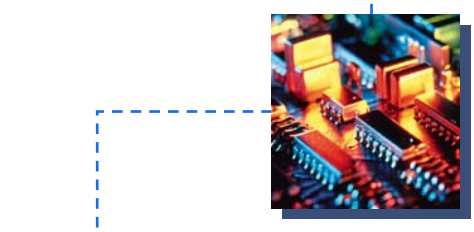
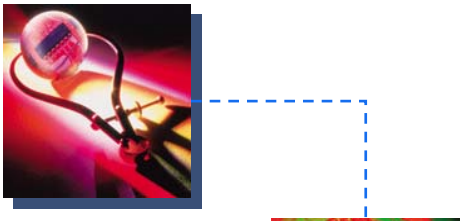
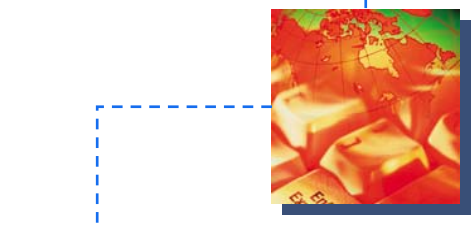
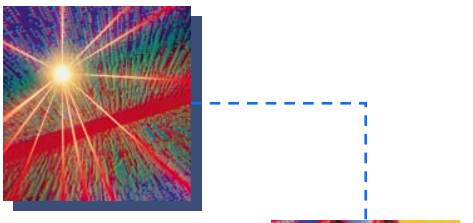
IT-Security im Jahr 2003

(Deutschland)









Eine Analyse der

META Group Deutschland GmbH

http://www.metagroup.de

Copyright

Dieser Untersuchungsbericht wurde von der META Group Deutschland GmbH erstellt. Die darin enthaltenen Daten und Informationen wurden in Zusammenarbeit mit der Firma TechConsult GmbH gewissenhaft und mit größtmöglicher Sorgfalt nach marküblichen Methoden und Grundsätzen ermittelt. Für ihre Vollständigkeit und Richtigkeit kann jedoch keine Garantie übernommen werden.

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Management Summary

1.1 Status und Trends bei Anwendern

Spätestens seit der Häufung von sicherheitsrelevanten Zwischenfällen in der Öffentlichkeit und den Ereignissen vom 11. September 2001 ist IT-Sicherheit in aller Munde. Die Aussagen der im Rahmen dieser Studie befragten deutschen Anwenderunternehmen sprechen für sich: 76 Prozent berichten von Schäden, die in den vergangenen zwei Jahren im eigenen oder bei ihnen bekannten Unternehmen entstanden waren. Dabei wurden vor allem Wiederherstellungskosten oder Umsatzverluste nach einem Systemausfall sowie der Verlust von Daten verursacht. Ebenfalls stark präsent sind Klagen über den unautorisierten Zugriff auf Daten sowie Missbrauch oder Manipulation von Daten.

Aus Sicht der befragten Unternehmen ist die Gefahr durch Virenbefall und „bösartigen" Code als eindeutig höchstes Sicherheitsrisiko zu bewerten. Weitere Gefahrenquellen sind nach Einschätzung der Anwenderorganisationen das unautorisierte Eindringen Fremder ins Unternehmensnetzwerk, insbesondere in Gestalt von Hackern ohne wirtschaftliche Interessen. Befürchtet werden außerdem die Manipulation oder Offenlegung von Transaktionen im Web und über Email sowie der Missbrauch von Benutzerrechten durch eigene Mitarbeiter („Innentäter").

Diese Ergebnisse deuten prinzipiell auf eine hohe Sensibilisierung der deutschen Unternehmen in Hinsicht auf einzelne Sicherheitsthemen hin. Der Weg vom Lippenbekenntnis hin zur Ergreifung konkreter Sicherheitsmaßnahmen ist jedoch steinig. Trotz leicht erhöhten Sicherheitsbewusstseins auf Unternehmensebene vermisst die META Group bei den Anwenderorganisationen einen ganzheitlichen Blick auf die IT-Sicherheit. Die vorliegende Untersuchung zeigt, dass IT-Security in Deutschland vorwiegend als technisches und produktorientiertes Thema begriffen wird. Bei den organisatorischen Maßnahmen gibt es hingegen noch hohen Nachholbedarf.

Nur 25 Prozent der im Rahmen der vorliegenden Studie befragten Unternehmen verfügten Anfang 2003 über eine dedizierte IT-Sicherheitsorganisation im Unternehmen. Selbst große Unternehmen mit mindestens 1.000 Mitarbeitern können in nur 53 Prozent der Fälle ein solches IT-Sicherheits-Team vorweisen. Damit liegen sie noch weit von den 75 Prozent der großen Global-2000-Unternehmen entfernt, die nach Schätzungen der META Group bereits Ende 2001 eine Security-Organisation hatten. Auch bei der personellen Ausstattung der Unternehmen im Bereich der IT-Sicherheit gibt es bei den Unternehmen erheblichen Nachholbedarf.

Ähnlich sieht es hinsichtlich der Security Policy als Grundlage für IT-Sicherheits-Infrastrukturen aus: Während nur 48 Prozent der deutschen Unternehmen eine schriftlich fixierte Security Policy haben, sind 37 Prozent hier bislang untätig geblieben und haben auch keine entsprechende Planung für die Zukunft.

Dies hat unter anderem zur Folge, dass sich die „Security-Awareness" bei den Anwendern innerhalb der einzelnen Unternehmen nicht ausreichend entwickeln kann. Die vorliegende Untersuchung zeigt, dass die deutschen Unternehmen gerade das geringe Sicherheitsbewusstsein der Anwender im

Unternehmen als derzeit größtes Hemmnis für die Durchsetzung eines hohen Sicherheitsniveaus einschätzen. Außerdem fühlen sich die Verantwortlichen durch geringe Security-Budgets und die schlechte Messbarkeit von Risiken beziehungsweise des Return on Investment (ROI) behindert, gefolgt vom klassischen Thema „Personalmangel". Als weniger ausschlaggebend werden hingegen unreife Sicherheitstechnologien, unsichere Server-Betriebssysteme und die gegebenenfalls schwierige Integration von unterschiedlichen Produkten erachtet. Damit wird deutlich, dass die wahren Hemmnisse aus Sicht der Anwenderunternehmen nicht in erster Linie im technischen Bereich liegen, sondern vielmehr im Umfeld von Ressourcen, Prozessen und „weichen" Faktoren.

Bei der Entscheidungsfindung verfolgen die Anwenderunternehmen in der Regel einen reaktiven Ansatz. IT-Security wird heute seltener als „Enabler" für neue Angebote oder die Erschließung neuer Märkte gesehen. Als wichtigste Entscheidungsgrundlage für die Höhe der IT-Security-Investitionen nennen die befragten Anwenderunternehmen vielmehr rechtliche Rahmenbedingungen, dicht gefolgt von Erfahrungswerten aus vergangenen Sicherheitsproblemen im Unternehmen. Außerdem orientieren sich die Unternehmen an den Anforderungen der Partner und Kunden an IT-Sicherheit. ROI-Analysen und Risk Assessment werden primär durch Unternehmen mit mindestens 500 Mitarbeitern als Entscheidungsgrundlage herangezogen. Der hohe Stellenwert rechtlicher Rahmenbedingungen wie etwa Basel II, KonTraG, das Bundesdatenschutzgesetz und EU-Direktiven wird jedoch nach Meinung der META Group mittelfristig dazu führen, dass auch die Bedeutung des Risk Assessments steigen wird. Dieses dürfte künftig eine wichtige Komponente für die Umsetzung etwa von Basel II bilden.

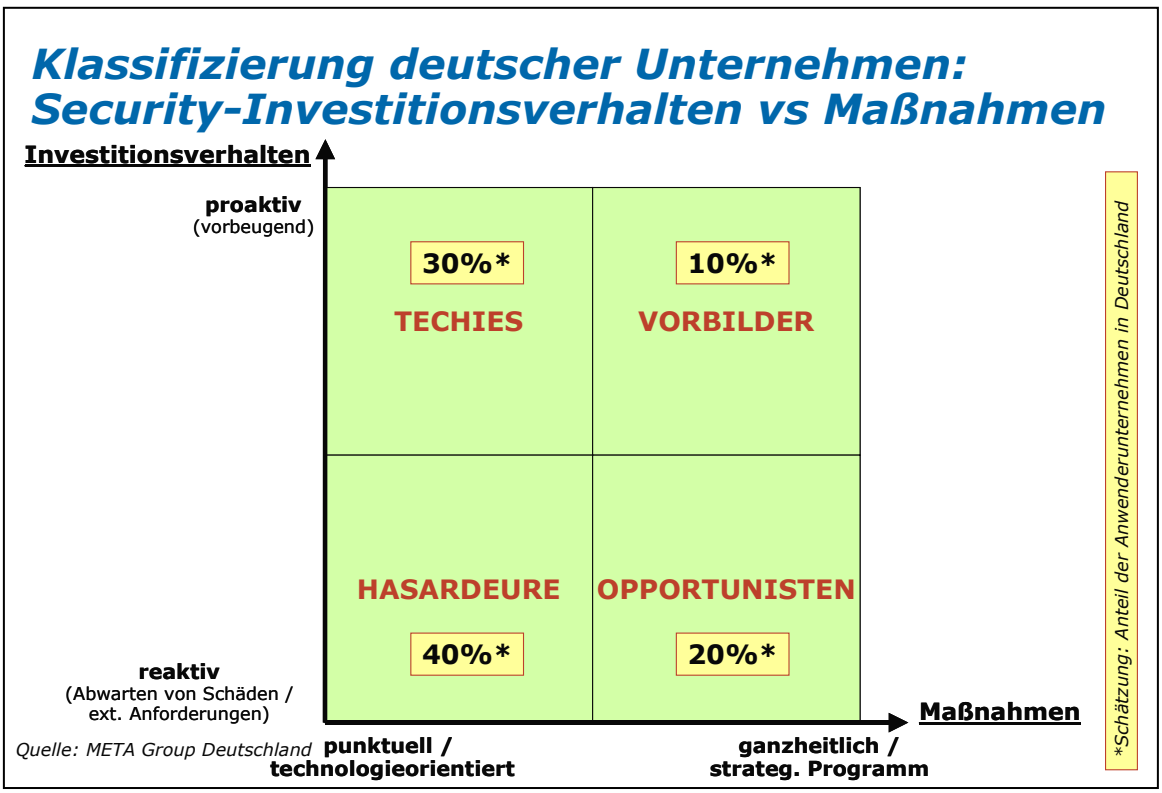


Abbildung 1: Klassifizierung deutscher Unternehmen nach Investitionsverhalten und Maßnahmen

Nach Schätzungen der META Group sind bei rund 70 Prozent der deutschen Unternehmen die Security-Maßnahmen als ausgesprochen punktuell und technologieorientiert zu betrachten (siehe Abbildung 1). Davon sind 30 Prozent so genannte “Techies”, die zwar durchaus vorbeugend, aber primär technologieorientiert investieren,. Gar 40 Prozent sind als “Hasardeure” zu bewerten, die aufgrund externer Anforderungen punktuelle Maßnahmen einleiten, aber gleichzeitig auch sicherheitsrelevante Zwischenfälle in Kauf nehmen, bevor umfassendere Maßnahmen eingeleitet werden. Die restlichen 30 Prozent der Anwenderunternehmen verfügen über Ansätze eines ganzheitlichen strategischen Programms für Informationssicherheit. Nur etwa ein Drittel dieser Unternehmen geht dabei aber proaktiv vor und führt beispielsweise umfassende Risikoanalysen im Unternehmen durch.

Die monetäre Bewertung des Nutzens von IT-Sicherheit ist zumeist schwierig. Für viele Bereiche der IT-Security ist der Return on Investment (ROI) schwer quantitativ nachweisbar. Nach Einschätzung der META Group besteht hier allzu leicht die Gefahr, das eigene Gewissen zu beruhigen, indem auf Basis unvollständiger und ungenauer Daten exakte ROI-Werte berechnet werden. Die META Group rät Anwenderunternehmen vielmehr zu einer pragmatischen Vorgehensweise, die den ROI im Sinne des „Nutzens“ begreift. Dieser sollte als eine Kombination aus quantifizierbarem Nutzen (Einsparungen, Prozessverbesserung), quantifizierbarer Risikominimierung (sofern zuvor eine Risikoanalyse erfolgt ist) und eher subjektiv wahrgenommenen Verbesserungen der Informationssicherheit betrachtet werden. Damit lassen sich nicht zuletzt auch Sicherheitsprioritäten und –anforderungen in einzelnen Unternehmensbereichen ausloten.

Gleichwohl macht es für Anbieter von Lösungen im Einzelfall Sinn, den ROI dem Kunden gegenüber zu kommunizieren. Die ROI-Analyse sollte aber glaubwürdig und für den Kunden leicht nachvollziehbar sein; die ROI-Argumentation allein reicht für die Kaufentscheidung selten aus und sollte daher primär als zusätzliches Verkaufsargument des Anbieters dienen.

Angesichts der Entscheidungsgrundlagen bei Investitionen in IT-Sicherheit sowie den wahrgenommenen Hemmfaktoren und Sicherheits-Risiken stellt sich die Frage, ob das Sicherheitsbewusstsein in deutschen Unternehmen generell gestiegen ist. Nach Meinung der META Group muss hierzu eine differenzierte Betrachtungsweise vorgenommen werden. Da sich die Unternehmen bei Investitionsentscheidungen stark an bestehenden Erfahrungen mit Schäden orientieren, liegt hinsichtlich der “Mainstream”-Themen (z.B. Viren) heute bereits eine hohe Sensibilisierung vor. Bei neueren Themen wie etwa der Sicherheit von Web Services oder mobilen Systemen ist die “Drohkulisse” jedoch noch nicht so stark durch entsprechende Erfahrungswerte - im Sinne von nachweisbaren Schäden - untermauert. Ähnliches gilt für organisatorische Lücken, deren Auswirkungen nur indirekt nachvollziehbar sind. Zwar wird etwa das mangelnde Sicherheitsbewusstsein der unternehmensinternen Anwender als Hemmnis erkannt, Gegenmaßnahmen werden aber nur in unzureichendem Maß ergriffen. Dennoch stellen dortige Sicherheitslücken eine erhebliche Gefahr für die Anwenderunternehmen dar. Damit werden auch in Zukunft Awareness-Kampagnen auf der Agenda der Anbieter von Lösungen und Dienstleistungen stehen müssen.

1.2 Status und Trends bei Anbietern

1.2.1 Lösungen

Die Anbieterlandschaft im Bereich IT-Security ist nach wie vor sehr fragmentiert. Eine Kategorisierung der Anbieter ist sowohl nach Themen und Technologien als auch nach der Strategie beziehungsweise dem Kerngeschäft des Anbieters möglich. So positionieren sich etwa Anbieter von Punktlösungen in der Regel als „Technologietreiber“ und stehen vor der Herausforderung, den Innovationsvorsprung in ihrem Marktsegment so lange wie möglich zu halten. Anbieter von kompletten Security-Suites wiederum nutzen ihre breite installierte Basis und ihr Branding aktiv für Neugeschäft. Sie sind nicht immer in allen Bereichen auf Anhieb technologieführend, adaptieren aber oftmals neue Technologien durch Zukauf von kleineren Anbietern. Systems-Management-Anbieter konzentrieren sich typischerweise auf Security-Management, sind aber teilweise auch in anderen Security-Marktsegmenten aktiv. Für sie stellen IT-Sicherheits-Funktionalitäten sowohl eine neue Umsatzquelle dar als auch ein Mittel zur Kundenbindung und Differenzierung gegenüber Mitbewerbern. Ähnliches gilt für die großen Anbieter von Netzwerktechnologien. Kundenbindung spielt auch für die Systemhersteller beziehungsweise Anbieter von Plattformen (Hardware, Betriebsumgebungen) eine wesentliche Rolle. Die Bereitstellung sicherer und verlässlicher Produkte steht hier im Vordergrund - der Umsatz mit IT-Sicherheit fällt bei diesen Anbietern weniger stark ins Gewicht als der Gewinn an Vertrauen bei der Kundschaft.

