

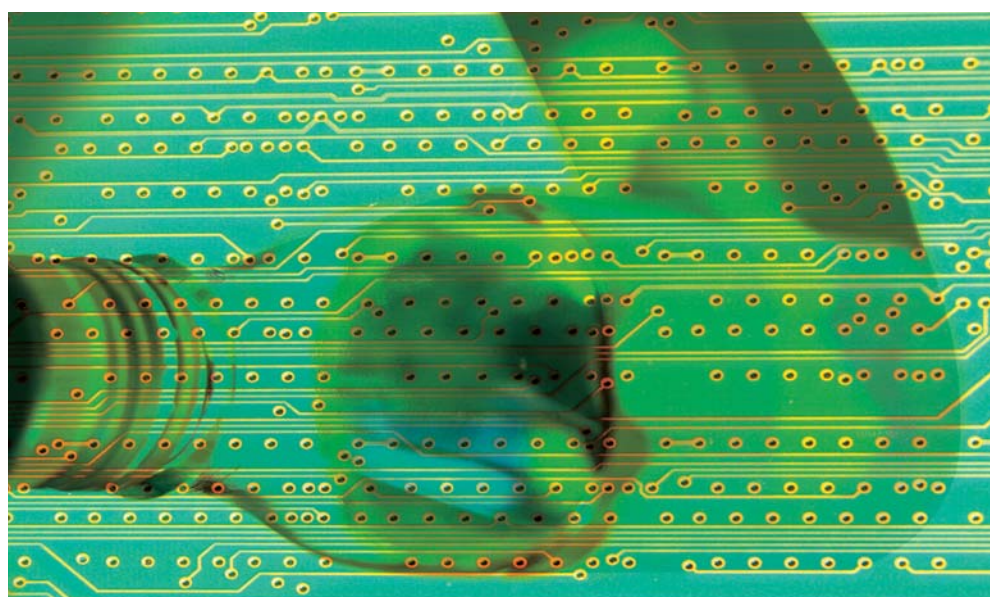
FAZIT
Forschung

Schriftenreihe

Informations- und Medientechnologien in Baden-Württemberg

Irene Bertschek, Thomas Döbler (Hrsg.)

Open Source Software und IT-Sicherheit
Unternehmensbefragung Frühjahr 2005
in Baden-Württemberg



Irene Bertschek, Thomas Döbler (Hrsg.)

Open Source Software und IT-Sicherheit

Unternehmensbefragung Frühjahr 2005 in Baden-Württemberg

Impressum

Herausgeber der FAZIT-Schriftenreihe:

MFG Stiftung Baden-Württemberg
Breitscheidstr. 4, D-70174 Stuttgart
Tel. +49 (0)711/90715-300, Fax +49 (0)711/90715-350

Zentrum für Europäische Wirtschaftsforschung GmbH (ZEW)
L 7,1, D-68161 Mannheim
Tel. +49 (0)621/1235-01, Fax +49 (0)621/1235-224

Fraunhofer-Institut für System- und Innovationsforschung (Fraunhofer ISI)
Breslauer Straße 48, D-76139 Karlsruhe
Tel. +49 (0)721/6809-0, Fax +49 (0)721/689152

Schutzgebühr € 8,-

© MFG Stiftung Baden-Württemberg, Juli 2005 – www.fazit-forschung.de

Inhaltsverzeichnis

EINFÜHRUNG

Das Projekt FAZIT:

Forschung zu Informations- und Medientechnologien in Baden-Württemberg5

Thomas Döbler

UNTERNEHMENSBEFRAGUNG FRÜHJAHR 2005

Open Source Software und IT-Sicherheit:

Ergebnisse der ersten FAZIT-Unternehmensbefragung15

Irene Bertschek, Jörg Ohnemus

SEKUNDÄRANALYSEN

Open Source Software61

Jörg Ohnemus

IT-Sicherheit in Unternehmen81

Katrin Schleife, Oliver Schmid

ANHANG

Über die Autoren101

Über das Projekt FAZIT102

Über die Partnerinstitutionen103

Das Projekt FAZIT: Forschung zu Informations- und Medientechnologien in Baden-Württemberg

Thomas Döbler

1. Ausgangspunkt und Zielsetzung der ersten FAZIT-Unternehmensbefragung.....	7
2. Ergebnisse der ersten FAZIT-Unternehmensbefragung.....	8
2.1. Open Source Software.....	9
2.2. IT-Sicherheit.....	9
3. FAZIT – Was ist das?.....	10
4. Literatur.....	14

1. Ausgangspunkt und Zielsetzung der ersten FAZIT-Unternehmensbefragung

Die rasanten Entwicklungen im Bereich der Informations- und Kommunikationstechnologien (IKT) sorgen nicht nur in den Branchen der Informations- und Medienwirtschaft für weiter ungebremste Dynamik und Veränderung, sondern sind auch in zahlreichen Anwenderbranchen des industriellen und Dienstleistungssektors ein Treiber für Innovation und das Entstehen neuer Marktpotenziale. Unbestritten ist IKT derzeit die grundlegende Triebfeder für Wirtschafts- und Beschäftigtenwachstum und damit im nationalen und internationalen Wettbewerb entscheidend für den Wohlstand von Regionen. FAZIT, das *Forschungsprojekt für aktuelle und zukunftsorientierte Informations- und Medientechnologien und deren Nutzung in Baden-Württemberg*, startete mit der ersten von acht repräsentativ angelegten Unternehmensbefragungen seine Untersuchung zu Bedeutung und Potenzialen von IKT in der baden-württembergischen Wirtschaft.

Im April und Mai 2005 wurde einer Zufallsstichprobe von rund 9000 baden-württembergischen Unternehmen aus Anbieter- und Anwenderbranchen von IKT¹ ein standardisierter Fragebogen per Post zugesandt: Neben allgemein konjunkturellen Bewertungen und Einschätzungen, die in jeder der halbjährlichen Befragungswellen erhoben werden, stehen regelmäßig Fragen zur Computer- und Internetnutzung, allerdings mit variierenden Schwerpunkten, im Zentrum. Schwerpunktthemen bei dieser ersten Befragung waren Open Source Software (OSS) und IT-Sicherheit; diese wurden vor allem deshalb gewählt, da neben den Ergebnissen der Sekundäranalysen in den Vorstudien insb. IT-Firmen und -Entwickler den beiden Themen eine wachsende Bedeutung zuschreiben. OSS, entstanden als Reaktion auf die Begrenzungen und Beschränkungen, die mit proprietärer Software oftmals verbunden sind, erfreut sich in den letzten Jahren einer zunehmenden Beliebtheit.² Der sekundäranalytisch angelegte Beitrag von Jörg Ohnemus in diesem Band („Open Source Software“) führt u.a. die Unterschiede zwischen proprietärer und offener Software genauer aus. Zentral ist, dass durch die Offenlegung des Quellcodes bei OSS, Interessierte und Anwender die Möglichkeit haben, die Software weiterzuentwickeln und gewünschte Anpassungen vorzunehmen.³ Damit werden IT-Anwender unabhängiger von Lizenzgebern und der teils restringierenden Lizenzvergabe; zudem entfallen auch Lizenzgebühren⁴ und die gewünschten Softwareanpassungen können, entsprechendes technisches Know-How vorausgesetzt, selbst vorgenommen werden. Da der Einsatz von OSS sich vielfach allein schon unter Kostengesichtspunkten als vorteilhaft erweist, hat diese offene Software nicht nur bei privaten Nutzern und öffentlichen Verwaltungen, dies belegen etwa die Umstellungen von Windows auf Linux, an Attraktivität gewonnen, sondern stößt auch bei

¹ Vgl. zu den untersuchten Branchen des Informations- und Mediensektors sowie der Anwenderbranchen den nachfolgenden Beitrag von Bertschek und Ohnemus.

² Vgl. hierzu u.a. Maass und Scherm 2005, S. 161 ff.

³ Dass OSS „frei“ ist, meint nicht, dass es an OSS keine Urheberrechte gäbe, die urheberrechtliche Verwertungsrechte werden jedoch verwendet, um den Nutzer Pflichten aufzuerlegen, die zur kostenfreien Weitergabe und Offenlegung des Quellcodes führen (vgl. u.a. Weber 2000, S. 2 ff.).

⁴ Vgl. hierzu ausführlich Spindler 2005, S. 14 ff.

Unternehmen verstärkt auf Interesse und Nutzungsbereitschaft. Handelt es sich bei OSS noch um ein vergleichsweise innovatives Thema für Unternehmen, steht das zweite Thema, IT-Sicherheit, dagegen seit geraumer Zeit schon auf deren Agenda.⁵ Die Studien, die von Katrin Schleife und Oliver Schmid zusammenfassend in diesem Band vorgestellt werden („IT-Sicherheit in Unternehmen“ ab S.87) belegen gleichwohl, dass auch die IT-Sicherheit in vielen Unternehmen stiefmütterlich behandelt wird. Dass etwa das Firmenmanagement gesetzlich für Schäden, die beispielsweise durch Hacker, Viren oder Datendiebstahl entstehen, zur Verantwortung gezogen werden kann – teilweise sogar mit dem Privatvermögen – ist den Führungskräften noch wenig bewusst. Zudem wird der Blick für IT-Sicherheit erst allmählich in der notwendigen Weise erweitert: Lange wurde nämlich IT-Sicherheit ausschließlich mit Sicht auf externe Bedrohungen wie Computerviren, Würmer, Trojanische Pferde und Hacker betrachtet, die interne, beispielsweise von Mitarbeitern ausgehende Gefahr aber vernachlässigt.

Beide Themen beinhalten somit unverändert ein hohes Maß an Brisanz und Aktualität und es ist davon auszugehen, dass deren Bedeutung eher noch weiter steigt. Jedenfalls eröffnen sie Anbietern und Anwendern zahlreiche Chancen: Chancen für Kosteneinsparungen, für persönliche und unternehmerische Sicherung vor Schadensfällen, für Wettbewerbsvorteile, für Wachstum und neue IT-Entwicklungen. Ob und inwieweit diese Chancen bereits in der baden-württembergischen Wirtschaft genutzt werden, war Zielsetzung der ersten FAZIT-Unternehmensbefragung.

2. Ergebnisse der ersten FAZIT-Unternehmensbefragung

Die 603 auswertbaren Fragebögen liefern, empirisch abgesichert und statistisch hochgerechnet, eine ganze Palette an Ergebnissen, die interessante Interpretationen und politisch wie ökonomisch wertvolle Schlussfolgerungen mit Differenzierungen nach Unternehmensgröße und Branche zulassen. In dem Beitrag von Bertschek und Ohnemus werden die Ergebnisse der ersten FAZIT Unternehmensbefragung ausführlich vorgestellt und diskutiert.

Der IT- und Mediensektor hat sich als bedeutende Triebfeder in der baden-württembergischen Wirtschaft etabliert. Insgesamt sind 8,6 Prozent aller Unternehmen in Baden-Württemberg dem IT- und Mediensektor zuzurechnen und erwirtschaften 7,4 Prozent des Umsatzes (siehe auch Abbildung 1, S. 19). Laut der ersten FAZIT-Unternehmensbefragung rechnen rund 38 Prozent der befragten Unternehmen im dritten Quartal 2005 mit einer besseren Geschäftslage im Vergleich zum ersten Quartal. In den Branchen Chemie, Maschinenbau, Medizin-, Mess-, Steuer- und Regelungstechnik, Automobil, Verkehr, Bank- und Versicherungsgewerbe und technische Dienstleistungen geht dagegen nur jedes vierte Unternehmen mit diesem Optimismus in die nächsten Monate. Diese Zuversicht des IT- und Mediensektors findet sich durch die für 2005 geplanten Investitionen in Informations- und Kommunikationstechnologien durchaus gestützt:

⁵ Vgl. ausführlich Ecker 2005.

Denn zumindest Unternehmen mit 250 und mehr Beschäftigten beabsichtigen – branchenübergreifend – ihre Investitionstätigkeit in IKT in diesem Jahr gegenüber dem Vorjahr zu steigern. Die Durchdringung des Arbeitsalltages mit Informations- und Kommunikationstechnologien ist insgesamt in den untersuchten baden-württembergischen Branchen weit fortgeschritten; vor allem in den Branchen des IT- und Mediensektors, aber auch im Bank- und Versicherungsgewerbe sowie bei den technischen Dienstleistern liegt der Anteil der Beschäftigten, die den überwiegenden Anteil ihrer Arbeit am Computer verrichten, zwischen 80 und 90 Prozent, wobei branchenübergreifend die häufigsten Anwendungen im Bereich der Büro- und Kommunikationssoftware liegen.

2.1. Open Source Software

Über alle untersuchten Branchen hinweg nutzt bereits fast jedes fünfte Unternehmen in Baden-Württemberg OSS; überdurchschnittliche Verbreitung findet sich dabei neben der Informations- und Medienbranche vor allem auch bei Unternehmen des Bank- und Versicherungsgewerbes. Sehr deutlich lässt sich ein Zusammenhang zwischen der Unternehmensgröße und der Nutzung von OSS belegen: Mit zunehmender Unternehmensgröße wird auch OSS häufiger genutzt. Dieses Ergebnis überrascht zunächst angesichts der genannten Kostenvorteile von OSS gegenüber proprietärer Software. Zu erwarten wäre gewesen, dass gerade kleinere Unternehmen verstärkt die mit dem Einsatz von OSS verbundenen Kostenvorteile nutzen⁶. Der Widerspruch erklärt sich bei genauerer Analyse durch ein teils großes Informationsdefizit, was vor allem kleine Unternehmen betrifft; anders als größere Unternehmen mit ihren eigenen EDV-Abteilungen, sind sie nämlich mit den Möglichkeiten und den Vorteilen von OSS kaum vertraut. Da bestehende Lizenzverträge nur bei einer Minderheit der Firmen, dagegen mangelndes Know-How im Umgang mit OSS ein wichtiges Hemmnis für den Einsatz von OSS im Unternehmen sind, eröffnet sich hier ein noch wenig bearbeitetes Feld mit zahlreichen Chancen für die IT-Firmen und -Entwickler, die aufgedeckten Informations- und Know-How-Defizite bei kleineren Firmen systematisch zu beseitigen.

Darüber hinaus zeigen sich grundsätzlich Entwicklungspotenziale für IT-Firmen, aber auch für -Berater im Bereich der Einsatzmöglichkeiten von OSS: denn OSS wird vor allem bei den Internetanwendungen und – schon deutlich abgeschwächt – noch bei den Serverbetriebssystemen eingesetzt. Im Bereich der Datenbanken, der Softwareentwicklung oder der Bürosoftware, aber auch der Sicherheit scheinen dagegen zahlreiche Einsatzmöglichkeiten noch ungenutzt brach zu liegen.

2.2. IT-Sicherheit

Um IT-Sicherheit scheinen sich bei einem ersten Blick auf die Daten nahezu alle Unternehmen zu kümmern. Allerdings zeigt eine genauere Analyse, dass sich das Sicherheitsverständnis

⁶ Ob und inwieweit kleine Unternehmen Kostenvorteile von OSS realisieren können, wird widersprüchlich behandelt. Einerseits ist OSS in der Regel kostengünstiger als proprietäre Software, setzt aber andererseits ein Mindestmaß an Software-Know-How voraus.

oftmals auf den Einsatz von Virenschutzprogrammen beschränkt. Dass schon auf den Einsatz von Firewalls jedes fünfte Unternehmen verzichtet, belegt auch bei dieser Thematik, dass auf Anwenderseite noch beträchtlicher Nachholbedarf – damit gleichzeitig aber Geschäftschancen für IT-Anbieter – besteht. Was den Datenverlust durch Viren, Trojaner oder Würmer im Zeitraum von Anfang 2004 bis zum Befragungszeitpunkt angeht, schneidet der Informations- und Mediensektor bei einem Branchenvergleich am besten ab. In den Anwenderbranchen hatte im betrachteten Zeitraum ein deutlich höherer Anteil an Unternehmen Datenverluste zu verzeichnen. So war im verarbeitenden Gewerbe jedes vierte Unternehmen von Datenverlust betroffen. Unternehmen mit bis zu vier Beschäftigten erlitten fast doppelt so oft wie Unternehmen mit mindestens 250 Beschäftigten einen Datenverlust.

Betrachtet man über den Virenschutz und den Einsatz von Firewalls hinausgehende Sicherheitsmaßnahmen, so zeigt sich, dass nur rund zwei Drittel der Unternehmen Maßnahmen für einen gesicherten Datenzugang einsetzen oder regelmäßig und standardisierte Datensicherungen in Form von Backups vornehmen. Weniger als ein Drittel der Unternehmen verwenden Verschlüsselungsverfahren bei der Datenübertragung. Der Anteil an Unternehmen, die digitale Signaturen einsetzen oder ihre IT-Sicherheitsrichtlinien schriftlich fixiert haben, fällt hierzu nochmals deutlich ab, wobei gerade letztere Maßnahme eher bei größeren Unternehmen eine Rolle spielen dürfte. Nach der Einschätzung des Schutzes durch die getroffenen IT-Maßnahmen gefragt, fühlen sich nur 10 Prozent der Unternehmen "eher schlecht" und weitere zwei Prozent "schlecht" geschützt. Diese Ergebnisse deuten darauf hin, dass die IT-Sicherheit in den Unternehmen nicht immer die notwendige Aufmerksamkeit zu genießen scheint. IT-Sicherheit stellt keine einmalige Angelegenheit dar, sondern ist kontinuierlich und immer wieder aufs Neue ein Brennpunkt in den Unternehmen ist: Maßnahmen und Instrumente zum Schutz der Firmendaten sind ständig und stetig zu prüfen, zu aktualisieren und anzupassen, um den steigenden Risiken und Gefährdungen gewachsen zu sein. Schließlich kann mangelnde IT-Sicherheit nicht nur zu materiellen Schäden, sondern auch zu immateriellen Schädigungen in Form von Image- oder Vertrauensverlust führen. Um auch bei knapper werdenden und rückläufigen IT-Budgets IT-Sicherheitsmaßnahmen in der erforderlichen Breite erbringen zu können, bieten sich nun wiederum vermehrt der Einsatz und die Anwendung von OSS an. Für IT-Firmen, -Entwickler und -Berater eröffnen sich hier eine Fülle an geschäftlich nutzbaren Betätigungsfeldern, für die IT-Anwender kann dies hohe Sicherheit zum vertretbaren Preis bedeuten.

3. FAZIT – Was ist das?

FAZIT ist ein im Rahmen der Zukunftsoffensive III vom Land Baden-Württemberg gefördertes, auf vier Jahre angelegtes gemeinnütziges Forschungsprojekt der MFG Stiftung Baden-Württemberg zu aktuellen und zukunftsorientierten Informations- und Medientechnologien und deren Nutzung in Baden-Württemberg, das in Kooperation mit den beiden Partnern, dem Zentrum für Europäische Wirtschaftsforschung (ZEW), Mannheim und dem Fraunhofer Institut für Innovations- und Systemforschung (Fraunhofer ISI), Karlsruhe, durchgeführt wird.

Zentrales Ziel des Projekts FAZIT ist es, im Verlauf des Forschungsprozesses, relevante gesellschaftliche, branchenspezifische und technologische Umbrüche sowie Triebkräfte für Innovationen und Arbeitsplätze zu identifizieren, grundlegende Einsichten und Hinweise auf neue Märkte für Informations- und Kommunikationstechnologien zu gewinnen, neue Marktchancen aufzuzeigen und nicht zuletzt durch neue Forschungsthemen Orientierung für Wissenschaft und Wirtschaft gleichermaßen zu schaffen. Um dies zu erreichen, werden dabei aktuelles Monitoring und zukunftsorientierte Forschung in inhaltlich und methodisch innovativer Weise verknüpft; schließlich ist durch die Anlage und Durchführung von FAZIT gewährleistet, dass gewonnene Ergebnisse und erarbeitete Erkenntnisse in die relevanten Zielgruppen aus Wissenschaft, Wirtschaft und Politik transferiert werden. Grundlage für die bis zum Jahr 2020 reichenden Prognosen ist eine umfassende Analyse von Aufbau und Struktur des regionalen IT- und Medienmarkts in Baden-Württemberg sowie der inhärenten Entwicklungslinien und Veränderungskräfte. Angesichts der gewachsenen und weiter wachsenden wirtschaftlichen und gesellschaftlichen Bedeutung des IT- und Medienbereichs und angesichts der zunehmenden Marktdynamik und sich verändernden Absatzmärkten⁷ kommt dem Zugriff auf aktuelle Daten, die eine langfristige Analyse von Rahmenbedingungen und Entwicklungstrends erlauben, eine besondere Wichtigkeit zu. Doch ebenso wie für andere europäische Regionen liegen auch für Baden-Württemberg derartige Daten und Informationen in nur sehr eingeschränktem Maße vor⁸, obwohl kaum bestritten wird, dass die Verfügbarkeit solcher Daten sowohl für Forschung und Entwicklung als auch für innovationspolitische Entscheidungsträger von großer Bedeutung ist. Zu berücksichtigen ist zudem, dass nicht nur die Produktion von IKT von Relevanz ist, sondern insbesondere auch deren Nutzung. Die IKT haben aufgrund ihres Querschnittscharakters weit reichende Konsequenzen auf wirtschafts-, technologie-, bildungs- und gesellschaftspolitische Handlungsfelder. Abgeleitet aus dem übergeordneten Ziel des Forschungsprojekts, aktuelle und zukunftsorientierte IT- und Medientechnologien und deren Nutzung in Baden-Württemberg systematisch zu untersuchen, ergeben sich eine Reihe von Unterziele, die in verschiedenen Modulen bearbeitet werden.

Im Modul „IKT-Monitoring“, das schwerpunktmäßig vom Zentrum für Europäische Wirtschaftsforschung (ZEW), Mannheim verantwortet wird, geht es u.a. darum,

- eine detaillierte und regional fokussierte Bestandsaufnahme des IT- und Medienstandorts in Baden-Württemberg als Status-quo-Analyse durchzuführen;
- fortlaufend Daten über die Nutzung von IT- und Medientechnologien in Baden-Württemberg sowohl auf Anbieterseite als auch auf Nachfragerseite zu erheben. Hierbei werden Determinanten, Ziele und Potenziale, Hemmnis- und Förderfaktoren für die Nutzung von IT- und Medientechnologien analysiert;

⁷ In Baden-Württemberg macht die IT- und Medienwirtschaft mit rund 22.000 Unternehmen (ohne Selbstständige) und mehr als 300.000 Erwerbstätigen rund zehn Prozent der Bruttowertschöpfung aus und übertrifft damit die traditionell starken Segmente Fahrzeug- und Maschinenbau (vgl. Statistisch prognostischer Bericht des Statistischen Landesamt Baden Württemberg 2002, insbesondere S. 99f.).

⁸ So werden die meisten Daten national erhoben, die spezifische regionale Branchenstruktur und die damit verbundenen Auswirkungen auf das Marktumfeld werden damit nur unzureichend abgebildet; die verfügbaren Einzelstudien zu speziellen Regionen oder Teilbranchen sind oftmals diskontinuierlich und wenig vergleichbar, das statistischen Datenmaterial ist eher vergangenheitsorientiert und erfasst mitunter die Branche nur sehr grob.

- eine solide Wissensbasis über die kontinuierliche Entwicklung des IT- und Mediensektors in Baden-Württemberg zu erhalten.

Mittels regelmäßig im Halbjahresrhythmus durchgeführter Umfragen bei Anbietern und Anwendern von IKT sollen einerseits aktuelle Entwicklungen im IKT-Bereich erfasst und andererseits die Komplexität, mit der die Nutzung von IKT verbunden ist, Rechnung getragen werden. Die so gewonnene Datenbasis sowie die darauf aufbauenden Analysen stellen eine solide Wissensbasis für Entscheidungsträger in Wirtschaft, Wissenschaft und Politik auf regionaler Ebene dar. Entscheider aus Wissenschaft und Wirtschaft erhalten eine regelmäßige Übersicht möglicher Entwicklungspfade des IT- und Mediensektors und haben so die Möglichkeit, frühzeitig zu reagieren. Darüber hinaus werden die Interessen der Nachfrager und Anbieter gegenüber gestellt und abgeglichen⁹, womit insb. kleineren und mittleren Unternehmen, die häufig keine Ressourcen für eine kontinuierliche Branchenbeobachtung haben, Informationen über Entwicklungschancen gegeben werden können.

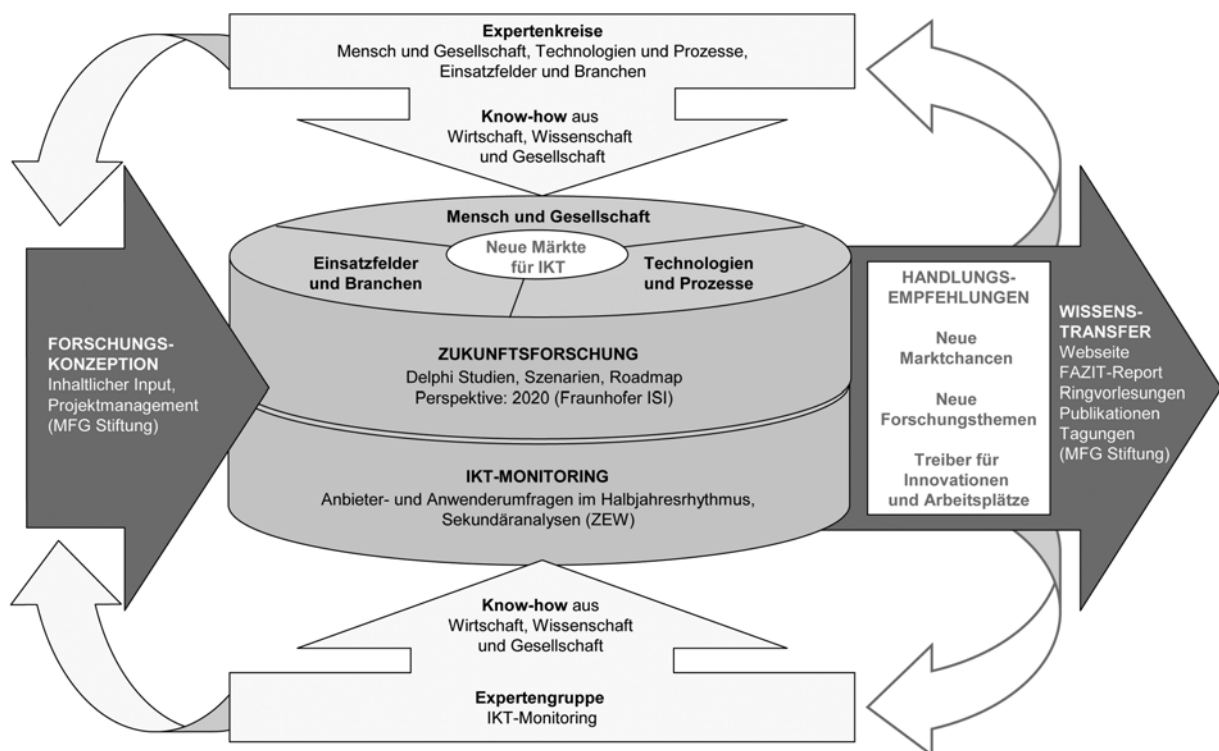
Im Mittelpunkt der Zukunftsforschung, die schwerpunktmäßig vom Fraunhofer ISI, Karlsruhe bearbeitet wird, stehen mögliche Entwicklungspfade von Informations- und Medientechnologien bis 2020 in den Bereichen "Mensch und Gesellschaft" (Leitthema 1), "Technologien und Prozesse" (Leitthema 2) und "Einsatzfelder und Branchen" (Leitthema 3). Diese Leitthemen zur Strukturierung der relevanten Forschungs- und Entwicklungsfelder sind bewusst breit und übergeordnet gehalten, um einen möglichst offenen Rahmen für den Forschungsaustausch zu schaffen. Für jedes Leitthema baut das Forschungsteam eine interdisziplinäre, regionale Experten- und Transfergruppe auf, die über die gesamte Projektlaufzeit betreut wird. Sie setzt sich aus Akteuren der IT- und Medienforschung sowie profunden Branchenkennern in Baden-Württemberg zusammen. Auf diese Weise können die ermittelten Trends der Informations- und Kommunikationstechnologie detailliert und in Bezug zur regionalen Besonderheit des Sektors bewertet, Chancen und Problemfelder aufgezeigt und den Experten aus der Region vermittelt werden. Gemeinsam mit den Experten werden Wirkungsdimensionen und Handlungsbedarf ermittelt. Die Beteiligten übernehmen damit zugleich eine wichtige Rolle im Wissenstransfer. Sie werden die in den Szenario-Analysen und Delphi-Studien¹⁰ erarbeiteten Forschungsergebnisse zurück in ihre Institutionen tragen und somit aktiv im Wissenstransfer mitwirken.

Die Weitergabe der Forschungsergebnisse ist Aufgabe des Wissenstransfers, das ebenso wie die Forschungskonzeption von FAZIT schwerpunktmäßig von der MFG Stiftung Baden Württemberg verantwortet wird. Der Wissenstransfer in die Regionen wird durch die Einbeziehung von Forschern und Wissenschaftlern aus baden-württembergischen Universitäten, Fachhochschulen und Forschungseinrichtungen vorbereitet. Die Beteiligten wirken als Multiplikatoren in ihrem jeweiligen Bereich, um die Forschungsergebnisse an eine möglichst breite Gruppe

⁹ Wechselseitige Informationsdefizite, etwa über die jeweiligen Motive und Probleme oder Bedarfe bei der Anwendung und Nutzung von IKT, be- und verhindern manche Innovationschance.

¹⁰ Insbesondere in volatilen Märkten mit einer so dynamischen Technologieentwicklung wie dem IT- und Mediensektor verwendet man zunehmend Methoden wie Delphi-Studien und Szenario-Analysen, um Produkte und Märkte frühzeitig systematisch zu entwickeln.

weiterzugeben (z.B. Kollegen, Fachpublikum, Nachwuchswissenschaftler, Ausbilder, etc.). Eine thematische Klammer setzt dabei die Wissenschaftskommunikation, die Forschungsinhalte und -ergebnisse für die Zielgruppen aufbereitet und verbreitet. Zusätzlich werden die Ergebnisse des Projekts der Öffentlichkeit mit Hilfe von Publikationen und Veranstaltungen/ Seminaren zielgruppenspezifisch in ganz Baden-Württemberg vermittelt. Der Wissenstransfer stützt sich auf die Ergebnisse der Module IKT-Monitoring und Zukunftsforschung/Foresight. Durch die kontinuierliche Datenerhebung und die laufenden Zwischenergebnisse von Delphi-Studien, Szenarioanalysen und Fachtagungen/Forschungskonferenzen werden periodische Informationsknotenpunkte generiert und ein kontinuierlicher Informationsfluss sichergestellt. Die abschließende, integrierende Maßnahme der Wissenstransfer-Strategie stellt die Abschlusspublikation dar, die zentrale Forschungsergebnisse der gesamten Projektlaufzeit prägnant zusammenfasst. In der nachfolgenden Abbildung werden die verschiedenen Module mit ihren wechselseitigen Verzahnungen sowie der Integration der Experten noch dargestellt:



Der vorliegende Forschungsbericht zu „Open Source und IT-Sicherheit. Unternehmensbefragung Frühjahr 2005 in Baden-Württemberg“ ist der erste Band der FAZIT Schriftenreihe, in denen die Forschungsergebnisse von FAZIT künftig regelmäßig publiziert werden. Es handelt sich in diesem Band um die Ergebnisdarstellung der ersten, im Mai 2005 abgeschlossenen Befragung von baden-württembergischen Anbietern und ausgewählten Anwendern von IKT. Vorgehensweise und Ergebnisse dieser ersten Unternehmensbefragung werden im Beitrag von Bertschek und Ohnemus vorgestellt.

4. Literatur

- Bärwolff, Matthias; Gehring, Robert A.; Lutterbeck, Bernd (Hrsg.) (2005)
Open Source Jahrbuch 2005 – Zwischen Softwareentwicklung und Gesellschaftsmodell.
Berlin.
- Eckert, Claudia (2004)
IT-Sicherheit: Konzept – Verfahren – Protokolle. München, Wien.
- Maass, Christian; Scherm, Ewald (2005)
Open-Source-Software und Standardisierung. In: Bärwolff, Matthias; Gehring, Robert A.;
Lutterbeck, Bernd (Hrsg.) (2005): Open Source Jahrbuch 2005 – Zwischen Soft-
wareentwicklung und Gesellschaftsmodell. Berlin, S. 161-176.
- Spindler, Gerald (2005)
Rechtsfragen der Open Source Software. In: [http://www.vsi.de/inhalte/aktuell/
studie_final_safe.pdf](http://www.vsi.de/inhalte/aktuell/studie_final_safe.pdf), zugegriffen am 15.04.2005
- Statistisches Landesamt Baden Württemberg (Hrsg.) (2002)
Statistisch prognostischer Bericht – Daten Analysen Perspektiven Jahr 2002, Stuttgart.
- Weber, Steven (2000)
The Political Economy of Open Source Software. BRIE Working Paper 140, E-conomy
Project Working Paper 15, June 2000, University of Berkeley/Ca.

Open Source Software und IT-Sicherheit: Ergebnisse der ersten FAZIT-Unternehmensbefragung

Irene Bertschek, Jörg Ohnemus

1. Einleitung	17
2. Branchenabgrenzung	17
3. Fragebogendesign.....	19
4. Stichprobenziehung	20
5. Feldverlauf und Auswertung	21
5.1. Nonresponse-Analyse.....	24
5.2. Hochrechnung.....	24
6. Ergebnisse der Umfrage	25
6.1. Die konjunkturelle Lage im ersten Quartal 2005: IT- und Mediensektor optimistischer als Anwenderbranchen.....	25
6.2. Ein Viertel der großen Unternehmen plant Erhöhung der IKT-Investitionen in 2005...27	
6.3. Computer- und Internetnutzung im Arbeitsalltag weit fortgeschritten	28
6.4. Anteil älterer Arbeitnehmer im IT- und Mediensektor unterdurchschnittlich	30
6.5. Unternehmensgröße ist für Softwareanwendungen maßgeblich.....	31
6.6. Open Source Software.....	33
6.6.1 Nutzung und Einsatz von Open Source Software	33
6.6.2 Großer Informationsbedarf bei Open Source Software.....	34
6.6.3 Einsatzbereiche von Open Source Software.....	36
6.6.4 Zuverlässigkeit und Kostenaspekte wichtigste Gründe für den Einsatz von OSS ...	40
6.6.5 Hemmnisse für den Einsatz von Open Source Software.....	41
6.6.6 Geplanter Einsatz von Open Source Software bis Mitte 2006 gering.....	43
6.7. IT-Sicherheit.....	44
6.7.1 Sicherheitsbewusstsein in der IT- und Medienbranche stärker ausgeprägt als in Anwenderbranchen	44
6.7.2 Virenschutzprogramme und Firewalls häufigste IT-Sicherheitsmaßnahmen	45
6.7.3 Unternehmensexterne Faktoren als Hemmnis für umfassende IT-Sicherheit.....	48
6.7.4 Kaum Veränderungen des Anteils für IT-Sicherheit am IT-Budget geplant	49
7. Anhang	52

Tabellenverzeichnis

Tab. 1: Responsequote nach Größenklassen	21
Tab. 2: Responsequote nach Wirtschaftszweigen	22
Tab. 3: Verteilung der Antworten auf Fax, Brief und Internet.....	22
Tab. 4: Antwort vor oder nach Erinnerungsschreiben	23
Tab. 5: Online-Antworten nach Wirtschaftszweigen	23
Tab. 6: Häufigkeit des Einsatzes von Open Source Software (ungewichtet).....	24
Tab. 7: Ergebnisse der Konjunkturfragen	26
Tab. 8: Branchenabgrenzung.....	52

Abbildungsverzeichnis

Abb. 1: Anteil der Unternehmen bzw. Umsatzanteil ausgewählter Branchen an der Gesamtzahl an Unternehmen bzw. am Gesamtumsatz in Baden-Württemberg	19
Abb. 2: Investitionserwartungen in IKT für 2005.....	28
Abb. 3: Computer- und Internetnutzung nach Branchen	29
Abb. 4: Computer- und Internetnutzung nach Unternehmensgröße	29
Abb. 5: Anteil der Beschäftigten die 50 Jahre und älter sind	30
Abb. 6: Verbreitung von Softwareanwendungen.....	31
Abb. 7: Nutzung von CAD- und CAE-Software nach Branchen	32
Abb. 8: Verbreitung von Softwareentwicklungsprogrammen nach Branchen und Größenklassen	32
Abb. 9: Nutzung von Open Source Software nach Branchen und Unternehmensgrößenklassen	33
Abb. 10: Bestehende Informationsdefizite über Open Source Software	35
Abb. 11: Einsatzbereiche von OSS	36
Abb. 12: Nutzung von OSS nach Einsatzbereichen und Branchen	37
Abb. 13: Nutzung von OSS nach Einsatzbereichen und Anzahl der Mitarbeiter (1)	38
Abb. 14: Nutzung von OSS nach Einsatzbereichen und Anzahl der Mitarbeiter (2)	39
Abb. 15: Faktoren für den Einsatz von Open Source Software	40
Abb. 16: Gründe gegen den Einsatz von Open Source Software	41
Abb. 17: Faktoren gegen den Einsatz von Open Source Software nach Branchen	42
Abb. 18: Geplanter Einsatz von OSS in den nächsten 12 Monaten.....	43
Abb. 19: Einsatz von IT-Sicherheitsvorkehrungen und Datenverluste durch Viren	45
Abb. 20: Verwendete IT-Sicherheitsmaßnahmen	46
Abb. 21: Verwendung von Zutrittssicherung und Sicherheitsrichtlinien nach Anzahl der Mitarbeiter.....	47
Abb. 22: Schutz durch IT-Sicherheitsmaßnahmen	48
Abb. 23: Hemmnisse für eine umfassende IT-Sicherheit im Unternehmen	49
Abb. 24: Anteil für IT-Sicherheit am gesamten IT-Budget (in Prozent)	50
Abb. 25: Erwarteter Anteil für IT-Sicherheit am IT-Budget für 2005 im Vergleich zu 2004 ...	50
Abb. 26: Erwarteter Anteil für IT-Sicherheit am IT-Budget für 2005 im Vergleich zu 2004 nach Anzahl der Mitarbeiter.....	51
Abb. 27: Fragebogen der ersten FAZIT-Unternehmensbefragung.....	57

1. Einleitung*

Im Rahmen des Forschungsprojekts FAZIT fand im Frühjahr 2005 die erste Unternehmensbefragung in Baden-Württemberg statt. Die Erhebung, die vom Zentrum für Europäische Wirtschaftsforschung GmbH (ZEW), Mannheim, durchgeführt wurde, fokussierte auf die beiden Schwerpunktthemen Open Source Software und IT-Sicherheit. Dieser Forschungsbericht stellt die methodische Konzeption sowie die Ergebnisse dieser Umfrage vor und enthält ferner Hintergrundinformationen zu den beiden Schwerpunktthemen. Ziel der FAZIT-Unternehmensbefragungen ist es, Determinanten, Ziele und Potenziale, Hemmnis- und Förderfaktoren sowie die ökonomischen Auswirkungen der Nutzung von Informations- und Kommunikationstechnologien (IKT) in Baden-Württemberg zu erfassen und zu analysieren. Durch die so gewonnenen Erkenntnisse sollen konkrete Empfehlungen für Wirtschaft, Politik und Wissenschaft generiert werden. Die repräsentativen Befragungen werden halbjährlich im IT- und Mediensektor und in weiteren Branchen des verarbeitenden Gewerbes und Dienstleistungssektors durchgeführt.

Gerade der IT- und Mediensektor ist inzwischen ein wichtiger Bestandteil der baden-württembergischen Wirtschaftsstruktur. Mit über 35.000 Unternehmen und Selbständigen und mit rund 300.000 Erwerbstätigen erwirtschaftete der IT- und Mediensektor (nach den Definitionskriterien des Statistischen Landesamtes Baden-Württemberg) in 2001 rund 10 Prozent der Bruttowertschöpfung des Landes.¹ Es ist davon auszugehen, dass dieser Anteil inzwischen höher liegt, nachdem der IT- und Mediensektor bereits in den neunziger Jahren ein überdurchschnittliches Wachstum aufweisen konnte. Aber nicht nur im IT- und Mediensektor spielen neue Informations- und Kommunikationstechnologien (IKT) eine Rolle, wenngleich die Unternehmen dieses Sektors häufig die intensivsten Nutzer ihrer Produkte sind. Als so genannte Basistechnologien werden IKT inzwischen in fast allen Wirtschaftszweigen mehr oder weniger intensiv eingesetzt. Im Fokus der Analysen stehen deshalb neben den Unternehmen des IT- und Mediensektors auch Unternehmen aus Anwenderbranchen (von IT- und Medientechnologien) – sowohl aus dem verarbeitenden Gewerbe als auch aus dem Dienstleistungssektor.

2. Branchenabgrenzung

Beim IT- und Mediensektor handelt es sich um einen Querschnittssektor, der sowohl Bereiche des verarbeitenden Gewerbes als auch des Dienstleistungssektors umfasst. Die bei FAZIT verwendete Branchenabgrenzung für den IT- und Mediensektor orientiert sich an der Definition des Statistischen Landesamtes.²

* Neben den beiden Autoren waren am ZEW folgende Personen am Projekt beteiligt: Thorsten Doherr, Julia Häring, Hiltrud Niggemann (p-wert, Dortmund), Katrin Schleife.

¹ Vgl. Statistisch Prognostischer Bericht, Statistisches Landesamt Baden-Württemberg, 2001. Die Angabe für die Anzahl der Unternehmen im IT- und Mediensektor beruht auf der FAZIT Branchenabgrenzung und den Angaben der Umsatzsteuerstatistik 2002.

² Vgl. Statistisch Prognostischer Bericht, Statistisches Landesamt Baden-Württemberg, 2001, S. 113.

