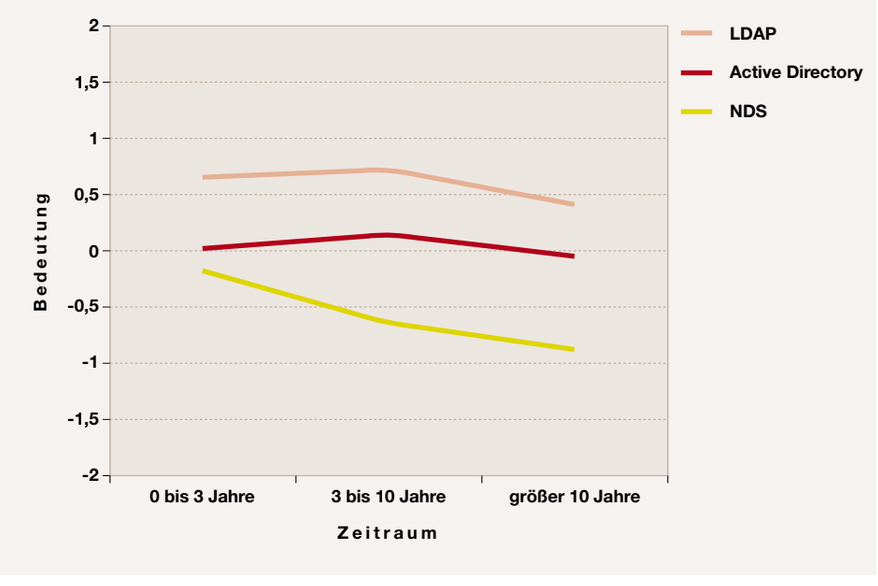



Abbildung 7.11: Bedeutung verschiedener Standards und Produktlösungen für Verzeichnisdienste


VIRTUELLE POSTSTELLEN: Trotz der Ende-zu-Ende Problematik könnten zentrale Alternativ-Modelle temporär eine wichtige Rolle spielen.

TRÄGERMEDIUM FÜR SIGNATURSCHLÜSSEL: Auch weiterhin wird die Chipkarte wichtigstes Trägermedium sein.

BUSINESS-CASES: Viele Experten bezweifeln eine weite Verbreitung von Anonymitätsdiensten aufgrund fehlender Geschäftsfälle und derzeit mangelndem Kundeninteresse.

litätsproblematik bei der Nutzung von PKIs (vgl. Abbildung 7.12). Nach Einschätzung der Experten werden durch die zunehmende Verankerung der Bedeutung von Ende-zu-Ende Sicherheit im Selbstverständnis der Anwender und deren Auswirkungen auf den Markt die PKIs zur Interoperabilität gezwungen sein. Bis dahin könnten alternative zentrale Modelle wie zentrale Kryptogateways oder „virtuelle Poststellen" ergänzend wirken.

Als wichtigstes Trägermedium für Signaturschlüssel bei der Nutzung von PKIs sehen die Experten die Chipkarte, die auch über die nächsten zehn Jahre weiter an Bedeutung gewinnen wird (siehe Abbildung 7.13). Weniger bedeutsam hingegen werden USB-Token eingestuft, die insbesondere über einen längeren Zeitraum wieder an Bedeutung verlieren dürften. Grundsätzlich wird die Sicherheit von an einem seriellen Bus mit vielen unbekannten Geräten betriebenen USB-Token in Frage gestellt. Allerdings werden durchaus Anwendungen im Bereich der Authentifizierung oder als persönlicher Datenspeicher gesehen. Bei Chipkarten wird vor allem erwartet, dass sie Anwendung auf oder als digitale (Personal- und Dienst-)Ausweise finden werden. Alternative Trägermedien für Signaturschlüssel sehen die Experten in durch sichere Betriebssysteme verwaltete Schlüssel auf PCs, PDAs oder Mobiltelefonen, die teilweise tamper-evident gebaut werden. Unter tamper-evidence versteht man Geräte, bei denen sichergestellt ist, dass Manipulationen durch das Gerät selbst oder durch den Benutzer erkannt werden.

### Zusammenfassung

Bei den in der Studie betrachteten Technologiekomponenten Verzeichnisdienste und Trägermedien sowie bei der Bewertung der möglicherweise eingeschränkten Ende-zu-Ende Sicherheit kann man zusammenfassend festhalten:

- Globale Verzeichnisdienste werden nach Auflösung datenschutzrechtlicher Fragen und Zusammenführung von Einzeldienstverzeichnissen spätestens 2007 verfügbar sein. Die heute verfügbaren Produkte werden langfristig an Bedeutung verlieren.
- Wichtigstes Trägermedium bleibt auch weiterhin die Chipkarte. USB-Tokens werden eine nur geringe und vorrübergehende Rolle spielen.
- Die Befragten sagen der Ende-zu-Ende Sicherheit vor dem Hintergrund der Interoperabilitätsproblematik bei der Nutzung von PKIs wachsende Bedeutung voraus.

## 7.3.2 Anonymität

Bei der Nutzung von Kommunikationsnetzen, insbesondere des Internet, fallen eine Vielzahl den Nutzer in seinem Verhalten beschreibenden Informationen an. Anonymität wird dabei differenziert betrachtet. So wird beispielsweise bei elektronischen Bezahlvorgängen zwischen Bezahler- und Händleranonymität unterschieden. Innerhalb dieser Studie wird insbesondere auf die Bezahleranonymität eingegangen [Kelt 01]. Schon seit Beginn der 1990er Jahre existieren Bestrebungen, die auch als „Datenspuren" bezeichneten, bei Kommunikationsvorgängen anfallenden Informationen mit Hilfe von Anonymitätsdiensten zu vermeiden. Innerhalb dieses Abschnitts soll die mögliche Verbreitung und Entwicklung von Anonymitätsdiensten, sowie der für ihre Realisierung notwendigen Technologie, untersucht werden.

### Ergebnisse

Anonymitätsdienste sind in verschiedenen Einsatzgebieten und Anwendungsfällen vorstellbar. Wie aus Abbildung 7.14, ① ersichtlich, erwarten die Befragten die weite Verbreitung von Anonymitätsdiensten bei elektronischen Bezahlvorgängen in etwa fünf Jahren. Allerdings geht über ein Viertel der Befragten von gar keiner zukünftigen Verbreitung in diesem Anwendungsfall aus. Begründet wird dies vor allem mit dem Fehlen von Geschäftsfällen (Business-Cases). Derzeit ist die Dienstleistung wichtiger als die Anonymität bei Bezahlvorgängen. Daneben wird die technische Realisierung weitreichender Anonymität und die sicherheitspolitische Wünschbarkeit teilweise in Frage gestellt. Interessante Anwendungsfälle und ein möglicher Markt werden bei Mautsystemen bei Micropayments und bei elek-

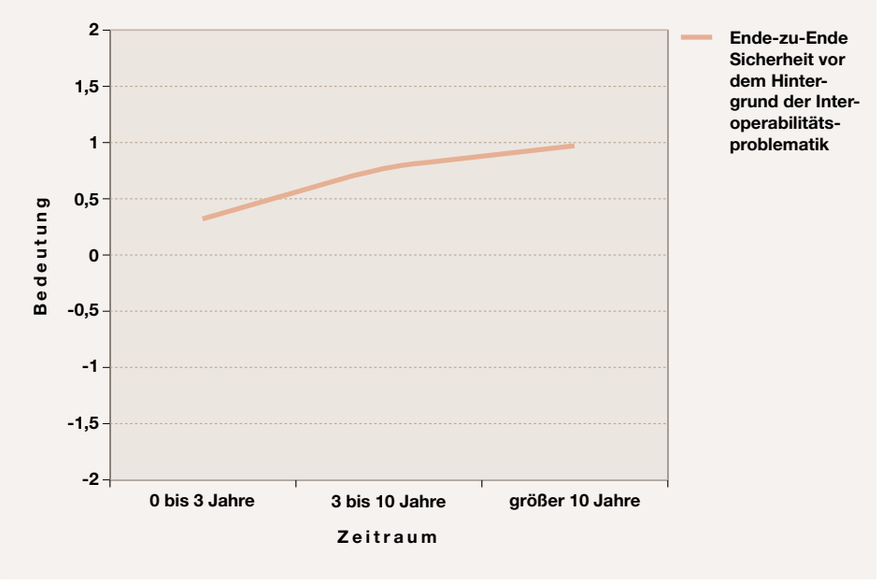



Abbildung 7.12: Bedeutung von Ende-zu-Ende-Sicherheit

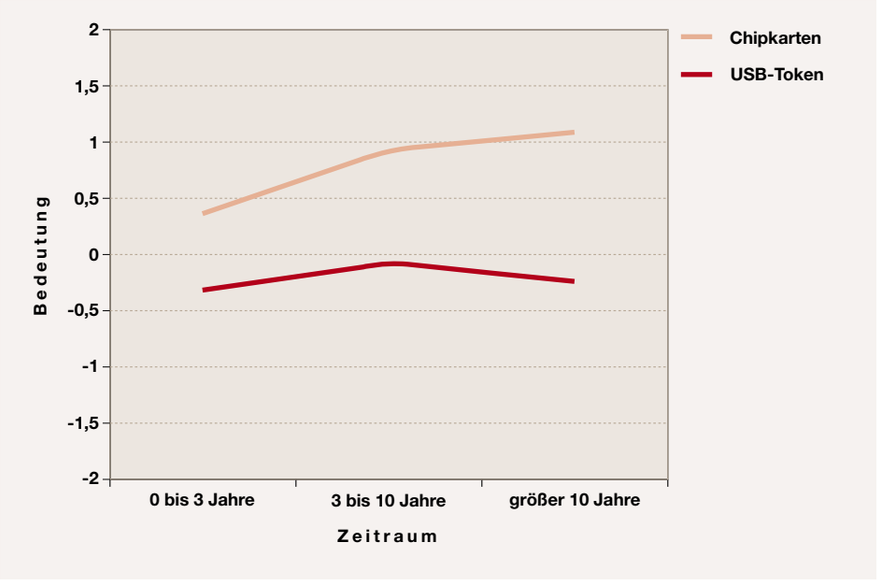



Abbildung 7.13: Bedeutung verschiedener Trägermedien für Signaturschlüssel bei der Nutzung von PKIs

tronischen Münzen gesehen. Grundlegende Verfahren existieren bereits, allerdings sind bisherige Initiativen mangels Kundeninteresse gescheitert.

Bei Anonymitätsdiensten bzgl. Inhaltsabfragen, wie sie zur Zeit bspw. über das HTTP- (Hypertext Transfer Protocol) oder WAP-Protokoll (Wireless Application Protocol) stattfinden, sehen die Experten bereits in vier Jahren eine weite Verbreitung. Anwendungspotenziale werden für Informationsabfragen mit vertraulichen und sensitiven Daten, z.B. für die Meinungsforschung, gesehen. Viele der Befragten sehen jedoch keine neuen Potenziale.

In Elektronischen Diskussionsforen, wie sie das Usenet bietet, aber auch in allen anderen Formen elektronischer Foren, wie Chatrooms oder HTML-basierten Anwendungen, werden Anonymitätsdienste nach Ansicht der Befragten in vier Jahren weit verbreitet sein. Positive Anwendungsmöglichkeiten werden in Bereichen zur anonymen Aussprache gesehen, in denen sich Benutzer über Pseudonyme bewegen können. Allerdings wird auch vor Gefahren durch Missbrauch gewarnt.

Ein sehr uneinheitliches Bild ergibt sich bei der Bewertung der Verbreitung von Anonymitätsdiensten bei der Mailkommunikation. Über ein Viertel der Befragten erwarten überhaupt keine Verbreitung und betrachten anonyme E-Mail-Kommunikation aufgrund der Gefahren durch E-Mail-Spamming als unerwünscht. Andererseits geht nahezu ein Viertel der Befragten davon aus, dass solche Dienste bereits verbreitet sind bzw. es innerhalb eines Jahres sein werden. Als Beispiel für pseudonymisierende Verfahren werden Webmail-Dienste genannt, bei denen oftmals der tatsächliche Nutzer nicht zu ermitteln ist. Anwendungs- und Technologiepotenziale werden in speziellen Anwendungen wie elektronischen Abstimmungen und Wahlen sowie in anonymer Informationsabfrage gesehen.

Ein Themenfeld, das mit zunehmender Debatte um die Telekommunikationsüberwachungsverordnung (TKÜV) an Bedeutung gewinnt, sind Anonymitätsdienste bei Mobilfunkanwendungen mit dem Ziel der Vermeidung von Bewegungsprofilen. Die Befragten prognostizieren eine weite Verbreitung solcher Dienste in etwa sechs Jahren. Allerdings erwartet auch hier über ein Viertel der Befragten überhaupt keine Verbreitung. So werden, bei kleiner werdenden Funkzellen, keine technischen Möglichkeiten gesehen, Anonymität providerunabhängig zu erreichen. Die meisten Experten erwarten einen schwer auflösbaren Konflikt im Zusammenhang mit der möglichen Einschränkung der Strafverfolgung durch solche Dienste. Insbesondere wird in der jetzigen Situation erwartet, dass der Datenschutz in der aktuellen Diskussion gegenüber der inneren Sicherheit in der Priorität zurückfällt. Überwiegend werden keine oder keine neuen Anwendungspotenziale gesehen. Auch gelten die Technologien als noch nicht marktreif. Praktisch wird derzeit die Anonymität durch das häufige Wechseln von Prepaid-Karten erreichet.

Anonymisierungdienste werden als zweischneidiges Schwert gesehen. Sie bieten einerseits die Möglichkeit, berechtigte Datenschutz-Anliegen für die Nutzer zu etablieren, andererseits eröffnen sie Möglichkeiten zum Missbrauch. Dies drückt sich in der Skepsis der Experten gegenüber der weiten Verbreitung der Akzeptanz von Anonymisierungsdiensten, trotz der möglichen missbräuchlichen Nutzung dieser Dienste, aus. Eine Akzeptanz wird, wie in Abbildung 7.15, ① ersichtlich, in frühestens sechs Jahren erwartet. Über ein Viertel erwartet überhaupt keine Akzeptanz, aufgrund des Missbrauchspotenzials und des negativen Images, das mit Anonymität assoziiert wird. Grundsätzlich wird die Akzeptanz als abhängig von der Qualität der verfügbaren Lösungen und der Vertrauenswürdigkeit der Anbieter gesehen.

Die augenblicklich angebotenen Anonymisierungsdienste sind größtenteils kostenfrei nutzbar, da es sich häufig um Angebote von universitären Einrichtungen handelt, die nicht mit dem Ziel der Gewinnerbringung verbunden sind. Insgesamt ist jedoch absehbar, dass bisher kostenlos im Interneterbrachte Dienstleistungen vermehrt kostenpflichtig angeboten werden. Die Befragten bezweifeln aber, dass die Akzeptanz für kostenpflichtige Anonymisierungsdienste unter den Internetnutzern jemals weit verbreitet sein wird (siehe Abbildung 7.15, ②). Zum einen gehen die meisten Befragten nicht davon aus, dass die Benutzer bereit sind, dafür Geld auszugeben, zum anderen untergräbt der Bezahlvorgang selbst oder gar die Interakti-

ANONYMITÄTSDIENSTE BEI MOBILFUNKANWENDUNGEN: Die Vermeidung von Bewegungsprofilen durch Anonymitätsdienste wird in 6 Jahren weit verbreitet sein.

AKZEPTANZ VON ANONYMISIERUNGSDIENSTEN: Trotz der möglichen missbräuchlichen Nutzung dieser Dienste wird eine Akzeptanz in 6 Jahren erwartet.

KOSTENPFLICHTIGE ANONYMISIERUNGSDIENSTE: Nach heutigem Stand sind die meisten Internet-Benutzer nicht bereit, für Anonymisierungsdienste Geld auszugeben. Vielfach wird der Schutz der Privatsphäre als Teil staatlicher Fürsorgepflicht gesehen.

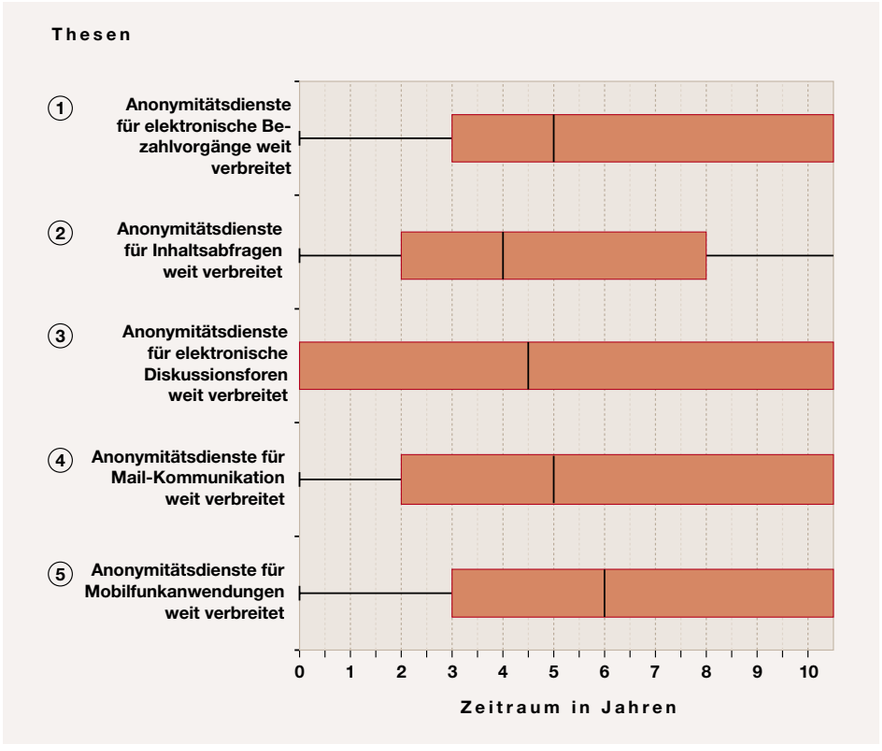



Abbildung 7.14: Ergebnisse der Thesen zu Anonymitätsdiensten

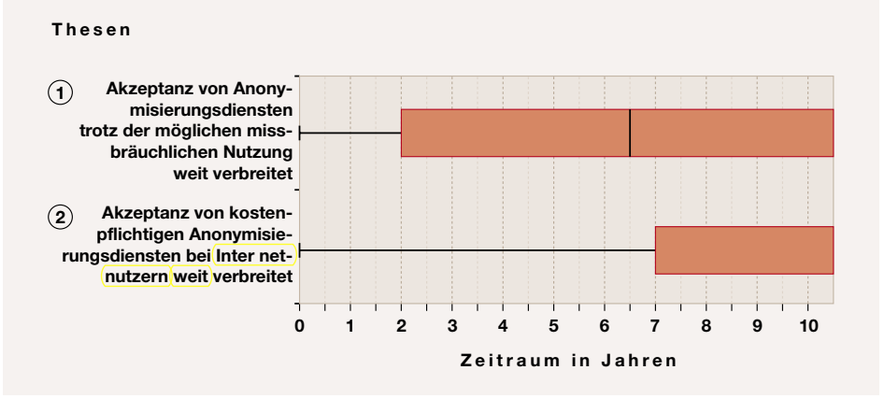
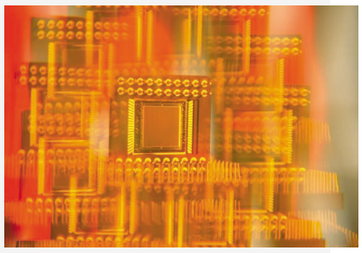



Abbildung 7.15: Ergebnisse der Thesen zur Akzeptanz von Anonymisierungsdiensten



on mit einem Zweiten bereits die Anonymität. Problematisch ist auch die Intransparenz der Dienstleistung, die dem Internetnutzer die Kontrolle darüber erschwert, ob er überhaupt eine Leistung erhalten hat. Einzig im Gesundheitswesen werden mögliche Marktchancen erwartet.

Obgleich die Bedeutung kostenpflichtiger Anonymisierungsdienste für Internetnutzer derzeit als gering eingestuft wird, erwarten die Befragten ein mittleres Ansteigen über die nächsten zehn Jahre, wie in Abbildung 7.16 ersichtlich ist. Viele der Befragten betrachten die Sicherstellung der Privatssphäre und damit auch der Anonymität bei Bezahlvorgängen als Grundschutz, der in die Fürsorgepflicht des Staates fällt und damit – ähnlich wie beim Datenschutz – auch generell zu regulieren ist. Nichtsdestotrotz werden kostenpflichtige Dienste in Nischenbereichen wie bei erotischen Inhalten, Datenbankabfragen und kostenpflichtigen Mediendiensten Anwendung finden.

In Abbildung 7.17 ist absolut aufgezeigt, welchen Betrag ein Internetnutzer in den nächsten Jahren bereit sein wird, für Anonymisierungsdienste auszugeben. Rund die Hälfte der Befragten erwartet dabei in den nächsten zehn Jahren nicht, dass kostenpflichtige Dienste von den Nutzern angenommen werden. Die übrigen gehen davon aus, dass dieser Betrag über die nächsten Jahre nahezu linear auf bis zu sieben Euro pro Monat ansteigen wird. Fast zwei Drittel aller Befragten vertreten die Ansicht, dass derzeit keine Bereitschaft besteht, kostenpflichtige Anonymisierungsdienste zu verwenden, was sich im niedrigen Betrag für „heute“ in Abbildung 7.17 ausdrückt.

### Zusammenfassung

Obwohl die Bedeutung der Privatsphäre der Bürger immer wieder herausgehoben wird, ist die Einschätzung der Befragten bezüglich der Etablierung geeigneter Dienste ernüchternd. Trotz der Verfügbarkeit der benötigten Technologien wird mangels wirtschaftlicher Nutzungsmöglichkeiten die weite Verbreitung nur langsam erwartet. In diesem Kontext ist die Forderung, den Schutz der Privatsphäre als Teil staatlicher Fürsorgepflicht zu begreifen (der entsprechende Infrastrukturen im Rahmen seiner Datenschutzgesetzgebung durchsetzen könnte) durchaus diskussionswürdig.

Im Einzelnen lassen sich die Ergebnisse wie folgt zusammenfassen:

- Die Bewertung von Anonymitätsdiensten ergibt ein sehr inhomogenes Bild. Während sich die Befragten bei HTTP-Anwendungen und elektronischen Diskussionsforen weitgehend einig sind, dass diese 2007 weit verbreitet sein werden, differieren die Experteneinschätzungen bei der Bewertung von Anonymitätsdiensten bei Bezahlvorgängen, bei der Mail-Kommunikation sowie bei der Erfassung von Bewegungsprofilen bei Mobilfunkanwendungen. Während jeweils die Mehrzahl solche Dienste bis 2009 erwartet, glauben jeweils ein Viertel nicht an eine solche Verbreitung – vor allem aufgrund fehlender Wirschaftlichkeit. Bei der Mailkommunikation wird darüber hinaus die Wünschbarkeit solcher Dienste in Frage gestellt.

- Die Befragten erwarten mehrheitlich, dass Anonymisierungsdienste trotz des möglichen Missbrauchpotenzials etwa 2009 weit verbreitet sein werden.

- Obwohl die weite Verbreitung kostenpflichtiger Anonymisierungsdienste nach heutigem Stand nicht zu erwarten ist, werden diese in den nächsten zehn Jahren leicht an Bedeutung hinzugewinnen.

- Etwa zwei Drittel der Befragten erwarten, dass die Benutzer nicht bereit sind, regelmäßig Geld für Anonymisierungsdienste auszugeben. Die übrigen Befragten erwarten langfristig einen Betrag von sieben Euro je Monat und Nutzer.

## 7.3.3 Kryptographie

Der Einsatz kryptographischer Verfahren zum Schutz des Inhalts einer zu übermittelnden Nachricht, sowie zur sicheren Authentisierung von Kommunikationspartnern, spielt in der modernen Kommunikation eine zunehmend wichtige Rolle.

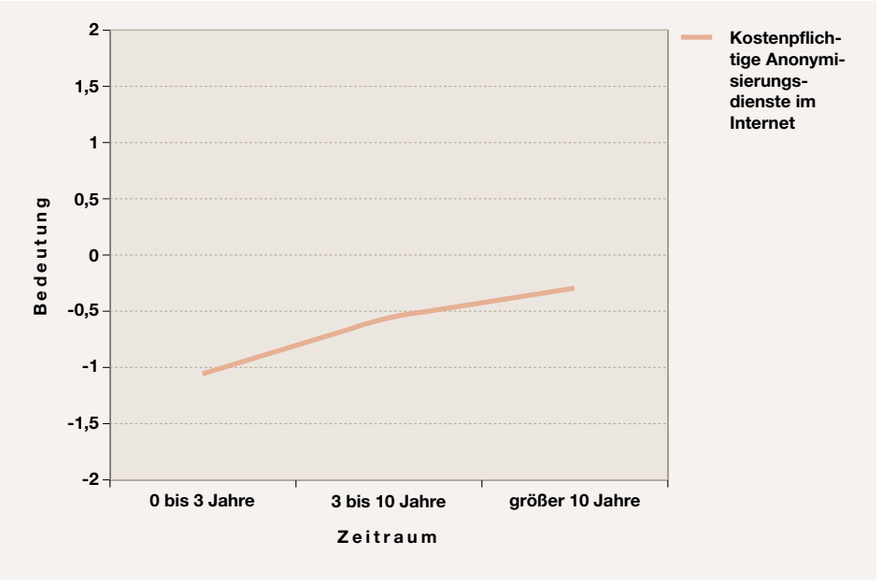



Abbildung 7.16: Bedeutung kostenpflichtiger Anonymisierungsdienste für Internetnutzer

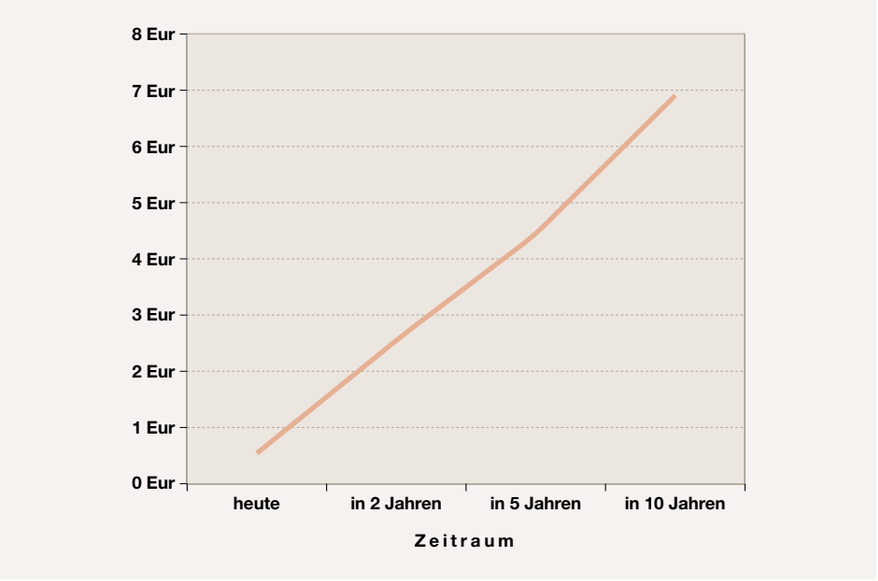



Abbildung 7.17: Höhe der Zahlungsbereitschaft eines Internetnutzers für Anonymisierungsdienste

Viele technische Maßnahmen zur Realisierung der Schutzziele verwenden kryptographische Mechanismen. Kryptographie (griechisch für Geheimschrift) und Kryptoanalyse (systematische Untersuchung kryptographischer Verfahren mit dem Ziel, ihre Schwächen herauszufinden oder sie vollständig zu brechen). stellten ursprünglich die Fertigkeit zur geheimen Kommunikation bzw. deren Aufhebung dar und gehen zurück bis in die altgriechische Zeit. Sie nehmen einen wichtigen Platz in der Geschichte ein, da viele historische Ereignisse von ihrem Einsatz beeinflusst wurden. Wer wichtige Informationen am besten schützen und sich Informationen über den Gegner unbemerkt beschaffen konnte, hatte strategische Vorteile und war auch in der Lage, seine Feinde effektiver zu bekämpfen und zu besiegen [Sing 99, Kahn 67]. Die beiden Disziplinen werden zusammengefasst unter dem Begriff Kryptologie. Sie war für sehr lange Zeit den militärischen, geheimdienstlichen und teilweise industriellen Bereichen vorbehalten. Die Entwicklung der Kryptologie kann man grob in zwei Hauptkategorien, die klassische und die moderne Kryptologie, aufteilen. Erstere beschäftigte sich fast ausschließlich mit den Verschlüsselungsverfahren und hat heute nur noch eine historische Bedeutung. Die moderne Kryptologie hingegen ist eine Wissenschaft, die sich nicht nur mit dem Entwurf und der Analyse der Verschlüsselungsverfahren beschäftigt, sondern auch mit dem Entwurf und der Analyse anderer Klassen kryptographischer Primitive (z.B. digitaler Signaturen) und komplexer kryptographischer Protokolle zur Realisierung verschiedener Aspekte mehrseitiger Sicherheit. Veröffentlichungen, welche die Entwicklung moderner Kryptographie besonders geprägt haben, sind Shannon's Papier über theoretische Behandlung kryptographischer Systeme [Shan 49] und das Konzept der Public-Key Kryptographie [DiHe 76]. Allerdings kündigte die britische Regierung Ende der neunziger Jahre an, dass die Public-Key Kryptographie bereits Anfang der siebziger Jahre von britischen Behörden erfunden wurde [Sing 99].

Die Sicherheit solcher kryptographischer Systeme kann nach verschiedenen Gesichtspunkten beurteilt werden. Sie kann auf der Geheimhaltung der verwendeten Verfahren basieren. Dies hat den Nachteil, dass eine Untersuchung des Systems auf mögliche Sicherheitsprobleme durch unabhängige Experten verhindert wird. Daher favorisiert man in der modernen Kryptographie die Ansicht, dass die Sicherheit eines kryptographischen Systems ausschließlich von der Geheimhaltung des verwendeten Schlüssels abhängen soll und nicht von der Geheimhaltung der zugrunde liegenden Algorithmen. Dies wird heute als das Kerckhoff'sche Prinzip bezeichnet, benannt nach dem holländischen Linguisten Kerckhoff von Nieuwenhof. Die moderne Kryptographie arbeitet unter Beachtung dieses Prinzips und setzt analytische Methoden ein, um die Sicherheit der Verfahren in verschiedenen Modellen zu untersuchen und gegebenenfalls zu beweisen.

Eine andere Art der Sicherheit ist die heuristische Sicherheit, auch Ad-hoc Sicherheit genannt. Hierbei wird nur argumentiert, dass jeder erfolgreiche Standardangriff mehr Ressourcen im Sinne von Rechenleistung und Speicher benötigt als dem Angreifer zugesprochen werden. Neue und noch unbekannte Angriffe können jedoch nicht ausgeschlossen werden. Folglich ist dieser Sicherheitstyp kritisch, da in der Vergangenheit viele Sicherheitslücken in heuristisch sicheren Systemen gefunden wurden. Die nächste Form der Sicherheit ist die informationstheoretische Sicherheit; dies bedeutet, dass die Sicherheit eines Systems unabhängig von den dem Angreifer zur Verfügung stehenden Ressourcen gewährleistet ist. Mit anderen Worten: auch wenn der Angreifer über beliebig viel Ressourcen verfügt, kann er die Sicherheit eines solchen Systems nicht brechen, wobei mit „Sicherheit" das jeweilige Schutzziel gemeint ist. Es gibt auch andere Modelle, in denen z.B. die Sicherheit gegen einen Angreifer gezeigt wird, der beliebig viel Rechenleistung, aber nur begrenzten Speicher zur Verfügung hat [Crypto97]. Informationstheoretische Sicherheit ist gewünscht, aber häufig nicht einfach oder effizient zu erreichen. Eine schwächere Sicherheitsform ist die komplexitätstheoretische Sicherheit; sie bedeutet, dass die Sicherheit des Systems von den Ressourcenbeschränkungen des Angreifers abhängt. Mit anderen Worten: das System bleibt sicher gegen alle Angreifer, die nicht mächtiger sind als in einer Annahme[6] vorgege-

[6] Die klassische Komplexitätstheorie beschäftigt sich mit

ben. Diese Sicherheitsform hat jedoch den Nachteil, dass sie auf der Annahme basiert, dass bestimmte Probleme nicht effizient, d.h., mit vertretbarem Aufwand, zu lösen sind, vor allem nicht mit den Ressourcen, die dem Angreifer zur Verfügung stehen. Die Wahl geeigneter Berechnungsmodelle bekam neue Aufmerksamkeit, als in [Shor 97] gezeigt wurde, dass gewisse Probleme (Faktorisierung, diskreter Logarithmus) effizient (mit polynomieller Laufzeit) auf einem (theoretischen) Quantencomputer lösbar sind.

Für beweisbare Sicherheit wird zunächst ein geeignetes formales Angreifermodell aufgestellt und die zu beweisende Sicherheitseigenschaft in diesem Modell definiert. Dann wird formal gezeigt, dass das zugrunde liegende kryptographische System diese Definition erfüllt. Beispielsweise kann man die Sicherheit eines asymmetrischen Verschlüsselungssystems gegen passive Angriffe in einem komplexitätstheoretischen Modell wie folgt definieren: Ein polynomieller Angreifer kann nicht mit einer signifikant höheren Wahrscheinlichkeit als bei purem Raten (1/2) die Verschlüsselung der Nachricht 0 von der Verschlüsselung der Nachricht 1 unterscheiden. Eine Sicherheitsdefinition soll also zwei wichtige Aspekte spezifizieren, nämlich welche Fähigkeiten (Ressourcen) dem Angreifer zugesprochen werden und welche Aufgaben er bewältigen soll, um als erfolgreich gegen das entsprechende Schutzziel zu gelten. Verschiedene kryptographische Primitive haben unterschiedliche Sicherheitsdefinitionen. Eine Blockchiffre gilt als sicher, wenn man beweisen kann, dass sie sich von einer Zufallspermutation nicht unterscheiden lässt. In ähnlicher Weise wird die Sicherheit für einen Authentikationscode definiert. Die stärkste Sicherheitsdefinition für ein asymmetrisches Verschlüsselungssystem ist die Sicherheit gegen sog. Adaptive Chosen Ciphertext Attacks (CCA) im Sinne der Ununterscheidbarkeit [GoMi 84, Shou 98]. Für ein Signatursystem ist dies gegen Adaptive Chosen Message Attacks [GMR 88]. Hierbei wird die Sicherheit des Systems unter dem entsprechenden Angriff (z.B. CCA) auf ein bekanntes hartes Problem reduziert.

der worst-case Komplexität verschiedener Probleme. Für kryptographische Sicherheit müssen jedoch alle Instanzen eines Problems schwierig sein und nicht nur manche.

Eine Verbesserung der rein heuristischen Vorgehensweise bietet das Random Oracle Modelle [BeRo 93]. Es ist ein idealisiertes Modell, in dem die Sicherheit kryptographischer Systeme bewiesen wird. Hierbei werden kryptographische Funktionen erst durch ein idealisiertes Zufallsorakel ersetzt. Als nächstes wird die Sicherheit des Systems in dem entsprechenden Angreifermodell unter einer geeigneten Sicherheitsdefinition bewiesen. Schließlich werden die Zufallsorakel durch effiziente konkrete kryptographische Primitive ersetzt, wobei diese keine Sicherheitslücken haben sollten. Obwohl der letzte Schritt wiederum keinen formalen Beweis liefert, stellt das Modell eine bessere Alternative zu Ad-hoc Sicherheitsbeweisen dar. Allerdings sind ihm auch Grenzen gesetzt, wie beispielsweise ein in [CGH 98] künstlich konstruiertes Gegenbeispiel zeigt.

Andere Formen der Sicherheit basieren auf physikalischen Modellen und Annahmen wie der Quantentheorie [Vita 01, RiPo 01] oder manipulationssicherer Hardware mit Seitenkanälen[7] (Side Channels) geringer Kapazität.

Beweisbare Sicherheit ist inzwischen zu einem wichtigen Grundsatz der Kryptographie geworden. Sie hat jedoch auch ihre Grenzen. Beispielsweise kann sie nicht die Möglichkeit ausschließen, dass gewisse Angriffsklassen nicht in das für die beweisbare Sicherheit übliche Angreifermodel fallen, wie z.B. Differential Power Analysis [Crypto99] und Timing Attacks [Koch 95]. Des weiteren sollten die Implementierungen der entsprechenden Verfahren keine Schwachstellen haben. Daher soll die Erweiterung der beweisbaren Sicherheit diese Möglichkeiten berücksichtigen.

Kryptographische Annahmen basieren im Allgemeinen häufig auf mathematischen Problemen, zu deren Lösung noch keine effizienten Algorithmen bekannt sind. Effizient heisst hier, dass sich die erforderliche Laufzeit bezüglich eines geeigneten Parameters, des sog. Sicherheitspa-

[7] Kryptographische Algorithmen werden normalerweise in mathematischen Modellen analysiert. In der Praxis sind diese Algorithmen und die dazugehörigen Berechnungen jedoch in eine physikalische Umgebung eingebettet (z.B. in einen Chip), die dem Angreifer nützliche Seiteninformationen liefern könnte, z.B. der benötigte Energieverbrauch für bestimmte Berechnungen (Differential Power Analysis [Crypto99], siehe auch http://www.iaik.tugraz.at/research/).

rameters, polynomiell verhält. Diese Probleme sind Gegenstand langjähriger algorithmischer Untersuchungen und gelten trotzdem noch als schwer lösbar. Somit bilden sie eine bessere Grundlage für die Sicherheit kryptographischer Systeme als heuristische Argumente. Die meisten dieser Probleme sind zahlentheoretischer Natur. Das bekannteste und vielleicht älteste von ihnen ist wohl das Faktorisierungsproblem. Es bezeichnet die Schwierigkeit, gegebene sehr große Zahlen (von mehreren hundert Dezimalstellen) effizient in ihre Primfaktoren zu zerlegen. Für geeignet gewählte Zahlen, d.h. solche, die sehr große Primfaktoren mit bestimmten Eigenschaften besitzen, ist noch kein effizienter allgemeiner Faktorisierungsalgorithmus bekannt [MvOV 97, Kali 98]. Die auf diesem Problem basierende Annahme heißt Faktorisierungsannahme. Ein weiteres bekanntes Problem aus der Zahlentheorie ist das sog. Diskrete Logarithmus Problem (DL) [McCu 90]. In bestimmten mathematischen Strukturen (endliche Körper, elliptische und hyperelliptische Kurven [Kobl 87, Kobl 98]) ist auch zur Lösung dieses Problems noch kein effizienter Algorithmus bekannt. Es gibt zahlreiche weitere Annahmen, die mit den beiden zuvor genannten meistens in irgendeiner Form verwandt und häufig auch stärker[8] sind. Einige bekannte Annahmen sind die RSA Annahme [RSA 78], die Quadratische-Reste (QR) Annahme [GoMi 84], die Diffie-Hellman (DH) Annahme [DiHe 76] und die Decision-Diffie-Hellman (DDH) Annahme [Crypto93, Shou 97, ANTS 98b, ACMEC 00].

Zur Formulierung dieser Annahmen sind verschiedene Parameter von zentraler Bedeutung, u.a. die zugrunde liegende mathematische Struktur und die über diese Struktur bekannte Information [SaSt 01]. Zur Bestimmung theoretischer unterer Schranken für den Schwierigkeitsgrad eines Problems (z.B. DL) betrachtet man das Problem in dem sog. generischen Modell. In diesem Modell geht man davon aus, dass einem Algorithmus, der das Problem lösen soll, keine spezifische Information über die zugrunde liegende mathematische Struktur bekannt ist (z.B. wie ihre Elemente kodiert sind). Ein generischer Algorithmus zur Lösung diskreter Logarithmen kann für beliebige algebraische Gruppen eingesetzt werden [ANTS 98b]. In [Shou 97] wird u.a. die Komplexität generischer Algorithmen zur Lösung diskreter Logarithmen bestimmt. Allerdings sind dem generischen Modell auch Grenzen gesetzt, da es nicht zur Analyse beliebiger Probleme verwendet werden kann [Fisc 00].

Es gibt derzeit unterschiedliche und sehr ausgeklügelte, jedoch noch aufwändige Algorithmen zur Faktorisierung großer Zahlen oder zur Lösung diskreter Logarithmen in verschiedenen algebraischen Strukturen [MvOV 97, Lens 00]. Ein Beispiel ist die Faktorisierung der 512-Bit langen RSA Modulozahl [CDL$^+$ 00] mittels des sog. Faktorisierungsalgorithmus Number Field Sieve [LLMP 90]. Um in der Praxis sichere kryptographische Systeme zu erhalten, müssen die Parameter der entsprechenden Annahmen geeignet gewählt werden [LeVe 01].

Zu den wichtigen kryptographischen Primitiven (Grundbausteinen) gehören Einweg- und Hashfunktionen, Verschlüsselungs- und Authentikationsverfahren. Diese können prinzipiell in die zwei Klassen der symmetrischen und der asymmetrischen (Public-key) Verfahren unterteilt werden. Symmetrische Verfahren benötigen den gleichen geheimen Schlüssel für ihre Funktionen, während asymmetrische Verfahren unterschiedliche Schlüssel, einen geheimen und einen öffentlichen, für unterschiedliche Funktionen benötigen. Symmetrische und asymmetrische Primitive haben ihre Vor- und Nachteile, z.B. hinsichtlich des Schlüsselmanagements und der Erreichung gewisser Schutzziele: Zur Verwendung symmetrischer Primitive benötigt jedes mögliche Paar der Kommunikationspartner den gleichen geheimen Schlüssel. Zudem müssen diese Schlüssel authentisch und integer verteilt werden. Bei asymmetrischen Verfahren hingegen reicht ein authentischer Kanal zur Schlüsselverteilung aus. Im Allgemeinen ist das Schlüsselmanagement für asymmetrische Verfahren effizienter. Hierzu verwendet man die sog. Public-Key Infrastrukturen (PKI). Allerdings sind diese auch nicht völlig unproblema-

[8] Eine Annahme $A$ ist stärker als eine Annahme $B$ bedeutet: Findet man einen Algorithmus, der das der Annahme $B$ zugrunde liegende Problem löst, so kann man diesen verwenden, um das der Annahme $A$ zugrunde liegende Problem zu lösen, aber nicht umgekehrt. Wünschenswert ist, dass die Sicherheit auf schwächeren Annahmen beruht.

tisch [ABD+ 00, Elli 99, ElSc 00]. Weiterhin bieten asymmetrische Primitive wie die digitale Signatur die Nichtabstreitbarkeitseigenschaft, welche Disputauflösungen ermöglicht (siehe auch [MvOV 97] für weitere Vergleiche).

Einwegfunktionen gehören zu den fundamentalsten kryptographischen Primitiven in der komplexitätstheoretischen Kryptographie. Informell hat eine Funktion die Einwegeigenschaft, wenn der Funktionswert für alle Eingaben effizient zu berechnen ist, aber die Umkehrung mit vertretbarem Aufwand nicht möglich sein soll. Derzeit ist es nicht bekannt, ob solche Funktionen existieren. Es gibt jedoch sinnvolle Kandidaten, deren Einwegeigenschaft stark vermutet wird [Gold 01]. Eine wichtige Klasse von Einwegfunktionen sind kryptographische Hashfunktionen. Grundsätzlich erstellt eine Hashfunktion aus einem beliebig langen Quelltext einen kurzen Hashwert mit fester Länge (z.B. 128 Bit). Üblicherweise soll eine kryptographische Hashfunktion kollisionsresistent sein, um sichere Verwendbarkeit zu ermöglichen [Pren 98], d.h. es soll mit vertretbarem Aufwand nicht möglich sein, zwei unterschiedliche Eingaben mit dem gleichen Hashwert zu finden. Allerdings hängen die Sicherheitsanforderungen an eine Hashfunktion von der jeweiligen Anwendung ab. Hashfunktionen werden vielseitig eingesetzt, z.B. zur Integritätssicherung in Verbindung mit digitalen Signaturen, wobei aus Effizienz- und Sicherheitsgründen der Hashwert einer Nachricht (statt der Nachricht selbst) signiert wird. Eine weitere Anwendungen ist der Einsatz von Hashfunktionen für symmetrische Authentikation (Message Authentication Code). Bekannte kryptographische Hashverfahren sind MD5 [Rive 92], SHA-1 [NIST 95] und RIPEMD [DBP 96].

## Ergebnisse

Bei der Bewertung symmetrischer Verfahren wird der Advanced Encryption Standard (AES) nach Einschätzung der Befragten den Data Encryption Standard (DES) und die darauf basierende Triple-DES-Verschlüsselung für kommerzielle Zwecke in spätestens vier Jahren abgelöst haben (Abbildung 7.18, ①). AES (Advanced Encryption Standard) ermöglicht im Gegensatz zu DES (Data Encryption Standard) variable Schlüssellängen und damit verschiedene Sicherheitsniveaus. AES ist besser für Softwareimplementierungen optimiert als DES. Daher werden zusätzliche Potenziale bei der Integration von Softwareverschlüsselung in der Applikationsebene gesehen. Überwiegend werden jedoch keine neuen Anwendungsfelder erwartet. Viele sehen die Ablösung von Triple-DES als eine Frage der Ablösung alter Anwendungen, da neue im Wesentlichen AES implementieren.

ADVANCED ENCRYPTION STANDARD (AES): wird in spätestens 4 Jahren DES und Triple-DES abgelöst haben, die nur noch aus Kompatibilitätsgründen in neuen Produkten eingesetzt werden.

Wie aus Abbildung 7.19 ersichtlich, erwarten die Experten über die nächsten zehn Jahre das langsame Ansteigen der Mindest-Schlüssellängen, die als sicher erachtet werden, auf die Maximallänge von 256 Bit, die der Standard erlaubt. Die Triple-DES-Verschlüsselung für den kommerziellen Einsatz wird in den nächsten zehn Jahren stark an Bedeutung verlieren, siehe Abbildung 7.20. Mittelfristig wird erwartet, dass Triple-DES aus Kompatibilitätsgründen in Verschlüsselungs-Suites wie SSL (Secure Socket Layer), S/MIME (Secure Multipurpose Internet Mail Extension) und IPSec sowie in Hardwaremodulen noch Einsatz finden wird.

In der asymmetrischen Kryptographie basieren die verwendeten Verfahren überwiegend auf drei mathematischen Problemen: Dem Faktorisierungs- und RSA-Problem, dem Problem des diskreten Logarithmus in endlichen Körpern und zunehmend auf dem Problem des diskreten Logarithmus auf elliptischen Kurven. Bei Verfahren, die auf dem Faktorisierungs- und RSA-Problem beruhen, wird erwartet, dass die als hinreichend erachteten Schlüssellängen über die nächsten zehn Jahre von derzeit 1024 Bit auf 2048 bzw. 3072 Bit nahezu linear ansteigen und die darauffolgende Zeit auf diesem Niveau verbleiben. Bei Verfahren auf Basis des diskreten Logarithmus in endlichen Körpern erwarten die Experten langfristig ein Ansteigen auf etwa 3072 Bit. Im Gegensatz zu RSA werden nach Ansicht der Befragten die derzeitigen Schlüssellängen von 1024 Bit etwas länger verwendet werden. Lediglich bei Verfahren, die sich das Problem des diskreten Logarithmus auf elliptischen Kurven zunutze machen, wird davon ausgegangen, dass die derzeitigen Schlüssellängen von etwa 160 Bit auch für die nächsten Jahre ausreichend sein werden und langfristig auf etwa 256 Bit ansteigen werden.

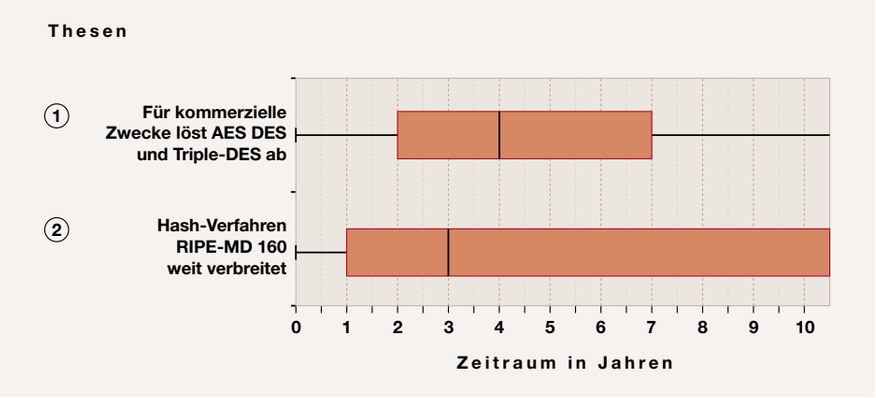



Abbildung 7.18: Ergebnisse der Thesen zu symmetrischen Verfahren und Integritätssicherungsverfahren

DISKRETER LOGARITHMUS AUF ELLIPTISCHEN KURVEN: Verfahren, die auf diesem mathematischen Problem beruhen, werden langfristig andere Verfahren wie RSA ablösen.

Um die Bedeutung aktueller und zukünftiger asymmetrischer Verfahren einzuschätzen, wurden die Experten nach verschiedenen Systemen befragt. Das Ergebnis ist in Abbildung 7.21 aufgezeichnet. Nach Einschätzung der Befragten werden dabei zukünftig Verfahren auf Basis des Problems des diskreten Logarithmus auf elliptischen Kurven eine zunehmend größere Bedeutung haben, während die derzeit am weitesten verbreiteten, auf dem Faktorisierungsproblem basierenden Verfahren, deutlich an Bedeutung verlieren werden. Alle anderen Verfahren werden sich über die nächsten zehn Jahre kaum in Ihrer Bedeutung verändern.

Verfahren, die auf dem Faktorisierungsproblem basieren, machen sich die Jahrhunderte alte Annahme zu nutze, dass es sehr schwierig ist, große Zahlen in ihre Primfaktoren zu zerlegen. Da diese Verfahren, wie z.B. RSA, zu den ersten praktisch eingesetzten asymmetrischen Verschlüsselungsverfahren gehörten, verfügen sie heute über eine weitreichende Marktpenetration. RSA wird heute zur Verschlüsselung und für die Digitale Signatur eingesetzt. Ebenfalls zu den frühen asymmetrischen Verfahren gehören diejenigen, die auf der Schwierigkeit des Ziehens diskreter Logarithmen (in endlichen Körpern) basieren. Diese, zu denen das ElGamal-Verschlüsselungsverfahren und das Diffie-Hellmann Schlüsselaustauschverfahren gehören, werden ebenfalls für Verschlüsselung und Digitale Signaturen eingesetzt.

In die vergleichsweise neuen Verfahren, die sich die Schwierigkeit diskreter Logarithmus auf elliptischen Kurven zunutze machen, werden hohe Erwartungen gesetzt, auch aufgrund kürzerer Schlüssellängen und effektiver Implementierungsmöglichkeiten in Hardware. Hingegen werden den Verfahren, die auf dem Problem des diskreten Logarithmus in Klassengruppen von imaginär quadratischer Ordnung, auf dem Problem der kürzesten Basisvektoren in Gittern (insbesondere NTRU), sowie auf dem XTR diskreten Logarithmus Problem beruhen, mittelfristig kaum Chancen außerhalb des akademischen Bereichs gegeben. Über die gefragten Verfahren hinaus erwarten die Experten langfristig eine Zunahme der informationstheoretisch sicheren Verfahren. Im Gegensatz zu den üblichen, komplexitätstheoretisch sicheren Verfahren, sind informationstheoretische auch gegen Angreifer sicher, deren Rechenleistung unbeschränkt ist.

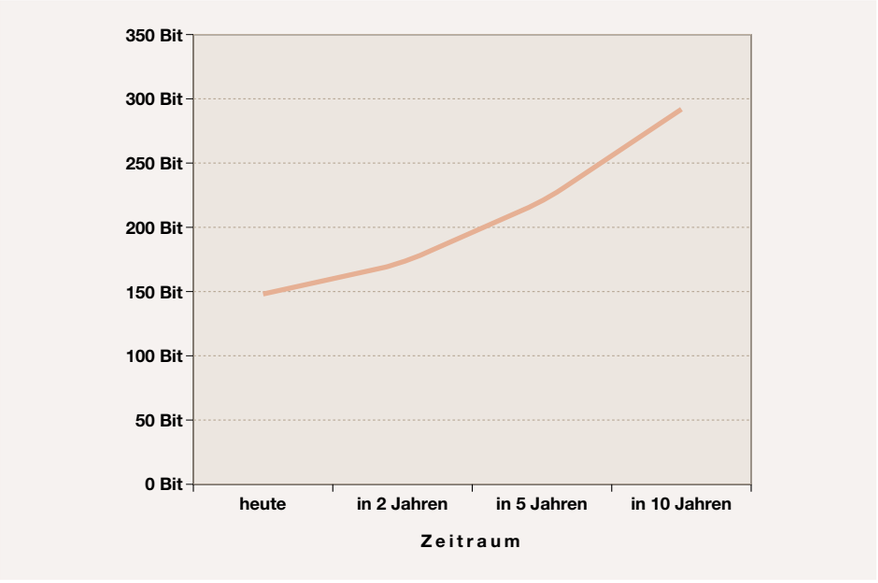



Abbildung 7.19: Länge des in AES verwendeten und als sicher erachteten Schlüssels

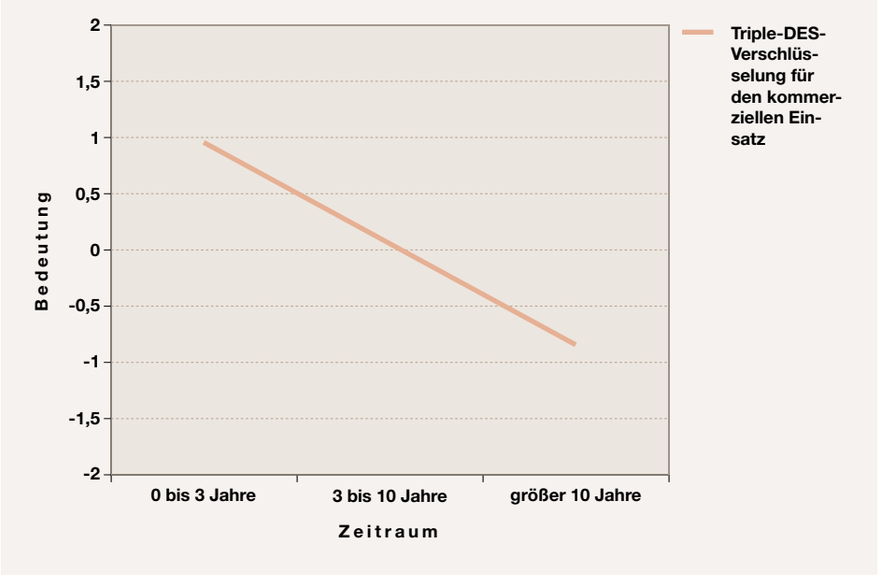



Abbildung 7.20: Bedeutung der Triple-DES-Verschlüsselung für den kommerziellen Einsatz

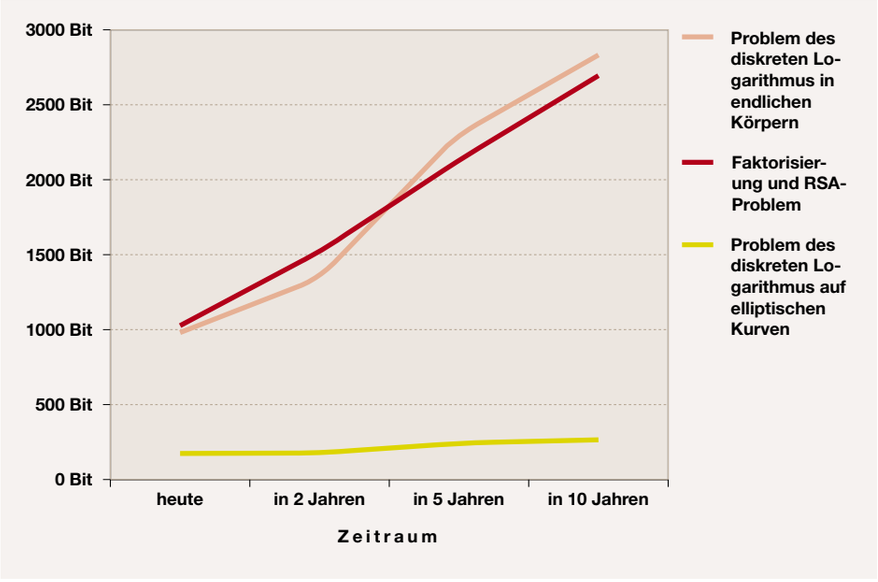



Abbildung 7.21: Schlüssellängen für kryptographische Verfahren auf Basis unterschiedlicher mathematischer Methoden

### Zusammenfassung

Die derzeit eingesetzten kryptographischen Verfahren werden auch in den nächsten Jahren noch eine dominante Rolle spielen. Obwohl beispielsweise DES in neuentwickleten Protokollen und Systemen bereits sehr schnell verschwinden wird, bleibt es aus Kompatibilitätsgründen in Produkten mit älteren Protokoll-Suites weiterhin eine nennenswerte Komponente. Auch bei den asymmetrischen Verfahren ist in den nächsten Jahren keine revolutionäre Abkehr von den derzeit benutzten Verfahren zu erwarten.

- Bei den symmetrischen Verfahren kann davon ausgegangen werden, dass AES alle DES-basierten Verfahren spätestens 2007 abgelöst haben wird. Die Expertern erwarten darüber hinaus, dass 2008 die maximal im AES-Standard vorgesehene Schlüssellänge von 256 Bit für einen adäquaten Schutz nötig sein wird.

- Die Bewertung der asymmetrischen Verfahren lässt auf eine zunehmende Bedeutung von Verfahren auf Basis des Problems des diskreten Logarithmus auf elliptischen Kurven schließen, während die derzeit am weitesten verbreiteten, auf dem Faktorisierungsproblem basierenden Verfahren, deutlich an Bedeutung verlieren werden. In den nächsten zehn Jahren werden sich alle anderen betrachteten Verfahren kaum in ihrer Bedeutung verändern. Die Schlüssellängen werden in diesem Zeitraum nahezu linear ansteigen.

## 7.3.4 Standards

Für die Implementierung kryptographischer Verfahren haben sich verschiedene Standards entwickelt (siehe Abbildung 7.22). Der IEEE Standard P1363, dessen Entwicklung lange Zeit in Anspruch genommen hat und der ständig weiterentwickelt wird, wird sich nach Ansicht der Experten langsam zum Industriestandard entwickeln und hat gute Chancen, zukünftige Interoperabilität zu gewährleisten. P1363 verfügt über einen sehr guten wissenschaftlichen Hintergrund und unterstützt in den Versionen P1363-2000 und P1363a neben den herkömmlichen Verfahren, die auf Faktorisierung bzw. diskreten Logarithmen beruhen, auch Verfahren auf der Grundlage elliptischer Kurven. Die Ausführungen P1363.1 bzw. P1363.2 standardisieren darüber hinaus Verfahren auf Basis kürzester Basisvektoren wie NTRU bzw. Passwort-basierte Systeme.

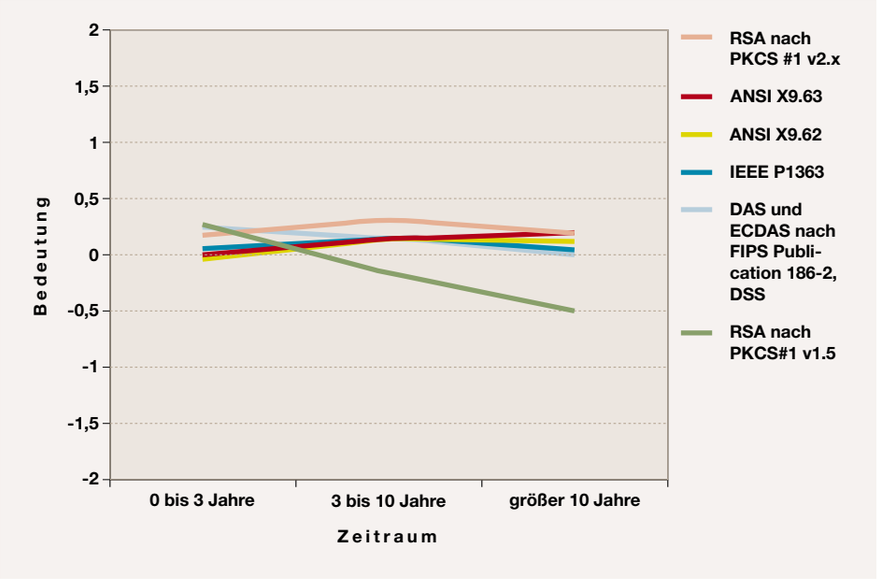



Abbildung 7.22: Bedeutung verschiedener Standards für die Implementierung kryptographischer Verfahren

PKCS#1 V2.X: Wird in den nächsten Jahren als Verschlüsselungsstandard dominieren.

Der heute weit verbreitete Verschlüsselungsstandard nach dem RSA-Verfahren PKCS #1 in der Version 1.5 wird in den nächsten Jahren deutlich an Bedeutung verlieren und durch die Version 2.0 abgelöst werden. Im Gegensatz zur Version 1.5, die gegen eine ganze Klasse von Angriffen anfällig war, wird in PKCS#1 v2.x die beweisbar sichere RSA-Variante Optimal Asymmetric Encryption Protocol (OAEP) verwendet. Aufgrund der Erwartung der allgemeinen Verdrängung von RSA-basierten Systemen wird allerdings über die nächsten zehn Jahre wieder eine leicht abnehmende Bedeutung erwartet. Wie aus Abbildung 7.22 ersichtlich ist, messen die Befragten auch den Diskreten-Logarithmus basierten Signaturstandards DSA und ECDSA (nach FIPS Publication 186-2, Digital Signature Standard; DSS) langfristig weniger Bedeutung zu.

Mit den amerikanischen ANSI-Standards X9.62 (Elliptic Curve Digital Signature Algorithm, ECDSA) und X9.63 (Elliptic Curve Key Agreement and Key Management, ECDH) stehen dem Markt erstmals einheitliche Formate für die Verwendung von elliptischen-Kurven basierten Kryptosystemen zur Verfügung, die nach Ansicht der Experten eine zunehmend größere Bedeutung erlangen werden. Anwendungspotenziale werden kurzfristig im Bereich qualifizierter elektronischer Signaturen und in der Implementierung von Smartcards gesehen. Mittelfristig werden Potenziale im Bereich fortgeschrittener elektronischer Signaturen, und aufgrund von US-Vorgaben beispielsweise, auch für den NATO-Bereich gesehen.

Die Ergebnisse des durch die Europäische Union geförderten NESSIE-Projektes (New European Schemes for Signatures, Integrity and Encryption) werden nach Ansicht der Befragten über die nächsten zehn Jahren eine mittlere Bedeutung erlangen. Die Experten erwarten von NESSIE keine wesentlichen Impulse. So ist der Erfolg derartiger europäischer Initiativen von der internationalen Akzeptanz, vor allem in den USA, abhängig. Lediglich im Hash-Bereich könnten interessante Ergebnisse erzielt werden (siehe Abbildung 7.23).

RIPE-MD 160: Das innerhalb eines EU-Projektes entwickelte Hash-Verfahren wird in 3 Jahren weit verbreitet sein. Lediglich der US-amerikanische Standard SHA-1 wird dann größere Bedeutung haben.

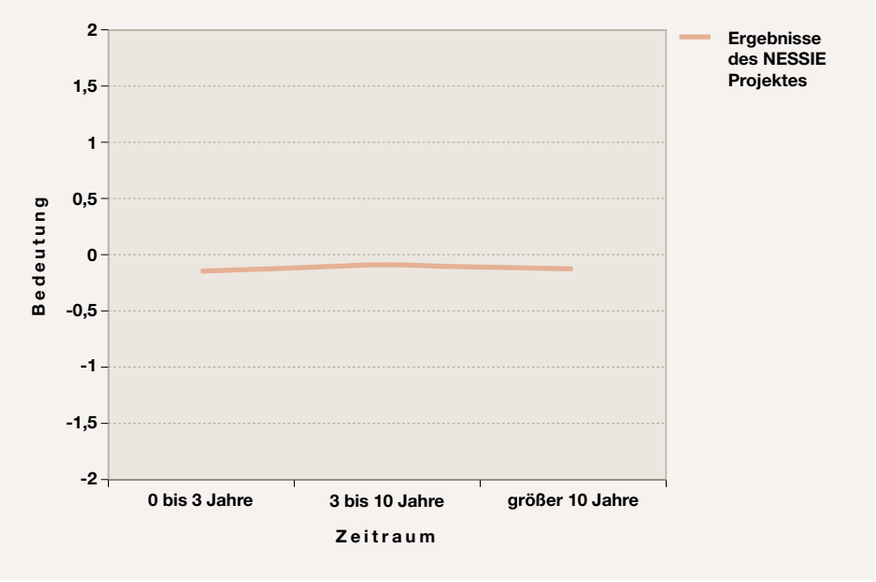



Abbildung 7.23: Bedeutung des NESSIE-Projektes

## Zusammenfassung

Die Bewertung der Standards spiegelt die erwartete Entwicklung bei den kryptographischen Verfahren wider. So wird langfristig eine Verdrängung der RSA-basierten Standards durch Standards für elliptische Kurven erwartet.

- Der IEEE-Standard P1363, der einen breiten Bereich kryptographischer Verfahren abdeckt, wird sich nach Ansicht der Befragten zum Industriestandard entwickeln. Auch die elliptische Kurven-basierten ANSI-Standards X9.62 und X9.63 werden eine zunehmend größere Bedeutung spielen.
- Die derzeit bedeutenden Standards DSA, ECDSA (diskreter Logarithmus-basiert) und PKCS (RSA-basiert) werden hingegen langfristig an Bedeutung verlieren. Bereits mittelfristig wird die PKCS-Version 1.5 durch die Version 2.0 abgelöst werden.
- Enttäuschend ist die Bewertung des von der EU geförderten NESSIE-Projektes. Die Ergebnisse werden nach Ansicht der Befragten über die nächsten zehn Jahre kaum einen Einfluss auf die Standardisierungsaktivitäten haben.

## 7.3.5 Verfahren zur Integritätssicherung

Neben Vertraulichkeit sind Authentizität und Integrität einer Nachricht die wichtigsten Sicherheitsziele. Als Integritätssicherungsverfahren werden vornehmlich kryptographische Hash-Funktionen eingesetzt. Dies sind typischerweise kollisionsfreie Einwegfunktionen, d.h. es ist schwierig, aus dem Funktionswert den Eingabewert zu folgern.

Das innerhalb des EU-Projektes RIPE entwickelte Hash-Verfahren RIPE-MD 160 wird nach Ansicht der Experten frühestens in drei Jahren weit verbreitet sein (siehe Abbildung 7.18, ②). Insbesondere sind derzeit die Hash-Verfahren MD5 und SHA-1 deutlich weiter verbreitet. Derzeit wird das RIPE-MD 160 beispielsweise im Kryptogateway SINA [Bund 03b] oder im PLUTO-Chip [Bund 03a] des BSI eingesetzt. Weitere Anwendungspotenziale werden im Bereich der qualifizierten elektronischen Signatur gesehen.

In Abbildung 7.24 ist die Bewertung verschiedener Hash-Verfahren aufgezeigt. Dem durch die NSA entwickelten US-Standard SHA-1, der heute als Marktführer gilt, wird die größte Bedeutung beigemessen. Obwohl die Befragten einen Bedeutungsrückgang und eine zunehmende

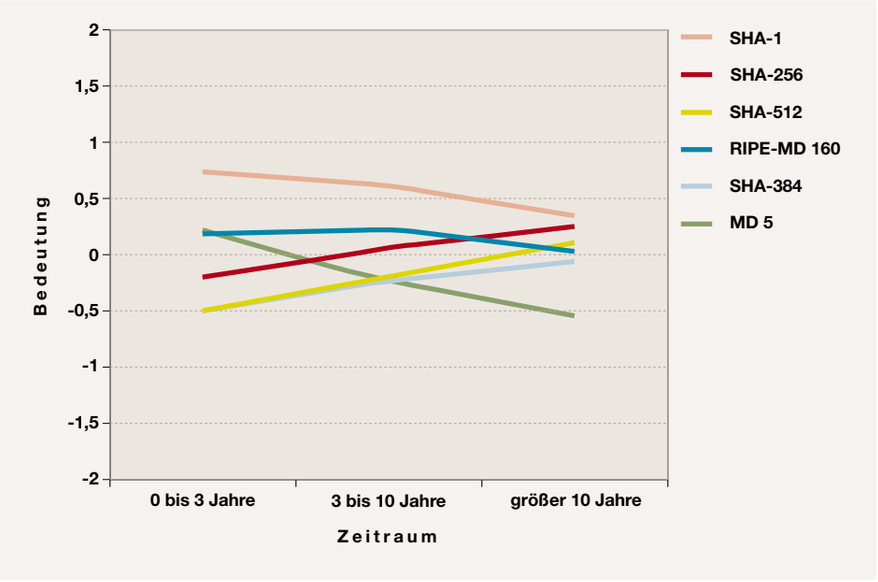



Abbildung 7.24: Bedeutung verschiedener Hash-Verfahren

Ablösung durch seine Nachfolger erwarten, wird davon ausgegangen, dass auch in zehn Jahren SHA-1 der vorherrschende Standard sein wird. Die SHA-1 Nachfolger SHA-256, SHA-384 und SHA-512 spielen derzeit eine untergeordnete Rolle, gewinnen aber über die nächsten zehn Jahre an Bedeutung. Während SHA-1 genau wie RIPE-MD 160 einen 160 Bit-langen Hashwert generiert, werden bei dessen Nachfolgern 256, 384 bzw. 512 Bit lange Hashwerte erzeugt. Diese werden beispielsweise in neuen Signaturverfahren benötigt. Das von Ronald Rivest entworfene und als unsicher eingestufte Hash-Verfahren MD5 wird derzeit noch in vielen Anwendungen eingesetzt. Die Experten erwarten eine stark abnehmende und in zehn Jahren nur noch untergeordnete Bedeutung dieses Verfahrens.

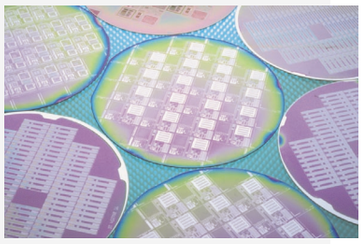
### Zusammenfassung

Anders als bei den Eregbnissen des NESSIE-Projektes werden dem im EU-Projekt RIPE entwickelten Hash-Standard RIPE-MD 160 gute Zukunftsaussichten prognostiziert. Die größte Bedeutung wird allerdings nach wie vor dem US-Standard SHA-1 und langfristig seinen Nachfolgern beigemessen. MD5 von Ronald Rivest hingegen wird bereits mittelfristig weitestgehend verdrängt sein.

## 7.3.6 Beweisbare Sicherheit

Lange Zeit wurden Verfahren lediglich einer so genannten „Ad-Hoc-Analyse" unterzogen. Darin wird das kryptographische System und dessen Primitive auf alle gängigen Angriffsmuster und -verfahren überprüft. Diese Methode ist nicht sehr effektiv, da Fehler immer wieder übersehen werden. Dies zeigen die vielfältigen Beispiele von entdeckten Fehlern in Protokollen wie X.509 [I'Mi 90], SSH [Abad 97] sowie PKCS#1 und SSL [Crypto98a].

Um dieses Problem zu lösen, wurden bereits sehr früh kryptographische Verfahren vorgestellt, deren Sicherheit sich ausschließlich auf ein als schwer angenommenes mathematisches Problem reduzieren lässt. Im Bereich der asymmetrischen Kryptographie basieren die Verfahren im Wesentlichen auf komplexitätstheoretischen Annahmen, wie beispielsweise der Schwierigkeit, große Zahlen zu faktorisieren oder dem Ziehen diskreter Logarithmen. Zum Nachweis der Sicherheit werden dabei ähnlich zur Komplexitätstheorie Reduktionsbeweise eingesetzt, mit denen gezeigt wird, dass das Brechen eines bestimmten kryptographischen Verfahrens mindestens so schwierig ist wie die zugrunde liegende (komplexitätstheoretische) Annahme.



BEWEISBAR SICHERE VERFAHREN: Spielen heute bereits eine wichtige bemerkenswerte Rolle.

TEIL-AUTOMATISCHE ÜBERPRÜFUNG: Insbesondere im Hochsicherheitsbereich, sowie bei der Evaluierung und Zertifizierung komplexer Protokolle werden Verifikations-Werkzeuge und -Methoden an Bedeutung hinzugewinnen.

Die Annahmen selbst bleiben auch bei diesen Beweisen unbewiesen. So sind die meisten der heute eingesetzten Verfahren wie RSA nicht so sicher wie die Faktorisierung großer Zahlen, wie oftmals angenommen. D.h. es kann sehr wohl sein, dass ein Angreifer das System bricht, ohne dabei eine Lösung für das Faktorisierungsproblem gefunden zu haben.

Obwohl bereits sehr früh Verfahren vorgestellt wurden, deren Sicherheit den aufgestellten Definitionen beweisbar entsprachen, sieht man diesen ersten Systemen an, dass sie weniger aus funktionalen sondern vielmehr aus beweistechnischen Gründen konstruiert wurden und damit hoffnungslos ineffizient waren [GoMi 82]. Heute existieren hingegen eine ganze Reihe verschiedener beweisbar sicherer Verfahren [Crypto98b, BeRo 94, BeRo 96].

### Ergebnisse

Die Befragten gehen, wie in Abbildung 7.25 ersichtlich, davon aus, dass beweisbar sichere Verfahren in den nächsten Jahren leicht an Bedeutung hinzugewinnen werden, insbesondere in Bereichen, in denen eine hohe Verlässlichkeit gefordert wird, wie z.B. bei qualifizierten elektronischen Signaturen. Praktikabilitätsprobleme, die heute noch existieren, werden nach Ansicht der Experten gelöst werden, so dass dies noch für lange Zeit der Standardansatz für asymmetrische Kryptographie sein wird. Allerdings wird auch darauf hingewiesen, dass Spezialaspekte bei der Bewertung von Systemen nicht außer acht gelassen werden dürfen.

Für die Verlässlichkeit eines Kryptosystems ist es darüber hinaus unerlässlich, die Implementierungen der kryptographischen Verfahren zu überprüfen. Hierzu existieren seit einiger Zeit Methoden und Werkzeuge, mit deren Hilfe eine teil-automatische Überprüfung möglich ist [HLSS 96, Form 95, SOR 93]. Die Bedeutung wird zur Zeit als gering eingestuft; die Experten gehen jedoch von einer stark ansteigenden Bedeutung innerhalb der nächsten zehn Jahre aus (siehe Abbildnug 7.26). Insbesondere im Hochsicherheitsbereich sowie für Evaluierung und Zertifizierung und bei komplexen kryptographischen Protokollen, beispielsweise für den Zahlungsverkehr bzw. für elektronische Wahlen, werden Anwendungspotenziale erwartet. Allerdings sind auch viele der Befragten skeptisch; so wird die automatische Verifikation der Implementierung als schwierig angesehen und die Analyse auf Algorithmen- oder Modellebene als geeigneter eingestuft.

Die Entwicklung beweisbar sicherer kryptographischer Verfahren erfordert eine formale Modellbildung. Dabei werden die Rahmenbedingungen abstrakt formalisiert, um sie mathematisch fassbar zu machen. Manchmal, wie beim Random-Oracle-Modell, werden bestimmte Gegebenheiten idealisiert oder abstrahiert. Diese Modellbildung (bspw. Generic Model, Random Oracle) für die Entwicklung kryptographischer Verfahren wird nach Ansicht der Befragten über die nächsten Jahre eine konstant neutrale Bedeutung behalten (siehe Abbildung 7.27). Insgesamt wird den Ansätzen, kryptographische Verfahren zu beweisen, eine hohe Bedeutung beigemessen. Gleichzeitig aber wird davor gewarnt, andere Methoden, wie die Kryptanalyse, zu vernachlässigen.

### Zusammenfassung

Bei der Bewertung von beweisbarer Sicherheit sehen die Befragten erstaunlicherweise eine bereits heute bedeutsame Rolle bei kryptographischen Verfahren und erwarten in den nächsten Jahren ein weiteres Ansteigen. Bei der derzeitig unbedeutenden werkzeug-basierten Verifikation der Implementierungen ist eine starke Aufwärtsentwicklung zu erwarten und die eher weniger bekannten generischen Modelle werden auch zukünftig eine mittlere Rolle spielen.

## 7.3.7 Quanten-Computing

Als einer der langfristigen Forschungstrends innerhalb der Informatik gilt Quanten-Computing. Aufgrund des massiven Parallelrechnens, das Quantenrechner ermöglichen, können bestimmte Probleme mit exponentieller Komplexität mit Hilfe neuer Algorithmen in polynomineller Zeit gelöst werden. Dazu zählen unter anderem auch das Faktorisieren von Primzahlen oder das Ziehen diskreter Logarithmen, auf denen asymmetrischen Verschlüsselungsverfahren wie RSA

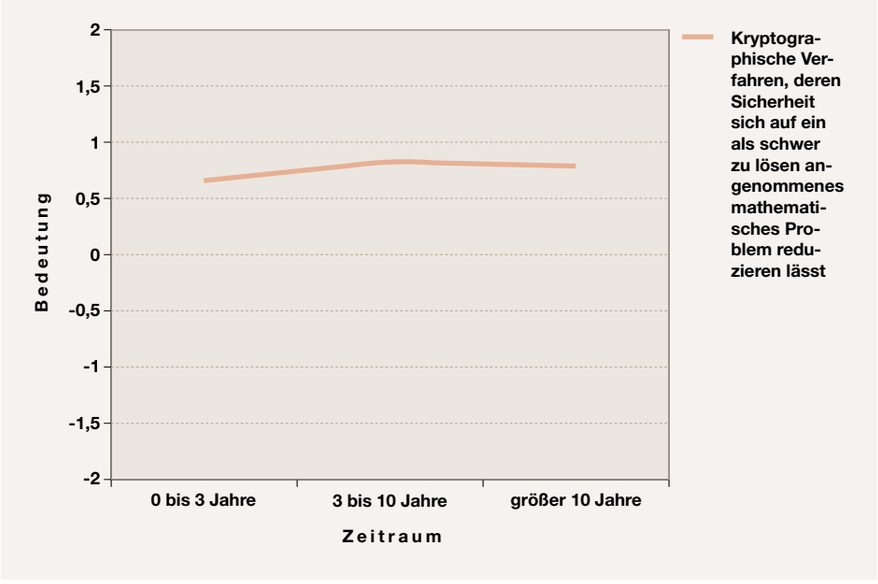



Abbildung 7.25: Bedeutung kryptographischer Verfahren, deren Sicherheit auf ein mathematisches Problem reduzierbar ist

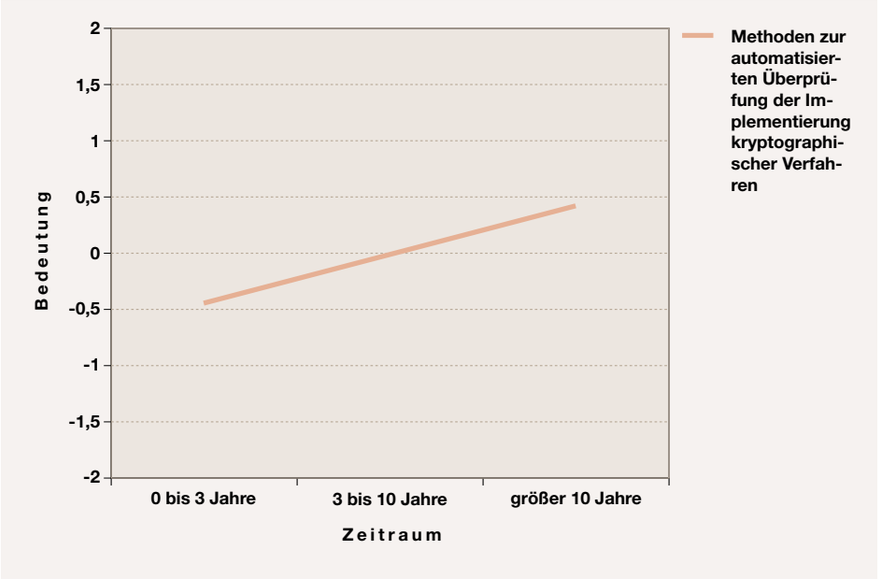



Abbildung 7.26: Bedeutung von Methoden zur automatisierten Prüfung der Implementierung kryptographischer Verfahren

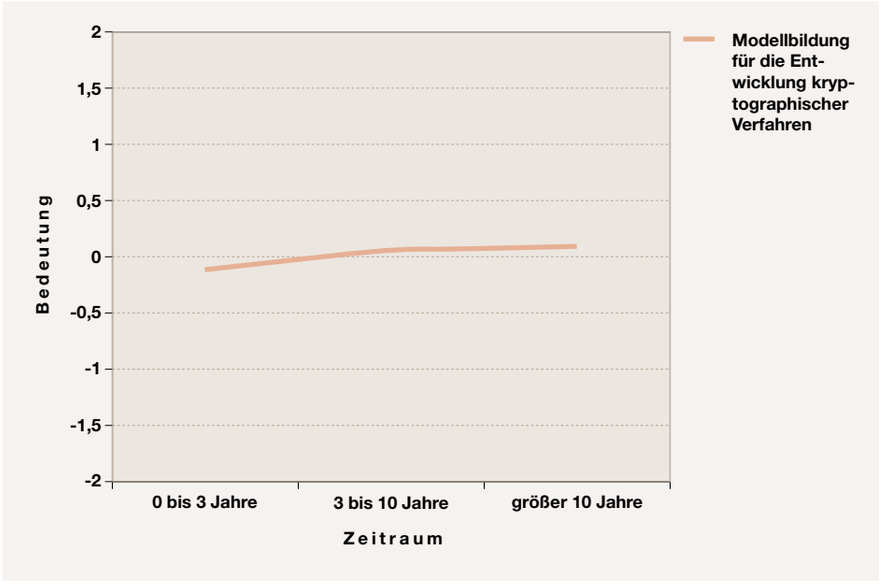



Abbildung 7.27: Bedeutung der Modellbildung für die Entwicklung kryptographischer Verfahren

AUF QUANTENMECHANISCHEN PRINZIPIEN BERUHENDE SIGNATURVERFAHREN: Diese Verfahren werden nicht innerhalb der nächsten 10 Jahren erwartet.

STEGANOGRAPHISCHE VERFAHREN: Diese Methoden zur vertraulichen Kommunikation werden kaum eine nennenswerte Rolle spielen.

oder Diffie-Hellman basieren. Während Kryptoanalytiker gespannt auf den Quantencomputer warten, arbeiten Kryptographen an Verschlüsselungs- und Signatursystemen, die ihre Geheimnisse schützen, selbst wenn ein mächtiger Quantencomputer dagegen antritt. Diese Systeme setzen in aller Regel ebenfalls die Verfügbarkeit von Quantencomputern für die sichernde Seite voraus.

Andererseits (und nicht zu verwechseln mit Quantum Computing) ermöglichen die Regeln der Quantenphysik völlig neue Konzepte in der Kommunikationskryptographie. So können vertrauliche Nachrichten so übermittelt werden, dass ein Abhören physikalisch ausgeschlossen werden kann (Quantenkryptographie).

## Ergebnisse

Nach Ansicht der Befragten werden Quantenrechner-resistente, asymmetrische, kryptograpische Verfahren in etwa drei Jahren verfügbar sein (siehe Abbildung 7.28, ①). Da auf absehbare Zeit keine ernsthafte Bedrohung durch Quantenrechner zu erwarten ist, sehen die Befragten momentan keine Bedeutung über den akademischen Bereich hinaus, erwarten jedoch eine sprunghafte Zunahme, sobald solche Systeme verfügbar sein werden. Unter dieser Annahme, dass Quantenrechner allgemein verfügbar sind, d.h. auch die „ehrlichen Nutzer" über solche verfügen, gibt es bereits sichere Verfahren [OTU 00].

Auf quantenmechanischen Prinzipien beruhende Schlüsseleinigungsverfahren werden nach Ansicht der Befragten in etwa acht Jahren verfügbar sein (siehe Abbildung 7.28, ②). Mögliche Einsatzbereiche werden bei Hochsicherheitsanwendungen und bei der Anbindung von Rechenzentren gesehen. Derzeit existieren einige Systeme [SGG+ 02], deren Sicherheit jedoch noch unklar ist.

Auf quantenmechanischen Prinzipien beruhende Signaturverfahren werden hingegen nicht innerhalb des betrachteten Zeitraums von zehn Jahren erwartet (siehe Abbildung 7.28, ③). Die Notwendigkeit wird auch nur im Zusammenhang mit der sicheren Schlüsselverteilung gesehen.

Nach Ansicht der Befragten werden steganographische Verfahren für das Sicherstellen vertraulicher Kommunikation kaum Bedeutung erlangen (siehe Abbildung 7.29). Anwendungsbereiche werden in Ländern mit Kryptoregulierung sowie im geheimdienstlichen Bereich gesehen. Nur wenige sehen einen kommerziellen

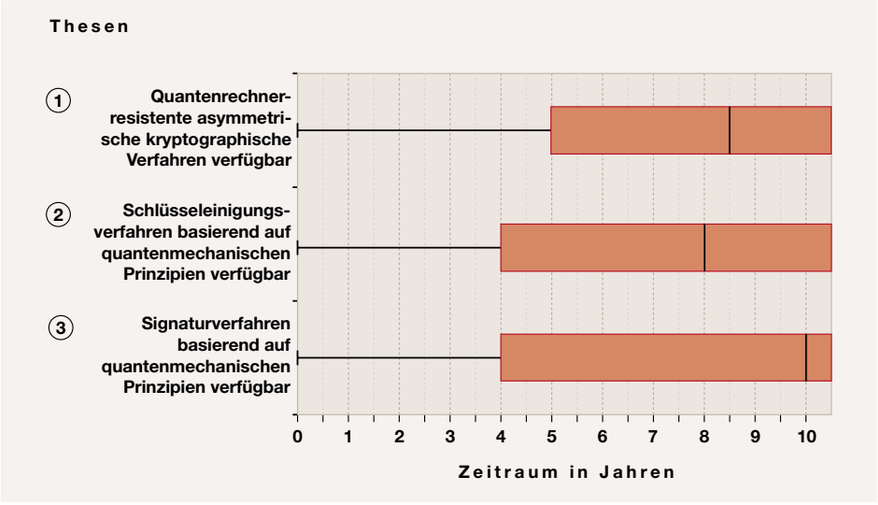



Abbildung 7.28: Ergebnisse der Thesen zu Quantenkryptographie

STANDARDISIERTE KRYPTOGRAPHISCHE VERFAHREN: In spätestens 4 Jahren werden diese nicht-veröffentlichte Verfahren im kommerziellen Bereich abgelöst haben.

Nutzen von Steganographie. Die Technologie selbst wird in anderen Bereichen, z.B. als Wasserzeichen für elektronische Medien, im Urheberschutz und in Urheberschaftsbeweisen verwendet.

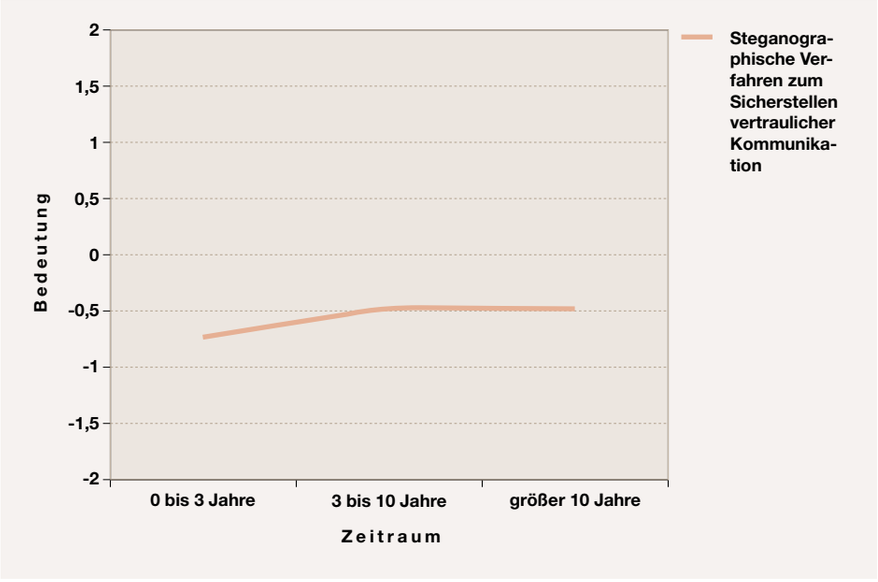
Nach den durch den französischen Kryptographen Kerckhoff aufgestellten Grundanforderungen an Kryptosysteme sollte die Offenlegung der Details von Chiffiersystemen deren Sicherheit nicht beeinträchtigen. Diese sollte einzig durch die Vertraulichkeit des Schlüssels begründet werden. Die Offenlegung kryptograpischer Verfahren ist daher zu einer essentiellen Voraussetzung für die Akzeptanz kryptographischer Verfahren geworden. Die Erfahrung zeigt, dass viele der nicht-veröffentlichten kommerziellen Algorithmen gebrochen wurden. Die Veröffentlichung ermöglicht nicht nur die Überprüfung durch die wissenschaftliche Gemeinde, sondern schafft auch das nötige Vertrauen für den Einsatz des Verfahrens.

### Ergebnisse

Die Experten erwarten, dass standardisierte kryptographische Verfahren bei kommerziellen Produkten in spätestens vier Jahren nicht-veröffentlichte kryptographische Verfahren abgelöst haben werden (Abbildung 7.30). Die Befragten gehen davon aus, dass insbesondere im kommerziellen und privaten Bereich in Zukunft kaum ein Benutzer sich in ein Abhängigkeitsverhältnis mit einer proprietären Lösung begeben wird. Viele prognostizieren auch im Bereich der militärischen Kommunikation einen Richtungswandel zu offenen Verfahren, insbesondere aufgrund von Interoperabilitätsanforderungen. Einzig im Bereich kryptographischer Chipkarten auf physikalischer Ebene wird die Vorgehensweise der Nicht-Offenlegung als sinnvoll eingestuft, beispielsweise um Side-Channel-Attacks zu erschweren.

## 7.3.8 Open-Source-Software

Unter Open-Source-Software versteht man Software, die der Open-Source-Definition genügt. Die wesentlichen Kriterien sind die freie Weiterverbreitung der Software, die Verfügbarkeit des Quellcodes und das Recht, die Software zu verändern. Damit steigert Open-Source-Software die Transparenz und die Revisionsfähigkeit der Software. Gleichzeitig können mit der Offenlegung des Quellcodes vermeintliche Schwächen eines Programmes aufgedeckt werden und durch das Recht auf Veränderung sofort behoben werden.




ABHÄNGIGKEIT VON EINZELNEM HERSTELLER VERHINDERT: Dieser Eigenschaft von Open-Source-Software wird zukünftig die größte Bedeutung beigemessen.

Abbildung 7.29: Bedeutung steganographischer Verfahren zur Sicherstellung vertraulicher Kommunikation

## Ergebnisse

Im folgenden Abschnitt sollen verschiedene Aspekte der Verwendung und Verbreitung von Open-Source-Software betrachtet werden (siehe Abbildung 7.31). Die größte Bedeutung für den Einsatz von Open-Source-Software wird derzeit der Open-Source-Eigenschaft beigemessen, die eine Abhängigkeit von einzelnem Hersteller verhindert. Die Experten erwarten, dass diese auch in zehn Jahren noch die bedeutsamste Eigenschaft bleiben wird. Hingegen rechnen die Befragten der Open-Source-Eigenschaft, bei der der Nutzer sich selbst an der Entwicklung und Qualitätssicherung beteiligen kann, mit Abstand die geringste Bedeutung zu. Alle anderen Eigenschaften werden in ihrer Bedeutung sehr dicht beieinander und über die nächsten zehn Jahre steigend bewertet. Lediglich die Eigenschaft, die „Hintertüren" im System aufdecken helfen soll, wird nach Ansicht der Befragten in ihrer Bedeutung in zehn Jahren leicht hinter die übrigen Eigenschaften abfallen.

Das Open-Source-Konzept ermöglicht einen Quellcode-Review durch beliebige unabhängige Experten. Diese Eigenschaft spielt vor allem im Betriebssystembereich sowie bei der Bewertung der zugrunde liegenden Algorithmen eine Rolle. Neben sicherheitskritischen Bereichen könnte nach Ansicht der Experten vor allem die öffentliche Verwaltung hiervon profitieren. Skepsis wird geäußert im Zusammenhang mit der Problematik, dass diese Open-Source-Eigenschaft gerne als Argument verwendet, allerdings nur selten genutzt wird.

Ähnlich wird die Eigenschaft bewertet, die verhindert, dass „Hintertüren" im System eingebaut werden. Hier erzielt der Nutzer nur dann einen konkreten Vorteil, wenn jemand das System wirklich überprüft und die Ergebnisse veröffentlicht (und nicht etwa selbst nutzt). Dies erscheint schwer nachprüfbar und die Befragten sind überwiegend skeptisch, ob dies überhaupt so eintreten wird. Mit zunehmender Komplexität der Softwaresysteme nimmt darüber hinaus die Wahrscheinlichkeit ab, Hintertüren zufällig zu entdecken [CERT 01, CERT 02a]. Einige Experten gehen weiter und warnen vor einem vermeintlichen Sicherheitsgefühl, das das Open-Source-Konzept hervorrufen könnte.

Open-Source-Software hat den Vorteil, dass alle Algorithmen und die zugehörigen Implementierungen offengelegt sein müssen. Damit ist augeschlossen, dass das System auf dem Prinzip der „Sicherheit durch Geheimhaltung" basiert. Diese Eigenschaft ist für viele Nutzer ent-

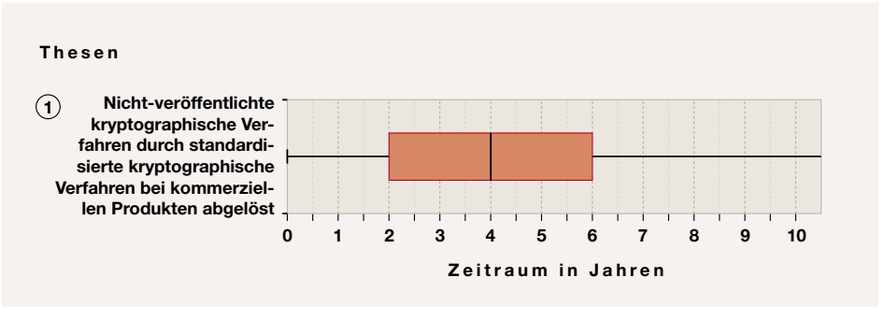



Abbildung 7.30: Ergebnis der These zu Offenlegung kryptographischer Verfahren

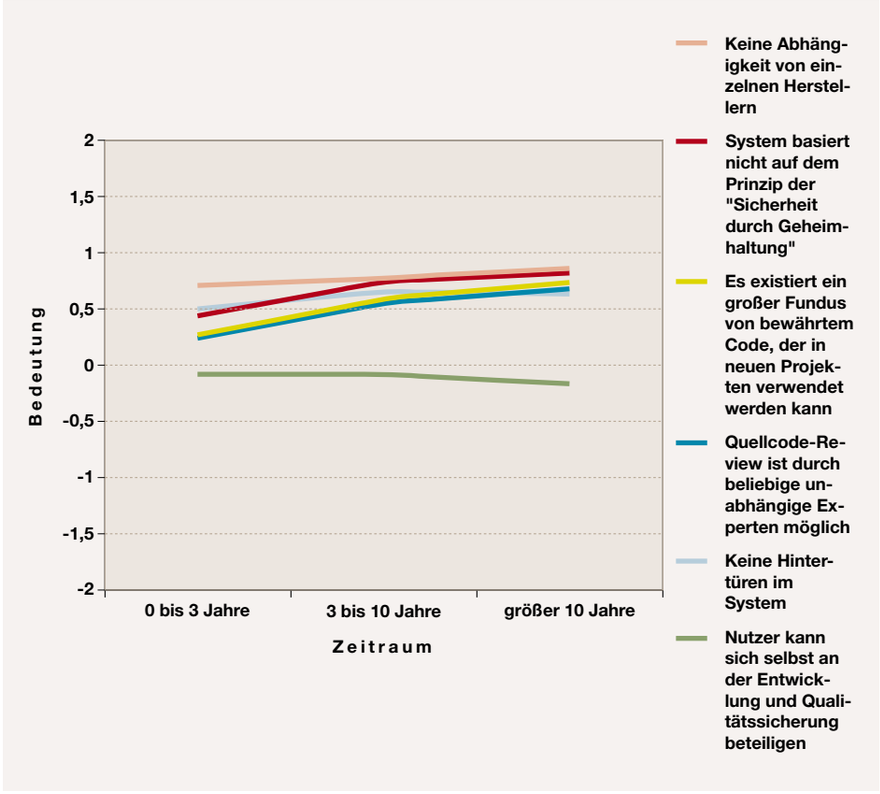



Abbildung 7.31: Bedeutung verschiedener Open-Source-Eigenschaften

scheidend. Allerdings rechnen einige Experten mit einem Rückgang des Open-Source-spezifischen Vorteils, da erwartet wird, dass zukünftig auch bei nicht-Open-Source-Software die Algorithmen offengelegt werden.

Das Open-Source-Konzept verringert die Abhängigkeit von einzelnen Herstellern. Obwohl dieser Eigenschaft eine große Bedeutung beigemessen wird, verweisen die Befragten auf die großen Monopolstrukturen des derzeitigen Softwaremarktes. Viele sehen Gefahren durch die Entstehung neuer Anhängigkeiten, beispielsweise von einem Linux-Kernel.

Die geringste Bedeutung wird der Möglichkeit beigemessen, dass sich der Nutzer selbst an der Entwicklung und Qualitätssicherung beteiligen kann. Als realistisch wird dies nur für Fachexperten aus dem Forschungs- und Entwicklungsumfeld (F&E) und nur bei kleinen Projekten angesehen. Oft ist die Umsetzung zu kostenaufwendig und zu komplex. Die meisten Experten schließen die Nutzung dieser Eigenschaft für die Mehrheit der Anwender aus.

Bei dem Open-Source-Konzept existiert ein großer Fundus von bewährtem Code, der in neuen Projekten verwendet werden kann. Neben dem Problempotenzial im lizenzrechtlichen Bereich werden vor allem Gefahren durch die Verbreitung von fehlerhafter Software gesehen.

### Zusammenfassung

Bei der Bewertung der Eigenschaften von Open-Source Software wird der Verringerung der Abhängigkeit von einzelnen Herstellern durch dieses Konzept die größte Bedeutung beigemessen, während die Möglichkeit für die Nutzer selbst am Entwicklungsprozess teilzunehmen die mit Abstand geringste Bedeutung hat. Alle anderen Eigenschaften bewegen sich mit leicht steigender Tenedenz dicht beieinander.

## 7.3.9 Zentrale Authentisierungsverfahren im Internet

ZENTRALE AUTHENTISIERUNGSVERFAHREN IM INTERNET: Derartige Verfahren spielen heute kaum eine Rolle, werden allerdings innerhalb der nächsten 10 Jahre erheblich an Bedeutung hinzugewinnen.

Bei zahlreichen Diensten, die heute über das Internet bereitgestellt werden, sind Identifizierungs- bzw. Authentisierungsinformationen anzugeben. Aufgrund der Vielzahl der Diensteanbieter sind die Kriterien, denen diese Informationen genügen müssen, sehr unterschiedlich. Daraus ergibt sich eine Vielzahl von Benutzernamen und Passwörtern. Seit etwa zwei Jahren werden zentrale Authentisierungsdienstleistungen angeboten, welche ein Single-Sign-On realisieren und dem Internetnutzer das mehrfache Anmelden für unterschiedliche Dienste abnehmen sollen.

### Ergebnisse

Obwohl derzeit zentrale Authentisierungsverfahren im Internet noch von untergeordneter Bedeutung sind, erwarten die Befragten, dass deren Bedeutung für die Internetnutzung innerhalb der nächsten zehn Jahre deutlich zunehmen wird. Die Zunahme wird teilweise auch im Zusammenhang mit der Etablierung von PKIs und der Durchsetzung von Signaturanwendungen gesehen. Gleichzeitig wird die Etablierung sogenannter Single-Sign-On Verfahren entscheidend für die Nutzung einer Vielzahl von Diensten im Netz sein. Es werden Anwendungsmöglichkeiten vor allem im E-Commerce und E-Banking-Bereich gesehen. Weitere Anwendungsfelder sind beispielsweise Jugend- und Kinderschutz, geschlossene Nutzergruppen sowie B2B-Anwendungen (z.B. Händlerzugang). Einige Experten sehen generelle Gefahren zentraler Authentisierungverfahren als „Single Point of Failure" sowie durch ungelöste Sicherheitsprobleme und aufgrund der möglichen Profilerfassung und -verwertung. Generell erfordern solche Konzepte ein weitreichendes Vertrauen der Anwender in Anbieter und Betreiber.

Bei der Bewertung konkreter Authentisierungsverfahren gehen die Befragten davon aus, dass die derzeitigen Produkte auch weiterhin nur wenig Bedeutung haben werden (siehe Abbildung 7.32). Das zentrale Authentisierungsverfahren

MS Passport bzw. .NET Passport wird dabei über die nächsten zehn Jahren nur unwesentlich an Bedeutung hinzugewinnen. Die Experten gehen davon aus, dass sich aus Privacy-Bedenken und ungeklärten rechtlichen Problemen, sowie aufgrund des mangelnden Vertrauens in den Hersteller/Anbieter Microsoft, der Dienst nicht durchsetzen wird. Andererseits ermöglicht die hohe Integrationstiefe in Standardprodukte eine hohe Marktpenetration; die zukünftige Bedeutung hängt damit von der weiteren Entwicklung von Marktmacht und -struktur ab. Als Einsatzbereiche sehen die Befragten neben dem allgemeinen E-Commerce mit dem Endkundenmarkt (B2C) bezahlte Mediendienste sowie den Jugend- und Kinderschutz.

Das im Rahmen des Sun Liberty Alliance Project zu realisierende zentrale Authentisierungsverfahren wird nach Ansicht der Experten in den nächsten drei Jahren etwas an Bedeutung hinzugewinnen und Microsofts MS Passport leicht einholen. Langfristig wird allerdings auch diesem Verfahren keine große Bedeutung beigemessen. Im Gegensatz zum Microsoft-Dienst sieht man als Anwendungsbereichen neben bezahlten Medienangeboten und Kinderschutz, insbesondere das universitären Umfeld und den F&E-Bereich. Auch sehen die Befragten das Vertrauensproblem günstiger als bei Mircosoft und damit auch ein größeres Potenzial für einheitliche, anerkannte Standards sowie deren Akzeptanz. Allerdings ist das grundsätzliche Problem, beispielsweise der möglichen Profilerfassung und -verwertung, dadurch nicht aus der Welt. Problematisch werden der geringe Bekanntheitsgrad des Dienstes sowie die Lizenzpolitik von Sun als Hemmnis für die Verbreitung gesehen. Einige der Befragten sind der Meinung, dass herstellerspezifische Lösungen durch herstellerunabhängige Verfahren ersetzt werden.

Die Experten gehen davon aus, dass zentrale Authentisierungsverfahren andere Authentisierungsverfahren nie ablösen werden (siehe Abbildung 7.33). Es wird nach Ansicht der Befragten immer Dienste geben, die keine zentrale Authentifizierung benötigen, in vielen Bereichen sind Punkt-zu-Punkt Verfahren sinnvoller. Skeptisch wird auch das zentralistische Konzept in der dezentralen Internet-Umgebung gesehen. Weiterhin wird die Vertrauensproblematik und das damit verbundene Misstrauen gegenüber zentraler Kontrolle, sowie datenschutzrechliche und sicherheitstechnische Bedenken, angebracht. Dabei wird erwartet, dass die Sicherheitsbedenken den (Bequemlichkeits-)Nutzen übersteigen werden. Darüber hinaus benötigen Unternehmensrichtlinien eigene, unabhängige, lokale und dezentral administrierte Verfahren, die durch zentrale Verfahren nicht umsetzbar sind.

ANDERE AUTHENTISIERUNGSVERFAHREN: Es wird nicht erwartet, dass zentrale Authentisierungsverfahren alle anderen Authentisierungsarten ablösen werden.

Da zentrale Authentisierungsverfahren für viele Anwendungen, wie z.B. im B2C und C2C E-Commerce-Bereich, als wünschenswert betrachtet werden, beispielsweise um eine bessere Bedienbarkeit für Anwender durch Ersetzen unübersichtlich gewordener Passwörter und PINs zu erreichen, wird eine Koexistenz verschiedener Authentisierungsverfahren erwartet. Positive Effekte auf die zukünftige Entwicklung von Single-Sign-On Diensten werden von Zertifizierungen der Verfahren durch anerkannte staatliche Stellen erwartet.

## Zusammenfassung

Obwohl die Experten noch ungelöste Sicherheitsprobleme sehen, werden sich Single-Sign-On Dienste für viele Anwendungen, insbesondere im Consumer-Bereich mittelfristig durchsetzen, da es für Nutzer und Anbieter ein großes Vereinfachungspotenzial bietet. Im Unternehmensbereich hingegen sind solche Systeme auch aufgrund der Vertrauensproblematik und der Umsetzung eigener Richtlinien schwieriger. Zusammenfassend läßt sich festhalten:

- Zentrale Authentisierungsverfahren im Internet spielen derzeit kaum eine Rolle, werden allerdings in den nächsten zehn Jahre erheblich an Bedeutung hinzugewinnen. Die heute verfügbaren Produkte von Microsoft und Sun Microsystems bleiben allerdings weiterhin nur von gerninger Bedeutung.

- Es ist nicht damit zu rechnen, dass zentrale Authentisierungsverfahren alle anderen Authentisierungsverfahren ablösen werden.

AKZEPTANZ BIOMETRISCHER VERFAHREN: Die Akzeptanz dieser Verfahren im Alltag wird nicht vor 7 Jahren erwartet. Vor allem bei der technischen Zuverlässigkeit herrscht Skepsis.


Abbildung 7.32: Bedeutung verschiedener zentraler Authentisierungsverfahren

## 7.3.10 Biometrie

Unter Biometrie versteht man in der Informationstechnologie die Erfassung und den Vergleich individueller Eigenschaften einer bestimmten Person (z.B. Fingerabdruck, Iris, Stimme, Gesichtsmerkmale, Gestik) durch technische Systeme, um die Person zu identifizieren und ihr den Zugang zu geschützten Bereichen oder Ressourcen zu gewähren. Die Kombinationen mehrerer biometrischer Eigenschaften, sogenannter Muster, gelten dabei als wesentlich schwerer zu fälschen als herkömmliche Sicherheitsmerkmale, wie beispielsweise die Personal Identification Number (PIN). Vor dem Hintergrund der zunehmenden öffentlichen Diskussion über den breiten Einsatz biometrischer Verfahren sollen in diesem Abschnitt einige biometrische Verfahren und deren Einsatz betrachtet werden.

### Ergebnisse

Bei der Frage nach der Akzeptanz biometrischer Verfahren im Alltag erwartet die Mehrheit der Befragten, dass die Akzeptanz in sieben Jahren weit verbreitet sein wird, während ein Viertel nicht vor zehn Jahren damit rechnet (Abbildung 7.34). Bedenken werden aufgrund von Privacy-Bedenken, mangelnder Zuverlässigkeit der Technologie und einer hinreichend kritischen Öffentlichkeit geäußert. Neue Anwendungspotenziale werden für die substanzielle Verbesserung der Zugangs- und Zugriffssicherheit und in der Identifizierung gesehen. So wären komfortorientierte Identifikationsanwendungen möglich, die eine Identifikation „im Vorbeigehen" durchführen und damit eine Ablösung von Passwörtern und herkömmlichen Ausweissystemen ermöglichen. Auch die Schaffung sicherer persönlicher Mobilgeräte rückt dann in den Bereich des Möglichen. Zuvor müssten, so die überwiegende Ansicht, die Datenschutzproblematik gelöst und technisch ausgereifte biometrische Systeme entwickelt werden. Die Befragten erwarten, dass die politische Diskussion weiterhin strittig bleiben wird.

Bei der Bewertung biometrischer Verfahren zur Identifizierung von Personen erwarten die Experten bei allen betrachteten Verfahren eine Zunahme ihrer Bedeutung mit unterschiedlichem Ausmaß über die nächsten zehn Jahre (siehe Abbildung 7.35). So wird der Iriserkennung auch in zehn Jahren nach wie vor die geringste Bedeutung zugerechnet. Die Gründe hierfür werden in der geringen psychologischen Akzeptanz und der Angst vor medizinischen Schäden gesehen. Die Augen wer-

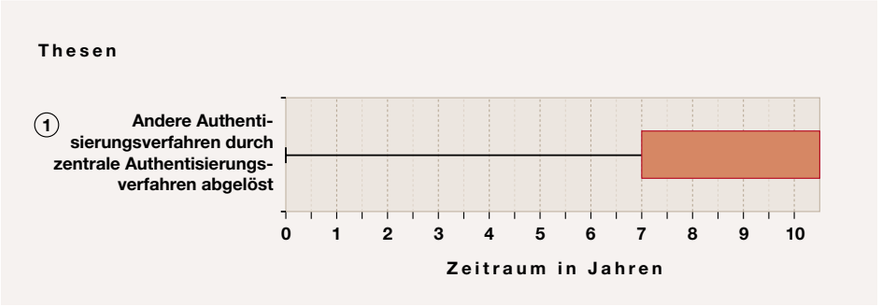



Abbildung 7.33: Ergebnis der These zu Authentisierungsverfahren

den in hohem Maße als verletzlicher Privatbereich angesehen. Die Iriserkennung wird sehr stark mit physikalischer Zugangskontrolle im Hochsicherheitsbereich (kritische Infrastrukturen wir Kernkraftwerke, militärischer Bereich) assoziiert. In diesen Bereichen ist die Akzeptanz aufgrund des positiven Images höher. Bei Überwindung des Akzeptanzproblems wäre aufgrunder des geringen Täuschungsrisikos auch eine Anwendung für Geldautomaten für höhere Beträge denkbar.

Eine erhebliche Zunahme in seiner Bedeutung wird nach Ansicht der Befragten die Identifizierung von Personen anhand der Sprechererkennung gewinnen. Zukünftig werden Anwendungsmöglichkeiten in der Zutritts- und Zugangssicherung, bei Telefontransaktionen, bei Personenüberwachungen, im Automobil, bei Gerätesteuerung (z.B. im Heimbereich), sowie bei mobilen Systeme wie dem Handy gesehen. Auch ein „elektronischen Pförtner" wäre damit realisierbar. Obwohl die Technologie der Sprechererkennung derzeit noch nicht ausgereift ist, verfügt das Verfahren über zahlreiche funktionale Aspekte und entspricht am ehesten dem „natürlichen" menschlichen Identifizierungsverhalten. Die hohen Anforderungen an die Umgebung und den Benutzer, zu hohe Fehlerraten, mangelnde Stabilität und Probleme mit „aufgenommener Stimme" machen dessen Einsatz derzeit schwierig.

Die größte Bedeutung erwarten die Befragten langfristig für Identifikationsverfahren auf Basis der Gesichtserkennung. Diesem Verfahren wird eine bessere Akzeptanz als bei anderen zugesprochen, da es ähnlich wie die Sprechererkennung dem natürlichen menschlichen Identifizierungsverhalten entspricht und eine Identifikation „im Vorbeigehen" ermöglicht. Anwendungsbereiche werden vornehmlich bei der Verbrechensprävention und -bekämpfung, z.B. für Fahndungs- und Überwachungssysteme oder bei Grenzkontrollen, gesehen. Auch ein Einsatz zur Zutrittssicherung in weniger sensiblen Bereichen, allerdings kombiniert mit weiteren Verfahren, ist denkbar.

Obwohl in seiner Bedeutung als gering eingestuft, sehen die Befragten in der Handschriftenerkennung, die bereits in der Unterschrift als die „natürliche" Freischaltung für verbindliche Willenserklärungen gilt, bei Voraussetzung moderner Erkennungsmethoden, ein geringes Missbrauchspotenzial. Als mögliche Anwendungsbereiche werden neben der Autorisierung von Transaktionen (z.B. als Ersatz für die Signier-PIN) vor allem die Zugangs- und Zugriffssicherung gesehen, wie z.B. der Login bei PDAs. Viele der Befragten sehen die gleichen Anwendungsfälle wie bei der digitalen Signatur.

Die Fingerabdruckerkennung, der derzeit und für die nächsten drei Jahre die größte Bedeutung beigemessen wird, wird längerfristig diesen Stellenwert nicht halten können. Obwohl das Verfahren preiswert, einfach nutzbar, sowie hygienisch akzeptabel ist, und der Fingerabdruck im Bewusstsein der Menschen ein Substitut für Eindeutigkeit ist, wird es jedoch zunehmend, historisch bedingt, als kriminalisierend empfunden. Darüber hinaus sind die Verfahren zu unzuverlässig und leicht zu täuschen [TKZ 02]. Anwendungsbereiche sehen die Befragten insbesondere bei Personalisierungsanwendungen sowie als Passwortersatz für die persönliche Infor-

SPRECHERERKENNUNG: Diese Verfahren, die dem natürlichen menschlichen Identifizierungsverhalten entsprechen, werden zukünftig weiter an Bedeutung zunehmen.

GESICHTSERKENNUNG: Mittelfristig wird die Gesichtserkennung den Fingerabdruck als wichtigstes biometrisches Identifikationsverfahren ablösen.

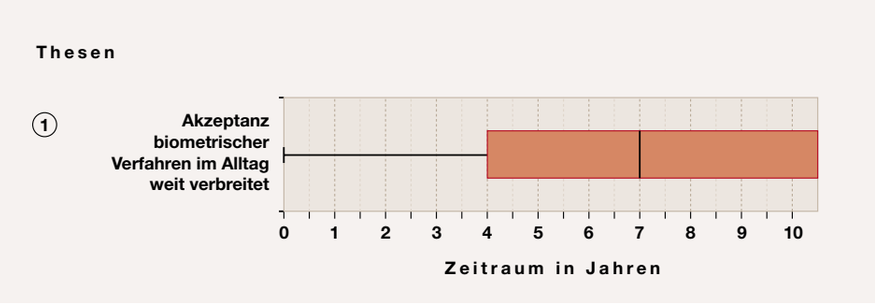



Abbildung 7.34: Ergebnis der These zu Akzeptanz biometrischer Verfahren im Alltag

mationstechnik (PDA, Handy, Laptop), z.B. zur Freischaltung von Karten und Geräten. Auch die Verwendung zur Zutrittskontrolle in Bereichen mit geringen Sicherheitsanforderungen bzw. als Login am Arbeitsplatz wäre denkbar.

Als weitere biometrische Technologien zur Personenidentifikation wurden beispielsweise Verfahren auf Basis der Erkennung von Gehirnwellenmustern oder der DNA-Analyse genannt, bleiben aber weitgehend Einzelmeinungen. Die Experten erwarten, dass bei den Unsicherheiten der jetzigen Technologien nur Verfahren akzeptabel sein werden, die verschiedene biometrische Merkmale kombinieren.

Die Befragten erwarten, dass das Erfassen und Vergleichen biometrischer Merkmale zur Authentisierung mittels Chipkarten (Smartcards) frühestens in sieben Jahren weit verbreitet sein wird, viele gehen sogar davon aus, dass dies nicht innerhalb der nächsten zehn Jahre eintreten wird (siehe Abbildung 7.36, ①). Diese Einschätzung wird vor allem damit begründet, dass die Technik hierfür noch nicht ausgereift ist. Zum einen sind die Fehlerraten solcher Systeme noch zu hoch, zum anderen sind solche Verfahren nur sinnvoll, wenn sowohl der Sensor, als auch der Vergleich mit dem Refenzmuster auf der Karte durchgeführt wird, was derzeit von den Chipkarten nicht geleistet werden kann. Für eine weite Verbreitung werden solche Systeme als zu teuer angenommen. Anwendungspotenziale werden als PIN-Ersatz bei Chipkarten sowie bei elektronischen Ausweisen gesehen.

Das Erfassen und Vergleichen biometrischer Merkmale zur Authentisierung mittels mobiler persönlicher Endsysteme wird nach Ansicht der meisten Experten in sechs Jahren weit verbreitet sein (siehe Abbildung 7.36, ②). Mögliche Anwendungsbereiche sind beispielsweise die Benutzererkennung zum Schutz vor unbefugter Benutzung oder (auch öffentliche) Single-Sign-On-Systeme. Ebenfalls denkbar ist die Kombination mit elektronischen Bezahlsystemen zur Autorisierung von Zahlungen mittels mobiler Endgeräte. Es werden allerdings auch mögliche Gefahren bei Verwendung von PDAs oder Mobiltelefonen gesehen, da diese Gegenstände des täglichen/öffentlichen Gebrauchs sind. Die Verbreitung wird nach Einschätzung der Befragten von der technischen Zuverlässigkeit und dem Preis abhängen. Etwa ein Viertel der Befragten rechnet nicht vor zehn Jahren mit einer weiten Verbreitung.

Bei der Bewertung von biometrischen Verfahren als Hilfsmittel für die sichere Identifizierung gegenüber Dritten, bspw. durch einen Personalausweis mit biometrischen Merkmalen, ergibt sich eine unterschiedliche Einschätzung. Einerseits wird erwartet, dass in sieben Jahren solche Verfahren weit verbreitet sein werden, beispielsweise als Bürgerkarte, in einer elektronischen Erweiterung von Personalausweis oder Reisepass, bzw. als Hilfsmittel zur Kriminalitätsbekämpfung. Andererseits erwartet mehr als ein Viertel der Befragten deren Verbreitung erst in deutlich über zehn Jahren (siehe Abbildung 7.36, ③). Neben Datenschutzbedenken bestehen erhebliche Zweifel an der Zuverlässigkeit der Technik, die sich in naher Zukunft nicht ändern wird. Die Befragten weisen auch auf die starke Abhängigkeit

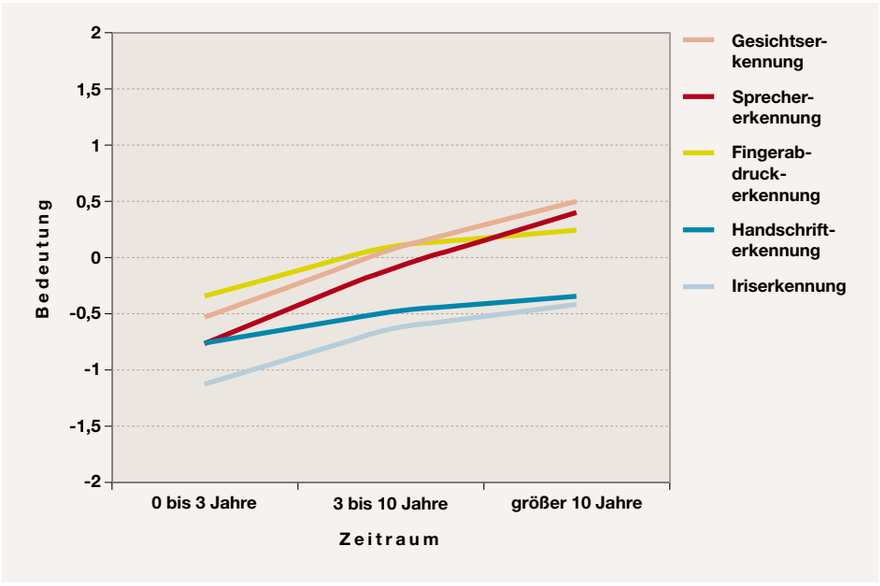



Abbildung 7.35: Bedeutung verschiedener biometrischer Verfahren zur Identifikation von Personen

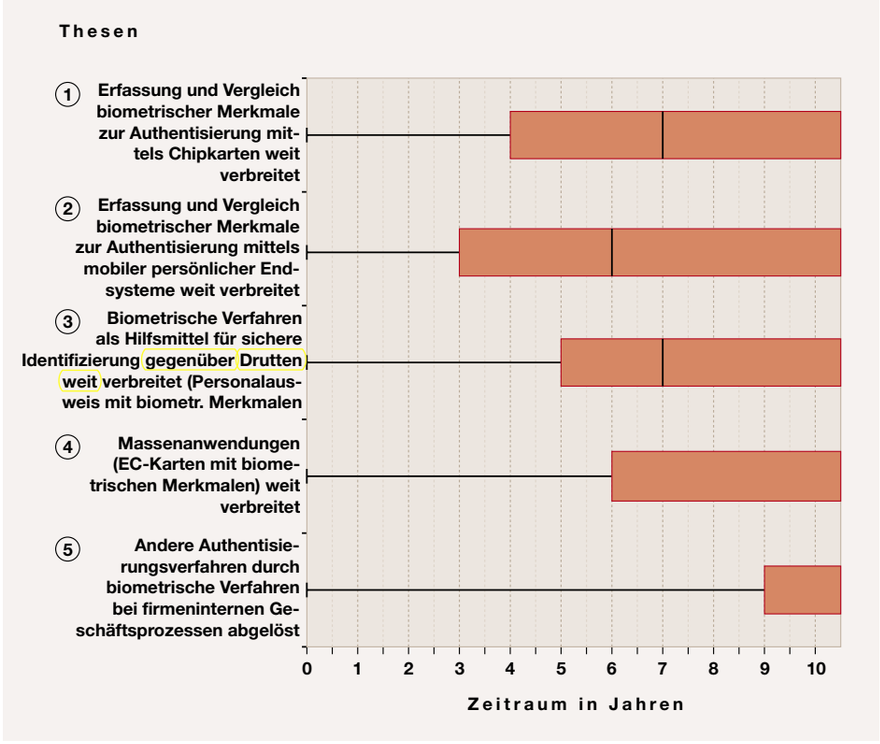



Abbildung 7.36: Ergebnisse der Thesen zu Identifizierung und Authentisierung mit Hilfe biometrischer Verfahren

von politischen Vorgaben und auf das Ergebnis der gesellschaftspolitischer Diskussion hin.

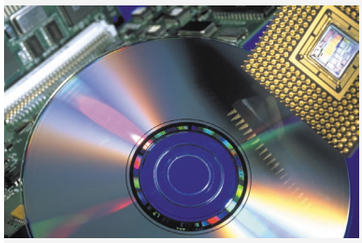
Massenanwendungen, wie bspw. EC-Karten mit biometrischen Merkmalen, werden nach Einschätzung der Befragten nicht vor zehn Jahren weit verbreitet sein (siehe Abbildung 7.36, ④). Zum einen sind die Kosten für einen breiten Einsatz noch zu hoch bei unklarem Vorteil für die Nutzer, beispielsweise gegenüber Alternativen wie PIN. Zum anderen ist die Sicherheit und die Fehlerrate im Masseneinsatz noch unzureichend. Insbesondere ist die Rechtsverbindlichkeit der biometrischen Identifikation aufgrund dieser Unsicherheiten noch nicht absehbar. Problematisch sehen die Experten auch eine zu erwartende, aber inakzeptable Umkehrung der Beweislast zu Lasten der Verbraucher, beispielsweise bei Bankkarten. Bei einem technologischen Durchbruch sehen die Befragten Anwendungsmöglichkeiten als Patientenkarten, als PIN-Ersatz bei EC-Karten oder als zusätzliche Signaturfunktion auf solchen Karten.

Die Experten sind sich einig, dass biometrische Verfahren bei firmeninternen Geschäftsprozessen nie andere Authentisierungsverfahren vollständig ablösen werden (siehe Abbildung 7.36, ⑤). Die Haupthindernisse werden dabei in der mangelnden technischen Reife und den hohen Kosten solcher Systeme gesehen. Viele sehen den Einsatz nur als sinnvolle Ergänzung bzw. nur in Teilbereichen als Ersatz herkömmlicher Authentisierungsverfahren.

## Zusammenfassung

Die Bewertung biometrischer Verfahren ist im Wesentlichen von zwei Polen bestimmt: Zum einen von der Nachfrage und Wünschbarkeit solcher Systeme und zum anderen von der Skepsis bzgl. der Machbarkeit verlässlicher Verfahren. Auch datenschutzrechtliche Aspekte und die Angst vor Missbrauch beeinflussen die Beurteilung der Biometrie. Zusammenfassend erhält man folgende Bewertung:

- Die Akzeptanz biometrischer Verfahren wird von den Befragten unterschiedlich bewertet. Während die Mehrheit eine weite Verbreitung bis 2010 sieht, erwartet ein Viertel der Befragten dies nicht vor 2013.
- Bei der Beurteilung biometrischer Verfahren zur Identifizierung von Personen kann man Folgendes festhalten: Das derzeit wichtigste Verfahren, die Fingerabdruckerkennung, wird mittelfristig seine Bedeutung verlieren und durch die Gesichtserkennung als wichtigstes Verfahren abgelöst werden. Eine erhebliche Zunahme wird der Sprechererkennung zugewiesen, während der Iriserkennung auch weiterhin, außer in Randbereichen, kaum Chancen eingeräumt werden.
- Der Einsatz biometrischer Verfahren zur Authentisierung mittels Chipkarte oder persönlichem Endgerät wird mehrheitlich vor 2010 erwartet. Erstaunlicherweise sind die Befragten bei Chipkarten deutlich skeptischer als bei den persönlichen Endgeräten.
- Biometrische Merkmale werden nach Ansicht der Befragten erst 2010 als Hilfsmittel für die sichere Identifizierung gegenüber Dritten weit verbreitet sein. Für Massenanwendungen, beispielsweise auf EC-Karten, wird dies hingegen nicht vor 2013 erwartet.
- Bei firmeninternen Prozessen werden biometrische Verfahren andere Authentisierungsverfahren nie vollständig ablösen.



# 8 Technologiebereiche

Das folgende Kapitel beschreibt die Ergebnisse der Studie in den Technologiebereichen Rechnertechnik, Netze und Kommunikation, Datenbanken und Wissensmanagement sowie Softwaretechnik. Entsprechend der Vorgehensweise (Kapitel 5) ergeben sich diese aus dem aktuellen Stand der Forschung, aus Einzelgesprächen mit Experten und aus einer umfangreichen Fragebogenaktion mit Kennern der jeweiligen Fachgebiete.

Im Abschnitt 8.1 wird die zukünftige Entwicklung im Bereich der Rechnertechnik dargestellt. Hier wird vor allem eine Leistungssteigerung der Hardware bei gleichzeitiger Miniaturisierung und fallenden Preisen erwartet. Dies beruht auf einer steigenden Effizienz der Herstellungsprozesse, aber auch auf völlig neuen Ansätzen wie z.B. der Ausnutzung quantenmechanischer Effekte oder der Verwendung alternativer Materialien. Parallel dazu lassen sich eine Vereinfachung in der Handhabung von Rechnersystemen, durch neue Interaktionsformen wie Spracheingabe oder Handschriftenerkennung, und eine zunehmende Einbettung neuer Funktionsgruppen in Prozessoren feststellen. Insbesondere im Hochleistungsbereich werden sich neue Konzepte (Grid Computing), auch außerhalb des rein wissenschaftlichen Bereiches, durchsetzen.

Die fortschreitende Vernetzung von Rechnersystemen wird im Abschnitt 8.2 beschrieben. Neben der steigenden Leistungsfähigkeit, z.B. durch Ausbau der Glasfaserverkabelung und Einsatz neuer Multiplexverfahren, ist in vielen Bereichen eine Konvergenz unterschiedlicher Technologien zu erwarten. Der Wunsch der Benutzer nach sicherer Übertragung und nach Mobilität wirft zusätzliche Fragen auf, die in der Studie näher betrachtet werden. Die zunehmende Dienstorientierung und die damit einhergehende Ausrichtung angebotener Leistungen auf den Kunden macht den Einsatz flexiblerer Konzepte, wie aktiver und programmierbarer Netze, erforderlich.

Die Beherrschung des – nicht zuletzt auch durch die zunehmende Vernetzung – stetig wachsenden Informationsangebots ist Gegenstand des Bereichs Datenbanken und Wissensmanagement, der in Abschnitt 8.3 dargestellt wird. Auch hier lassen sich erhebliche Kapazitätssteigerungen erkennen, die im wesentlichen durch Leistungs- und Kapazitätssteigerungen der unterliegenden Hardware ermöglicht werden. Darüber hinaus sind aber auch die Vereinfachung der Bedienschnittstellen sowie die Weiterentwicklung der Datenmodelle und der verfügbaren Funktionalität wesentliche Faktoren, die im Rahmen der Studie untersucht werden.

Abschließend beschreibt Abschnitt 8.4 die aktuellen Entwicklungen, die im Bereich der Softwaretechnik zu beobachten sind. Die oben beschriebene Leistungszunahme der unterliegenden Komponenten ermöglicht immer komplexere und leistungsfähigere Anwendungen. Um diese realisieren zu können, sind entsprechende Methoden und Verfahren aus dem Software Engineering erforderlich. So sind z.B. einheitliche und einfach erlernbare Methoden und Werkzeuge zur Beschreibung von Softwaresystemen und einheitliche Modelle zum Austausch der Informationen zwischen den Werkzeugen wesentliche Voraussetzungen für die Entwicklung derart komplexer Anwendungen. Auch eine weitgehende Automatisierung des Entwicklungsprozesses oder eine Wiederverwendung von Komponenten der verschiedenen Phasen des Entwicklungszyklus spielen hierbei eine wesentliche Rolle.

In jedem der vier Abschnitte werden spezifische Trends des Bereiches diskutiert (z.B. Einsatz neuer Technologien bei der Prozessorherstellung im Bereich Rechnertechnik). Für jeden dieser Trends werden neben dem aktuellen Stand der Forschung die Ergebnisse der Expertenbefragungen dargestellt und mit der Vorgängerstudie [SETIK 00] verglichen.

## 8.1 Rechnertechnik

Die Evolution der Mikroelektronik ermöglichte eine Veränderung der Gesellschaft durch die Informations- und Kommunikationstechnologie während der letzten Jahrzehnte. Der jetzigen, weitgehend auf Silizium basierenden, Technologie wurde zwar schon mehrmals das Ende vorausgesagt, aber Moore's Gesetz [Inte 02] gilt nach wie vor und eröffnet neue Möglichkeiten der Rechnertechnik. Es zeichnet sich ab, dass wir in Zukunft von kleinsten, spontan miteinander kommunizierenden Prozessoren umgeben sein werden, die aufgrund ihrer geringen Größe und ihrem niedrigen Preis selbst in (beliebige) Alltagsgegenstände integriert werden können [Matt 02, Matt 03]. Weiser's Vision einer ubiquitären Computer-Landschaft (ubiquitous computing), in der Computer immer weniger sichtbar werden [Weis 91], ist keine Science Fiction mehr, sondern wird zunehmend Realität. Ermöglicht wird dieses Szenario durch immer leistungsfähigere, kleinere und preiswertere Prozessoren und Speichersysteme [Inte 02]. Noch im Jahr 2000 waren etwa 50 Millionen Transistoren auf einem Intel Pentium 4-Chip zu finden. Heute ist der von Intel angekündigte Banias-Chip bereits mit 77 Millionen Transistoren bestückt [Mage 02]. Noch im Jahr 2000 wurden Transistoren mit einer Gatterlänge von 30 Nanometern (nm) im Labor entwickelt, heute arbeiten 15-nm-Labormuster bereits im Terahertz-Bereich und ermöglichen damit Prozessoren mit Taktraten von 100 GHz und mehr [Stil 01].

Angesichts derartiger Tendenzen wird in dieser Studie untersucht, welche Prognosen über kurz-, mittel- und langfristige Entwicklungen in der Rechnertechnik aufgestellt werden können. Dazu werden die folgenden Fragestellungen betrachtet:

- Welche Prozessorarchitekturen werden in den nächsten Jahren dominieren?
- Welche grundlegenden Materialien und Technologien werden dabei verwendet?
- Welche Speichertechnologien werden eingesetzt?
- Welchen Veränderungen wird die Mensch-Maschine-Schnittstelle unterworfen sein?
- Welche Architekturentwicklungen sind im Hochleistungsbereich zu erwarten?

Die Fortschritte in der Rechnertechnik induzieren Evolutionen und Revolutionen in vielen Bereichen der Informations- und Kommunikationstechnologie, werden aber umgekehrt auch von übergreifenden Trends (Kapitel 6) beeinflusst. Tabelle 8.1 zeigt diesen Einfluss und die Ausprägungen der übergreifenden Trends wie sie sich seit der Vorgängerstudie [SETIK 00] aus dem Jahr 2000 verändert haben.

**Automatisierung und Vereinfachung** (Abschnitt 6.1): Mit der allgegenwärtigen Verbreitung von Computern steigt das Bedürfnis nach einfachen und intelligenten Schnittstellen zur Bedienung. Diese Anforderung wirkt sich in vielerlei Hinsicht auf die Rechnertechnik aus: Zum einen führt sie zu neuen Technologien wie Spracheingabe oder Handschriftenerkennung sowie zu biometrischen und quantentechnischen Verfahren zur (automatischen) Authentifikation von Benutzern (Abschnitt 8.1.5). Zum anderen forciert sie die Entwicklung von Hochleistungssystemen, die als virtuelle Rechner aus einer Vielzahl autonomer Komponenten bei Bedarf zusammengestellt werden und neue Leistungspotenziale eröffnen (Grid-Computing). In Abschnitt 8.1.6 wird darauf näher eingegangen.

**Integration und Standardisierung** (Abschnitt 6.4): Der Trend zur Integration und Standardisierung ist in der Rechnertechnik sowohl auf der technischen Ebene als auch auf der Produktionsebene auszumachen. Auf der technischen Ebene vollzieht sich der Integrationsprozeß in vielen Bereichen. Bei der Entwicklung neuer Prozessoren sind die Hersteller bemüht, weitere Funktionsgruppen wie Kryptographie oder Cache-Hierarchien auf einem Chip zu integrieren (Abschnitt 8.1.2), bei der Entwicklung von Hochleistungsrechnern auf der Basis von Grids oder Clustern werden heterogene Rechnersysteme über standardisierte Schnittstellen und Protokolle zu virtuellen Rechnern kombiniert, die kooperativ an der Lösung von komplexen Problemen arbeiten (Abschnitte 8.1.6 und 8.1.4). Auf der Pro-

duktionsebene sind die Prozessorhersteller mit ständigen Verbesserungen und Leistungssteigerungen konfrontiert, die an die wirtschaftliche Substanz gehen können. Es ist deshalb nicht verwunderlich, dass über entsprechende Konsortien und Gremien auch Verfahren in der Rechnertechnik standardisiert werden. Beispiele für solche Standardisierungsbemühungen sind in der Halbleiter- und Nanotechnologie im Rahmen des International Sematec-Konsortiums zu finden und in der EUV-Lithografie (Extreme Ultra Violet) im Rahmen der EUV LLC-Gruppe. Nur so können, unter dem Druck der vom Markt geforderten Konvergenz, Innovationen wie selbstorganisierende Ad-Hoc-Sensornetze oder optische Netze entstehen, wie sie zum Beispiel in [Inte 02] angedacht werden (Abschnitt 8.1.3). Auch Kapitel 8.2 befasst sich mit Teilaspekten dieser Fragestellung.

**Kapazitäts- und Leistungssteigerung** (Abschnitt 6.5): Dieser Trend ist der eigentliche Motor der Rechnertechnik. Sowohl in der Prozessortechnik als auch bei den Rechnerarchitekturen werden erhebliche Anstrengungen unternommen, die Leistung von Rechensystemen ständig zu erhöhen. Dazu werden nicht nur Alternativen zu herkömmlichen Prozessoren untersucht, es werden auch neue Halbleitertechnologien als Ersatz für das seit Jahren verwendete Silizium diskutiert (Abschnitte 8.1.1 und 8.1.2). Mit innovativen Architekturkonzepten wird zudem versucht, die verfügbare (und beobachtbare) Leistung von Rechensystemen zu verbessern (Abschnitt 8.1.6). Insbesondere bei der Erhöhung der Speicherkapazitäten sind in letzter Zeit erhebliche Fortschritte erzielt worden (Abschnitt 8.1.4), die nicht zuletzt mit dem stark korrelierenden Trend zur Miniaturisierung (Kapitel 6.7) zusammenhängen.

**Konvergenz** (Abschnitt 6.6): Die Konvergenz von Informations- und Kommunikationstechnik beeinflußt die Entwicklungen in der Rechnertechnik zunehmend und zeigt sich deutlich in den Anstrengungen, die die Prozessorhersteller unternehmen, um auf Mobilität und drahtlose Kommunikation optimierte Prozessorarchitekturen zu entwickeln. Aktuelle Beispiele sind Intel's Banias-Plattform [Grif 02] oder AMD's Hammer-Chip [Webe 01] (Abschnitt 8.1.3).

**Miniaturisierung** (Abschnitt 6.7): Gerade im Bereich der Rechnertechnik bedeutet Miniaturisierung fast immer auch Kapazitäts- und Leistungssteigerung. Insofern korreliert dieser Trend sehr stark mit dem Trend zur Kapazitäts- und Leistungssteigerung (Kapitel 6.5). Bei der Fertigung von Prozessor- und Speicherchips wird versucht, immer kleinere Schaltelemente immer dichter zu packen, um damit einerseits den gestiegenen Erwartungen an Leistungsmerkmale von Prozessoren zu genügen und andererseits hohe Speicherkapazitäten pro Quadratzentimeter zu realisieren (Abschnitte 8.1.1, 8.1.2 und 8.1.4). Die Kehrseite der Medaille sind nicht unerhebliche Herausforderungen zum Beispiel bei den auf den Chips verwendeten Verbindungstechniken oder der Abwärmeregulierung.

**Mobilität** (Abschnitt 6.8): Eine direkte Folge der Miniaturisierung ist die Möglichkeit, leistungsfähige Geräte herzustellen, die klein genug sind, um mobil betrieben zu werden, aber auch leistungsstark genug, um den Anforderungen mobiler Anwender gerecht zu werden. Dies läßt sich am Beispiel der Mobiltelefone gut verdeutlichen: Aus einem großen, teuren, in der Funktionalität eingeschränkten Statussymbol hat sich innerhalb weniger Jahre ein handliches Alltagsgerät mit einer weit über die reine Sprachübertragung hinausgehenden Funktionalität entwickelt (Abschnitte 8.1.1, 8.1.2 und 8.1.4).

**Vernetzung und Flexibilisierung** (Abschnitt 6.9): Flexibilisierung bedeutet Abkehr von starren Strukturen und dynamische Anpaßbarkeit an aktuelle Erfordernisse. Insofern findet sich der allgemeine Trend zur Vernetzung und Flexibilisierung im Rahmen des Themenbereiches Rechnertechnik einserseits in den Entwicklungen von Parallel- und Hochleistungsrechnern (Abschnitt 8.1.6), und andererseits in der Bereitstellung adäquater Kernkomponenten schon auf der Prozessorebene (Abschnitte 8.1.1 und 8.1.2). Abzulesen ist dies beispielsweise an dem zunehmenden – auch kommerziellen – Einsatz von Cluster- und Gridstrukturen sowie an der Einbettung von WLAN-Technologien in Prozessoren.

**Verteilung und Dezentralisierung** (Abschnitt 6.10): Beim Cluster- bzw. Grid-Computing werden verteilte, autonome, aber nicht notwendigerweise homogene, Rechner zu virtuellen Rechnern hoher Leistungsklassen vernetzt (Abschnitt 8.1.6). Die damit einhergehende Dezen-

tralisierung von Rechnerleistung und Speicherkapazität kann zunehmend in modernern Rechnerarchitekturen beobachtet werden [CDK 01].

**Virtualisierung** (Abschnitt 6.11): Virtualisierung ist eine grundlegende Methodik in der Informations- und Kommunikationstechnik. Konzepte wie virtuelle Speicher, virtuelle Systemmodelle, Virtual Reality oder virtuelle Maschinen sind nur einige Beispiele. In der Rechnertechnik kommt Virtualisierung auf verschiedenen Ebenen zum Tragen: Auf der Speicherbausteinebene, wenn über virtuelle Speicherkanäle ein direkter Zugriff auf Speichersegmente ermöglicht wird, auf der Prozessorebene, wenn eine CPU (Central Processing Unit) als zwei oder mehr unabhängige virtuelle Prozessoren dargestellt wird (Abschnitte 8.1.1, 8.1.2, 8.1.3 und 8.1.4), auf der Systemebene, wenn heterogene Rechnersysteme im Rahmen des Grid-Computings zu virtuellen Höchstleistungsrechnern vernetzt werden (Abschnitt 8.1.6).

Andere übergreifende Trends wie Dienst- und Komponentenorientierung (Kapitel 6.2) bzw. Globalisierung und Wettbewerb (Kapitel 6.3) betreffen die im Rahmen dieser Studie betrachteten Rechnertechnik weniger und wurden von den Experten im Kontext anderer Kapitel (z.B. Kapitel 8.2 , 8.4 und 9) untersucht.

SCHALTELEMENTE: Die Herstellung optischer Gatter wird innerhalb der nächsten 4 Jahre erwartet. Biologische Gatter werden innerhalb der nächsten 5 Jahre nicht zur Verfügung stehen, die Herstellung von Quantengattern wird in den nächsten 5 Jahren möglich sein.

### 8.1.1 Einsatz neuer Technologien bei der Prozessorherstellung

Die Entwicklungen der Mikroelektronik waren der Motor für signifikante Veränderungen der Gesellschaft durch die Informations- und Kommunikationstechnologie während der letzten Jahrzehnte [Nefi 01]. Moore's Gesetzgilt nach wie vor und scheint auch langfristig zu keiner merklichen Reduktion der Entwicklungsdynamik in der Mikroelektronik zu führen [Inte 02]. Aluminium, seit über 30 Jahren für die Verdrahtung von Halbleiter-Bauelementen verwendet, erweist sich zunehmend für die neuen Generationen von Hochleistungsprozessoren als nicht mehr geeignet, da bei den kleinen Strukturen der Microchips auf Grund des hohen spezifischen Widerstandes von Aluminium ein erheblicher Teil der aufgenommenen Leistung in Wärme umgewandelt wird. In den Forschungslaboratorien der Prozessorhersteller wird deshalb bereits seit längerem nach Alternativen zur heutigen Prozessortechnologie gesucht. Die Entwicklungsansätze reichen von neuartigen Transistoren auf der Basis von Kohlenstoff-Nanotubes, programmierbaren DNA-Molekülen oder Quanten-Effekten [FLS 99, Rink 98], über den Ersatz von Aluminium durch Kupfer bei Transistorverbindungen zur Steigerung der Leitfähigkeit, bis hin zu völlig neuartigen Materialien auf Indium- oder Germanium-Basis. Fraglich ist jedoch, wann mit dem verbreiteten Einsatz derartiger Technologien gerechnet werden kann und welche Vorteile derartige Prozessoren gegenüber den klassischen Varianten versprechen. Deshalb wurde untersucht, welche Halbleitertechnologien zukünftig vorherrschen werden, wann Silizium seine dominante Rolle verlieren wird, welche Ersatzmaterialien verwendet werden, wann Aluminium durch das bedeutend leitfähigere Kupfer als Verbindungstechnologie abgelöst wird und welche Rolle photonische Transistor-Verbindungen in Zukunft spielen werden.

#### Ergebnisse

Optische, biologische und auf Quanteneffekten basierende Prozessoren werden als mögliche Alternativen zu herkömmlichen Transistor-Prozessoren betrachtet. Erst die industrielle Verfügbarkeit entsprechender Gatter erlaubt allerdings eine Verbreitung derartiger Prozessoren. Es stellt sich deshalb die Frage, wann entsprechende Schaltelemente zur Verfügung stehen werden.

Da die Entwicklungszeit für industriell gefertigte Prozessoren bis zur Serienreife mehrere Jahre beträgt, ist eine wichtige Frage, wann mit neuartigen Prozessoren auf Basis dieser Gatter zu rechnen sein wird. Abbildung 8.1 faßt die Ergebnisse der Expertenbefragung zu diesem Themenkomplex zusammen.

Mit der Herstellung optischer Gatter rechnen die Experten in den nächsten vier Jahren (siehe Abbildung 8.1, ①). Wie schon in der Vorgängerstudie [SETIK 00] sind die Experten der Industrie mit einem prognostizierten Zeithorizont von zwei bis drei Jahren optimistischer als ihre Kollegen aus der Wissenschaft, von denen die

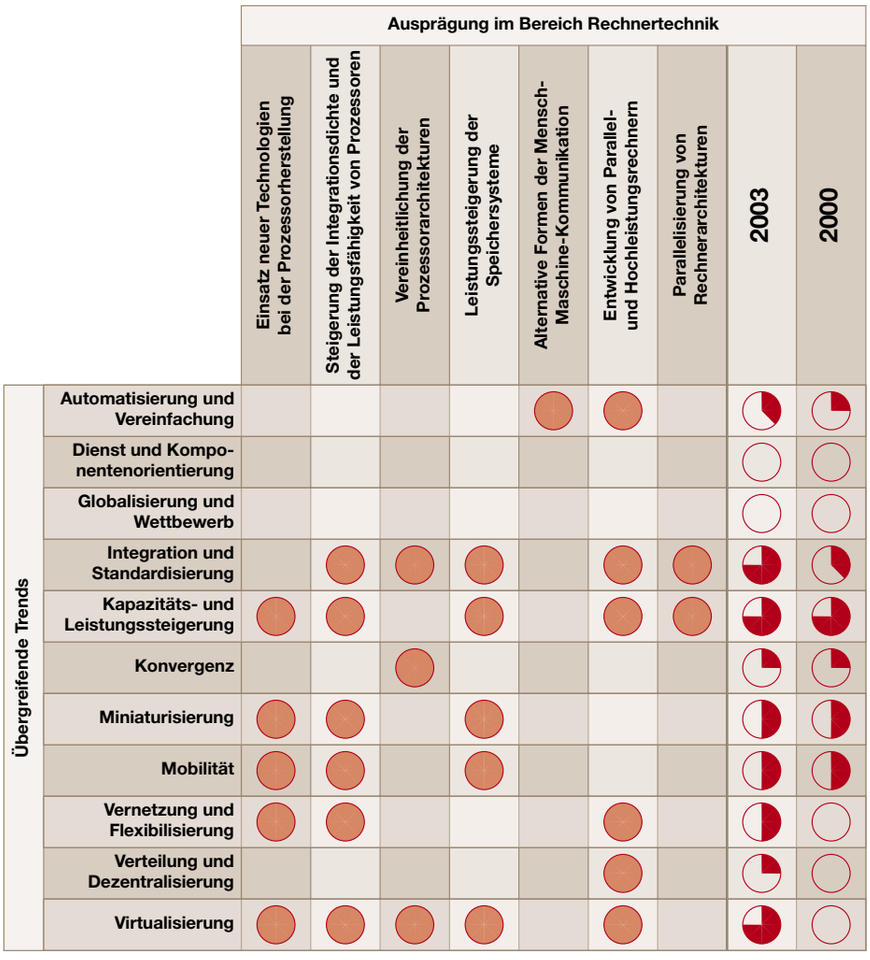



Tabelle 8.1: Ausprägungen übergreifender Trends im Technologiebereich Rechnertechnik

Verfügbarkeit optischer Gatter im Durchschnitt innerhalb der nächsten vier bis sechs Jahre angenommen wird, die aber auch in ihrer Schätzung eine breite Streuung aufweisen: Während einige Wissenschaftler von einem zwei-Jahres-Horizont ausgehen, sehen andere optische Gatter erst in sieben bis acht Jahren. Im Vergleich zur Vorgängerstudie ist jedoch festzuhalten, dass sämtliche Experten den Verfügbarkeitszeitraum insgesamt pessimistischer einschätzen als noch vor drei Jahren: Folgt man den Prognosen der Studie 2000, müssten optische Gatter außerhalb von Forschungslabors schon heute verbreitet sein. Dieser Zeitraum ist um etwa drei Jahre nach hinten korrigiert worden.