So unterschiedlich die Positionierungen der einzelnen Anbieter sein mögen – die Erfolgsaussichten für den einzelnen Anbieter hängen maßgeblich davon ab, wie konsequent er seine Strategie verfolgt und wie rasch er sein Portfolio an neue Herausforderungen anpasst. Schließlich durchlebt die IT-Sicherheit als Querschnittsthema einen permanenten Wandel, angetrieben durch ständig neue Anforderungen aus dem IT- und Business-Umfeld. Die Konsolidierung von Anbieterlandschaften bleibt zwar dabei nicht aus; sie erfolgt in der Regel aber nur in einzelnen Marktsegmenten – insbesondere dann, wenn die Pionier- und „Early-Adopter“-Phase im betreffenden Marktsegment vorüber ist und die breite Wachstumsphase beginnt.

Ob nun „Best-of-Breed“-Lösungen oder schlüsselfertige „Out-of-the-Box“-Lösungen bevorzugt werden, dürfte von den jeweiligen situationsbezogenen Anforderungen des Unternehmens abhängen. Höchste Priorität bei der Auswahl von Produkten genießen bei den Anwenderunternehmen die Flexibilität der Lösung, Service und Support, die Zukunftssicherheit des Anbieters sowie nicht zuletzt preisliche Aspekte. Best-of-Breed-Lösungen mögen gegebenenfalls skalierbarer und flexibler hinsichtlich der Einbindung in heterogene IT-Infrastrukturen sein und mehr Funktionalität bieten, dafür punkten schlüsselfertige Lösungen aus einer Hand oftmals beim Preis. Out-of-the-Box-Lösungen sind daher besonders für den Mittelstand interessant.

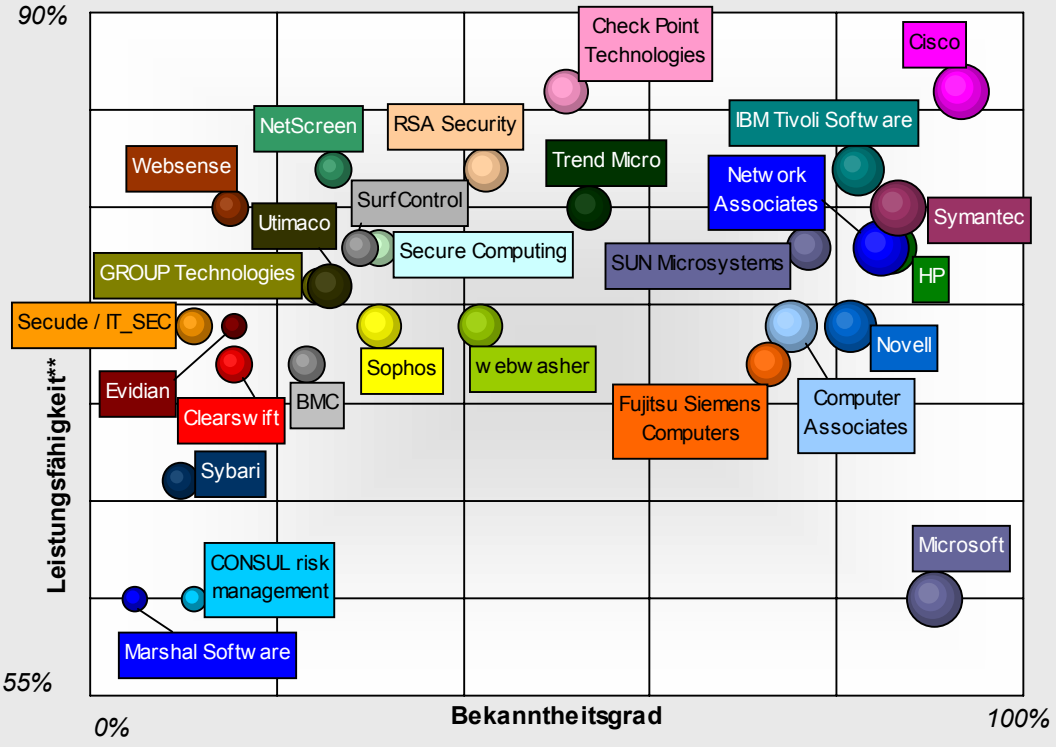
Wenn es um IT-Security-Produkte geht, fällt deutschen Anwenderunternehmen zuerst Symantec ein. Zu den fünf im Rahmen der vorliegenden Studie am häufigsten genannten Anbietern gehören ferner Network Associates / McAfee, Cisco, Check Point und Trend Micro. Dies zeigt die Untersuchung des ungestützten (das heißt ohne Vorgabe einer festen Anbieterliste ermittelten) Bekanntheitsgrades von

Security-Produktanbietern durch die META Group. Damit wird gleichzeitig allzu deutlich, dass die Unternehmen beim Thema IT-Sicherheit auf technologischer Ebene primär an Virenschutz und Netzwerksicherheit (v.a. Firewalls und VPNs) denken.

Bei der Bewertung der Leistungsfähigkeit ausgewählter Produktanbieter durch deutsche Anwenderunternehmen ergibt sich eine geringe Streuung der Werte – die Leistungsfähigkeit wird bei den meisten Anbietern zwischen „2“ (gut) und „2,5“ („gut bis befriedigend“) eingeschätzt (vergleiche Abbildung 2). Kein Anbieter schneidet „schlecht“ ab. In der Tat sind die Anwenderunternehmen in Bezug auf die Auswahlkriterien einigermaßen zufrieden mit den Anbietern. Kritische Punkte bleiben aber die Flexibilität der gebotenen Lösungen, die Service- und Support-Qualität und die Zukunftssicherheit der Anbieter: Hier hinkt der Zufriedenheitsgrad der Kunden hinter den hochgesteckten Erwartungen hinterher.

Bekanntheitsgrad und Leistungsfähigkeit ausgewählter Anbieter von Security-Lösungen*

*- Perception Survey Chart / Anwendermeinungsbild*** -*



Quelle: META Group Deutschland

Basis: 208 Unternehmen

**Die Größe der Kreise entspricht der Anzahl der Bewertungen zur Leistungsfähigkeit.*
***Transformierte Skala (100% entspricht sehr gut = 1 und 20% entspricht sehr schlecht = 5)*
****Die von der META Group getroffene Auswahl und Positionierung der Anbieterunternehmen reflektiert die Recherche der META Group durch Stichproben von Einschätzungen Dritter. Die Ergebnisse geben daher keinen Aufschluss über die tatsächliche Leistungsfähigkeit und/oder die tatsächliche Bekanntheit im Gesamtmarkt, weder absolut noch relativ zueinander.*

Abbildung 2: Bekanntheitsgrad und Leistungsfähigkeit ausgewählter Anbieter von Sicherheitslösungen

1.2.2 Dienstleistungen

IT-Security ist heute nicht mehr eine reine Domäne großer oder spezialisierter IT-Dienstleister, sondern wird aus vielen Service-Segmenten heraus als „Querschnittsthema“ oder „Enabler“ adressiert. So haben mittlerweile die meisten größeren Beratungsunternehmen und System-integratoren entsprechende Angebote im Portfolio. Nicht immer fallen die dabei realisierten Umsätze mit IT-Sicherheit ins Gewicht – dennoch ist es auch für kleine Dienstleister wichtig, den Sicherheits-anforderungen der Kunden nachzukommen und damit gleichzeitig für mehr Kundenbindung zu sorgen. Ähnliche Beweggründe haben Internet Service Provider (ISPs), die sich aber fast ausschließlich auf Security im Betrieb und Management der IT-Infrastrukturen (vor allem Netzwerke: VPN, Firewalls, IDS) konzentrieren.

Bei dedizierten Security-Dienstleistern sieht der Sachverhalt etwas anders aus. Diese konzentrieren sich in der Regel auf bestimmte Sicherheits-Themen oder Phasen im PLAN-BUILD-RUN-Zyklus und positionieren sich dort als Spezialisten. Der Know-how-Vorsprung in spezifischen Bereichen ist unabdingbar für den Erfolg dieser Anbieter.

Dedizierte Trust Center stellen eine Sonderkategorie dar. Diese Anbieter übernehmen für den Kunden den Betrieb von Trust Centern beziehungsweise einzelnen Funktionen wie die Ausgabe von digitalen Zertifikaten, die Registrierung neuer Nutzer oder Verzeichnisdienste. Um kommerzielle Trust Center ist es seit dem Ende des PKI-„Hype“ und dem Rückzug der Deutsche Post Signtrust stiller geworden. Die Zukunft der Trust Center wird maßgeblich davon abhängen, ob es ihnen gelingt, eine kritische Größe zu erreichen und sich in erfolgsversprechenden Marktnischen oder Branchen zu positionieren.

Ein Segment, an das manche IT-Dienstleister derzeit große Erwartungen hegen, sind Managed Security Services (MSS). Dedizierte Managed Security Service Provider (MSSPs), ISPs, System-integratoren, dedizierte Sicherheitsdienstleister sowie Produktanbieter adressieren zunehmend diesen Markt. Nach Beobachtungen der META Group steht die Vielzahl der Angebote derzeit in keinem Verhältnis zur Nachfrage der Kunden. Zwar könnten MSS angesichts des Mangels an qualifizierten Fachkräften auf der Anwenderseite Abhilfe für viele Probleme im Management von Sicherheits-infrastrukturen schaffen – nicht zuletzt im Mittelstand. Trotz der zunehmenden Resonanz auf Managed Firewall und VPN Services sind die geringe Sensibilisierung der Anwender für das Thema sowie teilweise erhebliche Qualitätsunterschiede bei den Angeboten der einzelnen Managed Service Provider derzeit jedoch noch problematisch. Von einer Konsolidierung des Marktes ist daher auszu-gehen. Die überlebenden MSSPs werden jedoch gestärkt aus der Konsolidierungsphase hervor-gehen.

Ein strittiges Thema ist die Bedeutung der Herstellerneutralität. Das Partnergeschäft spielt für viele im IT-Sicherheits-Umfeld aktiven Dienstleister eine tragende Rolle. Nicht zuletzt die Produktanbieter selbst bieten oftmals neben Support und Wartung auch produktorientierte Beratungs- und Trainings-leistungen – in einzelnen Fällen sogar Managed Security Services auf Basis ihrer eigenen Lösungen. Die befragten Anwenderunternehmen sehen die Herstellerneutralität jedoch vordergründig als ein

wichtiges Auswahlkriterium für Security-Services an. Vor allem aber legen sie großen Wert auf technologisches Spezialisten-Know-how sowie auf die Qualität von Service und Support. Weitere wichtige Auswahlkriterien sind die Betreuung des Kunden über den gesamten Service-Zyklus („PLAN-BUILD-RUN"), die Vertrauenswürdigkeit und das Image des Dienstleisters. Gleichzeitig ist auch technologisches Generalisten-Know-how beim Dienstleister gefordert, wobei der Anbieter nach Meinung der Anwender zu günstigen Preisen agieren sollte.

Die Unternehmen erweisen sich damit als sehr anspruchsvoll. Nach Meinung der META Group hängt der „Kriterien-Mix" bei der Anbieterauswahl stark von den spezifischen Anforderungen beim Kunden oder im Projekt ab. So dürfte etwa die Herstellerneutralität insbesondere in frühen Phasen des Entscheidungsprozesses beim Anwenderunternehmen relevant sein. Ist aber die Produktauswahl einmal vollzogen, liegt das Augenmerk vor allem auf einer sauberen Implementierung und Integration.

In der Tat ist das Security-Service-Thema in Deutschland immer noch eng verknüpft mit Produkten. Wenn es um IT-Sicherheits-Dienstleistungen geht, nennen die im Rahmen dieser Studie befragten Anwender am häufigsten den Lösungsanbieter Symantec - noch vor IBM Global Services, Siemens, Secunet, T-Systems und dem TÜV. Dies ist auch ein Zeichen dafür, wie wichtig den Anwender-unternehmen heute Support- und weitere produktorientierte Dienstleistungen sind.

Dennoch werden Sicherheitsaspekte jenseits der bloßen Technologie zunehmend Bestandteil der Angebote der Sicherheitsdienstleister. Hierzu gehören etwa die Unterstützung bei der Aufstellung von Security Policies, Risikoanalysen und Sicherheits-Audits. Ausschlaggebend ist unter anderem, dass sich der Preisdruck insbesondere bei standardisierten Services wie beispielsweise im Netzwerk-bereich erhöht hat. Außerdem haben deutsche Anwenderunternehmen erheblichen Nachholbedarf bei der Umsetzung einer ganzheitlichen Sicherheitsstrategie, die auch organisatorische Maßnahmen einschließt. Die Akzeptanz der Angebote rund um organisatorische IT-Sicherheit variiert bei den Anwenderunternehmen nach Einschätzung der META Group allerdings erheblich – abhängig vom Sicherheitsbewusstsein der jeweiligen Verantwortlichen und von den vorhandenen Budgets. Leider belassen es Unternehmen mit „reaktivem" Investitionsverhalten für IT-Security zu oft bei punktuellen, technologisch orientierten Maßnahmen. Hier müssen die Dienstleister noch große Anstrengungen zur Sensibilisierung der Anwenderunternehmen unternehmen.

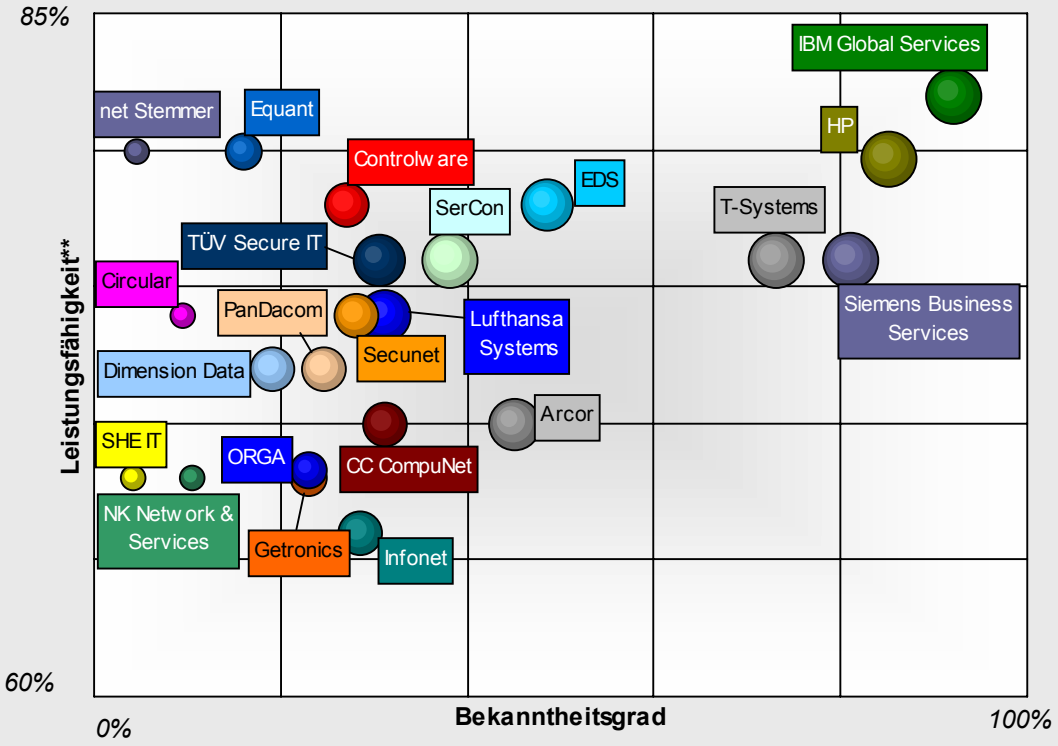
Dies gilt vor allem auch für den Mittelstand. Dieser wird zunehmend als neue Zielgruppe auch größerer Dienstleister entdeckt. Insbesondere im investitionsscheuen klassischen Mittelstand (Unternehmen unter 500 Mitarbeiter) wird es für die Dienstleister aufgrund der jeweils geringen Budgets nicht einfach sein, profitabel operieren können. Diese Zielgruppe ist daher mit geeigneten Lösungspaketen zu adressieren.