Dabei gliedert das ZEW den IT- und Mediensektor in folgende sieben Branchen.³

- Software
- IT- und Medienhardware
- (Tele-) Kommunikation und DV-Dienstleistungen
- Audiovisuelle Medien
- Druck / Verlag
- Werbung / Marktkommunikation
- Inhalte-Dienstleister

Zu den Anwenderbranchen von IT- und Medien-Produkten und/oder -Dienstleistungen werden nach der ZEW-Abgrenzung folgende Branchen (bzw. Teilbereiche der jeweiligen Branche) gezählt:⁴

- Chemische Industrie (Herstellung von chemischen Erzeugnissen)
- Maschinenbau
- Medizin-, Mess-, Steuer- und Regelungstechnik
- Automobilindustrie (Herstellung von Kraftwagen und Kraftwagenteilen)
- Verkehrsdienstleister
- Bank- und Versicherungsgewerbe
- Technische Dienstleister (insbesondere Forschung und Entwicklung, Architektur- und Ingenieurbüros, technische, physikalische chemische Untersuchung)

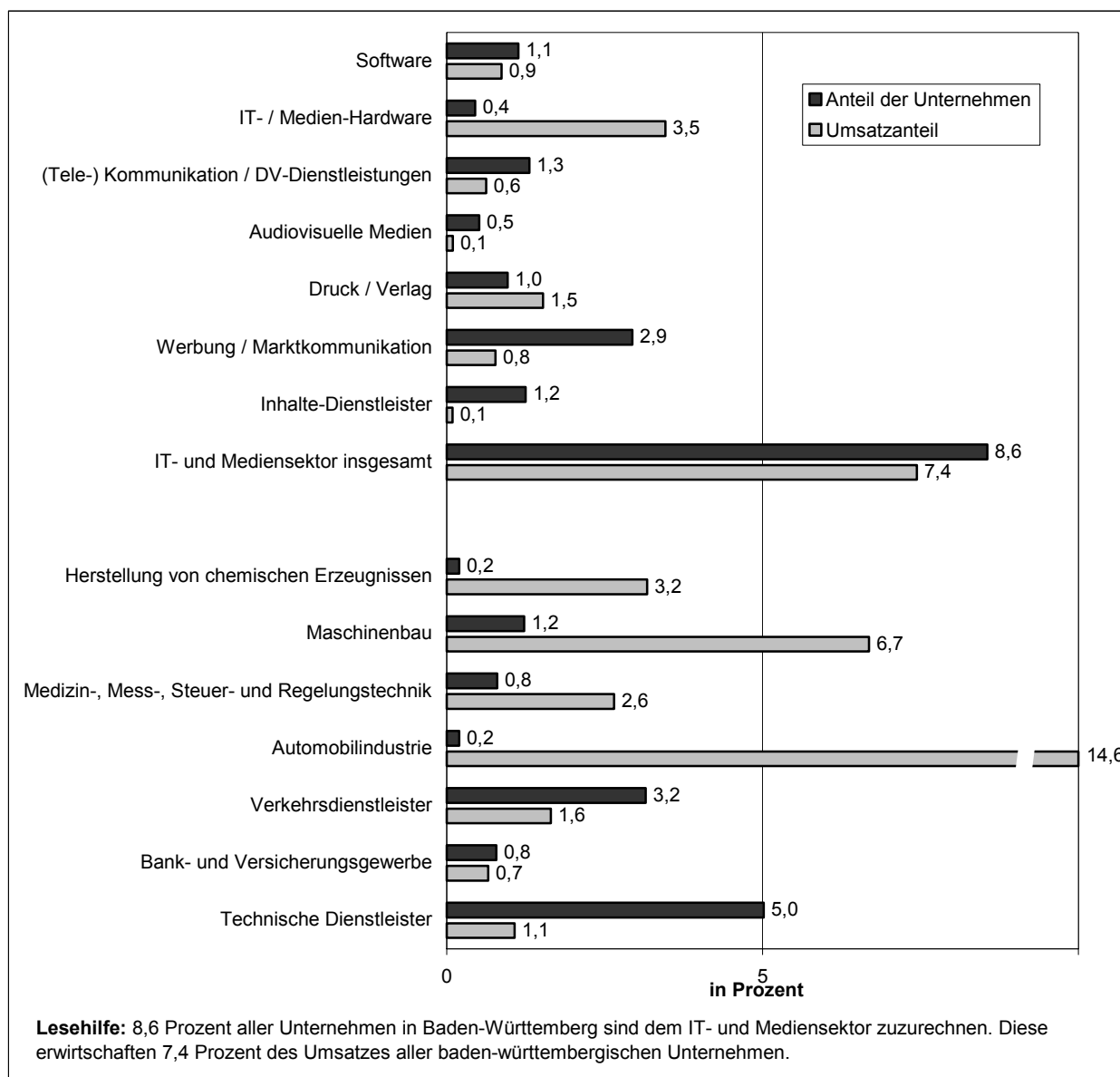
Abbildung 1 gibt einen Überblick über den Anteil der Unternehmen in den einzelnen Branchen (nach der FAZIT-Branchenabgrenzung) gemessen an der Gesamtzahl an Unternehmen in Baden-Württemberg. Weiterhin sind deren Umsatzanteile am Gesamtumsatz aller Unternehmen aufgeführt. Der IT- und Mediensektor umfasst somit 8,6 Prozent aller Unternehmen, die 7,4 Prozent des baden-württembergischen Unternehmensumsatzes erwirtschaften. Innerhalb des IT- und Mediensektors sind prozentual besonders viele Unternehmen in der Branche Werbung und Marktkommunikation tätig (2,9 Prozent). Den größten Umsatzanteil hingegen erwirtschaften die Unternehmen der Branche IT- und Medienhardware (3,5 Prozent). Wenig überraschend zeigt sich innerhalb der Anwenderbranchen die Dominanz der Automobilindustrie gemessen am Umsatzanteil (14,6 Prozent).⁵ Auf Grund von relativ geringen Antwortquoten in einzelnen Branchen oder Größenklassen wurden in der späteren Auswertung der Befragungsergebnisse einzelne Branchen zusammengefasst hochgerechnet und ausgewertet (näheres dazu in 5.2 Hochrechnung).

³ Eine detaillierte Darstellung der im IT- und Mediensektor zusammengefassten Unternehmen befindet sich in Tabelle 8 im Anhang.

⁴ Eine genauere Branchenabgrenzung befindet sich ebenfalls in Tabelle 8.

⁵ Man bedenke, dass in Baden-Württemberg Firmen wie DaimlerChrysler, Porsche und Bosch angesiedelt sind.

Abbildung 1: Anteil der Unternehmen bzw. Umsatzanteil ausgewählter Branchen an der Gesamtzahl an Unternehmen bzw. am Gesamtumsatz in Baden-Württemberg



Quelle: Statistische Berichte Baden-Württemberg – Finanz und Steuern, Statistisches Landesamt Baden-Württemberg, Stuttgart, 2. September 2004.

3. Fragebogendesign

Die Umfrage ist als kombinierte schriftliche/online-Befragung konzipiert. Die Ansprechpartner im Unternehmen erhalten ein Anschreiben zusammen mit einem zweiseitigen Fragebogen per Post zugesandt. Die Unternehmen können nun wählen, ob sie den Fragebogen per Fax oder Brief zurückschicken oder ob sie die Möglichkeit nutzen ihre Angaben über ein Internetbefragungstool abzugeben. Da das Zurücksenden per Fax der von den Unternehmen in der Regel präferierte Weg ist, wird der Fragebogen auf zwei separate Blätter gedruckt. Dadurch können Fehler, z.B. das zweimalige Zusenden derselben Seite, eingeschränkt werden. Das Ausfüllen des Fragebogens im Internet wird durch ein vom ZEW entwickeltes und bereits regelmäßig eingesetztes (und für die FAZIT-Unternehmensbefragung modifiziertes) Internettool ermöglicht.

Um Missbrauch (mehrmaliges Ausfüllen) und unaufgefordertes Ausfüllen des Fragebogens zu verhindern, erhält jedes Unternehmen ein persönliches Kenn- und Passwort, das nach dem vollständigen Ausfüllen des Fragebogens den Zugriff auf den Fragebogen deaktiviert. Die eingegebenen Daten werden auf einem gesicherten Server des ZEW abgespeichert.

Der angeschriebene Ansprechpartner der Unternehmen ist in der Regel der Geschäftsführer. Dieser sollte den Fragebogen gerade in kleineren und mittleren Unternehmen auch ausfüllen können, insbesondere was die allgemeinen Fragen zur Unternehmensstruktur sowie zur konjunkturellen Einschätzung betrifft. Hinzu kommt, dass kleinere und mittlere Unternehmen oft keine eigene IT-Abteilung oder IT-Verantwortlichen haben. Bei größeren Unternehmen kann es erforderlich sein, dass die Fragenblöcke von unterschiedlichen Personen ausgefüllt werden sollten, z.B. vom Geschäftsführer und vom IT-Verantwortlichen. Aus anderen Umfragen, u.a. auch mit IT-Fokus resultiert die Erfahrung, dass Fragebögen durchaus innerhalb von Unternehmen weiter gereicht und thematisch unterschiedliche Fragen auch von unterschiedlichen Personen mit der jeweiligen Fachkompetenz beantwortet werden.

Der Fragebogen (vgl. Abbildung 27 im Anhang) setzt sich aus zwei Teilen zusammen. Im ersten Teil werden die Unternehmen nach konjunkturellen Indikatoren, wie Umsatzentwicklung, Nachfrageentwicklung und Personalentwicklung aber auch nach einer allgemeinen Einschätzung ihrer wirtschaftlichen Lage befragt. Diese Fragen sollten zunächst mit Blick auf die gegenwärtige Situation (z.B. im ersten Quartal) und dann hinsichtlich der erwarteten Entwicklung im nächsten Quartal beantwortet werden. Auf diese Weise lässt sich ein repräsentatives Bild über die aktuelle und erwartete wirtschaftliche Lage des baden-württembergischen IT- und Mediensektors sowie der anderen in der Stichprobe vertretenen Branchen gewinnen. Dieser erste, allgemeine Teil des Fragebogens dürfte für alle Unternehmen gleichermaßen von Interesse sein und soll auch zur Motivation dienen, den gesamten Fragebogen auszufüllen. Der zweite, wesentlich längere Teil des Fragebogens beschäftigt sich neben allgemeinen Fragen zur Beschäftigtenstruktur und zur Computer- bzw. Internetnutzung im Unternehmen mit speziellen, von Welle zu Welle variierenden Schwerpunktthemen. Als solche wurden für die erste Befragung die Themen Open Source Software (OSS) und IT-Sicherheit gewählt. Zukünftige Umfragen werden sich mit anderen Schwerpunktthemen wie z.B. Internationalisierung, E-Commerce, Weiterbildungsmaßnahmen, etc. beschäftigen.⁶

4. Stichprobenziehung

Als Grundlage für die Stichprobenziehung dient der sehr umfangreiche Adressbestand des Verbands der Vereine Creditreform (VVC), der dem ZEW im Rahmen eines Kooperationsvertrags zur Verfügung steht und der auch für andere ZEW-Umfragen genutzt wird. Um die

⁶ Dabei ist durchaus denkbar, einige Schwerpunktthemen in spätere Befragungen erneut aufzunehmen, um die Entwicklung auf diesen Gebieten auch zeitlich analysieren zu können.

Repräsentativität der Stichprobe zu gewährleisten, wird bei der Ziehung der Unternehmen nach Branchen (insgesamt 14, vgl. 2. Branchenabgrenzung) und Größenklassen geschichtet. Die Größenklasse eines Unternehmens bezieht sich dabei auf die Anzahl der Mitarbeiter im Unternehmen. Bei der Stichprobenziehung werden folgende Klassen berücksichtigt: 1-4, 5-9, 10-19, 20-49, 50-249, 250-999 und mehr als 1000 Beschäftigte. Motiviert durch die Tatsache, dass gerade im IT- und Mediensektor sehr viele kleine Unternehmen mit wenigen Mitarbeitern zu finden sind, wurde die Größenklasseneinteilung sehr fein gewählt. Bei der späteren Auswertung und Hochrechnung der Daten wurden einzelne Größenklassen wieder zusammengefasst. Für die Bruttostichprobe wurden über 9000 Unternehmen anhand der eben festgelegten Kriterien zufällig aus dem Adressbestand der VVC ausgewählt. Dieser Wert wurde bewusst etwas großzügiger gewählt, da sich erst noch zeigen musste, auf welche Akzeptanz der Fragebogen (bzw. die Umfrage allgemein) bei den Unternehmen stößt.

5. Feldverlauf und Auswertung

Von den 9074 angeschriebenen Unternehmen der Bruttostichprobe haben insgesamt 623 Unternehmen den ausgefüllten Fragebogen zurückgesendet. Damit wurde eine Responsequote – vor Eliminierung stichprobenneutraler Ausfälle – von 6,9 Prozent erzielt. Unter stichprobenneutralen Ausfällen werden hier Adressen zusammengefasst, unter denen kein Unternehmen zu erreichen ist (z.B. wegen Insolvenz oder Schließung) oder von Unternehmen, die nicht zur Zielgruppe (IT- und Medien- bzw. Anwenderbranchen) gehören. Insgesamt waren 1533 stichprobenneutrale Ausfälle zu verzeichnen (dies entspricht einem Anteil von 16,9 Prozent an der Bruttostichprobe).

Tabelle 1: Responsequote nach Größenklassen^{*)}

Größenklasse (Mitarbeiter)	1-4	5-19	20-249	> 249
Quote	6,8%	8,0%	10,9%	7,7%

^{*)} Die Werte beziehen sich auf 7541 Unternehmen aus der Nettostichprobe und 603 auswertbare Fragebögen.

Quelle: Eigene Darstellung

Von den 7541 Unternehmen der Nettostichprobe, flossen 603 auswertbare Fragebögen in die Analyse ein⁷. Dies entspricht einer Nettoresponserate von 8,0 Prozent. In der Größenklasse 20 bis 249 Mitarbeiter wurde die höchste Responserate mit fast 11 Prozent erreicht (vgl. Tabelle 1). Betrachtet man die Responsequote nach Wirtschaftszweigen, liegt die Softwarebranche mit 13 Prozent an der Spitze. Allgemein war der Rücklauf im IT- und Mediensektor mit 8,7 Prozent etwas besser als in den Anwenderbranchen mit 7,5 Prozent (vgl. Tabelle 2).

⁷ Die restlichen 20 Unternehmen, die sich an der Befragung beteiligten, gehörten nicht dem IT- und Mediensektor bzw. den Anwenderbranchen an.

Tabelle 2: Responsequote nach Wirtschaftszweigen^{*)}

Branche	Quote
Software	13,0
IT- und Medien-Hardware	9,3
(Tele-) Kommunikation und DV-Dienstleistungen	6,9
Audiovisuelle Medien	7,2
Druck / Verlag	6,7
Werbung / Marktkommunikation	9,4
Inhalte-Dienstleister	8,1
IT und Mediensektor	8,7
Chemische Industrie	6,5
Maschinenbau	6,0
Medizin-, Mess-, Steuer- und Regelungstechnik	8,0
Automobilindustrie	5,2
Verkehrsdienstleister	6,6
Bank- und Versicherungsgewerbe	7,8
Technische Dienstleister	10,2
Anwenderbranchen	7,5

^{*)} Die Werte beziehen sich auf 7541 Unternehmen aus der Nettostichprobe und 603 auswertbare Fragebögen.

Quelle: Eigene Darstellung

Ein Großteil der Umfrageteilnehmer (48 Prozent) wählte das Fax zur Rücksendung des Fragebogens, 27 Prozent schickten den ausgefüllten Fragebogen per Post und ein Viertel machte von der Möglichkeit Gebrauch, den Fragebogen im Internet auszufüllen (vgl. Tabelle 3).

Tabelle 3: Verteilung der Antworten auf Fax, Brief und Internet

Antwortmöglichkeit	Fax	Brief	Internet
Quote	47,6%	27,2%	25,2%

Quelle: Eigene Darstellung

Der Rücklauf der Fragebögen verläuft in zwei Phasen. Alle Unternehmen, die nach dem ersten Anschreiben bis zu einem bestimmten Termin nicht antworten, werden in einer Nachfassaktion ein zweites Mal angeschrieben und gebeten, den nochmals beiliegenden Fragebogen auszufüllen. Bei der ersten Befragungswelle wurden insgesamt zwei Drittel der Fragebögen nach Versenden dieser Erinnerungsschreiben zurück geschickt, während nur ein Drittel der antwortenden Unternehmen gleich auf das erste Anschreiben reagiert haben (vgl. Tabelle 4). Dieses Ergebnis deutet darauf hin, dass ein Grund für die vergleichsweise geringe Rücklaufquote der bislang mangelnde Bekanntheitsgrad der FAZIT-Unternehmensbefragung ist.

Tabelle 4: Antwort vor oder nach Erinnerungsschreiben

Zeitpunkt	vor Erinnerungsschreiben	nach Erinnerungsschreiben
Quote	34,5%	65,5%

Quelle: Eigene Darstellung

Interessante Anhaltspunkte über die technologische Aufgeschlossenheit einzelner Branchen liefert die Betrachtung der Online-Antworten nach einzelnen Wirtschaftszweigen (vgl. Tabelle 5). Nicht sonderlich überraschend kommen über 61 Prozent der Unternehmen, die über das Internet an der Befragung teilgenommen haben, aus dem IT- und Mediensektor. Dabei stellt die Softwarebranche mit fast 18 Prozent den größten Anteil. Die Unternehmen des verarbeitenden Gewerbes weisen dagegen nur geringe Anteile an den Antworten per Internet auf.

Tabelle 5: Online-Antworten nach Wirtschaftszweigen *)

Branche	Quote
Software	17,8
IT- und Medien-Hardware	5,9
(Tele-) Kommunikation und DV-Dienstleistungen	11,8
Audiovisuelle Medien	5,3
Druck / Verlag	4,6
Werbung / Marktkommunikation	9,2
Inhalte-Dienstleister	6,6
IT und Mediensektor	61,2
Chemische Industrie	2,0
Maschinenbau	4,6
Medizin-, Mess-, Steuer- und Regelungstechnik	4,0
Automobilindustrie	1,3
Verkehrsdienstleister	7,9
Bank- und Versicherungsgewerbe	7,9
Technische Dienstleister	11,2
Anwenderbranchen	38,8

*) Die Werte beziehen sich auf 152 Unternehmen aus der Nettostichprobe die im Internet geantwortet haben. Abweichungen zu 100% ergeben sich durch Rundungen.

Quelle: Eigene Darstellung

5.1. Nonresponse-Analyse

Auf Grund der relativ geringen Ausschöpfung der Stichprobe (in der Regel kann bei schriftlichen Befragungen mit einer Responsequote bis maximal 25 Prozent gerechnet werden) und der recht speziellen Themenauswahl (insbesondere in puncto Open Source Software), wurde im Anschluss an die Feldphase eine Nonresponse-Analyse durchgeführt. Den insgesamt 242 (von ca. 1000 telefonisch kontaktierten) Unternehmen wurden vier kurze Fragen zu Open Source Software und IT-Sicherheit gestellt. Somit konnte festgestellt werden, inwieweit die Ergebnisse aus der schriftlichen Befragung dahingehend verzerrt sind, dass hauptsächlich Unternehmen, die OSS einsetzen, an der Umfrage teilgenommen haben. Tatsächlich machte die Nonresponse-Analyse eine solche Verzerrung deutlich, d.h. Unternehmen, die OSS einsetzen, sind in der schriftlichen bzw. Online-Befragung überrepräsentiert, während in der Gruppe der Unternehmen, die nicht an der Umfrage teilgenommen haben, der Anteil der OSS-Nutzer deutlich niedriger liegt (vgl. Tabelle 6). Die Ergebnisse der Nonresponse-Befragung wurden deshalb dazu verwendet, die Hochrechnungsfaktoren zu korrigieren, um der oben genannten Verzerrung Rechnung zu tragen.

Tabelle 6: Häufigkeit des Einsatzes von Open Source Software (ungewichtet)

Einsatz von OSS	Gruppe Nonresponse	Gruppe Umfrageteilnehmer
ja	22,5 %	49,6 %
nein	77,5 %	50,4 %

Quelle: Eigene Darstellung

5.2. Hochrechnung

Die aus der Umfrage generierten Daten wurden geschichtet auf die Grundgesamtheit aller baden-württembergischen Unternehmen der betrachteten Branchen hochgerechnet.⁸ Hierbei konnten die Daten nicht wie ursprünglich geplant für alle 14 Branchen getrennt hochgerechnet werden, da die Anzahl der auswertbaren Fragebögen in einzelnen Zellen zu gering war. Dabei wurden die einzelnen Branchen des IT- und Mediensektors nicht getrennt berücksichtigt, sondern der zusammengefasste IT- und Mediensektor hochgerechnet. Bei den Anwenderbranchen wurden die Chemische Industrie, der Maschinenbau, die Medizin-, Mess-, Steuer- und Regelungstechnik und die Automobilindustrie sowie die Verkehrsdienstleister zum verarbeitenden Gewerbe zusammengezogen. Sowohl das Bank- und Versicherungsgewerbe als auch die technischen Dienstleister wurden weiterhin separat hochgerechnet. Als weiteres Schichtungsmerkmal diente die Größenklasse (Anzahl der Mitarbeiter). Hier wurden die aus der Stichprobenziehung vorhandenen sieben Größenklassen ebenfalls zu vier Ausprägungen zusammengefasst: 1 bis 4 Beschäftigte, 5 bis 19 Beschäftigte, 20 bis 249 Beschäftigte und mehr als 249 Beschäftigte. Insgesamt standen somit 16 Zellen zur Hochrechnung zur Verfügung.

⁸ Fragen, bei denen die Unternehmen quantitative Angaben machen sollten, wurden auf den Gesamtumsatz der entsprechenden Branche hochgerechnet.

Wie schon im vorangegangenen Abschnitt angesprochen, wurden die Ergebnisse der Non-response-Befragung zur Korrektur herangezogen. Dabei fand eine unterschiedliche Adjustierung der Hochrechnungsfaktoren für Unternehmen mit und ohne Open Source Software statt. Grundsätzlich spielt die Adjustierung bei Fragen keine Rolle, bei denen man davon ausgehen kann, dass der Einsatz oder Nicht-Einsatz von Open Source Software keine Auswirkungen auf die Wahl der Antwort hat. D.h. adjustierter und nicht-adjustierter Hochrechnungsfaktor eines Unternehmens sind identisch. Da insbesondere bei den Konjunkturfragen kaum Unterschiede zwischen den Hochrechnungen (mit und ohne Adjustierung) festzustellen waren, wurden diese Daten mit dem nicht-adjustierten Hochrechnungsfaktor hochgerechnet, damit eine Vergleichbarkeit mit den Ergebnissen zukünftiger Umfragewellen garantiert werden kann.

Ferner wurden kategoriale Variablen (z.B. die Frage nach den eingesetzten Softwareanwendungen) auf Basis der Zahl der Unternehmen in den jeweiligen Branchen hochgerechnet, quantitative Variablen, z.B. der Anteil der Beschäftigten, die überwiegend am Computer arbeiten, wurden auf Basis des Umsatzes hochgerechnet. Die Daten der Grundgesamtheit beruhen dabei auf der Umsatzsteuerstatistik 2002 für Baden-Württemberg.⁹ Auf Grund ihrer relativ großen Anzahl an Unternehmen, dominieren bei den Anteilen der kategorialen Variablen kleine und mittlere Unternehmen. Große Unternehmen hingegen dominieren auf Grund ihrer großen Umsatzvolumina bei den Anteilen, die sich auf quantitative Angaben beziehen.

6. Ergebnisse der Umfrage

6.1. Die konjunkturelle Lage im ersten Quartal 2005:

IT- und Mediensektor optimistischer als Anwenderbranchen

Die Unternehmen des IT- und Mediensektors beurteilen ihre *aktuelle Geschäftslage* im April 2005 überwiegend positiv. 39 Prozent der Unternehmen des IT- und Mediensektors antworten per Saldo, dass es ihnen „gut“ bzw. „eher gut“ geht. Dagegen ziehen die Unternehmen der Anwenderbranchen bei dieser Frage kein so positives Fazit. Hier sind per Saldo nur knapp 8 Prozent der Ansicht, dass ihre persönliche Geschäftslage im Moment als „gut“ bzw. „eher gut“ zu beurteilen ist. Bezüglich der *Geschäftslage erwarten* 30 Prozent der Unternehmen mittelfristig eine Verbesserung, wobei auch hier der IT- und Mediensektor wesentlich zuversichtlicher ist als die Anwenderbranchen. Über 38 Prozent der Unternehmen des IT- und Mediensektors rechnen mit einer Verbesserung ihrer Geschäftslage im zweiten und dritten Quartal 2005. Bei den Anwenderbranchen liegt dieser Wert lediglich bei knapp 26 Prozent.

⁹ Statistische Berichte Baden-Württemberg – Finanz und Steuern, Statistisches Landesamt Baden-Württemberg, Stuttgart, 2. September 2004.

Tabelle 7: Ergebnisse der Konjunkturfragen

Geschäftslage									
	Beurteilung (Stand: April/Mai 2005)					Erwartungen II. und III. Quartal 2005			
	▲▲	▲	▼	▼▼	Saldo	▲	=	▼	Saldo
IT und Medien	21,5	48,0	21,9	8,6	39,0	38,2	57,1	4,6	33,6
Anwender	17,4	36,5	32,9	13,2	7,9	25,8	61,3	13,0	12,8
insgesamt	19,2	41,5	28,1	11,2	21,3	31,1	59,5	9,4	21,7

Umsatz									
	Beurteilung I. Quartal 2005				Erwartungen II. Quartal 2005				
	▲	=	▼	Saldo	▲	=	▼	Saldo	
IT und Medien	24,3	51,4	24,3	0,0	33,4	55,6	11,0	22,4	
Anwender	20,1	40,7	39,3	-19,2	29,1	56,0	14,9	14,2	
insgesamt	21,9	45,3	32,8	-11,0	30,9	55,8	13,2	17,7	

Nachfrage									
	Beurteilung I. Quartal 2005				Erwartungen II. Quartal 2005				
	▲	=	▼	Saldo	▲	=	▼	Saldo	
IT und Medien	31,2	49,2	19,6	11,6	33,3	55,8	10,9	22,4	
Anwender	21,3	40,4	38,3	-17,0	28,1	55,3	16,6	11,5	
insgesamt	25,5	44,2	30,2	-4,7	30,3	55,5	14,1	16,2	

Personal									
	Beurteilung I. Quartal 2005				Erwartungen II. Quartal 2005				
	▲	=	▼	Saldo	▲	=	▼	Saldo	
IT und Medien	9,1	83,9	7,0	2,1	8,8	86,4	4,8	4,0	
Anwender	10,6	80,8	8,6	2,0	5,0	89,8	5,2	-0,1	
insgesamt	10,0	82,1	7,9	2,0	6,6	88,4	5,0	1,6	

Legende: Geschäftslage (Beurteilung):

▲▲ gut; ▲ eher gut; ▼ eher schlecht; ▼▼ schlecht

Geschäftslage (Erwartung), Umsatz, Nachfrage, Personal:

▲ gestiegen / steigen; = gleich geblieben / bleiben; ▼ gesunken / sinken

Anmerkung: Abweichungen zu 100% und bei der Saldenbildung ergeben sich durch Rundungen.

Lesehilfe: Bei der Beurteilung der Nachfrage nach ihren Produkten oder Dienstleistungen im ersten Quartal 2005 antworten 25,5 Prozent aller Unternehmen, dass sie eine steigende Nachfrage im Vergleich zum vierten Quartal 2004 zu verzeichnen hatten. 44,2 Prozent der Unternehmen berichten von einer konstanten und 30,2 Prozent von einer gesunkenen Nachfrage.

Quelle: FAZIT-Unternehmensbefragung, Frühjahr 2005; Berechnungen des ZEW

Die *Unternehmensumsätze* entwickelten sich im ersten Quartal 2005 im Vergleich zum vierten Quartal 2004 in den untersuchten Branchen eher rückläufig. Insgesamt hatten per Saldo 11 Prozent der Unternehmen sinkende Umsätze zu verzeichnen. Die sinkenden Umsätze sind dabei vollständig den Anwenderbranchen zuzuschreiben, der IT- und Mediensektor konnte per Saldo seine Umsätze im Vergleichszeitraum konstant halten. Bei den *Umsatzerwartungen* für das zweite Quartal 2005 rechnen erfreulicherweise immerhin fast 18 Prozent der Unternehmen per Saldo mit steigenden Umsätzen. Allerdings erwarten auch hier per Saldo mehr Unternehmen des IT- und Mediensektors (22 Prozent) als Unternehmen aus den Anwenderbranchen (14 Prozent) einen Anstieg des Umsatzes.

Ein ähnliches Bild ergibt sich bei der *Nachfrageentwicklung* im ersten Quartal 2005. Per Saldo hatten hier annähernd 5 Prozent aller Unternehmen eine rückläufige Nachfrage nach ihren Produkten oder Dienstleistungen zu verzeichnen. Während per Saldo 12 Prozent der Unternehmen des IT- und Mediensektors ihre Nachfrage steigern konnten, mussten per Saldo 17 Prozent der Unternehmen der Anwenderbranchen einen Rückgang in Kauf nehmen. Die *Nachfrageerwartungen* stehen im Einklang mit den Umsatzerwartungen der Unternehmen. Mehrheitlich rechnen die Unternehmen sowohl insgesamt als auch differenziert nach IT- und Mediensektor und Anwenderbranchen mit einer gleich bleibenden Nachfrage im zweiten Quartal 2005 (im Vergleich zum ersten Quartal 2005).

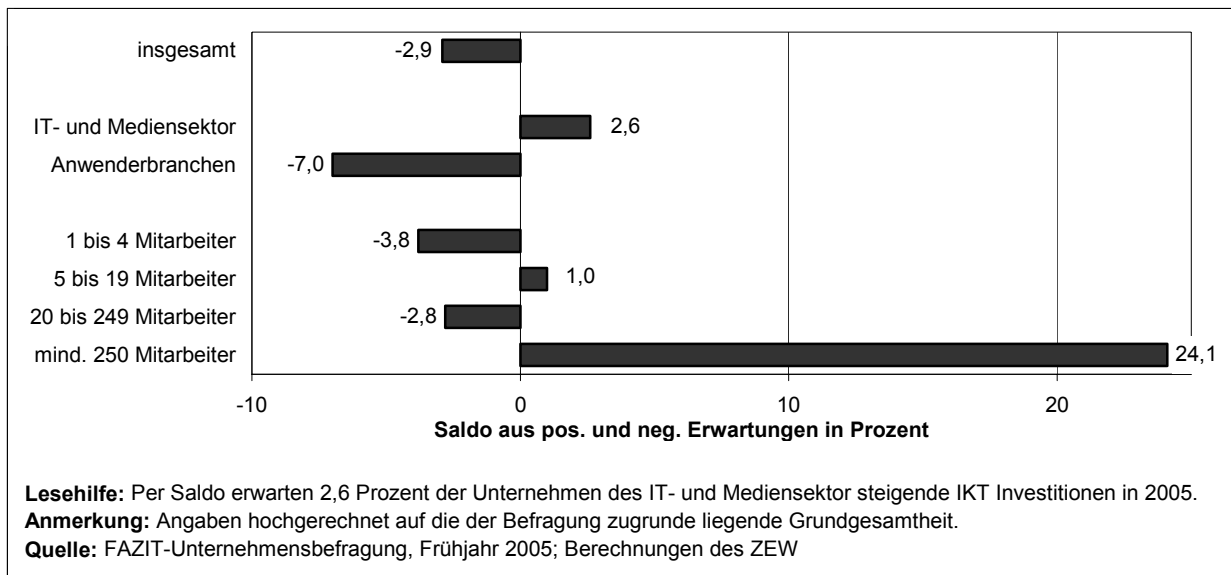
Die *Personalentwicklung* im ersten Quartal 2005 war von Stagnation gekennzeichnet. Insgesamt sagen über 82 Prozent der Unternehmen, dass sich ihr Personalbestand im ersten Quartal nicht verändert hat. Per Saldo geben 2 Prozent der Unternehmen an, zusätzliches Personal im ersten Quartal eingestellt zu haben. Bei der Veränderung des Personalbestands in den ersten drei Monaten 2005 im Vergleich zum letzten Quartal 2004 treten kaum Unterschiede zwischen dem IT- und Mediensektor und den Anwenderbranchen auf. Nur wenige Unternehmen (weniger als 7 Prozent) rechnen im zweiten Quartal mit einem zusätzlichen Personalbedarf. Allerdings gehen auch nur 5 Prozent von einer Reduktion ihres Personalbestandes aus. Dabei weisen die Unternehmen der Anwenderbranchen einen leicht negativen Saldo auf, während der IT- und Mediensektor per Saldo Personal einstellen will.

6.2. Ein Viertel der großen Unternehmen plant Erhöhung der IKT-Investitionen in 2005

Bei den von den Unternehmen für 2005 geplanten Investitionen in Informations- und Kommunikationstechnologien (IKT) zeichnen sich keine großen Veränderungen gegenüber dem Vorjahr ab. Fast 70 Prozent der Unternehmen erwarten gleich bleibende IKT-Investitionen. Interessant sind die Unterschiede bei der Betrachtung der Investitionstätigkeit nach Unternehmensgrößenklassen. Während kleine und mittlere Betriebe per Saldo eher mit rückläufigen IKT-Investitionen rechnen, erwarten per Saldo über 24 Prozent der Großunternehmen (mind. 250 Mitarbeiter) steigende Ausgaben für ihre Informations- und Kommunikationssysteme (vgl. Abbildung 2).

Unterschiedliche Entwicklungsrichtungen der erwarteten IKT-Investitionstätigkeit in 2005 zeigen auch die Unternehmen der Anwenderbranchen und des IT- und Mediensektors. In den Anwenderbranchen wollen per Saldo 7 Prozent der Unternehmen ihre Investitionstätigkeit zurückfahren, während im IT- und Mediensektor 3 Prozent der Unternehmen planen, ihre Investitionen zu erhöhen.

Abbildung 2: Investitionserwartungen in IKT für 2005



6.3. Computer- und Internetnutzung im Arbeitsalltag weit fortgeschritten

Mittlerweile ist der Arbeitsalltag stark durch die Computerisierung geprägt. In den betrachteten baden-württembergischen Branchen verrichtet jeder zweite Beschäftigte (knapp 52 Prozent) den überwiegenden Teil seiner Arbeit am Computer. Im IT- und Mediensektor liegt dieser Anteil weit überdurchschnittlich sogar bei knapp 88 Prozent, während er in den Anwenderbranchen 43 Prozent beträgt. Dort ist die Computerisierung insbesondere im Bank- und Versicherungsgewerbe sowie bei den technischen Dienstleistern, die generell als IT-intensive Branchen gelten, mit jeweils 85 bzw. 81 Prozent weit fortgeschritten (vgl. Abbildung 3). Die Betrachtung nach Größenklassen zeigt einen tendenziell mit der Größe des Unternehmens abnehmenden Anteil der Beschäftigten, die überwiegend am Computer arbeiten. In größeren Unternehmen, insbesondere des verarbeitenden Gewerbes, nutzt häufig nur ein kleinerer Teil der Beschäftigten, beispielsweise in der Verwaltung, einen PC (vgl. Abbildung 4). Insgesamt 56 Prozent der Beschäftigten haben am Arbeitsplatz Zugang zum Internet. Dieser Anteil liegt in den Anwenderbranchen bei 47 Prozent, im IT- und Mediensektor erreicht er 93 Prozent. Entsprechend der PC-Nutzungsintensität ist der Zugang zum Internet für Beschäftigte in kleineren Unternehmen stärker verbreitet als in größeren.

Abbildung 3: Computer- und Internetnutzung nach Branchen

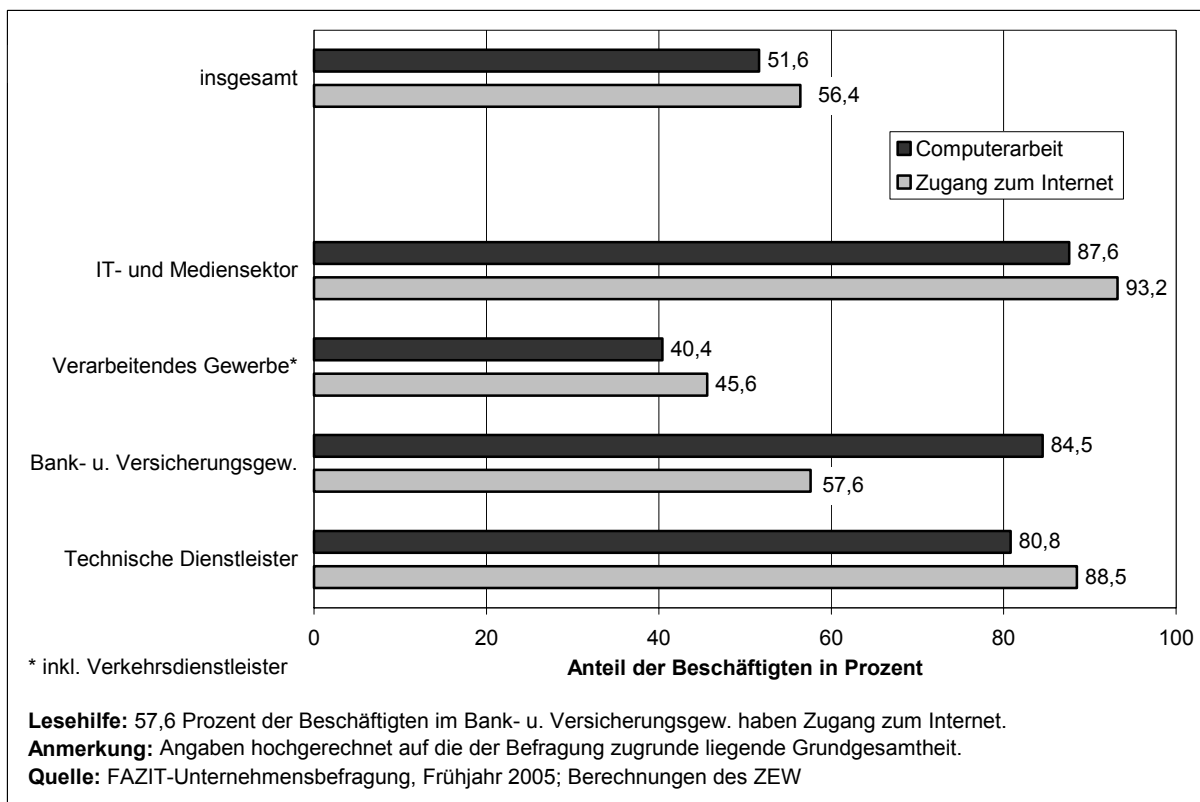
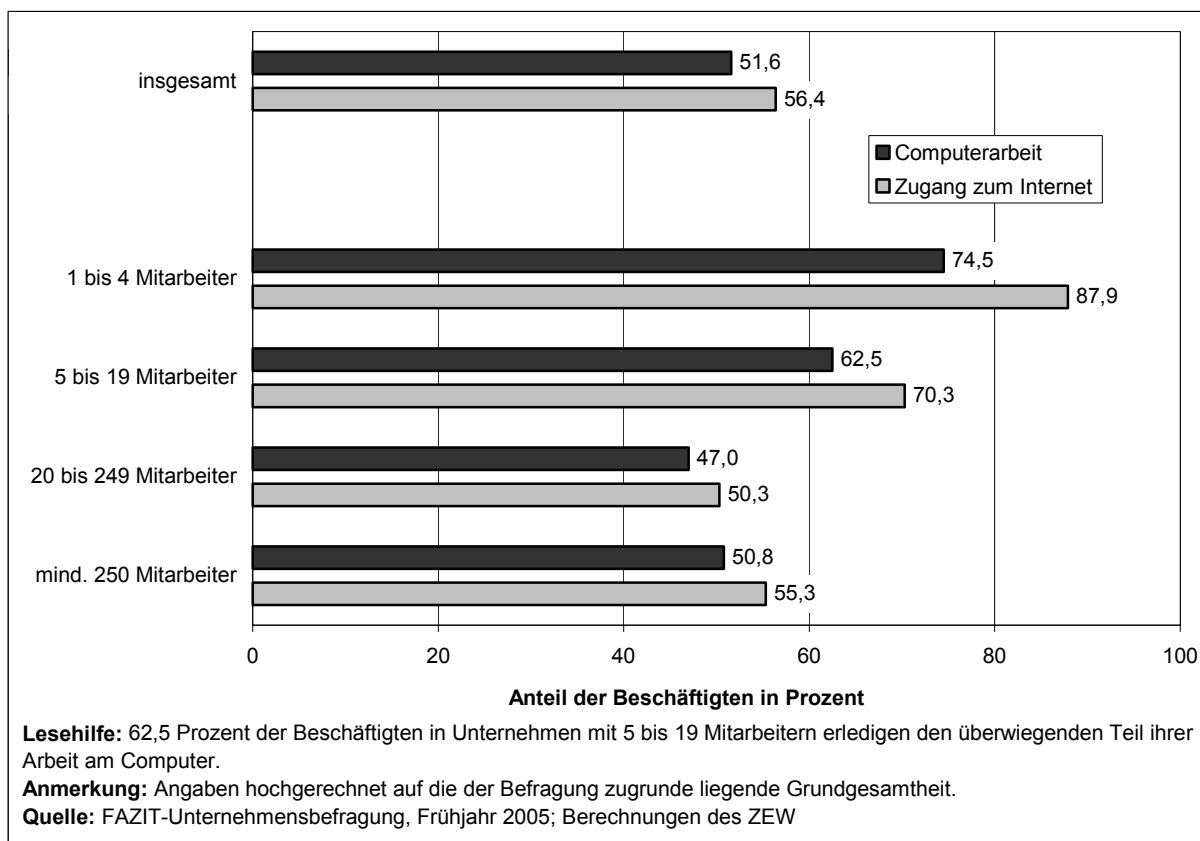


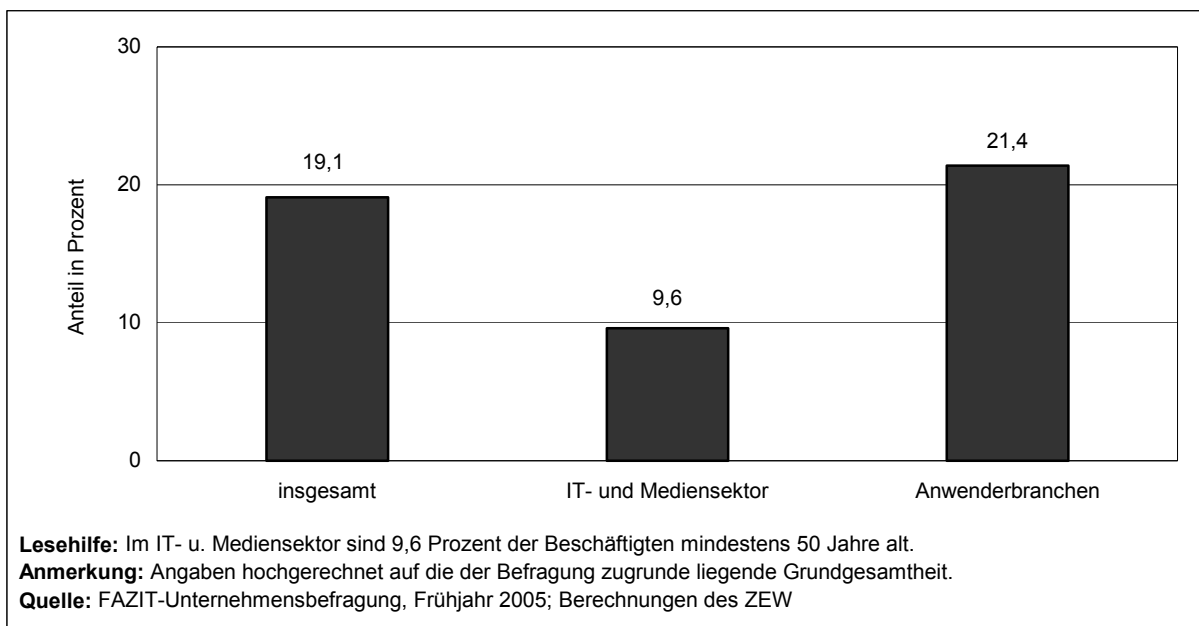
Abbildung 4: Computer- und Internetnutzung nach Unternehmensgröße



6.4. Anteil älterer Arbeitnehmer im IT- und Mediensektor unterdurchschnittlich

In den untersuchten Branchen Baden-Württembergs beträgt der Anteil von Mitarbeitern, die 50 Jahre oder älter sind, durchschnittlich 19 Prozent. Damit liegt Baden-Württemberg voll im Bundesdurchschnitt, wie eine Ende 2004 vom ZEW durchgeführte deutschlandweite Erhebung zeigt.¹⁰ Das Gefälle zwischen IT- und Medienbranche mit knapp 10 Prozent und Anwenderbranchen mit gut 21 Prozent ist hierbei sehr deutlich (vgl. Abbildung 5). Auch im Bank- und Versicherungsgewerbe liegt der Anteil Älterer mit 13 Prozent deutlich unter dem Durchschnitt, während er im verarbeitenden Gewerbe mit knapp 22 Prozent leicht über dem Durchschnitt liegt. Ältere Beschäftigte sind also in weniger IT-intensiven Branchen stärker vertreten, sei es weil sie generell eher für Tätigkeiten eingesetzt werden, die eine Nutzung neuer Technologien nicht erfordern oder weil sie selbst kein Interesse an der Nutzung neuer Technologien und entsprechenden Weiterbildungsmaßnahmen haben. Die Beschäftigung Älterer variiert kaum nach der Unternehmensgröße.