Ganz anders hingegen wird die Verfügbarkeit biologischer Gatter beurteilt. Hier decken sich die Prognosen der Vorgängerstudie und die jetzigen Aussagen der Experten, was den absoluten Zeitraum betrifft. Demnach werden biologische Gatter etwa im Jahr 2008 erwartet (Abbildung 8.1, ②). Anders als bei der Einschätzung optischer Gatter, sind die wissenschaftlichen Experten hier weitaus optimistischer als die Experten der Industrie, von denen die Verfügbarkeit biologischer Gatter nicht vor Anfang des nächsten Jahrzehnts erwartet wird.

Bei Quanten-Gattern herrscht Uneinigkeit: Im Durchschnitt gehen die Experten zwar von einer Verfügbarkeit in etwa fünf Jahren aus (siehe Abbildung 8.1, ③), allerdings mit einer großen Streuung zwischen vier und zehn Jahren. Diese Streuung ist in beiden Expertengruppen gleichermaßen zu finden. Es herrscht aber die einhellige Meinung vor, dass die Verfügbarkeit

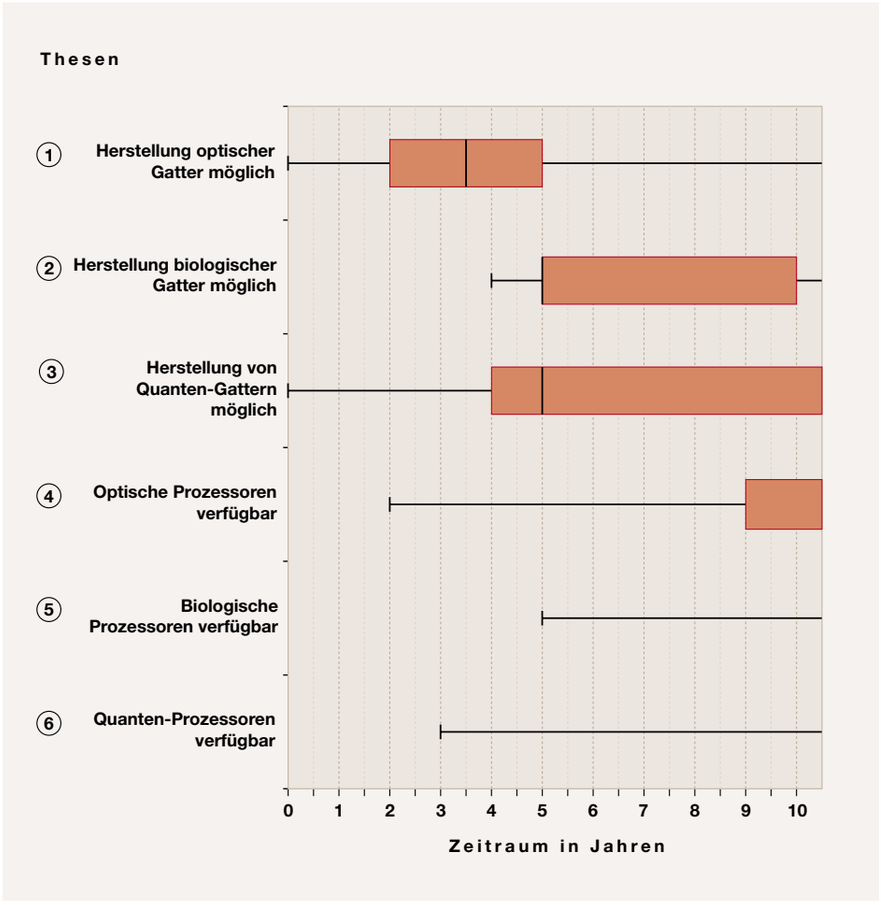



Abbildung 8.1: Ergebnisse der Thesen zum Einsatz neuer Technologien bei der Prozessorherstellung

von Quantengattern eine geringere Bedeutung besitzt als die optischer Gatter. Der Verfügbarkeit biologischer Gatter hingegen sei, nach Meinung der Experten, nur von geringer Bedeutung.

Der Einsatz optischer Gatter wird vorwiegend in der Bild- und Signalverarbeitung, bei der Entwicklung holographischer Speicher (Abschnitt 8.1.4) und als Grundbausteine für photonische Netzegesehen (Abschnitt 8.2.2), vorausgesetzt, die für eine Massenproduktion notwendigen Fertigungsprozesse seien etabliert und die Miniaturisierung der Gatter und der benötigten Laser sei beherrschbar.

Biologische Gatter werden vor allem in der Medizin, besonders im Bereich der Prothetik, und in der Gentechnik gesehen. Die wesentliche Einsatzvoraussetzung für biologischer Gatter ist allerdings die Beherrschung des Entwicklungs- und Produktionsprozesses. Vereinzelt wird auch darauf hingewiesen, dass biologische Bausteine, wie sie in DNA-Computern verwendet werden [Bons 03], keine Gatter im klassischen Sinne darstellen.

Als Anwendungsbereich von Quanten-Gattern wird von den Experten vornehmlich die Kryptographie gesehen (Abschnitt 7.3.7). Voraussetzungen für eine breite Verfügbarkeit von Quanten-Gattern seien aber eine Betriebsstabilität der Gatter und die Beherrschung der Fertigungsprozesse.

Darüber hinaus wird vereinzelt angemerkt, dass insbesondere für Höchstleistungsrechner Feldeffekt-Transistoren auf Gallium-Arsenid-Basis kurzfristig eingesetzt werden könnten und supraleitende Gatter in zehn bis zwölf Jahren verfügbar sein werden, sofern bis dahin die erforderlichen Niedrigtemperatur-Prozesse beherrschbar sind.

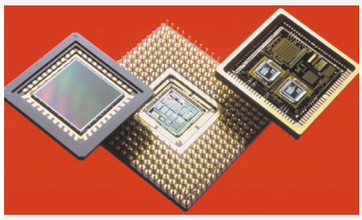
Die Verfügbarkeit optischer, biologischer und Quanten-Prozessoren kann nach Meinung aller Experten nur langfristig betrachtet werden, da Prozessoren in der Regel erheblich später zu erwarten seien als die entsprechenden Gatter. Bei der Prognose optischer Prozessoren gehen die Experten von einer Verfügbarkeit in ungefähr zehn Jahren aus (siehe Abbildung 8.1, ④), wobei die Wissenschafts-Experten dies sehr viel pessimistischer sehen und zu einem nicht unerheblichen Teil sogar anmerken, dass optische Prozessoren nie Produktreife erlangen würden, da die zu erwartenden technischen Schwierigkeiten einer Serienproduktion im Wege stehen würden. Biologische und Quanten–Prozessoren werden innerhalb des abgefragten Zeitraumes nicht erwartet (siehe Abbildung 8.1, ⑤ und ⑥), wobei den biologischen Prozessoren mehrheitlich eine untergeordnete Bedeutung beigemessen wird. Wie schon bei der Beurteilung der Verfügbarkeit von Gattern (siehe oben) zeigt sich auch hier im Vergleich zur Vorgängerstudie eine Korrektur der Prognose: Optische Prozessoren werden insgesamt drei Jahre später verfügbar sein, während die Vorhersage für biologische und Quanten-Prozessoren stabil bleibt. Vereinzelt wird, wie schon in der Vorgängerstudie, angemerkt, dass biologische Prozessoren nie existieren werden, da kein Bedarf bestünde und keine ausreichende Leistungsfähigkeit zu erwarten sei.

Die von den Experten aus Industrie und Wissenschaft angegebenen Anwendungsbereiche dieser Prozessorvarianten decken sich im wesentlichen mit denen der entsprechenden Gatter: Optische Prozessoren könnten vorwiegend im Bereich der Bild- und Signalverarbeitung sowie in der Kommunikations- und Vermittlungstechnik eingesetzt werden, ein Einsatz von Quanten-Prozessoren wird in erster Linie in der Kryptographie und zur Lösung hochkomplexer Probleme gesehen, biologische Prozessoren werden vornehmlich in der Massenspeicherung, der Robotik, der Raumfahrt und im Bereich Wearable Computing [Matt 02] erwartet. Es wird jedoch an verschiedenen Stellen darauf hingewiesen, dass die Basistechnologien gerade für die biologischen wie für die Quanten-Prozessoren noch äußerst rudimentär und daher weit von einem serienmäßigen Einsatz entfernt seien.

Bei den heute verwendeten Prozessorstrukturen treten aufgrund des hohen spezifischen Widerstandes von Aluminium Probleme durch zu hohe Wärmeverluste und Geschwindigkeitseinschränkungen beim Übergang zu noch kleineren Strukturen auf, da ein kleinerer Querschnitt sich negativ auf den Leitungswiderstand auswirkt. Mit Kupfer könnte der Querschnitt der Leitungen (bei gleicher Stromstärke) geringer als bei Aluminium ausfallen. Obwohl schon heute von verschiedenen Herstellern Prozessoren mit Kupfer-Verbindungen angeboten werden (z.B. IBM's Power3-Prozessoren im ASCI White Superrechner [IBM 03a], Sun's UltraSPARC III [Sun 03a] oder Intel's Coppermine Pentium III [Nico 00]), stellt sich die Frage nach einer großflächigen Ablösung von Aluminium durch Kupfer zur Verbindung von Transistoren. Hier sind sich die Experten weitgehend einig: Innerhalb von drei Jahren wird Kupfer Aluminium abgelöst haben (siehe Abbildung 8.2, ①), was sich mit der Einschätzung der Vorgängerstudie deckt. Dies wird allerdings zunächst nur im Hochleistungsbereich geschehen, vorausgesetzt die Herstellungsprozesse können rechtzeitig umgestellt werden. Für den Handheld- und PDA-Bereich sehen die Experten nach wie vor eine dominierende Rolle von Aluminiumverbindungen, hauptsächlich aus Kostengründen.

Zukünftige Mikroprozessoren werden - wenn Moore's Gesetz weiterhin Gültigkeit haben soll - Taktfrequenzen im hohen GHz-Bereich aufweisen (Abschnitt 8.1.2). Wegen der hohen Störempfindlichkeit und der begrenzten Übertragungsbandbreite der elektrischen Verbindungen stoßen herkömmliche Leiterplatten bei der theoretisch erzielbaren Leistungsfähigkeit an ihre Grenzen. Dieser Engpass kann mit optischen Verbindungstechniken, die Übertragungsfrequenzen im GHz-Bereich zulassen, beseitigt werden.

Die Verfügbarkeit optischer Verbindungstechnologien wird von den Experten sehr unterschiedlich eingeschätzt. Die Prognosen reichen von zwei Jahren bis zu mehr als zehn Jahren mit einem Mittel von etwa sechs Jahren. Die Industrieexperten sind dabei aber wesentlich optimistischer als die Wissenschaftler. Abbildung 8.2, ② zeigt das Gesamtergebnis.



PROZESSOREN: Optische Prozessoren werden innerhalb der nächsten 10 Jahre erwartet, biologische und Quanten-Prozessoren erst sehr viel später.

VERBINDUNGSTECHNIKEN: Die Ablösung von Aluminium durch Kupfer wird innerhalb von 3 Jahren erfolgen. Optische Verbindungstechniken werden in 8 Jahren erwartet.

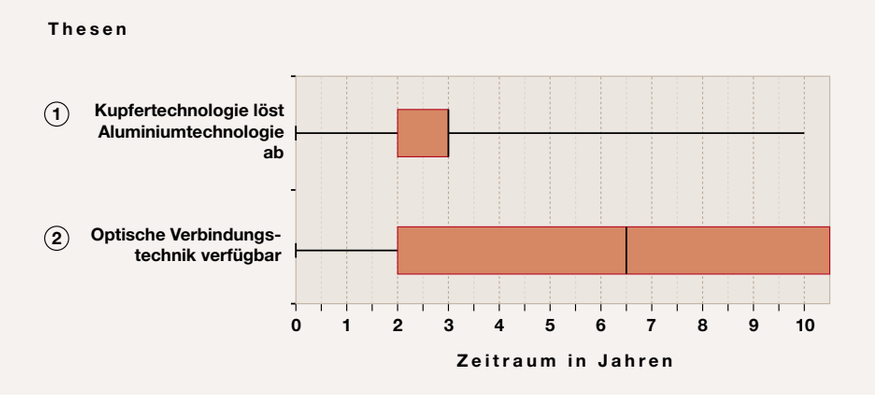



Abbildung 8.2: Ergebnisse der Thesen zur Verbindungstechnik

HALBLEITER-MATERIALIEN: Silizium wird weiterhin das vorherrschende Halbleitermaterial bleiben, allerdings mit abnehmender Bedeutung. Neben Silizium-Germanium gewinnen Indium-basierte Materialien langfristig an Bedeutung. Andere Werkstoffe werden nur in Spezialbereichen zum Einsatz kommen und spielen eine untergeordnete Rolle.

Gegenüber der konventionellen elektrischen Verbindungstechnik eröffnet die optische Verbindungstechnik nach Meinung der Experten neue Anwendungsgebiete. In Spezialbereichen der Vermittlungstechnik, bei der Entwicklung von On-Chip-Multiprozessorarchitekturen (Abschnitt 8.1.2) und als optische On-Chip-Interconnects zur Leistungssteigerung der Ein/Ausgabe von Hochleistungschips werden die hohen Übertragungsbandbreiten im GHz-Bereich und die geringe Signalverzerrung zu neuen Anwendungen führen. Aus Kostengründen, so wird von den Experten ausgeführt, werden optische Verbindungstechniken auf lange Sicht mit den rein elektrischen Ansätzen nicht konkurrieren können.

In der Bewertung zukünftiger Verbindungstechniken sind die Experten im Vergleich zur Vorgängerstudie insgesamt pessimistischer eingestellt. Während die Aluminium-Ablösung durch Kupfer nur um ein Jahr verzögert betrachtet wird, korrigieren die Befragten die Prognose für die Verfügbarkeit optischer Verbindungen um drei Jahre nach hinten. Einige Wissenschaftler gehen sogar davon aus, dass optische Verbindungstechniken on-chip, wenn überhaupt, erst sehr viel später möglich sein werden.

Bereits heute werden in vielen Einsatzbereichen die Silizium-basierten Chips bis an ihre Leistungsgrenze belastet. Dabei geht mehr als die Hälfte der Leistung als Wärme verloren [EaMi 02]. Es stellt sich deshalb die Frage nach effizienteren Halbleiter-Materialien und wie diese in ihrer Bedeutung eingeschätzt werden. Die Experten sind sich einig, dass Silizium nach wie vor eine hervorragende Bedeutung haben wird, insbesondere im Massenmarkt, wo Preisvorteile gegenüber der Konkurrenz durch effiziente Herstellungsprozesse erzielbar sind. Dennoch prognostizieren sie, dass Silizium langfristig durch Silizium-Germanium-Verbindungen verdrängt werden wird. Obwohl mit Gallium-Arsenid hergestellte Transistoren wesentlich höhere Schaltgeschwindigkeiten erreichen können und deshalb unter anderem für Sendeverstärker in Mobilfunktelefonen, in der Satellitennavigation und als Bausteine für Hochgeschwindigkeitscomputer verwendet werden, wird diesem Werkstoff nur eine untergeordnete Bedeutung attestiert. Langfristig wird er, da sind sich die Befragten einig, durch Gallium-Nitride und Indium-Verbindungen, die eine Schlüsselrolle bei optischen Speichern einnehmen werden und extrem hohe Taktfrequenzen erlauben, abgelöst (siehe Abbildung 8.3). Voraussetzung ist allerdings, dass die hohen Produktionskosten dieser Technologien gesenkt werden können.

Interessant ist, dass die Experten aus Wissenschaft und Industrie die Bedeutung der verwendeten Materialien nahezu identisch einschätzen, im Vergleich zur Vorgängerstudie aber deutlich unterschiedliche Prognosen stellen. Die langfristige Bedeutung von Silizium und Silizium-Germanium wird deutlich geringer eingeschätzt als noch vor drei Jahren, die Bedeutung von Gallium- und Indium-basierten Materialien wird hingegen wesentlich optimisti-

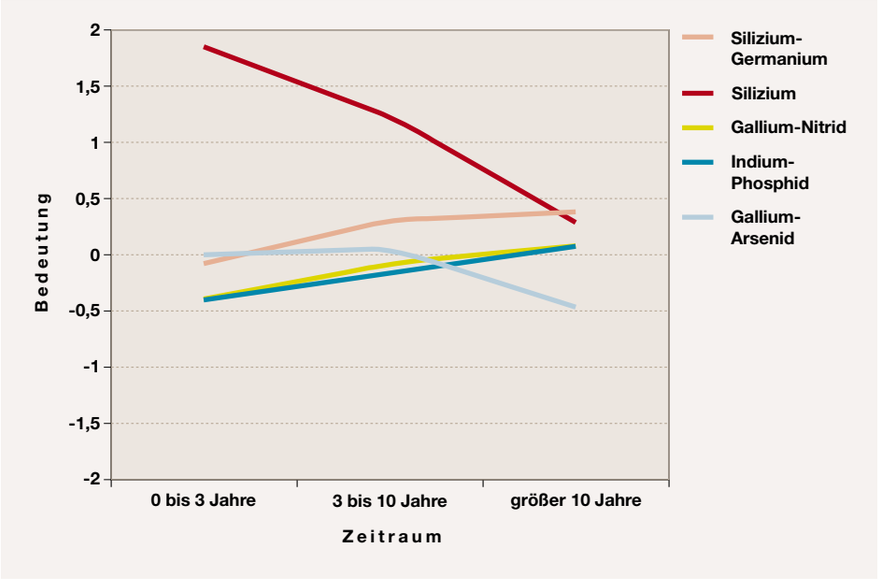



Abbildung 8.3: Bedeutung unterschiedlicher Halbleitertechnologien

scher beurteilt. Langfristig sehen die Experten eine nahezu identische Bedeutung der Materialien, ganz im Gegensatz zur Vorgängerstudie, in der Silizium noch eine deutlich dominierende Rolle spielte.

### Zusammenfassung

Die Experten wurden gebeten, neue Prozessor- und Halbleitertechnologien in ihrer kurz-, mittel- und langfrsitigen Bedeutung zu evaluieren. Dabei zeigt sich, dass zu herkömmlichen Prozessoren zwar Alternativen existieren, diese aber, wenn überhaupt, eher langfristig von Bedeutung sein werden. Eine Ausnahme bildet die mittelfristig stattfindende Ablösung von Aluminiumverbindungen durch Kupferverbindungen. Im einzelnen ergab sich folgendes:

- Die Herstellung optischer Gatter wird bis 2007 erwartet. Biologische Gatter werden nicht vor 2008 zur Verfügung stehen und die Herstellung von Quantengattern wird bis 2008 möglich sein.

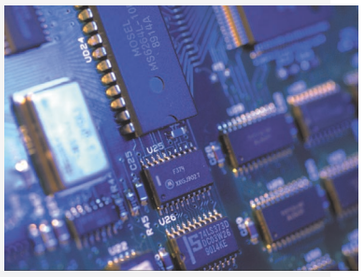
- Optische Prozessoren werden nicht vor 2013 erwartet, biologische und Quanten-Prozessoren nicht innerhalb der nächsten 10 Jahre.

- Die Ablösung von Aluminium durch Kupfer wird bis 2006 erfolgen. Optische Verbindungstechniken werden bis 2010 erwartet.

- Silizium wird zwar weiterhin die vorherrschende Basis für Halbleiter bilden, allerdings mit abnehmender Bedeutung. Neben Silizium-Germanium gewinnen Indium-basierte Materialien langfristig an Bedeutung. Andere Werkstoffe kommen nur in Spezialbereichen (z.B. Hochfrequenztechnik, optische Speicher) zum Einsatz.

## 8.1.2 Steigerung der Integrationsdichte und der Leistungsfähigkeit von Prozessoren

Ohne auf alternative Technologien, wie sie im ersten Abschnitt dieses Kapitels grundsätzlich untersucht wurden (Abschnitt 8.1.1), zu fokussieren, stellt sich generell die Frage, inwieweit die Leistungsfähigkeit herkömmlicher Konzepte noch gesteigert werden kann. Zwar gilt Moore's Gesetz nach wie vor, doch sieht selbst der Entdecker des Gesetzes, Gordon Moore, Grenzen des Wachstums [Bonn 03]. Von den Experten wurde deshalb die Langfristigkeit dieses Gesetzes hinterfragt, insbe-



STEIGERUNG DER INTEGRATIONSDICHTE: Mit der herkömmlichen Siliziumtechnologie sind auch ohne Quanteneffekte Steigerungen der Integrationsdichte noch mindestens für weitere 10 Jahre zu erzielen. Langfristig werden Größenordnungen von etwa zehn Milliarden Transistoren pro Chip erwartet.

MEHRPROZESSOR-CHIPS: Mehrprozessor-Chips werden in 5 Jahren weit verbreitet sein.

sondere vor dem Hintergrund der in letzter Zeit zu verzeichnenden stillen technologischen Revolutionen [Inte 02], die sich wie folgt zeigt: Die Prozessgeometrie auf einem Chip liegt heute weit unter 100 Nanometern und führt zu molekularen Produktionsprozessen, aktuelle Lithografietechniken haben den Sub-100-Nanometerbereich erreicht, mit inzwischen mehreren Kupferverdrahtungsschichten. Der kleinste in Serie produzierte CMOS-Transistor (Complementary Metal Oxide Semiconductor) besitzt nur noch eine Gatterlänge von 50 nm, die Gatterlänge von Forschungstransistoren liegt inzwischen unter 10 nm. Die ersten auf EUV-Technologien basierenden Prototypen sind entstanden und markieren einen weiteren Miniaturisierungsschub.

Neue Technologien wie drei-dimensionale Tri-Gate- und Terahertz-Transistoren adressieren die zunehmenden Probleme vermehrten Stromverbrauchs und zusätzlicher Wärmeabgabe herkömmlicher planarer Transistoren.

Mit Hilfe der Experten sollte geklärt werden, ob Moore's Gesetz bis zum Jahr 2013 weiterhin Bestand haben kann und ob davon ausgegangen werden kann, dass die von der SIA (Semiconductor Industry Association) prognostizierte Entwicklung in der Prozessor-Technologie, wie sie in der *2001 International Technology Roadmap for Semiconductors (ITRS)* angegeben ist [SIA 01, AEJ+ 02], so auch eintreffen wird. Der Fokus der Befragung beruht dabei nicht nur auf den klassischen Metriken (Anzahl der Transistoren pro Chip, Taktfrequenzen), sondern liefert auch eine Prognose über die Dominanz der Silizium-Technik selbst. Bei einer derartig rasanten Entwicklung, wie sie in der Integrationsdichte beobachtet werden kann, stellt sich außerdem die Frage nach der Integration von zusätzlichen Funktionalitäten auf einem Chip, wie sie ansatzweise in Intel's Banias-Plattform [Grif 02] oder AMD's Hammer-Chip [Webe 01] zur Unterstützung mobiler Anwender zu finden ist. Die Befragten wurden deshalb gebeten, eine Auswahl vorgegebener Funktionsgruppen direkt im Hinblick auf eine mögliche Prozessorintegration zu beurteilen. Eine indirekte Bewertung kann aus anderen Kapiteln dieser Studie insofern abgeleitet werden, als dass viele dort genannte Technologien erst durch eine entsprechende Leistungsfähigkeit von Prozessoren möglich wird (z.B. Sensornetze, Funknetze, photonische Netze in Abschnitt 8.2.7).

## Ergebnisse

Nach wie vor gehen die Experten davon aus, dass auch in den nächsten zehn Jahren Moore's Gesetz Gültigkeit haben wird: Silizium-basierte Chips bieten langfristig noch genügend Potenzial für entsprechende Integrationsdichten (siehe Abbildung 8.4, ①). Eine über diesen Zeitraum hinausgehende Prognose wird nur vereinzelt getroffen, obwohl die Technologie-Roadmap für Halbleiter der SIA [SIA 01] und die Prognosen der Prozessorhersteller (z.B. Intel [Inte 02]) in der Regel verlässlich einen Zeitraum von 15 Jahren abdecken. Insofern können die in dieser Studie abgefragten Prognosen über die nächsten zehn Jahre mit der SIA-Roadmap korreliert werden. Wie schon in der Vorgängerstudie [SETIK 00] liegen die Meinungen der Experten aus Wissenschaft und Industrie im Detail weit auseinander. Während die Wissenschaftler mehrheitlich von einem Ende der Entwicklung in etwa sechs bis sieben Jahren ausgehen, sehen die industriellen Experten dieses Ende nicht innerhalb der nächsten zehn Jahre. Die dann erreichte Steigerung der Integrationsdichte pro Chip dürfte nach Ansicht vieler Experten in etwa die Grenze von zehn Milliarden erreicht haben und damit den Produktionsprozess in die Nähe molekularer Strukturen rücken. Aufgrund dieser dann erreichten Integrationsdichte sehen die Befragten mehrheitlich in etwa fünf Jahren eine weite Verbreitung von Mehrprozessor-Chips (siehe Abbildung 8.4, ②) und sie gehen davon aus, dass ein Großteil der gewonnenen Leistung schon in zwei Jahren für ein auf größeren Cache-Speichern basierendes, verbessertes Cache-Management, zum Beispiel in fehlertoleranten Rechnerstrukturen, verwendet wird (siehe Abbildung 8.4, ③). Während die Experten aus der Wissenschaft die Verfügbarkeit von Mehrprozessor-Chips optimistischer sehen als die Befragten der Industrie, äußern sich letztere bei der Bereitstellung größerer Caches optimistischer (Abschnitt 8.1.4).

Die Experten weisen mehrheitlich darauf-hin, dass wesentliche Voraussetzungen

für die Steigerung der Integrationsdichte adäquate Lithographie-Techniken (z.B. Elektronenstrahl-Lithographie, Röntgen-Lithographie, optische Lithographie), die Beherrschung der Nanotechnologie und die Lösung des Abwärme-Problems sind. Daneben wird von einigen Experten angemerkt, dass für die Entwicklungs- und Produktionsprozesse leistungsfähige Werkzeuge notwendig seien, dies gelte insbesondere gerade für CAD-Tools (Computer Aided Design). Vereinzelt wird argumentiert, dass die zunehmende Integrationsdichte deswegen nicht für größere Caches verwendet werden wird, weil es mehr Sinn mache, den gewonnenen Platz eher für Multithreading bzw. Mehrprozessor-Chips zu nutzen als für größere Cache-Speicher. Die dafür notwendigen Werkzeuge für die Entwicklung paralleler Algorithmen seien allerdings noch nicht ausgereift. Auf diese Frage wird im Kapitel 8.4 näher eingegangen.

Eine zunehmende Integrationsdichte eröffnet neue Anwendungsfelder und die Integration von Funktionalitäten, die derzeit im wesentlichen von Spezialprozessoren geleistet werden (z.B. Grafik, Sound, Video). Deshalb wurden die Experten nach der Bedeutung der Integration diverser vorgegebener Funktionsgruppen in Prozessoren befragt. Abbildung 8.5 zeigt die Ergebnisse.

Nach Ansicht der Befragten ist die Integration kryptographischer Funktionen eine der vordringlichsten Aufgaben für die nächsten zehn Jahre. Dies ist eine direkte Folge der zunehmenden Vernetzung (Abschnitt 8.2.4) und Computerisierung der Gesellschaft (Kapitel 9), die auf einer sicheren und vertrauenswürdigen Kommunikation basieren muss (Kapitel 7.2 und Abschnitt 8.2.1). Die Bedeutung der Kryptographie-Integration wird von den Experten aus der Wissenschaft zwar höher eingeschätzt als von den Industrieexperten, langfristig aber sind sich beide Expertengruppen über die hervorragende Bedeutung einig. Ein gänzlich anderes Bild ergibt sich für die Signalverarbeitung, die eine der Voraussetzungen für multimediale Anwendungen und Sprachsteuerung darstellt (Abschnitt 8.1.5). Aus Sicht der Industrieexperten ist dies die wichtigste Funktionsgruppe, die für die Wissenschaftsexperten allerdings nur eine untergeordnete Rolle spielt. Die Bedeutungsentwicklung für Grafik, Sound und Video wird nach Ansicht der Experten parallel verlaufen, mit einer moderaten Steigerung über die nächsten zehn Jahre.

Als Anwendungsfelder für integrierte Prozessoren werden vor allem Multimedia (Synthetisierung von Musik, DVD (Digital Versatile Disc)), automotive Anwendungen, Maschinensteuerung, biometrische Verfahren, Virtual Reality sowie Videokonferenzen genannt. Vereinzelt wird angemerkt, dass auch auf lange Sicht nicht damit zu rechnen sei, dass Spezialprozessoren für Grafik und Video durch eine Integration dieser Funktionen in den Prozessor abgelöst werden, da letztere erheblich wirtschaftlicher hergestellt werden könnten. Von einigen Experten wird im Rahmen dieser Bewertung auf das System-on-a-Chip, also die Integration der gesamten Funktionalität eines Systems einschließlich Speicher auf einen Chip [CiSt 99] hingewiesen.

Bei der Beurteilung der Integration von Funktionsgruppen in Prozessoren (bzw. Multi-Prozessoren) ergibt sich im Vergleich zur Vorgängerstudie ein verändertes Bild. Wurden im Jahre 2000 den zur Diskussion gestellten möglichen Integrationen von Funktionsgruppen noch deutliche Steigerungen in der Bedeutung bescheinigt, so wird diese Einschätzung für alle Funktionsgruppen insgesamt abgeschwächt (siehe Abbildung 8.5). Läßt sich mittelfristig noch eine Zunahme der Bedeutung einzelner Funktionsgruppen ausmachen, so sind langfristig wesentliche Bedeutungszuwächse nur für die Integration von Kryptographie und Signalverarbeitung zu erkennen. Insbesondere ist - im Vergleich zur Vorgängerstudie - die stark abgeschwächte Bedeutung der Integration von Sound und Signalverarbeitung zu bemerken.

Prozessoren mit einer Taktfrequenz im unteren GHz-Bereich sind heute bereits serienreif. In den Forschungslabors der Hersteller wird inzwischen mit Taktfrequenzen zwischen 50 und 100 GHz experimentiert. Nach Meinung der Experten ist in sieben (Mehrheit der wissenschaftlichen Experten) bis zehn Jahren (Mehrheit der Industrieexperten) damit zu rechnen, dass derart leistungsfähige Prozessoren weit verbreitet sein werden (siehe Abbildung 8.4, ④). Es ist an dieser Stelle anzumerken, dass sich diese Einschätzung nicht mit

FUNKTIONSGRUPPEN: Vor allem die Integration kryptographischer Funktionalitäten gewinnt zukünftig an Bedeutung, langfristig wird die Integration von Signalverarbeitungsfunktionen erwartet.

TAKTFREQUENZ: Prozessoren mit Taktfrequenzen von 50 GHz oder mehr werden in etwa 8 Jahren verbreitet eingesetzt.

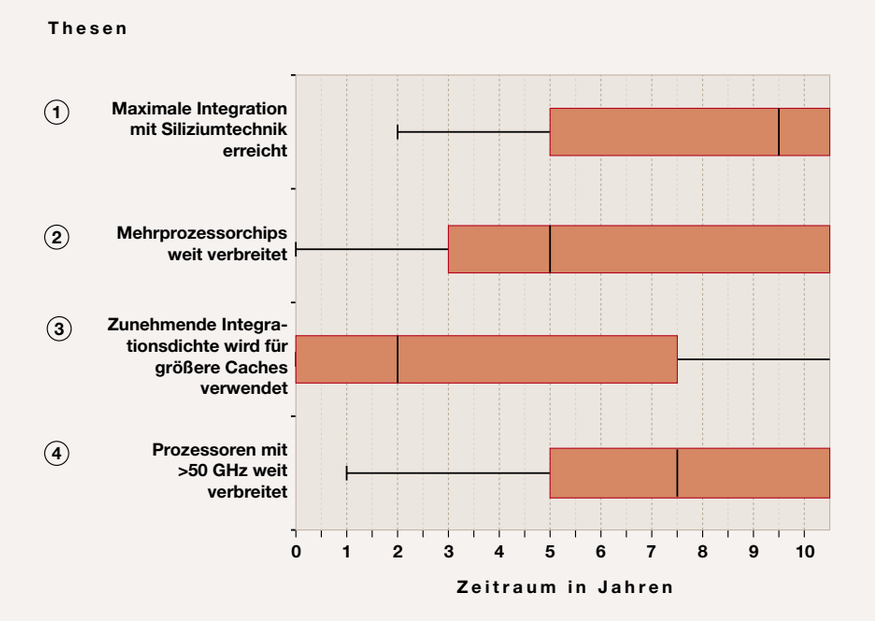



Abbildung 8.4: Ergebnisse der Thesen zur Steigerung der Integrationsdichte und Leistungsfähigkeit von Prozessoren

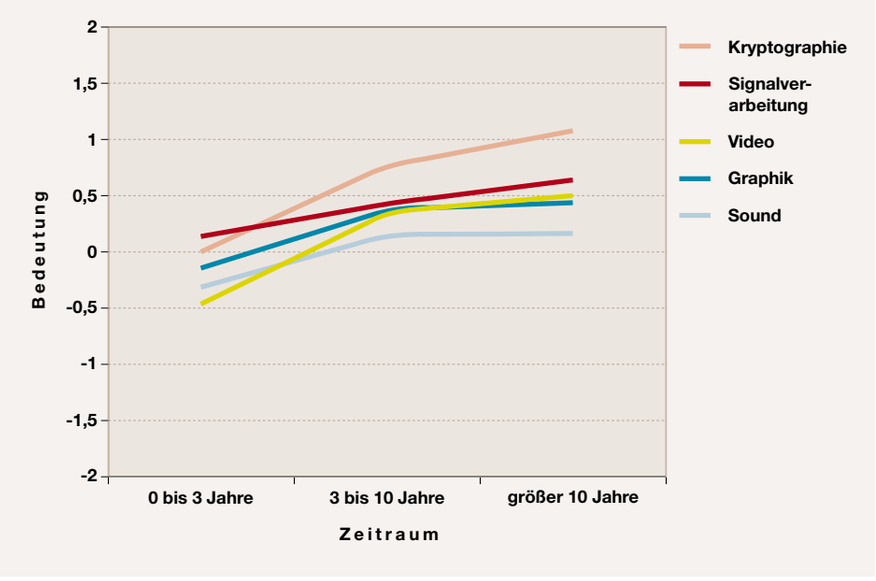



Abbildung 8.5: Bedeutung der Integration von Funktionsgruppen in den Prozessor

der International Technology Roadmap for Semiconductors [AEJ+ 02] deckt, die bis zum Jahr 2013 von 20-GHz-Taktungen ausgeht. Um dieses Ziel zu erreichen, werden als notwendige Technologien neben der Röntgen-Lithographie, die Verwendung von Kupfertechnologie (Abschnitt 8.1.1) sowie SOI (Silicon-on-Insulator) zur vollständigen dielektrischen Isolation jedes Bauelementes einer integrierten Schaltung [Kuhl 98], genannt.

### Zusammenfassung

Die Leistungsfähigkeit von Prozessoren wird sich exponentiell weiter entwickeln. Die zunehmende Integrationsdichte ermöglicht neue Konzepte von Prozessorstrukturen. Die Befragung der Experten zu diesem Umfeld hat zu folgenden Ergebnissen geführt:

- Mit der herkömmlichen Siliziumtechnologie sind auch ohne Ausnutzung von Quanteneffekten noch Verbesserungen der Integrationsdichte für mindestens weitere 10 Jahre zu erzielen. Bis zum Jahr 2013 werden Größenordnungen von etwa zehn Milliarden Transistoren pro Chip erwartet.
- Vor allem die Integration kryptographischer und Signalverarbeitungsfunktionen werden zukünftig an Bedeutung gewinnen. Dabei sehen die Experten aus der Industrie den höchsten Stellenwert im Bereich der Signalverarbeitung, während die Experten aus der Wissenschaft einen höheren Stellenwert im Bereich der Kryptographie erwarten.
- Mehrprozessor-Chips werden bis zum Jahr 2008 weit verbreitet sein werden.
- Prozessoren mit Taktfrequenzen von 50 GHz und mehr werden bis zum Jahr 2012 verbreitet eingesetzt.

## 8.1.3 Vereinheitlichung der Prozessorarchitekturen

Seit dem Erscheinen der Vorgängerstudie im Jahr 2000 hat sich die Technologielandschaft gerade im Bereich der Prozessorarchitekturen verändert. Einen guten Indikator für den aktuellen Stand der Entwicklungen liefert das alljährlich stattfindende Microprocessor Forum [Micr 03]. Die wohl wichtigste Beobachtung des Forums 2002 war die allgemeine Verfügbarkeit von 64-Bit-Prozessoren bei allen Herstellern [Vils 02]. Für eine langfristige Prognose wird jedoch interessant sein, ob sich aus der Vielzahl der 64-Bit-Architekturansätze (z.B. Intel's IA-64 [Stil 99a], Sun's und Fujitsu's SPARC64-V [Stil 99b]), IBM's PowerPC [Stil 99b]) Standardarchitekturen herauskristallisieren werden und welche Rolle Java-Prozessoren (z.B. picoJava [TaGo 99]) spielen werden.

Intel favorisiert seit der 80x86-Reihe die sogenannte Binär-Kompatibilität [HePa 03], d.h. Binärcode einer Architektur ist auf anderen Architekturen lauffähig. Dies bedeutet natürlich, dass Neuerungen problematisch einzuführen sind, da immer darauf geachtet werden muss, dass das neue System in der Lage ist, die für das Vorgängermodell entwickelte Software auszuführen [Mess 97]. Diese Art der Kompatibilität beschränkt sich naturgemäß nicht allein auf die unterliegende Prozessorarchitektur, sondern auch auf das darauf eingesetzte Betriebssystem. Anders ist die Situation im UNIX-Umfeld. Hier findet man typischerweise Quellcode-Kompatibilität. Es wird nicht erwartet, dass übersetzte Programme auf unterschiedlichen Architekturen lauffähig sind, sondern es wird derselbe Quellcode auf verschiedenen Architekturen übersetzt. Somit ist man von der unterliegenden Architektur weitgehend unabhängig, vorausgesetzt, es existiert ein Compiler, der das im Quelltext vorliegende Programm in Maschinencode der entsprechenden Architektur überführen kann. Durch die starke Verbreitung der Programmiersprache Java in den letzten Jahren ist eine weitere Art von Kompatibilität in den Vordergrund getreten. Hier wird Bytecode erzeugt, der auf einer virtuellen Maschine ausgeführt wird. Existiert für eine Architektur eine Implementierung dieser virtuellen Maschine, so kann der Bytecode dort zur Ausführung gebracht werden [Sun 02a]. Es ist dann unerheblich, welche Architektur dem System zugrunde liegt. Dieses Konzept wird als *Write Once, Run Anywhere* bezeichnet.

### Ergebnisse

Die Frage nach der Bedeutung der unterschiedlichen Prozessorarchitekturen wird von den befragten Experten einheitlich beantwortet (siehe Abbildung 8.6). Derzeit herrscht zwar noch Intel's 32-Bit-Architektur IA-32 vor, die 64-Bit-Architektur IA-64 wird jedoch schon mittelfristig eine hohe Bedeutung erlangen [Vils 02] und sich nach Meinung einiger Experten zum Industrie-Standard entwickeln. Langfristig jedoch wird diese Architektur gegenüber einer 128-Bit-Architektur an Bedeutung verlieren (siehe Abbildung 8.6), die vornehmlich im Server- bzw. Mainframe-Umfeld eingesetzt werden wird. Dies sehen insbesondere die Experten der Wissenschaft so. Die Bedeutung aller anderen Architekturen wird nach Meinung aller Befragten kontinuierlich zurückgehen, lediglich den derzeit noch relativ unbedeutenden Java-Prozessoren wird hauptsächlich von den Experten der Industrie mittel- bis langfristig eine steigende, aber dennoch untergeordnete, Bedeutung zugemessen. Von einigen Experten wird darauf hingewiesen, dass die Bedeutung der 64- bzw. 128-Bit-Architekturen eng an eine entsprechende Compilertechnologie geknüpft sei. Ebenso wird bemerkt, dass die Bedeutung der Architekturen wesentlich von der jeweiligen Marktmacht der Hersteller abhängig sei. Da nach Meinung aller Experten die Bedeutung der meisten zur Diskussion gestellten Architekturen langfristig sinken wird, stellt sich die Frage nach Alternativen. Obwohl von allen Experten mit Neuentwicklungen gerechnet wird, konnte weder von der Wissenschaft noch von der Industrie die Frage beantwortet werden, in welche Richtungen die Entwicklungen denn gehen könnten.

PROZESSORARCHITEKTUREN: IA-64 wird zur Zeit die neue Standardarchitektur. Innerhalb der nächsten 10 Jahre wird IA-64 allerdings gegenüber der 128-Bit-Architektur IA-128 an Bedeutung verlieren. Java–Prozessoren werden nur von rudimentärer Bedeutung sein, andere Prozessoren werden nur noch vereinzelt in Spezialbereichen zum Einsatz kommen.

KOMPATIBILITÄTSKLASSEN: Quellcode- und besonders Bytecode-Kompatibilität werden in 5 Jahren die derzeit noch vorherrschende Binärkompatibilität an Bedeutung übertreffen.

In der Beurteilung der Bedeutung unterschiedlicher Kompatibilitätsklassen sind sich die Experten einig (siehe Abbildung 8.7): Binär-Kompatibilität, heute als de facto-Standard von relativ größter Bedeutung, wird schon mittelfristig gegenüber Quellcode- und Bytecode-Kompatibilität an Bedeutung verlieren, trotz der starken Microsoft/Intel-Dominanz. Vereinzelt wird im Rahmen der Bytecode-Kompatibilität auf Java-Alternativen (z.B. C#) hingewiesen. Erwähnt wird von beiden Expertengruppen die Bedeutung der Bytecode-Kompatibilität in den Bereichen Embedded Systems und Web Services (Kapitel 9 und Abschnitt 8.4.2). Ebenfalls mehrfach erwähnt wird in diesem Zusammenhang die nicht unerhebliche Bedeutung des Open Source-Konzeptes und eine langfristig erwartete Ablösung der Java-Plattformen durch neue, heute noch unbekannte, Konzepte (Abschnitt 8.4.6).

Der Vergleich mit der Vorgängerstudie [SETIK 00] zeigt, dass die Bedeutungen von Prozessorarchitekturen und Kompatibilitätsklassen insgesamt zwar niedriger beurteilt werden, aber auf einem gleichbleibenden Niveau.

### Zusammenfassung

Die Fragestellungen zur Vereinheitlichung von Prozessorarchitekturen beurteilen die Experten aus Industrie und Wissenschaft gleich.

- Es wird erwartet, dass die Intel 64-Bit-Architektur IA-64 zur dominierenden Architektur der nächsten zehn Jahre wird, bevor sie um 2013 durch das 128-Bit-Pendant IA-128 verdrängt werden wird.
- Java-Prozessoren werden auch langfristig nur von rudimentärer Bedeutung sein, andere Prozessoren werden nur noch vereinzelt in Spezialbereichen zum Einsatz kommen.
- Quellcode- und Bytecode-Kompatibilität werden bis 2008 die derzeit noch vorherrschende Binärkompatibilität an Bedeutung übertreffen.

## 8.1.4 Leistungssteigerung der Speichersysteme

Seit Ende der 50er Jahre, als die ersten Plattenspeicher kommerziell eingesetzt wurden, hat sich die Entwicklung von Speichersystemen rasant beschleunigt: Heutige Festplattensysteme können pro Quadratzentimeter etwa 5 Millionen mal mehr Informationen halten als die damaligen Produkte. Während der letzten Dekade hat sich die Speicherdichte jährlich verdoppelt, auch jetzt ist ein Wachstumsstopp nicht zu erkennen.

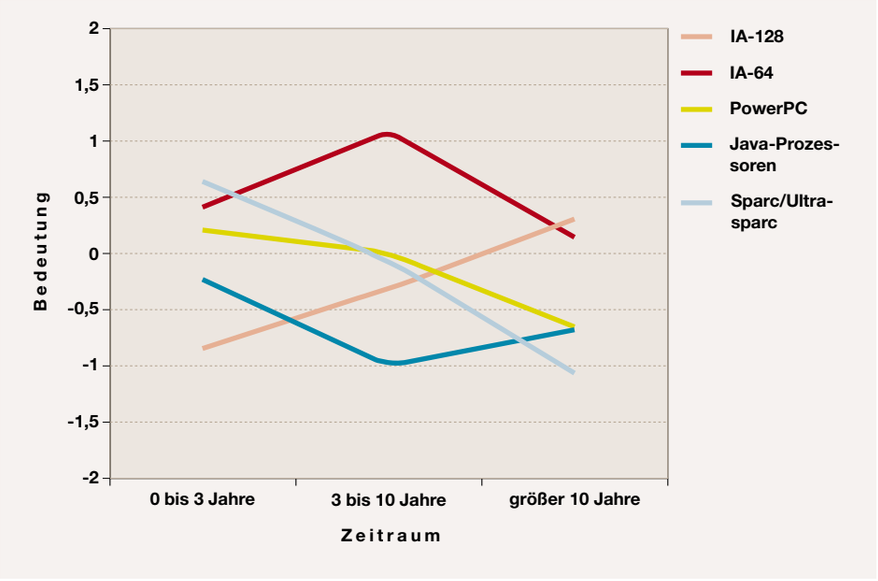



Abbildung 8.6: Bedeutung unterschiedlicher Prozessorarchitekturen

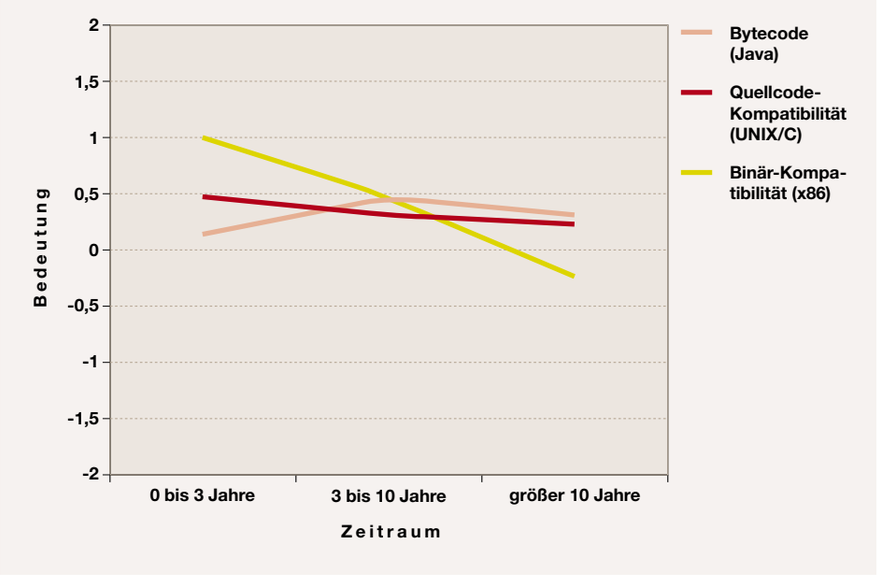



Abbildung 8.7: Bedeutung unterschiedlicher Kompatibilitätsklassen

Nach wie vor überwiegen die magnetischen Speichertechnologien, die inzwischen Speicherdichten im Gigabit-Bereich pro Quadratzentimeter erreichen. Werden die magnetischen Felder auf einer Platte jedoch zu klein, können sie ihre magnetische Ausrichtung nicht mehr aufrechterhalten. Die Folge ist der Verlust von Daten. Als ein Ausweg wird die Entwicklung neuer magnetischer Medien gesehen, die eine Veränderung der magnetischen Orientierung erschweren, zum Beispiel AFC (Antiferromagnetic Coupling). Sie zwingen benachbarte magnetische Schichten zu unterschiedlichen magnetischen Orientierungen. Dies erlaubt Speicherdichten im 100 Gigabit-Bereich pro Quadratzentimeter, ohne die magnetische Orientierung zu verlieren. Mit auf AFC aufbauenden Multilayer-Medien sollen schon kurzfristig zehnfache Speicherdichten angestrebt werden (siehe z.B. Fujitu's Synthetic Ferrimagnetic Media (SFM) Technologie [AAI+ 01]). Eine andere Technologie, die den bei immer kleiner werdenden magnetischen Speicherzellen auftretenden Superparamagnetismus auszuschalten versucht, ist das Heat Assisted Magnetic Recording (HAMR)-Verfahren [PW 02], mit dem pro Quadratzentimeter ein Datenvolumen im Terabyte-Bereich gespeichert werden kann. Im HAMR-Verfahren wird das Speichermedium mit einem Laserstrahl punktgenau an den Stellen erhitzt, an denen die Bits gespeichert werden sollen. Nach dem Beschreiben wird die Speicherstelle durch eine sofortige Kühlung stabilisiert. An der US-Universität Buffalo in New York wird mit der Spintronics-Technologie ein anderer Weg verfolgt. Hier wird der elektronische Spin und die Ladung Nickel-basierter, magnetischer Sensoren in der Größe weniger Atome ausgenutzt, um dicht gespeicherte Daten zu lesen. Nach Aussagen der Forscher seien mit dieser Technologie 50 und mehr DVDs auf Festplatten der Größe eine Scheckkarte speicherbar [Lyma 02].

Eine Steigerung der Speicherdichte wird langfristig auch von optischen Techniken erwartet. Eine Schlüsselrolle kommt dabei den auf Gallium-Nitrid basierenden blauen und violetten Lasern zu, die mit Wellenlängen von 400 bis 500 Nanometern arbeiten. Mit Blu-Ray hat sich ein erstes Industriekonsortium gebildet, das die nächste, auf solchen Lasern aufbauende, Generation hoch-kapazitiver optischer Speicher vorbereitet, welche die Speicherung mehrstündiger Monumentalfilme auf einer einzelnen Blu-Ray-CD zulassen [Mats 02]. Vor diesem Hintergrund wurde im Rahmen der Studie überprüft, welche Bedeutung die einzelnen Technologien kurz- bis langfristig haben werden.

Leistungssteigerungen von Speichersystemen werden nicht nur von den zugrunde liegenden Technologien bestimmt, sondern auch von der Organisation des Speichers. Nach wie vor sind die verfügbaren Speichersysteme in einer klassischen, auf dem Lokalitätsprinzip [HePa 03] basierenden, Hierarchie angelegt: Je weiter man sich von der CPU (Central Processing Unit) entfernt, desto langsamer und größer werden die Speicher. Auf der ersten Ebene befinden sich die Register des Prozessors. Diese werden typischerweise vom Cache-Speicher gefüttert, bei dem es sich in der Regel um einen sehr schnellen Assoziativspeicher handelt. Der Cache-Speicher kann direkt in den Prozessor integriert sein und wird dann als $1^{st}$ Level Cache (oder L1) bezeichnet. Stand der Technik ist heute, auch $2^{nd}$ Level Caches (oder L2) in Prozessoren zu integrieren. Im Gegensatz dazu stehen $3^{rd}$ Level Caches (oder L3), die sich nicht direkt im Prozessor befinden. Auf der nächst höheren Ebene befindet sich der Hauptspeicher, gefolgt vom Plattenspeicher, der wiederum vom Tertiärspeicher (Bandlaufwerke und optische Platten) bedient wird.

Die Experten wurden gebeten, die langfristig zu erwartenden Speichergrößen in dieser Hierarchie zu prognostizieren und gleichzeitig zu beurteilen, inwieweit das klassische Hierarchiekonzept noch adäquat ist oder ob es gar durch die sich abzeichnenden Technologien obsolet wird. Optische DVDs [TaGo 99], biologische Speicher und quantenmechanische Speicher wurden dahingehend untersucht, ob sie für eine Ablösung der derzeit üblichen Festplattensysteme in Frage kommen bzw. wann dies geschehen wird.

### Ergebnisse

Mit zunehmender Miniaturisierung stellt sich die Frage nach der Integration größerer Caches in Prozessoren. Nachdem die Befragten dies grundsätzlich bejahten (Abschnitt 8.1.2), wurde

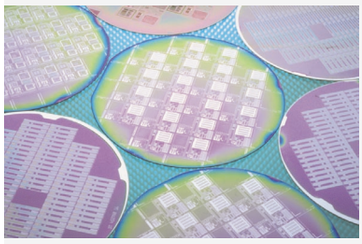
in diesem Abschnitt untersucht, wie sich die Größe der in Prozessoren integrierte Speicher, also der Caches, in den nächsten Jahren entwickeln wird.

Bei der Größe des integrierten (Cache-)Speichers wird weiterhin ein deutliches Wachstum erwartet. Während kurzfristig Caches bis zu einer Größe von etwa 25 Megabyte zu erwarten sind, wird sich die Steigerungsrate mittel- bis langfristig erheblich beschleunigen. Die Experten gehen davon aus, mittelfristig durchschnittliche Cache-Größen von 60 Megabyte zu erreichen, während in zehn Jahren mit Größen zwischen 300 Megabyte und 350 Megabyte zu rechnen ist (siehe Abbildung 8.8). Von den Experten wird vereinzelt auf die Notwendigkeit effizienter Cache Locking Mechanimsmen (z.B. Mehrwege-Locking) hingewiesen. Interessant sind in diesem Zusammenhang die sehr viel optimistischere Beurteilung durch die Industrie-Experten und die zu erkennende dramatische Beschleunigung bei Cache-Größen im Vergleich zur Vorgängerstudie [SETIK 00], die bis zum Jahr 2010 noch Cache-Größen von 64 Megabyte vorhergesagt hatte.

Begleitend wurde von den Experten abgefragt, ob integrierte Caches überhaupt ein Zukunftskonzept seien, ob nicht Fortschritte in der Hauptspeichertechnologie Caches überflüssig machen könnten und wann dies der Fall sein könnte. Im Zusammenhang mit der Frage nach der zu erwartenden Cache-Größe waren die Antworten im Gegensatz zur Vorgängerstudie eindeutig (siehe Abbildung 8.9, ①): Die weitaus meisten Experten gehen davon aus, dass eine solche Ablösung nie stattfinden werde, da sich die Speicherhierarchie bewährt habe und interne, schnelle Speicher immer eine große Bedeutung haben würden, auch wenn die Programmierung sich durch einen Verzicht auf Caches vereinfachen würde. Um entscheidende Beschleunigungen zu erreichen, bedürfe es vielmehr innovativer Konzepte in der Prozessorarchitektur. Vereinzelt wurde jedoch angemerkt, dass mittelfristig mit einer Reduktion der Anzahl der Cache-Hierarchieebenen durch die Verwendung schnellerer Bausteine wie zum Beispiel Rambus DRAMs (RDRAM) [Ramb 03] oder Double Data Rate SDRAMs (DDR SDRAM) [Infi 03] zu rechnen sei.

Während der Entwicklungsfokus bei Cache-Speichern primär die Optimierung der Geschwindigkeit ist, liegt er bei Hauptspeichern in der Kapazitätserweiterung bei gleichzeitiger Kostenminimierung. Es ist deshalb interessant, wie die Experten die Entwicklung der Hauptspeicherkapazitäten im Desktopbereich, bei Servern und Hochleistungsrechnern beurteilen. Die heute verfügbaren Technologien (Abschnitt 8.1.1) veranlassen die Experten, im Desktop-Bereich langfristig Hauptspeichergrößen zwischen 80 und 100 Gigabyte zu prognostizieren (siehe Abbildung 8.10). Im Server-Bereich wird mittelfristig eine starke Steigerung bis etwa 20 Terabyte erwartet, in zehn Jahren werden dann Kapazitäten von etwa 60 Terabyte als Standard angesehen, hauptsächlich auf Grund der stark in ihrer Bedeutung anwachsenden multimedialen Anwendungen. Im Hochleistungsbereich wird bis zum Jahr 2013 die Schallmauer von 100 Terabyte durchbrochen sein. Zu erwarten ist in der Folge die Annäherung an die Petabyte-Grenze (1 Petabyte entspricht 1000 Terabytes). Die meisten Experten sehen schon heute für daten-intensive Anwendungen keine ausreichenden Kapazitäten. Langfristig erwartete Anwendungen (z.B. im Bereich Realsimulation) werden daher den Bedarf an Hauptspeicherkapazitäten in den angegebenen Größenordnungen noch verstärken (Abschnitt 8.1.6 und Kapitel 9).

Wie sich die Entwicklungen der letzten Jahre auf die Prognosen ausgewirkt haben, läßt sich an den Abschätzungen der zu erwartenden Hauptspeicherkapazitäten im Vergleich zur Vorgängerstudie gut ablesen: Langfristig rechnen die Experten jetzt mit einer Hauptspeichergröße im Desktop-Bereich, die das fünffache dessen beträgt, was noch vor drei Jahren prognostiziert wurde. Im Server-Bereich wird das 60-fache angenommen, im Hochleistungsbereich das 25-fache. Weiterhin bleibt festzuhalten, dass in allen Bereichen die Experten der Wissenschaft die Entwicklung sehr viel optimistischer sehen als die Industrievertreter, insbesondere im Hochleistungs- und Server-Bereich, wo die Industrie nur moderate Zuwächse (in der Größenordnung vergleichbar denen der Vorgängerstudie) annimmt.



CACHES: Cache-Speicher werden in 5 Jahren eine durchschnittliche Größe von etwa 60 Megabyte besitzen, in 10 Jahren ist mit einer durchschnittlichen Größe von etwa 300 Megabyte zu rechnen.

HAUPTSPEICHER-KAPAZITÄTEN: Hauptspeicherkapazitäten werden weiter exponentiell wachsen. In 10 Jahren werden im Desktopbereich fast 100 Gigabyte erwartet. Für den Serverbereich werden dann etwa 60 Terabyte prognostiziert, wobei die Terabyte-Schwelle schon in 2 Jahren fallen soll. Für Hochleistungsrechner werden in 10 Jahren Hauptspeichergrößen von annähernd 0,25 Petabyte vorausgesagt.

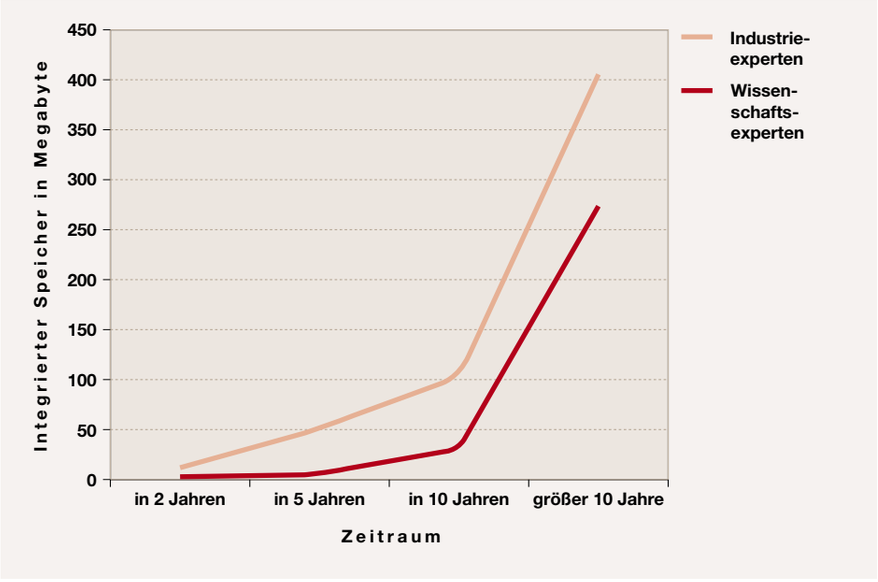



Abbildung 8.8: Entwicklung der im Prozessor integrierten Speicher

OPTISCHE SPEICHERMEDIEN: Eine Ablösung von Festplatten durch DVD-Laufwerke ist langfristig nicht zu erwarten. DVDs werden stattdessen die CD als wechselbaren Informationsträger ersetzen.

SPEICHERTECHNOLOGIEN: Elektronische und optische Speicher werden in 5 Jahren die größte Bedeutung besitzen. Magnetische Speicher werden in 10 Jahren nur noch eine untergeordnet Rolle spielen.

Welche Rolle optische Speichermedien im Rahmen der angesprochenen Speicherhierarchien spielen werden, wurde ebenfalls untersucht (siehe Abbildung 8.9, ②). Die Experten sind sich weitgehend einig, dass herkömmliche Festplattensysteme von optischen DVDs deswegen nicht abgelöst werden, weil Festplatten auch auf lange Sicht eine höhere Kapazität und Geschwindigkeit bei geringen Laufwerkskosten besitzen werden. Stattdessen wird eine Ablösung der CD (Compact Disc) als wechselbarem Informationsträger durch DVDs prognostiziert, dies nicht zuletzt vor dem Hintergrund größerer Kapazitäten [Rath 02]. Vereinzelt wird erwähnt, dass magnetische Festplatten langfristig eher durch Magnetoresistive Random Access Memory (MRAM) [Lamm 02] abgelöst werden könnten, die ein größeres Datenvolumen bei schnellerem Zugriff und geringerer Leistungsaufnahme erlauben als die klassischen elektronischen Speicher.

In der Beurteilung der Bedeutung vorgegebener Speichertechnologien sind sich die Experten aus Wissenschaft und Industrie einig und bestätigen im Wesentlichen die Ergebnisse der Vorgängerstudie (siehe Abbildung 8.11) .

Die heute noch dominierenden magnetischen Speicher werden schon mittelfristig von den optischen Speichern in ihrer Bedeutung verdrängt werden, da wiederbeschreibbare DVDs und entsprechende Recorder magnetische Bandsysteme und Diskettenlaufwerke ersetzen werden. Magneto-optische Alternativen werden zwar mittelfristig an Bedeutung gewinnen, sich aber nicht weiter durchsetzen.

Von einigen Experten wird angemerkt, dass magnetische Speicher durchaus noch an Bedeutung gewinnen könnten, falls den schon erwähnten MRAMs der Durchbruch gelingen sollte. Dann würden Magnetspeicher den gesamten Bereich der elektronischen Speicher übernehmen können.

Da Register, Arbeitsspeicher und Caches auch weiterhin über elektronische Speichertechnologien realisiert werden, wird sich die Bedeutung der elektronischen Speicher auf einem gleichbleibend hohen Niveau einpendeln und nach Meinung der Experten erst durch realisierte Quantenkonzepte zurückgehen.

Langfristig könnten nach Meinung der Experten biologische und quantenmechanische Speicher erkennbar an Bedeutung gewinnen, da dann die Entwicklungs- und Produktionsprozesse beherrschbar sein könnten, ähnlich wie schon im Abschnitt 8.1.2 im Zusammenhang mit Fragestellungen der Prozessorherstellung diskutiert.

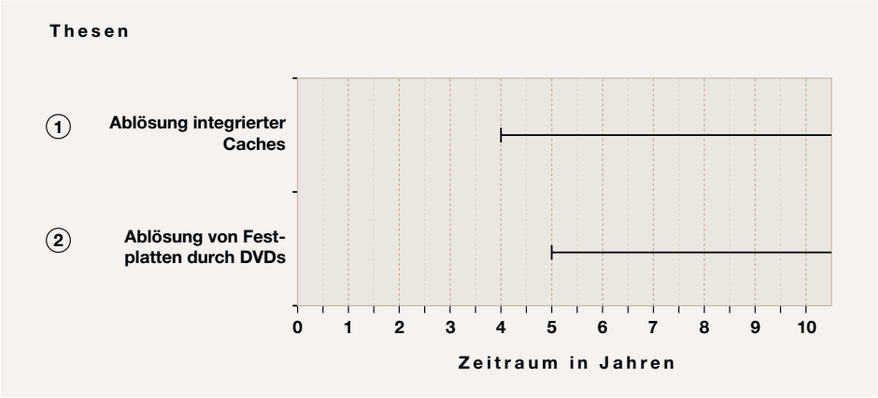



Abbildung 8.9: Ergebnisse der Thesen zur Leistungssteigerung der Speichersysteme

Im Gegensatz zum quantenmechanischen Speicher, der sehr große Datendichten erlaube, würden nach Meinung der Experten biologische Speicher nur geringe Dichten und langsame Zugriffszeiten gestatten. Zukünftige Anwendungsbereiche könnten für diese Varianten ebenfalls kaum angegeben werden. Für biologische Speicher seien, ähnlich wie bei biologischen Prozessoren, Anwendungen vornehmlich im medizinischen Bereich zu erwarten.

Vereinzelt wurden über die beschriebenen Speichertechnologien hinaus Hologrammspeicher [MoPs 99, Stie 99] genannt, die innerhalb der nächsten fünf Jahre die 200-fache Datendichte (bis zu einem Terabyte auf der Fläche einer herkömmlichen CD-ROM) und die 100-fache Geschwindigkeit (bis zu einem Gigabit pro Sekunde) herkömmlicher zweidimensionaler Speicher erreichen können.

### Zusammenfassung

Grundsätzlich bestätigen die Experten, dass die Entwicklung der Speicherkapazitäten auch in den nächsten zehn Jahren exponentiell steigen wird.

- Cache-Speicher werden bis 2008 eine durchschnittliche Größe von etwa 60 Megabyte besitzen, bis 2013 ist mit einer durchschnittlichen Größe von etwa 300 Megabyte zu rechnen.
- Hauptspeicherkapazitäten werden bis 2013 im Desktopbereich fast 100 Gigabyte erreichen, im Serverbereich etwa 60 Terabyte (wobei die Terabyte-Schwelle schon bis 2005 fallen wird) und im Hochleistungsbereich annähernd 0,25 Petabyte.
- Bei den Speichermedien ist eine Ablösung von Festplatten durch DVD-Laufwerke langfristig nicht zu erwarten. DVDs werden stattdessen CDs und Disketten als wechselbare Informationsträger ersetzen.
- Elektronische und optische Speicher werden schon mittelfristig die höchste Bedeutung erlangen, magnetische Speicher werden bis 2013 erheblich an Bedeutung verlieren.

## 8.1.5 Alternative Formen der Mensch–Maschine–Kommunikation

Vom Internet bis zur rechnergestützten Robotik: Neue Informations- und Kommunikations-Technologien besitzen einen erheblichen Einfluß darauf, wie wir zukünftig leben und lernen werden. Insofern wird es zunehmend wichtig, diese Technologien so zu entwerfen, dass sie Menschen in ihren Rollen als Lernende, Forschende oder bei ihrer Arbeit unterstützen. Diesem Aspekt widmet sich die Mensch-Maschine-Schnittstelle [RePo 97]. Im Rahmen dieser Studie wurde untersucht, welche Verfahren zur Datenerfassung, Maschinensteuerung und Informationsdarstellung welche Bedeutung haben werden.

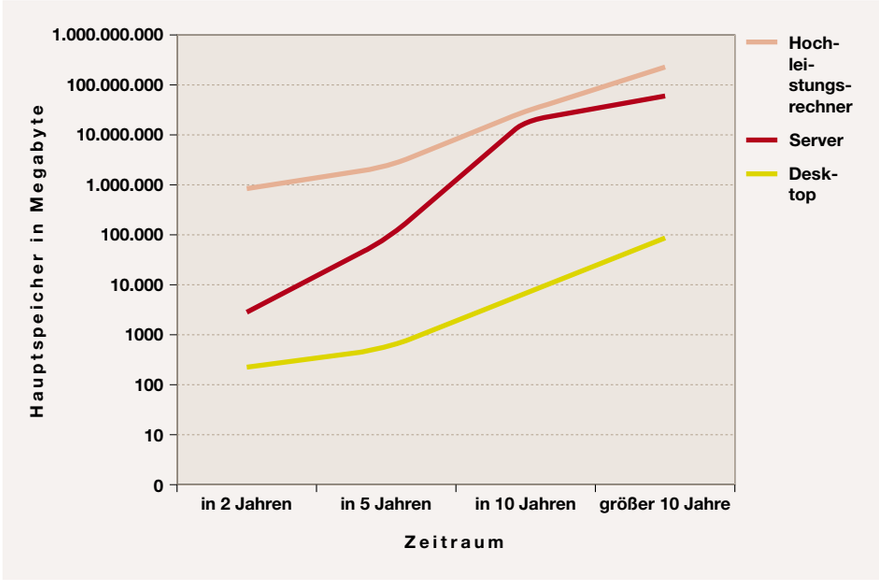



Abbildung 8.10: Entwicklung von Hauptspeicherkapazitäten (in MB)

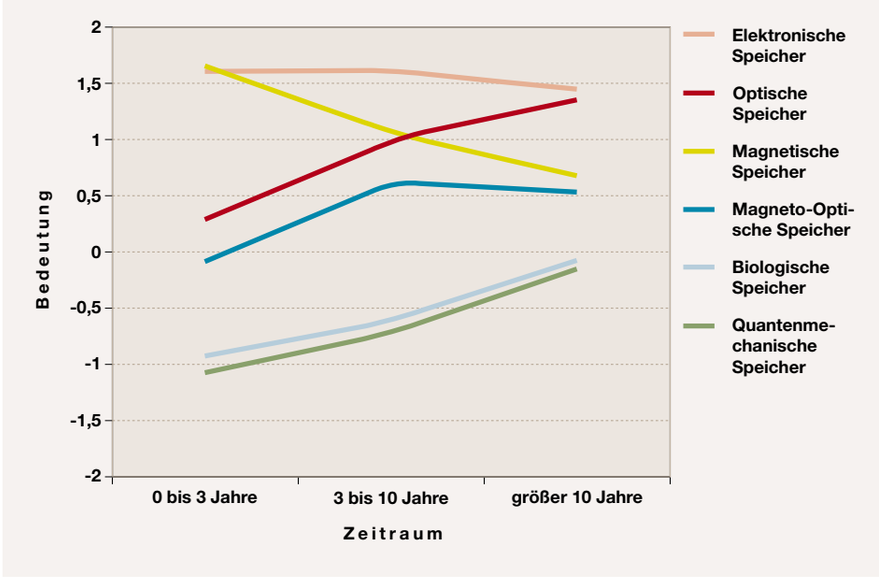



Abbildung 8.11: Bedeutung unterschiedlicher Speichertechnologien

An die derzeit überwiegend eingesetzten Eingabe- und Steuerungsverfahren (Tastatur, Maus) haben wir uns gewöhnt. Dennoch weisen sie Nachteile auf, die ihren Einsatz in bestimmten Umgebungen als nicht ideal erscheinen lassen. Deshalb werden seit einigen Jahren alternative Formen der Datenerfassung und Maschinensteuerung erprobt und inzwischen auch vereinzelt eingesetzt. Handschriftenerkennung und Spracheingabe [Bage 98] sind heute für Menschen mit Körperbehinderungen oder in speziellen Arbeitsumgebungen (z.B am Operationstisch, in Kraftfahrzeugen, im Katastropheneinsatz) wünschenswert. Im Rahmen der Maschinensteuerung sind auch andere Verfahren, die auf der Erkennung von Augenbewegungen, Gestik oder gar Gehirnströmen basieren, durchaus denkbar.

Zur Darstellung von Informationen werden heute vielfach CRTn (Cathode Ray Tube) und LCDe (Liquid Crystal Display) [Kuhl 99] eingesetzt. Die Experten wurden nach der zukünftigen Bedeutung dieser und anderer Ausgabemedien, wie LDTen (Laser Display Technology) [Siet 99] und DMD-Bildschirmen (Digital Mirror Device) [Texa 99] befragt.

## Ergebnisse

Langfristig wird die Tastatureingabe als klassisches Datenerfassungsverfahren nach Meinung der Experten an Bedeutung verlieren. Zwar sei die heutige Vormachtstellung der Tastatur zur Eingabe von Daten und Texten unbestritten, doch schon mittelfristig werde die Spracheingabe eine ähnliche Bedeutung besitzen. Dieses Ergebnis wird in Abbildung 8.12 verdeutlicht. Demnach wird die Tastatureingabe langfristig sogar nur einen ähnlichen Stellenwert besitzen wie die Datenerfassung per Handschriftenerkennung oder die Touchscreens heute. Die Spracherkennung wird dagegen nach Meinung der Experten die Tastatur als Standardwerkzeug zur Datenerfassung in ihrer Bedeutung ablösen und zukünftig zur wichtigsten Schnittstelle. Handschriftenerkennung wird zwar als die universellere Alternative zur Spracherkennung genannt, es wird aber davon ausgegangen, dass sie eher in Spezialbereichen (z.B. zur Eingabe von Informationen in elektronische Kalender) zum Einsatz kommen wird. Als weiteres Anwendungsgebiet wird Digital Ink im Zusammenhang mit Tablet PCs [Micr 02a] genannt. Tablet PCs besitzen Active Digitizer Screens, die eine handschriftliche Texteingabe oder den Entwurf von Freihandzeichnungen direkt über einen Digital Pen erlauben. Touchscreens erlauben die Eingabe über ein berührungssensitives Display. Ihnen wird, außer in Spezialbereichen (z.B. Maschinenwartung, Point-of-Interest-Displays), insgesamt wenig Bedeutung beigemessen. Vereinzelt werden als alternative Datenerfassungsverfahren auch Sensoren für Geräusche, Gerüche und Gestiken bzw. Mimiken sowie Scanner mit intelligenter Texterkennungs-Software (Optical Character Recognition) genannt.

Erwartungsgemäß ergeben sich für die Instrumente zur Maschinensteuerung ähnliche Beobachtungen wie bei den Verfahren zur Dateneingabe (siehe Abbildung 8.13). Die heute dominierenden Werkzeuge wie Tastatur und Maus werden schon mittelfristig an Bedeutung verlieren und durch Sprachsteuerungen abgelöst, die langfristig das vorherrschende Werkzeug sein werden und denen deshalb in den nächsten Jahren eine Schlüsselrolle zukommen wird. Voraussetzung sei nach Meinung der Experten allerdings eine zuverlässige Spracherkennung. In bestimmten Fällen, z.B. für komplizierte Steuerungen, werde weiterhin die Tastatur eingesetzt werden. Für Spezialanwendungen, bei denen Maus oder Tastatur wenig effizient seien, wie z.B. zur Haussteuerung, in Verkehrssituationen oder für Menschen mit Körperbehinderungen, müsse nach Ansicht der Experten die Bedeutung der Spracheingabe noch wesentlich höher eingestuft werden.

Die Bedeutung von Touchscreens zur Maschinensteuerung wird von den Befragten durchgehend als relativ gering eingestuft. Nach Ansicht der Experten stellen Steuerungssysteme mit komplexen Menüstrukturen (z.B. Point-of-Information, Point-of-Sales) allerdings ein ideales Einsatzgebiet für Touchscreens dar. Verfahren wie die Messung von Augenbewegungen, Gestiken und Gehirnströmen, besitzen kurz- bis mittelfristig keine Bedeutung. Langfristig jedoch rechnen vor allem die Experten aus der Wissenschaft mit einem leichten Bedeutungszuwachs. Danach könne Augenbewegung als Zusatz zur Sprachein-


DATENERFASSUNGS-VERFAHREN: Die Datenerfassung wird in 10 Jahren in erster Linie durch Spracheingabe und Handschriftenerkennung erfolgen. Die klassische Tastatureingabe wird erheblich an Bedeutung verlieren.

MASCHINENSTEUERUNG: Die Spracheingabe wird die heute dominierende Steuerung durch Maus und Tastatur in 10 Jahren abgelöst haben.

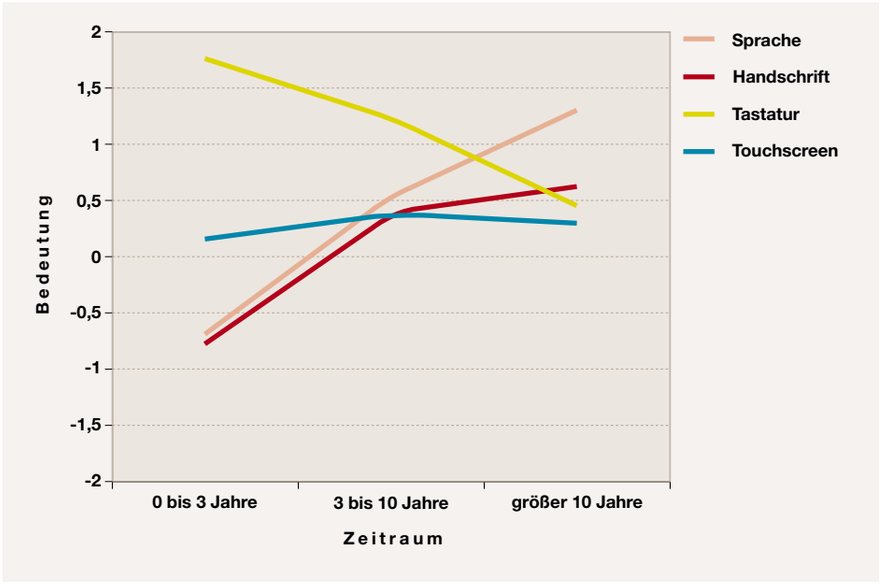



Abbildung 8.12: Bedeutung von Datenerfassungsverfahren

DARSTELLUNG VON INFORMATIONEN: Herkömmliche Röhrenmonitore (CRT) werden in 5 Jahren von Flüssig-Kristall-Bildschirmen (LCD) nahezu vollständig verdrängt sein, in 10 Jahren werden selbst LDTs und DMDs von größerer Bedeutung sein als CRTs.

gabe sowie als Ersatz für die Eingabe mit der Maus genutzt werden, während Gestik nur für einfache Steuerungen, zum Beispiel in Fahrzeugen, Verwendung finden würden, oder in Bereichen, in denen Spracherkennung wegen der hohen Umgebungsgeräusche nicht oder nur unzureichend angewendet werden kann (Flughäfen, Bahnhöfe, Produktionshallen). Gehirnstrom-Steuerung kann nach Meinung der Experten insbesondere in der Medizin, z.B. zur Prothesensteuerung, in Verbindung mit biologischen Prozessoren (Abschnitt 8.1.1) vorteilhaft sein. Anzumerken ist, dass die Experten aus der Industrie die Bedeutung der Gehirnstrom-Steuerung optimistischer beurteilen als die Wissenschafts-Experten. Vereinzelt wurden sensorische Steuerungsverfahren (z.B. Datenhandschuh) als alternative Möglichkeiten zur exakten Handhabbarkeit, zum Beispiel von Herstellungsprozessen und medizinischen Operationen, erwähnt. Es wurde außerdem vereinzelt darauf hingewiesen, dass sich sensorische Steuerungsverfahren ideal zum Einsatz beim Training von Robotern (Industrieroboter und Operationsroboter in der Medizin) oder der Fernsteuerung und -wartung von Maschinen eignen würde. Ebenfalls angemerkt wurde eine langfristige Bedeutung von kontextbezogenen Verfahren, bei denen sich die Anwendungen zur Maschinensteuerung automatisch an die durch eine geeignete Sensorik erfaßten Informationen zur Einsatz-Umgebung (z.B. Ort, Zeit, Aktivität, Wetter) anpassen kann [ChKo 00]. Insgesamt bestätigen die Experten die Beobachtungen der Vorgängerstudie [SETIK 00].

Die Darstellung von Informationen wird in den nächsten zehn Jahren nach einmütiger Meinung aller Experten überwiegend durch LCDs geschehen, wegen der offensichtlichen Vorteile dieser Technologie (großer Betrachtungswinkel, starker Kontrast, Größe, geringe Abwärme). Die derzeit noch am weitesten verbreiteten CRTn werden schon kurzfristig ihre Bedeutung verlieren. Dies wird, wie in Abbildung 8.14 zu erkennen ist, mittelfristig sogar dazu führen, dass neue Technologien wie LDTen und DMDs, die primär für digitale Kino-Anwendungen, großflächige Werbedarstellungen, holographische Darstellungen und leuchtstarke Beamer Verwendung finden werden, gegenüber Röhren-Monitoren an Bedeutung gewinnen werden, ein Ergebnis, das schon in der Vorgängerstudie prophezeit wurde. Es wird aber angemerkt, dass Patentrechte einer Verbreitung dieser Technologien im Wege stehen könnten.

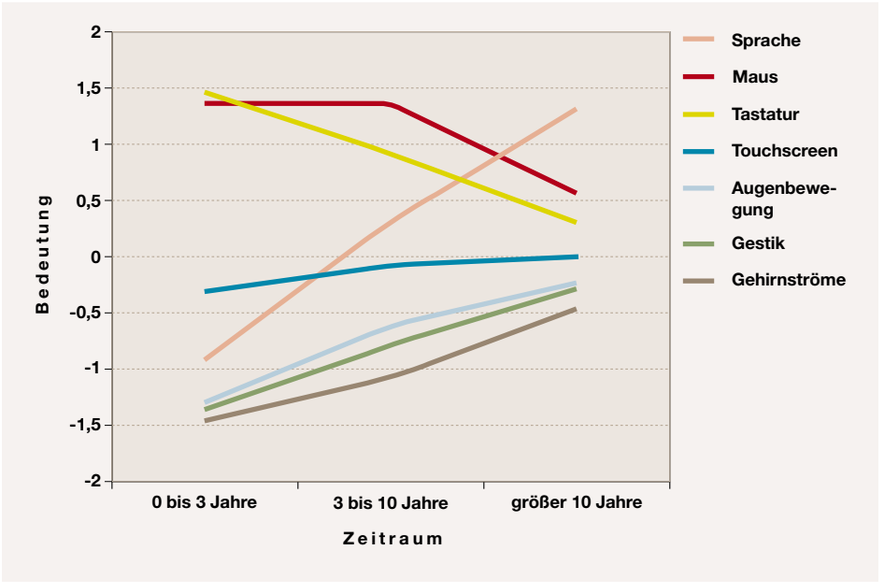



Abbildung 8.13: Bedeutung von Verfahren zur Maschinensteuerung

Vereinzelt wird darüber hinaus auf Plasmadisplays, deren Einsatz vorwiegend im Bereich von Großanzeigen erwartet wird, und auf die, auf selbstleuchtenden Polymeren basierenden, organischen Displays hingewiesen. Letzteren wird eine wachsende Bedeutung vorhergesagt, falls es gelingen sollte, große Diagonalen zu erreichen. Die direkte Einspielung von Daten und Informationen auf die Netzhaut, was im Bereich des Wearable Computing von Bedeutung sein wird, wird – wie in der Vorgängerstudie – als Randnotiz für die ferne Zukunft ebenfalls genannt [MIT 03].

## Zusammenfassung

Mittel- bis langfristig vollzieht sich im Bereich der Mensch-Maschine-Kommunikation ein Umbruch:

- Die Datenerfassung wird bis zum Jahr 2013 in erster Linie durch Spracheingabe und Handschriftenerkennung erfolgen. Die klassische Tastatureingabe wird dagegen erheblich an Bedeutung verlieren.
- Die Maschinensteuerung wird bis zum Jahr 2013 ebenfalls in erster Linie durch Sprache erfolgen, welche die herkömmlichen Verfahren wie Tastatur und Maus abgelöst haben wird.
- Herkömmliche, auf Röhrentechnologie basierende, Monitore werden bis 2006 gegenüber LCD-Bildschirmen keine Bedeutung mehr haben.
- LDT und DMD werden an Bedeutung gewinnen und bis 2006 eine größere Bedeutung besitzen als CRT-Monitore. Derartige Displays werden allerdings nur in Nischen-Bereichen eingesetzt werden.
- Eine gemeinsame Betrachtung der Abbildungen 8.11, 8.12, 8.13 und 8.14 bestätigt noch einmal eindrucksvoll den nahezu parallel stattfindenden Bedeutungsverlust der klassischen Rechnerkomponenten Magnetspeicher, Tastatur, Maus und CRT-Monitor. Der Grund dafür liegt nach Meinung der befragten Experten darin, dass diese Komponenten den hohen Anforderungen zukünftiger Anwendungen nicht mehr gewachsen sein werden.

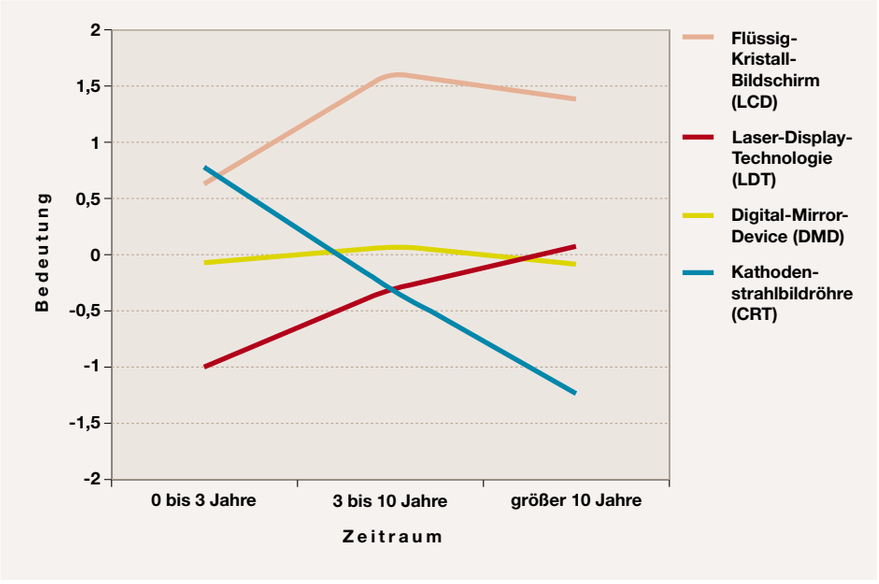



Abbildung 8.14: Bedeutung unterschiedlicher Technologien zur Informationsdarstellung

### 8.1.6 Entwicklung von Parallel– und Hochleistungsrechnern

Heutige und zukünftige Architekturen von Parallel- und Hochleistungsrechnern sind eine logische Konsequenz der fortschreitenden Bemühungen um Miniaturisierung (Abschnitt 8.1.2) und der Evolution der Rechnerarchitekturen. Die wesentlichen technologischen Entwicklungsschritte vom Großrechner der 60er Jahre zum modernen Grid-Computing sind in Abbildung 8.15 zusammengefasst (siehe auch [HePa 03]). Um 1960 wurde Rechnerleistung in der Form von Mainframes, hauptsächlich von IBM, angeboten. Eine Dekade später wurden die ersten kostengünstigeren Minicomputer eingeführt, die einen nicht unerheblichen Marktanteil gewinnen konnten.

In den 80er Jahren wurden nicht nur die ersten Personal Computer (PCs) verkauft, sondern auch die ersten Vektorrechner (z.B. der Firma Cray Research), denen um 1985 massiv-parallele Systeme folgten, um den steigenden Bedarf an Hochleistungskapazität zu decken.

Mit der großflächigen Verbreitung des Internet und des World Wide Web Anfang der 90er Jahre und der gleichzeitigen Verfügbarkeit von leistungsfähigen PCs und Workstations sowie Hochgeschwindigkeitsnetzen, zum Beispiel Gigabit-Ethernet (Kapitel 8.2), war die Möglichkeit global verteilter Anwendungen gegeben. Dies führte zum Durchbruch sogenannter Cluster [Buyy 99], mit denen neue Hochleistungsanwendungen möglich wurden. Mit der weiten Verbreitung von Internet- und Web-Technologien und der Verfügbarkeit vieler preisgünstiger Hochleistungs-Cluster kam zur Jahrtausendwende der Wunsch auf, weltweit verteilte Ressourcen (Computer, Datenbanken, etc.) für die Lösung komplexer Aufgaben zusammenzuschalten. Dies war die Geburtsstunde des Grid-Computings [FoKe 99], das für hochkomplexe Problemlösungen wie Monte Carlo Simulationen zur Vorhersage zukünftiger Ereignisse unter unsicheren Annahmen, Kalibrierungen von Ionisierungskammern, Design von Arzneimitteln oder ökologische Modellierungen verwendet wird.

Die Experten wurden im Rahmen der Studie gebeten, die nächsten Entwicklungsschritte im Hochleistungsbereich zu beurteilen. Dazu sollten sie die Bedeutung der unterschiedlichen Arten von Parallel- und Hochleistungsrechnern langfristig prognostizieren und klären, in welchen Größenordnungen derartige Rechnersysteme zum Einsatz kommen werden und welche Leistung von ihnen langfristig zu erwarten ist.

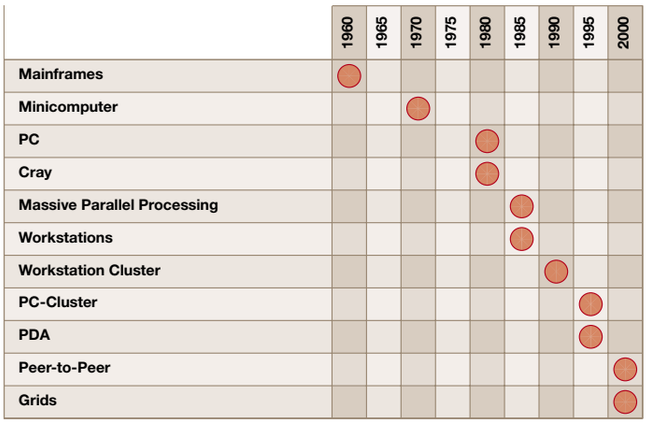



Abbildung 8.15: Technologieentwicklungen der letzten 40 Jahre (aus [Buyy 02])

VERBREITUNG PARALLELER SYSTEME: Parallele Systeme auf der Basis von Standardprozessoren werden in 6 Jahren weit verbreitet sein, in 5 Jahren werden massiv parallele Desktopsysteme auch im kommerziellen Umfeld erwartet. Diese Systeme werden weitgehend mit mehr als acht Knoten ausgestattet sein.

Wie schon in der Vorgängerstudie [SETIK 00] dargestellt, lassen sich nach [TaGo 99, HePa 03] Parallelrechner nach der Anzahl parallel verarbeiteter Operationen und Operanden in die Klassen SIMD (Single Instruction, Multiple Data) und MIMD-Maschinen (Multiple Instruction, Multiple Data) einordnen. Die wichtigsten Arten der ersten Klasse sind Arrayprozessoren und die kommerziell weitaus erfolgreicheren Vektorprozessoren [RePo 97]. Die meisten Systeme mit parallelen Prozessoren fallen in die MIMD-Klasse. Dazu gehören die Mehrprozessorsysteme, in denen die einzelnen Prozessoren über einen gemeinsamen Speicher kommunizieren, und die Mehrrechnersysteme, die im Gegensatz dazu keinen gemeinsamen Speicher besitzen. Mehrprozessorsysteme werden je nach Speicherarchitektur in UMA-Systeme (Uniform Memory Access) und NUMA-Systeme (Non Uniform Memory Access) aufgeteilt. In UMA-Systemen besitzt jede CPU dieselbe Zugriffszeit auf jedes Speichermodul, während bei NUMA-Systemen unterschiedliche Zugriffszeiten aufgrund der Lage der einzelnen Speichermodule entstehen können. Die zwei wesentlichen Kategorien von Mehrrechnersystemen sind massiv-parallele Systeme, d.h. Spezialrechner mit vielen CPUs, die über spezielle Hochgeschwindigkeitsnetze eng gekoppelt sind, und Cluster of Workstations (COW), übliche PCs oder Workstations, die über kommerziell erhältliche Verbindungstechnologien miteinander gekoppelt sind. Rechner innerhalb eines Clusters gehören typischerweise zu *einer* Administrationsdomäne. Mehrrechnersysteme, die verschiedenen Administrationsdomänen angehören, werden auch als Grids bezeichnet.

## Ergebnisse

Abbildung 8.16, ① zeigt, dass nach Meinung der meisten Experten in drei bis fünf Jahren Parallel-Systeme mit mehr als acht Knoten als Serversysteme weit verbreitet sein werden, eine Einschätzung, die gegenüber der Vorgängerstudie [SETIK 00] damit um 3 Jahre nach hinten korrigiert wurde. Typische Anwendungsgebiete für derartige Systeme werden in Bereichen gesehen, in denen Ausfallsicherheit eine große Rolle spielt, z.B. als Webserver, Transaktionsserver bei Datenbanken, im E-Commerce-Bereich oder im Bereich Wissensmanagement (siehe Kapitel 8.3). Voraussetzung hierfür sind allerdings eine adäquate Unterstützung durch geeignete Betriebssysteme (effiziente Lastverteilung), leistungsfähige Bussysteme und eine einfache Bedienbarkeit. Angemerkt werden in diesem Zusammenhang auch die aufkommenden Server Blades [Klip 02], mit denen es möglich sein wird, mehr Server pro Rack zu integrieren. Durchschnittlich zwei Jahre später sehen die Experten eine weite Verbreitung paralleler Systeme auf der Basis von Standardprozessoren (siehe Abbildung 8.16, ②), vorausgesetzt die Kommunikationsbandbreite zwischen CPUs ist signifikant verbesserbar und die Speicherlatenz ist senkbar. Bei der Prognose dieses Zeitraumes sind

die Experten der Industrie allerdings etwas pessimistischer als ihre Kollegen aus der Wissenschaft. Vereinzelt wird darauf hingewiesen, dass in der Industrie ein nicht unwesentliches Maß für den Einsatz von CPUs die Rechenleistung pro Watt aufgenommener Leistung sei und deshalb der Einsatz von Standardprozessoren für Parallelsysteme noch nicht optimal sei (Abschnitt 8.1.1). Schon ein weiteres Jahr später erwarten die Experten eine marktweite Verbreitung von parallelen Desktop-Systemen (siehe Abbildung 8.16, ③), eine Entwicklung, die nach Meinung der Experten zu einer verstärkten Verbreitung von Hochleistungsrechnern im kommerziellen Bereich in etwa fünf Jahren führen wird (siehe Abbildung 8.16, ④).

SPEICHERARCHITEKTUREN FÜR MEHRPROZESSORSYSTEME: NUMA-Architekturen werden in 2 Jahren bedeutender sein als UMA- und NORMA-Architekturen.

ARCHITEKTUREN VON HOCHLEISTUNGSRECHNERN: In 10 Jahren wird Grid-Computing die bedeutendste Hochleistungsarchitektur darstellen, noch vor dem mittelfristig bedeutenderem Cluster-Computing. Die Bedeutung von Vektorrechnern wird erheblich abnehmen.

Speicherarchitekturen für Mehrprozessorsysteme werden sich in Zukunft an der NUMA-Architektur messen lassen müssen (siehe Abbildung 8.17). Wie schon in der Vorgängerstudie zeigt sich bei allen Befragten ein deutlicher Trend von UMA-Architekturen zu NUMA. Das Skalierbarkeitsproblem von UMA ist nach Ansicht der Experten zu groß, um mit Architekturen von mehr als acht Prozessoren umgehen zu können. NUMA hingegen ist beliebig skalierbar und deswegen sowohl zum Bau kleiner als auch sehr großer Systeme einsetzbar. NUMA wird wiederholt als das Zukunftskonzept bezeichnet, wobei allerdings angemerkt wird, dass die tatsächliche Verbreitung von einem geeigneten Programmiermodell (Kapitel 8.4) abhängig sein wird. Zum Vergleich zeigt Abbildung 8.17 noch die Bedeutung von Systemen mit verteiltem Speicher in der NORMA-Architektur (No Remote Memory Access), die häufig bei der Beantwortung dieser Frage als Alternative genannt werden. Die Bedeutungen von NORMA und UMA werden nach Meinung der Experten ähnlich abnehmen. Vereinzelt wurden noch unorganisierte, vernetzte Systeme und COMA-Architekturen (Cache Only Memory Architecture) genannt, die langfristig wegen ihrer Flexibilität an Bedeutung gewinnen könnten.

Abbildung 8.18 fasst die erwartete Bedeutung der unterschiedlichen Architekturen von Hochleistungsrechnern zusammen. Die Experten aus Industrie und Wissenschaft sind sich darin einig, dass Cluster- und Grid-Computing mittel- bis langfristig die dominierenden Architekturen für Hochleistungsrechner darstellen werden, vorausgesetzt die erforderlichen Kommunikationsbandbreiten sind verfügbar. Im Laufe der nächsten zehn Jahre werden die heute noch bedeutenden Vektorrechner stark zurückgehen, aber weiterhin für Anwendungen mit starkem Modellierungscharakter und hohen numerischen Anforderungen (z.B. Crash-Tests, Simulation physikalischer Systeme oder Wetterprognosen) hervorragend eingesetzt werden können. Als Alternative könnten Hochleistungsrechner dienen, die aus heterogenen Vektorkomponenten, Speicherkopplungen und verteilten Speichern bestehen. Nach Meinung der Experten werden Hochleistungsrechner dieser Art in etwa drei Jahren verfügbar sein (siehe Abbildung 8.19, ②), eine sehr viel pessimistischere Prognose als noch vor drei Jahren [SETIK 00], wo die Experten die Verfügbarkeit für das Jahr 2001 in Aussicht stellten. Als problematisch sehen die Experten in diesem Zusammenhang den derzeitigen Mangel an Programmiermodellen bzw. geeigneten Entwicklungswerkzeugen (siehe Kapitel 8.4) wie z.B. speziellen Compilern, die als Voraussetzungen für einen verbreiteten Einsatz angegeben werden. Vereinzelt wird angemerkt, dass auch unorganisierte, vernetzte heterogene Systeme an Bedeutung gewinnen können, Anwendungsszenarios werden allerdings nicht gegeben.

Die Experten sind sich bei der Beantwortung der Frage, wann eine effiziente E/A (Ein-/Ausgabe) zum dominierenden Faktor bei Hochleistungsrechnern werden wird, nicht einig: Während ein Teil der befragten Experten, hauptsächlich aus der Industrie, meint, dass dies schon heute der Fall sei, geht ein anderer Teil davon aus, dass dieser Fall erst mittelfristig eintreten werde (siehe Abbildung 8.19, ①). Im Gegensatz zu dieser Einschätzung steht die Prognose der Vorgängerstudie [SETIK 00], die davon ausging, dass E/A schon im Jahr 2003 zum dominierenden Faktor wird. Multithreading (siehe Abbildung 8.19, ③) als ein Parallelisierungsmechanismus, bei dem einem Betriebssystem mehrere virtuelle Prozessoren zur Verfügung gestellt werden (Abschnitt 8.1.2), wird von den Experten mehrheitlich mittelfristig in typischen Serverumgebungen erwartet.

Obwohl die Experten von einer weiteren Steigerung der Leistungsfähigkeit von

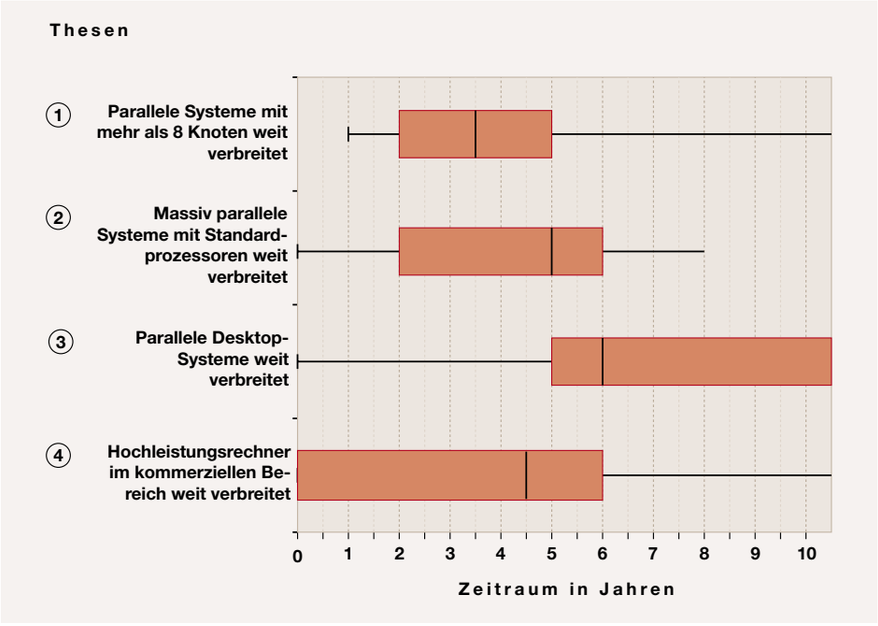



Abbildung 8.16: Ergebnisse der Thesen zur Entwicklung von Parallelrechnern

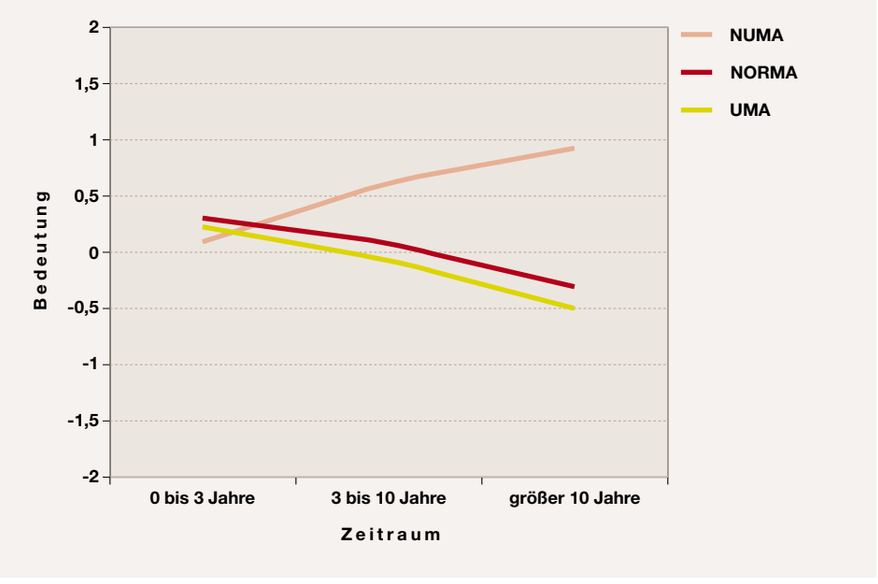



Abbildung 8.17: Bedeutung unterschiedlicher Speicherarchitekturen für Mehrprozessorsysteme

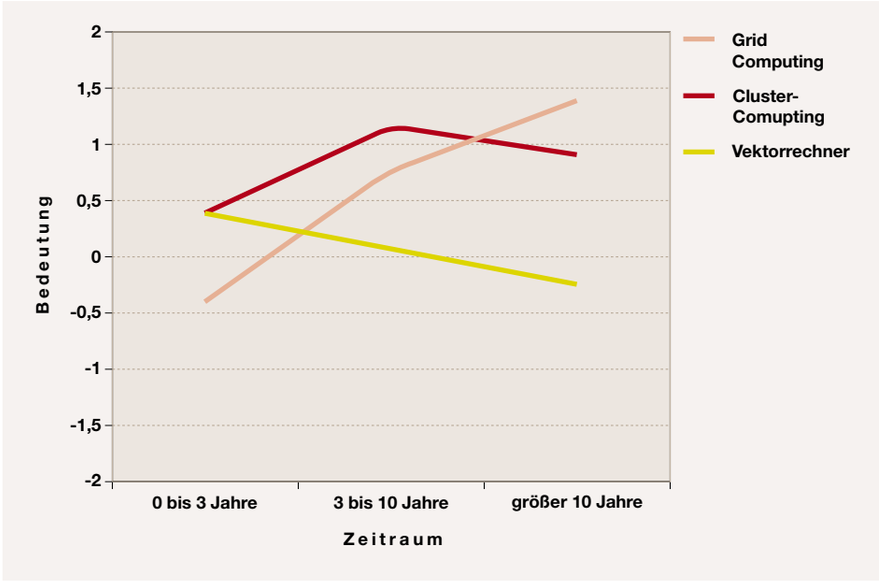



Abbildung 8.18: Bedeutung unterschiedlicher Architekturen für Hochleistungsrechner

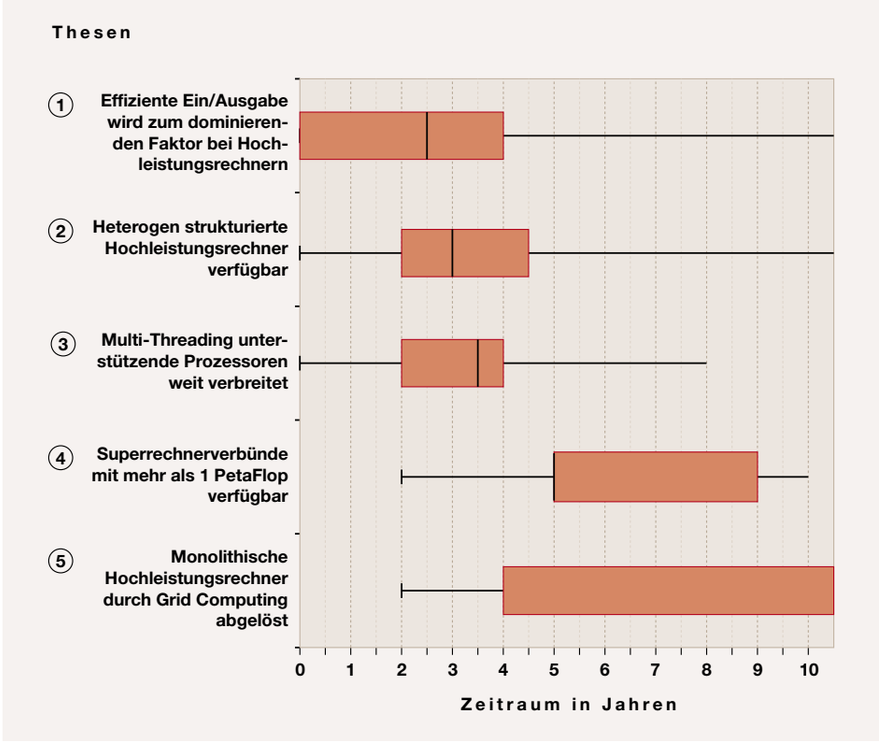



Abbildung 8.19: Ergebnisse der Thesen zur Entwicklung von Hochleistungsrechnern

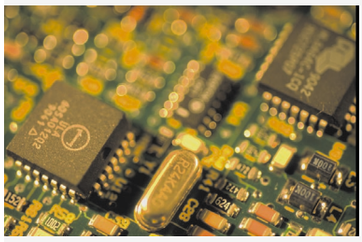
Hochleistungsrechnern ausgehen, ist nicht zu erwarten, dass Superrechnerverbünde mit einer Rechenleistung von mehr als 1 PetaFlop vor Ablauf der nächsten fünf Jahre zur Verfügung stehen werden (siehe Abbildung 8.19, ④), eine Prognose, die sich mit der entsprechenden Aussage der Vorgängerstudie [SETIK 00] deckt. Die Experten aus der Industrie sehen dies allerdings mit einer Erwartung von sechs Jahren etwas pessimistischer als die Experten aus der Wissenschaft. Anwendungen derartiger Höchstleistungsrechner werden z.B. im militärischen Bereich, in der Gentechnik, in der Materialwissenschaft oder für wissenschaftliche Simulationen wie virtuelle Atomtests oder Klimasimulationen gesehen. Grundlegende Voraussetzungen hierfür seien aber Netze zwischen den einzelnen Rechnern, die über extrem hohe Bandbreiten (Abschnitt 8.2.2) bei geringen Latenzzeiten verfügen müssten sowie eine Software-Infrastruktur, die eine Nutzung solcher Verbünde überhaupt erst ermöglichen würde. Vereinzelt wird angemerkt, dass derartige Verbünde Kopplungen von circa einer Million CPUs erlauben müssten.

Abbildung 8.19, ⑤ spiegelt die Uneinigkeit der Experten bei der Beurteilung der Ablösung heute üblicher, monolithischer Hochleistungsrechner durch Grid-Computing-Konzepte wider. Eine Expertengruppe sieht eine Ablösung in etwa sechs Jahren, unter der Voraussetzung schneller Kommunikationkanäle und entsprechender Infrastrukturdienste. Eine gleichstarke andere Gruppe sieht auch langfristig keine Ablösung. Stattdessen müssten heutige und zukünftige Hochleistungsrechner im Rahmen des Grid-Computing-Paradigmas als Teil des Grids betrachtet werden. Die hervorragende Bedeutung des Grid-Computing ist allerdings auch für diese Expertengruppe unbestritten (siehe Abbildung 8.18).

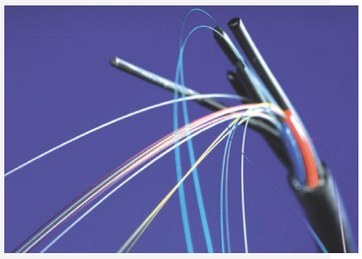
## Zusammenfassung

Die Ergebnisse der Befragung manifestieren einen bevorstehenden Paradigmenwechsel im Bereich paralleler und Hochleistungsrechner:

- Parallele und Hochleistungssysteme auf der Basis von Standardprozessoren werden langfristig ebenso weit verbreitet sein wie massiv parallele Desktopsysteme, auch im kommerziellen Umfeld.
- NUMA-Architekturen werden schon mittelfristig UMA- und NORMA-Architekturen in der Bedeutung abgelöst haben.
- 2013 wird Grid-Computing die bedeutendste Hochleistungsarchitektur darstellen, noch vor Cluster-Computing, das nur mittelfristig eine höhere Bedeutung besitzt. Die Bedeutung von Vektorrechnern wird erheblich abnehmen.
- 2008 werden Höchstleistungsrechner durch den Verbund vieler Einzelrechner mit einer aggregierten Rechenleistung von mehr als einem PetaFlop zur Verfügung stehen.



SUPERRECHNERVERBÜNDE: Mit Höchstleistungsrechnern, die über mehr als 1 PetaFlop Rechenleistung verfügen, ist durch den Verbund vieler Einzelrechner innerhalb der nächsten 5 Jahre zu rechnen.



## 8.2 Netze und Kommunikation

Der in allen Bereichen wahrnehmbare Wandel von der Industriegesellschaft zur Informationsgesellschaft ist einerseits treibende Karft des immer weiter fortschreitenden Einsatzes der Telekommunikation und andereseits erst durch die Entwicklung entsprechender Technologien umsetzbar geworden. Durch den weltumspannenden Austausch von Informationen jeglicher Art ist die, besonders im wirtschaftlichen Umfeld wahrnehmbare, Globalisierung erst ermöglicht worden. Im weithin verwendeten Begriff der Informations- und Kommunikations-Systeme (IuK) drückt sich bereits der Stellenwert der Telekommunikation bei der Informationsverarbeitung aus.

In diesem Kapitel der Studie werden die vielfältigen Entwicklungen im Bereich der Kommunikationsnetze und ihrer Anwendungen analysiert. Dabei werden sowohl die Trends bei neu entstehenden Technologien als auch beim Einsatz neuer Betriebskonzepte beleuchtet. Die Darstellung orientiert sich dabei an den in Abschnitt 6 eingeführten, übergreifenden Trends, deren Ausprägungen im Bereich der Netze und Kommunikation im Folgenden detailliert dargestellt werden. Der dabei aufgezeigte Zusammenhang zwischen den übergreifenden Trends und ihrer jeweiligen Ausprägung in Entwicklungen im Bereich der Netze und der Kommunikation ist nochmals übersichtlich in Tabelle 8.2 veranschaulicht. Aus dieser Tabelle ist auch ersichtlich, wie sich die Ausprägungen der übergreifenden Trends gegenüber der Vorgängerstudie [SETIK 00] aus dem Jahr 2000 verändert haben.

**Automatisierung und Vereinfachung** (Abschnitt 6.1): In vielen Bereichen der Telekommunikation ist ein Zusammenwachsen bestehender Technologien zu beobachten. Diese Konvergenz der Netze, wie sie in den Abschnitten 8.2.3 und 8.2.4 analysiert wird, ist durch den übergreifenden Trend zur Automatisierung und Vereinfachung getrieben. Durch die damit einhergehende Reduktion der Technologievielfalt ist ein einfacherer Betrieb und langfristig auch eine einfachere Installation möglich. Auch die Dienst- und Komponentenorientierung (Abschnitt 8.2.5) trägt aus Nutzersicht zur Automatisierung und Vereinfachung bei. Mit der Entwicklung flexibel programmierbarer Netze wird versucht, skalierbare Lösungen zum Aufbau komplexer Netze zu entwickeln, da bei der Umsetzung dieses Ansatzes viele Funktionalitäten in Software realisiert werden können. Die Entwicklungen im Umfeld dieser Technologie werden im Abschnitt 8.2.6 untersucht.

**Dienst- und Komponentenorientierung** (Abschnitt 6.2): Dieser übergreifende Trend schlägt sich direkt als Paradigma im Bereich der Kommunikation nieder und wird entsprechend in einem eigenen Abschnitt (8.2.5) untersucht. Von der konsequenten Umsetzung des Dienstgedankens werden eine Vereinfachung bei der Dienstnutzung durch den Endkunden sowie bessere Möglichkeiten zum Leistungsvergleich erwartet [HAN 99]. Ebenso zeigt sich der Gedanke der Dienstorientierung bei der Umsetzung von Sicherheitsdiensten, wie sie exemplarisch im Abschnitt 8.2.1 und 8.2.8 beschrieben werden. Dort wird auch auf neue Fragestellungen bezüglich der Sicherheit bei der Umsetzung des Dienstgedankens, beispielsweise durch aktive Inhalte, eingegangen.

**Globalisierung und Wettbewerb** (Abschnitt 6.3): Die in den Abschnitten 8.2.3 und 8.2.4 beschriebene Konvergenz im Bereich der Netze ist eine Folge und zugleich eine Triebfeder der immer weiter fortschreitenden Globalisierung und des intensivierten Wettbewerbs. Die Entwicklungen beim Einsatz des weltweit standardisierten UMTS (Universal Mobile Telecommunication System) [KAL+ 01], wie sie im Abschnitt 8.2.7 beschrieben werden, zeigen die Umsetzung dieses übergreifenden Trends an einer konkreten Technologie.

**Integration und Standardisierung** (Abschnitt 6.4): Der Einsatz von Technologien wie UMTS (Abschnitt 8.2.7) ist durch Integration und Standardisierung erst möglich geworden. Ebenso wird die Konvergenz der Netze (Abschnitte 8.2.3 und 8.2.4) durch die Standardisierung erheblich erleichtert. Die Erschließung des neuen Anwendungsfelds Mobile Computing [Roth 02] in den letzten Jahren (Abschnitt 8.2.7), ist ebenfalls erst durch vermehrte Integration und Standardisierung ermöglicht worden, Da sämtliche Anwendungen dort die reibungslose, und da-

mit standardisierte, Zusammenarbeit unterschiedlichster Geräte erfordern.

**Kapazitäts- und Leistungssteigerung** (Abschnitt 6.5): Viele Entwicklungen im Bereich der Kommunikationsnetze sind erst durch Steigerung der Hardwareleistung und die damit einhergehende Erhöhung der Übertragungskapazitäten (Abschnitt 8.2.2) ermöglicht worden. Die immer wieder umgesetzte Vereinheitlichung von Technologien ist hier ebenso zu nennen, wie die Dienstorientierung (Abschnitt 8.2.5) und Anwendungen im Bereich des Mobile Computing (Abschnitt 8.2.7). Weiterhin ermöglicht die fortschreitende Leistungssteigerung die Entwicklung leistungsfähigerer Sicherheitssysteme (Abschnitt 8.2.1).

**Konvergenz** (Abschnitt 6.6): Wie bereits mehrfach beschrieben, zeigt sich der übergreifende Trend zur Konvergenz in vielen Bereichen der Kommunikationsnetze. Natürlicher Weise direkt beim Zusammenwachsen bestehender Technologien aber auch bei der Entwicklung neuer Techniken, wie der flexibel programmierbaren Netze (8.2.6), die durch Virtualisierung von Funktionalitäten eine langfristige Konvergenz ermöglichen. Der Einsatz von Infrastrukturen für das Mobile Computing (Abschnitt 8.2.7) zwingt, auf Grund der hohen Investitionskosten, zur Vereinheitlichung, also zur Konvergenz der Technologien und führt damit auch zu neuen Fragestellungen im Bereich der Sicherheit mobiler Systeme (Abschnitt 8.2.8).

**Miniaturisierung** (Abschnitt 6.7): Leistungssteigerung bei gleichbleibendem Volumen und Gewicht und damit Mobilität sind die direkte Konsequenz der zunehmenden Miniaturisierung. Damit lassen sich sowohl leistungsfähigere Koppelkomponenten als auch mobile Endgeräte mit immer höherer Leistung realisieren. Entsprechend spiegelt sich der übergreifende Trend zur Miniaturisierung sowohl beim Zusammenwachsen der Netze als auch im Anwendungsfeld des Mobile Computing (Abschnitt 8.2.7 und 8.2.7) wider.

**Mobilität** (Abschnitt 6.8): Erst in den letzten Jahren wird besonders von Endkunden eine zunehmende Mobilität bei der Inanspruchnahme von Kommunikationsleistungen gefordert. Somit hat sich auch die Nutzung mobiler Endgeräte (Abschnitt 8.2.7 und 8.2.7) enorm verstärkt. Gleichzeitig erfordert die Kommunikation zwischen mobilen Systemen auch den Aufbau bzw. die Vereinheitlichung von Netzen.

**Vernetzung und Flexibilisierung** (Abschnitt 6.9): Grundsätzlich lässt sich der Trend zur Vernetzung und Flexibilisierung in vielen Bereichen beobachten. Besonders ausgeprägt ist er im Bereich des mobile Computings (Abschnitt 8.2.7) feststellbar. Besonders mit der zunehmenden Vernetzung mobiler Endsysteme treten neue Sicherheitsfragestellungen auf (Abschnitt 8.2.8). Die geforderte Flexibilisierung wirkt aber auch als Triebfeder für die zunehmende Konvergenz der Netze (Abschnitte 8.2.3 und 8.2.4) und die Entwicklung neuer Konzepte, welche diese Flexibilisierung unterstützen, wie beispielsweise die in Abschnitt 8.2.5 beschriebene Dienstorientierung.

**Verteilung und Dezentralisierung** (Abschnitt 6.10): Kommunikationsnetze unterstützen an sich die Verteilung und Dezentralisierung, weil sie den Austausch von Informationen über nahezu beliebige Entfernungen ermöglichen. Im Bereich der Anwendungen von Kommunikationsinfrastrukturen wird eben diese Verteilung und Dezentralisierung immer stärker nachgefragt, so dass die Konvergenzbestrebungen zur Leistungssteigerung ebenso wie die vermehrte Dienstorientierung (Abschnitt 8.2.5) als Konsequenz dieses übergreifenden Trends betrachtet werden müssen. Bei der Absicherung von Netzen ergeben sich durch die Dezentralisierung sowohl neue technische Möglichkeiten zur Implementierung komplexer Systeme, als auch neue Sicherheitsfragestellungen, welche die Verteilung als solche betreffen (Abschnitt 8.2.1).

**Virtualisierung** (Abschnitt 6.11): Bereits der Austausch von Informationen ohne Bindung an ein reales Gut setzt den Trend zur Virtualisierung um. Innerhalb des Bereichs der Kommunikationsnetze findet dieser Trend besonders bei der Entwicklung neuer Konzepte, die eine einfache Bewältigung komplexer Umgebungen ermöglichen sollen, wie Dienstorientierung (Abschnitt 8.2.5) oder flexibel programmierbare Netze (Abschnitt 8.2.6), seinen Niederschlag. Die Vereinheitlichung bestehender Strukturen ist aber ohne fortschreitenden Virtualisierung nicht denkbar.

| Übergreifende Trends | Ausprägung im Bereich Netze und Kommunikation: Internetsicherheit | Erhöhung der Übertragungskapazitäten | Konvergenz der Transportsysteme - zunehmende Vernetzung | Konvergenz im Telekommunikationsbereich | Konvergenz von Sprach- und Datenkommunikation | Dienstorientierung, garantierte Dienstgüte und Dienstplattformen | Flexible und programmierbare Netze | Mobile Computing | Einsatz von UMTS | Sicherheit in drahtlosen Netzen | 2003 | 2000 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Automatisierung und Vereinfachung | | | ● | ● | ● | ● | ● | | | | ◔ | ◕ |
| Dienst und Komponentenorientierung | ● | | | | | ● | | | | ● | ◔ | ◕ |
| Globalisierung und Wettbewerb | | | ● | ● | ● | ● | | | ● | | ◕ | ◑ |
| Integration und Standardisierung | | | ● | | ● | ● | ● | ● | ● | | ◕ | ◕ |
| Kapazitäts- und Leistungssteigerung | ● | ● | ● | | ● | ● | | ● | ● | | ◕ | ◔ |
| Konvergenz | | | ● | ● | ● | ● | ● | ● | ● | ● | ◕ | ◕ |
| Miniaturisierung | | | ● | | ● | | | ● | | | ◔ | ○ |
| Mobilität | | | ● | | ● | | | ● | ● | | ◑ | ◔ |
| Vernetzung und Flexibilisierung | | | ● | | ● | ● | | ● | ● | ● | ◕ | ◔ |
| Verteilung und Dezentralisierung | ● | ● | ● | | ● | ● | | | | | ◕ | ○ |
| Virtualisierung | | | ● | ● | ● | ● | ● | | | | ◕ | ◔ |

Tabelle 8.2: Ausprägungen übergreifender Trends im Technologiefeld Netze und Kommunikation

In den folgenden Abschnitten werden die vielfältigen, bereits angeklungenen, Entwicklungen im Bereich der Kommunikationsnetze im Detail untersucht. Dazu werden zunächst Aspekte der Kommunikationssicherheit am Beispiel des Internets diskutiert (Abschnitt 8.2.1). Weiter hin werden die Auswirkungen und Entwicklungen bei der Erhöhung der Übertragungskapazitäten in Netzen diskutiert (Abschnitt 8.2.2). Daran anschließend wird die Ergebnisse der Befragung über die in allen Anwendungsbereichen zunehmende Vernetzung dargestellt (Abschnitt 8.2.3). Eine detaillierte Untersuchung über die Konvergenz von Netzen und Endgeräten schließt sich an (Abschnitt 8.2.4) und ermöglicht anschließend die Evaluation neuer Konzepte im Bereich der Netze wie Dienstorientierung (Abschnitt 8.2.5) und flexibel programmierbarer (Abschnitt 8.2.6) Netze. Am Ende des Kapitels Netze und Kommunikation werden die Entwicklungen bei der mobilen Kommunikation ausführlich, mit einem eigenen Abschnit über Sicherheitsaspekte in diesem Anwendungsfeld, untersucht (Abschnitte 8.2.7 und 8.2.8).

## 8.2.1 Internetsicherheit

Das Internet als weltweiter Zusammenschluss verteilter Computersysteme ist aus dem beruflichen und privaten Alltag kaum noch wegzudenken. Aufgrund der vielfältigen Gefährdungen, die mit der Internet-Nutzung einhergehen können, gewinnt die Frage nach der sicheren Internet-Nutzung zunehmend an Bedeutung. Innerhalb dieses Abschnitts sollen aus diesem Grund Technologien untersucht werden, die eine sichere Nutzung

des Internet und anderer auf der Internet-Technologie basierender Netze gewährleisten können.

#### 8.2.1.1 Sicherheits-Gateways

Unter einem Sicherheits-Gateway oder einer Firewall wird hier ein IT-System verstanden, das den Übergang zwischen zwei Rechnernetzen absichert. Ziel dieser Maßnahme ist es beispielsweise, das interne Netz vor Angriffen aus dem externen Netz zu schützen sowie unerwünschten Datenabfluss vom internen in das externe Netz zu verhindern. Sicherheitsgateways können auch lokal auf Arbeitsplatzrechnern laufen und deren Kommunikationsschnittstelle sichern, beispielsweise bei sogenannten Personal-Firewalls.

Der Schutz interner Netze wird erreicht, indem unsichere IP-Adressen und Dienste durch Sicherheits-Gateways abgeschaltet oder durch weitere Maßnahmen abgesichert werden (z.B. Verschlüsselung). Zugriffskontrolle und Auditing sorgen zusätzlich dafür, dass das Prinzip der minimalen Rechte durchgesetzt wird und Angriffe durch entsprechende Protokollierung erkannt werden.

##### Ergebnisse

Derzeit ordnen die Experten einfachen Paketfiltern die größte Bedeutung bei der Implementierung von Sicherheits-Gateways zu (vgl. Abbildung 8.20). Allerdings wird die Bedeutung als rückläufig angesehen; in zehn Jahren dürften andere Verfahren, beispielsweise dynamische Filter mit Zustandsfunktionen (Stateful-Inspection) Paketfilter in der Bedeutung überholt haben. Langfristig stehen komplexe Richtlinien dem Einsatz von Paketfiltern entgegen. Es wird damit gerechnet, dass Paketfilter auch in Zukunft noch eine wichtige Grundkomponente bei Firewalls darstellen werden und sowohl in Unternehmen zur Erstabschottung, als auch im Privatbereich zum Einsatz kommen.

In den nächsten drei Jahren wird nach Ansicht der Befragten die Bedeutung von Applikationsfiltern stark zunehmen und auf einem hohen Niveau verbleiben. Diese Systeme sind leistungsfähiger, komplexer und effizienter, oftmals aber nur für bestimmte Klassen von Kommunikationsverbindungen einsetzbar. Außerdem sind detailliertere Richtlinien erforderlich. Teilweise wird die Ansicht vertreten, dass zentral administrierte Sandbox-Umgebungen auf den Endrechnern der Nutzer Applikationsfilter überflüssig machen oder die Behandlung von Sicherheit auf die Anwendungsschicht des OSI-Schichtenmodells verschoben werden könnte. Hauptanwendungsbereiche für Applikationsfilter werden bei Unternehmensfirewalls gesehen.

Nach Ansicht der Experten werden Screened Subnets in Zukunft an Bedeutung gewinnen. Bei einem Screened Subnet handelt es sich um ein Teilnetz zwischen einem zu schützenden Netz und einem externen Netz, in dem Firewall-Komponenten für die Kontrolle der Verbindungen und Pakete sorgen. Dieses Teilnetz dient nur zum Transport der Pakete ins bzw. aus dem Internet. Ein Screened Subnet besteht aus einem Application-Gateway und einem oder zwei Paketfiltern. Die Paketfilter befinden sich vor und/oder hinter dem Gateway und bilden mit diesem ein Teilnetz. Die Filterregeln werden so gestaltet, dass jede Verbindung, von innen oder außen, über das Gateway gehen muss.

Die Anwendungsbereiche von Screened Subnets werden in Unternehmensnetzen, in Behörden und bei Hochsicherheitsanwendungen gesehen. Bei langfristig sinkenden Kosten und höherer Effizienz ist auch eine Ablösung von Applikationsfiltern durch Screened Subnet denkbar. Die Befragten erhoffen sich zukünftig weitere Technologien, beispielsweise Systeme mit Content-Checking-Fähigkeiten sowie deutlich mehr Systeme für mobile Netze.

Die Bedeutung von Firewall-Systemen vor dem Hintergrund der zunehmenden Nutzung kryptographischer Verfahren durch Nutzer und der damit verbundenen Gefahr der „Tunnelung" von Firewalls wird nach Aussage der Befragten langfristig leicht rückläufig sein (vgl. Abbildung 8.21).

Einige der Befragten prognostizieren eine zukünftige Einschränkung der Tunneling-Möglichkeiten durch Firewall-Richtlinien. Andere erwarten das Herausbilden neuer Firewalltechnologien, die Sicherheit auch bei z.B. Tunneln bieten bzw. sehen die Notwendigkeit einer zunehmenden Verlagerung von Firewallfunktionen in die Endsysteme.

APPLIKATIONSFILTER: In spätestens 3 Jahren werden Applikationsfilter die einfachen Paketfilter als bedeutsamste Sicherheits-Gateways abgelöst haben. Langfristig werden auch überwachte Applikationsfilter eine bedeutende Rolle spielen.

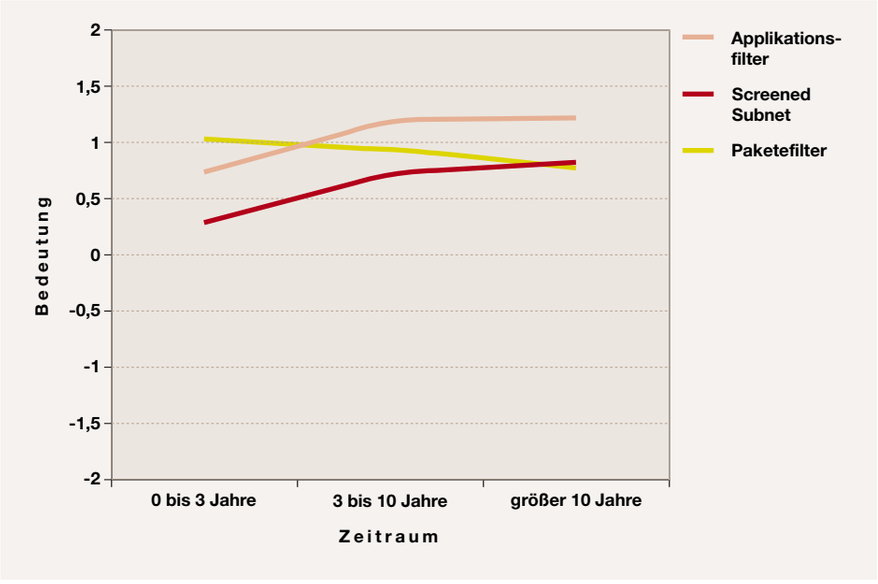



Abbildung 8.20: Bedeutung von Mechanismen zur Implementierung von Sicherheits-Gateways

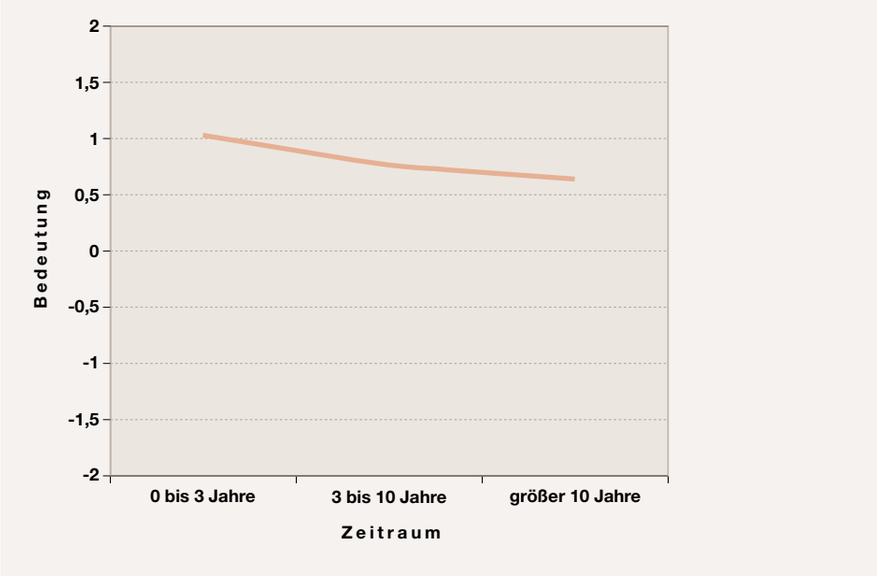



Abbildung 8.21: Bedeutung von Firewall-Systemen vor dem Hintergrund der zunehmenden Nutzung kryptographischer Verfahren

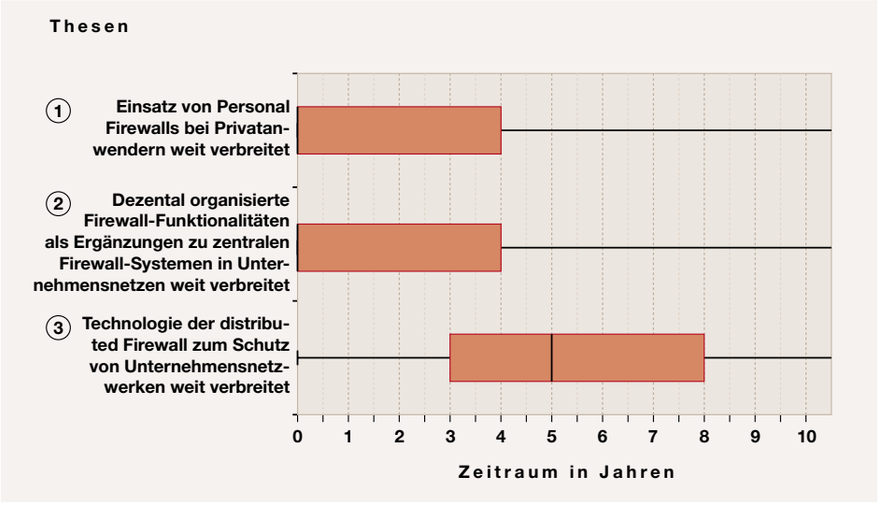



Abbildung 8.22: Ergebnisse der Thesen zum Einsatz von Firewalls

DEZENTRAL ORGANISIERTE FIREWALL-FUNKTIONALITÄTEN: Der Einsatz von dezentralen Firewalls und Personal-Firewalls ist bereits heute weit verbreitet. In Unternehmensnetzen ergänzen sie zentrale Sicherheitsgateways.

CONTENT CHECKING: Content Checking wird in 10 Jahren die selbe hohe Bedeutung wie der Virenscan erreicht haben.

Der Einsatz von Personal Firewalls bei Privatanwendern ist nach Ansicht der Experten bereits weit verbreitet (vgl. Abbildung 8.22, ①). Unter Personal Firewalls werden dabei Softwareprodukte verstanden, die Firewall-Funktionalitäten auf dem Client-Rechner des Nutzers realisieren. Die Befragten erwarten, dass Firewalls zukünftig in Kombination mit Virenscannern oder als Bestandteile des Betriebssystems angeboten werden. Im Vergleich zum unzureichenden Einsatz anderer Sicherheitstools, wie beispielsweise Backup-Software, sind Firewall-Systeme bereits weit verbreitet.

Neue Potenziale erwarten die Befragten beispielsweise durch hardwarebasierte Firewalls (z.B. ROM-Frozen Rules) und eine Verringerung der Gefährdungslage durch DDoS-Angriffe (Distributed Denial of Service). Allerdings wird auch davor gewarnt, dass solche Tools die Nutzer in falscher Sicherheit wiegen könnten, beispielsweise durch deren fehlerhaften Einsatz.

Dezentral organisierte Firewall-Funktionalitäten sind als Ergänzung zu zentralen Firewall-Systemen bereits in Unternehmensnetzen weit verbreitet (vgl. Abbildung 8.22, ②). Die Firewall-Funktionalität „wandert" damit zum Client. Dezentrale Ansätze bieten nach Ansicht der Experten mehr Flexibilität in der Individualisierung der Kommunikationsprozesse und ermöglichen differenziertere Nutzerprofile und Schutzniveaus. Diese Tendenz wird durch die Integration von Firewall-Funktionalität in vielen Betriebssystemen gestützt.

Als sinnvoll werden allerdings einheitliche und zentral verwaltete Richtlinien angesehen. Denkbar ist auch eine Kombinationen aus Firewall und IDS (Intrusion Detection System), bei der die Firewallregeln durch das IDS im Endsystem aktiv beeinflusst werden können. Insgesamt gilt eine zentrale Administration der Clients zur Entlastung der Mitarbeiter als unumgänglich.

Firewall-Systeme bieten typischerweise Funktionalitäten wie Virenscan, Content Checking und URL-Blocking an. Dem Virenscan, also dem Scannen von über die Firewall kommunizierten Inhalten auf Viren, wird über die nächsten zehn Jahre annähernd unverändert die größte Bedeutung beigemessen (vgl. Abbildung 8.23). Dies gilt für nahezu alle Anwendungsbereiche von Firewalls. Allerdings weisen die Experten darauf hin, dass zentrales Virenscanning, das ressourcenintensiv ist und daher ein Skalierungsproblem darstellen kann, nicht von der Verwendung von clientseitigen Scannern enthebt.

Das Content Checking, also das Scannen von über die Firewall kommunizierten Inhalten auf aktive Inhalte (z.B. Java [Sun 02a], Java-Applet, Java-Script, ActiveX (ActiveX Controls) [Micr 02b]), wird hingegen über die nächsten zehn Jah-

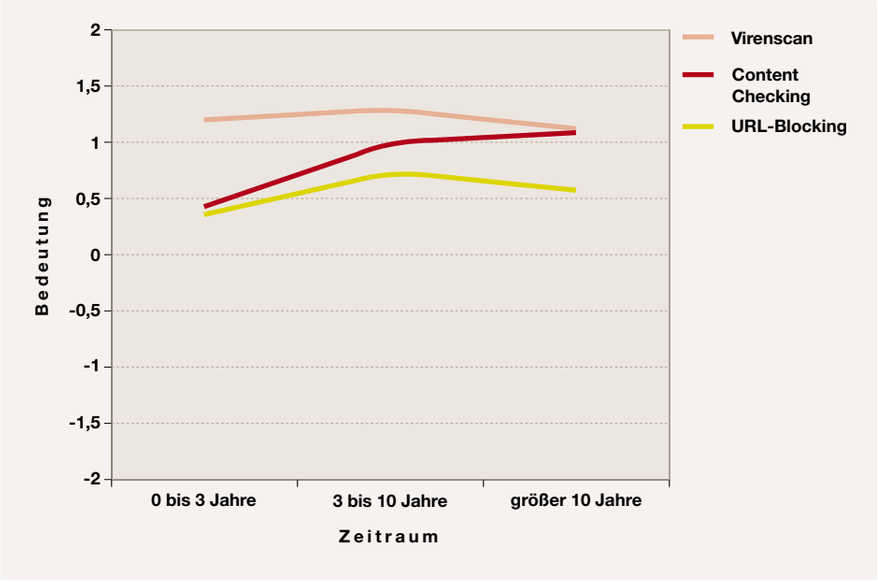



Abbildung 8.23: Bedeutung von Funktionalitäten in Firewall-Systemen

re weiter an Bedeutung hinzugewinnen. Auch im Bereich des Content Checking erscheint das Skalierungsproblem; zusätzlich werden datenschutzrechtliche Bedenken gesehen, da prinzipiell die kommunizierten Inhalte an zentraler Stelle überwacht werden. Das Hauptproblem sehen die Befragten im grundsätzlichen Sperren aktiver Inhalte, da viele Funktionalitäten aufgerufener Anwendungen auf aktive Komponenten nicht verzichten.

Das deutlich weniger bedeutende URL-Blocking, also Funktionen, die eine Anfrage des Benutzers kategorisieren und abhängig von vorgegebenen Filterlisten und Regeln gegebenenfalls blockieren, wird auch in Zukunft kaum zusätzliche Bedeutung erlangen.

Solche Systeme können zur Verhinderung von Spammingund zur DDoS-Abwehr eingesetzt werden. Darüber hinaus sind sie zur Erfüllung rechtlicher Auflagen, insbesondere bei großen Institutionen, essenziell. Allerdings ist der Aufwand nur bei homogenen URL-Bedürfnissen innerhalb eines Unternehmens effizient leistbar. Weiterhin besteht die Gefahr des Missbrauchs durch Inhaltskontrolle. Um diese zu vermeiden, ist die Beteiligung der Mitarbeiter für die Akzeptanz unerlässlich, aber auch zeitintensiv.

Gegen DoS-Attacken (Denial of Service) ist das Prinzip der Distributed Firewallgerichtet. Eine nach diesem Prinzip aufgebaute verteilte Firewall besteht aus einer Reihe von Systemen, die untereinander sicher, z.B. über IPSec, kommunizieren und von denen ein jedes einen definierten Übergangspunkt zum internen Netz darstellt. Wird eines dieser Systeme Opfer eines DoS-Angriffs, so werden die internen Verbindungen zu diesem unterbrochen, während die restlichen Systeme die angebotenen Internet-Dienste aufrecht erhalten.

In diesem Kontext erwarten die Experten, dass die Technologie der Distributed Firewall zum Schutz von Unternehmensnetzen in fünf Jahren weit verbreitet sein wird (vgl. Abbildung 8.22, ③). Distributed Firewalls werden nicht nur zum Schutz vor DoS-Angriffen als sinnvoll angesehen, sondern auch grundsätzlich zum Ausbalancieren zentraler Netzknoten bzw. als effiziente Lösung für Netze mit verschiedenen Übergabestellen. Damit können vermehrt hochverfügbare Anwendungen über offene Netze betrieben und gleichzeitig ein wirksamer Schutz des eigenen Netzes gewährleistet werden.

Allerdings bezweifeln einige Experten die technische Wirksamkeit dieser Maßnahme bzw. den Nutzen im Verhältnis zu

den hohen Kosten. Auch würden neue Angriffstechniken diese Lösung absehbar einholen. Ein offenes Problem ist nach wie vor das Fehlen zentraler Managementmöglichkeiten für große Installationen oder für Auditing-Funktionen, insbesondere für dezentrale Architekturen und Personal Firewalls.

#### Zusammenfassung

Bei der Bewertung der Sicherheits-Gateways sind sich die Experten weitgehend einig. Sie erwarten in den nächsten Jahren im Wesentlichen keine großen Veränderungen.

- Die derzeit größte, aber langfristig rückläufige Bedeutung wird einfachen Paketfiltern zugeordnet, während Applikationsfiltern bereits mittelfristig die größte Bedeutung zukommen wird. Screened Subnets werden ebenfalls an Bedeutung zulegen und langfristig sogar Paketfilter ablösen.

- Die Befragten erwarten, dass Verfahren zur verschlüsselten Tunnelung zunehmen und dadurch Firewall-Systeme nur in geringem Maße an Bedeutung verlieren werden.

- Der Einsatz von Personal-Firewall-Software wird von den Experten bereits im Jahr 2003 als weit verbreitet angesehen. Darüberhinaus wird mittelfristig deren Integration mit Virenscannern erwartet.

- Ebenfalls bereits im Jahr 2003 weit verbreitet sind nach Einschätzung der Befragten dezentral organisierte Firewall-Funktionalitäten, allerdings nur als Ergänzung und unter Verwendung zentral verwalteter Richtlinien.

- Bei den Firewall-Funktionalitäten wird über die nächsten zehn Jahre dem Virenscan die größte Bedeutung beigemessen. Im gleichen Zeitraum wird erwartet, dass das Content Checking weiter aufholt und mit dem Virenscan gleichzieht. Das URL-Blocking wird weiterhin nur von untergeordneter Bedeutung sein.

- Die Befragten erwarten frühstens im Jahr 2008 die weite Verbreitung von Distributed Firewalls, teilweise wird auch die technische Wirksamkeit im Verhältnis zu den Kosten bezweifelt.

### 8.2.1.2 Sicherheitsprotokolle

Neben Protokollen zur Steuerung und Übertragung der zu kommunizierenden Informationen existieren in der Internet-Protokoll-Familie auch Protokolle, die eine vertrauliche und authentische Kommunikation über das Internet sicherstellen sollen. In diesem Abschnitt soll die Verbreitung und Bedeutung von Sicherheitsprotokollen für die vertrauliche und authentische Internet-Kommunikation untersucht werden.

Ein wichtiger Grund für die Sicherheitsprobleme im Internet ist, dass beim ursprünglichen Design vieler Netzwerkprotokolle Sicherheitsmaßnahmen nicht ausreichend berücksichtigt wurden und bei der Implementierung Mängel beim Software Engineering auftraten. So hatten Sicherheitsaspekte auch bei der Konzeption der weit verbreiteten Internet-Protokoll-Suite TCP/IP (Transmission Control Protocol/Internet Protocol) [IETF 81]keine vorrangige Bedeutung, worauf heute viele Angriffe im Internet zurückzuführen sind. Aufgrund der rasanten Entwicklung des Internet und der damit verbundenen Sicherheitsprobleme wurden kryptographische Protokolle und Methoden entwickelt, die auf den verschiedenen funktionalen Schichten innerhalb des Netzwerks aufsetzen.

Um die Sicherheit eines Kommunikationssystems zu gewährleisten, müssen je nach Schutzziel zusätzliche Absicherungen in Form von weiteren Protokollen eingesetzt werden. Eine dieser Sicherheitsmaßnahmen ist die Spezifizierung einer Sicherheitsarchitektur für IP (Internet Protocol) [IETF 81], genannt IPSec (Internet Protocol Security) [IETF 99] [Atki 96], die zu IPv4 kompatibel ist und die die Schutzziele Vertraulichkeit, Authentizität und Integrität auf der IP-Ebene garantieren soll. Eine kryptographische Sicherheitsbetrachtung von IPSec findet sich in [FeSc 99].

Ein weiteres, oft zur Sicherung der Datenübertragung im Internet eingesetztes Protokoll, ist SSL (Secure Socket Layer)

[FKK 96], das auf der Transportschicht arbeitet. Dieses Protokoll sichert u.a. HTTP-Verbindungen (Hypertext Transfer Protocol). Das HTTP-Protokoll ermöglicht vor allem die Kommunikation zwischen Browsern und Webservern und hat sich zum wichtigsten Protokoll im Internet entwickelt. Heute werden auch vertrauliche Informationen über das WWW (World Wide Web) ausgetauscht und daher ist die Sicherung der entsprechenden Verbindungen erforderlich. SSL hat sich inzwischen als Quasi-Standard etabliert und wurde nach geringfügigen Modifikationen als TLS (Transport Layer Security) [IETF 99] von der IETF standardisiert. SSL/TLS soll die Schutzziele Authentizität der Kommunikationspartner, Vertraulichkeit und Integrität der Daten erreichen.

TLS: Das TLS-Protkoll wird mittelfristig wichtigstes Sicherheitsprotokoll im Internet bleiben.

Des Weiteren ist das Secure Shell (SSH) Protokoll auf der Anwendungsschicht zu nennen [Ylön 96, Ylön 01]. SSH soll u.a. die Schutzziele Authentizität und Vertraulichkeit erreichen. Motivation für die Entwicklung von SSH war, die unsicheren Dienste für das remote Login in Rechnersysteme zu ersetzen.

SSH: SSH wird langfristig eine recht hohe Bedeutung halten.

IPSEC: IPv6 integriert IPSec und wird im IP-Bereich das dominierende Sicherheitsprotokoll.

S-HTTP: S-HTTP wird sich langfristig nicht gegenüber TLS durchsetzen können

S/MIME: Auch zukünftig wird das S/MIME-Format bei der Verschlüsselung und dem Signieren von E-Mails vorherrschend sein.

## Ergebnisse

Das derzeit wichtigste Protokoll für sichere WWW-Transaktionen im Internet ist das TLS-Protokoll. Es gewährleistet eine zuverlässige Datenübertragung zwischen zwei Systemen und sichert die Kommunikation auf der Ebene der Transport-Schicht. Mittelfristig wird es seine Bedeutung halten (vgl. Abbildung 8.24), längerfristig erwarten die Experten allerdings einen Rückgang zu Gunsten der dann zu erwartenden Verbreitung von IPSec auf Basis von IPv6. TLS ist heute die Standardtechnologie für sichere Web-Verbindungen, insbesondere bei solchen mit lediglich einseitiger Vertrauensbeziehung. Weiterhin ist es leicht verfügbar, da die Technologie in weit verbreiteten Standardprodukten wie Webbrowsern bereits integriert ist. Zunehmend wird TLS auch zur zweiseitigen Authentisierung, beispielsweise im E-Commerce, genutzt.

Die sichere Terminalanwendung SSH wird vor allem zum sicheren Zugriff von Unix- und Linux-Systemen eingesetzt und ist beispielsweise für die Fernwartung solcher Systeme unerlässlich. SSH wird in seiner Bedeutung recht hoch und langfristig beständig bewertet. Durch die Fähigkeit, TCP-Ports sicher zu tunneln, ermöglicht SSH die Punkt-zu-Punkt-Sicherung zahlreicher Internet Dienste wie POP3 und SMTP.

Der Einsatz des IP-Sicherungsprotokolls IP-Sec als Bestandteil von IPv4 wird in den nächsten zehn Jahren erheblich an Bedeutung verlieren und vollständig von IPv6 mit integriertem IPSec abgelöst werden, welches – derzeit kaum eingesetzt – sich in den nächsten zehn Jahren zum wichtigsten Internet-Sicherheitsprotokoll entwickeln wird. IPSec wird derzeit zur Sicherung von Punkt-zu-Punkt Verbindungen, z.B. der Links zwischen Internet-Routern, nach Ansicht der Befragten zukünftig aber in erster Linie zum Aufbau von Virtual Private Networks (VPN) eingesetzt, z.B. zur Kopplung von Firmen-Netzen oder zum Remote-LAN-Access.