Bei der Bewertung der Leistungsfähigkeit ausgewählter Dienstleister durch deutsche Anwender-unternehmen ergibt sich eine geringe Streuung der Werte – die Leistungsfähigkeit wird bei den meisten Dienstleistern als „gut" bis „befriedigend" eingeschätzt (siehe Abbildung 3). In der Tat sind die Anwenderunternehmen in Bezug auf die Auswahlkriterien einigermaßen zufrieden mit den Anbietern.

Allein im Hinblick auf Spezialisten-Kenntnisse und die Qualität von Service und Support erwarten sich die Kunden mehr als die Dienstleister bislang bieten können.

Bekanntheitsgrad und Leistungsfähigkeit ausgewählter Security-Dienstleister*

*- Perception Survey Chart / Anwendermeinungsbild*** -*



Quelle: META Group Deutschland *Basis: 200 Unternehmen*

**Die Größe der Kreise entspricht der Anzahl der Bewertungen zur Leistungsfähigkeit.*
***Transformierte Skala (100% entspricht sehr gut = 1 und 20% entspricht sehr schlecht = 5)*
****Die von der META Group getroffene Auswahl und Positionierung der Anbieterunternehmen reflektiert die Recherche der META Group durch Stichproben von Einschätzungen Dritter. Die Ergebnisse geben daher keinen Aufschluss über die tatsächliche Leistungsfähigkeit und/oder die tatsächliche Bekanntheit im Gesamtmarkt, weder absolut noch relativ zueinander.*

Abbildung 3: Bekanntheitsgrad und Leistungsfähigkeit ausgewählter Security-Dienstleister

1.3 Marktentwicklung

Der Markt für IT-Security-Produkte und –Dienstleistungen befand sich Anfang 2003 im Spannungsfeld zwischen steigenden Sicherheitsanforderungen und angespannten IT-Budgets. Jährliche Wachstumsraten in Höhe von 20 bis 30 Prozent, wie sie bis vor zwei Jahren noch zu beobachten waren, sind heute passé. Der Stellenwert der IT-Sicherheit wächst jedoch unvermindert weiter. 37 Prozent der deutschen Unternehmen geben an, im Jahr 2004 ihr Sicherheits-Budget gegenüber 2003 erhöhen zu wollen; immerhin 40 Prozent rechnen mit konstanten Ausgaben. Nur knapp ein Viertel der Befragten rechnet mit abnehmenden Investitionen in IT-Security beziehungsweise hat die Budgets für 2004 noch

nicht festgelegt. IT-Sicherheit stellt bei deutschen Unternehmen insgesamt eine relativ feste Größe dar, die aufgrund der Anforderungen von rechtlichen Institutionen, Partnern und Kunden nicht Gegenstand umfassender Budget-Kürzungen sein kann.

Durchschnittlich über sechs Prozent des IT-Budgets geben deutsche Unternehmen mit mindestens 50 Mitarbeitern heute für IT-Sicherheit aus. Rund 40 Prozent der Ausgaben beziehen sich dabei auf Maßnahmen für „Datenschutz“ und Vertraulichkeit, der Rest auf Verfügbarkeitsthemen beziehungsweise „Datensicherheit“. Trotz nahezu stagnierender IT-Ausgaben wird der Security-Markt im Jahr 2003 immerhin um sieben Prozent auf knapp 3 Milliarden EUR wachsen. Die Umsätze im Service-Bereich werden dank des anhaltenden Know-how- und Personalmangels bei Anwendern mit acht Prozent etwas stärker zunehmen als bei Hardware- und Software-Produkten (sechs Prozent).

Die META Group geht davon aus, dass die Talsohle im Markt für IT-Sicherheit im Jahr 2003 durchschritten wird – eine halbwegs stabile weltweite politische und gesamtwirtschaftliche Situation vorausgesetzt. Das durchschnittliche jährliche Wachstum (CAGR) im IT-Sicherheits-Markt wird zwischen 2002 und 2005 rund 9,5 Prozent betragen. Damit gehört IT-Sicherheit zu den wichtigen Wachstumssegmenten im Bereich der Informationstechnologie.

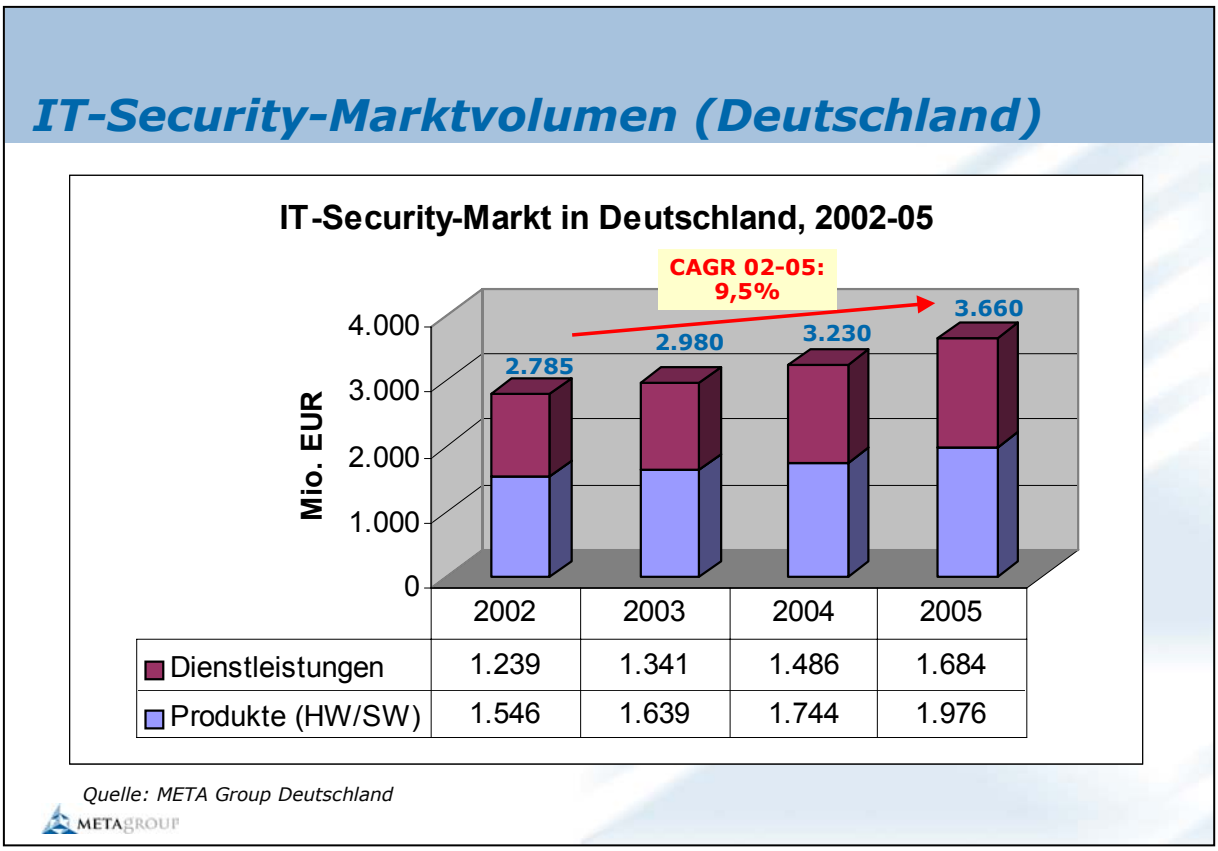


Abbildung 4: Marktentwicklung in Deutschland – IT-Security

Die META Group erwartet bis Ende 2004 vor allem Wachstumsimpulse aus dem Dienstleistungssektor, der diskreten Fertigungsbranche, von Banken, Versicherungen und Finanz-

dienstleistungen sowie aus der Gruppe der Logistikunternehmen, Telekommunikationsdienstleister und Energieversorger. Zurückhaltend bei den Investitionen in IT-Sicherheit sind hingegen die öffentliche Hand beziehungsweise Non-Profit-Organisationen, die prozessorientierte Fertigung und der Handel.

Das Marktwachstum wird weitestgehend von großen Unternehmen und vom gehobenen Mittelstand mit 500 bis unter 1.000 Mitarbeitern getragen. Letzterer zeigt aktuell sehr aggressive Investitionspläne für IT-Sicherheit. Der klassische Mittelstand als Segment der Unternehmen mit weniger als 500 Mitarbeitern erweist sich hinsichtlich der künftigen Security-Investitionen bis 2004 hingegen noch als sehr zurückhaltend. Rechtliche Rahmenbedingungen wie Basel II werden langfristig jedoch auch im Mittelstand entsprechende Maßnahmen zur Schadensverhütung mit anstoßen.

Standardisierte Technologien mit geringer Komplexität finden bei Anwenderunternehmen derzeit den meisten Zuspruch. Virenattacken werden von den Anwenderunternehmen in Deutschland als höchstes Sicherheitsrisiko eingestuft, und so ist es auch nicht weiter verwunderlich, dass der Einsatzgrad von Virenschutzlösungen heute nah an der 100%-Marke liegt. Auch Firewalls sind mittlerweile in den meisten Unternehmen Standard. Im Ranking der Anfang 2003 eingesetzten Technologien bei den Sicherheits-Investitionen folgen darüber hinaus Lösungen für die Server-Zugriffskontrolle und Sicherheitsüberwachung sowie für die Nutzer-Authentifizierung (lokal und „remote“). Stetiges Wachstum ist auch bei Virtual Private Networks (VPNs) zu verzeichnen. Entsprechende Investitionen sind vergleichsweise leicht zu rechtfertigen, geht es bei VPNs in der Regel doch nicht nur um Sicherheit, sondern auch um konkret nachweisbare Einsparungseffekte und Effizienz.

Der Markt für Virenschutz- und Firewall-Produkte ist zwar reif, aber noch nicht gesättigt. Die Anforderungen sind in diesem Bereich einer starken Dynamik unterworfen. Fragen rund um Content Security, Sicherheitsmanagement, Web Services und mobile Technologien sorgen für permanenten Innovationsdruck. Dies bestätigt auch die vorliegende Untersuchung: Die deutschen Anwenderunternehmen legen im Jahr 2003 verstärktes Augenmerk auf Content Security (Email- und Web-Filtering, SPAM-Filter). Der Wissensstand der Anwender über Ziele, Nutzen und Ausrichtung der einzelnen Lösungen ist jedoch derzeit noch sehr „durchwachsen“. Es ist nach Einschätzung der META Group nicht auszuschließen, dass zunächst in kleinerem Umfang investiert wird und sich erst nach umfassenden Bewusstseinskampagnen der Anbieter ab 2004 Content-Security-Lösungen in der Breite durchsetzen werden.

Der Markt für IT-Security-Dienstleistungen profitiert derzeit vom Personalmangel bei deutschen Anwenderunternehmen. Gerade in wirtschaftlich unsicheren Zeiten möchten sich die Unternehmen ungern an neue Mitarbeiter binden und greifen daher für abgegrenzte Aufgabenstellungen auf externe Dienstleister zurück. Vor allem bei der Implementierung von Security-Lösungen, der Konzeption unternehmensweiter IT-Sicherheit und –Architekturen sowie für Managed Firewall Services nehmen deutsche Unternehmen in den Jahren 2003 und 2004 Sicherheitsdienstleister in Anspruch. Managed Services für Firewalls gehören zu den wenigen Bereichen, auf die vor allem auch der Mittelstand künftig verstärkt zugreifen wird.

Dienstleistungen rund um Penetration Testing, Ethical Hacking, Sicherheits-Audits und Risk Assessment sind allmählich im Kommen. Dies zeigt, dass das Sicherheitsbewusstsein, aber auch die Unsicherheit in Hinsicht auf die Verlässlichkeit der eigenen Security-Infrastrukturen und –Prozesse in den vergangenen Jahren zugenommen hat. Methoden des Risk Assessments müssen jedoch noch heranreifen. Sie werden mittelfristig vorwiegend in großen Unternehmen zum Einsatz kommen.

Die langfristige technologische Planung der Anwenderunternehmen ab dem Jahr 2004 sieht auch verstärkt die Verschlüsselung für PCs und Email-Kommunikation sowie den Aufbau von Public-Key-Infrastrukturen (PKI) vor. Nach dem Scheitern vieler PKI-Projekte in der Vergangenheit sind die Unternehmen nunmehr aber zurückhaltender geworden. Neue Vorhaben werden heute selektiv und vorsichtig angegangen. Auch das Outsourcing der Certificate Authority im Rahmen von PKI-Projekten wird künftig langsam zunehmen. Typischerweise werden PKI-Projekte zunächst für spezielle Bereiche oder Nutzergruppen realisiert; manchmal erfolgt in einer Ausbauphase der Roll-Out in weiteren Unternehmensbereichen. Die META Group geht in Deutschland insgesamt von einem geringen, aber stetigen Wachstum der PKI-Investitionen aus. Damit entwickelt sich das Thema zwar langsamer als vor zwei Jahren noch weitläufig vermutet, aber es steht weiterhin auf der Agenda vor allem großer Unternehmen.

Weitere langfristig orientierte Themen sind WLAN-Sicherheit bzw. –Verschlüsselung, die Verschlüsselung auf Anwendungsebene (z.B. Extranet, Dokumentenmanagement etc.), Intrusion Detection Systeme (IDS), Web Single Sign-On, Directories sowie generell Identity Management als übergreifender Ansatz. Auch die Sicherheit von Web Services wird allmählich ins Blickfeld rücken.

Im Bereich der Sicherheitsdienstleistungen erwähnenswert sind Managed Security Services. Während nach Einschätzung der META Group die Reife von Managed VPN und Firewall Services bereits heute relativ weit gediehen ist, führen Managed Services für Intrusion Detection und Vulnerability Scanning mittelfristig noch ein Nischendasein. Entsprechende Dienste für Vulnerability Scanning werden weltweit erst bis Ende 2003 heranreifen, gefolgt von Managed Services für Intrusion Detection (2003/2004), Security Monitoring und Response (2004) sowie für Authentifizierung und Administration (2004/2005). Der deutsche Markt wird nach Einschätzung der META Group dieser Entwicklung um etwa ein Jahr hinterherhinken.

2 Untersuchungsmethode und Stichprobencharakteristika

Die Multi-Klienten-Studie „IT-Security im Jahr 2003“ widmet sich der Erhebung der aktuellen Situation im Bereich der IT-Sicherheit, geplanter Initiativen im Anwenderumfeld und der zu erwartenden Marktentwicklung in Deutschland. Die Studie beleuchtet insbesondere die wirtschaftlichen Aspekte und Entscheidungswege im Zusammenhang mit IT-Security. Im Fokus steht zudem ein Überblick über die im Markt agierenden Dienstleister und Lösungspartner.

Insgesamt wurden im Februar 2003 209 Unternehmen zum Stand der IT-Sicherheit und der künftigen Planung befragt. Die Befragung erfolgte telefonisch anhand eines detaillierten Fragebogens. Die Antworten der Unternehmen wurden softwaretechnisch ausgewertet und, wo erforderlich, gemittelt.