Abbildung 5: Anteil der Beschäftigten die 50 Jahre und älter sind

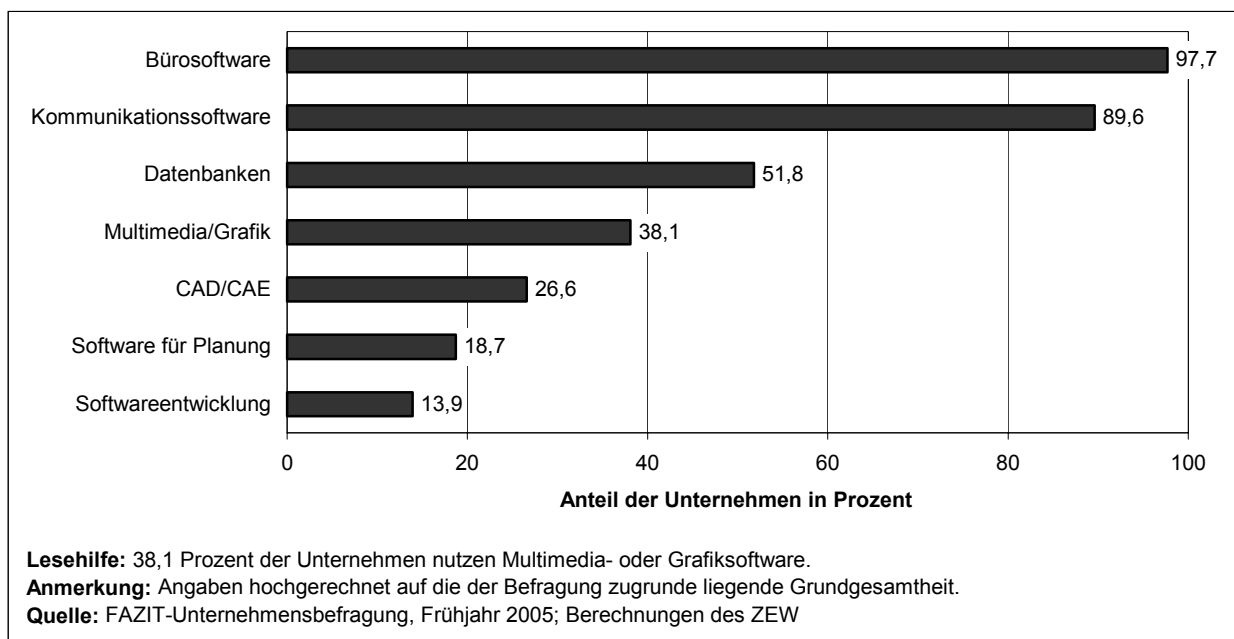


¹⁰ IKT-Report – Unternehmensbefragung zur Nutzung von Informations- und Kommunikationstechnologien, Zentrum für Europäische Wirtschaftsforschung GmbH (ZEW), Mannheim, 2005.

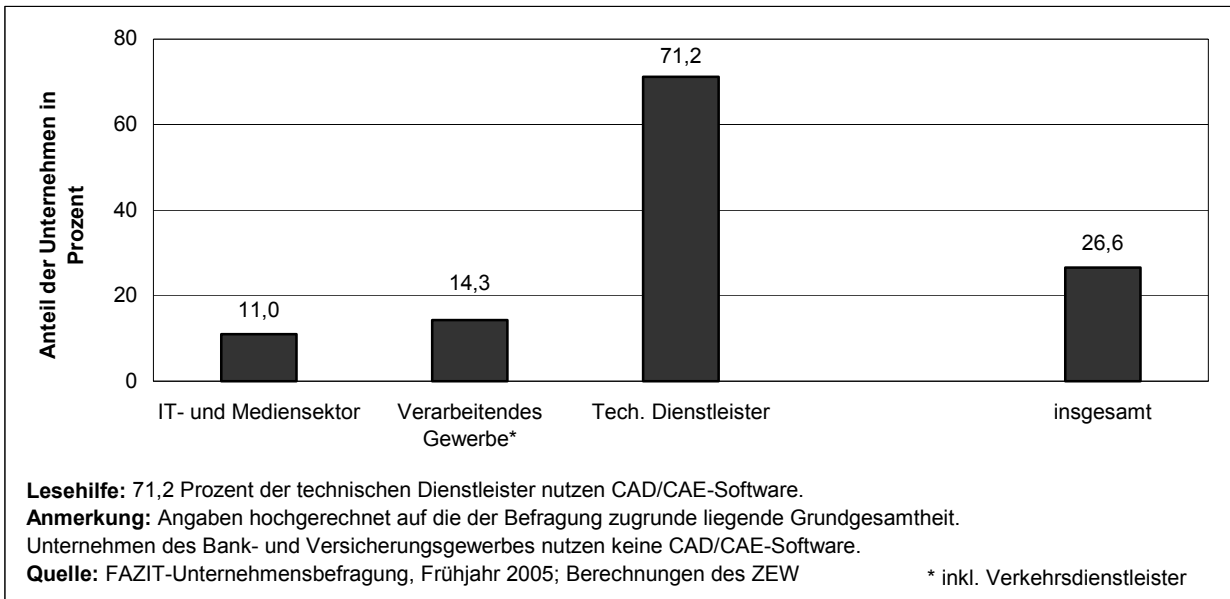
6.5. Unternehmensgröße ist für Softwareanwendungen maßgeblich

In der täglichen Unternehmenspraxis werden verschiedene Softwareanwendungen genutzt. An erster Stelle steht die Bürosoftware, die mit 98 Prozent Verbreitung fast in jedem Unternehmen vorzufinden ist (vgl. Abbildung 6). Mit knapp 90 Prozent folgt die Kommunikationssoftware. Archive und Datenbanken finden in immerhin jedem zweiten Unternehmen Anwendung. Durchschnittlich 38 Prozent der Unternehmen nutzen Multimedia und/oder Grafiksoftware. Weniger verbreitet ist Software für Computer Aided Design (CAD) und Computer Aided Engineering (CAE) mit knapp 27 Prozent. Eine Betrachtung nach Branchen zeigt hier jedoch, dass CAD und CAE erwartungsgemäß vor allem in der Branche technische Dienstleister, und zwar bei 71 Prozent der Unternehmen, eingesetzt wird (vgl. Abbildung 7). Am unteren Ende rangieren Software für Planung, Steuerung und Controlling (knapp 19 Prozent) sowie die relativ speziellen Softwareentwicklungsprogramme (14 Prozent).

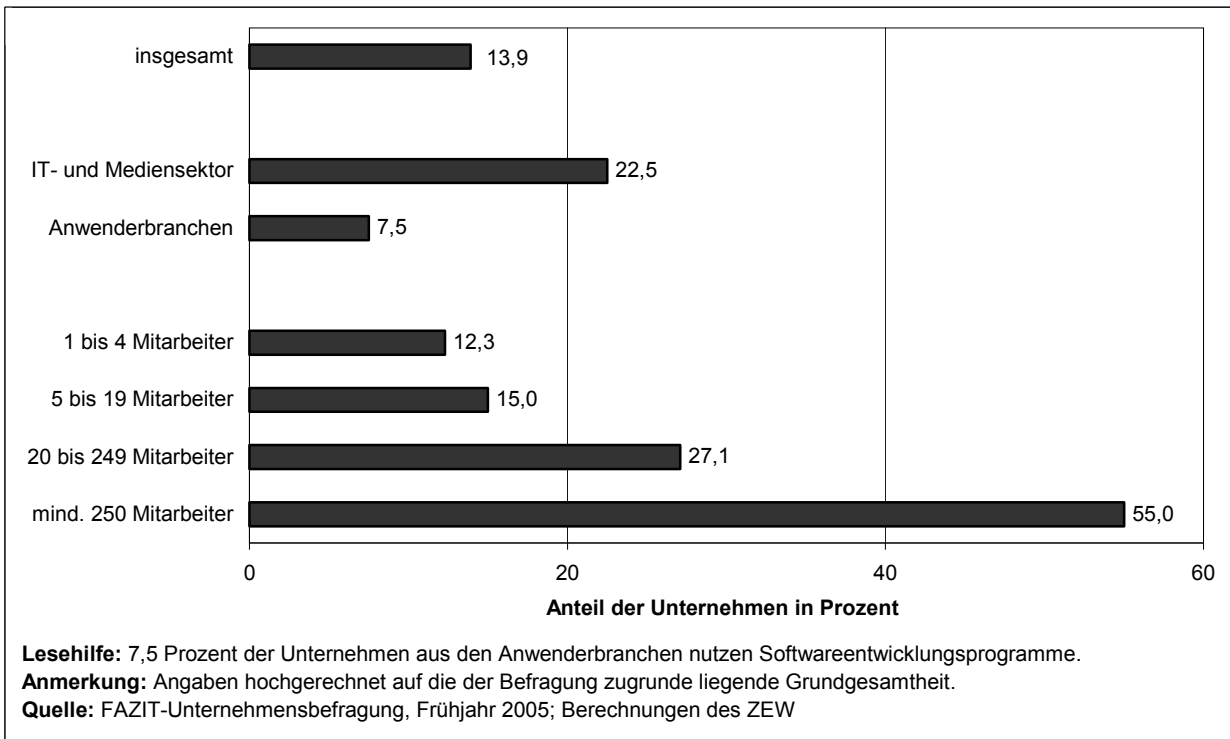
Abbildung 6: Verbreitung von Softwareanwendungen



Generell steigt die Nutzungswahrscheinlichkeit für alle genannten Softwareanwendungen mit zunehmender Unternehmensgröße an. Die geringste Streuung zeigt sich bei der Bürosoftware, die auch in den kleinen Unternehmen mit ein bis vier Beschäftigten bei einer Verbreitung von 97 Prozent liegt und in jedem Unternehmen mit mindestens 250 Beschäftigten zu finden ist. Dagegen werden Softwareentwicklungsprogramme als Spezialanwendungen nur bei 12 Prozent der kleinen Unternehmen (1 bis 4 Beschäftigte), aber immerhin bei 55 Prozent der großen Unternehmen (ab 250 Beschäftigte) eingesetzt.

Abbildung 7: Nutzung von CAD- und CAE-Software nach Branchen

Am häufigsten werden Programme zur Entwicklung von Software in der IT- und Medienbranche, bei knapp 23 Prozent der Unternehmen, eingesetzt. In den Anwenderbranchen ist die Entwicklung von Software und daher auch die Anwendung entsprechender Programme mit einem Anteil von 8 Prozent der Unternehmen eher selten (vgl. Abbildung 8).

Abbildung 8: Verbreitung von Softwareentwicklungsprogrammen nach Branchen und Größenklassen

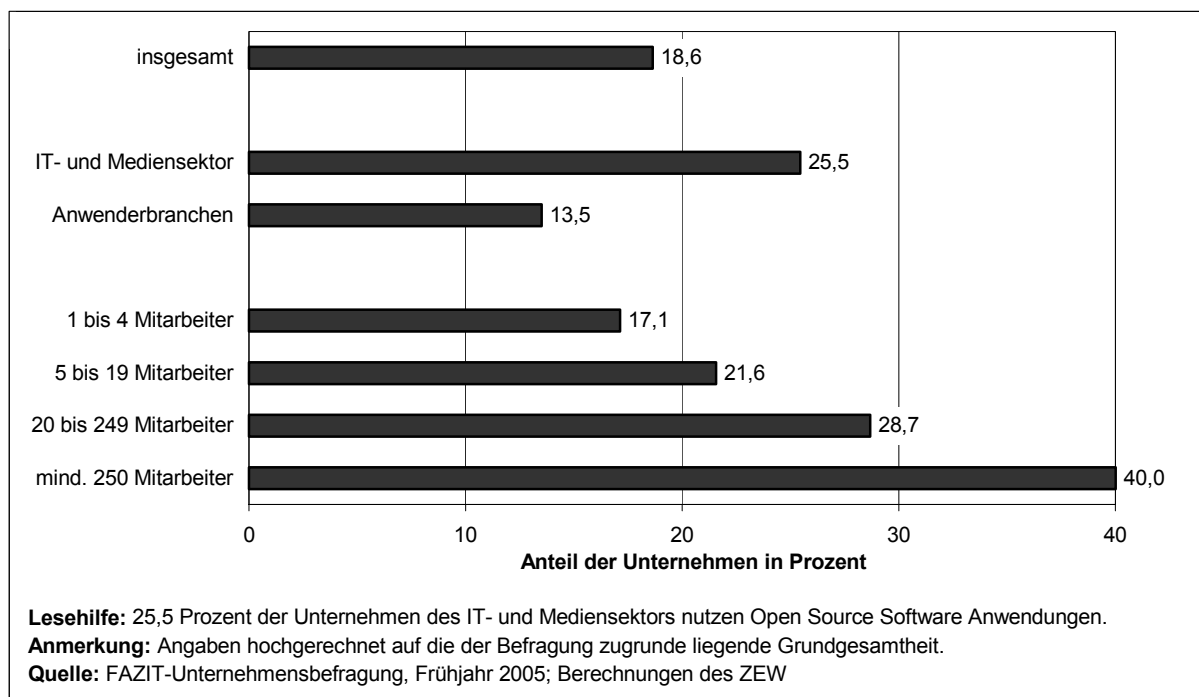
6.6. Open Source Software

Ein Themenschwerpunkt der ersten FAZIT-Unternehmensbefragung beschäftigt sich mit Open Source Software (OSS) in Unternehmen.¹¹ Neben der Nutzung bzw. Nicht-Nutzung dieser Software stehen insbesondere Faktoren für und gegen den Einsatz von OSS im Mittelpunkt der Befragung. Interessante Ergebnisse liefert auch die Frage, über welchen Informationsstand baden-württembergische Unternehmen bezüglich OSS verfügen.

6.6.1 Nutzung und Einsatz von Open Source Software

Insgesamt nutzen 19 Prozent der baden-württembergischen Unternehmen in irgendeiner Form Open Source Software. Mit diesem Ergebnis liegt Baden-Württemberg nahezu auf gesamtdeutschem Niveau. Nach einer vom ZEW 2004 durchgeführten deutschlandweiten Befragung (vgl. Beitrag Open Source Software ab S.61), nutzen über ein Viertel der Unternehmen mit mehr als vier Beschäftigten OSS. Auch bei der FAZIT-Unternehmensbefragung ergibt sich eine Nutzungsintensität von fast 25 Prozent, wenn man kleine Unternehmen mit weniger als fünf Mitarbeitern nicht berücksichtigt.¹²

Abbildung 9: Nutzung von Open Source Software nach Branchen und Unternehmensgrößenklassen



Zwischen den verschiedenen Branchen treten allerdings große Unterschiede auf. Während nur etwas weniger als 14 Prozent der Unternehmen, die den Anwenderbranchen zuzurechnen sind, OSS einsetzen, ist die Verbreitung im IT- und Mediensektor mit fast 26 Prozent deutlich

¹¹ Weiterführende Informationen zum Thema OSS finden sich in dem Beitrag „Open Source Software (OSS)“ von Ohnemus ab Seite 61 und den dort aufgeführten Literaturverweisen.

¹² Allerdings sind die Ergebnisse auf Grund der unterschiedlichen Branchenabgrenzungen beider Untersuchungen nur beschränkt vergleichbar.

größer (vgl. Abbildung 9). Innerhalb der Anwenderbranche nutzen Unternehmen des Bank- und Versicherungsgewerbes mit einem Anteil von fast 22 Prozent OSS überdurchschnittlich häufig. Betrachtet man den Einsatz von OSS nach Größenklassen, bestätigt sich auch für Baden-Württemberg ein bereits in vergleichbaren Studien festgestelltes Resultat:¹³ Je größer ein Unternehmen, desto größer die Nutzungswahrscheinlichkeit von Open Source Software. So verwenden nur gut 17 Prozent der Unternehmen mit 1 bis 4 Beschäftigten OSS, während bei den großen Unternehmen (mit mind. 250 Beschäftigten) 40 Prozent Open Source Software einsetzen (vgl. Abbildung 9). Dieses Ergebnis könnte zum einen darin begründet liegen, dass in Großunternehmen zahlreichere Einsatzmöglichkeiten für OSS vorhanden sind, aber auch in der Tatsache, dass größere Unternehmen eher eigene EDV-Abteilungen unterhalten, die mit den Möglichkeiten und den Vorteilen von Open Source Software besser vertraut sind.

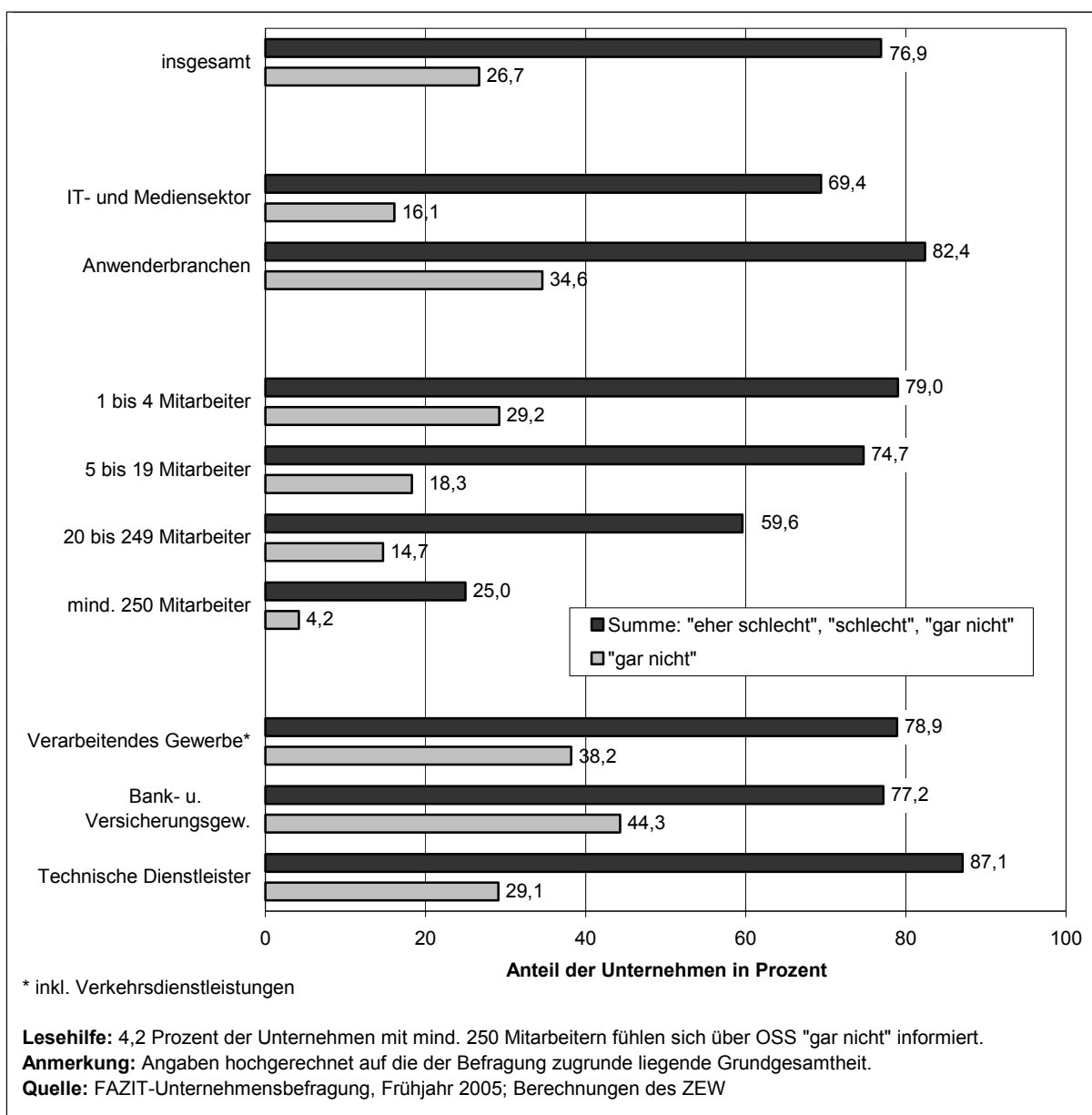
6.6.2 Großer Informationsbedarf bei Open Source Software

Beim Thema Open Source Software besteht bei vielen baden-württembergischen Unternehmen ein Informationsdefizit. Fast 27 Prozent aller Unternehmen geben in einer Selbsteinschätzung an, über das Thema Open Source Software „gar nicht“ informiert zu sein. Bezieht man zusätzlich noch die Unternehmen mit ein, die sich „eher schlecht“ bzw. „schlecht“ über OSS informiert fühlen, ergibt sich ein Wert von fast 77 Prozent (vgl. Abbildung 10).

Es lohnt sich, die Zahlen zum Informationsgrad über OSS genauer zu analysieren, um einen Überblick zu erhalten, bei welchen Unternehmen die meisten Informationsdefizite festzustellen sind. Im IT- und Mediensektor ist der Anteil der Unternehmen, die über OSS nicht informiert sind, mit 16 Prozent erwartungsgemäß deutlich geringer als bei den Unternehmen der Anwenderbranchen (35 Prozent). Innerhalb der Anwenderbranchen sind es vor allem Unternehmen des Bank- und Versicherungsgewerbes sowie das verarbeitende Gewerbe (inklusive Verkehrsdienstleister), die sich zu 44 bzw. 38 Prozent über Open Source Software gar nicht informiert fühlen.

¹³ Ein Beispiel ist wiederum die repräsentative IKT-Umfrage, die das ZEW Ende 2004 bei Unternehmen ab 5 Beschäftigten in Deutschland durchgeführt hat (vgl. Beitrag „Open Source Software“ ab S.61).

Abbildung 10: Bestehende Informationsdefizite über Open Source Software

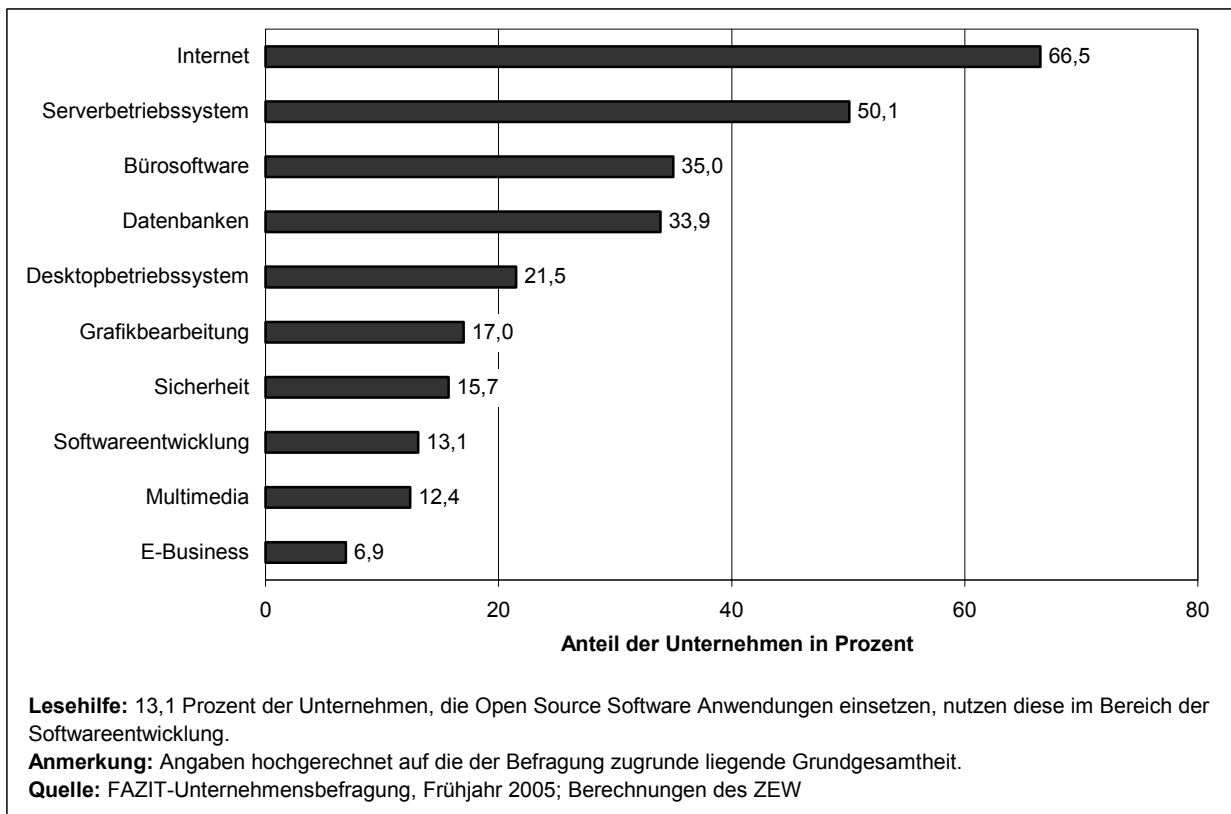


Besonders bei Unternehmen mit weniger als 250 Mitarbeitern besteht ein deutlicher Informationsbedarf. Während bei den kleinen Unternehmen der Anteil der Nicht-Informierten bei überdurchschnittlichen 29 Prozent liegt, sind nur 4 Prozent der Großunternehmen gar nicht über OSS informiert.

6.6.3 Einsatzbereiche von Open Source Software

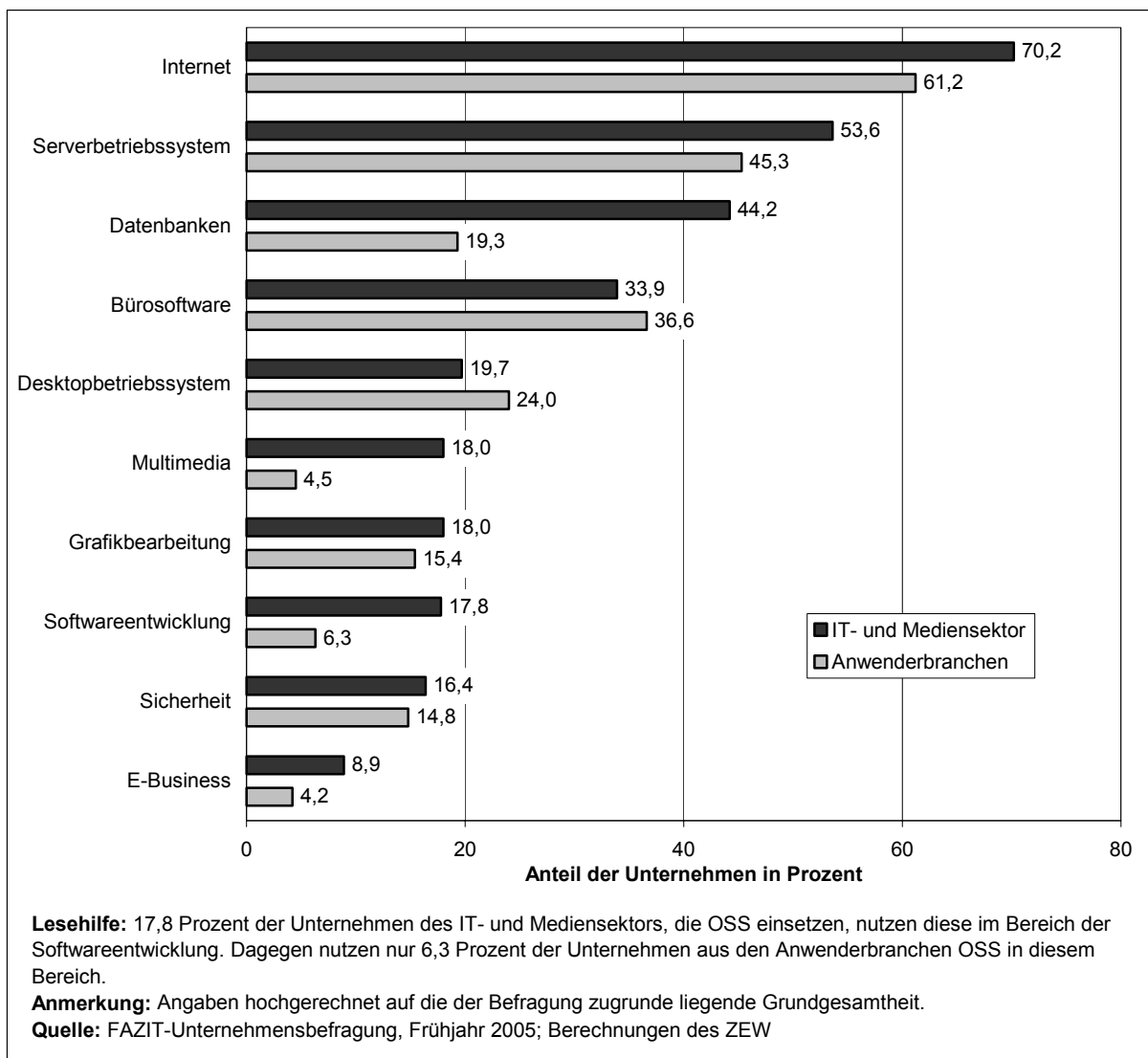
Am weitesten verbreitet sind Open Source Internetanwendungen, wie z.B. der Internetbrowser Firefox oder der Apache Webserver. Über 66 Prozent der Unternehmen, die OSS einsetzen, nutzen diese oder ähnliche Anwendungen. OSS Serverbetriebssysteme liegen mit 50 Prozent an zweiter Stelle, gefolgt von Bürosoftware, die in 35 Prozent der Unternehmen zum Einsatz kommt. In den Bereichen Softwareentwicklung (13 Prozent), Multimedia (12 Prozent) und vor allem E-Business (7 Prozent) werden OSS Produkte dagegen relativ selten eingesetzt (vgl. Abbildung 11).

Abbildung 11: Einsatzbereiche von OSS



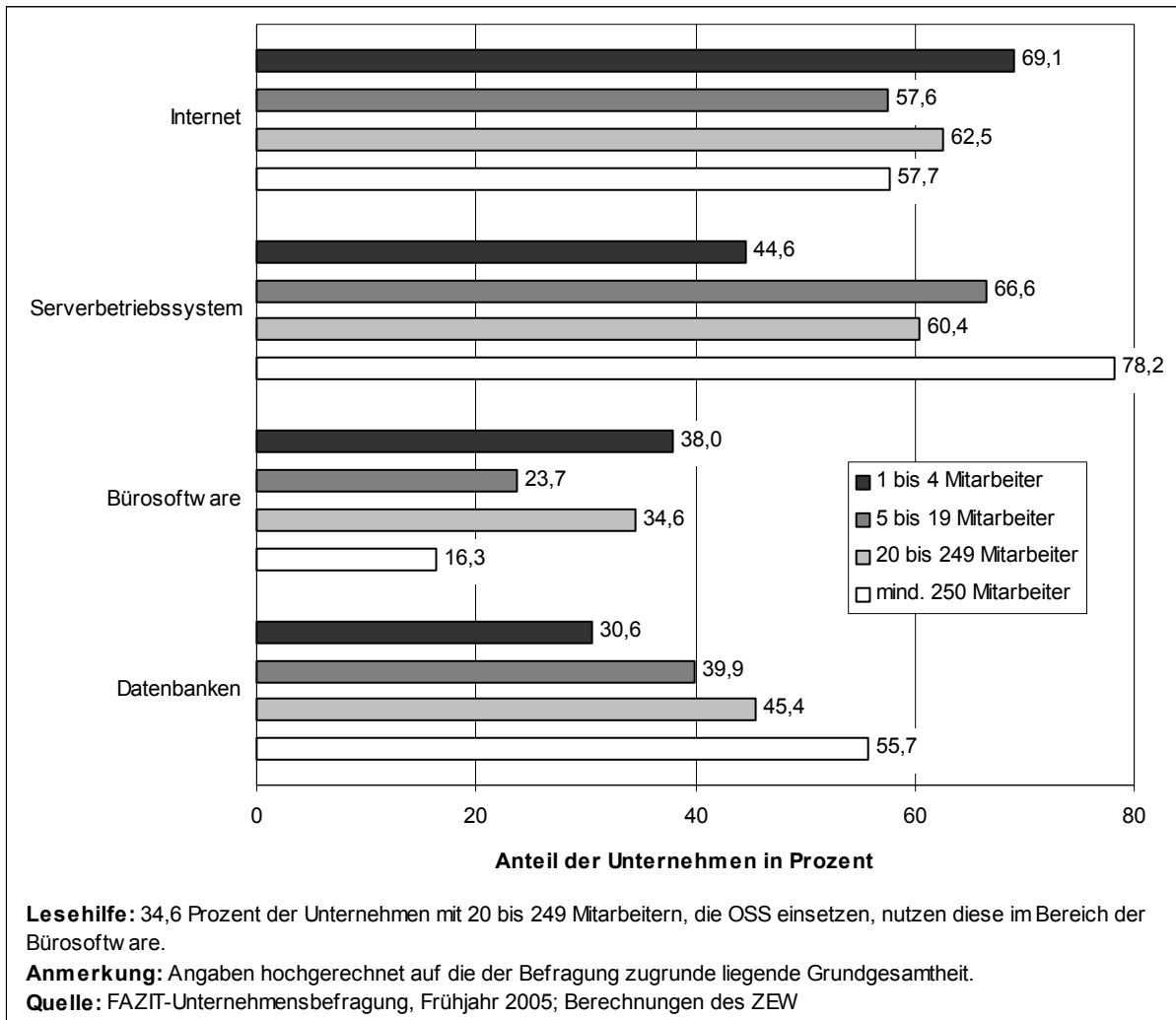
Betrachtet man den IT- und Mediensektor und die Anwenderbranchen getrennt, so zeigt sich, dass in fast allen Bereichen die Unternehmen des IT- und Mediensektors im Vergleich zu den Anwenderbranchen OSS stärker nutzen. Besonders deutlich sind die Nutzungsunterschiede auf den Gebieten Multimedia, Softwareentwicklung, E-Business und Datenbanken. Eine relativ stärkere Nutzung bei den Anwenderbranchen gibt es nur im Bereich der Bürosoftware und den Desktopbetriebssystemen (vgl. Abbildung 12).

Abbildung 12: Nutzung von OSS nach Einsatzbereichen und Branchen



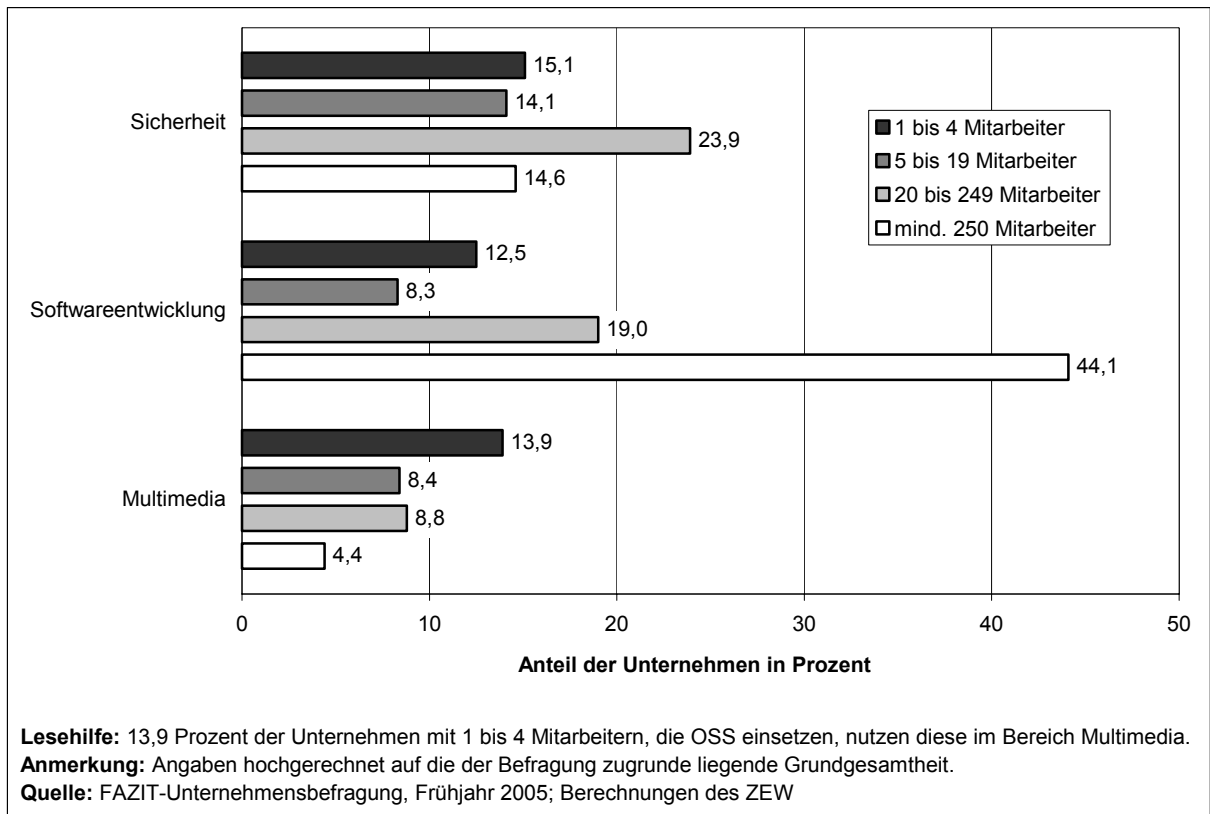
Die vier insgesamt am weitesten verbreiteten Einsatzgebiete von OSS (Internet, Serverbetriebssysteme, Datenbanken und Bürosoftware) sind in Abbildung 13 nach Größenklassen dargestellt. Während Bürosoftware besonders bei kleinen Firmen beliebt ist, kommen Serverbetriebssysteme und Datenbanken häufiger in Großunternehmen zum Einsatz.

Abbildung 13: Nutzung von OSS nach Einsatzbereichen und Anzahl der Mitarbeiter (1)



Interessante Einsichten liefert auch die Betrachtung der Nutzung nach Größenklassen bei den relativ selten eingesetzten OSS Anwendungen. Im Bereich Sicherheit und Multimedia treten zwar Unterschiede auf, diese sind jedoch im Vergleich zur Softwareentwicklung eher gering. Unternehmen mit mindestens 250 Beschäftigten nutzen zu 44 Prozent OSS Softwareentwicklungsprogramme. Der Anteil in den kleineren Größenklassen liegt dagegen nur zwischen 8 und 19 Prozent (vgl. Abbildung 14).