Das Secure Hyper Text Transfer Protocol (S-HTTP) wird mittelfristig nach Einschätzung der Befragten an Bedeutung hinzugewinnen, langfristig betrachtet allerdings wieder abnehmen. S-HTTP ist ein komplexes Protokoll, das die Daten auf der Anwendungsschicht sichert. Es hat sich auf Grund seiner Komplexität gegenüber SSL und TLS bisher nicht durchsetzen können.

Secure Multimedia Internet Mail Enhancement (S/MIME) wird nach Ansicht der Experten nach einem leichten Ansteigen innerhalb der nächsten drei Jahre eine gleichbleibende Bedeutung insbesondere im Bereich der E-Mail-Signatur und -Verschlüsselung haben. S/MIME wird als die zukünftige Standardmethode zur Sicherung von E-Mails gesehen.

## Zusammenfassung

Die Ergebnisse lassen die Schlussfolgerung zu, dass sich langfristig Sicherheitsprotokolle durchsetzen werden, die auf der IP-Ebene aufsetzen. Protokolle hingegen, die auf den höheren Schichten des OSI-Schichtenmodells ansetzen, beispielsweise auf der Transport- oder Anwendungsschicht arbeiten, werden mittelfristig an Bedeutung verlieren. Zusammenfassend kommen die Befragten zu folgender Einschätzung:

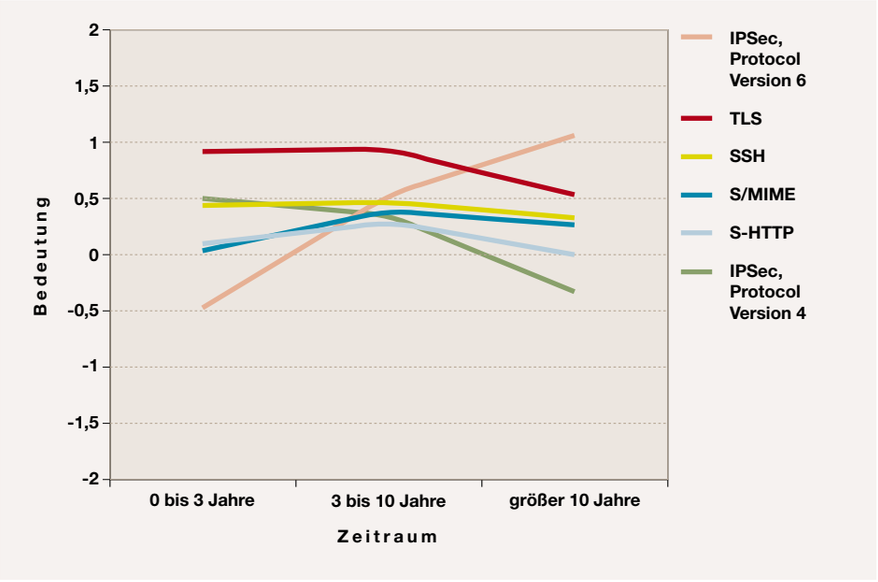



Abbildung 8.24: Bedeutung von Protokollen für Internet-Sicherheit

- Das derzeit wichtigste Sicherheitsprotokoll im Internet, TLS, wird seine Bedeutung in den nächsten drei Jahren beibehalten, danach allerdings hinter IPSec zurückfallen. IPSec wird, mittelfristig als Zusatz von IPv4 und langfristig als Bestandteil von IPv6, erheblich an Bedeutung hinzugewinnen und sich in etwa zehn Jahren zum wichtigsten Internet-Sicherheitsprotokoll entwickeln.

- Die Terminalanwendung Secure Shell wird wegen ihres abgegrenzten Einsatzbereiches über die nächsten zehn Jahre keine wesentlichen Veränderungen erfahren. Sowohl S/MIME als auch S-HTTP werden nach Einschätzung der Experten langfristig keine große Bedeutung erlangen. Erstaunlich ist, dass die Befragten für S-HTTP mittelfristig eine zunehmende Bedeutung prognostizieren.

### 8.2.1.3 Intrusion Detection

Nachdem sich in den vergangenen Jahren Sicherheits-Gateways (siehe Abschnitt 7.1.4) weitgehend etabliert haben, sind alternative Werkzeuge zur Erkennung und Behandlung von Sicherheitsverletzungen entstanden, insbesondere IDS [BSI 98, Gess 01].

Unter „Intrusion" versteht man dabei die Verletzung der Sicherheitsmaßnahmen eines IT-Systems. Das Ziel von IDS ist es, diese Verletzungsversuche zu erkennen, sie dem für die Systemsicherheit zuständigen Personal zu melden und geeignete Gegenmaßnahmen zu ergreifen bzw. das IRS (Intrusion Response System – System für Intrusions-Gegenmaßnahmen) mit geeigneten Informationen über den Angriff zu versorgen.

Das Erkennen einer Intrusion findet in der Analysekomponente eines IDS statt. Dabei unterscheidet man grundsätzlich die Signaturerkennung und die Anomalieerkennung. Während die Signaturerkennung versucht, bekannte Angriffe zu identifizieren, hat die Anomalieerkennung das Ziel, die unmittelbaren Folgen eines Angriffs zu erkennen (z.B. atypisches Systemverhalten).

#### Ergebnisse

Wie in Abbildung 8.25 ersichtlich, wird der Signaturerkennung als Verfahren zur Datenanalyse bei IDS eine über die nächsten Jahre gleich bleibende Bedeutung beigemessen. Die Befragten erwarten, dass solche Verfahren zukünftig mit Firewalls kombiniert und in Router und Switches integriert werden. Die Si-

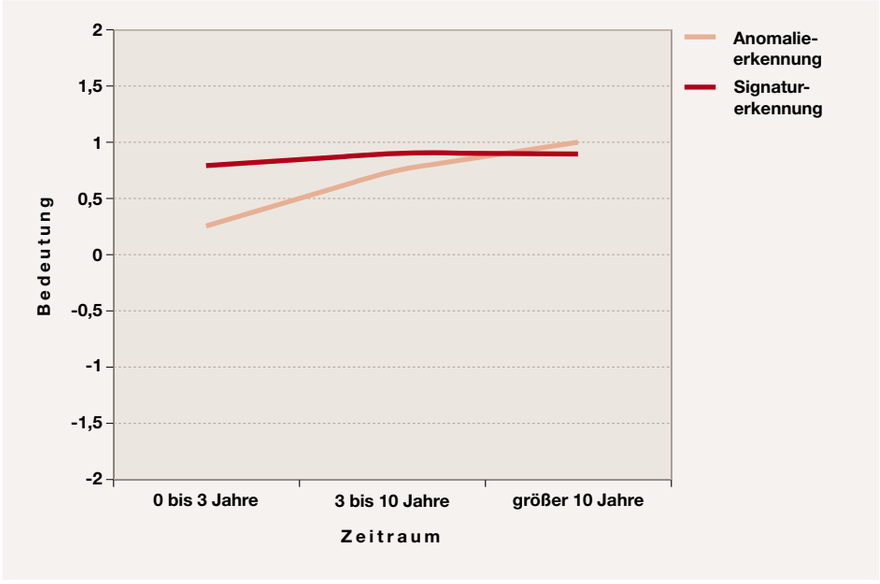



Abbildung 8.25: Bedeutung von Verfahren zur Datenanalyse bei Intrusion Detection Systemen

SIGNATURERKENNUNG UND ANOMALIEERKENNUNG: Anomalieerkennung ist derzeit weniger verbreitet wird aber in zehn Jahren die Signaturerkennung eingeholt haben. Ihr Einsatz wird vornehmlich in hochsensitiven Bereichen erwartet.

IDS: IDS werden in 3 Jahren weit verbreitet sein.

IRS: IRS werden in 4 Jahren weit verbreitet sein.

gnaturerkennung wird insbesondere bei E-Mails, Downloads und für die Bekämpfung bekannter Angriffe für die bereits Erfahrungswerte existieren gesehen.

Die Anomalieerkennung, die zur Feststellung bisher unbekannter Angriffsmuster eingesetzt wird und derzeit weniger verbreitet ist, wird nach Ansicht der Befragten in den nächsten Jahren an Bedeutung gewinnen und in zehn Jahren die Signaturerkennung als bedeutendstes Verfahren zur Datenanalyse eingeholt haben. Bedrohungen werden zunehmend von bislang unbekannten Angriffsmethoden erwartet. Allerdings wird auch davon ausgegangen, dass Signaturerkennung und Anomalieerkennung sich ergänzen und nicht gegenseitig ausschließen werden.

Als Einsatzbereiche für die Anomalieerkennung werden insbesondere hochsensitive Bereiche wie in der Bundeswehr, in Forschungslabors oder bei Dienstleistungsanbieter mit Zugriff auf sensitive Unternehmensdaten genannt, beispielsweise im Finanzbereich oder künftig bei elektronischen Wahlen. Die Befragten erwarten, dass noch länger Probleme im Zusammenhang mit diesem Verfahren ungelöst bleiben. So können Anomalien „verschmieren" und unentdeckbar werden. Weiterhin ist es schwierig, eine Balance zwischen zu „scharfer" und zu „unscharfer" Einstellung zu finden, um einen effektiven Trade-Off zwischen Falschmeldungen und übersehenen Anomalien zu erreichen.

Wie in Abbildung 8.26, ① ersichtlich, werden IDS als integraler Bestandteil von Firewall-Systemen nach Ansicht der Experten in drei Jahren weit verbreitet sein. Bereits heute werden diese in der Überwachung von Unternehmensnetzen, vorwiegend in größeren Unternehmen, eingesetzt. Einige der Befragten betrachten Intrusion Detection eher als unabhängigen, aufgesetzten Mechanismus.

Die Befragten erwarten, dass der Einsatz der IRS in vier Jahren weit verbreitet sein wird (vgl. Abbildung 8.26, ②). Dadurch ergeben sich neue Anwendungspotenziale für ein selbstorganisierendes, adaptives Sicherheitsmanagement. Einige Funktionen von IRS, wie der Gegenschlag, werden als rechtlich bedenklich eingestuft. Intelligente Response-Maßnahmen sind aus Sicht der Befragten noch nicht ausgereift und bergen Gefahren, da sie eine detaillierte System- und Anwendungskenntnis erfordern.

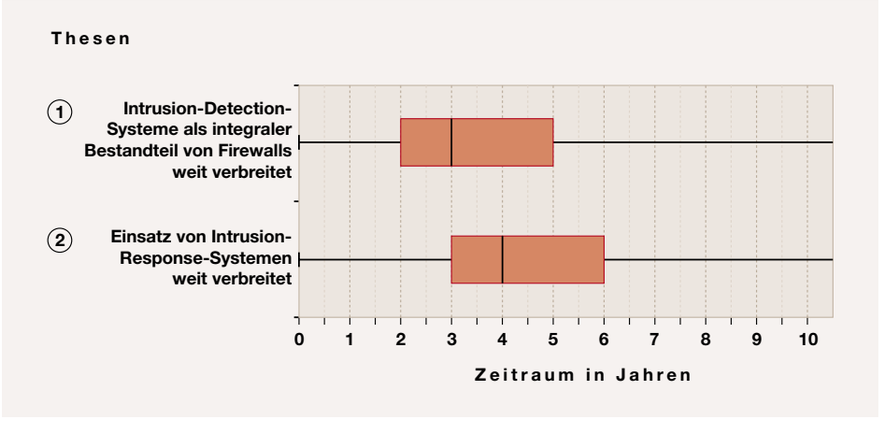



Abbildung 8.26: Ergebnisse der Thesen zum Einsatz von Intrusion Detection und Intrusion Response

### Zusammenfassung

Die weitgehend homogenen Erwartungen der Befragten lassen sich wie folgt zusammenfassen:

- Bei den Verfahren zur Datenanalyse erwarten die Experten, dass die derzeit vorherrschende Signaturerkennung über die nächsten Jahre in ihrer Bedeutung unverändert bleibt, langfristig aber von der Anomalieerkennung eingeholt wird.

- Grundsätzlich wird erwartet, dass IDS bis zum Jahr 2006 als integrale Bestandteile von Sicherheits-Gateways weite Verbreitung finden werden. Der Einsatz von IRS wird etwa im Jahr 2007 erwartet.

#### 8.2.1.4 Aktive Inhalte

Die anhaltende Entwicklung des Internet hat mehr und mehr den Bedarf an multimedialer und interaktiver Information geweckt. Mit dieser Entwicklung entstand in den letzten Jahren eine neue Form der Kommunikation im World Wide Web, die sogenannten Executable Contents (aktive Inhalte). Diese, in der Regel in Internet-Dokumente eingebetteten Programme, ermöglichen ein höheres Maß an Dynamik und Flexibilität, als es bisher mit statischen HTML-Seiten oder CGI-Skripten erreicht wurde.

Die verbreitetsten Technologien dieser Art sind ActiveX und Java-Applets. In die gleiche Kategorie lassen sich die browserspezifischen Erweiterungen über Plugin-Technologien, wie beispielsweise Shockwave Director-Dateien und weitere einreihen. In vielen Browsern sind bereits Komponenten zur Interpretation von Skriptsprachen, die auf dem Zielrechner ausgeführt werden, wie beispielsweise JavaScript oder VB-Script, enthalten.

Ein solches aus dem Netz geladenes Programm, welches manuell oder automatisch zur Ausführung gebracht wird, birgt ein gewisses Potenzial an Risiken. Eine verlässliche Vorhersage der von aktiven Inhalten auszuführenden Aktionen ist in der Regel nicht möglich. Darüber hinaus werden im Internet viele Inhalte anonym angeboten und eine Authentifizierung ist oftmals nur eingeschränkt oder gar nicht möglich.

Ein qualitativer Unterschied zum gezielten Transfer von Applikationen, zum Beispiel von FTP-Servern, ergibt sich aus dem von den Anbietern meist beabsichtigten automatischen Ausführen der aktiven Inhalte. Damit läuft ein Benutzer Gefahr, dass beim Surfen im WWW Programme unbeabsichtigt auf dem eigenen Desktop zur Ausführung kommen.

Risiken dieser Technologien bestehen nicht nur für den Zielrechner selbst, sondern für die komplette Systemumgebung. Befindet sich der Zielrechner beispielsweise im Intranet einer Firma

oder einer Behörde, kann der ausgeführten Applikation unter Umständen das gesamte Netzwerk zur Verfügung stehen. Gängige Gegenmaßnahmen wie Sicherheitsgateways oder Firewalls sind hier lediglich von eingeschränktem Nutzen, da diese gegen Eingriffe von außen konzipiert wurden. Zugriffe auf den lokalen Rechner können für den Anwender fatale Folgen haben und können neben Eingriffen in das Dateisystem wie das Auslesen oder die Modifikation von sensiblen Benutzerdaten beispielsweise DoS (Denial-of-Service)-Angriffe auf das lokale System ermöglichen.

MECHANISMEN ZUR ABSICHERUNG AKTIVER INHALTE: Vertrauensbasierende Mechanismen wie Protection Lists und Signieren aktiver Inhalte durch den Anbieter werden mittelfristig deutlich an Bedeutung gewinnen.

UNGESICHERTE ÜBERMITTLUNG AKTIVER INHALTE: Die ungesicherte Übermittlung aktiver Inhalte wird in absehbarer Zeit nicht durch sichere Mechanismen abgelöst werden.

## Ergebnisse

Die Experten wurden nach der Bedeutung von vertrauensbasierenden Mechanismen zur Absicherung aktiver Inhalte gefragt, der Signierung von Inhalten durch den Anbieter und der Protection List. Ein Problem liegt in der Schwierigkeit, die exakte Funktionalität aktiver Inhalte im Voraus zu ermitteln. Diese Mechanismen definieren eine Vertrauensbasis, indem bestimmte Autoren, Anbieter oder eine Reihe von Quelladressen als vertrauenswürdig eingestuft werden. Im negativen Fall wird der aktive Inhalt bzw. die Seite entweder nicht geladen, kommt also nicht zur Ausführung, oder unterliegt einer funktionellen Einschränkung. Diese Art des „digitalen Vertrauens" wird im Regelfall über entsprechende Listen geregelt oder erfolgt durch so genannte Zertifikate.

Beide Mechanismen zur Absicherung aktiver Inhalte, sowohl das Signieren aktiver Inhalte durch den Anbieter als auch Protection Lists, werden nach Ansicht der Experten in den nächsten Jahren weiter an Bedeutung gewinnen, wobei das Signieren gegenüber den Protection Lists stets als bedeutender angesehen wird (vgl. Abbildung 8.27).

Die Experten sehen Anwendungsbereiche für das Signieren aktiver Inhalte in der Software-Distribution, im sicheren Updaten und in der Fernwartung, sowie bei interaktiven Diensten, verteilten Anwendungen und mobilen Agenten. In vielen Bereichen des elektronischen Handels, des elektronischen Lernens oder bei Online-Spielen werden solche Maßnahmen unerlässlich sein. Die zunehmende Sensibilität der Nutzer und die zunehmende Verfügbarkeit globaler Verzeichnisdienste wird nach Ansicht der Experten die Bedeutung weiter erhöhen. Problematisch wird eingestuft, dass lediglich der Anbieter, nicht aber die von ihm angebotene Funktion des aktiven Inhalts, authentifiziert werden kann. Bei vielen Anbietern ergibt sich darüber hinaus das Problem der Skalierbarkeit des Systems.

Protection Lists haben die Funktion, vertrauenswürdige Anbieter in einer Liste zusammenzufassen und mit entsprechenden Rechten für die Ausführung aktiver Inhalte zu versehen. Nur aktive Inhalte ausschließlich dieser Anbieter gelangen zur Ausführung. Anwendungsbereiche werden in selektiver Datenkommunikation, bei elektronischen Formularsystemen und, wie auch beim zuvor genannten Mechanismus, bei interaktiven Diensten, verteilten Anwendungen und mobilen Agenten gesehen. Allerdings erfordert dieser Mechanismus einen hohen Pflegeaufwand oder das Zurückgreifen auf andere Dienste. Dieser Aufwand sei nach Aussage der meisten Befragten zu hoch, die Protections Lists wären zu inflexibel und ohne Signatur nur begrenzt vertrauenswürdig.

Die Experten erwarten nicht, dass die authentische und integere Übermittlung aktiver Inhalte mit Hilfe geeigneter Mechanismen in absehbarer Zeit die ungesicherte Übermittlung aktiver Inhalteabgelöst haben wird (vgl. Abbildung 8.28, ①). Obwohl mögliche Standardtechnologien vorhanden sind und ein hoher Bedarf in vielen Anwendungsbereichen wie beispielsweise Web-Services und -Applikationen, Distribution von Software-Produkten, automatische Software-Updates, Systemdiagnose, Verhandlung und Matchmaking genannt wird, sehen die Experten zahlreiche Hemmnisse und halten die Mechanismen für zu aufwendig und zu teuer. Es wird darauf verwiesen, dass authentische und integere Übermittlung allein keine ausreichende Sicherheit bedeutet. So sind nach Ansicht der Experten weiterhin wirkungsvolle Sandbox-Systeme (s.u.) sowie eine sichere Einbindung in das Betriebssystem nötig.

Die Befragten gehen, wie in Abbildung 8.28, ② ersichtlich, davon aus, dass derzeit ungeprüftes Ausführen von akti-

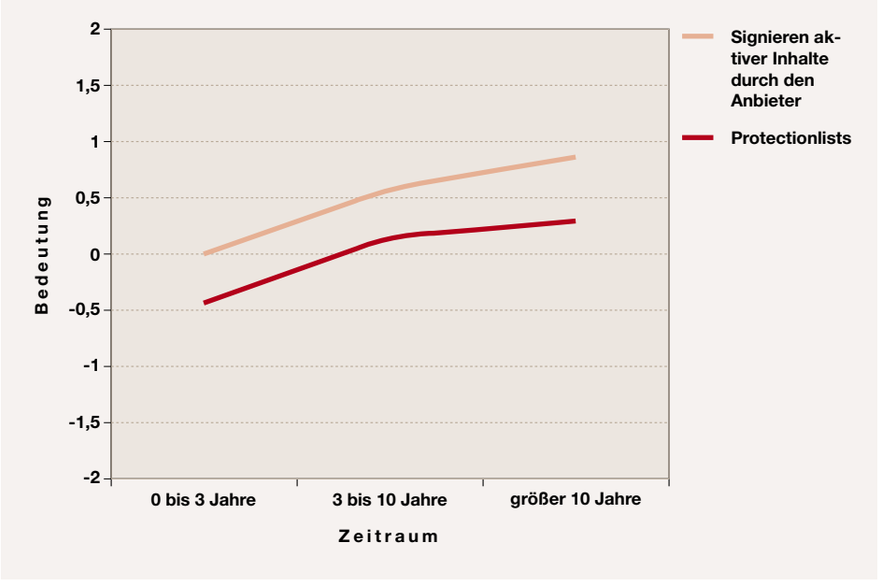



Abbildung 8.27: Bedeutung von Mechanismen zur Absicherung aktiver Inhalte

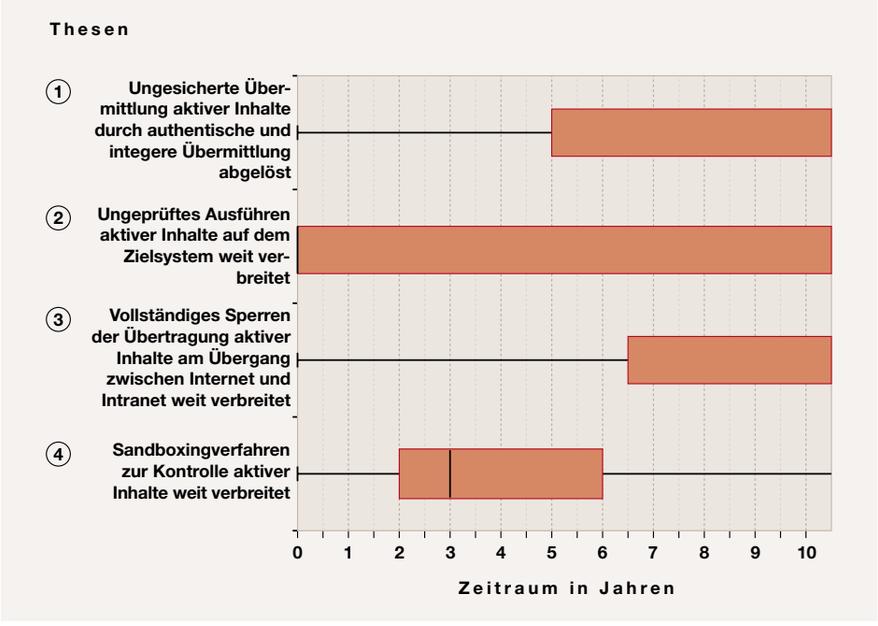



Abbildung 8.28: Ergebnisse der Thesen zu Sicherheitsfragestellungen bei aktiven Inhalten

ven Inhalten auf dem Zielsystem bei den Nutzern, insbesondere im privaten Bereich, vorherrschend sei. Und dies, obwohl das Sicherheitsrisiko beträchtlich ist und die tendenzielle Entwicklung zu mehr Sicherheit strebt.

UNGEPRÜFTES AUSFÜHREN VON AKTIVEN INHALTEN: Es ist derzeit bei den Nutzern weit verbreitet, aktive Inhalte ungeprüft auf den Zielsystemen auszuführen.

Das vollständiges Sperren der Übertragung aktiver Inhalte an das Zielsystem am Übergang zwischen Intranet und Internet wird hingegen nach Ansicht der Experten nicht durchsetzbar sein (vgl. Abbildung 8.28, ③). Die überwiegende Mehrheit der Befragten ist der Meinung, dass der damit einhergehende Funktionsverlust für den Anwender das Nutzungspotenzial auf ein nicht mehr praktikables Maß verringert. Aktive Inhalte werden heute immer häufiger eingesetzt und für viele Anwendungen kann nicht mehr darauf verzichtet werden. Die Experten erwarten, dass im Zweifelsfall der Funktionalität Vorrang vor der Sicherheit gegeben wird. Lediglich als temporäre Maßnahme im Falle einer akuten Gefährdungslage sind solche Maßnahmen denkbar.

VOLLSTÄNDIGE SPERREN DER ÜBERTRAGUNG AKTIVER INHALTE: Das vollständige Sperren der Übertragung aktiver Inhalte wird nie weit verbreitet sein.

Will man keine vertrauensbasierenden Techniken zur Kontrolle aktiver Inhalte einsetzen, kann man entweder alle aktiven Inhalte ungeprüft ausführen lassen, alle aktiven Inhalte nicht zur Ausführung kommen lassen oder das Sandboxing-Verfahren einsetzen. Die Ausführung der aktiven Inhalte geschieht hierbei nicht direkt im Betriebssystem des Zielsystems, sondern in einer eigens dafür implementierten Ausführungsumgebung oberhalb der Betriebssystemschicht. Diese Umgebung koppelt die aktiven Inhalte komplett von ihrer Außenwelt und den Systemressourcen ab und lässt keinerlei Zugriffe nach außen zu. Die Befragten sind überwiegend der Meinung, dass sich Sandboxing-Verfahren zur Kontrolle aktiver Inhalte durchsetzen werden. Erwartet wird eine weite Verbreitung in den nächsten drei Jahren (vgl. Abbildung 8.28, ④). Allerdings gelten diese derzeit als zu ineffizient und zu langsam, durch Bindung vieler Ressourcen und derer Funktionalität als zu sehr eingeschränkt. Mittelfristig werden mit Initiativen wie TCPA oder Palladium [Manf 02] verbesserte Sandboxing-Verfahren mit Hardwareunterstützung erwartet.

SANDBOXING-VERFAHREN: Sandboxing-Verfahren zur Kontrolle aktiver Inhalte sind in 3 Jahren weit verbreitet.

Technologien zur Prüfung aktiver Inhalte sind derzeit ohne größere Relevanz, werden aber nach Ansicht der Experten langfristig an Bedeutung gewinnen, wie Abbildung 8.29 zu entnehmen ist. Die wichtigste Rolle werden dabei auch weiterhin Secure Proxys spielen. Deren Funktionsprinzip ähnelt dem einer Firewall. Sie werden zwischen dem äußeren Netzwerk und den Anwendern installiert und prüfen die Eigenschaften der empfangenen und an das Zielsystem weiterzuleitenden aktiven Inhalte. Allerdings sehen die Befragten durch die Technologie vor allem einen Schutz vor bekannten Angriffen gewährleistet und weisen auf mögliche Probleme bei Ende-zu-Ende verschlüsselten aktiven Inhalten hin. Einige der Experten sehen in der Fortführung der Technologie in Zukunft die Verfügbarkeit von so genanntem Proof-Carrying Code, der einen durch den Client überprüfbaren Sicherheitsbeweis mitführt.

TECHNOLOGIEN ZUR PRÜFUNG AKTIVER INHALTE: Technologien zur Prüfung aktiver Inhalte wie Secure Proxys oder Remote Sandboxes werden in 10 Jahren nennenswerte Bedeutung erlangen.

Bei Remote Execution werden die aktiven Inhalte in einer Remote-Sandbox ausgeführt, die als sicher betrachtet werden kann. Die Kommunikation mit dem Anwender geschieht dabei über ein Protokoll, ähnlich den X-Protokollen der UNIX-Welt, wobei ausschließlich Informationen der graphischen Benutzeroberfläche übertragen werden. Diese Technologie, die derzeit relativ unbedeutend ist, wird nach Ansicht der Experten in den kommenden Jahren wesentlich an Bedeutung gewinnen. Allerdings wird neben datenschutzrechtlichen Bedenken auch auf das Skalierungsproblem hingewiesen und darauf, dass sichere Sandboxen auch lokal realisiert werden können.

Die dritte Möglichkeit ist die Kombination von Secure Proxys und Remote Sandboxing. Dem wird in der Praxis ähnliche Bedeutung wie der Remote Execution beigemessen.

Als weitere Alternativen werden Technologien zum Ressourcenzugriff über Attributszertifikate und Capabilities, für die die Verfügbarkeit von Policy-Informationen und deren (verteilte) Administration entscheidend ist, genannt.

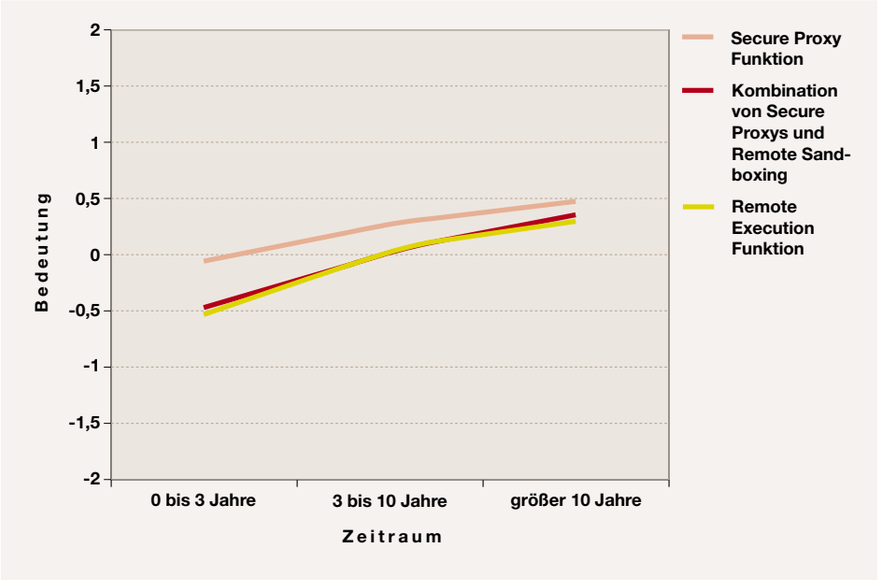



Abbildung 8.29: Bedeutung von Technologien zur Prüfung aktiver Inhalte

### Zusammenfassung

Zusammenfassed kann man feststellen, dass die Experten eine steigende Sensibilisierung durch die Anwender erwarten. Dies drückt sich sowohl in der erwarteten Verbreitung ausgefeilter Technologien zum Schutz vor aktiven Inhalten, als auch in der tendenziellen Akzeptanz solcher Systeme durch die Anwender aus. Allerdings bringen die Experten auch klar zum Ausdruck, dass sie nicht erwarten, dass Anwender zugunsten der Sicherheit funktionelle Einschränkungen hinnehmen werden.

- Sowohl das Signieren aktiver Inhalte durch den Anbieter als auch Protection-Lists werden in den nächsten Jahren weiter an Bedeutung gewinnen. Dabei wird aufgrund der höheren Vertrauenswürdigkeit und durch den geringeren Verwaltungsaufwand für den Benutzer das Signieren aktiver Inhalte immer wichtiger sein als Protection Lists.
- Die Experten erwarten nicht, dass in absehbarer Zeit die authentische und integere Übermittlung aktiver Inhalte unsichere Verfahren ablösen wird. Derzeit ist das ungeprüfte Ausführen von aktiven Inhalten bei den Nutzern weit verbreitet.
- Das vollständige Sperren der Übermittlung aktiver Inhalte, beispielsweise an einem Sicherheits-Gateway, ist nicht durchsetzbar.
- Einhellig wird hingegen erwartet, dass Sandboxing-Verfahren zur Kontrolle aktiver Inhalte bis zum Jahr 2006 weit verbreitet sein werden.
- Technologien zur Prüfung aktiver Inhalte sind derzeit ohne große Relevanz, werden allerdings langfristig an Bedeutung gewinnen. Dabei werden auch weiterhin Secure Proxys die wichtigste Rolle spielen, während Remote-Execution-basierte Systeme sowie kombinierte Systeme aus datenschutzrechtlichen Gründen weniger zur Geltung kommen.

## 8.2.2 Erhöhung der Übertragungskapazitäten

Von den Informations- und Kommunikationstechnologien zeigen sich besonders die hardwarenahen Bereiche wie Prozessoren und Speichertechnologien aber auch die direkt auf Hardware aufbauenden Netztechnologien als Triebfedern für den stetigen Zuwachs an verfügbarer Rechen-, respektive Übertragungsleistung, tragen also zur steten Kapazitäts- und Leistungssteigerung

GLASFASERANSCHLUSS BIS ZUM ENDGERÄT (FTTD): Eine weite Verbreitung dieser Technologie in Unternehemen wird erst in 9 Jahren erwartet.

ÜBERTRAGUNGSTECHNIKEN MIT DATENRATEN GRÖSSER 1 GBIT/S: In 6 Jahren werden entsprechende Techniken weit verbreitet sein, auch wenn von vielen Experten ein derart hoher Bandbreitenbedarf nicht gesehen wird

TREND ZUR DRAHTLOSEN VERNETZUNG: WLans werden in 3 Jahren als Infrastruktur für mobile Computing weit verbreitet sein.

(Abschnitt 8.1) bei. Die zunehmende Verteilung und Dezentralisierung von Arbeitsprozessen und Endgeräten (Abschnitt 9.1) erfordert ihrerseits ständig höhere Übertragungsleistungen. Innerhalb der vorliegenden Studie wurden deshalb in einem eigenen Teilbereich die Erwartungen der befragten Experten hinsichtlich der Leistungsentwicklung im Bereich der Kommunikationstechnologien abgefragt.

Dabei wurden sowohl Entwicklungstendenzen innerhalb bestehender und bereits etablierter Technologien, wie Glasfasernetze oder hochratige Zugangstechnologien (xDSL [Hart 00]) als auch Erwartungen an neue bzw. bisher nicht weit verbreitet eingesetzte Technologien wie WLANs (Wireless LAN) oder photonische Netze [Detk 99] abgefragt. Eine Betrachtung der erwarteten Bandbreiten im Zugangs-, Verteil- und Weitverkehrsbereich rundet diesen Abschnitt des Kapitels Netze und Kommunikation ab.

Mit der Datenübertragung über Glasfasern können nahezu beliebig hohe Datenraten erzielt werden [HePa 03]. FTTD (Fiber To The Desktop) [MaZi 99] kann als Gradmesser für den Bandbreitenbedarf bei diesen Endgeräten gesehen werden.

Grundsätzlich zeigt das Vordringen jeglicher Art hochratiger Übertragungssysteme zum Desktop, unabhängig vom Medium, den Bandbreitenbedarf an. Drahtlose Kommunikationstechniken, die neue Anwendungsfelder erschließen oder höhere Datenraten ermöglichen, sind besonders im Bereich der Verteilnetze als Gradmesser für zunehmende Übertragungskapazitäten zu sehen.

Mit dem zunehmenden Einsatz von Glasfaser wird auch eine Evolution der Koppelkomponenten notwendig. Die Vermittlung durch photonische Netze könnte hier bisher ungeahnte Datenraten ermöglichen [PeTh 00]. Die immer noch zunehmende Anzahl von Internetnutzern [Bund 02] erfordert im Zugangsbereich eine weitere Verbreitung von asymmetrischen Zugangstechnologien, die den Kommunikationsprofilen im Internet (Client-Server) entsprechen. Die zunehmende Verbreitung dieser Technologien respektive die Ablösung der bestehenden symmetrischen Techniken wie ISDN (Integrated Services Digital Network) [Kanb 98] stellen ebenfalls einen Indikator für die Erhöhung der Übertragungskapazitäten dar. Abbildung 8.30 zeigt einen Überblick über die entsprechenden Ergebnisse der Befragung, die im Folgenden erläutert werden.

### Ergebnisse

Der Durchschnitt der Experten geht davon aus, dass der Glasfaseranschluss bis zum Endgerät (FTTD) in Unternehmen erst in neun Jahren verbreitet sein wird (Abbildung 8.30, ①). Teilweise werden auch deutlich frühere Prognosen abgegeben. Damit decken sich die Einschätzungen mit den Ergebnissen der Befragung aus dem Jahr 2000 [SETIK 00]. Einige der Befragten merken aber auch an, dass hohe Datenraten heute bereits auf Basis der bestehenden Kupferverkabelung realisierbar seien. Als Anwendungsfelder werden neben klassischen bandbreitenintensiven Anwendungen wie Videokonferenzen und Virtual Reality-Applikationen auch Bereiche genannt, in denen hohe Abhörsicherheit oder geringste elektromagnetische Störung (Produktionssteuerung) notwendig sind.

Der allgemeine Einsatz hochratiger Anbindung der Endsysteme durch Übertragungstechniken mit Datenraten größer 1 GBit/s wird von den Befragten bereits deutlich früher als FTTD im Jahr 2009 erwartet (Abbildung 8.30, ②). Damit ergibt sich auch bei dieser These eine ähnliche Einschätzung wie im Jahr 2000. Damals wurde der weit verbreitete Einsatz dieser Übertragungtechniken für das Jahr 2007 erwartet. Allerdings wird von den Experten Bedenken bezweifelt, dass herkömmliche Endsysteme (auf dem Desktop) entsprechende Datenraten überhaupt verarbeiten können und, dass es einen Bedarf für derartig hohe Datenraten gebe.

Mit der drahtlosen Vernetzung im lokalen Netz (WLAN) ergeben sich sowohl für Unternehmen als auch für Privatanwender neue Vernetzungs- und Anwendungsmöglichkeiten. Der weit verbreitete Einsatz dieser Technologie wird bereits, ähnlich wie im Jahr 2000, für das Jahr 2006 erwartet (Abbildung 8.30, ③). Der Trend zur drahtlosen Vernetzung hält also unvermindert an. Nach Meinung vieler Befragten bieten sich WLANs auch zum Aufbau einer alternativen Infrastruktur für mobile Computing durch sog. Hotspots (Zu-

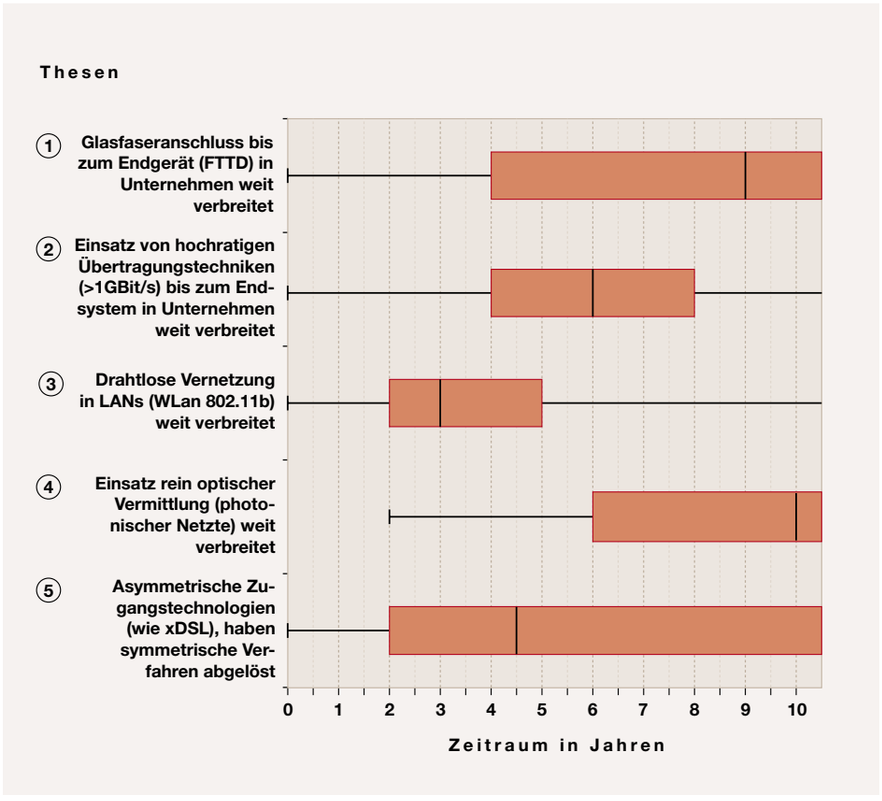



Abbildung 8.30: Ergebnisse der Thesen zu Erhöhung der Übertragungskapazitäten

gangspunkt zu mobilen Netzen an Punkten mit hoher Endgerätedichte) an (Abschnitt 8.2.7).

Vom Einsatz photonischer Netze erwarten die Experten einen sprunghaften Anstieg der realisierbaren Bandbreiten, da auf Grund der dort eingesetzten rein optischen Vermittlung wesentlich höhere Verarbeitungsgeschwindigkeiten möglich sind [Krau 02]. Der Einsatz dieser Technologie wird nach Einschätzung der Befragten allerdings erst in zehn Jahren erfolgen (Abbildung 8.30, ④). Probleme bei der technischen Realisierung der optischen Vermittlung werden hier ebenso als Begründung für die pessimistische Prognose gegeben wie auch die Frage nach einem derart hohen Bandbreitenbedarf im Backbone. Nach Meinung vieler Experten sind die existierenden Backbones bereits heute nicht voll ausgelastet. Im Jahr 2000 waren die Befragten wesentlich optimistischer und sagten photonische Netze bereits für das Jahr 2007 voraus.

Eine Ablösung der bisherigen symmetrischen Netzzugangstechnologien (z.B. ISDN) durch asymmetrische Zugangstechniken, wie sie von xDSL-Produkten realisiert werden, wird nach Einschätzung der Experten bis zm Jahr 2007 stattfinden (Abbildung 8.30, ⑤). Obwohl einige der Befragten diese Ablösung bereits wesentlich früher sehen, deckt sich die durchschnittliche Prognose sehr gut mit den Ergebnissen der Befragung aus dem Jahr 2000 [SETIK 00]. Von vielen Experten wird in diesem Zusammenhang allerdings angemerkt, dass Zugangstechnologien immer den Kommunikationsprofilen der Anwendungen folgen werden. Mit der zunehmenden Verbreitung von Peer-to-Peer-Netzen [West 03] [FrSu 01] werden demnach symmetrische Zugangsverfahren wieder an Bedeutung gewinnen. Weiterhin gehen die Befragten nicht davon aus, dass sich xDSL-Technologien auf Grund ihrer technischen Beschränkungen (Leitungslängen) auch in der Fläche außerhalb von Ballungsräumen einsetzen lassen.

Um die Ausprägung des Trends zur Kapazitäts- und Leistungssteigerung im Bereich der Rechnerkommunikation deut-

PHOTONISCHE NETZE: Technische Probleme und mangelnder Bedarf an Bandbreite lassen die Verbreitung dieser Technologie erst in 10 Jahren zu.

ASYMMETRISCHE ZUGANGSTECHNIKEN: Symmetrische Verfahren für den Netzzugang werden bis in 4 Jahren von asymmetrischen Verfahren wie xDSL abgelöst. Eine völlige Verdrängung wird aber nicht stattfinden.

BANDBREITEN IN ALLEN BEREICHEN: Die Experten sagen auch weiterhin ein exponentielles Wachstum der Bandbreiten voraus.

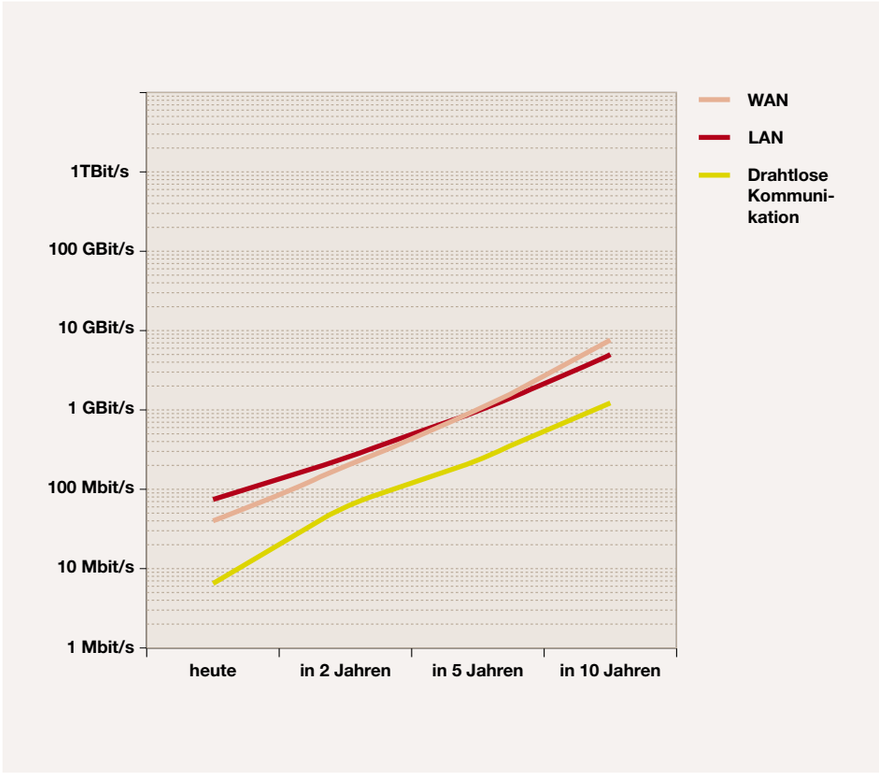



Abbildung 8.31: Entwicklung der Bandbreiten im privaten Bereich

licher aufzuzeigen, wurde von den Befragten eine Einschätzung über die Bandbreitenentwicklung für private und gewerbliche Anwender abgefragt. Die Ergebnisse sind in den beiden Abbildungen 8.31 (für den privaten Bereich) und 8.32 (für den geschäftlichen Bereich) dargestellt.

Sowohl im privaten als auch im geschäftlichen Bereich zeigt die logarithmische Darstellung deutlich ein exponentielles Wachstum der zur Verfügung stehenden Bandbreiten in allen Bereichen. Im Vergleich beider Abbildungen wird deutlich, dass im Mobilbereich für jegliche Anwender die annähernd gleiche Bandbreite erwartet wird. Hingegen zeigt sich im LAN (Local Area Network) eine deutliche Differenzierung. Für gewerbliche Anwender wird von den Experten ein deutlich höherer Anstieg in den Bandbreiten vorhergesagt. Auffallend ist weiterhin, dass der Bandbreitenzuwachs im Unternehmensbackbone und in WANs (Wide Area Network) für Unternehmen langfristig stagnieren wird. Durch die Anmerkungen der Experten lässt sich diese Entwicklung nicht deutlich begründen. Viele Befragte haben allerdings darauf hingewiesen, dass sie eine langfristige Prognose über die nutzbaren Bandbreiten für sehr schwierig halten.

## Zusammenfassung

Die Betrachtung unterschiedlichster Auswirkungen der Erhöhung der Übertragungsraten hat bestätigt, dass dieser Trend, wie bereits in der Vorgängerstudie im Jahr 2000 prognostiziert, weiter anhalten wird. Langfristig sehen die Experten Beschränkungen eher durch den Markt und den Bedarf der Anwender als durch den Mangel an geeigneten Technologien. Im Einzelnen ergaben sich folgende Aussagen:

- Glasfaseranschluss bis zum Endgerät (FTTD) wird in Unternehmen, ähnlich wie 2000 vorhergesagt, im Jahr 2012 weit verbreitet eingesetzt.
- Der Einsatz von hochratigen Übertragungstechniken (größer 1 GBit/s) bis zum Endsystem wird in Unternehmen im Jahr 2009, zwei Jahre später

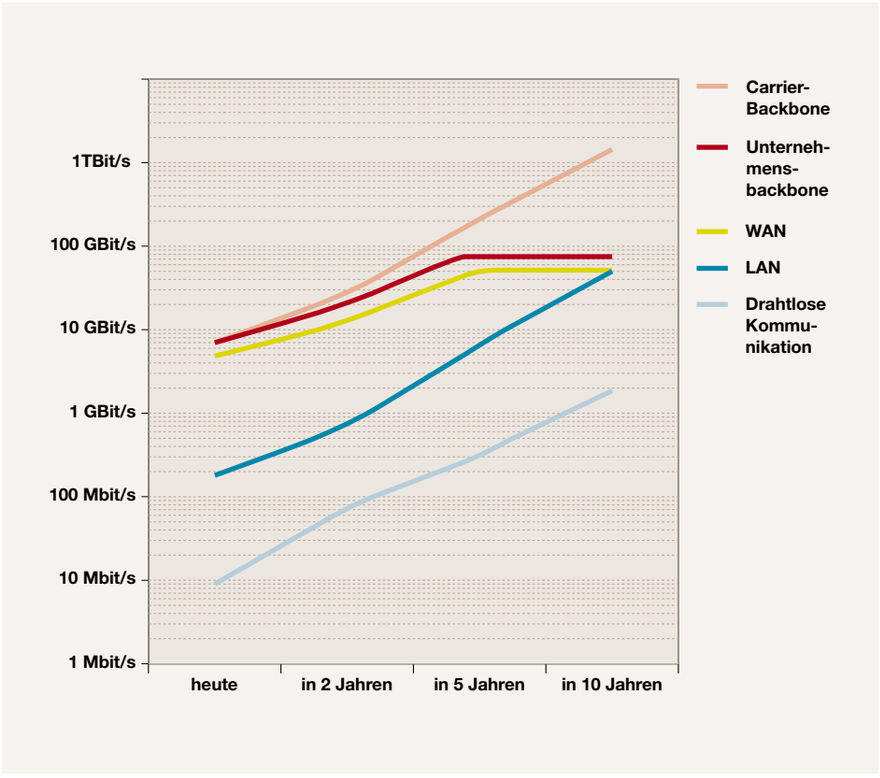



Abbildung 8.32: Entwicklung der Bandbreiten im geschäftlichen Bereich

als im Jahr 2000 prognostiziert, weit verbreitet sein.

- Drahtlose Vernetzung in LANs (WLAN) wird 2006 weit verbreitet sein.
- Der Einsatz von rein optischer Vermittlung (photonische Netze) wird erst im Jahr 2013 weit verbreitet sein.
- Asymmetrische Zugangstechnologien (wie xDSL), die den derzeitigen Zugriffsprofilen entsprechen, werden die derzeitigen symmetrischen Verfahren (wie ISDN) im Jahr 2007 abgelöst haben. Symmetrische Verfahren werden dabei aber nicht völlig verdrängt.

### 8.2.3 Zunehmende Vernetzung

Zur Zeit ist ein globaler Trend zur Konvergenz von unterschiedlichsten Rechnersystemen in ein durchgängiges Gesamtsystem zu verzeichnen. Darüber hinaus kommt es auch zu einer Vereinheitlichung der eingesetzten Technologien. Zusätzlich entstanden in den letzten Jahren Technologien wie MPLS (Multi Protocol Label Switching) [Davi 00], die explizit als vereinheitlichende, sog. Overlay-Technologien entworfen wurden, um eine weitere Vernetzung bereits bestehender Systeme zu vereinfachen. Mit der Digitalisierung des Rundfunks (DVB (Digital Video Broadcasting) [DAB 03, PSF$^+$ 00], DAB (Digital Audio Broadcasting) [DAB 03, Frey 97]) bieten sich neue Möglichkeiten zur Anbindung von Endsystemen an Kommunikationsnetze. Ebenso entstanden in den letzten Jahren neue, drahtlose LAN-Technologien, die ebenfalls zur zunehmenden Vernetzung beitragen werden.

Im Bereich der Protokolle und Dienste wird versucht, auf ein einheitliches Protokoll, IP, aufzubauen und damit, per Konstruktion, einfachste Möglichkeiten zur Vernetzung und eine bestmögliche Konvergenz zu erreichen [Scha 00]. Allerdings verstärkte sich in den letzten Jahren die Annahme, dass IP nur bedingt als Basisprotokoll für Dienste mit hohen Anforderungen an eine gleichbleibende Dienstgüte geeignet ist [Detk 01]. Eine Vielzahl von

zusätzlich zu IP entwickelten Protokollen und Diensten wie DiffServ (Differentiated Services) [IETF 02] oder IntServ (Integrated Services) [IETF 97b] sollen diese Lücke schließen.

Die Frage nach einer Konvergenz der Protokollwelt im Zuge der weiteren Vernetzung stellt sich nach der Versteigerung der UMTS-Lizenzen auch im Bereich der mobilen Netze. Daher werden in diesem Abschnitt nicht nur Entwicklungen im Bereich der „klassischen" Backbones (MPLS, WAN) sondern auch im Bereich der mobilen (Zugangs-)Netze (UMTS, DECT (Digital Enhanced Cordless Technologies) [Walk 98], WLAN) untersucht. Eine Betrachtung neuer Einsatzgebiete für Kommunikationsnetze, wie Automobile oder Haushalte [IGS 01], rundet diesen Abschnitt, zusammen mit einer Untersuchung von alternativen Infrastrukturen zum Aufbau von Kommunikationsnetzen, ab.

BACKBONE-TECHNOLOGIEN UND -PROTOKOLLE: IPv6 und WDM werden sich langfristig durchsetzten. MPLS wird nur vorrübergehend bedeutend.

BEREICH DER LOKALEN, ZUGANGS- UND VERTEILNETZE: xDSL und Gigabit-Ethernet werden in diesem Umfeld langfristig die bedeutendsten Technologien.

## Ergebnisse

Um einen Überblick über die Einschätzung der Experten zu Entwicklungen im Bereich der Rechnerkommunikation zu erhalten, wurde zunächst die Bedeutung typischer Protokolle in Backbones, Verteil- und Zugangsnetzen sowie im Bereich der mobilen Datenkommunikation abgefragt. Die Ergebnisse sind in den folgenden Abbildungen dargestellt.

Im Bereich der Backbones ist die Entwicklung von IPv4 und IPv6 besonders auffallend. Aus Abbildung 8.33 ist deutlich erkennbar, wie innerhalb der nächsten zehn Jahre IPv6 IPv4 als bedeutendstes Protokoll ersetzt. Eine ähnliche Prognose über den Ablösungszeitraum wurde von den Experten bereits in der Vorgängerstudie [SETIK 00] gegeben: Damals wurde die Ablösung von IPv4 durch IPv6 ebenfalls in drei bis zehn Jahren erwartet. Die Befragten sind also gegenüber der Untersuchung im Jahr 2000 pessimistischer geworden.

Ebenfalls im Vergleich zur Vorgängerstudie zeigt sich, dass sich die Einschätzung der Experten bezüglich Frame Relay und ATM (Asynchronous Transfer Mode) [Sieg 03] nicht wesentlich verändert hat. Wie damals wird die relative Bedeutungslosigkeit dieser Technologien im Vergleich zu den anderen abgefragten Übertragungsmethoden erst in zehn Jahren vorausgesagt. Absolut ergibt sich also eine um drei Jahre pessimistischere Prognose.

Auch für SDH (Synchronous Digita Hirarchy), MPLS und WDM (Wavelength Division Multiplexing) lassen sich ähnliche Verschiebungen der Prognosen feststellen. MPLS und WDM werden in den nächsten zehn Jahren an Bedeutung gewinnen, wobei MPLS nach den Aussagen der Experten am Ende des Prognosezeitraums wieder an Bedeutung verlieren wird. Für SDH wird eine Stagnation auf hohem Niveau vorhergesagt. Diese Entwicklung wurde in ähnlicher Form, mit identischen Zeiträumen, bereits in der Vorgängerstudie aufgezeigt.

Im Bereich der Backbone-Technologien und -protokolle werden sich demnach langfristig IPv6 und WDM durchsetzen. MPLS wird hinter diesen beiden Technologien zurückbleiben. Auffallend ist weiterhin, dass sich im Vergleich zu den in Vorgängerstudie ermittelten Zeiträumen, vom Zeitpunkt der Befragung aus betrachtet, keine Änderungen in den Prognosen ergeben haben, die Experten also gegenüber ihren Einschätzungen vor drei Jahren „vorsichtiger" wurden.

Im Bereich der lokalen, Zugangs- und Verteilnetze werden die Ergebnisse aus der Vorgängerstudie [SETIK 00] bestätigt. In Abbildung 8.34 ist deutlich der Bedeutungsverlust des klassischen Ethernets [Hanc 96] gegenüber allen anderen abgefragten Technologien zu erkennen. Mit Ausnahme der Zugangstechnologieklasse xDSL, die über den gesamten Prognosezeitraum in ihrer Bedeutung hoch eingeschätzt wird, erfahren alle anderen betrachteten Technologien langfristig eine Aufwertung. Aus der relativen Betrachtung ergibt sich eine Ablösung des klassischen Ethernets durch Varianten mit höherer Übertragungsrate in etwa fünf Jahren.

Im Bereich der Verteilnetze zeigt sich eine Konsolidierung von auf Satelliten basierenden Verteilstrukturen. Gleichzeitig ist ein Bedeutungszuwachs bei den digitalen Funktechniken DVB und DAB zu beobachten. Diese Einschätzung der Entwicklung durch die Experten kann als Indiz dafür gesehen werden, dass diese Technologien mit der fortschreitenden Verbreitung des digitalen Rundfunks auch für die Zwecke der Datenkommunikation verwendet werden könnten.

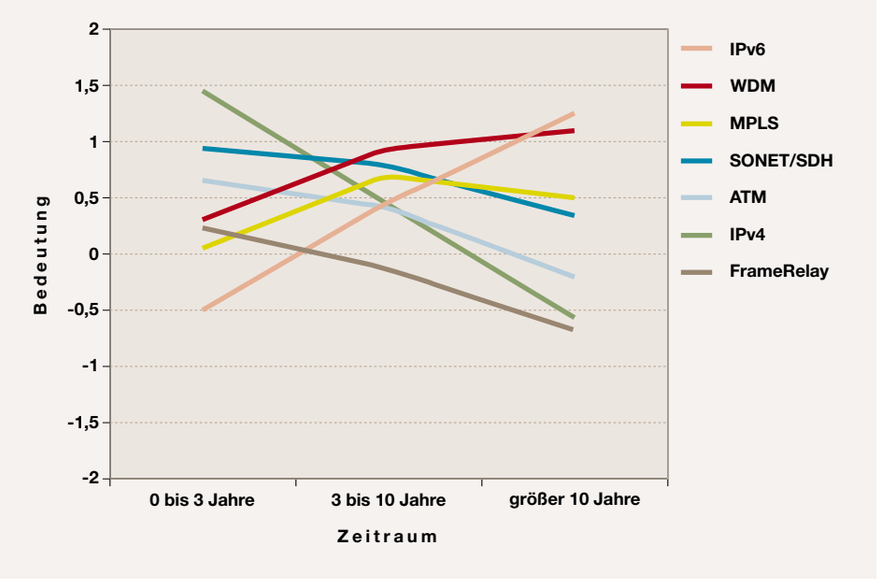



Abbildung 8.33: Bedeutung von Übertragungstechnologien für beliebige Übertragungen im Backbone

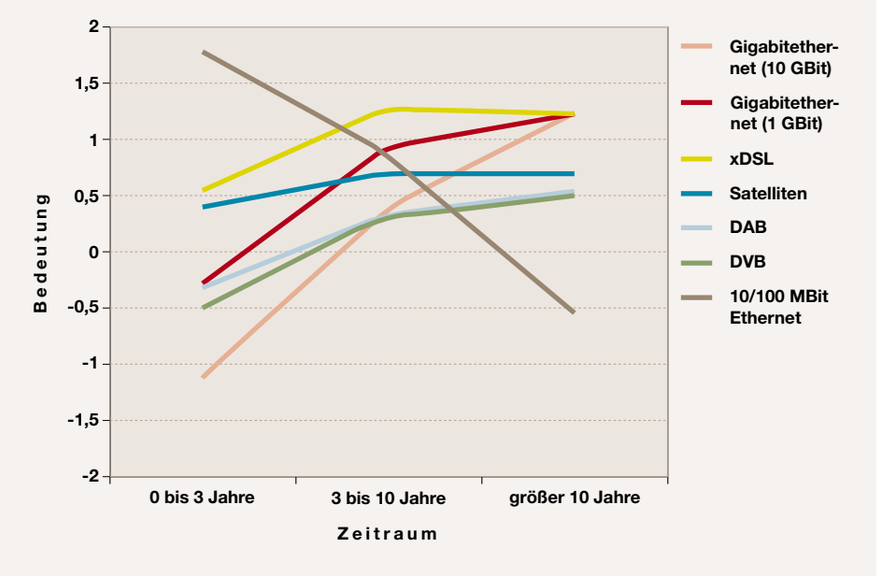
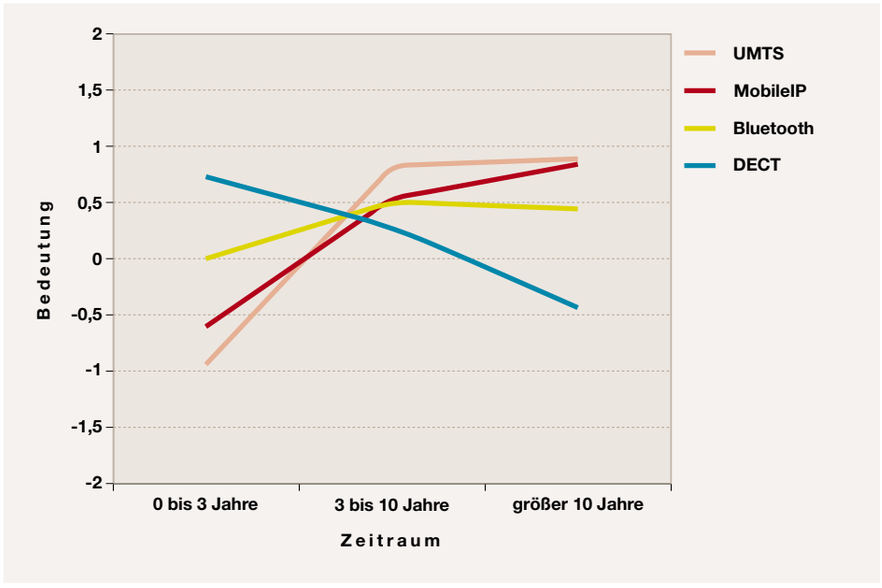



Abbildung 8.34: Bedeutung von Übertragungstechnologien für beliebige Übertragungen in lokalen, Zugangs- und Verteilnetzen




DATENÜBERTRAGUNG AN DER LUFTSCHNITTSTELLE: UMTS MobileIP sind langfristig die bedeutendsten Technologien bei der mobilen Datenübertragung.

BASISPROTOKOLLE FÜR DIE KOMMUNIKATION MIT IP: xDSL und WDM werden sich langfristig durchsetzen.

Abbildung 8.35: Bedeutung von Übertragungstechnologien für beliebige Übertragungen im Mobilbereich

Mit der rasanten Entwicklung im Bereich der Mobilkommunikation in den letzten Jahren wurde eine detaillierte Abschätzung der Entwicklungen in diesem Bereich unerlässlich. Innerhalb dieser Studie wurde deshalb die Einschätzung der Experten bezüglich der im Moment gängigen Technologien in diesem Bereich ebenso wie eine Bewertung zukünftiger Technologien abgefragt. Dabei standen Technologien für die Datenübertragung über die Luftschnittstelle im Vordergrund. Auf eine detaillierte Betrachtung von GSM (Global System for Mobile Communications) [Roth 02] als seit Jahren etablierter Technologie wurde verzichtet.

Abbildung 8.35 zeigt die Ergebnisse der Befragung. In der dargestellten Entwicklung ist deutlich erkennbar, wie sich die Verhältnisse nach Einschätzung der Experten deutlich zu Gunsten von UMTS entwickeln. DECT, das heute noch von den Experten als bedeutendste Technologie zur Datenübertragung an der Luftschnittstelle angesehen wird, verliert im Beobachtungszeitraum stark an Bedeutung. Bis zu einem gewissen Grad und in vielen Anwendungsfällen gilt Bluetooth als Nachfolgetechnologie von DECT. Dennoch nimmt die Bedeutung von Bluetooth bei weitem nicht in dem Maß zu, wie es nötig wäre, um nach der Einschätzung der Experten als Nachfolgetechnologie für DECT zu gelten. Neben UMTS erfährt nur noch MobileIP als umfassendes Transportprotokoll in mobilen Umgebung einen ähnlich starken Bedeutungszuwachs.

IP wird als Universalprotokoll angesehen, auf das sich in Zukunft jegliche Art von Kommunikation abstützen wird. Deshalb wurde im Rahmen dieser Studie die Einschätzung der Experten bezüglich unterschiedlichster Basisprotokolle für die Kommunikation mit IP abgefragt. Dabei wurden zunächst Basistechnologien für leitungsgebundene Kommunikation untersucht (Abbildung 8.36). Ein weiterer Fragenblock widmete sich der Entwicklung im Bereich der mobilen Kommunikation (Abbildung 8.37).

Für den Zugangsbereich zeigt sich, dass xDSL-Technologien ISDN langfristig ablösen werden. Bei den Backbone-Infrastrukturen verlieren ATM und SDH beständig an Bedeutung, während die Bedeutung von WDM auch langfristig ansteigt. Diese Aussagen bestätigen den Trend zu IP over $\lambda$ (IP over lambda) [Ghan 00].

Besonders im Bereich der Kommunikation mit mobilen Endgeräten über die Luftschnittstelle wird zukünftig der Austausch beliebiger Daten neben der Übermittlung

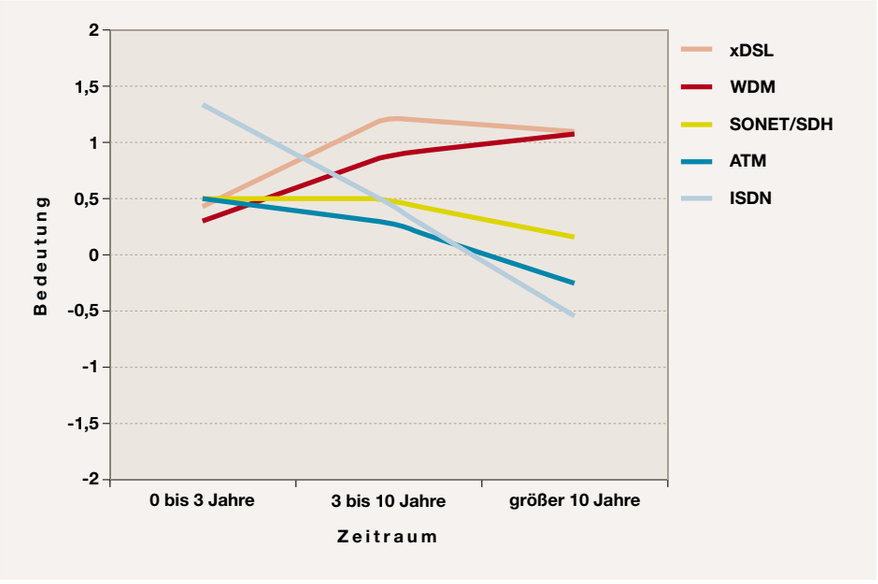



Abbildung 8.36: Bedeutung von Übertragungstechnologien für IP-basierte Anwendungsprotokolle im Backbone und Zugangsnetz

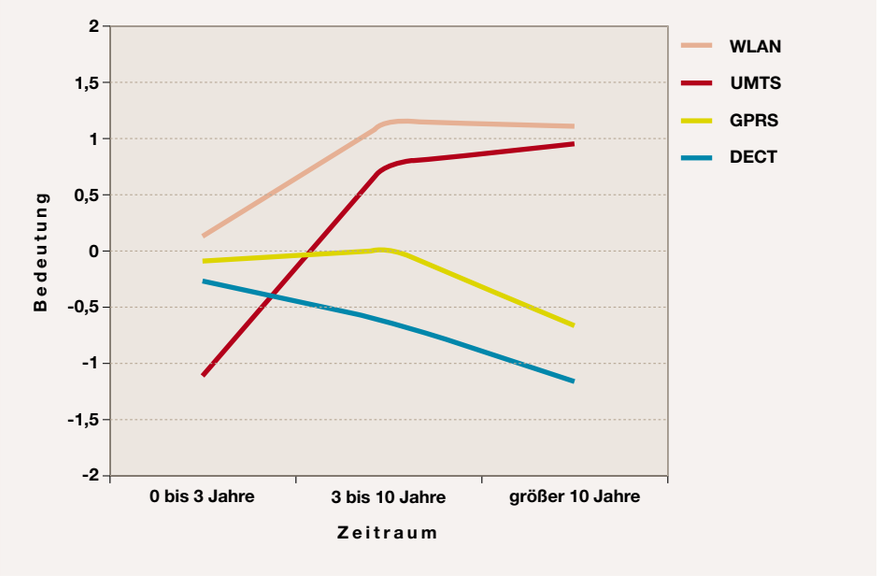



Abbildung 8.37: Bedeutung von Übertragungstechnologien für IP-basierte Anwendungsprotokolle im Bereich der Mobilkommunikation

von Telefongesprächen zunehmen. Damit stellt sich die Frage nach Protokollen und Technologien, die als Basis für IP-basierte Übertragungen in Mobilnetzen verwendet werden können. In Abbildung 8.37 ist die Einschätzung der Experten bezüglich WLAN, UMTS, GPRS (General Packet Radio Service) [HeSa 01]und DECT dargestellt. Deutlich zu erkennen ist, wie die bereits etablierten Technologien GPRS und DECT in den nächsten zehn Jahren zugunsten von UMTS und WLAN an Bedeutung verlieren. Weiterhin ist anzumerken, dass den WLAN-Technologien über den gesamten Beobachtungszeitraum, vor allem aber innerhalb der nächsten fünf Jahre deutlich mehr Bedeutung zugemessen wird als UMTS. Möglicherweise gehen die Experten davon aus, dass UMTS als durchgängige Infrastruktur kurzfristig nicht zur Verfügung stehen wird. Die Einschätzung der Experten bezüglich UMTS wird im Abschnitt 8.2.7 nochmals im Detail dargestellt.

Zur endgültigen Konvergenz der Transportnetze wird zur Zeit IP als grundlegendes Protokoll für alle höheren Dienste vorgeschlagen. Unter dem Stichwort „everything over IP" [Haas 00] wird an einer entsprechenden Vereinheitlichung der Kommunikationnetze geforscht und gearbeitet. Im Vordergrund steht dabei die Integration von Anwendungen und Protokollen, die hohe Qualitätsanforderungen an das unterliegende Netz z.B. bezüglich Bandbreite und Verzögerung stellen. Als Schlüssel zur Integration von bzw. auf IP wird deshalb die Umsetzung geeigneter Technologien zur Durchsatzsteigerung in IP gesehen. Innerhalb der Studie wurde deshalb die Einschätzung der Befragten über die Bedeutung unterschiedlichster Technologien zur Durchsatzsteigerung abgefragt. Die Einschätzung der Experten ist in Abbildung 8.38 dargestellt.

Hier ist zu erkennen, dass von den Experten heute IP-Switching bevorzugt wird. Langfristig gewinnen aber MPLS und Wirespeed-Routing an Bedeutung. Die Encapsulierungstechnik für ATM, MPOA (Multi Protokoll over ATM), verliert nach einem kurzen Anstieg zusammen mit der Basistechnologie ATM (siehe Abbildung 8.33) an Bedeutung. Weiterhin zeigt die Grafik deutlich, dass die beschriebenen Entwicklungen nur in einem sehr engen Bereich stattfinden. Noch vor drei Jahren wurde in der Vorgängerstudie [SETIK 00] an dieser Stelle Wirespeed-Routing in der langfristigen Entwicklung deutlich favorisiert. Diese Technologie wird zwar von den Experten langfristig immer noch in ihrer Bedeutung am höchsten eingeschätzt, allerdings ist der Abstand zu alternativen Techniken wie MPLS oder Wirespeed-Routing sehr gering.

Neben IP auf der Vermittlungsschicht des OSI-Schichtenmodells (Open Systems Interconnection) [ISO 7498] bietet sich mit MPLS die Möglichkeit zu einer Vereinheitlichung der verschiedenen Transporttechnologien zu einem durchgängigen Netz, bei gleichzeitig hohem Investitionsschutz [DaRe 00]. Für die durchgehende Nutzbarkeit von MPLS müssen allerdings noch organisatorische Fragestellungen, wie die Zusammenarbeit unterschiedlichster Provider in einem Netz, gelöst werden. Vor diesem Hintergrund wurde von den Experten eine Einschätzung über die Verbreitung von MPLS als Backbone-Technologieund den Aufbau eines Provider-überspannenden MPLS-Netzes abgefragt. Die diesbezüglichen Einschätzungen der Experten sind in Abbildung 8.39 dargestellt.

Bereits für das Jahr 2007 sagen die Experten den weit verbreiteten Einsatz von MPLS in Backbone-Netzen voraus (Abbildung 8.39, ①). Ein durchgängiges MPLS-Netz, das Providergrenzen überspannt, wird von der Mehrheit der Experten innerhalb des Untersuchungszeitraums von zehn Jahren allerdings nicht gesehen (Abbildung 8.39, ②). Allerdings rechnen einige Befragte bereits in einem Zeitraum von zwei bis fünf Jahren mit der Realisierung entsprechender Netze.

Im Automobilsektor sind in den letzten Jahren Fahrzeuge auf den Markt gekommen, die bereits Internetzugang vom Fahrzeug aus bieten (z.B. [BMW 03]). Grundsätzlich sehen die Befragten eine Anbindung von Automobilen an Telekommunikationsnetze bereits in fünf Jahren weit verbreitet (Abbildung 8.40, ①).

Elektrische Haushaltsgeräte, die eine Zugangsmöglichkeit zu Kommunikationsnetzen bieten, sind nach Meinung der Mehrheit der Experten erst im Jahr 2008 weit verbreitet (Abbildung 8.40, ②). Begründet wird dies mit Problemen bei der Vereinheitlichung der Schnittstellen und Vernet-

IP-BASIERTE ÜBERTRAGUNGEN IN MOBILNETZEN: UMTS und WLan werden langfristig die Basis für IP-Kommunikation in mobilen Netzen bilden.

TECHNOLOGIEN ZUR DURCHSATZSTEIGERUNG: Aus den Aussagen der Befragten läßt sich keine klare Prognose über zukünftig eingesetzte Technologien ableiten. Sowohl MPLSals auch Wirespeed-Routinggewinnen langfristig an Bedeutung.

MPLS IN BACKBONE-NETZEN: Bereits in 4 Jahren wird der Einsatz von MPLS weit verbreitet sein.

DURCHGÄNGIGES MPLS-NETZ: Die Provider-übergreifende Nutzung von MPLS wird sich in den nächsten 10 Jahren nicht durchsetzen.

INTERNETZUGANG VOM FAHRZEUG: Der Zugriff auf Kommunikationsnetze von Automobilen ist in 5 Jahren weit verbreitet.

ELEKTRISCHE HAUSHALTSGERÄTE: Die Anbindung von Kleingeräten im Haushalt an Kommunikationsnetze ist in 8 Jahren weit verbreitet.

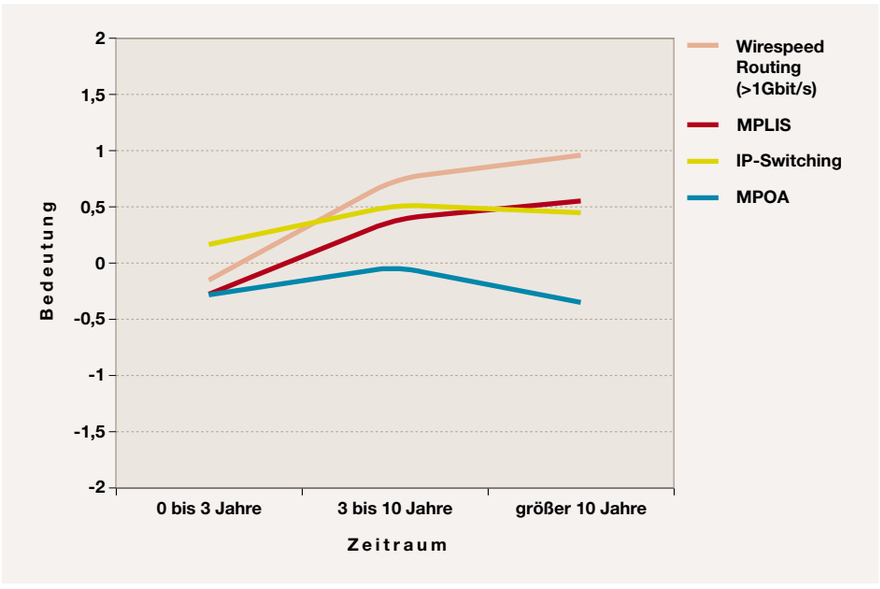



Abbildung 8.38: Bedeutung von Technologien zur Durchsatzsteigerung von IP

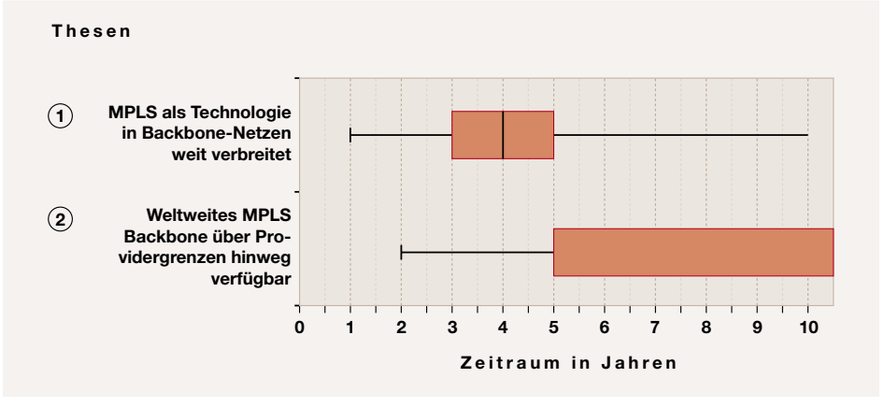



Abbildung 8.39: Ergebnisse der Thesen zur Entwicklung von MPLS

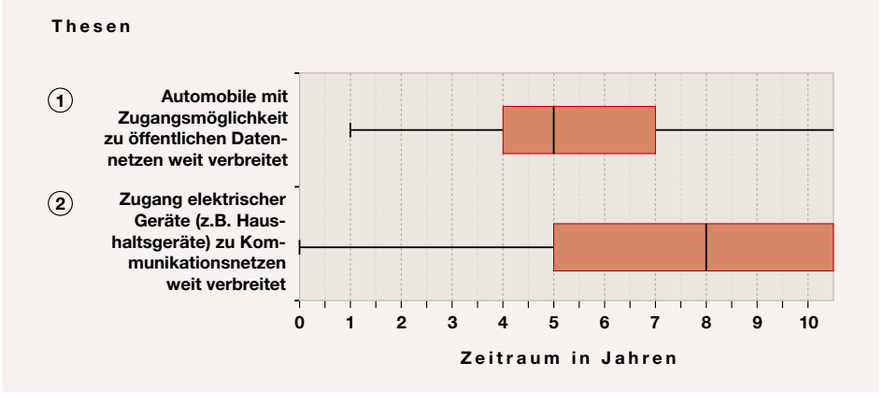



Abbildung 8.40: Ergebnisse der Thesen über neue Anwendungsgebiete vom Kommunikationsnetzen

zungstechnologien (Hausbusse) aber auch mit fehlenden „Killerapplikationen" und mangelnder Akzeptanz am Markt. (Eine detaillierte Analyse der Technologien und der Marktentwicklungen in diesem Bereich findet sich in [IGS 01]). Die durchschnittliche Prognose ist aber im Vergleich zur Vorgängerstudie [SETIK 00] dennoch pessimistischer geworden. Damals wurde eine weite verbreitete Vernetzung von Hausgeräten für das Jahr 2006, also zwei Jahre früher, vorhergesagt.

VERTEILINFRASTRUKTUREN: Bestehende Strukturen werden nach Aussagen der Experten nur zum Aufbau von Verteilnetzen verwendet. Das bestehende TV-Kabel-Netz hat hierbei die größte Bedeutung.

Mit dem Vordringen der Kommunikationsnetze und ihrer Anwendungen in bisher wenig erschlossene Bereiche stellt sich auch die Frage nach alternativen Infrastrukturen zum Aufbau solcher Netze. Mit der Wiederverwendung bestehender Leitungs- oder Kommunikationsinfrastrukturen bietet sich die Möglichkeit, neue Anwendungsbereiche einfach, ohne den Aufbau eigener Infrastrukturen, wie sie beispielsweise in hohem Maße für den Mobilfunk nötig waren, zu erschließen. Besonders zum Erreichen einer breiten Masse an Endkunden bietet es sich an, bestehende Verteilinfrastrukturen, wie Stromnetze oder TV-Kabel zu verwenden.

Das TV-Kabel-Netz wird im Bereich der Zugangsnetze von den Experten heute, wie in Zukunft, in seiner Bedeutung deutlich höher eingeschätzt als das Stromnetz. Dies ist auch im Backbone der Fall, allerdings werden die beschriebenen Verteilinfrastrukturen zum Aufbau von Backbones von den Experten als nahezu unbedeutend eingestuft. Viele der Befragten merken an, dass sich Verteilinfrastrukturen prinzipiell nicht zum Aufbau von Backbones eignen (Abbildung 8.41).

## Zusammenfassung

Der übergreifende Trend zur Konvergenz und Vereinheitlichung im Bereich der Kommunikationsnetze wird durch die Auswertung des entsprechenden Fragenblocks innerhalb der Studie bestätigt. Protokolle und Technologien, die eine Vereinheitlichung der Kommunikationsinfrastrukturen bei gleichzeitig zunehmender Vernetzung erlauben, werden von den Experten langfristig klar favorisiert. Allerdings ist die Entwicklung über den Beobachtungszeitraum teilweise indifferent.

- Im Bereich der Backbones wird mittelfristig eine Ablösung von IPv4 durch IPv6 erwartet. Daneben wird langfristig WDM als Basistechnologie eingesetzt werden. Damit bestätigt sich der Trend zu IP over $\lambda$. Hingegen wird MPLS nur eine Bedeutung als Übergangstechnologie beigemessen.

- Gigabit-Ethernet wird im Bereich der Zugangsnetze das im Moment verbreitete klassische Ethernet (mit Datenraten bis 100 MBit/s) ablösen. xDSL wird im Lauf der nächsten zehn Jahre an Bedeutung verlieren. DAB und DVB werden zukünftig ebenfalls zum Aufbau von Verteil- und Zugangsnetzen verwendet werden.

- Für die Mobilkommunikation sehen die Experten UMTS und MobileIP langfristig als Schlüsseltechnologien. Im Moment steht in diesem Bereich nach Meinung der Experten jedoch DECT im Vordergrund. Bluetooth wird auch langfristig nicht ähnlich bedeutend wie UMTS oder MobileIP.

- Bei leitungsgebundenen Infrastrukturen für IP-Netze wird langfristig der Einsatz von WDM im Backbone und xDSL im Zugangsbereich vorhergesagt. Etablierte Technologien wie ATM, SDH oder ISDN werden nach Meinung der Experten bereits mittelfristig an Bedeutung verlieren.

- Als Trägertechnologien für IP werden in mobilen Umgebungen von den Experten UMTS und WLAN bevorzugt. WLANs sind besonders mittelfristig die bedeutendste Technologieklasse in diesem Umfeld. DECT und GPRS werden in den Hintergrund treten.

- Bei den Methoden zur Durchsatzsteigerung von IP zeigt die Befragung ein uneinheitliches Bild. MPLS und Wirespeed-Routing werden zwar bedeutender als andere Technologien in diesem Umfeld, allerdings lässt sich auf Grund der Wertungen der Experten keine deutliche Aussage über zukünftige Entwicklungen treffen.

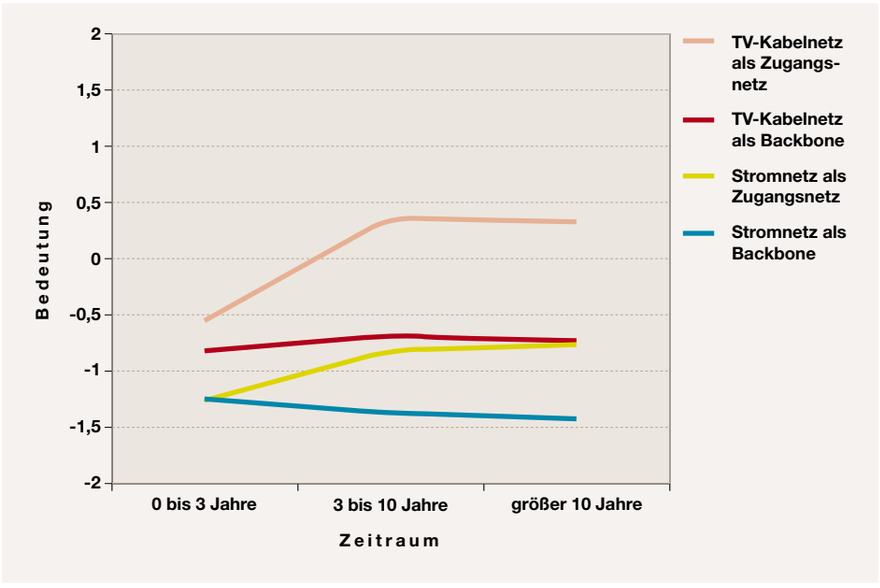



Abbildung 8.41: Bedeutung von bestehenden Infrastrukturen zum Aufbau von Kommunikationsnetzen

- MPLS-Netze sind nach den Ergebnissen der Befragung bereits im Jahr 2007 weit verbreitet. Ein durchgängiges MPLS-Netz wird allerdings von der Mehrheit der Befragten innerhalb der nächsten zehn Jahre nicht erwartet.
- Automobile mit Zugangsmöglichkeit zu öffentlichen Datennetzen sind 2008 weit verbreitet .
- Der Zugang elektrischer Geräte (z.B. Haushaltsgeräte) zu Kommunikationsnetzen ist erst 2011 weit verbreitet.
- TV-Kabel-Netze werden in den nächsten zehn Jahren in ihrer Bedeutung als Infrastruktur zum Aufbau von Zugangsnetzen stark zunehmen und damit Stromnetze in ihrer Bedeutung verdrängen. Im Backbone-Bereich erlangen weder Kabel- noch Stromnetze relevante Bedeutung.

### 8.2.4 Konvergenz der Netze und Endgeräte

Der übergreifende Trend zur Konvergenz (Abschnitt 6.6) zeigt sich im Bereich der Kommunikationsinfrastrukturen besonders ausgeprägt. Hervorzuheben ist hierbei das Zusammenwachsen von Mobil- und Festnetz zu einer durchgängigen Infrastruktur [Will 00]. Neben der Konvergenz der Netze ist auch ein Zusammenwachsen der Strukturen bei der Dienstnutzung und -bereitstellung zu beobachten [Euro 97]. Beide Konvergenzbestrebungen, im Bereich der Netze und der Dienste, wirken sich auch auf die Endgeräte aus, die entweder die Nutzung mehrerer Dienste oder die Anbindung an unterschiedliche Netze erlauben.

Heutige Datennetze bieten, besonders im Verteil- und Zugangsbereich, noch keine ausreichenden Qualitätseigenschaften, um eine durchgehende Übertragung von Sprachdaten über Datennetze (Ende zu Ende) zu ermöglichen [DaPe 00]. Allerdings werden laufend leistungsfähigere Vermittlungssysteme entwickelt und die zunehmenden Datenraten im lokalen Netz (Abschnitt 8.2.2) ermöglichen durch Over-Provisioning annehmbare Übertragungsqualität auch für Sprachdaten. Mit der absehbaren Bewältigung der grundsätz-

lichen technischen Probleme bei der Bereitstellung von QoS (Quality of Service) treten organisatorische Fragestellungen in den Vordergrund. So ist derzeit eine Einigung der Provider auf einen einheitlichen Mechanismus zur Signalisierung und Bereitstellung von QoS-Anforderungen nicht absehbar [Pige 01], obwohl entsprechenden Technologien existieren.

Eine Einschätzung der Entwicklungstendenzen beim Zusammenwachsen von Sprach- und Datenkommunikation wurde in diesem Abschnitt der Studie durch grundsätzliche Fragen nach der Ablösung der leitungsvermittelten Kommunikation aber auch durch Detailbetrachtungen im Bereich der Mobilkommunikation und VoIP (Voice over IP) abgefragt. Die Entwicklung im Mobilbereich wird am Ende dieses Kapitels in einem eigenen Abschnitt (8.2.7) ausführlich untersucht. Deshalb wird hier nur auf die Konvergenz der Endgeräte bezüglich Sprach- und Datenkommunikation eingegangen. Um grundsätzlich die Entwicklung beim Zusammenwachsen von Sprach- und Datennetzen zu beleuchten, wurden die Experten abschließend um eine Einschätzung der verhältnismäßigen Entwicklung von Umsatz und Volumen gebeten.

EINHEITLICHE DIENSTNUTZUNG UNABHÄNGIG VOM VERWENDETEN TRANSPORTNETZ: Eine Konvergenz der Dienste bezüglich des unterliegenden Netzes wird in 5 Jahren erwartet.

KONVERGENZ AUF NETZEBENE: Ein einheitliches Transprotnetz wird in 5 Jahren erwartet. Allerdings bezweifeln viele Experten generell eine entsprechende Vereinheitlichung.

VEREINHEITLICHUNG DER ENDGERÄTE: Endgeräte, die den Zugang zu unterschiedlichsten Transportnetzen erlauben, sind in 4 Jahren weit verbreitet.

## Ergebnisse

Der Trend zur Konvergenz der Endgeräte und der Netze wurde durch Thesen über das Zusammenwachsen der Dienste und Endgeräte ebenso geprüft, wie durch die Abfrage von Tendenzen bei der Vereinheitlichung der Netze. Auch im Bereich der an sich weitgehend standardisierten Dienste im Anwendungsgebiet der Kommunikationsnetze kann ein Zusammenwachsen der zugrundeliegenden Infrastrukturen erkannt werden. Die meisten Dienste im Bereich der klassischen Telekommunikationsnetze bauen bereits auf der einheitlichen Technologie des digitalen Telefonnetzes (ISDN) auf. Allerdings sind auch neue Vereinheitlichungsbestrebungen zu erkennen. So ist es seit kurzem möglich, den aus den GSM-Netzen bekannten SMS (Short Message Service) auch über das Festnetz zu nutzen [Gole 01].

Die einheitliche Abrechnung der Dienstnutzung ist in Deutschland mit der Liberalisierung des Telefoniesektors weiter fortgeschritten, aber noch nicht endgültig verwirklicht. Viele Leistungen werden noch abhängig vom benutzten Transportnetz und nicht auf die eigentliche Dienstnutzung bezogen abgerechnet. Die Befragten sehen die Konvergenz auf Dienst-Ebene, also die einheitliche Dienstnutzung unabhängig vom verwendeten Transportnetz in etwa fünf Jahren umgesetzt (Abbildung 8.42, ①). Im Jahr 2000 wurde diese Konvergenz bereits für das Jahr 2003 von den Experen vorhergesagt. Besonders Dienste, die direkt von Personen benutzt werden, wie jegliche Art von Multimediadiensten, würden nach Meinung der Experten von einer derartigen Konvergenz profitieren.

Eine Vereinheitlichung des Transportnetzes ist durch die Liberalisierung im Telefonmarkt zwingend notwendig, um den Kunden durchgängig Telefoniedienste anbieten zu können. Der Trend zur Konvergenz in diesem Bereich zeigt sich auch durch die weit fortgeschrittene technologische Standardisierung. Eine vollständige Konvergenz auf Netzebene, also die Existenz eines einheitlichen Transportnetzes (Abbildung 8.42, ②) wird von den Experten allerdings in den nächsten zehn Jahren nicht erwartet. Damit wird eine Übereinstimmung mit Prognose aus dem Jahr 2000 erzielt. Auch damals hielt die Mehrheit der Expetrten eine derart starke Konvergenz für unrealisitisch.

Im Sektor der mobilen Endgeräte (Abschnitt 8.2.7) lässt sich seit Jahren die Vereinigung vielfältigster Funktionalitäten in einem Endgerät feststellen. Im Bereich der Endgeräte für TK-Netze ist dieser Trend ebenfalls auszumachen. Der Funktionsumfang von Mobil- und Tischtelefonen nimmt stetig zu, Standards für die mobile Anbindung im in-house-Bereich, z.B. DECT, lassen die Grenzen zwischen mobilen und fest installierten Geräten verschwimmen. Endgeräte, die den Zugang zu unterschiedlichen (Transport-)Netzen erlauben sind noch nicht weit verbreitet. Mit Kombigeräten für DECT und GSM [Sage 03] sind erste Ansätze erkennbar. Die endgültige Vereinheitlichung der Endgeräte wird in etwa vier Jahren erwartet, wobei die Angaben der Experten stark schwanken, so dass manche Experten auch der Meinung sind, dass eine Konvergenz der Endgeräte in den nächsten zehn Jahren nicht zu erwarten sei (Abbildung 8.42, ③). Noch vor drei Jahren wurde in der Vorgänger-

studie [SETIK 00] eine weite Verbreitung entsprechender Endgeräte bereits für das Jahr 2003 vorhergesagt. Als typische Geräte, die in Zukunft den Zugang zu verschiedenen Netzen ermöglichen werden, benennen die Experten Fernseher mit Set-Top-Boxen und Mobiltelefone.

Sprachkommunikation auf Basis von IP (VoIP) gilt als Schlüssel für ein endgültiges Zusammenwachsen der Daten- und Sprachnetze. Die Befragung ergab, dass eine Verfügbarkeit entsprechender Techniken, die eine Sprachkommunikation auf Basis von IP mit der aus Sprachnetzen üblichen Qualität ermöglicht, bereits für das Jahr 2007 erwartet wird. Die Experten sehen hier auch, wie aus Abbildung 8.42, ④ erkennbar ist, einen sehr engen Zeitraum für die Umsetzung entsprechender Technologien, weisen aber explizit darauf hin, dass eine Erweiterungen der QoS-Mechanismen in IP erforderlich sei. In der Vorgängerstudie wurde die weite Verbreitung von IP-basierter Telefonie bereits für das Jahr 2004 prognostiziert.

Mit der Frage nach der Ablösung der leitungsvermittelnden Kommunikation durch paketvermittelte Übertragung, wie sie beispielsweise IP bietet, wurde die grundsätzliche Tendenz beim Zusammenwachsen von Sprach- und Datenkommunikation abgefragt. Eine Ablösung der Leitungsvermittlung durch die Paketvermittlung wird im Durchschnitt in sieben bis acht Jahren erwartet. Im Zugangsnetz auf der sog. Last Mile wird die Ablösung allerdings erst in etwa zehn Jahren erwartet. Damit wird der langfristige Trend zur Konvergenz von Sprach- und Datennetzen bestätigt.

Zusätzlich zeigt die nach Backbone (Abbildung 8.42, ⑤) und Zugangsnetz (Abbildung 8.42, ⑥) getrennte Auswertung, dass eine Konvergenz im Backbone wesentlich früher erwartet wird. Anzumerken ist hier auch, dass die Experten aus dem Industrieumfeld die Entwicklung wesentlich optimistischer, etwa zwei Jahre früher, einschätzen, als die Experten aus dem Forschungsumfeld. Im Jahr 2000 ging die Mehrheit der Befragten davon aus, dass die Ablösung der leitungsvermittelnden durch die paketvermittelnde Kommunikation im Prognosezeitraum der Vorgängerstudie, also bis 2010, nicht eintreten würde.

Wie bereits in der Einleitung zu diesem Abschnitt angedeutet, spiegelt sich die Konvergenz der Netze auch im Bereich der Endgeräte wider. In etwa fünf Jahren, zwei Jahre später als noch in der Vorgängerstudie prognostiziert, werden von den Experten kombinierte, fest installierte Endgeräte erwartet (Abbildung 8.42,⑦), die sowohl für Sprach- als auch für Datenkommunikation verwendet werden können. Mobile Endgeräte mit den selben Eigenschaften werden im Jahr 2006, ebenfalls zwei Jahre später als in der Vorgängerstudie prognostiziert, erwartet (Abbildung 8.42, ⑧). Im Vergleich zur Entwicklung in den Netzen findet die Konvergenz der Endgeräte etwa zwei bis vier Jahre früher statt und kann somit als „Enabler" für die Konvergenz im Netzbereich angesehen werden. Kombinierte mobile Endgeräte werden nach Aussagen der Experten hierbei ein besondere Rolle spielen. Erste Versionen werden von den Experten aus der Industrie bereits in zwei Jahren erwartet.

Das immer stärkere Zusammenwachsen der Kommunikation in Mobil- und Festnetzen, respektive eine Vereinheitlichung der entsprechenden Infrastrukturen, wird auch durch das Verhältnis der Kommunikationsvolumina in beiden Netzen bestimmt. Dabei richten sich Konvergenzbestrebungen nicht unbedingt am Kommunikationsvolumen sondern möglicherweise auch an den erzielbaren Umsätzen aus. Abbildung 8.43 zeigt die Einschätzungen der Experten bezüglich des erwarteten Verhältnisses der Volumina und Umsätze im Fest- und Mobilnetz.

Aus der Darstellung ist ersichtlich, dass die Entwicklung für die übertragenen Datenmengen und die erzielten Umsätze nach Einschätzung der befragten Experten sehr ähnlich verlaufen. Langfristig wird sich grob ein Verhältnis von 1:1 einstellen. Viele Experte merken allerdings an, dass dies eher auf einer weiteren Steigerung der Datenmenge im Mobilbereich zurückzuführen sei als auf einer Abnahme der Menge im Festnetz.

Abbildung 8.44 zeigt abschließend die relative Entwicklung von Sprach- und Datenkommunikation, wie sie von den befragten Experten gesehen wird. Deutlich zu erkennen ist dabei, dass sich das Verhältnis von Sprach- zu Datenkommunikation, sowohl bei Umsätzen als auch beim über-

SPRACHKOMMUNIKATION AUF BASIS VON IP: VoIP mit der Qualität heutiger Sprachnetze ist in 4 Jahren verfügbar.

ABLÖSUNG DER LEITUNGSVERMITTLUNG DURCH DIE PAKETVERMITTLUNG: Die Paketvermittlung wird die Leitungsvermittlung in 7 Jahren in ihrer Bedeutung verdrängt haben.

KOMBINIERTE, FEST INSTALLIERTE ENDGERÄTE: In 5 Jahren sind Endgeräte verbreitet, die sowohl zur Sprach- als auch zur Datenkommunikation verwendet werden können.

KOMBINIERTE MOBILE ENDGERÄTE: Mobile Endgeräte zur Nutzung von Sprach- und Datenkommunikation sind in 3 Jahren verbreitet.

VOLUMINA UND UMSÄTZE IM FEST- UND MOBILNETZ: Das starke Übergewicht der Kommunikation im Festnetz wird langfristig durch Steigerungen im Mobilbereich aufgehoben.

ENTWICKLUNG VON SPRACH- UND DATENKOMMUNIKATION: Aus dem Übergewicht der Sprachkommunikation entwickelt sich ein leichtes Übergewicht der Datenkommunikation.

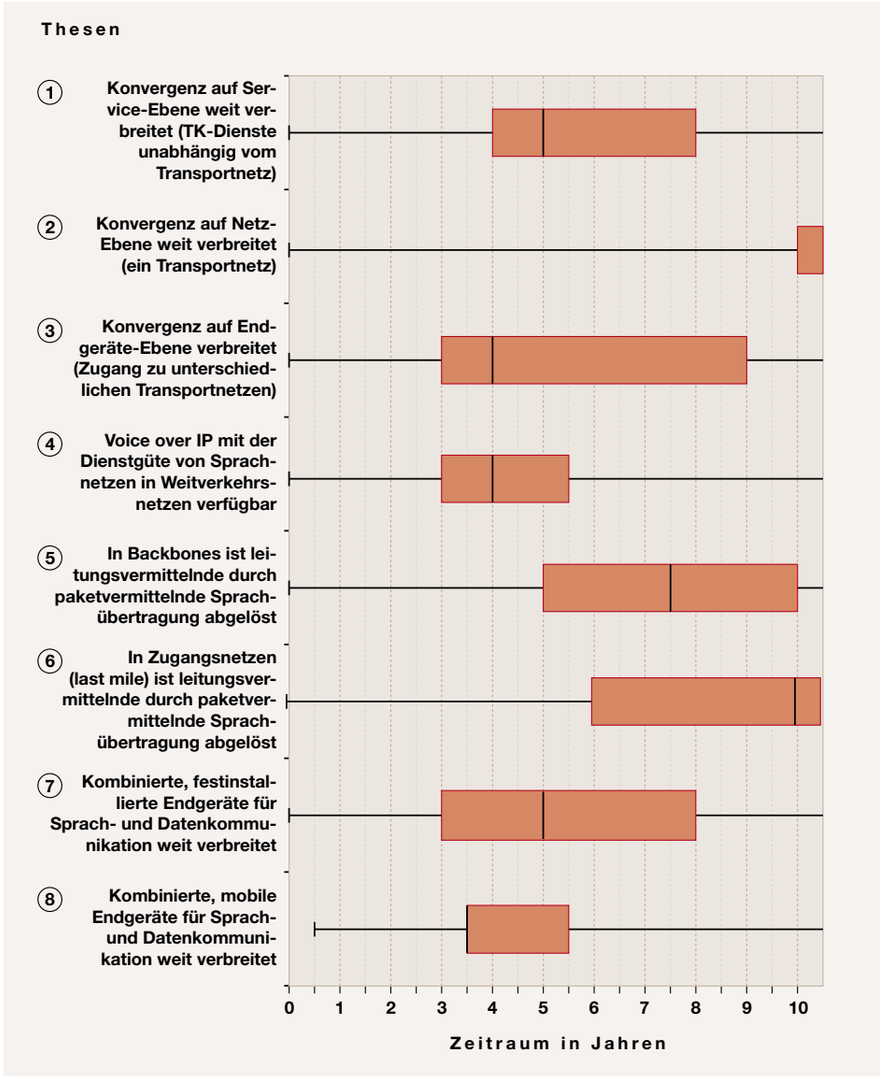



Abbildung 8.42: Ergebnisse der Thesen im Bereich Konvergenz der Netze und Endgeräte

tragenen Volumen vom heutigen starken Übergewicht der Sprachkommunikation zu einem Übergewicht der Datenkommunikation hin verschieben wird. Die Befragten weisen diesbezüglich darauf hin, dass sie hohe Steigerungen im Bereich der Datenkommunikation erwarten, die einem nahezu konstanten Aufkommen an Sprachkommunikation gegenüberstehen, wodrurch sich langfristig ein Übergewicht der Datenkommunikation ergibt. Zudem wird angemerkt, dass bereits heute im Bereich der Datenkommunikation Leistungen zu Grenzkosten angeboten werden. Nach dem Boom der letzen Jahre und der damit verbundenen, teilweise mehr als bedarfsgerechten Bereitstellung von Bandbreite, rechnen die Experten nicht mit steigenden Preisen im Bereich der Datenkommunikation. Diese Einschätzung spiegelt sich auch in der nahezu identischen Entwicklung bei Volumen und Umsatz wider.

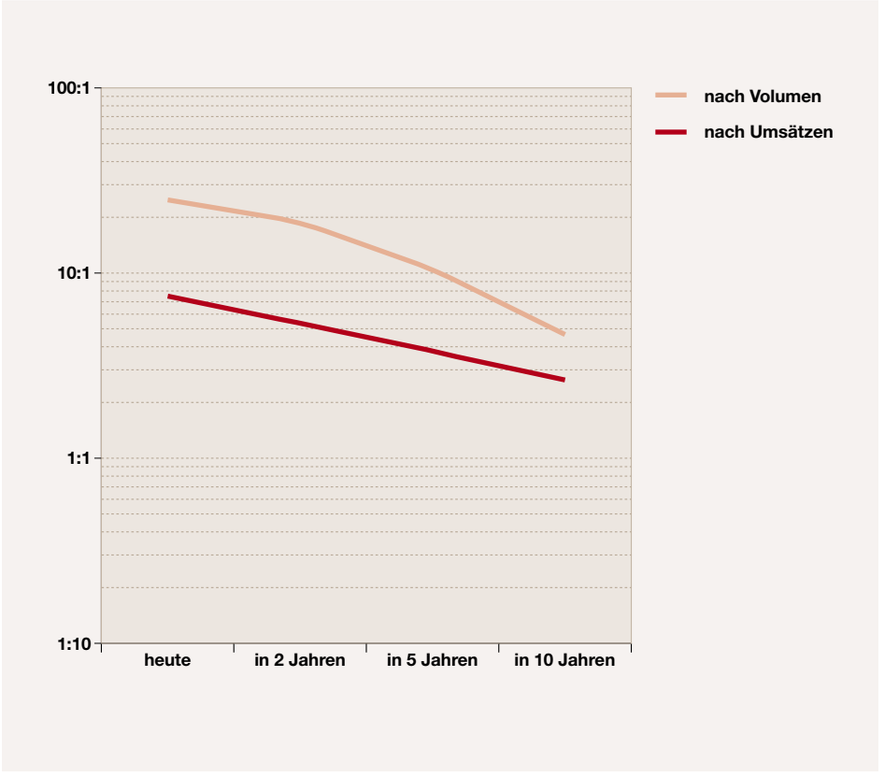



Abbildung 8.43: Entwicklung des Verhältnisses zwischen Fest- und Mobilkommunikation in TK-Netzen

## Zusammenfassung

Langfristig wird von den Experten eine gänzliche Konvergenz sowohl der Netze, als auch der zugehörigen Endgeräte erwartet. Der Trend zu einem einheitlichen Netz für Sprach- und Datenkommunikation wird von den Experten auch durch die Einschätzung der relativen Umsatz- und Volumenentwicklung in Sprach- und Datennetzen bestätigt. Der Trend zur Konvergenz spiegelt sich im Bereich der Kommunikationsnetze wie folgt wider:

- Das Zusammenwachsen von Diensten, also ein einheitliches Dienstangebot unabhängig vom zugrundeliegenden Transportnetz wird 2008 erwartet.
- Ein einheitliches Transportnetz wird nach Meinung der Experten bis zum Jahr 2013 nicht verbreitet sein.
- Endgeräte, die den Zugang zu unterschiedlichen Transportnetzen ermöglichen, werden 2007 erwartet. Auch hier halten einige Experten eine entsprechende Vereinheitlichung für unrealistisch.
- IP-basierte Sprachkommunikation (VoIP) mit einer Dienstgüte, die mit heutigen Sprachnetzen vergleichbar ist, wird auch in Weitverkehrsnetzen im Jahr 2007 verfügbar sein.
- Die paketvermittelnde Übertragung wird die leitungsvermittelnde Übertragung im Bereich der Sprachübertragung auf Backbones in etwa im Jahr 2011 ablösen.
- In Zugangsnetzen wird die paketvermittelnde Sprachübertragung die leitungsvermittelnde Übertragung erst 2013 ablösen.
- Kombinierte Endgeräte für Sprach- und Datenkommunikation im Bereich der fest installierten Endgeräte sind im Jahr 2008 weit verbreitet.

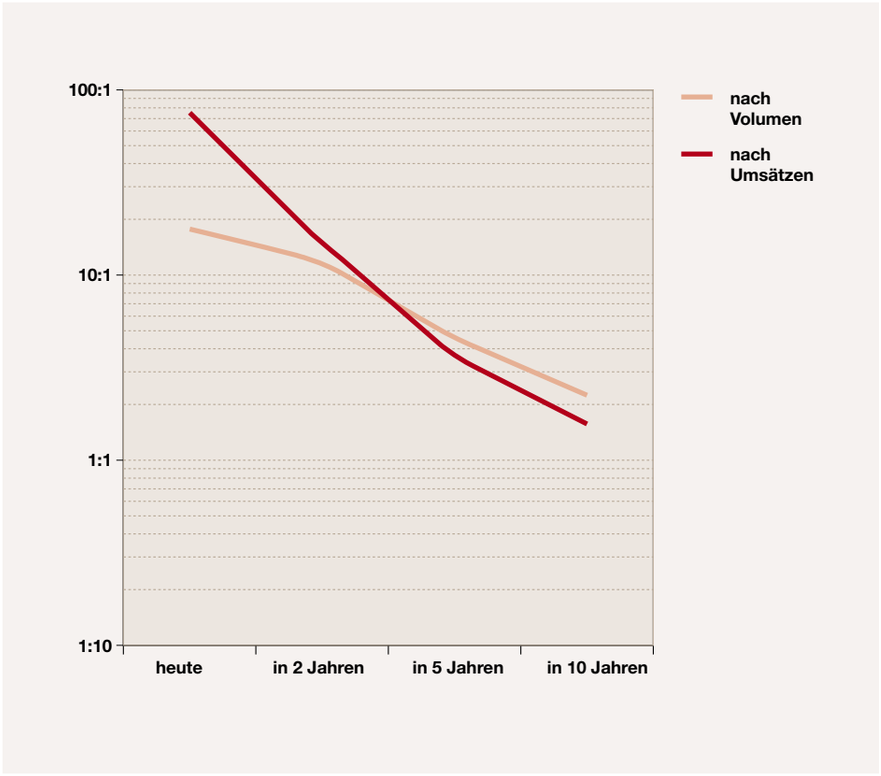



Abbildung 8.44: Relative Entwicklung von Sprach- und Datenkommunikation

- Bereits im Jahr 2006 werden mobile, kombinierte Endgeräte für Sprach- und Datenkommunikation weit verbreitet sein.

- Bei der Entwicklung der Kommunikation im Festnetz im Verhältnis zur Kommunikation im Mobilnetz wird von den Experten langfristig ein Gleichgewicht prognostiziert. In der heutigen Situation sehen sie ein starkes Übergewicht der Kommunikation im Festnetz.

- Das Verhältnis von Sprach- zu Datenkommunikation wird sich sowohl im Volumen als auch in den Umsätzen von einem deutlichen Übergewicht der Sprachkommunikation hin zu einem leichten Übergewicht der Datenkommunikation entwickeln.

### 8.2.5 Dienstorientierung, garantierte Dienstgüte und Dienstplattformen

Mit der wahrnehmbaren Leistungssteigerung im Bereich der Kommunikationsnetze trat der rein funktionale Aspekt der Diensterbringung in den Hintergrund. Ein Dienst muss nicht nur eine bestimmte (Kommunikations)Leistung zur Verfügung stellen, sondern diese auch mit der geforderten Qualität erbringen. Wie im Abschnitt 8.2.4 bereits beschrieben, wird die Bereitstellung garantierter Dienstgüten in Datennetzen als Schlüssel zur Konvergenz der Netze gesehen.

Der Grad der Umsetzung der Dienstorientierung in Kommunikationsnetzen zeigt sich besonders an den zur Verfügung stehenden Managementschnittstellen. Bei einer dienstorientierten Leistungserbringung muss diese auch durch entsprechende Managementschnittstellen unterstützt werden [HAN 99], die ein dienstorientiertes Management erlauben und damit das klassische Komponentenmanagement ab-

lösen. In [Lang 01] wurden bereits vor einigen Jahren entsprechende Schnittstellen vorgeschlagen.

Um eine bestimmte Dienstgüte garantieren zu können sind sowohl geeignete Architekturen für deren Bereitstellung als auch entsprechende Signalisierungsprotokolle notwendig. Seit einigen Jahren werden in diesem Bereich Ansätze wie IntServ oder DiffServ zur Bereitstellung von QoS und RSVP (Resource Reservation Setup Protocol) [IETF 97a] zur Signalisierung der QoS-Anforderungen neben Ansätzen, die direkt auf Übertragungstechniken basieren, diskutiert.

Entsprechend dieser Ausgangslage wurden von den Experten Einschätzungen zur Verbreitung von Managementschnittstellen, Dienstgütearchitekturen und entsprechenden Beschreibungstechniken ebenso wie eine Bewertung existierender Ansätze zur Signalisierung von Dienstgüteanforderungen und zur Bereitstellung von Dienstgüte abgefragt.

## Ergebnisse

Mit einer Ablösung des komponentenorientierten Managements durch dienstorientiertes Management ist nach Aussage der Experten in etwa acht Jahren zu rechnen (Abbildung 8.45, ①). Noch in der Vorgängerstudie [SETIK 00] hatten die Experten eine Ablösung in etwa für das Jahr 2005 prognostiziert. Eine völlige Ablösung des komponentenorientierten Managements wird, ebenfalls im Bezug zur Vorgängerstudie, zunehmend in Frage gestellt. Ebenso weisen einige Experten darauf hin, dass die Konzepte des Dienstmanagements noch nicht ausgereift genug seien, um eine zügige Umsetzung zu ermöglichen.

Standardisierte Beschreibungstechniken zur Spezifikation der Funktionalität und der Güte eines Dienstes werden als Schlüssel zu einer umfassenden, dienstorientierten Leistungserbringung mit entsprechendem Trading gesehen. Die Verfügbarkeit entsprechender Beschreibungstechniken wird von der Mehrheit der Experten in etwa sechs Jahren erwartet (Abbildung 8.45, ②). Gegenüber der Befragung im Jahr 2000 hat sich diese Prognose um zwei Jahre nach hinten verschoben.

Dienstgütegarantien, die auch Ende-zu-Ende eingehalten werden, sind besonders im Internet notwendig, wenn dieses als umfassende Infrastruktur sowohl für Sprach- als auch für Datenkommunikation genutzt werden soll. Besonders Multimediadienste sind, wie in Abschnitt 8.2.4 beschrieben, auf entsprechende Dienstgütegarantien im Internet angewiesen. Mit einer Verbreitung von Dienstgütegarantien im Internet rechnet die Mehrheit der Befragten in etwa sieben Jahren (Abbildung 8.45, ③). Auffallend ist, dass im wissenschaftlichen Umfeld die Verbreitung von QoS-Garantien im Internet bereits zwei Jahre früher, im Jahr 2007, vorhergesagt und damit die Prognose aus dem Jahr 2000 getroffen wird.

In einem dienstorientierten Markt können Dienste unterschiedlichster Provider vom Kunden nach speziellen Vorgaben wie z.B. Qualitätsanforderungen ausgewählt werden. Diese idealen Möglichkeiten sind im Moment noch nicht gegeben [UMTS 00]. Allerdings hat die Befragung ergeben, dass bereits im Jahr 2008 entsprechende Möglichkeiten bestehen werden. Optimistische Nennungen gehen vom Jahr 2006 aus (Abbildung 8.45, ④). Im Jahr 2000 hatte noch die Mehrheit der Experten vorhergesagt, dass eine kundenspezifische Dienstzusammenstellung nach Dienstgüteanforderungen bereits heute (2003) möglich sein wird.

In der Einleitung zu diesem Abschnitt wurde bereits auf die Notwendigkeit geeigneter Schnittstellen für ein dienstorientiertes Management hingewiesen. Entsprechende Schnittstellen, über die Großkunden die vom Provider erbrachte Dienstgüte überwachen können, werden von der Mehrheit der Experten in fünf Jahren erwartet, wobei optimistische Nennungen bereits vom Jahr 2005 ausgehen und wenige Experten diese Schnittstellen bereits heute für realisiert betrachten (Abbildung 8.45, ⑤). Für Privatkunden werden entsprechende Schnittstellen erst in etwa neun Jahren erwartet (Abbildung 8.45, ⑥).

Wird der Gedanke der Dienstorientierung konsequent umgesetzt, dann müssen auch Managementschnittstellen bereitgestellt werden, die es den Kunden und Nutzern ermöglichen, selbständig aktive Managementeingriffe durchzuführen, um beispielsweise Konfigurationsparameter zu ändern. Eine Verbreitung von Ma-

DIENSTORIENTIERTES MANAGEMENT: Eine Ablösung des Komponentenmangements durch das Dienstmanagement findet erst in 8 Jahren, deutlich später als noch in der Vorgängerstudie prognostiziert, statt

BESCHREIBUNGSTECHNIKEN: Das Trading von Diensten wird in etwa 6 Jahren durch die Verbreitung entsprechender Beschreibungstechniken ermöglicht.

DIENSTGÜTEGARANTIEN IM INTERNET: Ende-zu-Ende Zusicherung von QoS wird in 7 Jahren verbreitet sein.

KUNDENSPEZIFISCHE DIENSTZUSAMMENSTELLUNG NACH DIENSTGÜTEANFORDERUNGEN: In 5 Jahren werden Möglichkeiten zur kundenspezifischen Dienstzusammenstellung bestehen.

VOM PROVIDER ERBRACHTE DIENSTGÜTE: Großkunden können über entsprechende Schnittstellen die Dienstgüte in 5 Jahren überwachen, Privatkunden erst in 9 Jahren.

AKTIVE MANAGEMENTEINGRIFFE: Großkunden können in 7 Jahren die Dienstgüte aktiv selbst beeinflussen. Für Privatkunden ist die Umsetzung entsprechender Schnittstellen in den nächsten 10 Jahren nicht zu erwarten.

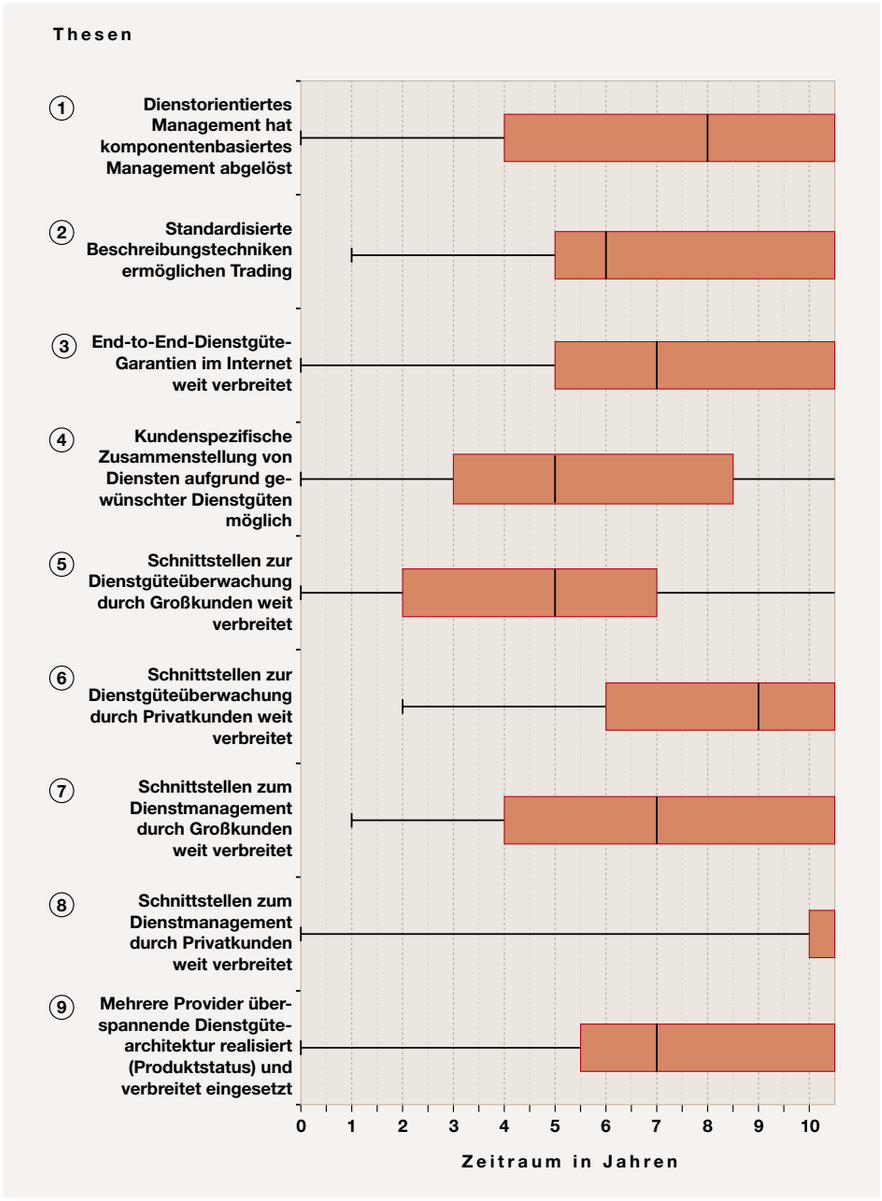



Abbildung 8.45: Ergebnisse der Thesen zu Dienstorientierung und Dienstgüte

nagementschnittstellen zur Beeinflussung der Dienstgüte für Großkunden wird von den Experten in sieben Jahren, von einigen Experten bereits wesentlich früher, erwartet (Abbildung 8.45, ⑦). Bei Privatanwendern zeigt sich ein deutlich indifferenteres Bild: Die Mehrheit der Experten sehen innerhalb des Beobachtungszeitraums von zehn Jahren keine Verbreitung dieser Schnittstellen. Einige wenige Experten gehen bereits heute von einer Verbreitung derartiger Schnittstellen aus, wenn extrem standardisierte Dienste „on-demand" verfügbar sind (Abbildung 8.45, ⑧).

Zur Bereitstellung einer garantierten Dienstgüte bei weltweiter Kommunikation ist der Einsatz einer durchgängigen, das heißt Provider-übergreifenden, Dienstgütearchitektur unerlässlich. In den letzten Jahren wurde eine Vielzahl von Architekturen vorgeschlagen, welche die Provider-übergreifende Bereitstellung von Dienstgüte ermöglichen. Allerdings sind die meisten dieser Ansätze nicht über ein Betastadium hinaus gekommen. Entsprechend gehen die befragten Experten davon aus, dass eine Provider-übergreifende QoS-Architektur mit Produktstatus erst in sieben Jahren verbreitet eingesetzt werden wird (Abbildung 8.45, ⑨). Eine detaillierte Betrachtung von einzelnen Technologien und Protokollen zur Bereitstellung von garantierten Dienstgüten erfolgt im weiteren Verlauf dieses Abschnittes.

Wie bereits erwähnt, sind in den letzten Jahren eine Vielzahl von Mechanismen zur Bereitstellung garantierter Dienstgüten, besonders im Multimediaumfeld, entwickelt worden. Zur Abschätzung der zukünftigen Entwicklung in diesem Bereich wurde von den Experten die Einschätzung der Bedeutung von verschiedenen Mechanismen zur Bereitstellung von QoS abgefragt. Die entsprechenden Ergebnisse sind in Abbildung 8.46 dargestellt.

Eine wirklich deutliche Entwicklung ist aus den Ergebnissen der Befragung nicht ableitbar. Auffallend ist, dass alle abgefragten Technologien in ihrer Bedeutung sehr eng zusammen liegen. Erkennbar ist jedoch, dass von den Experten MPLS langfristig als bedeutendste Technologie betrachtet wird. Die heute noch an erster Stelle stehenden, auf SDH und ATM basierenden Technologien, werden innerhalb des Prognosezeitraums relativ zu den anderen Technologien stark an Bedeutung verlieren.

Wird die Auswertung allerdings nach Angaben aus dem Industrieumfeld und dem Bereich der Forschungsinstitute aufgeteilt so ergibt sich ein anderes Bild: Die Unentschlossenheit der Experten zeigt sich im Bereich der Industrie noch stärker.

Nach Meinung der Experten aus der Wissenschaft ergibt sich ein deutlicher Vorsprung in der Bedeutung von MPLS gegenüber allen anderen Technologien, der über den gesamten Beobachtungszeitraum weiter ausgebaut wird. Im Vergleich zur Vorgängerstudie ist in diesem Bereich mit MPLS eine neue Technologie erschienen, die von den Experten auch bereits favorisiert wird.

Neben der reinen Bereitstellung von garantierter Dienstgüte in Kommunikationsnetzen müssen auch Protokolle zur Verfügung stehen, mit denen die gewünschte Qualität eines Dienstes signalisiert werden kann. Je nach unterliegender Dienstgütearchitektur muss die Möglichkeit bestehen, die Dienstgüteanforderungen sehr feingranular und auch zwischen Transitsystemen zu signalisieren. Im Rahmen der vorliegenden Studie wurde die Einschätzung der Experten bezüglich der beiden Protokolle IPv6 und RSVP abgefragt. Die Entwicklung der Bedeutung dieser beiden Technologien ist in Abbildung 8.47 dargestellt.

Es ist deutlich erkennbar, dass die Experten langfristig IPv6 gegenüber RSVP vorziehen. Kurzfristig wird beiden Technologien von den Experten die gleiche Bedeutung zugewiesen. Der langfristige Bedeutungsverlust von RSVP könnte darin begründet liegen, dass die Experten langfristig die Verbreitung von IPv6 auch als Transportprotokoll erwarten (Abschnitt 8.2.3, Abbildung 8.33) und somit RSVP als Zusatzprotokoll zu IPv4 nicht mehr eingesetzt werden muss.

Eine vollständige Dienstorientierung erfordert auch die dynamische und kundengerechte Bereitstellung von Diensten. Um diesen Vorgang zu vereinfachen und zu beschleunigen erweisen sich standardisierte Plattformen als zweckmäßig. Die Entwicklung und Implementierung von Diensten auf Basis von Dienstplattformen wird durch die Existenz herstellerübergreifender Schnittstellen deutlich vereinfacht.

PROVIDER-ÜBERGREIFENDE QOS-ARCHITEKTUR: Eine Provider-übergreifende Architektur mit Produkstatus ist in 5 Jahren verfügbar.

MECHANISMEN ZUR BEREITSTELLUNG VON QoS: MPLS wird langfristig die bedeutendste Technologie bei der Bereitstellung und Garantie von Dienstgüte.

DIENSTGÜTE-ANFORDERUNGEN: Mit der zunehmenden Verbreitung von IPv6 werden auch QoS-Anforderungen mit diesem Protokoll signalisiert werden.

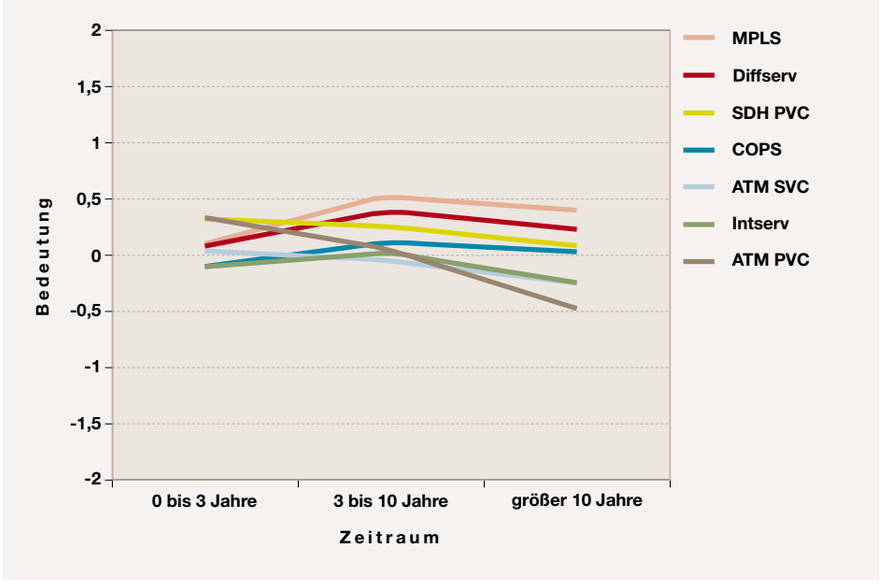



Abbildung 8.46: Bedeutung von Mechanismen zur Bereitstellung garantierter Dienstgüten (z.B. für Multimedia-Anwendungen)

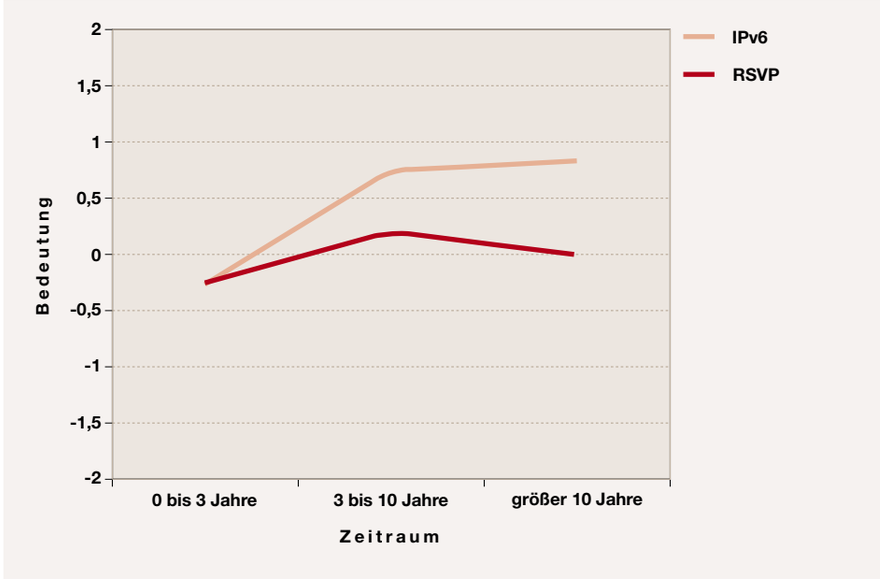



Abbildung 8.47: Bedeutung von Protokollen zur Signalisierung von Dienstgüteanforderungen

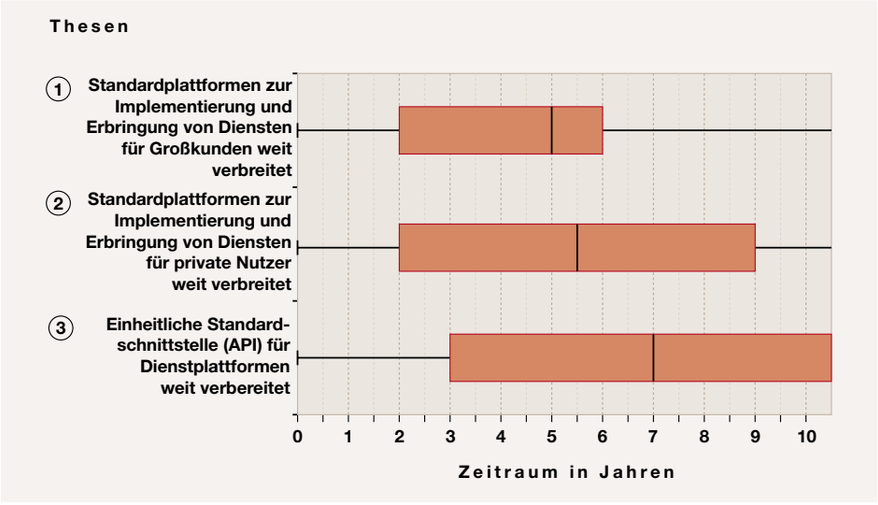



Abbildung 8.48: Ergebnisse der Thesen zu Dienstplattformen

Werden Dienste für Großkunden implementiert, wird die weite Verbreitung von Dienstplattformen bereits ein Jahr früher, also 2008 erwartet (Abbildung 8.48, ①). Die Befragten aus dem Bereich der Wissenschaft sehen diese These bereits im Jahr 2006, und damit zwei Jahre früher, bestätigt.

Die Mehrheit der Experten erwartet den weit verbreiteten Einsatz von Dienstplattformen bei der Diensterbringung für private Nutzer etwa im Jahr 2009 (Abbildung 8.48, ②). Einzelne Experten sehen diese Plattformen, wie z.B. den standardisierten Zugriff auf E-Mail oder die defacto Standardplattform Windows-PC bereits heute weit verbreitet.

Eine API (Application Programmers Interface), zum Zugriff auf Dienstplattformen, die damit eine standardisierte Dienstimplementierung erlaubt, wird von den Experten in etwa sieben Jahren erwartet. Mit Java und diversen Scriptsprachen wie Perl oder CGI (Common Gateway Interface) [GGB 01] stehen nach Meinung einiger Experten bereits heute geeignete Schnittstellen zur Verfügung. Auch hier sehen die Befragten, die nicht im industriellen Umfeld tätig sind, ähnlich wie bei der Verbreitung von Dienstplattformen, zwei Jahre früher, bereits im Jahr 2008 eine weite Verbreitung dieser Schnittstellen.

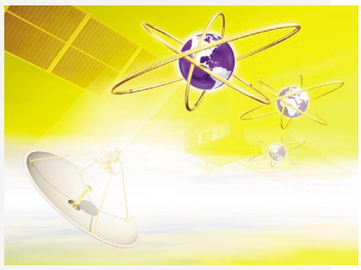
## Zusammenfassung

Die Betrachtung der Entwicklungen im Bereich der Dienstorientierung, Erbringung von Dienstgüte und Nutzung von Dienstplattformen hat vor allem gezeigt, dass die Experten in ihrer Einschätzung heute wesentlich pessimistischer sind als noch bei der vorangegangenen Befragung im Rahmen der Vorgängerstudie. Im einzelnen hat sich folgendes ergeben:

- Dienstorientiertes Management hat 2011, sechs Jahre später als in der Vorgängerstudie prognostiziert, das komponentenbasierte Management abgelöst.
- Standardisierte Beschreibungstechniken für die Funktionalität und Güte von Diensten ermöglichen im Jahr 2009 die automatische Auswahl von Diensten und Dienstanbietern (Trading) .
- End-to-End-Dienstgüte-Garantien sind im Internet 2010 weit verbreitet. Nur Experten aus der Wissenschaft unterstützen noch die Vorhersage (im Jahr 2006) von 2000.
- Die kundenspezifische Zusammenstellung von Diensten aufgrund gewünschter Dienstgüten ist ab 2008 möglich, war aber 2000 schon für 2003 vorhergesagt.

EINSATZ VON DIENSTPLATTFORMEN: Die Diensterbringung auf Basis standardisierter Plattformen ist für private Nutzer in 6 Jahren, für Großkunden in 5 Jahren, weit verbreitet.

ZUGRIFF AUF DIENSTPLATTFORMEN: Der standardisierte Zugriff auf Dienstplattformen über eine API ist in 7 Jahren weit verbreitet.



- Im Jahr 2010 ist eine mehrere Provider überspannende Dienstgütearchitektur realisiert (Produktstatus) und wird verbreitet eingesetzt.
- Schnittstellen, über die Kunden die vom Dienstanbieter garantierte Dienstgüte überwachen, werden von Großkunden 2008 weit verbreitet eingesetzt. Für Privatkunden werden diese erst 2012 verbreitet nutzbar sein.
- Schnittstellen, über die Kunden die vorhandenen Dienstgüten durch Managementeingriffe selbst beeinflussen können, werden von Großkunden ab 2010 weit verbreitet eingesetzt. Für Privatanwender ist eine klare Prognose nicht möglich.
- Als Mechanismus zur Bereitstellung garantierter Dienstgüten prognostizieren die Experten aus der Wissenschaft, auch langfristig, für MPLS als neuer Technologie in diesem Bereich die größte Bedeutung. Aus den Aussagen der Experten im industriellen Umfeld lässt sich, auch langfristig, keine deutliche Prognose ableiten.
- Als Protokoll zur Signalisierung von Dienstgüteanforderungen wird langfristig, wie es sich auch als Transportprotokoll durchsetzen wird, IPv6 verwendet werden.
- Ab 2009 werden standardisierte Plattformen zur Implementierung und Erbringung von Diensten für den privaten Nutzer weit verbreitet eingesetzt.
- Zur Erbringung und Implementierung von Diensten für Großkunden werden standardisierte Plattformen im Jahr 2008 weit verbreitet eingesetzt.
- Eine einheitliche Schnittstelle für Dienstplattformen (API) ist 2010 weit verbreitet.

## 8.2.6 Flexible programmierbare Netze

Der methodische Ansatz der flexibel programmierbaren Netze basiert auf dem Grundgedanken, Dienst- und Komponentenorientierung auch innerhalb der Kommunikationsnetze und nicht nur bei ihrer Anwendung umzusetzen. Damit können individuell, also kundenspezifisch, Netze mit bestimmten Eigenschaften auf Basis der bereits vorhandenen Vermittlungskomponenten aufgebaut werden. Innerhalb des MSF (Multiservice Switching Forum) [Mult 02] wird bereits an der Spezifikation von Schnittstellen gearbeitet, die eine einfache, herstellerübergreifende Implementierung von Vermittlungsfunktionen unterschiedlichster Komplexität auf bestehenden Systemen zulassen. Aus dem Blickwinkel der Provider, die bisher, je nach Kundenwünschen, unterschiedlichste Netze in Hardware aufbauen mussten, tragen die flexibel programmierbaren Netze damit zur Automatisierung und Vereinfachung bei. Die Entwicklung einer API zur Realisierung von Vermittlungsfunktionalitäten [Mult 02] unterstützt den Einsatz des Konzepts der flexibel programmierbaren Netze, in dem so die Möglichkeit geboten wird, kurzfristig die vorhandenen Vermittlungsfunktionen an neue Anforderungen anzupassen.

Der Entwicklungstrend der flexibel programmierbaren Netze [Giem 99] zeigt sich nicht nur im ständig steigenden Einsatz von VPNs (Virtual Private Network) oder entsprechend flexibler Vermittlungskomponenten, sondern auch in einer entsprechend angepassten Flexibilisierung des Managements dieser Komponenten und der Weiterentwicklung von flexiblen Managementmethoden [HAN 99], wie des Managements by Delegation [Moun 97] und dem Einsatz mobiler Agenten [GHR 99, PhKa 98, RoHo 98].

Die zunehmende Flexibilisierung der Kommunikationsnetze zeigt sich zunächst durch den Einsatz von VPNs, der sich mittlerweile auch auf das Standardprotokoll IP ausdehnt. Langfristig ist eine Ablösung der derzeitigen, monolithischen Vermittlungskomponenten durch programmierbare Systeme notwendig, um den Entwicklungsansatz der flexibel programmierbaren Systeme vollständig umsetzen zu können. Ebenso muss

innerhalb dieser Komponenten eine kundenspezifische Trennung der Vermittlungsfunktionalitäten möglich sein. Zum effizienten Management der dabei entstehenden hoch dynamischen und vernetzen Systeme bietet sich der Einsatz von Konzepten wie mobiler Agenten oder des „Managements by Delegation“ an .

## Ergebnisse

Eine weite Verbreitung von VPNs auf der Basis von IP wird vom Durchschnitt der Befragten im Jahr 2006 erwartet (Abbildung 8.49, ①). Bei einer detaillierten Betrachtung zeigt sich, dass 25% der Befragten aus dem wissenschaftlichen Umfeld IP-VPNs bereits heute als weit verbreitet betrachten. Die Mehrheit der Wissenschaftler sieht eine weite Verbreitung dieser Technologie allerdings erst in drei Jahren.

Eine Ablösung der derzeit vorhandenen, monolithischen Vermittlungssysteme durch flexibel programmierbare Systeme wird von den Experten erst in zehn Jahren erwartet (Abbildung 8.49, ②). Begründet wird dies mit den zu erwartenden großen Problemen beim Management und Aufbau dieser Komponenten. Zusätzlich wird angemerkt, dass sich entsprechende Komponenten gegen die Konkurrenz einfacher, aber preiswerter, monolithischer Systeme auf Basis von ASICs (Application-Specific Integrated Circuit) (Abschnit 8.1 und [Kieß 99]) behaupten müssen. In der Vorgängerstudie [SETIK 00] wurde diese These von den Experten noch optimistischer bewertet: Sie rechneten mit der weiten Verbreitung flexibler Netzkomponenten bereits im Jahr 2008, also fünf Jahre früher.

Getrennte Ablaufumgebungen auf Netzkomponenten, die kundenabhängig Forwardingmechanismen bieten, werden nach Meinung der Befragten erst in neun Jahren erwartet (Abbildung 8.49, ③). Auch hier wird die pessimistische Prognose mit vermuteten Managementproblemen begründet. Andererseits merken einige Experten an, dass mit MPLS und VPN-Konzepten bereits heute eine Basis für die Umsetzung entsprechender Komponenten geschaffen sei. Auch hier waren die Befragten im Jahr 2000 wesentlich optimistischer und sagten die weite Verbreitung entsprechender Komponenten ebenfalls fünf Jahre früher voraus.

Mit der Umsetzung des Paradigmas der mobilen Agenten bietet sich die Möglichkeit, auch in hochgradig heterogenen und verteilten Systemen, übersichtliche Mangementlösungen zu schaffen. Somit bieten diese Systeme eine Möglichkeit, der Komplexität im Management flexibel programmierbarer Netze zu begegnen. Sichere und interoperable Systeme, die mobile Agenten einsetzen, werden von den Befragten im Jahr 2008 erwartet (Abbildung 8.49, ④). Im Vergleich zur Vorgängerstudie ist hier die Prognose ebenfalls um zwei Jahre pessimistischer ausgefallen. Besonders die von den Experten erwarteten Sicherheitsprobleme führen hier zu einer wenig optimistischen Bewertung, wenngleich im Bereich des Managements und des E-Commerce Anwendungsmöglichkeiten für mobile Agenten gesehen werden.

Wie bereits in der Einleitung zu diesem Abschnitt angemerkt, sehen die Experten skalierende Managementansätze wie „Management by Delegation“ als Voraussetzung für den Aufbau flexibler, dynamischer Netze. Eine weite Verbreitung dieses Konzepts, das auch eine dynamische Erweiterung der Managementfunktionalität zur Laufzeit zulässt, erwarten die Experten im Jahr 2008 (Abbildung 8.49, ⑤). Auch diese These wurde mit einer Differenz von etwa drei Jahren, deutlich pessimistischer bewertet als im Jahr 2000. Als Probleme bei der Umsetzung nennen die Befragten hier den gestiegenen Aufwand zur Beherrschbarkeit dieses Managementansatzes und ähnlich hohe Sicherheitsprobleme wie beim Einsatz mobiler Agenten.

## Zusammenfassung

Im Bereich der flexibel programmierbaren Netze hat sich bei allen Thesen gezeigt, dass die Experten mit ihren Einschätzungen gegenüber der Vorgängerstudie im Jahr 2000 pessimistischer geworden sind. Offenbar sind die Überlegungen nach der rein funktionalen Umsetzbarkeit der beschriebenen Ansätze den weit komplexeren Fragestellungen Managements und Sicherheit (im Sinne von Security) gewichen.

VPNS AUF DER BASIS VON IP: In 3 Jahren ist mit einer weiten Verbreitung dieser Technologie zu rechnen.

FLEXIBEL PROGRAMMIERBARE SYSTEME: Technische und organisatorische Probleme behindern nach Meinung der Experten eine Ablösung monolithischer durch flexibel programmierbare Komponenten, die auch erst in 10 Jahren erwartet wird.

GETRENNTE ABLAUFUMGEBUNGEN AUF NETZKOMPONENTEN: Probleme beim Management dieser Komponenten lassen eine weite Verbreitung erst in 9 Jahren zu.

MOBILE AGENTEN: Systeme auf Basis mobiler Agenten werden wegen der vielfältigen Sicherheitsproblematiken bei iherem Einsatz erst in 5 Jahren erwartet.

MANAGEMENT BY DELEGATION: Die Befragten erwarten einen hohen Mangementaufwand und massive Sicherheitsproblem beim Einsatz dieser Lösungen, den sie in etwa 5 Jahren erwarten.

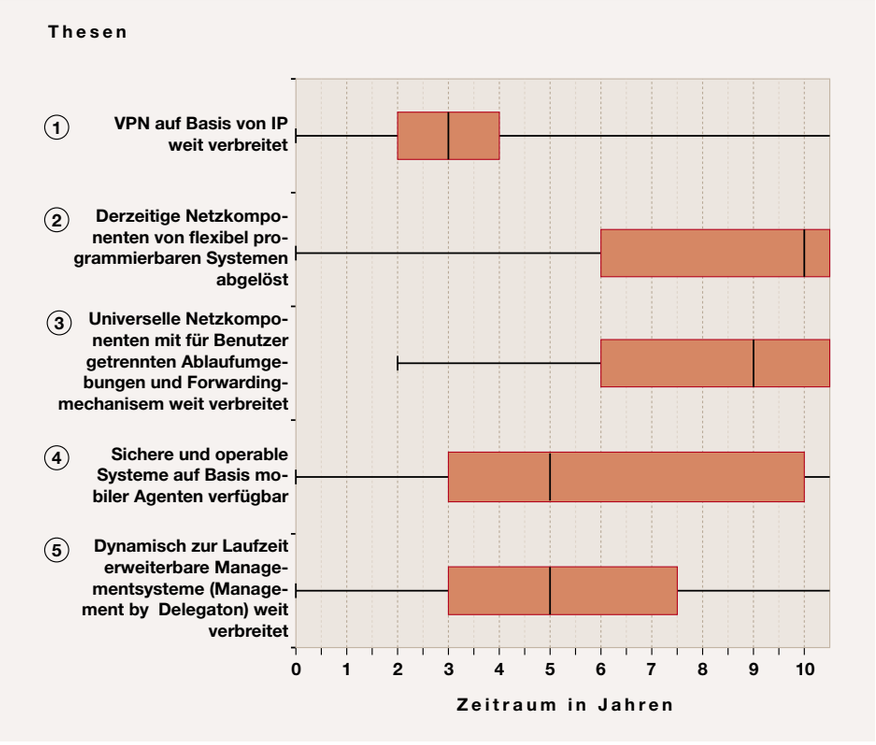



Abbildung 8.49: Ergebnisse der Thesen zu flexibel programmierbaren Netzen

- VPNs auf Basis von IP werden im Jahr 2006 weit verbreitet eingesetzt.
- Derzeitige Netzkomponenten werden von flexibel programmierbaren Systemen nicht vor 2013 abgelöst. Im Jahr 2000 wurde hierfür noch das Jahr 2008 prognostiziert.
- Universelle Netzkomponenten, die für Benutzer getrennte Ablaufumgebungen zur Verfügung stellen, um spezifische Forwardingmechanismen zu realisieren, werden ab 2012 weit verbreitet eingesetzt.
- Sichere und operable Systeme auf Basis mobiler Agenten sind im Jahr 2008 verfügbar.
- Drei Jahre später als in der Vorgängerstudie prognostiziert werden dynamisch zur Laufzeit erweiterbare Managementsysteme (Management by Delegatoin) erst im Jahr 2008 weit verbreitet eingesetzt werden.

### 8.2.7 Mobile Computing und drahtlose Netze

Der Sektor des Mobile Computing zeigt sich als klassischer Querschnittsbereich der Informations- und Kommunikationstechnik. Praktisch alle in Abschnitt 6 bezeichneten übergreifenden Trends finden in diesem Bereich ihren Niederschlag. An erster Stelle ist der anhaltende Trend zur Mobilität (vgl. 6.8) zu nennen, der als Triebfeder für dieses Gebiete der Rechnerkommunikation betrachtet werden muss. Die für mobile Endsysteme entwickelten Infrastrukturen wie GSM, WLANs oder UMTS tragen zur weiteren Vernetzung und Flexibilisierung (vgl. 6.9) bei und erschließen neue Anwendungsgebiete für Kommunikationsnetze, wie am Ende von Abschnitt 8.2.3 beschrieben. Die heute wahrnehmbare weite Verbreitung mobiler Endgeräte, die ihrerseits neue Formen der mobilen Kommunikation fordert, ist erst durch die Kapazitäts und Leistungssteigerung (vgl. 6.5) der letzten Jahre bei gleichzeitiger Miniaturisierung (vgl. 6.7) ermöglicht worden. Die dabei erschlossenen Märkte wirken mittlerweile wieder

als Triebfeder für weitere Leistungssteigerung und Miniaturisierung (vgl. Abbildung 5.2 in Abschnitt 5). Große Anwendungsfelder, wie beispielsweise die Mobiltelefonie, konnten erst nach umfangreicher Integration und Standardisierung (vgl. 6.4) erschlossen werden. Für neue Anwendungsfelder, wie ad-hoc Networking, wird eine erfolgreiche Standardisierung als Voraussetzung für zukünftige Entwicklungen gesehen. Durch den enormen technischen Aufwand, der notwendig ist, um eine Infrastruktur für mobile Netze aufzubauen, fördern diese Entwicklungen auch den Trend zur Konvergenz (vgl. 6.6) auf eine oder wenige Infrastrukturen. Neuere Entwicklungen wie GPRS oder HSCSD (High Speed Circuit Switched Data) [Roth 02], die auf der vorhandenen GSM-Infrastruktur aufbauen, bestätigen diesen Trend.

In diesem Abschnitt werden sowohl die zukünftigen Entwicklungen im Bereich der Mobilität der Endgeräte als auch Anwendungsprotokolle und Infrastrukturen beleuchtet. Ein Ausblick auf die weiteren Entwicklungsmöglichkeiten im Bereich der Mobilkommunikation rundet diesen Abschnitt ab. UMTS wird hier explizit als Infrastruktur betrachtet, weil sie, wie keine andere Technologie, die verschiedenen Trends im Bereich der Mobilkommunikation vereint. Damit entstehen oft gegenläufige Entwicklungen, die eine langfristige Prognose über den Einsatz dieser Technologie erschweren. Neben den technischen Problemen auf der Luftschnittstelle wird auch die Frage nach geeigneten Hintergrundinfrastrukturen sowie möglichen Organisationsformen beim Einsatz von UMTS gestellt.