Befragt wurden dabei Unternehmen mit mindestens 50 Mitarbeitern. 51 Prozent der Befragungsteilnehmer sind dem Segment der kleinen und mittelständischen Unternehmen mit unter 500 Mitarbeitern zuzurechnen, die verbleibenden 49 Prozent stammen aus dem gehobenen Mittelstand beziehungsweise sind Großunternehmen. Betrachtet man ausschließlich die Anzahl der Mitarbeiter in Deutschland, so nehmen die „lokalen“ Mittelständler 56 Prozent der Nettostichprobe ein, gegenüber 44 Prozent Großunternehmen.

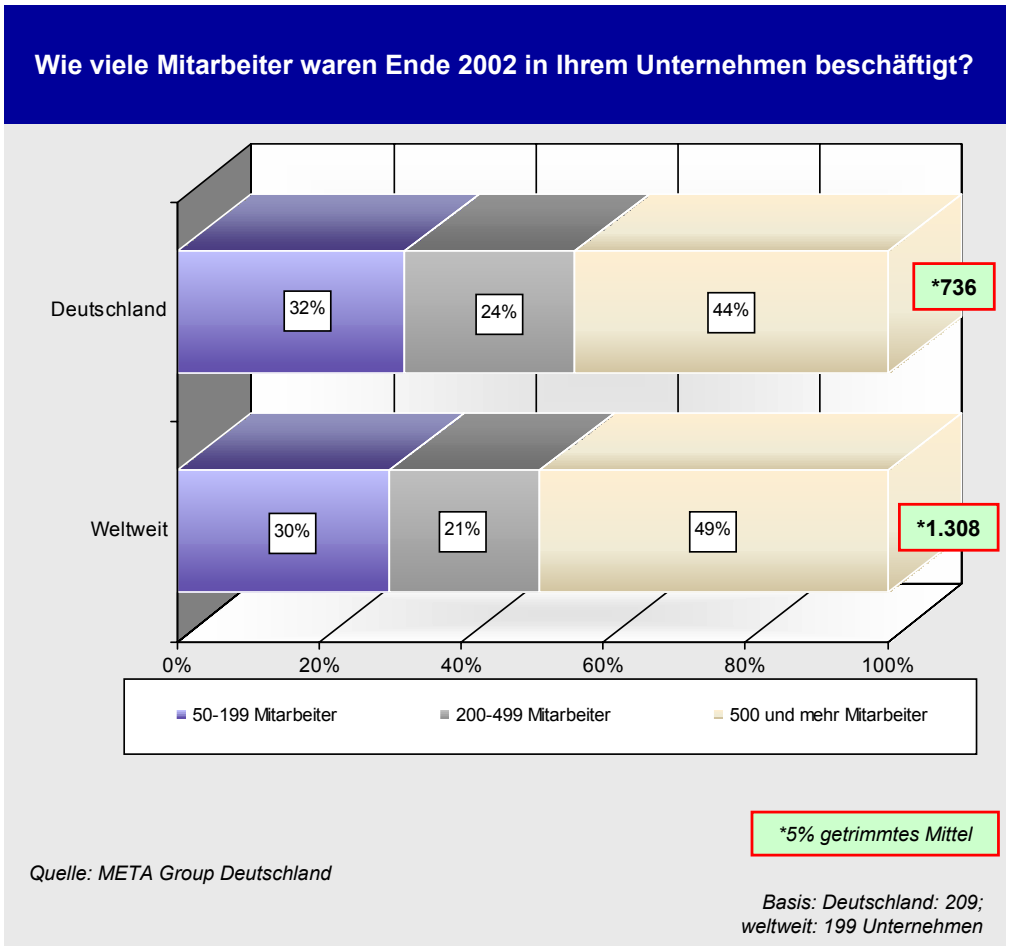


Abbildung 5: Mitarbeiterverteilung der befragten Unternehmen

Im Rahmen der Studie wurden die wesentlichen Branchensegmente in Deutschland berücksichtigt und – wo statistisch erforderlich und möglich – zu Gruppen zusammengefasst. Die Definition der Branchen ist Abschnitt 10.4 (Fragebogen) zu entnehmen. Aus statistischen Gründen und abweichend von diesen Definitionen wurden einzelne Unternehmen anderen Branchenkategorien zugeordnet, sofern diese Unternehmen durch Affinitäten zu diesen Branchen gekennzeichnet waren (siehe Abbildung 7).

Die realisierte Stichprobenverteilung orientiert sich an der Grundgesamtheit der am Markt bestehenden Branchenzugehörigkeit und kann als näherungsweise repräsentativ für die reale Branchenverteilung in Deutschland gelten.

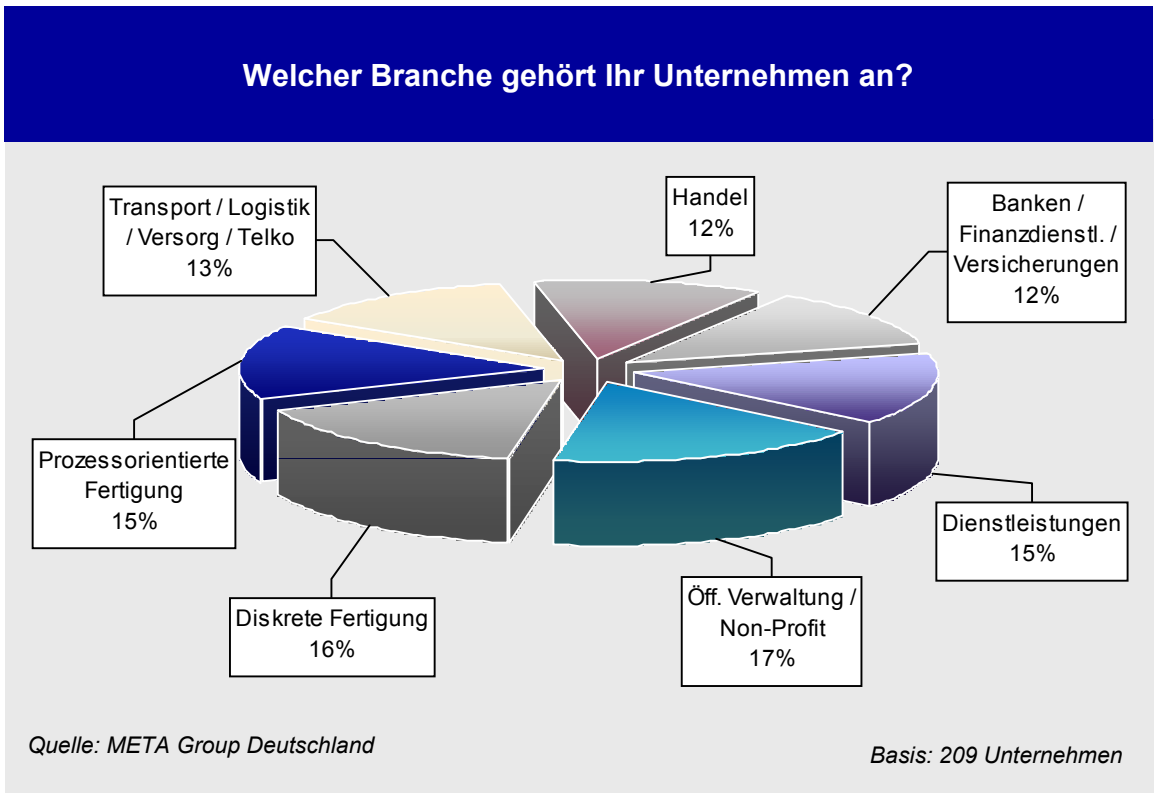


Abbildung 6: Branchenverteilung der realisierten Befragungs-Stichprobe

Kategorie	Branchensegmente	Anteil an Stichprobe [%]
Diskrete Fertigung	Diskrete Fertigung	16,3
Prozessorientierte Fertigung	Prozessorientierte Fertigung	13,4
	Primärer Sektor	1,4
Transport, Telekommunikation, Versorgung	Transport und Logistik	7,2
	Telekommunikation	1,4
	Versorgung	4,3
Dienstleistungen	Business Services	12,4
	Medien	2,4
Handel	Einzelhandel	6,7
	Großhandel	4,8
	Versandhandel	0,5
Banken, Finanzdienstleistungen, Versicherungen	Banken und Finanzdienstleistungen	9,6
	Versicherungen	2,9
Öffentliche Verwaltung, Non-Profit	Gesundheitswesen	0,5
	Bildung	0,5
	Öffentliche Hand	15,8
Quelle: META Group Deutschland		

Abbildung 7: Zuordnung einzelner Branchensegmente zu Branchenkategorien

Die Umsatzverteilung bei den befragten Anwenderunternehmen (Durchschnittswerte) in Deutschland ist nachfolgend dargestellt. 39 Prozent der Befragten haben 2001 Umsätze in Höhe von weniger als 50 Millionen EUR getätigt.

Bei Betrachtung der weltweiten Umsätze der Unternehmen verschiebt sich das Gewicht etwas in Richtung höherer Umsätze. 65 Prozent der Befragten haben 2001 weltweite Umsätze in Höhe von mindestens 50 Millionen EUR getätigt. Der Mittelwert der globalen Umsätze liegt bei über 1,5 Mrd. EUR.

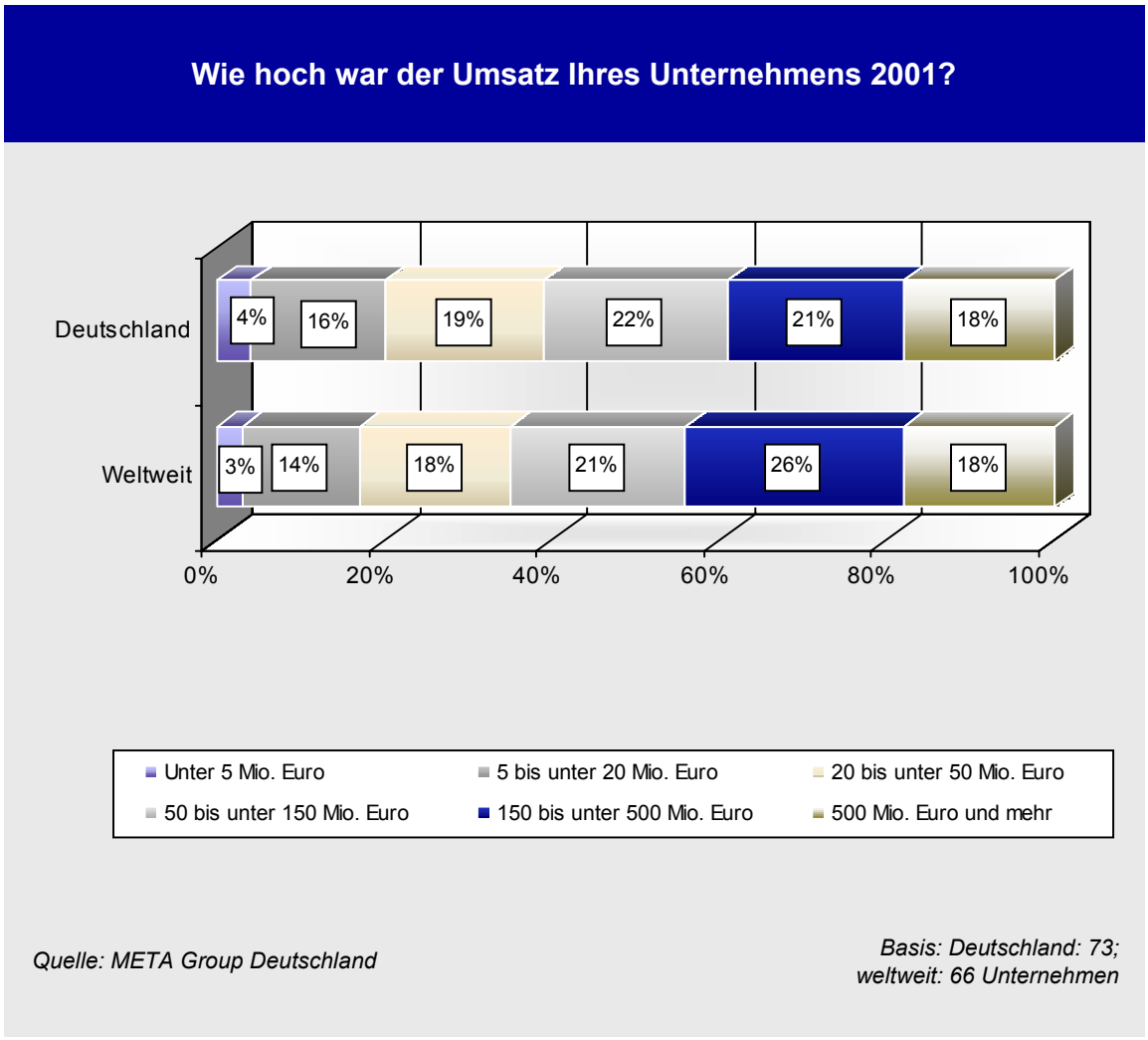


Abbildung 8: Umsatz der befragten Unternehmen

Die befragten Anwenderunternehmen verfügten Ende 2002 in Deutschland durchschnittlich über 420 PCs sowie 65 Notebooks. Nicht vernachlässigbar ist mittlerweile auch die Anzahl an PDAs: Der Mittelwert liegt hier bei 21 und damit nicht allzu weit unter der durchschnittlichen Anzahl an Servern im Unternehmen (29). Der Einsatzgrad von PCs bei den befragten Anwendern liegt im Durchschnitt bei 57 Prozent, wobei es Abweichungen zwischen einzelnen Branchen gibt.

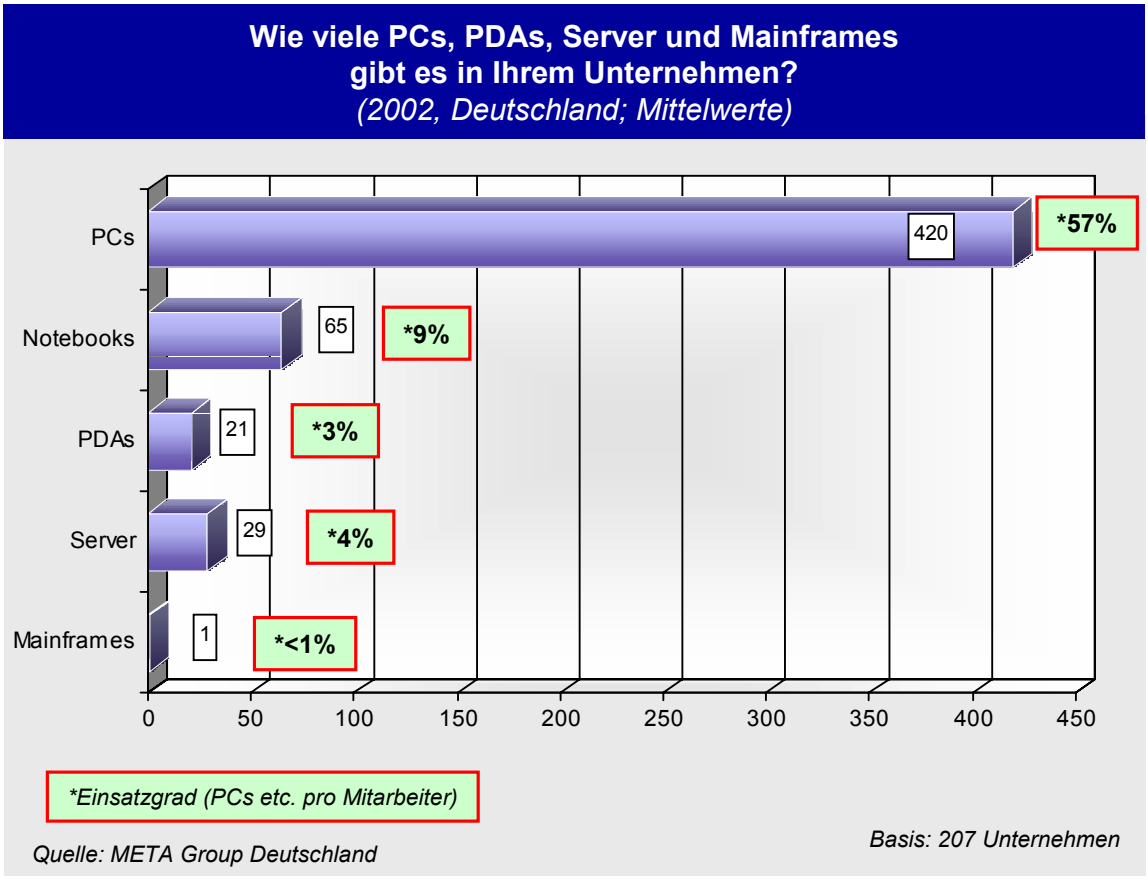
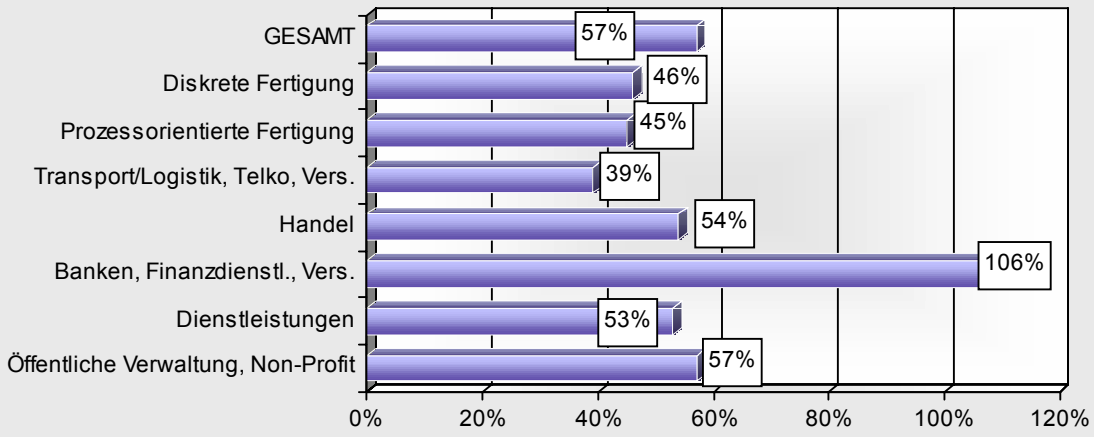