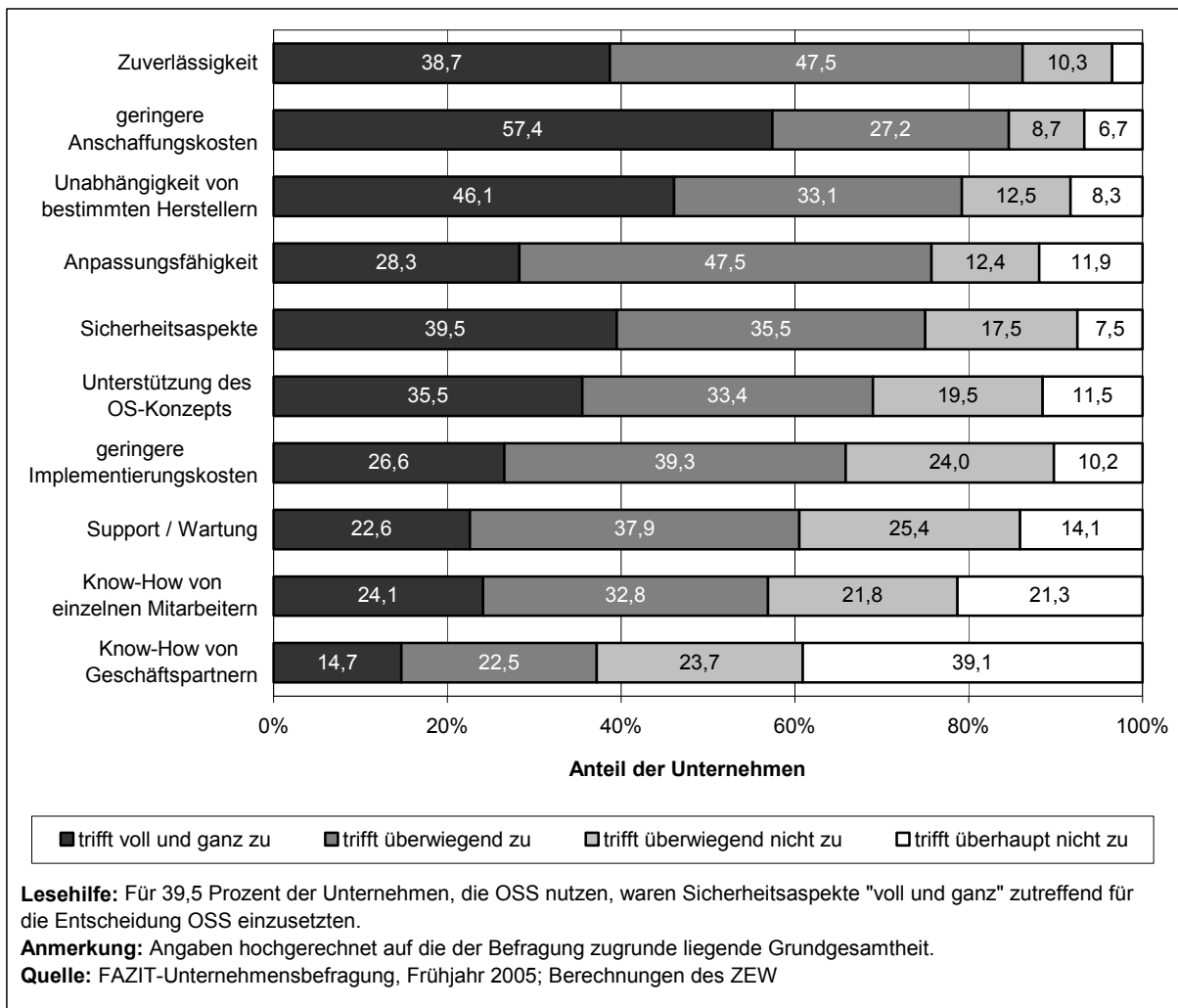
Abbildung 14: Nutzung von OSS nach Einsatzbereichen und Anzahl der Mitarbeiter (2)



6.6.4 Zuverlässigkeit und Kostenaspekte wichtigste Gründe für den Einsatz von OSS

Als wichtigster Faktor für den Einsatz von Open Source Software wurde mit über 86 Prozent die Zuverlässigkeit dieser Software genannt. Nur geringfügig weniger Unternehmen geben an, dass Kostenaspekte in Form von geringeren Anschaffungskosten den Ausschlag für die Entscheidung, OSS einzusetzen, gegeben haben. Für insgesamt 57 Prozent der Unternehmen trifft das Kostenargument sogar „voll und ganz“ zu. Dagegen spielen das Know-How von einzelnen Mitarbeitern (57 Prozent) und das Know-How von Geschäftspartnern (37 Prozent) bezüglich OSS nur eine geringe Rolle für die OSS Einsatzentscheidung (vgl. Abbildung 15).

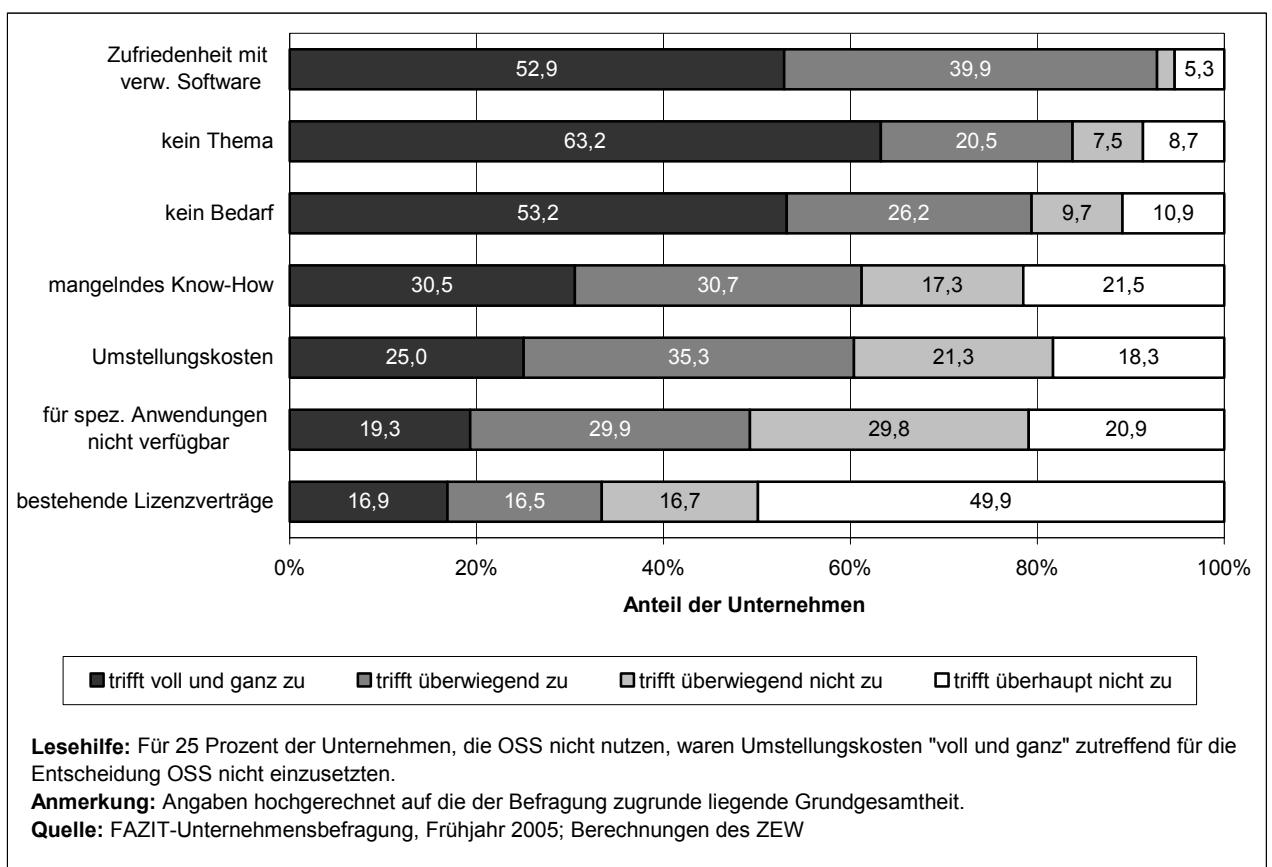
Abbildung 15: Faktoren für den Einsatz von Open Source Software



6.6.5 Hemmnisse für den Einsatz von Open Source Software

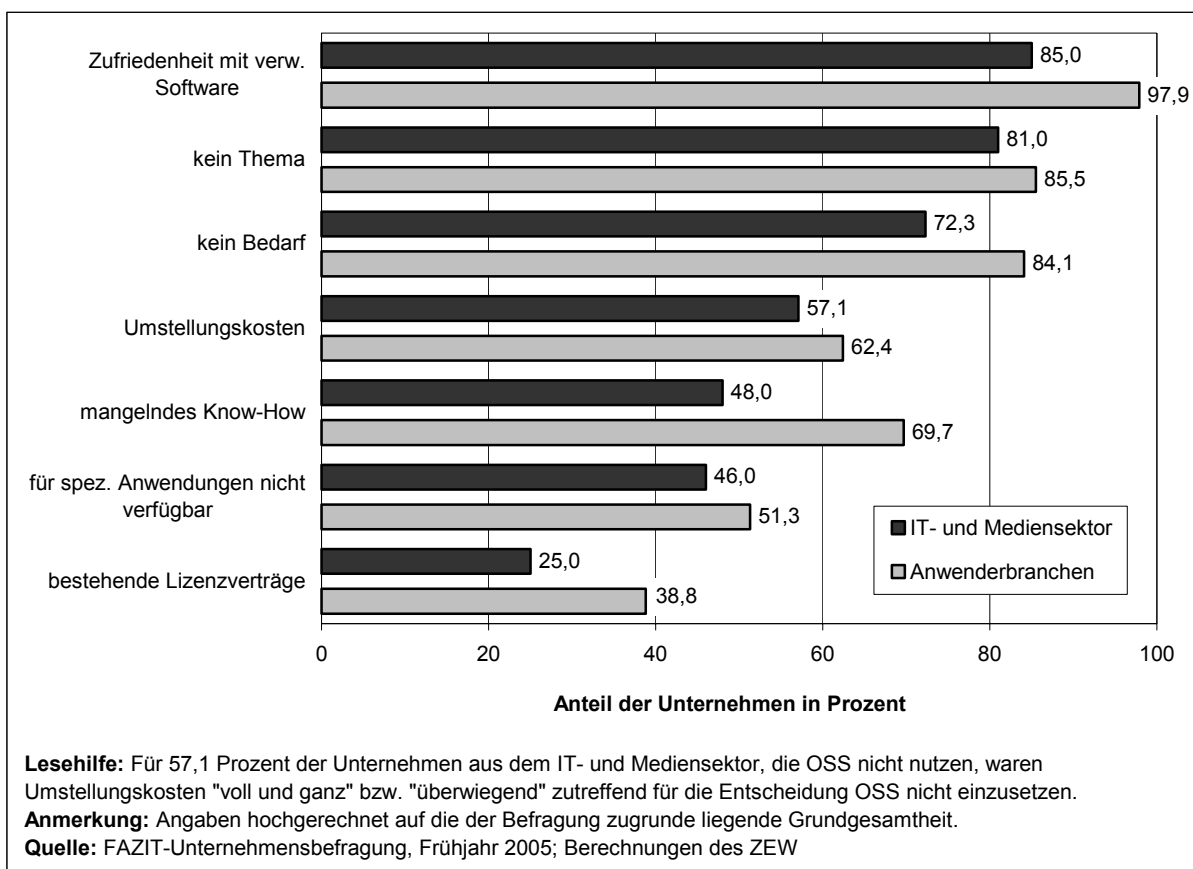
Unternehmen, die keine Open Source Software einsetzen, tun dies hauptsächlich aus Zufriedenheit mit der verwendeten (kommerziellen) Software. 93 Prozent der Unternehmen nennen diesen Grund als „voll“ bzw. „überwiegend“ zutreffend. Dass die Verwendung von OSS Systemen bisher kein Thema im Unternehmen war, sagen 84 Prozent. Mit einer Zustimmungsrate von 79 Prozent rangiert der Aspekt, dass im Unternehmen kein Bedarf für OSS besteht, an dritter Stelle. Bestehende Lizenzverträge spielen dagegen kaum eine Rolle bei der Entscheidung gegen OSS. Nur für etwas mehr als 33 Prozent der Unternehmen trifft dieser Punkt „voll“ bzw. „überwiegend“ zu (vgl. Abbildung 16).

Abbildung 16: Faktoren gegen den Einsatz von Open Source Software



Interessanterweise spielen alle Hemmnisfaktoren in den Anwenderbranchen eine (zum Teil deutlich) größere Rolle als bei den Unternehmen des IT- und Mediensektors (vgl. Abbildung 17). Dies ist ein Hinweis auf eine generell höhere Hemmschwelle der Anwenderbranchen bei der Verwendung von OSS. Den größten Unterschied zwischen beiden Sektoren weist die Kategorie „bestehende Lizenzverträge“ auf. Nur 25 Prozent der Unternehmen des IT- und Mediensektors nennen diesen Aspekt als Grund gegen den Einsatz von OSS. Dieser Wert liegt in den Anwenderbranchen um gut die Hälfte höher (39 Prozent). Ebenfalls deutliche Unterschiede zwischen beiden Sektoren bestehen bei der Kategorie „mangelndes Know-How im Unternehmen“. Hier liegt der Wert für die Anwenderbranchen um 45 Prozent über dem Wert des IT- und Mediensektors.

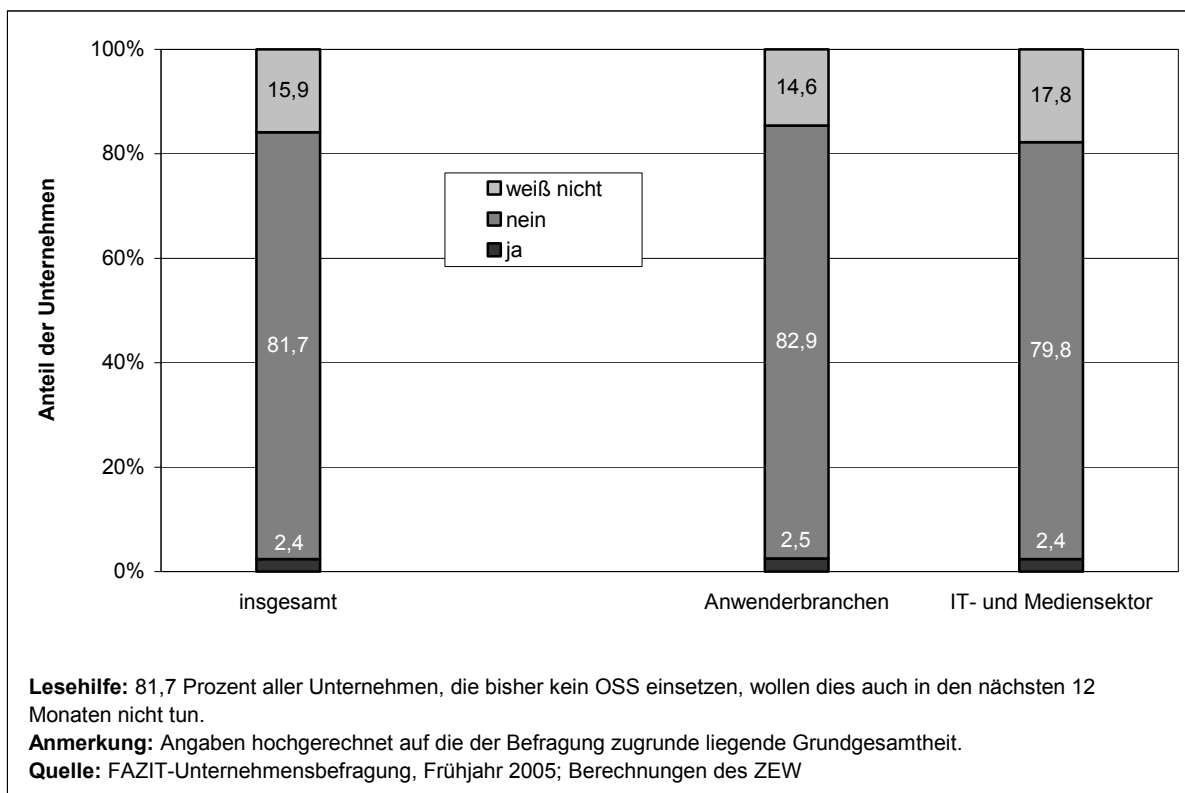
Abbildung 17: Faktoren gegen den Einsatz von Open Source Software nach Branchen



6.6.6 Geplanter Einsatz von Open Source Software bis Mitte 2006 gering

Unternehmen, die bisher keine Open Source Software eingesetzt haben, planen den Einsatz dieser Technologie auch in der nahen Zukunft kaum. Nur 2,4 Prozent der Unternehmen wollen in den nächsten 12 Monaten OSS erstmals einsetzen. Dagegen sagen über 80 Prozent, dass sie nicht die Absicht verfolgen dies zu tun. In diesem Punkt treten nur geringe Unterschiede zwischen dem IT- und Mediensektor und den Anwenderbranchen auf. Allerdings gibt es einen bedeutenden Anteil (fast 16 Prozent) an Unternehmen, der noch nicht weiß, ob er Open Source Software einsetzen wird (vgl. Abbildung 18).

Abbildung 18: Geplanter Einsatz von OSS in den nächsten 12 Monaten



6.7. IT-Sicherheit

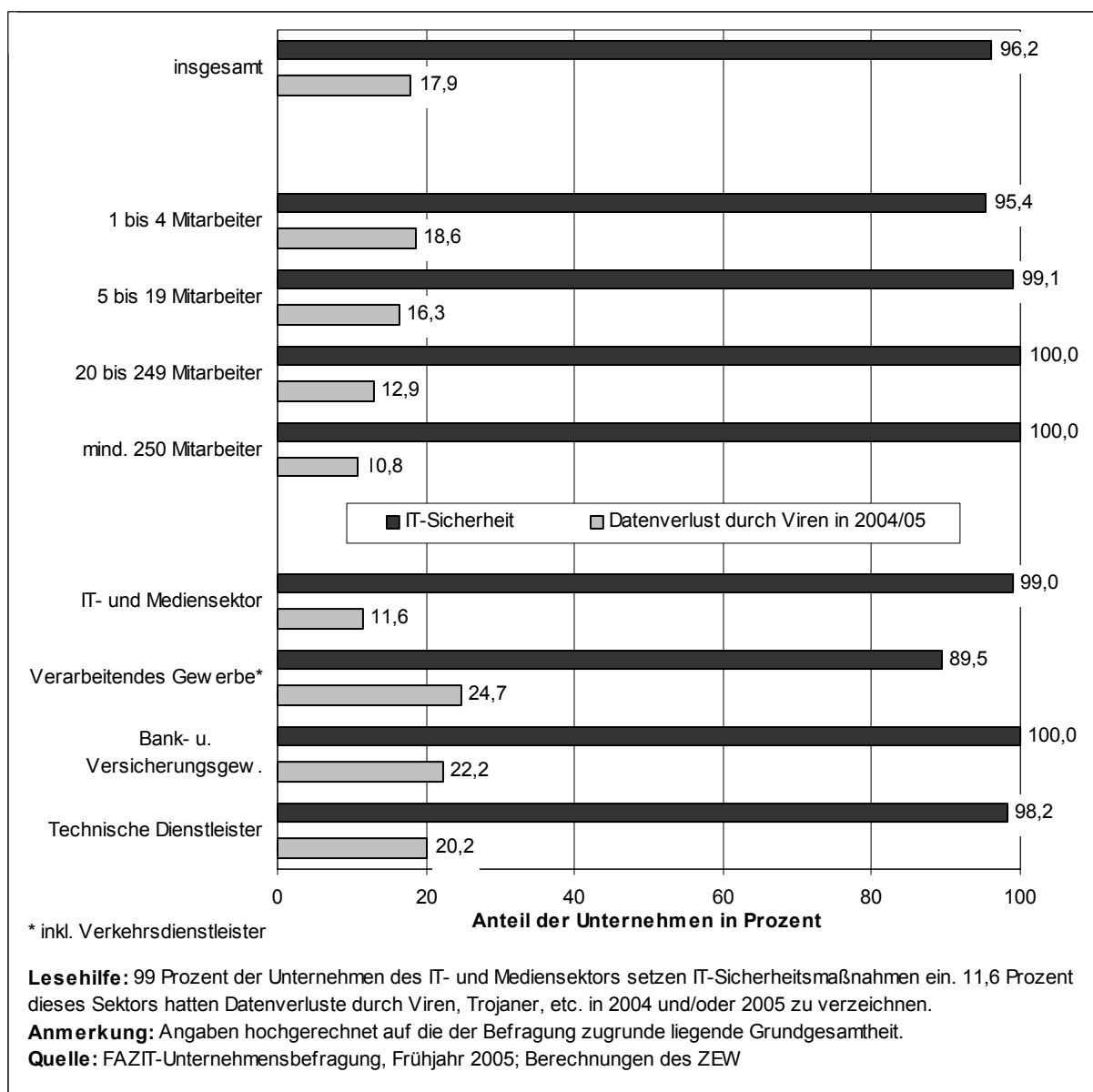
In Anbetracht der zunehmenden Vernetzung von Computern und des damit ständig steigenden Gefahrenpotentials für die Sicherheit von Daten, haben IT-Sicherheitsmaßnahmen in den letzten Jahren stark an Bedeutung gewonnen.¹⁴

6.7.1 Sicherheitsbewusstsein in der IT- und Medienbranche stärker ausgeprägt als in Anwenderbranchen

Insgesamt 96 Prozent der Unternehmen in den befragten Branchen geben an, IT-Sicherheitsvorkehrungen zu treffen. Bei Unternehmen mit mindestens 20 Beschäftigten beträgt dieser Anteil sogar 100 Prozent. Betrachtet man die einzelnen Sicherheitsmaßnahmen separat, so zeigt sich, dass diese bei größeren Unternehmen generell häufiger vertreten sind als bei kleineren, und dass das Sicherheitsbewusstsein in der IT- und Medienbranche stärker ausgeprägt ist als in den Anwenderbranchen.

Auch scheinen die Sicherheitsmaßnahmen in IT- und Medien-Unternehmen effektiver zu sein, denn nur knapp 12 Prozent dieser Unternehmen geben an, in 2004 und/oder 2005 einen Datenverlust auf Grund von Viren, Trojanern, Würmern oder ähnlichem verzeichnet zu haben. Dies liegt deutlich unter dem Durchschnitt von 18 Prozent über alle betrachteten Branchen. Ebenso waren in 2004 und/oder 2005 größere Unternehmen seltener von einem Datenverlust betroffen als kleine und mittlere (vgl. Abbildung 19).

¹⁴ Weiterführende Informationen zum Thema IT-Sicherheit finden sich in dem Beitrag „IT-Sicherheit in Unternehmen“ von Schleife und Schmid ab Seite 81 und den dort aufgeführten Literaturverweisen.

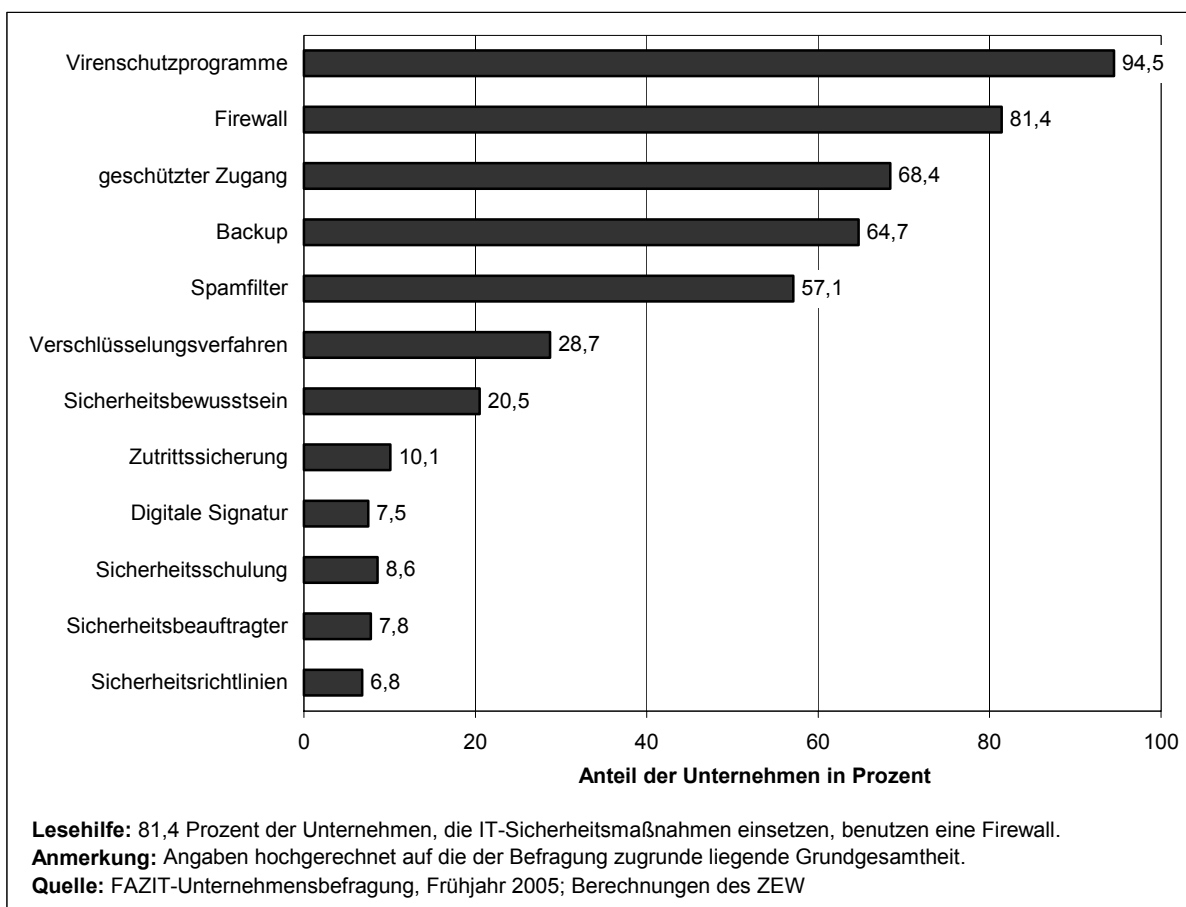
Abbildung 19: Einsatz von IT-Sicherheitsvorkehrungen und Datenverluste durch Viren

6.7.2 Virenschutzprogramme und Firewalls häufigste IT-Sicherheitsmaßnahmen

Die am weitesten verbreitete IT-Sicherheitsmaßnahme sind Virenschutzprogramme (95 Prozent, vgl. Abbildung 20), und zwar sowohl im IT- und Mediensektor (97 Prozent) als auch in den Anwenderbranchen (93 Prozent). Diesen nahezu flächendeckenden Einsatz dieser Sicherheitsmaßnahme bestätigen auch andere Unternehmensstudien (vgl. Beitrag „IT-Sicherheit in Unternehmen“ von Schleife und Schmid, S.81). Alle Unternehmen mit mindestens 250 Beschäftigten verfügen über diese Form der Gefahrenabwehr. Am zweithäufigsten wurde mit gut 81 Prozent der Einsatz einer Firewall bzw. Systeme, die vor unerwünschten Zugriffen schützen und eine möglichst sichere Netznutzung ermöglichen sollen, genannt. Auch diese Systeme sind bei allen Unternehmen ab 250 Beschäftigten flächendeckend vorhanden. Gut zwei Drittel der Unternehmen (68 Prozent) in den betrachteten Branchen ergreift Maßnahmen für einen gesicherten Datenzugang, zum Beispiel durch Passwörter oder biometrische Verfahren.

Die Verbreitung solcher Maßnahmen ist bei großen Unternehmen ab 250 Beschäftigten wiederum vollständig, während sie bei Unternehmen mit weniger als 5 Beschäftigten bei knapp 64 Prozent liegt. In 65 Prozent der Unternehmen findet eine regelmäßige und standardisierte Datensicherung in Form von Backups statt, wobei diese Sicherheitsmaßnahme bei IT- und Medien-Unternehmen mit 77 Prozent deutlich häufiger zum Einsatz kommt als in der Anwenderbranche. Mehr als die Hälfte der Unternehmen (57 Prozent) setzen auf Spamfilter zur Identifikation so genannter "Schrott"-Mails, wobei die Nutzung in Unternehmen mit mindestens 20 Beschäftigten bei über 70 Prozent liegt. Diese Anteile sind im Vergleich zu anderen Studien eher niedrig (vgl. Beitrag „IT-Sicherheit in Unternehmen“ von Schleife und Schmid, S.81)¹⁵.

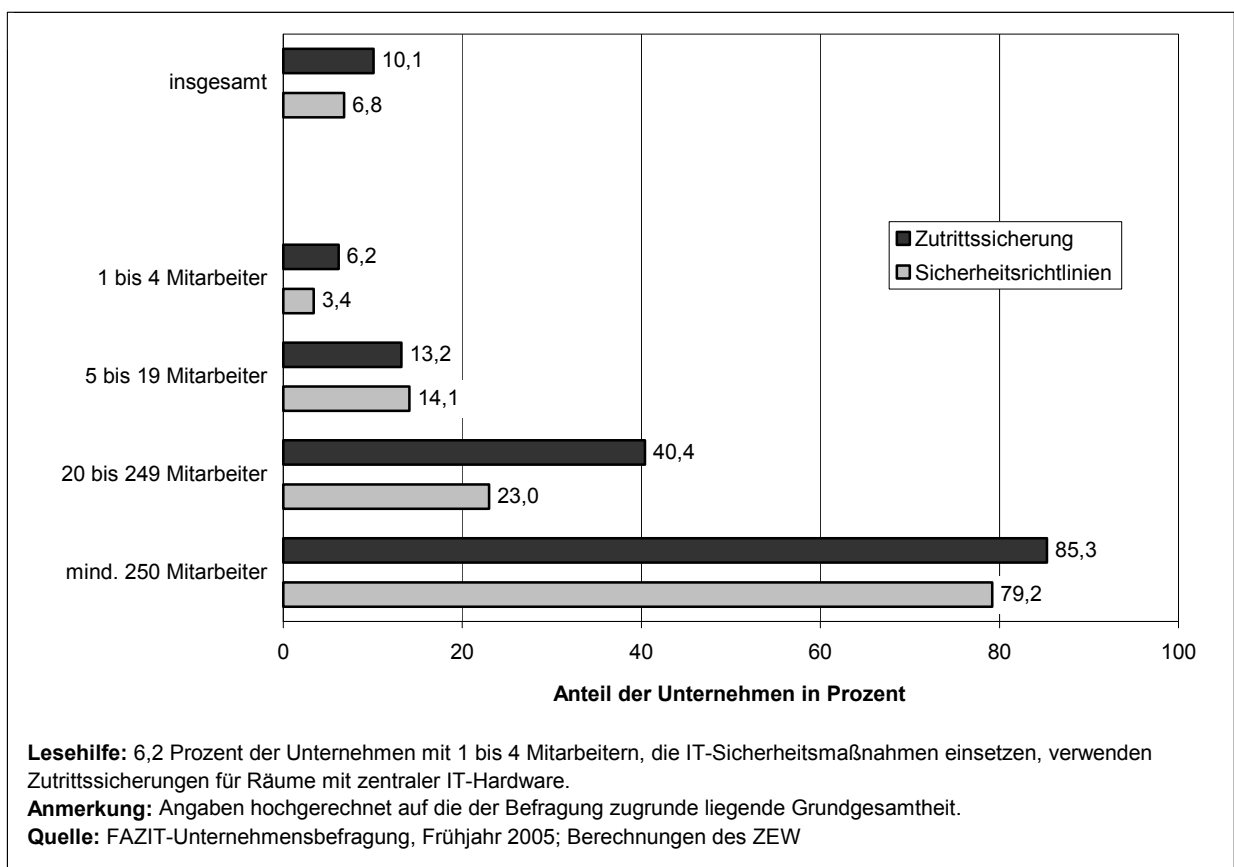
Abbildung 20: Verwendete IT-Sicherheitsmaßnahmen



¹⁵ Allerdings ist bei Vergleichen mit anderen Studien zu berücksichtigen, dass diese in der Regel nicht repräsentativ sind. Beispielsweise war die CAL-Studie, auf die hier Bezug genommen wird, als Online-Befragung konzipiert. Dies lässt vermuten, dass insbesondere IT-intensive Unternehmen an der Umfrage teilgenommen haben, die auch ein überdurchschnittliches Bewusstsein für IT-Sicherheit haben.

Weitergehende Sicherheitsmaßnahmen sind bei deutlich weniger als der Hälfte der Unternehmen zu finden. Knapp 29 Prozent der Unternehmen setzen Verschlüsselungsverfahren bei der Datenübertragung ein. Weniger als 10 Prozent der Unternehmen beschäftigen einen IT-Sicherheitsbeauftragten (8 Prozent), führen Sicherheitsschulungen für Administratoren durch (9 Prozent) oder setzen digitale Signaturen ein (8 Prozent). Lediglich 7 Prozent haben ihre IT-Sicherheitsrichtlinien schriftlich fixiert. Die Zutrittssicherung zu Räumen mit zentraler IT-Hardware spielt naturgemäß vor allem in größeren Unternehmen eine wichtige Rolle. Sie findet sich in 85 Prozent der Unternehmen mit mindestens 250 Beschäftigten im Vergleich zu einem Gesamtdurchschnitt von 10 Prozent. Auch setzen größere Unternehmen verstärkt auf schriftlich fixierte Sicherheitsrichtlinien (vgl. Abbildung 21).

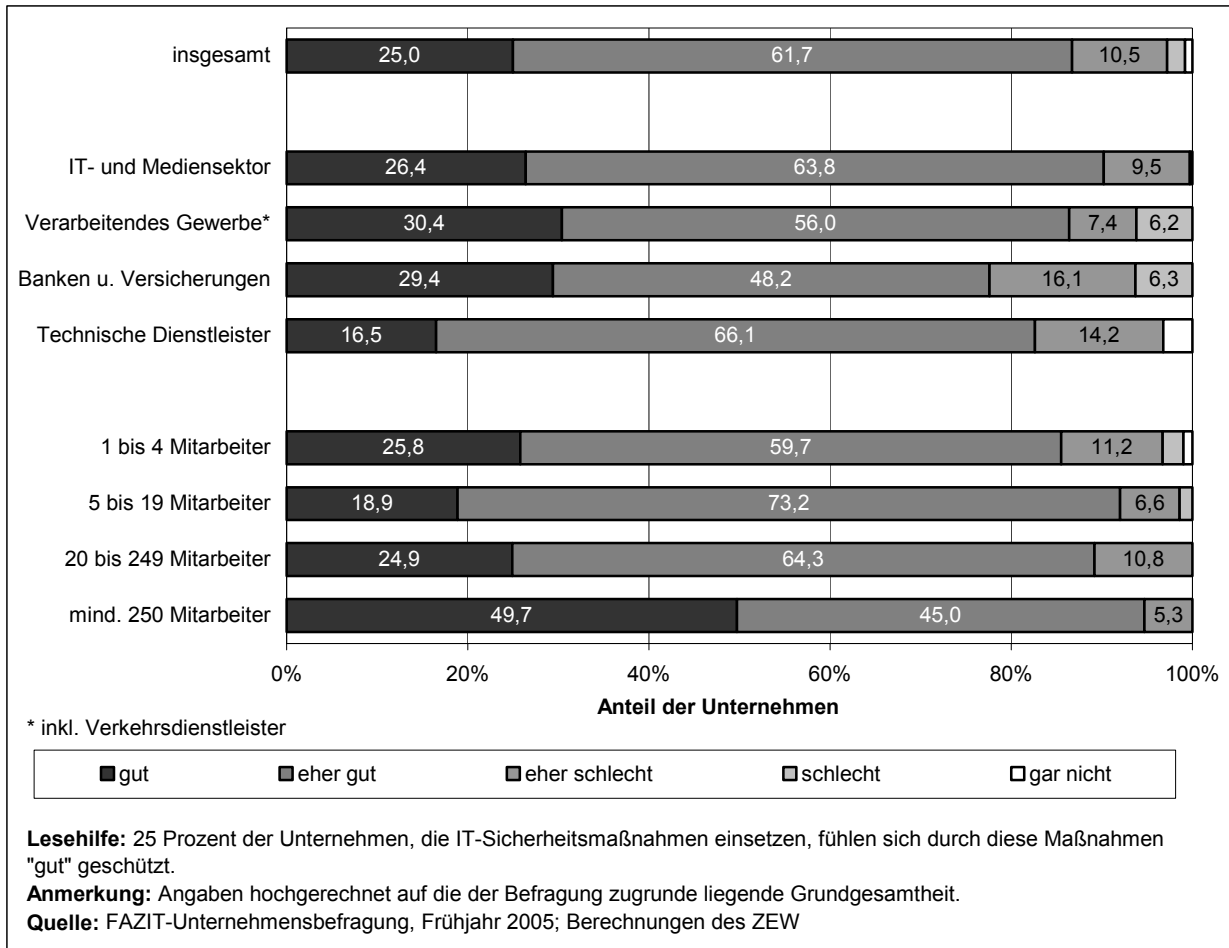
Abbildung 21: Verwendung von Zutrittssicherung und Sicherheitsrichtlinien nach Anzahl der Mitarbeiter



Fragt man die Unternehmen, wie gut sie sich durch die vorgenommenen IT-Sicherheitsmaßnahmen geschützt fühlen, so halten ein Viertel der Unternehmen den Schutz für „gut“, 62 Prozent für „eher gut“. Jedes zehnte Unternehmen fühlt sich „eher schlecht“ und zwei Prozent der Unternehmen fühlen sich „schlecht“ geschützt. Nur 0,8 Prozent sind der Meinung, dass die getroffenen IT-Sicherheitsmaßnahmen keinerlei Schutz bieten. Die positive Einschätzung der Sicherheitsvorkehrungen liegt im IT- und Mediensektor nur leicht über den Werten der Anwenderbranche. Nach Größenklassen betrachtet fühlen sich die größten Unternehmen mit mindestens 250 Beschäftigten am besten geschützt, darunter knapp die Hälfte „gut“ und 45 Prozent

„eher gut“. Bei Unternehmen mit weniger als 250 Beschäftigten entfallen die meisten Antworten auf die „eher gut“-Kategorie (vgl. Abbildung 22).

Abbildung 22: Schutz durch IT-Sicherheitsmaßnahmen

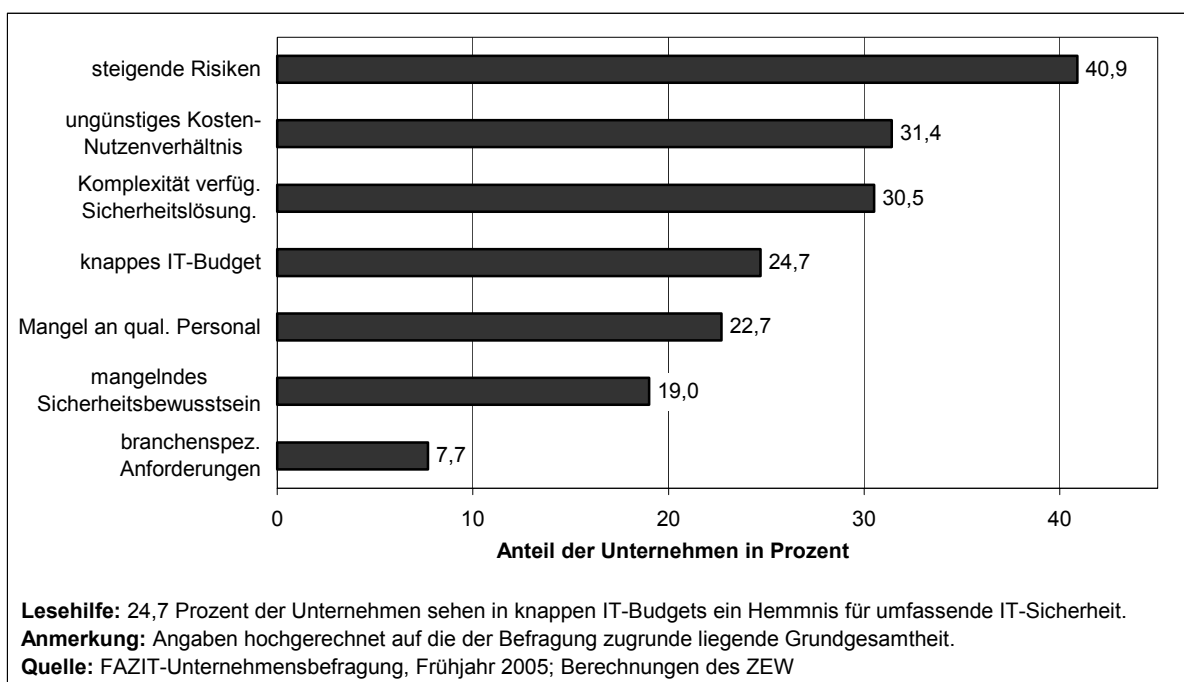


6.7.3 Unternehmensexterne Faktoren als Hemmnis für umfassende IT-Sicherheit

Den Haupthemmnisfaktor für eine umfassende IT-Sicherheit stellen die "steigenden Risiken durch die Weiterentwicklung von Viren sowie anderen gefährdenden Maßnahmen, mit denen die Sicherheitslösungen nicht Schritt halten können", dar. Insgesamt halten 41 Prozent der Unternehmen diesen Faktor für maßgeblich. Fast ein Drittel der Unternehmen (31 Prozent) sehen ein ungünstiges Kosten-Nutzen-Verhältnis als Hemmnis für eine umfassende IT-Sicherheit. Ebenso hoch (31 Prozent) ist der Anteil der Unternehmen, welche die Komplexität der verfügbaren Sicherheitslösungen als Hemmnis betrachten. Als weiterer Hemmnisfaktor für eine umfassende IT-Sicherheit werden von einem Viertel der Unternehmen knappe oder rückläufige IT-Budgets genannt, dicht gefolgt vom Mangel an qualifiziertem Personal (23 Prozent). Generell mangelndes Sicherheitsbewusstsein im Unternehmen gilt für immerhin 19 Prozent der Unternehmen als Problem. Lediglich knapp 8 Prozent der Unternehmen in den betrachteten Branchen sehen einen Hemmnisfaktor darin, dass branchenspezifische Sicherheitsanforderungen bei

den angebotenen Lösungen nicht ausreichend berücksichtigt werden (vgl. Abbildung 23). In anderen Unternehmensbefragungen mit vergleichbaren Antwortkategorien wird das knappe IT-Budget als mit Abstand wichtigster Hemmnisfaktor genannt (vgl. Beitrag „IT-Sicherheit in Unternehmen“ von Schleife und Schmid, S.81). Etwa zwei Drittel der Unternehmen beklagen diesen Umstand.

Abbildung 23: Hemmnisse für eine umfassende IT-Sicherheit im Unternehmen



6.7.4 Kaum Veränderungen des Anteils für IT-Sicherheit am IT-Budget geplant

Für 41 Prozent der Unternehmen macht der Budgetanteil für IT-Sicherheit am gesamten IT-Budget zwischen 1 und 5 Prozent aus, ein Budgetanteil von 6 bis 10 Prozent steht immerhin noch für 13 Prozent der Unternehmen zur Verfügung. Weitere knappe 13 Prozent der Unternehmen haben keinerlei Budget für die IT-Sicherheit angesetzt (vgl. Abbildung 24). Für das Jahr 2005 rechnen die meisten Unternehmen (83 Prozent), mit einem im Vergleich zu 2004 gleich bleibenden Anteil für IT-Sicherheit am IT-Budget. Insgesamt 9 Prozent erwarten eine Erhöhung und 8 Prozent eine Senkung des für IT-Sicherheit zur Verfügung stehenden Budgetanteils (vgl. Abbildung 25 und Abbildung 26).