## Ergebnisse

Die Mobilität der Anwender zusammen mit ihren Endgeräten ist nur möglich, wenn neben geeigneten Infrastrukturen auch Dienste angeboten werden, die eine für den Endanwender sinnvolle Benutzung dieser Infrastrukturen zulassen. Um Mobile Computing für eine Vielzahl von Anwendern zu ermöglichen, müssen Infrastrukturen mit entsprechend hohen Datenraten existieren und zusätzlich müssen die darauf realisierten Dienste die notwendige Flexibilität bieten. WLANs werden als eine Möglichkeit angesehen, neben den klassischen Mobilfunknetzen GSM und UMTS, eine Infrastruktur für Mobile Computing aufzubauen, die hohe Datenraten bietet. Gleichzeitig fordert die mobile Nutzung von Diensten eine flexible Verlagerung der Dienstnutzung von Endgerät zu Endgerät ebenso wie die Mobilität des Endgerätes während der Dienstnutzung.

WLANs, die als öffentliches Zugangsnetz zur Verfügung stehen, werden von den Experten bereits Ende des Jahres 2006 erwartet (Abbildung 8.50, ①). Von einem WLAN als öffentliches Zugangsnetz versprechen sich die Experten vor allem neue Anwendungen im geschäftlichen Bereich. Gleichzeitig wird angemerkt, dass sich WLANs wesentlich einfacher aufbauen lassen als UMTS-Netze und damit zumindest kurzfristig und bei Insellösungen (Hotspots) zu bevorzugen sind.

Hochratige Anbindungen mobiler Endgeräte erlauben beispielsweise auch die Nutzung von Multimediadiensten wie Bildtelefonie. Nach Meinung der Experten sind Anbindungen der Endgeräte mit Datenraten größer-gleich 10 MBit/s in sechs Jahren weit verbreitet (Abbildung 8.50, ②). Von den Befragten wird in diesem Zusammenhang angemerkt, dass mit dem WLAN-Standard zwar bereits eine Technologie existiert, die eine hohe Datenrate zuläßt, diese aber nur allen Endgeräten gemeinsam, als shared Medium, zur Verfügung steht und nicht exklusiv genutzt werden kann. Damit begründet sich auch die Meinung einiger Experten, welche die hochratige, exklusive Anbindung mobiler Endgeräte über die Luftschnittstelle in den nächsten zehn Jahre nicht erwarten.

Die beliebige Nutzung eines Dienstes ohne Rücksicht auf das verwendete mobile Gerät ist nach Meinung der Befragten in sechs Jahren möglich (Abbildung 8.50, ③). Allerdings wird angemerkt, dass es immer Dienste geben wird, die ein spezifisches Endgerät voraussetzen, also die Mobilität, im Sinne einer freien Auswahl des Endgeräts einschränken.

WLAN ALS ÖFFENTLICHES ZUGANGSNETZ: WLANs werden bereits in 3 Jahren als öffentlicher Zugang zu drahtlosen Netzen weit verbreitet eingesetzt werden.

HOCHRATIGE ANBINDUNGEN MOBILER ENDGERÄTE: In 6 Jahren werden hochratige Anbindungen (>= 10 MBit/s) über die Luftschnittstelle weit verbreitet sein. Allerdings stehen die Datenraten nicht exklusiv für ein Endgerät zur Verfügung.

MOBILITÄT, IM SINNE EINER FREIEN AUSWAHL DES ENDGERÄTS: Die Nutzung eines Dienstes, unabhängig vom verwendeten Endgerät, ist in 6 Jahren möglich.

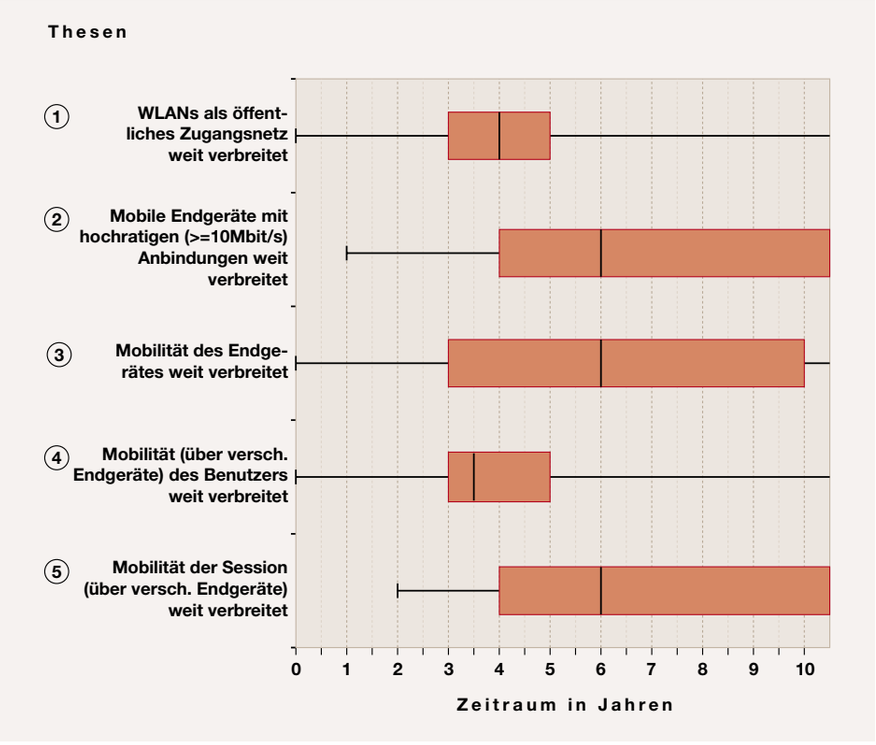



Abbildung 8.50: Ergebnisse der Thesen zu mobile Computing

MOBILITÄT DES BENUTZERS: Bereits heute können einige Dienste von mobilen Benutzern in Anspruch genommen werden. In 4 Jahren wird die mobile Dienstnutzung weit verbreitet sein.

MOBILITÄT DER SESSION: Von den Experten wird die beliebige Verlagerung einer Session nicht als vordringliches Problem angesehen. Die Umsetzung der Sessionmobilität ist in 6 Jahren zu erwarten.

INFRASTRUKTUREN FÜR MOBILE DATENKOMMUNIKATION: UMTS und WLAN erlangen langfristig die höchste Bedeutung beim Aufbau mobiler Netze.

Bereits im Jahr 2007 wird eine Nutzung von Diensten durch mobile Benutzer möglich sein. Diese Mobilität des Benutzers ist heute beispielsweise schon beim Telefoniedienst realisiert und wird schrittweise auf andere Dienste ausgedehnt werden (Abbildung 8.50, ④).

Die Verlagerung einer Session während der Dienstnutzung, also die Mobilität der Session wird von den Experten als schwer zu bewältigendes Problem gesehen, dessen Lösung jedoch für eine weitere Ausdehnung des Mobile Computing als nicht zwingend notwendig erachtet wird. Entsprechend wird prognostiziert, dass die Mobilität der Session erst in sechs Jahren verbreitet sein wird (Abbildung 8.50, ⑤). Eine Vielzahl der Befragten geht davon aus, dass dies innerhalb der nächsten zehn Jahre nicht realisiert werden wird.

Die Möglichkeit des Zugangs zum Internet von mobilen Endgeräten aus gilt als Gradmesser für die fortschreitende Ausbreitung des Mobile Computing. Im Moment existiert eine Vielzahl von technischen Möglichkeiten, den Internetzugang von mobilen Endgeräten aus zu nutzen. Ein Abschätzung des Einsatzgrades dieser Technologien liefert eine deutliche Perspektive für die Verbreitung und Konvergenz von Infrastrukturen für mobile Datenkommunikation. Entsprechend wurde von den Experten eine Einschätzung über die Bedeutung von GSM, GPRS, HSCSD, UMTS und WLAN als mögliche Technologien für einen mobilen Netzzugang abgefragt. Abbildung 8.51 zeigt die Bewertung der Bedeutung dieser Techniken durch die Befragten.

Langfristig werden UMTS und WLAN die größte Bedeutung erlangen. Die auf GSM aufsetzenden Technologien GPRS und HSCSD sowie GSM selbst, werden zunehmend an Bedeutung verlieren. Die Entwicklung der Bedeutung von UMTS und WLAN verläuft nach Meinung der Experten fast identisch. Damit ist es auf Basis der Aussagen der Experten nicht möglich, die Infrastruktur der Zukunft eindeutig zu bestimmen. Es wird aber deutlich, dass sowohl WLANs als auch UMTS vom heutigen Standpunkt aus ein großes Entwicklungspotenzial zugesprochen wird.

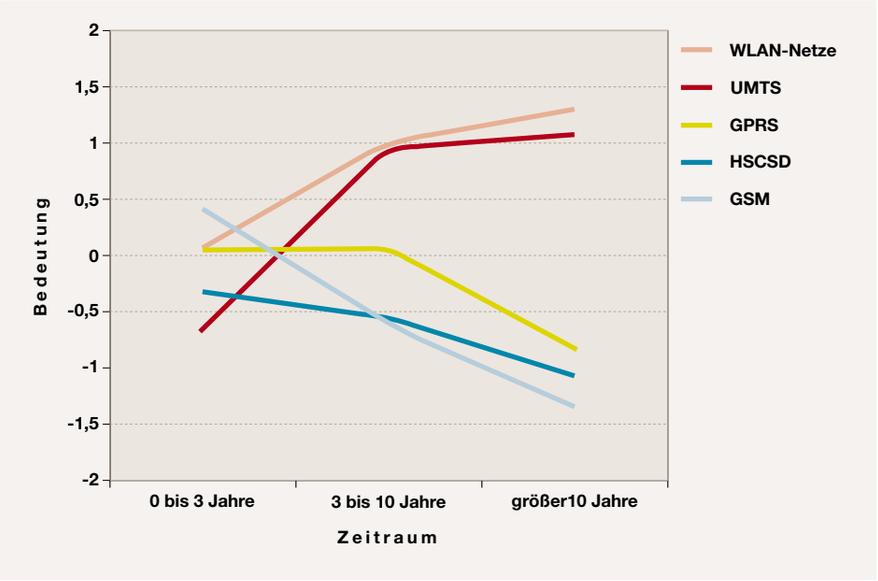



Abbildung 8.51: Bedeutung von Infrastrukturen für den mobilen (Inter)Netzzugang

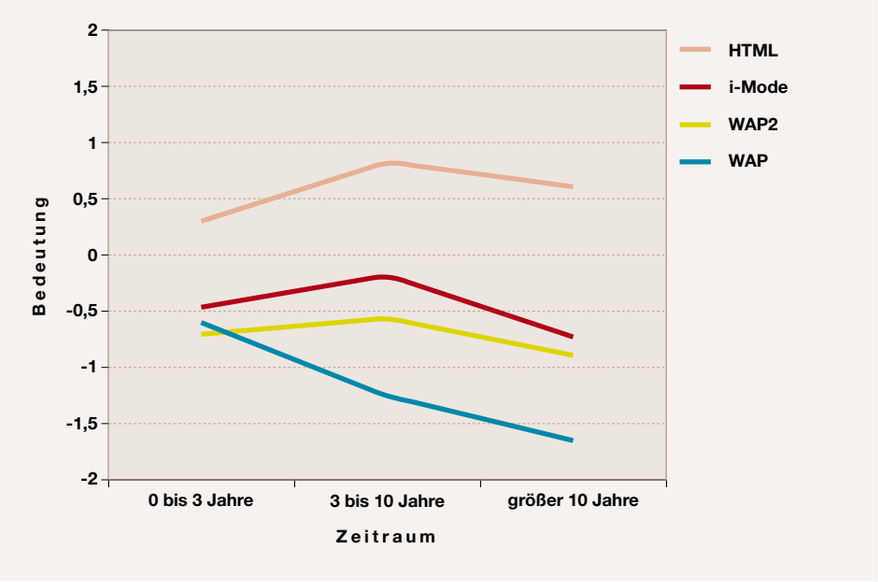



Abbildung 8.52: Bedeutung von Anwendungsprotokollen für mobile Endgeräte

Neben den Technologien für den mobilen Netzzugang sind auch standardisierte Anwendungsprotokolle notwendig, um eine mobile Dienstnutzung zu ermöglichen. Mit WAP (Wireless Application Protocol), dem Nachfolger WAP2 sowie I-Mode und HTML (Hyptertext Markup Language) [MuKe 01] wurden den Experten bekannte Anwendungsprotokolle zur Bewertung vorgelegt. Abbildung 8.52 zeigt die dabei ermittelten Einschätzungen.

ANWENDUNGSPROTOKOLLE FÜR MOBILE ENDGERÄTE: HTML wird sich auch in mobilen Netzen als Anwendungsprotokoll durchsetzen.

WAP und WAP2 (siehe zum Beispiel die Spezifikation auf der Web-Seite www.zionwap.net/wapspec.htm) haben bereits heute eine geringere Bedeutung als I-Mode und HTML, das über den gesamten Prognosezeitraum hinweg in seiner Bedeutung wesentlich höher eingeschätzt wird als alle anderen Protokolle. Nach ihren Aussagen gehen die Experten davon aus, dass sich mit steigenden Übertragunsraten im Mobilbereich HTML als im Festnetz bereits etabliertes Anwendungsprotokoll durchsetzen wird. Ebenso erwarten die Befragten langfristig die Entwicklung neuer Anwendungsprotokolle für mobile Endgeräte. Spezielle Produkte oder Standards werden von den Experten allerdings nicht genannt. Aus dieser Einschätzung ergibt sich auch der Verlust an Bedeutung bei allen abgefragten Technologien am Ende des Prognosezeitraums.

NETZE DER 4. GENERATION: Weiterentwicklungen der G3-Technologien sind in 8 Jahren verfügbar.

KONVERGENZ VON 3G-TECHNIKEN: Die Möglichkeit einer Konvergenz der etablierten 3G-Techniken zu einem neuen 4G-Standard wird von vielen Experten bezweifelt. Dennoch wird in 8 Jahren die Verfügbarkeit entsprechender Technologien prognostiziert.

INFRASTRUKTUREN FÜR DEN MOBILEN NETZZUGANG: Eine Beschränkung des Ausbaus von Infrastrukturen (Funkmasten) ist nach Meinung der Experten in den nächsten 10 Jahren nicht zu erwarten.

Die Betrachtung des Bereichs Mobile Computing wird durch die Abschätzung einiger Prognosen über die zukünftige Entwicklung im Bereich der drahtlosen Netze abgeschlossen. Die Einschätzung der weiteren Entwicklungsmöglichkeiten dieser Netze steht dabei stellvertretend für die zukünftigen Entwicklungen im gesamten Bereich des Mobile Computings. Wie aus Abbildung 8.53 ersichtlich, wurden den Experten Thesen zur Weiterentwicklung und Konvergenz der 3G-Netze wie UMTS und WLAN ebenso zur Bewertung vorgelegt, wie eine These zur Einschätzung der gesellschaftlichen Akzeptanz der Mobilfunkinfrastrukturen.

Die Befragten gehen davon aus, dass Netze der 4. Generation durch Weiterentwicklung der bisherigen Techniken in etwa acht Jahren verfügbar sein werden (Abbildung 8.53, ①), prognostizieren also einen ähnlichen Innovationszyklus wie bei der Weiterentwicklung von GSM, das 1991 den Regelbetrieb aufnahm [EVB 01]. Von vielen Experten wird allerdings die Notwendigkeit zu einer Weiterentwicklung der 3G-Netze bezweifelt, da die vorhandenen Techniken als ausreichend leistungsfähig bewertet werden.

Ähnliche Prognosen werden von den Befragten für die Konvergenz von 3G-Techniken gegeben. Durch Konvergenz bestehender Technologien entstandene Netze werden ebenfalls in acht Jahren erwartet (Abbildung 8.53, ②). Viele Experten geben jedoch zu bedenken, dass eine derartige Konvergenz wegen der stark unterschiedlichen Realisierungen der verschiedenen bestehenden Technologien, wie WLAN oder Bluetooth, und den fehlenden technologieübergreifenden Managementansätzen praktisch nicht stattfinden wird.

Infrastrukturen für den mobilen Netzzugang erfordern den flächendeckenden und sichtbaren Einsatz von Infrastruktureinrichtungen wie Funkmasten oder Access-Points. Die gesundheitlichen Gefahren, die von der elektromagnetischen Abstrahlung dieser Einrichtungen ausgehen sind noch nicht völlig erfasst und in der Bevölkerung regt sich zunehmend Widerstand gegen die Aufstellung neuer Sendemasten [Elek 03]. Für die Entwicklung zukünftiger Netze könnte dies bedeuten, dass nur noch auf bereits vorhandene Zugangspunkte (Sendemasten) zurückgegriffen werden kann, was die Leistungsfähigkeit neuer Netze erheblich einschränken könnte. Allerdings sehen die Experten nicht, dass dieser Zustand innerhalb der nächsten zehn Jahre eintreten wird (Abbildung 8.53, ③). Begründet wird diese Einschätzung mit der immer weiter reduzierten Sendeleistung bei der Entwicklung neuer Technologien sowie der zunehmenden Aufklärung der Bevölkerung durch gesicherte Forschungsergebnisse.

In UMTS-Netzen wird mit CDMA (Code Devision Multiple Access) ein bisher nicht weit verbreitetes Verfahren zum Mulitplexing auf der Luftschnittstelle verwendet. Erste UMTS-Prototypen haben gezeigt [KAL$^+$ 01], dass der Einsatz von CDMA nicht unproblematisch ist.

UMTS bietet in seiner Anwendung wesentlich mehr Möglichkeiten (z.B. Video-on-Demand) als das bisher verwendete GSM [KAL$^+$ 01]. Allerdings wird die Viel-

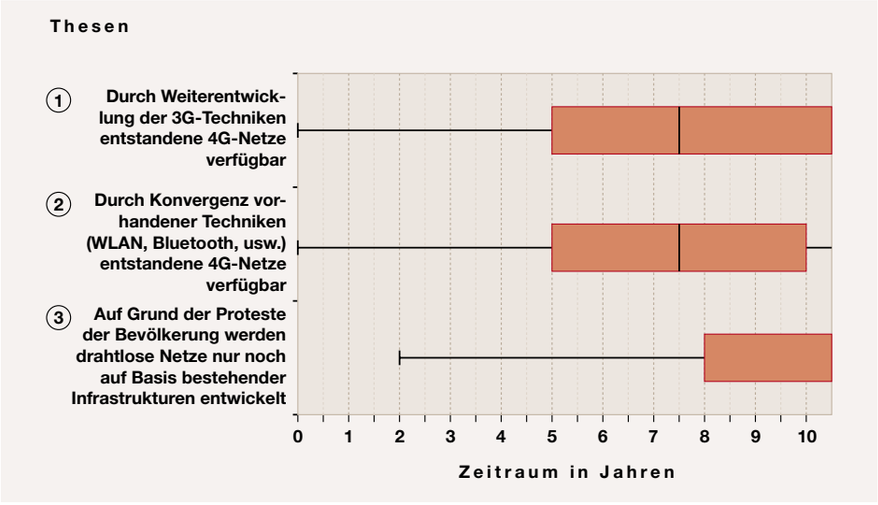



Abbildung 8.53: Ergebnisse der Thesen zur Weiterentwicklung drahtloser Netze

falt der Funktionen erst einsetzbar sein, wenn die Zusammenarbeit zwischen den einzelnen Anbietern intensiviert und flexibilisiert wird [UMTS 01]. Da UMTS als Technologie in der Vorgängerstudie [SETIK 00] nicht betrachtet wurde, existieren in diesem Bereich keine Vergleichswerte.

Die Beseitigung der Probleme bei der Verwendung von CDMA in UMTS-Netzen wird von der Mehrheit der Experten bereits im Jahr 2005 erwartet (Abbildung 8.54, ①). Angemerkt wird hier, dass einige Hersteller dieses Problem bereits heute als gelöst betrachten. Entsprechend sind in den Antworten der Experten auch deutlich frühere Prognosen zu finden.

Mit der steigenden Verbreitung von UMTS werden auch neue, bisher nicht realisierbare, Dienste für mobile Engeräte (z.B. Videokonferenz, Internetzugang, kontextsensitive Dienste [Dey 00], siehe auch Abschnitt 9.3) erwartet. Viele dieser Dienste sind allerdings für den Endanwender nur zufriedenstellend nutzbar, wenn sie durchgängig im gesamten Netz ohne Rücksicht auf den aktuellen Provider genutzt werden können. Um die Vielfalt der technischen Möglichkeiten nutzen zu können, ist also eine technische und organisatorische Trennung des Netz- und Dienstbetriebs in UMTS notwendig. Der Vollzug dieser Trennung wird von der Mehrheit aller Experten in fünf Jahren erwartet (Abbildung 8.54, ②). Auffallend ist, dass die Befragten, die im industriellen Umfeld tätig sind, hier mit etwa acht Jahren eine deutlich pessimistischere Prognose abgeben. In diesem Zusammenhang wird häufig angemerkt, dass die hohen Preise, die für den Erwerb der UMTS-Lizenzen gezahlt werden mussten, die Netzanbieter auch langfristig zwingen werden, Kunden massiv an das eigene Netz zu binden, was z.B. durch das Angebot eigener Dienste durch den Netzanbieter erfolgen kann.

UMTS bietet neben dem reinen Telefoniedienst auch Datenkommunikationsdienste mit hoher, exklusiver Bandbreite (bis 2 MBit/s) und zugesicherten Qualitätseigenschaften an. Wie im Abschnitt 8.2.5 beschrieben, ist die Bereitstellung von QoS bereits im Festnetz eine Fragestellung, die einer zügigen Konvergenz der Netze entgegensteht. Die Spezifikation von UMTS als Dienst an der Luftschnittstelle bietet eine Vielzahl von Qualitätsparametern [3GPP 03]. Allerdings ist derzeit nicht klar, welche leitungsgebundene Infrastruktur verwendet werden soll, um ein flächendeckendes UMTS-Netz aufbauen zu können. Von den Experten wurde deshalb eine Einschätzung über die Bedeutung verschiedener Hintergrund-Infrastrukturen für UMTS abgefragt. Die entsprechenden Ergebnisse sind in Abbildung 8.55 dargestellt.

Aus der Abbildung ist ersichtlich, dass alle abgefragten Technologien im Moment annähernd gleich bewertet werden. Langfristig wird sich aber nach der Einschätzung der Experten IP als Hintergrund-

CDMA IN UMTS-NETZEN: Technische Probleme beim Einsatz dieses Multiplexingverfahrens sind in 2 Jahren gelöst.

TECHNISCHE UND ORGANISATORISCHE TRENNUNG DES NETZ- UND DIENSTBETRIEBS IN UMTS: Die hohen Kosten für die UMTS-Lizenzen lassen nach Meinung der Experten aus der Industrie diese Trennung auch langfristig nicht zu und wird erst in 8 Jahren und damit 4 Jahre später als vom Durchschnitt aller Befragten prognostiziert, erwartet.

HINTERGRUND-INFRASTRUKTUREN FÜR UMTS: Langfristig wird nur IP den Bedarf für Datenkommunikation im UMTS-Netz bewältigen können.

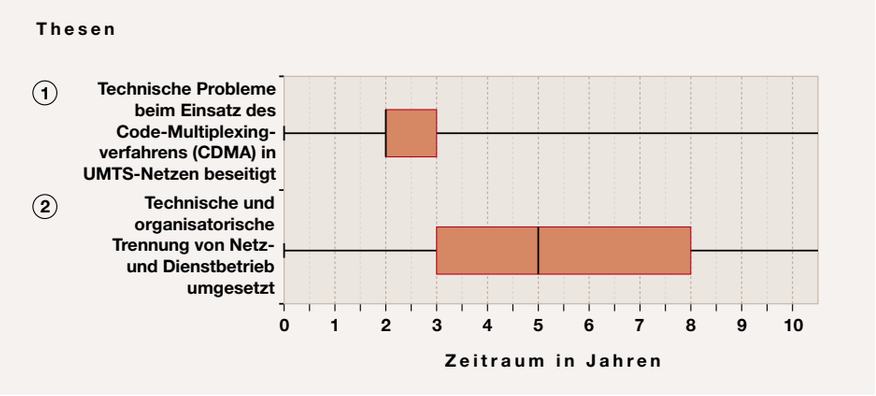



Abbildung 8.54: Ergebnisse der Thesen zum Einsatz von UMTS

Infrastruktur durchsetzen. Nach ihrer Meinung erfordert das zu erwartende Aufkommen an Datenverkehr (keine Sprachdaten) eine einfache und preiswerte Infrastruktur im Backbone. ATM und SDH werden von einigen Befragten als „Zwischenlösung" bezeichnet, die besonders beim Aufbau des Netzes eine hohe Verlässlichkeit bieten, dann aber zunehmend irrelevant würden. ISDN, das heute noch zur Anbindung von GSM-Sendemasten verwendet wird, wird stark an Bedeutung verlieren, da es den Bandbreitenbedarf von UMTS nicht decken kann.

## Zusammenfassung

Die Auswertung der Fragen zu diesem Bereich hat das Zusammenspiel der teilweise gegenläufigen Trends verdeutlicht und zugleich gezeigt, dass dieser Bereich der Rechnerkommunikation enorme Entwicklungschancen bietet. Die Einführung von UMTS liefert besonders in organisatorischer Sicht eine Menge an Herausforderungen. Die Experten haben in diesem Bereich folgende Prognosen aufgestellt:

- WLANs, die öffentlich als Zugangsnetz zur Verfügung stehen, sind im Jahr 2006 weit verbreitet.
- Mobile Endgeräte mit hochratigen (>=10MBit/s) Anbindungen sind 2009 weit verbreitet, allerdings werden diese Bandbreiten nicht exklusiv zur Verfügung stehen.
- 2009 ist es weit verbreitet, dass mobile Benutzer beliebige Dienste auf beliebigen mobilen Geräten nutzen können (Mobilität des Gerätes).
- Bereits 2007 können mobile Benutzer beliebige Dienste (neben Telefonie) auf mobilen Geräten nutzen (Mobilität des Benutzers).
- Die Mobilität der Session, also die beliebige Unterbrechung und Wiederaufnahme der Dienstnutzung bei einem Wechsel des Endgeräts wird von den Experten nicht als vordringliche Fragestellung betrachtet. Ihre Umsetzung wird für das Jahr 2009 prognostiziert.
- UMTS und WLAN setzen sich langfristig als Technologien für den drahtlosen Netzzugang durch.
- Als Anwendungsprotokoll in mobilen Netzen wird sich, ebenso wie im Festnetz HTML durchsetzen.
- 4G-Netze, die durch Weiterentwicklung der 3G-Techniken entstanden sind, sind in acht Jahren verfügbar.
- Durch Konvergenz vorhandener Techniken (WLAN, Bluetooth, usw.) sind drahtlose Netze der 4. Generation (4G) nach Meinung der Experten nur schwer zu entwickeln. Die Verfügbarkeit von Technologien, die durch Konvergenz entstanden sind, wird für das Jahr 2011 vorhergesagt.
- Bis zum Jahr 2013 wird sich nicht die Notwendigkeit ergeben, auf Grund von Protesten aus der Bevölkerung neue drahtlose Netze nur noch

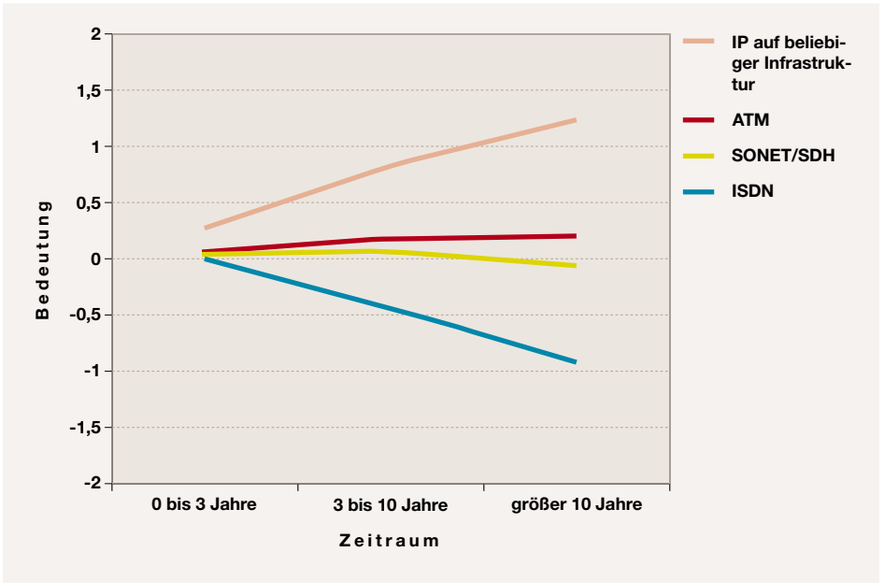



Abbildung 8.55: Bedeutung von Technologien zum Einsatz als Hintergrund-Infrastrukturen für UMTS

auf Basis bestehender Infrastrukturen (Größe und Lage von Funkzellen) zu entwickeln.

- Technische Probleme beim Einsatz des von CDMA in UMTS-Netzen sind nach Meinung der Experten im Jahr 2005 beseitigt.
- Die technische und organisatorische Trennung von Netz- und Dienstbetrieb in UMTS-Netzen ist nach der Einschätzung aller Befragten ab 2008 durchgeführt.
- Als Hintergrund-Infrastruktur für UMTS wird sich IP langfristig durchsetzen.

## 8.2.8 Sicherheit in drahtlosen Netzen

### 8.2.8.1 GSM

Ursprünglich als europäisches Verfahren zur digitalen Mobilkommunikation entwickelt, ist der Standard GSM inzwischen das international erfolgreichste zellulare Mobilfunkkonzept.

Der GSM-Standard wurde mit dem Anspruch entwickelt, keine zusätzlichen Sicherheitsrisiken gegenüber dem Festnetz mit sich zu bringen. Das Hauptaugenmerk wurde dabei auf die Luftschnittstelle gelegt, die gegenüber der herkömmlichen Festnetzleitung als anfälliger für Lauschangriffe galt, da man sich nicht physikalisch an eine Leitung anschließen muss, um mithören zu können, sondern der Zugang überall möglich ist. Drei Schutzziele werden dabei verfolgt: die Sicherstellung der Vertraulichkeit auf Verbindungsebene (nicht Ende-zu-Ende), die Authentizität der Nutzer gegenüber dem Netz und die Sicherheit gegenüber der Erstellung von Bewegungsprofilen. Die Umsetzung dieser Schutzziele ist allerdings weitgehend unbefriedigend und immer wieder teilweise heftiger Kritik ausgesetzt.

Zur Identifikation mobiler Teilnehmer wird im GSM-Mobilfunknetz die so genannte „SIM-Karte" (subscriber identification module) verwendet, auf der u.a. der geheime Schlüssel zur Authentikation des mobilen Endgeräts gegenüber einer Basisstation gespeichert ist. Diese Identifikation ist in bestimmten Fällen angreifbar. So kann mit Hilfe einer „partitioning attack" innerhalb weniger Minuten der geheime Schlüssel anhand des Authentifikationsvorgangs rekonstruiert werden [RRTS 02]. Dieses Verfahren erfordert zwar keinen Eingriff in die SIM-Karte, benötigt jedoch physikalischen Zugang zum Endgerät, um

unter anderem Stromaufnahme und elektromagnetische Abstrahlung der Karte zu messen. Auf diese Weise ist es möglich, SIM-Karten zu fälschen und auf Kosten anderer Teilnehmer zu benutzen.

Auch die Funktionen zur Sicherstellung der Vertraulichkeit sind nur unzureichend implementiert. Bereits 1999 gelang es Forschern, die beiden Versionen A5/1 und A5/2 des in GSM zur Verschlüsselung benutzten Stromchiffre A5 zu brechen [BSW 01]. Dass A5 eigentlich geheim ist, hat sich nicht als zusätzlicher Schutz bewährt. Vielmehr wird als Grund für die Vielzahl an Sicherheitslücken im GSM-Protokoll die Informationspolitik der Standardisierungsgremien genannt, die die Spezifikationen der verwendeten Kryptoverfahren nicht der akademischen Welt offenlegten.

Durch einen Designfehler im GSM-Standard ist es weiterhin möglich ganze Gespräche „abzufangen". Möglich wird dies, da nur das Netz das Endgerät authentifiziert - nicht aber umgekehrt. Diese Schwäche macht sich der sogenannte „IMSI-Catcher" zunutze, um Gespräche zu belauschen [Fox 02].

In dem folgenden Abschnitt werden die Expertenaussagen zu potenziellen sowie bereits bestehenden Anwendungen von GSM-Standard beschrieben. Den Schwerpunkt bilden aber die Ergebnisse zu den Sicherheitseigenschaften von .

ABWICKELN VON BEZAHLVORGÄNGEN ÜBER GSM-NETZE: Unterschiedlich werden Bezahldienste über GSM bewertet. Mehrheitlich wird die Verbreitung Mobilfunk-basierter Dienste in 5 Jahren erwartet.

PAYBOX: Dem mittlerweile eingestellten, aber über lange Zeit marktführenden Bezahldienst wird langfristig eine sinkende Bedeutung beigemessen.

## Ergebnisse

Das Abwickeln von Bezahlvorgängen über GSM-Netze sowie die dafür erforderlichen Endgeräte werden nach Ansicht der meisten Experten in fünf Jahren weit verbreitet sein (Abbildung 8.56, ①). Andererseits vertritt ein Viertel der Befragten die Ansicht, dass dies nicht innerhalb der nächsten zehn Jahre eintreten wird. Dabei spielt bei dieser Einschätzung die erwartete Ablösung des GSM-Standards durch UMTS eine wesentliche Rolle. Weiterhin ist die Marktsituation derzeit noch unklar und es werden hinreichende Alternativen gesehen, die sich bewährt haben (beispielsweise kartenbasierte Zahlungsarten wie VISA oder Bankeinzug über EC-Karte). Eine Einigung zwischen Banken und Netz-Providern wird als zusätzliche Schwierigkeit gesehen. Einige der Befragten halten die Anwendungen für eine Zahlungsabwicklung auf Basis von GSM für zu unhandlich und die Hemmschwelle beim Nutzer für zu hoch.

Insgesamt aber gehen die Befragten von einer steigenden Relevanz aus, insbesondere aufgrund der Zunahme kostenpflichtiger Inhalte. Auch die hohe Verbreitung der mobilen Endgeräte werde hierzu beitragen; indes würde damit der Ausschluss von Kunden, die kein Mobiltelefon besitzen, in Kauf genommen. Die Experten warnen insbesondere eindringlich davor, die Sicherheit des Bezahlsystems von dem des GSM-Netzes abhängen zu lassen.

Bei der Beurteilung von Verfahren zur Abwicklung von Bezahlvorgängen über GSM-Netze sehen die Befragten, wie in Abbildung 8.57 ersichtlich ist, derzeit die größte Bedeutung bei dem Produkt Paybox, des mittlerweile insolventen gleichnamigen Unternehmens. Das System hat bereits einen hohen Durchdringungsgrad und wird als durchaus sinnvoll angesehen, solange keine umfassende PKI (Public Key Infrastructure) verfügbar ist (für eine detaillierte Betrachtung der PKI siehe 7.3.1). Deutlich zum Ausdruck kommt auch, dass das System nur als Übergangslösung geeignet ist, daher wird in den nächsten Jahren mit einer rückläufigen Bedeutung gerechnet. Als Anwendungsbereiche werden kleinpreisige Bezahlvorgänge wie bei Kiosken, Taxis, Flohmärkten, Duty Free Shops etc. gesehen.

Das Verfahren Streetcash des Leipziger Unternehmens inatec ist überwiegend unbekannt und hat eine recht geringe Verbreitung und wird nach Ansicht der Befragten auch über die nächsten zehn Jahre unverändert bleiben. Ebenfalls eher unbekannt ist das Verfahren PayitMobile, dem aber in den nächsten zehn Jahren eine steigende Bedeutung beigemessen wird und hinter dem die Gesellschaft für Zahlungssysteme (GZS) steht.

Langfristig werden Verfahren erwartet, die auf transferierbaren, anonymen digitalen Münzen basieren. Dies ist deshalb erstaunlich, da bisherige Pilotversuche in den vergangenen Jahren nicht weitergeführt wurden, nicht zuletzt aufgrund der Komplexität der Verfahren. Im Gegensatz zu den derzeitigen Systemen handelt es sich dabei um ein echtes anonymes Bezahlsystem ohne ein im Hinter-

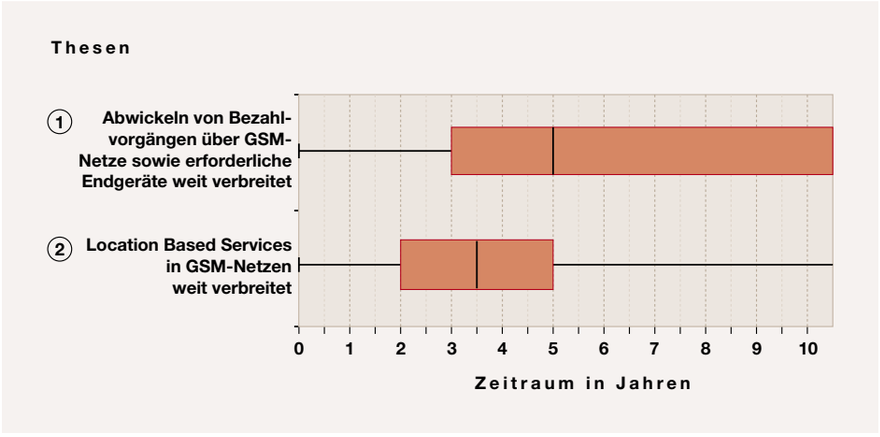



Abbildung 8.56: Ergebnisse der Thesen zu Sicherheit in GSM

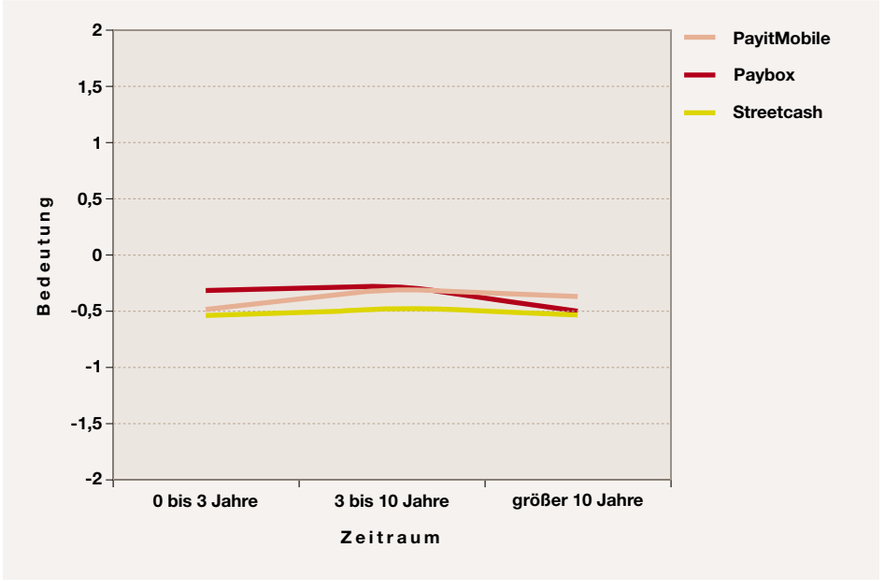



Abbildung 8.57: Bedeutung von Verfahren zur Abwicklung von Bezahlvorgängen in GSM-Netzen

grund geführtes Konto. Dabei werden, ähnlich wie bei echten Münzen, digitale Münzen verschiedener Stückelung durch ein Geldinstitut ausgegeben und können durch den Benutzer frei zusammengestellt und zur Begleichung von Dienstleistungen verwendet werden. Ein Beispiel für ein solches System ist das von der Deutschen Bank mittlerweile eingestellte „DigiCash" [Chau 92, Schl 02]. Einen breiten Überblick über zukünftige elektronische Bezahlverfahren bietet auch Abschnitt 9.6.

LOCATION-BASED SERVICES: Standortbezogene Dienste werden bereits in 3 Jahren weit verbreitet sein. Insbesondere im Verkehrs- und Logistikbereich werden zahlreiche Anwendungspotenziale gesehen.

Standortbezogene Dienste (Location-Based Services) könnten dem Nutzer eines GSM-Mobilfunknetzes die Inanspruchnahme von Dienstleistungen in Abhängigkeit von seinem Aufenthaltsort erlauben.

EOTD-VERFAHREN: Assisted GPS und dieses Verfahren werden sich zur Ortsbestimmung langfristig durchsetzen und das derzeitig vorherrschende Cell-Id-Verfahren verdrängen.

Nach Ansicht der Experten werden LBS (Location Based Service) in GSM-Netzen innerhalb der nächsten drei Jahre weit verbreitet sein (Abbildung 8.56, ②). Dadurch verspricht man sich neue Anwendungspotenziale, beispielsweise für Verkehrsinformationen, Wegbeschreibungen oder Angebote, die sich auf den aktuellen Ort beziehen. Aber auch die Möglichkeit, differentielle Gebühren zu erheben (z.B. für Maut-ähnliche Leistungen) oder der Einsatz im Logistikbereich bzw. im Transportwesen ist denkbar. Die Technologien gelten heute schon als verfügbar, allerdings fehlen noch die entsprechenden Content-Anbieter. Die Experten weisen auch auf die Gefahren für den Datenschutz hin, die durch Lokalisierungsdienste entstehen, beispielsweise wenn die Lokalisierungsinformationen Dritten in die Hände gelangen oder durch die Dienstanbieter missbraucht werden.

Zur Ortsbestimmung von Mobilfunknutzern in GSM-Netzen wird derzeit das Cell-ID-Verfahren von den Befragten hinsichtlich seines praktischen Einsatzes als am bedeutsamsten gesehen (siehe Abbildung 8.58). Bei diesem Verfahren wird die Zellen-Identifikationsnummer der GSM-Basisstation in geographische Koordinaten umgewandelt oder einem geographischen Ort zugewiesen. Das Verfahren erreicht je nach Zellendichte eine Genauigkeit von 100 m bis 15 km. Als Anwendungsbereiche werden Notfall- und Pannenrufsysteme sowie die Strafverfolgung gesehen. Allerdings gehen die Experten in den nächsten Jahren von einer sinkenden Bedeutung aus, insbesondere aufgrund der mangelnden Genauigkeit. Dabei ist das Verfahren in kleinzellularen Netzen wie UMTS oder WLAN präziser und dürfte möglicherweise dort an Bedeutung gewinnen.

Das EOTD-Verfahren, bei dem die Signallaufzeit vom Mobiltelefon zur Basisstation zur Standortbestimmung herangezogen wird, erreicht eine Genauigkeit von 50m bis 100m. Es wird nach Einschätzung der Experten weiter an Bedeutung hinzugewinnen und das Cell-ID Verfahren mittelfristig ablösen. Aufgrund der höheren Genauigkeit sind zusätzliche Anwendungsmöglichkeiten wie Diebstahlaufklärung oder Navigationsdienste denkbar. Von einigen Experten wird das Verfahren als bereits technisch überholt angesehen.

Assisted GPS, das GPS-Daten (Global Positioning System) und, zur Aufhebung einer möglichen GPS-Positionsverschleierung, Daten aus dem GSM-Netz verwendet, erreicht eine Genauigkeit von bis zu 2m. Die Verschleierung des GPS-Signals durch das US-Verteidigungsministerium wurde im Mai 2000 aufgehoben, kann aber jederzeit wieder eingeführt werden. Assisted GPS ermöglicht präzise Maut- und Navigationssysteme. Dieses Verfahren, das derzeit keine Rolle spielt, wird bereits in den nächsten drei Jahren stark an Bedeutung gewinnen. Die Experten erwarten darüber hinaus, dass innerhalb dieses Zeitraums GPS zunehmend durch das europäische Verbundvorhaben Galileo ersetzt wird.

## Zusammenfassung

Man kann bei der Bewertung von GSM-basierten Diensten festhalten, dass die Einschätzungen der Experten stark von der Skepsis gegenüber der mangelnden Sicherheit aktueller Dienste geprägt ist, sowie von der allgemeinen Erwartung, dass viele Dienste im GSM-Netz von UMTS bzw. anderen Technologien abgelöst werden.

- Die Abwicklung von Bezahlvorgängen über das GSM-Netz wird von den Experten unterschiedlich bewertet. Während die Mehrheit die Verbreitung bis 2008 erwartet, rechnet über ein Viertel mit dieser nicht vor 2013. Insbesondere wird eindringlich davor gewarnt, die Sicherheit des Bezahlsystems von dem des GSM-Netzes abhängig zu machen.

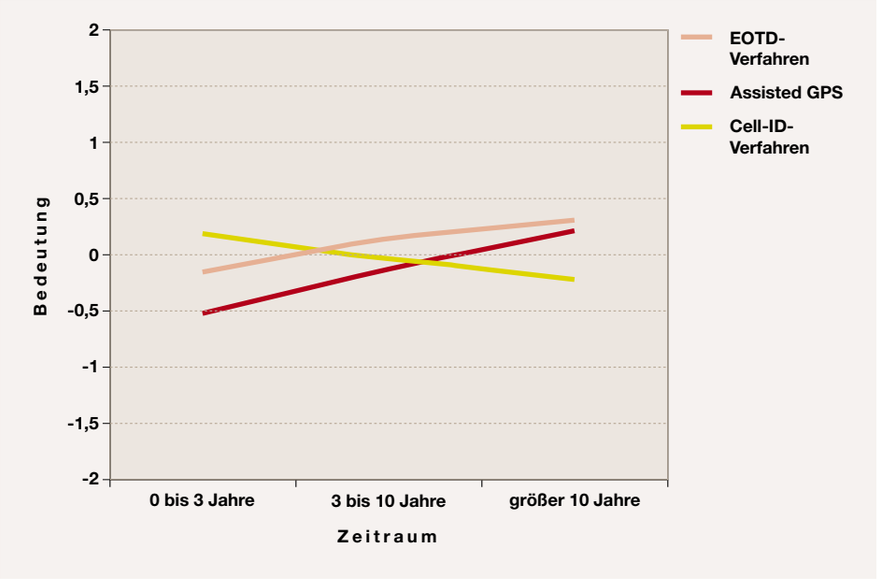



Abbildung 8.58: Bedeutung von Verfahren zur Ortsbestimmung in GSM-Netzen

- Bei der Bewertung aktueller Produkte wird langfristig „PayitMobile" die größte Bedeutung beigemessen. Die geringsten Chancen werden hingegen dem Streetcash-Verfahren eingeräumt. Offensichtlich sind die Träger von „Paybox" zu einer ähnlichen Einschätzung gekommen sind wie die befragten Experten – mit der Konsequenz der Einstellung des Dienstes.

- Die Befragten erwarten, dass standortbezogene Dienste für GSM bis 2006 weit verbreitet sein werden. Dabei werden mittelfristig dem EOTD- (Enhanced Observed Time Difference) und dem derzeit unbedeutenden Assited GPS-Verfahren die besten Chancen eingeräumt. Das derzeit vorherrschende Cell-ID-Verfahren wird aufgrund der ungenauen Technik zukünftig erheblich an Bedeutung verlieren.

#### 8.2.8.2 UMTS

Bei UMTS handelt es sich um ein universell nutzbares Mobilfunknetz der so genannten dritten Generation („3G") im Frequenzband von 2 GHz. UMTS soll die bestehenden zellularen Mobilfunknetze (z.B. GSM 900, GSM 1800/DCS 1800), schnurlose Systeme (z.B. CT, DECT), private Bündelfunksysteme (TETRA) sowie drahtlose lokale Netze LAN zusammenführen und neue Dienste bereitstellen.

Im Gegensatz zu Mobilfunknetzen der zweiten Generation wird UMTS kein abgeschlossenes System darstellen. Durch die Verschmelzung von UMTS mit dem Festnetz und dem Internet werden sowohl Mobilfunk- als auch Festnetzteilnehmer neuen Gefahren ausgesetzt.

Die Sicherheit der dritten Generation baut auf der der zweiten Generation auf [Walk 00]. Dabei werden teilweise bestehende Sicherheitsdienste übernommen, wie beispielsweise die Authentifizierung des Teilnehmers gegenüber dem Netzwerk (verbesserte Algorithmen), die Verschlüsselung an der Funkschnittstelle (Schlüssel von 64 auf 128 Bits erweitert) und der Einsatz eines UMTS Subscriber Identity Module (USIM). Darüber hinaus werden bestehende Schwächen beseitigt und zum Teil neue Sicherheitsdienste implementiert. Als Verbesserungen können vor allem die verschlüsselte Übertragung der Authentifizierungsdaten und Übertragungsschlüssel innerhalb des Netzwerks, der Nachweis „frischer" und die Begrenzung der Lebensdauer alter Schlüssel, die Gewährleistung der Datenintegrität und die Möglichkeit, Sicherheitseigenschaften

nachträglich zu ergänzen oder zu ändern, genannt werden. Im Bereich der verwendeten Verfahren wurden nicht nur neue Algorithmen eingeführt (z.B. KASUMI [Walk 00], die auf der Blockchiffre Misty [Mits 97] basiert, für Verschlüsselung und Integrität), sondern durch die Veröffentlichung und wissenschaftliche Evaluation hat sich auch ein Paradigmenwechsel vollzogen.

GEGENSEITIGE AUTHENTIFIZIERUNG: Die Einführung dieser Sicherheitsfunktion ermöglicht erstmals viele Kommunikationsanwendungen im E-Commerce- und E-Government-Bereich.

ANWENDUNGSSPEZIFISCHE SICHERHEITSDIENSTE: TCP/IP-basierte Sicherheitsdienste wie die IPSec-Protokollfamilie werden die anderen Sicherheitsdienste in 10 Jahren ablösen.

BEDROHUNGEN AUF UMTS-ENDGERÄTE: Die Gefährdung durch Bedrohungen auf UMTS-Endgeräte wird in den nächsten 10 Jahren erheblich an Bedeutung hinzugewinnen.

## Ergebnisse

Bei der Bewertung der Sicherheitseigenschaften von UMTS-Netzen für die vertrauliche und integere Kommunikation über UMTS-Netze, die über die Sicherheitseigenschaften bisheriger GSM-Netze hinausgehen, wird die gegenseitige Authentifizierung von USIM (Universal Subscriber Identity Module) und dem Netz sowie der Überprüfung der übertragenen Daten auf Unverfälschtheit zukünftig die größte Bedeutung erlangen (siehe Abbildung 8.59). Die gegenseitige Authentifizierung ermöglicht nach Ansicht der Befragten erst „ernsthafte" Kommunikationsanwendungen, beispielsweise für E-Commerce, E-Government- und DRM-Anwendungen (Digital Rights Management), und ermöglicht den Schutz gegen Netznachbildungen, beispielsweise um Angriffe durch IMSI-Catcher abzuwehren. Durch die Integritätsprüfung werden darüber hinaus Anwendungen wie Steuerungs- und Regelungsaufgaben über Mobilfunknetze realisierbar (Fernwirksysteme, Fernüberwachung). Allerdings werden noch Defizite bei kryptographischen Verfahren gesehen, die auf Kanälen mit höherer Fehlerhäufigkeit, wie drahtlose Systeme, effizient arbeiten.

Kurzfristig dürfte nach Ansicht der Experten die Erhöhung der Längen des geheimen Authentisierungsschlüssel und des auszuhandelnden Sitzungsschlüssels von 64 auf 128 Bit eine wichtige Rolle bei der Einschätzung der neuen Sicherheitseigenschaften spielen. Langfristig werden allerdings auch 128-Bit-Schlüssel als unzureichend angesehen. Genauso wichtig bewerten die Experten die Bedeutung der verwendeten Algorithmen, insbesondere im Hinblick auf die im GSM verwendeten und mehrfach als unsicher eingestuften Algorithmen. Im Gegensatz zu GSM sind diese im UMTS-Standard offengelegt und werden in der Wissenschaft analysiert. Die automatische Begrenzung der Lebensdauer der temporären Schlüssel wird in diesem Kontext als weniger bedeutsam angesehen.

Im Bereich der Datenkommunikation über UMTS sind sich die Experten über die Entwicklung uneinig. Während ein Teil der Experten davon ausgeht, dass TCP/IP-basierteDienste alle anderen Dienste frühestens in acht Jahren abgelöst haben werden, betrachten andere TCP/IP dafür als ungeeignet (Abbildung 8.60, ①). Obwohl „all-over-IP" die Interoperabilität mit anderen Netzen und damit eine einheitliche Kommunikationsinfrastruktur, kostengünstigere Gateways, Router und Ende-zu-Ende Applikationen ermöglicht und zentraler Forschungsgegenstand vieler Provider ist, herrscht Skepsis vor, ob das paketorientierte TCP/IP für die spezifischen Gegebenheiten im Mobilfunk geeignet ist, insbesondere für QoS-sensible Dienste wie die Echtzeitübertragung von Sprache oder Video.

Im Bereich TCP/IP-basierter Sicherheitsdienste, wie sie beispielsweise durch die IPSec-Protokollfamilie repräsentiert werden, gehen die Experten davon aus, dass diese alle anderen möglichen Sicherheitsdienste erst in zehn Jahren ablösen werden (Abbildung 8.60, ②). Neben den bereits genannten grundsätzlichen Bedenken gegenüber TCP/IP im Zusammenhang mit UMTS weisen die Experten darauf hin, dass zusätzlich zu den allgemeinen IPSec-Diensten anwendungsspezifische Sicherheitsdienste wie lokale Authentifizierung benötigt werden. Daneben müssen auch Anforderungen des Funknetzes und der verfügbaren Ressourcen an Bandbreite und Rechenleistung der Endgeräte berücksichtigt werden. Vorteile werden in der erreichbaren Interoperabilität gesehen.

Die Befragten gehen davon aus, dass einwirkende Bedrohungen auf UMTS-Endgeräte innerhalb der nächsten Jahre erheblich an Bedeutung gewinnen werden (siehe Abbildung 8.61). Dem Einbringen von ausführbaren Inhalten mit Schadfunktion in diese neuen, für UMTS-Netze geeignete mobile Endgeräte wird dabei eine etwas größere Bedeutung beigemessen. Die Experten verweisen allerdings darauf, dass dies kein UMTS-spezifisches Problem ist, sondern vielmehr vom Betriebssystem der verwendeten Endgeräte

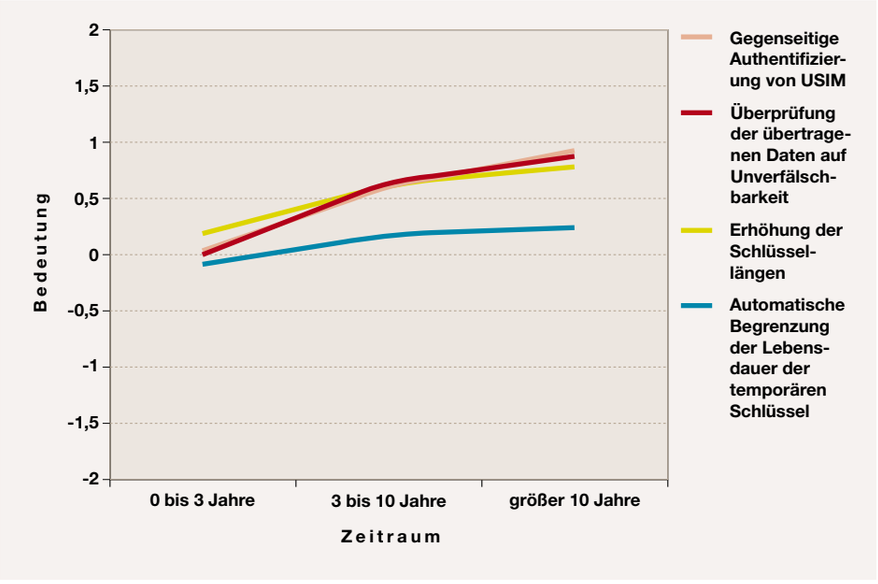



Abbildung 8.59: Bedeutung verschiedener Sicherheitseigenschaften von UMTS

KOPPLUNG DER UMTS-NETZE MIT DEM INTERNET: Innerhalb der nächsten 3 Jahre werden hierbei neue Gefahrenpotenziale erwartet, insbesondere gerichtet auf die UMTS-Netzinfrastruktur über Internet-Gateways.

abhängt. So dürfte dieses Problem bereits bei den heute verfügbaren GSM-Geräten auftreten, auf denen ausführbarer Code läuft. Besonders gefährlich wird diese Entwicklung aufgrund der sensiblen Funktionen , die mobile Endgeräten als persönliche Systeme erhalten. Bei der Verwendung der Endgeräte zum Signieren von Transaktionen könnten Angreifer diese vor dem Signaturvorgang ohne dessen Kenntnis manipulieren. Weiterhin unschlüssig sind die Experten, ob der Einsatz von Java in den Endgeräten die Bedrohung reduzieren kann oder nicht.

Das Ausspähen von durch den Benutzer im mobilen Endgerät gespeicherten sensiblen Daten durch das Einbringen von Trojanern wird über die nächsten Jahre ebenfalls an Bedeutung zunehmen. Dabei werden Gefahrenpotenziale für Industriespionage, aber auch das Ausforschen persönlicher Verhaltensweisen gesehen. Im wesentlichen sehen die Befragten ähnliche Entwicklungen wie bei der vorangegangenen Fragestellung. Insgesamt nimmt diese Bedrohung an Bedeutung zu, da das mobile Endgerät zum universellen persönlichen IT-Device wird.

Durch die Kopplung der UMTS-Netze mit dem Internet können neue Bedrohungen auf UMTS-Endgeräte einwirken (siehe Abbildung 8.62). Die Experten erwarten, ausgehend von einem niedrigen Niveau, einen sprunghaften Anstieg der Bedrohungen innerhalb der nächsten drei Jahre und ein weiteres leichtes Ansteigen für die darauf folgenden Jahre. Die größte Bedeutung wird dabei Angriffen auf die UMTS-Netzinfrastruktur über das Internet-Gateway beigemessen, da von jedem IP-fähigen Endgerät im Internet ein solcher Angriff möglich sein wird. Daher werden IDS in Internet-Gateways als notwendig erachtet.

Angriffe auf die UMTS-Netzinfrastruktur über TCP/IP-fähige Endgeräte der UMTS-Nutzer hingegen könnten mit ähnlichen Schutzmechanismen wie im Internet abgewehrt werden. Darüber hinaus könnten böswillige Endanwender leichter abgewehrt werden. In der Bedeutung vergleichbar sehen die Befragten DDoS-Angriffe auf die Internet-Gateways des UMTS-Netzes. Als gefährdet werden terminkritische Anwendungen angesehen, z.B. elektronische Wahlen (zu Online-Wahlen siehe Abschnitt 9.8).

Die geringste Bedeutung weisen die Befragten dem Missbrauch der Endgeräte von UMTS-Nutzern für das Durchführen von DDoS-Angriffen gegen Dritte zu. Viele sind der Meinung, dass die Leistungsfähigkeit der Anbindung nicht ausreichend ist, um die nötige Schlagkraft zu entwickeln.

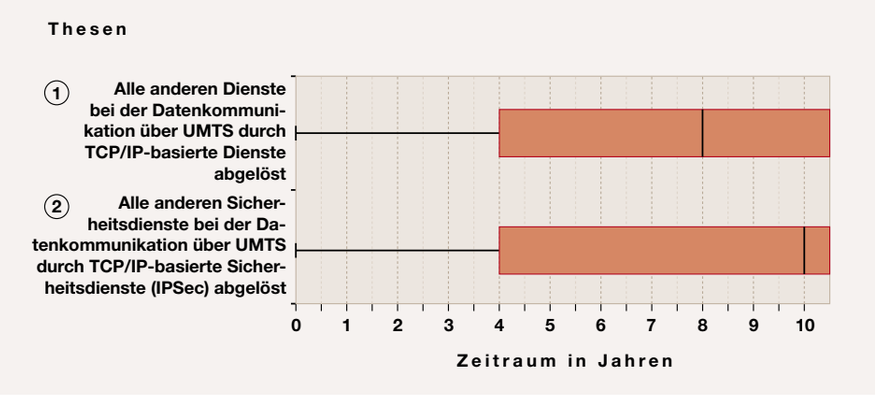



Abbildung 8.60: Ergebnisse der Thesen zu Datenkommunikation über UMTS

Darüber hinaus wird es einfacher möglich sein, die betroffenen Endgeräte zu identifizieren und auszuschalten.

### Zusammenfassung

Die Experten erwarten, insbesondere im Hinblick auf die prognostizierte Verbreitung von UMTS, eine Zunahme der Bedeutung UMTS-spezifischer Bedrohungen bzw. der neuen UMTS-Sicherheitseigenschaften innerhalb der nächsten drei Jahre.

- Die wichtigste neue Sicherheitseigenschaft ist nach Ansicht der Experten die gegenseitige Authentifizierung der USIM sowie die Integritätsprüfung der übertragenen Daten. Diese ermöglichen vielfach erst die Verwendung der Mobilfunktechnolgie für zahlreiche neue Dienste. Kurzfristig wird auch die Erhöhung der Länge des Sitzungsschlüssels eine Rolle spielen. Die automatische Begrenzung der Lebensdauer des Schlüssels wird hingegen als weniger bedeutsam eingestuft.
- In der Bewertung von UMTS zur Datenkommunikation spiegeln die unterschiedlichen Ansichten der Experten den allgemeinen Diskussionsstand bei der Frage nach einheitlichen Transportprotokollen wider. So steht ein Großteil der Experten der völligen Ablösung aller UMTS-Dienste durch TCP/IP-basierte Dienste sehr skeptisch gegenüber und damit auch der Ablösung von möglichen anderen Sicherheitsdiensten durch TCP/IP-basierte Dienste.
- Die Befragten erwarten, dass in den nächsten Jahren die Bedrohungen durch das Einbringen von ausführbaren Inhalten mit Schadfunktion bzw. zum Ausspähen der übertragenen Daten zunehmen werden. Dabei wird die Gefahr durch Programme mit Schadfunktion etwas höher eingestuft.
- Die Kopplung der UMTS-Netze mit dem Internet über Gateways wird nach Ansicht der Experten vor allem in der Zeit bis 2006 neue Bedrohungspotenziale schaffen. Dabei wird Angriffen auf die UMTS-Netzwerkinfrastruktur über das Internet-Gateway die größte Bedeutung beigemessen. Etwas geringer wird die Gefährdung durch Angriffe auf die UMTS-Infrastruktur über TCP/IP-fähige Endgeräte sowie externe DDoS-Angriffe eingestuft. Die geringste Gefahr sehen die Experten durch interne DDoS-Angriffe.

## 8.2.8.3 Drahtlose Technologien

Auch im Datenverkehr nimmt seit Jahren die Bedeutung drahtloser Netze stetig zu. So schaffte der 1997 offiziell verabschiedete WLAN-Standard IEEE (Institute of Electrical and Electronics Engineers) 802.11 die Grundlage für ein nichtproprietäres Funknetzwerk. Der Standard lässt den Herstellern einige Freiheiten,

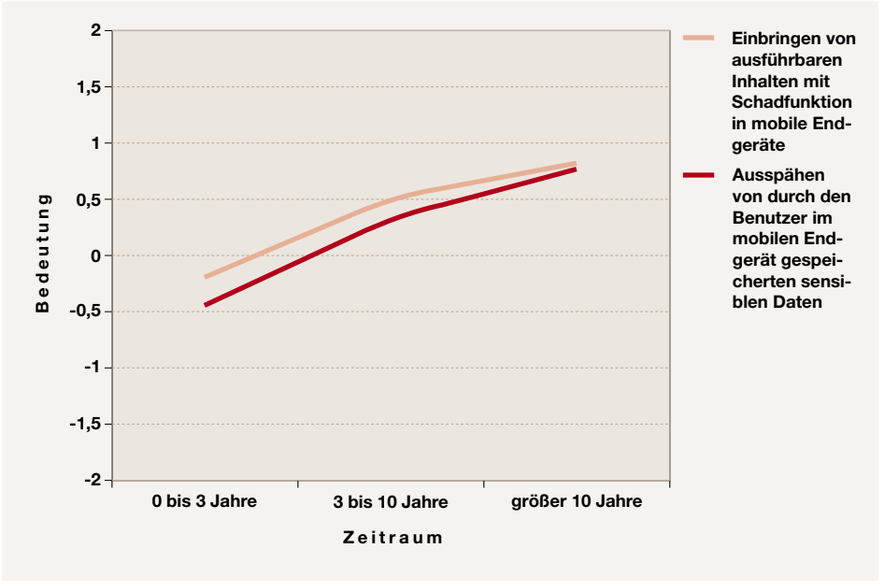



Abbildung 8.61: Bedeutung von Bedrohungen bei UMTS-Endgeräten

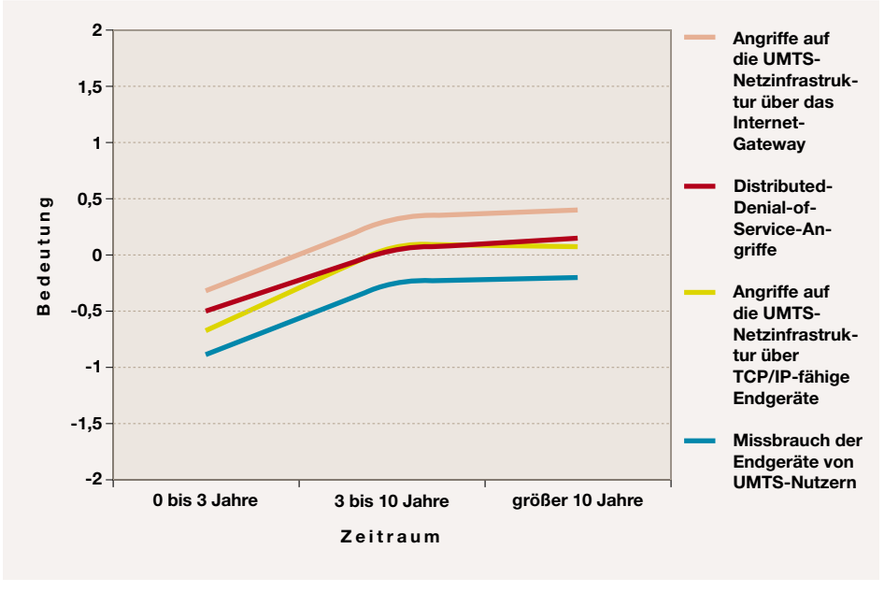



Abbildung 8.62: Bedeutung von Bedrohungen durch die Kopplung von UMTS und IP

aber gewährleistet weitgehend die Interoperabilität der Produkte unterschiedlicher Anbieter. Die heute verfügaren Systeme nach IEEE 802.11b bzw. 802.11a arbeiten im 2,4 bzw. 5 GHz-Band und erlauben Übertragungsraten von maximal 11 bzw. 55 MBit/s.

SICHERHEITSGEFÜHL: Die eingebauten Sicherheitsmechanismen bei Wireless-Produkten bieten derzeit keinerlei wirksamen Schutz.

Im Vergleich zu konventioneller leitungsgebundener Technik weisen funkbasierte Netze und Schnittstellen weitaus höhere Anforderungen an die Sicherheit auf. So befinden sich in den meisten drahtgebundenen Netzwerken die Verbindungskabel innerhalb des Gebäudes und damit im Allgemeinen innerhalb des Vertrauensbereichs des Anwenders. Ein potenzieller Angreifer müsste in jedem Fall bestimmte physische Sperren (Zugang zu den Räumen, Sicherheitspersonal, Türschlösser etc.) überwinden, bevor er einen Angriff starten kann. Angriffe auf Funksysteme können im Gegensatz hierzu ausserhalb des Gebäudes durchgeführt werden, mit einem erheblich geringeren Risiko für den Angreifer beispielsweise von einem parkenden Auto in unmittelbarer Nähe des Objektes. Analog zur Sicherheit drahtgebundener Systeme müssen in erster Linie drei Aspekte betrachtet werden:

Zur Sicherstellung der Vertraulichkeit muss der Funkverkehr derart geschützt werden, dass keine Informationen über dessen Inhalt abgehört werden können.

Im Rahmen der Zugangskontrolle muss das Funknetzwerk so geschützt werden, dass sich nur autorisierte Benutzer Zugang zum internen Netz verschaffen können. Ist dies nicht gewährleistet, können potenzielle Angreifer über die Funkschnittstelle möglicherweise Zugang zum internen Netzwerk erlangen. Des Weiteren ist die Zugangskontrolle bedeutsam, um ein Abfließen von Ressourcen über die Netzschnittstellen, beispielsweise durch Inanspruchnahme von Netz-Kapazitäten bzw. Nutzung von Accounts, zu verhindern.

Die Datenintegrität spielt eine wichtige Rolle, denn ist die Integrität von Datenpaketen in einem Netzwerk nicht gewährleistet, kann dies auch die Vertraulichkeit beeinflussen. Durch eine veränderte IP-Adresse im Header kann der Angreifer ganze Datenpakete an (s)eine Internetadresse senden und somit über deren Inhalt Kenntnis erlangen.

Vielfach dokumentierte Angriffe auf die bestehenden Sicherungsprotokolle, wie auf das im IEEE 802.11 Standard verwendete Wired-Equivalent-Privacy-Protocol (WEP), belegen die unzureichende Umsetzung der Sicherheitsfunktionen [DSK 02, BGW 01, FMS 01, SIR 02]. Hochproblematisch ist auch der leichtfertige Umgang der Nutzer, beispielsweise mit Funk-LANs ohne jeglichen Zugriffsschutz [Schm 01].

Auch bei anderen Wireless-Technologien, hier als Sammelbegriff für drahtlose Übertragungsverfahren wie IEEE 802.11, HiperLan/2, Bluetooth, IrDA, DECT/DMAP verwendet, sind gravierende Sicherheitslücken entdeckt worden, beispielsweise bei Bluetooth [JaWe 01].

Die im folgenden aufgeführten Einschätzungen und die beurteilten Thesen unterscheiden diese Technologien nicht explizit. Vielmehr werden grundsätzliche Fragestellungen zur Anwendung und zum Einsatz der drahtlosen Vernetzung aufgeworfen.

## Ergebnisse

Die Einschätzung der Befragten zur Benutzersensibilisierung gegenüber den Gefahren bei der Verwendung von Wireless-Technologien ist in Abbildung 8.63 aufgezeichnet. In spätestens drei Jahren wird nach Ansicht der Experten die Nutzung von Sicherheitsfunktionalitäten, die in standardisierten Wireless-Technologien vorhanden sind, weit verbreitet sein (Abbildung 8.63, ①). Obwohl derzeit das Gefahrenpotenzial noch unterschätzt wird, beispielsweise durch die Ausweitung von Unternehmensnetzen durch die Luftschnittstelle über Gebäudegrenzen hinweg, erwarten die Befragten eine zunehmende Sensibilisierung.

Die Experten weisen allerdings mit Nachdruck darauf hin, dass die derzeit eingebauten „Sicherheitsmechanismen" keinerlei adäquaten Schutz bieten und warnen vor einem falschen Sicherheitsgefühl. Die Fehler in den Standards müssten behoben und bis dahin andere Mechanismen, beispielsweise IPSec, eingesetzt werden.

Keine einheitliche Meinung haben die Experten darüber, ob ein auf Wireless-Technologien beruhendes Netzwerk als

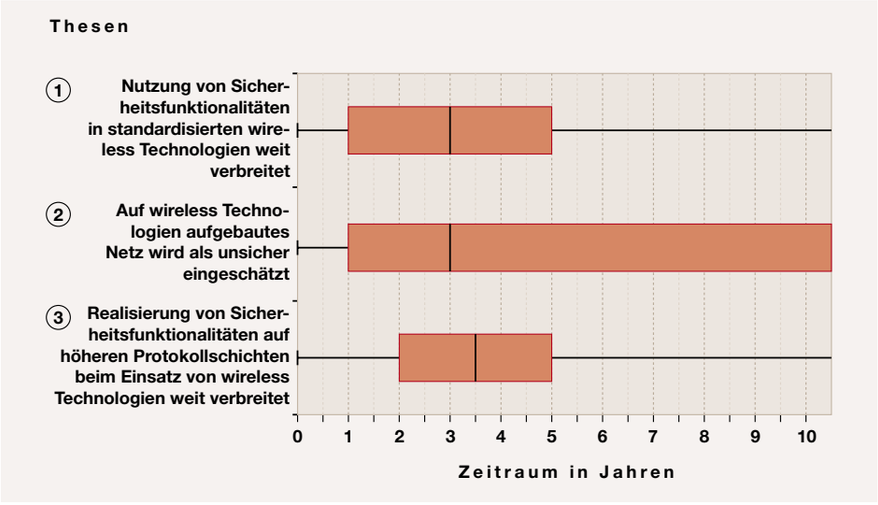



Abbildung 8.63: Ergebnisse der Thesen zu Sicherheitsfunktionen in Wireless-Technologie-Netzen

„unsicheres Netz" angesehen werden muss (siehe Abbildung 8.63, ②). Während die Mehrheit davon ausgeht, dass sich in spätestens drei Jahren diese Einsicht durchgesetzt haben wird, sind über ein Viertel der Meinung, dass drahtlose Netze wohl nie als völlig unsicher angenommen werden und halten dies für nicht sinnvoll, da davon ausgegangen wird, dass sich das Netz sichern lässt bzw. nicht unsicherer ist als das „normale" Internet. Außerdem ließe sich mit einem „vollständig unsicheren" Netz kein Geld verdienen, was zur Disqualifikation der Technologie führen würde.

Das Realisieren von Sicherheitsfunktionalitäten auf höheren Protokollschichten beim Einsatz eines auf Wireless-Technologien beruhenden Netzwerkes wird nach Einschätzung der Experten in etwa drei Jahren weit verbreitet sein (Abbildung 8.63, ③). So sind die Sicherheitsprotokolle für die höheren Protokollschichten drahtloser Netztechnologie unabhängig und spielen bereits heute eine wichtige Rolle. Die Befragten erwarten daher eine Ablösung der WLAN-Sicherung durch Ende-zu-Ende Protokolle wie IPSec oder TLS, obwohl Sicherheitsmechanismen auf den unteren Schichten als wirkungsvoller erachtet werden. Überraschend ist die allgemeine Einschätzung, dass sich Wireless-Techniken ohne angemessene Sicherheitsfunktionalität insbesondere im kommerziellen Bereich nicht durchsetzen werden. Angesicht des möglichen Schadens und der Einfachheit möglicher Angriffe besteht bei den Verantwortlichen in den Unternehmen kaum noch die Bereitschaft, die damit verbundenen Risiken leichtfertig zu tragen.

Bei der Beurteilung der spezifischen Bedrohungen in Wireless-Technologie-Netzen wird dem Ausspähen von im Netzwerk kommunizierten Daten durch nicht berechtigte Teilnehmer die größte Bedeutung auf einem über die nächsten Jahre nahezu stabilen Niveau zugewiesen (Abbildung 8.64). Das Ausspähen fremder Netze ist vielfach schon eine Art „Hobby" und wird nach Ansicht der Experten vermutlich erst durch verbesserte integrierte Sicherheitsmaßnahmen eingedämmt. Motivation für die Angriffe sind Neugierde, unlauterer Wettbewerb, organisierte Kriminalität und Industriespionage. Durch eine adäquate Verschlüsselung und Integritätsprüfung ließe sich diese Bedrohung einfach beseitigen.

DoS-Angriffe durch das in Betrieb nehmen von Störsendern im genutzten Frequenzband werden nach Ansicht der Experten in den nächsten drei Jahren an Bedeutung hinzugewinnen. Allerdings gehen die Befragten durch zielgerichtete Attacken im Nahfeld von einer leichten Ortsbestimmung und Beseitigung der Störquelle aus. Angriffe könnten aber auch wie bei den militärischen ECM-Maßnahmen (Elec-

SICHERHEITSFUNKTIONALITÄTEN AUF HÖHEREN PROTOKOLLSCHICHTEN: Derartige Funktionalitäten werden in 3 Jahren weit verbreitet sein. Link-Sicherungskonzepte werden zunehmend durch Ende-zu-Ende Protokolle ersetzt werden.

AUSSPÄHEN VON IM NETZWERK KOMMUNIZIERTEN DATEN: Dies wird auch in Zukunft die größte Bedrohung für drahtlose Netze darstellen.


Abbildung 8.64: Bedeutung verschiedener Bedrohungen für Wireless-Technologie-Netze

tronic Counter-Measures) durch Störsender von Flugzeugen aus durchgeführt werden. Auch politisch oder terroristisch motivierte Aktionen sind denkbar.

Das unbeabsichtigte spontane Vernetzen mit fremden, auf Wireless-Technologie beruhenden Geräten und die damit verbundene Bedrohung, ausgespäht zu werden, wird kurzfristig an Bedeutung hinzugewinnen, langfristig aber wieder zurückgehen. Gefährdet sehen die Befragten vor allem Kleingeräte, beispielsweise PDAs (Personal Digital Assistant) und Mobiltelefone mit Bluetooth. Allerdings erhoffen sich die Befragten auch in diesem Kontext verbesserte Sicherheit durch überarbeitete Standards.

## Zusammenfassung

Insgesamt gehen die Experten davon aus, dass die Sicherheitsschwächen von Funknetzen durch die Benutzer erfasst und in den Sicherheitsrichtlinien berücksichtigt werden. Zusammenfassend erhält man die folgende Einschätzung:

- Die Befragten erwarten zwar, dass die in den standardisierten Wirelesstechnologien eingebauten Sicherheitsfunktionen ab 2006 von den Benutzern verwendet werden, weisen jedoch nachdrücklich darauf hin, dass diese keinerlei wirksamen Schutz gegen böswillige Angreifer bieten.
- Ebenfalls bis 2006 werden nach Einschätzung der Befragten Sicherheitsfunktionalitäten in den höheren Protokollschichten realisiert sein. Darüber hinaus werden bisherige Link-Sicherungskonzepte, die vornehmlich die Luftschnittstelle sichern, durch Ende-zu-Ende Protokolle ersetzt werden.
- Bei der Bewertung der spezifischen Bedrohungen für drahtlose Netze wird die größte Bedeutung im Bereich des Ausspähens der im Netzwerk kommunizierten Daten erwartet. Das unbeabsichtige spontane Vernetzen wird nur mittelfristig an Bedeutung hinzu gewinnen. Die derzeit geringste Bedeutung haben DoS-Angriffe, beispielsweise durch Störsender. Es wird jedoch ausgegangen, dass diese in den nächsten Jahren weiter zunehmen werden.

## 8.3 Datenbanken und Wissensmanagement

Wissen wird als Produktionsfaktor weiter an Bedeutung gewinnen [Schü 01]. Spätestens durch die starke Verbreitung des Internet ist es möglich geworden, auf eine nahezu unbegrenzte Menge von Informationen zuzugreifen. Oft wird auch vom „Information Overload" gesprochen, denn wir werden von einer immer größer werdenden Informationsflut „überrollt". Eine Zielrichtung bei der Entwicklung betriebswirtschaftlicher Anwendungen im Datenbankbereich ist daher die Generierung von Wissen, d.h. von neuen und dauerhaften Kenntnissen, aus Informationen. Die effiziente Speicherung und Repräsentation von Wissen und die Verarbeitung von Informationen stellen wichtige Erfolgsfaktoren im Wettbewerb dar. Die maschinelle Verarbeitung von Informationen geschieht durch Daten, die in Datenbanken gehalten werden. Daten sind also die Bausteine von Informationen [Hein 93].

Datenbanksysteme werden eine immer wichtigere Rolle in Unternehmen und Behörden spielen, um eine effizientere Nutzung von Informationen zu erreichen. Ihre Bedeutung wird durch die weltweit zunehmende Vernetzung noch vergrößert [KeEi 01]. Gleichzeitig wird der effiziente Einsatz von Datenbanksystemen auf Grund der zunehmenden Informationsmenge und der steigenden Komplexität der Anwendungen immer schwieriger. In gewachsenen IT-Infrastrukturen liegt darber hinaus eine Verteilung der Daten auf unterschiedliche Datenbankserver oder Datenträger vor. Hieraus entsteht dringender Bedarf, auch die Datenbanksysteme kontinuierlich weiterzuentwickeln.

Gewinnung, Verwaltung, Verarbeitung und Repräsentation von Wissen sind Gegenstand des Technologiefeldes Datenbanken und Wissensmanagement, das in diesem Abschnitt ausführlich betrachtet wird. Dabei werden Fragen nach der Sicherheit von Datenbankanwendungen eine immer wichtiger werdende Rolle bei ihrem Design und Entscheidungen über ihren Einsatz spielen. Unternehmen halten immer mehr Daten in Datenbanken und die Auswertung dieser Daten hat eine immer größere Bedeutung für die Unternehmensführung. Aus diesem Grund steigen die Schäden, die ein Angriff auf ein Datenbanksystem (DBS) hätte: zum einen, weil der Zugriff auf eine enorme Datenmenge erfolgt, zum anderen weil zentrale Abläufe im Unternehmen unterbrochen werden können. Bei einer Vernetzung verschiedener Datenbanksysteme verstärkt sich diese Problematik noch, weil der Zugang zu einer Datenbank auch den Zugriff auf andere ermöglichen kann (siehe hierzu auch Abschnitt 8.2.1). Aus diesem Grund wird versucht, die Sicherheit, die in vielen Schichten auf unterschiedliche Arten garantiert werden muss, durch neue Technologien und Konzepte zu erhöhen. Dabei spielen auch die in Abschnitt 7.2 näher beschriebenen Entwicklungen auf dem Gebiet der Authentisierung und Identifikation eine große Rolle, die allerdings neue, leistungsstarke Hardware verlangen.

Zunächst werden anhand der übergreifenden Trends aus Abschnitt 6 die für dieses Technologiefeld bedeutsamsten Entwicklungen identifiziert und im Folgenden näher erläutert:

**Automatisierung und Vereinfachung** (Abschnitt 6.1): Für die Anwender wird es zukünftig immer wichtiger, Systeme einfach bedienen zu können und einen hohen Automatisierungsgrad zu erreichen. Benutzerfreundlichkeit nimmt deshalb auch bei Datenbanksystemen einen hohen Stellenwert ein. Dabei erleichtern Standarddateiformate die Datenverwaltung und ermöglichen die Integration heterogener Informationsquellen ohne großen Aufwand (siehe Abschnitt 8.3.2). Zusätzlich vereinfachen neue Technologien im Bereich der Datenanalyse wie Data Warehouses oder Data Mining die Verarbeitung und Auswertung großer Datenmengen. Darüber hinaus werden einfachere Abfragen eine Nutzung von Datenbanken ohne besondere Fachkenntnisse erlauben (siehe 8.3.5).

**Dienst- und Komponentenorientierung** (Abschnitt 6.2): Durch neue Technologien wie XML können Daten abstrahiert werden und anhand von Struktur- und Metainformationen systemübergreifend genutzt werden, wie in Abschnitt 8.3.3 beschrieben. Auch bei der Datenanalyse ist der Trend der Abstraktion erkennbar, z.B. bei der Auswertung konkreter Informationen durch Data Mining und die Ableitung abstrakter Zusatzinformationen daraus.

**Globalisierung und Wettbewerb** (Abschnitt 6.3): Für Unternehmen spielt die effiziente Speicherung und Auswertung umfangreicher Daten heute eine immense Rolle [Schü 01]. Die rasanten Entwicklungen im CRM, die umfangreichen Möglichkeiten, verschiedenste Daten miteinander in Verbindung zu bringen, aber auch die Sammlung und zentrale Nutzung dezentral gewonnener Daten, beispielsweise in internationalen Unternehmen, zeigen den Einfluss des Wettbewerbs und der Globalisierung auf Business Systeme (siehe zu dieser Systemklasse auch Abschnitt 8.4.6). Der Wettbewerbsdruck zwingt Unternehmen zu immer komplexeren Anwendungen. Er zeigt sich aber auch auf dem Markt für Datenbanksysteme: hier werden sich in Zukunft wenige Unternehmen durchsetzen, wobei Open Source Datenbanken auch eine Konkurrenz für die Anbieter propriäterer Systeme darstellen könnten (siehe Abschnitt 8.3.5).

**Integration und Standardisierung** (Abschnitt 6.4): Im Bereich Datenbanken und Wissensmanagement spielen Integration und Standardisierung inzwischen eine entscheidende Rolle [Ditt 02]. Programmierschnittstellen werden standardisiert und ermöglichen damit die Integration neuer Funktionalitäten in Datenbanksysteme (siehe hierzu Abschnitt 8.3.2). Dies gilt vor allem für ingenieurtechnische Anwendungen wie CAD sowie für die Einbindung komplexer Multimediadaten oder geographischer Informationen. Auch die Integration proprietärer IT-Systeme und bestehender Geschäftsprozesse sowie die zunehmende Nutzung des Internet im Datenbankbereich werden durch Standardisierungsbemühungen entscheidend unterstützt und vorangetrieben. Hierbei spielt XML eine wichtige Rolle, da es branchen-, applikations- und herstellerübergreifend den Informationsaustausch und die Schnittstellenproblematik zwischen Anwendungssystemen wesentlich vereinfachen kann [PASS 00].

**Kapazitäts- und Leistungssteigerung** (Abschnitt 6.5): Die steigende Vernetzung von Datenbanksystemen sowie neue Technologien, z.B. verbesserte Speichermedien und leistungsstarke Netzwerkinfrastrukturen, ermöglichen eine effizientere Verwaltung stetig wachsender Datenbestände (siehe hierzu auch 8.1 und 8.2.2). Damit ist eine Leistungssteigerung sowohl bei Interaktionen zwischen vernetzten Systemen als auch bei Transaktionen innerhalb von Datenbanken verbunden, was im Kontext von E-Commerce, aber auch zur Datenanalyse unerlässlich ist (siehe Abschnitt 8.3.4).

**Konvergenz** (Abschnitt 6.6): Dieser Trend ist im Datenbankbereich in verschiedenen Zusammenhängen zu beobachten. Es entstehen Datenmodelle, die verschiedene Ansätze miteinander verschmelzen, z.B. objektrelationale Datenbanken. Datenbankerweiterungen und proprietäre Schnittstellen konvergieren zunehmend zu definierten Standardschnittstellen. Dadurch können heterogene Daten in Datenbanksysteme integriert werden, was zu einer Homogenisierung aller Informationsquellen in Metadatenmodellen führt (siehe Abschnitt 8.3.2).

**Miniaturisierung** (Abschnitt 6.7): Dieser übergreifende Trend ist im Bereich der Datenbanken nur im übertragenen Sinne erkennbar, nämlich dann, wenn Datenbanksysteme auf PDAs oder Notebooks integriert werden. Das setzt allerdings eine Miniaturisierung auf Ebene der Hardware und eine Integration in neue, mobile Endgeräte voraus. Deshalb wird dieser Trend v.a. in den Abschnitten 8.1 und 9.2 betrachtet.

**Mobilität** (Abschnitt 6.8): Datenbanksysteme werden immer mehr in mobile Endgeräte integriert und die Vielfalt ihrer Anwendungen steigt in diesem Bereich enorm an. Allerdings setzt dies keine so umfangreichen Veränderungen bei den Datenbankkonzepten voraus, als dass die Mobilität als spezifischer Trend im Datenbankbereich angesehen werden könnte. Ausführliche Beschreibungen und Ausprägungen dieses Trends finden sich in den Abschnitten 8.1.4, 8.2.7 und 9.3 wieder.

**Vernetzung und Flexibilisierung** (Abschnitt 6.9): Die Interoperabilität von Datenbanksystemen wird durch die zunehmende Vernetzung, vor allem über das Internet, in Zusammenhang mit dem Trend zur Standardisierung gefördert. Auch der Zugriff auf heterogene Datenquellen über Struktur- und Metainformationen, z.B. durch XML, ermöglicht eine flexiblere Nutzung verschiedenster Informationen, siehe Abschnitt 8.3.3.

**Verteilung und Dezentralisierung** (Abschnitt 6.10): Im Datenbankbereich ist der Trend der Verteilung und Dezentralisierung insbesondere bei Datenverwaltung und -analyse festzustellen (siehe Abschnitt 8.3.4). Um das rasant wachsende Datenaufkommen effizient verarbeiten zu können, werden zunehmend dezentrale Datenbanktechnologien eingesetzt und verteilte, auch heterogene Informationsquellen integriert. Des weiteren ist hier das wichtige Thema der Sicherheit in Datenbanksystemen zu erwähnen, auf das in Abschnitt 8.3.6 eingegangen wird. Aufgrund der steigenden Vernetzung und Interoperabilität, vor allem über das Internet, spielt die Integration von Sicherheitsmechanismen eine entscheidende Rolle. Eine ausführliche Behandlung des Themas Sicherheit findet sich in Kapitel 7.

**Virtualisierung** (Abschnitt 6.11): Virtualisierung ist ein Grenzfall bei der Behandlung der betrachteten übergreifenden Trends. Auf der einen Seite erwecken komplexe DBS, die eine Integration verteilter Daten(banken) realisieren, den Eindruck, als wären sie eine einzelne isolierte Anwendung. Auf der anderen Seite ist gerade diese Verteilung und Dezentralisierung effizient und oftmals technisch notwendig. Eine Datenbankanwendung alleine stellt aber noch keinen Schritt hin zur Virtualisierung von Geschäftsprozessen oder ganzen Unternehmen dar. Deshalb sei für eine genaue Betrachtung der Ausprägungen dieses Trends auf die Abschnitte 9.4 und 9.9 verwiesen.

In Tabelle 8.3 werden die oben genannten übergreifenden Trends nochmals aufgelistet und den spezifischen Trends dieses Technologiefeldes gegenübergestellt, die sich in den Gliederungspunkten dieses Abschnittes wiederfinden. Dabei zeigt sich, dass insbesondere die Trends zu Integration und Standardisierung einen sehr starken Einfluss auf die Entwicklungen im Bereich der Datenbanktechnologien haben. Ausserdem sind Trends wie Kapazitäts- und Leistungssteigerung sowie Vernetzung und Flexibilisierung in Zukunft wichtig für das Technologiefeld Datenbanken und Wissensmanagement. Im Folgenden werden nun die einzelnen spezifischen Trends im Bereich der Datenbanken ausführlich untersucht.

### 8.3.1 Datenmodellierung und Datenbanksysteme

Die Informations- und Datenverarbeitung wird zunehmend komplexer und erfordert daher neue technische Hilfsmittel. Um die immer größer werdende Datenflut kontrolliert und sinnvoll nutzen zu können, werden z.B. Inferenzmechanismen eingesetzt, die vorhandene Daten mit logikbasierten Regeln auswerten und daraus zusätzliche Informationen gewinnen. Der Vorgang der Wissensbildung, d.h. spezielles Wissen aus bestehendem, allgemeinem Wissen abzuleiten, wird Deduktion genannt [ElNa 00]. Im Bereich der Datenbanken zeichnet sich die Entwicklung ab, deduktive Techniken zur Wissensgenerierung in Datenbanksysteme (DBS) zu integrieren. Im Rahmen der vorliegenden Studie wurde ermittelt, welchen Einfluss diese Entwicklung auf die marktüblichen Datenbanksysteme haben wird und wann mit einer umfassenden Integration solcher Techniken zu rechnen ist.

Relationale Datenbanksysteme dominieren heute als etabliertes Konzept das Technologiefeld der Datenbanken. Ein Großteil aller Geschäfts- und Prozessdaten in Wirtschaft und Verwaltung ist in relationalen Datenbanksystemen abgelegt. Die verwendeten Datentypen und Abfragemöglichkeiten sind für Standardanwendungen vollkommen ausreichend, da Informationen in Tabellenform vorliegen und klar strukturiert miteinander verknüpft sind. Als Folge der Entwicklung neuer Technologien haben sich allerdings neue Anforderungen an Datenbanksysteme ergeben, z.B. bei komplexen Daten, vor allem im Multimediabereich, aber auch bei Schnittstellen zu proprietären IT-Systemen und bei der Integration von semistrukturierten Daten durch XML [HSH$^+$ 97, Davi 96]. Auch die Integration neuer Funktionen und Anwendungen wie CAD (Computer Aided Design) oder CASE (Computer Aided Software Engineering) oder die Verarbeitung geographischer Daten (Abschnitt 8.3.2) ist mit relationalen Datenbanksystemen nur unzureichend zu bewältigen [CoBe 02, ElNa 00]. Vordefinierte Typkonzepte und darauf abgestimmte Anfragesprachen bieten keine Möglichkeit, neben der reinen Datenverwaltung auch neue Medientypen oder anwendungsspezifische Regeln zu integrieren.

| Übergreifende Trends | Ausprägung im Bereich Datenbanken: Datenmodellierung und Datenbanksysteme | Standardisierung von Schnittstellen und Anwendungsintegration | Interoperabilität, Elexibilisierung und Vernetzung von Datenbanken | Datenanalyse und Datenauswertung | Performancesteigerung und Technologiefortschritt | Sicherheit in Datenbanken | 2003 | 2000 |
|---|---|---|---|---|---|---|---|---|
| Automatisierung und Vereinfachung | | ● | | ● | | | ◔ | ◔ |
| Dienst und Komponentenorientierung | | | ● | ● | | | ◔ | ○ |
| Globalisierung und Wettbewerb | | | | | | | ○ | ○ |
| Integration und Standardisierung | ● | ● | ● | | ● | | ◕ | ◕ |
| Kapazitäts- und Leistungssteigerung | | | ● | ● | ● | | ◕ | ◔ |
| Konvergenz | ● | ● | | | | | ◔ | ◔ |
| Miniaturisierung | | | | | | | ○ | ○ |
| Mobilität | | | | | | | ○ | ○ |
| Vernetzung und Flexibilisierung | | ● | ● | ● | | | ◔ | ◔ |
| Verteilung und Dezentralisierung | | | ● | | | ● | ◔ | ◔ |
| Virtualisierung | | | | | | | ○ | ○ |

Tabelle 8.3: Ausprägungen übergreifender Trends im Technologiefeld Datenbanken und Wissensmanagement

Aufgrund der neuen Anforderungen ist es nicht ausreichend, bestehende Systeme herstellerseitig um gewisse Datentypen, Indexstrukturen und Funktionalitäten zu erweitern. Vielmehr ist es erforderlich, das etablierte relationale Datenmodell flexibler zu gestalten und um objektorientierte Komponenten zu erweitern. So ist es jedem Entwickler möglich, neue Funktionen, Typen, Regeln und somit neue Anwendungen in Datenbanksysteme zu integrieren und die immer komplexeren Anforderungen bewältigen zu können. Dies wird mit objektrelationalen Datenbanksystemen erreicht [KeEi 97]. Dem gegenüber steht die Entwicklung rein objektorientierter Datenbanken, denen ein völlig anderes Datenmodell zugrunde liegt. Hierbei sind Informationen nicht in Tabellenform miteinander verknüpft, sondern liegen als Objekte mit Eigenschaften und Funktionen in einer Hierarchie vor [CoBe 02, Voss 00].

Für die Verarbeitung sehr großer Datenmengen stehen zudem auch multidimensionale Datenbanksysteme zur Verfügung, in denen die Daten nicht nur in zweidimensionalen Tabellen, sondern in mehrdimensionalen Matrizen und Quadern abgelegt sind. Dies ermöglicht effizientere Abfragen und komplexere Auswertungen der Informationen [CoBe 02].

Im vorliegenden Abschnitt wird untersucht, wie sich die (teilweise) konkurrierenden Datenmodelle bzw. Datenbanksysteme in den kommenden Jahren weiterentwickeln werden und welche Rolle vor allem objektrelationale Systeme künftig spielen werden.

## Ergebnisse

Die befragten Experten erwarten, dass deduktive Datenbanktechniken zur Unterstützung der Datenanalyse und Wissensgenerierung in vier Jahren verfügbar sein werden, wie in Abbildung 8.65, ① ersichtlich. Damit werden die Aussagen der Industrievertreter aus der Vorgängerstudie [SETIK 00] bestätigt, während sich die damals sehr optimistisch ausgefallenen Erwartungen der Vertreter aus der Wissenschaft nicht erfüllt haben. Zwar existieren bereits heute ansatzweise entsprechende Erweiterungen in den gängigsten Datenbanksystemen, diese seien allerdings bisher noch nicht ausgereift und würden daher bei den Usern auf wenig Akzeptanz stoßen. Anwendungsgebiete sehen die Befragten in der Verwaltung besonders großer Datenmengen, z.B. im komplexen Knowledge Management und im CRM (Customer Relationship Management), vor allem bei Data Mining und Data Warehousing (vgl. Abschnitt 8.3.4), aber auch zur semantischen Analyse von natürlicher Sprache oder im geographischen Bereich, z.B. zur Optimierung von Navigationssystemen.

In Zukunft werden objektrelationale Datenbanksysteme eine zunehmend wichtige Rolle spielen. Auf die Frage, wann objektrelationale Datenbanksysteme rein objektorientierte Systeme ablösen werden, antworten die Experten, dass dies in ca. fünf Jahren zu erwarten sei (Abbildung 8.65, ②). Allerdings betonen auch einige, dass eine völlige Verdrängung niemals eintreten werde, weil beide Konzepte ihre spezifischen Anwendungsmöglichkeiten haben und deshalb nicht in direkter Konkurrenz zueinander stehen. Insgesamt zeichnet sich jedoch im Vergleich zur Studie 2000 ein deutlicher Trend zu objektrelationalen Datenbanken ab. Die Befragten messen diesen Systemen inzwischen eine größere Bedeutung bei und erwarten eine weitgehende Verdrängung rein objektorientierter Datenbanken bereits einige Jahre früher als in der Vorgängerstudie. Als Anwendungsbereiche für objektrelationale Datenbanksysteme sehen die Experten komplexe Anwendungen wie webbasierte und multimediale Informationssysteme. So ist beispielsweise ein Städteinformationssystem vorstellbar, in dem Anfahrtspläne, Photographien sowie andere mit Bildern angereicherte Dokumente ebenso wie Audio- und Videosequenzen verarbeitet werden. Weiterhin ermöglichen objektrelationale Datenbanksysteme die Integration von Funktionen wie CAD oder CASE (Abschnitt 8.3.2 und 8.4.5). Rein objektorientierte Datenbanksysteme werden hauptsächlich Einsatz in wissenschaftlichen Spezialgebieten finden, bei denen ihre Komplexität und die damit verbundenen Implementierungs- bzw. Bedienungsschwierigkeiten kein Hemmnis darstellen. Von einigen Experten wird darauf hingewiesen, dass sich auch in Bereichen, in denen Navigation entscheidend ist, objektorientierte Systeme behaupten werden.

Eine echte Konkurrenz stellen die objektrelationalen Datenbanken dagegen für die rein relationalen Systeme dar. Eine Verdrängung relationaler Systeme erwarten die Befragten in fünf Jahren (vgl. Abbildung 8.65, ③), wobei Vertreter aus der Wirtschaft mit Prognosen von mehr als zehn Jahren pessimistischer sind als ihre Kollegen aus Wissenschaft und Forschung. Die Experten betonen, dass es eine unbedingte Voraussetzung für eine solche Ablösung sei, die Technologien objektrelationaler Datenbanken noch weiter zu verbessern, vor allem bzgl. der Standardisierung von Objekten und von Abfragemechanismen. Da relationale Datenbanken heute weit verbreitet sind, müssten sich zudem für die Anwender deutlich sichtbare Vorteile ergeben, damit sich ein Umstieg auf objektrelationale Systeme lohne.

Den Einsatz multidimensionaler Datenbanksysteme sehen die Experten hingegen bisher lediglich in wenigen Spezialanwendungen, insbesondere zur effizienteren Verwaltung und Analyse sehr großer Datenmengen, z.B. beim Data Mining und in Data Warehouses. Da die Entwicklung dieser neuen Technologie jedoch noch nicht abgeschlossen sei, erwarten die Befragten in absehbarer Zeit keine Ablösung relationaler Systeme durch multidimensionale (vgl. Abbildung 8.65, ④).

Insgesamt lässt sich daher folgern, dass in den kommenden Jahren zwar vor allem objektrelationale Datenbanksysteme stark an Bedeutung gewinnen werden, jedoch die Dominanz relationaler Systeme so schnell noch nicht durchbrechen können, da diese für viele Datenbankanwendungen nach wie vor die besten Möglichkeiten bieten.

DEDUKTIVE DATENBANKTECHNIKEN: Datenbanksysteme, die deduktive Datenbanktechniken integrieren, werden in den nächsten 4 Jahren verfügbar sein.

DATENBANKSYSTEME: Objektrelationale Datenbanksysteme werden stark an Bedeutung gewinnen und objektorientierte sowie rein relationale Systeme in 5 Jahren weitgehend abgelöst haben. Eine vollständige Verdrängung relationaler Datenbanken durch andere Modelle ist aber nicht zu erwarten.

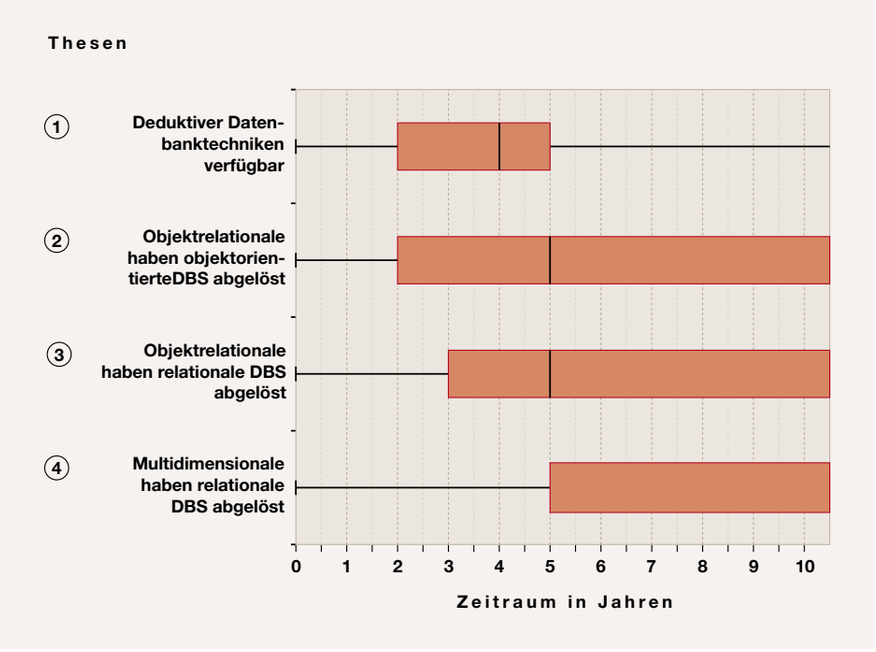



Abbildung 8.65: Ergebnisse der Thesen zu Datenmodellierung und Datenbanksystemen

## Zusammenfassung

Die Auswertung des ersten Fragenbereiches hat ergeben, dass im Wesentlichen zwei Tendenzen abzusehen sind: Um die immer größer und komplexer werdenden Datenbestände verarbeiten zu können, werden sich in den kommenden Jahren neue Techniken wie deduktive Datenbanken zur effizienteren Informationsverarbeitung durchsetzen. Des Weiteren werden sich künftig objektrelationale Datenbanksysteme zunehmend in vielen Bereichen behaupten. Die Ergebnisse lassen sich in folgenden Thesen zusammenfassen:

- Datenbanksysteme, die deduktive Datenbanktechniken integrieren, werden bis 2007 verfügbar sein.
- Objektrelationale Datenbanksysteme werden künftig von großer Bedeutung sein. Eine weitgehende Ablösung objektorientierter, aber auch rein relationaler Systeme durch objektrelationale Datenbanken ist bis 2008 abzusehen.
- Rein relationale Datenbanken werden durch andere Modelle bis 2013 nicht verdrängt werden.
- Multidimensionale Datenbanksysteme werden sich erst nach 2013 zur Verarbeitung sehr großer Datenmengen durchsetzen.

## 8.3.2 Standardisierung von Schnittstellen und Anwendungsintegration

Mit zunehmender Verteilung und Vernetzung von Systemen, vor allem über das Internet, werden auch Datenbanksysteme mit modernen Technologien erweitert. Welche Trends dabei für die Integration neuer Funktionalitäten in Datenbanken verfolgt werden und welche für den Markt überhaupt interessant sind, wurde im Rahmen der vorliegenden Studie untersucht.

Für die Integration und Erweiterung von Datenbank-Funktionalität, z.B. im Multimediabereich sowie für komplexere Anwendungen wie CAD und CASE , sind Erweiterungsmöglichkeiten herkömmlicher Datenbanksysteme notwendig [CoBe 02]. Solche Erweiterungen auf Basis relationaler Datenmodelle werden bereits seit mehreren Jahren angeboten, im Bereich der objektrelationalen Datenbanksysteme existieren solche Möglichkeiten nur ver-

einzelt (z.B. in Form des Universal Server von Informix [Info 98]). Generell müssen zur breiten Integration von Funktionalität objektorientierte Methoden eingebunden werden (vgl. Abschnitt 8.3.1). In der vorliegenden Studie wurde deshalb untersucht, inwieweit solche Funktionen in Datenbanksysteme integriert werden sollten, um neue Anwendungsbereiche für Datenbanken zu erschließen, welche aktuellen Entwicklungen es gibt und welche Trends abzusehen sind. Da sich bereits heute abzeichnet, dass insbesondere geographische Funktionalität und Funktionen im Bereich CAD und CAM (Computer Aided Manufacturing) in Zukunft von Bedeutung sein werden, schließt sich an die Evaluierung von Erweiterungsmöglichkeiten zusätzlich die Frage nach der Relevanz dieser Funktionalitäten in den kommenden Jahren an.

Weiterhin wurde die Frage der Einbindung spezieller Verfahren zur Lösung statistischer Probleme gestellt. Dazu zählen evolutionäre Algorithmen und neuronale Netze. Evolutionäre Algorithmen haben ihre Wurzeln in der Bionik und basieren auf Grundmechanismen der biologischen Evolution, indem sie deren Methoden und Vorgänge imitieren. Unter dem Begriff evolutionäre Algorithmen werden verschiedene verwandte Algorithmen wie Genetic Programming, Evolutionsstrategien oder genetische Algorithmen subsumiert [Pohl 99]. Diese Methoden geben oft sehr gute Näherungslösungen für Optimierungsaufgaben, die aufgrund ihrer Komplexität durch herkömmliche Lösungsmethoden nicht zu bewältigen sind, z.B. in Fertigungssystemen, zur Optimierung von Ressourcenverteilungen oder auch in der Bioinformatik [Niel 96]. Neuronale Netze wurden im Rahmen der Forschung zu KI (künstliche Intelligenz) entwickelt und sind ein Rechenmodell für die Informationsverarbeitung [ElNa 00]. Die Vorteile neuronaler Netze gegenüber dem heute verwendeten, auf der Von-Neumann-Architektur basierenden, Rechenmodell sind die Lernfähigkeit und die Parallelität bei der Informationsverarbeitung. Wie die biologischen Vorbilder, die Nervensysteme von Lebewesen, bestehen künstliche neuronale Netze (KNN) aus einer Menge von Neuronen (Units), die über gewichtete Verbindungen vernetzt sind [NKK 01]. Anwendungsgebiete der resultierenden lernfähigen Methoden sind v.a. die Mustererkennung, aber auch nichtlineare Regression und Klassifikation von Objekten (siehe hierzu auch Abschnitt 8.3.4).

## Ergebnisse

Die Auswertung der Frage, welche Funktionalität in den kommenden Jahren weit verbreitet in Datenbanken integriert sein wird, lässt eine Bestätigung der Trends und Aussagen der Studie 2000 [SETIK 00] erkennen. Die damals vorausgesagte Fokussierung auf Webfunktionalitäten ist heute bereits in vielen Bereichen und in großem Umfang verwirklicht worden, z.B. in Data Warehouses, die es ermöglichen, Daten netzweit adäquat zu repräsentieren, aufzubereiten und zur Verfügung zu stellen. Als nächster Schritt wird von den Experten nun für die kommenden zwei Jahre die umfassende Integration von XML als Standardschnittstelle und -datenformat prognostiziert [XML 99, HeMe 02]. Nur dadurch können die Interoperabilitätsanforderungen durch die steigende Verteilung und Vernetzung von Datenbanksystemen bewältigt werden. In einem Zeitraum von zwei bis fünf Jahren werden Datenbanksysteme stärker zur Verwaltung sehr großer Datenbestände eingesetzt. Auch die Einbindung proprietärer IuK-Systeme durch EAI sowie von Web Services werden als neue Funktionalitäten erwähnt. In fünf bis zehn Jahren werden sich laut der Experten schließlich auch komplexe Funktionalitäten in Datenbanksystemen durchgesetzt haben. Hierbei sind vor allem die Integration von Multimedia- und geographischen (3D-)Daten sowie von Spracherkennung, die einer sich ändernden Mensch-Maschine-Interaktion Rechnung trägt, bedeutend (vgl. Abschnitt 8.1).

DEFINIERTE UND VEREINHEITLICHTE PROGRAMMIERSCHNITTSTELLEN: Derartige Schnittstellen für die Integration neuer Funktionen von DBS sind in 3 Jahren weit verbreitet.

Definierte und vereinheitlichte Programmierschnittstellen für die Integration neuer Funktionalität in Datenbanksysteme, insbesondere zum effizienten Einsatz von spezifischen Funktionen im Umgang mit Texten, Bildern und räumlichen Daten, werden nach Aussage der Experten in drei Jahren verbreitet zur Verfügung stehen (vgl. Abbildung 8.66, ①). Damit hat sich die entsprechende Trendprognose der Vorgängerstudie bestätigt, die Entwicklung der Schnittstellen scheint sich allerdings um ein Jahr zu verzögern. Als not-

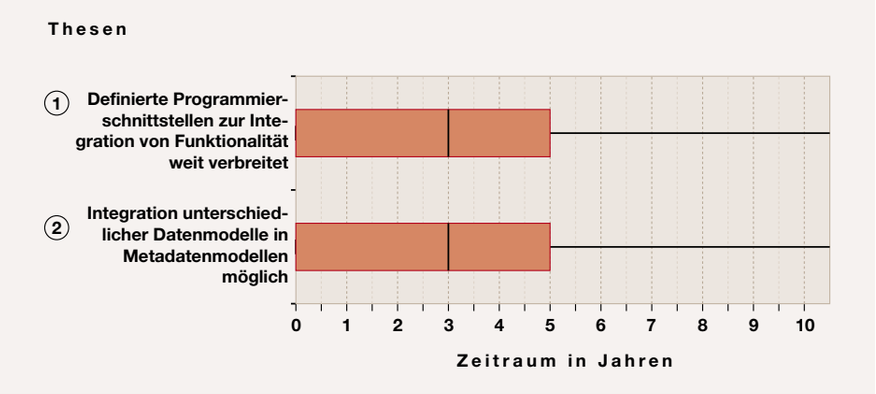



Abbildung 8.66: Ergebnisse der Thesen zu Integration von Funktionalität in Datenbanksystemen

INTEGRATION UNTERSCHIEDLICHER DATENMODELLE: Verschiedene Datenmodelle können in 3 Jahren in Metadatenmodellen integriert werden.

CASE-FUNKTIONALITÄTEN: Die Integration von Funktionen für CASE nimmt in den nächsten 10 Jahren stark zu. Der Integration geographischer Daten wird aber die größte Bedeutung zugemessen.

wendige Technologien dafür sehen die Befragten XML und Java an.

Die Auswertung ergibt auch, dass eine Integration unterschiedlicher Datenmodelle in Metadatenmodellen innerhalb der nächsten drei Jahre möglich sein wird. So können übergeordnete Schnittstellen geschaffen werden, um die Interoperabilität zwischen verschiedenen Datenbanksystemen und -modellen und ihre Integration zu gewährleisten. Damit können die jeweiligen Stärken relationaler, objektorientierter und objektrelationaler Datenbanken besser miteinander kombiniert werden (vgl. Abschnitte 8.3.1 und 8.3.5). Interessant ist hierbei, dass zahlreiche Vertreter aus Wissenschaft und Forschung diese These bereits heute als erfüllt betrachten, wohingegen Experten aus der Praxis einen Konsens über die Standardisierung solcher Metadatenmodelle noch vermissen.

Die befragten Experten gehen davon aus, dass vor allem die Integration von Funktionen zur Verarbeitung geographischer Daten innerhalb der nächsten zehn Jahre stetig weiterentwickelt und an Bedeutung gewinnen wird (vgl. Abbildung 8.67). Anwendungsmöglichkeiten werden im Bereich von Geo-Informations- und Navigationsystemen, z.B. bei GPS, aber auch in Logistik und SCM (Supply Chain Management) gesehen. Funktionalitäten zur Unterstützung von elektronischer Konstruktion, Zusammenbauanalyse und Ähnlichkeitssuche (CAD, CAM etc.) werden in den nächsten Jahren nur geringfügig an Bedeutung gewinnen, obwohl v.a. in der Automobilbranche und im Maschinenbau bereits Bedarf vorhanden ist. Die Experten sehen die Gründe hierfür in bisher unzureichenden Möglichkeiten, Konstruktions- und Produktionsdaten effizient zu beschreiben. Eine stetig wachsende Bedeutung wird hingegen bei der Integration von CASE-Funktionalitäten in Datenbanken erwartet, wobei auch hier der Bedarf bereits vorhanden ist, die technische Umsetzung allerdings noch einige Jahre auf sich warten lässt. CTI (Computer Telephone Integration) messen die Experten aus der Wirtschaft sehr wenig Bedeutung zu, während Vertreter aus Forschung und Wissenschaft zumindest gewisse Einsatzmöglichkeiten im CRM sehen. Die Ergebnisse sind in Abbildung 8.67 zusammengefasst dargestellt.

Allgemein merken die Befragten mehrmals an, dass es noch kontrovers diskutiert wird, bis zu welchem Maß es sinnvoll ist, komplexe Funktionalitäten in Datenbanksysteme zu integrieren. Denn diese müssten dadurch natürlich sehr viel leistungsstärker werden. Klare Schnittstellen und getrennte Bereitstellung von Funktionalitäten (Diversifikation) stehen hierbei einer umfassenden Integration von Funktionalität gegenüber. Diese Diskussion wird weiterführend nochmals im Rahmen der Flexibilisierung und Interoperabilität von Datenbanken aufgegriffen (vgl. Abschnitt 8.3.3).

Auch die Integration von Verfahren zur Lösung statistischer Probleme wurde in diesem Fragenkomplex untersucht. Die-

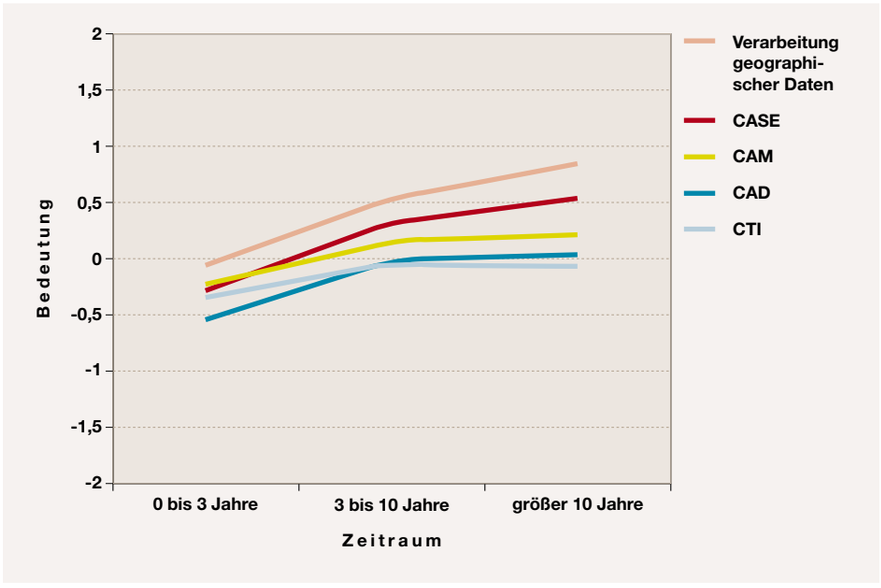



Abbildung 8.67: Bedeutung der Integration unterschiedlicher Funktionen in Datenbanksystemen


NEURONALE NETZE:
Neuronale Netze haben die gleiche Bedeutung wie evolutionäre Algorithmen. Experten aus der Wirtschaft messen beiden Verfahren höhere Bedeutung zu als Vertreter der Forschung.

sem Gebiet wird allgemein aber kaum Bedeutung zugemessen. Interessant ist, dass Vertreter der Forschung sowohl evolutionären Algorithmen als auch neuronalen Netzen geringere Bedeutung zumessen als Kollegen aus der Wirtschaft, die momentan offenbar noch größere Hoffnungen in diese Verfahren setzen. Als allgemeine Anwendungsgebiete werden hauptsächlich Data Mining und unscharf formulierte Abfragen (Fuzzy Logic) sowie Optimierungs- und Simulationsaufgaben genannt. Neuronale Netze finden dabei Anwendung im Multimediabereich, vor allem bei Spracherkennung und Grafikanalysen, vereinzelt wurden aber auch Prognose- bzw. Diagnosesysteme (z.B. in der Medizin oder im Finanzwesen) und Regelungstechnik erwähnt. Evolutionäre Algorithmen hingegen werden eher im Bereich komplexer Optimierungsaufgaben eingesetzt werden, z.B. in Navigationssystemen zur Tourenplanung.

## Zusammenfassung

Die Auswertung dieses Fragenkomplexes hat ergeben, dass ein wichtiges Merkmal künftiger Datenbanksysteme die Integration anwendungsspezifischer Funktionen sein wird, v.a. in den Bereichen Telekommunikation, Multimedia sowie Konstruktion und Navigation. Dabei lassen sich folgende Trends absehen:

- Definierte und vereinheitlichte Programmierschnittstellen zur Funktionsintegration werden bis 2006 zur Verfügung stehen. Dies wird stark zur Interoperabilität unterschiedlicher Datenbanksysteme beitragen. XML spielt dabei sowohl als Standardschnittstelle als auch in Metadatenmodellen eine wichtige Rolle.

- Die Integration von Funktionalität zur Verarbeitung geographischer Daten sowie eingebundene Funktionen ingenieurtechnischer Anwendungen werden in den kommenden Jahren von großer Bedeutung sein, auch wenn noch einige technologische Schwierigkeiten zu bewältigen sind.

- Statistische Verfahren werden verstärkt in Datenbanken eingebunden, z.B. im Multimediabereich oder um komplexe Optimierungsaufgaben zu lösen.

### 8.3.3 Interoperabilität, Flexibilisierung und Vernetzung von Datenbanken

Die globale Vernetzung bietet völlig neue Möglichkeiten im Datenbankbereich. Durch das Internet werden zum einen immer mehr heterogene, dezentrale Informationsquellen jeglicher Art verfügbar. Zum anderen ergeben sich auch zusätzliche Möglichkeiten, Datenbanksysteme mit Funktionalitäten und Anwendungen anzureichern sowie deren Interaktion zu verbessern. Um die Potenziale ausschöpfen zu können, die sich hierbei für das die elektronische Geschäftsabwicklung (E-Business) bieten, ist es erforderlich, Datenbanksysteme mit Internet-Technologien zu verknüpfen und Web-Funktionalitäten zu integrieren. In der vorliegenden Studie wurde deshalb untersucht, inwieweit dies bereits geschehen ist bzw. wie der Stand der Entwicklungen ist und welche Tendenzen hierbei abzusehen sind. Weiterführende Betrachtungen der Anwendungspotenziale des Internet finden sich in Abschnitt 9.1.

Grundlage für Interoperabilität und Vernetzung von Datenbanksystemen ist in erster Linie eine Vereinheitlichung von Schnittstellen. Durch die Möglichkeit des Zugriffs auf Metadaten, also auf Informationen über Daten [CoBe 02], kann dann zusätzlich eine Vielfalt heterogener Informationsquellen in Datenbanken integriert bzw. abgefragt werden, was mit herkömmlichen Datenbankanwendungen nur eingeschränkt möglich ist. Auch im Bereich Multimedia ist eine effiziente Nutzung heterogener Daten durch die Standardisierung von Schnittstellen und den Zugriff auf Metainformationen von großer Bedeutung [FH-F 99, OMG 99]. Metadatenformate wie XML und XMI oder Techniken zum Datenaustausch wie EDI [OMG 99], bieten Strukturinformationen für eine Verarbeitung bzw. Weiterverarbeitung dieser Datenbestände. XML (eine vereinfachte Form von SGML) ist deshalb so bedeutend, weil es universell und plattformübergreifend eingesetzt werden kann.

Die Integration von Webserver-Funktionalität in Datenbanksysteme ermöglicht Datenaustauch und -verwaltung durch Internet-basierte Transaktionen. Dabei werden Datenbankoperationen gebündelt und über Internet-Technologien, also vor allem HTTP (Hypertext Transfer Protocol) übermittelt. Die Experten wurden zu den Konzepten der Integration von Webserver-Funktionalität in Datenbanksysteme und der Transaktionen befragt. Die Nutzung verteilter Informationen durch Web-Datenbankabfragen und Web-basierte Transaktionen ist durch einfachen Datenaustausch zwischen Client (z.B. Web-Browser) und Server (Web- und/oder Datenbankserver) mittels Skriptsprachen wie Perl oder PHP oder durch Java oder ActiveX bereits möglich [Flan 96, JoNy 95]. Bei der ersten Variante bilden CGI (Common Gateway Interface) oder API (Application Programming Interface) die Schnittstellen zwischen Internet und Datenbankanwendungen, bei Java erledigt dies eine unabhängige und eigenständige Applikation [Amor 01, CoBe 02, ElNa 00]. Heute existieren zwei Möglichkeiten, wie Java-Applets, unter Nutzung des Java Socket Interface, auf Datenbanksysteme remote zugreifen können: zum einen durch die Nutzung einer Zweier-Architektur, in der alle Client-Funktionen komplett in Java implementiert sind und der Client ein HTTP- und Datenbank-Server ist, zum anderen durch die Nutzung einer Dreier-Architektur, wobei ein unabhängiger Java-Server als Gateway genutzt wird. Dieses Gateway vermittelt die Anfragen und Antworten zwischen dem Java-Applet und dem Datenbankserver, d.h. der Client fungiert als HTTP-, Gateway- und Datenbank-Server. Heute erfordern diese beiden Möglichkeiten allerdings einen sehr hohen Programmieraufwand [EbFi 01].

Weiterhin ist in diesem Zusammenhang auch die Diskussion interessant, bis zu welchem Maß es sinnvoll ist, komplexe Funktionalitäten in Datenbanksysteme zu integrieren, da diese dadurch natürlich sehr viel leistungsstärker werden müssen. Alternativ ist eine klar getrennte Bereitstellung von Funktionalitäten z.B. durch Web-Services möglich (Diversifikation), in diesem Fall also eine strikte Trennung von Webservern und Datenbankanwendungen (vgl. hierzu auch Abschnitt 8.3.2).

Im Zusammenhang mit der zunehmenden Interoperabilität von Datenbanksystemen sind Standarddateiformate von zu-

nehmender Bedeutung. Es wurde zur Diskussion gestellt, welche Rolle insbesondere XML spielt, einerseits zur standardisierten Ein- und Ausgabe in Datenbanken und andererseits bei der Integration und Abfrage semistrukturierter Daten, die z.B. unvollständig sind oder häufigen Änderungen unterliegen. XML entwickelt sich immer mehr zu einer Schlüsseltechnologie für neue Datenbankentwürfe und -realisierungen, die beliebige, auch multimediale, Daten speichern können. Eine Durchdringung des Marktes mit verteilten, vernetzten und interoperablen Datenbanksystemen wird es aus jetziger Sicht erst dann geben, wenn diese semistrukturierten Informationen verfügbar und integraler Bestandteil der Datenbanken sind [CoBe 02]. Bis wann dies eintreten wird, wurde in der vorliegenden Studie zur Diskussion gestellt. Zusätzliche Abschätzungen zu den Anwendungspotenzialen finden sich in Abschnitt 9.1.

Schließlich wurde dem Konzept der Vereinfachung und Flexibilisierung von Datenbanken Rechnung getragen. Denn nur dadurch wird eine Verbreitung der genannten Technologien möglich sein. Dabei wird v.a. die benutzerfreundliche Bedienbarkeit eine entscheidende Rolle spielen. Dieser Aspekt ist insbesondere im Sinne einer einfachen Kommunikation zwischen dem System und dem Benutzer und damit einer effizienten Nutzung von Informationen in Unternehmen und Behörden sehr wichtig. Sogenannte Expertensysteme, auch Managementinformationssysteme oder Entscheidungsunterstützungssysteme genannt, ermöglichen selbst ungeübten Anwendern (z.B. Führungskräfte ohne tiefgreifende technische Kenntnisse), Datenbanken mit geringem Einarbeitungsaufwand einsetzen und Informationen adäquat aufbereiten zu können. Dies wird entscheidend zu einer weiteren Verbreitung von Datenbanksystemen beitragen. Die Entwicklungen im Bereich der Expertensysteme und des Management-by-wire werden in den Abschnitten 9.4 und 9.5 ausführlich beschrieben. Zur einfacheren Bedienbarkeit ist darüber hinaus die Möglichkeit wünschenswert, sprachunabhängige Datenbankanfragen zu formulieren. Im Zuge der Internationalisierung gewinnt diese Problemstellung weiter an Gewicht. Schon heute wäre es oftmals sinnvoll, bei Suchanfragen nicht nur die verfügbaren Informationen in einer bestimmten Sprache zu verarbeiten, sondern ebenso auf Einträge in anderen Sprachen zurückgreifen zu können.

Obwohl bis heute fast ausschließlich SQL (Structured Query Language) als Abfragesprache in Datenbanksystemen benutzt wird, gibt es auf diesem Gebiet eine Reihe anderer Technologien und auch SQL selbst wird ständig weiterentwickelt. Abschließend wurde deshalb von den Befragten noch erläutert, welche Abfragesprachen für Datenbanken sich zukünftig durchsetzen werden.

## Ergebnisse

Die Nutzung heterogener Informationsquellen gewinnt stark an Bedeutung. Dies trifft insbesondere für internetweite Datenbankanwendungen zu. Die dafür notwendige Standardisierung von Datenbankschnittstellen wurde in der vorliegenden Studie in mehreren Thesen aufgegriffen. Die Ergebnisse der Umfrage prognostizieren, dass in fünf Jahren Datenbankschnittstellen weit verbreitet sind, die den Zugriff auf Metadaten heterogener Datenquellen erlauben (vgl. Abbildung 8.68, ①). Große Potenziale, vor allem bei der Einbindung proprietärer IuK-Systeme, der Interaktion verschiedener Anwendungen durch EAI, zur Archivierung oder im Knowledge Management werden von den Experten erwartet, sobald die Standardisierungsbemühungen bei Metadatenmodellen erfolgreich waren.

Die Verfügbarkeit solcher normierten und standardisierten Schnittstellen, präzisiert auf die Bereiche World Wide Web und Multimedia, z.B. für Audio- und Videostreaming oder Multimedia-Informationssysteme wird in ca. vier Jahren erwartet (vgl. Abbildung 8.68, ②). Eine weitgehende Adaption der Datenbanksysteme an diese Normen erwarten die Experten jedoch erst in sechs bis sieben Jahren, da sich die Hersteller nur langsam an derartige Standardisierungen anpassen.

Zur Integration heterogener Daten verliert Electronic Data Interchange als altbewährte, aber nicht flexible Infrastruktur für standardisierten Datenaustausch schon heute rasant an Bedeutung. In zehn Jahren wird es kaum noch verwendet wer-

DATENBANKSCHNITTSTELLEN: Standardisierte Schnittstellen, die den Zugriff auf Metadaten heterogener Informationsquellen ermöglichen, werden in 5 Jahren verbreitet sein. Normierte und standardisierte Schnittstellen im Multimediabereich werden in 4 Jahren verfügbar sein.

ELECTRONIC DATA INTERCHANGE: EDI wird als Format zur Integration heterogener Daten rasch an Bedeutung verlieren und von XML abgelöst werden.

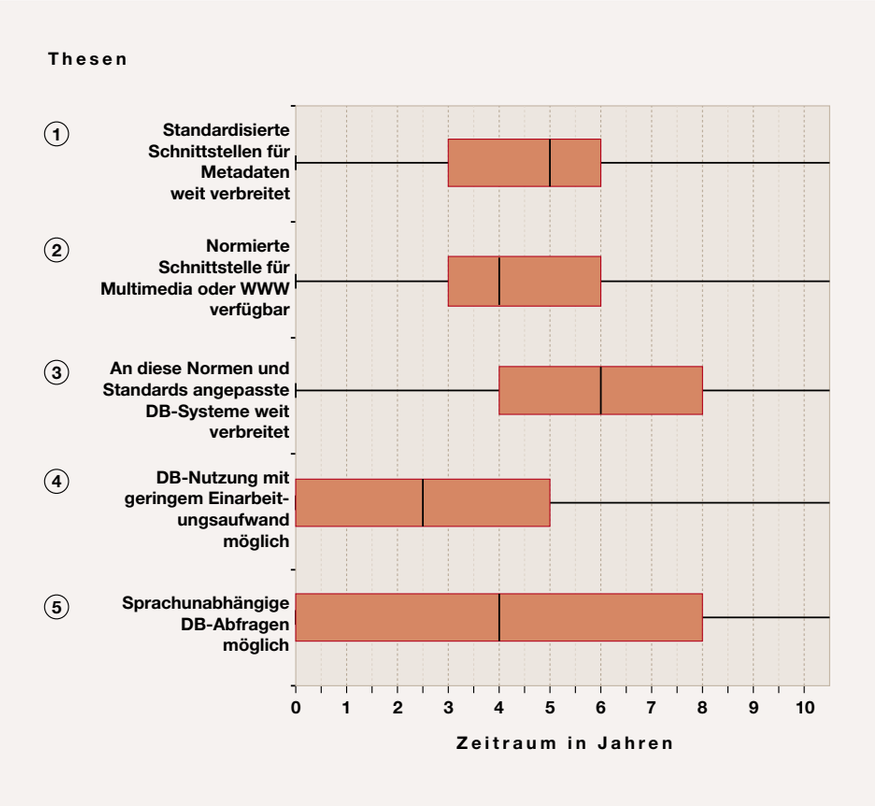



Abbildung 8.68: Ergebnisse der Thesen zu Standardisierung von Datenbankschnittstellen sowie zu Vereinfachung und Flexibilisierung

den. Den Grund dafür sehen die Befragten in der Verdrängung durch standardisierte XML-Schemata wie ebXML oder RosettaNet. XML wird laut Aussagen vieler Experten innerhalb der nächsten drei Jahre zum Standardformat jeglichen Datenaustauschs, da es als Metasprache im Gegensatz zu EDIFACT eine flexible Spezifikation der Austauschformate und -bedingungen ermöglicht [Amor 01]. Profitieren wird davon vor allem das E-Business, insbesondere im zwischenbetrieblichen Bereich (z.B. E-Procurement, SCM etc.). Die Ergebnisse der Umfrage sagen aber auch deutlich aus, dass die Weiterentwicklung von XML bald abgeschlossen sein wird. Interessanterweise erwähnen etliche Befragte, für eine langfristige Betrachtung sei die technische Entwicklung eines XML-Nachfolgers entscheidend. Dieses Thema wird bei der Betrachtung der Digitalisierung und Automatisierung von Wertschöpfungsketten und des E-Commerce in Abschnitt 9.1 nochmals behandelt.

Die Nutzung und Verwaltung von global verfügbaren Informationen ist durch Web-Datenbankabfragen und Internet-basierte Transaktionen realisierbar. Die oben genannten Technologien wie CGI, API und der damit realisierte Datenaustausch sind allerdings nicht ohne weiteres in bestehende Datenbanksysteme integrierbar. Deshalb ist eine weitreichende Verbreitung von Webserver-Funktionalität als fester Bestandteil von Datenbanksystemen erst in drei Jahren abzusehen (vgl. Abbildung 8.70, ①). Damit haben sich die Prognosen der Industrievertreter in der Vorgängerstudie bestätigt, während sich die damaligen Aussagen der Vertreter aus der Wissenschaft als zu optimistisch herausgestellt haben [SETIK 00]. Dies ist wohl auch damit zu erklären, dass sich die Integration dieser Technologien oft schwierig gestaltet, wie einige Befragte anmerken.

Für Datenbanken ist das Konzept der Transaktionen von besonderer Bedeutung. Sie werden verwendet, um mehrere Datenbankoperationen zu bündeln und als

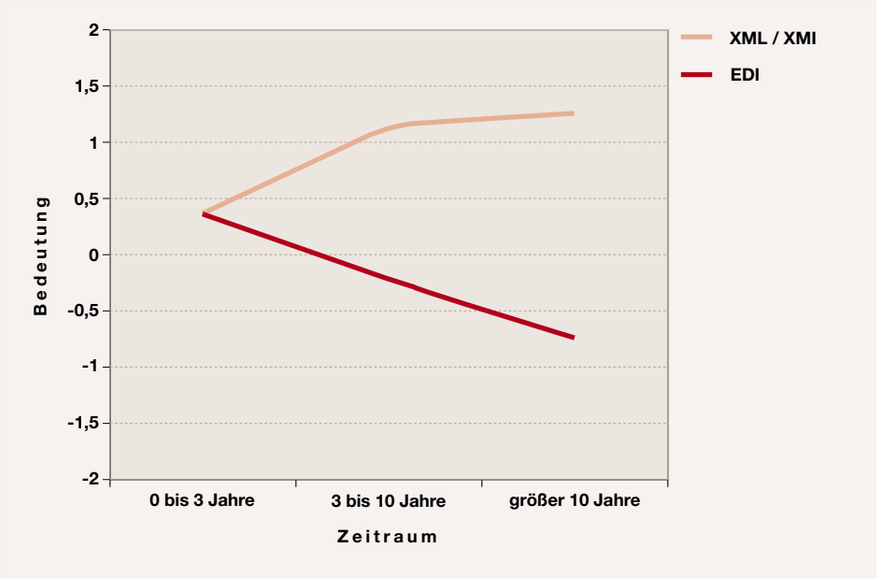



Abbildung 8.69: Bedeutung verschiedener Techniken zur Integration von heterogenen Daten

Einheit auszuführen. Im Internet-Umfeld bedeutet dies, dass Transaktionen nicht nur lokal, sondern ebenso verteilt ausführbar sein müssen. Konzepte und Datenbanksysteme, die diese Transaktionen über das Internet erlauben, sind noch nicht verfügbar. Solche HTTP-basierten Transaktionen inklusive einer geeigneten Transaktionsverwaltung werden erst in vier Jahren im Datenbankbereich als Basistechnologie weit verbreitet sein (vgl. Abbildung 8.70, ②). Damit wurden die optimistischen Erwartungen der Vorgängerstudie nicht erfüllt, vor allem weil Tools zur Transaktionsverwaltung noch zu optimieren und zu standardisieren bzw. eventuell sogar in ein Nachfolgeprotokoll von HTTP einzubinden seien. Als Hemmnis bei der Umsetzung dieser Technologien wird von einigen Experten auf die kritische Sicherheit der Systeme hingewiesen, da hier oft vertrauliche und geschäftsrelevante Informationen in Datenbanken zugänglich gemacht werden (vgl. Abschnitt 8.3.6).

Im Rahmen der Vereinheitlichung wird das Thema der Integration bzw. Diversifikation von Funktionalität von Datenbanksystemen, wie auch schon in der letzten Studie, kontrovers diskutiert. Während die Integration das Ziel verfolgt, möglichst viele Funktionen direkt in die Datenbank zu integrieren und somit eine Vielzahl von Benutzern abzudecken, ist das Ziel der Diversifikation die Definition klarer Schnittstellen in Struktur- bzw. Schichtenmodellen und die getrennte Bereitstellung der erforderlichen Funktionalität. Einige Befragte begrüßen eine strikte Diversifikation, also eine Trennung von Daten und Anwendungen, um die zunehmende Komplexität bewältigen zu können. Andere Experten hingegen befürchten, dass den Entwicklern dazu das notwendige Maß an Abstraktionsvermögen fehle. Deshalb plädieren sie für eine umfassende Integration von Funktionalität in Datenbanksysteme. Wie in der Studie 2000 prognostiziert, haben sich die beiden Konzepte bzgl. ihrer Bedeutung im Datenbankbereich inzwischen angenähert, d.h. Diversifikation hat an Bedeutung verloren. Dies sei damit zu erklären, dass die Integration von Funktionalität durch immer leistungsfähigere und robustere Datenbanksysteme erleichtert wird. Diese Diskussion wurde bereits im Rahmen der Schnittstellen und Anwendungsintegration angestoßen (vgl. Abschnitt 8.3.2).

Im Rahmen der Flexibilisierung und Vereinfachung wurden zwei Methoden zur Diskussion gestellt. Zum einen schätzen die Experten, dass einfache Benutzerschnittstellen, die eine einfache und schnell erlernbare Nutzung von Datenbanken ohne großen Einlese- und Einarbeitungsaufwand ermöglichen, in zwei

TRANSAKTIONEN: In 3 Jahren wird Webserver-Funktionalität als integraler Bestandteil von Datenbanksystemen weit verbreitet sein. HTTP-basierte Transaktionen werden jedoch erst in 4 Jahren als Basistechnologie Einsatz finden.

FUNKTIONALITÄT: Die Frage, inwieweit Funktionen in Datenbanksysteme integriert oder ob Funktionalität durch klare Schnittstellen abgetrennt werden sollte (Integration vs. Diversifikation), wird weiterhin sehr kontrovers diskutiert.

VEREINFACHUNG: Die Benutzerfreundlichkeit von Datenbanksystemen wird sich in den kommenden 3 Jahren erheblich verbessern. In den nächsten 4 Jahren werden sprachunabhängige Datenbankabfragen Interoperabilität fördern.

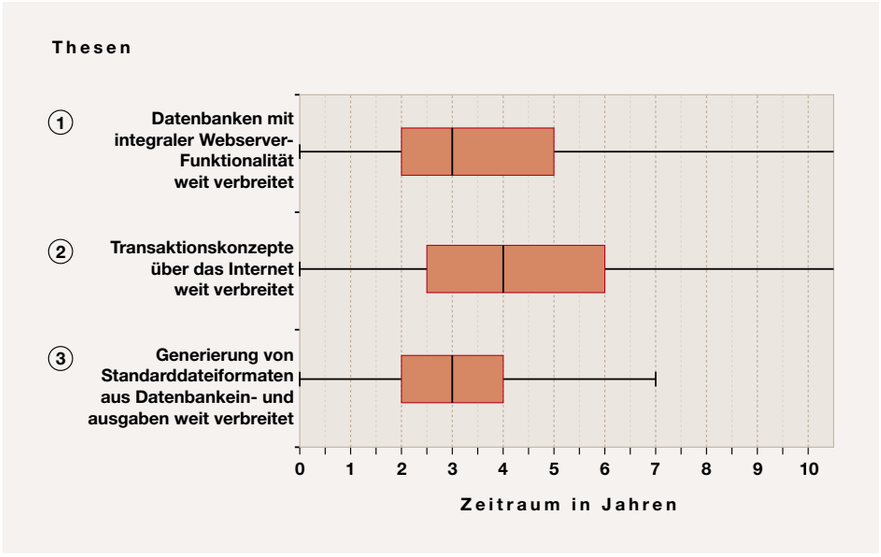



Abbildung 8.70: Ergebnisse der Thesen zu Vernetzung und Interoperabilität

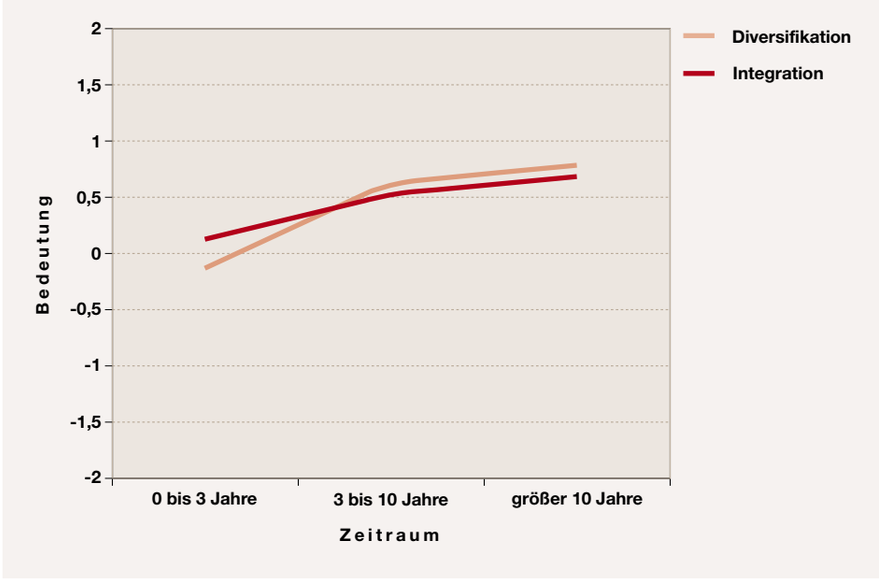



Abbildung 8.71: Bedeutung von Integration bzw. Diversifikation für DBS

bis drei Jahren verfügbar sind (vgl. Abbildung 8.68, ④). Zwar ist dies bei einfachen Datenbankanwendungen für den privaten Gebrauch (z.B. Microsoft Access) bereits möglich, bei komplexeren Datenbanksystemen im Unternehmensumfeld jedoch noch nicht, obwohl immer mehr Unternehmensrollen im Managementbereich Gebrauch von Entscheidungsunterstützungssystemen und Informationssystemen im Bereich Knowledge Management, -Recovery und -Retrieval machen.

Im Hinblick auf die zunehmende globale Vernetzung ist weiterhin die Möglichkeit wünschenswert, sprachunabhängige Datenbankabfragen zu formulieren. Die damit einhergehende Internationalisierung von Datenbanken prognostizieren die Befragten für den Zeitraum der kommenden vier Jahre (vgl. Abbildung 8.68, ⑤). Damit ist die Prognose der Vorgängerstudie eindeutig bestätigt worden und befindet sich auf einem guten Weg zur Realisierung. Von Bedeutung wird die Abfrage von Informationen unterschiedlicher Sprachen v.a. in den Bereichen Knowledge Discovery, bei länderübergreifenden Informationssystemen und für die Weiterentwicklung des World Wide Web sein.

Für Datenbank-Abfragetechniken sind semistrukturierte Daten wie XML sehr wichtig, diese werden allerdings bereits in drei Jahren auf dem Höhepunkt ihrer Bedeutung angelangt sein (vgl. Abbildung 8.72). Insbesondere zum Ansprechen von nicht in Tabellen abgelegten Informationen verlangen vor allem Experten aus der Wissenschaft eine Weiterentwicklung zu einer noch flexibleren, offeneren und dynamischen Technologie.

Die Generierung und Verarbeitung von XML oder anderer Standard-Dateiformate aus Ein- und Ausgaben von Datenbanken wird nach Ansicht der Experten erst in drei Jahren weit verbreitet sein (vgl. Abbildung 8.70, ③), obwohl die notwendigen Technologien bereits vorhanden sind.

Bei den derzeit verwendeten Abfrage-Sprachen wird SQL weiterhin seine dominierende Stellung in kommerziellen Datenbanksystemen behalten, langfristig jedoch im Vergleich zu Alternativen etwas an Bedeutung verlieren (vgl. Abbildung 8.73). Daneben schätzen die Befragten insbesondere XQL (XML Query Language) sowie XSL (Extensible Stylesheet Language) als die in den nächsten zehn Jahren bedeutendsten Abfragesprachen ein. Diese XML-basierten Technologien ermöglichen es, auch semistrukturierte Daten zu durchsuchen, die nicht in Tabellenform, sondern in beliebigen Dokumenten vorliegen [Robi 99]. Graphische Methoden wie GQL (Graphical Query Language) oder QBE (Query-By-Example) hingegen sind trotz ihrer Benutzerfreundlichkeit kaum von Bedeutung, da sie keine komplexen Aufgaben lösen können. Die für objektorientierte Systeme entwickelte OQL (Object Query Language) soll zwar in den kommenden drei Jahren leicht an Bedeutung gewinnen, bleibt jedoch nach Meinung der Experten langfristig unbedeutend. Dies ist mit der Tatsache zu erklären, dass der SQL-Standard um objektorientierte Funktionalitäten erweitert und weiterentwickelt wird [ISO 9075] und damit eine eigenständige objektorientierte Abfragesprache unnötig macht.

Hier ergibt sich ein interessanter Unterschied zur Vorgängerstudie: Zwar wurde die Dominanz von SQL bereits vor drei Jahren deutlich ausgedrückt, jedoch erwarteten die Experten damals, dass sich - wenn überhaupt - eher graphisch-orientierte Abfragesprachen durchsetzen könnten, während heute XML-basierte Abfragesprachen wichtiger erscheinen. Dies wird mit einer Trendwende weg von der alleinigen Fokussierung auf Benutzerfreundlichkeit hin zu einer umfassenden Integration und Interoperabilität jeglicher Systeme, vor allem proprietärer IuK-Systeme, erklärt. XML kann hier sowohl als Basis für Abfragesprachen als auch in anderen Bereichen wichtige Beiträge leisten (vgl. auch Abschnitt 8.3.2).

STANDARD-DATEIFORMATE: Die Bedeutung von XML als Standarddateiformat sowie zur Integration semistrukturierter Daten wird in den nächsten drei Jahren stark zunehmen.

ABFRAGE-SPRACHEN: Als Datenbank-Abfragesprache wird SQL weiterhin seine dominierende Stellung behalten, in den kommenden Jahren werden allerdings XML-basierte Abfragesprachen an Bedeutung gewinnen.

## Zusammenfassung

Die Auswertungen haben aufgezeigt, dass im Zuge der wachsenden Vernetzung, vor allem über das Internet, Interoperabilität, Flexibilisierung und Verteilung in Zukunft wichtige Erfolgskriterien von Datenbanksystemen sind. Dies erfordert noch eine stärkere Verbreitung und marktliche Durchdringung von Standard-Dateiformaten sowie einen weiteren Anstieg von integrierter Webserver-Funktionalität in Datenbanksystemen. Im einzelnen haben sich folgende Prognosen ergeben:


Abbildung 8.72: Bedeutung von semistrukturierten Daten für Abfragetechniken

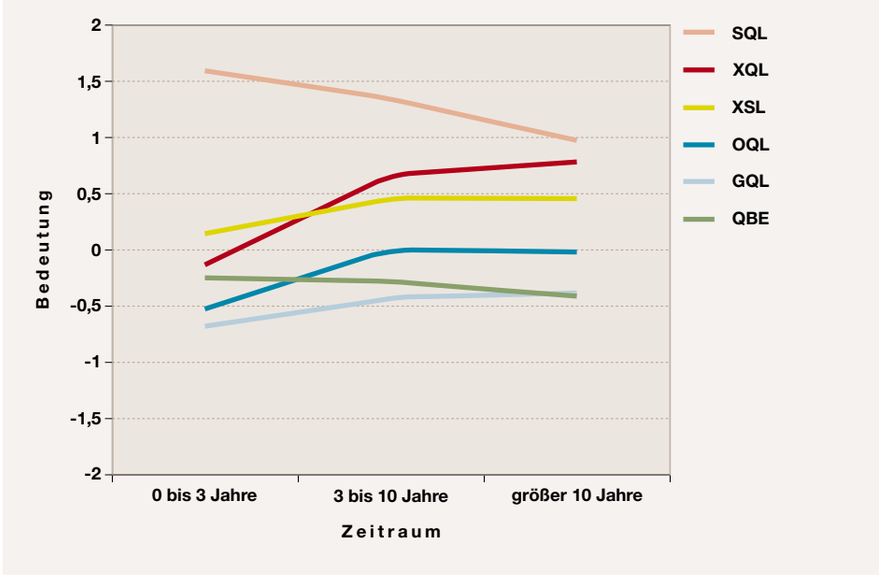



Abbildung 8.73: Bedeutung unterschiedlicher Datenbank-Abfragesprachen

- Standardisierte Schnittstellen, die den Zugriff auf Metadaten heterogener Datenquellen ermöglichen, werden eine breite Akzeptanz finden. Die Integration dieser Standards in Datenbanksysteme wird bis 2008 erwartet. Normierte Schnittstellen, vor allem im Multimediabereich, werden bis 2010 von DBS adaptiert sein.