Abbildung 9: Skizzierung der Hardware-Infrastruktur (Server und Endgeräte)

Der Einsatzgrad an PCs, Notebooks, PDAs, Server und Mainframes bei den befragten Anwendern ist nachfolgend nach Branchen aufgeschlüsselt. Es wird deutlich, dass große Unterschiede zwischen den einzelnen Branchen bestehen.

PC-Einsatzgrad nach Branchen*
(2002, Deutschland; Mittelwert)



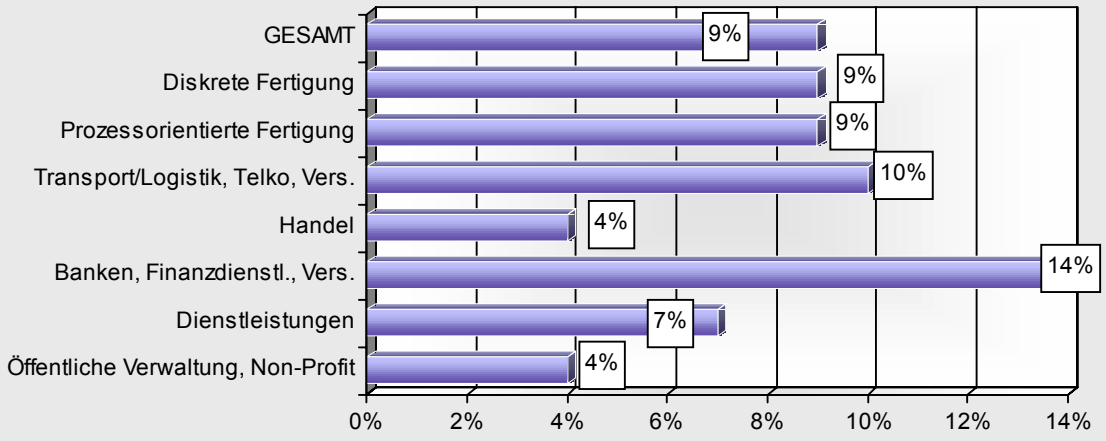
**Einsatzgrad: PCs pro Mitarbeiter*

Quelle: META Group Deutschland

Basis: Diskr. Fert. 34, Prozessfert. 30, Logistik/Vers./Telko 27, Handel 24, Banken/Versichg. 26, Dienstl. 31, Öff. Verw. 35 Unternehmen

Abbildung 10: PC-Einsatzgrad nach Branchen

Einsatzgrad von Notebooks nach Branchen*
(2002, Deutschland; Mittelwert)



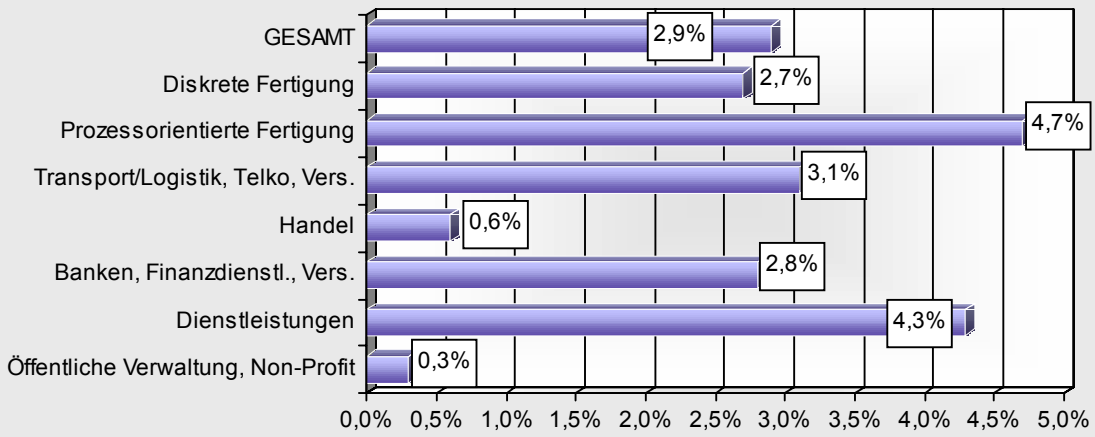
**Einsatzgrad: Notebooks pro Mitarbeiter*

Quelle: META Group Deutschland

Basis: Diskr. Fert. 34, Prozessfert. 30, Logistik/Vers./Telko 27, Handel 23, Banken/Versichg. 26, Dienstl. 31, Öff. Verw. 34 Unternehmen

Abbildung 11: Notebook-Einsatzgrad nach Branchen

PDA-Einsatzgrad nach Branchen*
(2002, Deutschland; Mittelwert)



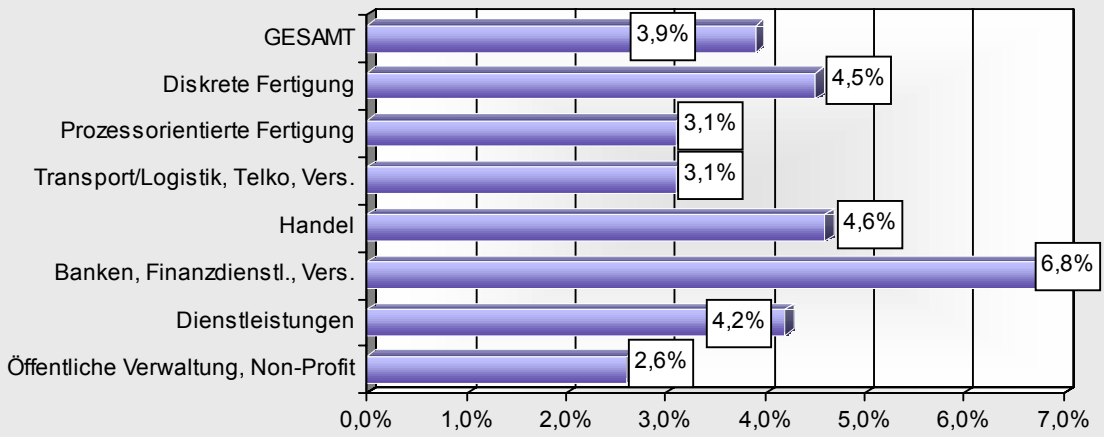
**Einsatzgrad: PDAs pro Mitarbeiter*

Quelle: META Group Deutschland

Basis: Diskr. Fert. 34, Prozessfert. 29, Logistik/Vers./Telko 27, Handel 22, Banken/Versichg. 26, Dienstl. 31, Öff. Verw. 35 Unternehmen

Abbildung 12: PDA-Einsatzgrad nach Branchen

Server-Einsatzgrad nach Branchen*
(2002, Deutschland; Mittelwert)



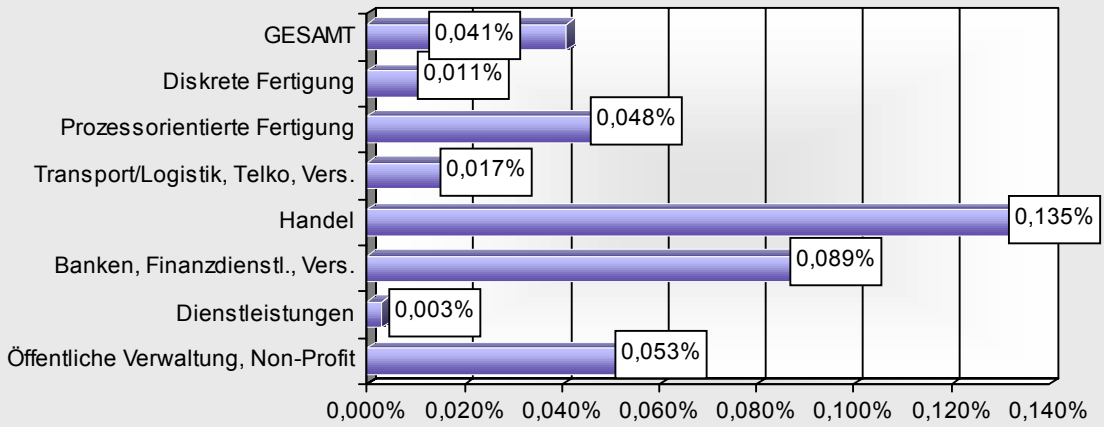
**Einsatzgrad: Server pro Mitarbeiter*

Basis: Diskr. Fert. 33, Prozessfert. 30, Logistik/Vers./Telko 27, Handel 24, Banken/Versichg. 25, Dienstl. 31, Öff. Verw. 35 Unternehmen

Quelle: META Group Deutschland

Abbildung 13: Server-Einsatzgrad nach Branchen

Mainframe-Einsatzgrad nach Branchen*
(2002, Deutschland; Mittelwert)



**Einsatzgrad: Mainframes pro Mitarbeiter*

Quelle: META Group Deutschland

Basis: Diskr. Fert. 32, Prozessfert. 30, Logistik/Vers./Telko 27, Handel 24, Banken/Versichg. 26, Dienstl. 30, Öff. Verw. 34 Unternehmen

Abbildung 14: Mainframe-Einsatzgrad nach Branchen

Im Rahmen der Untersuchung wurden vorzugsweise Entscheider befragt, die qualifizierte Auskunft zum Thema Informationssicherheit im Unternehmen geben können. Bei den befragten Ansprechpartnern im Unternehmen überwiegen mit einem Anteil von 57 Prozent IT-Leiter und Chief Information Officers (CIO). Darauf folgen mit 17 Prozent die IT-Security-Leiter beziehungsweise Chief Information Security Officers (CISO) sowie System- und Netzwerkadministratoren (zehn Prozent der Befragten). Zwölf Prozent der Ansprechpartner stammen aus nicht-technischen Bereichen; hierzu gehören die obere Managementebene, das Controlling/Finanzwesen sowie die Datenschutzbeauftragten.

Es sei darauf hingewiesen, dass diese Verteilung der Positionen die Stichprobe charakterisiert und Anhaltspunkte dafür liefert, welche Positionen Einfluss auf Entscheidungen im IT-Security-Umfeld haben. Eine detaillierte Analyse der Verantwortlichkeiten nach Unternehmensbereichen und Aufgaben hingegen ist Kapitel 4 zu entnehmen.

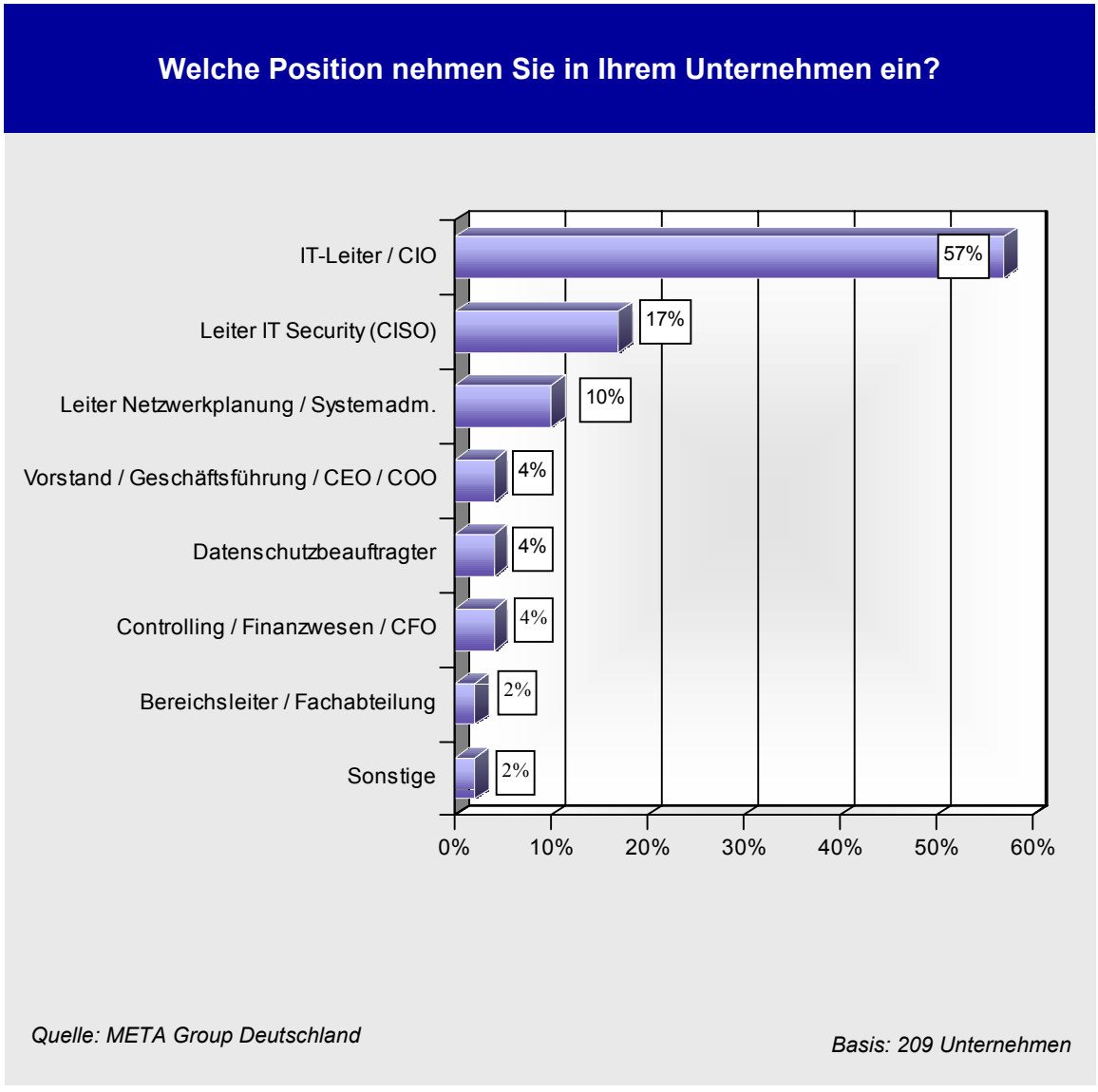


Abbildung 15: Position der Befragungsteilnehmer im Unternehmen

Generell ist der IT-Leiter oder CIO mit Abstand die häufigste Position, die für das Thema IT-Sicherheit als Ansprechpartner dient. Die Analyse nach Branchen und Unternehmensgrößen zeigt, dass dedizierte IT-Security-Verantwortliche beziehungsweise Chief Information Security Officers (CISOs) in vergleichsweise hohem Umfang bei Banken, Finanzdienstleistern und Versicherungen und bei großen Unternehmen anzutreffen sind. Im Mittelstand rekrutiert sich der Security-Ansprechpartner relativ häufig auch aus den Reihen der System- und Netzwerkadministratoren. Je kleiner das Unternehmen, desto wichtiger wird auch die Geschäftsführung beziehungsweise die Business-Management-Ebene als Ansprechpartner.