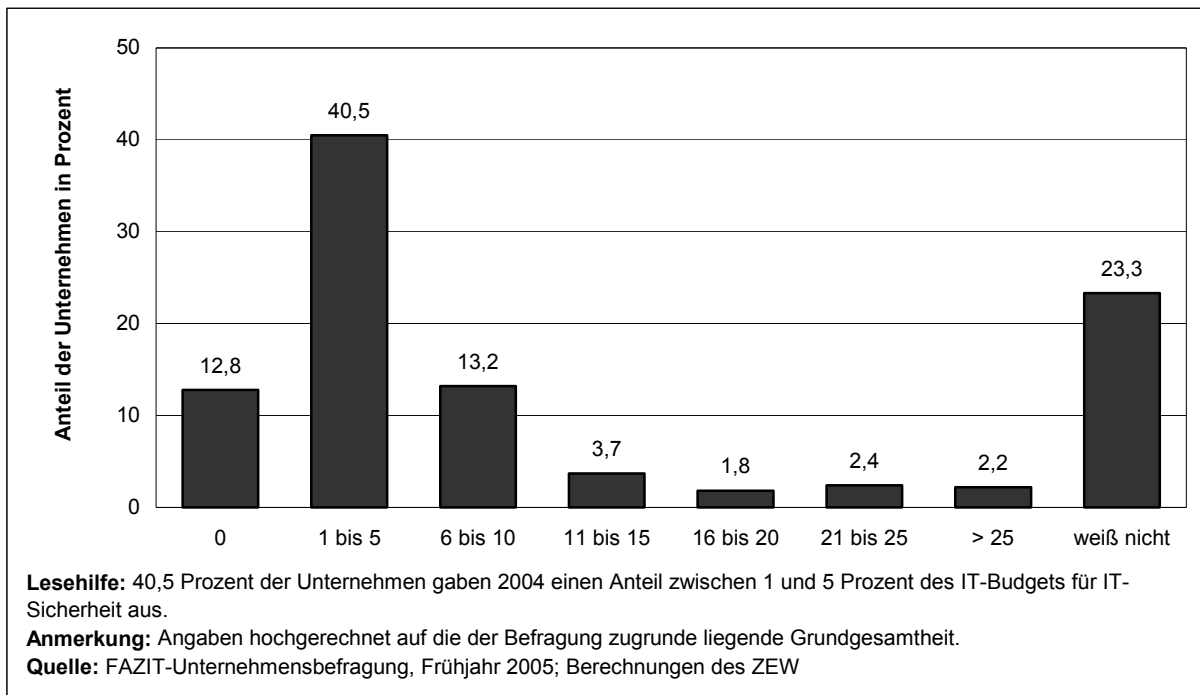
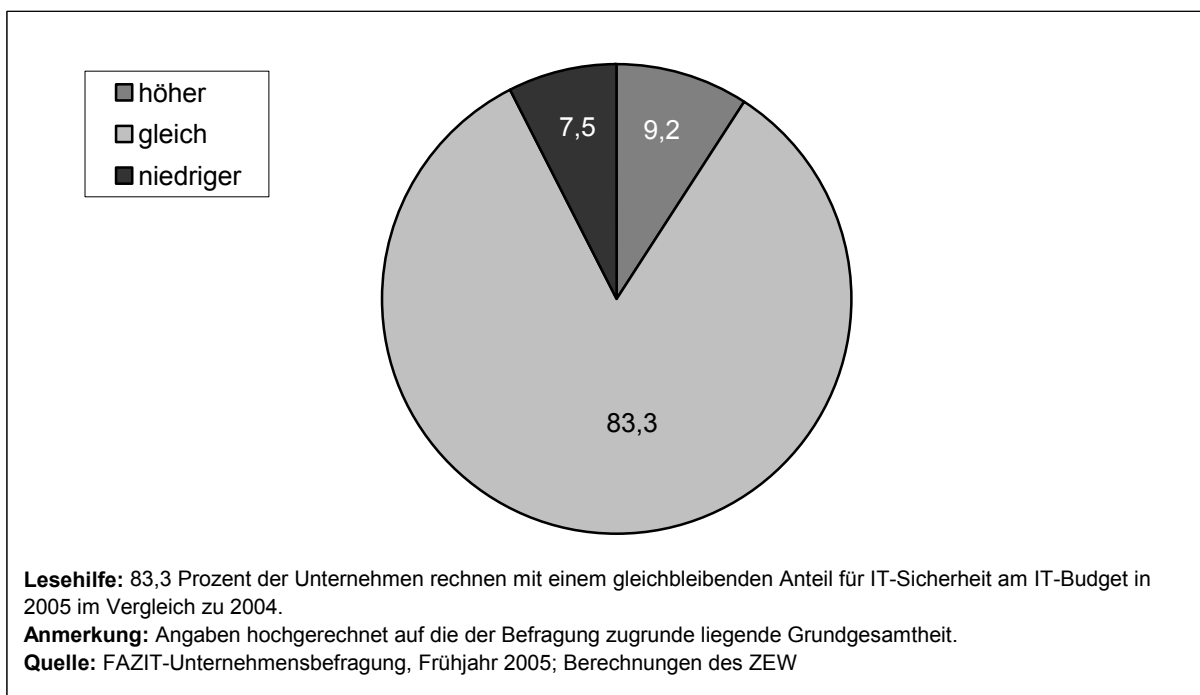
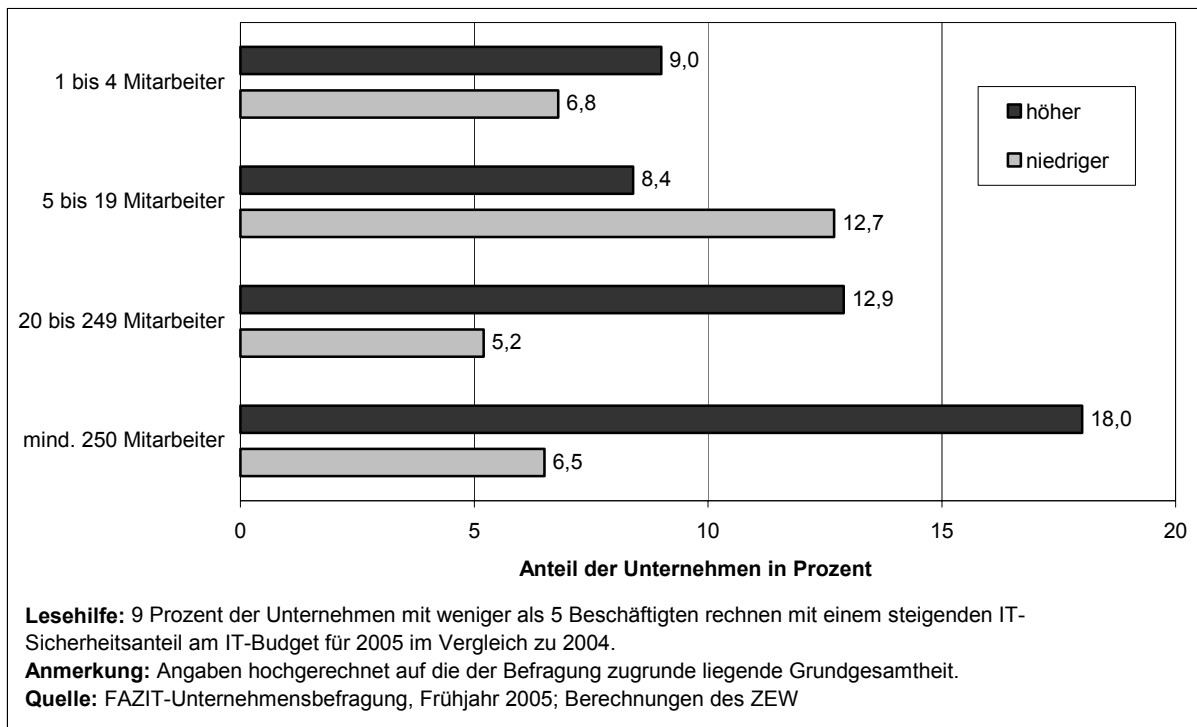
Abbildung 24: Anteil für IT-Sicherheit am gesamten IT-Budget (in Prozent)**Abbildung 25:** Erwarteter Anteil für IT-Sicherheit am IT-Budget für 2005 im Vergleich zu 2004

Abbildung 26: Erwarteter Anteil für IT-Sicherheit am IT-Budget für 2005 im Vergleich zu 2004 nach Anzahl der Mitarbeiter



7. Anhang

Tabelle 8: Branchenabgrenzung

IT- und Mediensektor	
WZ 2003	Bezeichnung
Druck / Verlag	
22.11	Verlegen von Büchern
22.12	Verlegen von Zeitungen
22.13	Verlegen von Zeitschriften
22.15	Sonstiges Verlagsgewerbe
22.21	Drucken von Zeitungen
22.22	Drucken anderer Druckerzeugnisse
22.23	Druckweiterverarbeitung
22.24	Druck- und Mediovorstufe
22.25	Erbringung von sonstigen druckbezogenen Dienstleistungen
Audiovisuelle Medien	
22.14	Verlegen von bespielten Tonträgern und Musikalien
22.31	Vervielfältigung von bespielten Tonträgern
22.32	Vervielfältigung von bespielten Bildträgern
22.33	Vervielfältigung von bespielten Datenträgern
24.65	Herstellung von unbespielten Ton-, Bild- und Datenträgern
74.81	Fotografisches Gewerbe und fotografische Laboratorien
92.11	Film- und Videofilmherstellung
92.13	Kinos
92.2	Rundfunkveranstalter, Herstellung von Hörfunk- und Fernsehprogrammen
92.32.5	Technische Hilfsdienste für kulturelle und unterhaltende Leistungen
(Tele-) Kommunikation	
64.12	Private Post- und Kurierdienste
64.3	Fernmeldedienste
72.1	Hardwareberatung
72.3	Datenverarbeitungsdienste
72.4	Datenbanken
72.5	Instandhaltung und Reparatur von Büromaschinen, Datenverarbeitungsgeräten und -einrichtungen
72.6	Sonstige mit der Datenverarbeitung verbundene Tätigkeiten

Software / DV-Dienstleistungen	
72.21	Verlegen von Software
72.22	Softwareberatung und -entwicklung
Werbung / Marktkommunikation	
74.13	Markt- und Meinungsforschung
74.14	Unternehmens- und Public-Relations-Beratung
74.4	Werbung
74.87.1	Ausstellungs-, Messe- und Warenmarkteinrichtungen
IT- / Medien-Hardware	
30.01	Herstellung von Büromaschinen
30.02	Herstellung von Datenverarbeitungsgeräten und -einrichtungen
32.1	Herstellung von elektronischen Bauelementen
32.2	Herstellung von Geräten und Einrichtungen der Telekommunikationstechnik
32.3	Herstellung von Rundfunkgeräten sowie phono- und videotechnischen Geräten
33.40.3	Herstellung von Foto-, Projektions- und Kinogeräten
71.33	Vermietung von Büromaschinen, Datenverarbeitungsgeräten und -einrichtungen
Inhalte-Dienstleister	
71.40.3	Leihbüchereien und Lesezirkel
71.40.4	Videotheken
74.85	Sekretariats-, Schreib- und Übersetzungsdienste; Copy-Shops
74.87.5	Auskunfteien
92.12	Filmverleih und Videoprogrammanbieter
92.31.6	Selbstständige Schriftstellerinnen und Schriftsteller
92.31.7	Selbstständige Bühnen-, Film-, Hörfunk- und Fernsehkünstlerinnen und -künstler
92.40.1	Korrespondenz- und Nachrichtenbüros
92.40.2	Selbstständige Journalistinnen, Journalisten, Pressefotografinnen und Pressefotografen
92.51	Bibliotheken und Archive

Anwenderbranchen:

WZ 2003	Bezeichnung
Herstellung von chemischen Erzeugnissen	
24.11	Herstellung von Industriegasen
24.12	Herstellung von Farbstoffen und Pigmenten
24.13	Herstellung von sonstigen anorganischen Grundstoffen und Chemikalien
24.14	Herstellung von sonstigen organischen Grundstoffen und Chemikalien
24.15	Herstellung von Düngemitteln und Stickstoffverbindungen
24.16	Herstellung von Kunststoffen in Primärformen
24.17	Herstellung von synthetischem Kautschuk in Primärformen
24.2	Herstellung von Schädlingsbekämpfungsmitteln, Pflanzenschutz- und Desinfektionsmitteln
24.3	Herstellung von Anstrichmitteln, Druckfarben und Kittungen
24.41	Herstellung von pharmazeutischen Grundstoffen
24.42	Herstellung von pharmazeutischen Spezialitäten und sonstigen pharmazeutischen Erzeugnissen
24.51	Herstellung von Seifen, Wasch-, Reinigungs- und Poliermitteln
24.52	Herstellung von Duftstoffen und Körperpflegemitteln
24.61	Herstellung von pyrotechnischen Erzeugnissen
24.62	Herstellung von Klebstoffen und Gelatine
24.63	Herstellung von ätherischen Ölen
24.64	Herstellung von fotochemischen Erzeugnissen
24.66	Herstellung von sonstigen chemischen Erzeugnissen, anderweitig nicht genannt
24.7	Herstellung von Chemiefasern

Maschinenbau	
29.11	Herstellung von Verbrennungsmotoren und Turbinen (ohne Motoren für Luft- und Straßenfahrzeuge)
29.12	Herstellung von Pumpen und Kompressoren
29.13	Herstellung von Armaturen
29.14	Herstellung von Lagern, Getrieben, Zahnrädern und Antriebselementen
29.21	Herstellung von Öfen und Brennern
29.22	Herstellung von Hebezeugen und Fördermitteln
29.23	Herstellung von kälte- und lufttechnischen Erzeugnissen, nicht für den Haushalt
29.24	Herstellung von sonstigen nicht wirtschaftszweigspezifischen Maschinen, anderweitig nicht genannt
29.31	Herstellung von land- und forstwirtschaftlichen Zugmaschinen
29.32	Herstellung von sonstigen land- und forstwirtschaftlichen Maschinen
29.41	Herstellung von handgeführten kraftbetriebenen Werkzeugen
29.42	Herstellung von Werkzeugmaschinen für die Metallbearbeitung
29.43	Herstellung von Werkzeugmaschinen, anderweitig nicht genannt
29.51	Herstellung von Maschinen für die Metallerzeugung, von Walzwerkseinrichtungen und Gießmaschinen
29.52	Herstellung von Bergwerks-, Bau- und Baustoffmaschinen
29.53	Herstellung von Maschinen für das Ernährungsgewerbe und die Tabakverarbeitung
29.54	Herstellung von Maschinen für das Textil-, Bekleidungs- und Ledergewerbe
29.55	Herstellung von Maschinen für das Papiergewerbe
29.56	Herstellung von Maschinen für bestimmte Wirtschaftszweige, anderweitig nicht genannt
29.6	Herstellung von Waffen und Munition
29.71	Herstellung von elektrischen Haushaltsgeräten
29.72	Herstellung von nicht elektrischen Heiz-, Koch-, Heißwasser- und Heißluftgeräten, anderweitig nicht genannt
Medizin-, Mess-, Steuer- und Regelungstechnik, Optik, Uhren	
33.1	Herstellung von medizinischen Geräten und orthopädischen Erzeugnissen
33.2	Herstellung von Mess-, Kontroll-, Navigations- u.ä. Instrumenten und Vorrichtungen
33.3	Herstellung von industriellen Prozesssteuerungseinrichtungen
33.4	Herstellung von optischen und fotografischen Geräten (ohne 33.40.3 Herstellung von Foto-, Projektions- und Kinogeräten)
33.5	Herstellung von Uhren
Herstellung von Kraftwagen und Kraftwagenteilen	
34.1	Herstellung von Kraftwagen und Kraftwagenmotoren
34.2	Herstellung von Karosserien, Aufbauten und Anhängern
34.3	Herstellung von Teilen und Zubehör für Kraftwagen und Kraftwagenmotoren

Verkehr / Hilfs- und Nebentätigkeiten für den Verkehr	
60.21	Personenbeförderung im Linienverkehr zu Land
60.22	Betrieb von Taxis und Mietwagen mit Fahrer
60.24	Güterbeförderung im Straßenverkehr
63.12	Lagerei
63.21	Sonstige Hilfs- und Nebentätigkeiten für den Landverkehr
63.3	Reisebüros und Reiseveranstalter
63.4	Spedition, sonstige Verkehrsvermittlung
Bank- / Versicherungsgewerbe	
65.11	Zentralbanken
65.12	Kreditinstitute (ohne Spezialkreditinstitute)
65.21	Institutionen für Finanzierungsleasing
65.22	Spezialkreditinstitute
65.23	Finanzierungsinstitutionen, anderweitig nicht genannt
66.01	Lebensversicherungen
66.02	Pensions- und Sterbekassen
66.03	Sonstiges Versicherungsgewerbe
67.11	Effekten- und Warenbörsen
67.12	Effektenvermittlung und -verwaltung (ohne Effektenverwahrung)
67.13	Sonstige mit dem Kreditgewerbe verbundene Tätigkeiten
67.2	Mit dem Versicherungsgewerbe verbundene Tätigkeiten
Technische Dienstleister	
73.1	Forschung und Entwicklung im Bereich Natur-, Ingenieur-, Agrarwissenschaften und Medizin
73.2	Forschung und Entwicklung im Bereich Rechts-, Wirtschafts- und Sozialwissenschaften sowie im Bereich Sprach-, Kultur- und Kunstwissenschaften
74.2	Architektur- und Ingenieurbüros
74.3	Technische, physikalische und chemische Untersuchung

Abbildung 27: Fragebogen der ersten FAZIT-Unternehmensbefragung

Bitte senden Sie den ausgefüllten Fragebogen bis Freitag, den 6. Mai 2005, an Fax-Nr. 0621/1235-4300
(oder per Post, Gebühr zahlt Empfänger) zurück an das Zentrum für Europäische Wirtschaftsforschung GmbH (ZEW)

FAZIT – Forschung: Unternehmensbefragung in Baden-Württemberg

ZEW

FAZIT – Unternehmensbefragung

Postfach 10 34 43

68034 Mannheim

Beantworten Sie bitte die folgenden Fragen für Ihr Hauptgeschäftsfeld.

Die Geschäftslage in meinem/unserem Unternehmen beurteile ich zur Zeit als ...

gut eher gut eher schlecht schlecht

Die Geschäftslage in Ihrem Unternehmen wird sich mittelfristig (in den nächsten 6 Monaten) ...

verbessern nicht verändern verschlechtern

Ist der Umsatz Ihres Unternehmens im ersten Quartal 2005 gegenüber dem Vorquartal ...

gestiegen gleich geblieben gesunken

Um wie viel Prozent ca.? _____ Prozent

Wird der Umsatz Ihres Unternehmens im zweiten Quartal 2005 gegenüber dem ersten Quartal 2005 ...

steigen gleich bleiben sinken

Um wie viel Prozent ca.? _____ Prozent

Ist die Nachfrage (Auftragsbestand) nach Ihren Produkten und/oder Dienstleistungen im ersten Quartal 2005 gegenüber dem Vorquartal ...

gestiegen gleich geblieben gesunken

Wird die Nachfrage (Auftragsbestand) nach Ihren Produkten bzw. Dienstleistungen im zweiten Quartal 2005 gegenüber dem ersten Quartal 2005 ...

steigen gleich bleiben sinken

Ist Ihr Personalbestand im ersten Quartal 2005 gegenüber dem Vorquartal ...

gestiegen gleich geblieben gesunken

Um wie viel Prozent ca.? _____ Prozent

Wird Ihr Personalbestand im zweiten Quartal 2005 gegenüber dem ersten Quartal 2005 ...

steigen gleich bleiben sinken

Um wie viel Prozent ca.? _____ Prozent

1) Wie viele Beschäftigte in Vollzeitkapazität (ohne Auszubildende) hatte Ihr Unternehmen im Jahresdurchschnitt 2004?

_____ Personen

2) Wie viele Auszubildende hatte Ihr Unternehmen im Jahresdurchschnitt 2004?

_____ Personen

3) Wie hoch war in Ihrem Unternehmen in 2004 der durchschnittliche Anteil der Beschäftigten, die 50 Jahre und älter waren?

ca. _____ Prozent

4) Wie viel Prozent der Beschäftigten, ohne Auszubildende, gehörten in Ihrem Unternehmen im Jahresdurchschnitt 2004 zu einer der folgenden drei Qualifikationsgruppen?
Es geht dabei jeweils um den höchsten Bildungsabschluss:

Universitäts- oder Fachhochschul-Abschluss oder Berufsakademie

ca. _____ Prozent

abgeschlossene Lehre, betriebliche Ausbildung oder Fachschulabschluss, einschließlich Meister und Techniker

ca. _____ Prozent

ohne Berufsabschluss, also ungelernte oder angelernte Beschäftigte

ca. _____ Prozent

5) Wie groß ist der Anteil Ihrer Beschäftigten, die den überwiegenden Teil der Arbeit an einem Computer erledigen?

ca. _____ Prozent

6) Wie groß ist der Anteil Ihrer Beschäftigten mit Zugang zum Internet?

ca. _____ Prozent

7) Welche der folgenden Softwareanwendungen werden bei Ihnen in der täglichen Unternehmenspraxis genutzt?

- Bürosoftware (z.B. Textverarbeitung, Tabellenkalkulation)
- Kommunikationssoftware (z.B. E-Mail Software, Internetbrowser)
- Archive, Datenbanken
- Software für Planung, Steuerung oder Controlling (z.B. PPS, ERP, integrierte Betriebssoftware)
- Software für Computer Aided Design (CAD) oder Computer Aided Engineering (CAE)
- Softwareentwicklungsprogramme
- Multimedia- und/oder Grafiksoftware

8) In welchen Bereichen in Ihrem Unternehmen wird Open-Source-Software eingesetzt?

- Server-Betriebssystem (z.B. Linux)
- Desktop-Betriebssystem (z.B. Linux)
- Bürosoftware (z.B. OpenOffice)
- Internet (z.B. Mozilla Firefox, Apache Webserver)
- Datenbanken (z.B. MySQL)/Content Management Systeme (z.B. Typo 3)
- E-Business (z.B. osCommerce, Enhydra)
- Softwareentwicklung (z.B. Eclipse)
- Multimedia (z.B. Media Portal, CDex)
- Grafikbearbeitung (z.B. Gimp)
- Sicherheit (z.B. GnuPG)
- in keinem Bereich → weiter mit Frage 10a) und 10b)

Rücksendung erbeten bis Freitag, den 6. Mai 2005 an Fax 0621/1235-4300

Falls in Ihrem Unternehmen Open-Source-Software eingesetzt wird:

9) Was waren bestimmende Faktoren für die Entscheidung, in Ihrem Unternehmen Open-Source-Software einzusetzen?

	trifft voll und ganz zu	trifft über- wiegend zu	trifft über- wiegend nicht zu	trifft überhaupt nicht zu
Anpassungsfähigkeit	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Zuverlässigkeit	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sicherheitsaspekte	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Support/Wartung	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
geringere Anschaffungskosten	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
geringere Implementierungskosten	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Unabhängigkeit von einem bestimmten Hersteller/Distributor	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Know-How einzelner Mitarbeiter	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Know-How von Geschäftspartnern	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Unterstützung des Open-Source-Konzepts	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Bitte beantworten Sie Frage 10a) und 10b) nur, falls Sie in Ihrem Unternehmen keine Open-Source-Software einsetzen:

10a) Aus welchen Gründen findet Open-Source-Software in Ihrem Unternehmen bislang keinen Einsatz?

	trifft voll und ganz zu	trifft über- wiegend zu	trifft über- wiegend nicht zu	trifft überhaupt nicht zu
mangelndes Know-How im Unternehmen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Zufriedenheit mit verwendeter Software	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
bestehende Lizenzverträge	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
mangelndes Vertrauen in das Open-Source-Konzept	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
für spezielle Anwendungen in unserem Unternehmen nicht verfügbar	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Umstellungskosten	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
kein Bedarf in unserem Unternehmen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
bislang kein Thema	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

10b) Planen Sie in den nächsten 12 Monaten Open-Source-Software einzusetzen?

ja nein weiß nicht

11) Wie gut fühlen Sie sich über das Thema Open-Source-Software informiert?

gut eher gut eher schlecht schlecht gar nicht

12) Welche IT-Sicherheitsvorkehrungen setzen Sie derzeit ein?

- Geschützter Zugang zu Daten (z.B. Passwort, Biometrische Verfahren, Smartcard)
- digitale Signatur
- Verschlüsselungsverfahren bei der Datenübertragung
- regelmäßige und standardisierte Datensicherung (Backup)
- Virenschutzprogramme
- Spamfilter
- Firewall oder ähnliche Systeme
- Zutrittssicherung zu Räumen mit zentraler IT-Hardware (z.B. Server)
- schriftliche IT-Sicherheitsrichtlinien
- Sicherheitsschulung für Administratoren
- Steigerung des Sicherheitsbewusstseins bei Mitarbeitern
- Beschäftigung eines IT-Sicherheitsbeauftragten

13) Wie gut fühlt sich Ihr Unternehmen durch die vorgenommenen IT-Sicherheitsmaßnahmen geschützt?

gut eher gut eher schlecht schlecht gar nicht

14) Was sind Ihrer Meinung nach die größten Hemmnisse für eine umfassende IT-Sicherheit in Ihrem Unternehmen?

- mangelndes Sicherheitsbewusstsein im Unternehmen
- knappe oder rückläufige IT-Budgets
- Mangel an qualifiziertem Personal
- ungünstiges Kosten-/Nutzenverhältnis
- Komplexität der verfügbaren Sicherheitslösungen
- branchenspezifische Sicherheitsanforderungen werden bei angebotenen Lösungen nicht ausreichend berücksichtigt
- steigende Risiken durch Weiterentwicklung von Viren etc., mit denen IT-Sicherheitslösungen nicht Schritt halten können

15) Hatten Sie in letzter Zeit auf Grund eines Befalls durch Viren, Trojaner, Würmer, etc. Datenverluste zu verzeichnen?

ja, in 2005 ja, in 2004 nein, weder in 2004 noch 2005

16) Wie groß war 2004 der Anteil für IT-Sicherheit am IT-Budget in Ihrem Unternehmen?

0% 1 – 5% 6 – 10% 11 – 15%
 16 – 20% 20 – 25% > 25% weiß nicht

17) Ist der vorgesehene Anteil für IT-Sicherheit am IT-Budget in diesem Jahr (im Vergleich zum Vorjahr) in Ihrem Unternehmen...

höher gleich niedriger

18) Wie hoch waren im Jahr 2004 Ihre Investitionen in Informations- und Kommunikationstechnologien (IKT)?

ca. _____ Euro

19) Welche Entwicklung der Investitionen in IKT erwarten Sie für das Jahr 2005? Die Ausgaben werden ...

steigen gleich bleiben sinken

Um wie viel Prozent ca.? _____ Prozent

20) Wie hoch war der Umsatz Ihres Unternehmens (inkl. Exporte) im Jahr 2004? (im Fall einer Bank: bitte Zins- und Provisionserträge; im Fall einer Versicherung: bitte Beitragseinnahmen angeben)

Umsatz (ohne MWSt.): _____ Euro

Rücksendung erbeten bis Freitag, den 6. Mai 2005 an Fax 0621/1235-4300

Ordnen Sie bitte Ihr Unternehmen gemäß der hauptsächlich ausgeübten wirtschaftlichen Tätigkeit einem Wirtschaftszweig entsprechend der beigefügten Liste (siehe Rückseite Fragebogen Blatt 1) zu.

Übertragen Sie bitte hierfür die in der Liste angegebene Nummer:

ODER

Falls es Ihnen anhand der Liste nicht gelungen ist, den wirtschaftlichen Schwerpunkt Ihres Unternehmens zu bestimmen, nennen Sie uns bitte Ihr umsatzstärkstes Produkt/Ihre umsatzstärkste Dienstleistung:

Liste der Wirtschaftszweige zur Einordnung Ihres Unternehmens:

Software / DV-Dienstleistungen

- 01 Verlegen von Software
- 02 Softwareberatung und -entwicklung
- 03 Hardwareberatung
- 04 Datenverarbeitungsdienste
- 05 Datenbanken
- 06 Instandhaltung und Reparatur von Büromaschinen, Datenverarbeitungsgeräten und -einrichtungen
- 07 Sonstige mit der Datenverarbeitung verbundene Tätigkeiten

IT- / Medien-Hardware

- 08 Herstellung von Büromaschinen
- 09 Herstellung von Datenverarbeitungsgeräten und -einrichtungen
- 10 Herstellung von elektronischen Bauelementen
- 11 Herstellung von Geräten und Einrichtungen der Telekommunikationstechnik
- 12 Herstellung von Rundfunkgeräten sowie phono- und videotecnischen Geräten
- 13 Herstellung von Foto-, Projektions- und Kinogeräten
- 14 Herstellung von anderen optischen und fotografischen Geräten
- 15 Vermietung von Büromaschinen, Datenverarbeitungsgeräten und -einrichtungen

(Tele-) Kommunikation

- 16 Private Post- und Kurierdienste
- 17 Fernmeldedienste

Audiovisuelle Medien

- 18 Herstellung von unbespielten Ton-, Bild- und Datenträgern
- 19 Fotografisches Gewerbe und fotografische Laboratorien
- 20 Verlegen von bespielten Tonträgern und Musikalien
- 21 Vervielfältigung von bespielten Tonträgern
- 22 Vervielfältigung von bespielten Bildträgern
- 23 Vervielfältigung von bespielten Datenträgern
- 24 Film- und Videofilmherstellung
- 25 Kinos
- 26 Rundfunkveranstalter, Herstellung von Hörfunk- und Fernsehprogrammen
- 27 Technische Hilfsdienste für kulturelle und unterhaltende Leistungen

Druck / Verlag

- 28 Verlegen von Büchern
- 29 Verlegen von Zeitungen
- 30 Verlegen von Zeitschriften
- 31 Sonstiges Verlagsgewerbe
- 32 Drucken von Zeitungen
- 33 Drucken anderer Druckerzeugnisse
- 34 Druckweiterverarbeitung
- 35 Druck- und Mediovorstufe
- 36 Erbringung von sonstigen druckbezogenen Dienstleistungen

Werbung / Marktkommunikation

- 37 Markt- und Meinungsforschung
- 38 Unternehmens- und Public-Relations-Beratung
- 39 Werbung
- 40 Ausstellungs-, Messe- und Warenmarkteinrichtungen

Inhalte-Dienstleister

- 41 Auskunftsteien
- 42 Sekretariats-, Schreib- und Übersetzungsdienste; Copy-Shops
- 43 Selbstständige Schriftstellerinnen und Schriftsteller
- 44 Selbstständige Bühnen-, Film-, Hörfunk- und Fernsehkünstlerinnen und -künstler
- 45 Korrespondenz- und Nachrichtenbüros
- 46 Selbstständige Journalistinnen, Journalisten, Pressefotografinnen und Pressefotografen
- 47 Bibliotheken und Archive
- 48 Leihbüchereien und Lesezirkel
- 49 Filmverleih und Videoprogrammanbieter (an andere Wirtschaftszweige)
- 50 Videotheken (Verleih an Endverbraucher)

Herstellung von chemischen Erzeugnissen

- 51 Herstellung von chemischen Grundstoffen (Industriegase, Farbstoffe, Düngemittel, Kunststoffe)
- 52 Herstellung von Schädlingsbekämpfungsmitteln, Pflanzenschutz- und Desinfektionsmitteln
- 53 Herstellung von Anstrichmitteln, Druckfarben und Kittungen
- 54 Herstellung von pharmazeutischen Erzeugnissen
- 55 Herstellung von Seifen, Wasch-, Reinigungs- und Körperpflegemitteln sowie von Duftstoffen
- 56 Herstellung von sonstigen chemischen Erzeugnissen (pyrotechnische Erzeugnisse, Klebstoffe und Gelatine, ätherische Öle, fotochemische Erzeugnisse)
- 57 Herstellung von Chemiefasern

Maschinenbau

- 58 Herstellung von Maschinen für die Erzeugung und Nutzung von mechanischer Energie (ohne Motoren für Straßenfahrzeuge) (Verbrennungsmotoren und Turbinen, Pumpen und Kompressoren, Armaturen, Lager, Getriebe, Zahnräder und Antriebselemente)
- 59 Herstellung von sonstigen Maschinen (Öfen, Brenner, Hebezeugen, Fördermittel, kälte- und lufttechnische Erzeugnissen)
- 60 Herstellung von land- und forstwirtschaftlichen Maschinen
- 61 Herstellung von Werkzeugmaschinen (handgeführte kraftbetriebene Werkzeuge, Werkzeugmaschinen für die Metallbearbeitung)
- 62 Herstellung von Maschinen für sonstige Wirtschaftszweige (Maschinen für die Metallerzeugung, Bau- und Baustoffmaschinen; Maschinen für das Ernährungsgewerbe; Maschinen für das Bekleidungs-gewerbe; Maschinen für das Papiergewerbe)
- 63 Herstellung von Waffen und Munition
- 64 Herstellung von Haushaltsgeräten

Medizin-, Mess-, Steuer- und Regelungstechnik, Optik, Uhren

- 65 Herstellung von medizinischen Geräten und orthopädischen Erzeugnissen
- 66 Herstellung von Mess-, Kontroll-, Navigations- u.ä. Instrumenten und Vorrichtungen
- 67 Herstellung von industriellen Prozesssteuerungseinrichtungen
- 68 Herstellung von Uhren

Herstellung von Kraftwagen und Kraftwagenteilen

- 69 Herstellung von Kraftwagen und Kraftwagenmotoren
- 70 Herstellung von Karosserien, Aufbauten und Anhängern
- 71 Herstellung von Teilen und Zubehör für Kraftwagen und Kraftwagenmotoren

Verkehr / Hilfs- und Nebentätigkeiten für den Verkehr

- 72 Landverkehr (Personenbeförderung im Linienverkehr, Betrieb von Taxis und Mietwagen mit Fahrer, Güterbeförderung im Straßenverkehr)
- 73 Lagerei
- 74 Sonstige Hilfs- und Nebentätigkeiten für den Verkehr
- 75 Reisebüros und Reiseveranstalter
- 76 Spedition, sonstige Verkehrsvermittlung

Bank- / Versicherungsgewerbe

- 77 Kreditinstitute
- 78 Sonstige Finanzierungsinstitutionen
- 79 Mit dem Kreditgewerbe verbundene Tätigkeiten
- 80 Versicherungsgewerbe
- 81 Mit dem Versicherungsgewerbe verbundene Tätigkeiten

Forschung und Entwicklung / Technische Dienstleister

- 82 Forschung und Entwicklung im Bereich Natur-, Ingenieur-, Agrarwissenschaften und Medizin
- 83 Forschung und Entwicklung im Bereich Rechts-, Wirtschafts- und Sozialwissenschaften sowie im Bereich Sprach-, Kultur- und Kunstwissenschaften
- 84 Architektur- und Ingenieurbüros
- 85 Technische, physikalische und chemische Untersuchung

Open Source Software

Jörg Ohnemus

„Die Idee von 'freier Software' entwickelte sich aus dem Bedürfnis vieler Programmierer, vorhandene Software nach den eigenen Anforderungen weiterentwickeln zu können. Dazu fehlte aber der kommerziellen Software technisch der Quellcode, der zur Änderung und Weiterentwicklung von bestehender Software erforderlich ist, und rechtlich die Erlaubnis der Rechteinhaber, die gekaufte Software zu verändern.“

*Axel Metzger und Till Jäger
„Open Source Software und deutsches Urheberrecht“*

1. Einleitung	63
2. Hintergrundinformationen	63
3. Geschichte von Open Source Software	64
4. Softwarelizenzen	65
5. Open Source Softwareentwicklung	67
6. Nutzung von Open Source Software in Unternehmen	71
7. Schlussbemerkungen	77
8. Literatur und weiterführende Informationen	79

1. Einleitung

Open Source Software (OSS) erfreut sich immer größerer Beliebtheit, was sich beispielsweise am durchschlagenden Erfolg des Open Source Internetbrowsers Firefox aus der Mozilla-Entwicklergemeinschaft zeigt. Gerade in Europa verzeichnet der Browser einen ständigen Zuwachs an Marktanteilen und veranlasste jüngst Microsoft, seine Weiterentwicklung des Internet Explorers früher als geplant auf den Markt zu bringen (Patalong, 2005). Wohl in keinem anderen Endnutzersegment hat der Softwareriese aus Redmond (USA) im Moment einen ähnlich starken Konkurrenten aus der Open Source Gemeinschaft.

Aber was ist eigentlich Open Source Software? Mit dieser Frage sind viele Computernutzer, die sich zum ersten Mal mit Lizenz- und Preismodellen von Softwareprogrammen beschäftigen, konfrontiert. Das es sich bei Open Source Software um kostenlos erhältliche Softwareprogramme handelt, beleuchtet nur einen Aspekt unter vielen (für viele Softwarenutzer ist dies der Wichtigste). Hinter dem Begriff Open Source steht jedoch viel mehr, für manche Menschen sogar eine eigene Weltanschauung.

Dieser Beitrag gibt dem Leser einen Überblick über Open Source Software. Er verdeutlicht, worum es sich bei OS-Software handelt und zeigt deren *geschichtliche Entwicklung* auf. Ferner gibt er einen Überblick über die wesentlichen Unterschiede zwischen proprietärer (kostenpflichtiger) und Open Source Software. Ein weiterer Abschnitt dieses Beitrags widmet sich den *Motiven und Hintergründen* von Programmierern und Softwareentwicklern, sich an Open Source Projekten zu beteiligen. Dazu werden Resultate einiger Studien zu diesem Thema vorgestellt. Abschließend werden wichtige Ergebnisse aus Studien der vergangenen Jahre zum *Einsatz von Open Source Software* auf professioneller Ebene, d.h. in Unternehmen und öffentlichen Einrichtungen, präsentiert.

2. Hintergrundinformationen

Die konventionelle Methode, Software herzustellen, war über viele Jahre durch kommerziell arbeitende Softwarefirmen geprägt. Noch heute ist der überwiegende Teil der eingesetzten Software kommerzieller Art. Der wohl bekannteste Hersteller proprietärer, d.h. käuflich zu erwerbender Software ist Microsoft mit seinen weltweit bekannten Produkten Windows und Office.

Die Lizenzbestimmungen von proprietärer Software sichern den Herstellern das Eigentumsrecht an ihren Produkten. Durch das Ausliefern der Programme in Binärdatenform, einer für den Computer verständlichen Aneinanderreihung von Codes, schützen sie ihre Produkte ganz praktisch vor unerlaubtem Kopieren oder Nachahmen. Der Quellcode (engl. Source Code) ist der vom Programmierer geschriebene, menschenlesbare Programmtext. Er ist das am besten

gehütete Geheimnis (fast) jeder kommerziell arbeitenden Softwarefirma. Ohne den Zugang zum Quellcode eines Programms ist es für andere Softwareentwickler nicht möglich, die internen Abläufe und Funktionsweisen der Programme nachzuvollziehen. Eine Weiterentwicklung oder auch spezielle Anpassung kann nur durch den Hersteller vorgenommen werden.

Jeder Nutzer von proprietärer Software ist deshalb bei Programmanpassungswünschen auf das Wohlwollen des Herstellers angewiesen, diese für ihn durchzuführen. Im Gegensatz dazu ist die Veröffentlichung des Quellcodes ein elementarer Bestandteil von Open Source Software. Jeder Interessierte hat so die Möglichkeit, die Software weiterzuentwickeln bzw. gewünschte Anpassungen selbst vorzunehmen.

3. Geschichte von Open Source Software

Ursprünglich wurde Software als kostenlose Zugabe beim Kauf eines Computers mitgeliefert. Der Quellcode dieser Software war für Jedermann frei verfügbar. Die Hardwarehersteller, zur damaligen Zeit vor allem IBM, erhofften sich dadurch eine schnelle Weiterentwicklung ihrer, im Vergleich zur Hardware als weniger wichtig eingestuften Softwareprodukte. Geld wurde zur damaligen Zeit ausschließlich mit dem Verkauf von Hardware erzielt.

Mit dem Stopp der Auslieferung des Quellcodes für sein damaliges Betriebssystem UNIX, Mitte der sechziger Jahre, läutete IBM die faktische Trennung von Hard- und Software ein. Die Computerindustrie erkannte, dass man mit der Entwicklung und dem getrennten Verkauf von Software sehr viel Geld verdienen konnte. Es entstand ein neuer Industriezweig, der streng abgeschottet Software entwickelte. Durch Non-Disclosure Agreements (Verschwiegenheitsvereinbarungen) wurden die in den Softwarefirmen beschäftigten Entwickler an der freien Weiterentwicklung der Software gehindert. Nach nur zehn Jahren gab es kaum noch frei verfügbare, quelloffene Software.

Getrieben von der Unzufriedenheit mit den Nachteilen der proprietären Softwareentwicklung konstituierte Richard Stallman vom Massachusetts Institute of Technology (MIT) 1984 das GNU¹ Projekt. Ziel war es, an die bereits in den sechziger Jahren praktizierte Zusammenarbeit von Softwareentwicklern anzuknüpfen, und ein UNIX-ähnliches Betriebssystem zu schaffen, welches ausschließlich aus freien Softwarequellen besteht. Stallman vertrat die Ansicht, dass Quellcode vervielfältigt, verändert und weitergegeben werden sollte. Um dies sicherzustellen, stellte er das GNU-Projekt unter die von ihm geschaffene General Public License (GPL), die verhindert, dass andere Softwareentwickler die Programme modifizieren und anschließend kommerziell vertreiben. Die Free Software Foundation (FSF) wurde im Jahr 1985 als Koordinationsstelle und zur Generierung von Einnahmen für das GNU Projekt gegründet.² 1991

¹ GNU ist eine rekursive Abkürzung für „Gnu’s Not Unix“.