- Die Bedeutung von XML als Standarddateiformat sowie der Integration semistrukturierter Daten wird zunehmen und bis 2006 die Interoperabilität von Datenbanksystemen stark verbessern.

- EDI wird in den kommenden Jahren kaum noch Bedeutung beim standardisierten Datenaustausch von hauptsächlich heterogenen Daten im Geschäftsbereich haben und bereits 2006 weitgehend durch XML-Schemata abgelöst werden.

- Bis 2006 wird Webserver-Funktionalität als integraler Bestandteil von Datenbanksystemen zunehmend Transaktionen über das Internet ermöglichen. HTTP-basierte Transaktionen werden jedoch erst ab 2007 als Basistechnologie im Datenbankbereich verbreitet sein.

- Einfache Benutzerschnittstellen werden ab 2006 verfügbar sein und die Bedienbarkeit von Datenbanken erheblich erleichtern, auch bei komplexeren Datenbanksystemen. Ab 2007 werden zudem sprachunabhängige Datenbankabfragen verbreitet sein.

- Als Datenbank-Abfragesprache wird SQL weiterhin seine dominierende Stellung in kommerziellen Datenbanksystemen behalten, in den kommenden Jahren werden allerdings vor allem XML-basierte Abfragesprachen an Bedeutung gewinnen.

### 8.3.4 Datenanalyse und Datenauswertung

Infolge der wachsenden Bedeutung von strukturierten Informationen im Allgemeinen und der immer größeren Anwendungsmöglichkeiten, die sich im Datenbankbereich ergeben, spielen effiziente Datenanalyse und komplexe Datenauswertung eine immer wichtigere Rolle. Hierbei sind zwei Trends zu unterscheiden:

Zum einen konzentrieren sich Datenanalyseverfahren auf die Auswertung und Verwaltung aktueller Daten. Dies ist durch Begriffe wie OLTP, OLAP und Data Warehouses gekennzeichnet [KeEi 97]. Zum anderen setzen sich zunehmend Konzepte zur Wissensgenerierung (Knowledge Discovery) durch. Dabei wird anhand bestehender Datensammlungen nach nützlichen Zusammenhängen, Mustern und daraus ableitbaren Zusatzinformationen gesucht, ohne dass spezielle Eigenschaften oder Attribute der Datensätze bekannt sein müssen. Dieser Trend ist hauptsächlich unter dem Schlagwort Data Mining bekannt [GMD 99].

OLTP ist in traditionelle Datenbanksysteme integriert, ermöglicht dort Transaktionen wie Updates oder Abfragen aktueller Daten und kann daher als Kernstück von Datenbankanwendungen gesehen werden. OLTP arbeitet also prozess- bzw. transaktionsorientiert mit begrenzten Datenbeständen, die auf dem aktuellsten Stand gehalten werden. Im Gegensatz dazu bezieht sich OLAP auf die komplexere Analyse sehr großer Datenmengen. Einfache Drag&Drop-Anwendungen ermöglichen dabei schnelle ad hoc-Abfragen mit geringem Aufwand. Die Daten werden in Data Warehouses gespeichert, die das zentrale Datenarchiv eines Unternehmens darstellen und beispielsweise für historische Zeitreihenanalysen verwendet werden. Eine Data Mart ist eine Untermenge des Data Warehouse und wird meist dann eingesetzt, wenn eine Trennung innerhalb der Organisation, beispielsweise bei der Verwendung eines Data Warehouse durch mehrere Abteilungen, oder der Daten vorliegt [MoRo 01]. Je nach zugrunde liegendem Architekturkonzept unterscheidet man bei den Analysemethoden Relational OLAP, Multidimensional OLAP und Hybrid OLAP, eine Verbindung der beiden lezteren. Teilweise werden OLAP-Funktionalitäten als Erweiterungen von SQL in bestehende Datenbanksysteme eingebunden, für komplexere Einsatzmöglichkeiten jedoch werden OLAP-Tools als eigenständige Anwendungen eingesetzt.

Der Bereich Knowledge Discovery bzw. Data Mining hat im Gegensatz dazu das Ziel, die immer größer werdende Da-

tenmenge sinnvoll zu nutzen. Es wird deshalb mit Methoden des Data Mining versucht, aus gegebenen, eventuell historisch gewachsenen und meistens sehr großen Datenbeständen neue Zusammenhänge und Erkenntnisse zu gewinnen [RaSc 99, Univ 99]. Es handelt sich also um Verfahren zur Wissensgenerierung, die immer weitere Verbreitung finden und die in Unternehmen immer öfter auch als entscheidungsunterstützende Systeme (Decision Support Systeme, DSS) eingesetzt werden [NFD 99, Tecm 99]. Im Wesentlichen lassen sich beim Data Mining zwei Zielrichtungen unterscheiden: Zum einen wird über Objektstrukturen versucht, Muster und besondere Eigenschaften zu ermitteln und dadurch Vorhersagen über das zukünftige Verhalten der Untersuchungsobjekte (Aktienkurse, Käufer, Wetter etc.) zu treffen. Die eingesetzten Methoden sind Ähnlichkeitssuche, Klassifikationen von Objekten und Clusterbildung. Zum anderen werden auf Basis bekannter Informationen, d.h. Attributwerte, Implikations- und Assoziationsregeln abgeleitet, um das beobachtete Verhalten von Objekten zu beschreiben (z.B. das Kaufverhalten von Kunden). Die eingesetzten Methoden sind Datenableitung, Abhängigkeitsanalyse, Regression und Assoziationsregeln [Hand 02].

Der gesamte Bereich der Datenanalyse und Datenauswertung wird im Rahmen des Wissensmanagement bzw. Knowledge Management erheblichen Einfluss auf Unternehmen haben. Deshalb werden die oben beschriebenen Technologien intensiv auf ihre zukünftige Entwicklung hin untersucht. Es wird diskutiert, welche Bedeutung verschiedene Datenanalyseverfahren sowie Datenauswertungsmethoden haben und welche neuen Anwendungsbereiche und Trends sich dabei ergeben werden. Auch auf Technologien zur Speicherung ausgewerteter Daten und diesbezügliche Architekturen wird eingegangen. Schließlich werden noch Bedeutung und Entwicklung umfassender Informationssysteme untersucht, deren Infrastruktur auf Datenanalyse und -auswertung basiert.

FORTGESCHRITTENE ANALYSEALGORITHMEN: Datenbanksysteme, die fortgeschrittene Analysealgorithmen für große Datenmengen integrieren, werden in drei Jahren verfügbar sein.

VERFAHREN ZUR DATENVERARBEITUNG: OLTP bleibt das wichtigste Verfahren in Datenbanken, langfristig wird v.a. MOLAP an Bedeutung gewinnen.

## Ergebnisse

Dem Bereich der Datenanalyse und Datenauswertung wird von den Befragten eine sehr große Bedeutung beigemessen. Eine wichtige Entwicklung stellen dabei fortgeschrittene Analysealgorithmen für große Datenmengen dar. Diese Aussage bestätigt den allgemeinen Trend zu einer verstärkten Integration von Funktionalität in Datenbanksysteme (vgl. Abschnitt 8.3.2), denn die Experten prognostizieren, dass solche Algorithmen als Basisoperationen in drei Jahren in Datenbanksystemen integriert sein werden (vgl. Abbildung 8.74). Somit haben sich bei dieser These eher die Erwartungen der Industrievertreter aus der Studie 2000 bestätigt, die damals etwas pessimistischer als ihre Kollegen aus der Wissenschaft waren [SETIK 00]. Als Anwendungsmöglichkeiten wurden v.a. Data Warehouses und Data Mining genannt.

Bezüglich neuer Anwendungsgebiete im Bereich Knowledge Discovery bzw. Data Mining im Allgemeinen ergaben sich interessante Aussagen. Die Experten sehen hierbei kurzfristig hauptsächlich Nutzen in der Auswertung von Kundendaten, wie es beim CRM bereits heute verfolgt wird, um z.B. Kaufverhalten und Konsumtrends zu ermitteln. In zwei bis fünf Jahren werde dann eine eher wissenschaftliche Nutzung eintreten, z.B. zur Mustererkennung in der Genforschung. Langfristig schließlich sei eine Weiterentwicklung der Technologien abzusehen, so dass komplexe Systeme und Datenbestände ausgewertet und optimiert werden könnten. Als Beispiele wurden Wettervorhersagen und Klimaforschung, Verkehrsleitsysteme, aber auch Gentechnologie genannt.

Im Kontext der Verfahren zur Datenverarbeitung wird OLTP weiterhin die größte Bedeutung behalten (siehe Abbildung 8.75). Die Anwendungsgebiete von OLTP und OLAP sind grundsätzlich zu unterscheiden. OLTP wird bereits seit Langem von traditionellen DBS unterstützt und bietet ausreichend Möglichkeiten zur Verwaltung aktueller Datenbestände des operativen Tagesgeschäftes, z.B. bei Buchhaltung, Personalwesen, Bestellsystemen etc. OLAP hingegen ist zur Analyse großer Datenmengen geeignet und findet deshalb in eher strategischen Bereichen wie der Unternehmensentwicklung Anwendung. Bei den Online Analytical Processing Verfahren wird vor allem MOLAP eine stark wachsende Bedeutung beigemessen. Diesen Trend erklären einige Befragte mit einer allgemeinen Entwicklung

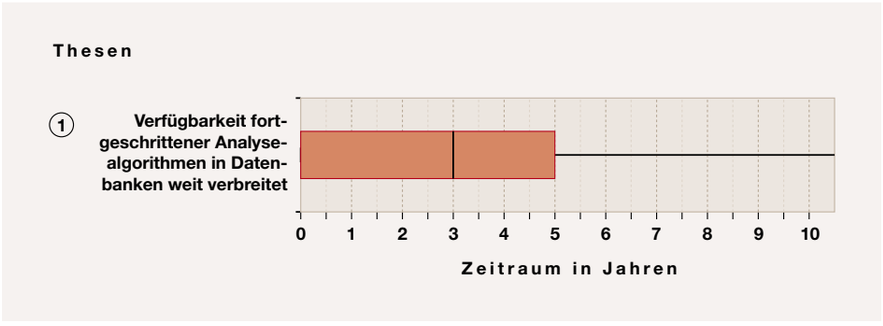



Abbildung 8.74: Ergebnis der These zu Verfügbarkeit fortgeschrittener Analysealgorithmen als Basisoperationen

ÄHNLICHKEITSSUCHE: Im Data Mining wird die Ähnlichkeitssuche die bedeutendste Auswertungsmethode werden.

hin zu multidimensionalen Datenbankarchitekturen (vgl. Abschnitt 8.3.1). ROLAP und HOLAP verlieren dementsprechend an Bedeutung bzw. würden in multidimensionale Konzepte integriert.

Um die Zielsetzung der Wissensgenerierung zu verfolgen, gibt es mehrere Methoden. Bei der Frage, welche Datenauswertungsmethoden sich beim Data Mining durchsetzen werden, lässt sich offenbar noch kein eindeutiger Trend abschätzen (vgl. Abbildung 8.76). Dabei werden von den Experten v.a. der Ähnlichkeitssuche und der Klassifikation von Objekten große Bedeutung beigemessen. Anwendungsgebiete werden hauptsächlich im CRM und in gezieltem Marketing erwartet, z.B. zur Analyse des Kaufverhaltens von Konsumenten. Aber auch in der Forschung, z.B. in der Biotechnologie, sei der Einsatz solcher Methoden sinnvoll. Andere Verfahren wie Clusterbildung, Datenableitung (Deviation Detection) und das Finden von Assoziationsregeln sind nach Einschätzung der Befragten für den breiten Einsatz weniger wichtig, finden aber in Spezialgebieten sehr wohl Verwendungsmöglichkeiten.

Auch bei den Trends zur Entwicklung umfassender Informationssysteme lagen die Prognosen der Befragten für die einzelnen Systeme, ähnlich wie in der Vorgängerstudie, sehr nah zusammen (vgl. Abbildung 8.77). Knowledge Management Systemen sowie DSS wurden insgesamt die höchsten Stellenwerte eingeräumt. Für die bereits verbreiteten Data Warehouses bzw. OLAP-Systeme hingegen wird langfristig eine abnehmende Bedeutung erwartet. Grund dafür ist laut Expertenaussagen die Ablösung einfacher Data Warehouses durch komplexere betriebswirtschaftliche Informationssysteme, die unter dem Begriff Business Intelligence zusammengefasst werden. Dabei würden bisher oft unscharf definierte bzw. voneinander abgegrenzte Systeme wie Executive Information Systems und Management Information Systems miteinander verschmelzen. Insgesamt schätzen die Experten die Entwicklungen im Bereich der Informationssysteme als sehr wichtig ein, weil dadurch Unternehmensplanung und -steuerung optimiert werden könnten.

## Zusammenfassung

Der Datenanalyse und der Datenauswertung werden sehr wichtige Rollen im Bereich der DBS beigemessen. Anwendungsgebiete sind insbesondere die Nutzung vorhandener Informationen (z.B. Kundendaten) und betriebswirtschaftliche Prognosen oder Entscheidungsunterstützung. Zusammenfassend lassen sich folgende Prognosen festhalten:

- Fortgeschrittene Analysealgorithmen für große Datenmengen werden bis 2006 als Basisoperationen in Datenbanksystemen verfügbar sein.

- OLTP bleibt das wichtigste Verfahren zur Datenverarbeitung und -analyse. Bis 2013 wird ROLAP an Bedeutung verlieren, während v.a. MOLAP an Bedeutung gewinnen wird.

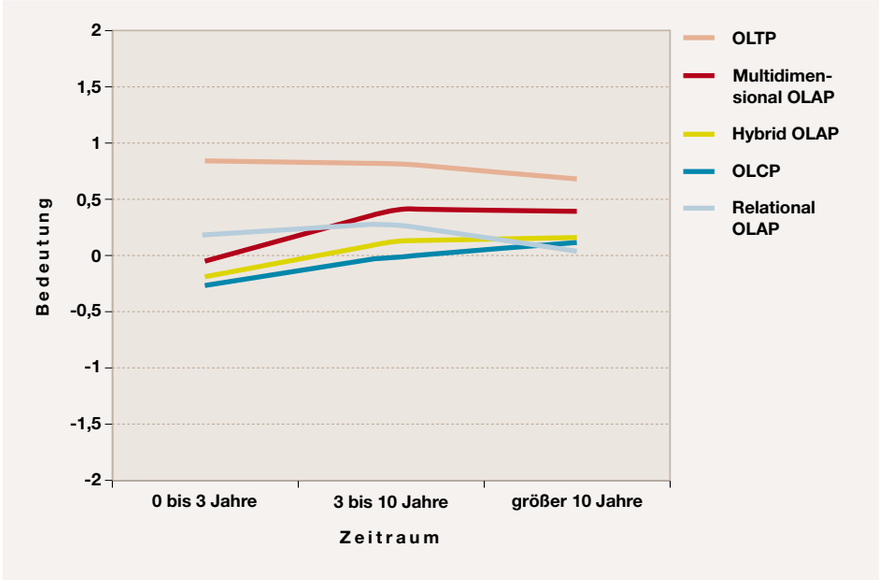



Abbildung 8.75: Bedeutung unterschiedlicher Datenanalyseverfahren

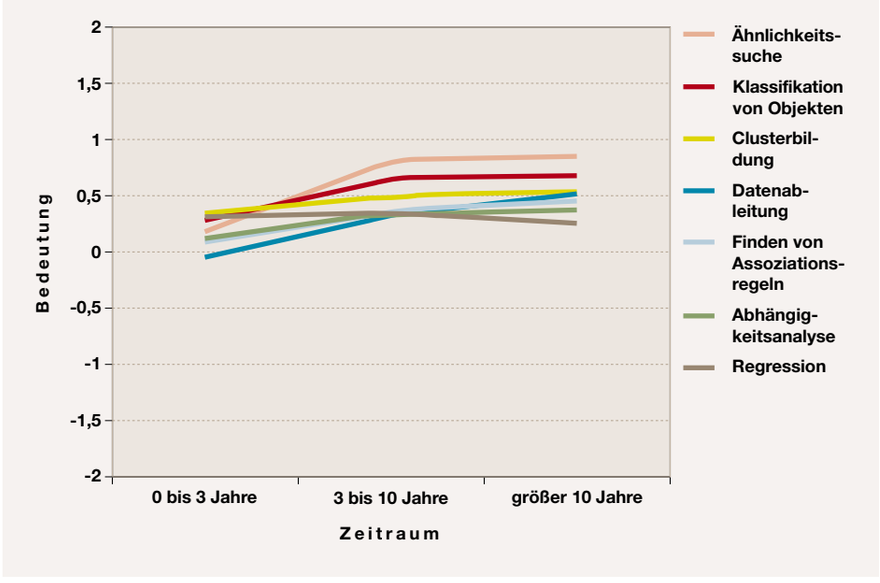



Abbildung 8.76: Bedeutung unterschiedlicher Datenauswertungsmethoden im Data Mining

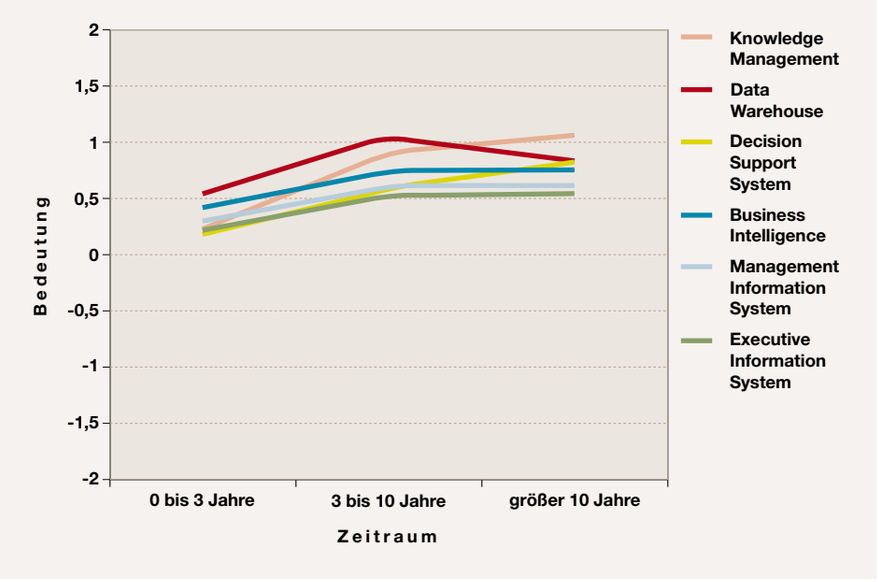



Abbildung 8.77: Bedeutung unterschiedlicher Informationssysteme

- Als Datenauswertungsmethoden werden v.a. die Ähnlichkeitssuche und die Klassifikation von Ojekten an Bedeutung gewinnen. Anwendungsgebiete sind CRM und Marketing.

- Knowledge Management und Decision Support Systeme werden im Bereich der Informationssysteme wichtiger werden, während Data Warehouses langfristig von abnehmender Bedeutung sind.

### 8.3.5 Performancesteigerung und Technologiefortschritt

Mit zunehmender Verwendung von Datenbanksystemen sowie Internet-basierten und multimedialen Anwendungen wächst auch das zu verarbeitende und zu verwaltende Datenvolumen, was nach Technologien verlangt, die die erforderliche Performancesteigerung bei Datenbanksystemen erbringen können. Dabei spielt die Hardwareentwicklung in Form neuer Speichertechnologien eine wesentliche Rolle (siehe hierzu auch Abschnitt 8.1). Nach [Rahm 99a] können Datenbanksysteme die zukünftige „Datenflut“ aber nur bewältigen, wenn Bearbeitungszeiten für Transaktionen erheblich verkürzt werden, also die Performance der Datenbanksysteme deutlich gesteigert wird. Neben der Integration von Tertiärspeichern und neuen Indexstrukturen spielen daher effizientere Abfragetechniken für Transaktionen innerhalb von Datenbanksystemen eine wichtige Rolle [Baum 99, Rahm 99a]. Ebenso begünstigen Performancesteigerungen im Netzwerkbereich (vgl. Abschnitt 8.2.2) eine steigende Marktdurchdringung von parallelen Datenbanksystemen [CoBe 02].

Ein weiterer wichtiger Aspekt bei der Betrachtung von Datenbanksystemen ist die Frage, wie sich die unterschiedlichen Datenmodelle, die parallel und teilweise miteinander verzahnt entwickelt wurden, verändern werden und welche Bedeutung diese Konzepte in den kommenden Jahren für Datenbanksysteme haben werden. In diesem Zusammenhang wird auch auf die unterschiedlichen Datenbank-Architekturen eingegangen. Zur Einschätzung der Zukunft des Marktes interessiert zudem die Frage, welche Hersteller sich im Bereich der Datenbanksysteme künftig durchsetzen werden und ob eventuell Open Source Anwendungen, deren Quellcode frei verfügbar ist [Amor 01], eine Rolle in diesem Markt spielen werden.

Im sogenannten Semantic Web soll es Computern bzw. Systemen in Zukunft ermöglicht werden, miteinander zu kommunizieren, Informationen über das Internet zu finden und dadurch komplexere Aufgaben selbständig lösen zu können [Stum 02]. Dies bedeutet, dass Informationen jeglicher Art semantisch, also auf Basis der Wortbedeutung, vorliegen und abrufbar sein müssen. Dabei spielen Metadaten und Ontologien eine wichtige Rolle, um Informationen objektorientiert zu spezifizieren und die Objekte und deren Beziehungen zueinander formal zu beschreiben [BLHL 01]. Gerade im Bereich von Datenbanksystemen kann die Nutzung des semantischen Datenmodells zu einer einfacheren Interoperabilität zwischen Datenbanken und zu mehr Interaktion mit anderen Anwendungen führen, wenn sich die verschiedenen Systeme „verstehen" können [CoBe 02]. Deshalb wurde diesem Thema, das ursprünglich im Rahmen der Forschung zu künstlicher Intelligenz entwickelt wurde, ein größerer Fragenkomplex in der vorliegenden Studie gewidmet. Es werden Anwendungsmöglichkeiten sowie notwendige Technologien für Ontologien und Semantik analysiert.

SPEICHERTECHNOLOGIEN:
Die Entwicklungen im Bereich der Speichertechnologien fördern die Entstehung neuer Datenbanktechniken. Nur so können jährliche Zuwachsraten des Datenvolumens von etwa 100% bewältigt werden, nicht zuletzt durch die Integration von Tertiärspeichern in Datenbanksysteme in 4 bis 5 Jahren.

TERTIÄRSPEICHER:
Tertiärspeicher werden in 5 Jahren verbreitet in Datenbanksysteme integriert sein.

## Ergebnisse

Gerade im Zuge einer fortschreitenden Digitalisierung und Archivierung vieler Daten, durch die Integration vor allem multimedialer Anwendungen (vgl. Abschnitt 8.3.2) und in Verbindung mit der Entwicklung neuer Speichertechnologien wird in Zukunft ein weiterer Zuwachs des zu verarbeitenden und zu verwaltenden Datenvolumens erwartet (vgl. Abbildung 8.78). Dieser Aspekt führt zu sehr unterschiedlichen Einschätzungen. Die größte Gruppe der Experten erwartet innerhalb der nächsten zehn Jahre relativ konstante jährliche Zuwachsraten von 80-120% beim Datenvolumen. Etwa ein Drittel der Befragten geht davon aus, dass, nach der sich momentan vollziehenden Digitalisierung vieler Daten, das jährliche Wachstum auf 10-50% zurückgeht. Während die Experten aus dem akademischen Bereich den Rückgang des Wachstums bereits in zwei Jahren erwarten, rechnen die Befragten aus der Industrie mit der Verlangsamung erst nach zwei bis fünf Jahren. Allerdings gehen einige der Experten von sogar langfristig exponentiell steigenden Zuwachsraten aus.

Neue Speichertechnologien könnten in erheblichem Maße dazu beitragen, dem stetig wachsenden Datenvolumen sowie immer komplexeren Anforderungen Stand zu halten [Rahm 99b]. Die Leistungssteigerung in diesem Zusammenhang ist dabei eng an die Hardwareentwicklung gekoppelt (siehe hierzu Abschnitt 8.1). Die Experten prognostizieren, dass in einem Zeitraum von etwa fünf Jahren neue Speichertechnologien auch neue Datenbanktechniken ermöglichen werden (vgl. Abbildung 8.79, ①). Damit würde der Zeitrahmen für diese These im Vergleich zu den Aussagen der Vorgängerstudie um zwei Jahre nach hinten verschoben [SETIK 00], wobei Forschungsvertreter sich optimistischer geben und die These durchaus bereits in drei Jahren erfüllt sehen. Für den Zeitraum der nächsten fünf Jahre erwarten die Befragten, dass bzgl. der Nutzung für Datenbanksysteme vor allem optische und magneto-optische Speichermedien relevant sind. In fernerer Zukunft, also in mehr als zehn Jahren, könnten dann holographische und biologische Speicher von Bedeutung werden.

Um sehr große Datenmengen (d.h. im Terabyte-Bereich) zu archivieren, werden Tertiärspeicher wie Magnetbänder oder magneto-optische Speichermedien eingesetzt (siehe hierzu ebenfalls Abschnitt 8.1). Im Zusammenhang mit Datenbanken ergeben sich mit der Nutzung externer Tertiärspeicher neue Möglichkeiten, große Datenmengen zu verwalten, ohne die Performance von Datenbanksystemen zu stark zu reduzieren [ElNa 00]. Von den Befragten wird betont, dass der Zugriff auf tertiäre Speichermedien allerdings noch wesentlich schneller werden muss, bevor diese Technologie effektiv in Datenbanksysteme integriert und weit verbreitet eingesetzt werden könne. Dies wird in ca. fünf Jahren erwartet (vgl. Abbildung 8.79, ②).

Auch die Nutzung paralleler Datenbanksysteme, die in einem Netzwerk über mehrere Computer verteilt arbeiten, verspricht deutliche Leistungssteigerungen. Entgegen den Erwartungen der Vorgängerstudie werden diese Systeme allerdings noch nicht 2004, sondern erst in ca. vier Jahren weit verbreitet eingesetzt sein (vgl. Abbildung 8.79, ③). Die Experten sehen hier gu-


Abbildung 8.78: Jährliches Wachstum des zu verarbeitenden Datenvolumens

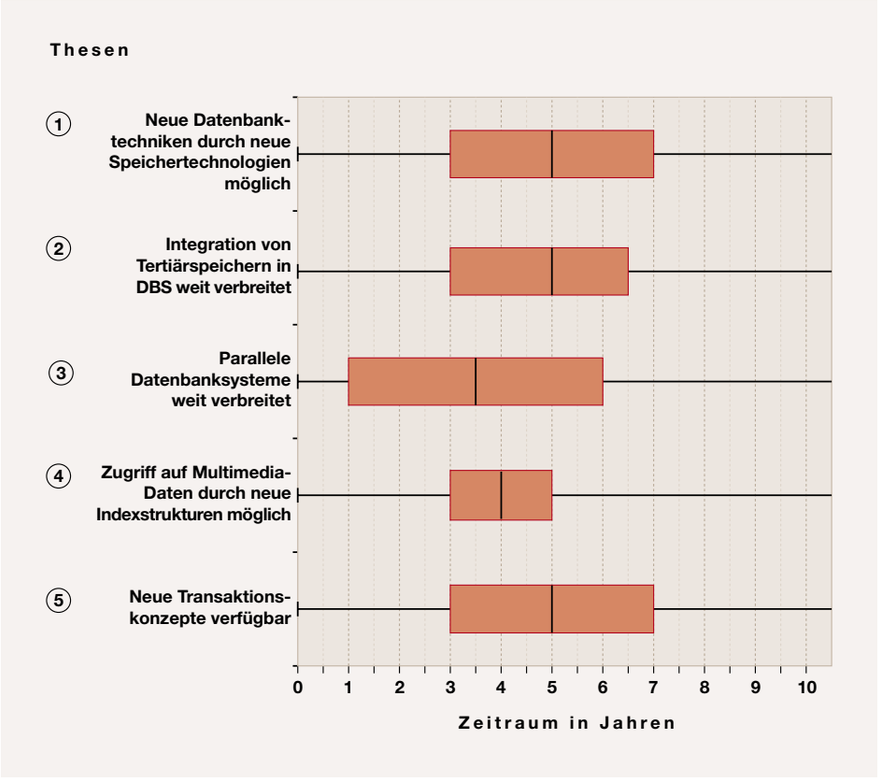



Abbildung 8.79: Ergebnis der Thesen zu Performancesteigerung

te Einsatzmöglichkeiten vor allem für Anwendungen mit hohen Transaktionszeiten (z.B. OLAP ), bei interaktiven Datenbank-Anwendungen wie CAD oder CASE sowie im Multimediabereich, wo restriktive Antwortzeiten eingehalten werden müssen, z.B. bei Videoanwendungen. Einige Experten merken an, dass insbesondere die Parallelisierung zu einer deutlichen Verbesserung der Skalierbarkeit von Datenbanksystemen beitragen wird. Die beschriebene Entwicklung wird sich nach Meinung einiger Befragten allerdings nur dann durchsetzen können, wenn leistungsfähige Hochgeschwindigkeitsnetze für diese Systeme verfügbar sind (siehe hierzu Abschnitt 8.2).

PARALLELISIERUNG: parallele Datenbanksysteme werden in 4 Jahren weit verbreitet eingesetzt.

TRANSAKTIONSKONZEPTE: Neue Transaktionskonzepte und Indexstrukturen werden in 4 bis 5 Jahren zur effizienteren Verarbeitung des wachsenden Datenvolumens beitragen.

DATENMODELLE: Relationale Datenbanksysteme bleiben zwar sehr wichtig, werden allerdings immer mehr durch objektrelationale sowie XML-basierte Systeme abgelöst werden.

Für einen schnelleren Zugriff auf Multimediadaten (z.B. Video- und Audioinformationen) sowie auf nicht sortierte Daten, die zunehmend auf Sekundär- und Tertiärspeicher (z.B. DVDs) ausgelagert werden, ist die Integration spezifischer Datenstrukturen, sogenannter Indexstrukturen, notwendig. Sie ermöglichen weiterhin effiziente Datenbankoperationen wie Such- oder Sortieroperationen. Auch bei dieser These weichen die Prognosen der letzten Studie von den aktuellen Ergebnissen ab: Die Umsetzung dieser Datenstrukturen zur Optimierung von Abfragetechniken verzögert sich um einige Jahre. So erwarten die Befragten einen umfassenden Einsatz neuer Indexstrukturen, die einen Zugriff auf Multimedia-Informationen ermöglichen, mittlerweile erst nach weiteren vier Jahren Entwicklungsarbeit (vgl. Abbildung 8.79, ④).

Die zunehmende Verwendung von Datenbanken im Multimediabereich sowie für Anwendungen im Internet erfordert auch die Entwicklung neuer Transaktionskonzepte. So sind z.B. für Datenbankanwendungen mit integrierten interaktiven Funktionen wie CAD oder von Multimediadaten wesentlich längere Transaktionszeiten und komplexere Transaktionsmechanismen notwendig als bei klassischen Datenbankanwendungen im Bankenbereich oder im E-Commerce. Bei diesen Anwendungen dauern Zugriff und Bearbeitung von Daten lediglich wenige Sekunden. Geeignete Transaktionskonzepte zur Erfüllung neuer Anforderungen wie z.B. Möglichkeiten, Änderungen an Daten zurücksetzen zu können, sind jedoch erst in fünf Jahren verfügbar (vgl. Abbildung 8.79, ⑤). Hier ergibt sich eine deutliche Abweichung zu den Ergebnissen der Vorgängerstudie, in der das Eintreten dieser These bereits 2004 erwartet wurde. Dies wird, wie auch bei den letzten Thesen, mit der damals herrschenden und inzwischen nur noch gedämpft vorhandenen Multimedia- und Internet-Euphorie erklärt, aber auch mit neuen technischen Schwierigkeiten (z.B. bei der Strukturierung von Multimediadaten).

In der vorliegenden Studie wurden erneut die wichtigsten Datenmodelle bzw. Datenbanktechniken bezüglich ihrer technischen Weiterentwicklung zur Diskussion gestellt. Dabei wird in den nächsten zwei bis drei Jahren das relationale Datenmodell nach wie vor als am häufigsten verwendet angesehen, seine Bedeutung nimmt in Zukunft jedoch stetig ab. Bei dieser Frage ergaben sich wieder sehr interessante Veränderungen der Trends im Vergleich zur Vorgängerstudie. Die Experten erwarten in den nächsten zehn Jahren eine wachsende Bedeutung vor allem von objektrelationalen , aber auch von Web- bzw. XML-basierten und bei multidimensionalen Datenbanksystemen. Dieser Trend war bereits 2000 abzusehen, die Verhältnisse dieser drei Modelle zueinander haben sich jedoch zugunsten einer immer stärker werdenden Bedeutung objektrelationaler Datenbanken verschoben. Objektorientierten Systemen wird weit weniger Bedeutung zugemessen als noch vor drei Jahren. Die objektorientierten Systeme werden aufgrund der objektrelationalen Datenbanksysteme überflüssig bzw. vollständig in diese integriert werden. Die Zusammenhänge zeigt Abbildung 8.80.

Die Experten nennen folgende langfristigen Anwendungsbereiche für einige Systeme: Multidimensionale Datenbanksysteme sind insbesondere für ausgiebige Datenanalysen geeignet (vgl. Abschnitt 8.3.4), objektrelationale Datenbanken setzen sich langfristig als Standard für sämtliche Datenbankanwendungen durch und relationale Systeme behalten weiterhin ihre Bedeutung als „flache“ Anwendung für alle Bereiche, nicht aber im Multimedia-Umfeld. Eine ausführliche Betrachtung verschiedener Datenbankmodelle ist am Anfang dieses Kapitels zu finden (vgl. Abschnitt 8.3.1).

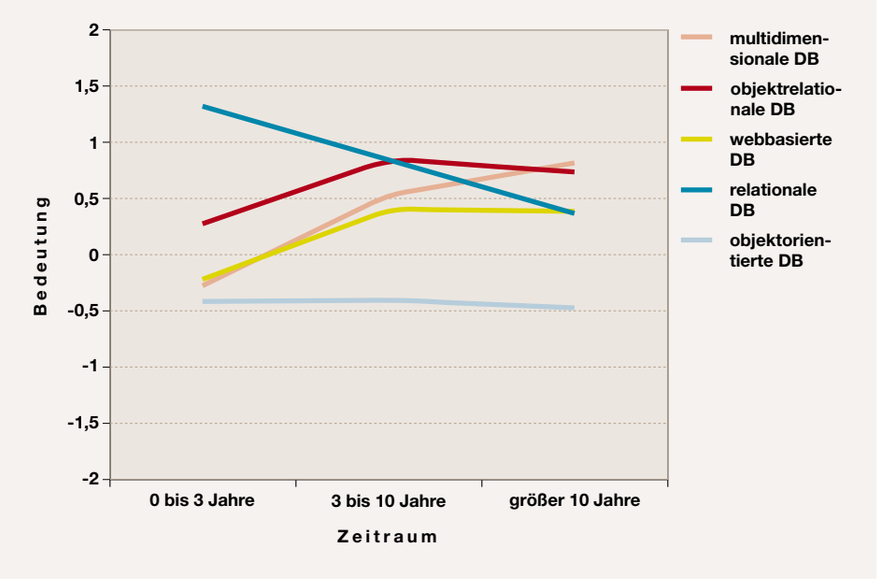



Abbildung 8.80: Bedeutung unterschiedlicher Datenbanktechniken bzw. Datenmodelle

REALISIERUNGSKONZEPT: Client-Server Datenbanken behalten auch langfristig eine deutlich höhere Bedeutung als Desktop-Datenbanken.

DATENBANKSYSTEME: Die gängigen Datenbanksysteme Oracle, IBM DB2 sowie Microsoft SQL Server werden nach wie vor den Markt dominieren, aber Open Source Datenbanken werden künftig an Bedeutung gewinnen.

Das Internet beruht heute vorwiegend auf der Client-Server Architektur, die durch kooperative Transaktionen zwischen mehreren Anwendungen bzw. Systemen gekennzeichnet ist [Sche 02a]. Im Zuge der zunehmenden Nutzung von Datenbanken über das Internet spiegelt sich diese Architektur auch bei Datenbanksystemen selbst wider. Dieser Trend wird von den befragten Experten bestätigt: Als Realisierungskonzept von Datenbanken nimmt die Bedeutung von Desktop-Datenbanken innerhalb der nächsten Jahre ab (vgl. Abbildung 8.81). Der Client-Server Architektur bei Datenbanken wird von den Befragten eine deutlich höhere Bedeutung zugemessen, jedoch bleibt die Bedeutung über die nächsten Jahre hinweg nahezu konstant, da dieses Konzept bereits heute als Standardarchitektur anzusehen sei. Einige Experten merken zusätzlich an, dass in Zukunft Desktop-Datenbanken im Rahmen zunehmender Vernetzung keine eigenständige Rolle mehr spielen, sondern in Client-Server Datenbanken integriert würden, z.B. als lokale Cache-Datenbanken bzw. Replikate.

Beim Vergleich der wichtigsten Datenbanksysteme bzw. konkreten Produkte hat sich die beherrschende Marktstellung der drei größten Hersteller Oracle, IBM und Microsoft gefestigt. Einige der befragten Experten erwarten sogar, dass sich auch langfristig bei der Weiterentwicklung der Datenbanksysteme keine „Newcomer" durchsetzen können. Somit bleiben Oracle, IBM DB2 sowie Microsoft SQL Server die bedeutendsten Datenbanken, wobei Oracle von allen Experten genannt wird. Diese Entwicklung wurde bereits in der Vorgängerstudie vorausgesagt.

Open Source Anwendungen sind dadurch gekennzeichnet, dass der Quellcode des Systems veröffentlicht ist, Beiträge zur Weiterentwicklung somit jeder Entwickler beisteuern kann und sie sehr kostengünstig oder sogar frei verfügbar sind. Im Bereich der Datenbanken nehmen sie in den kommenden drei Jahren an Bedeutung zu, werden dann aber ihr Wachstumspotenzial bereits erschöpft haben, vor allem weil bekannte Open Source Datenbanksysteme (z.B. MySQL oder PostgreSQL) im Business-Bereich lediglich für kleinere Anwendungen geeignet erscheinen (vgl. Abbildung 8.82). Allerdings gibt es seit kurzem auch hier interessante Weiterentwicklungen: SAP DB wurde 2001 in ein Open Source Projekt umgewandelt [SAP 02], fand bisher aber noch wenig Beachtung, obwohl diese frei verfügbare Datenbank wesentlich leistungsstärker als andere Open Source Datenbanken ist und plattformunabhängig große Funktionalität bereitstellt [Bank 02]. Es ist aber noch vollkommen unklar, ob und in welchem Maß die-

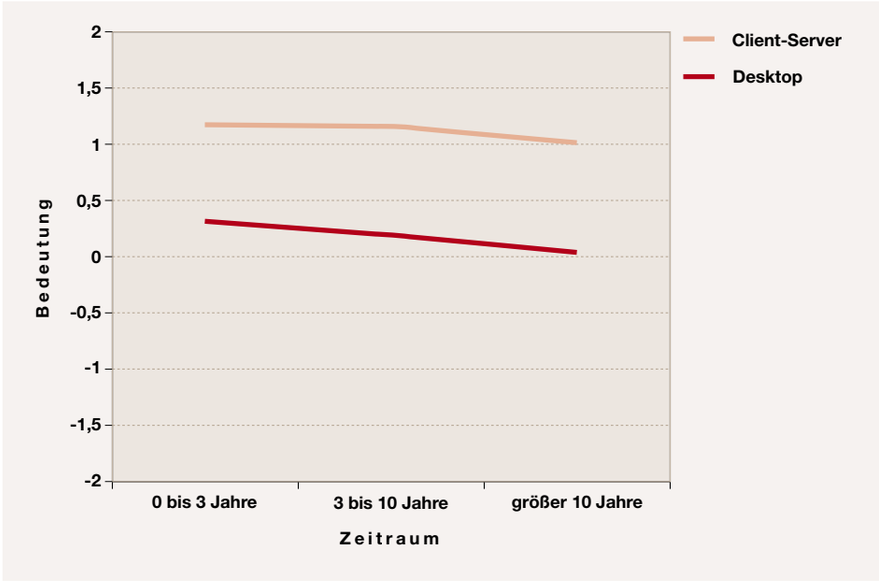



Abbildung 8.81: Bedeutung unterschiedlicher Realisierungskonzepte von Datenbanken

DATEN MIT UNSCHÄRFE: Die Integration solcher Daten wird in ca. 6 Jahren weit verbreitet sein.

ONTOLOGIEN: Ontologien werden in 6 Jahren für intelligente Suchagenten im Internet und in 5 Jahren zur Interoperabilität von Datenbanksystemen eingesetzt. Semantische Datenbankabfragen werden in 7 bis 8 Jahren verbreitet sein.

se kostengünstige Alternative eine ernsthafte Konkurrenz zu den oben genannten kommerziellen Datenbank-Herstellern werden kann. Generell sehen Experten aus Wissenschaft und Forschung langfristig deutlich größere Chancen für den Einsatz von Open Source Datenbanken als Vertreter der Wirtschaft.

Die Integration von Daten mit Unschärfe (Fuzzy-Logic) in Datenbanksysteme lässt nach Expertenmeinungen noch mindestens sechs Jahre auf sich warten (vgl. Abbildung 8.83, ①). Fuzzy Logic beinhaltet Daten, die unklar formuliert sind und ständigen Veränderungen ausgesetzt sind [Voss 00]. Anwendungsmöglichkeiten seien vor allem Business Intelligence und Entscheidungssysteme.

Die Thesen zu Ontologien wurden von den Experten wie folgt bewertet: Zur Interoperabilität von Datenbanksystemen bzw. zur Abfrage von Metainformationen, also von „Daten über Daten" [Stum 02], werden in fünf Jahren Ontologien weit verbreitet eingesetzt, zur Realisierung intelligenter Suchagenten im Internet dagegen erst in sechs Jahren (vgl. Abbildung 8.83, ③). Vertreter aus Wissenschaft und Forschung erwarten die Realisierung „intelligenter" Suchagenten, die eigenständig mit Systemen und Anwendungen interagieren können, allerdings erst in etwa sieben bis acht Jahren. Aktuelle Forschungserkenntnisse würden nämlich noch technologische Mängel bei Ontologien aufzeigen. So wird von den Befragten mehrfach erwähnt, dass einheitliche Standards und Klassifikationen für Ontologien eingeführt werden müssten. Bei der Abfrage von Metainformationen seien Ontologien vor allem im Wissensmanagement nützlich und könnten somit einen Beitrag zur Interoperabilität und Integration verschiedener Datenbanksysteme leisten. Als Einsatzmöglichkeiten werden für Suchagenten hauptsächlich Suchmaschinen sowie E-Business genannt, z.B. für effiziente Recherchen oder zur Einkaufsoptimierung.

RDF (Resource Description Framework) und XML sind Basistechnologien zur Realisierung von Ontologien, also Spezifikationen von Informationen bzw. Objekten und Klassen und deren Beziehungen zueinander [BLHL 01]. Die Experten erwarten, dass XML als Standardrahmen über die nächsten zehn Jahre hinweg die größte Bedeutung zukommen wird (vgl. Abbildung 8.84), wobei RDF auf XML basiert und sich die beiden Konzepte durchaus ergänzen.

Um Ontologien formal beschreiben und erstellen zu können, müssen auch Relationen von Objekten und Klassen dekla-

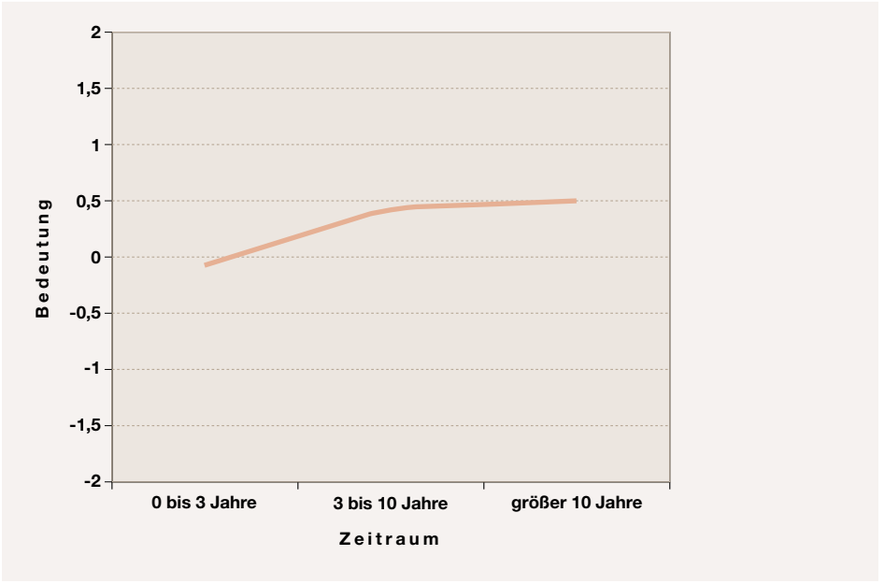



Abbildung 8.82: Bedeutung von Open-Source Anwendungen bei Datenbanken

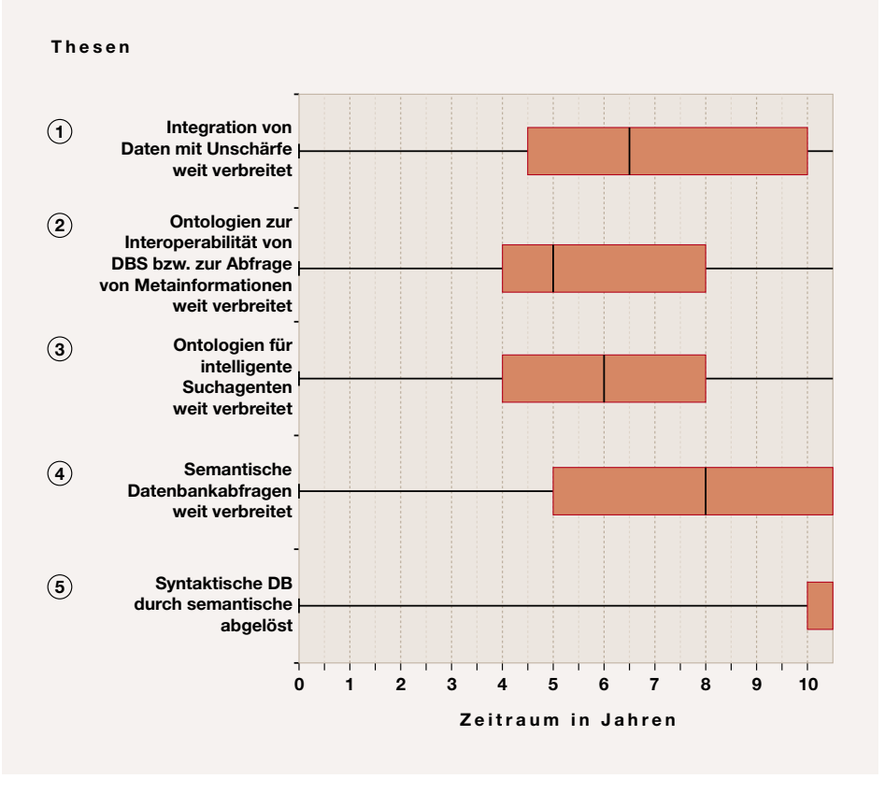



Abbildung 8.83: Ergebnisse der Thesen zu Ontologien und Semantik

SEMANTISCHE DATENBANKABFRAGEN: Datenbankabfragen auf Basis der Wortbedeutung werden in 8 Jahren in DBS weit verbreitet eingesetzt werden, aber zeichenbasierte Abfragen innerhalb der nächsten 10 Jahre nicht ablösen können.

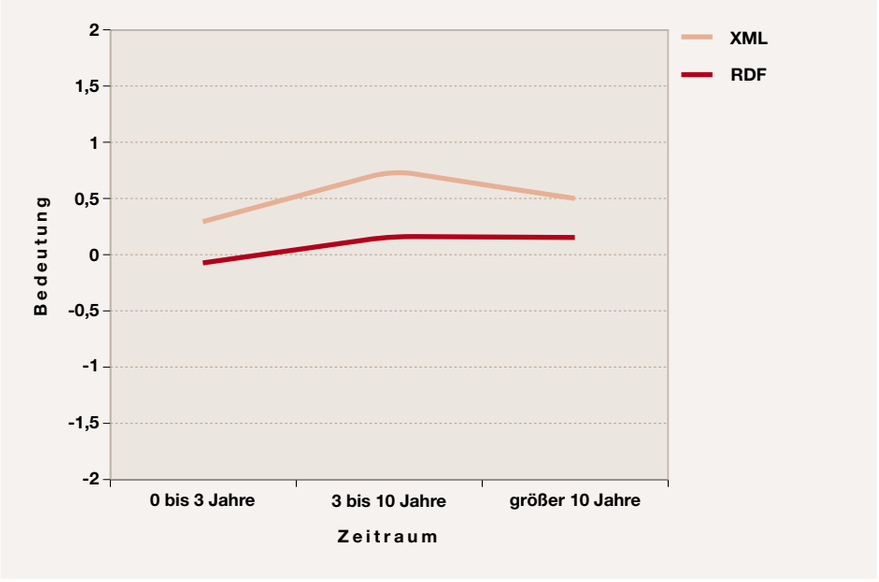



Abbildung 8.84: Bedeutung verschiedener Technologien zur Realisierung von Ontologien

riert sein. Hierzu dienen Sprachkonstrukte als „Dolmetscher", wodurch die Äquivalenz verschiedener Ressourcen gewährleistet wird [Stum 02]. Bei den Ontologiesprachen gibt es unterschiedliche Ansätze: DAML (DARPA Agent Markup Language) und OIL (Ontology Inference Layer) bauen auf dem RDF-Schema auf, OML (Ontology Markup Language) und SHOE (Simple HTML Ontology Extensions) sind Erweiterungen von HTMLund XOL (Ontology Exchange Language) basiert auf XML. Die Experten schreiben dem Bereich der Ontologien allgemein nur eine geringe zukünftige Bedeutung zu, Anwendungsmöglichkeiten werden lediglich in Spezialgebieten erwartet, z.B. bei professionellen und komplexen Suchfunktionen. Unter den Ontologiesprachen werden der Kombination aus DAML und OIL sowie der XML-basierten XOL die größten Chancen eingeräumt, sich durchzusetzen (vgl. Abbildung 8.85). Die nahezu gleich hohe Einschätzung der anderen Konzepte und die Nähe aller Nennungen zueinander zeigt aber deutlich die Unsicherheit bzw. Unentschlossenheit der Experten.

Eine weite Verbreitung von semantischen Datenbankabfragen, also Abfragen auf Basis der Wortbedeutung, ist laut der Expertenmeinungen in acht Jahren zu erwarten (Abbildung 8.83, ④). Eindeutig abgelehnt wurde hingegen die These, semantische Datenbankabfragen könnten syntaktische, also zeichenbasierte Abfragen, zukünftig völlig ersetzen. Dies werde niemals eintreten, da einige Anwendungen und Daten nicht effizient modelliert werden könnten, um auf sie semantisch zugreifen zu können (siehe Abbildung 8.83, ⑤). Die Befragten merkten allerdings an, dass sich in ferner Zukunft jedoch eine Transformation zwischen syntaktischen und semantischen Abfragen durchsetzen könnte, die den Usern die Abfrage erleichtert.

## Zusammenfassung

Um die enormen Anforderungen erfüllen zu können, die durch stetig wachsendes Datenvolumen und immer komplexer werdende Aufgaben entstehen, sind Performancesteigerung im Hardwarebereich und Technologiefortschritt sehr wichtige Aspekte im Datenbankbereich, nicht zuletzt wegen ihrer deutlichen Auswirkungen auf die bestehenden Datenbanktechnologien. Die Auswertung dieses großen Fragenkomplexes hat folgende Trends erkennen lassen:

- Im Mittel wird das zu verarbeitende und verwaltende Datenvolumen in den nächsten Jahren um etwa 100% jährlich ansteigen.

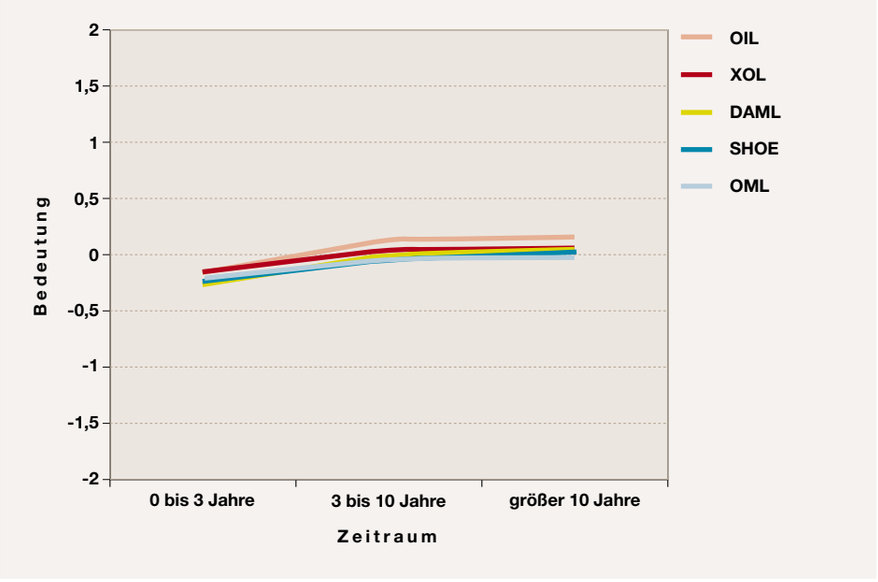



Abbildung 8.85: Bedeutung verschiedener Konzepte zur Beschreibung von Ontologien

- Der technologische Fortschritt im Bereich externer Speichertechnologien wird bis 2007 zu einer weit verbreiteten Integration von Tertiärspeichern in Datenbanksysteme führen.

- Weiterentwicklungen der Speichertechnologien, vor allem bei optischen und magneto-optischen Speichermedien, ermöglichen spätestens 2008 die Entstehung neuer Datenbanktechniken. Dabei spielt die Integration von Tertiärspeichern in Datenbanksysteme ebenso eine Rolle.

- Parallele Datenbanksysteme, neue Indexstrukturen und Transaktionskonzepte, vor allem im Multimediabereich, werden bis 2008 verbreitet sein.

- Relationale Datenbanksysteme werden kurzfristig eine dominierende Stellung behalten, mittelfristig jedoch immer mehr durch objektrelationale sowie Web- bzw. XML-basierte Systeme abgelöst werden.

- Oracle, IBM DB2 sowie Microsoft SQL Server werden die bedeutendsten Datenbanken bleiben, wobei Open Source Datenbanksysteme an Bedeutung gewinnen werden, allen voran SAP DB.

- Ontologien werden bis 2008 zur Realisierung intelligenter Suchagenten im Internet sowie zur Interoperabilität von Datenbanksystemen verbreitet eingesetzt. RDF und XML (Extensible Markup Language) [XML 99] spielen dabei als Standardrahmen und Basis für Ontologiesprachen eine wichtige Rolle. Semantische Datenbankabfragen sind bis 2010 in Datenbanksysteme integriert, werden jedoch syntaktische Abfragen niemals vollkommen ablösen.

### 8.3.6 Sicherheit in Datenbanken

Mit wachsender Verteilung und Vernetzung von Datenbanken, vor allem auch über das Internet, gewinnen Sicherheitsaspekte zunehmend an Bedeutung. Allgemein sind für Transaktionen über das InternetDatenschutz, Vertraulichkeit und Datenintegrität Grundvoraussetzungen. Dies gilt insbesondere auch für die Nutzung von Datenbanksystemen, da hier das offene Konzept des Internets mit der Sicherheit von Daten in Unternehmen oder Behörden in Einklang zu bringen ist [Amor 01].

IDENTIFIKATION UND AUTHENTISIERUNG: Zur Gewährleistung von Sicherheit im Datenbankbereich wird der Aspekt der Identifikation und Authentisierung auch langfristig die größte Bedeutung haben.

Im Bereich der Datenbanken spielen v.a. die Zugriffskontrolle (Autorisierung), die den Zugriff auf Objekte (Dateien oder Betriebsmittel) durch Subjekte (Benutzer oder Prozesse) definiert und operationalisiert sowie die damit verbundene Identifikation und Authentisierung der Benutzer eine wichtige Rolle. Hierbei handelt es sich um Sicherheitsanforderungen der Datenbank, um die Daten vor unberechtigten Zugriffen zu schützen. Die Sicherstellung der Integrität der abgefragten Daten ist hingegen eine Anforderung des Benutzers, um zu garantieren, dass tatsächlich die Daten aus der Datenbank manipulationsfrei übermittelt werden. Dies ist insbesondere bei verteilten Systemen entscheidend, um gleichzeitige Datenzugriffe durch mehrere User oder Prozesse zu steuern und den Verlust von Informationen zu verhindern [ElNa 00].

Neben diesen klassischen Sicherheitsaspekten spielt das Auditing eine wichtige Rolle in modernen Datenbanksystemen. Unter Auditing wird die Protokollierung von Transaktionen verstanden, anhand derer die Richtigkeit und Vollständigkeit der Sicherheitsregeln verifiziert werden kann [KeEi 97]. Allerdings ist diese Methode im Datenbankbereich nicht eindeutig zu bewerten. Während diese Funktionalität einerseits helfen kann, unberechtigte Angriffe abzuwehren, steht sie der Anforderung des Benutzers nach anonymen Inhaltsabfragen entgegen.

## Ergebnisse

Im Gegensatz zur Vorgängerstudie [SETIK 00] wurde dem Aspekt der Sicherheitseigenschaften von Datenbanken von den Befragten eine größere Bedeutung beigemessen. Die Auswertung dieses Fragenkomplexes zeigt, dass bereits heute Identifikation und Authentisierung beim Zugang auf Datenbanksysteme sowie die Zugriffskontrolle als sehr wichtig eingeschätzt werden.

Laut der Expertenmeinungen kommt inzwischen auch der Datenintegrität eine ebenso hohe Bedeutung zu. Das wird mit dem schwierigen Umgang mit Daten in immer komplexeren, verteilten Datenbanksystemen erklärt. Der Zugriffskontrolle (Autorisierung) wird von den Experten in den kommenden zehn Jahren ebenfalls steigende Bedeutung zugemessen. Hierzu wurde auch mehrmals angemerkt, dass dies als eine absolute Grundfunktion von Datenbanksystemen zu betrachten sei.

Im Vergleich zu den anderen genannten Sicherheitsaspekten wurde Auditing etwas weniger Bedeutung zugemessen. Abbildung 8.86 zeigt diese Entwicklungen im Detail. Dennoch sehen die befragten Experten in einem Zeitraum von drei bis zehn Jahren Anwendungsbereiche für Auditing in Datenbanksystemen vor allem als Kontrollinstrument von komplexen Systemen, aber auch z.B. von Administratoren. Dies wird laut Expertenaussagen insbesondere wegen der wachsenden Anzahl (rechts-)verbindlicher Transaktionen künftig bedeutender werden. Momentan sei effizientes Auditing in Datenbanksystemen allerdings noch zu aufwendig und zu kostenintensiv. Dieser skeptischeren Meinung sind vor allem Vertreter aus Wissenschaft und Forschung, während Industrievertreter bereits heute Bedarf für Auditing sehen. Beide Expertengruppen nähern sich jedoch in Ihren Aussagen innerhalb der kommenden zehn Jahre stetig aneinander an.

Es wurde darüber hinaus angemerkt, dass Datenbank-Sicherheit allgemein in Zukunft als Bestandteil von Gesamt-Sicherheitsarchitekturen (mit zentraler Administration) für sämtliche IT-Systeme eingebunden werden könnte, was insbesondere für sensitive Daten in Business-Anwendungen unerlässlich sein wird. Besonders hervorgehoben wurde die zunehmende Bedeutung von Anonymität beim Zugriff auf Datenbanken. Dies betrifft insbesondere die Anwendungen, bei denen Daten über Datenzugriffe gesammelt werden, z.B. bei E-Commerce-Anwendungen über das Internet. Im Gegensatz zur Vorgängerstudie wurde dem Aspekt der Sicherheitseigenschaften von Datenbanken von den Befragten grundsätzlich eine größere Bedeutung beigemessen. Die Auswertung dieses Fragenkomplexes zeigt, dass bereits heute Identifikation und Authentisierung beim Zugang zu Datenbanksystemen sowie die Zugriffskontrolle als sehr wichtig eingeschätzt werden.

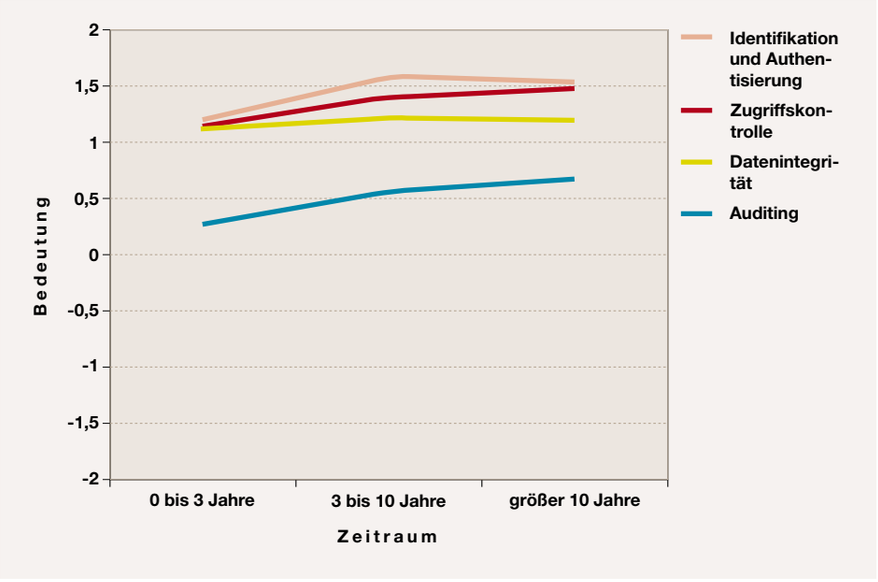



Abbildung 8.86: Bedeutung verschiedener Sicherheitsaspekte in Datenbanksystemen

## Zusammenfassung

Sicherheitsaspekte werden im Datenbankbereich, v.a. aufgrund des immer umfassenderen Einsatzes von Datenbanken im Internet, zukünftig eine größere Rolle spielen. Detaillierte Analysen verschiedener Sicherheitstechnologien finden sich im Kapitel 7 und insbesondere in Abschnitt 8.2.1. Die wichtigsten Ergebnisse der Fragen im direkten Zusammenhang mit Datenbanken sind:

- Identifikation und Authentisierung wird der wichtigste Sicherheitsmechanismus bleiben.
- Auditing hat heute eine geringe Bedeutung, wird aber langfristig immer wichtiger werden.

## 8.4 Softwaretechnik

Die Softwaretechnik ist eine Schlüsseldisziplin im Bereich der Informations- und Kommunikationstechnik. Unter Softwaretechnik wird die ingenieursmäßige Entwicklung von Softwaresystemen verstanden. Der rasante Fortschritt in den Bereichen Architektur, Modellierung, Vorgehensmodelle, Werkzeuge, Beschreibungstechniken sowie Kommunikationstechnologien, Infrastrukturen oder Middleware zeigt, wie umfangreich und dynamisch die Entwicklungen in diesem Themenkomplex sind [Somm 92].

Im Rahmen dieser Arbeit wird in strukturierter Form eine Einschätzung von Trends und Entwicklungen im Bereich Softwaretechnik vorgenommen. Die Strukturierung des Themenfeldes leitet sich dabei auf der Basis der zu Beginn dieser Studie beschriebenen übergreifenden Trends (vgl. Abschnitt 6) ab.

So wird zu Beginn der Trend zur Komponentenorientierung und Dienstnutzung diskutiert. Dieser Trend ist insbesondere vor dem Hintergrund zunehmender Komplexität der Software zu betrachten. Die Verwendung oder die Nutzung von Komponenten und Diensten ermöglicht eine Erhöhung der Wiederverwendung, was maßgeblich zur Beherrschung der Komplexität von Software-Systemen erforderlich ist. Es werden in diesem Zusammenhang auch zahlreiche Komponenten-Technologien und -Architekturen evaluiert.

Daneben wird auf die Systematisierung des Entwicklungsprozesses eingegangen. Dieser Teil befasst sich insbesondere mit der Erfassung, Integration und Bewertung von Systemanforderungen sowie der Diskussion der Entwicklungsdokumentation. Die Dokumentation soll in diesem Kontext idealerweise durchgängig, nachvollziehbar und konsistent über alle Phasen der Softwareerstellung hinweg sein.

Daran schließt sich eine Evaluierung von formalen und grafischen Beschreibungstechniken an. Hierbei wird untersucht, wann diese in Werkzeugen integriert sein werden und welche Unterstützung diese im Verlauf der Entwicklung anbieten.

Ferner wird die Bedeutung von Qualitätssicherung weiter abgeschätzt. Im Mittelpunkt der Diskussion stehen hierbei die Methoden des Tests und der Verifikation.

In diesem Kapitel wird ausführlich auf die Automatisierung des Entwicklungsprozesses eingegangen. Dies schließt sowohl die Betrachtung flexibler Entwicklungswerkzeuge, als auch die Integration dieser Werkzeuge in den Entwicklungsprozess ein. Zusätzlich werden Potenziale bei der Automatisierung untersucht, sowie die Tragfähigkeit bestehender CASE-Tool-Technologien (Computer Aided Software Engineering) bewertet.

Im Anschluss daran wird diskutiert, welche Systemklassen (z.B. Systeme im Bereich Automotive oder Telekommunikation) sowie welche Anforderungen an diese Systeme wie beispielsweise Mobilität oder Reaktivität künftig eine besondere Rolle spielen werden. Außerdem werden bestehende Entwicklungsparadigmen wie Objektorientierung oder visuelle Programmierung miteinander verglichen und ihr künftiger Bedeutungsverlauf abgeschätzt. Hierzu zählt auch die Abschätzung innovativer Entwicklungsmöglichkeiten wie beispielsweise Open Source.

Den Abschluss dieses Themenkomplexes bilden Trends und Thesen in den Bereichen Standardisierung und Zertifizierung. Diese beinhalten unter anderem eine Abschätzung wichtiger Vorgehensmodelle sowie die Evaluierung der Bedeutung von Zertifizierungsmassnahmen im Bereich Softwaretechnik.

Eine Einordnung der in diesem Bereich beschriebenen Trends und Thesen anhand der übergreifenden Trends aus Abschnitt 6 liefert folgendes Ergebnis:

**Automatisierung und Vereinfachung** (Abschnitt 6.1): Die Automatisierung bietet sich im Bereich Softwaretechnik insbesondere zur Reduktion der Komplexität an. Hierzu ist es erforderlich Werkzeugkonzepte zu entwickeln, die es dem Entwickler ermöglichen, effizient Anforderungen zu definieren und diese mit Unterstützung der Entwicklungsumgebung über unterschiedliche Entwicklungsphasen hinweg bis hin zur Implementierung und zum Test zu verfolgen (vgl. Abschnitt 8.4.5).

Hierzu sind insbesondere Vereinfachungen durch Komponententechnologien (vgl. Abschnitt 8.4.1), ein systematischer Entwicklungsprozess (vgl. Abschnitt 8.4.2)

sowie Standards (vgl. Abschnitt 8.4.7) von großer Bedeutung.

**Dienst- und Komponentenorientierung** (Abschnitt 6.2): Die Dienst- und Komponentenorientierung ist auch im Bereich der Softwaretechnik zu finden. Hiervon betroffen sind insbesondere die Bereiche komponentenorientierte bzw. dienstbasierte Softwareentwicklung (vgl. Abschnitt 8.4.1). Die Nutzung dieser Technologien beeinflussen die Definition von Entwicklungsprozessen (vgl. Abschnitt 8.4.7 und 8.4.2), Integration und Nutzung von Beschreibungstechniken 8.4.3) sowie die Verwendung von Qualitätssicherungsmethoden (vgl. Abschnitt 8.4.4).

Eng verbunden mit der Dienst- und Komponentenorientierung ist die Schichtenbildung und Abstraktion und damit einhergehend die Kapslung von zusammengehörigen Funktionen. In diesem Themenfeld ergeben sich daraus unterschiedliche Ausprägungen. Hierzu gehören Three-Tier-Architekturen, Protokoll-Stacks oder die Nutzung von ASP (Active Server Pages) [Micr 02b] im Themenfeld Dienstentwicklung als Teil des Software Engineerings. Schichtung und Abstraktion wird insbesondere dann möglich, wenn Funktionen in Form von Modulen, Komponenten oder Objekten gebündelt werden können. Somit ist das Themenfeld Componentware (vgl. Abschnitt 8.4.1) eine grundlegende Voraussetzung für die Durchsetzung dieses Trends. Auch die Standardisierung von Schnittstellen (vgl. Abschnitt 8.4.7 und 8.4.5) spielen hierbei eine große Rolle. Ferner bietet sich die Abstraktion im Bereich der Softwareentwicklung an, um Systemanforderungen sowie das Systemdesign von konkreten Technologien zu abstrahieren. Dies ist heute vielfach über den Einsatz von formalen Beschreibungstechniken möglich (vgl. Abschnitt 8.4.3). Diese ermöglichen die Spezifikation von Systemen, ohne von Anfang an beispielsweise spezifische Qualitätseigenschaften der Hardware mit berücksichtigen zu müssen.

**Globalisierung und Wettbewerb** (Abschnitt 6.3): Dieser übergreifende Trend zeigt sich insbesondere im Bereich der Werkzeugherstellung, wobei zahlreiche Hersteller dieser Software im Wettbewerb um möglichst effiziente und vielfältig einsetzbare Entwicklungswerkzeuge stehen (vgl. Abschnitt 8.4.5). Ähnlich verhält es sich mit den Anbietern von Softwaretechnologien, wie beispielsweise Middelware-Architekturen, oder Kommunikationsinfrastrukturen (vgl. Abschnitt 8.4.1), die eine möglichst technologieunabhängige Entwicklung von Softwaresystemen unterstützen.

**Integration und Standardisierung** (Abschnitt 6.4): Der Trend zur Integration und Standardisierung hat eine große Ausprägung im Bereich der Entwicklungsautomation (vgl. Abschnitt 8.4.5) sowie der Komponentenorientierung (vgl. Abschnitt 8.4.1). In diesen Bereichen ist die Verfügbarkeit von Standards beispielsweise zur Interoperabilität von Werkzeugen oder zur Integration von Componentware in den Softwareentwicklungsprozess unverzichtbar. Standardisierung betrifft in gleicher Weise die Definition von Prozessmodellen und damit das Vorgehen bei der Softwareentwicklung (vgl. Abschnitt 8.4.7). Zudem ermöglicht die Standardisierung eine Erhöhung der Effektivität und Effizienz der Softwareerstellung und beeinflusst auf diese Weise insbesondere die dazu notwendigen Prozesse (vgl. Abschnitt 8.4.2 und 8.4.6).

**Kapazitäts- und Leistungssteigerung** (Abschnitt 6.5): Dieser übergreifende Trend betrifft insbesondere sehr berechnungsintenive Softwaretechnologien. Hierzu zählen Werkzeuge (vgl. Abschnitt 8.4.5), Infrastrukturen und Komponententechnologien (vgl. Abschnitt 8.4.1) sowie Test- und Verifikationstechniken (vgl. Abschnitt 8.4.4), um nur einige zu nennen.

**Konvergenz** (Abschnitt 6.6): Die Konvergenz im Sinne der in dieser Studie gegebenen Definition ist in diesem Themenfeld nur im Bereich der Systementwicklung zu beobachten (vgl. Abschnitt 8.4.6). Wurden bisher Programmiersprachen und Methoden auf Basis eines Programmierparadigmas weiterentwickelt, wird verstärkt eine Integration verschiedener Paradigmen angestrebt, um die Vorteile der verschiedenen Herangehensweisen zu verbinden. Dieser übergreifende Trend findet sich insbesondere in den Bereichen der Rechnernetze (vgl. Abschnitt 8.2) und der Anwendungen (vgl. Kapitel 9) wieder.

**Miniaturisierung** (Abschnitt 6.7): Die Miniaturisierung führt insbesondere dazu, dass Informations- und Kommunikationstechnik immer weitere Bereiche der

Softwaretechnik erschließen. So ist es möglich, im Bereich der Telekommunikation die JVM (Java Virtual Maschine) [Sun 02c] in Mobiltelefone zu integrieren oder Standard-Betriebssysteme mit eingeschränktem Funktionsumfang auf PDAs zu implementieren. Dies hat wiederum Auswirkungen auf die Systemerstellung (vgl. Abschnitt 8.4.6). Gleichermaßen ermöglicht diese Entwicklung neue Infrastrukturen, beispielsweise im Bereich der Telekommunikation wie MExE (Mobile Station Application Execution Environment) (vgl. Abschnitt 8.4.1).

**Mobilität** (Abschnitt 6.8): Die Mobilität stellt im Bereich der Softwaretechnik insbesondere Anforderungen an die Flexibilität und die Dynamik von Systemen. Dies erfordert vorwiegend neue Techniken der Systementwicklung sowie der Erweiterung von Beschreibungen auf diese neuen Systemeigenschaften (vgl. Abschnitt 8.4.6). Dieser übergreifende Trend findet sich besonders in zahlreichen Anwendungen wie beispielsweise der Anwendung mobiler Dienst in Abschnitt 9.3 wieder.

**Vernetzung und Flexibilisierung** (Abschnitt 6.9): Der übergreifende Trend zur Vernetzung und Flexibilisierung ermöglicht die Interoperabilität immer weiterer Systeme. Dies erfordert methodisch die Spezifikation von entsprechenden Standards im Bereich der Schnittstellen von Systemen und Systemkomponenten (vgl. Abschnitte 8.4.1 und 8.4.7). Zusätzlich fördert dieser Trend die Anwendungsmöglichkeiten von Technologien zur Entwicklung verteilter und vernetzter Anwendungen wie Java, .Net [Micr 02c] oder CORBA (Common Object Request Broker Architecture) [OMG 02].

**Verteilung und Dezentralisierung** (Abschnitt 6.10): Die Verteilung ist aus softwaretechnischer Sicht in zweierlei Hinsicht interessant. Zum Einen im Bereich der Verteilung von Systemen und zum Anderen im Bereich der verteilten Erstellung von Systemen. Im ersten Fall ergeben sich bislang nur sehr unflexibel spezifizier-, realisier- und vor allem garantierbare Anforderungen von Systemeigenschaften in den Bereichen Realzeitigkeit oder Dynamik (vgl. Abschnitt 8.4.6). Dennoch gibt es Technologien, welche die Realisierung dieser Anforderungen in Teilen über Konzepte wie Transparenz oder Persistenz von Objekten ermöglichen (vgl. Abschnitt 8.4.1). Im zweiten Fall stehen methodische Anforderungen im Vordergrund. Hier geht es in besonderer Weise darum, geeignete Entwicklungsprozesse und Beschreibungsmöglichkeiten zu definieren (vgl. Abschnitt 8.4.2 und 8.4.3), sowie bei der Automation geeignete Werkzeuge zu entwickeln, die in verteilten Entwicklungsumgebungen integriert werden können (vgl. Abschnitt 8.4.5).

**Virtualisierung** (Abschnitt 6.11): Die Virtualisierung ist in diesem Themenkomplex vorwiegend im Bereich der Automation zu finden (vgl. Abschnitt 8.4.5). Hierbei spiegelt sich dieser Trend in der Verbreitung von Simulationsmöglichkeiten wider. Dabei werden reale Repräsentationen über Werkzeuge simuliert, so dass Tests und Verifikationsmöglichkeiten im Rahmen der Qualitätssicherung gegeben sind (vgl. Abschnitt 8.4.4). Zudem ermöglichen Simulationen bereits in frühen Phasen der Systementwicklung eine prototypische Anwendung von Systemen.

In Tabelle 8.87 werden die Zuordnungen zwischen den übergreifenden Trends sowie den Trends und Entwicklungen im Themenfeld Softwaretechnik noch einmal grafisch veranschaulicht und zusammengefasst. Dabei fällt auf, dass die beiden übergreifenden Trends Verteilung und Dezentralisierung sowie Dienst- und Komponentenorientierung einen großen Einfluss auf die untersuchten Trends und Thesen haben. Im Vergleich zur Vorgängerstudie [SETIK 00] hat sich eine Verschiebung der stärksten Einflussfaktoren ergeben. In der letzten Studie waren diese die Integration und Standardisierung, die Kapazitäts- und Leistungssteigerung sowie die Vernetzung und Flexibilisierung.

### 8.4.1 Komponentenorientierung und Wiederverwendung

Die Nutzung von Komponenten und Diensten zur Erstellung von Systemen verspricht nicht nur Potenziale zur Reduktion der Systemkomplexität und zur Erhöhung der Software-Qualität, sondern auch Kostenvorteile oder Potenziale bei der Steigerung der Effizienz bei der Entwicklung. Diese Potenziale resultieren insbesondere aus der Möglichkeit zur Wiederverwendung. Die Bedeutung von Kom-

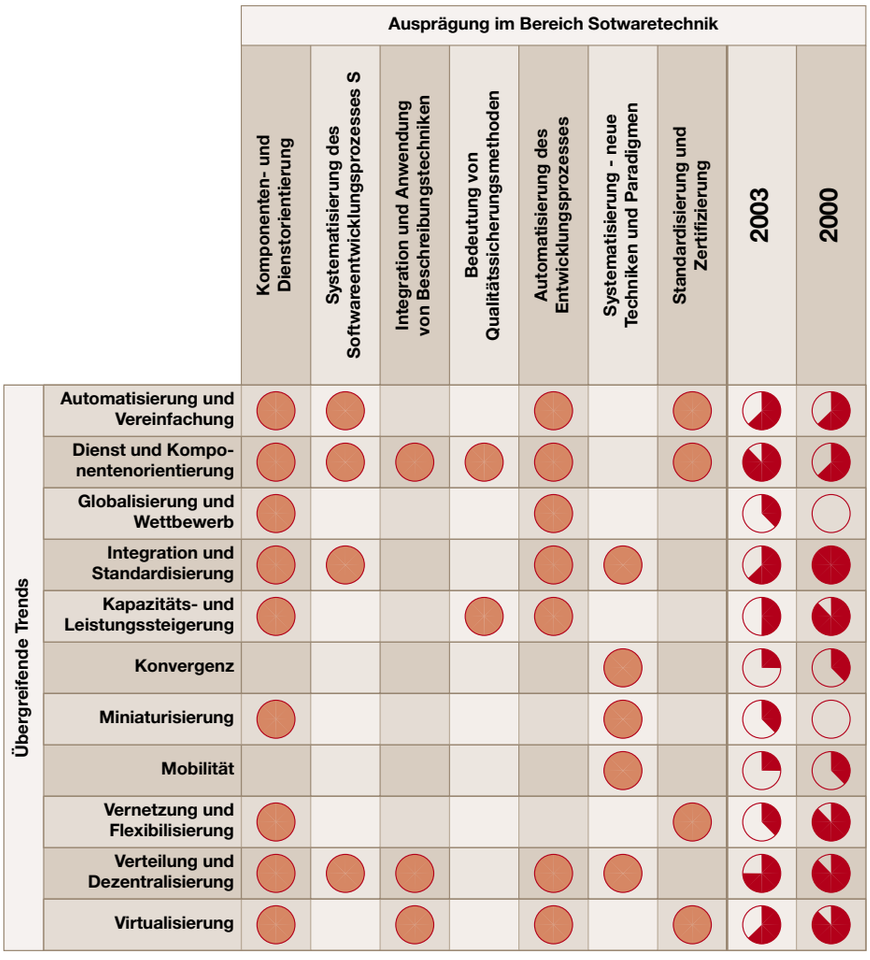



Abbildung 8.87: Ausprägungen übergreifender Trends im Technologiefeld Softwaretechnik

ponenten und Diensten wird in der Literatur gleichermaßen als hoch eingestuft [Szyp 98].

Die zunehmende Komponenten- und Dienstorientierung hat Auswirkungen auf zahlreiche Aspekte der Entwicklung. So beeinflussen diese Auswirkungen beispielsweise die Verwendung von Technologien in den Bereichen Softwarearchitekturen, Infrastrukturen oder Middleware-Plattformen. Aber auch methodisch müssen Vorgehensmodelle, Entwicklungsumgebungen oder Beschreibungstechniken an diese Konzepte angepasst werden. Nicht zuletzt führt die Verwendung von Komponenten oder Diensten aufgrund ihrer Wiederverwendbarkeit zu einer Reihe von Potenzialen zur Erhöhung der Effektivität und Effizienz bei der Softwareentwicklung.

## Ergebnisse

Zunächst wurde die Standardisierung von Softwarekomponenten adressiert. Die Frage zielt insbesondere darauf ab, zu welchem Zeitpunkt standardisierte Softwarekomponenten weit verbreitet sein werden. Die Befragung hat ergeben, dass eine weite Verbreitung in frühestens zwei Jahren, und spätestens in sieben Jahren gegeben ist. Im Durchschnitt wird diese Entwicklung allerdings in fünf Jahren erwartet. Der Trend wird in einem Zeitintervall von insgesamt fünf Jahren erwartet, so dass eine gewisse Unsicherheit bei der Beurteilung dieses Trends beobachtet werden kann (vgl. Abbildung 8.88, ①). Die Bewertung des Zeitrahmens dieser These fällt sowohl bei der Wissenschaft als auch bei der Industrie ähnlich aus. Die Erwartung ist mit zwei bis drei Jahren seitens

STANDARDISIERTE SOFTWAREKOMPONENTEN: Standardisierte Softwarekomponenten werden in 5 Jahren weit verbreitet sein.

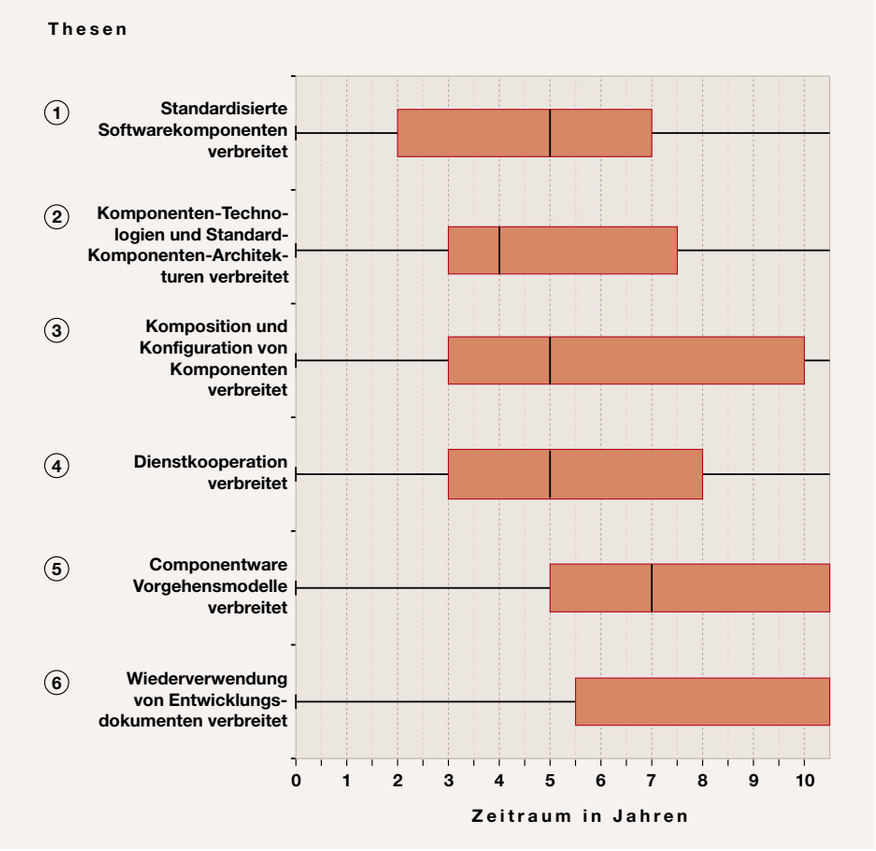



Abbildung 8.88: Ergebnisse der Thesen zur Komponentenorientierung und Wiederverwendung

der Industrie im Vergleich zu vier Jahren seitens der Wissenschaft optimistischer. In einem Vergleich mit der Vorgängerstudie [SETIK 00] ergibt sich, dass sich der Erwartungshorizont insgesamt um zwei Jahre nach hinten verschoben hat im Vergleich zum ursprünglich geplanten Zeithorizont.

Die Anwendungsmöglichkeiten von standardisierten Softwarekomponenten sind dabei sehr vielfältig und reichen von GUI-Programmierung (Grafical User Interface) im Bereich der Benutzeroberflächen bis zur Entwicklung komplexer Business-Applikationen wie z.B. SAP. Als weitere Anwendungsfelder werden dabei unter anderem die Bereiche Middleware, Betriebssysteme, Datenbanken, aber auch Werkzeuge, Web- und Desktopanwendungen sowie Netzwerke genannt. Ebenfalls eingeschlossen sind Anwendungen im Bereich dynamischer und mobiler Systeme im End-User-Bereich. Zudem wurde angemerkt, dass Komponenten insbesondere dann große Potenziale bei der Softwareentwicklung bieten, wenn es sich dabei um kleine flexibel einsetzbare Bausteine handelt. Die hohe Fehlerfreiheit standardisierter Komponenten wird sich ebenfalls positiv auf die Qualität der Systeme, in denen diese verbaut sind, auswirken.

Eingebettete Technologien sind insbesondere Komponententechnologien wie CORBA, EJB (Enterprise Java Beans) [Sun 03b], ActiveX oder COM (Component Object Model) [Micr 99]/DCOM (Distributed Component Object Model) [Thie 00] auf Middlewareebene oder UML (Unified Modelling Language) auf der Ebene der Beschreibung von Systemen. Zahlreiche Experten betonen die besondere Bedeutung von klaren Schnittstellen und damit einhergehend die Bedeutung von Technologien zur Beschreibung von Schnittstellen und Kommunikationsstrukturen wie SOAP (Simple Object Access

Protocol) [SOAP 03] oder XML (Extensible Markup Language) [XML 99]. Auch plattformunabhängige Programmiertechnologien wie Java werden als Technologien zur Realisierung dieses Trends vorausgesetzt. Gleichermaßen sind die Verfügbarkeit von (möglichst einfachen) Standards zur Spezifikation von Schnittstellen, als auch Standard-Softwarearchitekturen, -Geschäftsabläufen oder -Beschreibungssprachen unverzichtbar. Nicht zuletzt hängt diese Entwicklung von der „politischen" Unterstützung der Standardisierungsprozesse ab.

Für die Nutzung standardisierter Softwarekomponenten ist die Verfügbarkeit standardisierter Komponenten-Technologien und Standard-Architekturen unverzichtbar. Sie bilden die Voraussetzung dafür, dass Komponenten bei der Systementwicklung integriert werden können. Eine Umsetzung der vorangegangenen These ist in Folge dessen nur dann möglich, wenn sich Komponenten-Technologien bereits in den Unternehmen durchgesetzt haben werden. Daher wurde untersucht, wann eine weite Verbreitung dieser Technologien bzw. Architekturen gegeben ist. Es hat sich herausgestellt, dass der erwartete Zeitrahmen für das Eintreten dieser These zwischen drei und sieben bis acht Jahren beträgt. Der Median liegt dabei bei vier Jahren (vgl. Abbildung 8.88, ②). Bei einer Detaillierung dieser Zahlen ergibt sich, dass die Experten aus der Industrie die Verfügbarkeit geeigneter Technologien zur Nutzung von Standard-Softwarekomponenten in vier Jahren erwarten, während die Experten aus der Wissenschaft diese Entwicklung erst in sechs bis sieben Jahren erwarten. Im Vergleich zur Vorgängerstudie zeigt sich, dass diese These beide Male nominell gleich eingeschätzt wird. Somit verschiebt sich die Erwartung im Vergleich zur letzten Studie um drei Jahre in die Zukunft.

Einfache Standards ermöglichen die Nutzung der Komponenten-Technologien. Im Bereich der Business-Systeme müssen entsprechende Frameworks für die Erbringung von Business-Logik existieren, damit eine Umsetzung der oben angesprochenen Entwicklung möglich ist. Hinzu kommt, dass standardisierte Sprachen, Kommunikations- und Architektur-Technologien wie Java, SOAP, ActiveX, Java Beans [Sun 02b] oder EJB verbreitet und angewendet werden müssen. Ferner werden die einfache Anwendung sowie die Abstraktion von technischen Details wie Betriebssysteme oder der Integration von Quality of Service Parametern für die Durchdringung der Technologien ausschlaggebend sein.

In diesem Zusammenhang stellt sich die Frage, wie sich moderne Prozesse bei der Softwareerstellung durch die Nutzung von Komponenten verändern werden. Eine alternative Entwicklungsmethode auf der Basis von Softwarekomponenten ist in diesem Zusammenhang die Entwicklung von Software durch die Komposition und Konfiguration von Softwarebausteinen. In diesem Zusammenhang wurde evaluiert, wann diese Art der Softwareentwicklung verbreitet sein wird. Die Bewertung dieser These durch die Experten hat gezeigt, dass sich dieser Trend in fünf Jahren durchgesetzt haben wird. Der erwartete Zeitrahmen beträgt hierbei drei bis zehn Jahre, so dass die Unsicherheit bei dieser Aussage sehr hoch ist (vgl. Abbildung 8.88, ③).

Eine Differenzierung dieser Aussage nach Experten aus der Industrie und Experten aus der Wissenschaft zeigt mit vier bis fünf Jahren eine deutlich optimistischere Erwartungshaltung der Experten aus der Industrie gegenüber den Experten aus der Wissenschaft mit neun Jahren. Auffällig ist auch, dass die Experten aus der Wissenschaft diese Entwicklung erst in fünf bis mehr als zehn Jahren erwarten, während die Experten aus der Industrie einen Zeitrahmen von zwei bis acht Jahren vorgeben. Im Gegensatz zur Vorgängerstudie zeigt sich, dass die Erwartung sich um drei Jahre in die Zukunft verschoben hat.

Software über Komposition und Konfiguration zu entwickeln, kann in unterschiedlichen Anwendungsbereichen zum Einsatz kommen. Als Beispiele sind Netzwerkanwendungen, Internetanwendungen genauso genannt worden wie GUIs oder Datenbankanwendungen (insbesondere bei der Evaluation großer Datenmengen, beispielsweise im Anwendungsfeld Medizin). Ebenso ist diese Art der Entwicklungsunterstützung bei Office-Anwendungen (Finanzsoftware), Web- und Multimediadiensten (ASP) sowie verteilten und Agentensystemen (beispielsweise Ferndiagnose und -wartung) vorstellbar. Diese Art der Erstellung würde darüber hinaus die Mög-

KOMPONENTEN-TECHNOLOGIEN UND STANDARD-ARCHITEKTUREN: Standardisierte Komponenten-Technologien und Standard-Architekturen für Componentware werden in 4 Jahren weit verbreitet sein.

KOMPOSITION UND KONFIGURATION VON SOFTWAREBAUSTEINEN: Software durch Komposition und Konfiguration von Komponenten zu implementieren, ist in 5 Jahren weit verbreitet.

lichkeit bieten, Softwareentwicklung beispielsweise über Drag & Drop auch Laien zugänglich zu machen. Auch die Entwicklung komplexer Softwaresysteme wie beispielsweise COTS (Commercial Off-The-Shelf) [Deif 98b] wird durch diese komponentenorientierte Vorgehensweise maßgeblich unterstützt. Gleichermaßen werden Potenziale im Bereich mobiler und dynamischer Systeme gesehen, bei denen die Art der Komposition und Konfiguration sehr flexible Netzdienste ermöglichen würde. Vorsichtiger ist die Einschätzung bei der Anwendung dieser Methodik im Bereich sicherheitskritischer Systeme, da viele der Quellen kommerzieller Komponenten nicht einsehbar sind.

DIENSTE UND KOOPERATION VON DIENSTEN: Software in Form von Diensten bzw. Kooperation von Diensten bereit zu stellen, ist in 5 Jahren weit verbreitet.

Die Umsetzung dieser Methodik setzt die Existenz eines Komponentenmarktes voraus, über den Komponenten in den unterschiedlichen Anwendungsbereichen auf der Basis von Standard-Komponententechnologien mit entsprechenden Aufrufprotokollen verfügbar sind. Zudem müssen Märkte für die auf den Komponenten aufbauenden Dienste und Business-Modelle entstehen. Ferner sind geeignete Beschreibungstechniken, standardisierte Komponentenverzeichnisse und Schnittstellenstandards erforderlich sowie Standards für Geschäftsprozesse. Ebenfalls notwendig sind Codegeneratoren, die diese Vorgehensweise umsetzen können und die es ermöglichen, aus bestehendem Code Komponenten zu generieren. Auch in diesem Zusammenhang sind geeignete Komponenten-Architekturen unverzichtbar. Methodisch sind ebenfalls Rückkopplungen möglich, die eine Anpassung von Softwarebausteinen und damit von Anforderungen an Systeme erfordern.

Die Abstraktion von Technologie-Aspekten und Implementierungsdetails ermöglicht eine weitere Form der Softwareentwicklung, nämlich die durch Dienste und Kooperation von Diensten. In diesem Zusammenhang wurde im Rahmen der Studie evaluiert, wann sich der Trend zur Bereitstellung von Diensten bzw. kooperativen Diensten (z.B. Application Service Provisioning) durchgesetzt hat. Die Studie hat gezeigt, dass die Experten diese Entwicklung in fünf Jahren erwarten (vgl. Abbildung 8.88, ④). Auffällig sind die Unterschiede zwischen Wissenschaft und Industrie. Dabei zeigt sich, dass die Experten aus der Industrie diesen Trend in etwa vier Jahren erwarten, während die Experten aus der Wissenschaft einen Wert von acht Jahren prognostizieren.

Die Experten sehen Potenziale insbesondere dann, wenn für erhebliche Ressourcen zur Erbringung einer Anwendung benötigt werden, dies aber nicht vom Entwickler selbst zur Verfügung gestellt werden können. Ein Beispiel hierzu wäre die Evaluierung großer Datenmengen wie dies bei Datenbanksystemen im Bereich Data-Warehousing oder Data-Marts über OLTP (Online Transaction Processing) [Stür 90] und OLAP (Online Analytical Processing) [GrHe 99, DSVH 97] oder Systemen zur Verarbeitung von geografischen Informationen oder Daten der elektronischen Zusammenbauanalyse und Ähnlichkeitssuche der Fall ist (vgl. Abschnitt 8.3). Schließlich werden noch mobile Systeme oder Anwendungen wie Fernwartung und Ferndiagnose im Netzwerkbereich genannt. Grundsätzlich wird die Ausweitung dieses Trends vom Netzwerkbereich auf den Applikationsbereich erwartet. Einige Experten sind bei der Bewertung dieser These allerdings etwas vorsichtiger und erwarten nur einen eingeschränkten Einsatz von Diensten bei der Softwareentwicklung, was unter anderem auf mangelnde Infrastrukturen und einen fehlenden Markt zurückzuführen sei. Hinzu kommt, dass Dienste Softwaresysteme nur dort ersetzen können, wo die Schnittstellen und Abhängigkeiten klein genug sind.

Vorausgesetzt werden bei der Bewertung dieser These die Existenz geeigneter Infrastruktur-Technologien wie beispielsweise CORBA sowie normierte Sprachen oder Standards für Geschäftsprozesse. Ebenfalls werden Dienst-Märkte als förderlich vorausgesetzt sowie geeignete Business-Modelle, die eine Vermarktung und Propagierung der Dienste begünstigen. Ferner sind Referenz- und Schichtenmodelle erforderlich, welche Transparenz bei der Verteilung von Daten realisieren bzw. eine verlässliche Verfügbarkeit und Sicherheit von Transaktionen gewährleisten. Damit eng verbunden werden geeignete Beschreibungstechniken für Service Level Aggreements (SLAs), Sicherheitsgarantien (QoS) oder standardisierte Schnittstellendefinitionen benötigt.

Auf Technologieebene wurden vier unterschiedliche Technologie-Klassen im Bereich Componentware evaluiert. Hierzu zählen zunächst die Komponenten-Technologien auf Architekturebene wie .Net, CORBA und EJB, Komponententechnologien auf Code-Ebene wie ActiveX und Java Beans, Dienstarchitekturen wie Jini [Sun 99] sowie Kommunikationsmechanismen wie RPC (Remote Procedure Call) [OG 97] oder Java RMI (Java Remote Method Invocation) [JRMI 03]. Die Ergebnisse sind in den Abbildungen 8.89, 8.90, 8.91 sowie 8.92 und in den folgenden Absätzen beschrieben.

Bei den Komponententechnologien auf Architekturebene zeigt sich, dass bis auf EJB keiner anderen Technologie eine größere Bedeutung beigemessen wird (vgl. Abbildung 8.89).

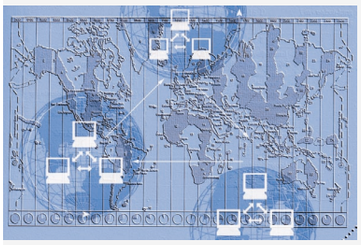
Im Kontext von .Net werden folgende Kommentare gegeben: Grundsätzlich kann sich aufgrund der Marktmacht von Microsoft diese Technologie durchsetzen. Hemmend wirken jedoch die mangelnde Plattformunabhängigkeit sowie die unzureichende Zuverlässigkeit. Hinzu kommt, dass die Bedeutung dieser Technologie vorwiegend im Codebereich liegen wird. Begünstigend für CORBA wird angesehen, dass diese Technologie sich für verteilte und insbesondere sicherheitskritische Anwendungen eignet und sehr gut skaliert. Somit kann CORBA besonders vorteilhaft in Großbetrieben eingesetzt werden. Dagegen spricht allerdings die hohe Komplexität. CORBA wird zwar heute eine große Bedeutung beigemessen, für die Zukunft wird allerdings ein gravierender Bedeutungsverlust vorhergesagt. EJB bietet sich an, um große Serverapplikationen und mehrschichtige Geschäftsanwendungen zu entwickeln. Die Anwendungsfelder reichen von E-Business-Systemen bis hin zu betrieblichen Informatonssystemen. Vorteilhaft ist dabei die gute Skalierbarkeit sowie die hohe Ausfallsicherheit. Als Komponententechnologie wird EJB derzeit und in Zukunft als beste Alternative angesehen. Bei SunONE [Sun 03d] sind sich die Experten nicht ganz sicher, ob diese Technologie sich durchsetzen wird oder nicht. Es wird angemerkt, dass dies vorwiegend von der Entwicklung von .Net abhängt. Zugute kommt SunONE allerdings die hohe Ausfallsicherheit und die gute Skalierbarkeit der Anwendungen.

Für die Komponententechnologien auf Code-Ebene ActiveX und Java Beans hat sich gezeigt, dass die Bedeutung nicht besonders hoch ist. Allerdings bietet Java Beans langfristig mehr Potenzial als beispielsweise ActiveX. Zusätzlich wurde von einige Experten erwähnt, dass es in diesem Umfeld zumindest in den kommenden zehn Jahren keinen signifikanten Bedarf für neue Technologien geben wird (vgl. Abbildung 8.90).

Die stark abfallende Bedeutung von ActiveX resultiert nach Meinung der Experten unter anderem daraus, dass diese Technologie in .Net integriert ist und somit von der .Net-Entwicklung abhängen oder durch die .Net-Technologie abgelöst werden wird. Kritisch werden bei dieser Technologie die Sicherheitsprobleme insbesondere bei Netzanwendungen gesehen. Die Plattformabhängigkeit wird ebenfalls hemmend bewertet. Zudem wird die Bedeutung im Enterprise- und Server-Bereich sowie in großen Softwareprojekten eher als gering eingestuft. Bei Java Beans werden größere Potenziale gesehen. Diese resultieren beispielsweise daraus, dass keine Ablöse- oder Folgetechnologie existiert und darüber hinaus Java Beans als Basistechnologie für andere Technologien herangezogen werden kann. Trotz des insgesamt abfallenden Bedeutungsverlaufs der Komponententechnologien auf Code-Ebene werden von den Experten der Bedarf neuer Technologien in diesem Umfeld nicht gesehen. Die Ergebnisse sind grafisch in Abbildung 8.90 noch einmal zusammengefasst.

Bei der Einschätzung der Diensttechnologien bewerten die Experten den Bedeutungsverlauf normal. Es sind bis auf die Einschätzung der Technologien UDDI (Universal Description, Discovery and Integration)/WSDL (Web Service Definition Language) keine herausragenden Verläufe zu erkennen. Ausschließlich UDDI/WSDL wird langfristig eine größere Bedeutung eingeräumt (vgl. Abbildung 8.91).

Zu einigen Technologien wurden intensiv Kommentare angegeben, die im Folgenden zusammengefasst werden: Bei Jini wurde angemerkt, dass diese Technologie sich bislang nicht durchgesetzt hat und auch in Zukunft nicht durchsetzen wird. Die Anwendungen werden eher in Nischenbereichen bei eingebetteten Systemen oder COTS-Produkten gesehen. Zu-



KOMPONENTEN-TECHNOLOGIEN AUF ARCHITEKTUREBENE: Bei diesen Technologien wird EJB ein herausragender Stellenwert beigemessen.

KOMPONENTEN-TECHNOLOGIEN AUF CODE-EBENE: Die Bedeutung dieser Technologien wird insgesamt nicht besonders hoch eingestuft.

DIENSTTECHNOLOGIEN: Die Bedeutung von Dienstarchitekturen wird insgesamt eher niedrig eingestuft.

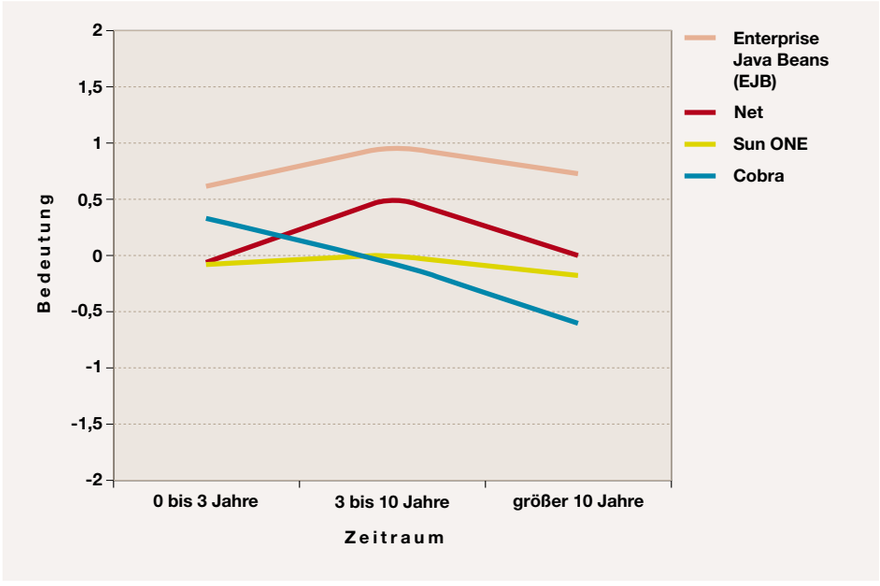



Abbildung 8.89: Bedeutung von Komponenten-Technologien auf Architektur-Ebene


Abbildung 8.90: Bedeutung von Komponenten-Technologien auf Code-Ebene

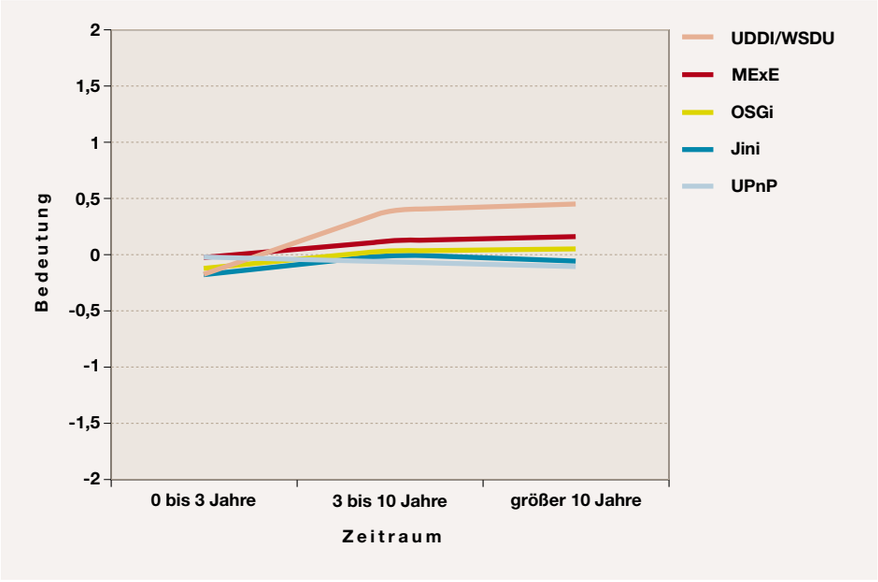



Abbildung 8.91: Bedeutung von Dienst-Architekturen

sätzlich wurde erwähnt, dass beispielsweise MExE an Bedeutung gewinnen könnte, wenn Anwendungen für Smartphones vermehrt erforderlich werden. Dem steht entgegen, dass nicht klar eingeschätzt werden kann, wie sich die Entwicklung im Bereich der Mobiltelekommunikation vollziehen wird. UDDI/WSDL wurde intensiv diskutiert. Die Anwendungen, in denen diese Technologie insbesondere zum Einsatz kommen wird, sind Web Services oder verteilte betriebliche Informationssysteme. Die Verbreitung dieser Technologie wird begünstigt durch eine stärkere Integration von UDDI/WSDL in bestehende Entwicklungswerkzeuge.

Bei der Bewertung der Kommunikationstechnologien hat sich folgendes Bild ergeben. Die Experten erwarten einen Bedeutungswechsel von traditionellen Technologien wie RPC und Java RMI hin zu modernen Internettechnologien wie SOAP und Mischungen bzw. Kombinationen aus HTTP und XML. In Folge dessen wird die Bedeutung von RPC und Java RMI künftig abnehmen und HTTP sowie XML weiter zunehmen. Ein Bedarf neuer Technologien wird nicht gesehen (vgl. Abbildung 8.92). Dabei wurde trotz dieser Entwicklung angemerkt, dass die traditionellen Kommunikationstechnologien weiterhin eingesetzt werden, da diese inzwischen eine hohe technologische Reife besitzen und sich die Konzepte als tragfähig herausgestellt haben.

Es ergeben sich für die beschriebenen Technologien unterschiedliche Klassen von Einsatzfeldern. Während sich RPC und Java RMI vorwiegend für die Entwicklung von Client-Server-Architekturen und insbesondere verteilter Anwendungen eignen, bezieht sich der Einsatz von SOAP oder allgemein HTTP in Kombination mit XML primär auf den Bereich verteilter webbasierter Dienste.

Insgesamt kann bei einem Vergleich der Ergebnisse der Komponenten-Technologien mit den Ergebnissen der Vorgängerstudie [SETIK 00] festgehalten werden, dass die Einschätzungen und Erwartungen zur Vorgängerstudie sehr ähnlich verlaufen. So wurde auch bei der letzten Studie EJB ein besonderer Stellenwert eingeräumt.

Ein vorwiegend organisatorischer Aspekt bei der Verwendung von Komponenten ist der Aspekt der Vorgehensmodelle. Hier wurde untersucht, zu welchem Zeitpunkt standardisierte Vorgehensmodelle auf der Basis von Componentware, die noch dazu einfach implementiert werden können, von einer breiten Basis von Unternehmen eingesetzt werden. Die Auswertung dieser These hat ergeben, dass der Einsatz in sieben Jahren erwartet wird (vgl. Abbildung

KOMMUNIKATIONS-TECHNOLOGIEN: XML und HTTP werden im Kontext von Kommunikationstechnologien bei zukünftiger Softwaretechnik einen herausragenden Stellenwert besitzen.

STANDARDISIERTE VORGEHENSMODELLE: Standardisierte und in den Unternehmen anwendbare Vorgehensmodelle auf der Basis von Componentware sind in durchschnittlich 7 Jahren weit verbreitet.

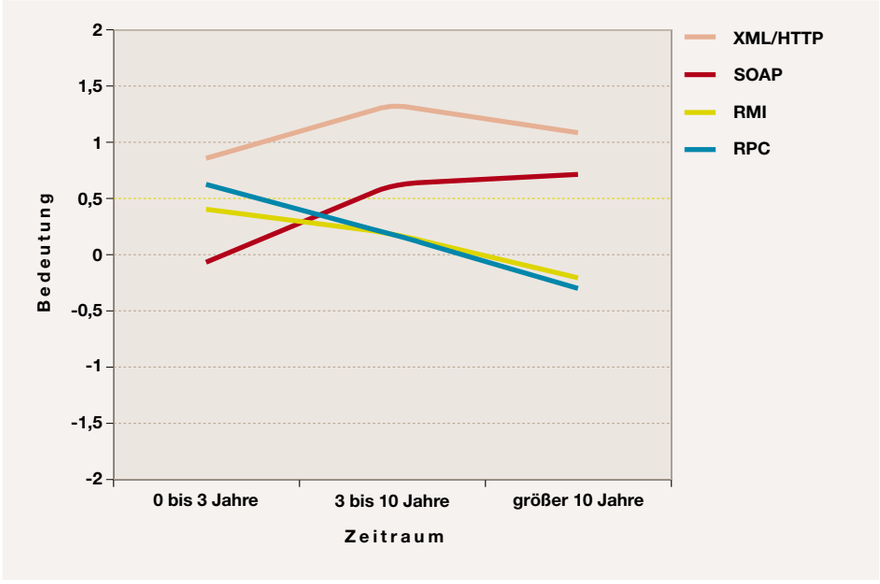



Abbildung 8.92: Bedeutung von Kommunikationsmechanismen

8.88, ⑤). Im Vergleich zur Vorgängerstudie verschiebt sich die Bewertung dieser These um weitere drei Jahre in die Zukunft.

Mögliche Vorgehensmodelle, die für komponentenorientierte Softwareentwicklung sinnvollerweise eingesetzt werden können, sind nach Meinung der Experten das V-Modell (IABG - Vorgehensmodell '97) [IABG 99], der Unified Process (Unified Process) [ZBGK 02] sowie Extreme Programming [Beck 00]. Die Anwendungsfelder liegen vorwiegend im Bereich Standardsoftwareentwicklung, insbesondere in den Bereichen Banken, sowie CRM- (Customer Relationship Management) und ERP-Systeme (Enterprise Resource Planing), aber auch Internetauftritte, Businesssoftware oder E-Commerce-Anwendungen. Die Definition von präzisen Vorgehensaktivitäten ist insbesondere bei der Softwareerstellung sowie dem Qualitäts- und Risk-Management zu beobachten, was vorwiegend für sicherheitskritische Anwendungen relevant ist. Interessant sind diese Aspekte vor allem für Großunternehmen sowie öffentlichen Verwaltungen. Auch bei der Integration und Konfiguration von Standardsoftware wie SAP oder anderen COTS-Produkten in den Unternehmen ist die Definition und und Nutzung präziser Vorgehensmodelle unerlässlich.

Die Verbreitung von Vorgehensmodellen erfordert einerseits Werkzeuge zur Definition, Implementierung und zum Tailoring der Modelle und andererseits Komponententechnologien wie .Net, ActiveX, CORBA und EJB einschließlich neuer Paradigmen wie beispielsweise Programming by Contract. Auch Objektorientierung wird hier als sinnvolle Technologie angesehen. Alternativ dazu ist es notwendig, in bestehende Entwicklungstools die Vorgehensweisen stärker zu integrieren. Es sind parallel zu Werkzeugen zur Realisierung des Vorgehens auch Werkzeuge für die Definition und Umsetzung von Geschäftsprozessen erforderlich. Für die Verwaltung von Dokumenten sind in diesem Zusammenhang Repository-Technologien unverzichtbar. Außerdem müssen die Akzeptanz gegenüber Vorgehensmodellen in den Unternehmen verbessert werden und Standards bei der Entwicklung (im Prozess) gefördert werden. Hierzu bietet sich die Nutzung formaler Methoden an. Hinzu kommen passende Infrastrukturen und Schnittstellenstandards. Als weitere wichtige Voraussetzung werden die Verbesserung der Ausbildung zum methodischen Software Engineering im Allgemeinen sowie die Förderungen der Kenntnisse über „Best Practices" in diesem Umfeld im Besonderen angesehen.

Die Leistungsfähigkeit komponentenbasierter Softwareentwicklung wird insbesondere durch die großen Potenziale der Wiederverwendung möglich. Aus diesem Grund wurde untersucht, bis wann die Wiederverwendung von Entwicklungsdokumenten aller Prozessphasen der Softwareerstellung zusätzlich zu ausführbarer Software weit verbreitet sein wird. Die Auswertung zeigt, dass eine Verbreitung von Wiederverwendung erst in über zehn Jahren erwartet wird (vgl. Abbildung 8.88, ⑥). Die Prognose dieser These deckt sich mit der Einschätzung in der Vorgängerstudie, so dass sich offensichtlich für die Befragten keine sichtbare Weiterentwicklung im Bereich der Wiederverwendung von Entwicklungsdokumenten ergeben hat.

Wiederverwendung betrifft nach Meinung der Experten generell alle Phasen der Softwareentwicklung und vorzugsweise die Anforderungsanalyse. Die Wiederverwendung lohnt sich nicht nur bei hochkritischen sondern auch bei sehr umfangreichen komplexen Systemen insbesondere im Bereich der eingebetteten Systeme. Dabei dient die Wiederverwendung vorwiegend dazu, die Wirtschaftlichkeit zu steigern und die Komplexität der Systeme beherrschbar zu machen.

In diesem Zusammenhang reichen die erforderlichen Technologien von Entwicklungsumgebungen mit integriertem Konfigurationsmanagement und Dokumentenmanagement über normierte Repositories und Technologien zur Spezifikation wie XMI (XML Metadata Interchange) [OMG 99] oder XML bis hin zu Projekt- und Code-Bibliotheken oder Komponentensuchmaschinen mit entsprechend einfach bedienbaren und standardisierten Schnittstellen. Von besonderer Bedeutung sind formale Spezifikationsmethoden zur präzisen Beschreibung der Syntax und Semantik von Komponenten.

Nicht zuletzt wurde in diesem Abschnitt evaluiert, wie groß der Wiederverwendungsanteil von Entwicklungsdokumenten in den kommenden Jahren ist. Dabei hat sich herausgestellt, dass der Anteil an wiederverwendeten Dokumenten derzeit zehn Prozent beträgt und langfristig gesehen auf etwa 30 Prozent ansteigen wird. Der Verlauf ist in Abbildung 8.93 dargestellt.

### Zusammenfassung

In diesem Themenkomplex lassen sich eine Reihe von Kernaussagen zusammenfassen.

- Die Verbreitung standardisierter Softwarekomponenten wird sich bis 2008 weiter durchsetzen.
- Zusätzlich werden sich Komponententechnologien mittelfristig weiter am Markt behaupten. Bedeutende Technologien werden in diesem Zusammenhang ActiveX, Java Beans, UDDI/WSDL sowie XML/HTTP und SOAP sein.
- Die Methode, über die Komposition und Konfiguration von Softwarebausteinen Systeme zu erstellen, wird sich bis zum Jahr 2008 durchsetzen.
- Die dienstorientierte Softwareentwicklung wird sich gleichermaßen bis 2008 durchsetzen.
- Vorgehensmodelle für Componentware werden sich im Gegensatz zum dienstorientierten Ansatz bis 2010 am Markt behaupten.
- Die Komponentenorientierung bietet in weiten Teilen des Entwicklungsprozesses Potenzial zur Wiederverwendung. Es hat sich herausgestellt, dass die Experten selbst langfristig nicht mit einer deutlichen Erhöhung der Wiederverwendung der Entwicklungsdokumentation über alle Entwicklungsphasen hinweg rechnen. Insgesamt verdreifacht sich langfristig der Wiederverwendungsanteil der Entwicklungsdokumentation auf über 30 Prozent. Dabei wird es sich jedoch vorwiegend um ausführbaren Code handeln.

WIEDERVERWENDUNG VON ENTWICKLUNGSDOKUMENTEN: Die Wiederverwendung von Entwicklungsdokumenten aller Entwicklungsphasen, zusätzlich zu ausführbarer Software, ist erst in ferner Zukunft mit über 10 Jahren weit verbreitet.

WIEDERVERWENDUNGSANTEIL VON ENTWICKLUNGSDOKUMENTEN: Der Wiederverwendungsanteil von Entwicklungsdokumenten wird von derzeit geschätzten und gerundeten 10% langfristig auf etwa 30% ansteigen.

## 8.4.2 Systematisierung des Entwicklungsprozesses

Die Systematisierung des Entwicklungsprozesses beschäftigt sich insbesondere mit der Problemstellung, wie Anforderungen sinnvoll erarbeitet, erfasst und angemessen im Rahmen des Entwicklungsprozesses weiterverarbeitet werden können. Mögliche Lösungen für diese Pro-

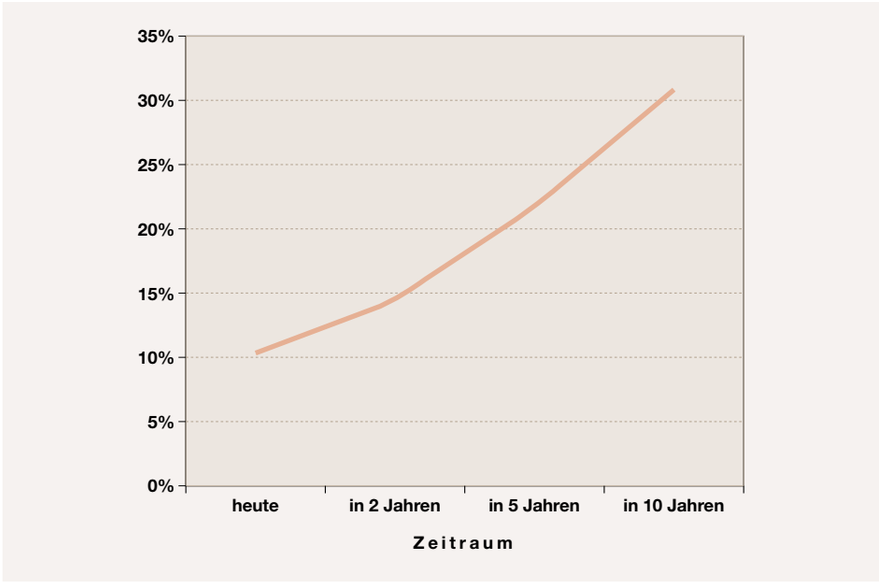



Abbildung 8.93: Zuwachs des Wiederverwendungsanteils von Entwicklungsdokumenten

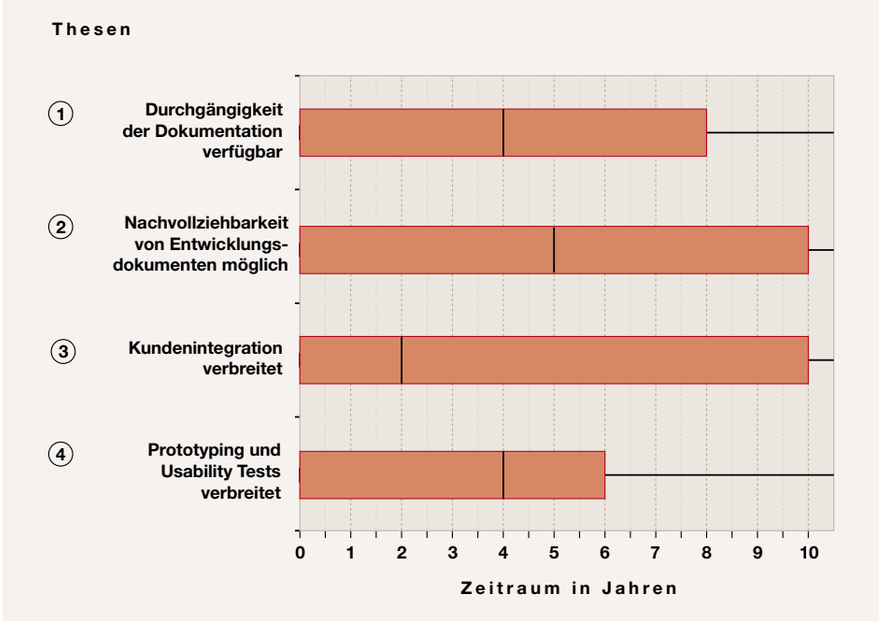



Abbildung 8.94: Ergebnisse der Thesen zur Systematisierung des Entwicklungsprozesses

blemstellungen werden im Folgenden detailliert diskutiert [Deif 98b, Deif 01].

Der Entwicklungsdokumentation fällt im Rahmen dieser Diskussion eine besondere Bedeutung zu. Die Systematisierung beinhaltet hierbei die Fragestellung, wie eine Dokumentation gestaltet werden muss, damit diese zur Verarbeitung von Anforderungen herangezogen werden kann. Dabei sind insbesondere zwei Aspekte von Bedeutung: die Durchgängigkeit sowie die Nachvollziehbarkeit (Traceability) der Dokumentation. Was unter diesen beiden Begriffen zu verstehen ist, wird im Folgenden skizziert.

Unter Durchgängigkeit wird die Verfügbarkeit einer konsistenten Entwicklungsdokumentation über alle Entwicklungsphasen, d.h. von der Anforderungsdefinition bis zum Roll Out, verstanden. Dies impliziert, dass es keine Methoden- oder Werkzeugbrüche zwischen den Entwicklungsphasen geben darf.

Nachvollziehbarkeit beschreibt eine Entwicklungsdokumentation, welche es ermöglicht, über die unterschiedlichen Entwicklungsphasen hinweg Zusammenhänge zwischen den jeweiligen Entwicklungsdokumenten herzustellen und konsistent halten zu können. Dies ist insbesondere dann wichtig, wenn es Änderungen in den Anforderungen gibt und Systemmodifikationen erforderlich werden. Eine Verbesserung der Dokumentation im Hinblick auf diese beiden Eigenschaften kann insbesondere durch die Integration formaler, grafischer Beschreibungstechniken erfolgen. Diese eignen sich zum Einen zur Visualisierung komplexer Zusammenhänge und zum Anderen aufgraund der zugrunde liegenden Systemmodelle zur formalen Sicherstellung der Konsistenz und Korrektheit von Systemen.

Ein weiterer Aspekt, der in diesem Themenkomplex bearbeitet wird, ist die Erfassung und Sicherstellung von Anforderungen. Hierzu wird evaluiert, welche Bedeutung der Integration des Kunden nicht nur bei der Erfassung der Anforderungen, sondern auch im Verlauf des Entwicklungsprozesses beigemessen wird und wie die spezifizierten Anforderungen erfolgreich umgesetzt werden können. Für eine erfolgreiche Umsetzung wird insbesondere die Rolle der Usability Tests diskutiert.

## Ergebnisse

Bei der Betrachtung der Systematisierung des Entwicklungsprozesses wurde zunächst die Durchgängigkeit der Entwicklungsdokumentation analysiert. Dabei wurden die Experten befragt, wann eine durchgängige Vorgehensweise zur Erstellung von Dokumenten von der Anforderungsdefinition angefangen, über die Analyse und das Design, bis hin zum Roll Out verfügbar sein wird. Dabei hat sich ergeben, dass die Experten diese Entwicklung in den nächsten vier Jahren erwarten. Dies beruht darauf, dass die Interpretation von Durchgängigkeit bei den Experten unterschiedlich ausfällt. Während einige Experten unter Durchgängigkeit eher eine syntaktische Beziehung zwischen den Dokumenten verstehen, sind für andere insbesondere die semantischen Zusammenhänge zwischen den Dokumenten relevant. Beide Betrachtungsszenarien führen allerdings zwangsläufig zu sehr unterschiedlichen Einschätzungen, was nicht zuletzt durch die enorme Streuung der Ergebnisse dokumentiert wird (vgl. Abbildung 8.94, ①). Im Vergleich zur Vorgängerstudie [SETIK 00] hat sich herausgestellt, dass sich die Erwartung einer durchgängigen Entwicklungsdokumentation weiter um ein Jahr in die Zukunft verschoben hat.

DURCHGÄNGIGE VORGEHENSWEISE: Eine durchgängige Vorgehensweise zur Erstellung von Dokumenten von der Anforderungsdefinition, der Analyse, dem Design bis hin zum Roll Out wird in 4 Jahren verfügbar sein.

Die Einsatzgebiete, die für diesen Trend als relevant angesehen werden, sind insbesondere sicherheitskritische Systeme sowie betriebliche Anwendungen bzw. standardisierte Anwendungen wie ERP oder Office-Produkte. Es wurde zudem angemerkt, dass die Dokumentation insbesondere bei umfangreichen und komplexen Systemen von besonders hoher Bedeutung sei, wobei dies nicht bedeute, dass eine gute durchgängige Dokumentation bei individuellen und proprietären Anwendungen vernachlässigt werden könne. Probleme sehen die Experten beispielsweise in der mangelnden Kompatibilität der Entwicklungsdokumente.

Die Voraussetzungen einer derartigen Vorgehensweise und Dokumentation sind wie folgt charakterisiert: Die Vorgehensweise muss unabhängig von der Entwicklungsinfrastruktur, welche durch bestehende Technologien, Methoden und Werkzeuge charakterisiert sind, sein. Zudem ist es erforderlich, dass es Organisationen gibt, die verwendbare Standards defi-

nieren und deren Durchsetzung fördern. Ebenso sind Werkzeuge notwendig, die eine derartige Dokumentation phasenübergreifend implementieren. Flexible Metamodelle der Dokumentenstrukturen bilden die Basis dieser Integration. Für die erforderliche Dokumentenstruktur und die darauf aufbauende Vorgehensweise sollte über Werkzeuge oder Leitlinien eine Anpassung für unterschiedliche Projektarten möglich sein.

NACHVOLLZIEHBARKEIT: Die Entwicklungsdokumentation ermöglicht in 5 Jahren die Nachvollziehbarkeit und konsistente Änderbarkeit von Systemanforderungen über den gesamten Entwicklungsprozess.

KUNDENINTEGRATION: Es ist in 2 Jahren weit verbreitet, den Kunden im Bereich Auftragssoftware während des gesamten Entwicklungsprozesses einzubeziehen.

Da es sich um eine sehr strenge und standardisierte Form der Softwareentwicklung handelt, ist es erforderlich, dass diese Vorgehensweise von den Mitarbeitern akzeptiert und angenommen wird. Trotz der enormen Komplexität, die eine durchgängige Methode bei komplexen Softwaresystemen hätte, müsste diese überschaubar und trotzdem leicht anwendbar sein.

Zusätzlich wurde untersucht, wie die Experten die Entwicklungen im Bereich der Nachvollziehbarkeit der Entwicklungsdokumentation einschätzen. Hierzu wurde untersucht, wann die Entwicklungsdokumentation eine nachvollziehbare und konsistente Änderbarkeit von Systemanforderungen über den gesamten Entwicklungsprozess ermöglichen wird. Diese Entwicklung erwarten die Experten in fünf Jahren. Dabei reicht der Zeithorizont von heute bis in zehn Jahren (vgl. Abbildung 8.94, ②). Im Vergleich zur Vorgängerstudie verschiebt sich der Erwartungswert dieser These weiter in die Zukunft.

Die Nachvollziehbarkeit der Dokumentation ist zwar insbesondere sinnvoll in komplexen und insbesondere sicherheitskritischen Software-Systemen, dennoch wird der Bedarf nach Nachvollziehbarkeit grundsätzlich bei allen Systemklassen gesehen. Zusätzlich wurde angemerkt, dass die Realisierung aufgrund mangelnder Schnittstellen und oftmals aufgrund mangelnder Projektressourcen nicht umgesetzt werden können.

Damit die Nachvollziehbarkeit der Entwicklungsdokumentation adäquat umgesetzt werden kann, sind nicht nur der Einsatz standardisierter Beschreibungstechniken und Entwicklungswerkzeuge, sondern auch intelligente Modellierungskonzepte, die Systemänderungen automatisch mitverfolgen und dabei aufkommende Konflikte beheben können, bis hin zu standardisierten Vorgehensweisen, die von den Entwicklern angenommen und umgesetzt werden, notwendig. Hinzu kommt, dass Systeme prinzipiell eher deskriptiv und funktional ausgelegt sein müssen, da ansonsten die Garantie der Konsistenz nur schwer nachweisbar ist.

Ein weiterer Aspekt der in zahlreichen Software-Entwicklungsprojekten ungeklärt ist, ist der Aspekt der Kundenintegration. Im Rahmen dieser Studie wurde die Sinnhaftigkeit der Kundenintegration diskutiert. Dabei wurden die Experten mit der These konfrontiert, ab wann mit einer Verbreitung der Einbeziehung von Kunden in den gesamten Entwicklungsprozess gerechnet werden kann. Das Eintreten dieser These wird von Experten in zwei Jahren, d.h. 2005 erwartet (vgl. Abbildung 8.94, ③). Eine Aufschlüsselung in die jeweiligen Expertengruppen gibt dabei weiteren Aufschluss bei der Interpretation der Bewertung. Bei einer differenzierten Betrachtung der Expertenmeinungen zeigt sich, dass die Meinungen insgesamt deutlich voneinander abweichen. So erwarten die Experten aus der Wissenschaft diese Entwicklung bereits in zwei Jahren, während die Experten aus der Industrie diese erst in fünf Jahren erwarten. Bei der Vorgängerstudie lag die Erwartung im Jahr 2008. Folglich fällt die Erwartung in dieser Studie deutlich optimistischer aus. Dies liegt nicht zuletzt daran, dass der Notwendigkeit der Kundenintegration heute ein höherer Stellenwert eingeräumt wird, als in der vergangenen Studie.

Die Kundenintegration ist insbesondere bei Systemen sinnvoll, bei denen eine ständige Änderung der Anforderungen zu erwarten ist. Dies ist oftmals bei kleiner und mittelgroßer Software oder Individualsoftware der Fall. Die Integration ist immer zur Validierung und Meilensteinprüfung in Prozessen sinnvoll, die Änderungen von Anforderungen unterstützen.

Methodisch wird vorausgesetzt, dass geeignete Beschreibungen der Systeme zur Verfügung stehen, wie Metaphern oder Designmustern [BDRS 97], die eine Abstraktion von komplizierten technischen Details ermöglichen und die über Werkzeuge verwaltet werden können. Aus Sicht der Vorgehensweise erfordert dies sehr flexible Prozesse wie sie beispielsweise im Bereich des Extreme Programming vorherrschen.

Neben der Kundenintegration, die insbesondere die Sicherstellung der Umsetzung von Anforderungen zum Ziel hat, ist ein weiteres Mittel zur Qualitätssicherung die Anwendung von Usability Tests. Dabei wurde evaluiert, wann Rapid Prototyping und Usability Tests zur systematischen Validierung der Kundenanforderungen eine weite Verbreitung finden werden. Es hat sich gezeigt, dass die befragten Experten diese Entwicklung in vier Jahren erwarten. Dabei wird ein Zeithorizont angegeben, der von heute bis in sechs Jahren reicht. Die Erwartung der Experten aus der Wissenschaft ist dabei mit drei Jahren positiver als die der Experten aus der Industrie mit fünf Jahren. Diese Einschätzung bestätigt bis auf sehr geringe Abweichungen die Ergebnisse der letzten Studie (vgl. Abbildung 8.94, ④).

Usability Tests sind nach Meinung der Experten bei innovativen Systemen von besonderer Bedeutung. Auch im Bereich der Produktentwicklung spielt Usability eine herausragende Rolle. Hervorgehoben werden in diesem Zusammenhang die Bereiche der Entwicklung grafischer Benutzeroberflälchen, von Individualsoftware oder der Entwicklung und Verbindung von Schnittstellen. Kritisch wird in diesem Zusammenhang angemerkt, dass die Kundenintegration prinzipiell sinnvoll ist, es aber in vielen Fällen problematisch ist, diese Anforderungen den Kunden verständlich zu machen. Hierzu sind insbesondere die Installation entsprechender Prüfmechanismen erforderlich. Dabei kann es sich beispielsweise um Prüfstände oder Simulationen handeln, anhand derer der Kunde die Software testen kann. Ebenso ist der Einsatz komfortabler Prototyping-Werkzeuge unverzichtbar. Dies schließt insbesondere die Einbindung von Methoden zur Testfallgenerierung mit ein.

Im Gegensatz zur Vorgängerstudie wurde in dieser Studie zusätzlich evaluiert, welche Phasen der Entwicklung heute bzw. in den kommenden Jahren bei der Softwareentwicklung besonders relevant sein werden. Dabei wurde insbesondere gefragt, wie groß der Anteil unterschiedlicher Entwicklungsaktivitäten wie dem Requirements Engineering oder der Qualitätssicherung am gesamten Entwicklungsprozess sind. Es zeigen sich insbesondere folgende Entwicklungen (vgl. Abbildung 8.95):

Die Anforderungsanalyse wird deutlich von einem derzeitigen Anteil von elf Prozent am Entwicklungsprozess auf 23 Prozent ansteigen. Der Anteil des Designs wird derzeit insgesamt auf 16 Prozent eingeschätzt mit einer steigenden Tendenz in der Zukunft. Langfristig wird ein Anteil von 22 Prozent erwartet. Die Implementierung wird deutlich an Anteilen verlieren. Derzeit wird der Implementierungsaufwand mit 36 Prozent des Gesamt-Entwicklungsprozesses angegeben. Dieser wird sich langfristig auf 20 Prozent reduzieren. Die Qualitätssicherung wird sich von derzeit 15 Prozent geringfügig auf 19 Prozent erhöhen, die Installation und Wartung hingegen wird sich geringfügig von derzeit 23 Prozent auf 20 Prozent reduzieren.

Zur Entwicklung der Anforderungsanalyse wurde kommentiert, dass diese unter anderem davon abhängen wird, welche Werkzeuge für die Beschreibung und Integration von Anforderungen verfügbar sein werden. Die Notwendigkeit für diese Entwicklung zeigt sich insbesondere darin, dass Anforderungen immer flexibler werden und somit die Änderungsdynamik steigt. Eine traditionelle Integration von Änderungsanforderungen erfordert das Durchlaufen des gesamten Prozesses mit dem Schwerpunkt auf der Phase der Implementierung. Die Aktivitäten werden sich im Gegensatz dazu künftig verstärkt auf die frühen Phasen der Softwareentwicklung verlagern, während die späteren Phasen stärker automatisiert ablaufen, wodurch die Dynamik einfacher in den Entwicklungsprozess integriert werden kann.

Beim Design werden generell zwei gegenläufige Entwicklungstendenzen gesehen: Zum Einen wird aufgrund der zunehmenden Integration von Software-Komponenten in der Entwicklung ein Rückgang der Design- Aktivitäten prognostiziert, zum Anderen fördert die steigende Tendenz zu automatisch generiertem Code eine Verlagerung der Entwicklungsaktivitäten von der Implementierung auf das Design. Dies wird insgesamt unterstützt durch eine damit eng verbundene, ausführlichere und umfangreichere Dokumentation. Die Erwartung zeigt allerdings insgesamt, dass tendenziell mit einer Erhöhung der Aktivitäten in der Phase des Designs zu rechnen ist (vgl. Abbildung 8.95).

RAPID PROTOTYPING UND USABILITY TESTS: Eine weite Verbreitung von Prototyping und Usability Tests zur systematischen Validierung der Kundenanforderungen wird in 4 Jahren erwartet.

ENTWICKLUNGSAKTIVITÄTEN: Der Anteil der Entwicklungsaktivitäten in den unterschiedlichen Entwicklungsphasen wie dem Requirements Engineering oder der Implementierung werden sich in den kommenden Jahren deutlich verändern. Requirements Engineering, Design und Qualitätssicherung gewinnen z.T. massiv an Bedeutung, während die Implementierung gravierend an Bedeutung verliert. Auch die Wartung und Installation wird tendenziell an Bedeutung abnehmen.

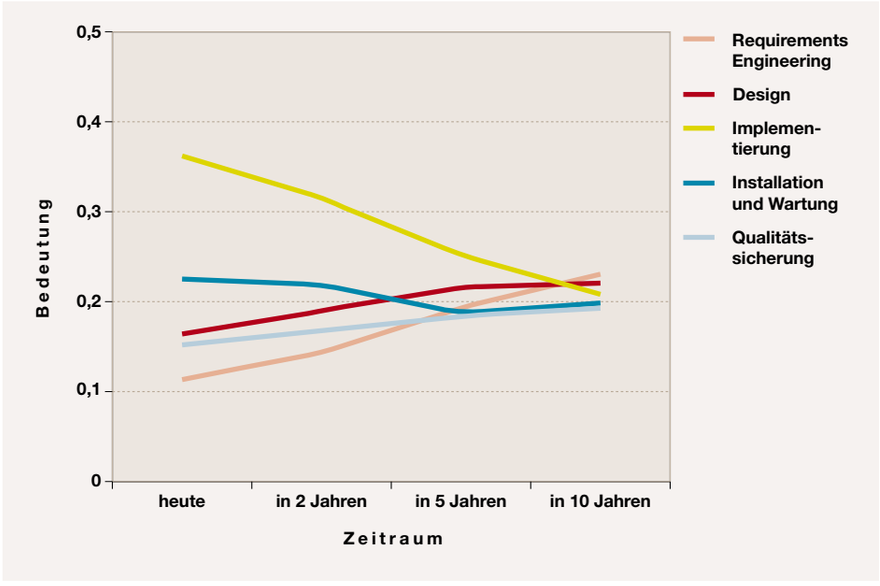



Abbildung 8.95: Zuwachs der Entwicklungsaktivitäten unterschiedlicher Entwicklungsphasen

ERHÖHUNG DER BENUTZERFREUNDLICHKEIT: Deutliche Potenziale zur Erhöhung der Benutzerfreundlichkeit sind insbesondere durch intuitive Bedienbarkeit (wie Metaphern), Online-Hilfen sowie durch die Definition von Benutzerprofilen gegeben.

Dazu kommt, dass die Phase des Designs durch neue Techniken wie Designmuster oder moderne Entwicklungsmethoden immer beherrschbarer wird, was insbesondere auf die mit den Mustern verbundene Reduktion der Komplexität zurückgeführt werden kann. Dies sind unter anderem Erklärungen für den moderaten Anstieg der Designaktivitäten.

Die Implementierung wird aufgrund von Weiterentwicklungen im Bereich der Codegenerierung, der Weiterentwicklung und Definition weiterer Standards sowie der zunehmenden Durchdringung von Componentware deutlich abnehmen.

Die Testaktivitäten werden sich ausweiten und insbesondere frühe Phasen der Softwareentwicklung stärker mit einbinden. Die Integration von Komponenten sowie die steigende Automatisierung wird den QS-Aufwand reduzieren. Insbesondere bei der Entwicklung von Komponenten werden QS-Aktivitäten deutlich ansteigen.

Die Prognose im Bereich Wartung und Installation kann nur schwer eingeschätzt werden, da dies sehr stark vom Projekt- und Softwareumfang abhängt.

Es wurde zusätzlich diskutiert, welche Möglichkeiten der Erhöhung der Benutzerfreundlichkeit künftig eine Rolle spielen werden. Dabei haben sich die in Abbildung 8.96 beschriebenen Entwicklungen ergeben. Die untersuchten Merkmale waren in diesem Zusammenhang die intuitive Bedienbarkeit (beispielsweise durch die Integration von Metaphern), die methodische Unterstützung durch Vorschläge und Simulationen, Online-Hilfen (über Text, Video und Audio), Reduktion des Funktionsumfangs sowie verschiedene Benutzerprofile (wie beispielsweise Experten und Laien).

Es hat sich herausgestellt, dass insbesondere die beiden Eigenschaften der intuitiven Bedienbarkeit sowie unterschiedliche Benutzerprofile künftig eine große Bedeutung erlangen werden. Dabei unterscheidet diese beiden Entwicklungen, dass für beide Eigenschaften ein geringfügig unterschiedliches Ausgangsniveau gilt. So wird der intuitiven Bedienbarkeit heute bereits ein höherer Stellenwert eingeräumt, während dies bei den Benutzerprofilen derzeit nicht der Fall ist. Eine methodische Unterstützung durch Vorschläge und Simulationen hat ebenfalls eine steigende Tendenz und wird langfristig eine große Bedeutung erlangen. Der Verlauf entspricht dem der Benutzerprofile, jedoch mit insgesamt geringerer Bedeutung. Die Reduktion des Funktionsumfangs wird von den Experten nicht als relevant eingestuft, obwohl der Bedeutungs-

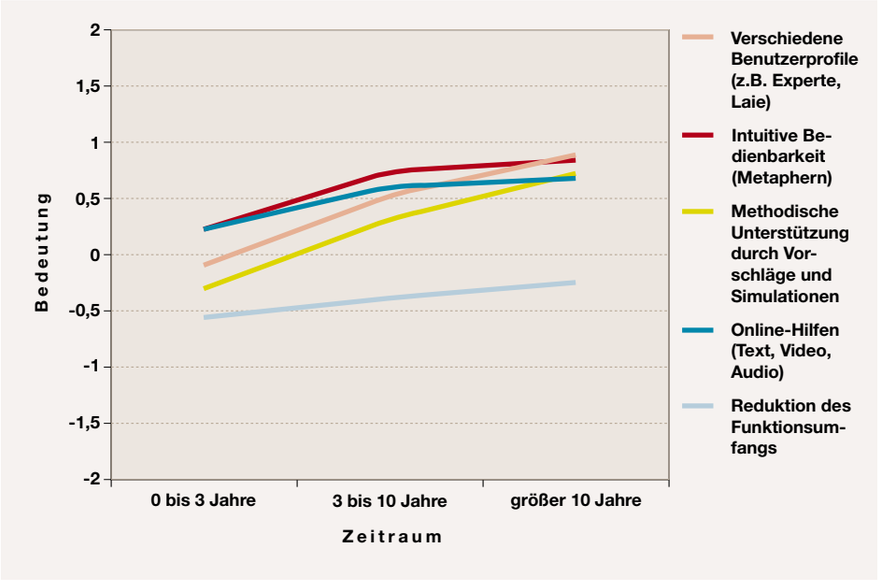



Abbildung 8.96: Bedeutung von Eigenschaften zur Erhöhung der Benutzerfreundlichkeit

verlauf tendenziell steigend ist. Die Angabe sonstiger Eigenschaften zeigt darüber hinaus, dass einem Bedarf zusätzlicher Eigenschaften keine große Bedeutung beigemessen wird.

### Zusammenfassung

Im Bereich der Systematisierung der Entwicklungsdokumentation haben sich folgende Ergebnisse herausgestellt:

- Eine über alle Entwicklungsphasen durchgängige Entwicklungsdokumentation wird bis zum Jahr 2007 verfügbar sein.
- Mit der Nachvollziehbarkeit der Entwicklungsdokumentation wird bis 2008 gerechnet.

Im Bereich der Evaluierung von Kundenanforderungen werden folgende Ergebnisse prognostiziert:

- Es wird eine deutlich stärkere Integration des Kunden am Entwicklungsprozess und insbesondere bei der Sicherstellung der Anforderungsintegration geben. Dieses Vorgehen wird bis 2005 verbreitet sein.
- Zusätzlich werden sich Usability Tests bei der Software- und Systementwicklung durchsetzen. So können Kundenanforderungen systematisch validiert werden. Diese Art der Qualitätssicherung wird bis 2007 weit verbreitet sein.

## 8.4.3 Integration und Anwendung von Beschreibungstechniken

Die Bedeutung und Notwendigkeit von formalen und grafischen Beschreibungstechniken im Softwaredesign ist inzwischen unumstritten. Dies zeigt insbesondere die weite Verbreitung von Modellierungssprachen wie UML. Grundsätzlich eignen sich nach [SETIK 00, BDJ+ 99, GKRB 96, BDD+ 92] Beschreibungstechniken insbesondere zur Erfassung, Analyse, Definition und Dokumentation von Kundenanforderungen. Ferner können sie zur Evaluierung von Konsistenz- und Korrektheitseigenschaften bei der Spezifikation von Systemen verwendet werden. Somit dienen sie insbesondere zur Kommunikation zwischen Systemanalytikern und Systemanwendern. Dies ist jedoch nur dann sinnvoll, wenn eine Abstimmung zwischen der Beschreibungstechnik zur Modellierung von Systemen und der Implementierung stattfindet.

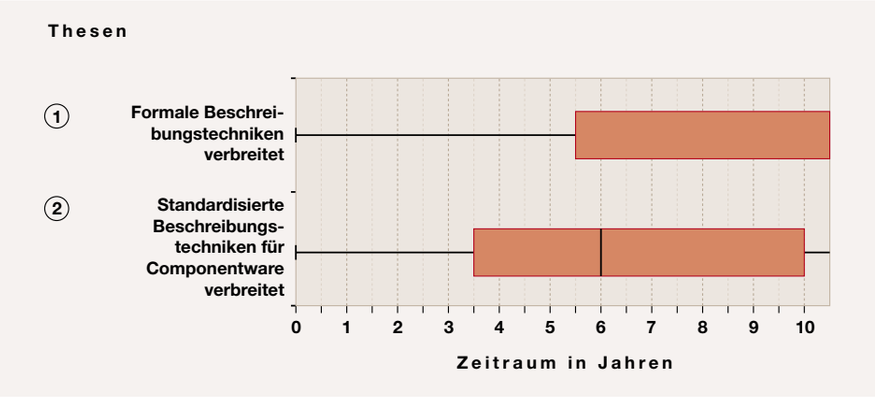



Abbildung 8.97: Ergebnisse der Thesen zur Integration und Anwendung von Beschreibungstechniken

FORMALE BESCHREIBUNGSTECHNIKEN: Eine weite Verbreitung formaler Beschreibungstechniken mit präziser Syntax und Semantik zur Entwicklung von Software wird langfristig nicht erwartet.

Über grafische Beschreibungstechniken können nach [Berg 97] komplexe Zusammenhänge einfach veranschaulicht werden. Dies resultiert nach [Endr 96] insbesondere aus der Fähigkeit des Menschen, die Bandbreite des visuellen Kanals und seine Fähigkeit zur assoziativen Mustererkennung auszunutzen und einen wahlfreien Zugriff zu gestatten. Hinzu kommt, dass sich Beziehungen zwischen Elementen in zwei Dimensionen prinzipiell einfacher notieren lassen, als bei einer rein textuellen, eindimensionalen Darstellung.

In diesem Abschnitt stehen insbesondere Trends und Thesen im Vordergrund, die sich auf die Anwendung formaler und grafischer Beschreibungstechniken als Hilfsmittel bei der Softwareerstellung beziehen. Bislang ist noch immer ungeklärt, in welchen Bereichen der Softwareerstellung sich formale und grafische Beschreibungsmittel eignen. Aus diesem Grund erfolgt in dieser Studie eine ausführliche Diskussion, in welchen Phasen der Softwareentwicklung der Einsatz der angeführten Beschreibungstechniken sinnvoll ist.

## Ergebnisse

Zunächst wurde untersucht, ob sich formale Beschreibungstechniken weiter bei der Entwicklung von Software durchsetzen werden. Im Einzelnen wurde untersucht, ab welchem erwarteten Zeitraum formale Beschreibungstechniken mit präziser Syntax und Semantik weit verbreitet bei der Entwicklung von Software eingesetzt werden. Es zeigt sich, dass diese These nach Aussage der befragten Experten in mehr als zehn Jahren erst zutreffen wird (vgl. Abbildung 8.97, ①). Ein Vergleich mit der Vorgängerstudie ist nicht direkt möglich. In der letzten Studie wurde nach einer weiten Durchdringung von formalen Beschreibungstechniken am Beispiel der UML gefragt. Dabei hat sich gezeigt, was inzwischen Wirklichkeit geworden ist, nämlich dass bis heute eine weite Verbreitung dieser Technologie stattgefunden hat. In dieser Studie wurde allerdings die Frage ausgeweitet nach generellen Formalismen. Dabei zeigt sich eine deutlich vorsichtigere Einschätzung.