Abbildung 16 bis Abbildung 26 zeigen die Verteilung der maßgeblichen Positionen nach Branchen und Unternehmensgrößen im Detail.

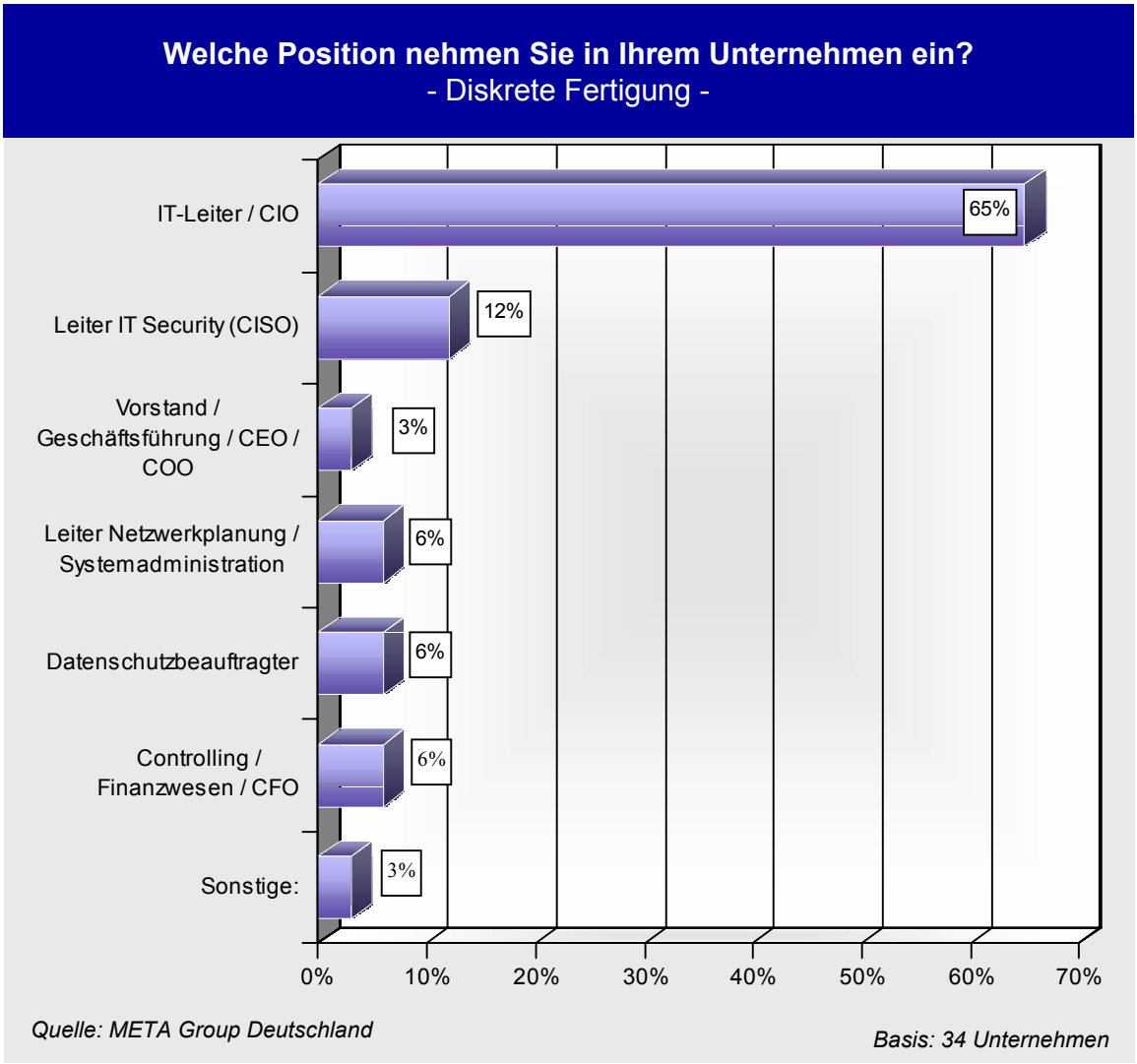


Abbildung 16: Position der Befragungsteilnehmer im Unternehmen – Diskrete Fertigung

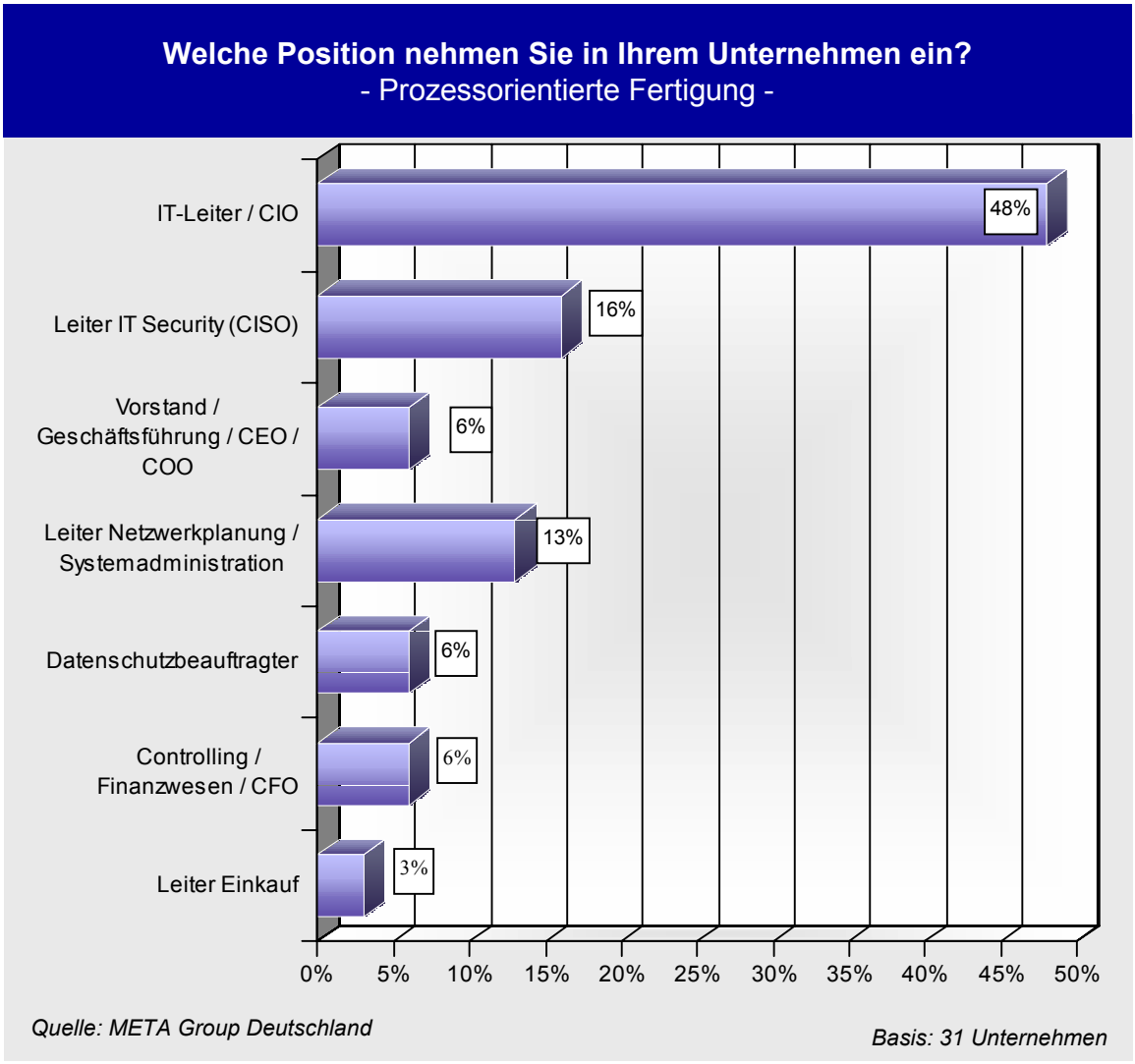


Abbildung 17: Position der Befragungsteilnehmer im Unternehmen – Prozessorientierte Fertigung

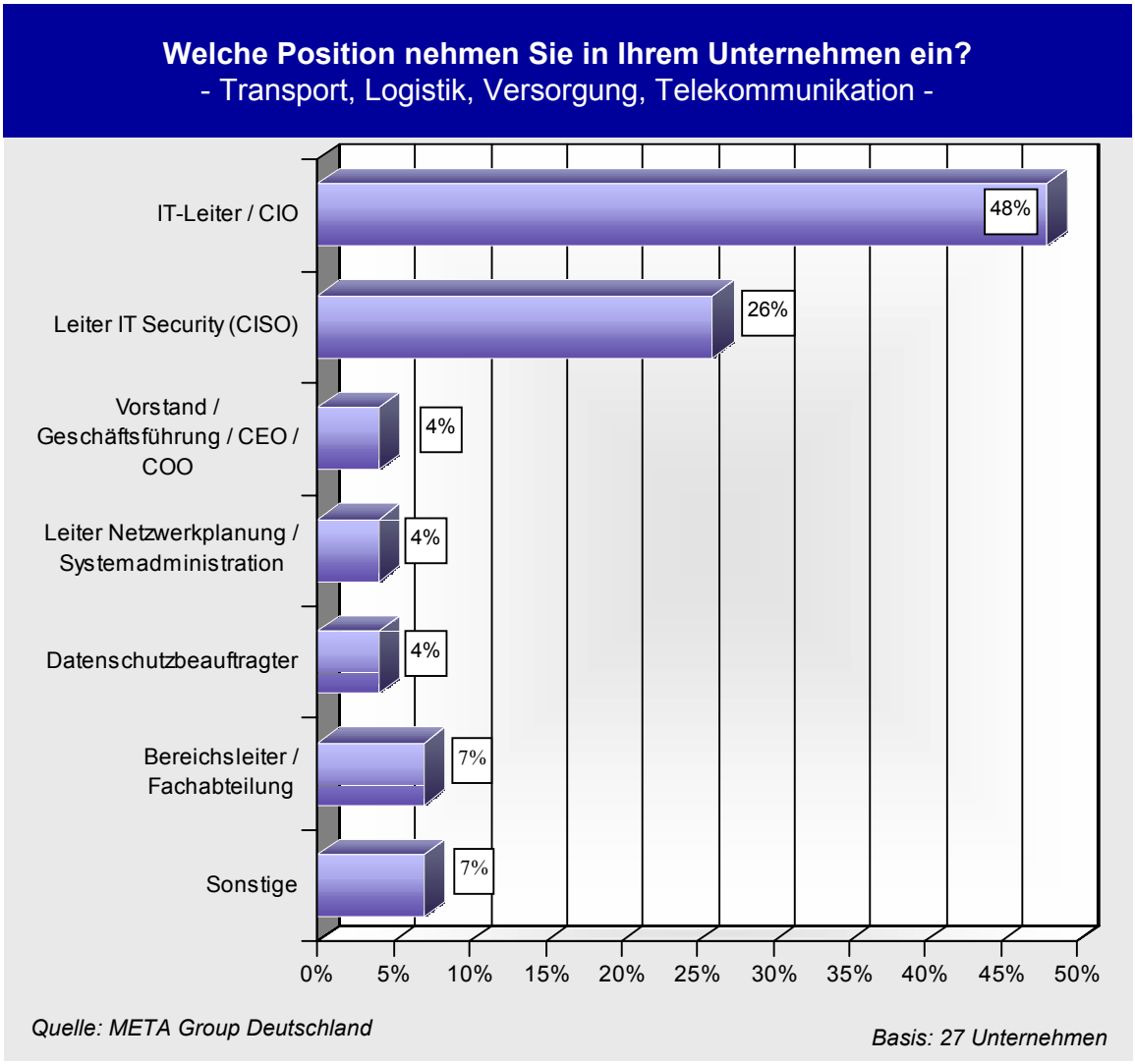


Abbildung 18: Position der Befragungsteilnehmer im Unternehmen – Logistik/Telko/Versorgung