² Einnahmen wurden hauptsächlich durch den Verkauf von Benutzerhandbüchern erzielt.

startete der finnische Student Linus Torvald mit der Entwicklung eines Betriebssystem-Kerns, einem wichtigen Bestandteil, der dem GNU-Projekt bisher noch fehlte. Durch die inzwischen vorhandene Möglichkeit des privaten Zugangs zum Internet, stieß der Aufruf von Torvald, weitere Beiträge und Verbesserungen für sein Betriebssystemprojekt Linux³ beizusteuern, auf große Resonanz. Weltweit beteiligten sich zahlreiche Softwareprogrammierer an der Weiterentwicklung. Linux wurde ebenfalls unter die GPL gestellt. Weitere Open Source Projekte bzw. Programme wie Bind, Samba, Apache entstanden auf ähnliche Weise.

Von Eric S. Raymond, Bruce Perens und Tim O'Reilly wurde im Jahr 1998 schließlich der Begriff Open Source Software für Programme mit frei zugänglichem Quellcode geprägt. Mit der Begrifflichkeit wollte man hauptsächlich den „antikommerziellen Beiklang von ‚Free Software‘ vermeiden“ (Henkel, 2004, S. 23). Im Englischen besitzt das Adjektiv „free“ sowohl die Bedeutung Freiheit im Sinne von Freiheit des Geistes und der Wissenschaft als auch Freiheit von Kosten im Sinne von gratis. Da die Möglichkeit der kostenlosen Nutzung mitunter ein wichtiges Charakteristikum freier Software ist, aber bei weitem nicht das Wichtigste, soll mit dem Begriff Open Source Software die Entwicklungsdynamik, das hohe Qualitätsniveau und die Bedeutung freier Software für die Computerindustrie in den Vordergrund gerückt werden (O'Reilly, 1999).

4. Softwarelizenzen

Der Nutzung von Software sind rechtliche Grenzen gesetzt, die in Form einer Lizenzvereinbarung in Kraft treten. Im Grunde kann man zwei Lizenztypen unterscheiden: freie Software⁴ und proprietäre Software.

Bei kommerzieller Software werden die Rechte des Käufers bzw. Nutzers vielfach eingeschränkt. Dabei wird Nutzern die Weiterverbreitung der Software, die Veränderung des Quellcodes (falls überhaupt verfügbar) und die Weiterverbreitung veränderter Versionen durch die Lizenzbestimmungen untersagt. Bei Open Source Software hingegen wird jedem gestattet, den Quellcode zu verändern bzw. zu verbessern, um die Software langfristig weiterzuentwickeln.

Nur Software, die von einer durch die Open Source Initiative (OSI) anerkannten Lizenz geschützt ist, kann als Open Source Software bezeichnet werden. Für die Anerkennung durch die OSI muss die Lizenz folgende Voraussetzungen erfüllen.⁵

- Jeder muss das Recht haben, die Software frei weiterzugeben.
- Das Programm muss den Quellcode beinhalten oder die Möglichkeit, den Quellcode zum Selbstkostenpreis zu bekommen.

³ Der Name Linux entstand aus einer Kombination von Linus und UNIX.

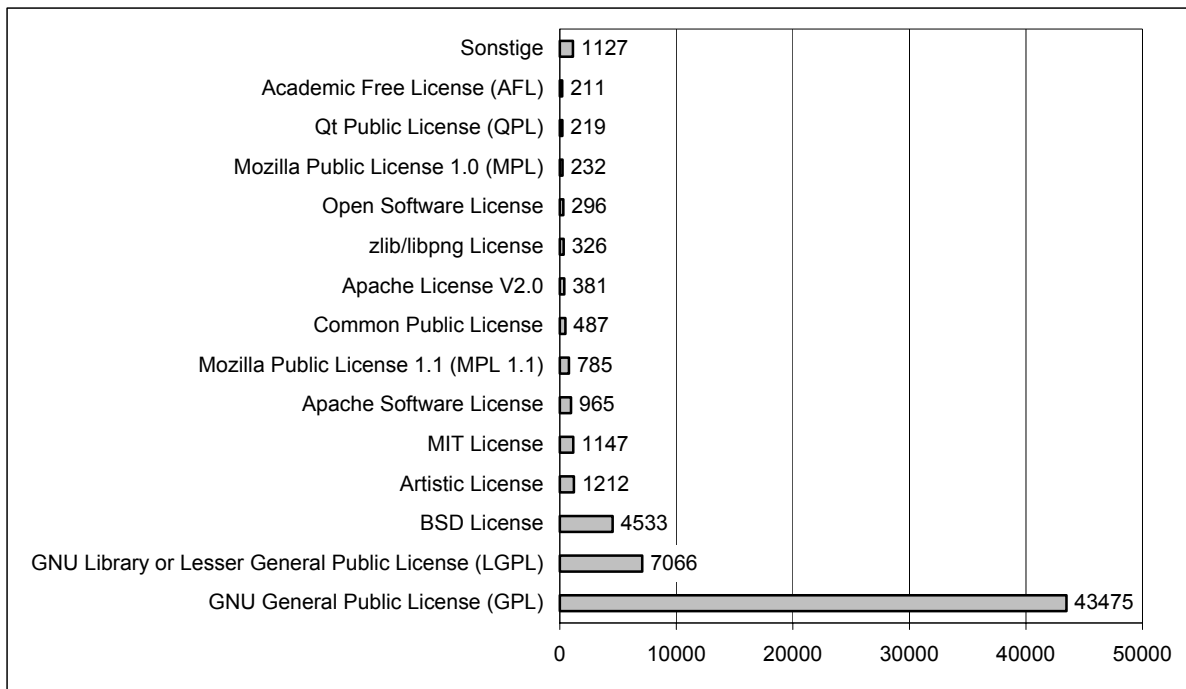
⁴ Freie Software und Open Source Software (OSS) werden an dieser Stelle synonym benutzt.

⁵ Eine ausführliche Liste mit den Anforderungen an eine OS-Lizenz findet man unter www.opensource.org.

- Veränderungen an der Software müssen zulässig sein und ihre Weitergabe unter den Lizenzbedingungen der Ausgangssoftware muss gestattet sein.
- Es darf keine Einschränkung auf bestimmte Nutzer oder bestimmte Verwendungsgebiete erfolgen, d.h. die Lizenz darf niemanden benachteiligen.
- Die Lizenz darf die Weitergabe zusammen mit anderer Software nicht einschränken, d.h. sie darf z.B. nicht verlangen, dass alle anderen Programme, die auf demselben Medium weitergegeben werden, ebenfalls quelloffen sein müssen.
- Die genannten Rechte dürfen nicht durch andere Lizenzen beschränkt werden.

Die Offenheit des Quellcodes und die Erlaubnis, diesen zu verändern sind die Grundlagen von Open Source Software. Nur damit ist es Anwendern überhaupt möglich gemacht, einen Beitrag zur Weiterentwicklung des Softwareprodukts zu leisten.

Abbildung 1: Häufigkeit der verwendeten OSS-Lizenzen auf sourceforge.net



Quelle: http://sourceforge.net/softwaremap/trove_list.php?form_cat=14, Stand 02.05.2005.

Neben der schon angesprochenen GNU General Public License, gibt es eine Vielzahl weiterer von der Open Source Initiative akzeptierter Lizenzen, die zum Teil auf gewisse OSS-Produkte speziell zugeschnitten sind. Abbildung 1 gibt eine Übersicht über die Verwendungshäufigkeit verschiedener OS-Lizenztypen auf sourceforge.net, der weltweit größten Internet Plattform für Open Source Projekte⁶. Von den mehr als 62.000 Softwareprojekten, die auf sourceforge.net eingestellt sind, dominiert eindeutig die GNU GPL. Fast 70 Prozent der Projekte werden unter diesem Lizenztyp betrieben. Mit weitem Abstand folgen die GNU Library/Lesser General Public License (7.066) und die BSD License (4.533).

⁶ sourceforge.net bietet Open Source Entwicklern kostenlos Dienste wie z.B. Versionsverwaltung und Projekt-Homepages an.

5. Open Source Softwareentwicklung

Ein Open Source Projekt wird meist durch ein spezielles (Software-) Problem, mit dem sich ein Entwickler konfrontiert sieht, ins Leben gerufen. Er schreibt ein erstes Programm und macht dessen Quellcode öffentlich zugänglich. Diese Person wird meist auch Projektleiter eines Open Source Projektes. Um ihn herum bildet sich ein Team von Programmierern, die sich besonders für das entsprechende Produkt bzw. Problem interessieren. Im Verlauf der Projektentwicklung werden diese Teammitglieder oft zu so genannten Maintainern, die für einzelne Bereiche Zuständigkeit und Verantwortung übernehmen. Die Mitarbeit an einem Open Source Projekt steht grundsätzlich jedem offen. In das Kernteam aufgenommen zu werden, ist für die meisten Entwickler eine Auszeichnung. Der Einfluss der Gründerriege auf das endgültige Produkt ist dabei unterschiedlich hoch. Oft entscheiden letztlich die Mitglieder, ob eine Software geändert oder ein neuer Baustein hinzugefügt wird.

Im Folgenden werden die charakteristischen Eigenschaften von OSS-Programmierern sowie ihre Beweggründe, sich an der Entwicklung von Open Source Software zu beteiligen, analysiert. Die Darstellung basiert auf Umfragen in der OSS-Entwicklergemeinschaft.

Im Jahr 2002 führte das International Institute of Infonomics an der Universität Maastricht zusammen mit Berlecon Research eine mehrteilige Studie zu Free/Libre Open Source Software (im Weiteren kurz FLOSS genannt) durch. Ziel der von der Europäischen Kommission in Auftrag gegebenen Analyse war es, die Informationslücken bezüglich Open Source Software durch eine gründliche Untersuchung sämtlicher mit OSS verbundener Aspekte zu beheben.

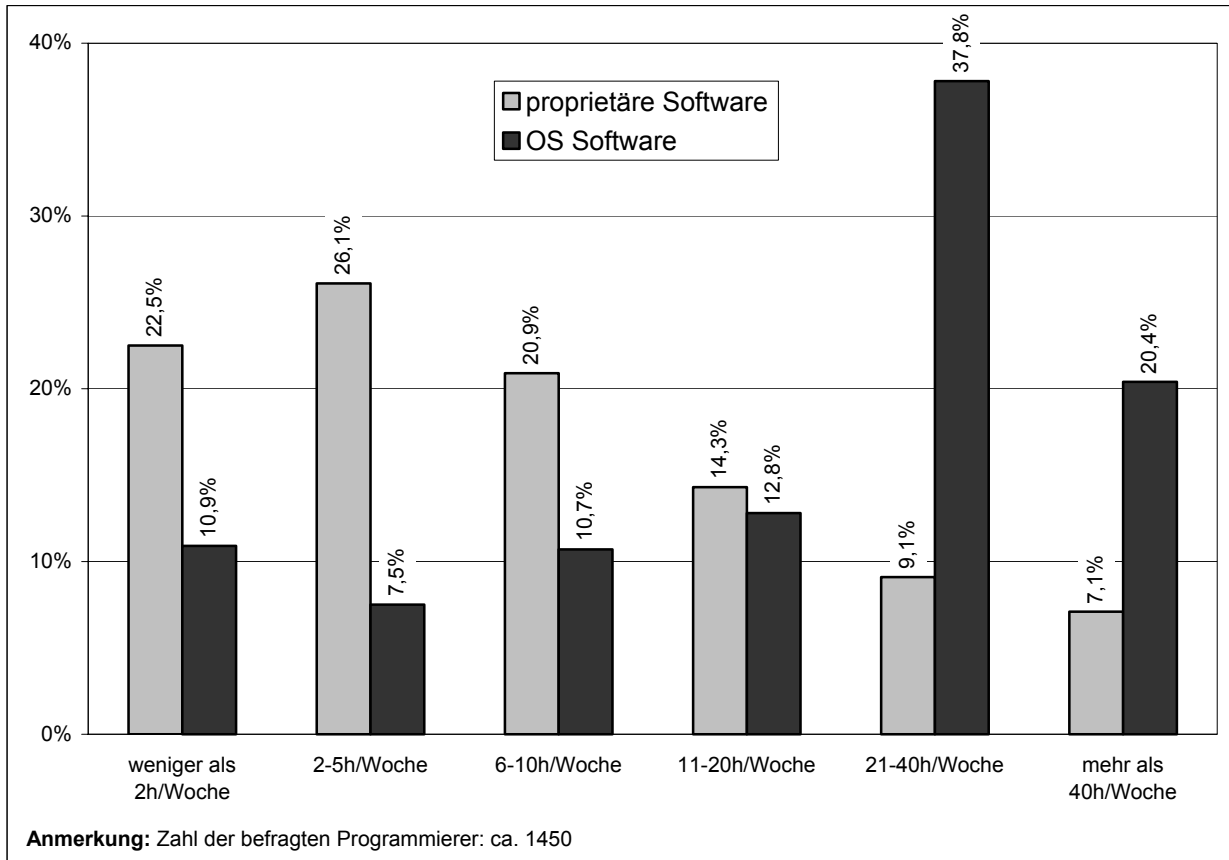
Der vierte Teil von FLOSS (Ghosh et al., 2002), beschäftigt sich mit der Open Source Software Entwicklergemeinschaft. Die Ergebnisse basieren auf einer Onlinebefragung, an der sich im Frühjahr 2002 weltweit über 2700 OS-Softwareentwickler beteiligten.⁷ Auf der Basis dieser Umfrage wurden neben zahlreichen weiteren Aspekten auch interessante Informationen bezüglich der persönlichen Charakteristika und den Teilnahmemotiven von Individuen an Open Source Projekten gewonnen.

Die Entwicklung von OSS ist eine eindeutige Domäne jüngerer Männer. Nur ein verschwindend geringer Teil, etwas mehr als ein Prozent, der OSS-Community ist weiblich. Das Durchschnittsalter von OSS-Entwicklern liegt in dieser Studie bei 26 Jahren, wobei nur 25 Prozent älter als 30 Jahre sind. Durchschnittlich beginnt ein Programmierer mit 23 Jahren seine Entwicklertätigkeit in OS-Projekten. 70 Prozent der OSS-Entwickler besitzen als höchsten Bildungsabschluss einen Universitätsabschluss. Der überwiegende Teil in der Stichprobe ist im IT-Sektor beschäftigt. Dabei stellen Softwareentwickler und Programmierer mit zusammen fast

⁷ Der Fragebogen wurde auf einigen OSS-Plattformen veröffentlicht und später von den Teilnehmern der Umfrage an andere Entwickler weitergeleitet.

45 Prozent die größte Gruppe. Danach folgen Studenten, die etwa 16 Prozent der OS-Entwickler ausmachen. Open Source Programmierer weisen kein überdurchschnittlich hohes Einkommen auf, was natürlich auch an der Tatsache liegt, dass relativ viele von ihnen Studierende sind. Mehr als 50 Prozent verdienen weniger als 2000 Euro bzw. US-Dollar pro Monat. Nur fünf Prozent haben ein Monatseinkommen von über 7500 Euro bzw. US-Dollar.

Abbildung 2: Von Programmieren verwendete Zeit für die Entwicklung von OSS bzw. von proprietärer Software

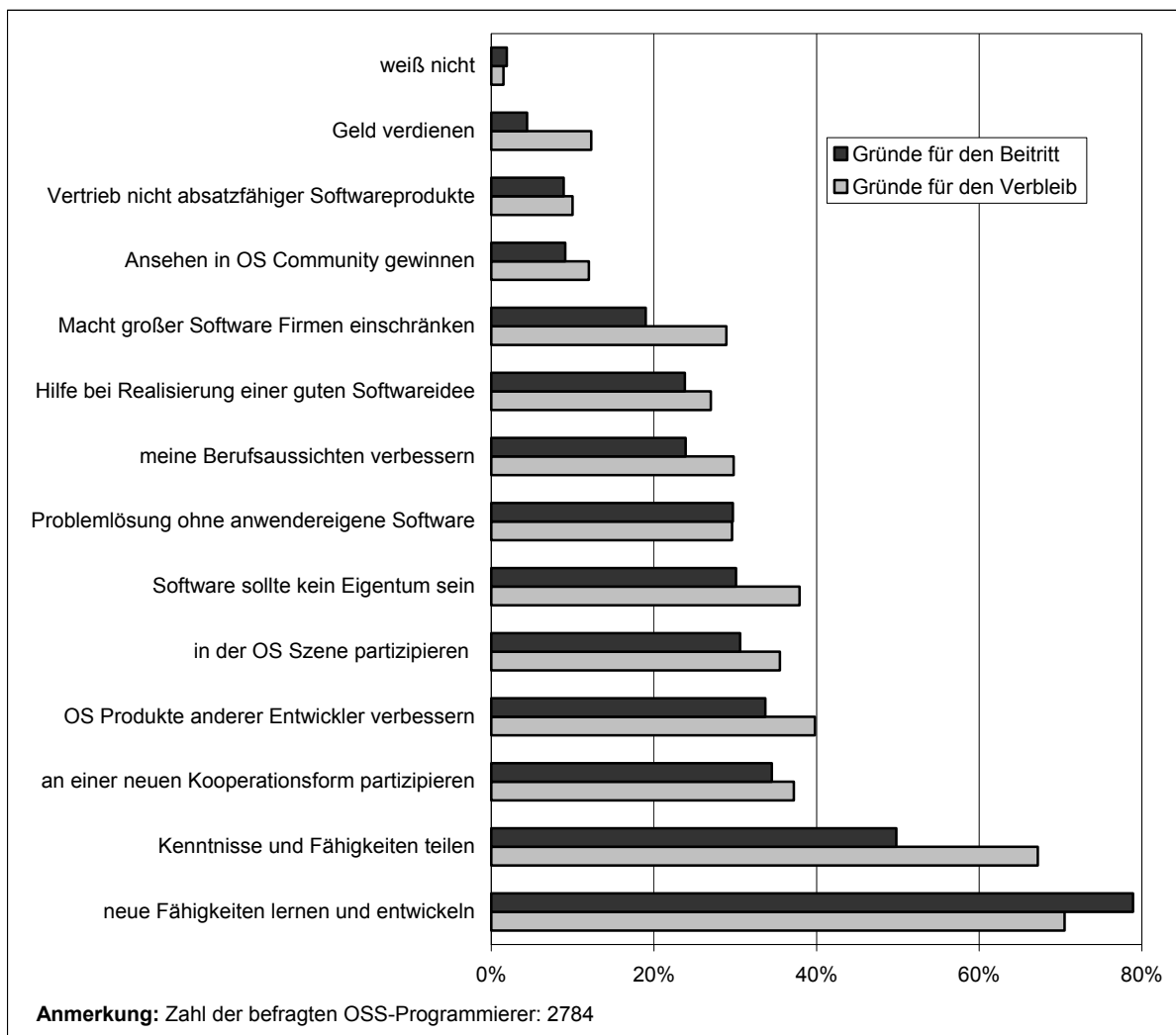


Quelle: Ghosh et. al 2002, S. 22

Gefragt nach der Zeit, die sie mit der Entwicklung von OSS verbringen, geben etwas weniger als 50 Prozent an, dass sie sich höchstens fünf Stunden pro Woche damit beschäftigen. Dies lässt den Schluss zu, dass OSS-Entwicklung, trotz des hohen Anteils von professionellen Softwareentwicklern (etwa die Hälfte der Entwickler in der Stichprobe gab an, auch proprietäre Software zu programmieren), eher als Hobby betrachtet wird. Abbildung 2 gibt einen Überblick über die verwendete Zeit zur Programmierung von OSS und proprietärer Software von den Entwicklern, die sowohl OSS als auch proprietäre Software programmieren. Die Ergebnisse lassen zudem vermuten, dass die Entwicklung proprietärer Software weniger Zeit zur Programmierung von OSS lässt (und umgekehrt). Dieser Vermutung widerspricht hingegen eine Analyse der Gruppe von OS-Programmierern, die mehr als 40 Stunden pro Woche für deren Entwicklung aufbringen. Aus dieser Gruppe geben fast 50 Prozent an, 21 Stunden und mehr für die Programmierung proprietärer Software zu verwenden. Allerdings ist diese besonders aktive Entwicklergruppe eher klein. Grundsätzlich gilt, dass gerade auch aus dem Bereich der proprietären Softwareentwicklung erhebliche Beiträge zur OSS-Entwicklung geliefert werden.

Im Folgenden wird auf die Motive für eine Beteiligung an der Entwicklung von Open Source Software eingegangen. Die Teilnehmer der FLOSS Studie in 2002 wurden gebeten, aus einer Liste von Antwortmöglichkeiten maximal vier Kategorien auszuwählen, die für sie entscheidend waren, an einem OSS-Projekt mitzuarbeiten. In Abbildung 3 sind die Ergebnisse graphisch dargestellt. Als Hauptgrund sowohl zum Eintritt als auch zum Verbleib in einem OSS-Projekt wird das „Lernen und Weiterentwickeln neuer Fähigkeiten“ (79 bzw. 71 Prozent) genannt. An zweiter Stelle steht der „Austausch von Wissen und Fähigkeiten“ mit anderen (67 bzw. 50 Prozent). Das eher egoistische Motiv einer „Verbesserung der Berufsaussichten“ wird von nur knapp 24 Prozent der Befragten als Grund für den Eintritt angegeben. Bezug nehmend auf die in der Einleitung angesprochene eigene Weltanschauung von OSS-Entwicklern wird dem Aspekt, dass „Software kein proprietäres Gut sein sollte“, ein sehr hoher Stellenwert hinsichtlich des Verbleibs in der OSS-Gemeinschaft beigemessen. 38 Prozent der Befragten nannten diesen Grund.

Abbildung 3: Gründe für den Beitritt und den Verbleib in der OS-Gemeinschaft



Quelle: Ghosh et al. 2002, S. 45

Vom Stanford Institute for Economic Policy Research (SIEPR) wurde 2003, in Anlehnung an den vierten Teil der europäischen FLOSS Studie, das Free/Libre/Open Source Software Survey for 2003 (im Nachfolgenden kurz FLOSS-US genannt) durchgeführt (David et al., 2003). Insgesamt füllten fast 1600 Entwickler den im Internet veröffentlichten Fragebogen der FLOSS-US Studie aus.⁸ Ein Hauptunterschied zwischen den beiden Untersuchungen liegt in der geographischen Herkunft der Umfrageteilnehmer. Während sich an der ursprünglichen Studie hauptsächlich Europäer beteiligten (über 70 Prozent), war die weltweite Streuung der Teilnehmer bei FLOSS-US größer. Nur etwas mehr als 50 Prozent der Umfrageteilnehmer kamen aus Europa.

In den Hintergrundinformationen zur OSS-Community unterscheidet sich FLOSS-US nicht wesentlich von den Ergebnissen der ursprünglichen FLOSS Studie. Auch hier ist wiederum der überwiegende Teil der Open Source Entwickler männlich (über 98 Prozent) und 50 Prozent der Programmierer sind zwischen 23 und 33 Jahren alt. Im Gegensatz zur europäischen FLOSS Untersuchung sind mehr Studenten und weniger nichtselbständig Beschäftigte in der OSS-Entwicklergemeinschaft tätig. Der Anteil der Selbständigen ist in beiden Studien etwa gleich (14 bzw. 16 Prozent). Auch bezüglich des Bildungsabschlusses gibt es große Übereinstimmungen zwischen beiden Stichproben. Ein Aspekt, den FLOSS nicht beleuchtet, ist die Frage nach dem Kenntnisstand des Arbeitgebers über die OSS-Entwicklungstätigkeit seiner Beschäftigten. Vor dem Hintergrund, dass viele Programmierer hauptberuflich im IT-Sektor beschäftigt sind, ist dies ein interessanter Punkt. Die Ergebnisse zeigen, dass bei über 70 Prozent der abhängig Beschäftigten der Arbeitgeber Kenntnis über deren Entwicklertätigkeit hat. Bei über 27 Prozent wird die Entwicklung sogar vom Vorgesetzten in Auftrag gegeben. Bei 21 Prozent weiß der Arbeitgeber nicht, das sein Mitarbeiter OS-Software mitprogrammiert und nur bei weniger als 3 Prozent ist eine Mitarbeit von Seiten des Arbeitgebers ausdrücklich unerwünscht.

In FLOSS-US sagen über 47 Prozent der Teilnehmer, dass Software quelloffen sein soll. Im Vergleich zur ähnlichen europäischen FLOSS Fragestellung, dass „Software kein proprietäres Gut sein sollte“, ist die Zustimmung hier noch ausgeprägter.

Auf Grund der Tatsache, dass an FLOSS bzw. FLOSS-US die Beteiligung japanischer Programmierer recht gering war⁹, hat das Mitsubishi Research Institute (Japan) im Auftrag des japanischen Ministeriums für Wirtschaft, Handel und Industrie eine Onlineumfrage unter dem Titel Free/Libre/Open Source Software Japanese Developers Online Survey durchgeführt (Mitsubishi Research Institute, 2004). Mit knapp 550 auswertbaren Fragebögen ist die Zahl der Teilnehmer, im Vergleich zu den beiden anderen FLOSS Umfragen, eher gering. Allerdings wurden bei FLOSS-Japan nur japanische OSS-Entwickler zur Teilnahme aufgefordert.

⁸ An beiden Umfragen, sowohl an der europäischen als auch an der amerikanischen FLOSS Studie, konnten sich OSS-Entwickler weltweit beteiligen.

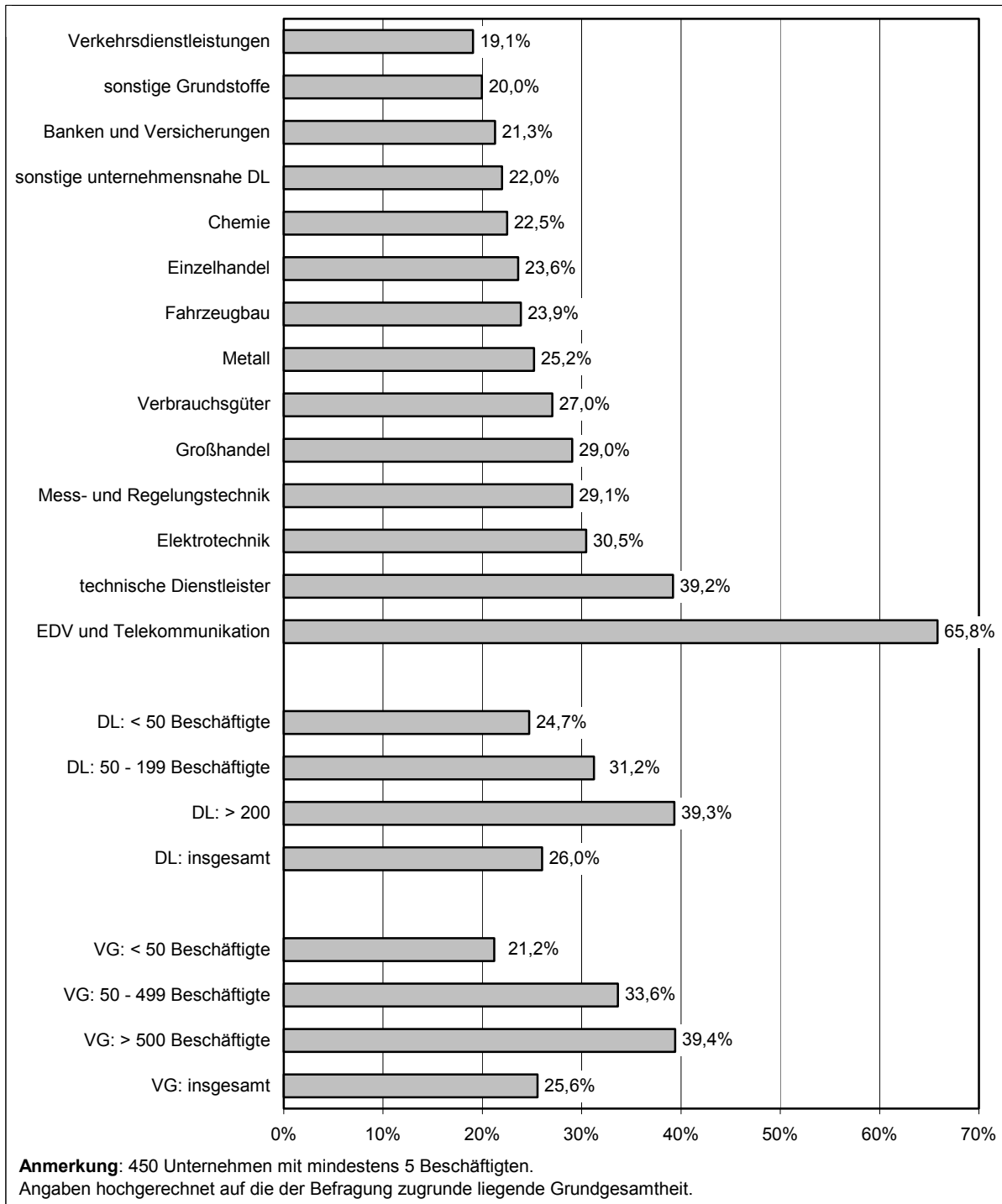
⁹ Der Grund für die mangelnde Teilnahme japanischer Programmierer ist zum Teil dadurch zu begründen, dass beide Umfragen in englischer Sprache durchgeführt wurden.

Bezüglich der hier angesprochenen Ergebnisse unterscheidet sich die japanische FLOSS Untersuchung in weiten Teilen nicht von ihren beiden Vorgängerstudien. Ein interessanter Unterschied ist das höhere Durchschnittsalter der Entwickler in der japanischen OS-Community (mit 31 Jahren im Vergleich zu FLOSS um 5 Jahre höher). Die Aussagen bezüglich der Teilnahmemotivation unterscheiden sich auch unter japanischen OSS-Entwicklern nicht sonderlich von den Ergebnissen der anderen Untersuchungen. Auf eine weitere Darstellung der Ergebnisse wird deshalb verzichtet.

6. Nutzung von Open Source Software in Unternehmen

Neben der privaten Nutzung von Open Source Software wird der professionelle Einsatz in Unternehmen und öffentlichen Einrichtungen immer stärker in den Vordergrund rücken. Bereits 2001 veröffentlichte das damalige Bundesministerium für Wirtschaft und Technologie einen Leitfaden zum Einsatz von Open Source Software in kleinen und mittelständischen Unternehmen (BMWi, 2001). 2003 beschloss die Stadtverwaltung von München, 14.000 Computer auf das Betriebssystem Linux umzustellen. Auch die Bundestagsverwaltung untersuchte ausführlich eine Einführung ihres in die Jahre gekommenen Betriebssystems Windows NT. Alternativ zum Erwerb einer neueren Windowsversion empfahl sich das OSS-Betriebssystem Linux. Man einigte sich schließlich, im Desktopbereich weiterhin das Betriebssystem Windows einzusetzen, während im Serverbereich und bei komplementären Diensten auf OSS zurückgegriffen werden sollte. Neue Zahlen zur Nutzung von Open Source Software in deutschen Unternehmen liefert eine Umfrage des Zentrums für Europäische Wirtschaftsforschung (ZEW), Mannheim. Im Mittelpunkt der Ende 2004 durchgeführten repräsentativen Befragung von mehr als 4400 Unternehmen mit fünf und mehr Beschäftigten aus verschiedenen Dienstleistungsbranchen und dem verarbeitenden Gewerbe stand die Nutzung und Verbreitung von Informations- und Kommunikationstechnologien. Die aus diesen Studien gewonnenen Zahlen zum Einsatz von Open Source Software werden im folgenden Abschnitt analysiert.

Laut der ZEW Studie wird bei einem Viertel der Unternehmen Open Source Software eingesetzt, wobei der Anteil bei den Dienstleistungsunternehmen nur geringfügig höher ist als bei den Unternehmen des verarbeitenden Gewerbes (vgl. Abbildung 4). Betrachtet man die Unternehmen gesondert nach der Zahl ihrer Mitarbeiter, so zeigt sich in beiden Wirtschaftsbereichen ein fast identisches Bild. OSS wird demnach eher in großen Unternehmen eingesetzt. Differenziert nach einzelnen Branchen zeigt sich ein großer Anteil OSS-nutzender Unternehmen bei den EDV- und Telekommunikationsdienstleistern (66 Prozent). Mit weitem Abstand folgen die technischen Dienstleister (40 Prozent). In allen anderen Branchen liegt der Anteil von OSS-nutzenden Unternehmen zwischen 19 Prozent (Verkehrsdienstleister) und 31 Prozent (Unternehmen der Elektrotechnik).

Abbildung 4: Anteil deutscher Unternehmen die OSS einsetzen

Quelle: ZEW, eigene Erhebung, 4. Quartal 2004.

Neben der allgemeinen Nutzung von OSS wurden die OSS-nutzenden Unternehmen auch nach dem jeweiligen Anwendungsbereich befragt, in dem sie OSS einsetzen (vgl. Tabelle 1). Die drei vorgegebenen Antwortmöglichkeiten waren: OSS als Serverbetriebssystem, OSS als Betriebssystem für den PC und OSS als Anwendersoftware. Betriebssysteme für Server sind mit 73 Prozent die häufigste OSS-Anwendung. Weniger verbreitet sind OSS-Betriebssysteme für PCs (53 Prozent). Interessant sind die nach der Unternehmensgröße differenzierten Ergebnisse

zu den beiden Betriebssystemvarianten. Während in größeren Unternehmen vermehrt OSS-Serverbetriebssysteme zum Einsatz kommen, werden in kleineren Unternehmen relativ häufiger OSS-Desktopbetriebssysteme verwendet.

Tabelle 1: Einsatz von OSS nach verschiedenen Anwendungsbereichen

	OSS-Serverbetriebs- system	OSS-Desktop- betriebssystem	OSS- Anwendersoftware
Gesamt	72,7%	53,1%	63,5%
Verarbeitendes Gewerbe	74,6%	49,5%	55,6%
Dienstleistungssektor	72,3%	53,7%	64,9%
Branchen:			
Verbrauchsgüter	81,6%	58,7%	49,7%
Chemie	77,8%	39,8%	42,9%
sonstige Grundstoffe	72,9%	39,4%	64,0%
Metall	64,0%	42,7%	56,9%
Elektrotechnik	78,4%	52,8%	65,6%
Mess- und Regelungstechnik	77,7%	46,9%	63,0%
Fahrzeug	78,2%	41,2%	62,8%
Großhandel	79,7%	51,2%	58,8%
Einzelhandel	58,9%	57,7%	60,9%
Verkehrsdienstleistungen	78,0%	53,1%	67,8%
Banken und Versicherungen	79,8%	33,6%	55,8%
EDV und Telekommunikation	88,9%	60,9%	72,9%
technische Dienstleister	72,6%	54,9%	75,4%
sonstige unternehmensnahe Dienstleister	79,4%	47,3%	63,9%
Verarbeitendes Gewerbe:			
unter 50 Beschäftigte	65,7%	54,4%	55,5%
50 - 499 Beschäftigte	85,0%	43,8%	56,1%
mehr als 500 Beschäftigte	89,1%	40,0%	51,8%
Dienstleistungssektor:			
unter 50 Beschäftigte	70,1%	55,3%	67,3%
50 - 199 Beschäftigte	79,9%	49,5%	56,2%
mehr als 200 Beschäftigte	80,0%	38,5%	60,2%

1441 Unternehmen, die Open Source Software einsetzen.
Angaben hochgerechnet auf die der Befragung zugrunde liegende Grundgesamtheit.

Quelle: ZEW, eigene Erhebung, 4. Quartal 2004.

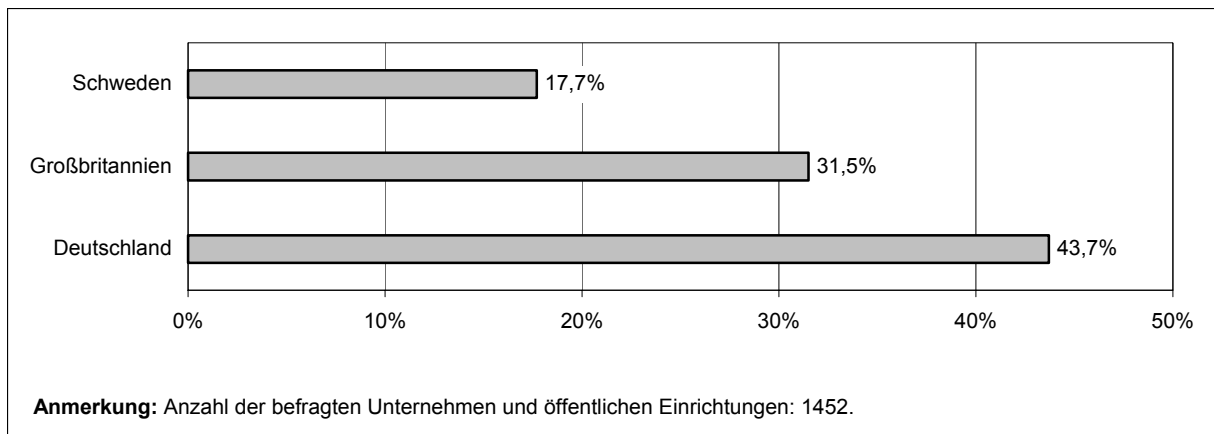
In Österreich wurde 2003 eine Umfrage zum Einsatz und den Erfahrungen mit Open Source Software in Unternehmen von *lizenzfrei it consulting* in Zusammenarbeit mit der Universität Linz durchgeführt (Leitner 2004). Die Ergebnisse dieser Untersuchung basieren auf den Antworten von über 900 Unternehmen. Mehr als die Hälfte der teilnehmenden Unternehmen gab an (54 Prozent), Open Source Software bereits einzusetzen. Da die Teilnahme an der Umfrage grundsätzlich freiwillig war, ist davon auszugehen, dass eher Unternehmen, die bereits OSS einsetzen (und mit dem OSS-Konzept vertraut sind) bereit waren, den Fragebogen auszufüllen. Dies führt dazu, dass diese Umfrage ein eher zu positives Bild über den Einsatz von OSS aufzeigt.

Bezüglich der Einsatzbereiche von OSS in österreichischen Unternehmen liegen Serverbetriebssysteme (74 Prozent) an erster Stelle, gefolgt von Internetanwendungen (69 Prozent) und Datenbanken (59 Prozent). Ein nur geringer Anteil an Unternehmen setzt Open Source Software zur Multimedia (9 Prozent) und Grafikbearbeitung (23 Prozent) ein.

Bei der Frage nach den Beweggründen für den Einsatz von Open Source Software nannten 88 Prozent der Unternehmen Kostenreduktion als einen bestimmenden Faktor. Nicht überraschend liegt hier der Produktsupport, der bei vielen OSS-Anwendungen nur aus Beiträgen in Internetforen besteht, mit 50 Prozent am unteren Ende. Das Fehlen von qualifiziertem Personal wird von den meisten Unternehmen sowohl bei der Frage nach den Problemen bei der Einführung von OSS als auch bei den allgemeinen Nachteilen von OSS angegeben (53 bzw. 44 Prozent). Die Unternehmen, die angaben keine OSS zu nutzen, nannten das „mangelnde Know-How im Unternehmen“ als Hauptgrund für den Nichteinsatz (72 Prozent). Unklar bleibt hier allerdings, ob es sich dabei um ein generell mangelhaftes Wissen über Open Source Software handelt oder nur bezüglich gewisser unternehmensrelevanter OSS-Applikationen. Weitere Gründe, die seitens der Unternehmen gegen den OSS-Einsatz sprechen, sind die „Zufriedenheit mit der bisher verwendeten Software“ (70 Prozent) und die „mangelnde Bekanntheit“ von OSS-Produkten (67 Prozent). Der letzte Punkt macht deutlich, dass OS-Produkte durch einen höheren Bekanntheitsgrad durchaus in der Lage wären, mehr Marktanteile zu gewinnen.

Auch die bereits erwähnte FLOSS Studie widmet sich (in ihrem ersten Teil) der Nutzung von OSS in Unternehmen und öffentlichen Einrichtungen (Berlecon Research, 2002a). Die dort vorgestellten Ergebnisse beziehen sich auf Unternehmen und öffentliche Einrichtungen mit mehr als 100 Beschäftigten in Deutschland, Schweden und Großbritannien. Insgesamt wurden über 1450 Unternehmen und öffentliche Einrichtungen in den drei beteiligten Ländern befragt.

Auf die Frage, ob sie bereits Open Source Software einsetzen oder planen, dies in den nächsten 12 Monaten zu tun, antworteten die Umfrageteilnehmer in den drei Ländern recht unterschiedlich. In Deutschland gaben 44 Prozent der Unternehmen und Einrichtungen an, OSS zu nutzen. Dagegen war der Anteil in Großbritannien mit 31 Prozent und in Schweden mit nur knapp 18 Prozent wesentlich geringer (vgl. Abbildung 5). Die folgenden Ergebnisse beziehen sich auf die Unternehmen, die angaben OSS zu nutzen (insgesamt sind dies knapp 400 Unternehmen).