Beschreibungstechniken bieten vorwiegend Hilfestellungen bei der Strukturierung komplexer Software, sowie der Gewährleistung von Sicherheitseigenschaften insbesondere bei sicherheitskristischen Systemen an. Bei den letztgenannten Systemen sollte es sich allerdings aus Gründen der Verifizierbarkeit um kleine abgeschlossene Einheiten, wie beispielsweise die Bremssteuerung oder Motorsteuerung in einem Automobil, handeln. Potenziale werden auch im Bereich der Daten-, Funktions- und Prozessmodellierung sowie der Steuerungs- und Regelungstechnik im Allgemeinen gesehen.

Die erforderlichen Technologien sind zunächst Werkzeuge, welche die Realisierung der Beschreibungstechniken ermöglichen. Zudem sind Spezifikationen der Beschreibungstechniken erforderlich, die einfach zu verstehen und anzuwen-

den sind. Die Standardisierung von Sprachen und Werkzeugen wird ebenfalls als Erfordernis genannt, wie beispielsweise VDM, Z, OCL (Object Constraint Language) [IBM 03b] oder Doors. Abstraktion ist gleichermaßen eine wichtige Voraussetzung zur Integration von ausdrucksstarken Formalismen.

Wie im vorangegangenen Abschnitt beschrieben, sind in besonderer Weise Beschreibungssprachen zur Nutzung von Komponenten und zu deren Integration in den Entwicklungsprozess erforderlich. In diesem Kontext wurde evaluiert, wann mit entsprechend spezifischen und standardisierten Beschreibungstechniken für Softwarekomponenten zu rechnen ist. Es zeigt sich, dass standardisierte Beschreibungstechniken für Componentware erst in sechs Jahren erwartet werden (vgl. Abbildung 8.97, ②). Die Prognose der Experten aus der Wissenschaft sind dabei mit sieben bis acht Jahren deutlich pessimistischer als die der Experten aus der Industrie mit fünf bis sechs Jahren.

Die Anwendungen der beschriebenen Techniken sind insbesondere bei komplexen Softwareprojekten zu sehen. Es wird von den Experten insbesondere auf die hohe Effizienz bei der Nutzung von Komponenten sowie die mit den Komponenten verbundene Qualitätssicherung hingewiesen (vgl. Abschnitt 8.4.1). Die Anwendung von Beschreibungstechniken zur Integration von Softwarekomponenten erfordert jedoch die Verfügbarkeit von Werkzeugen zur Spezifikation. Darüber hinaus werden Technologien wie UML oder XML/XMI als sinnvoll für die Modellierung angesehen. Alle aufgeführten Technologien müssen von den Firmen, die Komponenten nutzen möchten, sowohl in ihrer Infrastruktur, als auch in ihrer Organisation, beispielsweise durch Schulungen der Mitarbeiter, eingeführt werden.

Weiterhin wurde untersucht, inwieweit die einzelnen Entwicklungsphasen von am Markt verfügbaren Beschreibungstechniken unterstützt werden. Dabei wurde evaluiert, welche Beschreibungstechniken sich besonders zur Dokumentation in den unterschiedlichen Phasen der Softwareentwicklung eignen. Dabei haben sich die in Abbildung 8.98 illustrierten Zuordnungen ergeben. In der Abbildung sind auf der Abszissenachse die unterschiedlichen Entwicklungsphasen zu sehen angefangen mit dem Requirements Engineering über das Design bis hin zur Installation und Wartung. Diesen Phasen werden auf der Ordinatenachse jeweils unterschiedlichen Beschreibungstechniken gegenübergestellt. Die Größe der an den Schnittpunkten angetragenen Kreise ergeben die Bedeutung einer Beschreibungstechnik für die jeweilige Entwicklungsphase.

Zunächst zeigt sich, insbesondere in den frühen Phasen der Softwareentwicklung, dass UML mit ihren Use Cases sowie natürliche Sprache besondere Bedeutung besitzen. In der Phase der Realisierung, d.h. bei Design und Implementierung sind andere Techniken wie Klassendiagramme, Statecharts oder SDL (Specification and Description Language) [IEC 03] zu favorisieren. Im Bereich der Qualitätssicherung sind insbesondere die Techniken UML oder die Verwendung natürlicher Sprache zu nennen. Bei der Wartung und Installation verlieren alle Beschreibungstechniken bis auf die natürliche Sprache an Bedeutung.

BESCHREIBUNGSTECHNIKEN FÜR SOFTWAREKOMPONENTEN: Eine weite Verbreitung standardisierter Beschreibungstechniken für Softwarekomponenten wird in 6 Jahren erwartet.

DOKUMENTATION IN DEN UNTERSCHIEDLICHEN PHASEN DER SOFTWAREENTWICKLUNG: UML und natürliche Sprache in den frühen Phasen der Softwareentwicklung, UML, Klassendiagramme und Statecharts in den Realisierungsphasen sowie natürliche Sprache in den Phasen der Qualitätssicherung und des Roll Out.

## Zusammenfassung

Für dieses Themenfeld haben sich bei der Befragung die nachfolgende Aussagen ergeben:

- Die befragten Experten rechnen mit einer weiteren Durchdringung formaler Beschreibungstechniken mit einer präzisen Syntax und Semantik bis 2008.

- Durch den zunehmenden Trend zu Komponentenorientierung werden sich bis 2009 insbesondere Beschreibungstechniken für Componentware am Markt durchsetzen.

- Es hat sich gezeigt, dass sich formale Beschreibungstechniken insbesondere in den früheren Phasen der Entwicklung zur Dokumentation eignen. Interessant ist hierbei auch, dass die Experten der natürlichen Sprache in den meisten Fällen eine sehr große Bedeutung beigemessen haben (siehe auch Abschnitt 8.1.5).

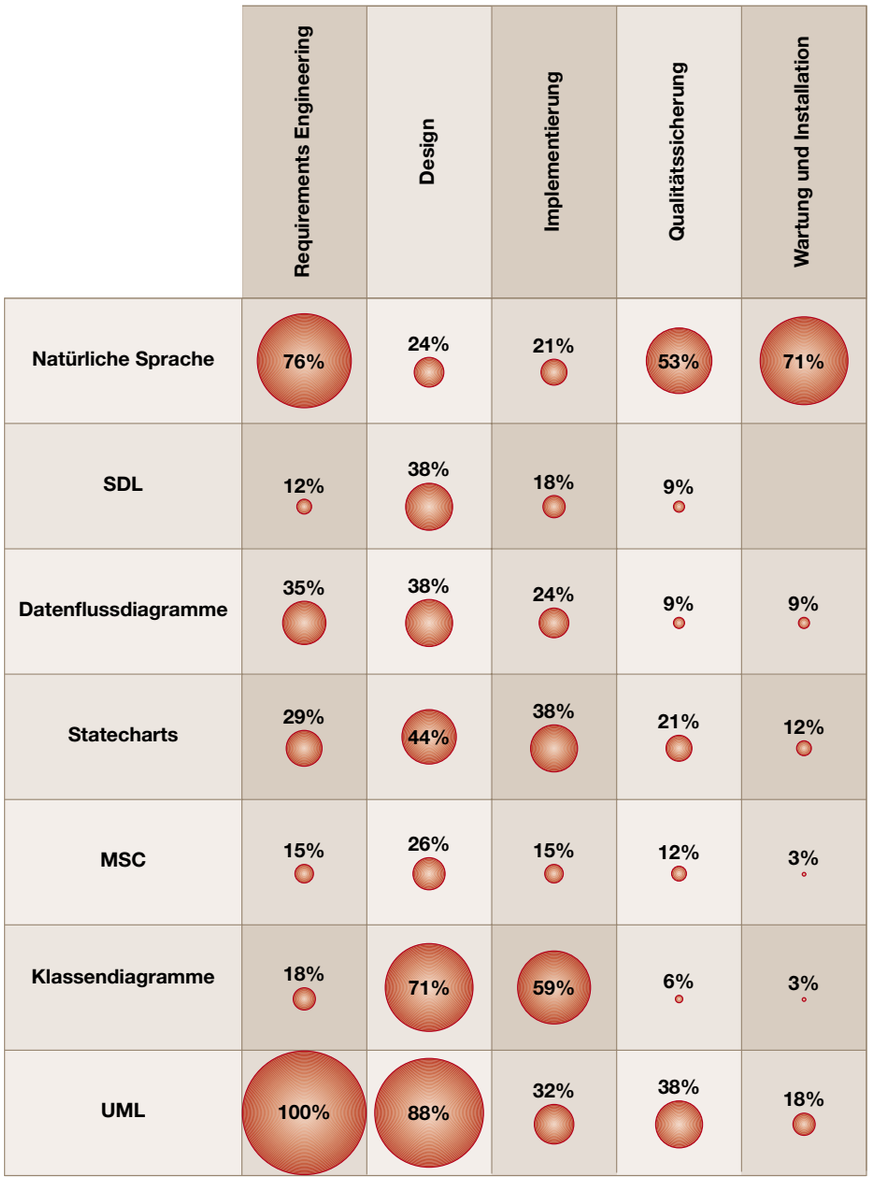



Abbildung 8.98: Ergebnisse der Gegenüberstellung des Unterstützungsgrades von Beschreibungstechniken und Entwicklungsphasen im Software Engineering

### 8.4.4 Bedeutung von Qualitätssicherungsmethoden

Die Qualitätssicherung schließt sich traditionell in der Softwareentwicklung an die Implementierung an und bezieht sich vorwiegend auf ausführbaren Code [Somm 92]. Moderne Ansätze weichen dies auf und fordern zudem, die Qualitätssicherung auch auf andere Entwicklungsdokumente außer Code zu beziehen sowie bereits in frühen Entwicklungsphasen mit der Qualitätssicherung, beispielsweise der Anforderungen, zu beginnen [Raus 01, BGH+ 98, BrSl 99, Beck 00]. In diesem Teil der Studie werden ausschließlich die Qualitätssicherungsmethoden Tests und Verifikation zur Sicherung der Qualität diskutiert. Usability Tests und andere alternative Methoden zur Sicherstellung von Kundenanforderungen wurden bereits in Abschnitt 8.4.2 detailliert beschrieben.

Der Unterschied zwischen den beiden eingangs vorgestellten Methoden kann dadurch zum Ausdruck gebracht werden, dass Tests dazu dienen, Fehler zu finden, während die Verifikation dazu dient, die Zuverlässigkeit eines Systems sicherzustellen [Somm 92, Babe 91]. Die gebräuchlichsten Testverfahren sind hierbei black-box-Tests, die das Interaktionsverhalten einer Software testen, sowie white-box-Tests, welche die inneren Strukturen und nicht nur die Schnittstellen einer Software betrachten. Die Verifikation hingegen überprüft, ob ein vorhandenes Programm eine gegebene Spezifikation erfüllt.

Diese beiden Qualitätssicherungsmethoden wurden im Rahmen dieser Arbeit diskutiert. Dabei wurde evaluiert, welche Bedeutung den Tests und der Verifikation im Rahmen der Qualitätssicherung beigemessen wird und welche Entwicklung sich für beide Methoden in den kommenden Jahren einstellen wird. Die Ergebnisse der Auswertung des Bedeutungsverlaufs sind in Abbildung 8.99 beschrieben.

#### Ergebnisse

Für das Software Engineering existieren die beiden bereits eingeführten Methoden der Tests und der Verifikation zur Qualitätssicherung. Im Rahmen dieser Studie wurde untersucht, welchen Anteil die jeweiligen Methoden künftig im Rahmen der Qualitätssicherung haben werden. Diese Prognose ist für die Entwicklung von Werkzeugen oder der Potenzialanalyse interessant. Bei der Untersuchung dieser beiden Methoden haben sich für deren künftige Entwicklung die in der Abbildung 8.99 gezeigten Werte ergeben. Dabei ergibt sich, dass beide Methoden sich fundamental in ihrer Entwicklung voneinander unterscheiden. Eine Betrachtung der Anteile der Qualitätssicherungsmethoden zeigt die derzeit eingeschätzte Verteilung. Demnach wird der Anteil von Testaktivitäten in der Qualitätssicherung derzeit auf etwa 70 Prozent geschätzt. Der Anteil der Verifikation beträgt im Gegensatz dazu nur etwa zehn Prozent. Während der Anteil der Verifikation langfristig auf etwa 18 Prozent wächst, fällt der Testanteil auf prognostizierte 65 Prozent. Dies zeigt künftig insbesondere Potenziale im Bereich der Verifikation.

Es wurde zusätzlich angemerkt, dass die Verifikation trotz des erwarteten Zuwachses dennoch zu komplex und berechnungsintensiv für eine breite Anwendung bei der Qualitätssicherung ist. Daher wird vielfach die größte Anwendung in eher kleinen sicherheitskritischen Softwarebausteinen gesehen. Die effizientere Lösung der Qualitätssicherung ist hingegen der Test. Dieser kann auf beliebige Anwendungen bezogen werden. Insgesamt ist für beide Methoden erforderlich, klare Schnittstellen bei der Entwicklung von Software zu definieren.

#### Zusammenfassung

Die Abschätzung der beiden Qualitätssicherungsmethoden Tests und Verifikation hat ergeben, dass insgesamt die Testaktivitäten langfristig leicht zurückgehen, während sich die Verifikationsaktivitäten in diesem Zusammenhang nahezu verdoppeln. Dennoch wird langfristig erwartet, dass Verifikationstechniken nur in kleinen sicherheitskritischen Softwareteilen eine größere Rolle spielen werden.

QUALITÄTSSICHERUNG: Der Anteil der Tests beträgt derzeit etwa 70%. Dieser Anteil wird langfristig um 5% auf 65% absinken. Im Gegensatz dazu verdoppelt sich der Anteil der Verifikation von derzeit nahezu 9% auf etwa 18%.

FLEXIBILITÄT VON ENTWICKLUNGSWERKZEUGEN: Flexible, unternehmensweite Entwicklungsumgebungen werden in 7 Jahren erwartet.

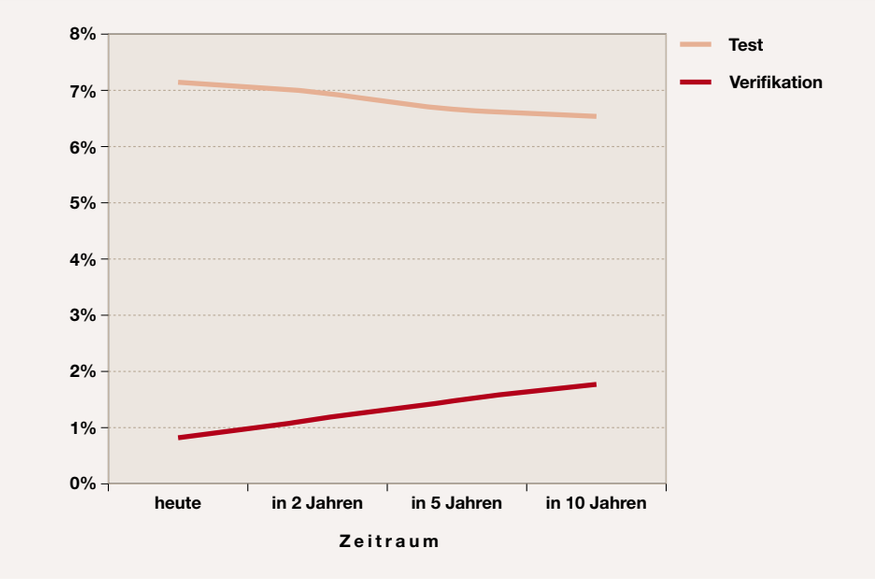



Abbildung 8.99: Anteil von Verifikation und Tests an der Qualitätssicherung

### 8.4.5 Automatisierung des Entwicklungsprozesses

Die Effizienz und Qualität der Softwareentwicklung hängt maßgeblich vom Grad der Automatisierung im Entwicklungsprozess ab. Dabei unterstützen Werkzeuge folgende Zielsetzungen [BeHu 96, GKRB 96, Deif 98a, Endr 96]: die Erhöhung der Produktivität, die Verbesserung der Softwarequalität, die Unterstützung der Prozeßstandardisierung, die Verbesserung der Kommunikation und Dokumentation sowie die Vereinfachung von Abläufen, Systemen oder Software. Die Qualität eines Werkzeuges kann daran gemessen werden, ob und wie es diese Ziele unterstützt und welche Möglichkeiten zur konsistenten Interoperabilität mit anderen Werkzeugen existieren.

Nachdem Werkzeuge oft nur einen Ausschnitt des Entwicklungsprozesses abdecken, ist das Zusammenarbeiten mehrerer unterschiedlicher Werkzeug in einer Entwicklungsumgebung unerlässlich aber nicht wünschenswert. Ein großes Handicap ist dabei, dass oftmals die Schnittstellen sowie die Modelle der einzelnen Werkzeuge nicht miteinander vereinbar und interoperabel sind. Dies ist eine Folge der mangelnden Standardisierung, fehlenden Metamodelle oder proprietärer Werkzeugkonzepte. Trends, die im Bereich der Entwicklungsautomation zu erwarten sind, werden in diesem Teil der Arbeit vorgestellt und diskutiert.

#### Ergebnisse

Eine für viele Software-Entwicklungsprojekte notwendige Anforderung ist die der Flexibilität. Flexibilität von Entwicklungswerkzeugen bedeutet, dass Werkzeuge unterschiedliche Modelle verarbeiten, erweitern oder austauschen können. Dies ist insbesondere dann sinnvoll, wenn unterschiedliche Werkzeuge bei der Softwareentwicklung zum Einsatz kommen. Die Befragung hat ergeben, dass die Experten die Möglichkeit zur Implementierung flexibler Werkzeuge und damit flexibler Entwicklungsumgebungen in sieben Jahren erwarten (vgl. Abbildung 8.100, ①). Im Vergleich zur Vorgängerstudie [SETIK 00] wird das damalige Ergebnis weitgehend bestätigt.

Für einige Experten ist bereits heute ein hohes Maß an Flexibilität realisiert, wenngleich es noch große Potenziale zur Erhöhung der Interoperabilität insbesondere im Bereich phasenübergreifender Werkzeugkopplungen gibt. Handlungsbedarf gibt es dagegen noch im Bereich der In-

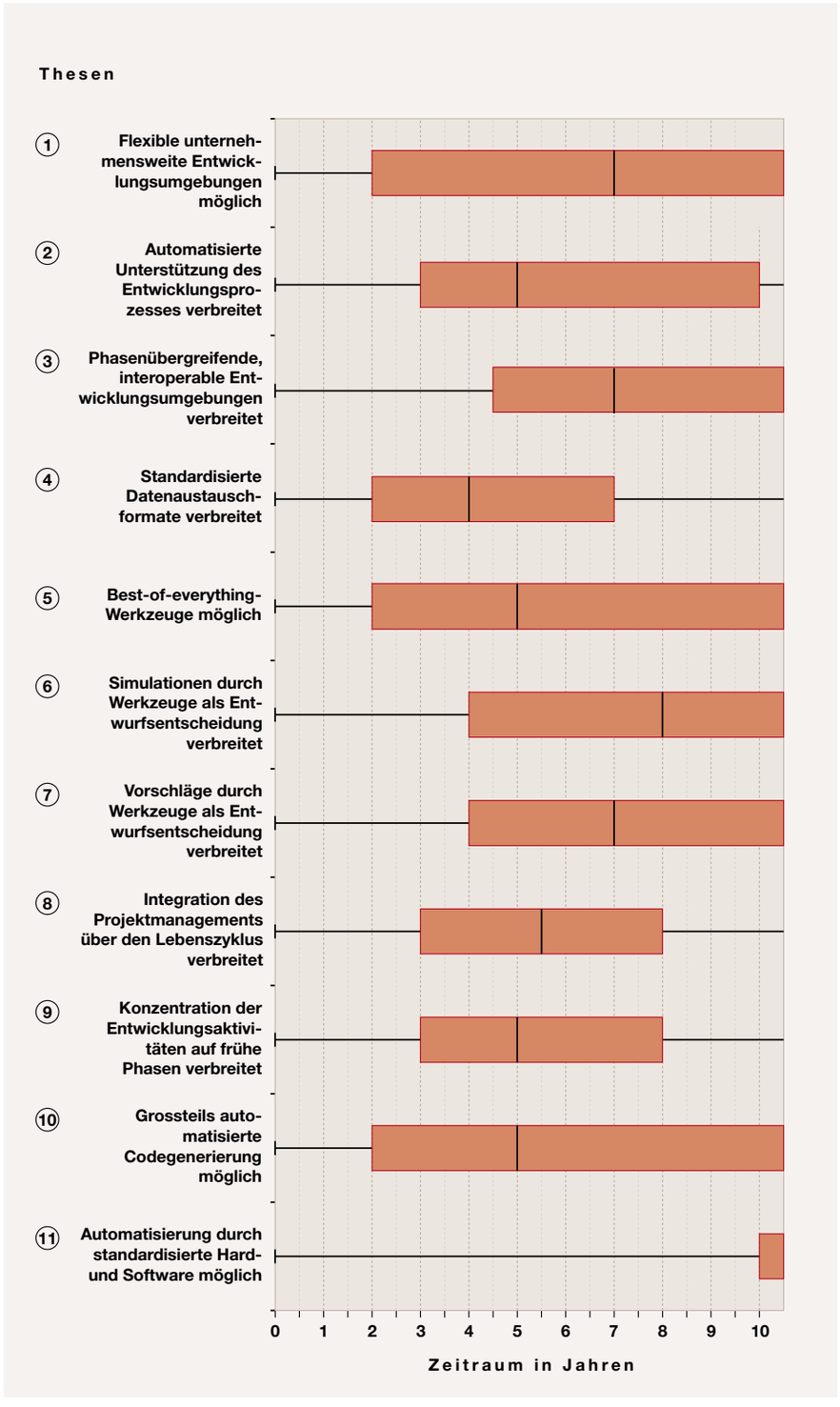



Abbildung 8.100: Ergebnisse der Thesen zur Automatisierung des Entwicklungsprozesses

tegration unterschiedlicher Programmiersprachen, Metamodellen und Designmuster. Es wird allerdings hinzugefügt, dass Anwender künftig vorwiegend Standard-Komponenten bzw. Web Services einsetzen bzw. beanspruchen werden und daher die prinzipielle Bedeutung von Werkzeugen eher zurückgehen wird. Dies bedeutet allerdings eine stärkere Verbreitung von Dienstentwicklungswerkzeugen. Typische Technologien, die in diesem Kontext bei der Integration erforderlich sein werden und von den Experten aufgezählt werden, sind Java-Technologien wie J2EE (Java 2 Platform Enterprise Edition) [Sun 03c] oder Java auf Implementierungsebene oder UML auf Spezifikationsebene. Auch Bibliotheken von Designmustern und ausgereifte Codegeneratoren werden verstärkt erforderlich sein.

UNTERSTÜTZUNG DER ENTWICKLUNG: Eine Verbreitung massiv automatisierter unterstützter Entwicklungsprozesse beispielsweise durch Designmuster wird in 5 Jahren erwartet.

INTEROPERABILITÄT: Entwicklungsumgebungen, die eine Reihe von Transformationen und Konsistenzchecks zwischen den einzelnen Entwicklungsphasen übernehmen werden in 7 Jahren weit verbreitet sein.

STANDARDISIERTE DATEN-AUSTAUSCHFORMATE: Die Verbreitung von standardisierten Datenaustauschformaten (wie XML oder XMI) zum Austausch und zur Verarbeitung von Daten zwischen Werkzeugen unterschiedlicher Hersteller wird in 4 Jahren erwartet.

Neben der Flexibilität ist die automatisierte Unterstützung der Entwicklung beispielsweise durch die Verfügbarkeit und Realisierung von Designmustern ebenfalls von großer Bedeutung. Es wurde deshalb untersucht, wann Entwicklungsprozesse durch diese Muster automatisiert unterstützt werden können. Es zeigt sich, dass die Experten eine Verbreitung dieser methodischen Hilfestellung in fünf Jahren erwarten (vgl. Abbildung 8.100, ②). Der Vergleich zur Vorgängerstudie zeigt, dass sich die Einschätzung nicht korrigiert werden muss. In Folge dessen hat sich seit der letzten Erhebung nach Einschätzung der Experten nicht viel verändert.

Die automatisierte Entwicklungsunterstützung durch Werkzeuge bezieht sich nach Aussage der Experten in besonderer Weise auf die Entwicklung von Oberflächen oder Datenbankanwendungen. Weitere Anwendungen sind im Bereich Standardsoftware aber auch im Anlagenbau oder im Bereich Leitsysteme zu sehen. Aus Sicht der Realisierung sind Technologien wie Datenbanken, CASE-Tools oder Java-Technologien wie J2EE erforderlich. Aus der Perspektive des Vorgehens ist zusätzlich die Identifikation und Abbildung von „Best Practices" auf die Designmuster notwendig. Auch Möglichkeiten zur individuellen Konfiguration von Werkzeugen sind essentiell, um die Interoperabilität zu fördern.

Im Kontext der Flexibilität von Werkzeugen wurde im Detail untersucht, wann mit der Interoperabilität entwicklungsphasenabhängiger Werkzeugfunktionen zu rechnen ist. Die Experten wurden gefragt, wann Entwicklungsumgebungen verbreitet sein werden, bei denen Modell-Transformationen und Konsistenzchecks zwischen unterschiedlichen Entwicklungsphasen standardmäßig umgesetzt sind. Mit dieser Entwicklung kann nach Aussage der Experten innerhalb der nächsten sieben Jahre gerechnet werden. Außerdem erwarten sowohl die Experten aus der Industrie, als auch aus der Wissenschaft diese Entwicklung frühestens in etwa vier Jahren, wobei sie allerdings auch die Möglichkeit offen lassen, dass dies erst in über zehn Jahren der Fall sein kann. Im Vergleich zur Vorgängerstudie wird dieser Trend deutlich vorsichtiger eingeschätzt und die Erwartung verlagert sich um etwa fünf Jahre in die Zukunft (vgl. Abbildung 8.100, ③).

Modelltransformationen zwischen Werkzeugen ermöglichen nach der Aussage der Experten insbesondere die Verkürzung von Entwicklungszeiten und sind somit wünschenswert. Es ergibt sich jedoch das Problem, dass zur Realisierung von Transformationen und Konsistenzchecks formale Modelle erforderlich sind, die heute in seltenen Fällen in Projekten ohne großen Entwicklungsdruck definiert und installiert werden können. Hinzu kommt, dass die Modelle nicht nur syntaktisch harmonisieren müssen, sondern darüber hinaus auch semantisch gleich interpretiert werden müssen. Hierzu ist insbesondere eine Weiterentwicklung in den Bereichen Normung und Standardisierung erforderlich. Aber auch Technologien zur technologieunabhängigen Beschreibung der Modelle, wie beispielsweise XML, sind weiter wünschenswert.

Die Interaktion zwischen unterschiedlichen Werkzeugen setzt die Verfügbarkeit von geeigneten Austauschformaten voraus. Es wurde in dieser Studie evaluiert, bis wann standardisierte Datenaustauschformate am Markt verbreitet sein werden. Dabei hat sich herausgestellt, dass die Experten mit einer Verbreitung in etwa vier Jahren rechnen (vgl. Abbildung 8.100, ④). Die Erwartung schwankt zwischen zwei und sieben Jahren. Im Vergleich zur Vorgängerstudie zeigt sich, dass die Einschät-

zung weitgehend bestätigt wird, jedoch mit zunehmender Unsicherheit.

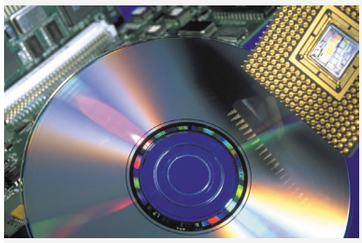
Die Experten sehen als Anwendungspotenziale insbesondere den Datenaustausch zwischen Werkzeugen, den Datenaustausch zwischen komponentenbasierten Anwendungen oder Webanwendungen bzw. den Austausch von Modellen z.B. Klassenmodellen wie sie in der UML verwendet werden. Allerdings besteht hierbei wiederum die Problematik der semantischen Vereinbarkeit. Ein weiteres Anwendungsfeld können innerbetriebliche und zwischenbetriebliche Integrationsszenarien von Geschäftsabläufen sein. Die Basis für diese Anwendungen ergibt sich aus der Existenz und breiten Anwendung einheitlicher Standards, die den Datenaustausch und die Interoperabilität zwischen den verwendeten Werkzeugen regeln. Außerdem müssen diese Standards von den Werkzeugherstellern unterstützt werden.

Durch die Verfügbarkeit herstellerunabhängiger, phasenübergreifender und modellunabhängiger interoperabler Werkzeuge können Entwicklungsumgebungen individuell definiert, konfiguriert und optimiert werdem. Die Summe der dabei entstehenden Werkzeuge wird als Best-of-Everything-Werkzeug bezeichnet. Es wurde evaluiert, wann diese Art der Spezifikation von Werkzeugumgebungen möglich sein wird. Als Ergebnis hat sich gezeigt, dass diese Verfügbarkeit in fünf Jahren prognostiziert wird (vgl. Abbildung 8.100, ⑤). Der erwartete Zeithorizont ist mit zwei bis weit über zehn Jahren allerdings sehr breit gestreut. Somit sind die Aussagen mit einer großen Unsicherheit versehen.

Die Anwendungsfälle von Best-of-Everything-Werkzeugen sehen die Experten differenziert. Einige der Experten sehen die Notwendigkeit dieser Flexibilität vereinzelt bei der Entwicklung von Standardsoftware und deren Herstellern, andere Experten beschreiben generell einen großen Bedarf an Flexibilität, der allerdings aufgrund von Einzelinteressen der führenden Werkzeug-Hersteller nicht bedient werden kann. Dabei werden umfangreiche Konfigurationsmöglichkeiten der Werkzeuge, über normierte Datenaustausch- und Datenspeicherformate, beispielsweise unter Verwendung von XML und XMI, sowie einheitliche Schnittstellen zum Import und Export von gemeinsamen Entwicklungsmodellen, vorausgesetzt.

Neben der Betrachtung technischer Rahmenbedingungen von Entwicklungsumgebungen wurde in diesem Themenkomplex zusätzlich die methodische Unterstützung durch Werkzeuge untersucht. In diesem Zusammenhang sind zwei unterschiedliche Techniken evaluiert worden: zum Einen die Unterstützung durch Simulationen und zum Anderen die Unterstützung durch Vorschläge. Langfristig erwarten die Experten die Verbreitung dieser Unterstützungstechniken. Die Erwartung liegt dabei in sieben Jahren bei den Vorschlägen und acht Jahren bei den Simulationen. Eine Differenzierung in Experten aus der Wissenschaft und Experten aus der Industrie zeigt dass Simulationen weiter in der Zukunft (Industrie: ab sechs Jahren bis weit über zehn Jahren bzw. Wissenschaft: ab drei Jahren bis weit über zehn Jahren) erwartet werden, als Vorschläge (Industrie ab drei Jahren bis weit über zehn Jahren bzw. Wissenschaft ab einem Jahr bis weit über zehn Jahren). Ein Vergleich zur Vorgängerstudie [SETIK 00] zeigt deutliche Unterschiede. Bei den Simulationen hat sich die Einschätzung massiv in die Zukunft korrigiert, während bei den Vorschlägen die Prognose vergleichsweise optimistischer angegeben wurde. Dennoch ist dieser Trend aus heutiger Sicht, wie auch in der vergangenen Studie beschrieben, – wenn überhaupt – langfristig zu erwarten (vgl. Abbildung 8.100, ⑥ und ⑦).

Simulationen sind sehr vielfältig einsetzbar und reichen von der Regelungs- und Steuerungstechnik, über die Oberflächenentwicklung, Performance-Optimierung über die Konstruktion, Fertigung und Logistik, bis hin zu eingebetteten und technischen Systemen im Allgemeinen sowie Datenbanken im Besonderen. Aber auch Internet-basierte Systeme können davon profitieren. Prinzipiell sind Simulationen in allen Bereichen sinnvoll, aber der Aufwand lohnt sich vielfach nicht, nach Meinung der Experten. Die Simulation setzt leistungsfähige Werkzeuge, Codegeneratoren und Plattformen voraus. Vorbilder werden in diesem Zusammenhang in der Automobil- und Luftfahrtindustrie gesehen.



BEST-OF-EVERYTHING-WERKZEUG: Es wird erwartet, dass in 5 Jahren die Installation von Best-of-Everything-Werkzeugen möglich sein wird.

METHODISCHE UNTERSTÜTZUNG DURCH WERKZEUGE: Es wird erwartet, dass Werkzeuge integrierte Simulationen in 8 Jahren verbreitet eingesetzt werden können. Eine Unterstützung durch Vorschläge wird bereits in 7 Jahren verbreitet sein.

Bei der Vorschlagstechnik werden im Bereich der Anwendungen zunächst Regelsysteme und Internet-Applikationen genannt. Aber auch Enterprise Software und Client-Server-Software könnten von Vorschlägen profitieren. Die Potenziale sind insbesondere in der deutlichen Beschleunigung des Entwicklungsprozesses zu sehen. Sinnvoll wäre in diesem Zusammenhang die Existenz umfangreicher Designmustern-Bibliotheken sowie Kodierungsrichtlinien. Ferner setzt eine Nutzung von Vorschlägen Datenbanken voraus, über die in Abhängigkeit von spezifizierten Designmustern und dem verfügbaren Automatisierungsgrad Softwarebausteine ausgewählt werden können. Gleichermassen ist eine problembezogene, automatische Verfügbarkeit von Expertenwissen unverzichtbar. Insgesamt müssen Sammlungen von Designmustern und „Best Practices" in Datenbanken vorhanden sein. Zudem bedarf es geeigneter Semantiken und Algorithmen, über die auf dieses Wissen effizient zugegriffen werden kann. Auch aus dem Bereich der künstlichen Intelligenz können hierzu Ergebnisse beigetragen werden.

INTEGRATION VON PROJEKTMANAGEMENT-ASPEKTEN: Eine Verbreitung von Projektmanagement-Aspekten in Entwicklungswerkzeugen über alle Entwicklungsphasen hinweg wird in 5 bis 6 Jahren erwartet.

VERLAGERUNG DER ENTWICKLUNGSAKTIVITÄTEN: Es wird in 5 Jahren erwartet, dass sich die Entwicklungsaktivitäten auf die frühen Phasen der Softwareentwicklung und somit insbesondere auf die Definition und die Spezifikation der Kundenanforderungen verlagern.

Neben technischen Aspekten sind organisatorische Aspekte bei der Softwareentwicklung relevant. Diese beiden Aspekte werden in vielen Fällen getrennt voneinander innerhalb der Disziplinen Projektmanagement und Softwareentwicklung betrachtet. Beispielsweise werden in Vorgehensmodellen wie dem V-Modell oder dem RUP (Rational Unified Process) [Kruc 98] diese Aspekte in unterschiedlichen Vorgehensbausteinen gekapselt. Dennoch gibt es eine starke Relation zwischen diesen beiden Aspekten, da ein effektives und effizientes Management ohne Kenntnis der Software nach Aussage einiger Experten nicht möglich ist. Ebenso wäre eine Entwicklung ohne Einhaltung von organisatorischen Rahmenbedingungen nicht zielführend.

Die aufgezeigten wechselseitigen Abhängigkeiten unterstreichen die Bedeutung der Diskussion der These, wann mit einer Integration von Projektmanagement-Aspekten in Werkzeugen zu rechnen ist. Mit einer derartigen Integration rechnen die Experten in den nächsten fünf bis sechs Jahren (vgl. Abbildung 8.100, ⑧).

Die Integration von Projektmanagementfunktionen spielt nach Meinung der Experten insbesondere dann eine große Rolle, wenn es sich um die Entwicklung großer Software-Systeme handelt. Hervorgehoben wird in diesem Zusammenhang in besonderer Weise komplexe Standardsoftware wie COTS. Bei der Integration organisatorischer Aspekte sollten dabei insbesondere Funktionen des Controllings sowie der Prozessverbesserung, bekannt aus Konzepten wie CMM (Capability Maturity Model) [Dymo 02] oder ISO-Normen (International Organization for Standardization) [ISO 9001] (vgl. Abschnitt 8.4.7), integrieren werden. Von besonderer Bedeutung ist diese Entwicklung bei der verteilten und/oder simultanen Entwicklung von Software.

Voraussetzungen für diese Entwicklung könnte die Verfügbarkeit von integrierten Werkzeugen sein, die entweder auf der Basis von Standards realisiert oder durch führende Hersteller am Markt durchgesetzt werden. Unterstützen würden dies normierte Datenaustauschsprachen wie beispielsweise XMI oder XML. Zudem wäre es in diesem Zusammenhang sinnvoll Artefakte zu beschreiben, welche Projektmanagement-Funktionalitäten in Vorgehensmodells integrieren. Darauf aufbauend sind Metriken zur Bewertung von organisatorischen Projekteigenschaften unerlässlich. Kritisch wird angemerkt, dass die Komplexität bei der Kopplung von Entwicklungswerkzeugen und Projektmanagement-Tools sehr hoch sei und die Verfügbarkeit von flexiblen Metamodellen erfordern würde.

Aus Vorgehenssicht ist die Frage interessant, ob durch die Einführung geeigneter Werkzeugkonzepte eine wünschenswerte Verlagerung der Entwicklungsaktivitäten auf frühere Phasen des Prozesses erfolgen kann. Dies führt nach Meinung der Experten zu einer Konzentration der Entwicklungsaktivitäten auf die Realisierung von Anforderungen und wird daher im Kontext der Softwaretechnik als besonders relevant eingestuft, da in Folge dessen Inkonsistenzen im Design und der Implementierung vermieden oder reduziert werden können. Die Experten erwarten, dass diese Verlagerung in fünf Jahren stattfinden wird (vgl. Abbildung 8.100, ⑨). Diese Einschätzung entspricht den Ergebnissen der Vorgängerstudie.

Besondere Bedeutung für die Verlagerung der Entwicklungsaktivitäten auf die frü-

hen Phasen sehen die Experten in kleinen und mittelgroßen, sehr kundenorientierten Projekten. Bei Großprojekten sei der Bezug zur Anforderungsdefinition nicht so sehr auf die frühen Phasen beschränkt, sondern aufgrund evolutorischer [Raus 01] oder iterativer [Nuse 01] Vorgehensweisen zur Erstellung von nachfolgenden Versionen oder Varianten permanent gegeben. Angemerkt wird darüber hinaus, dass der Begriff „frühe Phasen" nicht unbedingt zeitlich einzuordnen ist, sondern sich vorwiegend fachlich auf die Anforderungsdefinition bezieht. Technologien, die eine derartige Entwicklung fördern, sind Komponenten und Designmuster, die bereits im Design und in der Implementierung die Verwendung fertiger Bausteine ermöglichen. Zudem sei die Bedeutung von Codegeneratoren, welche die Generierung von Software für zahlreiche unterschiedliche Programmiersprachen und Entwicklungsplattformen ermöglichen, unerlässlich. Diese Generatoren sollten darüber hinaus auch die Möglichkeit bieten, abstrakte und möglichst semiformal in Prosa spezifizierte Anforderungen in Software umzuwandeln. Softwarekomponenten bieten hierbei eine geeignete Basis, sofern derartig abstrakte Beschreibungen für die Komponenten existieren.

Alle beschriebenen Aspekte beziehen sich vorwiegend auf die aktive Durchführung von Entwicklungsaktivitäten. Die Automatisierung dieser Aktivitäten würde zu einer Erhöhung der Leistungsfähigkeit bei der Erstellung von Software führen.

So wurde die Frage, wann es möglich sein werde, große Teile des Codes automatisch zu generieren mit einem durchschnittlichen Zeithorizont von fünf Jahren beantwortet (vgl. Abbildung 8.100, ⑩). Die Differenzierung nach Experten aus der Industrie und Wissenschaft zeigt gravierende Unterschiede in dieser Einschätzung. Die Experten aus der Wissenschaft bestätigen diese These bereits heute, wenngleich die Erwartung bei drei bis vier Jahren liegt. Experten aus der Industrie sehen eine Bestätigung der These frühestens in zwei eher in fünf bis sechs Jahren. Insgesamt unterscheidet sich die Erwartung im Jahr 2008 von der der Vorgängerstudie [SETIK 00] im Jahr 2005 und führt somit zu einer deutlichen Verschiebung der Prognose in die Zukunft.

Die Möglichkeiten zu einer umfangreichen Codegenerierung werden sehr stark davon abhängen, wie sich die Komponenten- und Compilertechnologien entwickeln. Es ist nach Meinung der Experten zu vermuten, dass dieser Trend bei der Durchsetzung von Komponententechnologien an Bedeutung verliert. Andererseits fördert die Verbreitung mit formalen Techniken, wie Spezifikationstechniken (vgl. UML), die Notwendigkeit zur Automatisierung der Implementierung. Durch die modellbasierte Spezifikation wird die Codegenerierung von der konkreten Programmiersprache abstrahiert.

Von einigen Experten wird das Potenzial der Automatisierung bei komplexen Anwendungen eher gering eingeschätzt, sofern keine Komponenten im obigen Sinn eingesetzt werden. Es wird in diesem Zusammenhang mehrmals erwähnt, dass in spezifischen Bereichen, wie der Entwicklung von Benutzeroberflächen oder Datenbankanwendungen große Potenziale für eine Erhöhung des Automationsgrades existieren. Die notwendigen Technologien ähneln denjenigen der vorigen These. Auch hier werden Designmuster und umfangreiche Codegeneratoren als relevant angesehen. Hinzu kommen allerdings geeignete Repositories, Komponententechnologien sowie flexible und interoperable Entwicklungsumgebungen. Die Tools sollten in diesem Kontext außerdem in der Lage sein, visuelle Programmierung bzw. natürlichsprachliche Beschreibungen stärker zu integrieren. Insbesondere beim Design werden Modellierungswerkzeuge gefordert, welche in der Lage sind, stärker semiformale Beschreibungen zu verarbeiten.

Die Standardisierung von Hard- und Software unterstützt die Vereinfachung von Entwicklungsaktivitäten. Es wurde in diesem Kontext untersucht, ob diese Standardisierung zu einer Erhöhung des Automatisierungsgrades in der Softwareentwicklung führt. Dies ist von den Experten mehrheitlich verneint worden. Im Vergleich zur Studie 2000 fällt diese Einschätzung deutlich pessimistischer aus: In der Vorgängerstudie wurde eine Automatisierung noch mittelfristig erwartet.

AUTOMATION DER CODIERUNG: Die automatische Codegenerierung großer Teile der Software ist in 5 Jahren möglich.

AUTOMATION GROSSER TEILE DES ENTWICKLUNGSPROZESSES: Es wird langfristig nicht erwartet, dass die Standardisierung von Hard- und Software einen standardisierten und großteils automatisierten Entwicklungsprozess ermöglicht.

Grundsätzlich sind Automatisierungspotenziale in allen Anwendungsbereichen und insbesondere im Bereich der eingebetteten Systeme möglich. Ausnahmen bilden dabei lediglich Systeme, für die keine standardisierten Komponenten wirtschaftlich herstellbar sind, beispielsweise im Bereich militärischer Anwendungen oder Anwendungen im Bereich Verkehr oder Raumfahrt.

CASE-TOOLS: Derzeitigen Werkzeugkonzepten wird kurz- und langfristig keine große Bedeutung beigemessen. Der Bedarf wird ebenfalls nicht besonders hoch eingeschätzt.

Es wurden nicht nur konzeptionelle Aspekte untersucht, sondern darüber hinaus auch konkrete Technologien, z.B. CASE-Tools. Von den Experten wird die Bedeutung derartiger Werkzeuge sehr unterschiedlich eingeschätzt. Die Ergebnisse dieser Bewertung sind grafisch in Abbildung 8.101 beschrieben.

Die Ergebnisse zeigen, dass Werkzeugen wie UML/RT (Unified Modelling Language for Real Time) [GBSS 98] und Together [Borl 03] heute und in Zukunft ein großer Stellenwert beigemessen wird. Doors wird von der Bedeutung her heute eher gering eingeschätzt, langfristig hingegen eine größere Bedeutung prognostiziert. Für die restlichen Werkzeuge wird insgesamt eine eher geringe Bedeutung beigemessen. Diese generelle Einschätzung deckt sich tendenziell mit den in der Vorgängerstudie beschriebenen Entwicklungen von CASE-Tools, wenngleich unterschiedliche Werkzeuge evaluiert wurden.

ANTEIL DES AUTOMATISIERUNGSGRADES: Der Anteil der Werkzeugunterstützung wird mittelfristig etwa um 50% zunehmen und sich langfristig mehr als verdoppeln.

Abschließend wurde noch der künftig erwartete Verlauf der Automatisierung abgeschätzt. Dabei wurde hinterfragt, wie groß der Anteil des Automatisierungsgrades, der durch Werkzeuge realisiert wird, gemessen am gesamten Entwicklungsprozess heute, in zwei, fünf und zehn Jahren sein wird. Dabei hat sich gezeigt, dass von einem geschätzten Anteil von derzeit 23 Prozent sich dieser Anteil auf 27 Prozent in zwei Jahren, 36 Prozent in fünf Jahren und 46 Prozent in zehn Jahren erhöhen wird. Tendenziell hat sich der überproportionale Verlauf des Automatisierungsgrades im Vergleich zur Vorgängerstudie [SETIK 00] bestätigt. Der Ergebnisverlauf ist in Abbildung 8.102 grafisch veranschaulicht.

## Zusammenfassung

Die Aussagen im Themenfeld Automatisierung des Entwicklungsprozesses können wie folgt zusammengefaßt werden:

- Es wird bis 2010 damit gerechnet, dass flexible CASE-Werkzeuge verfügbar sind, die dynamisch in heterogene Entwicklungsumgebungen integriert werden können.
- Werkzeuge werden den Entwicklungsprozess methodisch stärker unterstützen beispielsweise durch die Integration von Designmustern unterstützen. Eine weite Verbreitung solcher Werkzeuge wird bis 2008 erwartet.
- Bis zum Jahr 2007 wird mit der Verbreitung von Standard-Formaten zum Austausch von Daten und Modellen zwischen Werkzeugen gerechnet.
- Die Möglichkeit, Best-of-Everything-Werkzeuge zu installieren, wird bis 2008 gegeben sein. Hierbei handelt es sich um Werkzeugverbünde, die sich phasenübergreifend interoperabel installieren und konfigurieren lassen.
- Methodisch werden Werkzeuge bis 2011 die Entwicklung von Software durch die Integration von Vorschlägen und Simulationen deutlich erleichtern und unterstützen.
- Projektmanagementaspekte werden bis 2009 in Entwicklungswerkzeugen phasenübergreifend integriert sein.
- Langfristig, d.h. etwa bis zum Jahre 2009, wird mit einer deutlichen Verschiebung der Entwicklungsaktivitäten auf die frühen Phasen der Entwicklung durch den Einsatz von Werkzeugen gerechnet.
- Zudem wird mit einer deutlichen Erhöhung der Codegenerierung bis 2008 gerechnet. In diesem Zusammenhang wird langfristig ein prozentualer Anteil von knapp 50 Prozent automatisch generierten Codes erwartet.

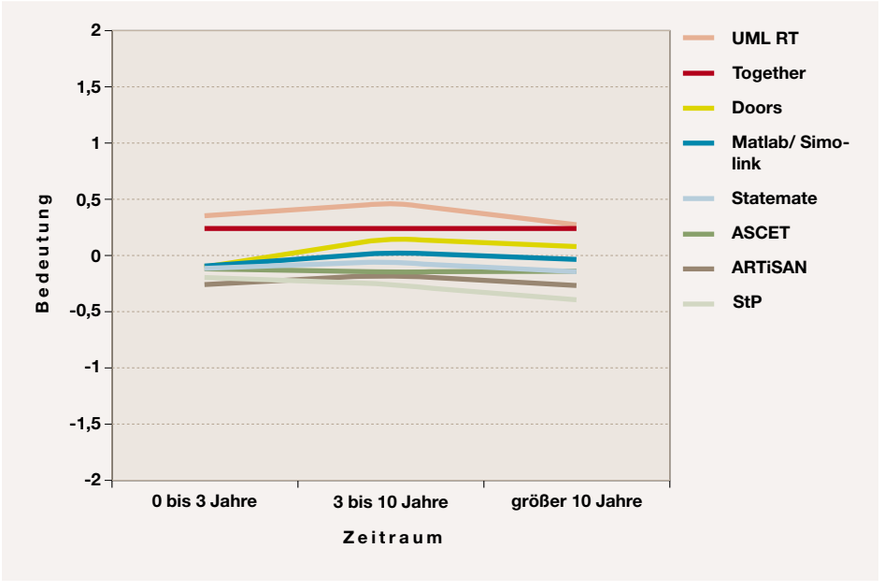



Abbildung 8.101: Bedeutung von Entwicklungswerkzeugen

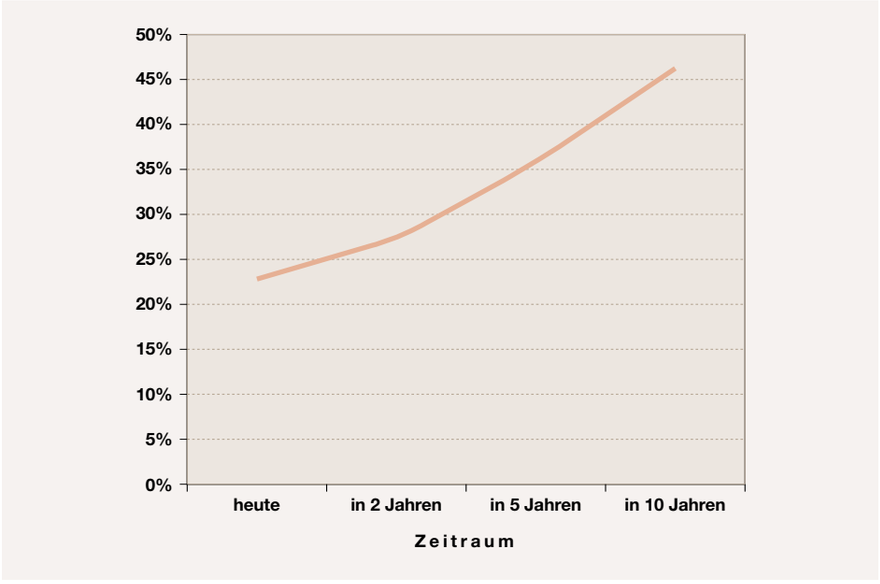



Abbildung 8.102: Zuwachs des automatisch generierten Codes

- Die Standardisierung von Software und Hardware wird langfristig bei der Automatisierung von Entwicklungsprozessen keine besondere Rolle spielen.

- Derzeit verfügbaren CASE-Werkzeugen wird für die Zukunft keine besondere Bedeutung beigemessen. Nur die Werkzeuge UML/RT sowie Together werden als besonders relevant bewertet.

### 8.4.6 Neue Techniken und Paradigmen der Systementwicklung

Heute steckt in einem Mittelklassewagen „mehr Software als in der Apollo 11, die immerhin auf dem Mond gelandet ist" [Haff 02]. Dies vermag ein Bild davon zu geben, mit welcher Dynamik die Entwicklung immer komplexerer Software vor sich gegangen ist. Inwieweit das Softwarevolumen weiterhin ansteigen wird, ist dabei genauso interessant wie die Frage, welche Eigenschaften die Systeme in Zukunft aufweisen müssen, um die Anforderungen des Marktes zu erfüllen. Von Embedded Systems, d.h. der „Einbettung" in Hardware bzw. spricht man, wenn die Software nur einen Teil der Gesamtlösung darstellt [BHS 99]. Eingebettete Systeme sind auf ihre Aufgabe hin maßgeschneidert und meist ist die enthaltene Software gar nicht als solche zu erkennen, wie dies beispielsweise im Fahrzeug bei der Steuerung des Airbag oder der Einspritzpumpe der Fall ist. Eng mit der Einbettung verbunden ist die Eigenschaft der Dynamik, deren Bedeutung für die Softwareentwicklung ebenso stieg wie das bei Mobilität der Fall war. Hier waren v.a. neue Anwendungen in der Telekommunikation die Treiber der Innovationen in der Softwareentwicklung. Generell kann die Zukunft der genannten Bereichen mit der des Internetverglichen werden: hier wie dort fand und findet eine Entwicklung statt von einfachen, statischen Anwendungen hin zu immer komplexeren und dynamischen Systemen.

Neben der Eigenschaft der Reaktivität, für die die Tatsache entscheidend ist, dass das System auf Veränderungen der Umgebung den Anforderungen entsprechend reagiert, werden die Experten auch nach der Bedeutung von Echtzeitfähigkeit gefragt. Diese liegt vor, wenn die einzelnen Verarbeitungsschritte eines Systems innerhalb einer vorgegebenen Zeitspanne ausgeführt werden. Damit hängt bei Realzeitsystemen die Gültigkeit einer Operation nicht nur vom logischen Ergebnis, sondern auch von der dafür benötigten physikalischen Zeit ab. Bei vielen sicherheitskritischen Implementierungen von Echtzeit-(Betriebs-)systemen wird sogenannte harte Echtzeit gefordert, d.h. eine Verletzung der vorgegebenen Reaktionszeit ist nicht tolerierbar. Dies ist beispielsweise bei der Steuerung von Kraftwerken oder medizinischen Geräten der Fall. Haben Echtzeitaufgaben dagegen zwar eine vorgegebene Reaktionszeit, deren Verletzung aber noch nicht sofort weitreichende Folgen hat, spricht man von weicher Echtzeit. Das Ergebnis hat nach der Zeitüberschreitung immer noch einen gewissen Wert, z.B. bei mp3-Playern oder Videokonferenzsystemen.

Weitere Systemeigenschaften, deren zukünftige Bedeutungen evaluiert wurden, sind die Vernetzung über das Internet und die Verteilung. Diese Eigenschaften sind nicht trennscharf, sondern können sich überlappen und/oder werden nicht einheitlich benannt. Die Ergebnisse der diesbezüglichen Fragen zeigen nicht nur, welche Softwaresysteme zukünftig nachgefragt werden, sondern implizit auch, welche Anwendungen an Bedeutung gewinnen werden.

In den letzten Jahren haben sich einige Systemklassen als bedeutende Treiber der Innovationen in jeweils mehreren Technologiebereichen – Datenbanken, Rechnertechnik oder auch Rechnernetze – herausgestellt. Systemklassen umfassen eine Menge individueller Systeme, die sich hinsichtlich ihrer Anwendung bzw. ihres Einsatzgebietes, aber auch bezüglich der geforderten Systemeigenschaften und verwendeten Technologien ähnlich sind. Die Systemklassen, die sich als besonders wichtig bezüglich ihrer Ausbreitung und ihres Einflusses auf andere Bereiche herausgestellt haben, sind Business-Systeme, Integrierte Gebäudesysteme, Systeme im Automotive-Bereich und Telekommunikationssysteme. Unter dem etwas unpräzisen Begriff der Business-Systeme versteht man Anwendungen, die für die Planung, Steuerung und Kontrolle von Un-

ternehmensprozessen eingesetzt werden. In Abschnitt 9.4 wird näher auf Management Information Systeme eingegangen, und Abschnitt 9.5 zeigt, wie solche Systeme Unternehmensabläufe und Organisationsstrukturen verändern werden. Integrierte Gebäudesysteme erledigen die Steuerung der gesamten Haustechnik, des Zutritts und der Arbeitsumgebung. Aus Sicht der Anwender lassen sich hier eine Fülle von Anwendungsmöglichkeiten benennen: durch eine intelligente, vernetzte Klimasteuerung können Energie und Kosten gespart (hier spricht man auch von IHSReWo) und der Komfort erhöht werden. Genauso bieten integrierte Gebäudesysteme älteren oder behinderten Menschen intelligente Unterstützung und damit Möglichkeiten, weiterhin ein selbständiges und angenehmes Leben zu führen. Eine ausführliche Analyse dieser Systeme bietet [IGS 01].

Weniger vielfältig, aber umso schneller, gingen die Veränderungen bei den Systemen im Bereich des Automobils vor sich. Hier sind im wesentlichen drei Einsatzbereiche von Software zu unterscheiden: zur Unterhaltung und Erhöhung des Komforts der Insassen, zur Erhöhung der Wirtschaftlichkeit und/oder Leistung des Fahrzeugs und in Form sicherheitsrelevanter Einrichtungen. Welche der genannten Anwendungen von Softwaresystemen im Bereich Automotive besonders im Interesse der Nachfrager liegen, wurde genauso evaluiert wie die Frage nach der zukünftigen Bedeutung dieser Systemklasse. Sicherheitsfragen werden auch bei Telekommunikationssystemen eine entscheidende Rolle spielen, die zudem noch hohe Anforderungen an die Softwareentwicklung stellen, da meist eine Reihe der oben genannten Systemeigenschaften (v.a. Mobilität, Reaktivität, Realzeitigkeit, Dynamik) erfüllt sein müssen.

Aus diesen Anforderungen ergibt sich ein immer komplexerer Entwicklungsprozess, der entsprechend mächtige Entwicklungstechniken und Entwicklungsparadigmen erfordert. Unter einem Programmierparadigma versteht man ein Konzept bzw. Denkschema, das Programmiersprachen zugrunde liegt, d.h. „Programmiersprachen gleichen Typs basieren auf demselben Programmierparadigma" [Schn 98]. Allerdings folgt keine der existierenden Programmiersprachen in reiner Form einem einzigen Programmierparadigma. Vielmehr wird versucht, verschiedene Paradigmen in eine Sprache zu integrieren, wobei eines der Paradigmen dominierend ist.

Ein Schlagwort der 90er Jahre war Objektorientierung. Mit objektorientierten Programmiersprachen soll die traditionelle Trennung zwischen Daten und Funktionen aufgehoben werden. Objekte der Realität lassen sich so auf Objekte im Programm abbilden, die aus Daten und den Funktionen, die auf diese Daten angewendet werden können, bestehen. Jedes Objekt ist durch seine Identität, sein Verhalten und seinen Zustand eindeutig beschrieben [Oest 01]. Neben der Objektorientierung werden weitere Paradigmen wie funktionale und visuelle Programmierung oder Bausteinorientierung untersucht. Funktionale Programmiersprachen basieren auf dem sogenannten Lambdakalkül der Funktionstheorie. Aus dem Zusammensetzen der drei Basisfunktionen Aneinanderketten, Iterieren und Rekursion können alle möglichen Funktionen realisiert werden [Pepp 00]. Bei der visuellen Programmierung dagegen kommen primär grafische Notationen zum Einsatz. Dadurch soll die Verständlichkeit von Programmen erhöht und die Programmierung gegenüber der Verwendung konventioneller Werkzeuge und Sprachen erleichtert werden [Schi 97]. Im Zusammenhang mit der Diskussion über Bausteinorientierung ist die Einschätzung der Bedeutung, die der Open Source Gedanke, aber auch frei verfügbare Software-Systeme oder -Komponenten für die Software-Entwicklung haben werden, interessant. Das Thema Open Source wurde in Abschnitt 8.3.5 bereits angeschnitten.

### Ergebnisse

Das Volumen von Software wird nach Meinung der Experten – und hierbei herrscht Einigkeit zwischen den Vertretern der Industrie und denen aus dem wissenschaftlichen Bereich – relativ konstant zunehmen und in zehn Jahren etwa zwei- bis dreimal höher sein als heute (vgl. Abbildung 8.103). Dabei stellt dies einen Nettowert dar, da zwar in allen Bereichen neue umfangreiche Systeme entwickelt werden, gleichzeitig aber auch „Altlasten", d.h. überholte Software-

Produkte, aber auch ganze Systeme und Systemklassen ausgemustert werden. Allerdings sind zwei relativ gleich starke Lager auszumachen: der eine Teil der Befragten erwartet keinen nennenswerten Anstieg, einige wenige sogar eine Abnahme der Softwaregröße, was darauf zurückgeführt wird, dass es aufgrund des stärkeren Einsatzes von Standard-Software in der Summe immer weniger Individualsoftware geben wird. Die andere Hälfte der Experten rechnet dagegen mit einem Anstieg von mehr als 50 Prozent pro Jahr, weil die Komplexität von Software weiterhin steigt und gleichzeitig viele bisherige Hardware-Realisierungen durch Software ersetzt werden. Im Ergebnis entspricht die kurzfristige Prognose der Voraussage der letzten Studie [SETIK 00], die damalige langfristige Erwartung einer Verzwanzigfachung des Softwarevolumens wurde jedoch deutlich nach unten revidiert. Aber selbst eine Verdoppelung erfordert fortschrittliche Techniken für den Umgang mit komplexer Software.

SOFTWAREGRÖSSE: Das Volumen von Software wird innerhalb der nächsten 10 Jahre konstant bis auf etwa 250% des heutigen Wertes anwachsen.

VERNETZUNG ÜBER DAS INTERNET: Die bedeutendste Eigenschaft von Softwaresystemen wird während der nächsten 10 Jahre diese Vernetzung bleiben.

MOBILITÄT: Während Mobilität heute zu den untergeordneten Systemeigenschaften zählt, wird die Bedeutung langfristig stark ansteigen, aber trotzdem hinter Vernetzung und Verteilung zurückbleiben.

In den letzten Jahren sind eine Reihe von Systemeigenschaften zu zentralen Aspekten vieler Softwaresysteme und Systemklassen avanciert. Die Vernetzung über das Internet wird dabei über die nächsten zehn Jahre die größte Bedeutung haben, auch wenn die Experten aus dem universitären Umfeld langfristig kein Wachstum mehr sehen. Der Grund für die Dominanz dieser Eigenschaft liegt in der Vielzahl der Anwendungsgebiete. So spielt die Vernetzung im Unternehmensbereich eine immer größere Rolle für Informationssysteme. Als Voraussetzung und Basis für E-Business-Anwendungen und in der Forschung ermöglicht sie verteiltes Arbeiten und die Verwaltung und Auswertung großer Datenmengen. Ein Beispiel für diese umfassende Vernetzung sind Grid-Anwendungen, die im Abschnitt 8.1.6 näher untersucht werden. Gleichzeitig nehmen die Anwendungen im Bereich der Haushaltsgeräte und des Home Entertainment schnell zu, siehe hierzu auch Abschnitt 9.2.

Die Prognosen für Verteilung, Mobilität und Einbettung in Hardware fallen relativ ähnlich aus, wobei Mobilität den stärksten Zuwachs verzeichnen kann. Die Trennung der verschiedenen Systemeigenschaften fällt dabei in vielen Bereichen schwer. Verteilung beispielsweise ist heute v.a. für Informationssysteme von Bedeutung, wird zukünftig aber auch in mobilen Systemen eine große Rolle spielen, z.B. bei mobilen Agentensystemen. Weitere Anwendungsbereiche sind Verzeichnisdienste und Prozesssteuerungen. Steuerungssysteme sind nahezu untrennbar mit dem Begriff der Einbettung verbunden, stellen sie doch die Hauptanwendung von Embedded Systems dar. Die fortschreitende Elektronisierung und Automation vieler Abläufe (vgl. Abbildung 8.104) spiegelt die steigende Bedeutung der Einbettung wider. Einen deutlichen Anstieg der Bedeutung eingebetteter Systeme wurde in der Vorgängerstudie erst viel später, nämlich nach dem Jahr 2010, erwartet. Wichtig sind in Hardware eingebettete Softwaresysteme aber schon heute sowohl im privaten Leben für Haushaltsgeräte oder im Auto als auch zur Steuerung von Flugzeugen, für die Rüstungsindustrie und generell in der Robotik, die ihre Anwendungen immer mehr auch in der Medizintechnik findet. Seltener genannt wurde dagegen der Bereich der Unterhaltungselektronik.

Die deutlichste Zunahme in der Bedeutung während der nächsten zehn Jahre verzeichnet die Systemeigenschaft Mobilität. Damit werden die Vorhersagen der Befragten der Studie 2000 bestätigt, die damals einen Anstieg der Bedeutung ab 2003 erwarteten. Der starke Anstieg ist hauptsächlich auf geplante Anwendungen in den Bereichen Automotive und Telekommunikation zurückzuführen. Gerade in der Kommunikation wird für die nächsten Jahre eine Vielzahl von verschiedenen mobilen Geräten mit umfassenden Funktionalitäten erwartet (siehe hierzu Abschnitte 8.2.7 und 9.3). Als problematisch wird allerdings angesehen, dass der Markt für Software, die Mobilität geeignet und umfassend unterstützt, von wenigen Herstellern dominiert wird. Einige Experten äussern die Sorge, dies könnte die nötigen und möglichen Entwicklungen in diesem Bereich verzögern.

Den geringsten Bedeutungszuwachs im Kontext der Systemeigenschaften weist die Reaktivität auf (Abbildung 8.104). Hauptanwendungen sind auch hier die Steuerung, beispielsweise in der Logistik oder der Fertigung in Form von Dialog- und Transaktionssystemen. Das entscheidende Kriterium für eine höhere Relevanz sei eine verbesserte Bedienerfreundlich-

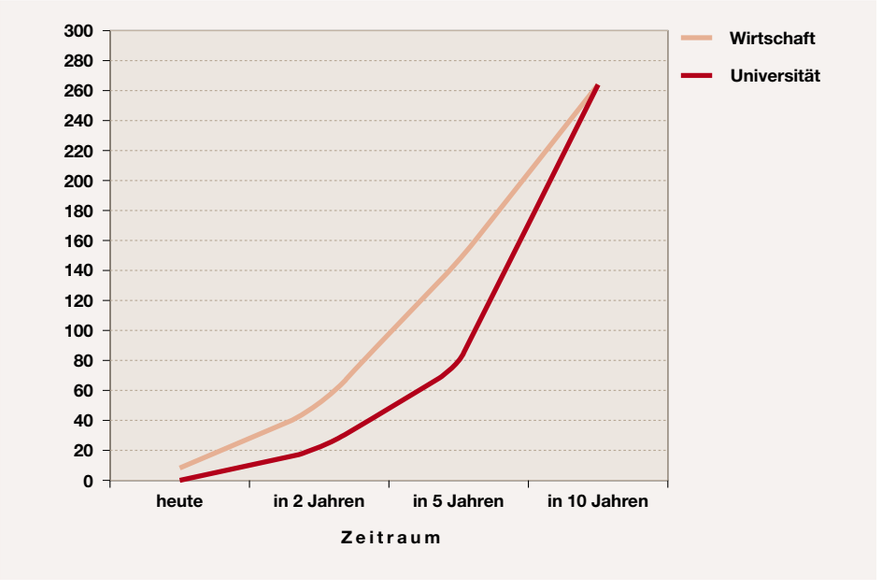



Abbildung 8.103: Zuwachs der Softwaregröße

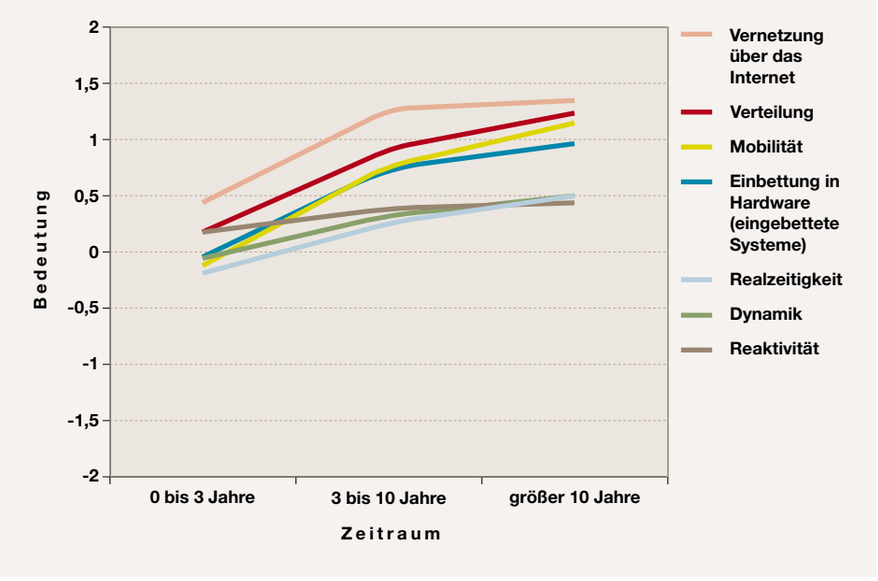



Abbildung 8.104: Bedeutung verschiedener Systemeigenschaften

keit, da bisher zu wenig grafische Benutzeroberflächen eingesetzt würden, die eine einfache Bedienung ermöglichen.

Eng miteinander verbunden, und dementsprechend ähnlich in den Zukunftsaussichten, sind die Dynamik und die Echtzeitfähigkeit von Systemen. Dynamik ist v.a. für Expertensysteme (siehe auch Abschnitte 8.3.4 und 9.4) und Web Services von Bedeutung. Der Echtzeitfähigkeit wird heute die geringste Bedeutung beigemessen, obwohl mittlerweile einige Tools wie Rational Rose RealTime existieren, die trotz der Komplexität der entsprechenden Systeme deren Entwicklung gut unterstützen können. Die niedrige Bedeutung basiert interessanterweise v.a. auf den pessimistischen Prognosen der Industrievertreter, obwohl gerade hier Realzeitigkeit eine wichtige Anforderung ist, sei es zur Steuerung von Automobilen oder Flugzeugen oder in der Medizin. Ein Grund für die dennoch niedrige Einschätzung ist die nötige hohe Korrektheit und Zuverlässigkeit und die schwere Testbarkeit dieser Systeme.

BUSINESS SYSTEME: Die Klasse der Business Systeme wird die heutige große Bedeutung in den nächsten 10 Jahren beibehalten.

Generell werden an zukünftige Systeme höhere Anforderungen bezüglich ihrer Sicherheit, Robustheit und Verfügbarkeit gestellt, da immer komplexer werdende und mehrere Anwendungen integrierende Systeme entstehen werden und beherrscht werden müssen. Viele Experten äussern aus diesem Grund die Erwartung, dass Systeme bzw. Softwareprodukte von immer weniger Unternehmen bereitgestellt werden können. Neben der erwähnten Komplexität hat dies auch seinen Grund in sogenannten Netzwerkeffekten, d.h. Benutzer profitieren davon, dass viele andere das selbe Tool auch verwenden.

Die gerade beschriebenen Entwicklungen bei den Systemeigenschaften lassen sich direkt auf die unterschiedlichen Systemklassen abbilden. In den Expertengesprächen, die der Fragebogenaktion vorausgingen, wurden vier solcher Klassen von Softwareanwendungen als besonders zukunftsweisend identifiziert. Die Ergebnisse der schriftlichen Befragung zeigen, dass Integrierte Gebäudesysteme und Systeme im Bereich Automotive zwar rapide an Bedeutung gewinnen werden, aber trotzdem hinter Telekommunikationssystemen und Business Systemen zurückbleiben. Mit Business Systemen bezeichnet man umfangreiche Anwendungen mit einem zum Teil hohen Verteilungsgrad zur Steuerung und Planung umfassender Unternehmensprozesse. Darunter fallen Informationssysteme, ERP-Systeme, aber auch Anwendungen im Bereich E-Business (siehe hierzu Kapitel 9). In der Vergangenheit waren neue Entwicklungen bei diesen Systemen oft der Treiber für neue Geschäftsmodelle, z.B. bei der Einführung vernetzter Management Information Systeme. Deutliche Beispiele für die Wirkungskette von Rechnertechnik bzw. -netzen über die Entwicklung neuer Systeme hin zu ungekannten Geschäftsmodellen stellen E-Business oder SCM dar. Da revolutionäre Entwicklungen im Bereich der Business Systeme nicht erwartet werden, wird sich die Bedeutung dieser Systemklasse in den nächsten zehn Jahren kaum verändern und auf dem momentanen sehr hohen Niveau bleiben, wie Abbildung 8.105 zeigt. Bereits in der Studie 2000 wurde Business Systemen ein besonders hoher Stellenwert eingeräumt. Die gleichbleibende Bedeutung ist das Ergebnis einer interessanten gegenläufigen Einschätzung: Während die Experten aus dem universitären Umfeld eine stetig steigende Bedeutung prognostizieren, sehen die Vertreter der Wirtschaft v.a. langfristig einen Abwärtstrend, weil revolutionäre Fortschritte in diesem Bereich nicht zu sehen sein werden. Wie im Kontext einzelner Systemeigenschaften bereits angesprochen, erwarten viele Experten gerade bei den Business Systemen eine Standardisierung, die zu einer Konsolidierung auf dem Markt für ERP-, CRM- und SCM-Software führen werde.

Wie auch in mehreren anderen Themengebieten innerhalb der Studie zu sehen, werden innerhalb der nächsten zehn Jahre Systeme im Telekommunikationsbereich eine immer größere Bedeutung für die IuK-Technik erlangen (siehe Kapitel 8.2 und 9). Der immer noch anhaltende Zuwachs beruht dabei weitgehend auf den Entwicklungen in der mobilen Kommunikation. Deren Zukunft wird entschieden von den Entwicklungen bei den Trägersystemen und den darauf basierenden Diensten und Anwendungen (siehe Abschnitt 9.3). Als besonders wichtig für die weiteren Entwicklungen im Bereich der Telekommunikationssysteme werden Sicherheitsfragen angesehen (vgl. Kapitel sowie Abschnitte 8.2.1 und 8.2.8).

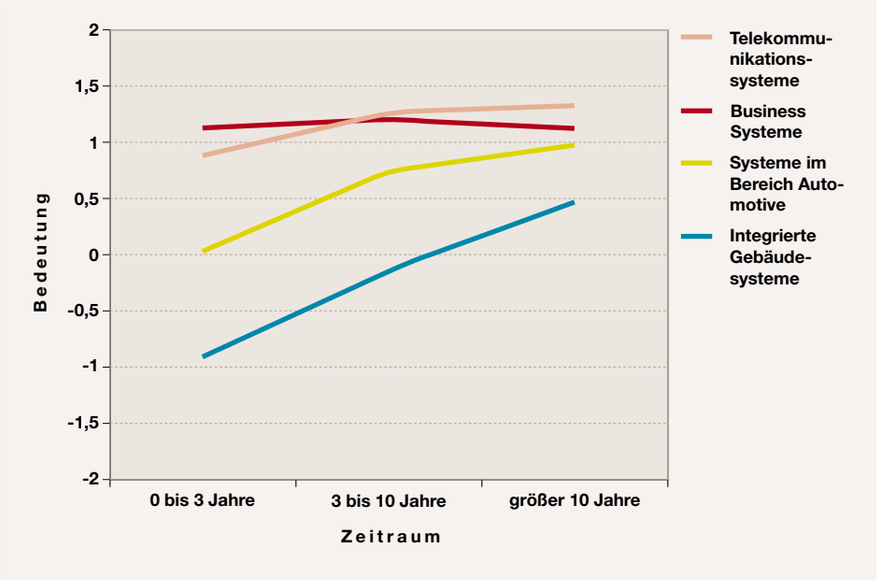



Abbildung 8.105: Bedeutung verschiedener Systemklassen

INTEGRIERTE GEBÄUDESYSTEME: Die Bedeutung komplexer Steuer- und Kontrollsysteme für Gebäude wird über die nächsten 10 Jahre hinweg stark zunehmen.

Genauso wie Telekommunikationssysteme sind auch Systeme im Bereich Automotive geprägt von der zunehmenden Mobilität und Einbettung immer komplexerer Software. Obwohl der Anteil der Software am Automobil sowohl bezüglich der Zahl der Komponenten als auch hinsichtlich der Kosten in den letzten Jahren schon stark gestiegen ist, wird die Bedeutung derartiger Softwaresysteme langfristig weiter wachsen. Dabei steht einer immer weiter fortschreitenden Integration neuer Funktionen die „Freiheit" des Autofahrens, also gerade die Unabhängigkeit von steuernden und unterhaltenden Systemen gegenüber. Interessant bei der Analyse der Ergebnisse ist, dass auch hier die Experten aus dem wissenschaftlichen Umfeld einen anhaltend starken Anstieg der Bedeutung dieser Systemklasse erwarten, während die Experten aus der Industrie langfristig nur noch ein sehr schwaches Wachstum vorhersagen. Dieses Wachstum resultiert v.a. aus einem breiteren Einsatz von Steuerungen sicherheitsrelevanter Komponenten und von Anwendungen zur Navigation und Stauvermeidung, während die unmittelbare Integration von Unterhaltungs- und Kommunikationselektronik in das Automobil kaum zunehmen wird. Derartige Dienste und Funktionen (in der Vergangenheit wurde hier oft der Begriff „rollendes Büro" verwendet) werden weiterhin hauptsächlich von unabhängigen, nicht fest integrierten Geräten erbracht. Denn die Verwendungsdauer mobiler Kommunikations- und Unterhaltungsgeräte ist meist kürzer als die eines Automobils und die eingebaute Technik wäre bald nach dem Kauf veraltet. Inwieweit die Hersteller auf diesen Umstand reagieren, z.B. durch eine kostenlose Erneuerung eingebauter Geräte nach einer gewissen Zeit, bleibt abzuwarten.

Eine noch stärkere Zunahme der Bedeutung wird der Bereich der Elektronik und Software in Gebäuden erfahren. Integrierte Gebäudesysteme (IGS) werden deutlich wichtiger werden, auch wenn sie heute noch keine große Beachtung finden. Ziel ist die Entwicklung intelligenter Gebäude, die eine integrierte Steuerung der gesamten Haustechnik und der im Gebäude befindlichen Geräte erlauben [IGS 01]. Aber gerade der Aspekt der Einbindung von Haushaltsgeräten (siehe hierzu auch Abschnitt 9.2) in ein umfassendes, komplexes Steuer- und Kontrollsystem wird von den Experten nicht betont. Offensichtlich trennen die Menschen immer noch sehr stark zwischen dem Gebäude an sich und der Einrichtung, die sich darin befindet. Dass die Bedeutung dieser Systemklasse trotzdem so stark steigt, liegt an den Möglichkeiten hinsichtlich Ökologie, Komfort und Gesundheit, aber auch an höherer Sicher-

heit durch die Integration von Zugangssystemen. Während die meisten Experten die Ausbreitung komplexer, integrierter Gebäudesysteme sowohl für den privaten als auch für den betrieblichen und öffentlichen Bereich erwarten, werden IGS von manchen als reine Spezialanwendung für die Industrie und dort im Zusammenhang mit der Anlagenautomatisierung gesehen.

In den Fragebögen wurde oft angemerkt, dass in allen genannten Systemklassen eine sich immer noch fortsetzende Ablösung von spezieller Hardware durch Software zu beobachten sei. Bei der Realsierung von eingebetteten Systemen (embedded systems) wird auch weiterhin die Software immer mehr Funktionalitäten übernehmen, die bisher Hardware-seitig gelöst wurden. Besonders an Bedeutung zunehmen werden auch in den nächsten Jahren komplexe Steuerungs- und Regelsysteme, die v.a. in der industriellen Fertigung und in der Logistik eingesetzt werden.

Die zu Beginn dieses Abschnitts analysierten Systemeigenschaften können nur mit geeigneten Ansätzen bei der Programmierung realisiert werden. Einige, teils konkurrierende, teilweise aber auch auf ganz spezifische Anforderungen zugeschnittene Programmierparadigmen, d.h. haben sich herausgebildet. Es wird von den Experten auch nicht erwartet, dass in absehbarer Zeit ganz neue Paradigmen aufkommen werden. Einigkeit unter den Befragten herrscht darüber, dass kurz- und mittelfristig die Objektorientierung dominant bleiben wird (vgl. Abbildung 8.106), da sie universell einsetzbar ist. Eine zukünftige Erweiterung dieses Ansatzes ist beispielsweise die Aspektorientierung. Allerdings wird das Paradigma der Objektorientierung langfristig einer schnell an Bedeutung gewinnenden Bausteinorientierung weichen müssen, wie dies bereits in der Studie 2000 prognostiziert wurde. Bei der Baustein- bzw. Komponentenorientierung werden Softwaremodule kombiniert und konfiguriert. Für dieses Vorgehen wird ein weites Anwendungsfeld (Betriebssysteme, Server- und Netzdienste) gesehen, allerdings nur, wenn genügend ausgereifte formale Beschreibungstechniken entwickelt werden. Dieses Ergebnis wird gestützt durch Abschnitt 9.9, in dem die Entwicklung eines globalen Marktes für Softwarekomponenten innerhalb von drei Jahren erwartet wird. Stark an Bedeutung gewinnen wird auch die Dienstorientierung, d.h. die Komposition und Konfiguration von Schnittstellen. Die Anwendung dieses Paradigmas sehen die Experten hauptsächlich im Web-Bereich. Zu keiner Zeit eine bedeutende Rolle wird die Logikprogrammierung spielen, eventuell in einigen Spezialgebieten wie der Computerlinguistik oder im Bereich der künstlichen Intelligenz. Vor drei Jahren wurde der Logikprogrammierung statt dessen noch eine stärker werdende Rolle in der Wissensverwaltung, z.B. in Expertensystemen, vorausgesagt. Eine immer weiter abnehmende Bedeutung wird auch der funktionalen Programmierung beigemessen. Obwohl dieses Paradigma von einigen Experten als „natürliches Vorgehen" bei der Softwareentwicklung bezeichnet wir und für komplexe und/oder hochkritische Systeme geeignet sei, bestehen erhebliche Akzeptanzprobleme. Hinter den drei genannten bleibt, trotz einer Zunahme ihrer Bedeutung über den gesamten Prognosezeitraum hinweg, die visuelle Programmierung zurück. Diese wird v.a. bei der Entwicklung von Oberflächen, z.B. für Datenbanken, eine Rolle spielen.

Eine im Vergleich zur Vorgängerstudie stark gestiegene Bedeutung für die gesamte IuK hat Open Source Software (im Kapitel 7 wird darauf eingegangen. Auch im Bereich der Datenbanken gibt es Trends hin zu Open Source Lösungen, vgl. Abschnitt 8.3.5). Entgegen der Studie 2000, wo eine Verbreitung erst nach 2010 gesehen wurde, wird sich quelloffene Software bereits in vier Jahren am Markt behaupten können (Abbildung 8.107). Mögliche Gründe für die wachsende Bedeutung sind der Paradigmenwechsel, gerade in der öffentlichen Verwaltung, und die realisierbaren Kostenersparnisse. Als unbedingte Voraussetzung für einen schnellen und breiten Akzeptanzgewinn werden professioneller Support, umfassende ergänzende Serviceleistungen und ausgereifte Migrationsmöglichkeiten angesehen.

Ein grundlegender Meinungsunterschied zwischen den Experten betrifft die Sicherheit und Zuverlässigkeit solcher Systeme. Ein Teil der Experten sieht die Stärken von Open Source gerade bei sicherheitsrelvanten Anwendungen und ausfallsicheren Systemen wie ERP- oder Web-Servern. Andere wiederum sehen Chancen v.a. in wenig unternehmenskritischen

BAUSTEINORIENTIERUNG: Langfristig wird dieses Programmierparadigma das Wichtigste werden, in den kommenden 7 Jahren wird der Objektorientierung aber die größte Bedeutung beigemessen.

OPEN SOURCE: Quelloffene Software wird innerhalb von 4 Jahren am Markt weit verbreitet sein.

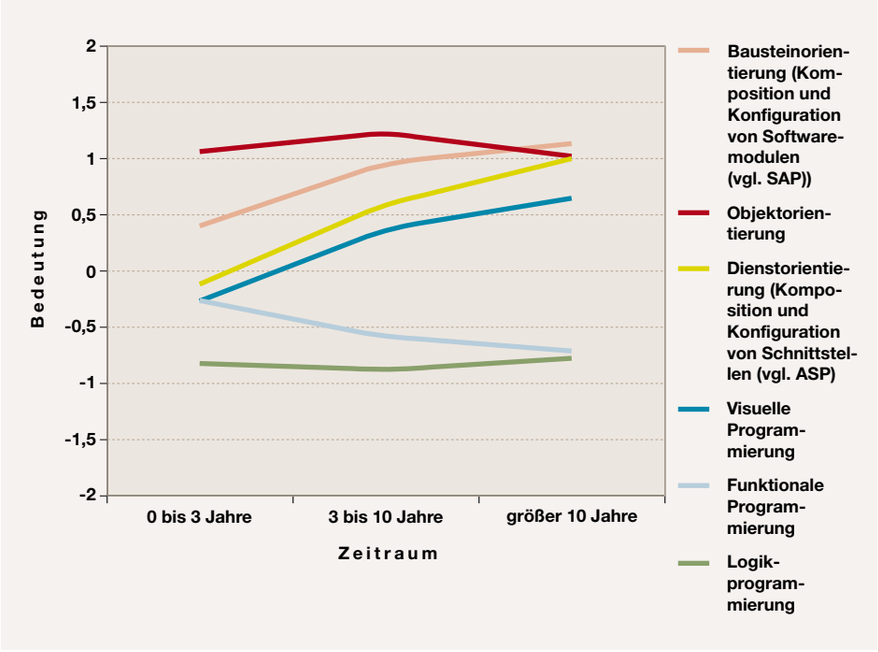



Abbildung 8.106: Bedeutung verschiedener Programmierparadigmen

Bereichen, z.B. bei kleineren Applikationen oder Office-Anwendungen. Als Beispiele für den Erfolg des Open Source Gedanken und als am weitesten verbreitete Systeme werden das Betriebssystem Linux, der Webserver Apache und verschiedene Webbrowser genannt. Die Chancen von Open Source Software, sich über den akademischen Bereich und die Fokussierung auf Betriebssystem und Internet hinaus durchzusetzen, werden neben den oben genannten Kriterien auch von der Entwicklung geeigneter grafischer Oberflächen bzw. einer generell einfacheren Bedienbarkeit abhängen.

## Zusammenfassung

In der Systementwicklung gibt es eine Reihe neuer Trends. Dies gilt für die Eigenschaften, die Softwarelösungen zukünftig haben müssen, ebenso wie für die Einsatzgebiete dieser Lösungen. Die neuen bzw. veränderten Anforderungen verlangen nach einer Anpassung der Vorgehensweise bei der Softwareentwicklung. Der Vergleich verschiedener Ansätze der Programmierung ergab im Bereich der Systementwicklung kurz zusammengefasst folgende Ergebnisse:

- Das Softwarevolumen wird konstant ansteigen und sich bis 2013 um den Faktor zwei bis drei erhöhen.
- Die Vernetzung über das Internet wird die bedeutendste Systemeigenschaft bleiben. Daneben werden Verteilung und Mobilität stark an Bedeutung gewinnen.
- Während die große Bedeutung von Business Systemen nahezu konstant bleibt, werden Telekommunikationssysteme immer wichtiger und ab 2006 die größte Bedeutung erlangen.
- Objektorientierung ist das mit Abstand wichtigste Programmierparadigma, ab dem Jahr 2013 wird der Bausteinorientierung aber die größte Bedeutung beigemessen werden.
- Die Verbreitung von Open Source Software wird weiter ansteigen. Als entscheidend für die zukünftige Bedeutung werden besserer Support und Service sowie eine einfachere Bedienbarkeit angesehen.

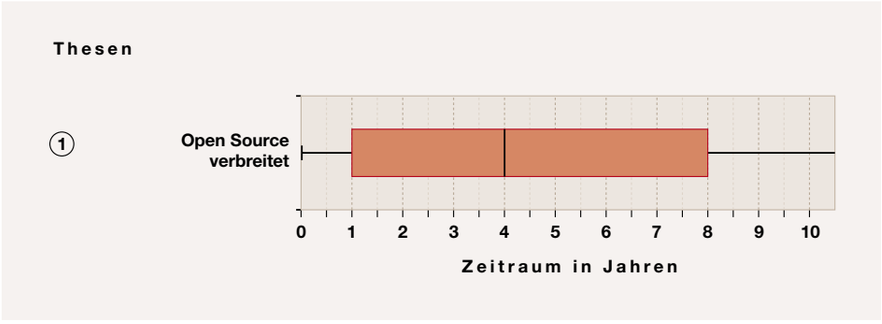



Abbildung 8.107: Ergebnis der These zu Open Source Software

### 8.4.7 Standardisierung und Zertifizierung

Die bisherigen Ergebnisse der Studie im Bereich des Software-Engineering zeigen, dass die Anforderungen an die in Zukunft zu entwickelnde Software weiter steigen werden, weil die Komplexität und die Funktionalität zunehmen. Ein weiterer, nicht zu unterschätzender Aspekt sind die in der EDV-Branche existierenden Überkapazitäten und der Kostendruck bei Unternehmen wie bei der öffentlichen Hand. Diese Entwicklung hat zwei Auswirkungen, denen zukünftig mehr Beachtung geschenkt werden muss: Zum einen muss die Entwicklung von Software schneller und billiger werden. Dies wird durch verteilte Entwicklung, teils mit Entwicklerteams aus Ländern mit deutlich niedrigeren Löhnen, aber auch durch den Verzicht auf umfangreiche Tests und Qualitätssicherung (QS) versucht. Der Zeit- und Kostendruck, der nicht zuletzt durch die harte Konkurrenz aufgrund der vielen freien Kapazitäten der IT-Dienstleister bedingt ist, bringt das Risiko mit sich, dass Software nicht mit der richtigen Vorgehensweise und nötigen Sorgfalt entwickelt wird. Somit heisst stärkerer Wettbewerb für den Kunden nicht unbedingt auch bessere Produkte. Zum anderen benötigen Auftraggeber Kriterien und Richtlinien, nach denen sie Anbieter beurteilen und einteilen können. Da bei Softwareentwicklungsprojekten in den seltensten Fällen das Produkt schon fertig ist, bevor es gekauft wird, muss ein Unternehmen genauso wie eine staatliche Behörde in der Lage sein, vor der Auftragsvergabe auf anderem Wege Lieferanten zu bewerten.

Um diese Probleme bereits im Vorhinein und auf breiter Basis zu lösen, gibt es seit vielen Jahren Bestrebungen, Richtlinien einzuführen, die zum Erfolg einer jeden Entwicklung beitragen sollen. Zum einen gibt es eine Vielzahl von Qualitätsstandards und -methoden, die auch hinreichend bekannt sind. Während sie in größeren Entwicklungsorganisationen eingeführt wurden, hat sich eine Zertifizierung der Lieferanten auf dieser Basis noch nicht durchgesetzt. Wann diese Zertifizierung verbreitet sein wird, ist Gegenstand des folgenden Abschnitts. Zum anderen sind zur Arbeitsteilung wie zur Erhöhung der Softwarequalität in komplexen Projekten Vorgehensmodelle notwendig, die alle nötigen Prozessschritte eines Softwareprojektes beschreiben. In den letzten Jahren haben sich viele solcher Methoden und Entwicklungsstandards entwickelt. Es wird gezeigt, wie sich diese verschiedenen Vorgehensweisen unterscheiden, welche Bedeutung für den Entwicklungsprozess sie haben und wie sie sich weiterentwickeln werden. In großen Organisationen lassen sich solche Richtlinien oftmals leichter implementieren. Inwieweit auch kleinere und mittlere Unternehmen (KMU) solche Vorgehensmodelle oder Prozessstandards anwenden, wurde aus diesem Grund ebenfalls gefragt.

#### Ergebnisse

Die Zertifizierung von Software in Bereichen, in denen Qualität und Zuverlässigkeit für das Leben, die Gesundheit und die Umwelt entscheidend sind, ist seit jeher vom Gesetzgeber vorgegeben. Diese Bereiche sind beispielsweise Flug- und

Fahrzeuge und sicherheitskritische industrielle Anlagen sowie Kraftwerke. In anderen Bereichen, wie z.B. Banken und der Datenschutz, werden Qualitätsstandards in fünf Jahren weit verbreitet eingesetzt werden (vgl. Abbildung 8.108). In der letzten Studie [SETIK 00] wurde die Verbreitung der Zertifizierung zwei Jahre früher erwartet. Wie oben angesprochen wird eine solche Zertifizierung in Zukunft auch eine Rolle bei der Lieferantenbeurteilung und -auswahl spielen. Von einigen Experten wird hier angemerkt, dass ein solches Qualitätsmanagement-System in den Entwicklungsprozess integriert sein und sachgerechter angewandt werden muss. Die Gründe für den bisher wenig verbreiteten Einsatz von Zertifizierungen sehen die Befragten im Mangel an einer einfachen und verbreiteten formalen Methode der Zertifizierung, aber hauptsächlich in den Kosten. Die wichtigste Voraussetzung für die Verbreitung ist gerade eine ausreichend hohe Zahl neutraler und anerkannter Zertifizierungsstellen und allgemein bekannter Siegel bzw. Zertifikate.

Neben der Prüfung von Qualitäts-Standards und der darauf basierenden Vergabe von Zertifikaten nach Beendigung der Entwicklung ist es sinnvoll, von Anfang an in Unternehmen Vorgehensmodelle und Prozess-Standards zu definieren. Diese müssen so angelegt sein, dass ihre Umsetzung für Unternehmen sinnvoll und machbar ist und dass die Einhaltung kontrolliert werden kann. Während große Firmen solche Vorgehensweisen schneller und einfacher adaptieren können, fällt eine Implementierung kleinen und mittleren Unternehmen oftmals schwer. Deshalb wird es auch noch acht Jahre dauern, bis die beschriebenen Vorgaben in KMU weit verbreitet ein- und umgesetzt werden (vgl. Abbildung 8.108), während in der Vorgängerstudie eine Durchdringung von Vorgehensmodellen bereits für 2007 erwartet wurde. Die Akzeptanz fehlt heute noch in vielen Fällen, weil der Aufwand steigt (für die Implementierung, aber auch danach in jedem Projekt, weil eine Einhaltung verlangt wird), die Flexibilität in Projekten sinkt und im allgemeinen das Bewusstsein für die fachliche und sachliche Notwendigkeit solcher Standards weitgehend noch fehlt. Auf der anderen Seite wird von Experten darauf hingewiesen, dass solche Modelle und Standards ja bereits verfügbar sind und dass, wie oben angesprochen, viele Abnehmer einen in dieser Hinsicht formalen Anforderungen genügenden Entwicklungsprozess verlangen.

Welche Vorgehensmodelle und Softwareentwicklungs-Standards existieren und wie die Erwartungen der Experten hinsichtlich der zukünftigen Bedeutung sind, wird im folgenden dargestellt. Dabei fällt deutlich auf, dass sich keines der genannten Modelle von anderen abhebt und alle leicht in ihrer Bedeutung zunehmen, ausser dem RUP, der über den gesamten Analysezeitraum hinweg die wichtigste Rolle spielen wird. Gerade die Vertreter der Industrie sehen auch langfristig noch eine Zunahme der Bedeutung, während die Experten aus der Forschung einen stetig fallenden Trend erwarten. Wichtig ist der RUP v.a. für die objektorientierte Entwicklung, von deren Bedeutung auch die Verbreitung dieses Vorgehensmodells abhängig sein wird. Das generische V-Modell wird im Software Engineering durch spezifische Vorgehensweisen und Entwicklungsmethoden implementiert und dadurch langfristig abgelöst (vgl. Abbildung 8.109). Das V-Modell wird als Vorgehensmodell für objektorientierte Software vom RUP überholt. Es ist nun die Aufgabe der öffentlichen Hand als Initiator des V-Modells, das RUP für den Softwareinhalt seiner Ausschreibungen zu fordern.

Die heute geringste Bedeutung in diesem Umfeld haben Catalysis und Cleanroom, deren Bedeutung auch nicht merklich zunimmt. Beide Modelle werden auch langfristig keine Bedeutung erlangen. Bei Catalysis wird der Grund in dem niedrigen Bekanntheitsgrad gesehen, darüber hinaus wird es von einigen Experten als zu schwer verständlich eingeschätzt. Cleanroom, das in der Vergangenheit etwas verbreiteter war, werde aufgrund des hohen Preises ausser in Hochsicherheitsanwendungen kaum noch verwendet. Das CMM wird leicht an Bedeutung gewinnen und wird v.a. für die Beurteilung interner Softwareabteilungen und das Benchmarking von Lieferanten eingesetzt werden. Ein Vorteil dieses Ansatzes ist die Anwendbarkeit auf verschiedenste Software-Arten. Gewisse Varianten des CMM-Ansatzes werden als ISO-Normen Verbreitung finden. Sehr kontrovers diskutiert wird dagegen die Verbreitung der

ZERTIFIZIERUNGEN: In 5 Jahren wird die Zertifizierung von Software hinsichtlich definierter Qualitätsstandards verbreitet sein.

VORGEHENSMODELLE: In kleinen und mittleren Unternehmen werden Vorgehensmodelle und Prozess-Standards in 8 Jahren verbreitet eingesetzt werden.

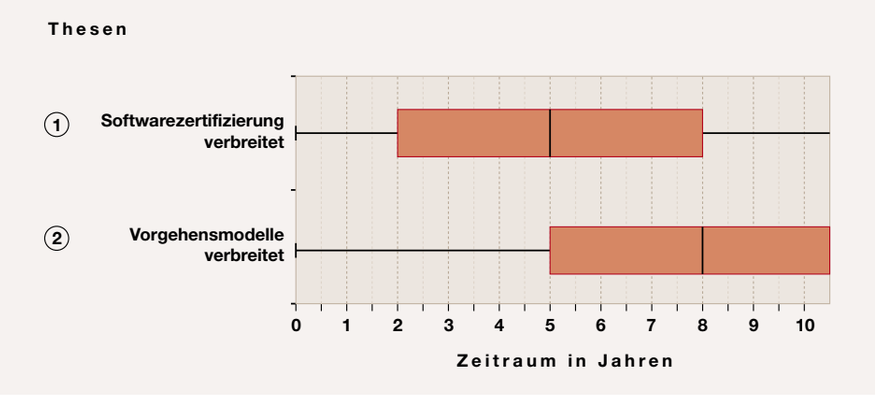



Abbildung 8.108: Ergebnisse der Thesen zu Standardisierung und Zertifizierung

RATIONAL UNIFIED PROCESS: Dieses Vorgehensmodell wird während der nächsten 10 Jahre das Bedeutendste bleiben, während das V-Modell rapide seine hohe Wichtigkeit verliert.

ISO-Normen im Software Engineering. Die steigende Bedeutung ist auf die Einschätzungen der Experten aus dem akademischen Umfeld zurückzuführen, die zwar heute eine relativ geringe Bedeutung sehen, aber bis in zehn Jahren diese Standards als die wichtigsten ansehen. Hier liegt der Grund in der breiten Anwendbarkeit auf alle Arten von Software und die Systementwicklung im Allgemeinen. Allerdings wird mehrmals angemerkt, dass die Anforderungen zu schwach bzw. die Prüfungen nicht streng genug seien. Allerdings werden aufgrund des allgemeinen Zertifizierungsdrucks neue ISO/IEC-Normen erwartet, die für eine gestiegene Bedeutung sorgen werden.

Die größte Bedeutung im Kontext der Vorgehensmodelle wird der Rational Unified Process über die nächsten zehn Jahre hinaus behalten, auch wenn einige andere Standards langfristig Relevanz gewinnen. Gerade die Vertreter der Industrie sehen auch langfristig noch eine Zunahme der Bedeutung, während die Experten aus der Forschung einen stetig fallenden Trend erwarten. Wichtig ist der RUP v.a. für die objektorientierte Entwicklung, von deren Bedeutung auch die Verbreitung dieses Vorgehensmodells abhängig sein wird. Während der Unified Process leicht zunimmt, verliert das V-Modell rapide an Bedeutung, wobei die Experten aus der Forschung den Bedeutungsverlust als nicht so deutlich erwarten. Obwohl das V-Modell für alle Arten von Software, von Unternehmens-Software über den staatlichen Bereich bis hin zu Embedded Software, geeignet ist, wird es zunehmend unattraktiv. Beeinflussen kann die öffentliche Hand, die dieses Vorgehensmodell fordern, die zukünftige Entwicklung. Wird diese Forderung fallen gelassen bzw. ersetzt, könnte das V-Modell noch schneller aus der Praxis verschwinden.

## Zusammenfassung

Die Auswertung des abschließenden Kapitels zum Technologiebereich Softwaretechnik hat folgende Ergebnisse geliefert:

- Die Zertifizierung von Software ist in Bereichen, in denen Qualität und Zuverlässigkeit der Lösung eine große Rolle spielen, ab 2008 weit verbreitet.
- In kleinen und mittleren Unternehmen wird der verbreitete Einsatz von Vorgehensmodellen und Prozess-Standards 2011 zu beobachten sein.
- Das V-Modell, das heute zu den bedeutendsten Vorgehensmodellen gehört, wird bis 2013 nahezu bedeutungslos werden. RUP wird während der nächsten zehn Jahre der wichtigste Standard sein.

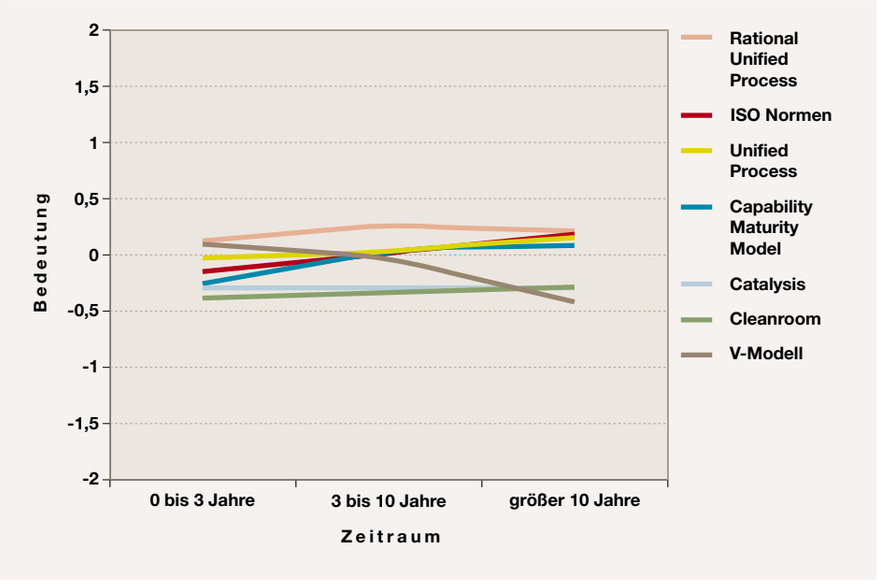



Abbildung 8.109: Bedeutung verschiedener Vorgehensmodelle und Softwareentwicklungs-Standards für Entwicklungsprozesse

# 9 Anwendungen

Technologien können sehr nachhaltige Auswirkungen auf Wirtschaft und Gesellschaft haben – dies hat die Vergangenheit mit der Veränderung des täglichen Lebens, beispielsweise durch Elektrizität, Automobile und Telephone, immer wieder deutlich gemacht [Nati 03, Inte 01]. Eines der Ziel dieser breit angelegten Trendstudie ist, mögliche Anwendungsfelder und Auswirkungen der in den vorangegangenen Kapiteln untersuchten Technologien zu beleuchten. Wie schon die Vorgängerstudie kann auch diese Studie nicht alle denkbaren Einsatzgebiete von Informations- und Kommunikationstechnologien umfassend empirisch abfragen, analysieren und diskutieren. Daher stehen in diesem Kapitel Anwendungsfelder im Vordergrund, in denen die übergreifenden Trends aus Kapitel 6 besonders deutlich auftreten:

**Automatisierung und Vereinfachung** (Abschnitt 6.1): Die integrierten Anwendungen im elektronischen Handel sind ein gutes Bespiel für diesen Trend (vgl. Abschnitt 9.1). So bieten Online-Händler ein „One Click Shopping" an: automatisch wird durch einen Klick auf ein gewünschtes Produkt der Kauf getätigt, die Zahlungsabwicklung aktiviert und der Versand der Ware veranlasst. Die innerbetrieblichen Geschäftsprozesse werden vollständig digitalisiert und automatisiert abgewickelt (vgl. Abschnitt 9.4). Durch die Integration aller Daten der verschiedenen Anwendungen ist ein Unternehmen jederzeit in der Lage, automatisch generierte Geschäftszahlen sozusagen auf Knopfdruck abzurufen (vgl. Abschnitt 9.6). Der Trend zur Vereinfachung zeigt sich deutlich bei Benutzerschnittstellen von Kleinstcomputern wie z.B. Mobiltelefonen oder PDAs. Einfache und auf die Anwendung fokussierte Benutzerführung hat mit zum schnellen Erfolg von Mobiltelefonen beigetragen (vgl. Abschnitt 9.2). Neue Verfahren wie das Bezahlen über Mobiltelefone, die Geldkarte oder Micropaymentsysteme sollen den Einkauf gerade von geringwertigen Gütern deutlich vereinfachen (vgl. Abschnitt 9.6). Erleichterungen werden dem Internet-Nutzer in Zukunft auch durch vielfältige E-Government Dienstleistungen, wie z.B. Online-Wahlen angeboten (vgl. Abschnitt 9.8).

**Dienst- und Komponentenorientierung** (Abschnitt 6.2): Komponentenorientierte Softwareentwicklung ermöglicht die fachliche Strukturierung von Anwendungen und die Wiederverwendung von programmiertem Code. Die einzelnen Komponenten kommunizieren über definierte Schnittstellen miteinander. Durch die Kommunikation über das Internet lassen sich neue Geschäftsmodelle entwickeln, die auf dem Handel fachlicher Komponenten basieren. Das Application Service Providing basiert beispielsweise auf dem Vertrieb von Diensten (vgl. Abschnitt 9.9). Einzelne Dienste lassen sich kaufen, mieten oder werden je nach Nutzung abgerechnet. In Zukunft werden Dienste auf elektronischen Marktplätzen angeboten und es erscheint möglich, ganze Geschäftsmodelle ausschließlich aus bereits existierenden Komponenten zusammenzustellen. Dienste und Komponenten sind dabei nicht auf die Nutzung über das Internet beschränkt. Gerade im mobilen Bereich äußert sich dieser Trend in der Entwicklung von Diensten, die sich der Kunde nach Bedarf auf sein Endgerät laden kann (vgl. Abschnitt 9.3).

**Globalisierung und Wettbewerb** (Abschnitt 6.3): Der Trend zu Globalisierung und Wettbewerb zeigt sich sehr deutlich im bei der elektronischen Geschäftsabwicklung (vgl. Abschnitt 9.1). Durch das Internet bietet sich die Möglichkeit, unmittelbar und direkt weltweit Handel zu betreiben. Ermöglicht wird diese Entwicklung durch die Durchsetzung weltweiter Kommunikationsstandards (vgl. Abschnitt 9.4). Die globale Ausrichtung der Geschäftsmodelle führt zu internationaler Konkurrenz. Als Beispiele für die Globalisierung der Märkte werden im Abschnitt 9.9 der Handel mit IT-Komponenten und

das Angebot von Application Service Providern betrachtet . Diese Dienst- und Komponentenorientierung ist eine Folge des harten Wettbewerbs und der Konzentration der Unternehmen auf ihre Kernkompetenzen (vgl. Abschnitt 9.5).

**Integration und Standardisierung** (Abschnitt 6.4): Die Standardisierung vieler Geschäftsprozesse ermöglicht die flexible Vernetzung von Wertschöpfungsketten. Der Trend zu Integration und Standardisierung zeigt sich deutlich im Abschnitt Digitalisierung und Automatisierung von Wertschöpfungsketten (vgl. Abschnitt 9.4), wie auch im Themenbereich Flexibilisierung von Organisationsstrukturen (vgl. Abschnitt 9.5). Hier werden modulare Organisationseinheiten integriert zu virtuellen Unternehmen. Aber auch bei den Endgeräten geht der Trend zur Standardisierung. So werden sich in Zukunft Kleinstgeräte über standardisierte Schnittstellen ad hoc selbstständig miteinander verbinden können (vgl. Abschnitt 9.2).

**Kapazitäts- und Leistungssteigerung** (Abschnitt 6.5): Hardware hat in den letzten Jahrzehnten drastische Kapazitäts- und Leistungssteigerungen erfahren (vgl. Kapitel 8.1). In Verbindung mit dem übergreifenden Trend zur Miniaturisierung finden sich verschiedene Computertechnologien in immer mehr Endgeräte wieder (vgl. Abschnitt 9.2). In der Folge erreichen kleine Geräte wie Mobiltelefone heute schon Rechenleistungen und Speicherkapazitäten, die vor zehn Jahren noch großen, stationären Rechnern vorbehalten waren. Zusammen mit hohen drahtlosen Übertragungskapazitäten ermöglichen sie damit die Nutzung komplexer elektronischer Dienste auch unabhängig vom jeweiligen Standort des Anwenders (vgl. Abschnitt 9.3). Ebenfalls stark auf Kapazitäts- und Leistungssteigerung angewiesen sind Anwendungen im Bereich digitale Medien. Abschnitt 9.7 untersucht die Produktion und Verbreitung von digitalen Filmen (Video-on-Demand und digitales Kino), während Abschnitt 9.9 die darauf aufbauenden Geschäftsmodelle analysiert.

**Konvergenz** (Abschnitt 6.6): Dem Trend zur Konvergenz wird in diesem Teil der Studie ein eigenes Kapitel gewidmet (vgl. Abschnitt 9.7). Die Konvergenz der Medien-, Informations-, und Telekommunikationsindustrie führt zu völlig neuen Anwendungen und Geschäftsmodellen. Für viele neue Anwendungen konvergieren die Endgeräte. So wird es zukünftig möglich sein, über das Internet Fernsehen zu empfangen und mit dem Fernseher im Internet zu surfen. Im Abschnitt 9.2 werden konvergierende Endgeräte wie der Internetkühlschrank thematisiert. Im mobilen Bereich konvergieren beispielsweise PC, PDA und Mobiltelefon zu sogenannten Smartphones (vgl. Abschnitt 9.3).

**Miniaturisierung** (Abschnitt 6.7): Die Kombination der übergreifenden Trends Kapazitäts- und Leistungssteigerung mit Miniaturisierung fördert die Verbreitung von sehr leistungsfähigen Rechnern in fast allen Bereichen des täglichen Lebens. Damit verbunden ist eine große Zahl neuer Anwendungsmöglichkeiten (vgl. Abschnitt 9.2). Besonders aber im mobilen Einsatz zeigt sich dieser übergreifende Trend sehr ausgeprägt, wie immer kleinere Notebooks, PDAs und Mobiltelefone vor Augen führen (vgl. Abschnitt 9.3). Der Miniaturisierungstrend scheint bisher ungebrochen. Allerdings stößt er langsam an den Schnittstellen zum Menschen an Grenzen, da wegen der Bedienbarkeit Displays und Tastaturen kaum noch verkleinert werden können.

**Mobilität** (Abschnitt 6.8): Höhere Leistung und zunehmende Miniaturisierung fördern von der technischen Seite her den übergreifenden Trend zu Mobilität. Hinzu kommt der wachsende Bedarf der Anwender, zu jeder Zeit an jedem Ort auf alle notwendigen Daten für private oder geschäftliche Aufgaben zugreifen zu können. Dies ermöglichen sowohl stationäre Systeme, die auf zentral gehaltene Daten Zugriff gewähren können (vgl. Abschnitt 9.2), als auch mobile Systeme, welche Daten mitführen und Zugriff auf weitere Dienste über drahtlose Übertragungswege bieten (vgl. Abschnitt 9.3).

**Vernetzung und Flexibilisierung** (Abschnitt 6.9): Der übergreifende Trend der Vernetzung und der damit möglichen Flexibilisierung ist einer der wichtigsten Trends für viele Anwendungen und findet sich daher in allen Bereichen in diesem Kapitel wieder. So lassen sich sowohl Rechner (vgl. Abschnitt 9.2), als auch Menschen (über mobile Kommunikation, vgl. Abschnitt 9.3) und Organisationen (vgl. Abschnitte 9.4, 9.5 und 9.9) miteinander „vernetzen“, um die jeweiligen Stärken miteinander verbinden und flexibler auf

veränderte Bedingungen reagieren zu können. Es ist zu erwarten, dass dieser übergreifende Trend auch in vielen anderen Bereichen weiter an Bedeutung gewinnen wird, etwa in der öffentlichen Verwaltung (vgl. Abschnitte 9.1 und 9.8), im unternehmerischen Rechnungswesen (vgl. Abschnitt 9.6) oder auch in der vernetzten Online-Unterhaltung wie beispielsweise in Form von internetbasierten Computerspielen (vgl. Abschnitt 9.7).

**Verteilung und Dezentralisierung** (Abschnitt 6.10): Beide äußern sich besonders deutlich in digitalisierten Wertschöpfungsketten (vgl. Abschnitt 9.4) und modernen Organisationsstrukturen und Arbeitsformen (vgl. Abschnitt 9.5). Diese werden heute immer seltener zentralistisch gesteuert, sondern sind zunehmend auf verteilte Leistungserstellung ausgerichtet. Eine Folge davon sind auch neue Geschäftsmodelle wie Komponentenlieferanten und Application Service Provisioning (vgl. 9.9).

**Virtualisierung** (Abschnitt 6.11): Dieser übergreifende Trend findet sich bei vielen Anwendungen über das Internet, wie beispielsweise dem virtuellen Besuch von Geschäften, Messen oder Sportveranstaltungen wieder (vgl. Abschnitte 9.1 und 9.7). Virtualisierung zeigt sich auch deutlich in so genannten „virtuellen Unternehmen“, also Verbunde von einzelnen Unternehmen, die nach außen wie ein einzelnes, großes Unternehmen erscheinen und gemeinsam Produkte und Dienstleistungen erstellen und am Markt absetzen (vgl. Abschnitt 9.5). Beispielhaft wird dies bei der Gestaltung elektronischer Zahlungsverfahren genauer untersucht (vgl. Abschnitt 9.6).

Tabelle 9.1 stellt im Überblick dar, in welchen Anwendungsbereichen sich die übergreifenden Trends deutlich auswirken.

## 9.1 Anwendungen auf Basis der Internet-Infrastruktur

Die vielfältigen Anwendungsmöglichkeiten des Internet durchdringen die Gesellschaft im privaten wie auch im geschäftlichen Bereich. Einige exemplarische Entwicklungen sollen in diesem Abschnitt betrachtet werden. Das Internet ist ein Informations-, Kommunikations- und Unterhaltungsmedium. Der Anwender kann sich im Internet beispielsweise mit Produktinformationen versehen, private Videokonferenzen abhalten und virtuelle Orte wie Museen besuchen. Mit das bedeutendste Anwendungsfeld ist jedoch elektronischer Handel.

Die Studie geht an dieser Stelle der Frage nach, welche Bedeutung das Internet in Zukunft für den Handel haben wird. Der Trend, traditionelle Geschäftsprozess in IuK-Systemen abzubilden, wirft die Frage auf, wie sich einige Branchen durch den Einfluss der Informations- und Kommunikationstechnologien entwickeln werden. Im privaten Bereich werden Supermarkt-Artikel, Bücher und Reisen von den Experten auf ihre Eignung für den E-Commerce eingeschätzt. Als eines der wesentlichen Ergebnisse dieses Kapitels zeigt sich, dass im B2C (Business-to-Consumer) wie auch im B2B (Business-to-Business) einige Geschäftsprozesse durch das Internet vollständig substituiert, andere Prozesse dagegen lediglich unterstützt werden. Eine Form der Unterstützung ist die Bereitstellung von Unternehmens- und Produktinformationen. Wie der Privatkunde sich dort mit Informationen versorgen kann, so wird auch im geschäftlichen Bereich die Suche nach Zulieferern, Kooperationspartnern und Firmenkunden vorwiegend über das Internet abgewickelt. Der Umsatz im B2B E-Commerce ist in den letzten Jahren trotz der Einbrüche an den Kapitalmärkten und der Konsolidierung unter den Marktplatzbetreibern stark gestiegen. Aber auch die ersten B2C Marktplätze wie Ebay oder Autoscout24 haben im letzten Jahr den Break-Even-Point erreicht [Koll 03], [APS 02]. Dem B2C E-Commerce wird noch ein deutliches Wachstumspotenzial zugesprochen. Derzeit werden als Hemmnisse für den Online-Handel vor allem nicht ausreichende Sicherheitsmechanismen von den Endkunden angegeben (vgl. Abschnitt 9.8). Gerade die Sicherheitsmechanismen, insbesondere die digitale Signatur, sind Grundvoraussetzung für das aufkommende Schwerpunktthema in der Informations- und Kommunikationsindustrie: dem E-Government [PiQu 01]. Einige Verfahrensvorgänge der öffentlichen Verwaltung werden bereits über das Internet angeboten, wie beispielsweise die Abgabe der Steuererklärung in elektronischer Form. Im Rahmen dieser Befragung wurden exemplarisch Behördengän-

KLUFT ZWISCHEN INTERNET-NUTZERN UND -NICHTNUTZERN: Der Digital Divide wird sich in den kommenden Jahren weiter vergrößern.

PRIVATE TÄGLICHE AUFGABEN: Aufgaben des privaten Bereichs werden in Zukunft vermehrt über das Internet abgewickelt werden

ONLINE GEKAUFTE PRODUKTE DES TÄGLICHEN BEDARFS: Der Anteil von Online-Einkäufen von Produkten des täglichen Bedarfs wird in 10 Jahren von 2% auf 18% angestiegen sein.

| | | Ausprägung im Bereich Anwendungen | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Anwendung auf der Basis der Internet-Infrastruktur | Allgegenwärtige Verbreitung von Kleinstcomputern | Nutzung mobiler Dienste | Digitalisierung und Automatisierung von Wertschöpfungsketten | Flexibilisierung von Organisationsstrukturen und Arbeitsformen | Controlling, Finanzdienstleistungen und Zahlungsverfahren | Konvergenz von Informations-Unterhaltungsmedien | Konvergenz von Informations- und Unterhaltungsmedien | Entstehung neuer Geschäftsmodelle und Märkte | 2003 | 2000 |
| Übergreifende Trends | Automatisierung und Vereinfachung | ● | ● | | ● | | ● | | ● | | ◔ | ◔ |
| | Dienst und Komponentenorientierung | | | ● | | | | | | ● | ◔ | ◑ |
| | Globalisierung und Wettbewerb | ● | | | ● | ● | | | | ● | ◑ | ◕ |
| | Integration und Standardisierung | | ● | | ● | ● | | | | | ◑ | ◑ |
| | Kapazitäts- und Leistungssteigerung | | ● | ● | | | | ● | | ● | ◑ | ◕ |
| | Konvergenz | | ● | ● | | | | ● | | | ◔ | ◔ |
| | Miniaturisierung | | ● | ● | | | | | | | ◔ | ◔ |
| | Mobilität | | ● | ● | | ● | | | | | ◔ | ◔ |
| | Vernetzung und Flexibilisierung | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ◕ |
| | Verteilung und Dezentralisierung | | | | ● | ● | | | | ● | ◔ | ◕ |
| | Virtualisierung | ● | | | | ● | ● | ● | | | ◑ | ◑ |

Tabelle 9.1: Ausprägungen übergreifender Trends im Anwendungsbereich

ge, Bürgersprechstunden und öffentliche Informationsveranstaltungen betrachtet.

## Ergebnisse

Mit der wachsenden Bedeutung des Internet für nahezu alle Bereiche des täglichen Lebens (Information, Bildung, Unterhaltung, Business) wachsen auch die Auswirkungen auf diejenigen Personengruppen, die nicht an das Internet angeschlossen sind. Die nationale wie auch die internationale Kluft zwischen Internet-Nutzern und -Nichtnutzern – bezeichnet als so genannter „Digital Divide" – wird sich in den kommenden Jahren weiter vergrößern (vgl. Abbildung 9.1). Hier unterscheiden sich die Aussagen der Experten aus dieser Studie nicht von denen der Vorgängerstudie [SETIK 00].

Einige private tägliche Aufgaben werden bereits heute durch Anwendungen auf Basis der Internet-Infrastruktur unterstützt. Die Experten prognostizieren jedoch für die kommenden Jahre einen deutlichen Anstieg der Bedeutung des Internet für die private Nutzung (vgl. Abbildung 9.2). Sie sehen beispielsweise großes Entwicklungspotenzial in der Kommunikation mit Behörden, dem E-Government. Informations- und Bildungsangebote werden in Zukunft vermehrt über das Internet bezogen werden. Die bereits genutzten Angebote wie Bankgeschäfte und Reisebuchungen werden weiter ausgebaut sowie E-Commerce und Versandhandel vermehrt von Privatpersonen akzeptiert.

Das Internet wird in Zukunft von Privatnutzern vermehrt als Einkaufsplattform genutzt werden. Online gekaufte Produkte des täglichen Bedarfs haben nach Aus-


Abbildung 9.1: Bedeutung des Digital Divide

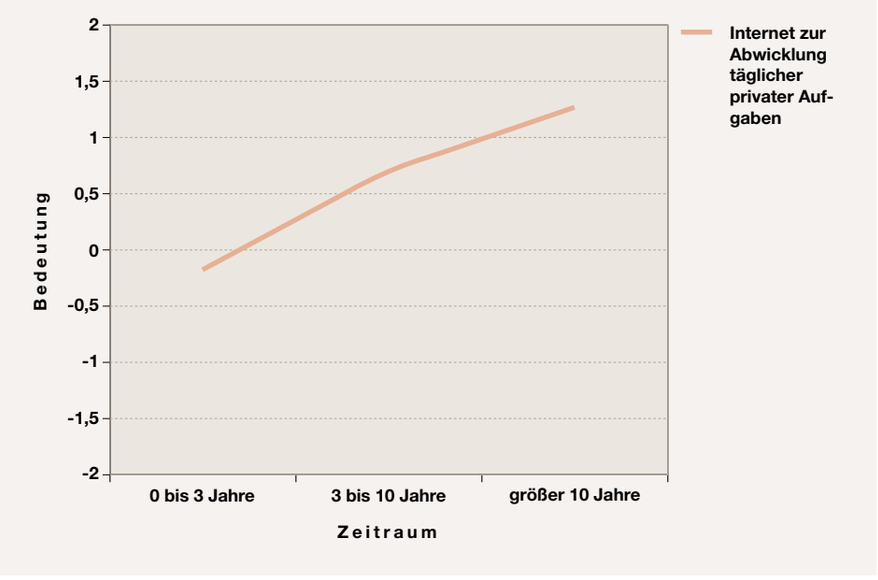



Abbildung 9.2: Bedeutung des Internet als wesentliche Infrastruktur für die Abwicklung täglicher privater Aufgaben

ONLINE-DIENSTLEISTUNGEN: In 3 Jahren wird der traditionelle Handel durch Online-Dienstleistungen erweitert sein.

BUCHHANDEL: Der Buchhandel im Internet wird den klassischen Buchhandel nicht ersetzen.

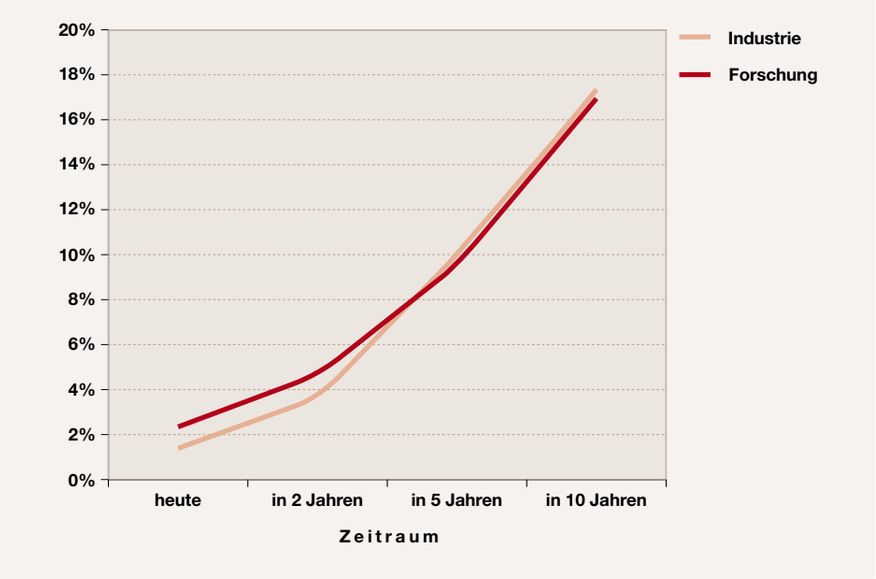



Abbildung 9.3: Anteil an Online-Einkäufen von Produkten des täglichen Bedarfs

sagen der Experten heute einen Anteil von etwa 2% des privaten Handels. Sie erwarten, dass sich der Anteil in den kommenden zwei Jahren verdoppeln wird. In fünf Jahren werden etwa 9% des täglichen privaten Konsums und in zehn Jahren fast 18% über das Internet abgewickelt werden (vgl. Abbildung 9.3). Die Prognosen der Experten aus der Wirtschaft sind bei dieser Frage nahezu deckungsgleich mit den Aussagen der Wissenschaftler. Viele Güter des täglichen Bedarfs lassen sich jedoch nur bedingt online handeln. Als größtes Problem sehen die Experten die Abwicklung der Logistik. Gerade Produkte des täglichen Bedarfs sollen häufig sofort benutzt oder konsumiert werden können. Je schneller die Lieferung erfolgt, um so eher ist der Kunde bereit, auch solche Güter online zu bestellen. Der Online-Handel wird den traditionellen Handel nur unterstützen. Das Internet wird nicht das kommunikative und soziale Erlebnis des Einkaufens, sowie das Betrachten und Aussuchen eines realen Produkts ersetzen.

Die IuK-Technologien bieten vielfältige Möglichkeiten, bestehende Geschäftsprozesse zu unterstützen. Im geschäftlichen Bereich wird es in Zukunft vermehrt Online-Dienstleistungen geben, die den stationären (Offline-) Handel ergänzen. Im Vordergrund steht nach Ansicht der Experten die Möglichkeit, mit dem Kunden zu kommunizieren, ihm Informationen über Produkte anzubieten und weitergehende Dienstleistungen wie Ordertracking oder Beschwerdemanagement anzubieten. Diese Entwicklung wird bereits in den kommenden drei Jahren erwartet (vgl. Abbildung 9.4, ①). Um den Kunden mit solchen Dienstleistungen optimal zu erreichen, fordern die Experten als notwendige technologische Entwicklung breitbandige mobile Netze.

Als eine Möglichkeit, wie durch das Internet ein traditionelles Geschäftsmodell ersetzt werden kann, wird B2C E-Commerce am Beispiel „Buchhandel" betrachtet. Der große Markterfolg etwa von Amazon lässt fragen, wann das Internet den klassischen Buchhandel ablösen wird. Die befragten Experten waren sich jedoch - wie auch in der Vorgängerstudie - einig, dass diese Entwicklung nie eintreffen wird (vgl. Abbildung 9.4, ②). Stattdessen haben sie auf die Möglichkeit der Unterstützung des klassischen Buchhandels bei der Beratung des Kunden durch die Internettechnologie verwiesen. Übereinstimmend wird die Auffassung vertreten, dass der Anteil an online gehandelten Büchern in den kommenden Jahren noch weiter steigen wird. Interessanter erschien ihnen in diesem Zusammenhang die Betrachtung von eBooks, dem digitalen Vertrieb von Buchinhalten. Die Entwicklung von elek-

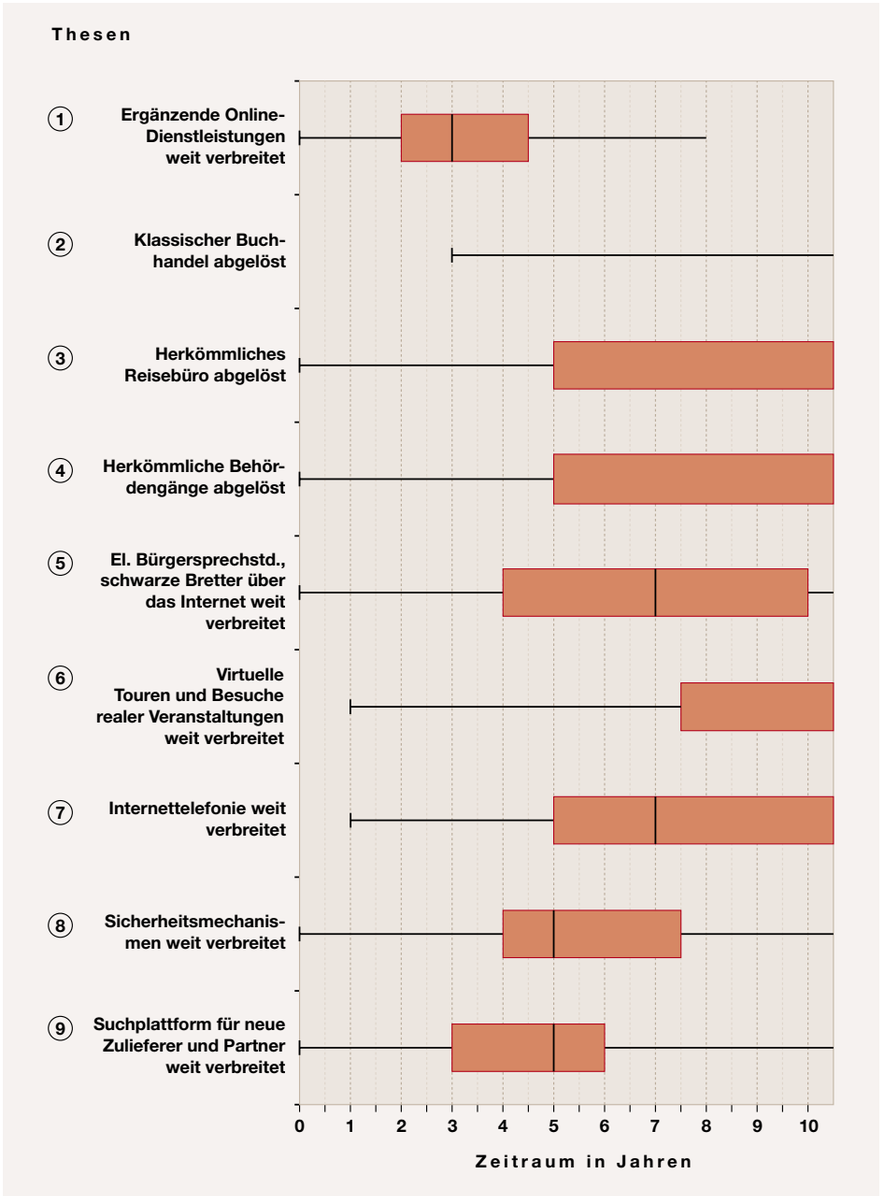



Abbildung 9.4: Ergebnisse der Thesen zu Anwendungen auf Basis der Internet-Infrastruktur

tronischem Papier und elektronischer Tinte könne zu gravierenden Veränderungen im Buchhandel führen.

Ein weiteres Beispiel in dieser Betrachtung ist die Frage nach der sich verändernden Bedeutung von Reisebüros. Auch hier lassen sich erfolgreiche Beispiele aus der Praxis anführen, wo Unternehmen Flugtickets ausschließlich über das Internet vertreiben, um Kosten zu sparen [MM 02]. Diese Frage wird von den Experten uneinheitlicher beantwortet als die Frage über den Buchhandel. Der Großteil der Befragten sieht eine Ablösung der Reisebüros durch das Internet erst in mehr als zehn Jahren (vgl. Abbildung 9.4, ③). Jedoch erwarten einige Experten die Ablösung der Reisebüros bereits im Jahr 2008, wohingegen ein anderer Teil dieses Ereignis wie beim Buchhandel nie eintreffen sieht. Der Blick auf die Vorgängerstudie zeigt ein ähnliches Antwortbild. Auch damals gab es Experten, die das Jahr 2007 prophezeit hatten, während andere den Zeitraum über zehn Jahre oder gar nie angegeben hatten. Eine wesentliche Aufgabe des Reisebüros liegt in der Beratung. Um diese Leistung adäquat durch eine Internetanwendung umsetzen zu können, erfordert es nach Ansicht der Experten noch vielfältigen Entwicklungsaufwand. Die Inhalte der Internetseiten müssten stärker multimedial ausgerichtet sein, beispielsweise durch 3D-Virtualisierungen der Reiseziele. Vorteile würden sich ergeben durch intelligente Routenplanung sowie Preisvergleiche.

REISEBÜROS: Das traditionelle Reisebüro wird erst in über 10 Jahren durch Internet-Angebote abgelöst werden.

BEHÖRDENGÄNGE: Behördengänge werden frühestens in 10 Jahren überflüssig.

ELEKTRONISCHE BÜRGERSPRECHSTUNDEN, SCHWARZE BRETTER: Elektronische Bürgersprechstunden, schwarze Bretter und Informationsveranstaltungen werden in 7 Jahren weit verbreitet sein.

BESUCHE VON REALEN VERANSTALTUNGEN: Virtuelle Besuche von Museen und Sportveranstaltungen werden erst in über 10 Jahren weit verbreitet sein.

Auch im Bereich der Verwaltungen greifen die Möglichkeiten der neuen Technologien. Dem Bürger werden durch E-Government in Zukunft Behördengänge abgenommen. Es bleibt die Frage, ob es hier zu einer Ablösung oder nur zu einer Ergänzung kommen wird. Die Experten antworten wie bei der Frage nach dem Reisebüro uneinheitlich. Für eine Gruppe werden Behördengänge erst in mehr als zehn Jahren überflüssig; für eine andere tritt diese Entwicklung bereits in fünf Jahren ein, während eine dritte Gruppe sie völlig verneint (vgl. Abbildung 9.4, ④). Im Vergleich zu der Vorgängerstudie hat sich auch bei diesem Thema die Meinung der Experten nicht gewandelt. Es wird auch hier eher zu einer Ergänzung als zu einer Ablösung kommen. An- und Ummeldungen von Wohnungen und Kraftfahrzeugen, die bereits eingeführte elektronische Steuererklärung, sowie elektronische Wahlverfahren werden wichtige Anwendungen des E-Government werden. Als notwendige Vorraussetzungen nennen die Experten Internet-Sicherheitstechnologien wie Verschlüsselungsverfahren und digitale Signaturen (vgl. Abschnitt 9.8).

Das Internet ist für Informationsdienste wie elektronische Bürgersprechstunden, schwarze Bretter und für Informationsveranstaltungen geeignet. Die Experten erwarten, dass bis zum Jahr 2010 derartige Dienste weit verbreitet sind (vgl. Abbildung 9.4, ⑤). In der Vorgängerstudie wurde - etwas optimistischer - bereits das Jahr 2007 angegeben. Die notwendigen Technologien haben sich jedoch in den letzten drei Jahren kaum verändert. Für eine weite Verbreitung sind noch immer bevölkerungsübergreifende, breitbandige Internet-Zugänge notwendig. Auch müssen die Audio- und Videokonferenzsysteme weiterentwickelt werden. Sprechstunden werden sicherlich in vielen Verwaltungsbereichen und für Bevölkerungsgruppen, die dem Internet nicht aufgeschlossen gegenüberstehen, weiterhin persönlich stattfinden.

Der virtuelle Besuch von Kulturstätten wie Museen virtuell über das Internet wird nach Ansicht der Experten erst in über zehn Jahren eine weite Verbreitung finden (vgl. Abbildung 9.4, ⑥). Ebenso werden sich virtuelle Besuche von realen Veranstaltungen wie beispielsweise Fußballspielen oder Formel1-Rennen nicht in naher Zukunft durchsetzen. Die Experten bleiben somit bei den Aussagen der Studie 2000. Das persönliche Erlebnis bei einem realen Museumsbesuch oder bei einer Sportveranstaltung ist nicht elektronisch zu ersetzen. Sinnvoll erscheinen virtuelle Besuche von Museen eher zur Reisevorbereitung. Virtuelle Sportveranstaltungen profitieren sicherlich von Zusatzberichterstattungen. Um einem realen Besuch jedoch nahe zu kommen, muss die Darstellungsqualität gesteigert werden. Die Displaytechnologie muss scharfe, große und dreidimensionale Bilder liefern und der Ton einen realen dreidimensionalen Raumeindruck erzeugen können. Die daraus resultierenden hohen Datenmengen über das Internet zu vertreiben, erfordert breitbandige Netze. Als weitere mögliche Anwendungen werden Theater- und Kon-

zertveranstaltungen genannt. Zusätzliche Interaktionsmöglichkeiten erlauben auch virtuelle Hauptversammlungen.

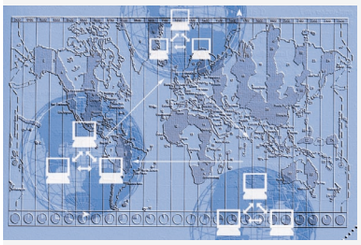
Im geschäftlichen Bereich wird das Internet schon jetzt als Suchplattform für neue Zulieferer und Kooperationspartner genutzt. Eine weite Verbreitung dieser Nutzungsweise erwarten die Experten bis zum Jahr 2008 (vgl. Abbildung 9.4, ⑦). In der Vorgängerstudie nannten sie noch das Jahr 2005. Die Entwicklung von standardisierten Beschreibungssprachen für Produkte und Dienstleistungen sind erforderlich, um automatisierte Plattformen zu schaffen. Durch eine Weiterentwicklung und Verbreitung des UDDI (Universal Description, Discovery and Integration) werden sich über das Internet angebotene Dienste und Web Services in Zukunft einfacher finden lassen (vgl. Abschnitt 9.4). Nach Aussagen der Experten können sich so agentenbasierte Kooperationsplattformen etablieren, über die schnell und kostengünstig geeignete Partner zur Bildung von virtuellen Netzwerken gefunden werden können. Gerade das Auffinden von Spezialanbietern wird über die Informationsmöglichkeiten im Internet deutlich vereinfacht.

Die Entwicklungen der Internettelefonie verliefen in den letzten drei Jahren langsamer, als die Experten im Jahr 2000 erwartet haben. Multimediale Konferenzen im privaten Bereich werden in der vorliegenden Studie erst in sieben Jahren und nicht schon in vier Jahren als weit verbreitet angesehen (vgl. Abbildung 9.4, ⑧). Benötigt werden wiederum breitbandige und kostengünstige Verbindungen, um eine hohe Marktdurchdringung von geeigneten Endgeräten zu erreichen. Neben Breitband-Festnetz nennen die Experten gerade auch mobile Breitband-Zugänge wie UMTS oder WLAN. Als mögliche Anwendungen sehen sie beispielsweise die Kommunikation mit älteren Menschen.

Für nahezu alle Anwendungen im Internet ist es erforderlich, Sicherheitsmechanismen bei Transaktionen zu verwenden (vgl. Abschnitt 7.1). Gerade in den Bereichen Online-Banking und E-Commerce ist die Notwendigkeit für den Einsatz von Sicherheitstechnologien offensichtlich, aber auch für zukünftig stattfindende virtuelle Behördengänge und Wahlen über das Internet sind sie unerlässlich. Ausgelöst durch immer wiederkehrende Pressemeldungen von aufgedeckten Sicherheitslöchern und geknackten Verschlüsselungscodes, hat sich derzeit noch keine breite Vertrauensbasis für Sicherheitstechnologien gebildet. Die Experten erwarten jedoch, dass in fünf Jahren Sicherheitsmechanismen allgemein als zuverlässig akzeptiert und weit verbreitet sein werden (vgl. Abbildung 9.4, ⑨). Zu den relevanten Technologien zählen sie Verschlüsselungssoftware auf Public-Key-Infrastruktur sowie die Anwendung digitaler Signaturen. Die Aufbewahrung des privaten Schlüssels sehen sie aber auch in fünf Jahren noch als Problem. Die Verwendung von Smartcards zur Speicherung des Schlüssels halten die Experten nicht für durchsetzungsfähig. Hingegen erwarten sie eine Verbreitung von biometrischen Verfahren zur Identifizierung und zur Ermittlung des privaten Schlüssels. Einig ist man sich darin, dass jedes Sicherheitssystem mit der Zeit gebrochen werden kann. Durch die Verbindung von Smartcards, biometrischen Verfahren und dem Einsatz von PIN-Nummern steigt der Aufwand für einen Missbrauch stark an, was bei den Nutzern Vertrauen für in die verwendete Sicherheitstechnologie bildet (siehe auch Abschnitt 7.3). In der Vorgängerstudie haben die Experten eine weite Verbreitung von Sicherheitsmechanismen dagegen bereits für das Jahr 2005 gesehen.

Gerade im Handel, sei es B2B oder B2C, stellt das Internet bereits heute die vorherrschende Infrastruktur für den Geschäftsverkehr in vielen Branchen dar. Im CRM zum Beispiel eröffnen sich gerade durch den Kontakt zum Kunden über das Internet viele Möglichkeiten. Auch für die Abwicklung geschäftlicher Prozesse wie SCM oder Logistikmanagement, für die Verknüpfung von ERP-Systemen oder die Kommunikation und Koordination von Unternehmen in virtuellen Organisationen wird die Architektur des Internet bereits jetzt verwendet. Nach Aussagen der Experten nimmt die Bedeutung des Internet als wesentliche Infrastruktur für die Abwicklung geschäftlicher Prozesse in den kommenden drei bis zehn Jahren und darüber hinaus noch weiter zu (vgl. Abbildung 9.5).

Die Bedeutung des E-Business innerhalb der verschiedenen Branchen wird in den kommenden Jahren weiter ansteigen. Langfristig bilden sich deutlich Cluster heraus. Die Experten erwarten im ersten



SUCHPLATTFORM FÜR NEUE ZULIEFERER UND KOOPERATIONSPARTNER: Das Internet wird in 5 Jahren weit verbreitet als Suchplattform für neue Zulieferer und Kooperationspartner genutzt werden.

INTERNETTELEFONIE: Internettelefonie wird in 7 Jahren weit verbreitet sein.

SICHERHEITSMECHANISMEN: Sicherheitsmechanismen sind in 5 Jahren als zuverlässig akzeptiert und weit verbreitet.

ABWICKLUNG GESCHÄFTLICHER PROZESSE: Die Bedeutung des Internet als Infrastruktur für die Abwicklung geschäftlicher Prozesse nimmt weiter zu.

BEDEUTUNG DES E-BUSINESS: Die Bedeutung des E-Business wird in den kommenden Jahren in allen Branchen weiter zunehmen.

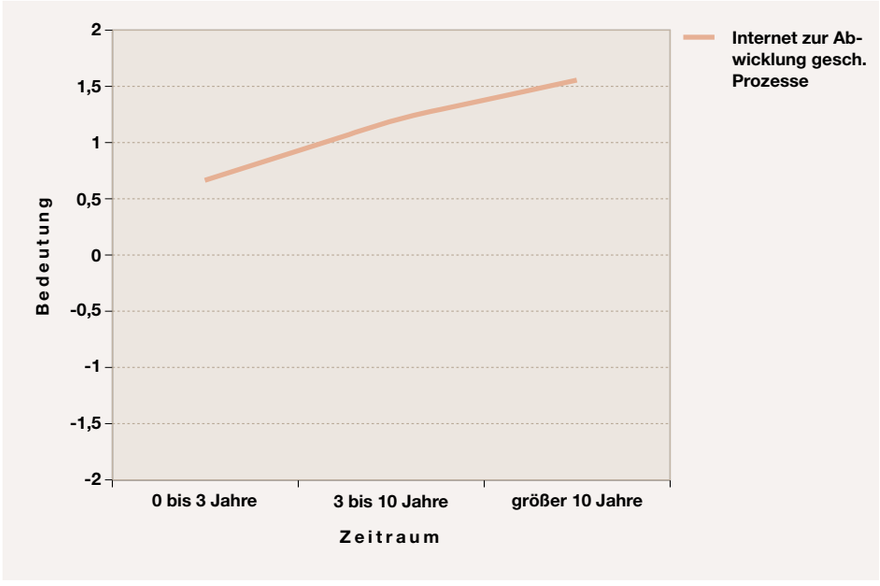



Abbildung 9.5: Bedeutung des Internet als wesentliche Infrastruktur für die Abwicklung geschäftlicher Prozesse

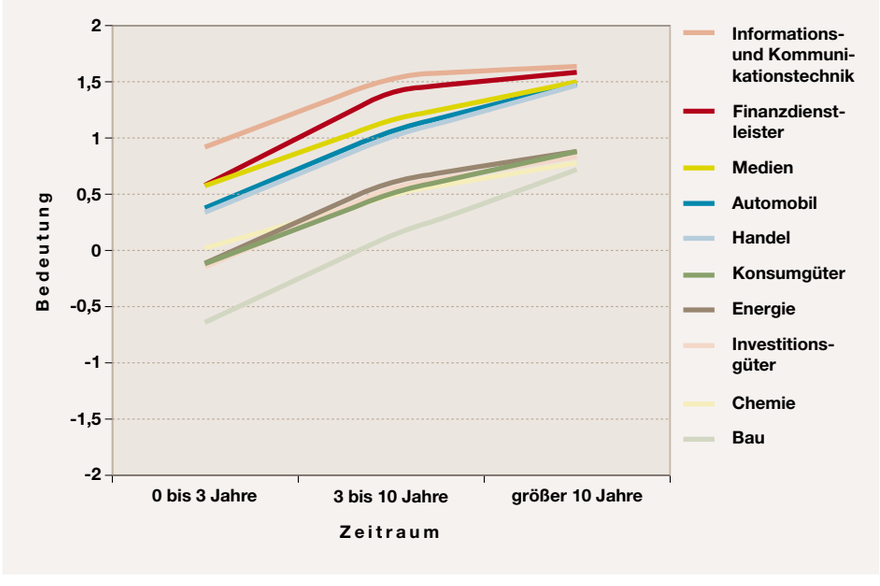



Abbildung 9.6: Bedeutung des E-Business in unterschiedlichen Branchen

Cluster einen starken Anstieg der derzeit noch geringen Bedeutung in den Branchen Bau, Chemie, Energie und Investitionsgüter auf ein mittleres Niveau in den nächsten drei bis zehn Jahren (vgl. Abbildung 9.6). Bereits heute spielt E-Business im zweiten Cluster, in den Branchen Automobil, Finanzdienstleistung, Informations- und Kommunikationstechnik, Handel und Medien, eine große Rolle. Die Experten erwarten für die kommenden Jahre einen stetigen Zuwachs der Bedeutung auf ein sehr hohes Niveau.

Nachfolgend werden die Aussagen der Experten zu den Anwendungmöglichkeiten elektronischer Geschäftsabwicklung in den verschiedenen Branchen kurz aufgelistet. Detailliertere Analysen zu den Themenbereichen finden sich in späteren Abschnitten. Eine E-Business Anwendung in der Automobilbranche ist das „global sourcing" von Zulieferteilen zu günstigen Auktionspreisen über einen Internet-Marktplatz. Ein prominentes Beispiel ist der Covisint-Marktplatz. Aber auch die vernetzte Fahrzeugkonstruktion, über globale Standorte verteilt, das Supply-Chain-Management mit der Just-in-Time Belieferung der Produktionsstraßen sowie der Kundenkontakt mit Information, Einkauf und Service sind bereits internetgestützt (vgl. Abschnitt 9.5). Im Finanzsektor ermöglicht das Internet eine Ablösung des Filialgeschäfts. Online-Banking und Online-Brokerage, wie auch die Nutzung des Internet als CRM-Tool und Informationsplattform, werden weiter an Bedeutung gewinnen (vgl. Abschnitt 9.6). In der Informations- und Kommunikationstechnik wird gerade die Einführung der UMTS-Netze einen bedeutenden Zuwachs an M-Commerce mit sich bringen. Local-Based-Services können mobile Beratungen und gezielte Produktbewerbungen ermöglichen, die den Handel positiv beeinflussen (vgl. Abschnitt 9.3). Sehr interessante Entwicklungen werden sich in der Medienbranche zeigen. Das Internet bietet neue Absatzwege gerade für Medieninhalte. Video-on-Demand wird in Zukunft ermöglicht und über das Internet vertrieben werden können. Dem entgegen stehen jedoch die derzeitigen Probleme durch File-Sharing-Tools und Online-Tauschbörsen, die empfindlichen Schaden in der Medienindustrie anrichten (vgl. Abschnitt 9.7).