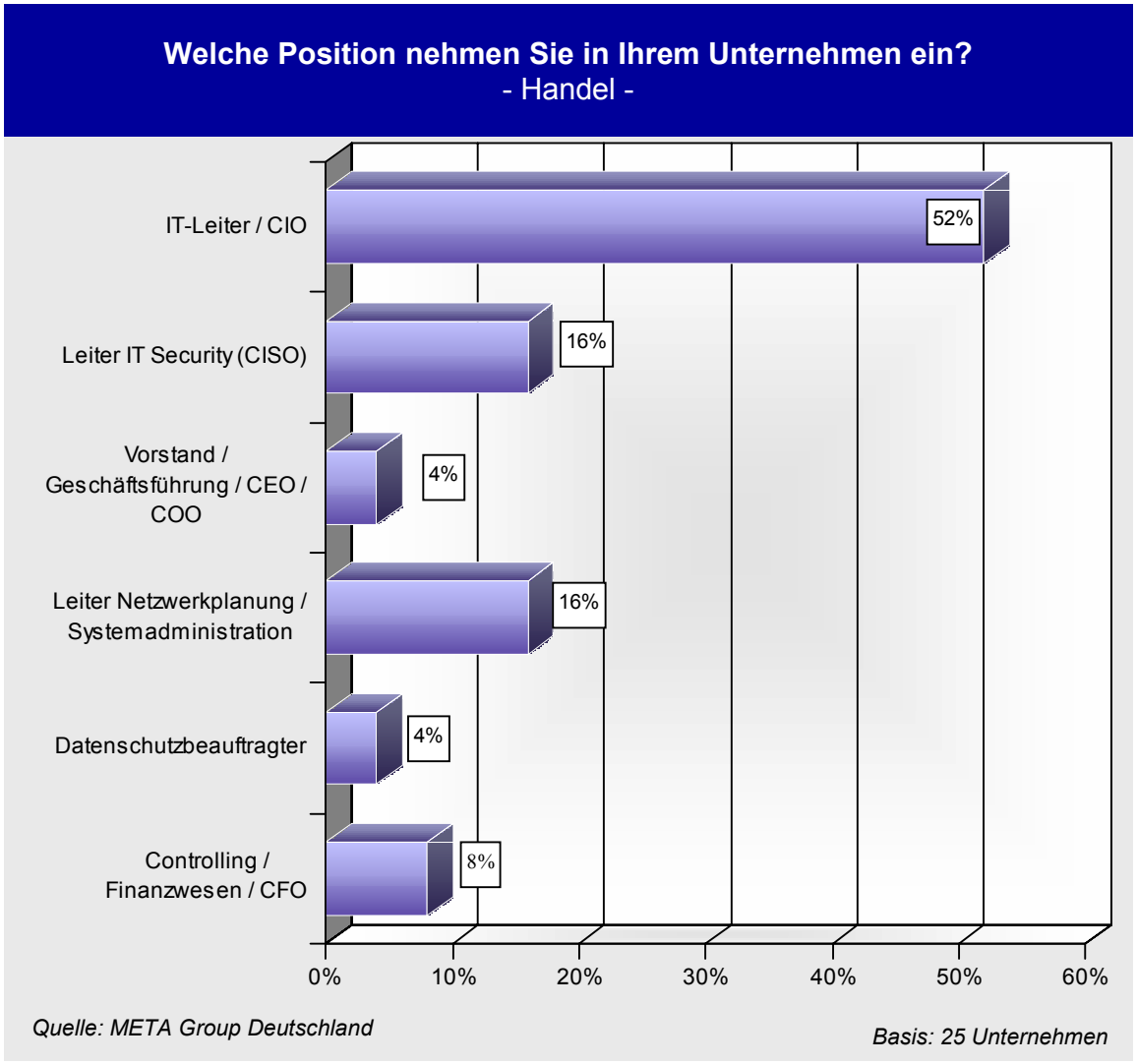


Abbildung 19: Position der Befragungsteilnehmer im Unternehmen - Handel

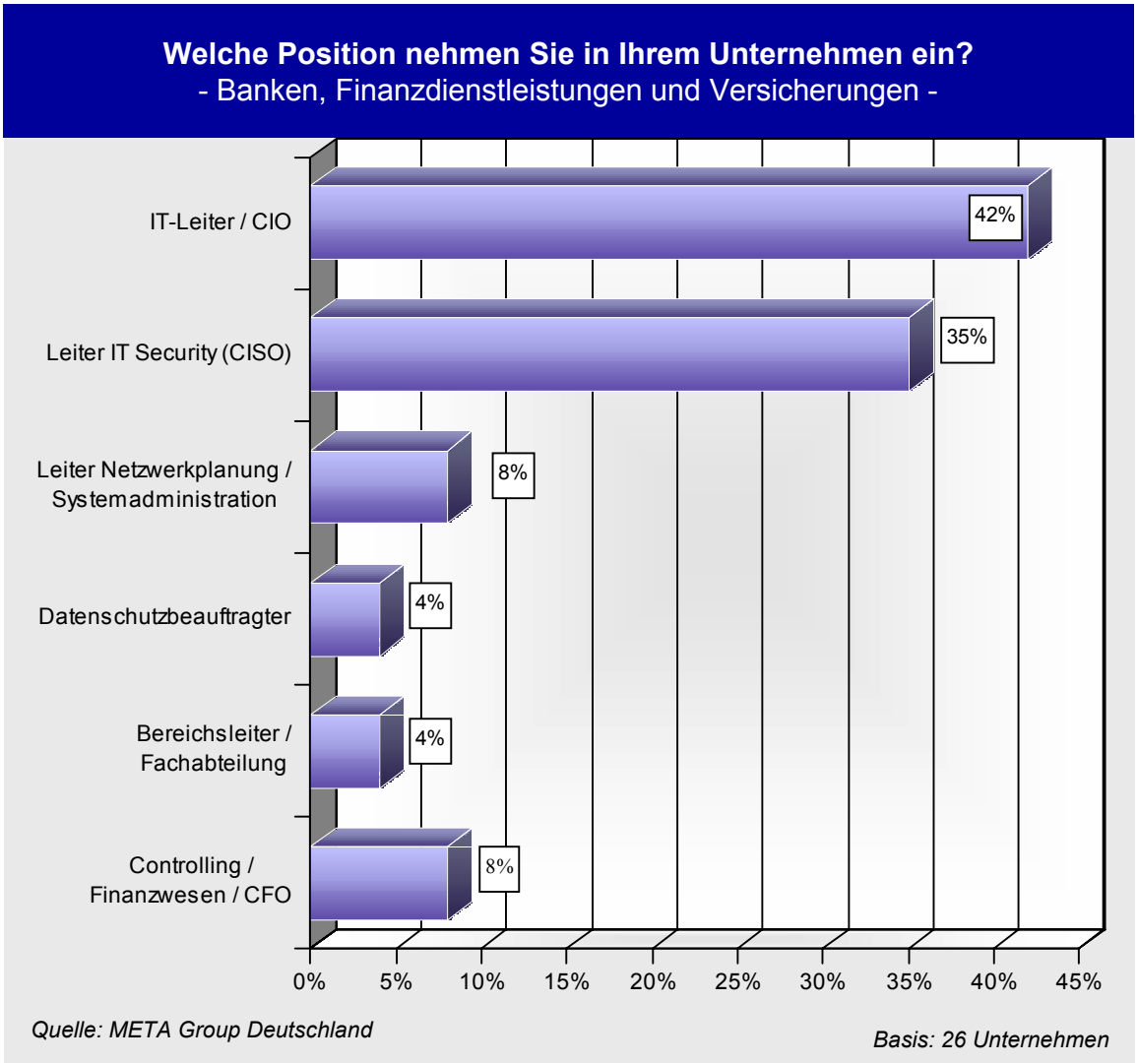


Abbildung 20: Position der Befragungsteilnehmer im Unternehmen – Banken, Versicherungen, Finanzdienstleistungen

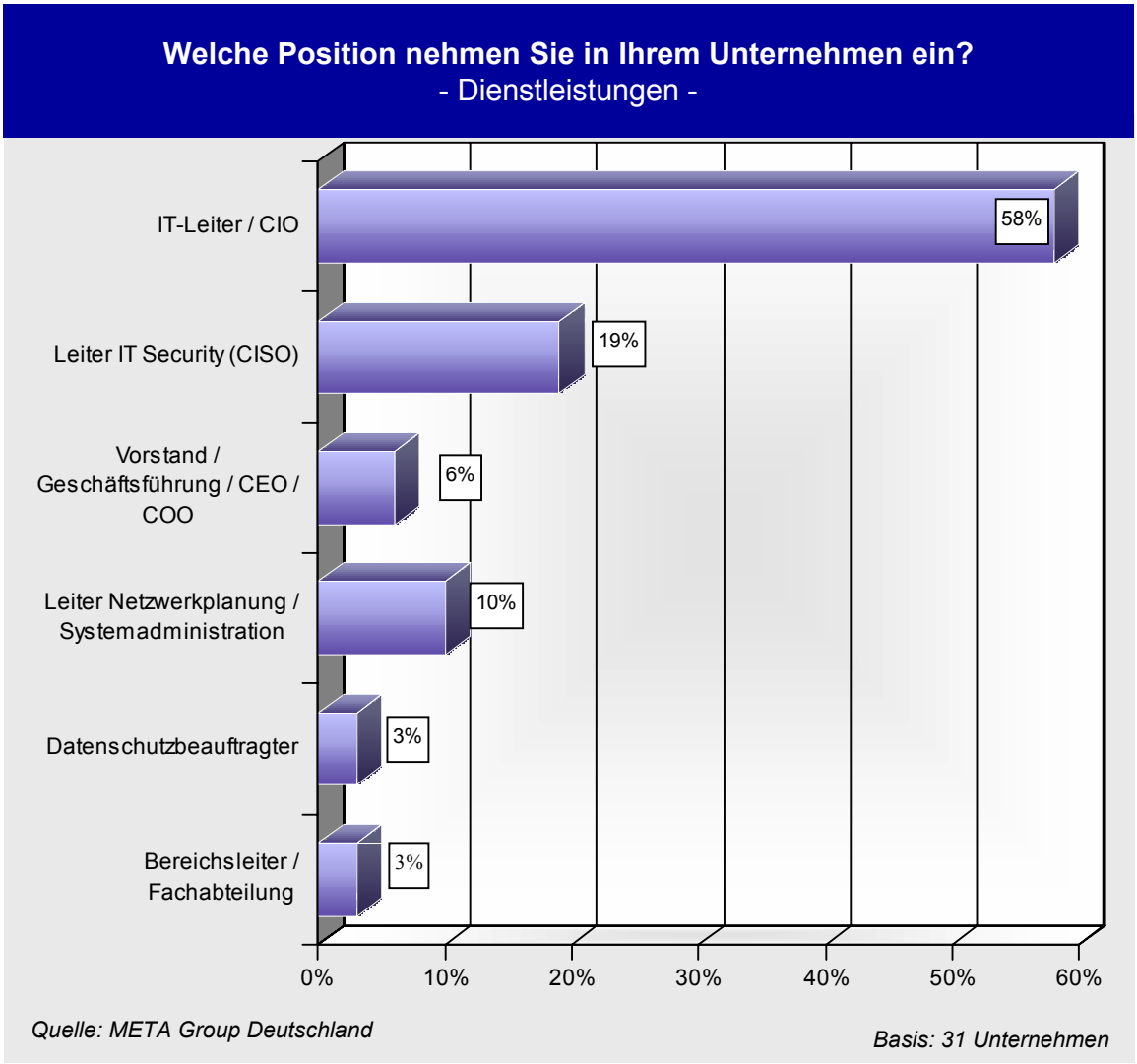


Abbildung 21: Position der Befragungsteilnehmer im Unternehmen - Dienstleistungen

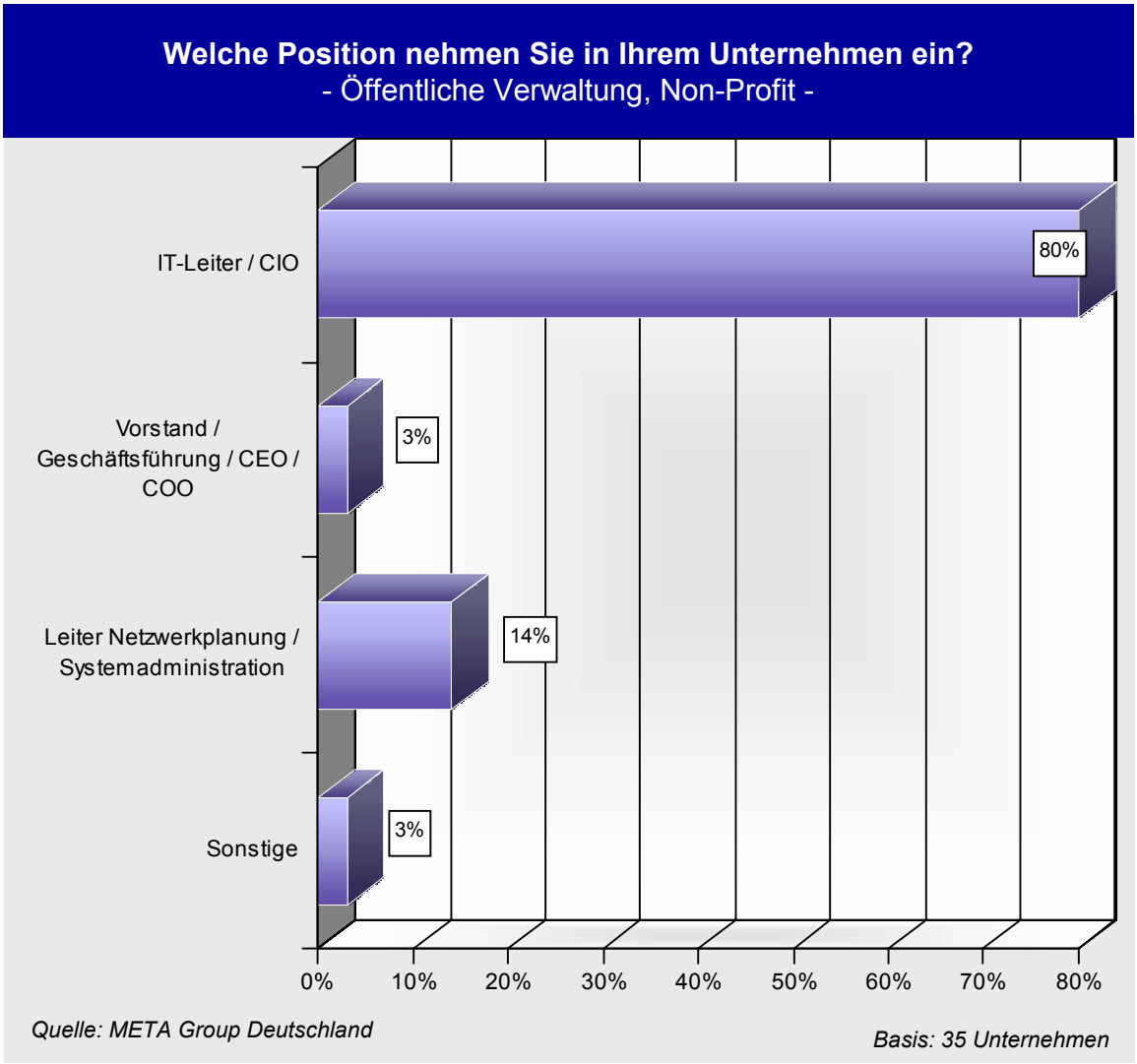
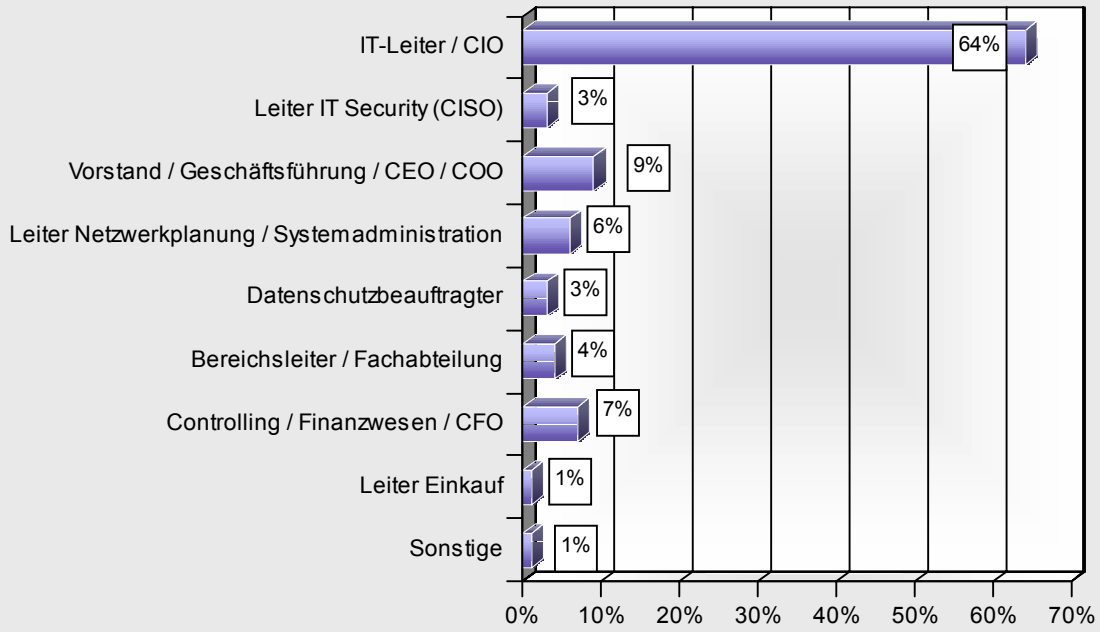


Abbildung 22: Position der Befragungsteilnehmer im Unternehmen – Öffentliche Hand / Non-Profit

Welche Position nehmen Sie in Ihrem Unternehmen ein?
- Unternehmen mit 50-199 Mitarbeitern -



Quelle: META Group Deutschland

Basis: 67 Unternehmen

Abbildung 23: Position der Befragungsteilnehmer im Unternehmen – 50-199 Mitarbeiter