Abbildung 5: Anteil der Unternehmen und öffentlichen Einrichtungen, die OSS einsetzen

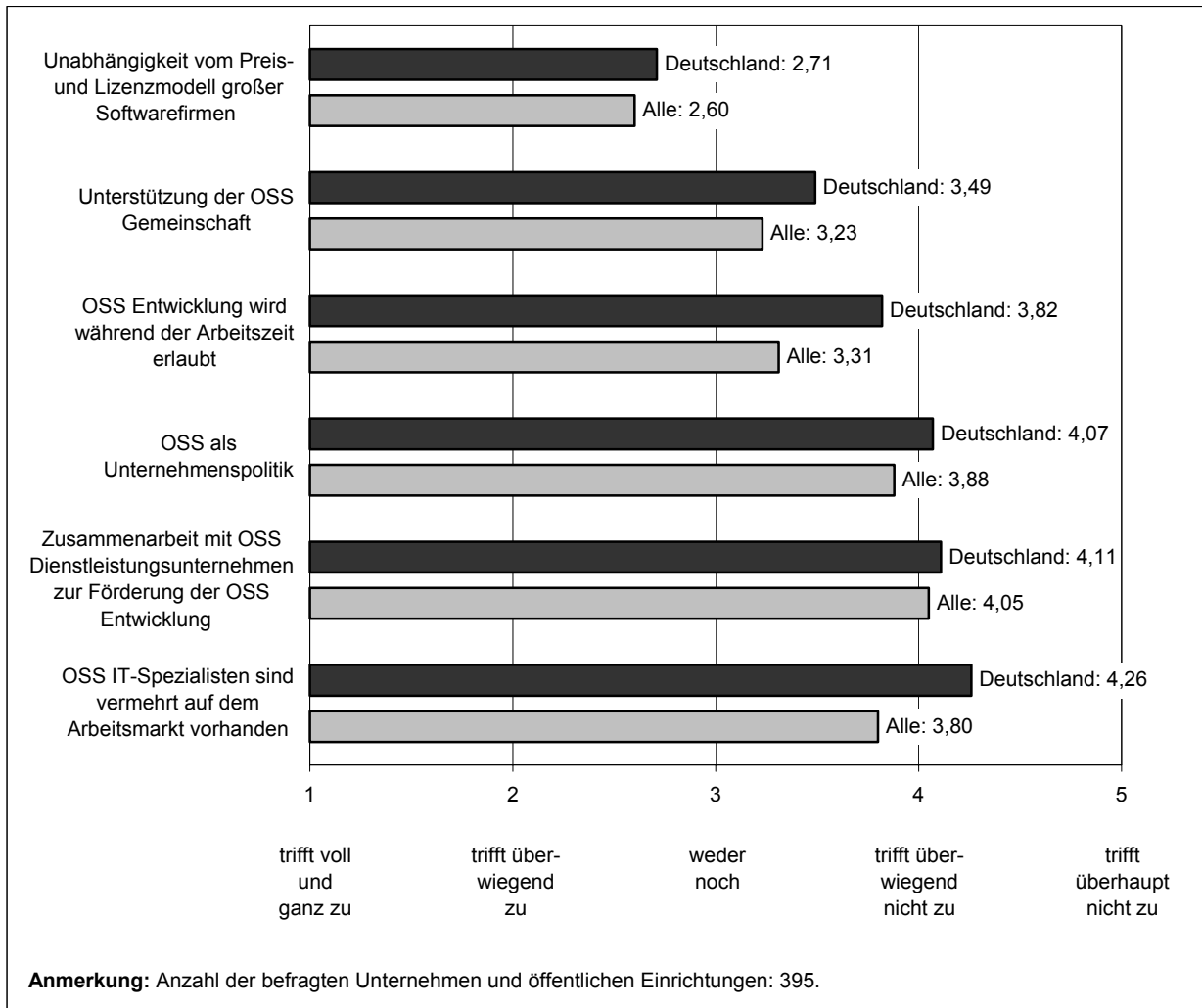
Quelle: Berlecon Research 2002a, S. 16.

Danach befragt, in welchen Anwendungsgebieten OSS eingesetzt wird, antworteten insgesamt 16 Prozent der Unternehmen, dass sie OSS als Serverbetriebssystem einsetzen. Auch in diesem Punkt gibt es große nationale Unterschiede. Während OSS-Serverbetriebssysteme in Deutschland von über 30 Prozent der Unternehmen genutzt werden, sind dies in Schweden und Großbritannien wesentlich weniger (sechs bzw. zehn Prozent). Auch in den anderen drei Anwendungsbereichen (Datenbanken, Desktopanwendungen und Internetseiten) liegen die deutschen Unternehmen und öffentlichen Einrichtungen, wenn auch nicht so deutlich, an der Spitze dieses europäischen Vergleichs.

Ein wesentlicher Teil der Studie beschäftigt sich mit der Einstellung der Unternehmen gegenüber Open Source Software. Dazu wurden sechs Aussagen formuliert, denen die Umfrageteilnehmer in verschiedenem Ausmaß¹⁰ zustimmen bzw. widersprechen konnten (vgl. Abbildung 6). Der Aussage, dass durch den Einsatz von OSS die Open Source Gemeinschaft unterstützt werden soll, konnten insgesamt nur etwa 35 Prozent der Unternehmen wenigstens zum Teil zustimmen. Bei dieser Frage liegen die deutschen Unternehmen mit 29 Prozent am Schluss. Dies zeigt, dass ideologische Verbundenheit mit der OSS-Community nicht als Hauptgrund für den vergleichsweise hohen Einsatz von OSS in Deutschland verantwortlich gemacht werden kann.

Ein weiteres Argument, welches für den Einsatz von Open Source Software spricht, ist die damit gewonnene Unabhängigkeit vom Preis- und Lizenzmodell großer Softwarefirmen. Diesem Argument können insgesamt 56 Prozent der Unternehmen zustimmen. Der Mittelwert liegt hier bei den deutschen Unternehmen etwas über dem Wert für alle Unternehmen (vgl. Abbildung 6), d.h. dass deutsche Unternehmen und öffentliche Einrichtungen diesem Argument im Vergleich zu den Unternehmen in Großbritannien und Schweden weniger zustimmen. Einen signifikanten Unterschied gibt es bei dieser Frage zwischen kleinen (100-500 Mitarbeiter) und großen Unternehmen (über 500 Mitarbeiter). Die großen Unternehmen stimmen dem Argument mit 62 Prozent eher zu als die kleinen Unternehmen mit nur 53 Prozent.

¹⁰ Auf einer Skala von 1, „trifft voll und ganz zu“, bis 5, „trifft überhaupt nicht zu“.

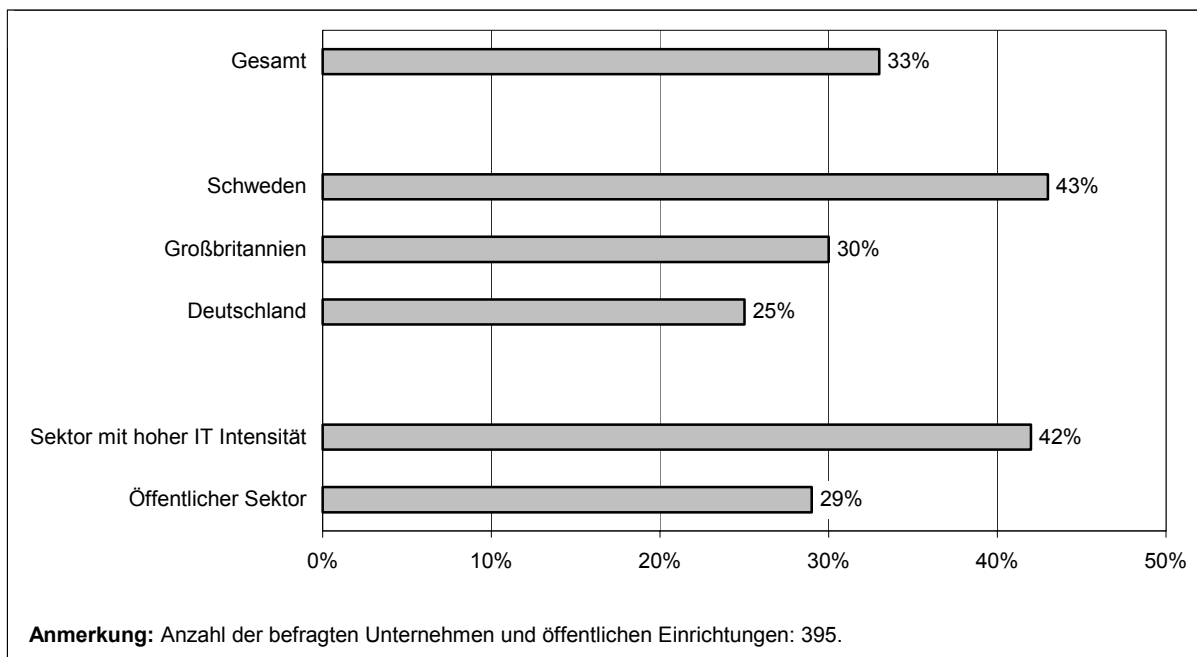
Abbildung 6: Einstellung gegenüber Open Source Software

Quelle: Berlecon Research 2002a, S. 29.

Ein interessanter Punkt bezüglich der Entwicklung von Open Source Software ist die Einstellung der Unternehmen zur Entwicklung von OSS durch ihre Mitarbeiter während der Arbeitszeit. Im Durchschnitt können dieser Aussage immerhin 36 Prozent aller Unternehmen, wenigstens zum Teil, zustimmen. Der Mittelwert aller Unternehmen liegt hier bei 3,3, wobei die deutschen Unternehmen und Einrichtungen mit 3,82 deutlich in Richtung der Aussage „trifft nicht zu“ tendieren (vgl. Abbildung 6). Trotz ihrer relativen Aufgeschlossenheit gegenüber dem Einsatz von OS-Software, sind die Unternehmen in Deutschland bezüglich der Entwicklung von OSS während der Arbeitszeit eher restriktiv eingestellt.

Laut der FLOSS Unternehmensbefragung ist für 33 Prozent der Unternehmen die eingesetzte Open Source Software ein wichtiger bis sehr wichtiger Bestandteil der IT-Infrastruktur (vgl. Abbildung 7). Allerdings geben auch 44 Prozent der Unternehmen an, dass für sie OSS kein wesentlicher Bestandteil der IT-Infrastruktur darstellt. Vergleicht man Unternehmen aus IT-intensiven Branchen mit Einrichtungen des öffentlichen Sektors, so zeigt sich, dass für erstere OSS wesentlich wichtiger ist als für letztgenannte.

Abbildung 7: Anteil der Unternehmen und öff. Einrichtung, für die OSS ein wichtiger oder sehr wichtiger Bestandteil der IT-Infrastruktur darstellt



Quelle: Berlecon Research 2002a, S. 31.

7. Schlussbemerkungen

Open Source Software genießt in der öffentlichen Diskussion immer mehr Aufmerksamkeit. Dies ist zu einem großen Teil den Erfolgen von Open Source Internetbrowsern wie Netscape und Mozilla/Firefox zu verdanken. Allerdings besteht bei der Frage, nach den besonderen Charakteristika von Open Source Software immer noch ein enormer Erklärungsbedarf.

Ziel dieses Beitrags ist es, dem Leser einen kurzen und kompakten Einblick in die historische Entwicklung und die technischen Besonderheiten von Open Source Software zu geben. Dazu wurden auch einige in den letzten Jahren erstellten Studien zur OS-Entwicklergemeinschaft und zum professionellen Einsatz von OSS vorgestellt.

Obwohl OSS bzw. Free Software ein Jahrzehnte altes Phänomen beschreibt, zeichnet sich die heutige OSS-Community (Menschen, die sich an der Entwicklung von OSS beteiligen) durch ihr geringes Durchschnittsalter aus. In mehreren Untersuchungen wurde zudem gezeigt, dass die Entwicklung von OS-Software fast ausschließlich von Männern betrieben wird. Zu den Hauptmotiven für die Teilnahme an der Entwicklung von OSS zählt sowohl der Wunsch, Kenntnisse und Fähigkeiten mit anderen zu teilen, d.h. ein eher altruistischer Motivationsgrund, als auch die Tatsache, sich neue Fähigkeiten durch die Softwareentwicklung anzueignen. Für die OSS-Community bedeutet das Wort „free“ im Wesentlichen Freiheit des Geistes und der Wissenschaft.

Betrachtet man hingegen die Gründe warum sich Unternehmen für den Einsatz von OSS entscheiden, stehen an erster Stelle die deutlich geringeren Lizenzkosten, die durch OSS im Vergleich zu proprietärer Softwarenutzung entstehen. Hier wird „frei“ eher im Sinne von kostenlos verstanden.

Deutsche Unternehmen liegen im europäischen Vergleich bei der Nutzung von Open Source Software an der Spitze. Diesen Schluss kann man aus den Ergebnissen der FLOSS Studie ziehen. Die aktuellen ZEW Ergebnisse bestätigen diese Nutzungszahlen (für große Unternehmen in Deutschland). Die in 2003 erstellte Prognose des Marktforschungsinstitut Soreon, dass bis 2007 jedes vierte Unternehmen in Deutschland Open Source Software einsetzen wird, hat sich nach ZEW-Berechnungen schon Ende 2004 erfüllt. Im Durchschnitt nutzt inzwischen über ein Viertel der Unternehmen OSS. Allerdings wurde auch deutlich, dass einzelne Branchen (z.B. EDV- und Telekommunikationsdienstleister) OSS weit überdurchschnittlich einsetzen.

Trotz des großen Erfolgs von OSS droht der OS-Community inzwischen eine neue Gefahr. Anfang Juni 2005 steht die Einführung von Softwarepatenten in Europa wieder auf der Tagesordnung des Europaparlaments. Vor allem Vertreter von Open Source Software wehren sich zusammen mit kleineren Softwareunternehmen vehement gegen die geplante Patentrichtlinie. Sie sind der Meinung, dass aus Furcht vor Patentverletzungen, viele Entwickler davon abgehalten werden, innovative Beiträge zu OS-Projekten beizusteuern.

8. Literatur und weiterführende Informationen

Bärwolff, Matthias; Gehring, Robert A.; Lutterbeck, Bernd (Hrsg.) (2005)

Open Source Jahrbuch 2005 – Zwischen Softwareentwicklung und Gesellschaftsmodell, Lehmanns Media – LOB.de, Berlin. In http://www.opensourcejahrbuch.de/2005/pdfs/OpenSourceJahrbuch2005_online.pdf, zugegriffen am 21.04.2005

Berlecon Research (2002a)

FLOSS Final Report – Part 1: Free/Libre Open Source Software: Survey and Study – Use of Open Source Software in Firms and Public Institutions – Evidence from Germany, Schweden and UK, Berlin. In http://www.berlecon.de/studien/downloads/200207FLOSS_Use.pdf, zugegriffen am 23.02.2005

Berlecon Research (2002b)

FLOSS Final Report – Part 2: Free/Libre Open Source Software: Survey and Study – Firms' Open Source Activities: Motivations and Policy Implications, Berlin. In http://www.berlecon.de/studien/downloads/200207FLOSS_Activities.pdf, zugegriffen am 23.02.2005

Berlecon Research (2002c)

FLOSS Final Report – Part 3: Free/Libre Open Source Software: Survey and Study – Basics of Open Source Software Markets and Business Models, Berlin. In http://www.berlecon.de/studien/downloads/200207FLOSS_Basics.pdf, zugegriffen am 23.02.2005

Brügge, Bernd; Harrhoff, Dietmar; Picot, Arnold; Creighton, Oliver; Fiedler, Marina; Henkel, Joachim (2004)

Open-Source-Software – Eine ökonomische und technische Analyse, Springer Verlag, Heidelberg.

Bundesministerium für Wirtschaft und Technologie (BMWi) (2001)

Open-Source-Software – Ein Leitfaden für kleine und mittlere Unternehmen. In <http://www.bmwi.bund.de/Redaktion/Inhalte/Pdf/open-source-software,property=pdf.pdf>, zugegriffen am 12.04.2005

David, Paul A.; Waterman, Andrew; Arora, Seema (2003)

FLOSS-US – Free/Libre/Open Source Software Survey for 2003, Stanford Institute for Economic Policy Research (SIEPR), Stanford University, California. In <http://www.stanford.edu/group/floss-us>, zugegriffen am 05.04.2005

e-cology Corporation (2003)

Open Source Software in Canada – A Collaborative Fact Finding Study. In http://www.e-cology.ca/canfloss/report/CANfloss_Report.pdf, zugegriffen am 11.04.2005

Gehring, Robert A.; Lutterbeck, Bernd (Hrsg.) (2004)

Open Source Jahrbuch 2004 – Zwischen Softwareentwicklung und Gesellschaftsmodell, Lehmanns Media – LOB.de, Berlin.

In <http://ig.cs.tu-berlin.de/osjb/OpenSourceJahrbuch2004.pdf>, zugegriffen am 21.04.2005

- Ghosh, Rishab A.; Glott, Rüdiger; Krieger, Bernhard; Robles, Gregorio (2002)
FLOSS Final Report – Part 4: Free/Libre Open Source Software: Survey and Study – Survey of Developers, International Institute of Infonomics, University of Maastricht. In http://www.infonomics.nl/FLOSS/report/FLOSS_Final4.pdf, zugegriffen am 23.02.2005
- Henkel, Joachim (2004)
Ökonomische und historische Aspekte, in: Picot, Arnold und Stefan Doeblin (Hrsg.), Open Source – Tagungsband, Hüthig Telekommunikation, Bonn, S. 19-28
- Lämmer, Anne; Pflüger, Kerstin; Uhe, Bianca; Singh, Mandeep (2001):
Open Source: Geschichte und Grundlagen. In <http://ig.cs.tu-berlin.de/oldstatic/w2000/ir1/referate1/k-1a>, zugegriffen am 21.04.2005
- Leitner, Andreas (2004)
OSS – Umfrage 2003: Der Einsatz und die damit verbundenen Erfahrungen von Open-Source-Software in österreichischen Unternehmen. In http://www.lizenzfrei.at/downloads/OSS-Umfrage_2003.pdf, zugegriffen am 18.02.2005
- Lütge, Gunhild (2003)
Programmierer aller Länder vereinigt Euch!, Die Zeit, 23.10.2003. In http://www.zeit.de/2003/44/Open_Source
- Mitsubishi Research Institute (2004)
Free/Libre/Open Source Software Japanese Developers Online Survey (FLOSS-JP). In http://oss.mri.co.jp/floss-jp/report_en.html, zugegriffen am 07.04.2005
- o.V.
Open-Source-Lizenzen. In <http://openfacts.berlios.de/index.phtml?title=Open-Source-Lizenzen>, zugegriffen am 21.04.2005
- O'Reilly (1999)
Open Source kurz & gut, O'Reilly. In http://www.oreilly.de/german/freebooks/os_tb/os_tb_1.htm#headings1-15, zugegriffen am 07.05.2005
- Pasche, Markus; von Engelhardt, Sebastian (2004)
Volkswirtschaftliche Aspekte der Open-Source-Softwareentwicklung, Arbeits- und Diskussionspapier der Wirtschaftswissenschaftlichen Fakultät der Friedrich-Schiller-Universität Jena.
- Patalong, Frank (2005)
Microsoft kämpft um seine Macht – mit Sicherheit, Spiegel-Online, In <http://www.spiegel.de/netzwelt/technologie/0,1518,341853,00.html>, zugegriffen am 16.02.2005
- Picot, Arnold; Doeblin, Stefan (Hrsg.) (2004)
Open Source – Tagungsband, Hüthig Telekommunikation, Bonn.
- Wheeler, David A. (2005)
Why Open Source Software / Free Software (OSS/FS, FLOSS, or FOSS)? Look at the Numbers! In http://www.dwheeler.com/oss_fs_why.html, zugegriffen am 05.04.2005

IT-Sicherheit in Unternehmen

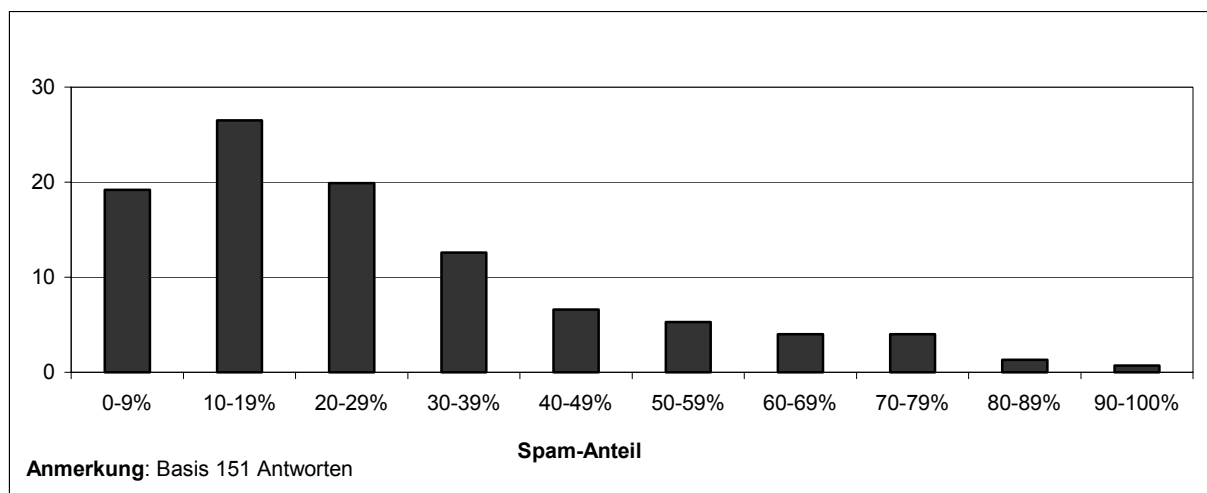
Katrin Schleife, Oliver Schmid

1. Einleitung	83
2. Geschichte der IT-Sicherheit.....	84
3. Grundanforderungen an IT-Sicherheit	85
3.1. Integrität	85
3.2. Vertraulichkeit.....	85
3.3. Verfügbarkeit.....	86
3.4. Authentizität	86
3.5. Verbindlichkeit.....	86
4. IT-Sicherheitsbedrohungen und Möglichkeiten der Abwehr.....	87
4.1. Schadhafte Programme.....	87
4.1.1. Viren und Würmer.....	87
4.1.2. Trojanische Pferde.....	88
4.2. Phishing	88
4.3. Denial-of-Service	89
4.4. Hacker.....	89
4.5. Schwachstelle Benutzer.....	89
5. Studien zur IT-Sicherheit in Unternehmen.....	90
5.1. Die Studien	90
5.2. Die IT-Sicherheitssituation in deutschen Unternehmen.....	91
5.2.1 Malware in Unternehmen weit verbreitet.....	91
5.2.2 Hohe Dunkelziffer im Bereich Computerkriminalität.....	92
5.2.3 Fehlverhalten der eigenen Mitarbeiter birgt hohes Schadenspotential.....	93
5.2.4 Vielfältige Abwehrmaßnahmen nötig	94
5.2.5 Einsatz von Sicherheitstechnologien nimmt zu.....	94
5.2.6 Unternehmen planen Erhöhung der Investitionen in IT-Sicherheit	96
5.2.7 Hemmnisfaktoren einer umfassenden IT-Sicherheit.....	97
6. Schlussbemerkungen	97
7. Literatur	98

1. Einleitung

Neue Informations- und Kommunikationstechnologien (IKT) bestimmen mehr und mehr die Arbeits- und Geschäftsprozesse in deutschen Unternehmen. Der Datenaustausch zwischen intern und extern vernetzten PCs, insbesondere die Nutzung des Internets sind mittlerweile ein wichtiger Bestandteil des Geschäftsalltags¹. Unabhängig davon, ob sich die Netznutzung auf den Austausch von E-Mails beschränkt, oder ob von den Unternehmen in großem Umfang E-Commerce und E-Business betrieben wird, muss die Sicherheit und Zuverlässigkeit der genutzten IKT sowohl innerhalb der Unternehmen als auch im Online-Kontakt zu den Geschäftspartnern gewährleistet sein. Unternehmensstudien zeigen jedoch, dass Unternehmensdaten und elektronische Geschäftsprozesse in vielen Unternehmen nur unzureichend gesichert sind. Der Vielzahl an externen und internen Gefahren steht oftmals nur eine geringe Zahl an Abwehrstrategien gegenüber. Das Problembewusstsein im Hinblick auf mögliche Gefährdungen der IT-Sicherheit ist bei den Entscheidern und Mitarbeitern im Unternehmen in vielen Fällen nicht ausreichend ausgeprägt. Aber auch knappe IT-Budgets oder der Mangel an qualifiziertem IT-Personal stellen Hemmnisse für eine ausreichende IT-Sicherheit dar. Zahlreiche Statistiken verweisen auf das volkswirtschaftliche Schadenspotential unzureichender IT-Absicherung.² Der Stuttgarter IT-Dienstleister NextiraOne geht für 2003 von weltweit rund 700 Millionen IT-Sicherheitsvorfällen aus (NextiraOne 2004). Die Europäische Kommission schätzt, dass mittlerweile rund 50 Prozent des weltweiten E-Mailverkehrs aus Spam-Mails besteht (siehe auch Abbildung 1).

Abbildung 1: Anteil an Spam an der eingehenden E-Mail



Quelle: Kes 2004, S.18.

¹ Die aktuelle IKT-Umfrage des ZEW kommt zu dem Ergebnis, dass 93 Prozent der Unternehmen in Deutschland Ende 2004 über einen Internetanschluss verfügten. Etwa die Hälfte der Beschäftigten (48 Prozent) hatte an ihrem Arbeitsplatz Zugang zum Internet (ZEW 2005).

² Statistische Angaben zu tatsächlichen Schäden können immer nur grobe Schätzungen wiedergeben. Der Grund liegt zum einen in Messproblemen. Zum anderen geben Unternehmen nur ungern Auskunft über ihre Schäden, da dies Rückschlüsse auf ihre möglicherweise unzureichende IT-Sicherheitsituation zuließe.

Den dadurch entstehenden Produktivitätsverlust bei Unternehmen in der EU beziffert die Europäische Kommission auf 2,5 Milliarden Euro pro Jahr (IHK-Köln 2004). Die durch Viren und ähnliche Schädlinge insgesamt entstandenen Kosten schätzt der E-Mail-Dienstleister Clearswift für 2003 auf weltweit etwa 20 Milliarden Dollar, der Software-Anbieter Trend Micro spricht gar von 55 Milliarden Dollar. Darin enthalten sind neben den Direktschäden auch Gewinnausfälle durch Kommunikationsbehinderungen (ASW 2004).

Der vorliegende Beitrag beleuchtet das Thema IT-Sicherheit von mehreren Seiten. Dabei wird zunächst eine kurze Einführung in die Geschichte der IT-Sicherheit gegeben. Im darauf folgenden Abschnitt werden die Grundanforderungen an sichere Daten, wie z.B. Integrität und Vertraulichkeit, erläutert. Welche Gefahren diesen Grundanforderungen drohen und welche Abwehrmöglichkeiten es gibt, wird im Anschluss daran dargestellt. Den Abschluss des Beitrags bilden ausgewählte Ergebnisse von Unternehmensstudien, die verschiedene Aspekte der IT-Sicherheit in den Unternehmen quantitativ erfasst haben.

2. Geschichte der IT-Sicherheit³

Informationstechnologische Sicherheit, die nicht nur die Sicherung von Daten, sondern auch die der Technik einbezieht, wird Mitte der 70er Jahre in den Unternehmen von Bedeutung. Die reine Lochkartentechnik früherer Jahre erforderte keinen besonderen Schutz. Vielmehr war diese Technik der Massenverarbeitung von Daten selbst, aufgrund ihrer Fehler- und Ausfallanfälligkeit, das größte Risiko für die Korrektheit der Ergebnisse. Mit der Einführung von Teilnehmer-Betriebssystemen jedoch, die den direkten Anschluss von Benutzersichtgeräten (Terminals) an Großrechner ermöglichten, erhielten die Computerbenutzer Online-Zugriff auf Daten, konnten sie bearbeiten und löschen. Um den Benutzerzugriff auf Programme und Daten zu regeln, entwickelte IBM einen Zusatz zu den bestehenden Betriebssystemen: RACF (Resource Access Control Facility). Der Einsatz dieses Programms gilt als eigentliche Geburtsstunde der IT-Sicherheit. RACF sorgt noch heute mit Hilfe von Benutzerkennung und Passwort für die Identifizierung und Authentisierung der Benutzer und führt ein Logbuch, das die Benutzerzugriffe protokolliert.

Die rasche Verbreitung von PCs in den Unternehmen in den 80er Jahren machte die Verwaltung von mehreren Benutzern und deren Zugriffsrechten erforderlich. Realisiert wurde dies mit der Entwicklung und Einführung eines RACF für PCs („SAFE-MAN“, später „SAFE-GUARD“ genannt). Mit der Vernetzung von PCs und dem Aufbau der so genannten Client-Server-Architektur stieg die Bedeutung der PCs für die Unternehmen enorm. Sie wurden zu einer bedeutenden Konkurrenz zu den zentralen Großrechnern, denn die Netzwerkbetriebssysteme verfügten über eine leistungsfähige Benutzerverwaltung und boten somit IT-Sicherheit in ähnlich großem Umfang wie die Großrechner.

³ Die Ausführungen in diesem Abschnitt basieren auf Görtz (2004) und BSI (2005).

In den späten 80er Jahren wurde das Internet, dessen Vorläufer ARPANET bis dahin dem US-Militär vorbehalten war, für zivile Zwecke freigegeben. Das Internet war zunächst für nicht-kommerzielle Zwecke gedacht, doch schon 1994 überstieg die Zahl der kommerziellen Nutzer die der wissenschaftlichen Teilnehmer. Der Bedarf an IT-Sicherheit stieg durch die Nutzung des Internet sprunghaft an. Anti-Virenprogramme und Verschlüsselungstechnologien kamen erstmals zum Einsatz, um sichere Online-Anwendungen zu ermöglichen. Sie leisten auch heute noch einen wichtigen Beitrag zur IT-Sicherheit. Darüber hinaus dienen Firewalls als Schutzmauer gegen unerwünschte Eindringlinge und sind für das sichere Agieren im Netz nicht mehr wegzudenken.

Mittlerweile gibt es unzählige Produkte auf dem Markt, die IT-Sicherheit gewährleisten sollen. Alle haben sie gemeinsam, dass sie ständig erneuert und den veränderten Anforderungen angepasst werden müssen, um genügend Schutz gegen immer neue Bedrohungen für Daten und Technik bieten zu können.

3. Grundanforderungen an IT-Sicherheit

Integrität, Vertraulichkeit, Verfügbarkeit, Authentizität, und/oder Verbindlichkeit sind die wichtigsten Eigenschaften sicherer Daten. Verschiedene Sicherheitsmaßnahmen kommen zum Einsatz, um diese allgemein gültigen Grundanforderungen, die im Folgenden näher erläutert werden, sicherzustellen. Die Ausführungen in diesem Kapitel basieren auf Eckert (2004a, 2004b).

3.1. Integrität

Die Gewährleistung von Datenintegrität bedeutet, dass Daten nur von Befugten in beabsichtigter und erkennbarer Weise modifiziert werden können. Dies erfordert die Festlegung von Rechten zur Nutzung von Daten, wie z.B. Lese- oder Schreibberechtigungen. Unerlaubte Manipulationen können zum einen durch unautorisierte Zugriffe auf Rechner und Daten, zum anderen durch das Abfangen und Verändern von Datenpaketen durch Dritte (Man-in-the-Middle-Attacken) beim Informationsaustausch zwischen zwei Parteien erfolgen. Durch diese Eingriffe sind die Vollständigkeit und/oder die Korrektheit der Informationen nicht mehr gewährleistet, die Datenintegrität ist verletzt.

3.2. Vertraulichkeit

Kryptografische Verfahren dienen dazu, die Vertraulichkeit sensibler Informationen bei deren Austausch zwischen Partnern auf dem gesamten Kommunikationsweg sicherzustellen. Vertraulichkeit bedeutet, dass nur die am Informationsaustausch beteiligten Partner in den Besitz dieser Informationen gelangen dürfen. Kriminelle Angriffe zielen häufig darauf ab, die Identität eines Partners vorzutäuschen und so an vertrauliche Informationen zu gelangen

(Spoofing-Angriffe). Um dies zu verhindern sollte die Übertragung der Daten verschlüsselt erfolgen. Sender und Empfänger benötigen einen gemeinsamen geheimen Schlüssel, um die jeweiligen Informationen lesen zu können. Eine Hauptschwierigkeit des vertraulichen Informationstransfers liegt dabei im Austausch dieses Schlüssels zwischen den beteiligten Partnern, da auch dieser nicht in die Hände Dritter gelangen darf.

3.3. Verfügbarkeit

Verfügbarkeit im Rahmen der IT-Sicherheit bedeutet, dass autorisierte Teilnehmer in der Nutzung von Daten oder Programmen nicht unautorisiert beeinträchtigt werden. So wird Verfügbarkeit z.B. durch technische Ausfälle oder durch kriminelle Angriffe, die zu einer Systemüberlastung führen (Denial of Service Attacks), eingeschränkt oder beseitigt. Von autorisierten Beeinträchtigungen wird hingegen gesprochen, wenn es aufgrund von Engpässen in der Prozessverwaltung zu „normalen“ Ausführungsverzögerungen kommt. Diese stellen a priori noch keine Verletzung der Verfügbarkeit dar.

3.4. Authentizität

Das Sicherheitsziel Authentizität wird unterteilt in die Sicherstellung der Echtheit von Daten einerseits und in die eindeutige Identifikation des Benutzers andererseits. Für die Gewährleistung der Authentizität von Daten kommen beispielsweise Message Authentication Codes, digitale Signaturen oder digitale Wasserzeichen zum Einsatz. Damit lassen sich Urheberschaft und Herkunft der Daten eindeutig zuordnen. Diese Kennzeichnung trifft jedoch keine Aussage darüber, ob das entsprechende Objekt (z.B. ein Programm) tatsächlich funktioniert oder nicht. Die Identifikation eines Teilnehmers und die damit mögliche Beschränkung seines Datenzugriffs können mit verschiedenen Mitteln der Benutzererkennung überprüft werden. Zu diesen gehören z.B. der Gebrauch von Passwörtern und Schlüsseln, der Einsatz von Smartcards oder die Erkennung biometrischer Merkmale. Mithilfe eines Authentifizierungsprotokolls („Logdateien“) können die erfolgreichen und zurückgewiesenen Datenzugriffe aufgezeichnet und überwacht werden.

3.5. Verbindlichkeit

Verbindlichkeit ist dann gewährleistet, wenn das Senden und Empfangen von Informationen eindeutig bestimmbar ist und nicht geleugnet werden kann. Von großer Bedeutung ist die Verbindlichkeit z.B. bei elektronischen Vertragsabschlüssen und der Verwendung der digitalen Signatur, um die Rechtsverbindlichkeit durchgeführter geschäftlicher Transaktionen zu garantieren. Es muss gewährleistet sein, „dass mit der Signatur nur genau die Daten signiert werden, die man gesehen, geprüft und mit der Unterschrift bewusst akzeptiert hat“ (Eckert 2004b, S. 24).

4. IT-Sicherheitsbedrohungen und Möglichkeiten der Abwehr

Die IT-Sicherheitsbedrohungen für private Nutzer wie für Unternehmen sind vielfältig und nehmen beständig zu. Neben höherer Gewalt (z.B. Feuer), organisatorischen Mängeln und technischem Versagen zählen vor allem menschliches Fehlverhalten und vorsätzliches Handeln zu den gravierendsten Bedrohungen. Beispiele aus den beiden letztgenannten Gefahrenbereichen werden im Folgenden näher erläutert und Möglichkeiten zu ihrer Abwehr vorgestellt.

4.1. Schadhafte Programme

Schadhafte Programme (Malware) beeinträchtigen meistens die Verfügbarkeit und Integrität von Daten, in einigen Fällen gefährden sie auch deren Vertraulichkeit. Sie werden im Vorfeld programmiert und benötigen somit im Moment ihrer Aktivierung keine Einflussnahme ihres Urhebers.

4.1.1. Viren und Würmer

Im November 1983 stellte Frederick Cohen im Rahmen seiner Doktorarbeit ein Programm vor, welches in der Lage war, andere Programme so zu verändern, dass es Teil des modifizierten Programms wurde. In Analogie zur Biologie werden seither Programme, die andere Programme auf diese Weise „infizieren“ können, Viren genannt, da sie selbst ohne einen Wirt nicht existieren können und sich von ihrem Wirt auf weitere Opfer verbreiten können.

Der eigentlichen Definition ist mit diesen beiden Eigenschaften, also dem Befall von Programmen und der Vermehrung, bereits Genüge getan, eine Schadensfunktion ist nicht zwingend erforderlich. So gibt es auch Viren, die lediglich als Beweis für die Durchführbarkeit einer Idee (Proof of Concept) dienen sollen und daher keine Daten zerstören, sondern beispielsweise Schwachstellen aufdecken.

Die möglichen Schadensfunktionen der Viren sind vielseitig. Sie reichen von teilweise zufälligen Schäden, wie der Nichtausführbarkeit der befallenen Datei, bis hin zu beabsichtigten Schädigungen, wie der Manipulation oder Löschung von Daten. Im Extremfall können Viren sogar die Hardware eines Rechners schädigen. Diese Schadensformen sind inzwischen jedoch kaum noch vertreten. Dafür nimmt die Zahl der Programme, die vertrauliche Daten weitergeben (Spyware) oder Hintertüren (Backdoors) zu PCs öffnen, massiv zu. Relativ häufig vertreten waren bis vor etwa fünf Jahren Makroviren, die nicht im herkömmlichen Sinne Dateien infizieren, sondern sich die Steuersequenzen von Office-Anwendungen zunutze machen, um sich in deren Dokumenten zu verbreiten. Da die Software-Hersteller auf diese Gefahr reagiert haben und Makroviren nun nicht mehr automatisch gestartet werden, ist die Gefahr, die von ihnen ausgeht, mittlerweile als gering einzustufen.

Würmer hingegen sind eigenständige Programme, die im Gegensatz zum Virus keine Dateien befallen, sondern als eigene Datei in meist mehreren Verzeichnissen auftauchen. Auch bei den Würmern gehört die Schadensfunktion nicht zu den definierenden Fähigkeiten. Jedoch können auch sie den Computer ihres Opfers auf verschiedenste Weise schädigen, indem sie beispielsweise gezielt Dateien zerstören, lokale Daten (z.B. Passwörter) an den Programmierer des Wurms übermitteln oder Speicherressourcen ausschöpfen. Seit 2002 ist eine Dominanz der Würmer unter der Malware zu beobachten, da viele Windows-Benutzer inzwischen keinen Überblick mehr über den Inhalt ihrer Systemordner haben und sich die ungewünschten Programme dort problemlos verstecken können.

4.1.2. Trojanische Pferde

Bei den Trojanischen Pferden (Trojanern), hat man sich bei der Namensfindung der griechischen Mythologie bedient. Diese Programme täuschen dem Anwender vor, nützliche Aufgaben erfüllen zu können, um Vertrauen zu erwecken. Gleichzeitig führen sie jedoch unerwünschte, verborgene Aktionen durch. So sind Trojaner mit besonderen Eigenschaften ausgestattet, um z.B. in ein System einzudringen, um Daten aufzuzeichnen oder zu manipulieren. Auf Grund dieser Täuschung werden Trojaner häufig vom Benutzer selbst installiert, teilweise aber auch durch Viren bzw. Würmer, die diese Installation als Teil ihrer Schadensfunktion haben. Trojaner selbst haben keine Reproduktionsfunktion.

Die aufgeführten Malware-Programme sind weit verbreitet und stellen daher für einen ungeschützten Rechner eine große Gefahr dar. Antiviren-Programme helfen, eine Infektion zu vermeiden, und sind in der Lage, infizierte Objekte sowie die gefundenen Viren anzuzeigen. In Kombination mit einer Firewall sind sie ein wirksamer Schutz gegen so genannte Malware. Während sich Unternehmen am sinnvollsten mit einer Netzwerkinstallation und einer Hardware-Firewall schützen können, gibt es für den privaten Anwender kostenlose Antiviren-Programme und Personal Firewalls.

4.2. Phishing

Diese relativ neue Gefahrenform wird überwiegend per E-Mail verbreitet. Phishing ist eine Methode, vertrauliche Informationen wie Passwörter, Kreditkartennummern, Bankzugangsdaten usw. zu stehlen. Der Benutzer wird aufgefordert, auf gefälschten Webseiten seine vertraulichen Daten einzugeben. Diese Webseiten ähneln den „echten“, z.B. den Seiten von Kreditinstituten, oftmals bis ins Detail, sodass die Opfer von Phishing keinen Verdacht schöpfen. Hier hilft meist ein gesundes Misstrauen des Benutzers, denn im Normalfall werden seriöse Anbieter eine solche Eingabe nicht von ihren Kunden fordern. In Deutschland bietet zudem das PIN/TAN-System von Banken und Sparkassen einen guten Schutz gegen den Online-Missbrauch von Bankzugangsdaten.

4.3. Denial-of-Service

Wörtlich übersetzt handelt es sich hier um die Nichtverfügbarkeit eines Dienstes, die auf verschiedenen Wegen herbeigeführt werden kann. Da diese Angriffe selten von einem einzelnen Rechner aus erfolgen, spricht man auch häufig von verteilten Angriffen oder DDos (wobei das erste D für Distributed steht). Meistens wird durch einen (D)DoS-Angriff versucht, durch das Ausnutzen von Schwachstellen Server zu überlasten, damit diese ihre eigentliche Aufgabe nicht mehr erfüllen können. Gelingt der Angriff, so liegt der Verlust der Verfügbarkeit vor. Die Gefahr, Opfer einer DoS-Attacke zu werden, besteht jedoch nur für Server von Unternehmen. Privatpersonen kommen lediglich zu Schaden, wenn sich der Angreifer Zugang zu ihrem PC verschafft, um von dort den Angriff durchzuführen. Gegen DoS-Angriffe kann man sich mit einer Firewall schützen. Da bei solchen Angriffen oft Sicherheitslücken ausgenutzt werden, ist die Installation von Patches, also Sicherheitsupdates, sehr wichtig.

4.4. Hacker

Von Hackern geht eine besondere Gefahr aus, da sie nicht wie ein Programm vorgegebene Routinen durchlaufen, sondern flexibel auf die gegebene Situation reagieren können. Dabei sollte man zwischen Hackern, die ihr Handwerk verstehen, und so genannten „Script-Kiddies“ unterscheiden. Letztere haben oft nur geringe Programmierkenntnisse und müssen sich bei ihren Aktivitäten auf die Fähigkeiten der von ihnen verwendeten Tools verlassen.

Hacker sind Personen, die sich unerlaubt Zugriff auf fremde Systeme verschaffen oder es zumindest versuchen. Sie nutzen dabei sowohl die Sicherheitslücken des angegriffenen Betriebssystems als auch andere Schwachstellen, wie beispielsweise unsichere Passwörter, aus. Nach dem erfolgreichen Zugriff auf das gehackte System ist lediglich der Verlust der Vertraulichkeit gegeben. Prinzipiell ist die Verfügbarkeit und Integrität der Daten bis dahin noch nicht gefährdet, da manche Hacker nur an der Herausforderung interessiert sind und nicht daran, wirklich Schaden zu verursachen. Erst wenn der Angreifer die Daten, auf die er nun Zugriff hat, manipuliert, gehen auch Verfügbarkeit und Integrität verloren.

Der erfolgreiche Angriff eines Hackers lässt sich oft schwerer nachweisen als vergebliche Versuche, da der Hacker mit der Veränderung von Logdateien seine Spuren verwischen kann. Wie gegen DoS-Attacken kann man sich gegen Hacker am besten mit Firewalls und Patches schützen.