Die Baubranche ist in Bezug auf E-Business nur wenig entwickelt. Dabei bieten sich durch das Internet vielfältige Möglichkeiten. Der Einkauf von Baumaterialien über Marktplätze wird sich in Zukunft etablieren. Der elektronische Austausch von Konstruktionsplänen sowie deren Visualisierung für den Kunden wird sich weiter entwickeln. Und schließlich werden Ausschreibungen für Bauaufträge vorwiegend online über das Internet abgewickelt. Der persönliche Kontakt zwischen den verschiedene Unternehmen ist gerade in der Baubranche besonders wichtig. Jedoch zeigt sich durch die oben von den Experten angeführten Punkte, dass auch hier die Bedeutung des E-Business in den kommenden Jahren zunehmen wird. In der Chemiebranche ist der Handel von Grundstoffen und Endprodukten über das Internet möglich. Die Energiebranche hat in Zukunft die Möglichkeit, neben Fernwartung der Kunden, zum Beispiel dem Ablesen von Zählerständen, auch den Vertrieb und das Rechnungswesen über das Internet abzuwickeln. Auch wird sich ein Energiehandel über Internetbörsen etablieren. Bei den Investitionsgütern, gerade im Anlagen- und Maschinenbau, zeigen sich ähnliche Tendenzen. Neben der Einkaufs- und Verkaufsunterstützung ermöglicht hier das Internet wiederum effiziente Fernwartung. Die kundenorientierte Planung und Entwicklung wird in Zukunft durch das Internet vermehrt unterstützt werden, und somit die Bedeutung des E-Business auch für diese Branche steigen.

Das Internet wird in Zukunft als Vertriebsplattform zur Akquisition neuer Kunden nur leicht an Bedeutung gewinnen. Die Experten unterscheiden in dieser Prognose nicht zwischen Großunternehmen und Mittelstand. Den Großunternehmen wird eine geringfügig höhere Nutzung dieser Anwendung zugesprochen (vgl. Abbildung 9.7). Die Experten begründen ihre Aussage damit, dass persönliche Kontakte weiterhin erforderlich seien. Key Accounts und Entscheider ließen sich nicht über das Internet finden. Es wird zu einer Koexistenz der verschiedenen Absatzwege kommen.

VERTRIEBSPLATTFORM ZUR AKQUISITION NEUER KUNDEN: Das Internet wird nicht die vorherrschende Vertriebsplattform zur Akquisition neuer Kunden werden.

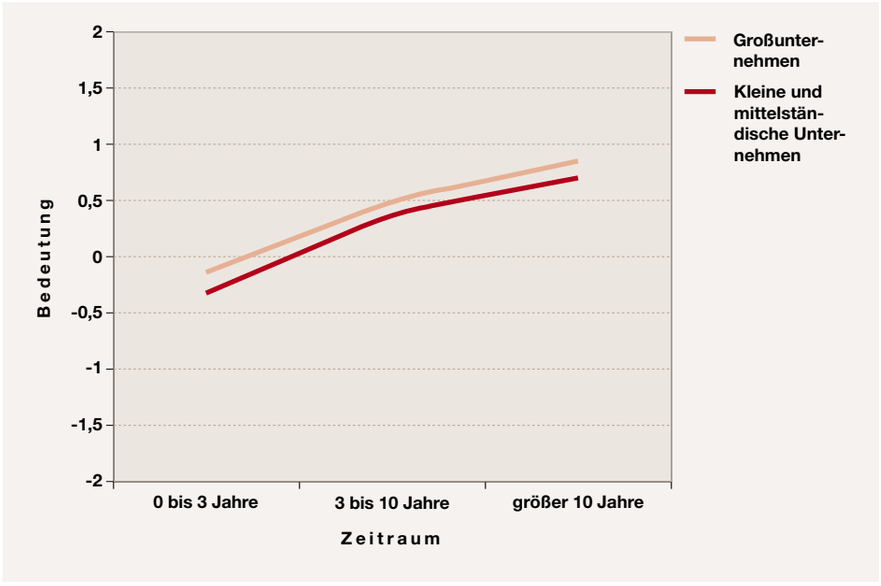



Abbildung 9.7: Bedeutung des Internet als Vertriebsplattform zur Akquisition neuer Kunden

## Zusammenfassung

Dieser Fragenkomplex hat die zunehmende Bedeutung des Internet auf nahezu alle privaten und geschäftlichen Bereiche deutlich gemacht. Das Internet ermöglicht viele ergänzende Anwendungen zu traditionellen Geschäftsprozessen und Verhaltensweisen, wird diese jedoch nicht ersetzen. Persönliche Kontakte und reale Eindrücke lassen sich nicht virtualisieren. Folgende Ergebnisse lassen sich bei der Befragung nach den Anwendungen auf Basis der Internet-Infrastruktur erkennen:

- Die Kluft zwischen Personen, die das Internet nutzen und denen, die es nicht nutzen, wird sich in den kommenden Jahren weiter vergrößern.
- Die Bedeutung des Internets als Element der Infrastruktur wird für die Abwicklung täglicher Aufgaben des privaten Bereichs in den nächsten Jahren stark ansteigen.
- Der Anteil an Online-Einkäufen von Produkten des täglichen Bedarfs wird in den nächsten zehn Jahren von derzeit 2% auf etwa 18% ansteigen.
- Den stationären (Offline-) Handel durch Online-Dienstleistungen zu erweitern, wird im Jahr 2006 weit verbreitet sein.
- Buchhandel und Reisebüro im Internet werden die traditionellen Angebote nie, bzw. erst in über zehn Jahren ersetzen.
- Herkömmliche Behördengänge werden nicht generell innerhalb der nächsten zehn Jahre durch virtuelle Behördengänge abgelöst, einige Anwendungen des E-Governments werden jedoch in den kommenden Jahren ergänzend eingeführt werden.
- Elektronische Bürgersprechstunden, elektronische schwarze Bretter und elektronische Informationsveranstaltungen werden bis zum Jahr 2010 weit verbreitet sein.
- Virtuelle Besuche von Museen und Sportveranstaltungen werden erst in über zehn Jahren weit verbreitet sein.
- Das Internet wird im Jahr 2008 weit verbreitet als Suchplattform für neue Zulieferer und Kooperationspartner genutzt werden.

- Internettelefonie wird bis zum Jahr 2010 weit verbreitet sein.
- Sicherheitsmechanismen werden im Jahr 2008 allgemein als zuverlässig akzeptiert und ihre Verwendung wird weit verbreitet sein.
- Die Bedeutung des Internets als wesentliche Infrastruktur für E-Business Anwendungen nimmt in allen Branchen in den kommenden Jahren weiterhin stark zu.
- Das Internet wird bei Großunternehmen wie auch beim Mittelstand nicht die vorherrschende Vertriebsplattform zur Akquisition neuer Kunden werden. Die Bedeutung steigt nur leicht in den kommenden Jahren.

## 9.2 Allgegenwärtige Verbreitung von Kleinstcomputern

Mark Weiser hat bereits vor einem Jahrzehnt die Idee vom „ubiquitous computing", also „überall integrierten Kleinstcomputern" aufgeworfen, da der klassische PC viel zu dominant sei und von den eigentlichen Aufgaben ablenke [Weis 91]. Er erwartet in seiner Vision die Verbreitung von Prozessoren, Speichern, Sensoren und Kommunikationsschnittstellen in nahezu jedem erdenklichen Gegenstand. Eine Vernetzung all dieser „intelligenten" Gegenstände untereinander ermöglicht den Zugriff auf beliebige Informationen unabhängig von Ort und Zeit. Auch wenn einige Technologien zur Umsetzung dieser Vision noch deutlich weiterentwickelt werden müssen, so weisen doch viele der in dieser Studie untersuchten Trends in die notwendige Richtung, wie zum Beispiel die Fortschritte in Prozessor- oder Kommunikationstechnologie (vgl. auch Kapitel 8.1 und 8.2). Die Bedeutung der Entwicklung von „ubiquitous computing" hat auch die EU erkannt und fördert diese im Rahmen der Initiative „Disappearing Computer" [DCI 03]. Sind diese Überlegungen zum Teil sehr idealistisch, so umfasst der ähnliche Begriff „pervasive computing" die schon sehr weit entwickelten, konkreten Ansätze aus der Industrie. Hier stehen bereits verfügbare Technologien wie beispielsweise PDAs (Personal Digital Assistant), Bluetooth und XML (Extensible Markup Language) [XML 99] und damit heute schon mögliche Anwendung im Vordergrund [Matt 01].

Nach einer allgemeinen Einschätzung der Bedeutung von Kleinstcomputern sind die darauf folgenden Prognosen der Experten nach haushaltsbezogenem und personenbezogenem Einsatz aufgeteilt. Das Szenario des vollvernetzten Haushaltes basiert auf drahtgebundenen wie drahtlosen LANs (Local Area Network), Prozessoren in Haushaltsgeräten und Smart-Label für die Identifikation. Damit ließen sich dann Serviceroboter realisieren, die „lästige Hausarbeiten" verrichten und sich dabei vom Internet aus steuern lassen. Am Ende stünde eine vollständig automatisierte Haushaltslogistik inklusive Einkauf, Lieferung und Abfallbeseitigung, welche die Bewohner von diesen Aufgaben befreien könnte [IGS 01]. Dagegen ermöglichen von überall erreichbare Server mit allen persönlichen Daten, individuell konfigurierbare Inneneinrichtungen und einfachste Benutzerschnittstellen an portablen und multifunktionalen Endgeräten dem Anwender eine bisher nicht gekannte Mobilität, die er ohne Verlust seiner vertrauten Umgebung nutzen kann. Notwendig sind dazu PnP-Vernetzung (Plug-and-Play) von Endgeräten und das „Heranrücken" der Rechner an den menschlichen Körper über Brillen-Displays, in Kleidung integrierte oder sogar implantierte Computer.

KLEINSTCOMPUTER IN ALLTAGSGEGENSTÄNDEN: Sowohl für den privaten als auch für den geschäftlichen Einsatz nimmt die Bedeutung von Kleinstcomputern in den nächsten Jahren deutlich zu.

### Ergebnisse

Für eine erste Einschätzung dieses Themenkomplexes beurteilten die Experten die generelle Bedeutung der Kleinstcomputer in Alltagsgegenständen (vgl. Abbildung 9.8). Sowohl im privaten, als auch im beruflichen Bereich wird eine deutliche Zunahme in den nächsten Jahren erwartet, wobei die private Nutzung heute auf einem niedrigeren Niveau gesehen wird, als die geschäftliche. Auffällig ist, dass die Befragten aus dem wissenschaftlichen Umfeld die private Bedeutung heute sehr schwach einschätzen, die langfristigen Prognosen sich aber mit den Experten aus der Praxis decken. Ein erster Block untersucht nun die Potenziale für Kleinstcomputer im Rahmen von Gebäudesystemen mit Schwerpunkt auf privaten Haushalten (vgl. Abbildung 9.9).

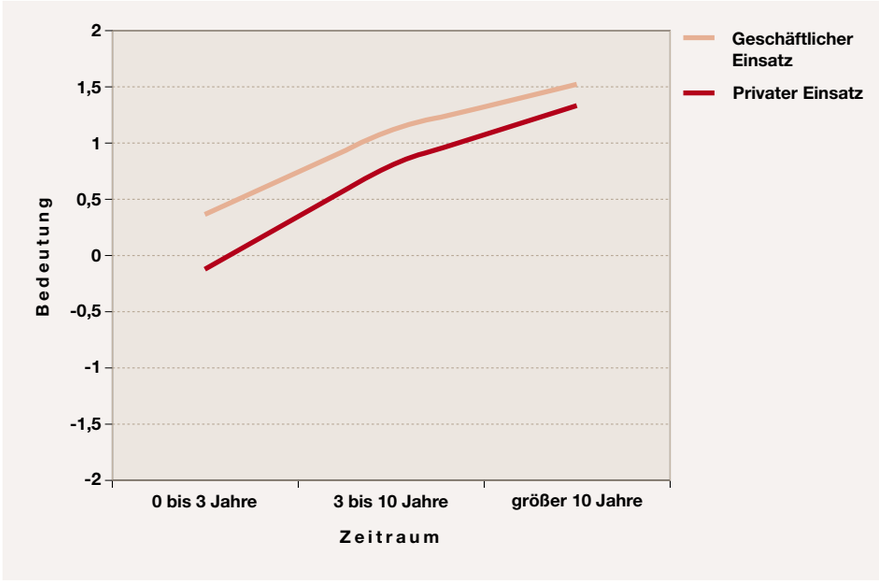



Abbildung 9.8: Bedeutung von Kleinstcomputern in Alltagsgegenständen

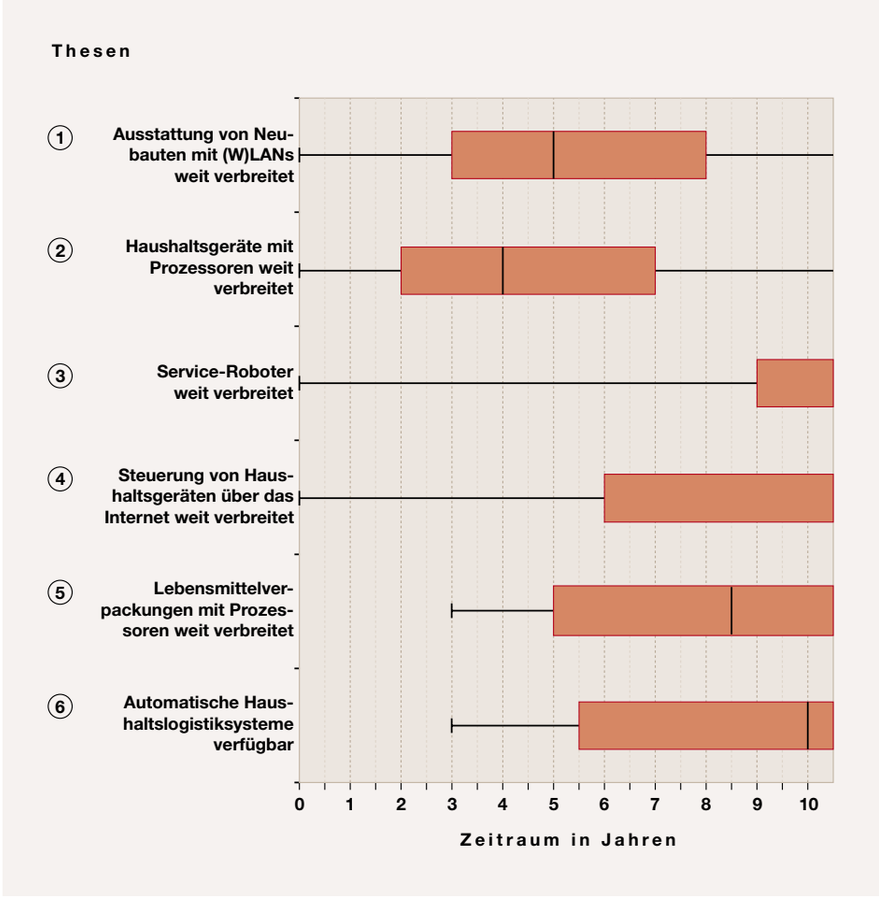



Abbildung 9.9: Ergebnisse der Thesen zu Kleinstcomputern in Haushalten

Wesentliche Grundlage für eine weit reichende Vernetzung verschiedenster Rechner innerhalb von Gebäuden ist die Verfügbarkeit einer geeigneten Netzinfrastruktur. Auch wenn alle notwendigen Technologien heute bereits zumindest für die drahtgebundene Verkabelung ausgereift sind, so erwarten die Experten eine weite Verbreitung des standardmäßigen Einbaus von (W)LANs in Neubauten erst in fünf Jahren (vgl. Abbildung 9.9, ①). Allerdings gilt diese Einschätzung vor allem für Wohnhäuser, da die meisten Bürogebäude bereits heute mit geeigneten Kabelschächten versehen sind und damit ohne großen Aufwand LANs verlegt werden können. Als Alternative zur herkömmlichen LAN-Verkabelung bieten sich drahtlose Technologien wie WLAN (Wireless LAN) und Bluetooth, aber auch die Nutzung der verlegten Stromleitung über den Powerline-Ansatz an. Hier besteht allerdings noch weiterer Entwicklungsbedarf vor allem hinsichtlich Reichweite und Sicherheit.

Damit die unterschiedlichsten Geräte in einem Haushalt überhaupt „intelligent" reagieren und miteinander interagieren können, müssen sie mit eigenen Prozessoren ausgestattet sein. So findet sich heute schon in vielen Geräten wie Kühlschränken, Mikrowellenöfen und Waschmaschinen Mikroelektronik, und es ist zu erwarten, dass ihr Funktionsumfang weiter zunimmt. Die Experten sehen daher eine weite Verbreitung von Prozessoren in Haushaltsgeräten bereits in vier Jahren (vgl. Abbildung 9.9, ②). Dazu sind aber weitere Anstrengungen bei der Zuverlässigkeit von Hard- und Software notwendig, denn die Verbraucher tolerieren keine häufig „abstürzenden" Geräte, vor allem wenn in der Folge größere Schäden entstehen können (z.B. verdorbene Lebensmittel durch einen nicht funktionierenden Kühlschrank).

Visionärer erscheinen Serviceroboter im täglichen Leben. Denkbare Aufgaben sind Haushaltsverrichtungen wie jegliche Art von Reinigung (Fassaden, Teppichboden, Rasen, Schwimmbad, etc.), aber auch die Unterstützung alter und kranker Menschen oder der Einsatz in Gefahrensituationen. Eine weite Verbreitung ist nach Meinung einiger Experten frühestens in neun Jahre zu erwarten, die meisten rechnen nicht innerhalb der nächsten zehn Jahre damit (vgl. Abbildung 9.9, ③), da auf der einen Seite viele notwendige Technologien noch deutlich weiter entwickelt werden müssen und auf der anderen Seite die Bereitschaft zur Nutzung derartiger Systeme noch kaum vorhanden ist. Der Vergleich zur Vorgängerstudie, in der nur ganz wenige Experten die breite Nutzung von Servicerobotern innerhalb der nächsten zehn Jahre erwartet haben, unterstreicht, dass sie diese Szenarien heute als weniger utopisch ansehen [SETIK 00].

Sind sowohl herkömmliche Haushaltsgeräte mit Prozessoren und Netzwerkanschlüssen ausgestattet, als auch der Haushalt durch Serviceroboter ergänzt, so ist ein weit reichender Zugriff auf Haushaltsgeräte über das Internet denkbar. Dieser kann sowohl zur Überwachung und Steuerung durch den Eigentümer dienen, als auch zur Fernwartung und -diagnose durch den Hersteller bei Defekten. Die Einschätzung der Experten weicht deutlich von der Prognose aus der Studie 2000 ab, denn die meisten Befragten halten eine weite Verbreitung in den nächsten zehn Jahren für unwahrscheinlich (vgl. Abbildung 9.9, ④). Als Voraussetzung wird die Verfügbarkeit der oben genannten Technologien und eine weitgehende Standardisierung der Schnittstellen genannt.

Ein weiterer Schritt ist die Ausstattung von Lebensmittelverpackungen mit integrierten Schaltkreisen, damit andere Geräte elektronisch Details von ihnen abfragen können. Für Produzenten und Händler eröffnet dies neue Möglichkeiten für effizientere Lagerhaltung, Logistik und Bezahlvorgänge. Beim Endkunden kann z.B. ein entsprechender Kühlschrank das Verfallsdatum überwachen und das Nachbestellen bestimmter Produkte vereinfachen. In Übereinstimmung mit der Vorgängerstudie halten die Befragten eine weite Verbreitung derartiger Szenarien allerdings erst in knapp neun Jahren für realistisch (vgl. Abbildung 9.9, ⑤). Auch wenn grundlegende Technologien (wie RFID (Radio Frequency Identification)) für erste Anwendungen bereits zur Verfügung stehen, sind noch Hürden wie weltweite Standardisierung einerseits und möglichst niedrige Kosten andererseits zu bewältigen, denn gerade der Handel ist eine globale Branche mit sehr hohem Margendruck.

(W)LANS IN NEUBAUTEN: Die Vernetzung in Gebäuden mit (W)LANs ist in 5 Jahren weit verbreitet.

PROZESSOREN IN HAUSHALTSGERÄTEN: Haushaltsgeräte sind in 4 Jahren zum Großteil mit Prozessoren ausgestattet.

Serviceroboter: Serviceroboter für die Unterstützung im Alltag sind in den nächsten 10 Jahren nicht auf breiter Front zu erwarten.

ZUGRIFF AUF HAUSHALTSGERÄTE ÜBER DAS INTERNET: Die Fernsteuerung von Haushaltsgeräten ist in den nächsten 10 Jahren nicht weit verbreitet.

LEBENSMITTELVERPACKUNGEN MIT INTEGRIERTEN SCHALTKREISEN: Chips in Verpackungen sind in 9 Jahren weit verbreitet.

Stehen die bis hier untersuchten Technologien auf breiter Basis in Haushalten zur Verfügung, sind in letzter Konsequenz Systeme möglich, die die komplette Logistik des Haushaltsbedarfs (oder auch von Restaurants) von der Bestellung bis zum Warenempfang automatisch abwickeln. Die Experten erwarten den Einsatz derartiger Systeme nicht vor dem Jahr 2013 (vgl. Abbildung 9.9, ⑥). Es sind noch viele Detailfragen zu klären, deren Lösungen sich zunächst in einem isolierten Teilbereich (siehe vorherige Thesen) bewähren müssen, bevor ein derart komplexes Gesamtsystem die Zuverlässigkeit für den täglichen Einsatz erreicht haben wird.

LOGISTIK DES HAUSHALTSBEDARFS: Systeme zu ihrer automatischen Abwicklung sind nicht in den nächsten 10 Jahre verfügbar.

Der zweite Block analysiert auf Personen konzentrierte Einsatzmöglichkeiten für Kleinstcomputer (vgl. Abbildung 9.10).

Um jederzeit von verschiedenen Standorten wie Büro, Hotel oder Wohnung alle wichtigen Daten verfügbar zu haben, müssen diese über einen Server mit eigenen Daten im Internet verfügbar sein. Unterschiedlichste Endgeräte (wie PC, Notebook, PDA, Mobiltelefon, MP3-Player) können dann über eine Art „privates Netzlaufwerk“ auf persönliche Einstellungen, Adressen, Kontakte, Emails und beliebige andere Dateien zugreifen. Obwohl die notwendigen Technologien und einige Pilotanwendungen bereits existieren, erwarten die Experten eine weite Verbreitung netzbasierter persönlicher Datenhaltung erst im Jahr 2012 (vgl. Abbildung 9.10, ①). Zu lösende Probleme sehen die Experten vor allem bei zu niedrigen Bandbreiten und bei rechtlichen und technischen Sicherheitsfragen ebenso, wie bei fehlenden profitablen Geschäftsmodellen.

SERVER MIT EIGENEN DATEN: Ortsunabhängiger Zugriff auf eigene Daten auf einem Internetserver ist in knapp 9 Jahren weit verbreitet.

Eine weitere Anwendung stärkerer Individualisierung ist die flexible Konfigurierbarkeit von Inneneinrichtungen. Im geschäftlichen Bereich sind Arbeitsplätze denkbar, die raum- und standortübergreifend die Einstellungen des Mitarbeiters übernehmen. Für Privatanwendungen eignen sich zum Beispiel Vorlieben für Hotelzimmer und Wohnanlagen, um hier einen „Heimat-Effekt“ zu erzielen, aber auch zu Hause, wenn unterschiedliche Personen abwechselnd verschiedene Räume nutzen. Eine weite Verbreitung derartiger Systeme sehen die Befragten in acht Jahren als realistisch an (vgl. Abbildung 9.10, ②), was eine leichte Verzögerung gegenüber der Vorgängerstudie darstellt. Notwendig wäre vor allem eine stärkere Abkehr vom papierbasierten Arbeiten, was allerdings nach den Expertenaussagen in Abschnitt 9.5 noch in weiter Ferne ist. Damit eng verbunden ist die einfache Einstellbarkeit und Bedienbarkeit dieser Individualisierungskonzepte.

FLEXIBLE KONFIGURIERBARKEIT VON INNENEINRICHTUNGEN: Eine weite Verbreitung von individuell einstellbaren Umgebungen ist in 8 Jahren realistisch.

Getreu dem Motto „Nur was ich bedienen kann, nutze ich auch!“ spielen intuitive und „mitdenkende“ Benutzerschnittstellen in fast allen elektronischen Geräten eine große Rolle (siehe auch Abschnitt 8.3.3). Dieser Aspekt ist besonders wichtig für eine weitere Verbreitung von Endgeräten und ihren Anwendungen über die bestehende und oft technikbegeisterte Nutzerbasis hinaus. Insbesondere bequeme oder ältere Menschen, die oft auch finanziell interessante Gruppen darstellen, ließen sich leichter als neue Kunden gewinnen. Die Einschätzung der Experten, dass derart einfache Benutzerschnittstellen erst im Jahr 2009 weite Verbreitung gefunden haben (vgl. Abbildung 9.10, ③), verdeutlicht das hier verborgene Verbesserungspotenzial. Die größte Hürde ist immer noch eine zuverlässige Spracheingabe, die, trotz großer Fortschritte, bisher nur in abgegrenzten Kontexten funktionieren. Weitere Möglichkeiten sind in einer standardisierten Symbolsprache (ähnlich wie bei CD-Playern) und während der Nutzung „dazu lernende“ Systeme zu sehen.

EINFACHE BENUTZERSCHNITTSTELLEN: Intuitive und mitdenkende Benutzerschnittstellen sind in 6 Jahre weit verbreitet.

Mobiltelefone sind ein gutes Beispiel für IuK-Technologie, die dank (meist) relativ einfacher Bedienbarkeit schnell eine hohe Verbreitung gefunden haben. Und neben der Möglichkeit zu telefonieren bieten sie zunehmend Funktionalitäten für umfangreiche Datendienste, wie Adressbuch, Kalender und Nachrichtenversand, die in den nächsten Jahren noch deutlich zunehmen werden, z.B. um Funktionalitäten wie bargeldlose Zahlungsfunktionen und Navigationssysteme. Hier steht die Frage im Mittelpunkt, wie gut multifunktionale Endgeräte künftig akzeptiert werden. Der nächste Abschnitt beleuchtet dann die Nutzung mobiler Dienste im Detail (Abschnitt 9.3). In der Studie 2000 erwarteten die Experten eine weite Verbreitung für das Jahr 2004, welche sich nun auf das Jahr 2008 verschoben hat (vgl. Abbildung 9.10, ④). Als Hauptgründe führen sie sowohl technische Hürden wie langsame und teure Internetverbindungen und zu komplexe Be-

MULTIFUNKTIONALE ENDGERÄTE: Kompakte Endgeräte mit umfangreicher Funktionalität sind in 5 Jahren weit verbreitet.

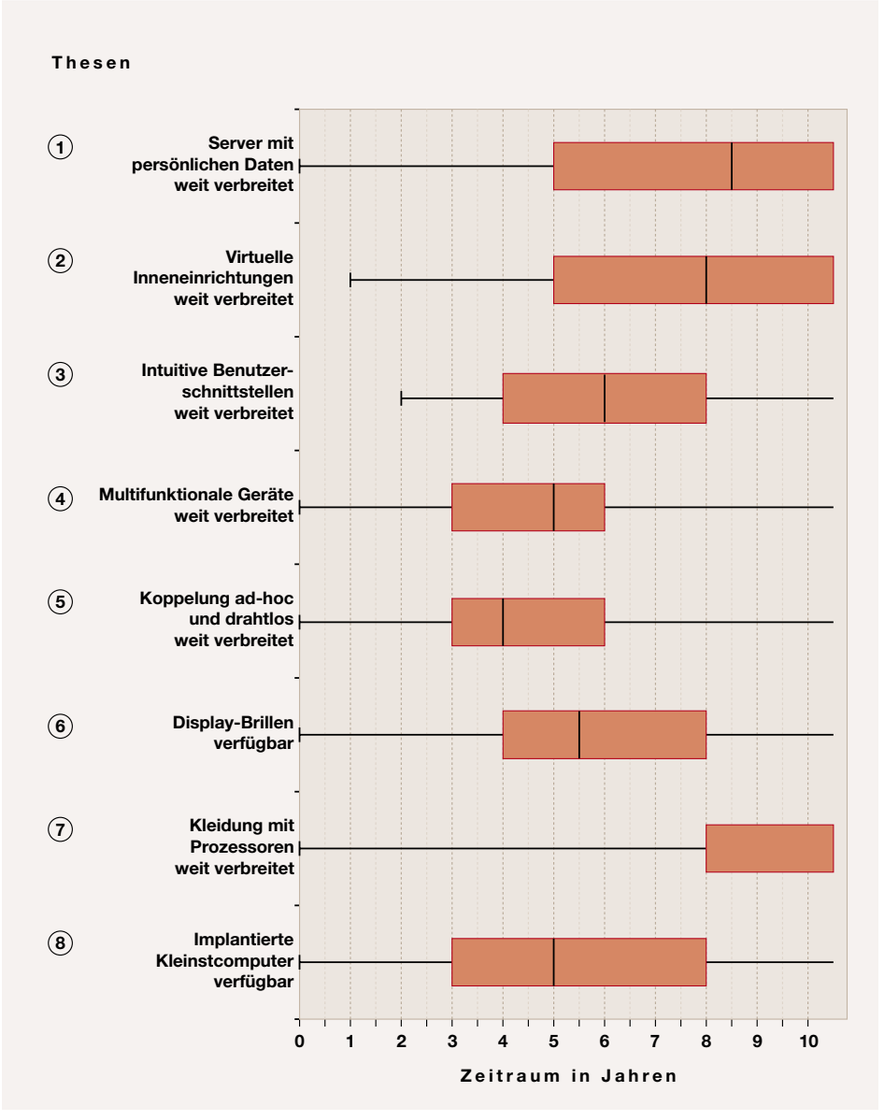



Abbildung 9.10: Ergebnisse der Thesen zu Kleinstcomputern im individuellen Einsatz

dienung der Datendienste an, als auch die Vermutung, dass die Nutzer mehrere spezialisierte Geräte einem Allroundgerät vorziehen (siehe auch Abschnitt 9.3).

Unabhängig davon wie sie im Detail aussehen werden, sollten sich Endgeräte ad-hoc und drahtlos miteinander koppeln lassen, um Daten für geschäftliche (z.B. Visitenkarten, Logistikdaten) und private (z.B. Kommunikation, Spiele) Anwendungen einfach austauschen zu können. Obwohl hier mit WiFi und Bluetooth die notwendigen Technologien bereitstehen und schon in vielen Produkten verfügbar sind, erwarten die Befragten eine weite Verbreitung erst in vier Jahren (vgl. Abbildung 9.10, ⑤). Probleme sehen die Experten in der Standardisierung der Protokolle auf höheren Kommunikationsebenen und bei der Implementierung geeigneter Sicherheitsmechanismen, wie Identifikation und Zugangsschutz.

Ein großes technisches Problem kompakter Endgeräte stellen die Displays dar, die heute maßgeblich Größe und Energieverbrauch bestimmen. Als Alternativen zu herkömmlichen Displays sind Brillen mit integrierten Displays denkbar, die auch eine Reihe neuer Anwendungen möglich machen, wie zum Beispiel als Navigationssystem, bei der technischen Wartung, in der Architektur und auch in der Unter-

ENDGERÄTE AD-HOC UND DRAHTLOS MITEINANDER KOPPELN: Die einfache Verbindung von Endgeräten ist in 4 Jahren weit verbreitet.

BRILLEN MIT INTEGRIERTEN DISPLAYS: Als Alternative zu herkömmlichen Displays sind Brillen mit Displays in 6 Jahren verfügbar.

haltung. Hier exisitieren schon seit einiger Zeit Prototypen und auch einige marktreife Produkte. Trotzdem halten die Experten derartige Brillen erst in knapp sechs Jahren für verfügbar (Abbildung 9.10, ⑥), da die Displaytechnik, die Datenanbindung und die Energieversorgung bisher noch nicht zufriedenstellend gelöst worden sind.

INTEGRATION VON KLEINSTRECHNERN IN KLEIDUNGSSTÜCKE: Eine weite Verbreitung von Rechnern in Kleidung ist die nächsten 10 Jahre nicht zu erwarten.

Einen weiteren Bereich tragbarer Computer stellt die Integration von Kleinstrechnern in Kleidungsstücke dar, zum Beispiel für Zugangsberechtigungen wie Skipässe oder die Überwachung gesundheitlich relevanter Messwerte. Trotz dieser denkbaren Anwendungsfelder zeigen sich die Experten pessimistisch, und nur wenige erwarten mit Computern versehene Kleidung innerhalb der nächsten zehn Jahre (vgl. Abbildung 9.10, ⑦). Als ein wesentlicher Grund führen sie die Schnelllebigkeit der Mode und den geringen Vorteil durch eine feste Integration an. Immerhin sind hier auch für angrenzende Bereiche interessante Forschungsfelder wie „Körper-LANs", Energieversorgung und Wasserbeständigkeit der Bauelemente zu finden.

IMPLANTATION VON COMPUTERN IN DEN MENSCHLICHEN KÖRPER: Derartige Ansätze sind in 5 Jahren verfügbar.

Noch einen Schritt weiter als Rechner in Kleidungsstücken geht die Implantation von Computern in den menschlichen Körper. Dies ermöglicht neue Anwendungen vor allem im medizinischen Bereich, zum Beispiel für die Überwachung von Kranken oder die präzise Dosierung von Medikamenten. Allerdings sind auch Möglichkeiten der persönlichen Datenspeicherung bis hin zum implantierten Personalausweis denkbar. Die Teilnehmer dieser Studie erwarten die Verfügbarkeit derartiger Technologien im Jahr 2008 (vgl. Abbildung 9.10, ⑧), sehen aber neben den technischen Herausforderungen im Bereich der Mikro- bzw. Nanotechnik vor allem Akzeptanzprobleme und ethische Bedenken als Hürden für eine weite Verbreitung. Allerdings fordern einige Experte mehr Mut und Kreativität, verfügbare Technologien sinnvoll einzusetzen, ohne die Risiken überzubewerten.

### Zusammenfassung

Hinsichtlich der Entwicklung und Verbreitung von Kleinstrechnern im Rahmen des „ubiquitous computing" ergeben die Prognosen der Experten ein differenziertes Bild:

- Generell nimmt die Bedeutung von Kleinstcomputern sowohl im geschäftlichen, als auch im privaten Umfeld in den nächsten Jahren deutlich zu.
- Die beiden Basistechnologien Prozessoren bzw. LANs sind in fast allen Geräten und Gebäuden in 2007 bzw. 2008 weit verbreitet.
- Eine weite Verbreitung über das Internet steuerbarer Haushaltsgeräte ist bis 2013 ebenso unwahrscheinlich, wie der breite Einsatz von Service-Robotern.
- Während Lebensmittelverpackungen in 2012 mit Schaltkreisen zur Identifikation ausgestattet werden, ist eine komplett automatisierte Haushaltslogistik bis 2013 nicht in Sicht.
- Über das Internet erreichbare Server mit allen persönlichen Daten sind 2012 weit verbreitet, individuelle und flexible Inneneinrichtungen bereits 2011.
- Multifunktionale Endgeräte sind 2008 weit verbreitet, unkompliziert und drahtlos können sie bereits 2007 verbunden werden, aber sehr einfache, intuitive und intelligente Benutzerschnittstellen stehen erst 2009 den meisten Engeräten zur Verfügung.
- Während Kleinstrechner in Kleidungsstücken bis 2013 keine weite Verbreitung finden, sind zumindest 2008 implantierbare Kleinstcomputer und 2009 Brillen mit Computerdisplays technisch ausgereift.

## 9.3 Nutzung mobiler Dienste

Die Zahl der Mobiltelefonnutzer ist in Deutschland noch rasanter gestiegen, als die des stationären Internets und rein statistisch betrachtet besitzen mehr als 50% aller Deutschen heute ein Mobiltelefon. Dieses rasante Wachstum überraschte selbst Unternehmen der Mobilfunkbranche und weckte in der Folge sehr hohe Erwartungen an Umsätze mit mobilen Diensten, die bis heute aber bei weitem noch nicht alle eingelöst wurden [Reic 02]. Dieser Abschnitt untersucht, inwiefern die

permanent an Leistungsfähigkeit zunehmenden mobilen Endgeräte herkömmliche Geräte ersetzen (siehe auch Kapitel 8.2.7), neue Dienste ermöglichen und damit weiter an Bedeutung für unsere Gesellschaft gewinnen können .

Von Diensten im stationären Internet unterscheiden sich mobile Dienste hinsichtlich der vier Spezifika Ortsflexibilität, „Personal Sphere“, ständige Konnektivität und Kontextsensitivität. Ortsflexibilität ist der wichtigste Aspekt, denn sie ermöglicht räumliche Unabhängigkeit bisher nur raumgebunden angebotener Dienste, wie Abrufen von Informationen oder Austauschen von Nachrichten. „Personal Sphere“ bezeichnet die Tatsache, dass es sich bei Mobiltelefonen noch mehr als bei PCs um persönliche Gebrauchsgegenstände handelt. Zu diesen bauen ihre Besitzer oft eine sehr enge Beziehung auf und bringen sie durch individuelle Anpassung der Geräte, z.B. durch besondere Gehäusefarben oder Hintergrundbilder, zum Ausdruck. Ständige Konnektivität fördert diese persönliche Bindung durch die durchgängige Erreichbarkeit, wie sie heute bereits am Kurznachrichtendienst SMS (Short Message Service) sehr geschätzt wird. Schließlich lässt die Kontextsensitivität, also das Berücksichtigen der Informationen, wo der Nutzer was, wann, mit welchen Zielen und Interessen tut, etliche neue Anwendungsfelder erwarten, z.B. Hinweise auf ein besonders günstiges Angebot in einem nahegelegenen Kaufhaus [RMF 02].

Da es für mobile Computersysteme prinzipiell eine nahezu unbegrenzte Zahl möglicher Anwendungen gibt, beschränkt sich diese Studie hier auf die folgenden Bereiche.

Nach einer generellen Einschätzung der Bedeutung von mobilen Diensten folgt die Untersuchung der künftigen Bedeutung unterschiedlicher Kommunikationsmedien. Neben Sprache hat sich in den letzten Jahren der Kurznachrichtendienst SMS überraschend schnell etabliert. Auf diesem Erfolg bauen die Nachfolgestandards EMS (Enhanced Message Service) mit einfachen Formatierungen, Ton und Grafiken und der auf noch umfangreichere Möglichkeiten ausgelegte MMS (Multimedia Message Service) auf. Einen Schritt weiter von schneller asynchroner hin zu synchroner Kommunikation geht das so genannte mobile Instant Messaging, also das „chatten“ mit einem oder mehreren Partnern in Echtzeit über die Tastatur des Mobiltelefons. Nachdem sich Mobiltelefone und PDAs (Personal Digital Assistant) immer weiter verbreiten, wird beispielhaft untersucht, wann mit einer Verdrängung papierbasierter Kalender und Adressbücher zu rechnen ist. Ein weiterer typischer Anwendungsbereich für mobile Geräte sind die so genannten LBS (Location Based Service), also ortsabhängige Dienste, als Spezialfall der Kontextsensitivität. Um nicht auf den Stand der Software bei der Auslieferung eingeschränkt zu sein, wird es immer wichtiger, auch Mobiltelefone nachträglich mit neuen Softwaremodulen ausstatten zu können. Andererseit verdrängen immer kleinere Notebooks zunehmend stationäre Personal Computer, so dass es nur noch eine Frage der Zeit ist, wann all diese Geräte in eine Klasse mobiler persönlicher Endgeräte konvergieren. Abschließend stehen exemplarisch für viele weitere denkbare Anwendungen zwei Szenarien im Mittelpunkt: zum einen die Unterstützung alter und kranker Menschen und zum anderen der Einsatz mobiler Rechner im Straßenverkehr.

## Ergebnisse

Die Bedeutung mobiler Computer und mobiler Kommunikation sehen die Experten in den nächsten drei Jahren weiter ansteigend (vgl. Abbildung 9.11). Danach erwarten sie allerdings nahezu eine Stagnation auf hohem Niveau, besonders im geschäftlichen Einsatz, denn hier gehört heute ein Mobiltelefon schon „dazu wie ein Anzug“. Die Experten aus der Praxis sehen hier sogar einen leichten Rückgang, was sie auf eine künftig höhere Verbreitung von Telekooperation zum Beispiel über Videokonferenzen und die daraus folgende verminderte Reisetätigkeit zurückführen (vgl. auch Abschnitt 9.5). Die gegenüber dem geschäftlichen Einsatz heute noch deutlich niedrigere Bedeutung mobiler Dienste im privaten Bereich verspricht hohes Wachstumspotenzial auch über die nächsten drei Jahre hinaus.

Weiteren Aufschluss über die unterschiedlichen mobilen Kommunikationswege gibt Abbildung 9.12. Eindeutig ist, dass die klassische Sprachtelefonie der wichtigste Kommunikationskanal bleiben wird, denn

BEDEUTUNG MOBILER COMPUTER UND MOBILER KOMMUNIKATION: Mobilität gewinnt weiter an Bedeutung, stagniert aber auf lange Sicht.

KLASSISCHE SPRACHTELEFONIE: Mündliche Kommunikation wird auch künftig die mobile Nutzung dominieren, wenn auch ergänzt durch SMS und MMS.

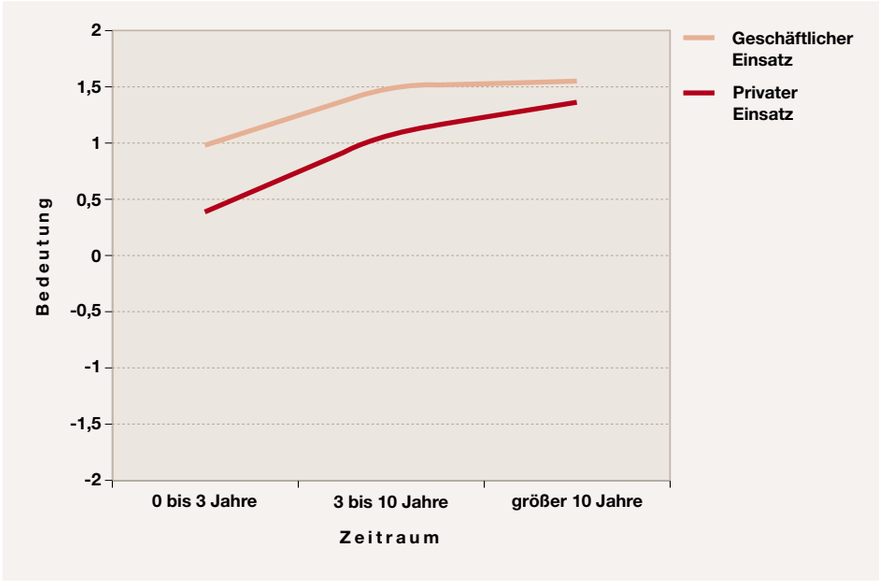



Abbildung 9.11: Bedeutung mobiler Computer und mobiler Kommunikation

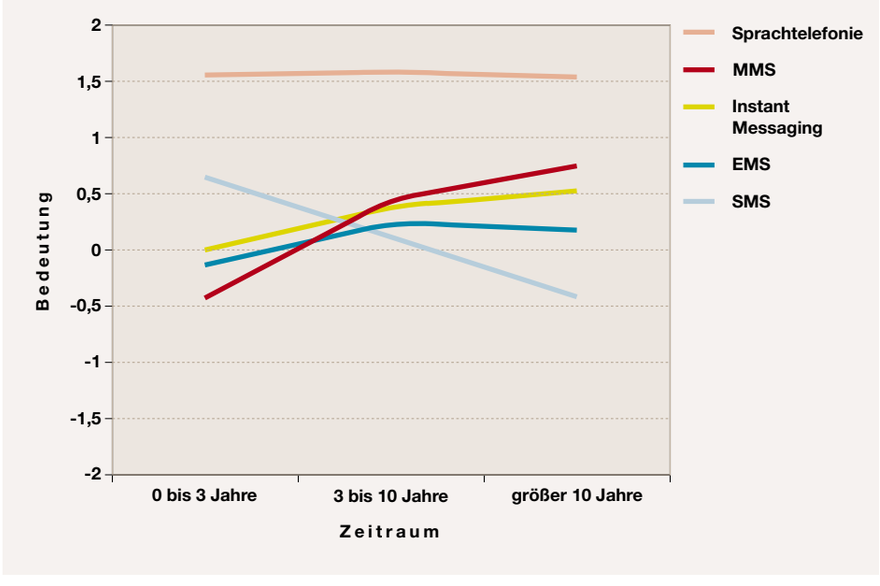



Abbildung 9.12: Bedeutung mobiler Kommunikationswege

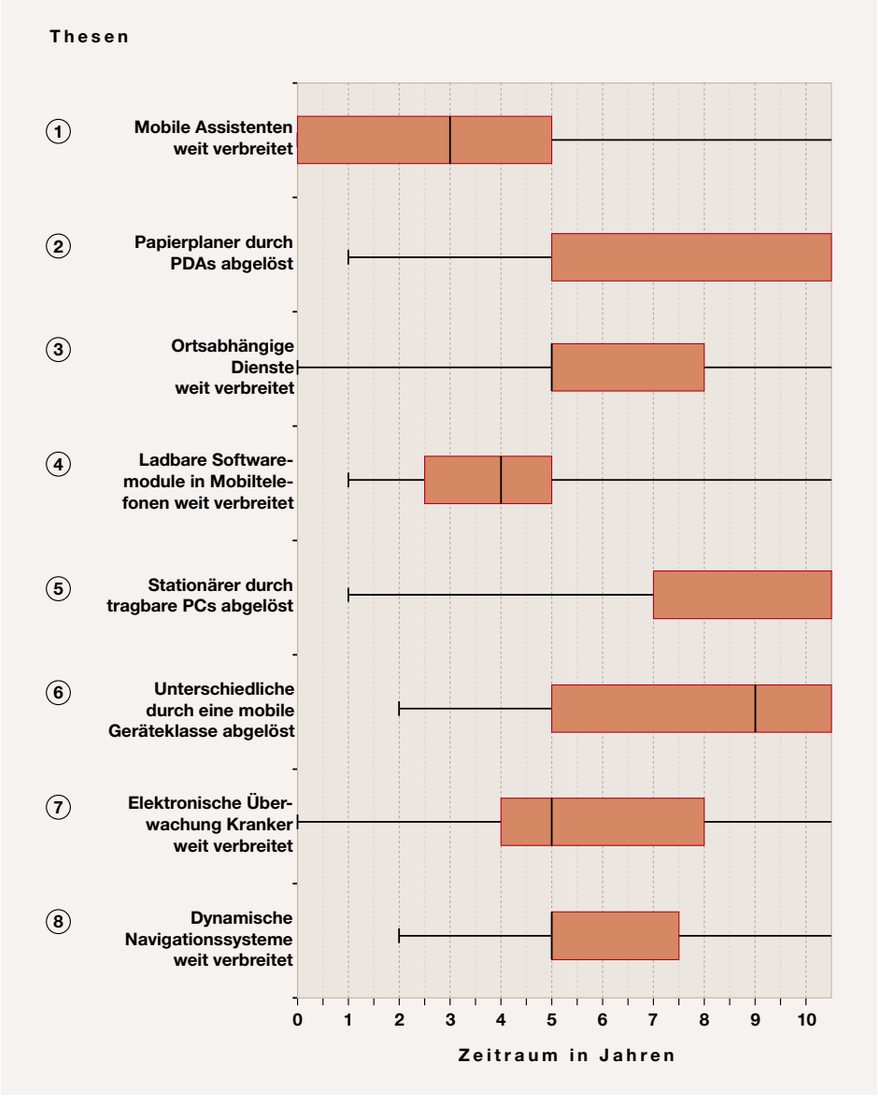



Abbildung 9.13: Ergebnisse der Thesen zu mobilen Diensten

direkter Sprachaustausch ist für den Menschen die einfachste Kommunikationsform und somit unverzichtbar. Dieses Ergebnis dämpft die ehemals euphorische Erwartung, dass Datendienste auf lange Sicht die Sprachkommunikation von der Bedeutung her ablösen werden [Dean 02]. Wahrscheinlicher ist eine weiterhin hohe Dominanz der Sprache, ergänzt durch einige, mobilitätsspezifische Datendienste, wie es heute schon mit SMS vor allem im privaten Bereich der Fall ist. Die Experten sehen aber eindeutig, dass dieser Dienst durch Nachfolgestandards wie EMS und insbesondere MMS ersetzt wird. Zu deren komfortablen und breiten Nutzung ist aber noch eine weitere Leistungssteigerung der Endgeräte hinsichtlich Übertragungsrate (GPRS (General Packet Radio Service) [HeSa 01], 3G) und Displayqualität (größer, mehr Farben) notwendig. Trotz der hohen Verbreitung auf Personal Computern sehen vor allem die Experten aus der Praxis für die Zukunft eine relativ geringe Bedeutung von Instant Messaging, wohingegen die Wissenschaftler dies bereits in drei Jahren als bedeutsamer erachten als die asynchronen Messagingdienste wie MMS. Dazu ist allerdings eine Standardisierung der Instant Messaging Protokolle als Voraussetzung anzusehen, welche selbst im stationären Internet noch nicht erreicht ist.

Die Vorgängerstudie erwartet eine weite Verbreitung von PDAs und Mobiltelefonen für das Jahr 2004 [SETIK 00]. Diese Prognose war der heutigen leicht voraus, denn heute schätzen die Experten, dass erst in drei Jahren derartige mobile Assistenten weit verbreitet sind (vgl. Abbildung 9.13, ①). Dabei sind die Prognosen der Experten aus der Industrie um ein Jahr optimistischer als die der Wissenschaftler. Die notwendigen Technologien stehen bereits zur Verfügung (z.B. leistungsfähige PDAs, breitbandige Funknetze), müssen allerdings noch weiter im Preis fallen.

VERBREITUNG VON PDAS UND MobiltelefonEN: Diese mobilen Assistenten sind in 3 Jahren weit verbreitet.

Pessimistisch äußern sich die Experten dazu, wann die Ablösung von papierbasierten Planern durch PDAs erreicht sein wird. Optimistische Einschätzungen sehen dies in fünf Jahren, die meisten aber erst in mehr als zehn Jahren (vgl. Abbildung 9.13, ②). Als technische Herausforderungen werden leistungsfähigere Displays und intuitivere Bedienung (eventuell ergänzt durch Spracheingabe) und nahtlose Integration mit anderen Systemen genannt.

ABLÖSUNG VON PAPIERBASIERTEN PLANERN DURCH PDAS: Die vollständige Ablösung ist auch die nächsten 10 Jahre nicht in Sicht.

Beispiele für LBS sind die Suche der nächstgelegenen Apotheke oder Tankstelle oder auch die Kombination mit Instant Messaging zum Anzeigen des Standorts der Kommunikationspartner. Obwohl die notwendigen Technologien heute bereits existieren und in Form von WAP-fähigen (Wireless Application Protocol) Mobiltelefonen auch recht weit verbreitet sind, sehen die Experten hier einen breiten Einsatz erst in fünf Jahren (vgl. Abbildung 9.13, ③). Als Gründe werden komplizierte Bedienung, Unzuverlässigkeit, mangelnde Abrechnungsmodelle und insbesondere datenschutzrechtliche Fragestellungen der genauen Lokalisierung der Endgeräte angeführt.

LBS: Ortsabhängige Dienste sind in 5 Jahren weit verbreitet.

Durch die Ausstattung mit Java [Sun 02a] können schon heute viele Mobiltelefone mit neuen Softwaremodulen erweitert werden, zum Beispiel mit Spielen oder geschäftlichen Spezialanwendungen, wie Kostenerfassungs- oder Börsenprogrammen. Es ist zu erwarten, dass die Kunden die damit gebotenen Möglichkeiten in vier Jahren in breitem Umfang nutzen (vgl. Abbildung 9.13, ④). Allerdings weisen die Experten darauf hin, dass einerseits noch weitere Leistungssteigerungen der Hardware (Prozessoren, Speicher, Displays und insbesondere Stromversorgung) und andererseits die Etablierung tragfähiger Geschäftsmodelle notwendige Voraussetzungen sind.

MOBILTELEFONE MIT NEUEN SOFTWAREMODULEN: Eine weite Verbreitung der Nutzung ladbarer Module auf Mobiltelefone ist in 4 Jahren realistisch.

Während Mobiltelefone damit immer mehr Funktionalitäten eines Personal Computers bieten, ersetzen Notebooks zunehmend stationäre PCs. Trotzdem erwarten die Experten, dass die Ablösung stationärer durch tragbare Rechner innerhalb der nächsten zehn Jahre nicht vollständig erreicht ist (vgl. Abbildung 9.13, ⑤), obwohl sie nahezu die gleichen Möglichkeiten bieten und deutlich flexibler im Einsatz sind.

ABLÖSUNG STATIONÄRER DURCH TRAGBARE RECHNER: Hier wird wohl nie eine vollständige Ablösung erreichbar sein.

Denkt man diese Konvergenz von Mobiltelefon und PC zu Ende, dann stellt sich die Frage, ob sich künftig eine mobile Geräteklasse (z.B. PDAs oder so genannte Smartphones) gegenüber einer „bunten Mischung“ von Endgeräten eindeutig durchsetzen kann. Dies erscheint den Experten erst in knapp neun Jahren als realistisch (vgl. Abbildung 9.13, ⑥), setzt aber viele der bereits genannten Weiterentwicklungen der Hardware und einfache Integration der Software voraus.

EINE MOBILE GERÄTEKLASSE: Mobile Geräte werden in 9 Jahre in eine mobile Geräteklasse konvergiert sein.

Die zur Verfügung stehenden Technologien machen es prinzipiell heute schon möglich, mobile Systeme zur Unterstützung der Überwachung alter und kranker Menschen relativ kostengünstig zu implementieren. So kann durch die Überwachung kritischer Körperfunktionen oder auch manuell bei Beschwerden ein Notruf abgesetzt werden, um so schneller geeignete Hilfe rufen zu können. Die Experten erwarten eine weite Verbreitung derartiger Systeme in etwa fünf Jahren, sehen aber kritische Punkte bei hohen Kosten, bisher fehlenden elektronischen Krankenakten und damit verbundenen Datenschutzproblemen (vgl. Abbildung 9.13, ⑦).

MOBILE SYSTEME ZUR UNTERSTÜTZUNG DER ÜBERWACHUNG ALTER UND KRANKER MENSCHEN: Derartige Systeme sind in 5 Jahren im breiten Einsatz.

Bereits in einigen Fahrzeugen im Einsatz sind dynamische Navigationssysteme, die ihre Routenplanung nicht nur auf lokalen, statischen Daten aufbauen, sondern auch aktuelle Stau- und Baustellenmeldungen einbeziehen. Denkbar wäre bei einer weiten Verbreitung künftig auch, dass in kritischen Situationen eine zentrale Verkehrsleitstelle den Verkehr optimal führen kann. Obwohl die notwendigen Technologien heute schon zur Verfügung stehen, erwarten die Experten eine hohe Verbreitung erst in etwa fünf Jahren (vgl. Abbildung 9.13, ⑧). Gründe dafür werden vor

DYNAMISCHE NavigationssystemE: Systeme, die dynamisch neue Daten bei der Navigation berücksichtigen sind in 5 Jahren weit verbreitet.

allem in den hohen Kosten der Navigationssysteme und den relativ langen Produktlebenszyklen von Automobilen gesehen.

### Zusammenfassung

Entwicklungen und Anwendungen auf Basis mobiler Technologien erwarten die Experten relativ früh. Sie sehen nur drei Thesen deutlich später als in fünf Jahren eintreten:

- Die Bedeutung mobiler Kommunikation wird die nächsten Jahre weiter zunehmen, dann aber auf hohem Niveau stagnieren oder gar leicht zurückgehen. Weiterhin den mit Abstand größten Anteil daran wird die Sprachtelefonie behalten, ergänzt durch Multimedia Messaging und mobiles Instant Messaging.
- Mobile Assistenten wie PDAs und Smartphones werden im Jahr 2005 weit verbreitet sein. Termine werden aber noch lange Zeit mit Hilfe von Papierkalendern geplant.
- Eine breite Akzeptanz von Location Based Services dürfte erst in 2008 erreicht sein. Dagegen erweitern die meisten Kunden ihre Mobiltelefone bereits im Jahr 2007 mit neuen, ladbaren Modulen.
- Im Jahr 2012 hat sich eine integrierte multifunktionale, mobile Geräteklasse gegenüber Mobiltelefonen und PDAs durchgesetzt.
- Als konkrete Anwendung sehen die Experten 2008 eine weite Verbreitung sowohl der Überwachung alter und kranker Menschen, als auch der Nutzung dynamischer Navigationssysteme.

## 9.4 Digitalisierung und Automatisierung von Wertschöpfungsketten

Auch wenn bereits in der Mitte des letzten Jahrhunderts Unternehmen zunehmend elektronische Datenverarbeitung einsetzten, so haben IuK-Systeme gerade durch die rasante Verbreitung des Internets deutlich an Bedeutung für die unternehmerische Wertschöpfung gewonnen. So widmet sich insbesondere die „Schnittstellendisziplin“ Wirtschaftsinformatik dem Einsatz von IuK-Systemen in Unternehmen. Ziel ist entweder eine „sinnhafte Vollautomation“ gut strukturierter Abläufe [Mert 95], oder, wenn dies nicht möglich ist, eine wirksame Unterstützung von Fach- und Führungskräften bei der Erledigung ihrer Aufgaben [MBK+ 01]. Heute sind für fast alle Bereiche eines Unternehmens IuK-Systeme verfügbar, und dementsprechend umfangreich ist auch die Thematik der Digitalisierung und Automatisierung von Wertschöpfungsketten [MBK+ 01, PRW 03]. Diese Studie kann daher nur einige Aspekte beispielhaft beleuchten.

Der Begriff „Management by Wire“ fasst Konzepte auf Basis von IuK-Technologien zusammen, die Führungskräften viele Managementaufgaben erleichtern können. Diese reichen von E-Mail-Systemen bis hin zu Werkzeugen zur strategischen Unternehmensführung. Eine speziellere Anwendung in diesem Bereich stellen die so genannten Expertensystemedar, die mit formalisiertem Wissen und auf Basis künstliche Intelligenz bei fachlichen Entscheidungen Unterstützung anbieten, beispielsweise bei der Fehlerbehebung in komplexen Anlagen. Simulationen dienen dagegen dazu, in einer virtuellen Welt verschiedene Szenarien kostengünstig und gefahrlos auszuprobieren, wie bei Crash-Tests in der Automobilbranche oder aber auch beim Durchspielen unternehmensstrategischer Entscheidungen. Ein Bereich, in dem die Automatisierung besonders weit fortgeschritten ist, stellt die eigentliche Produktion von Gütern in großen Stückzahlen wie beispielsweise bei integrierten Schaltkreisen dar. Lässt sich diese dazu noch sehr flexibel gestalten, so sind für jeden Kunden individuell angefertigte Produkte denkbar. Diese können trotzdem fast zu Massenproduktionspreisen angeboten werden, wie es einige Direktanbieter von PCs vorführen. Fernwartungssysteme bieten direkten Zugriff auf Endgeräte, wodurch dem Kunden bei Problemen direkter Support gegeben werden kann. Kooperieren mehrere Unternehmen miteinander und sind Mitarbeiter aus verschiedenen Unternehmen eng in gemeinsame, strukturierte Arbeitsabläufe eingebunden, so vereinfachen zwischenbetriebliche Workflowsysteme die Koor-

dination über die Unternehmensgrenzen hinweg. Lassen sich alle Schritte in geschäftlichen Abläufen direkt von Computern erledigen, so sind vollautomatisierte inner- oder zwischenbetriebliche Prozesse denkbar, wie sie z.B. im SCM (Supply Chain Management) zum Austausch kritischer Bestellinformationen eingesetzt werden. Notwendige Grundlage dazu sind allerdings breit akzeptierte Standards zum Datenaustausch wie die XML (Extensible Markup Language) [XML 99], die oft als Nachfolger von EDI (Electronic Data Interchange) angeführt wird, vielmehr aber eine neue Basistechnologie für darauf aufbauende Standards zum Datenaustausch darstellt (siehe auch Abschnitt 8.3.5). Auf XML basieren insbesondere die so genannten Web Services, aufgebaut auf den drei Standards SOAP (Simple Object Access Protocol) [SOAP 03], WSDL (Web Service Definition Language) und UDDI (Universal Description, Discovery and Integration) und der auf zwischenbetriebliche Geschäftsanwendungen spezialisierte Standard ebXML (Electronic Business XML). Diese und weitere Standards ermöglichen die unterschiedlichsten Ansätze zur elektronischen Geschäftsabwicklung. Die folgende Betrachtung fokussiert sich auf eine Auswahl derzeit in Theorie und Praxis besonders stark diskutierter Ansätze, welche nicht immer ganz trennscharf abgegrenzt werden können: ERP (Enterprise Resource Planing) dient der Unterstützung einer Vielzahl innerbetrieblich ablaufender Standardprozesse, wie Personalwesen oder Controlling. Data Warehousing sammelt für zuvor bestimmte Aspekte relevante Daten an einer Stelle und bietet Analysemöglichkeiten zur Entscheidungsunterstützung (siehe auch Abschnitt 8.3.4). CRM (Customer Relationship Management) strebt Aufbau und Verfestigung langfristig rentabler Kundenbeziehungen an. SCM stimmt die unternehmensinterne Produktion mit den Bedürfnissen der Kunden und den Möglichkeiten der Lieferanten eng ab. Schließlich zielt EAI (Enterprise Application Integration) auf die Integration all dieser Ansätze, um mit durchgängigen Daten und Prozessen logische Brüche zwischen den einzelnen Bereichen zu minimieren.

MANAGEMENT BY WIRE: Starke Unterstützung des Managements durch IuK-Systeme ist in 10 Jahren weit verbreitet.

EXPERTENSYSTEME: Diese werden in knapp 9 Jahren zur Entscheidungsunterstützung eingesetzt.

SIMULATIONEN: Simulationen von Produkten werden weiterhin in der Automobilbranche die größte Bedeutung haben.

## Ergebnisse

Das Führen von Mitarbeitern und Organisation ist charakterisiert durch viele Informations- und Kommunikationsprozesse. Daher liegt es nahe, viele Managementaufgaben durch IuK-Systeme zu unterstützen. Diese ermöglichen einerseits höhere Ortsunabhängigkeit von Führungskräften, und andererseits die Verarbeitung großer Datenmengen, zum Beispiel für das Controlling. Die Experten erwarten eine weite Verbreitung dieses so genannten „Management by Wire“ allerdings erst in zehn Jahren (vgl. Abbildung 9.14, ①), während sie dies in der Vorgängerstudie schon für das Jahr 2005 prognostizierten [SETIK 00]. Das Ergebnis wird auch damit erklärt, dass nach einer übertriebenen Technikeuphorie nun wieder die Bedeutung direkter menschlicher Kontakte zurück ins Bewusstsein getreten ist.

Neben dem Führen von Mitarbeitern ist das Fällen von Entscheidungen eine weitere zentrale Aufgabe des Managements. Hier können Expertensysteme durch das Bereitstellen aktuellster Zahlen und die Anwendung klar strukturierter Regeln eine gute Hilfe bei der Entscheidungsfindung bieten. In der Studie 2000 waren die Befragten noch sehr skeptisch gegenüber einer hohen Verbreitung von Expertensystemen, wohingegen sie dies heute immerhin für das Jahr 2011 erwarten (vgl. Abbildung 9.14, ②). Als notwendig nennen sie aber weitere deutliche Fortschritte im Bereich der formalen Wissensdarstellung und der künstliche Intelligenz.

Ähnlich einzuordnen sind die verschiedensten Simulationsansätze, welche zum Ziel haben, Abschätzungen über die Zukunft zu treffen. Die Befragten erwarten eine ähnlich starke Zunahme der Bedeutung von Simulationen über alle Branchen hinweg. Allerdings wird die Automobilbranche als wichtigster Einsatzbereich eingeschätzt, mit Abstand gefolgt von den Branchen Chemie, IuK-Technologie, Energie und Bau. Für Finanzdienstleistungen, Investitionsgüter, Handel, Medien und Konsumgüter dürften Simulationen nach Expertenmeinung künftig dagegen keine Rolle spielen (vgl. Abbildung 9.15).

Im Zuge der Digitalisierung unternehmerischer Leistungserstellung folgt auf die elektronische Produktentwicklung die au-

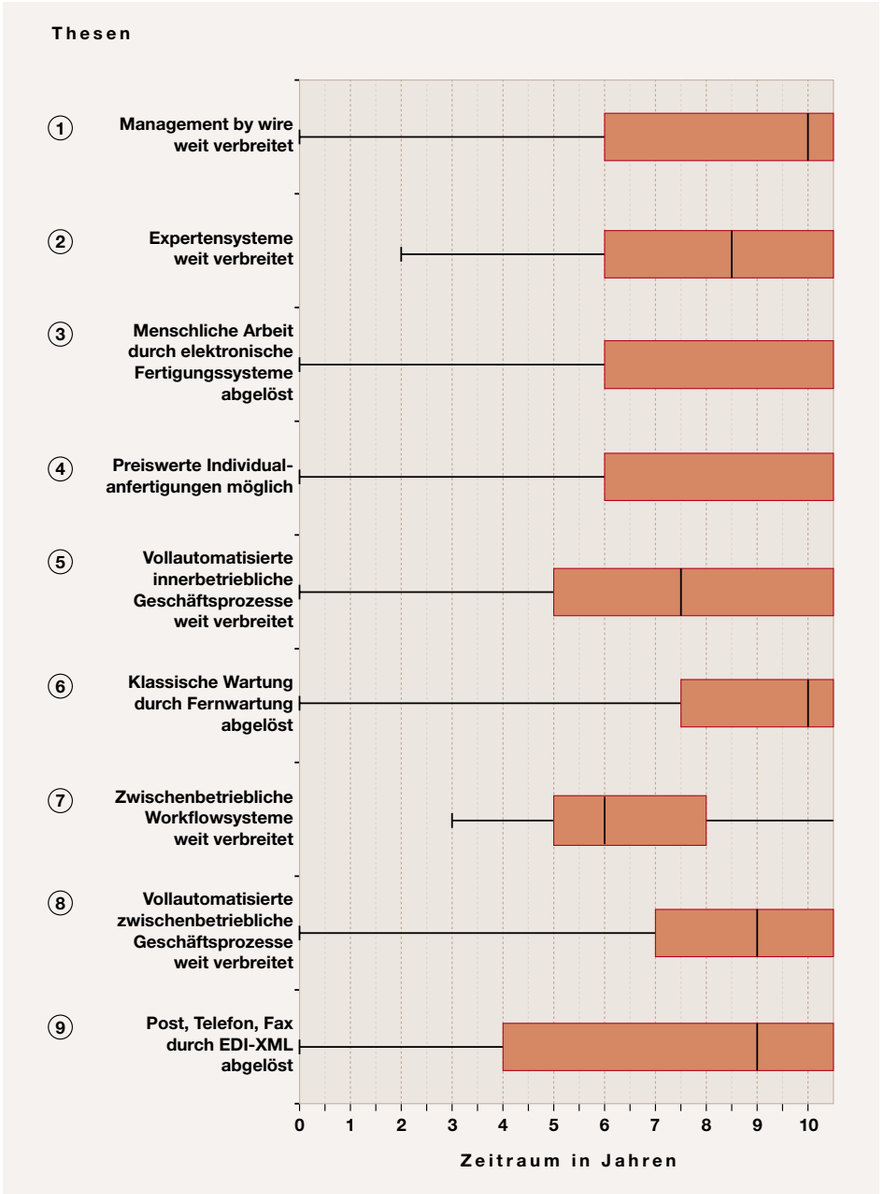



Abbildung 9.14: Ergebnisse der Thesen zu Digitalisierung und Automatisierung von Wertschöpfungsketten

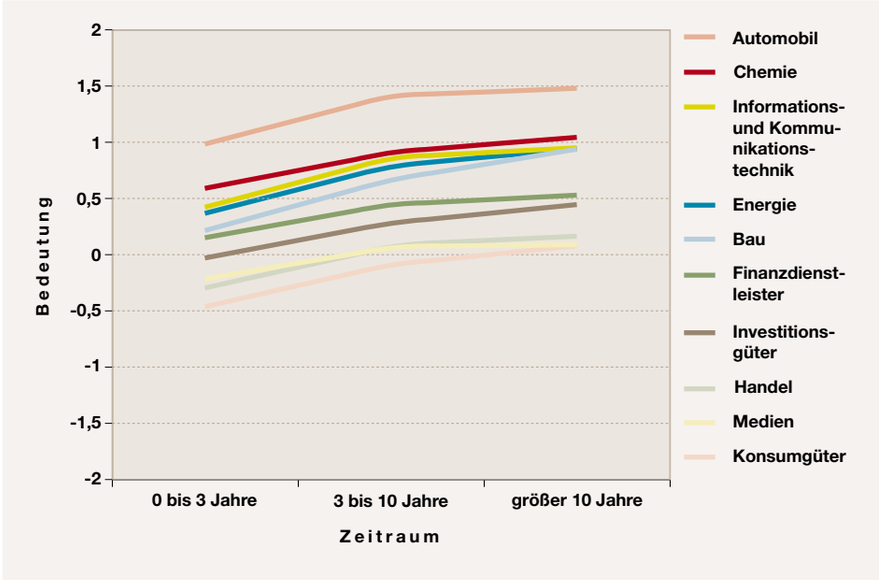



Abbildung 9.15: Bedeutung von Simulationsansätzen

AUTOMATISIERTE PRODUKTION: Ob menschliche Arbeit in den nächsten 10 Jahren durch maschinelle Arbeit abgelöst wird ist stark branchenabhängig

HOCH FLEXIBLE FERTIGUNGSSYSTEME: Dadurch kundenspezifische Produkte so günstig wie Massenprodukte herstellen zu können, ist für die nächsten 10 Jahre nahezu unmöglich.

VOLLAUTOMATISIERTE INNERBETRIEBLICHE GESCHÄFTSPROZESSE: Hier ist ein Automatisierungsgrad von 50% in 7 Jahren weit verbreitet.

FernwartungSSYSTEME: Systeme zur Wartung von Maschinen aus der Ferne lösen Wartung vor Ort frühstens in 10 Jahren ab.

tomatisierte Produktion. Wie schon in der Vorgängerstudie erwarten die Experten allerdings nicht, dass komplexe elektronische Fertigungssysteme in den nächsten zehn Jahren physische menschliche Arbeit generell ablösen werden (vgl. Abbildung 9.14, ③). Vielmehr sehen sie einen stark nach Branchen differenzierten Einsatz von Automatisierungstechnik, der sich in den nächsten Jahren nicht deutlich verändern dürfte.

Als einen weiteren Aspekt im Rahmen moderner Produktionstechnologien werden hoch flexible Fertigungssysteme gewünscht. Diese ermöglichen im Idealfall die Erstellung kundenspezifischer Individualanfertigungen mit nahezu gleichem Aufwand wie bei der klassischen Serienfertigung. Insgesamt halten die Experten dies bis 2013 für unrealistisch (Abbildung 9.14, ④). Während die Experten aus der Praxis diese These als unmöglich erreichbar bewerten, erwarten die Befragten aus der Forschung das Eintreten immerhin in neun Jahren. Gerade im Bereich von Produkten mit hohem Informationsanteil ergeben sich viele Möglichkeiten zur Individualisierung, aber auch bei „klassischen" Produkten rechnen sie mit weiteren Fortschritten beim „Mass Customization".

Die folgende These abstrahiert den Aspekt der Automatisierung auf alle unternehmerischen Abläufe. Die Befragten sollten einschätzen, wann es weit verbreitet sein wird, dass vollautomatisierte innerbetriebliche Geschäftsprozesse die Hälfte aller Geschäftsprozesse ausmachen. Sie erwarten dies in etwas mehr als sieben Jahren (Abbildung 9.14, ⑤). Allerdings halten die Experten nur relativ stark standardisierte Abläufe für die Automatisierung geeignet und führen deutliche Weiterentwicklungen der ausführenden IuK-Systeme als zwingend notwendige Voraussetzung an.

Um nach der Beschaffung teurer Konsum- und Investitionsgüter besseren Service anbieten zu können, ist es für die Hersteller von Vorteil, direkt über IuK-Systeme auf ihre Produkte beim Kunden zugreifen zu können. Eine Ablösung klassischer Wartung durch derartige Fernwartungssysteme erwarten die Experten allerdings erst in zehn Jahren (Abbildung 9.14, ⑥). Es ergibt sich ein ähnlich differenziertes Bild wie in der These zuvor, mit einer deutlich optimistischeren Einschätzung durch die Wissenschaftler im Vergleich zu den Befragten aus der Praxis. Als Hindernisse nennen sie die relativ langen Lebenszyklen wartungsintensiver Produkte und die noch fehlende Reife der Diagnosesysteme, die auf Expertensystemen (siehe oben) und künstlicher Intelligenz aufbauen.

Allgemeiner gehalten ist die Betrachtung von IuK-Systemen, die generell Abläufe zwischen Unternehmen unterstützen sollen. So erwarten die Fachleute, dass zwischenbetriebliche Workflowsysteme zur papierlosen Zusammenarbeit in sechs Jahren breit eingesetzt werden (vgl. Abbildung 9.14, ⑦), was nur eine leichte Verschiebung gegenüber der Studie 2000 darstellt. Als Voraussetzung werden hohe Zuverlässigkeit und Bandbreiten und detaillierte Zugriffsverwaltung auf die verteilten Systeme genannt.

Wie oben bereits auf innerbetrieblicher Ebene untersucht, mussten sich die Experten auch zur Automatisierung zwischen Unternehmen äußern. Die Ergebnisse sind damit vergleichbar, da die Experten vollautomatisierte zwischenbetriebliche Geschäftsprozesse in neun Jahren weit verbreitet sehen (vgl. Abbildung 9.14, ⑧). Der Verfügbarkeit leistungsfähiger Standards wird hier eine besonders hohe Bedeutung beigemessen.

XML gilt hierzu als erforderliche Basistechnologie (siehe auch Abschnitt 8.3.5). Allerdings erwarten die Befragten eine Ablösung des herkömmlichen Datenaustausches per Papier, Telefon und Fax durch XML-Anwendungen erst in neun Jahren (vgl. Abbildung 9.14, ⑨), viele halten eine vollständige Ablösung für gänzlich unrealistisch. Dieses Ergebnis stellt eine deutliche Abweichung von der letzten Prognose dar, in der der breite XML-Einsatz bereits für heute erwartet wurde und selbst pessimistische Stimmen diesen für das Jahr 2005 angaben.

Für eine tiefergehende Analyse mussten die Experten eine Auswahl wichtiger Standards hinsichtlich ihrer Bedeutung für die elektronische Geschäftsabwicklung, getrennt nach Großunternehmen und kleinen bzw. mittelständischen Unternehmen, einschätzen. Bei der Bewertung für Großunternehmen fällt der starke Bedeutungsanstieg von XML im Vergleich zur deutlichen Abnahme von EDIFACT (Electronic Data Interchange for Administration, Commerce and Transport) ins Auge (vgl. Abbildung 9.16). Hier drückt sich aus, dass ein Umstieg auf XML und darauf aufbauende Formate erwartet wird, ohne dass sie die bisher implementierten EDIFACT-Systeme mittelfristig vollständig ersetzen werden. Die drei derzeit viel diskutierten Web Services-Standards SOAP, UDDI und WSDL finden sich heute auf einem mittleren Niveau und gewinnen nur leicht an Bedeutung. Dagegen beginnt der Nachfolger von EDIFACT, ebXML, mit der niedrigsten Bedeutung, wird aber langfristig wichtiger als die Web Services-Standards eingestuft. Unterschieden nach Umfeld der Befragten geben die Experten aus der Industrie durchweg eine höhere Bedeutung der Standards an. Auffällig ist auch, dass für XML eine leichte Abnahme der Bedeutung bis in 10 Jahren erwartet wird. Das Bild für kleine und mittelständische Unternehmen weicht etwas ab (vgl. Abbildung 9.17), da sich hier EDIFACT schon heute auf einem deutlich geringeren Niveau befindet und auch dem Nachfolger ebXML nicht ganz die Bedeutung beigemessen wird wie für Großunternehmen. Auf lange Sicht wird aber auch hier ebXML höher eingestuft als die Web Services-Standards. Ganz klar dominiert hier XML, welches allerdings auch eine Grundlage der anderen hier betrachteten Standards darstellt.

Diese und weitere Standards und Technologien setzen Unternehmen in verschiedensten Bereichen der elektronischen Geschäftsabwicklung ein. Hier wurden CRM, Data Warehouses, EAI, EDI, SCM und Web Services als die wichtigsten Ansätze erachtet. Zuerst folgt wieder die Betrachtung für Großunternehmen, die zeigt, dass eine generelle Zunahme der Bedeutung aller Ansätze zu erwarten ist, was auch für das Nebeneinander und die gegenseitige Ergänzung spricht (vgl. Abbildung 9.18). In diesem Zusammenhang überrascht aber die vergleichsweise geringe Einschätzung von EAI, welches in der Literatur als eine wesentliche Grundlage für eine effiziente unternehmensweite IuK-Infrastruktur beschrieben wird, da das zentrale Ziel ja gerade die Integration einer heterogenen Anwendungslandschaft ist. Auffällig ist auch die starke Zunahme bei Web Services. Dabei resultiert diese vor allem aus der Einschätzung der Experten aus der Wissenschaft, welche die Bedeutung – im Gegensatz zu den Vertretern aus der Industrie – heute noch als gering einschätzen, aber ebenso eine mittel- und langfristige hohe Bedeutung erwarten. Die höchste Bedeutung sprechen die Befragten und knapp dahinter dem CRM zu. Für die kleinen und mittelständischen Unternehmen ergibt sich ein ähnliches Bild (vgl. Abbildung 9.19). Insgesamt wird allen Ansätzen

ZWISCHENBETRIEBLICHE WorkflowSYSTEME: Diese Systeme werden in 6 Jahren weit verbreitet eingesetzt.

VOLLAUTOMATISIERTE ZWISCHENBETRIEBLICHE GESCHÄFTSPROZESSE: Hier ist ein Automatisierungsgrad von 50% in 9 Jahren weit verbreitet.

XML: löst Datenaustausch per Papier, Telefon und Fax in 9 Jahren ab.

ebXML: Die Bedeutung von ebXML nimmt in den nächsten 10 Jahren am deutlichsten zu.

SCM: Supply Chain Management spielt künftig die größte Rolle bei der elektronischen Geschäftsabwicklung.

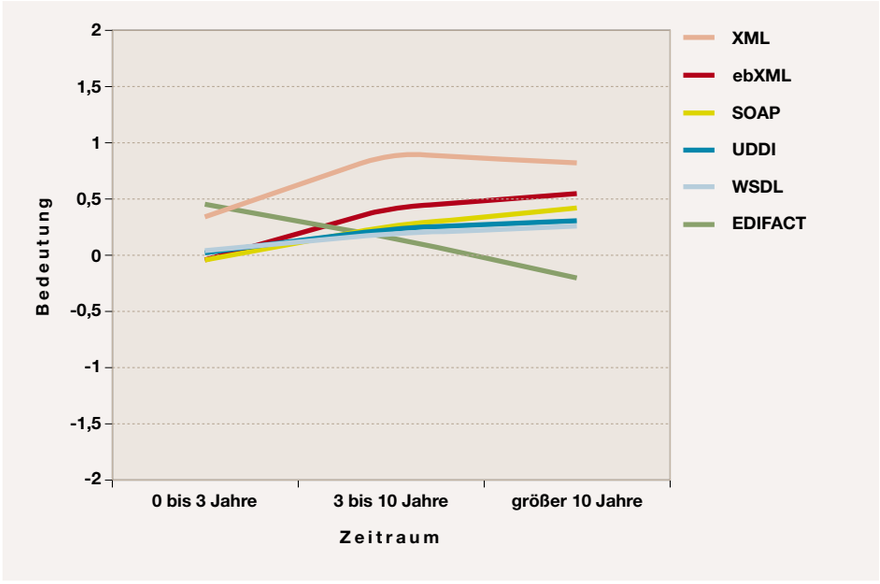



Abbildung 9.16: Bedeutung von Standards für die elektronische Geschäftsabwicklung in Großunternehmen

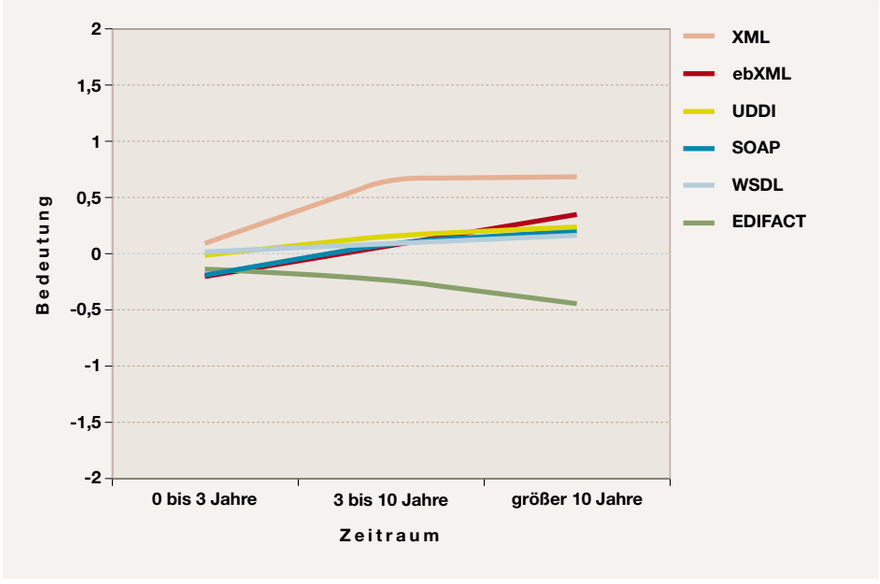



Abbildung 9.17: Bedeutung von Standards für die elektronische Geschäftsabwicklung in kleinen und mittelständischen Unternehmen

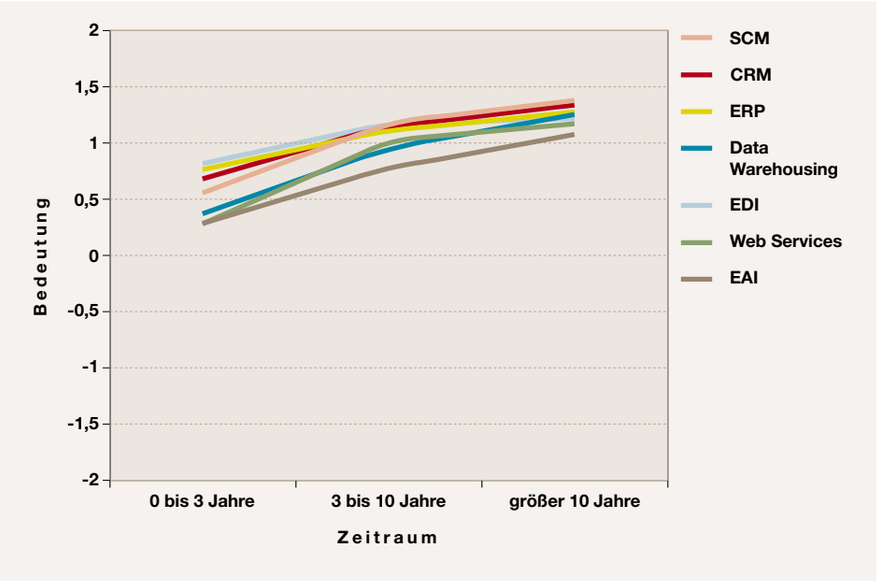



Abbildung 9.18: Bedeutung von verschiedenen Ansätzen zur elektronischen Geschäftsabwicklung in Großunternehmen

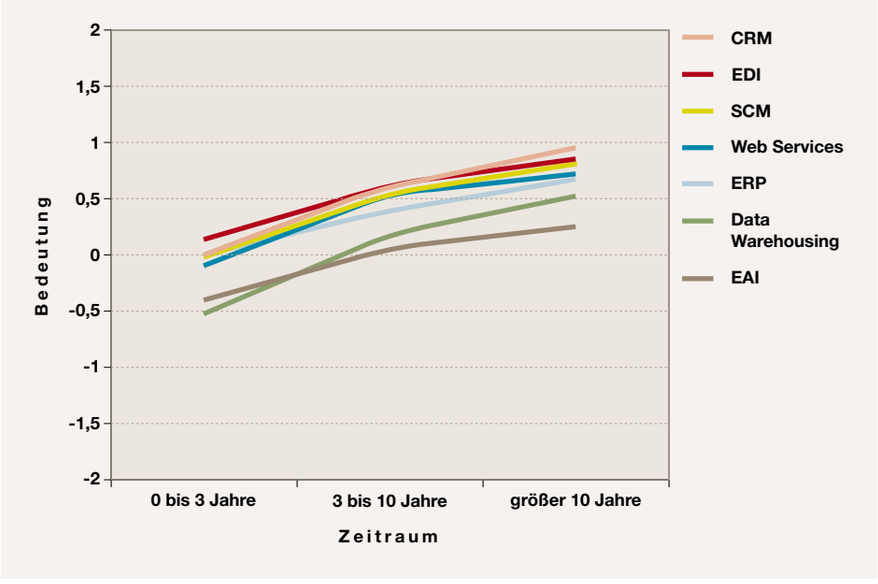



Abbildung 9.19: Bedeutung von verschiedenen Ansätzen zur elektronischen Geschäftsabwicklung in kleinen und mittelständischen Unternehmen

durchweg eine geringere Bedeutung als für Großunternehmen zugeordnet. Deutlich wird dies besonders bei der relativ niedrigen Einschätzung von EAI und Data Warehousing, wobei letzteres langfristig aufholen wird. Überraschend ist die hohe Einschätzung von EDI, welches meist als zu teuer für kleine Unternehmen gilt und daher oft in deren Umfeld vernachlässigt wird. Auf lange Sicht ordnen aber gerade die Vertreter aus der Praxis CRM noch höher ein, was durch die größere Abhängigkeit kleinerer Unternehmen von bestimmten Schlüsselkunden erklärt wird.

### Zusammenfassung

Hinsichtlich der Digitalisierung und Automatisierung von Wertschöpfungsketten äußern sich die Experten durchgehend zurückhaltend. Die meisten Thesen sehen sie erst in neun oder mehr Jahren eintreten:

- Stark auf IuK-Systemen basierende Managementmethoden und Expertensysteme sind frühstens 2011 weit verbreitet.
- Simulationen spielen weiterhin die größte Rolle in der Automobilbranche, mit Abstand gefolgt von Chemie, IuK, Energie und Bau.
- Weder die Ablösung menschlicher Arbeit durch elektronische Fertigungssysteme, noch die Verbreitung damit preiswert erstellter Individualanfertigungen, ist bis zum Jahr 2013 realistisch.
- Fernwartungssysteme haben frühstens 2013 die herkömmliche Wartung vor Ort abgelöst.
- Mehr als die Hälfte aller inner- bzw. zwischenbetrieblichen Geschäftsprozesse wird 2010 bzw. 2012 vollautomatisch abgewickelt.
- Workflowmanagementsysteme unterstützen bereits im Jahr 2009 die papierlose Zusammenarbeit zwischen Unternehmen auf breiter Basis.
- XML-basierte Standards dominieren auf lange Sicht die elektronische Abwicklung von Geschäftsprozessen. ebXML wird EDIFACT ablösen und übersteigt dabei die Bedeutung der Web Services-Standards.
- SCM und CRM bestimmen die künftige Entwicklung betrieblicher IuK-Systeme, dicht gefolgt von ERP, EDI, Data Warehousing und Web Services.EAI wird eine relativ geringe Rolle spielen.

## 9.5 Flexibilisierung von Organisationsstrukturen und Arbeitsformen

Eine zentrale Fragestellung bei der Gestaltung von Organisationen ist die Koordination verteilter Leistungserstellung und die Motivation der daran beteiligten Akteure. Ein wesentlicher Aspekt dabei ist der Informationsaustausch zwischen den verschiedenen Teilnehmern [PDF 02]. Die Entwicklung neuer IuK-Technologien – insbesondere das Internet – hat diesen Informationsaustausch in den letzten Jahren zum Teil deutlich verändert. Nach einer generellen Einschätzung der künftigen Bedeutung von IuK-Technologien untersucht dieser Abschnitt mit ausgewählten Fragen, welche Entwicklungen sich heute schon für den nächsten zehn Jahren für die Gestaltung von Arbeitsformen und Organisationen abzeichnen.

Zuerst beleuchten einige Fragen, wie sich IuK-Technologien auf die direkten Arbeitsabläufe von Mitarbeitern auswirken. So ist die Entwicklung vieler IuK-Technologien durch die Vision getrieben, materielle Informationsträger durch elektronische zu ersetzen, um Papier komplett aus der Büroarbeit zu verbannen [Pico 99]. Diese Ansätze stellen eine wesentliche Grundlage für flexiblere Arbeitsformen wie Heimarbeit oder Arbeiten auf Geschäftsreisen dar. Denn die Unabhängigkeit von einem physischen Medium vereinfacht den Zugriff auf die jeweils notwendigen Informationen, egal von welchem Standort aus. Somit wird auch Telekooperation ermöglicht, also „mediengestützte arbeitsteilige Leistungserstellung von individuellen Aufgabenträgern, Organisationseinheiten und Organisationen“ über mehrere Standorte hinweg [RMSE 00].

Immer größere Bedeutung erlangen flexible Wertschöpfungsketten. Innerhalb von Unternehmen ermöglicht eine Modularisierung der Organisationsstrukturen ei-

ne einfache Konfiguration unterschiedlicher Organisationseinheiten entsprechend der jeweiligen Kundenbedürfnisse. Reichen die unternehmensinternen Ressourcen nicht aus, erleichtern Kooperationsbörsen das Finden geeigneter Geschäftspartner. Ebenso erschließen neue Intermediäre zuvor nur schwer erreichbare Kundengruppen. Beides führt zu einem zunehmenden Verwischen vormals scharf gezogener Unternehmensgrenzen. In der Praxis lässt sich dieses Phänomen besonders ausgeprägt bei „Virtuellen Unternehmen" und BPO (Business Process Outsourcing) beobachten. Ein virtuelles Unternehmen stellt den Zusammenschluss mehrerer (zuvor) unabhängiger Unternehmen dar, die eine gemeinsame Leistung erbringen und gegenüber dem Kunden derart einheitlich auftreten, dass dieser den Eindruck bekommt, nur mit einem einzigen Unternehmen in Kontakt zu stehen. BPO bezeichnet den vielschichtigen Ansatz, größere zusammenhängende, aber strategisch weniger bedeutende, Funktionen aus einem Unternehmen herauszulösen und die notwendigen Prozesse von einem spezialisierten Drittanbieter abwickeln zu lassen. Entwickeln sich diese beiden Phänomene weiterhin in hoher Geschwindigkeit fort, so ist zunehmend mit sehr flexiblen Wertschöpfungsketten zu rechnen, die sich dynamisch aus den unterschiedlichsten, hoch spezialisierten Unternehmen zusammensetzen und über IuK-Systeme koordiniert werden (für eine ausführliche Diskussion der hier angesprochenen Aspekte und dabei auftretenden Probleme siehe [PRW 03]).

## Ergebnisse

In einer ersten Betrachtung haben die Experten die generelle Bedeutung von Informations- und Kommunikationstechnologien für betriebliche Organisationsstrukturen eingeschätzt. Während einige bereits heute spürbare Veränderungen feststellen, sehen andere eine Revolution noch bevorstehen, die zu grenzenlosen Unternehmen mit sehr flexiblen Strukturen führen wird. Einen Anstieg von mittlerer auf recht starke Bedeutung sehen die Experten besonders in den nächsten drei Jahren, danach ein nur noch leicht ansteigendes Niveau (vgl. Abbildung 9.20). Die Experten aus der Industrie gehen von einer geringeren Bedeutung heute, aber einem stärken Anstieg in der Zukunft aus, als die Experten aus der Wissenschaft.

Auch wenn die Befragten im Ersatz von Papier durch elektronische Medien wesentliche Vorteile in der einfacheren Handhabung und der leichteren Archivierung sehen, ist die Skepsis gegenüber einer weiten Verbreitung der Vision „papierloses Büro" im Vergleich zur Vorgängerstudie noch weiter gestiegen [SETIK 00]. So glaubt inzwischen kein Experte mehr, dass diese in den nächsten zehn Jahren wahr wird (vgl. Abbildung 9.21, ①). Hervorzuheben ist an dieser Stelle, dass alle notwendigen Technologien als weitgehend verfügbar angesehen werden, aber die Gewöhnung des Menschen an den Umgang mit Papier weiterhin zu groß ist. Daher spielt die Entwicklung von elektronischem Papier eine Schlüsselrolle um der Vision des vollständig papierlosen Büros näher zu kommen.

Ähnlich werden flexible Arbeitsformen wie Arbeiten auf Reisen oder zu Hause eingeschätzt. Auch wenn es heute schon etliche Einsatzgebiete gibt, so sehen die Experten hier noch weiteres Potenzial, allerdings stark abhängig von der Branche bzw. dem Einsatzbereich der Mitarbeiter. Daher erwarten nur wenige Fachleute eine Ablösung traditioneller Arbeitsformen innerhalb der nächsten zehn Jahre (vgl. Abbildung 9.21, ②). Eine wesentliche Voraussetzung auf dem Weg dorthin wird die Verfügbarkeit preiswerter und breitbandiger drahtloser wie drahtgebunder Übertragungstechnologien sein.

Deutlich optimistischer schätzen die Befragten den breiten Einsatz von Telekooperationen gerade in informationsintensiven Branchen und Bereichen ein. Auch wenn die Prognosen sich gegenüber der Studie 2000 heute leicht nach hinten verschoben haben, so erwarten die Experten eine weite Verbreitung von Telekooperation in fünf Jahren (vgl. Abbildung 9.21, ③), die Fachleute aus der Praxis sogar in drei Jahren. Hier existiert weiterer Entwicklungsbedarf, vor allem hinsichtlich einfacher zu bedienender Anwendungen.

Zunehmend lässt sich eine Modularisierung unternehmensinterner Organisationsstrukturen feststellen. Dies stützen auch die Experten mit ihrer Erwartung, dass interne Modularisierung ebenso wie

BEDEUTUNG VON INFORMATIONS- UND KOMMUNIKATIONSTECHNOLOGIEN FÜR BETRIEBLICHE OrganisationSSTRUKTUREN: Diese ist schon hoch, wird aber die nächsten 10 Jahre noch deutlich zunehmen.

papierloses Büro: Innerhalb der nächsten 10 Jahre ist ein Eintritt dieser Vision sehr unwahrscheinlich.

FLEXIBLE ARBEITSFORMEN: Diese werden traditionelle Arbeitsformen innerhalb der nächsten 10 Jahre nicht ablösen.

TelekooperationEN: Gerade in informationsintensiven Bereichen sind Telekooperationen in 5 Jahren weit verbreitet.

MODULARISIERUNG UNTERNEHMENSINTERNER OrganisationSSTRUKTUREN: Dieses Organisationskonzept wird in 6 Jahren weit verbreitet sein.

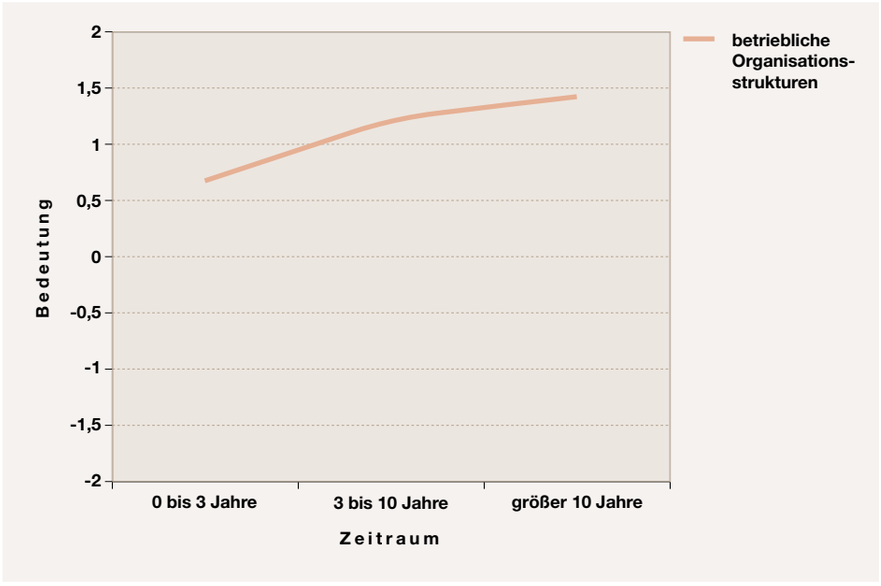



Abbildung 9.20: Bedeutung von IuK-Technologien für Organisationsstrukturen

ELEKTRONISCHE KOOPERATIONSBÖRSEN: Diese werden in 5 Jahren weit verbreitet genutzt.

REALE UND VIRTUELLE INTERMEDIÄRE: Der mit dem zunehmenden Wachstum des Internet verbundene Einsatz von realen und virtuellen Intermediären wird in 5 Jahren weit verbreitet sein.

VIRTUELLE UNTERNEHMENSVERBUNDE: Die Anzahl von virtuellen Unternehmensverbunden wird in den kommenden 5 Jahren stark zunehmen.

ETABLIERUNG VIRTUELLER UNTERNEHMEN DURCH VERNETZUNG UND STANDARDISIERUNG VON GESCHÄFTSPROZESSEN: Dies ist für die nächsten 10 Jahre nicht auf breiter Front zu erwarten.

eine entsprechende modulare Infrastruktur in sechs Jahren weit verbreitet sein wird (vgl. Abbildung 9.21, ④). Bis es aber soweit ist, einfach neue Organisationsstrukturen aus Modulen konfigurieren zu können, müsse die Flexibilität und die notwendige Standardisierung noch deutlich weiterentwickelt werden.

Reichen die Ressourcen im eigenen Unternehmen für eine bestimmte Aufgabe nicht aus, so können geeignete Partnerunternehmen diese ergänzen. Zunehmend dazu eignen sich internetbasierte Plattformen. So erwarten die Befragten, dass elektronische Kooperationsbörsen zur Suche von externen Partnern in fünf Jahren weit verbreitet genutzt werden (vgl. Abbildung 9.21, ⑤). Diesen Zeitraum gaben sie allerdings schon in der Vorgängerstudie an, was heute zu einer pessimistischeren Einschätzung führt. Die zentrale Herausforderung sehen die Fachleute hier in etablierten und verbindlichen Standards, um zum Beispiel auch SCM (Supply Chain Management) über diese Plattformen durchführen zu können.

Auf der anderen Seite ergibt sich für die Absatzseite und den dortigen Einsatz von Intermediären ein ähnliches Bild. Reale und virtuelle Intermediäre im Internet erwarten die Experten für das Jahr 2008 als weit verbreitet (vgl. Abbildung 9.21, ⑥), verglichen mit der letzten Prognose für 2004. Auch hier wird mangelnde Standardisierung als eine wesentliche Hürde angesehen, die es noch zu überwinden gilt.

Verbinden sich mehrere unabhängige Unternehmen zeitlich befristet zur Erstellung einer gemeinsamen Leistung, spricht man oft auch von virtuellen Unternehmen. Die Experten sehen es in fünf Jahren als weit verbreitet an, externe Partner und Unternehmen in derartige virtuelle Unternehmensverbunde einzugliedern (vgl. Abbildung 9.21, ⑦). Im Vergleich zur Studie 2000, die auch einen Eintritt in fünf Jahren erwartet, ist eine Verschiebung der Prognose zu erkennen. Als größte Herausforderungen für virtuelle Unternehmen nennen die Befragten die Etablierung von Standards und größeres Vertrauen zwischen den einzelnen Unternehmen.

Daher wurde ebenfalls abgefragt, wann die Experten eine weite Verbreitung der Etablierung virtueller Unternehmen durch Vernetzung und Standardisierung von Geschäftsprozessen sehen. Nur wenige erwarten dies innerhalb der nächsten zehn Jahre (vgl. Abbildung 9.21, ⑧), allerdings glauben einzelne, dass dies nie geschehen wird.

Wenn Geschäftsprozesse stark standardisiert sind, lassen sie sich auch leicht von anderen Organisationen beziehen, die die-


Abbildung 9.21: Ergebnisse der Thesen zur Flexibilisierung von Organisationsstrukturen und Arbeitsformen

se Prozesse jeweils besser abwickeln können, als das eigene Unternehmen. Dieses so genannte BPO findet sich zunehmend in strategisch weniger wichtigen Bereichen wie Rechnungswesen oder Personalverwaltung wieder. Die Befragten erwarten eine weite Verbreitung von BPO in sechs Jahren, im Gegensatz zur Vorgängerstudie prognostiziert aber nur wenige einen späteren Zeitpunkt, als acht Jahre (vgl. Abbildung 9.21, ⑨).

BUSINESS PROCESS OUTSOURCING: Das Auslagern umfangreicher Geschäftsprozesse ist in 6 Jahren weit verbreitet.

Als Endstufe der bisher diskutierten Entwicklungen sind hoch flexible Wertschöpfungsnetzwerke denkbar, die ad hoc für einen bestimmten Zweck konfiguriert, danach aber einfach wieder zerlegt werden können. Technologische Basis stellen vor allem neuere Web-Technologien wie Web Services dar. Auch hier vermuten die Fachleute eine weite Verbreitung in sechs, spätestens aber in neun Jahren (vgl. Abbildung 9.21, ⑩). Zu lösende Herausforderungen sind hier wiederum flexible und „intelligente“ Software, sowie Vertrauen und Sicherheit.

HOCH FLEXIBLE WERTSCHÖPFUNGSNETZWERKE: Derartige "Plug&PlayWertschöpfungsketten sind in 6 Jahren weit verbreitet.

### Zusammenfassung

Bei der Untersuchung der Auswirkungen von IuK-Technologien auf Arbeitsformen ergibt sich ein eher zurückhaltendes Bild, während der Einfluss auf Organisationsstrukturen für die nächsten Jahre als hoch eingeschätzt wird:

- Der Einfluss von IuK-Technologien auf Organisationen nimmt die nächsten Jahre weiter stark zu.
- Während Telekooperationsformen bis 2008 spürbar an Bedeutung gewinnen, sind weder hoch flexible Arbeitsformen, noch das papierlose Büro in absehbarer Zeit zu erwarten.
- Die weite Verbreitung der Modularisierung interner Organisationsstrukturen und der zugehörigen IuK-Infrastruktur ist im Jahre 2009 zu erwarten.
- Kooperationsbörsen zum Finden von Lieferanten und Partnern, sowie neue Intermediäre zum Absetzen der erstellten Leistungen sind ab 2007 als weit verbreitet einzustufen.
- Virtuelle Unternehmen sehen die Experten im Jahr 2008 als weit verbreitet an, allerdings bis 2010 nicht auf breiter Basis von voll standardisierten Geschäftsprozessen.
- Die Vernetzung unterschiedlichster Unternehmen untereinander gewinnt weiter an Bedeutung, wie die erwartete Verbreitung von BPO und von flexiblen, web-basierten Wertschöpfungssystemen bis zum Jahr 2009 verdeutlicht.

## 9.6 Controlling, Finanzdienstleistungen und Zahlungsverfahren

Im Folgenden wird die Integration der Informations- und Kommunikationstechnologien in Controlling, Finanzdienstleistungen und Zahlungsverfahren beleuchtet. Die Automatisierung von Geschäftsabläufen und die Vermeidung von Medienbrüchen bergen enorme Einsparmöglichkeiten. Das Streben nach komplett elektronischer Unterstützung von Wertschöpfungsketten führt gerade im E-Business zur Integration der Zahlungsabwicklung in das Leistungsspektrum elektronischer Märkte. Austausch und Verarbeitung von Daten in digitaler Form erleichtern die Integration der verschiedenen Anwendungen in der Unternehmung. Controlling-Informationssysteme können das Management durch die Datenintegration automatisch mit Kontroll- und Planungsinformationen versehen [BMR 00]. Exemplarisch werden in der Studie die Themen Echtzeitbilanzierung und Planungssysteme für kundenindividuelle Preisgestaltung angesprochen.

Die Verbreitung elektronischer Zahlungsverfahren und das online banking wirken sich umfassend auf die Finanzbranche aus. Nach einer Analyse der verschiedenen Zahlungsverfahren werden Finanzdienstleistungen betrachtet, die über das Medium Internet abgewickelt werden können [Merz 02]. Das Angebotsspektrum der Finanzdienstleister wird sich erweitern. Banken streben danach, den Kunden in allen finanziellen Fragen zu betreuen und erweitern ihr Leistungsspektrum durch Firmenzukäufe oder strategische Allianzen. Als Beispiel eines zunehmend an Bedeutung gewinnenden Abrechnungsverfahrens werden die Experten nach Leasing und Vermietung von Software befragt.

## Ergebnisse

Unternehmensdaten werden heute bereits weitgehend elektronisch erfasst. Aus ihnen lassen sich in kurzer Zeit wertvolle Managementinformationen extrahieren. Denkbar ist in Zukunft, dass das Rechnungswesen komplette Unternehmensbilanzen ad hoc erstellen kann. Durch ERP-Systeme (Enterprise Resource Planing) wie SAP wird E-Reporting bereits eingeführt. Hierfür ist jedoch die permanente Erfassung der Daten und die konsequente Synchronisierung sämtlicher Geschäftsprozesse notwendig. Die Anforderungen an die Datenbanken, die Netze und die Algorithmen sind sehr hoch. Die Meinungen der Experten gehen bei dieser Frage weit auseinander (vgl. Abbildung 9.22, ①). Einige sehen E-Reporting erst in mehr als zehn Jahren, die Mehrheit der Experten prognostiziert jedoch eine weite Verbreitung bereits in 8 Jahren. Hier unterscheiden sich die Aussagen deutlich von der Vorgängerstudie, in der bereits das Jahr 2006 für eine Verbreitung von Echtzeitberichten anvisiert wurde [SETIK 00].

Einheitlicher beantworten die Experten dagegen die Frage nach IuK-basierten Controllingsystemen, zu dem Zweck, auch in Massenmärkten flexible kundenindividuelle Preisgestaltung zu ermöglichen (vgl. Abbildung 9.22, ②). Sie erwarten eine weite Verbreitung im Jahr 2010. Als Beispiele aus den unterschiedlichen Branchen nennen sie Finanzdienstleistungen oder Flugbuchungen. Hier lassen sich „on demand" Kundenkonditionen ermitteln, um so den Umsatz zu maximieren oder die Kostenstruktur zu minimieren.

In Zukunft wird sich die Bedeutung der verschiedenen Zahlungsverfahren gerade im Endkundengeschäft verschieben. Während die Experten den Micropayment-Systemen, also der Zahlung kleiner Geldbeträge über das Internet, einen bedeutsamen Zuwachs vorhersagen, prognostizieren sie, dass die Zahlung per Rechnung an Bedeutung verlieren wird (vgl. Abbildung 9.23). Jedoch wird sie auch in mehr als zehn Jahren noch deutlich oberhalb der Geldkarte und anderen Verfahren wie z.B. Handy-Zahlverfahren rangieren. Dem Zahlen per Kreditkarte sprechen Wissenschaftler wie auch die Experten aus den Unternehmen in den kommenden Jahren eine gleich bleibend hohe Bedeutung zu. So wird die Kreditkarte in drei bis zehn Jahren sogar einen höheren Stellenwert als die Zahlweise per Rechnung besitzen. Dennoch sind die Kosten für eine Transaktion relativ hoch im Vergleich zu beispielsweise den Micropayment-Systemen. Nach Ansicht der Experten wird deren Marktdurchdringung viel Zeit in Anspruch nehmen, doch letztlich lassen sich durch Micropayment-Systeme Vorteile auf Kunden- und Verkäuferseite realisieren. Ihren Anwendungsbereich haben die Systeme vorwiegend im privaten Konsum und Internethandel, bei dem Klein- und Kleinstbeträge umgesetzt werden. Zahlung per Rechnung wird im privaten wie im geschäftlichen Bereich weiterhin eine große Bedeutung haben. Über sie werden auch in Zukunft die mittleren und hohen Geldbeträge abgewickelt.

Die Experten aus der vorliegenden Studie sind sich wie schon vor drei Jahren einig darüber, dass Online-Banking das herkömmliche Filialbanksystem nie ablösen wird (vgl. Abbildung 9.22, ③). Sicherlich lassen sich durch die zunehmende Zahl an online ausgeführten Transaktionen die Filialnetze ausdünnen. Auch ist der Prozentsatz von online abwickelbaren Standardtransaktionen sehr hoch; jedoch kann eine Bank nicht jeden Kunden online erreichen und nicht jeden sensiblen Geschäftsvorfall unpersönlich abwickeln. Zukünftige, einfach zu bedienende Authentisierungsverfahren wie die Biometrie, werden Online-Banking weiter an Bedeutung gewinnen lassen (vgl. Abschnitt 7.3.10). Es wird sich als eine Alternative neben den Filialbanken etablieren, doch wird dieser Prozess nicht zu einer Ablösung führen.

Im Privatkundenbereich werden elektronische Zahlungssysteme von den Experten ähnlich beurteilt (vgl. Abbildung 9.22, ④). Wie bereits in der Vorgängerstudie wird nicht erwartet, dass Bargeld tatsächlich durch elektronisches Geld ersetzt wird. Auch hier prognostizieren sie eine Koexistenz beider Möglichkeiten, wobei Verbesserungen in den Sicherheitstechnologien zu einer Bedeutungssteigerung der elektronischen Verfahren führen werden.

Die Experten erwarten, dass sich gerade für Kleinstbeträge Zahlungssysteme wie Micropayment, die Geldkarte oder Mobiltelefon-Zahlungssysteme wie Paybox in den kommenden sieben


UNTERNEHMENSBILANZEN: Erstellung kompletter Unternehmensbilanzen auf Knopfdruck ist in 8 Jahren weit verbreitet.

KUNDENINDIVIDUELLE PREISGESTALTUNG: IuK-basierte Controllingsysteme ermöglichen in 6 Jahren kundenindividuelle Preisgestaltung.

ZAHLUNGSVERFAHREN: Micropayment-Verfahren werden in der Bedeutung stark zunehmen.

ONLINE-BANKING: Das herkömmliche Filialbanksystem wird nicht durch Online-Banking abgelöst werden.

ELEKTRONISCHE ZAHLUNGSSYSTEME: Elektronische Zahlungsverfahren werden im Privatkundenbereich nicht das Bargeld ersetzen.

KLEINSTBETRÄGE: Im Jahr 2010 werden Zahlungssysteme für Kleinstbeträge weit verbreitet sein.

CORPORATE-FINANCE-AKTIVITÄTEN: In 5 Jahren werden Corporate-Finance-Aktivitäten überwiegend über das Internet abgewickelt.

BANKEN ALS VIRTUELLE LEISTUNGSANBIETER: Banken werden in 5 Jahren als virtuelle Leistungsanbieter am Markt auftreten.

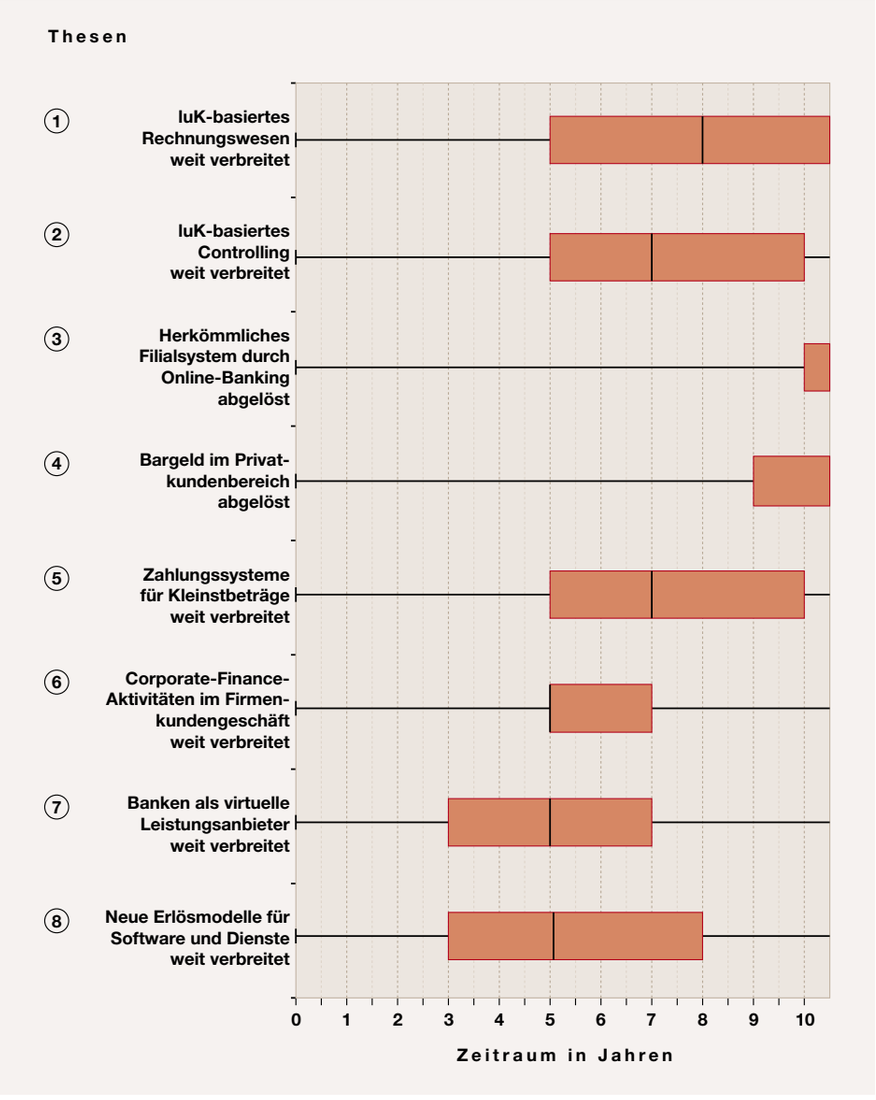



Abbildung 9.22: Ergebnisse der Thesen zu Controlling, Finanzdienstleistungen und Zahlungsverfahren

Jahren durchsetzen werden (vgl. Abbildung 9.22, ⑤). Der Endkundenhandel im Internet wird durch zukünftige Entwicklungen der Internetzahlungssysteme deutlich erleichtert werden. Doch der Kauf beispielsweise von Medieninhalten im Internet ist nicht die einzige Anwendung solcher Systeme: typische Einsatzgebiete finden sich auch im öffentlichen Nahverkehr, in Parkhäusern, Telefonzellen oder Fast-Food-Ketten.

Im Firmenkundengeschäft können viele Corporate-Finance-Aktivitäten in Zukunft überwiegend über das Internet abgewickelt werden. Die Experten aus der Vorgängerstudie hatten eine weite Verbreitung bereits bis zum Jahr 2005 erwartet. Diese Studie korrigiert den Zeitpunkt um drei Jahre nach hinten auf das Jahr 2008 (vgl. Abbildung 9.22, ⑥). Für Investment Banking, Risikomanagement und Mergers & Acquisitions ist die Einführung von übergreifend hohen Sicherheitsstandards notwendig.

In Zukunft werden Banken als virtuelle Leistungsanbieter am Markt auftreten und im Verbund mit verschiedenen Partnerunternehmen den Anforderungen des Kunden entsprechende maßgeschneiderte Angebote, so genannte „Tailored Ser-

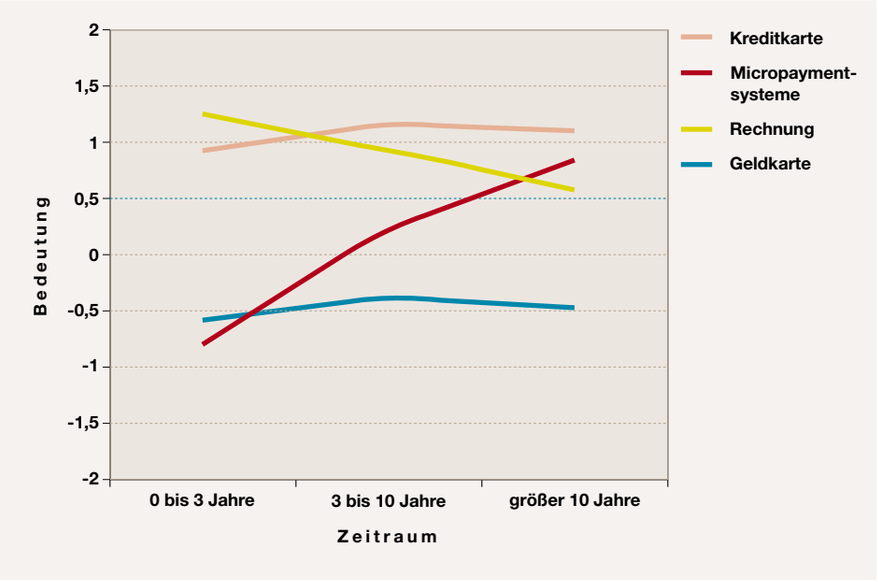



Abbildung 9.23: Bedeutung unterschiedlicher Zahlungsverfahren

vices“, konfigurieren können. Auch bei dieser Frage hat sich ergeben, dass die Experten vor drei Jahren die Entwicklungen im Banksektor optimistischer bewertet haben. Diese Studie revidiert den Zeitpunkt einer weiten Verbreitung von Banken als virtuelle Leistungsanbieter vom Jahr 2005 auf das Jahr 2008 (vgl. Abbildung 9.22, ⑦).

Neue Erlösmodelle wie Leasen oder Mieten von Software werden nach Aussagen der Experten in fünf Jahren weit verbreitet sein (vgl. Abbildung 9.22, ⑧). Gerade Großprojekte werden bei Anbietern wie HP, IBM oder Microsoft zunehmend über Leasing finanziert [Schu 02]. Weitere Einsatzgebiete sind die zeitlich begrenzte Nutzung von ASP-Diensten (Application Service Provisioning) im Internet. Die Experten weisen darauf hin, dass bei herunterladbarer Software die Beendigung der Nutzungsdauer schwierig zu kontrollieren ist und an dieser Stelle durch geeignete Kopierschutzmaßnahmen einem Missbrauch vorgebeugt werden muss. Darüber hinaus werden neue Erlösmodelle zu angemesseneren Lizenzierungen führen. Diese werden nur im erforderlichen Umfang und nur für den tatsächlich benötigten Zeitraum erworben. Der Kunde erwirbt nur die Lizenz für Produkte, die er tatsächlich für eine bestimmte Zeitspanne benötigt.

Neue Erlösmodelle für Software wie Pay-per-Use und Pay-per-Time werden in den folgenden Jahren nach Aussagen der Experten stark an Bedeutung gewinnen (vgl. Abbildung 9.24). Während derzeit der Anteil an gekaufter Software noch bei etwa 90% liegt, werden bereits in fünf bis zehn Jahren alternative Erlösmodelle 50% des Handels bestimmen. Gerade dem Geschäftskundenbereich bieten sich durch Miete oder Leasing entscheidende Vorteile. So kann der Kunde flexibler die benötigten Produkte zusammenstellen.

## Zusammenfassung

Auch in diesem Abschnitt wurde die Aussage bekräftigt, dass die IuK-Technologien traditionelle Vorgehensweisen durch neue Anwendungen oder Verfahren ergänzen, sie jedoch nicht vollständig ersetzen. Nachfolgend sind die Antworten der Experten zum Thema Preisgestaltungs-, Abrechnungs- und Zahlungsverfahren kurz zusammengefasst:

- Im Jahr 2011 wird es weit verbreitet sein, dass Unternehmen auf Knopfdruck aus ihren IuK-basierten Rechnungswesen-Systemen komplette Unternehmensbilanzen erstellen können.

LEASEN ODER MIETEN VON SOFTWARE: Leasen oder Miten von Software und Dienstleistungen wird in 5 Jahren weit verbreitet sein.

ANTEIL AN GEKAUFTER SOFTWARE: In 5-10 Jahren werden nur noch 50% der im Handel angebotenen Software käuflich erworben.

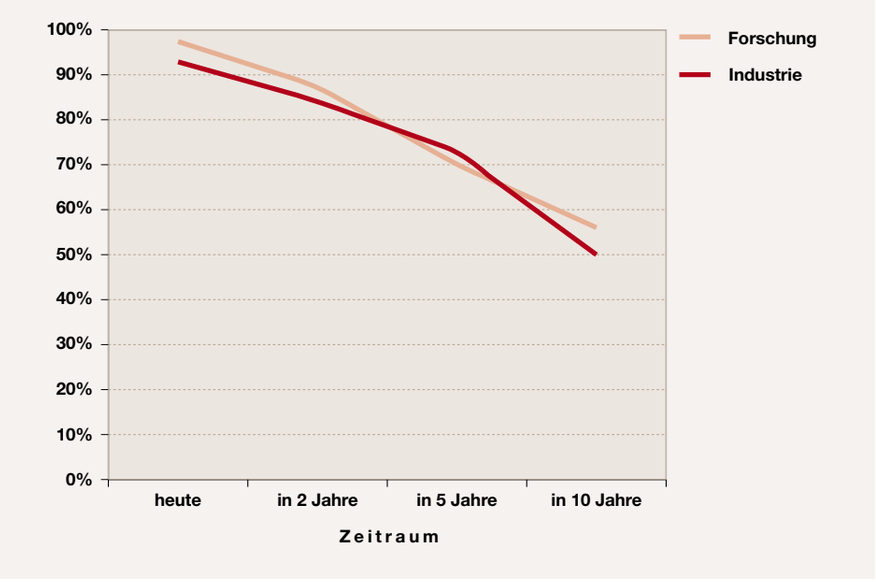



Abbildung 9.24: Anteil gekaufter Software gegenüber anderen Abrechnungsverfahren

- IuK-basierte Controllingsysteme, die eine kundenindividuelle Preisgestaltung ermöglichen, werden im Jahr 2009 weit verbreitet sein.
- Die Kreditkarte wird in den kommenden Jahren das bedeutendste Zahlverfahren sein. Micropayment-Verfahren werden in der Bedeutung stark zunehmen. Die Zahlweise per Rechnung wird dagegen leicht sinken. Geldkarten werden auch in Zukunft nicht an Bedeutung gewinnen.
- Das herkömmliche Filialbanksystem wird nicht durch Online-Banking abgelöst werden.
- Elektronische Zahlungsverfahren werden im Privatkundenbereich nicht das Bargeld ersetzen.
- Im Jahr 2010 werden Zahlungssysteme für Kleinstbeträge weit verbreitet sein.
- Im Jahr 2008 werden Corporate-Finance-Aktivitäten überwiegend über das Internet abgewickelt.
- Banken werden ab dem Jahr 2008 verbreitet als virtuelle Leistungsanbieter am Markt auftreten.
- Neue Erlösmodelle zur Abrechnung von Software und Dienstleistungen wie Miete oder Leasing werden im Jahr 2008 weit verbreitet sein.
- In 5-10 Jahren werden nur noch 50% der im Handel angebotenen Software käuflich erworben.

## 9.7 Konvergenz von Informations- und Unterhaltungsmedien

Der Medienmarkt basiert auf der Erstellung und Verbreitung von Inhalten. Diese können informierenden oder unterhaltenden Charakter haben. Die Entwicklungen der Informations- und Kommunikationstechniken und der Trend zur Digitalisierung beeinflussen gerade den Mediensektor stark. Die Informations- und Kommunikationstechnologie beschäftigt sich mit der Erstellung, Verarbeitung und Verbreitung von Daten in digitaler Form. Durch die der Informationen steht der Mediensektor technologisch auf derselben Basis wie der Informations- und Kommunikationssektor. Die dieser Märkte bewirkt eine Neustrukturierung der Produktions- und Verwertungsstufen im Mediensektor [Hass 02].

Der nachfolgende Abschnitt zeigt Konvergenzen bei der Produktion, Distribution und Konsumption von Mediengütern auf. In der Produktion geht der Trend

zur Mehrfachverwertung der Medieninhalte. Produktionen werden unabhängig von der späteren Nutzung gespeichert und können ad hoc zu, dem jeweiligen Ausgabemedium optimal entsprechenden, Einheiten gebündelt und umdefiniert werden. So kann eine Nachrichtenredaktion im Fernsehen ein Video ausstrahlen, dieselbe Nachricht im Internet mit einem Foto präsentieren und bei der Übertragung via WAP (Wireless Application Protocol) auf ein Mobiltelefon ohne graphische Elemente verfügbar machen. Die Verbreitung der Medieninhalte kann über die unterschiedlichsten Übertragungsmedien erfolgen. Der analoge und der digitale terrestrische Funk stehen mit Satellitenverbindungen und Kabelnetzen in Konkurrenz.

Konvergenz ist auch bei den Endgeräten festzustellen. So lässt sich mit dem PC über das Internet Fernsehen empfangen und Mobilfunkgeräte besitzen Internetbrowser [ZPS 01]. Gerade die Entwicklung der MHP (Multimedia Home Platform) lässt Fernsehen und Internet konvergieren. Die MHP ist rückkanalfähig und ermöglicht so Interaktivität. Fernsehgeräte können in Zukunft neben Programminformationen auch interaktive Spiele anbieten. Dies ist ein erster Schritt in Richtung interaktives Fernsehen.

Der folgende Teil der Befragung konzentriert sich auf die Nutzung multimedialer Inhalte für die Darstellung privater und geschäftlicher Informationen und für die Unterhaltung. Multimediale Techniken, interaktive Nutzungsmöglichkeit unterschiedlicher digitaler Medientypen wie Text, Bild, Audio und Video, schaffen virtuelle Realitäten [ScHe 99]. Für den Dialog mit dem Kunden können virtuelle Räume beispielsweise von Architekturbüros zur kostengünstigen aber realistischen Visualisierung von Messeständen und Gebäuden eingesetzt werden. Im Unterhaltungsbereich nimmt die Bedeutung von Computerspielen immer mehr zu. Ihre Verkaufserlöse übertrafen im letzten Jahr bereits die Einspielergebnisse von Kinofilmen [Will 02]. Die frühere Vision einer Konvergenz von interaktivem Fernsehen, Spielfilmen und Computerspielen erscheint bei anhaltender Leistungssteigerung der Computer erreichbar zu sein.

## Ergebnisse

Mit dem Umstieg auf digitales terrestrisches Fernsehen und Rundfunk wird die analoge Technik substituiert. Daraus ergibt sich innerhalb der nächsten Jahre ein Bedeutungszuwachs digitaler Medien für die Informationsbeschaffung und zur Unterhaltung (vgl. Abbildung 9.25). Gerade Informationsmedien wie Zeitschriften und Bücher werden in Zukunft vermehrt in digitaler Form produziert, gebündelt und an den Endkunden vertrieben, da so die Transaktionskosten stark gesenkt werden können. Die Kopplung von Fernsehen und Internet wird dem Kunden stets aktuelle Informationen zu Politik, Sport und ähnlichen Inhalten in digitaler Form personalisiert liefern können.

Die Experten erwarten, dass bereits in sieben Jahren vollständig digitale Produktionen von Medieninhalten wie Musik, Kinofilm und Fernsehen die analogen Techniken abgelöst haben werden (vgl. Abbildung 9.26, ①).

Allerdings müssen zuvor hohe Investitionen in die benötigten Geräte und in den Aufbau von Know-How fließen. Technischer Entwicklungsbedarf besteht gerade für Videoanwendungen noch bei geeigneten Speichermedien mit hoher Kapazität und hohem Datendurchsatz. Für die Aufnahme von Bildmaterial müssen hochauflösende Bildsensoren eingesetzt und die Datenströme in Echtzeit verlustfrei komprimiert werden. Als Resultat können dem Kunden bessere Bild- und Mehrkanal-Tonqualität geboten werden.

Das Fernsehen wird in Zukunft mit dem Internet konvergieren. Die Experten erwarten, dass bis zum Jahr 2010 internetfähige Fernsehgeräte weit verbreitet sein werden (vgl. Abbildung 9.26, ②). Allerdings ist noch offen, welche Anwendungsmöglichkeiten sich am Fernsehen durchsetzen werden. Möglich sind Programminformationen, erweiterte Nachrichtendienste, Produktinformationen, Wareneinkauf und interaktive Spiele. Die Experten erwarten dennoch eine Koexistenz des PCs neben dem internetfähigen Fernsehgerät. Ihre Erwartungen sind jedoch pessimistischer als in der Vorgängerstudie [SETIK 00]. Mittlerweile sind zwar erste Endgeräte am Markt verfügbar, die digitale Satellitenempfänger besitzen und die Multimedia-

BEDEUTUNGSZUWACHS DIGITALER MEDIEN: Die Bedeutung der digitalen Medien zur Information und Unterhaltung wird in den kommenden Jahren stark zunehmen.

DIGITALE PRODUKTIONEN VON MEDIENINHALTEN: Digitale Produktionsformen haben in 7 Jahren die analogen Techniken abgelöst.

INTERNETFÄHIGE FERNSEHGERÄTE: Internetfähige Fernsehgeräte sind in 7 Jahren weit verbreitet.


Abbildung 9.25: Bedeutung digitaler Medien zur privaten Informationsbeschaffung und zur Unterhaltung

VIDEO-ON-DEMAND UND INTERAKTIVES FERNSEHEN: Interaktives Fernsehen und Video-on-Demand werden klassisches Fernsehen und Videotheken nie ablösen.

MULTIMEDIALE WEITERBILDUNGSANGEBOTE: In 7 Jahren sind multimediale Weiterbildungsangebote weit verbreitet.

MULTIMEDIA UND VIRTUAL REALITY ALS MARKETING-INSTRUMENTE: Multimedia und Virtual Reality sind in 5 Jahren weit verbreitete Marketing-Instrumente.

Home-Plattform (MHP) unterstützen, dennoch sind die Lebenszyklen von Fernsehgeräten nicht mit denen eines PCs vergleichbar, so dass eine marktabdeckende Verbreitung dieser Technologie noch einige Jahre dauert.

Wie bereits in der Studie 2000 im Ergebnis festgehalten, verneinen die Experten eine Ablösung des klassischen Fernsehens und der Videotheken durch Video-on-Demand und interaktives Fernsehen (vgl. Abbildung 9.26, ③). Breitbandnetze ermöglichen in Zukunft Video-on-Demand, jedoch erwarten die Experten nur eine Ergänzung der Medienverwertungskette. Eine Ablösung des Fernsehens mit seinem fremd bestimmten Programmangebot sehen die Experten ebenso wenig wie die rasche Akzeptanz von interaktivem Fernsehen. Wohl lassen sich durch Video-on-Demand oder im Kinobereich durch E-Cinema Kosten für die Speicherung und Verteilung der Medien einsparen, doch kommt dem Gemeinschaftserlebnis beim Kinobesuch immer größere Bedeutung zu. Video-on-Demand wird ihn ebenso wenig ersetzen wie die klassische Videothek.

Nach Ansicht der Experten werden im Jahr 2010 multimediale Weiterbildungsangebote, beispielsweise von virtuellen Volkshochschulen, weit verbreitet sein (vgl. Abbildung 9.26, ④). Auch das Zutreffen dieser These wurde in der Vorgängerstudie bereits drei Jahre früher prognostiziert. Nach Ansicht der Experten lassen sich Lehrangebote über das Internet dann erfolgreich durchführen, wenn das Medium Internet einen realen Kursbetrieb ergänzt. Sehr wichtig erscheint in diesem Bezug auch der persönliche Kontakt zu einem realen Lehrer. Benutzerfreundliche Oberflächen und kurs- und leistungsverwaltende Software müssen eingesetzt werden. Für eine Audio- und Videoübertragung zum Schüler sind zudem Breitbandnetze notwendig. Als mögliche Anwendungsfelder nennen die Experten zum Beispiel innerbetriebliche Fort- und Weiterbildungen.

Im Marketing ermöglichen die Entwicklungen in den Informations- und Unterhaltungsmedien neue Möglichkeiten. So werden sich nach Ansicht der Experten in fünf Jahren Multimedia und Virtual Reality als Marketing-Instrumente durchgesetzt haben (vgl. Abbildung 9.26, ⑤). Durch die Weiterentwicklung der Endgeräte, wie hochwertige 3D-Displays, lassen sich über breitbandige Netze Produkte in virtuellen Räumen präsentieren. Nach der Studie 2000 hätten Multimedia und Virtual Reality bereits im kommenden Jahr weit verbreitet sein sollen.

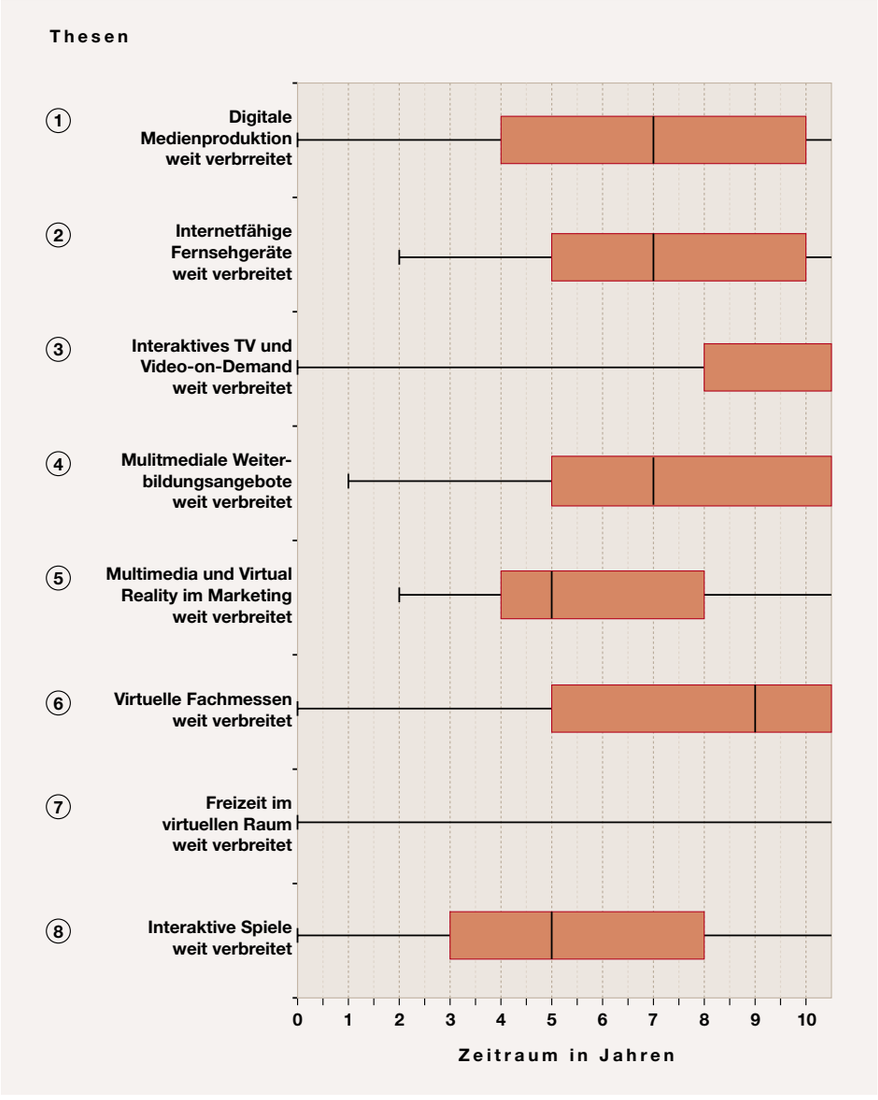



Abbildung 9.26: Ergebnisse der Thesen zu Konvergenz von Informations- und Unterhaltungsmedien

VIRTUELLE FACHMESSEN FÜR PRODUKTPRÄSENTATIONEN: Virtuelle Fachmessen werden frühestens in 9 Jahren weit verbreitet sein.

FREIZEIT IN VIRTUELLEN RÄUMEN: Freizeit in virtuellen Räumen zu verbringen wird sich nicht allgemein durchsetzen.

INTERAKTIVE SPIELE: In 5 Jahren werden Online-Spiele weit verbreitet sein.

Virtuelle Fachmessen für Produktpräsentationen schätzen die Experten unterschiedlich ein. Die Funktionen einer Messe sind komplexer und vielfältiger, als dass sie sich durch Virtual Reality abdecken ließen. Gerade persönliche Kontakte auf Messen lassen sich nicht einfach ersetzen. In einigen Branchen sind Produktpräsentationen mittels Virtual Reality gut denkbar, die Experten nennen als Beispiel die Medienbranche oder die Softwaretechnik. Virtual Reality wird sich eher als zusätzliche Präsentationsplattform neben traditionellen Messen etablieren. So erwarten die Experten eine weite Verbreitung frühestens in neun Jahren (vgl. Abbildung 9.26, ⑥).

Wie bereits vor drei Jahren erachten die Experten die Gruppe derer, die einen Großteil Ihrer Freizeit in virtuellen Räumen, in Phantasiewelten oder in Arenen verbringen, für vergleichsweise unbedeutend, so dass sie keine allgemeine Verbreitung dieser Handlungsweise prognostizieren (vgl. Abbildung 9.26, ⑦).

Interaktive Spiele, bei denen online mit realen oder künstlichen Spielpartnern in Echtzeit agiert wird, werden allerdings bereits in fünf Jahren eine weite Verbreitung erlangt haben (vgl. Abbildung 9.26, ⑧). Strategie-, Sport- und Wettkampfspiele werden zunehmend vernetzt ausge-

tragen. Breitbandige und kostengünstige Netze sowie leistungsfähige Endgeräte sind die wichtigsten technischen Voraussetzungen.

### Zusammenfassung

Im Bereich der Informations- und Unterhaltungsmedien stehen weitreichende Veränderungen bevor. Die Digitalisierung der Medien in Produktion, Verbreitung und Konsum wird innerhalb des nächsten Jahrzehnts vollzogen sein. Nachfolgend werden die einzelnen Ergebnisse der Expertenbefragung zu diesem Themengebiet kurz zusammengefasst:

- Die Bedeutung der digitalen Medien zur privaten Informationsbeschaffung und zur Unterhaltung wird in den kommenden Jahren stark zunehmen.
- Die vollständig digitale Produktion von Medieninhalten wird bis zum Jahr 2010 die analogen Techniken abgelöst haben.
- Internetfähige Fernsehgeräte sind in 2010 weit verbreitet.
- Interaktives Fernsehen und Video-on-Demand werden klassisches Fernsehen und Videotheken nie ablösen.
- Im Jahr 2010 sind multimediale Weiterbildungsangebote weit verbreitet.
- Multimedia und Virtual Reality sind im Jahr 2008 weit verbreitete Marketing-Instrumente.
- Virtuelle Fachmessen werden frühestens im Jahr 2012 weit verbreitet sein.
- Es wird nicht allgemein weit verbreitet sein, Freizeit in virtuellen Räumen zu verbringen.
- Im Jahr 2008 werden Online-Spiele weit verbreitet sein.

## 9.8 Rechtemanagement und elektronische Wahlverfahren

Das nachfolgende Kapitel betrachtet zwei aktuelle Anwendungsfälle von Sicherheitstechnologien näher, DRM-Systeme (Digital Rights Management) und elektronische Wahlverfahren.

Digitaltechnologie ermöglicht den Informationskonsumenten, die Informationen leicht zu bearbeiten, verlustfrei zu kopieren und schnell zu verbreiten. Diese Eigenschaften sind sehr attraktiv für die Informationsanbieter, da sie ihnen neue Geschäftsbereiche eröffnen. Leider bringen diese Merkmale digitaler Medien auch Gefahren und Bedrohungen mit sich. Unehrliche Nutzer können leicht Raubkopien anfertigen und diese sehr schnell verbreiten. Illegale Verbreitung und unautorisierte Nutzung sowie Manipulation digitaler Werke verursachen Urhebern und der Industrie erhebliche Schäden. Das Urheberrecht (Copyright) stellt das Recht an geistiger Schöpfung dar, die normalerweise in Form eines Werkes vorliegt. Allein der Urheber kann über die Veröffentlichung und Verwertung seines Werkes sowie dessen Veränderung entscheiden. Urheber können gewisse Rechte an ihren Werken an andere transferieren bzw. diese lizenzieren. Die DRM-Systeme sollen geeignete Umgebungen für die autorisierte und rechtmäßige Nutzung digitaler Güter bzw. Rechte an diesen Gütern und den Handel mit ihnen schaffen. Das vorrangige Ziel der DRM-Systeme ist es, die Rechte und Interessen von Urhebern und weiteren Rechteinhabern zu schützen. Um dies zu erreichen, spielen neben den technischen Maßnahmen auch rechtliche und wirtschaftliche Aspekte (z.B. Geschäftsmodelle) bedeutende Rollen. Im Folgenden wird ein kurzer Einblick in die grundlegenden technischen Maßnahmen gegeben.

In der Vergangenheit wurde eine Vielzahl technischer Verfahren gegen den Missbrauch und die Verletzung der Urheberrechte vorgeschlagen. Diese können im Wesentlichen in zwei Klassen, präventive und repressive Maßnahmen, mit unterschiedlichen Zielsetzungen, eingeteilt werden. Präventive Verfahren sollen unautorisierte Aktionen verhindern, während die repressiven vor illegalen Aktionen abschrecken sollen.

Präventive Maßnahmen setzen manipulationssichere Hard- bzw. Software voraus [NRC 00]. In der Praxis ist dies jedoch eine starke Annahme [AnKu 96, BGR+ 01]. Die Realisierung dieser Verfahren erfordert i.a. neben dem Einsatz hardwaretechnischer Maßnahmen auch den Einsatz und das Zusammenspiel verschiedener kryptographischer und sicherheitstechnischer Komponenten, wie Verschlüsselung, Zugriffsmechanismen usw.

Dagegen benötigen repressive Maßnahmen im Allgemeinen keine manipulationssichere Hard- bzw. Software und bedienen sich u.a. steganographischer Techniken zur Kennzeichnung der Daten. Sie sollen auch dann wirksam sein, wenn präventive Maßnahmen überlistet wurden. Die Datenkennzeichnungsverfahren sollen den Urhebern erlauben, ihre Urheberschaft zu beweisen oder Raubkopierer (nachweisbar) zu identifizieren.

Diese Verfahren betten urheber- bzw. nutzerspezifische Informationen, genannt Wasserzeichen, für den Konsumenten unwahrnehmbar in digitale Werke ein. Traditionell nennt man ein solches Verfahren Watermarking [KaPe 00] bzw. Fingerprinting [Wagn 83, Crypto85, Crypto95, CKLS 97]. Die wichtigste Anforderung an die zum Urheberschaftsschutz eingesetzten Kennzeichnungsverfahren ist die Robustheit gegen Angriffe, bei denen versucht wird, das Wasserzeichen zu entfernen. Die Robustheit ist im Allgemeinen eine starke Annahme. Die existierenden Verfahren sind in der Regel robust gegen bestimmte Klassen von Transformationen (bzw. Angriffe), wie z.B. Kompression, geometrische Operationen, Überlagerung mit Rauschsignalen, usw.

Die meisten existierenden Kennzeichnungslösungen eignen sich hauptsächlich für Bild- und Toninhalte. Die Mehrheit der Watermarking-Verfahren ist symmetrisch. Sie verwenden ein und denselben Schlüssel zur Einbettung und zur Extraktion bzw. Detektion des Wasserzeichens. Die Idee für den Urheberschutz ist, dass nur der Urheber den geheimen Schlüssel kennt und somit in der Lage ist, das Enthaltensein seines Wasserzeichens in seinem Werk zu zeigen. Einen anderen Ansatz bietet das asymmetrische Watermarking, bei dem ein geheimer Schlüssel zur Einbettung und ein öffentlicher Schlüssel zur Detektion des Wasserzeichens verwendet wird. Die existierenden asymmetrischen Verfahren sind jedoch unsicher [ESG 00].

Das Ziel der Fingerprinting-Verfahren ist es, die Quelle der illegalen Verteilung digitaler Werke zu identifizieren. Bei diesem Ansatz beinhaltet das Wasserzeichen Identifizierungsinformationen des entsprechenden Benutzers, z.B. des Käufers. Findet man ein unautorisiert verteiltes Werk, so soll man diese Information aus dem verteilten Werk extrahieren und den entsprechenden Benutzer identifizieren können.

Im zweiten Teil des Abschnitts werden verschiedene Formen der technischen Realisierung sowie der technischen Absicherung von elektronischen Wahlverfahren betrachtet. Unter einer Online-Wahl soll in diesem Abschnitt die Möglichkeit zur elektronischen Stimmabgabe verstanden werden, wobei durch den Vorgang der Online-Wahl die konventionelle Urnen-Wahl nachgebildet wird.

## Ergebnisse

Die Einschätzungen der Befragten sind in Abbildung 9.27 aufgezeichnet. Nach Ansicht von vielen Befragten werden sichere Watermarking-Verfahren in etwa fünf Jahren verfügbar sein (vgl. Abbildung 9.27, ①). Trotz des stark wachsenden Bedarfs an robusten Watermarking-Verfahren vertreten viele der Experten allerdings auch die Ansicht, dass keine hinreichend robusten Verfahren zu erwarten sind. Lediglich eine Kopplung an Hardware könnte die Erkennungsrate verbessern und die Fälschungssicherheit erhöhen. Neue Anwendungspotenziale werden im Bereich des Urheberschutzes und dem Originalitätsschutz, bei Urheberschaftsbeweisen für digitale Inhalte und zur Identifizierung von Raubkopien digitaler Werke gesehen. Damit ergeben sich neue Möglichkeiten für den Vertrieb von Unterhaltungsmedien über das Internet (Musik / Video on Internet).

Asymmetrische Watermarking-Verfahren werden in drei Jahren verfügbar sein (vgl. Abbildung 9.27, ②). Die Befragten gehen davon aus, dass technisch sinnvolle Watermarkingverfahren asymmetrisch realisiert werden, insbesondere ist das nötige Vertrauen in die teilnehmenden Parteien geringer und die Tamper-Resistance weniger

ROBUSTE WATERMARKING-VERFAHREN: Sichere Watermarking-Verfahren sind in 5 Jahren verfügbar.

ASYMMETRISCHE WATERMARKING-VERFAHREN: Asymmetrische Watermarking-Verfahren sind in 3 Jahren verfügbar.

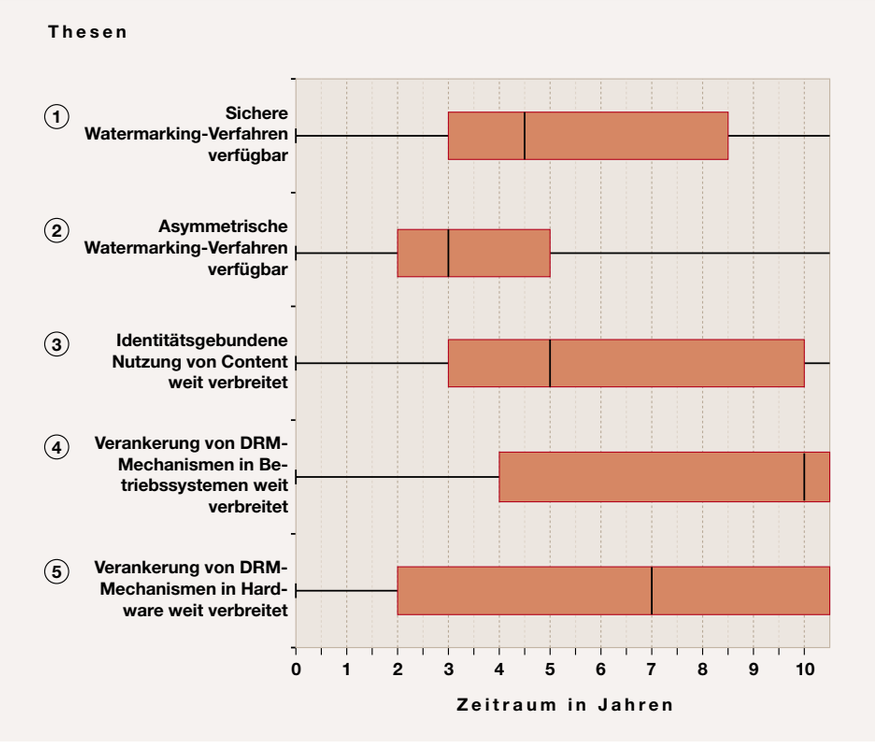



Abbildung 9.27: Ergebnisse der Thesen zu Rechtemanagement und elektronische Wahlverfahren

IDENTITÄTSGEBUNDENE NUTZUNG VON CONTENT: Identitätsgebundene Nutzung von Content wird in 5 Jahren weit verbreitet sein.

VERANKERUNG VON DRM-MECHANISMEN IN BETRIEBSSYSTEMEN: In 10 Jahren werden DRM-Systeme in Betriebssystemen verbreitet sein.

kritisch. Nach Ansicht der Experten könnten in der Zwischenzeit Alternativen wie „Zero-Knowledge Watermark Detection" hilfreich sein [Crav 99, AdSa 01].

Die weite Verbreitung von identitätsgebundener Nutzung von Content wird in etwa fünf Jahren erwartet (vgl. Abbildung 9.27, ③). Die Befragten erhoffen sich davon eine ganze Reihe neuer Anwendungspotenziale wie beispielsweise bei kostenpflichtigen Informations- und Unterhaltungsdiensten (Audio, Video), neue Modelle der Softwarelizensierung sowie verschiedene Formen personalisierter Inhalte. Darüber hinaus wird ein verbesserter Zugriffsschutz auf kommerzielle digitale Waren möglich mit dem entsprechenden Marken- und Wertschutz. Einige geben diesen Ansätzen hohes Potenzial zum Schutz von Inhalten, beispielsweise innerhalb von File-Sharing-Systemen. Andere sehen nur in Teilgebieten oder als Nischenprodukt Chancen. Kritisiert wird, dass zum einen keine passende Infrastruktur vorhanden ist und die technische Realisierung schwierig ist. Viele der Befragten gehen davon aus, dass die Industrie versuchen wird, derartige technische Entwicklungen zur Durchsetzung neuer Vertriebsmodelle weiter voranzutreiben. Allerdings wird die Akzeptanz durch den Nutzer bezweifelt. Einige hoffen sogar, dass der Markt solche Systeme nicht akzeptiert und verweisen auf ungelöste Sicherheits- und Datenschutzprobleme. Darüber hinaus wird kostenpflichtigen Diensten kaum Chancen eingeräumt, solange kostenfreier Content einfach verfügbar ist. Als Beipiel für Tendenzen der Industrie, technische Voraussetzungen für neue Lizensierungsmodelle zu schaffen wird Microsofts Palladium [Manf 02] und die Initiative des TCPA-Konsortiums (Trusted Computing Platform Alliance) [TCPA 03] genannt.

Daran knüpft die Frage an, wann die Verankerung von DRM-Mechanismen in Betriebssystemen weit verbreitet sein wird. Dies wird von den Befragten frühestens in zehn Jahren erwartet (vgl. Abbildung 9.27, ④); etwa ein Viertel der Befragten geht sogar davon aus, dass eine solche Verankerung nie verbreitet sein wird. Viele Experten sehen die Akzeptanz durch den Nutzer als nicht gegeben an

und bezweifeln die technische Wirksamkeit. Bisherige Ansätze haben viele Probleme verursacht ohne den gewünschten Effekt zu erzielen, beispielsweise der Kopierschutz bei CD-ROMs. Positive Effekte werden beispielsweise für die Lizenzierung von Standard-Software gesehen sowie durch die Schaffung neuer Verbreitungskanäle und neuer Geschäftsmodelle für digitale Inhalte. Auch Spezialgeräte wie internetfähige Abspielgeräte mit DRM als Grundausrüstung sind denkbar. Die Befragten erwarten, dass zukünftige Microsoft-Betriebssysteme derartige Mechanismen integrieren werden, wieder mit dem Verweis auf die Palladium-Initiative. Einige erwarten diese Tendenz nicht bei Open-Source Betriebssystemen.

Die weite Verbreitung der Verankerung von DRM-Mechanismen auf Hardwareebene wird in sieben Jahren erwartet (vgl. Abbildung 9.27, ⑤). Die Befragten sehen neben den bereits genannten weitere Anwendungsmöglichkeiten beispielsweise im Kopierschutz von Datenträgern und bei der Lizenzierung von Betriebssystemen. Im Kontext von hardwarebasierten DRM-Mechanismen wird die TCPA-Initiative genannt. Die Experten verweisen allerdings darauf, dass bereits heute DRM-Schutzmechanismen in Hardware angewendet werden, beispielsweise bei der DVD. Hierbei hat sich gezeigt, dass diese immer wieder ausgehebelt werden. Daher erwarten einige der Befragten keine durchgängige Lösung.

Sichere Online-Wahlverfahren für die Stimmabgabe über das Internet vom heimatlichen PC aus werden nach Ansicht der Befragten in etwa fünf Jahren verfügbar sein (vgl. Abbildung 9.27, ⑥). Es werden zahlreiche Anwendungspotenziale gesehen, beispielsweise mehr Elemente direkter Demokratie, evtl. auch Beteiligung an Hauptversammlungen von Aktiengesellschaften. Weitere Anwendungsfelder werden bei Meinungsumfragen, Vereinswahlen/-abstimmungen, politischen Schattenwahlen, wie beispielsweise bei Kandidatenaufstellungen und Vorstandswahlen (aber eher keine Bundestagswahlen), Sitzungsabstimmungen sowie grundsätzlich bei Wahlen ohne physische Präsenz gesehen. Als Voraussetzung wird die Verbreitung qualifizierter elektronischer Signaturen, anonymisierender Protokolle, sicherer Wahlzentren sowie vor allem vertrauenswürdiger Betriebssystemumgebungen gesehen. Auch wird darauf hingewiesen, dass neben technischen Problemen vor allem rechtliche und politische Fragestellungen für eine Etablierung ausschlaggebend sein dürften.

Für die Durchführung einer elektronisch gestützten Wahl gibt es verschiedene Möglichkeiten, deren Bedeutung durch die Experten zum Teil unterschiedlich bewertet wird und in Abbildung 9.28 aufgezeichnet ist. Insgesamt wird jedoch die derzeitige Bedeutung der vorhandenen Möglichkeiten als gering eingestuft. Die größte Bedeutung innerhalb der nächsten zehn Jahre wird dabei der elektronischen Wahl an einem vernetzten Wahlgerät in einem beliebigen Wahllokal innerhalb Deutschlands beigemessen. Diese Wahlkonstellation könnte bei Bundes-, Landes- oder Kommunalwahlen Anwendung finden. Die Befragten bewerten die Möglichkeit als zukunftsweisend, sofern Sicherheitsbedenken durch eine geeignete Infrastruktur und anonyme Wahlprotokolle ausgeräumt werden können. Wie bei den anderen Möglichkeiten müssen auch hier die übergreifenden Wahlrechtsgrundsätze eingehalten werden [UKK 01]. Der elektronischen Wahl von einem beliebigen PC aus über das Internet wird von den Befragten langfristig eine erhebliche Bedeutungssteigerung zugesprochen. Anwendungsbereiche werden allerdings weniger im politischen Bereich als bei Betriebswahlen, Meinungsumfragen und Hauptversammlungen von AGs erwartet. Viele sehen andererseits hohe Defizite bei den heutigen Wahlverfahren und juristische Probleme („Stimmenkauf") für den Einsatz bei Bundestagswahlen. Geringere Bedeutung wird nach Ansicht der Befragten die elektronische Wahl von einem mobilen persönlichen Endgerät über ein beliebiges Kommunikationsmittel haben. Anwendungsbereiche wären beispielsweise Hauptversammlungen von AGs oder Wahlen auf Parteitagen und großen Delegiertenversammlungen. Die elektronische Wahl an einem nicht vernetzten Wahlgerät im Heimat-Wahllokal wird mittelfristig mäßig an Bedeutung gewinnen jedoch langfristig wieder an Bedeutung verlieren. In erster Linie werden hier, als Übergangslösung, Möglichkeiten zur Aufwandsreduktion bei der Auswertung von Urnenwahlen gesehen.

VERANKERUNG VON DRM-MECHANISMEN AUF HARDWAREEBENE: In 7 Jahren werden DRM-Systeme auf Hardwareebene verbreitet sein.

SICHERE ONLINE-WAHLVERFAHREN: Sichere Online-Wahlverfahren für die Stimmabgabe über das Internet werden in 5 Jahren erwartet.

ELEKTRONISCH GESTÜTZTE WAHL: Der elektronischen Wahl an einem vernetzten Wahlgerät im Heimat-Wahllokal werden mittel- und langfristig die meisten Chancen eingeräumt.

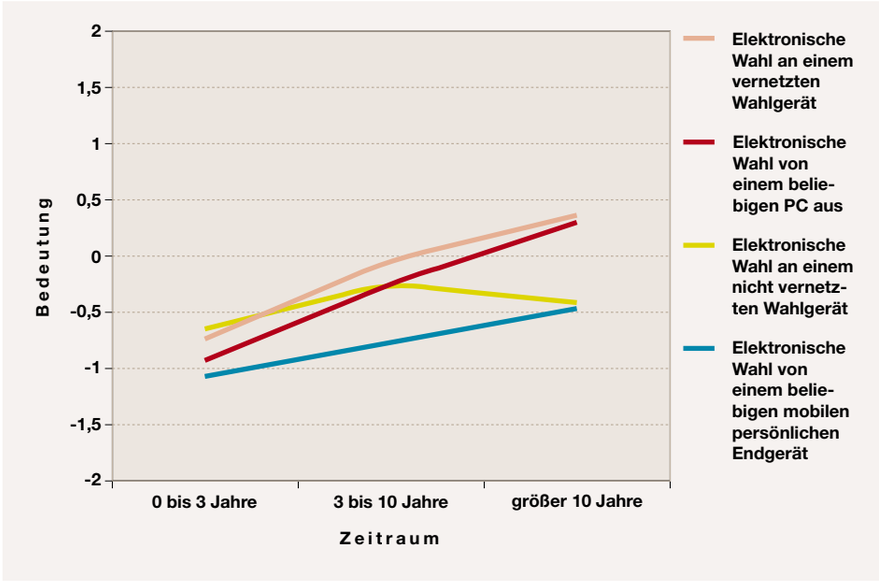



Abbildung 9.28: Bedeutung verschiedener elektronischer Wahlverfahren

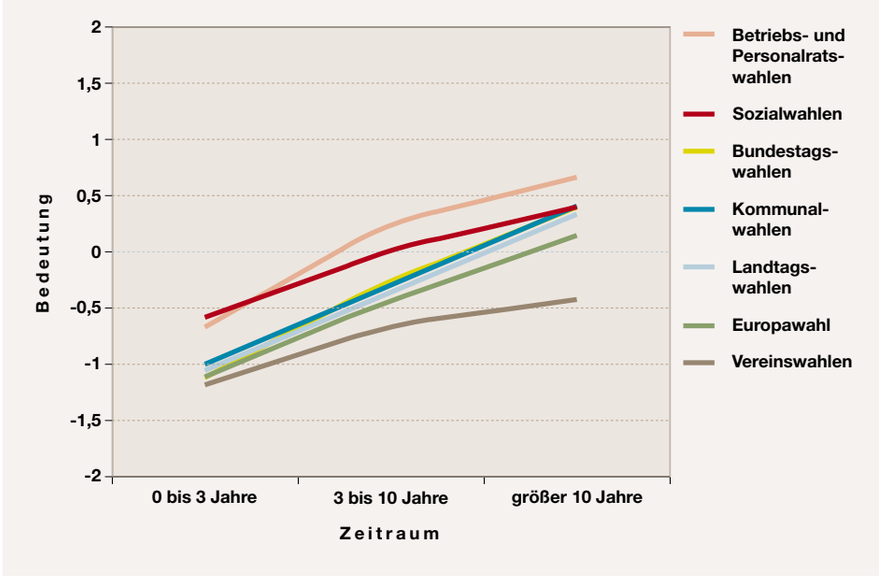



Abbildung 9.29: Bedeutung verschiedener Anwendungsfelder von Online-Wahlen

Bei der Bewertung der zukünftigen Bedeutung der Anwendungsfelder von Online-Wahlen sehen die Befragten mittel- und langfristig die größte Bedeutung bei Betriebs- und Personalratswahlen (vgl. Abbildung 9.29) . Weitere Anwendungen in diesem Zusammenhang sind beispielsweise Abstimmungen bei internen Organisationsprozessen, insbesondere bei Behörden und größeren Unternehmen. Positiv für die weitere Entwicklung wird die vorhandene Infrastruktur (Nutzung der Arbeitsplatzrechner, Intranet, zentrale Server) gesehen. Zur Klärung der rechtlichen Voraussetzungen werden sowohl Gesetzesänderungen als auch Betriebsvereinbarungen als notwendig erachtet. Eine große Bedeutung kommt Online-Wahlen, nach Ansicht der Befragten, sowohl derzeit als auch in den nächsten Jahren bei Sozialwahlen zu, beispielsweise bei Krankenkassenwahlen. Darin erhofft man sich eine stärkere Wahlbeteiligung, insbesondere bei jüngeren und „innovativen" Kunden. Bei Kommunal-, Landtags, Bundestagswahlen und Wahlen zum Europäischen Parlament spielen Online-Wahlen derzeit keine Rolle. Die Experten erwarten allerdings, dass Online-Wahlen in diesen Bereichen in den nächsten zehn Jahren erheblich an Bedeutung hinzugewinnen werden. Bei Kommunalwahlen werden zusätzliche Schwierigkeiten durch ein teilweise kompliziertes Wahlrecht (kumulieren und panaschieren) gesehen. Allerdings sind dort Pilotversuche sehr gut möglich. Bei Landtags- und Bundestagswahlen werden nach Einschätzung der Befragten noch höhere Sicherheitsstandards erwartet. Zusätzlich sind Gesetzesänderungen nötig. Da dies bei den Wahlen zum EU-Parlament europaweit geschehen müsste, wird die Bedeutung von Online-Wahlen dort geringer eingeschätzt. Insgesamt wird darauf hingewiesen, dass trotz der Etablierung von Online-Wahlen auch zukünftig traditionelle Alternativen vorhanden sein werden. Bei Wahlen zum Vereinsvorstand etc. erwarten die Befragten ebenfalls eine steigende Bedeutung von Online-Wahlen, allerdings wird diese in zehn Jahren deutlich unter dem der anderen betrachteten Wahlen liegen. Begründet wird dies damit, dass Vereine der technischen Entwicklung meist aus finanziellen Gründen nachfolgen. Darüber hinaus ist die zwischenmenschliche Kommunikation bei vielen Vereinen ein wichtiges Fundament der Vereinsarbeit; daher könnten, eher unpersönliche, Online-Wahlen nur bei sehr großen und überregionalen (z.B. Verbänden) oder bei Computer-affinen Vereinen Akzeptanz finden.

Nach Ansicht der Experten werden Online-Wahlen in den nächsten zehn Jahren als Ergänzung zu Urnen- und Briefwahlen erheblich an Bedeutung hinzugewinnen (vgl. Abbildung 9.30). Allerdings werden hinreichend große Sicherheitsstandards als zwingende Voraussetzung gesehen. Auch der alleinige Ersatz von Briefwahlen wird ähnlich optimistisch gesehen. Allerdings müsse nach Ansicht der Experten die Problematik des diskriminierenden Technikeinsatzes gelöst werden. Insbesondere eignen sich Briefwahlen ideal als „Experimentierfeld" für elektronische Wahlen. Dem alleinigen Ersatz von Urnenwahlen wird weniger Bedeutung beigemessen, obwohl dieser ebenfalls in den nächsten zehn Jahren an Bedeutung hinzugewinnen dürfte. Problematisch wird dies aus politischen Erwägungen gesehen. Insgesamt wird davon ausgegangen, dass Online-Wahlen nicht vor zwanzig bis dreißig Jahren andere Alternativen vollständig abgelöst haben werden.

Nach dem heutigen Stand der Technik können elektronische Wahlen die Sicherheitsanforderungen je nach Ausgestaltung des Wahlvorganges nur unvollständig erfüllen. So gewährleisten zur Zeit bekannte Verfahren für die Realisierung elektronischer Wahlen über das Internet nicht die Einhaltung des Grundsatzes der geheimen Wahl. Diese Tatsache führt nach Einschätzung der Experten derzeit nur zu einer mäßigen Akzeptanz von Online-Wahlen bei den Wählern und sie wird innerhalb der nächsten zehn Jahre nur in geringem Maße zunehmen (vgl. Abbildung 9.31). Nur hinreichend sichere Verfahren werden nach allgemeiner Einschätzung überhaupt als Alternative zu traditionellen Verfahren in Betracht gezogen werden. Dabei spielt das Wahlgeheimnis eine essenzielle Bedeutung, auch aus verfassungsrechtlicher Sicht. Aus Sicht der Wähler sind neben der Sicherheit auch die zunehmende Einfachheit bedeutsam.

BETRIEBS- UND PERSONALRATSWAHLEN: Betriebs- und Personalratswahlen wird langfristig die höchste Bedeutung bei den Anwendungen von Online-Wahlen zukommen.

ONLINE-WAHLEN ALS ERGÄNZUNG UND ERSATZ FÜR URNEN- UND BRIEFWAHLEN: Online-Wahlen als Ergänzung zu Urnen- und Briefwahlen werden langfristig an Bedeutung gewinnen.

AKZEPTANZ VON ONLINE-WAHLEN: Die Akzeptanz von Online-Wahlen wird langfristig nur mäßig an Bedeutung gewinnen.

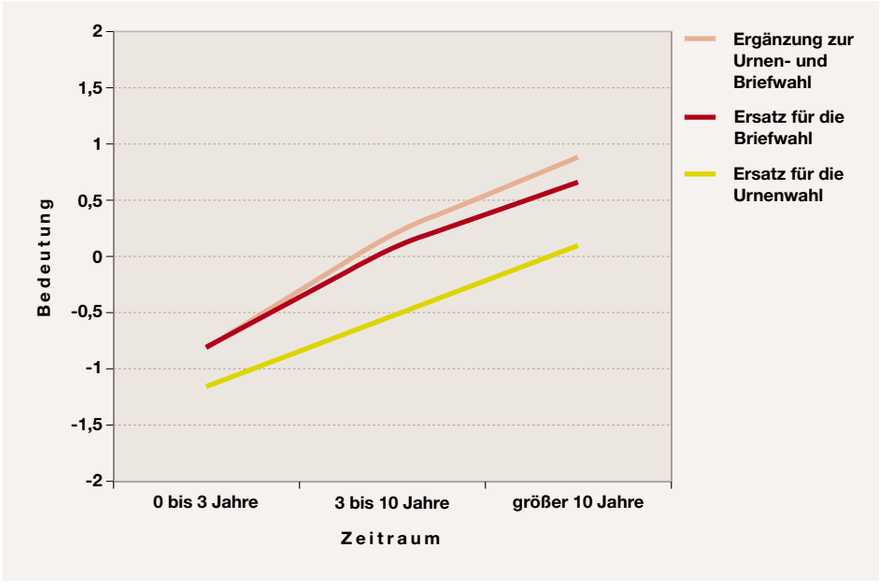



Abbildung 9.30: Bedeutung von Online-Wahlverfahren als Ergänzung oder Ersatz für Urnen- und Briefwahl

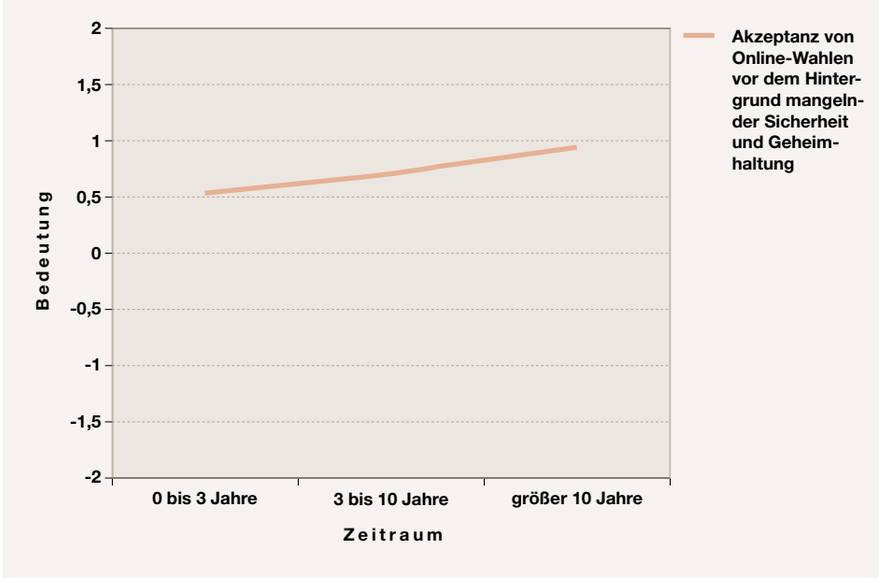



Abbildung 9.31: Bedeutung der Akzeptanz von Online-Wahlen vor dem Hintergrund mangelnder Sicherheit und Geheimhaltung

### Zusammenfassung

Bei der Bewertung des Digital-Rights-Managements tendieren die Befragten überraschenderweise trotz der teilweise erheblichen Skepsis gegenüber der technischen Wirksamkeit der derzeitigen Mechanismen zu einer relativ zeitnahen Etablierung von DRM-Systemen. In diesem Zusammenhang werden die Ergebnisse des TCPA-Konsortiums von vielen mit Spannung erwartet. Online-Wahlen werden nach einhelliger Auffassung stark an Bedeutung hinzugewinnen. Die Haupthindernisse bestehen neben den bisher unzureichenden technischen Rahmenbedingungen, insbesondere bzgl. der Sicherheit, vor allem im politischen Entscheidungsprozess. Mit Blick auf die Bedeutung von Abstimmungen und Wahlen als gesellschaftliches Fundament ist dies durchaus berechtigt. Zusammenfassend ergibt sich folgendes Bild:

- Sichere, robuste Watermarking-Verfahren und speziell asymmetrische Watermarking-Verfahren sind im Jahr 2006 verfügbar.
- Im Jahr 2008 ist die identitätsgebundene Nutzung von Inhalten weit verbreitet.
- Die Verankerung von DRM-Mechanismen im Betriebssystem und in der Hardware wird im Jahr 2013 bzw. 2010 weit verbreitet sein.
- Sichere Online-Wahlverfahren für die Stimmabgabe vom heimatlichen PC aus über das Internet sind im Jahr 2008 verfügbar.
- Bei der elektronisch gestützten Wahl wird mittelfristig die Wahl an einem vernetzten Wahlgerät in einem Wahllokal die größte Bedeutung haben, während die Wahl an einem nicht-vernetzten Wahlgerät eher eine Übergangslösung darstellt. Sowohl die elektronische Wahl über das Internet als auch die elektronische Wahl von einem beliebigen mobilen persönlichen Endgerät werden erheblich an Bedeutung hinzugewinnen, letzteres wird allerdings weiterhin insgesamt die geringste Bedeutung haben.
- Das zukünftig wichtigste Anwendungsfeld elektronischer Wahlen wird bei Betriebs- und Personalratswahlen gesehen, gefolgt von Sozialwahlen. Online-Wahlen im Bereich der „politischen" Wahlen spielen derzeit kaum eine Rolle, werden aber langfristig erheblich an Bedeutung hinzugewinnen. Den Wahlen in Vereinen wird kaum Bedeutung beigemessen.
- Online-Wahlen werden Urnen- und Briefwahlen vorwiegend ergänzen. Sie werden mittel- bis langfristig eher die Briefwahl statt der Urnenwahl ersetzen.
- Die Akzeptanz von Online-Wahlen wird in Zukunft kaum an Bedeutung gewinnen.

## 9.9 Entstehung neuer Geschäftsmodelle und Märkte

Der Begriff „New Economy" steht für und Strategien auf Basis der Informations- und Kommunikationstechnologie. Aber auch bei der „Old Economy", hält das Internet Einzug in die Strategie des Unternehmens. Es ermöglicht die Bildung von Wertschöpfungsnetzwerken, die flexible Vernetzung von Unternehmen, die auf ihre jeweiligen Kernkompetenzen fokussiert sind [PRW 03]. Spezialisierte Unternehmen können ihre Wertschöpfungsstufen als Komponenten oder Dienste im Internet anbieten. Dadurch entsteht ein neuer Markt für IT-Komponenten. Auf ihm lassen sich Lösungen für bestimmte Geschäftsprozesse einkaufen oder bei ASP-Anbietern (Application Service Provisioning) mieten.

Ein weiterer Markt entsteht um den Handel von Informationen. Als Beispiel wird in der Studie der Handel von Informationen über einzelne Internet-Nutzer betrachtet. Die Profildaten eines Nutzers zur direkten Bewerbung oder zur Anpassung und Neuentwicklung von Produkten sind wertvoll. Die Logdaten von Webservern, Suchmaschinen und Internetprovidern enthalten Informationen über die Surfgewohnheit der Nutzer. Geeignete Datamining-Tools können aus diesen Informationen Assoziationen ermitteln, Regeln ableiten und Handlungsempfehlungen geben. Die-

se Informationen stellen einen Wert dar, der gehandelt werden kann (vgl. Abschnitt 8.3.4).

## Ergebnisse

Auch in Zukunft wird die Bedeutung der IuK-Technologien für die Entstehung und Veränderung von Geschäftsmodellen und Märkten weiter zunehmen und langfristig ein hohes Niveau erreichen. Die Experten aus der Wissenschaft sehen den höchsten Bedeutungszuwachs bereits in den nächsten drei bis zehn Jahren, der danach weitgehend stagniert. Die Experten aus den Unternehmen schätzen die Bedeutung etwas niedriger ein (vgl. Abbildung 9.32). Den größten zukünftigen Einfluss der IuK-Technologien sehen die Experten in den Bereichen Telematik, Handel, Service und Dienstleistungen. Die Strategien vieler Unternehmen sind bereits auf elektronische Märkte ausgerichtet.

Das Internet wirkt sich seit einigen Jahren auf die strategische Unternehmensplanung aus. Als erfolgreiche Beispiele für effiziente Geschäftsmodelle durch Nutzung der Internettechnologie nennen die Experten den Versandhandel, die Abwicklung komplexer Procurement-Lösungen, wie auch die Möglichkeiten des Online-Marketing. Vor drei Jahren sahen die Experten eine Durchdringung des Internet in die Strategie eines Unternehmens bereits bis 2004 [SETIK 00]. Heute lassen sich erste Ergebnisse dieser Entwicklung erkennen. Doch sind die Prognosen der Experten aus der Wissenschaft und den Unternehmen zurückhaltender (vgl. Abbildung 9.33, ①). Sie erwarten eine weite Verbreitung der Durchdringung erst innerhalb der nächsten vier bis fünf Jahre.

Komponentenorientierte Softwareentwicklung bietet die Grundlage für flexible Kooperationsmöglichkeiten im Internet (vgl. Abschnitt 9.4 und 9.5). Wertschöpfungsstufen lassen sich unternehmensübergreifend mittels spezifischer Dienste und Komponenten verknüpfen. Die Experten erwarten, dass sich innerhalb der nächsten drei Jahre ein globaler Markt für Komponenten entwickelt hat (vgl. Abbildung 9.33, ②). Auf dem Weg dorthin müssten jedoch noch Standardisierungsprobleme gelöst werden. Die Entwicklung einheitlicher Schnittstellen wird als wesentliche Herausforderung für die Zukunft angesehen (vgl Abschnitt 8.4).

Möglich erscheint beispielsweise auch die komplette Umsetzung der etablierten oder branchenspezifischen Geschäftsabläufe ausschließlich auf Basis von Software-Komponenten. Wenn die Komponententechnologie weiter fortgeschritten ist, um eine einfache, eventuell sogar automatische, Vernetzung der fachlichen Komponenten zu unterstützen, sehen die Experten Einsatzmöglichkeiten für alle betrieblichen Anwendungen (vgl. Abbildung 9.33, ③). Standard-Module wie Internetauftritte oder Abrechnungsverfahren könnten auf diese Weise umgesetzt werden. Als zeitlichen Horizont für eine Verbreitung dieser Technologie als Basis für Geschäftsmodelle nennen die Experten die nächsten sechs Jahre (vgl. Abbildung 9.33, ④).

Application Service Provider bieten Software über das Internet zur Miete an. Der Kauf von Software sowie die lokale Installation auf Clients werden somit überflüssig. Im B2B-Bereich zeigt sich ein Trend hin zu „E-Business on demand“, einem Begriff der derzeit von IBM geprägt wird. Der Kunde soll in Zukunft nur für die Leistung bezahlen, die er tatsächlich zu einem bestimmten Zeitpunkt benötigt [Fina 02]. Die Experten erwarten eine weite Verbreitung von ASP-Lösungen bis zum Jahr 2008. Vor drei Jahren haben die Experten eine weite Verbreitung in etwa sieben bis acht Jahren prognostiziert. Diese Aussage wurde demnach durch die vorliegende Studie bestätigt. Voraussetzung für die Verbreitung von ASP sind leistungsfähige und sichere Netze. Zudem muss ein geeignetes Abrechnungsverfahren angewandt werden. Als potenzielle Anwendungsgebiete sehen die Experten neben Standard- und Individualsoftware auch den Komplex Unterhaltung sowie im geschäftlichen Bereich Anwendungen der gesamten Wertschöpfungskette.

Ein weiteres neues Geschäftsmodell bietet komplette Problemlösungskonzepte anstelle von Einzellösungen an. Komplexe Integrationsaufgaben sollen in Zukunft systematisch wieder verwendet werden können. In der Vorgängerstudie wurde eine weite Verbreitung bis zum Jahr 2005 erwartet, diese Prognose ist durch die vorliegende Studie auf das Jahr 2008 verschoben worden (vgl. Abbildung 9.33, ⑤).

BEDEUTUNG DER IUK-TECHNOLOGIEN: Die Bedeutung der IuK-Technologien auf die Entstehung und Veränderung von Geschäftsmodellen und Märkten wird weiter zunehmen.

STRATEGISCHE UNTERNEHMENSPLANUNG: Das Internet wird in 4-5 Jahren verstärkt Einfluss auf die strategische Unternehmensplanung nehmen.

GLOBALER MARKT FÜR KOMPONENTEN: In 3 Jahren wird es weit verbreitet sein, fachliche Komponenten auf einem globalen Marktplatz zu handeln.

GESCHÄFTSABLÄUFE AUSSCHLIESSLICH AUF BASIS VON SOFTWARE-KOMPONENTEN: Geschäftsmodelle mittels Komponenten zu realisieren wird in 6 Jahren weit verbreitet sein.

APPLICATION SERVICE PROVIDER: Das Mieten von Software bei Application Service Providern wird in 5 Jahren weit verbreitet sein.

KOMPLETTE PROBLEMLÖSUNGSKONZEPTE: In 5 Jahren wird das Anbieten von kompletten Problemlösungskonzepten anstelle von Einzellösungen weit verbreitet sein.

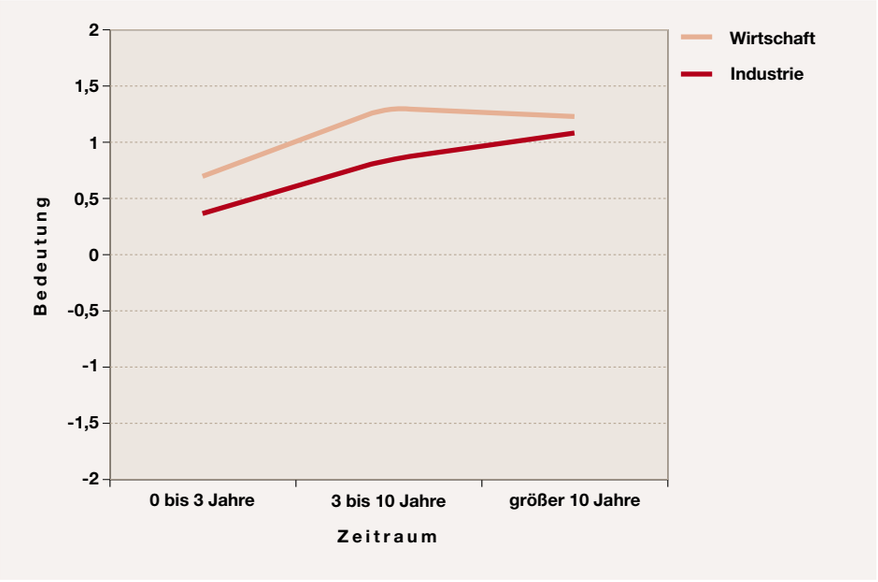



Abbildung 9.32: Bedeutung von IuK-Technologien für die Entstehung und Veränderung von Geschäftsmodellen und Märkten

DIGITALISIERUNG VON PRODUKTEN: Die Digitalisierung von Produkten wird in 5 bis 6 Jahren bestehende Branchenstrukturen verändern.

HANDEL MIT PERSONENBEZOGENEN DATEN: Der Handel mit personenbezogenen Daten ist in 5 Jahren weit verbreitet.

Die Experten nennen wiederum Standardisierungsprobleme als zu überwindendes Hemmnis, bevor solche Konzepte bei der Abwicklung sämtlicher Kundenprozesse zur Anwendung kommen können.

Die Digitalisierung von Produkten ermöglicht neue Branchenstrukturen. Am auffälligsten ist diese Entwicklung derzeit im Mediensektor. Von der Produktion, über die Verbreitung bis hin zur Konsumption werden Medien digitalisiert. In jeder Phase der Wertschöpfungskette ergeben sich dadurch Änderungen, von denen die Experten einige konkretisiert haben. Medieninhalte der Unterhaltungs- und Informationsindustrie, wie Text, Musik und Film, können „on demand" und räumlich verteilt produziert werden. Ihre Verbreitung erfolgt über die modernen Kommunikationswege äußerst schnell; Handelsstufen zwischen Produzenten und Konsumenten können wegfallen. Die Art der Konsumierung wandelt sich vom Realen hin zum Virtuellen: Papier könnte durch elektronische Zeitschriften und Bücher ersetzt werden, Musik und Filme können als Datei direkt aus dem Internet betrachtet werden. Auch der Finanzsektor wird durch die beeinflusst. Banken und Versicherungen bieten ihre Dienstleistungen im Internet an und konkurrieren so mit dem Filialgeschäft. Die Digitalisierung bewirkt deutliche Veränderungen. Die Experten erwarten ihren größten Einfluss innerhalb der nächsten fünf bis sechs Jahre (vgl. Abbildung 9.33, ⑥). Auffällig ist jedoch auch der Anteil an Experten der Unternehmen, die digitale Produkte zwar als Konkurrenz zu den bestehenden sehen, nicht jedoch als Substitut. Diese erwarten beispielsweise, dass Papier auch weiterhin als Medium genutzt werden wird, und dass das Filialgeschäft im Finanzsektor neben dem Internetgeschäft bestehen bleibt (vgl. Abschnitt 9.1).

Der Handel mit personenbezogenen Daten findet heute bereits zum Beispiel im One-to-One-Marketing oder in der Werbefinanzierung von Diensten statt. Die technische Grundlage bildet das Data-Mining (vgl. Abschnitt 8.3.4). Die derzeitigen Datenschutzgesetze schränken jedoch den Handel stark ein. Die Experten erwarten eine weite Verbreitung des Handels persönlicher Daten erst in den nächsten fünf Jahren (vgl. Abbildung 9.33, ⑦). Somit bleiben sie mit Ihrer Prognose bei dem bereits in der Studie 2000 anvisierten Jahr 2008. Zuvor müssen jedoch die rechtlichen Rahmenbedingungen weiter festgeschrieben werden. Anwendungen sind nach den Experten vorwiegend im Bereich Marketing zu finden. Gerade durch Kunden- oder Payback-Karten lässt sich das Kaufverhal-

ABLAGE VON PERSÖNLICHEN, DIGITALEN DATEN IM INTERNET: Die Ablage von persönlichen Daten im Internet bei einer digitalen, sicheren Bank wird frühestens in 10 Jahren weit verbreitet sein.

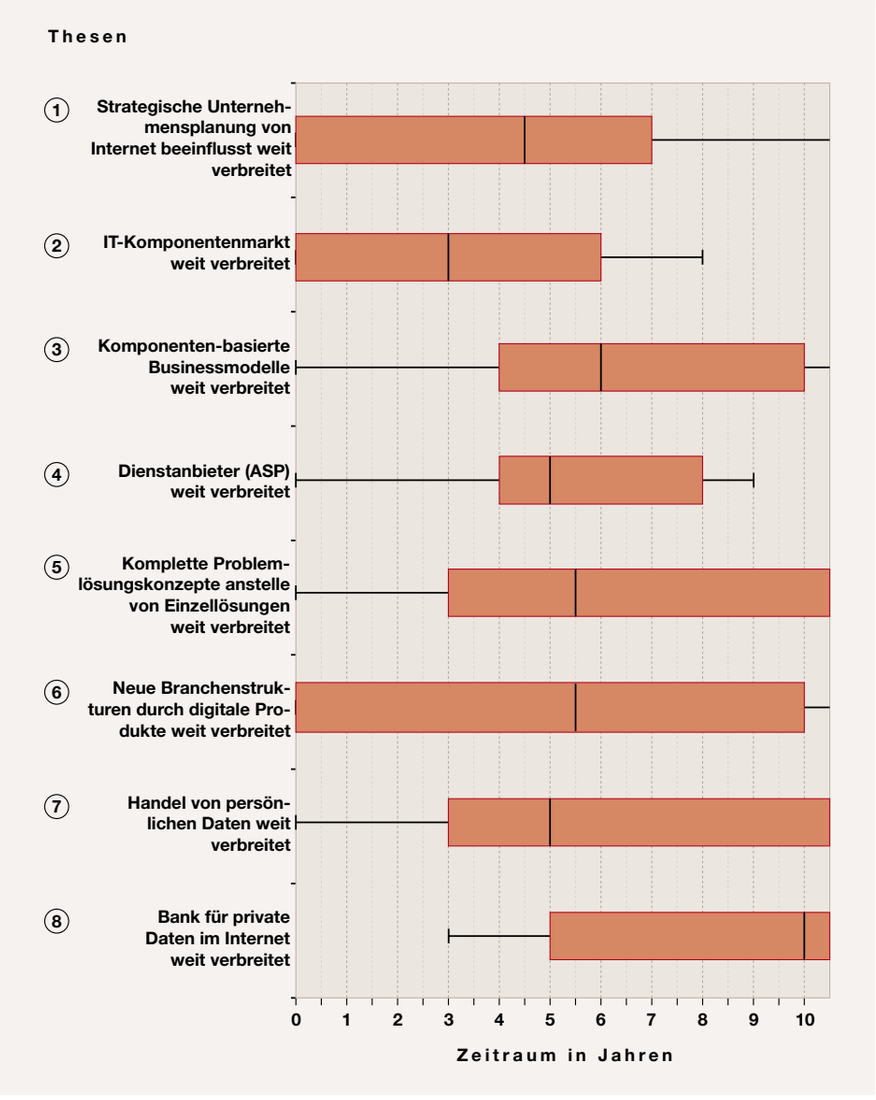



Abbildung 9.33: Ergebnisse der Thesen zu Entstehung neuer Geschäftsmodelle und Märkte

ten untersuchen und das CRM (Customer Relationship Management) verbessern.

Kritisch sehen die Experten die sichere Ablage von persönlichen, digitalen Daten im Internet bei einer Bank. Die Daten werden personalisiert verschlüsselt. Der Austausch von Urkunden zwischen Notariaten, Behörden und Privatpersonen ließe sich elektronisch vornehmen. Als größtes Problem wird dabei das Fehlen ausreichender Sicherheitsstandards angesehen. Zuerst müsse die Authentisierung des Nutzers eines solchen Systems geregelt werden. Es wird nach Ansicht der Experten viel Zeit benötigen, um bei den Nutzern eine Vertrauensbasis für die verwendeten Sicherheitstechnologien zu bilden, die zur Akzeptanz eines solchen Systems führt (vgl Abschnitt 7.3). Daher wird mit der Verbreitung einer Bank für persönliche Daten erst in zehn Jahren gerechnet (vgl. Abbildung 9.33, ⑧).

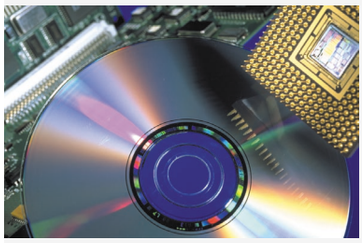
## Zusammenfassung

Die Entwicklung des Internets ermöglicht neue Geschäftsmodelle und eröffnet neue Märkte. Die Befragung der Experten hat folgende Ergebnisse erbracht:

- Die Bedeutung der IuK-Technologien für die Entstehung und Veränderung von Geschäftsmodellen und Märkten

wird in den kommenden Jahren weiter zunehmen.

- Der Einfluss des Internet auf die strategische Unternehmensplanung wird bis zum Jahr 2008 weit verbreitet sein.
- Bis 2006 wird der Handel mit fachlichen Komponenten auf einem globalen Marktplatz weit verbreitet sein.
- Ganze Geschäftsmodelle mittels Komponenten zu realisieren wird bis zum Jahr 2009 weit verbreitet sein.
- Das Mieten von Software bei Application Service Providern wird bis 2008 weit verbreitet sein.
- Im Jahr 2008 wird das Anbieten von kompletten Problemlösungskonzepten anstelle von Einzellösungen weit verbreitet sein.
- Die Digitalisierung von Produkten wird bis zum Jahr 2009 bestehende Branchenstrukturen radikal verändern.
- Der Handel mit personenbezogenen Daten wird bis 2008 weit verbreitet sein.
- Die Ablage von persönlichen Daten im Internet bei einer digitalen, sicheren Bank wird frühestens 2013 weit verbreitet sein.



# 10 Fazit

Diese Studie prognostiziert die wesentlichen Trends der kommenden zehn Jahre für IT-Sicherheit, Informations- und Kommunikationstechnologien und deren Anwendungen. Die weiterhin beispiellos schnelle technische Entwicklung bei gleichzeitig immer weiterer Verbreitung in allen Bereichen des täglichen Lebens erschweren präzise Prognosen. Die Konzeption dieser Studie begegnet beiden Aspekten durch die quantitative und qualitative Befragung ausgewiesener Experten, umfangreicher Literaturanalyse und insbesondere dem Vergleich mit der Studie aus dem Jahr 2000 [SETIK 00]. Gerade die eingeflossenen Erfahrungen aus der Vorgängerstudie in Verbindung mit überarbeiteten Fragebögen und der höheren Expertenanzahl stellen die hier getroffenen Aussagen auf ein solides Fundament.

In allen untersuchten Bereichen zeigt sich eine Verschiebung vieler Prognosen um durchschnittlich etwa drei Jahre gegenüber den Prognosen in der Vorgängerstudie. Insbesondere der damals herrschende Optimismus gegenüber der gedämpften Stimmung heute könnte ein erklärender Faktor dafür sein. Trotzdem lassen sich in allen Bereichen eine Reihe sehr interessanter Trendprognosen erkennen.

So zeigen die Analysen zum Thema IT-Sicherheit, dass einerseits die Integration von Sicherheit in Organisationen sowie die Verbreitung von Public-Key-Infrastrukturen im geschäftlichen und öffentlichen Bereich für die nahe Zukunft gesehen werden. Andererseits ist eine breite Anwendung von Sicherheitsfunktionen im privaten Einsatzumfeld nicht in Sicht, da hier beispielsweise Sicherheitseigenschaften als Entscheidungskriterium beim Produktkauf erst 2007 relevant werden. Trotzdem nutzen Privatanwender heute schon viele Sicherheitstechnologien eher unbewusst, wie bei Homebanking und GSM oder künftig auch bei Bluetooth und UMTS. Wenn also IT-Sicherheitstechnologien breiten Einsatz in möglichst vielen Anwendungen finden sollen, so müssen sie für den Nutzer unproblematisch bedienbar sein und unbemerkt ihren Dienst verrichten (vgl. Kapitel 7).

Im Bereich der Rechnertechnik behält Moore's Gesetz [Inte 02] noch weitere zehn Jahre Gültigkeit. Die heute verwendeten Basistechnologien wie Siliziumhalbleiter weichen auf lange Sicht neuen Technologien, z.B. auf Basis von Quanteneffekten. Erste Ansätze davon sind noch Labormuster und benötigen noch einige Jahre zur Erlangung von Serienreife. Die Beherrschbarkeit der notwendigen Entwicklungs- und Produktionsprozesse wird nun stärker zu beobachten sein. Weitere künftige Untersuchungsfelder stellen eingebette Systeme, Architekturen mit Kontextbezug, und vernetzte Speichersysteme dar (vgl. Kapitel 8.1).

Bei drahtgebundener Rechnerkommunikation erscheint nahezu unbegrenzte Bandbreite prinzipiell möglich, denn weniger technische Probleme als vielmehr mangelnde Nachfrage bremsen derzeit die Entwicklung. Gleichzeitig gewinnen drahtlose Netze weiter an Bedeutung. Hier ist noch unklar, inwiefern Bluetooth, WLAN und UMTS direkt konkurrieren oder sich eher ergänzen. Denn durch die Lizenzfreiheit und die günstige Technik droht mit WLANs möglicherweise eine Art „Anarchie" der drahtlosen Vernetzung von Endgeräten, die den Erfolg von UMTS gefährden könnte. Weiter wird auch zu verfolgen sein, wie gut sich die unterschiedlichen Netztechnologien integrieren lassen und ob die Vernetzung sämtlicher Endgeräte überhaupt möglich und sinnvoll ist (vgl. Kapitel 8.2).

Das zu verwaltende Datenvolumen wird die nächste zehn Jahre mit etwa 100% pro Jahr zunehmen. Damit werden die Anforderungen an die Leistungsfähigkeit und Bedienerfreundlichkeit von Datenbanksystemen weiterhin stark steigen. Objektrelationale Datenbanken werden früher eine bedeutendere Rolle spielen, als noch in der Vorgängerstudie erwartet. Sowohl

zur Erstellung von Metadatenmodellen, als auch bei der Verknüpfung heterogener Systeme dominieren künftig XML-basierte Technologien (vgl. Kapitel 8.3).

Die Studie hat gezeigt, dass Software künftig vielfach komplexer und umfangreicher sein wird. Um eine ingenieurmäßige Entwicklung von Systemen dennoch zu ermöglichen, werden sich insbesondere Konzepte und Technologien zur Modularisierung wie Software-Komponenten oder Dienste, Techniken zur Dokumentation in Form formaler Beschreibungstechniken sowie Werkzeuge zur Erhöhung des Automatisierungsgrades durchsetzen. Ziel wird künftig insbesondere die Entwicklungs stark verteilter Anwendungen sein, deren Integration methodisch unterstützt und vereinfacht wird (vgl. Kapitel 8.4).

Trotz all dieser Fortschritte in den Informations- und Kommunikationstechnologien kommt es nur in sehr wenigen Bereichen zu einer nahezu vollständigen Ablösung herkömmlicher Anwendungsszenarien. Allerdings wird auch deutlich, dass in fast allen Bereichen des privaten und geschäftlichen Lebens die Unterstützung und Ergänzung des Menschen durch technische Systeme in noch größerem Umfang zunehmen wird, als heute von der breiten Öffentlichkeit erwartet (vgl. Kapitel 9).

Für alle Bereiche, die innerhalb der Studie untersucht wurden, stellt Abbildung 10.1 überblicksartig einige ausgewählte Thesen hinsichtlich ihres prognostizierten Eintrittszeitpunktes dar.

Neben den spezifischen Trends in IT-Sicherheit, Technologien und Anwendungen lassen sich übergreifende Trends feststellen, die dort in unterschiedlicher Intensität auftreten (vgl. Kapitel 6). Die Einführungen in die einzelnen Teilbereiche beschreiben die Zusammenhänge zwischen den spezifischen und den übergreifenden Trends und stellen die Häufigkeit des Auftretens in einer Tabelle grafisch dar. Die Ergebnisse aus diesen Tabellen sind wiederum in Tabelle 10.1 als Übersicht für die gesamte Studie zusammengefasst und den Ergebnissen aus der Vorgängerstudie gegenübergestellt. Während die übergreifenden Trends „Integration und Standardisierung" und „Konvergenz" gegenüber 2000 an Bedeutung verloren haben, spielen „Vernetzung und Flexibilisierung", „Verteilung und Dezentralisierung" und „Virtualisierung" künftig eine größere Rolle. Besonders interessant ist die Tatsache, dass insbesondere bei den hardwarenahen Bereichen „Rechnertechnik" und „Netze und Kommunikation" deutlich mehr Zu- als Abnahmen zu erkennen sind, während gleichzeitig für die Anwendungen die Bedeutung der meisten übergreifenden Trends gleich bleibt oder gar abnimmt. Vor dem Hintergrund des anfangs beschriebenen Spiraleffekts (vgl. Kapitel 5) ließe sich dies darauf zurück führen, dass während der Erstellung der Studie 2000 durch das Aufkommen neuer Technologien viele neue Anwendungsideen entstanden sind, die allerdings an die Grenzen der damaligen technisch Möglichkeiten gestoßen sind. Während daher viele visionäre Anwendungsideen heute realistischer eingeschätzt werden, zeigt sich eine große Dynamik besonders dort, wo technische Weiterentwicklungen diese Ideen schließlich doch als konkrete und erfolgreiche Anwendungen nutzbar machen könnten.

Die hier angewandte Methodik hat sich in dieser und der vorangegangen Studie bewährt und interessante Ergebnisse erzielt, so dass nun angestrebt wird, die Expertenbefragungen weiterhin in regelmäßigen Abständen zu wiederholen. Um eine durchgängige Vergleichbarkeit wie zwischen den beiden vorliegenden Studien zu gewährleisten, werden viele Fragen unverändert gestellt, aber auch einige neue Trends und Technologien in die Untersuchung aufgenommen werden müssen. Außerdem bietet es sich gerade für langfristige Vorhersagen an, mit der dann verfügbaren größeren Zahl an Prognosewerten noch weitere statistische Auswertungen, wie beispielsweise Zeitreihenanalysen, vorzunehmen.

| Technologie | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Sicherheitsorganisation integraler Bestandteil der Unternehmensorganisation | | | ● | | | | | | | | |
| Kupfer löst Aluminium bei der Prozessorherstellung ab | | | | ● | | | | | | | |
| Integration unterschiedlicher Datenmodelle in Metadatenmodelle ist möglich | | | | ● | | | | | | | |
| Datenbanken mit integrierter Webserver-Funktionalität sind weit verbreitet | | | | ● | | | | | | | |
| Mobile persönliche Assistenten sind weit verbreitet | | | | ● | | | | | | | |
| PKI-Systeme für B2B und B2G-Anwendungen | | | | ● | | | | | | | |
| Optische Gatter sind verfügbar | | | | | ● | | | | | | |
| Sprachunabhängige Datenbankabfragen sind möglich | | | | | ● | | | | | | |
| Indexstrukturen ermöglichen den effizienten Zugriff auf Multimedia-Informationen | | | | | ● | | | | | | |
| xDSL verdrängt symmetrische Verfahren | | | | | ● | | | | | | |
| Einheitliche Dienstnutzung ist unabhängig vom Transportnetz | | | | | ● | | | | | | |
| Endgeräte mit Zugang zu unterschiedlichen Transportnetzen sind verbreitet | | | | | ● | | | | | | |
| Sprachkommunikation auf Basis von IP ist verbreitet | | | | | ● | | | | | | |
| Durchgängigkeit der Entwicklungsdokumentation ist verbreitet | | | | | ● | | | | | | |
| Open Source-Modell ist weit verbreitet | | | | | ● | | | | | | |
| Symmetrischer Verschlüsselungsstandard AES löst DES/Triple-DES-Standard für kommerzielle Zwecke ab | | | | | ● | | | | | | |
| Biologische Gatter sind verfügbar | | | | | | ● | | | | | |
| Quantengatter sind verfügbar | | | | | | ● | | | | | |
| Optische Speicher von magnetischen Speichern abgelöst | | | | | | ● | | | | | |
| Objektrelationale DBS lösen rein objektorientierte DBS ab | | | | | | ● | | | | | |
| IPv6 löst IPv4 ab | | | | | | ● | | | | | |
| Kombinierte Kommunikations-Endgeräte sind verbreitet | | | | | | ● | | | | | |
| QoS-spezifische Zusammenstellung von Diensten ist möglich | | | | | | ● | | | | | |
| Sichere und operable Systeme auf Basis mobiler Agenten sind verfügbar | | | | | | ● | | | | | |
| Nachvollziehbarkeit der Entwicklungsdokumentation ist verbreitet | | | | | | ● | | | | | |
| Konfiguration und Komposition von Komponenten ist verbreitet | | | | | | ● | | | | | |
| Unternehmensstrategien werden durch Internet wesentlich beeinflußt | | | | | | ● | | | | | |
| Zertifikate zur Bestätigung eines bestehenden Sicherheitsniveaus | | | | | | ● | | | | | |
| Identitätsgebundene Nutzung von Inhalten weit verbreitet | | | | | | ● | | | | | |
| Ontologien zur Realisierung intelligenter Suchagenten sind weit verbreitet | | | | | | | ● | | | | |
| Glasfaseranschluss zum Endgerät ist verbreitet | | | | | | | ● | | | | |
| Paketvermittlung löst Leitungsvermittlung ab | | | | | | | ● | | | | |
| Business Process Outsourcing ist weit verbreitet | | | | | | | ● | | | | |
| Sprache wird zum dominierenden Verfahren zu Dateneingabe und Maschinensteuerung | | | | | | | | ● | | | |
| End-to-End QoS verfügbar | | | | | | | | ● | | | |
| Flexible Entwicklungswerkzeuge sind verfügbar | | | | | | | | ● | | | |
| Entwicklungsunterstützung durch Vorschläge ist weit verbreitet | | | | | | | | ● | | | |
| Internet-fähige Fernsehgeräte sind weit verbreitet | | | | | | | | ● | | | |
| Elektronische Bürgersprechstunden sind weit verbreitet | | | | | | | | ● | | | |
| Biometrische Verfahren im Alltag sind akzeptiert | | | | | | | | ● | | | |
| Semantische Datenbankabfragen sind weit verbreitet | | | | | | | | | ● | | |
| Zugang elektrischer Geräte im Haushalt zu Kommunikationsnetzen | | | | | | | | | ● | | |
| Quantenmechanische Schlüsseleinigungsverfahren | | | | | | | | | ● | | |
| Dienstorientiertes Management löst komponentenorientiertes Management ab | | | | | | | | | ● | | |
| Vorgehensmodelle sind in KMUs weit verbreitet | | | | | | | | | ● | | |
| Bilanzen auf Knopfdruck sind weit verbreitet | | | | | | | | | ● | | |
| Prozessoren und Taktfrequenzen > 50 GHz sind weit verbreitet | | | | | | | | | | ● | |
| Grid-Computing besitzt höhere Bedeutung als Vektorrechner | | | | | | | | | | ● | |
| Universelle Netzkomponenten mit getrennten Ablaufumgebungen sind verbreitet | | | | | | | | | | ● | |
| Post, Telefon, Fax sind durch EDI-XML abgelöst | | | | | | | | | | ● | |
| Optische Prozessoren sind verfügbar | | | | | | | | | | | ● |
| Photonische Netze sind verbreitet | | | | | | | | | | | ● |

Abbildung 10.1: Prognosezeitpunkte ausgewählter Thesen

| Übergreifende Trends | Ausprägung im Bereich | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Rechnertechnik | | Netze und Kommunikation | | Datenbanken und Wissensmanagement | | Softwaretechnik | | Anwendungen | | 2003 | 2000 |
| | 2003 | 2000 | 2003 | 2000 | 2003 | 2000 | 2003 | 2000 | 2003 | 2000 | | |
| Automatisierung und Vereinfachung |  |  |  |  |  |  |  |  |  |  |  |  |
| Dienst und Komponentenorientierung |  |  |  |  |  |  |  |  |  |  |  |  |
| Globalisierung und Wettbewerb |  |  |  |  |  |  |  |  |  |  |  |  |
| Integration und Standardisierung |  |  |  |  |  |  |  |  |  |  |  |  |
| Kapazitäts- und Leistungssteigerung |  |  |  |  |  |  |  |  |  |  |  |  |
| Konvergenz |  |  |  |  |  |  |  |  |  |  |  |  |
| Miniaturisierung |  |  |  |  |  |  |  |  |  |  |  |  |
| Mobilität |  |  |  |  |  |  |  |  |  |  |  |  |
| Vernetzung und Flexibilisierung |  |  |  |  |  |  |  |  |  |  |  |  |
| Verteilung und Dezentralisierung |  |  |  |  |  |  |  |  |  |  |  |  |
| Virtualisierung |  |  |  |  |  |  |  |  |  |  |  |  |

Tabelle 10.1: Bedeutung der übergreifenden Trends in den einzelnen Bereichen

## Symbolverzeichnis

| | |
|---|---|
| **ActiveX** | ActiveX Controls; Technologie zur Realisierung interoperabler COM Komponenten und Diensten |
| **AES** | Advanced Encryption Standard |
| **AFC** | Antiferromagnetic Coupling; ein Verfahren zur Kapazitätssteigerung bei Festplatten, bei dem eine drei Atomlagen dicke Rutheniumschicht zwischen zwei magnetischen Schichten einer Festplattenoberfläche eine gekoppelte Magnetisierung in entgegengesetzte Richtungen erzeugt |
| **ANSI** | American National Standard Institute |
| **API** | Application Programmers Interface; standardisierte Schnittstelle zum Zugriff auf Funktionalitäten eines Softwaremoduls |
| **ASIC** | Application-Specific Integrated Circuit; für spezielle Anwendungen gefertigter Chip |
| **ASP** | Active Server Pages; System zur Generierung dynamischer Web-Inhalte |
| **ASP** | Application Service Provisioning |
| **ATM** | Asynchronous Transfer Mode; Technologie zur Datenübertragung |
| **B2B** | Business-to-Business |
| **B2C** | Business-to-Consumer |
| **BPO** | Business Process Outsourcing |
| **CAD** | Computer Aided Design; rechnergestützte Planung und Konstruktion |
| **CASE** | Computer Aided Software Engineering |
| **CC** | Common Criteria; gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit in der Informationstechnik |
| **CD** | Compact Disc; digitales, optisches Speichermedium |
| **CDMA** | Code Devision Multiple Access |
| **CGI** | Common Gateway Interface |
| **CMM** | Capability Maturity Model |
| **CMOS** | Complementary Metal Oxide Semiconductor; ein weit verbreiteter Halbleitertyp |
| **COM** | Component Object Model |
| **CORBA** | Common Object Request Broker Architecture |
| **COTS** | Commercial Off-The-Shelf |
| **CRM** | Customer Relationship Management |
| **CRT** | Cathode Ray Tube; Kathodenstrahl-Röhre |
| **CVS** | Concurrent Version System |

| | |
|---|---|
| **DAB** | Digital Audio Broadcasting |
| **DCOM** | Distributed Component Object Model |
| **DDoS** | Distributed Denial of Service |
| **DECT** | Digital Enhanced Cordless Technologies |
| **DES** | Data Encryption Standard |
| **DiffServ** | Differentiated Services; QoS-Architektur zur klassenbasierten Bereitstellung von QoS im Internet |
| **DMD** | Digital Mirror Device |
| **DoS** | Denial of Service |
| **DRM** | Digital Rights Management |
| **DSA** | Digital Signature Algorithm; Algorithmus für Digitale Signaturen, der auf dem Verfahren von ElGamal basiert. Dient der Erzeugung und Verifikation von Digitalen Signaturen sowie der Verteilung von Schlüsseln |
| **DVB** | Digital Video Broadcasting |
| **DVD** | Digital Versatile Disc; Nachfolgemedium der CD |
| **E/A** | Ein-/Ausgabe |
| **EAI** | Enterprise Application Integration |
| **ebXML** | Electronic Business XML |
| **ECDSA** | Elliptic Curve Digital Signature Algorithm |
| **EDI** | Electronic Data Interchange |
| **EDIFACT** | Electronic Data Interchange for Administration, Commerce and Transport |
| **EJB** | Enterprise Java Beans |
| **EMS** | Enhanced Message Service |
| **EOTD** | Enhanced Observed Time Difference; Verfahren zur Lokalisierung von Mobilfunkteilnehmern |
| **ERP-Systeme** | Enterprise Resource Planing |
| **ERP** | Enterprise Resource Planing |
| **EUV** | Extreme Ultra Violet; ein auf sehr kurzen Wellenlängen basierendes Belichtungsverfahren bei der Fertigung von Chips |
| **FTTD** | Fiber To The Desktop; Glasfaserverkabelung bis zu den Endgeräten der Benutzer |
| **G2B** | Government-to-Business |
| **G2C** | Government-to-Citizen |
| **G2G** | Government-to-Government |
| **GPRS** | General Packet Radio Service; Erweiterung von GSM zur Datenkommunikation |
| **GPS** | Global Positioning System |
| **GSM** | Global System for Mobile Communications; europäischer Mobilfunkstandard |
| **GUI** | Grafical User Interface |
| **Hotspots** | Zugangspunkt zu mobilen Netzen an Punkten mit hoher Endgerätedichte |

| | |
|---|---|
| **HSCSD** | High Speed Circuit Switched Data; Datentransporttechnologie für GSM-Netze |
| **HTML** | Hyptertext Markup Language |
| **HTTP** | Hypertext Transfer Protocol |
| **IDS** | Intrusion Detection System |
| **IEEE** | Institute of Electrical and Electronics Engineers |
| **IETF** | Internet Engineering Task Force |
| **IntServ** | Integrated Services; QoS-Architektur zur flowbasierten Bereitstellung von QoS im Internet |
| **IP over $\lambda$** | IP over lambda; direkte Übertragung von IP auf einer Wellenlänge eines Lichtwellenleiters |
| **IP** | Internet Protocol |
| **IPSec** | Internet Protocol Security; Sicherheitserweiterungen für IP |
| **IRS** | Intrusion Response System |
| **ISDN** | Integrated Services Digital Network; digitales Telefonnetz |
| **ISO** | International Organization for Standardization |
| **J2EE** | Java 2 Platform Enterprise Edition |
| **Java RMI** | Java Remote Method Invocation |
| **JVM** | Java Virtual Maschine |
| **LAN** | Local Area Network |
| **LBS** | Location Based Service; Ortsabhängiger Dienst |
| **LCD** | Liquid Crystal Display; Flüssigkristall-Bildschirm |
| **LDAP** | Lightweight Directory Access Protocol; Zugriffsprotokoll für Verzeichnisdienste |
| **LDT** | Laser Display Technology; Laserprojektor |
| **MD5** | Message Digest No. 5; Hashfunktion mit der Hashwertlänge 128 Bit |
| **MExE** | Mobile Station Application Execution Environment |
| **MHP** | Multimedia Home Platform; standardisierte Ausführungsplatform für Set-Top-Boxen |
| **MMS** | Multimedia Message Service |
| **MPLS** | Multi Protocol Label Switching |
| **MPOA** | Multi Protokoll over ATM |
| **MSF** | Multiservice Switching Forum; Zusammenschluss von Herstellern von Koppelkomponenten |
| **OCL** | Object Constraint Language |
| **OLAP** | Online Analytical Processing |
| **OLTP** | Online Transaction Processing |
| **OSI-Schichtenmodell** | Open Systems Interconnection; Schichtenmodell zur Beschreibung von Kommunikationssystemen |
| **PDA** | Personal Digital Assistant |

| | |
|---|---|
| **PGP** | Pretty Good Privacy |
| **PKCS** | Public Key Cryptography Standards |
| **PKI** | Public Key Infrastructure; Sicherungsinfrastruktur zur vertrauenswürdigen Erstellung, Verteilung und Verwaltung von öffentlichen und privaten Schlüsseln und zugehöriger Objekte wie Zertifikate und Sperrlisten |
| **PnP** | Plug-and-Play |
| **POP3** | Protokoll zum Zugriff auf E-Mail-Server |
| **PPS** | Produktions-Planungs-System |
| **QoS** | Quality of Service |
| **RFID** | Radio Frequency Identification |
| **RIPE-MD** | RIPE Message Digest; Kryptographische Hashfunktion, die im Rahmen des RIPE-Projektes der Europäischen Union aus MD4 entwickelt wurde |
| **RPC** | Remote Procedure Call |
| **RSVP** | Resource Reservation Setup Protocol; QoS-Reservierungsprotokoll im Internet |
| **RUP** | Rational Unified Process |
| **S-HTTP** | Secure HTTP |
| **S/MIME** | Secure Multipurpose Internet Mail Extension |
| **SCM** | Supply Chain Management |
| **SDH** | Synchronous Digita Hirarchy; WAN-Technologie |
| **SDL** | Specification and Description Language |
| **SHA** | Secure Hash Algorithm; Hashfunktion mit unterschiedlichen Hashwertlängen (SHA-1, SHA-256, SHA-384, SHA-512) |
| **SIA** | Semiconductor Industry Association; Vereinigung der US-amerikanischen Halbleiterindustrie |
| **Siebel UAN** | Siebel Universal Application Network |
| **SMS** | Short Message Service |
| **SMTP** | Simple Mail Transfer Protocol; Protokoll zum Austausch von E-Mails zwischen Rechnern |
| **SOAP** | Simple Object Access Protocol |
| **SOI** | Silicon-on-Insulator; ein Halbleiter-Herstellungsverfahren bei dem reine Silizium-Kristalle und -Oxide verwendet werden |
| **SSH** | Secure Shell |
| **SSL** | Secure Socket Layer |
| **TCP/IP** | Transmission Control Protocol/Internet Protocol; Kurzbezeichnung für die Internetprotokollwelt |
| **TCP** | Transmission Control Protocol |
| **TCPA** | Trusted Computing Platform Alliance |
| **TLS** | Transport Layer Security |
| **UDDI** | Universal Description, Discovery and Integration |

| | |
|---|---|
| **UML/RT** | Unified Modelling Language for Real Time |
| **UML** | Unified Modelling Language |
| **UMTS** | Universal Mobile Telecommunication System |
| **Unified Process** | Unified Process |
| **V-Modell** | IABG - Vorgehensmodell ‘97 |
| **VB-Script** | Visual Basic Script |
| **VoIP** | Voice over IP; Sprachübertragung über das Internet |
| **VPN** | Virtual Private Network |
| **WAN** | Wide Area Network |
| **WAP** | Wireless Application Protocol |
| **WDM** | Wavelength Division Multiplexing; Aufteilen einer Glasfaser in optische Kanäle |
| **WLAN** | Wireless LAN |
| **WSDL** | Web Service Definition Language |
| **WWW** | World Wide Web; verteilter Hypertext-Dienst im Internet |
| **XMI** | XML Metadata Interchange |
| **XML** | Extensible Markup Language |

# Index

## Literaturverzeichnis


[3GPP 03] 3GPP: *UMTS Specification*, März 2003, `http://www.3gpp.org`.

[AAI+ 01] ABARRA, E. N., B. R. ACHARYA, A. INOMATA, A. AJAN und I. OKAMOTO: *Synthetic Ferrimagnetic Media*. Fujitsu Science Technical Journal, 37(2):145–154, Dezember 2001, `http://magazine.fujitsu.com/us/vol37-2/paper05.pdf`.

[Abad 97] ABADI, MARTÍN: *On SDSI's Linked Local Name Spaces*. In: *10th IEEE Computer Security Foundations Workshop*. IEEE Computer Society Press, 1997.

[ABD+ 00] ADAMS, CARLISLE, MIKE BURMESTER, YVO DESMEDT, MIKE REITER und PHILIP ZIMMERMANN: *Which PKI (Public Key Infrastructure) is the right one?* In: JAJODIA, SUSHIL (Herausgeber): *Proceedings of the 7th ACM Conference on Computer and Communications Security*, Seiten 98–101, Athens, Greece, November 2000. ACM Press. Panel session.

[ABWP+ 00] ASOKAN, N., BIRGIT BAUM-WAIDNER, TORBEN P. PEDERSEN, BIRGIT PFITZMANN, MATTHIAS SCHUNTER, MICHAEL STEINER und MICHAEL WAIDNER: *Architecture*. In: LACOSTE, GÉRARD, BIRGIT PFITZMANN, MICHAEL STEINER und MICHAEL WAIDNER (Herausgeber): *SEMPER – Secure Electronic Marketplace for Europe*, Nummer 1854 in *Lecture Notes in Computer Science*, Seiten 45–64. Springer-Verlag, Berlin, Germany, August 2000.

[ACMEC 00] *Second ACM Conference on Electronic Commerce*, Minneapolis, MN USA, Oktober 2000. ACM Press.

[ADD+ 01] ALESSANDRI, D., M. DACIER, O. DEAK, K. JULISCH, B. RANDEL, J. RIORDAN, A. TSCHARNER, A. WESPI und C. WÜEST: *Towards a Taxonomy of Intrusion Detection Systems and Attacks*. Deliverable D3, EU Project IST-1999-11583 Malicious- and Accidental-Fault Tolerance for Internet Applications (MAFTIA), September 2001. Version 1.01.

[AdSa 01] ADELSBACH, ANDRÉ und AHMAD-REZA SADEGHI: *Zero-Knowledge Watermark Detection and Proof of Ownership*. In: MOSKOWITZ, IRA S. (Herausgeber): *Information Hiding—4th International Workshop, IHW 2001*, Band 2137 der Reihe *Lecture Notes in Computer Science*, Seiten 273–288, Pittsburgh, PA, USA, 2001. Springer-Verlag, Berlin, Germany.

[AEJ+ 02] ALLAN, A., D. EDENFELD, W. H. JR. JOYNER, A. B. KAHNG, M. RODGERS und Y. ZORIAN: *2001 Technology Roadmap for Semiconductors*. IEEE Transactions on Computers, 35(1):42–52, Januar 2002.

[Alep 96] ALEPH ONE: *Smashing The Stack For Fun And Profit*. Phrack Magazine, 7(49):File 14, 1996.

[ALM 01] AUTOR, D., F. LEVY und R. MURNANE: *The Skill Content of Recent Technological Change: an Empirical Exploration*. NBER Working Paper, 8337, 2001.

[Amor 01] AMOR, D.: *Die E-Business (R)Evolution*. Galileo, 3 Auflage, 2001.

[AnKu 96] ANDERSON, ROSS und MARKUS KUHN: *Tamper Resistance – a Cautionary Note*. In: *Proceedings of the 2nd USENIX Workshop on Electronic Commerce*, Seiten 1–11, Oakland, California, November 1996. USENIX.

[ANTS 98a] *Third International Algorithmic Number Theory Symposium (ANTS-III)*, Band 1423 der Reihe *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany, 1998.

[ANTS 98b] BONEH, DAN: *The Decision Diffie-Hellman problem*. In: [ANTS 98a], Seiten 48–63.

[ANTS 98c] HOFFSTEIN, J., J. PIPHER und J. SILVERMAN: *NTRU: A ring based public-key cryptosystem*. In: [ANTS 98a], Seiten 268–288.

[APS 02] ALBERS, S., G. PANTEN und B. SCHÄFERS: *Die eCommerce-Gewinner - Wie Unternehmen im Web profitabel wurden*. F.A.Z.-Institut, 2002.

[Atki 96] ATKINSON, RANDALL: *Security Architecture for the Internet Protocol*. Internet draft (draft-ietf-ipsec-archi-sec-01.txt), November 1996.

[Axel 00a] AXELSSON, STEFAN: *The Base-Rate Fallacy and the Difficulty of Intrusion Detection*. ACM Transactions on Information and System Security, 3(3):186–205, 2000.

[Axel 00b] AXELSSON, STEFAN: *Intrusion Detection Systems: A Taxonomy and Survey*. Technical Report, Dept. of Computer Engineering, Chalmers University of Technology, Sweden, 2000.

[Babe 91] BABER, R. L.: *Error-Free-Software*. Wiley Series in Software Engineering Practice, 1991.

[Bage 98] BAGER, J.: *Der gehörsame PC, Computergestützte Spracherkennung vor dem Durchbruch*. c't, 5:104–108, 1998.

[Bank 02] BANKE, K.: *Erfahrungswerte - Open-Source-RDBMS von SAP*, November 2002, `http://premium-link.net/$8740$1908208087/$/ix/02/08/078/@00050@/art.htm`.

[Baum 99] BAUMEISTER, MARKUS: *Ein Transaktionskonzept für die deduktive Objektbank ConceptBase*. Diplomarbeit, Rheinisch-Westfälische Technische Hochschule, Aachen, November 1999, `http://www-i5.informatik.rwth-aachen.de/mbp/dipl/dipl.html`.

[BDD+ 92] BROY, M., F. DEDERICHS, C. DENDORFER, M. FUCHS, T.F. GRITZNER und R. WEBER: *The Design of Distributed Systems – an Introduction to FOCUS*. Technischer Bericht -I-9203, Technische Universität München, Institut für Informatik, 1992.

[BDJ+ 99] BERGNER, K., B. DEIFEL, C. JACOBI, W. KELLERER, A. RAUSCH, A. SABBAH, V. SCHTÄTZ, M. SIHLING, A. VILBIG und S. VOGEL: *The Future of Information Technology – an interdisziplinary, scenario-based approach*. Technischer Bericht -I-0004, Technische Universität München, 1999.

[BDRS 97] BROY, M., E. DENERT, K. RENZEL und M. SCHMIDT: *Software Architectures and Design Patterns in Business Applications*. Technischer Bericht -I-9746, Institut für Informatik, November 1997.

[Beck 00] BECK, K.: *Extreme Programming. Das Manifest*. Addison Wesley, 2000.

[BeHu 96] BEHFOROOZ, A. und F. J. HUDSON: *Software Engineering Fundamentals*. Oxford University Press, 1996.

[Bell 99] BELLOVIN, STEVEN M.: *Distributed Firewalls*. ;login: magazine, Seiten 37–39, November 1999. Special Issue on Security.

[Berg 97] BERGNER, K.: *Spezifikation großer Objektgeflechte mit Komponentendiagrammen*. Doktorarbeit, Technische Universität München, 1997.

[BeRo 93] BELLARE, M. und P. ROGAWAY: *Random Oracles are Practical: A Paradigm for Designing Efficient Protocols*. In: ASHBY, VICTORIA (Herausgeber): *Proceedings of the 1st ACM Conference on Computer and Communications Security*, Seiten 62–73, Fairfax, Virginia, November 1993. ACM Press.

[BeRo 94] BELLARE, MIHIR und PHILLIP ROGAWAY: *Optimal Asymmetric Encryption — How to encrypt with RSA*. In: SANTIS, A. DE (Herausgeber): *Advances in Cryptology – EUROCRYPT '94*, Band 950 der Reihe *Lecture Notes in Computer Science*, Seiten 92–111. International Association for Cryptologic Research, Springer-Verlag, Berlin, Germany, 1994.

[BeRo 96] BELLARE, M. und P. ROGAWAY: *The exact security of digital signatures — how to sign with RSA and Rabin*. Lecture Notes in Computer Science, 1070:399–??, 1996.

[BGH+ 98] BREU, R., R. GROSU, F. HUBER, B. RUMPE und W. SCHWERIN: *Systems, Views and Models of UML*. In: SCHADER, MARTIN und AXEL KORTHAUS (Herausgeber): *The Unified Modeling Language, Technical Aspects and Applica tions*, Seiten 93–109. Physica Verlag, Heidelberg, 1998, http://www4.informatik.tu-muenchen.de/papers/BGHRS98.html.

[BGR+ 01] BARAK, BOAZ, ODED GOLDREICH, RUSSELL IMPAGLIAZZO, STEVEN RUDICH, AMIT SAHAI, SALIL VADHAN und KE YANG: *On the (Im)possibility of Obfuscating Programs*. In: KILIAN, JOE (Herausgeber): *Advances in Cryptology – CRYPTO '2001*, Band 2139 der Reihe *Lecture Notes in Computer Science*, Seiten 1–18. International Association for Cryptologic Research, Springer-Verlag, Berlin, Germany, 2001.

[BGW 01] BORISOV, NIKITA, IAN GOLDBERG und DAVID WAGNER: *Intercepting Mobile Communications: The Insecurity of 802.11*, Juli 2001, http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf,http://www.isaac.cs.berkeley.edu/isaac/wep-slides.pdf.

[BHS 99] BROY, M., F. HUBER und B. SCHÄTZ: *AutoFocus – Ein Werkzeugprototyp zur Entwicklung eingebetteter Systeme*. Informatik Forschung und Entwicklung, 14(3):121–134, 1999, http://www4.informatik.tu-muenchen.de/papers/BroyHuberSchaetz:IFE-AF:1999.html.

[BiSh 93] BIHAM, ELI und ADI SHAMIR: *Differential Cryptanalysis of the Data Encryption Standard*. Springer-Verlag, New York, 1993.

[BLHL 01] BERNERS-LEE, T., J. HENDLER und O. LASSILA: *The Semantic Web*, Mai 2001, http://www.sciam.com/2001/0501issue/0501berners-lee.html.

[BMR 00] BIETHAHN, JÖRG, HARRY MUCKSCH und WALTER RUF: *Ganzheitliches Informationsmanagement*. Oldenburg, 2000.

[BMW 03] BMW AG: *The BMW 7 Series. A new way to drive*, März 2003, http://www.bmw.com/e65/id14/3_a91_idrive.jsp.

[Bone 99] BONEH, DAN: *Twenty years of attacks on the RSA cryptosystem*. Notices of the American Mathematical Society (AMS), 46(2):203–213, 1999.

[Bonn 03] BONNERT, E.: *Moores Gesetz: In zehn Jahren ist Schluss*. Online, 2003, http://www.heise.de/newsticker/data/jk-11.02.03-000/.

[Bons 03] BONSOR, KEVIN: *How DNA Computers Will Work*, 2003, http://www.howstuffworks.com/dna-computer.htm.

[Borl 03] BORLAND: *To Our Valued Borland and TogetherSoft Customer*, 2003, http://www.borland.com/features/togethersoft.html.

[BrSl 99] BROY, M. und O. SLOTOSCH: *Enriching the Software Engineering Process by Formal Methods*. In: *Lecture Notes in Computer Science 1641*. Springer Verlag, 1999.

[BSI 01] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *IT-Grundschutzhandbuch, Standardisierungsmaßnahmen für den mittleren Schutzbedarf*. Bundesanzeiger, Verlagsgesellschaft, 2001.

[BSI 92] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *Handbuch für die sichere Anwendung der Informationstechnik*. Bundesdruckerei, 1992.

[BSI 98] HELDEN, J. VON und S. KARSCH: *Intrusion-Response Studie*. Technischer Bericht, debis IT-Security, Oktober 1998, http://www.bsi.de/literat/studien/ids/ids-stud.htm.

[BSW 01] BIRYUKOV, ALEX, ADI SHAMIR und DAVID WAGNER: *Real Time Cryptanalysis of A5/1 on a PC*. Lecture Notes in Computer Science, 1978, 2001.

[Bund 02] BUNDESMINISTERIUM FÜR WIRTSCHAFT UND ARBEIT: *Monitoring Informationswirtschaft, 5. Faktenbericht*, November 2002, http://193.202.26.196/bmwi/main2002_11.asp.

[Bund 03a] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *Kryptoprozessor PLUTO*, 2003, http://www.bsi.de/literat/faltbl/pluto.htm.

[Bund 03b] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *Sichere Inter-Netzwerk Architektur (SINA)*, 2003, http://www.bsi.de/fachthem/sina/.

[Buyy 99] BUYYA, RAJKUMAR (HERAUSGEBER): *High Performance Cluster Computing*, Band 1 und 2. Prentice Hall, New Jersey, USA, 1999.

[Buyy 02] BUYYA, RAJKUMAR: *Economic-based Distributed Resource Management and Scheduling for Grid Computing*. Doktorarbeit, School of Computer Science and Software Engineering, Monash University, Melbourne, Australia, 2002, http://www.buyya.com.

[CCITT 88] CCITT (CONSULTATIVE COMMITTEE ON INTERNATIONAL TELEGRAPHY AND TELEPHONY): *Recommendation X.509: The Directory—Authentication Framework*, 1988.

[CDK 01] COULOURIS, G., J. DOLLIMORE und T. KINDBERG: *Distributed Systems, Concepts and Design*. International Computer Science. Addison Wesley, 3. Auflage, 2001.

[CDL+ 00] CAVALLAR, STEFANIA, BRUCE DODSON, ARJEN K. LENSTRA, WALTER LIOEN, PETER L. MONTGOMERY, BRIAN MURPHY, HERMAN TE RIELE, KAREN AARDAL, JEFF GILCHRIST, GÉRARD GUILLERM, PAUL LEYLAND, JOËL MARCHAND, FRANÇOIS MORAIN, ALEC MUFFETT, CHRIS, CRAIG PUTNAM und PAUL ZIMMERMANN: *Factorization of a 512-Bit RSA Modulus*. In: PRENEEL, BART (Herausgeber): *Advances in Cryptology – EUROCRYPT '2000*, Band 1807 der Reihe *Lecture Notes in Computer Science*, Seiten 2–18, Brugge, Belgium, 2000. Springer-Verlag, Berlin, Germany.

[CERT 01] CERT: *Incident Note IN-2001-06: Verification of Dowloaded Software*. Juni 2001, http://www.cert.org/incident_notes/IN-2001-06.html.

[CERT 02a] CERT: *Advisory CA-2002-24: Trojan Horse OpenSSH Distribution*. August 2002, http://www.cert.org/advisories/CA-2002-24.html.

[CERT 02b] CERT COORDINATION CENTER: *CERT Advisory CA-2002-24 Trojan Horse OpenSSH Distribution*. Online, August 2002, http://www.cert.org/advisories/CA-2002-24.html.

[CGH 98] CANETTI, RAN, ODED GOLDREICH und SHAI HALEVI: *The Random Oracle Methodology, Revisited*. März 1998. 1st (draft) version.

[Chau 92] CHAUM, DAVID: *Achieving Electronic Privacy*. Scientific American, 267(2):96–101, August 1992.

[ChKo 00] CHEN, GUANLING und DAVID KOTZ: *A Survey of Context-Aware Mobile Computing Research*. Technical Report TR2000-381, Department of Computer Science, Dartmouth College, 2000.

[CiSt 99] CIANCIOLO, S. und A. STILLER: *Prozessorgeflüster*. c't, 5:21, 1999.

[CKLS 97] COX, INGEMAR, JOE KILIAN, TOM LEIGHTON und TALAL SHAMOON: *Secure Spread Spectrum Watermarking for Multimedia*. IEEE Transactions on Image Processing, 6(12):1673–1687, 1997.

[CoBe 02] CONNOLLY, TH. und C. BEGG: *Database Systems*. Addison-Wesley, 2002.

[Cohe 87] COHEN, FRED: *Computer Viruses, Theory and Experiments*. Computers & Security, 6:22–35, 1987.

[Comm 99] COMMON CRITERIA PROJECT SPONSORING ORGANISATIONS: *Common Criteria for Information Technology Security Evaluation*, August 1999, `http://csrc.ncsl.nist.gov/cc/ccv20/p1-v21.pdf(Part1-Intro&GeneralModel),http://csrc.ncsl.nist.gov/cc/ccv20/p2-v21.pdf(Part2-FunctionalRequirements),http://csrc.ncsl.nist.gov/cc/ccv20/p3-v21.pdf(Part3-AssuranceRequirements)`.

[Crav 99] CRAVER, SCOTT: *Zero Knowledge Watermark Detection, Information Hiding*. In: *LNCS*, Seiten 101–116. Springer Verlag, Berlin, 1999, `citeseer.nj.nec.com/craver00zero.html`.

[Cris 00] CRISCUOLO, PAUL J.: *Distributed Denial of Service*. TR CIAC-2319, Lawrence Livermore National Laboratory, 2000.

[CrSh 99] CRAMER, RONALD und VICTOR SHOUP: *Signature Schemes Based on the Strong RSA Assumption*. In: TSUDIK, GENE (Herausgeber): *Proceedings of the 6th ACM Conference on Computer and Communications Security*, Seiten 46–51, Singapore, November 1999. ACM Press.

[Crypto85] BLAKLEY, G. R., C. MEADOWS und G. B. PURDY: *Fingerprinting long forgiving Messages*. In: WILLIAMS, HUGH C. (Herausgeber): *Advances in Cryptology – CRYPTO '85*, Band 218 der Reihe *Lecture Notes in Computer Science*, Seite 180. International Association for Cryptologic Research, Springer-Verlag, Berlin, Germany, 1986.

[Crypto93] BRANDS, STEFAN: *Untraceable Off-line Cash in Wallet with Observers*. In: STINSON, DOUGLAS R. (Herausgeber): *Advances in Cryptology – CRYPTO '93*, Band 773 der Reihe *Lecture Notes in Computer Science*, Seiten 302–318. International Association for Cryptologic Research, Springer-Verlag, Berlin, Germany, 1994.

[Crypto94] DWORK, CYNTHIA und MONI NAOR: *An efficient existentially unforgeable signature scheme and its applications*. In: DESMEDT, YVO G. (Herausgeber): *Advances in Cryptology – CRYPTO '94*, Band 839 der Reihe *Lecture Notes in Computer Science*, Seiten 234–246. International Association for Cryptologic Research, Springer-Verlag, Berlin, Germany, 1994.

[Crypto95] BONEH, DAN und JAMES SHAW: *Collusion-Secure Fingerprinting for Digital Data*. In: COPPERSMITH, DON (Herausgeber): *Advances in Cryptology – CRYPTO '95*, Band 963 der Reihe *Lecture Notes in Computer Science*, Seiten 452–465. International Association for Cryptologic Research, Springer-Verlag, Berlin, Germany, 1995.

[Crypto96] BELLARE, MIHIR, RAN CANETTI und HUGO KRAWCZYK: *Keying Hash Functions for Message Authentication*. In: KOBLITZ, NEAL (Herausgeber): *Advances in Cryptology – CRYPTO '96*, Band 1109 der Reihe *Lecture Notes in Computer Science*, Seiten 1–15. International Association for Cryptologic Research, Springer-Verlag, Berlin, Germany, 1996.

[Crypto97] CACHIN, CHRISTIAN und UELI MAURER: *Unconditional Security Against Memory-Bounded Adversaries*. In: KALISKI, JR., BURTON S. (Herausgeber): *Advances in Cryptology – CRYPTO '97*, Band 1294 der Reihe *Lecture Notes in Computer Science*, Seiten 292–306. International Association for Cryptologic Research, Springer-Verlag, Berlin, Germany, 1997.

[Crypto98a] BLEICHENBACHER, DANIEL: *Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS*. In: KRAWCZYK, HUGO [Crypto98c], Seiten 1–12.

[Crypto98b] CRAMER, RONALD und VICTOR SHOUP: *A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack*. In: KRAWCZYK, HUGO [Crypto98c], Seiten 13–25.

[Crypto98c] KRAWCZYK, HUGO (Herausgeber): *Advances in Cryptology – CRYPTO '98*, Band 1462 der Reihe *Lecture Notes in Computer Science*. International Association for Cryptologic Research, Springer-Verlag, Berlin, Germany, 1998.

[Crypto99] KOCHER, PAUL, JOSHUA JAFFE und BENJAMIN JUN: *Differential Power Analysis*. In: WIENER, MICHAEL (Herausgeber): *Advances in Cryptology – CRYPTO '99*, Band 1666 der Reihe *Lecture Notes in Computer Science*, Seiten 399–397. International Association for Cryptologic Research, Springer-Verlag, Berlin, Germany, 1999.

[CWP+ 99] COWAN, C., P. WAGLE, C. PU, S. BEATTIE und J. WALPOLE: *Buffer Overflows: Attacks and Defenses for the Vulnerability of the Decade*. In: *Proceedings of the DARPA Information Survivability Conference and Exposition*, 1999.

[DAB 03] DAB: *The World Forum of Digital Audio Broadcasting*. Online, März 2003, `http://www.worlddab.org`.

[Damg 98] DAMGÅRD, IVAN (Herausgeber): *Lectures on Data Security: Modern Cryptology in Theory and Practise*, Band 1561 der Reihe *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany, 1998.

[DaPe 00] DAVIDSON, J. und J. PETERS: *Voice over IP - Grundlagen, Konzepte, Technologie, Anwendungen*. Markt und Technik, München, 2000.

[DaRe 00] DAVIE, B. und Y. REKHTER: *MPLS: Technology and Applications*. Morgan Kaufmann Publishers, 2000.

[Davi 96] DAVIS, J. R.: *Creating An Extensible, Object-Relational Data Management Environment – IBM's DB2 Universal Database*. In: *Database Associates International*, 1996.

[Davi 00] DAVIE, B. UND REKHTER, Y.: *MPLS. Technology and Applications*. Morgan Kaufmann Publishers, 2000.

[DBP 96] DOBBERTIN, HANS, ANTOON BOSSELAERS und BART PRENEEL: *RIPEMD-160: A strengthened version of RIPEMD*. In: *Proceedings of the 3rd International Workshop on Fast Software Encryption*, Band 1039 der Reihe *Lecture Notes in Computer Science*, Seiten 71–82. Springer-Verlag, Berlin, Germany, 1996.

[DCI 03] THE DISAPPEARING COMPUTER INITIATIVE: *The Disappearing Computer*, Januar 2003, `http://www.disappearing-computer.net`.

[DDT 97] DOMS, M., T. DUNNE und K. TROSKE: *Workers, Wages and Technology*. Quarterly Journal of Economics, 112:253–290, 1997.

[Dean 02] DEAN, D. R.: *Mobile Kommunikation – Wertschöpfung, Technologien, neue Dienste*, Kapitel Wie man den „M-Commerce"-Kunden gewinnt. Gabler, 2002.

[Deif 98a] DEIFEL, B.: *Grundkonzept zur werkzeugunterstützten Anforderungssammlung für komplexe Standardsoftware*. Interner Arbeitsbericht A4, FORSOFT, 1998.

[Deif 98b] DEIFEL, B.: *Theoretische und praktische Ansätze im Requirements Engineering für Standardsoftware und Anlagenbau*. Technischer Bericht -I-9832, Technische Universität München, Institut für Informatik, 1998.

[Deif 01] DEIFEL, B.: *Requirements Engineering komplexer Standardsoftware*. Doktorarbeit, Technische Universität München, 2001.

[Denn 90] DENNING, PETER J.: *Computers under Attack - Intruders, Worms and Viruses*. ACM Press, New York, 1990. 554 pages.

[Detk 99] DETKEN, O.: *Photonische Netze: Bandbreite alleine reicht nicht*. NetworkWorld, 03, 1999.

[Detk 01] DETKEN, O.: *Quality-of-Service (QoS): Garantierte Dienstgüte über das Internet*. Whitepaper DECOIT-QOS0107, Juli 2001, `http://www.decoit.de/whitepapers/DECOIT-QOS0107.pdf`.

[Deut 99] DEUTSCHER BUNDESTAG: *Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (Signaturgesetz)*, 1999, `http://www.parlamentsspiegel.de/cgi-bin/hyperdoc/show_dok.pl?k=BBD122/01`.

[Dey 00] DEY, A. K.: *Providing Architectural Support for Building Context-Aware Applications*. Doktorarbeit, Georgia Institute of Technology, 2000.

[DiHe 76] DIFFIE, WHITFIELD und MARTIN HELLMAN: *New Directions in Cryptography*. IEEE Transactions on Information Theory, IT-22(6):644–654, November 1976.

[Ditt 02] DITTRICH, K.: *Verteilte Datenbanksysteme*, November 2002, `http://iezzi.ch/files/unizh_HS/VDBS/vDBS_VL_notes.pdf`.

[DSK 02] DORNSEIF, MAXIMILIAN, KAY SCHUMANN und CHRISTIAN KLEIN: *Tatsächliche und rechtliche Risiken drahtloser Computernetzwerke*. In: *Datenschutz und Datensicherheit (DuD) 22 (2002)*. Vieweg, Wiesbaden, 2002.

[DSVH 97] DINTER, B., C. SAPIA, M. VRCA und G. HÖFLING: *Der OLAP Markt: Architekturen, Produkte, Trends*. Forwiss-Forschungsgruppe Wissensbasen, 1997.

[Dymo 02] DYMOND, K. M.: *CMM Handbuch. Das Capability Maturity Model für Software*. Springer-Verlag, Berlin, Germany, 2002.

[EaMi 02] EASTMAN, LESTER F. und UMESH K. MISHRA: *The Toughest Transistor Yet*. IEEE Spectrum, Seiten 28–33, May 2002.

[EbFi 01] EBERHART, A. und S. FISCHER: *Java-Bausteine für E-Commerce-Anwendungen*. Carl Hanser, 2001.

[Elek 03] ELEKTROSMOGNEWS.DE: *Aktuelle News zum Thema Mobilfunk und Elektrosmog*. Online, März 2003, `http://elektrosmognews.de`.

[ElGa 85] ELGAMAL, TAHER: *A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms*. IEEE Transactions on Information Theory, IT-31(4):469–472, Juli 1985.

[Elli 99] ELLISON, CARL: *The nature of a useable PKI*. Computer Networks, 31(8):823–830, Mai 1999.

[ElNa 00] ELMASRI, R. und S.B. NAVATHE: *Fundamentals of Database Systems*. Addison-Wesley, 2000.

[ElSc 00] ELLISON, CARL und BRUCE SCHNEIER: *Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure*. Computer Security Journal, 16(1):1–7, 2000.

[Endr 96] ENDRES A.: *Werkzeuge in der Programmentwicklung. Skript zur gleichnamigen Vorlesung im WS 95/96 am Institut für Informatik der Technischen Universität München*, 1996.

[ESG 00] EGGERS, J. J., J. K. SU und B. GIROD: *Asymmetric Watermarking Schemes*. In: *Sicherheit in Mediendaten*, Springer Reihe, Informatik Aktuell, September 2000.

[Euro 97] EUROPÄISCHE KOMMISSION: *Grünbuch zur Konvergenz der Branchen Telekommunikation, Medien und Informationstechnologie und ihren ordnungspolitischen Auswirkungen*. Report KOM-(97) 623, Dezember 1997, `http://europa.eu.int/ISPO/convergencegp/97623de.pdf`.

[Euro 01] EUROPEAN PARLIAMENT'S OFFICE FOR SCIENTIFIC AND TECHNOLOGICAL OPTIONS ASSESSMENT: *Development of Surveillance Technology and Risk of Abuse of Economic Information*. Directorate B, European Parliament, June 2001.

[EVB 01] EBERSPÄCHER, J., H.-J. VÖGEL und C. BETTSTETTER: *GSM: Switching, Services and Protocols*. John Wiley Sons, LTD., 2. Auflage, 2001.

[FePf 00] FEDERRATH, HANNES und ANDREAS PFITZMANN: *Schutzziele in IT-Systemen*. Datenschutz und Datensicherheit, Seiten 704–710, Dec 2000.

[FeSc 99] FERGUSON, NIELS und BRUCE SCHNEIER: *A Cryptographic Evaluation of IPsec*. Technischer Bericht, Counterpane, 1999.

[FH-F 99] FH-FURTWANGEN: *Multimediadatenbanken*, November 1999, `http://www.ai-lab.fh-furtwangen.de/veranstaltungen/oberseminar/db2/`.

[Fina 02] FINANCIAL TIMES DEUTSCHLAND: *IBM übernimmt Rechenzentren der Deutschen Bank*. Online, 2002, `http://www.ftd.de/tm/it/1040216119385.html?nv=rs`.

[Fisc 00] FISCHLIN, MARC: *A Note on Security Proofs in the Generic Model*. In: OKAMOTO, T. (Herausgeber): *Advances in Cryptology – ASIACRYPT '2000*, Band 1976 der Reihe *Lecture Notes in Computer Science*, Seiten 458–469, Kyoto, Japan, 2000. International Association for Cryptologic Research, Springer-Verlag, Berlin, Germany.

[FKK 96] FREIER, ALAN O., PHILIP KARITON und PAUL C. KOCHER: *The SSL Protocol: Version 3.0*. Internet Draft, Netscape Communications, 1996.

[Flan 96] FLANAGAN, D.: *Java in a Nutshell*. O'Reilly, 1996.

[FLS 99] FÖRSTER, A., H. LÜTH und T. SCHÄPERS: *Die neue Welt*. Spektrum der Wissenschaft, 6, 1999.

[FMS 01] FLUHRER, SCOTT, ITSIK MANTIN und ADI SHAMIR: *Weaknesses in the Key Scheduling Algorithm of RC4*. In: *8th Annual Workshop on Selected Areas in Cryptography*, Band 2259 der Reihe *Lecture Notes in Computer Science*, Seiten 1–24, Toronto, Canado, August 2001. Springer-Verlag, Berlin, Germany, `http://localhost/mirror/sites/link.springer.de/link/service/series/0558/papers/2259/22590001.pdf,http://www.crypto.com/papers/others/rc4_ksaproc.ps`.

[FoKe 99] FOSTER, I. und C. KESSELMAN: *The Grid: Blueprint for a Future Computing Infrastructure*. Morgan Kaufman Publishers, 1999.

[Form 95] FORMAL SYSTEMS (EUROPE) LTD.: *Failures-Divergence Refinement: FDR2*. Dezember 1995.

[Fox 02] FOX, DIRK: *Der IMSI-Catcher*. In: *Datenschutz und Datensicherheit (DuD ), 4/2002*, Seiten 212–215. Vieweg, Wiesbaden, 2002.

[Frey 97] FREYER, U. G.: *DAB. Digitaler Hörfunk*. Verlag Technik, 1997.

[FrSu 01] FROST und SULLIVAN: *The European Market for Enterprise Peer-to-Peer (P2P) Solutions*. Report B0003, 2001.

[Fyod 97] FYODOR: *The Art of Port Scanning*. Internet, September 1997.

[GBSS 98] GROSU, R., M. BROY, B. SELIC und G. STEFANESCU: *Towards a calculus for UML-RT specifications*, 1998.

[Gess 01] GESSNER, SANDRA: *Intrusion Detection - Terminologie und Überblick*. In: *Seminar Internet-Sicherheit. Universität des Saarlandes, Saarbrücken*, 2001.

[GGB 01] GUELICH, S., S. GUNDAVARAM und G BIRZNIEKS: *CGI-Programmierung mit Perl*. O'Reilly, 2001.

[Ghan 00] GHANI, N.: *Integration Strategies for IP Over WDM*. Folien eines Vortrags im Rahmen des Optical Networks Workshop, Dallas, USA, Januar 2000, `http://www.cs.buffalo.edu/~qiao/cse620/onw2000.pdf`.

[GHR 99] GRUSCHKE, B., S. HEILBRONNER und H. REISER: *Mobile Agent System Architecture — Eine Plattform für flexibles IT–Management*. Technischer Bericht 9902, Ludwig-Maximilians-Universität München, Institut für Informatik, München, August 1999, `http://wwwmnmteam.informatik.uni-muenchen.de/common/Literatur/MNMPub/Publikationen/ghr99/ghr99.shtml`.

[Giem 99] GIEMSA, F.: *Intelligente und Programmierbare Netze*. Hauptseminar zu überfachlichen Grundlagen Zukunftstechnologien der Informatik, Ludwig-Maximilians-Universität München, 1999.

[GKRB 96] GROSU, R., C. KLEIN, B. RUMPE und M. BROY: *State Transition Diagrams*. Technischer Bericht TUM-I-9630, Technische Universität München, 1996.

[GMD 99] GMD/IPSI–DELITE: *Knowledge Discovery/Data Mining*, November 1999, `http://www-cui.darmstadt.gmd.de/~Xferber/dm-ir/vi-neu/book_1.part_2.subdiv1_7.html`.

[GMR 88] GOLDWASSER, SHAFI, SILVIO MICALI und RON L. RIVEST: *A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks*. SIAM Journal on Computing, 17(2):281–308, April 1988.

[Gold 01] GOLDREICH, ODED: *Foundations of Cryptography*, Band Basic Tools. Cambridge University Press, 2001.

[Gole 01] GOLEM.DE: *Telekom bietet SMS im Festnetz*. Online, Juli 2001, `http://www.golem.de/0107/14703.html`.

[Goll 99] GOLLMANN, DIETER: *Computer Security*. John Wiley & Sons, 1999.

[GoMi 82] GOLDWASSER, SHAFI und SILVIO MICALI: *Probabilistic Encryption and How to Play Mental Poker Keeping Secret All Partial Information*. In: *Proceedings of the Fourteenth Annual ACM Symposium on Theory of Computing*, Seiten 365–377, San Francisco, California, 5–7 Mai 1982. .

[GoMi 84] GOLDWASSER, SHAFI und SILVIO MICALI: *Probabilistic Encryption*. Journal of Computer Security, 28:270–299, 1984.

[GrHe 99] GROTHEER, M. und H. HEBBEN: *Schrittliste zum Aufbau einer OLAP-Datenbank*. Controller Magazin, 3, 1999.

[Grif 02] GRIFFITH, ERIC: *Intel's Banias Starts with 802.11b*. Online, Dezember 2002, `http://www.internetnews.com/wireless/article.php/1558011`.

[GrYo 97] GREENWOOD, J. und M. YORUKOGLU: *1974*. Carnegie-Rochester Conference Series on Public Policy, 46:49–95, 1997.

[Haas 00] HAAS, R. UND MARTY, R.: *Everything over IP, IP over Everything*. Technischer Bericht Seminar 35-649, ETH Zürich, November 2000, http://www.raffy.ch/projects/IntEco-seminar-22.11.2000.doc.

[Haff 02] HAFFA UND PARTNER: *Eingebettete Software-Wiederverwendung*, August 2002, http://www.haffapartner.de/kunden/themenservice/ausgabe\%20KW39-02.htm.

[HAN 99] HEGERING, H.-G., S. ABECK und B. NEUMAIR: *Integrated Management of Networked Systems*. Morgan Kaufman Publishers, 1999.

[Hanc 96] HANCOCK, B.: *Advanced Ethernet/802.3 Management and Performance*. Butterworth-Heinemann, 2. Auflage, 1996.

[Hand 02] HANDL, A.: *Multivariate Verfahren*. Springer-Verlag, Berlin, Germany, 2002.

[Hart 00] HARTE, L. UND KIKTA, R.: *Delivering xDSL*. McGraw-Hill Companies, 2000.

[Hass 02] HASS, BERTHOLD: *Geschäftsmodelle von Medienunternehmen. Ökonomische Grundlagen und Veränderungen durch neue Informations- und Kommunikationstechnik*. Gabler, 2002.

[Hein 93] HEINRICH, L.: *Wirtschaftsinformatik*. Oldenbourg, 1993.

[HeMe 02] HEROLD, E. und W. MEANS: *XML in a Nutshell*. O'Reilley, 2002.

[HePa 03] HENNESSY, JOHN L. und DAVID A. PATTERSON: *Computer Architecture: A Quantitative Approach*. Morgan Kaufmann Publishers, San Francisco, 3. Auflage, 2003.

[HeSa 01] HEINE, G. und H. SAGKOB: *GPRS - Gateway zu Mobilfunknetzen der 3. Generation*. Franzis Verlag, 2001.

[HLSS 96] HUTTER, D., B. LANGENSTEIN, C. SENGLER und J. H. SIEKMANN: *Deduction in the Verification Support Environment (VSE)*. Lecture Notes in Computer Science, 1051:268–??, 1996.

[HoWe 01] HOULE und WEAVER: *Trends in Denial of Service Attack Technology*. Technischer Bericht, CERT Coordination Center, 2001.

[HSG 94] HORNSBY, J., B. SMITH und J. GUPTA: *The Impact of Decision-Making Methodology on Job Evaluation Outcomes*. Group and Organization Studies, Seiten 112–128, 1994.

[HSH+ 97] HOLLFELDER, S., F. SCHMIDT, M. HEMMJE, K. ABERER und A. STEINMETZ: *Transparent Integration of Continuous Media Support into a Multimedia DBMS*. In: *Arbeitspapiere der GMD*, 1997.

[IABG 99] IABG: *Willkommen zum V–Modell*, November 1999, http://www.v-modell.iabg.de/index.htm.

[IBM 03a] IBM CORPORATION: *ASCI White*. Online, 2003, http://www-1.ibm.com/servers/eserver/pseries/hardware/largescale/supercomputers/asciwhite/.

[IBM 03b] IBM CORPORATION: *Object Constraint Language (OCL)*, 2003, http://www-3.ibm.com/software/awdtools/library/standards/ocl.html.

[IEC 03] INTERNATIONAL ENGINEERING CONSOSRTIUM: *IEC: Specification and Description Language (SDL)*, 2003, http://www.iec.org/online/tutorials/sdl.

[IETF 02] INTERNET ENGINEERING TASK FORCE (IETF): *New Terminology and Clarifications for Diffserv RFC 3260*, April 2002, http://www.faqs.org/rfcs/rfc3260.html.

[IETF 81] INTERNET ENGINEERING TASK FORCE (IETF): *Internet Protocol RFC 791*, September 1981, ftp://ftp.isi.edu/in-notes/rfc791.txt .

[IETF 97a] INTERNET ENGINEERING TASK FORCE (IETF): *Resource ReserVation Protocol Version 1 Functional Specification RFC 2205*, September 1997.

[IETF 97b] INTERNET ENGINEERING TASK FORCE (IETF): *Specification of Guaranteed Quality of Service RFC 2212*, September 1997, ftp://ftp.isi.edu/in-notes/rfc2212.txt .

[IETF 99] INTERNET ENGINEERING TASK FORCE (IETF): *The TLS Protocol Version 1.0 RFC 2246*, Januar 1999, ftp://ftp.isi.edu/in-notes/rfc2246.txt .

[IETF 99] IETF ARBEITSGRUPPE IPSEC, November 1999, http://www.ietf.org/html.charters/ipsec-charter.html .

[IGS 01] BROY, M., A. BUTTERMANN, F. GEHRING, M. GARSCHHAMMER, H.-G. HEGERING, H. KELTER, A. PICOT, M. ULLMANN und S. VOGEL: *Integrierte Gebäudesysteme, Technologien, Sicherheit und Märkte*. SecuMedia Verlag, Ingelheim, 2001.

[I'Mi 90] I'ANSON, COLIN und CHRIS MITCHELL: *Security Defects in CCITT Recommendation X.509 - The Directory Authentication Framework*. Computer Communication Review, 20(2):30–34, April 1990.

[Infi 03] INFINEON TECHNOLOGIES AG: *DDR SDRAM Components*, 2003, http://www.infineon.com/cgi/ecrm.dll/ecrm/scripts/prod_cat.jsp?oid=-8005 .

[Info 98] INFORMIX: *Informix Dynamic Server Overview*, Juni 1998, http://www.informix.com/informix/products/ids/overview.htm .

[Inte 01] INTERNATIONAL MONETARY FUND: *World Economic Outlook. The Information Technology Revolution*. IMF (Washington, D.C.), 2001.

[Inte 02] INTEL CORPORATION: *Expanding Moore's Law, The Exponential Opportunity*, Fall 2002, ftp://download.intel.com/labs/eml/download/EML_opportunity.pdf .

[ISO 17799] ISO/IEC: *ISO 17799: Information Technology - Code of Practise for Information Security Management (2000)*, 2000, http://www.iso17799software.com .

[ISO 7498] ISO: *Information Processing Systems – Open Systems Interconnection – Basic Reference Model*, 1984.

[ISO 9001] DIN AUSSCHUSS QUALITÄTSSICHERUNG UND ANGEWANDTE STATISTIK (AQS) IM DIN DEUTSCHES INSTITUT FÜR NORMUNG E.V.; NORMENAUSSCHUSS INFORMATIONSVERARBEITUNGSSYSTEME (NI) IM DIN: *Deutsche Norm DIN ISO9000 Teil 3 Qualitätsmanagement- und Qualitätssicherungsnormen Leitfaden für die Anwendung von ISO 9001 und die Entwicklung, Lieferung und Wartung von Software*, 1992.

[ISO 9075] ISO: *ISO 9075: Database Language SQL*, 1999.

[JaWe 01] JAKOBSSON, MARKUS und SUSANNE WETZEL: *Security Weaknesses in Bluetooth*. Lecture Notes in Computer Science, 2020:176ff, 2001, http://link.springer-ny.com/link/service/series/0558/bibs/2020/20200176.htm;http://link.springer-ny.com/link/service/series/0558/papers/2020/20200176.pdf .

[JoNy 95] JONES, R. und A. NYE: *HTML und das World Wide Web*. O'Reilly, 1995.

[JRMI 03] JAVA.SUN.COM: *Java Remote Method Invocation*, 2003, http://java.sun.com/products/jdk/rmi/ .

[Kahn 67] KAHN, DAVID: *The Codebreakers — The Story of Secret Writing*. Macmillan Publishing Co, New York, USA, 1967.

[KAL+ 01] KAARANEN, H., A. AHTIAINEN, L. LAITINEN, S. NAGHIAN und V. NIEMI: *UMTS Networks*. John Wiley and Sons, Ltd., 2001.

[Kali 98] KALISKI, JR., BURTON S.: *Emerging Standards for Public-Key Cryptography*. In: DAMGÅRD, IVAN [Damg 98], Seiten 87–104.

[Kanb 98] KANBACH, A. UND KÖRBER, A.: *ISDN. Die Technik. Schnittstellen, Protokolle, Dienste, Endsysteme*. Hüthig-Verlag, 3. Auflage, 1998.

[KaPe 00] KATZENBEISSER, STEFAN und FABIEN A.P. PETITCOLAS: *Information Hiding: techniques for steganography and digital watermarking*. Artech House Publishers, 2000.

[KeEi 97] KEMPER, A. und A. EICKLER: *Datenbanksysteme*. Oldenbourg, 1997.

[KeEi 01] KEMPER, A. und A. EICKLER: *Datenbanksysteme. Eine Einführung*. Oldenbourg, 2001.

[Kelt 01] KELTER, HARALD: *Das Ende der Anonymität? Datenspuren in modernen Netzen*. SecuMedia Verlag, Ingelheim, 2001.

[Kieß 99] KIESS, F. M.: *IBM plant den Prozessorstandard für alle Netze*. Computerzeitung, 3:14, 1999.

[KKP 00] KÖHNTOPP, KRISTIAN, MARIT KÖHNTOPP und ANDREAS PFITZMANN: *Sicherheit durch Open Source? Chancen und Grenzen*. In: *Datenschutz und Datensicherheit (DuD) 24/9 (2000)*. Vieweg, Wiesbaden, 2000.

[Klip 02] KLIPPSTÄTTER, KRIEMHILDE: *Die Invasion der Blade-Rechner steht bevor*. Computerwoche Online vom 11.10.2002, 2002, `http://www.computerwoche.de/index.cfm?pageid=255&artid=41701&type=detail`.

[Knud 98] KNUDSEN, LARS R.: *Contemporary Block Ciphers*. In: DAMGÅRD, IVAN [Damg 98], Seiten 105–126.

[Kobl 87] KOBLITZ, NEAL: *A Course in Number Theory and Cryptography*. Nummer GTM 114 in *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, Germany, Berlin, 1987.

[Kobl 98] KOBLITZ, NEAL: *Algebraic Aspects of Cryptography*. Nummer 3 in *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, Germany, 1998.

[Koch 95] KOCHER, PAUL C.: *Cryptanalysis of Diffie-Hellman, RSA, DSS, and other Systems Using Timing Attacks*. Technischer Bericht, cryptography.com, Dezember 1995.

[Koll 03] KOLLMANN, TOBIAS: *Die Überlebenden des Internethypes*. Online, 2003, `http://www.manager-magazin.de/ebusiness/gruender/0,2828,239525-2,00.html`.

[Krau 02] KRAUSS, OTTMAR: *DWDM und Optische Netze: Eine Einführung in die Terabit-Technologie*. John Wiley Europe, Juli 2002.

[Kruc 98] KRUCHTEN, P.: *The Rational Unified Process – An Introduction*. Addison Wesley, 1998.

[Kuhl 98] KUHLMANN, U.: *Isomatte im Chip, Flinkere Chips mit SOI-Technologie*. c't, 17:28, 1998.

[Kuhl 99] KUHLMANN, U.: *Display-Boom ungebrochen*. c't, 20:20, 1999.

[LaMa 90] LAI, XUEJIA und JAMES L. MASSEY: *A Proposal for a New Block Encryption Standard*. In: DAMGARD, I.B. (Herausgeber): *Advances in Cryptology – EUROCRYPT '90*, Band 473 der Reihe *Lecture Notes in Computer Science*, Seiten 389–404. International Association for Cryptologic Research, Springer-Verlag, Berlin, Germany, 1990.

[Lamm 02] LAMMERS, DAVID: *Motorola to demo 1-Mbit magnetoresistive RAM*. Online, Juni 2002, http://www.eetimes.com/semi/news/OEG20020610S0054.

[Lang 01] LANGER, M.: *Konzeption und Anwendung einer Customer Service Management Architektur*. Dissertation, Technische Universität, München, März 2001.

[LBMC 94] LANDWEHR, CARL E., ALAN R. BULL, JOHN P. MCDERMOTT und WILLIAM S. CHOI: *A Taxonomy of Computer Program Security Flaws*. ACM Computing Surveys, 26(3):211–254, September 1994.

[Lens 00] LENSTRA, ARJEN K.: *Integer Factoring*. Designs, Codes and Cryptography, 19:101–128, 2000.

[LeVe 01] LENSTRA, ARJEN K. und ERIC R. VERHEUL: *Selecting Cryptographic Key Sizes*. Journal of Cryptology, 14(4):255–293, 2001.

[LiJo 97] LINDQVIST, ULF und ERLAND JONSSON: *How to Systematically Classify Computer Security Intrusions*. IEEE Symposium on Security & Privacy, Seiten 154–163, 1997.

[LLMP 90] LENSTRA, A. K., H. W. LENSTRA, M. S. MANASSE und J.M. POLLARD: *The number field sieve*. In: *22nd ACM Symposium on Theory of Computing*, Seiten 564–572, 1990.

[Lyma 02] LYMAN, JAY: *Data Storage Shrinks to Nanoscale*. Online, Juli 2002, http://sci.newsfactor.com/perl/story/18446.html\#story-start.

[Mage 02] MAGEE, MIKE: *Banias a 77 million transistor baby*. Online, September 2002, http://www.theinquirer.net/?article=5344.

[Manf 02] MANFERDELLI, J.: *Palladium*. In: *Microsoft Research Seminars Series - Security Workshop; Cambridge*, November 2002, http://research.microsoft.com/collaboration/university/europe/events/.

[Mats 94] MATSUI, MITSURI: *Linear Cryptanalysis Method for DES Cipher*. In: HELLESETH, T. (Herausgeber): *Advances in Cryptology – EUROCRYPT '93*, Band 765 der Reihe *Lecture Notes in Computer Science*, Seiten 386–397. International Association for Cryptologic Research, Springer-Verlag, Berlin, Germany, 1994.

[Mats 02] MATSUSHITA ELECTRIC INDUSTRIAL: *Large Capacity Optical Disc Video Recording Format Blu-Ray Disc Established*, Februar 2002, http://www.matsushita.co.jp/corp/news/official.data/data.dir/en020219-4/en020219-4.html.

[Matt 01] MATTERN, FRIEDEMANN: *Internet @Future - Jahrbuch Telekommunikation und Gesellschaft 2001*, Kapitel Ubiquitous Computing. Hüthig, 2001.

[Matt 02] MATTERN, FRIEDEMANN: *Vom Handy zum allgegenwärtigen Computer : Ubiquitous Computing: Szenarien einer informatisierten Welt*. In: *Analysen der Friedrich-Ebert-Stiftung zur Informationsgesellschaft*. Friedrich-Ebert-Stiftung, Bonn, April 2002, http://library.fes.de/fulltext/stabsabteilung/01183.htm.

[Matt 03] MATTERN, FRIEDEMANN: *From Distributed Systems to Ubiquitous Computing*. In: IRMSCHER, K. und K.-P. FÄHNRICH (Herausgeber): *Kommunikation in Verteilten Systemen*, Leipzig, 2003. Springer Verlag.

[MaZi 99] MAYER, M. und H. ZISLER: *Glasfasernetze in der Praxis. Planung, Beschaffung, Installation*. Hüthig und Pflaum-Verlag, 1999.

[MBK+ 01] MERTENS, P., F. BODENDORF, W. KÖNIG, A. PICOT und M. SCHUMANN: *Grundzüge der Wirtschaftsinformatik*. Springer, 2001.

[McCu 90] MCCURLEY, KEVIN S.: *The Discrete Logarithm Problem*. In: POMERANCE, CARL (Herausgeber): *Cryptology and Computational Number Theory*, Band 42 der Reihe *Proceedings of Symposia in Applied Mathematics*, Seiten 49–74, Providence, 1990. American Mathematical Society.

[McEl 87] MCELIECE, R. J.: *A Public-key Cryptosystem Based on Algebraic Coding Theory*. DSN Progress Report, Seiten 42–44, 1987.

[McHu 01] MCHUGH, JOHN: *Intrusion and intrusion detection*. International Journal of Information Security, 1(1):14–35, 2001.

[Medi 02] MEDIALINE: *Internet-Entwicklung*, August 2002, http://www.medialine.de/PM1D/PM1DD/PM1DDC/PM1DDCR/PM1DDCRA/pm1ddcra.htm.

[Mert 95] MERTENS, P.: *Wirtschaftsinformatik '95 - Wettbewerbsfähigkeit, Innovation, Wirtschaftlichkeit*, Kapitel Wirtschaftsinformatik - Von den Moden zum Trend. Physica, 1995.

[Merz 02] MERZ, MICHAEL: *E-Commerce und E-Business*. dpunkt, 2002.

[Mess 97] MESSMER, H.: *PC Hardware*. Addison Wesley, 5. Auflage, 1997.

[MeSt 89] MEIER, WILLI und OTHMAR STAFFELBACH: *Fast Correlation attacks on Stream Ciphers*. JC, 1(3):159–176, 1989.

[Micr 99] MICROSOFT GMBH: *Microsoft COM Technologies – Information and Resources for the Component Object Model–based Technologies*, November 1999, http://www.microsoft.com/com/?RLD=59.

[Micr 02a] MICROSOFT CORPORATION: *Digital Ink, Breakthrough Technology in Tablet PC, Brings the Power of the Pen to the Desktop*, Oktober 2002, http://www.microsoft.com/presspass/features/2002/Oct02/10-29tabletinking.asp.

[Micr 02b] MICROSOFT GMBH: *ActiveX Controls - Microsoft Papers, Presentations, Web Sites, and Books, for ActiveX Controls*, 2002, http://www.microsoft.com/com/tech/ActiveX.asp.

[Micr 02c] MICROSOFT GMBH: *.Net Framework Home Page - Developing the Future*, 2002, http://www.microsoft.com/netframework/.

[Micr 03] MICROPROCESSOR FORUM: *The Microprocessor Forum Home Page*, 2003, http://www.mdronline.com.

[MIT 03] MIT MEDIA LAB: *Wearable Computing*, März 2003, http://www.media.mit.edu/wearables/.

[Mits 97] MITSURU, MATSUI: *New Block Encryption Algorithm MISTY*. Lecture Notes in Computer Science, 1267:54–68, 1997, http://link.springer-ny.com/link/service/series/0558/bibs/1267/12670054.htm;http://link.springer-ny.com/link/service/series/0558/papers/1267/12670054.pdf.

[MM 02] MANAGER-MAGAZIN: *Discount Airlines - Tickets für 10 Euro*. Online, 2002, http://www.manager-magazin.de/unternehmen/artikel/0,2828,208727,00.html.

[MoPs 99] MOK, F. und D. PSALTIS: *Holographische Datenspeicher*. Spektrum der Wissenschaft, 1:50ff., 1999.

[MoRo 01] MOORMANN, J. und P. ROSSBACH: *Customer Relationship Management in Banken*. Bankakademie-Verlag (Frankfurt), 2001.

[Moun 97] MOUNTZIA, M.: *Flexible Agents in Integrated Network and Systems Management*. Doktorarbeit, Technische Universität München, 1997.

[MTF 03] MONACO, DE, TULMU und MACROS FRUTIGER: *When the Going Gets Tough the Tough Get Going*. Issues in Electronic Layout Developments, 3(54), 2003.

[MuKe 01] MUSCIANO, C. und B. KENNEDY: *HTML und XHTML*. O'Reilly Associates, 2001.

[Mult 02] MULTISERVICE SWITCHING FORUM: *MSF 2003 Technical Committee Plans and Roadmap*. Online, November 2002, http://www.msforum.org/techinfo/MSF_Roadmap_2003.pdf .

[MvOV 97] MENEZES, ALFRED J., PAUL C. VAN OORSCHOT und SCOTT A. VANSTONE: *Handbook of Applied Cryptography*. CRC Press series on discrete mathematics and its applications. CRC Press, 1997. ISBN 0-8493-8523-7.

[MVS 01] MOORE, DAVID, GEOFFREY VOELKER und STEFAN SAVAGE: *Inferring Internet Denial of Service Activity*. In: *Proceedings of the 10th USENIX Security Symposium*, Washington, D.C., August 2001. USENIX.

[Nati 77] NATIONAL BUREAU OF STANDARDS (NBS): *Specification for the Data Encryption Standard*. Federal Information Processing Standards Publication (FIPS PUB) 46, Januar 1977.

[Nati 91] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST): *The Digital Signature Standard (DSS)*. Federal Information Processing Standards Publication (FIPS PUB) 186, August 1991. Draft.

[Nati 01] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST): *Advanced Encryption Standard (AES)*. Federal Information Processing Standards Publication (FIPS PUB) 197, November 2001.

[Nati 03] NATIONAL ACADEMY OF ENGINEERING: *The Greatest Engineering Achievements of the 20th Century*, Januar 2003, http://www.greatachievements.org/ .

[Nefi 01] NEFIODOW, LEO A.: *Der sechste Kondratieff*. Rhein-Sieg Verlag, 5. Auflage, 2001.

[Neum 00] NEUMANN, PETER: *Robust Nonproprietary Software (2 pages)*. In: *RSP: 21th IEEE Computer Society Symposium on Research in Security and Privacy*, 2000, http://www.csl.sri.com/neumann/ieee00+.pdf .

[NFD 99] NFD - ABHANDLUNG: *Wissen ist Macht, aber nur, wenn es weitergegeben wird*, November 1999, http://www.darmstadt.gmd.de/NFD/Ausg399/abstr3.html .

[Nico 00] NICOLAI, J.: *Intel to showcase 1GHz 'Coppermine' Pentium III*. Online, 2000, http://www.cnn.com/2000/TECH/computing/02/01/hispeed.coppermine.idg/ .

[Niel 96] NIELÄNDER, U.: *LEO (Lab of Evolutionary Optimization)*, 1996, http://tu-chemnitz.de/informatik/HomePages/ModSim/Software/leo.html .

[NIST 95] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) COMPUTER SYSTEMS LABORATORY: *Secure Hash Standard*. April 1995, http://csrc.ncsl.nist.gov/fips/fip180-1.pdf .

[NKK 01] NAUCK, D., F. KLAWONN und R. KRUSE: *Neuronale Netze und Fuzzy-Systeme*. Vieweg, 2001.

[NRC 00] NATIONAL RESEARCH COUNCIL: *The Digital Dilemma, Intellectual Property in the Information Age*. National Academy Press, 2000.

[Nuse 01] NUSEIBEH, BASHAR: *Weaving Together Requirements and Architectures*. IEEE Computer, 34(2):115–117, 2001.

[OECD 00] ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT: *A new Economy? The changing Role of Innovation and Information Technology in Growth*. OECD, 2000.

[Oest 01] OESTEREICH, B.: *Objektorientierte Softwareentwicklung*. Oldenbourg, 5. Auflage, 2001.

[OG 97] THE OPEN GROUP: *DCE 1.1: Remote Procedure Call*, August 1997, www.opengroup.org/public/pubs/catalog/c706.htm.

[OMG 99] OBJEKT MANAGEMENT GROUP (OMG): *OMG's Press Releases of XMI Technology*, November 1999, http://www.omg.org/news/pr99/2_6.html.

[OMG 02] OMG: *CORBA - Common Object Request Broker*, November 2002, http://www.corba.org.

[OTU 00] OKAMOTO, TATSUAKI, KEISUKE TANAKA und SHIGENORI UCHIYAMA: *Quantum public-key cryptosystems*. Lecture Notes in Computer Science, Springer-Verlag, Berling, Germany, 1880:147–165, 2000.

[PASS 00] PASS IT-CONSULTING: *XML: Highway in die Zukunft des e-Business*, 2000, http://www.pass-consulting.com/internet/html_d/presseservice/extended_web500/feature_xml.pdf.

[PDF 02] PICOT, A., H. DIETL und E. FRANCK: *Organisation – Eine ökonomische Perspektive*. Schäffer-Poeschel (Stuttgart), 3. Auflage, 2002.

[Pepp 00] PEPPER, P.: *Funktionale Programmierung*. Springer-Verlag, Berlin, Germany, 2000.

[PeTh 00] PERRIER, P. und S. THOMPSON: *Optische Cross-Connects: Die neuesten Elemente des optischen Backbone-Netzes*. Alcatel Telcom Rundschau, 3, 2000, http://atr.alcatel.de/hefte/00i_3/de/pdf_de/07perrde.pdf.

[Pfit 96] PFITZMANN, BIRGIT: *Digital Signature Schemes — General Framework and Fail-Stop Signatures*, Band 1100 der Reihe *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany, 1996.

[PfKö 00] PFITZMANN, ANDREAS und MARIT KÖHNTOPP: *Anonymity, Unobservability, and Pseudonymity — A Proposal for Terminology*. Personal Communication, September 2000. Draft v0.4.

[PhKa 98] PHAM, A. und A. KARMOUCH: *Mobile Software Agents: An Overview*. IEEE Communications Magazine, 7(36):26–37, 1998.

[Pico 99] PICOT, A.: *Das Märchen vom papierlosen Büro*. IM Information Management & Consulting, 14(2):100, 1999.

[Pige 01] PIGER, STEFAN: *Konzepte zur Realisierung von dynamischen Virtual Leased Lines mit Hilfe von RSVP*. Diplomarbeit, Technische Universität Braunschweig, Braunschweig, Januar 2001, http://www.rvs.uni-hannover.de/people/piger/da/Diplomarbeit.html.

[PiQu 01] PICOT, ARNOLD und HANS-PETER QUADT: *Verwaltung ans Netz!* Springer, 2001.

[Pohl 99] POHLHEIM, H.: *Evolutionäre Algorithmen - Verfahren, Operatoren, Hinweise aus der Praxis*. Springer-Verlag, Berlin, Germany, 1999.

[PoSt 01] POWELL, DAVID und ROBERT STROUD: *Conceptual Modell and Architecture*. Deliverable D2, EU Project IST-1999-11583 Malicious- and Accidental-Fault Tolerance for Internet Applications (MAFTIA), November 2001.

[Pren 98] PRENEEL, BART: *The State of Cryptographic Hash Functions*. In: DAMGÅRD, IVAN [Damg 98], Seiten 158–182.

[PRS+ 01] PFITZMANN, BIRGIT, JAMES RIORDAN, CHRISTIAN STÜBLE, MICHAEL WAIDNER und ARND WEBER: *The PERSEUS System Architecture*. In: FOX, DIRK, MARIT KÖHNTOPP und ANDREAS PFITZMANN (Herausgeber): *VIS 2001, Sicherheit in komplexen IT-Infrastrukturen*, DuD Fachbeiträge, Seiten 1–18. Vieweg Verlag, 2001.

[PRW 03] PICOT, A., R. REICHWALD und R.T. WIGAND: *Die grenzenlose Unternehmung – Information, Organisation und Management, Lehrbuch zur Unternehmensführung im Informationszeitalter*. Gabler (Wiesbaden), 5. Auflage, 2003.

[PSF+ 00] PAUKENS, H., A. SCHÜMCHEN, J. FLASDIEK, C. HALBACH und D. BROCKMEYER: *Digitales Fernsehen in Deutschland*. Verlag Fischer (Reinhard), München, 2000.

[PSWW 00] PFITZMANN, ANDREAS, ALEXANDER SCHILL, ANDREAS WESTFELD und GRITTA WOLF: *Mehrseitige Sicherheit in offenen Netzen*. Vieweg, 2000.

[PtNe 98] PTACEK, THOMAS H. und TIMOTHY N. NEWSHAM: *Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection*. Technischer Bericht, Secure Networks, Inc., Suite 330, 1201 5th Street S.W, Calgary, Alberta, Canada, T2R-0Y6, Januar 1998.

[PW 02] PC-WELT: *Seagate: Bald 100 mal mehr Daten auf einer Festplatte?* Online, 27. August 2002, `http://www.idg.net/german/crd_auf_942844.html` .

[Rahm 99a] RAHM, E.: *Parallele Datenbanksysteme*, Oktober 1999, `http://www.informatik.uni-leipzig.de/ifi/abteilgungen/db/` .

[Rahm 99b] RAHM, E.: *Parallele Datenbanksysteme*, Oct 1999, `http://www.informatik.uni-leipzig.de/ifi/abteilungen/db` .

[Ramb 03] RAMBUS INCORPORATED: *Rambus RDRAM Overview*, 2003, `http://www.rambus.com` .

[RaSc 99] RANTZAU, R. und H. SCHWARZ: *A Multi-Tier Architecture for High-Performance Data Mining*. In: *Datenbanksysteme in Büro, Technik und Wissenschaft*. v.A. Buchmann, GI-Fachtagung BTW99, Freiburg, 1999.

[Rath 02] RATHJE, U.: *Technisches Konzept für die Datenarchivierung im Bundesarchiv*. Der Archivar, 55(2):117–120, 2002, `http://www.archive.nrw.de/archivar/2002-02/heft2_02_s117_126.pdf` .

[Raus 01] RAUSCH, A.: *Componentware Methodik des evolutionären Architekturentwurfs*. Doktorarbeit, Technische Universität München, 2001.

[Reic 02] REICHWALD, R.: *Mobile Kommunikation – Wertschöpfung, Technologien, neue Dienste*. Gabler, 2002.

[RePo 97] RECHENBERG, P. und G. POMBERGER: *Informatik-Handbuch*. Carl Hanser Verlag, 1997.

[Rink 98] RINK, J.: *Quäntchen für Quäntchen*. c't, 16:150–154, 1998.

[RiPo 01] RIEFFEL, ELEANOR und WOLFGANG POLAK: *An Introduction to Quantum Computing for Non-Physicists*. ACM Computing Surveys, 32(3):300–335, 2001.

[Rive 92] RIVEST, R.: *RFC 1321: The MD5 Message-Digest Algorithm*. April 1992, `ftp://ftp.internic.net/rfc/rfc1321.txt`,`ftp://ftp.math.utah.edu/pub/rfc/rfc1321.txt` . Status: INFORMATIONAL.

[RMF 02] REICHWALD, R., R. MEIER und N. FREMUTH: *Mobile Kommunikation – Wertschöpfung, Technologien, neue Dienste*, Kapitel Die mobile Ökonomie – Definition und Spezifika. Gabler, 2002.

[RMSE 00] REICHWALD, R., K. MÖSLEIN, H. SACHENBACHER und H. ENGLBERGER: *Telekooperation – Verteilte Arbeits- und Organisationsformen*. Springer-Verlag, Berlin, Germany, 2000.

[Robi 99] ROBIE, J.: *The Design of XQL*, Mar 1999, `http://ibiblio.org/xql/xql-design.html` .

[RoHo 98] ROTHERMEL, K. und F. HOHL (Herausgeber): *Mobile Agents (MA '98)*, Band 1477 der Reihe *LNCS*. Springer-Verlag, Berlin, Germany, 1998.

[Roth 02] ROTH, J.: *Mobile Computing: Grundlagen, Technik, Konzepte*. dpunkt-Verlag, Heidelberg, 2002.

[RPM 97] RANNENBERG, KAI, ANDREAS PFITMANN und GÜNTER MÜLLER: *Sicherheit, insbesondere mehrseitige IT-Sicherheit*. In: G. MÜLLER, A. PFITZMANN (Herausgeber): *Mehrseitige Sicherheit in der Kommunikationstechnik*, Seiten 21–29. Addison-Wesley, 1997.

[RRTS 02] RAO, JOSYULA R., PANKAJ ROHATGI, STEPHANE TINGUELY und HELMUT SCHERZER: *Partitioning Attacks: Or How to Rapidly Clone Some GSM Cards*. Seiten 31–41, 2002.

[RSA 78] RIVEST, RON L., ADI SHAMIR und LEONARD M. ADLEMAN: *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*. Communications of the ACM, 21(2):120–126, Februar 1978.

[Rubi 01] RUBIN, AVIEL D.: *White-Hat Security Arsenal Tackling the Threats*. Addison-Wesley, 2001.

[Sach 88] SACHS, L.: *Statistische Methoden*. Springer-Verlag, Berlin, Germany, 1988.

[Sage 03] SAGEM: *Sagem DECT-GSM*. Online, März 2003, `http://www.cellular-news.com/cell-phones/Sagem_DECT-GSM.shtml`.

[SAP 02] SAP: *SAP DB - the Open Source Database of SAP AG*, Feb 2002, `http://www.sapdb.org/pdf/backsapdb_eng.pdf`.

[SaSt 01] SADEGHI, AHMAD-REZA und MICHAEL STEINER: *Assumptions Related to Discrete Logarithms: Why Subtleties Make a Real Difference*. In: PFITZMANN, BIRGIT (Herausgeber): *Advances in Cryptology – EUROCRYPT '2001*, Band 2045 der Reihe *Lecture Notes in Computer Science*, Seiten 243–260, Innsbruck, Austria, 2001. Springer-Verlag, Berlin, Germany.

[Schü 01] SCHÜTT, P.: *Wissensmanagement: Mehrwert durch Wissen*. Falken, 2001.

[Scha 00] SCHARF, A.: *IP wird Universalprotokoll: Durchgängige Kommunikation vom Breitband zum lokalen Netz*. Monitor, 12, 2000, `http://www.monitor.co.at/index.cfm?issueid=127&rubid=6`.

[ScHe 99] SCHUMANN, MATTHIAS und THOMAS HESS: *Medienunternehmen im digitalen Zeitalter. Neue Technologien - Neue Märkte - Neue Geschäftsansätze.* Gabler, 1999.

[Sche 02a] SCHEIBL, H.-J.: *Datenbanken für das Internet*. Hanser, 2002.

[Sche 02b] SCHERZER, H. ET. AL.: *Application Interface for Smart Cards used as Secure Signature Creation Devices*. working draft, eEurope Smart Card (eESC), Januar 2002, `http://www.eeurope-smartcards.org/B2-Index.htm`.

[Schi 97] SCHIFFER, S.: *Visuelle Programmierung: Grundlagen, Potentiale und Grenzen*. Doktorarbeit, Johannes Kepler Universität Linz, 1997.

[Schl 02] SCHLOBINSKI, S., HELL, T.: *Referenzimplementierung eines Münz-basierten, anonymen Zahlungssystem auf dem iPAQ*. In: *Technical Report 02013*. Sirrix AG, Saarbrücken, 2002.

[Schm 01] SCHMIDT, CHRISTIAN: *Hacking Systems*. In: *ix Magazin für professionelle Informationstechnik Ausgabe 12/01*, Dezember 2001.

[Schn 91] SCHNORR, CLAUS P.: *Efficient Signature Generation by Smart Cards*. Journal of Cryptology, 4(3):161–174, 1991.

[Schn 96] SCHNEIER, BRUCE: *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. John Wiley & Sons, Second Auflage, 1996.

[Schn 98] SCHNEIDER, H.-J.: *Lexikon der Informatik und Datenverarbeitung*. Oldenbourg, 4. Auflage, 1998.

[Schu 02] SCHULZE, JAN: *Leasen oder nicht leasen*. Online, 2002, http://www.computerwoche.de/index.cfm?pageid=254&artid=39470&type=detail.

[Send 01] SENDEREK, RALPH: *How PGP Deals with Manipulated keys*. In: *Datenschutz und Datensicherheit (DuD) 10/2000*. Vieweg, Wiesbaden, 2001.

[SETIK 00] BROY, M., A. BUTTERMANN, F. GEHRING, M. GARSCHHAMMER, H.-G. HEGERING, H. KELTER, A. PICOT, M. ULLMANN und S. VOGEL: *Kommunikations- und Informationstechnik 2010: Trends in Technologie und Markt*. SecuMedia Verlag, Ingelheim, 2000.

[SGG+ 02] STUCKI, D., N. GISIN, O. GUINNARD, G. RIBORDY und H. ZBINDEN: *Quantum Key Distribution Over 67 km With a Plug&Play System*. New Journal of Physics, (4):41.1–41.8, Juli 2002, http://www.idquantique.com/files/njp-2002.pdf.

[Shan 49] SHANNON, C. E.: *Communication Theory of Secrecy Systems*. Bell System Technical Journal, 28:656–715, Oktober 1949.

[SHM 02] STANIFORD, S., J. HOAGLAND und J. MCALERNEY: *Practical Automated Detection of Stealthy Portscans*. Journal of Computer Security, 10(1/2), 2002.

[Shor 97] SHOR, PETER W.: *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*. SIAM Journal on Computing, 26(5):1484–1509, 1997.

[Shou 97] SHOUP, VICTOR: *Lower Bounds for Discrete Logarithms and Related Problems*. In: FUMY, WALTER (Herausgeber): *Advances in Cryptology – EUROCRYPT '97*, Band 1233 der Reihe *Lecture Notes in Computer Science*, Seiten 256–266. International Association for Cryptologic Research, Springer-Verlag, Berlin, Germany, 1997.

[Shou 98] SHOUP, VICTOR: *Why Chosen Ciphertext Security Matters*. Research Report RZ 3076 (#93122), IBM Research, November 1998.

[SIA 01] SEMICONDUCTORS INDUSTRY ASSOCIATION: *The National Technology Roadmap for Semiconductors 2001*, http://www.cs.utah.edu/~map/itrs/r1042.pdf.

[Sieg 03] SIEGMUND, G.: *ATM- Die Technik. Grundlagen, Netze, Schnittstellen, Protokolle*. Hüthig-Verlag, 2003.

[Siet 99] SIETMANN, R.: *Nummernspiele*. c't, 9:180–191, 1999.

[Sing 99] SINGH, SIMON: *The Code Book — The Secret History of Codes and Codebreaking*. Fourth Estate Ltd., London, UK, 1999.

[SIR 02] STUBBLEFIELD, ADAM, JOHN IOANNIDIS und AVIEL D. RUBIN: *Using the Fluhrer, Mantin, and Shamir Attack to Break WEP*. In: *Proceedings of the Symposium on Network and Distributed Systems Security (NDSS 2002)*, San Diego, CA, Februar 2002. Internet Society, http://www.isoc.org/isoc/conferences/ndss/02/proceedings/papers/stubbl.pdf.

[SOAP 03] W3C: *Simple Object Access Protocol (SOAP) 1.1*, 2003, http://www.w3.org/TR/SOAP/.

[Somm 92] SOMMERVILLE I.: *Software Engineering*. Addison-Wesley, 1992.

[SOR 93] SHANKAR, N., S. OWRE und J. M. RUSHBY: *A Tutorial on Specification and Verification Using PVS*. Preliminary Draft, Csl report, SRI International, Menlo Park, CA, USA, Februar 1993.

[Stal 98] STALLINGS, WILLIAM: *Cryptography & Network Security: Principles & Practice*. Prentice Hall International, 2nd edition Auflage, 1998.

[Stie 99] STIELER, W.: *Aus dem Reagenzglas, Plastik wird die Computertechnik verändern*. c't, 2, 1999.

[Stil 99a] STILLER, A.: *Prozessorgeflüster, Intels Weg zu 64 Bit*. c't, 12:28, 1999.

[Stil 99b] STILLER, A.: *Titanomachie, Microprocessor Forum 1999*. c't, 22:16–20, 1999.

[Stil 01] STILLER, A.: *Intel erobert die Tera-Hertzen*. Heise Online, 26.11.2001 2001, http://www.heise.de/newsticker/data/as-23.11.01-000/ .

[Stür 90] STÜRNER, G.: *Oracle Version 6.0. Die Datenbank für OLTP – Applikationen im Multi-User-Bereich*, 1990.

[StSa 03] STÜBLE, CHRISTIAN und AHMAD-REZA SADEGHI: *Bridging the Gap between TCPA/Palladium and Personal Security*. Technical Report TR03-011, Computer Science Department, Saarland University, Januar 2003.

[Stum 02] STUMM, B.: *Das Semantic Web - Ontologien, RDF, DAML+OIL*, Jan 2002, http://www.dbis.informatik.uni-kl.de/courses/seminar/WS0102/ausarbeitung3.pdf .

[Sun 99] SUN MICROSYSTEMS INCORPORATED: *Jini Connection Technology*, November 1999, http://www.sun.com/jini/ .

[Sun 02a] SUN MICROSYSTEMS INCORPORATED, 2002, http//java.sun.com/getjava .

[Sun 02b] SUN MICROSYSTEMS INCORPORATED: *Java Beans - The Only Component Architecture for Java Technology*, 2002, http://www.sun.com/products/javabeans/ .

[Sun 02c] SUN MICROSYSTEMS INCORPORATED: *The Java Virtual Machine Specification*, 2002, http://java.sun.com/docs/books/vmspec .

[Sun 03a] SUN MICROSYSTEMS GMBH: *Neue Business-Server*. Online, 2003, http://www.sun.de/Homepage/aktuell/2003/Business-Server/ .

[Sun 03b] SUN MICROSYSTEMS INCORPORATED: *Enterprise JavaBeans Technology*, 2003, http://java.sun.com/products/ejb/ .

[Sun 03c] SUN MICROSYSTEMS INCORPORATED: *Java 2 Platform, Enterprise Edition (J2EE) – Introduction*, 2003, http://java.sun.com/j2ee/ .

[Sun 03d] SUN MICROSYSTEMS INCORPORATED: *Sun ONE Studio 4 Update 1*, 2003, http://www.sun.de/Produkte/software/sundev/jde/general.html .

[Szyp 98] SZYPERSKI, C.: *Component Software Beyond Object-Oriented Programming*. Addison-Wesley, 1998.

[TaGo 99] TANENBAUM, A. und J. GOODMAN: *Computerarchitektur*. Prentice-Hall, 4. Auflage, 1999.

[TCPA 03] TCPA: *Trusted Computing Platform Alliance*. 2003, http://www.trustedcomputing.org .

[Tecm 99] TECMATH: *Digitales – On Demand*, November 1999, http://www.tecmath.de/news/medien_bulletin_12_97.html .

[Texa 99] TEXAS INSTRUMENTS: *TI demonstrates First Digital High-Definition Display System Based on Digital Micromirror Device (DMD) Technology*, November 1999, http://www.ti.com/corp/docs/press/company/1994/405asc.html .

[Thie 00] THIEL G.: *Komponentenmodelle DCOM, Javabeans, Enterprise Java Beans, CORBA*. Addison-Wesley, 2000.

[TKZ 02] THALHEIM, LISA, JAN KRISSLER und PETER-MICHAEL ZIEGLER: *Körperkontrolle — Biometrische Zugangssicherungen auf die Probe gestellt*. c't, (11):114, Mai 2002.

[Tsud 92] TSUDIK, GENE: *Message Authentication with One-Way Hash Functions*. In: *IEEE Infocom 1992*, Seiten 2055–2059, 1992.

[UKK 01] ULLMANN, MARKUS, FRANK KOOB und HARALD KELTER: *Anonyme Online-Wahlen - Lösungsansätze für die Realisierung von Online-Wahlen*. In: *Datenschutz und Datensicherheit (DuD) 11/2001*. Vieweg, Wiesbaden, 2001.

[UMTS 00] UMTS FORUM: *Enabling UMTS Third Generation Services and Applications*. UMTS Report 11, UMTS Forum, London, 2000.

[UMTS 01] UMTS FORUM: *The UMTS Third Generation Market Phase II: Structuring the Service Revenue Opportunities*. UMTS Forum 13, UMTS Forum, London, 2001.

[Univ 99] UNIVERSITÄT MÜNSTER: *Universelle Datenbanksysteme*, Dezember 1999, `http://wwwmath.uni-muenster.de/informatik/u/dbis/Vossen/Lehre/udbs9901.ps`.

[Vils 02] VILSBECK, CHRISTIAN: *Prozessortrends 2003*, Oktober 2002, `http://www.tecchannel.de/hardware/1060/index.html`.

[Vita 01] VITAÁNAYI, PAUL: *The Quantum Computing Challenge*. In: WILHELM, REINHARD (Herausgeber): *Informatics – 10 Years Back, 10 Years Ahead*, Band 2000 der Reihe *Lecture Notes in Computer Science*, Seiten 218–233. Springer-Verlag, Berlin, Germany, 2001.

[VoPa 03] VOSCHKE, T.U. und L.-M. U. PANGALOEW: *How to Cope With Serious Restrictions and Uncertainty*. Experiences in Delphi Studies, 3(1), 2003.

[Voss 00] VOSS, A.: *Das große PC & Internet Lexikon 2000*. Data Becker, 2000.

[VoVo 02] VOSSBEIN, R. und J. VOSSBEIN: *Lagebericht zur IT-Sicherheit*. In: *Management und Wissen - KES/KPMG-Sicherheitsstudie*, 2002.

[Wagn 83] WAGNER, N.: *Fingerprinting*. In: *Proceedings of the IEEE Symposium on Research in Security and Privacy*, Seiten 18–22, Oakland, CA, 1983. IEEE Computer Society, Technical Committee on Security and Privacy, IEEE Computer Society Press.

[Walk 98] WALKE, B.: *Mobilfunknetze und ihre Protokolle, Band 2*. Teubner-Verlag, Stuttgart, 1998.

[Walk 00] WALKER, MICHAEL: *On the Security of 3GPP Networks*. Lecture Notes in Computer Science, 1807:102–114, 2000, `http://link.springer-ny.com/link/service/series/0558/bibs/1807/18070102.htm;http://link.springer-ny.com/link/service/series/0558/papers/1807/18070102.pdf`.

[Webe 01] WEBER, FRED: *AMD's Next Generation Microprocessor Architecture*. Online, Oktober 2001, `http://www.amd.com/us-en/assets/content_type/DownloadableAssets/MPF_Hammer_Presentation.PDF`.

[WeCa 79] WEGMAN, MARK N. und J. LAWRENCE CARTER: *New Classes and Applications of Hash Functions*. In: *Proceedings of the 20th Symposium on Foundations of Computer Science (FOCS)*, Seiten 175–182. IEEE Computer Society Press, 1979.

[Weis 91] WEISER, M.: *The Computer for the 21st Century*. Scientific American, 265(9):66–75, 1991.

[West 03] WESTPHAL, R.: *P2P Computing*. Markt und Technik, München, 2003.

[Will 00] WILLIMOWSKI, I.: *FMC - Konvergenz von Fest- und Mobilfunknetzen*. VDE-Verlag, Berlin und Offenbach, 2000.

[Will 02] WILLIAMS, DMITRI: *Structure and Competition in the U.S. Home Video Game Industry*. The International Journal on Media Management, 4(1):41–54, 2002.

[XML 99] XML.ORG.: *The XML Industry Portal*, November 1999, `http://www.xml.org`.

[Ylön 96] YLÖNEN, T.: *SSH - Secure Login Connections Over the Internet*. In: *Proceedings of the 6th USENIX Security Symposium*, Seiten 37–42, San Jose, California, Juli 1996. USENIX.

[Ylön 01] YLÖNEN, T. ET. AL.: *The SSH-Protocol, current version*. working draft, Internet Engineering Task Force, 2001.

[ZBGK 02] ZUSER, W., S. BIFFL, T. GRECHENIG und M. KÖHLE: *Software Engineering mit UML und dem Unified Process*. Addison-Wesley, 2002.

[ZCC 00] ZWICKY, ELIZABETH D., SIMON COOPER und BRENT D. CHAPMAN: *Building Internet Firewalls*. O'Reilly Associates, 2000.

[Zimm 95] ZIMMERMANN, PHILIP R.: *The Official PGP User's Guide*. MIT Press, Cambridge, MA, USA, 1995. ISBN 0-262-74017-6.

[ZPS 01] ZERDICK, AXEL, ARNOLD PICOT und KLAUS SCHRAPE: *Die Internet-Ökonomie. Strategien für die digitale Wirtschaft*. European Communication Council Report. Springer, 3. Auflage, 2001.