4.5. Schwachstelle Benutzer

Ein nicht zu unterschätzendes Problem für die Sicherheit eines Systems sind die Anwender selbst. Mangelnde Kenntnisse im Umgang mit IT-Sicherheit können ungeahnte Folgen nach sich ziehen, wenn beispielsweise Antiviren-Programme aus Performance-Gründen beendet werden oder bei der Personal Firewall einfach jeder Zugriff per Mausklick erlaubt wird. Wird das Löschen wichtiger Daten gleich bemerkt, kann das umgehende Aufspielen eines Back-ups

das Problem beheben. Wird jedoch ein System mit Malware infiziert, können die mitunter erheblichen Schäden auch erst wesentlich später entdeckt werden.

Unsichere Passwörter können Hackern den unerlaubten Zugriff erleichtern, da das Knacken eines einfachen Passwortes (z.B. Namen oder einfache Buchstabenkombinationen) meist nur wenige Minuten, oft sogar nur Sekunden, benötigt.

Gegen den Menschen als Sicherheitslücke hilft nur die Schulung aller Mitarbeiter, die einen Computerarbeitsplatz haben. Zwar sind die Kosten für diese Weiterbildung hoch, aber im Zweifelsfall erheblich geringer als für die Wiederherstellung eines Systems nach einem Totalausfall. Die Kette der IT-Sicherheit ist nun mal nur so stark wie ihr schwächstes Glied.

5. Studien zur IT-Sicherheit in Unternehmen

Verschiedene Unternehmensstudien belegen, dass nahezu jedes Unternehmen bereits von IT-Sicherheitsproblemen, wie z.B. Spam, Viren-Infektionen oder Denial-of-Service-Attacken, betroffen war. Für die Unternehmen ist es daher in zunehmendem Maße wichtig, IT-Sicherheitsstrategien zu entwickeln und die Durchführung von Schutzmaßnahmen voranzutreiben. Im Folgenden werden sechs IT-Sicherheitsstudien aus den Jahren 2002 bis 2005 vorgestellt und anhand ausgewählter Fragen ein kurzer Überblick über die Situation in den deutschen Unternehmen im Hinblick auf IT-Sicherheit gegeben.

5.1. Die Studien

Anfang 2005 wurde die Unternehmensstudie des Management-Software-Anbieters Computer Associates in Zusammenarbeit mit dem Marktforschungsunternehmen Lünendonk veröffentlicht (im Folgenden kurz „CAL-Studie“ genannt). Die dieser Studie zugrunde liegende Befragung wurde Ende 2004 als Online-Umfrage durchgeführt. Für die Analyse der aktuellen Sicherheitsprobleme und der Erfahrungen mit den verschiedenen Abwehrmaßnahmen in den Unternehmen konnten 460 Fragebögen ausgewertet werden (Computer Associates 2005).

Netegrity, ein Unternehmensbereich von Computer Associates hat 2004 im Rahmen einer gemeinsam mit TÜV Secure iT GmbH durchgeführten Studie („Netegrity-Studie“) 216 Unternehmensvertreter verschiedener Branchen zum Stand der IT-Sicherheit befragt. Die anonymen Fragebögen waren Tagungs- und Seminarunterlagen von Fachveranstaltungen zur IT-Sicherheit beigelegt und richteten sich somit an Personen, die für das Thema IT-Sicherheit ohnehin schon sensibilisiert waren (Netegrity 2004).

Einen „Lagebericht zur Informationssicherheit“ liefern „Kes“ (Zeitschrift zur Informationssicherheit) und Microsoft in ihrer gemeinsamen Studie aus dem Jahre 2004 („Kes-Microsoft-Studie“). Der umfangreiche Fragebogen wurde der Zeitschrift „Kes“ beigelegt, sodass vorwiegend die Leserschaft und damit Personen, denen ein erhöhtes Sicherheitsbewusstsein unterstellt werden kann, zu den Antwortenden gehören. Die Ergebnisse können dementsprechend positiv verzerrt sein. Dies gilt es bei Rückschlüssen aus den Daten zu berücksichtigen. Als Basis für die Analyse dienen 163 Antworten, die zum überwiegenden Teil von deutschen (86%) aber auch von Unternehmen aus der Schweiz, aus Österreich, aus den USA oder aus sonstigen Ländern stammen (Kes 2004).

Eine weitere „Kes“-Sicherheitsstudie wurde im Jahre 2002 in Zusammenarbeit mit KPMG erstellt (kurz: „Kes-KPMG-Studie“). 260 Teilnehmer beantworteten den Fragebogen. Sie stammen in erster Linie aus großen mittelständischen Unternehmen sowie Großunternehmen und -institutionen. Die durchschnittliche Zahl der Mitarbeiter bei den teilnehmenden Unternehmen lag bei über 8000. Auch hier gilt es, mögliche positive Verzerrungen aufgrund eines unterstellten hohen Sicherheitsbewusstseins der Teilnehmer zu berücksichtigen (Kes 2002).

Im Rahmen einer Panelstudie zur IT-Sicherheit der Time Kontor AG (TK-Studie) konnten in den Jahren 2002 und 2003 deutschlandweit und branchenübergreifend jeweils gut 700 Entscheider für ein Interview gewonnen werden. Die meisten Befragten stammen aus mittelständischen Unternehmen. Die Interviews wurden telefonisch und/oder schriftlich durchgeführt (Time Kontor 2002 & 2003).

5.2. Die IT-Sicherheitssituation in deutschen Unternehmen

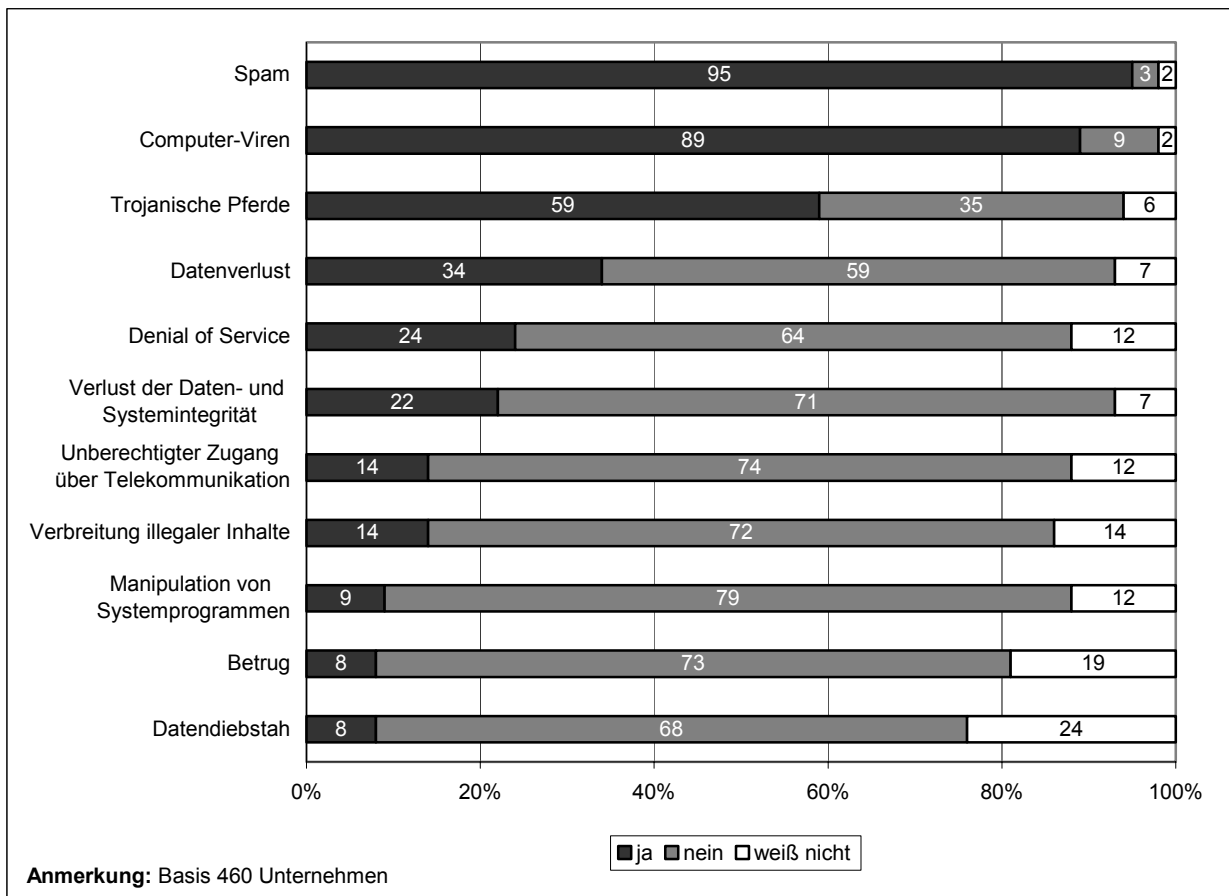
Durch die Nutzung von Informations- und Kommunikationstechnologien entstehen in den Unternehmen spezifische Sicherheitsbedrohungen, die sowohl die eingesetzte Hard- und Software als auch den organisatorischen Bereich betreffen. Ein bedeutendes Gefahrenpotential liefert zudem menschliches Fehlverhalten. In den genannten Unternehmensstudien werden das Ausmaß der Bedrohungen, die Formen der Abwehrmaßnahmen, die Höhe der Investitionen in IT-Sicherheit usw. quantitativ erfasst. Die Ergebnisse werden im Folgenden auszugsweise vorgestellt.

5.2.1 Malware in Unternehmen weit verbreitet

Die meisten der in den Studien befragten Unternehmen gaben Spam und Malware (Computer-Viren, Würmer, Trojanische Pferde) als diejenigen Sicherheitsprobleme an, mit denen ihr Unternehmen kürzlich konfrontiert war. So sahen sich 2004 laut *CAL-Studie* (siehe Abbildung 2) mehr als 95 Prozent der Unternehmen mit Spam konfrontiert, Viren und Würmer tauchten in 89 Prozent der Unternehmen auf, Trojaner bei 59 Prozent. Gemäß *Kes-Microsoft-Studie* waren 88 Prozent der Befragten von mindestens einer Malware-Kategorie betroffen. Wesentlich weniger Unternehmen sahen sich mit den verschiedenen Formen von Computerkriminalität, d.h. den gezielten Sicherheitsangriffen, konfrontiert. So wurden in der *CAL-Studie*

beispielsweise Betrug und Datendiebstahl von jeweils nur acht Prozent der Unternehmen als aktuelle Sicherheitsprobleme genannt. Hier ist allerdings auch die Zahl der „weiß nicht“-Antworten besonders hoch. Dies deutet auf eine hohe Dunkelziffer hinsichtlich dieser Gefahrenquellen hin. Während beim Auftreten von Spam oder Viren zumeist Sicherheitsprogramme Alarm schlagen bzw. aufgrund umfangreicher Medienberichterstattung die Aufmerksamkeit auf diese Gefahren gelenkt wird, ist dies bei Betrug oder Datendiebstahl oft nicht der Fall und die Entdeckung damit schwieriger. Datendiebstahl ist zudem häufig die Folge eines erfolgreichen Hacking-Angriffs. Dabei werden die hinterlassenen Spuren häufig verwischt, was eine Entdeckung weiter erschwert.

Abbildung 2: Mit welchen Sicherheitsproblemen wurden Sie/Ihr Unternehmen im vergangenen Jahr konfrontiert?



Quelle: Computer Associates 2005, S.9.

5.2.2 Hohe Dunkelziffer im Bereich Computerkriminalität

Diese Diskrepanz zwischen der empfundenen Bedrohung durch Malware und dem erfassten Auftreten von Computerkriminalität in den Unternehmen zeigen auch die Ergebnisse der *TK-Studie* aus dem Jahr 2002. Während insgesamt mehr als die Hälfte (56 Prozent) der Entscheider Sicherheitsvorfälle aufgrund von Viren, Würmern und Trojanern verzeichneten, lagen die Werte für Vorfälle wie Denial-of-Service-Attacken (9 Prozent), Hacking (6), Sabotage (4), Betrug (2) und Spionage (2) weitaus niedriger. Insgesamt ergibt sich für die Computerkriminalität damit jedoch ein nicht unerhebliches Schadenspotential.

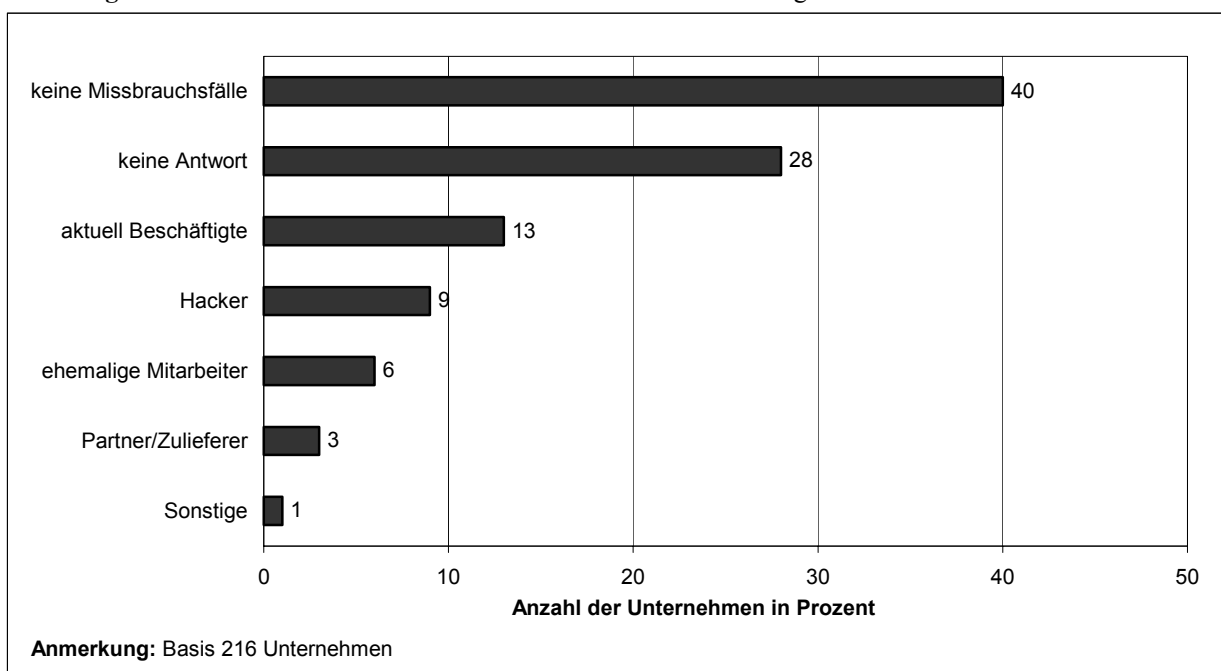
Darüber hinaus wurden in der *TK-Studie 2002* auch Vorfälle aufgrund von technischem Versagen oder Fehlbedienung untersucht. Diese Bereiche nehmen einen hohen Stellenwert ein: Immerhin 42 Prozent der Unternehmen waren mit sicherheitsrelevanten technischen Defekten konfrontiert und gut 20 Prozent hatten Systemausfälle aufgrund von Fehlbedienung zu verzeichnen.

5.2.3 Fehlverhalten der eigenen Mitarbeiter birgt hohes Schadenspotential

Die in der *Kes-Microsoft-Studie 2004* erfragte Schadensstatistik verdeutlicht, dass Irrtum und Nachlässigkeit der eigenen Mitarbeiter neben Malware ein erhebliches Schadenspotential beinhalten. Jeweils gut die Hälfte der Befragten bestätigte einen tatsächlich entstandenen Schaden durch diese beiden Formen der Sicherheitsverletzungen. Schon in der *Kes-KPMG-Studie 2002* wird „Irrtum und Nachlässigkeit eigener Mitarbeiter“ als bedeutendstes Einzelrisiko angesehen, dicht gefolgt von der Bedrohung durch Malware.

Die Bedeutung der „inneren Sicherheit“ unterstreicht auch die *Netegrity-Studie* aus dem Jahre 2004 (siehe Abbildung 3). Bei immerhin knapp einem Viertel der Unternehmen wurden unautorisierte Datenzugriffe von aktuell Beschäftigten (13 Prozent), ehemaligen Mitarbeitern (6) sowie Partnern und Zulieferern (3) verzeichnet. Dass 28 Prozent der Unternehmen keine Antwort auf diese Frage geben wollten, lässt vermuten, dass die tatsächliche Zahl dieser internen Sicherheitsverletzungen sogar noch viel höher liegt. Maßnahmen der Benutzerverwaltung, die z.B. regeln, wie schnell die Konten von ausgeschiedenen Mitarbeitern gelöscht werden, können hier die Sicherheit erhöhen.

Abbildung 3: Gab es in Ihrem Unternehmen Fälle von unautorisiertem Zugriff auf Daten oder Datendiebstahl?



Quelle: Netegrity 2004, S.5

5.2.4 Vielfältige Abwehrmaßnahmen nötig

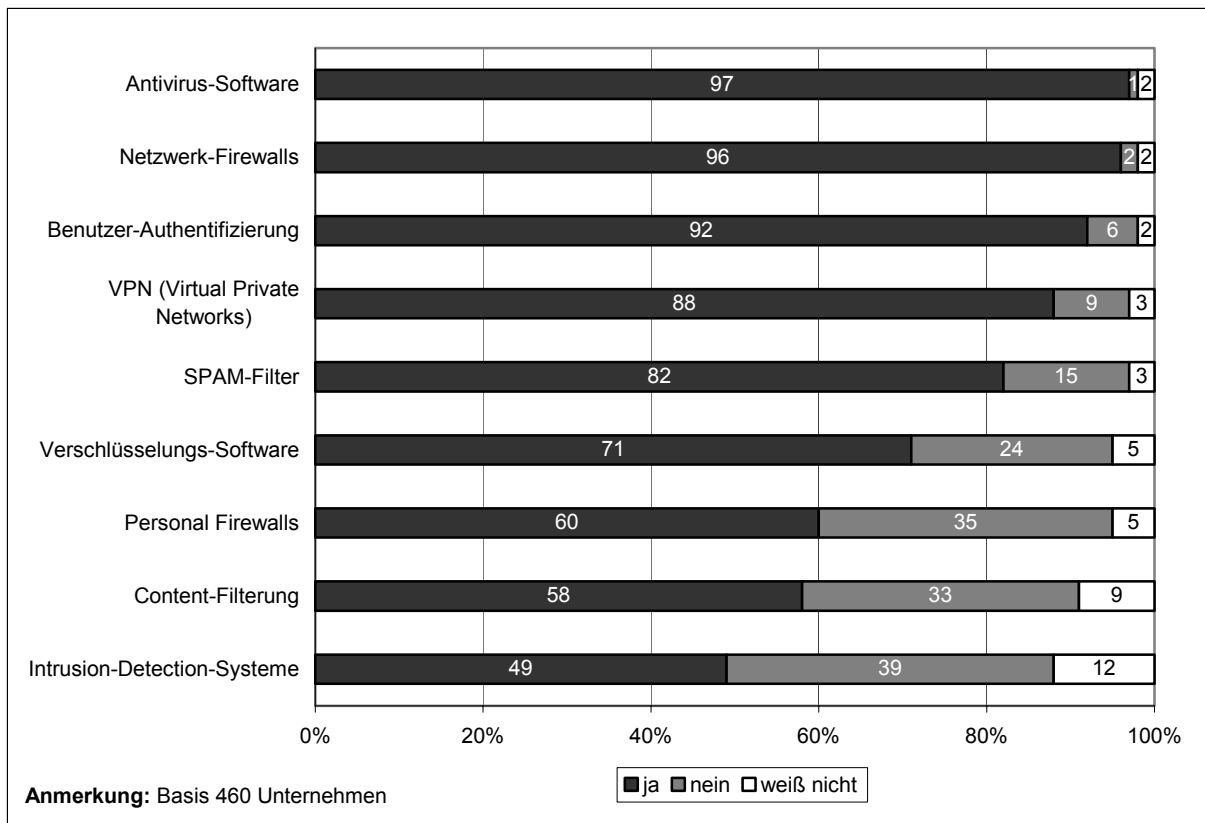
Bei der Vielzahl der möglichen Sicherheitsgefahren und der zunehmenden Häufigkeit ihres Auftretens ist es wichtig, genügend Abwehrmaßnahmen im IT-System der Unternehmen zu implementieren. Diese schließen neben technischen Maßnahmen auch organisatorische Schritte ein, wie z.B. die Schaffung eines Sicherheitsbewusstseins bei Mitarbeitern und Entscheidern sowie IT-Sicherheitsschulungen.

IT-Sicherheitsrichtlinien bilden die Basis einer umfassenden IT-Sicherheitsstrategie. Gemäß *TK-Studie* verfügten 2002 knapp drei Viertel der Unternehmen über solche Richtlinien. Eine branchenbezogene Auswertung verdeutlicht dabei große Unterschiede. Während im Bereich Finanzen/Versicherungswesen nahezu flächendeckend Sicherheitsrichtlinien vorliegen (94 Prozent), bejahten dies nur 57 Prozent der Unternehmen aus dem Baugewerbe. In gut der Hälfte der in 2002 befragten Unternehmen waren die Sicherheitsrichtlinien schriftlich fixiert. Für das Jahr 2004 verzeichnete die *Kes-Microsoft-Studie* bereits einen Anteil von insgesamt 60 Prozent mit schriftlich fixierten Richtlinien. Diese Zahlen berücksichtigen jedoch noch nicht die tatsächlichen Anstrengungen, die unternommen werden, um den Mitarbeitern diese Richtlinien auch nahe zu bringen. Die *TK-Studien* für die Jahre 2002 und 2003 verweisen hier auf Schwachstellen, da knapp ein Drittel der Mitarbeiter nicht mit den IT-Sicherheitsrichtlinien vertraut ist.

5.2.5 Einsatz von Sicherheitstechnologien nimmt zu

Verschiedene Sicherheitstechnologien kommen in den Unternehmen zum Einsatz, um sich vor den vielfältigen Gefahren zu schützen. Die *CAL-Studie* (siehe Abbildung 4) verzeichnet für das Jahr 2004 einen nahezu flächendeckenden Einsatz von *Anti-Virus-Software* (97 Prozent) und *Netzwerk-Firewalls* (96 Prozent) in den befragten Unternehmen. Angesichts der hohen Zahl von Unternehmen, die bereits von Malware betroffen waren und angesichts der möglichen Schadenshöhe, die unerlaubte Zugriffe von außen nach sich ziehen können, erweist sich die weite Verbreitung dieser Sicherheitsmaßnahmen als dringend notwendig.

Mit 92 Prozent gehört auch die *Benutzer-Authentifizierung* (z.B. durch Benutzername, Passwort) zu den Standard-Sicherheitsvorkehrungen. Über *Spam-Filter* verfügen laut *CAL-Studie* lediglich 82 Prozent der Unternehmen, was vor dem Hintergrund, dass fast jedes Unternehmen von Spam betroffen ist, niedrig erscheint. Möglicherweise sieht so mancher Unternehmer Spam eher als lästiges Übel denn als Gefahr an.

Abbildung 4: Welche sicherheitsrelevanten Tools sind in Ihrem Unternehmen im Einsatz?

Quelle: Computer Associates 2005, S. 14

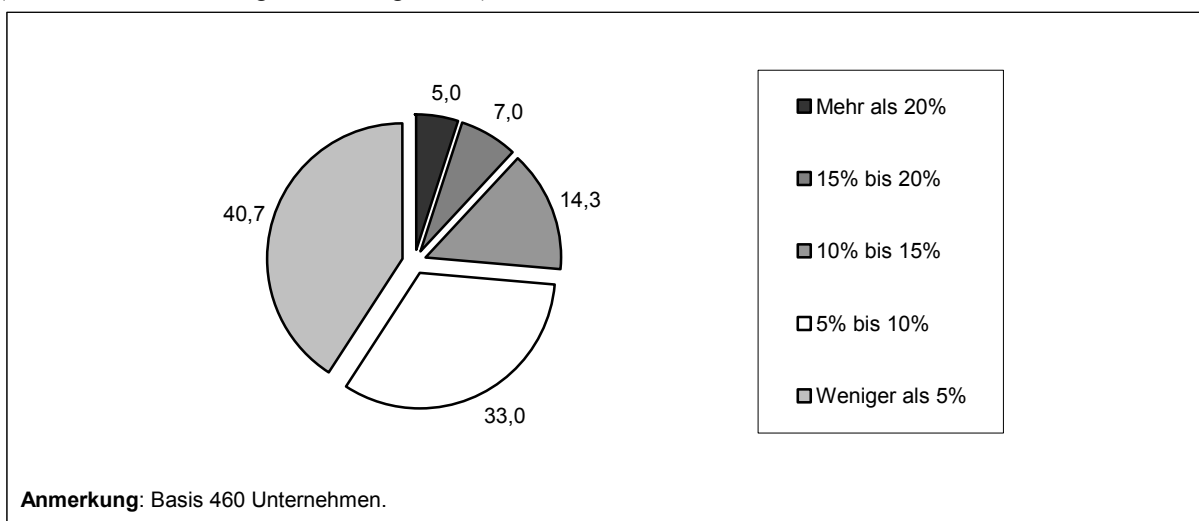
Die Verbreitung von *Personal Firewalls*, die z.B. auf den Laptops mobiler Mitarbeiter zum Einsatz kommen, ist mit 60 Prozent eher gering. *Intrusion-Detection-Systeme* dienen der Erkennung von Denial-of-Service-Angriffen und gehören 2004 bei der Hälfte der befragten Unternehmen zur Sicherheitsausstattung. Die genannten Zahlen der *CAL-Studie* für das Jahr 2004 verdeutlichen den zunehmenden Einsatz von IT-Sicherheitsmaßnahmen. So verzeichnet die *TK-Studie* für das Jahr 2002 in den Nutzeranteilen aller Sicherheitsmaßnahmen geringere Werte: 91 Prozent der Unternehmen nutzen Viren-Schutz-Programme, 83 Prozent haben Firewalls installiert. Lediglich in 27 Prozent der Unternehmen arbeiten in 2002 Intrusion Detection Systeme.

Anhand der *Kes-Studien* für die Jahre 2002 und 2004 wird darüber hinaus deutlich, dass sich das Ausmaß der Sicherheitsvorkehrungen zwischen Server, Clients und mobilen Endgeräten stark unterscheidet. Grundsätzlich weisen Serversysteme den höchsten Sicherheitsstandard auf. Hier ist der Umsetzungsgrad hinsichtlich Datensicherung (99 Prozent in 2004), Virenschutz (97 Prozent) und Firewalls (95 Prozent) mit Abstand am höchsten. Zudem wird im Server-Bereich besonderer Wert auf die physische Sicherheit gelegt. Lediglich die Authentifizierung der Benutzer erfolgt in allen drei Bereichen nahezu flächendeckend (Server: 98 Prozent in 2002, Clients: 97 Prozent, mobile Endgeräte: 95 Prozent).

5.2.6 Unternehmen planen Erhöhung der Investitionen in IT-Sicherheit

Im Jahre 2004 investierten fast alle Unternehmen in IT-Sicherheitslösungen (Netegrity-Studie: 98 Prozent). Der Anteil des IT-Budgets, der von den Unternehmen für IT-Sicherheit aufgewendet wurde, erreicht in den meisten Unternehmen (74 Prozent) eine Höhe von bis zu zehn Prozent. Dies zeigen sowohl die *TK-Studie* für 2002 als auch die *CAL-Studie* (siehe Abbildung 5) für das Jahr 2004. Letztere lässt zudem auf die wachsende Bedeutung des Themas IT-Sicherheit schließen: Obwohl die Gesamt-IT-Budgets in den vergangenen Jahren eher eingefroren oder sogar verringert wurden, gaben immerhin 45 Prozent der Unternehmen an, dass das IT-Sicherheitsbudget im Vergleich zum Vorjahr erhöht wurde. In 48 Prozent der Unternehmen ist es in etwa gleich geblieben.

Abbildung 5: Welcher Anteil des IT-Budgets wird für Sicherheit ausgegeben?
(Produkte, Dienstleistungen, Beratungen, etc.)



Quelle: Computer Associates 2005, S. 20.

Für das Jahr 2005 plant gemäß *CAL-Studie* mehr als ein Drittel der Unternehmen (35 Prozent) eine Erhöhung des IT-Sicherheitsbudgets. Gegenüber den Plänen für 2004 ist das ein Rückgang um zehn Prozentpunkte. Immerhin 57 Prozent wollen ihr IT-Sicherheitsbudget in 2005 unverändert lassen, lediglich acht Prozent planen eine Verringerung. Anzumerken ist jedoch, dass die Höhe der IT-Investitionen allein noch kein Gradmesser für die Wirksamkeit der eingesetzten Schutzmaßnahmen ist. Die Anschaffungskosten bestimmter Maßnahmen sind in vielen Fällen höher als die laufenden Kosten für die Folgejahre. Neben den Sachkosten erfordert beispielsweise die Einrichtung von Sicherheitsvorkehrungen mitunter einen hohen personellen Aufwand. Viele Unternehmen verzichten zudem auf eine Wirksamkeitskontrolle ihrer IT-Sicherheitsinvestitionen.

5.2.7 Hemmnisfaktoren einer umfassenden IT-Sicherheit

Ein zu knappes IT-Budget wird in vielen Studien als eines der Haupthemmnisse dafür angesehen, dass in Unternehmen nicht mehr für die IT-Sicherheit getan wird. Sowohl in der *TK-Studie* für das Jahr 2002 als auch in der *Kes-Microsoft-Studie* für das Jahr 2004 liegt der Anteil der Nennungen dieses Hemmnisfaktors bei etwa 60 Prozent. Als weitere wichtige Faktoren werden in diesem Zusammenhang mangelndes Sicherheitsbewusstsein bei Mitarbeitern und Management, fehlendes IT-Fachpersonal, Intransparenz von Kosten und Nutzen sowie fehlende integrierte Lösungen genannt.

6. Schlussbemerkungen

Die in diesem Artikel vorgestellten Studien zeigen, dass das Thema IT-Sicherheit durchaus im Bewusstsein von Unternehmensentscheidern eine Rolle spielt. Trotzdem sind die bisher eingesetzten Maßnahmen in vielen Fällen nicht ausreichend, um die vielfältigen internen wie externen Sicherheitsbedrohungen abwehren zu können. Vor allem in kleineren Unternehmen wird das Gefahrenpotential im Rahmen der IT-Sicherheitsbedrohungen tendenziell unterschätzt und die Gefahrenabwehr vernachlässigt. Die zunehmende Komplexität der Bedrohungen und das hohe Tempo der Veränderungen dürfen jedoch nicht zur Resignation führen, sondern erfordern umfangreiche, aufeinander abgestimmte Sicherheitsmaßnahmen, die in der Unternehmensstrategie fest verankert sind. Dies gilt insbesondere in Anbetracht der möglichen Schadenshöhe bei Eintreten eines Sicherheitsvorfalls.

Langfristig muss in den Unternehmen ein umfassendes Sicherheitsmanagement aufgebaut werden. Dies umfasst die laufende Analyse möglicher Gefahren und Risiken, den Einsatz entsprechender Schutzmaßnahmen, die Kontrolle der eingesetzten Mittel auf ihre Wirksamkeit sowie die Organisation von ständigen Updates und nötigen Neuanschaffungen im Rahmen der IT-Sicherheit. Von besonderer Bedeutung sind zudem die schriftliche Dokumentation der unternehmensinternen Sicherheitsrichtlinien und -konzepte sowie die Vermittlung der IT-Sicherheitsstrategie an die Mitarbeiter.

Unterstützt werden Unternehmen mittlerweile von einer Vielzahl an IT-Sicherheitsprodukten und -beratern. Eine Grundlage für deutsche Unternehmen stellt z.B. der „Leitfaden IT-Sicherheit“ des Bundesamts für Sicherheit in der Informationstechnik (BSI, 2004) dar. Er liefert einen kompakten und allgemeinverständlichen Überblick über die wichtigsten IT-Sicherheitsmaßnahmen, über gesetzliche Regelungen und mögliche Gefahren und gibt zahlreiche Handlungsempfehlungen.

7. Literatur

ASW (2004)

Anmerkungen zur Sicherheitslage der deutschen Wirtschaft 2003/2004. In http://www.asw-online.de/ASW_Sicherheitslage2003-04.pdf, zugegriffen am 04.05.2005

BSI (2004)

Leitfaden IT-Sicherheit, IT-Grundschutz kompakt. In <http://www.bsi.bund.de>, zugegriffen am 08.04.2005

BSI (2005)

Wie das Internet entstand. In http://www.bsi-fuer-buerger.de/internet/01_02.htm, zugegriffen am 04.05.2005

Computer Associates (2005)

Studie: Status IT-Security 2005. Komplexe Bedrohungen erfordern neue Ansätze für die IT-Sicherheit. In http://www.ca.com/de/products/etrust/security_studie_form.htm, zugegriffen am 29.04.2005

Eckert, Claudia (2004a)

IT-Sicherheit: Konzept – Verfahren – Protokolle. Oldenbourg Verlag, München

Eckert, Claudia (2004b)

IT-Sicherheit: Probleme, Lösungen und einige neue Herausforderungen. Thema Forschung 1/2004: IT-Sicherheit, S. 18-24.

Görtz, Horst (2004)

Die Geschichte der IT-Sicherheit – wie ich sie erlebte. Thema Forschung 1/2004: IT-Sicherheit, S. 28-32.

IHK-Köln (2004)

Hilfe im Kampf gegen den elektronischen Mail-Müll. In <http://www.ihk-koeln.de/Service/Presse/PresseinfosSepOkt2004/Spam.jsp>, zugegriffen am 04.05.2005

Kes (2002)

Lagebericht zur IT-Sicherheit: Kes-Microsoft Sicherheitsstudie 2002 (Teil I & II). In <http://www.kes.info/archiv/material/studie2002/>, zugegriffen am 08.04.2005

Kes (2004)

Von Geldmangel bis Mehrwert: Kes-Microsoft Sicherheitsstudie 2004. Sonderdruck. In <http://download.microsoft.com/download/a/8/8/a885d51f-6684-4f8a-af41-c87fd082242a/kes-Microsoft-Studie2004-Sonderdruck.pdf>, zugegriffen am 08.04.2005

Netegrity (2004)

Netegrity IT-Sicherheitsstudie 2004. In <http://www.ca.com/de/products/etrust/NetegrityStudie2004.pdf>, zugegriffen am 08.04.2005

NextiraOne (2004)

Störfälle bei der IT-Sicherheit nehmen zu. In <http://www.nextiraone.de/pres/presarch.htm>,
zugegriffen am 04.05.2005

Sopella, Robert (2005)

Daten an der Angel. Facts 1-2/2005, S. 54-55.

TimeKontor (2002)

Wie viel IT-Sicherheit braucht ein Unternehmen? In http://venture-route.com/TKSpace/digital_TrustSurvey2002.pdf, zugegriffen am 08.04.2005

TimeKontor (2003)

Wie viel IT-Sicherheit braucht ein Unternehmen? Entscheiderbefragung 2003 –
Management Summary. In <http://venture-route.com/TKSpace/Managementsummary2003.pdf>, zugegriffen am 13.04.2005

ZEW (2005)

IKT-Report. Zentrum für Europäische Wirtschaftsforschung GmbH, Mannheim

Anhang

Über die Autoren

Dr. Irene Bertschek studierte Volkswirtschaftslehre an der Universität Mannheim (Diplom) und der Université Catholique de Louvain, Louvain-la-Neuve, Belgien (Master of Arts) mit den Schwerpunkten Ökonometrie und Industrieökonomik. Im Rahmen des European Doctoral Program promovierte sie an der Université Catholique de Louvain. Seit 1999 ist sie am Zentrum für Europäische Wirtschaftsforschung (ZEW) in Mannheim beschäftigt und leitet dort seit 2001 die Forschungsgruppe Informations- und Kommunikationstechnologien.

Kontakt: bertschek@zew.de

Dr. Thomas Döbler studierte Soziologie, Psychologie und Volkswirtschaftslehre in München. Promotion zum Dr. oec. an der Universität Hohenheim; wissenschaftlicher Assistent zunächst am Fachgebiet Unternehmensführung, Organisation und Personal, dann am Fachgebiet Kommunikationswissenschaft und Sozialforschung, Universität Hohenheim. Ab 1998 Studienleiter an der Forschungsstelle für Medienwirtschaft und Kommunikationsforschung in Hohenheim. Seit 2005 Leiter IT- und Medienforschung, MFG Stiftung Baden-Württemberg.

Kontakt: doebler@mfg.de

Jörg Ohnemus studierte Volkswirtschaftslehre an der Universität Mannheim mit den Schwerpunkten Entwicklungsökonomik, Geld- und Währungspolitik, Finanzierung sowie Ökonometrie. Seit November 2004 ist er wissenschaftlicher Mitarbeiter in der Forschungsgruppe Informations- und Kommunikationstechnologien am Zentrum für Europäische Wirtschaftsforschung (ZEW), Mannheim.

Kontakt: ohnemus@zew.de

Katrin Schleife studierte Volkswirtschaftslehre an der Humboldt-Universität zu Berlin und an der Universität Zürich mit den Studienschwerpunkten Wirtschafts- und Computergestützte Statistik sowie Arbeitsmarktökonomik. Sie absolvierte ein einjähriges Praktikum am Institut für angewandte Demografie (IFAD) in Berlin. Seit März 2003 ist sie wissenschaftliche Mitarbeiterin in der Forschungsgruppe Informations- und Kommunikationstechnologien am Zentrum für Europäische Wirtschaftsforschung (ZEW), Mannheim.

Kontakt: schleife@zew.de

Oliver Schmid studierte Wirtschaftsinformatik an der Universität Mannheim. Seit Dezember 2002 ist er als wissenschaftlicher Mitarbeiter im Fachgebiet Empirische Wirtschaftsforschung und Mikroökonometrie der Technischen Universität Darmstadt tätig.

Kontakt: schmid@vwl.tu-darmstadt.de

Über das Projekt FAZIT

FAZIT erforscht Treiber für neue Märkte für IKT

Innovationen und neue Märkte – das sind wesentliche Faktoren im Wettbewerb der Regionen, um den Erhalt und die Schaffung von Arbeitsplätzen zu sichern. So steht im Mittelpunkt des Projekts FAZIT die Erforschung von neuen Märkten für Informations- und Kommunikationstechnologien (IKT) bis ins Jahr 2020. Durch regelmäßige Unternehmensbefragungen werden der Bedarf und die Einsatzmöglichkeiten für innovative Informations- und Medientechnologien in den Anbieter- wie auch in ausgewählten Anwenderbranchen in Baden-Württemberg erfasst. Die hier gewonnenen Daten und Ergebnisse fließen in die Zukunftsforschung ein. Hier werden in den drei Leitthemen „Mensch und Gesellschaft“, „Technologien und Prozesse“ und „Einsatzfelder und Branchen“ Thesen für die Befragung des externen Expertennetzwerks, bestehend aus führenden Vordenkern aus Wirtschaft, Wissenschaft, Politik und Gesellschaft generiert. Im Verlauf des Forschungsprozesses werden relevante gesellschaftliche, branchenspezifische und technologische Umbrüche sowie Treiber für Innovationen und Arbeitsplätze identifiziert. Grundlegende Einsichten und Hinweise auf neue Märkte für IKT werden gewonnen, neue Marktchancen aufgezeigt und durch neue Forschungsthemen Orientierung für Wissenschaft und Wirtschaft gleichermaßen geschaffen.

Gemeinnütziges, im Rahmen der Zukunftsoffensive III gefördertes Forschungsprojekt

FAZIT ist ein im Rahmen der Zukunftsoffensive III vom Land Baden-Württemberg gefördertes gemeinnütziges *Forschungsprojekt für aktuelle und zukunftsorientierte Informations- und Medientechnologien und deren Nutzung in Baden-Württemberg*. Projektträger ist die MFG Stiftung Baden-Württemberg, Stuttgart. Partner sind das Zentrum für Europäische Wirtschaftsforschung (ZEW), Mannheim, und das Fraunhofer-Institut für System- und Innovationsforschung (Fraunhofer ISI), Karlsruhe.

Mehr Informationen im Internet unter www.fazit-forschung.de

Über die Partnerinstitutionen

MFG Stiftung Baden-Württemberg

Die MFG Stiftung realisiert gemeinnützige Projekte in den Bereichen IT, Medien und Film. Im Mittelpunkt stehen dabei Forschung und Entwicklung, Kunst, Kreativität, Kultur sowie Aus- und Weiterbildung. Die MFG Stiftung führt insbesondere verschiedene Maßnahmen zur Vernetzung von Akteuren im Bildungs- und Forschungsbereich durch, wie z. B. durch Veranstaltungen (Kongresse, Workshops) sowie Fort- und Weiterbildungsmaßnahmen, und fördert innovative Projekte und Forschungsaktivitäten durch Studien, Stipendienprogramme und Wettbewerbe.

Internet: www.mfg.de/stiftung

Fraunhofer-Institut System- und Innovationsforschung

Die Abteilung "Regionen und Marktdynamik" des Fraunhofer-Instituts System- und Innovationsforschung analysiert die Wechselwirkungen der Elemente regionaler Innovationssysteme und die Entwicklung neuer Märkte für Produkte und Dienstleistungen. Dabei werden regionale Innovationssysteme betrachtet, aber auch die Gründung und Entwicklung kleiner und mittelständischer Unternehmen analysiert. Der wesentliche Fokus und Anwendungsbezug der Arbeiten liegt im Bereich der Informations- und Kommunikationswirtschaft.

Internet: www.isi.fhg.de

Zentrum für Europäische Wirtschaftsforschung

Das ZEW arbeitet auf dem Gebiet der anwendungsbezogenen empirischen Wirtschaftsforschung. Methodisch sind die Arbeiten primär mikroökonomisch und mikroökonomisch ausgerichtet. Die Forschungsgruppe Informations- und Kommunikationstechnologien (IKT) am ZEW befasst sich mit den Entwicklungen und den Auswirkungen der zunehmenden Verbreitung von IKT, wobei der Fokus insbesondere bei industrie- und arbeitsmarktökonomischen Fragestellungen liegt. Hierzu gehören beispielsweise die Auswirkungen der IKT-Nutzung auf Produktivität, Innovation, Unternehmensorganisation und Unternehmenswachstum sowie auf die Anforderungen an die Qualifikation der Beschäftigten.

Internet: www.zew.de

■ PROJEKTRÄGER



■ PARTNER