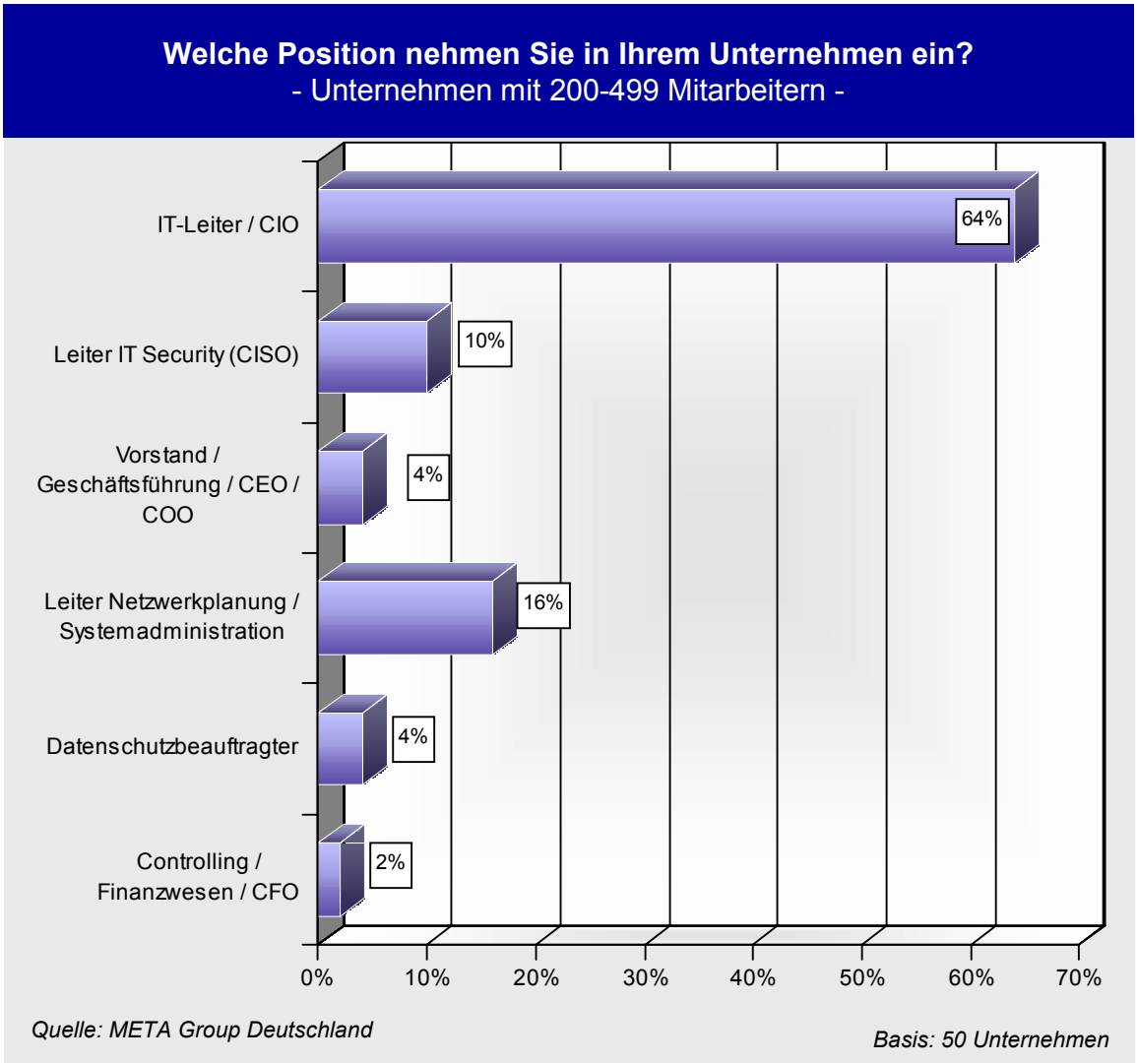


Abbildung 24: Position der Befragungsteilnehmer im Unternehmen – 200-499 Mitarbeiter

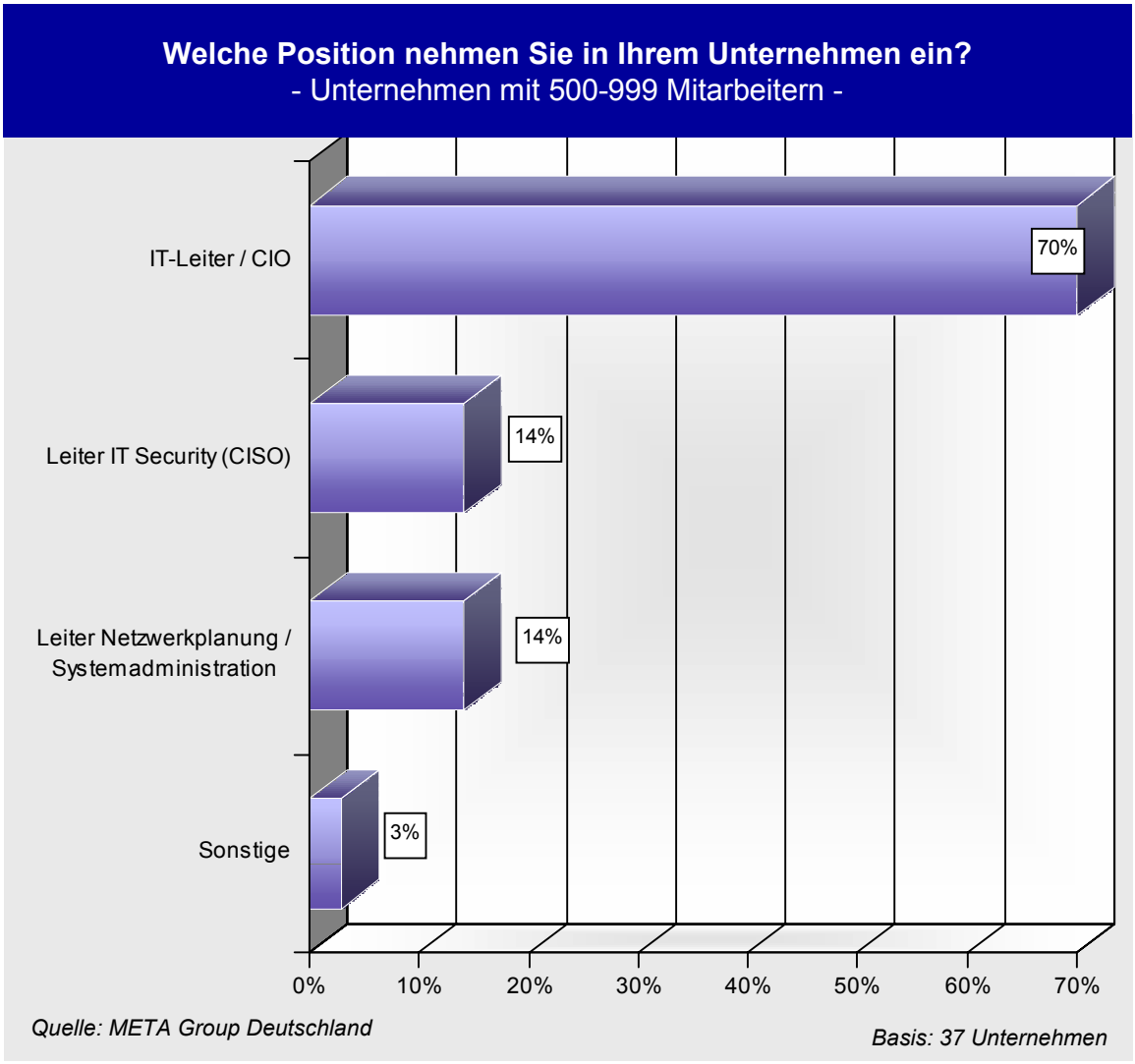


Abbildung 25: Position der Befragungsteilnehmer im Unternehmen – 500-999 Mitarbeiter

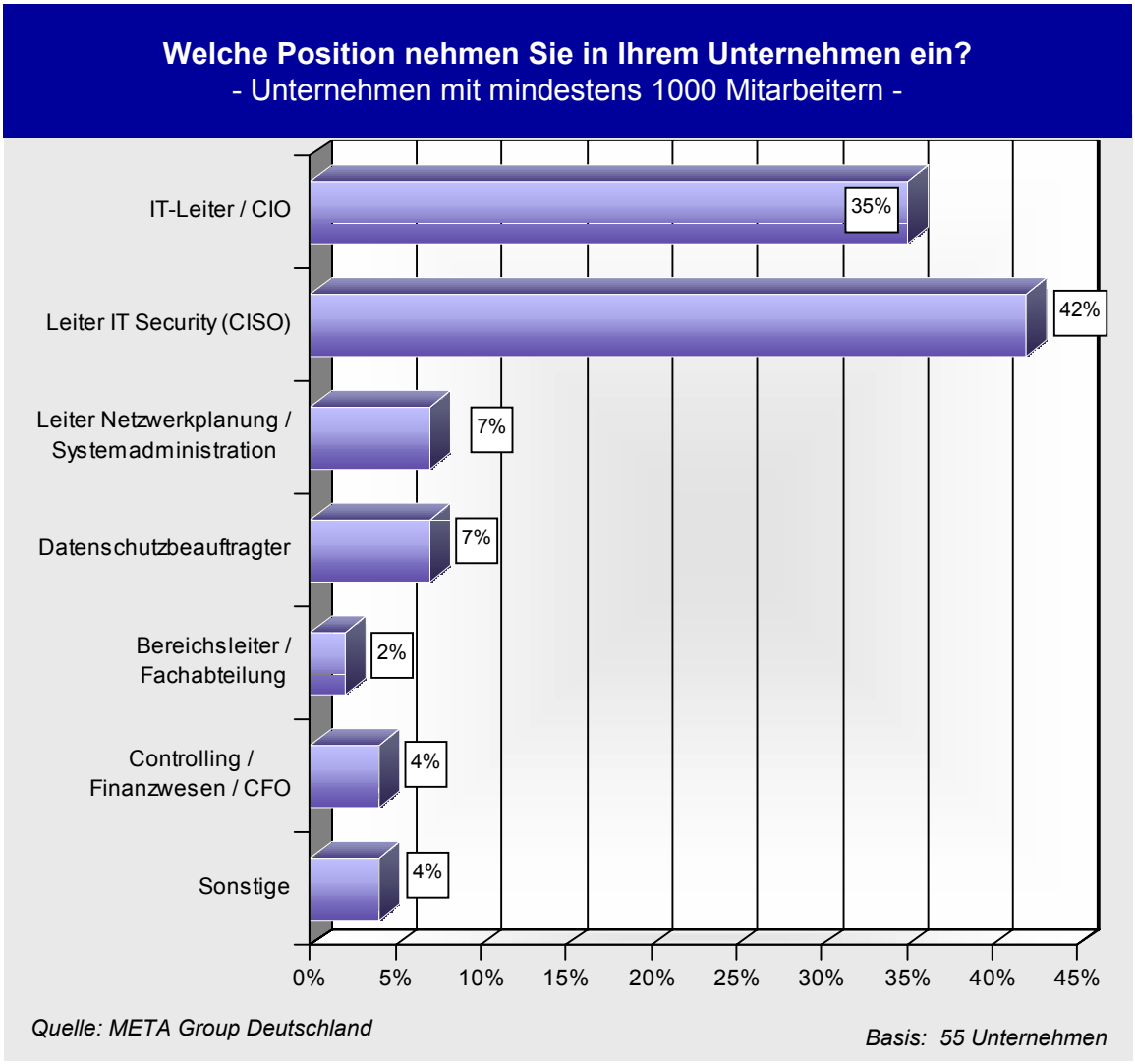


Abbildung 26: Position der Befragungsteilnehmer im Unternehmen – ab 1.000 Mitarbeiter

3 Organisatorische Aspekte der IT-Security

3.1 Security-Teams und Policies

Nur 25 Prozent der im Rahmen der vorliegenden Studie befragten Unternehmen verfügten Anfang 2003 über eine dedizierte IT-Sicherheitsorganisation im Unternehmen. Dieser erstaunlich niedrige Wert ist teilweise auf den beträchtlichen Anteil an mittelständischen Unternehmen in der Stichprobe zurückzuführen. In der Tat zeigt eine genauere Analyse nach Mitarbeiterzahl, dass nur neun Prozent der Unternehmen mit 50 bis unter 200 Beschäftigten über eine Sicherheitsorganisation verfügen, gegenüber 53 Prozent der Anwenderunternehmen mit mindestens 1.000 Mitarbeitern (siehe Abbildung 28). Verglichen mit den Global-2000-Unternehmen (den weltweit 2000 größten Anwenderunternehmen) haben die großen deutschen Unternehmen dennoch spürbaren Nachholbedarf. Nach Einschätzung der META Group hatten bereits Ende 2001 75 Prozent der Global-2000-Unternehmen unabhängige IT-Security-Teams aufgebaut.

Die META Group empfiehlt in diesem Zusammenhang, zunächst dedizierte IT-Security-Teams aufzubauen, die unternehmensintern als spezialisierte Consulting-Gruppen agieren. Sie sind verantwortlich für den Aufbau einer Policy auf allen Ebenen und für die Etablierung von Prozessen und Standards. Aufgabe der Sicherheits-Verantwortlichen ist es zudem, durch Kommunikation beziehungsweise internes Marketing das Security-Bewusstsein bei den Mitarbeitern zu schärfen und die Einhaltung der Policies sicherzustellen. Ohne dedizierte Security-Teams besteht die Gefahr, dass diese grundsätzlichen und konzeptionellen Aufgaben im Tagesgeschäft untergehen und damit nicht oder nur unvollständig erledigt werden.

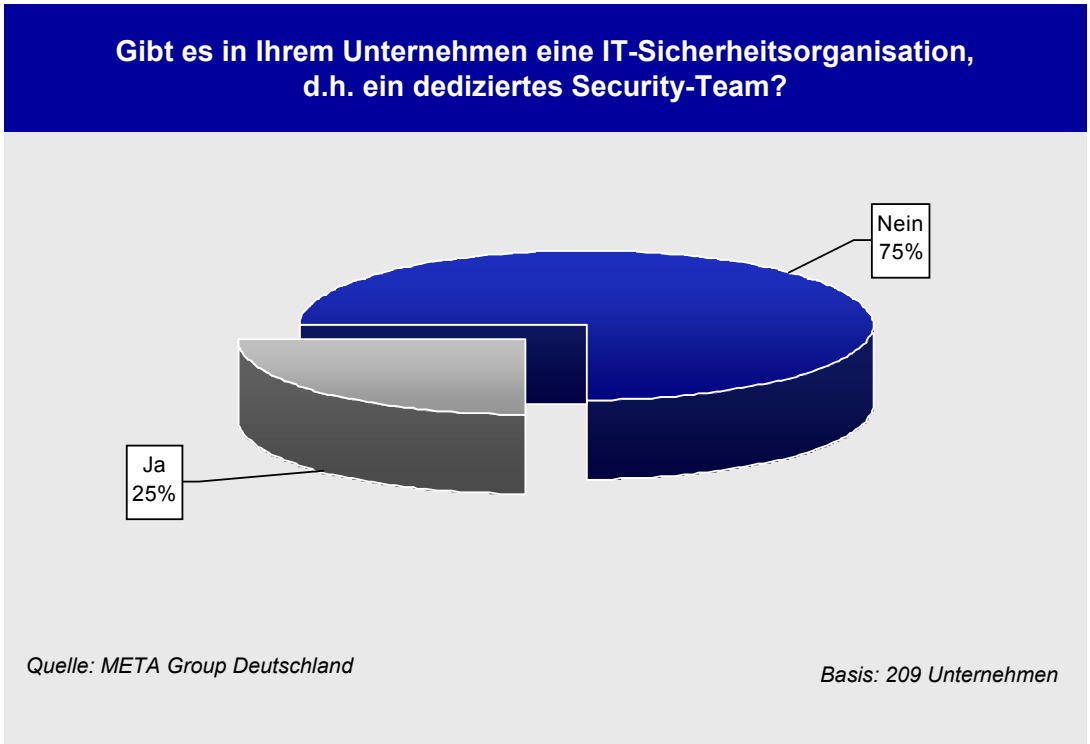
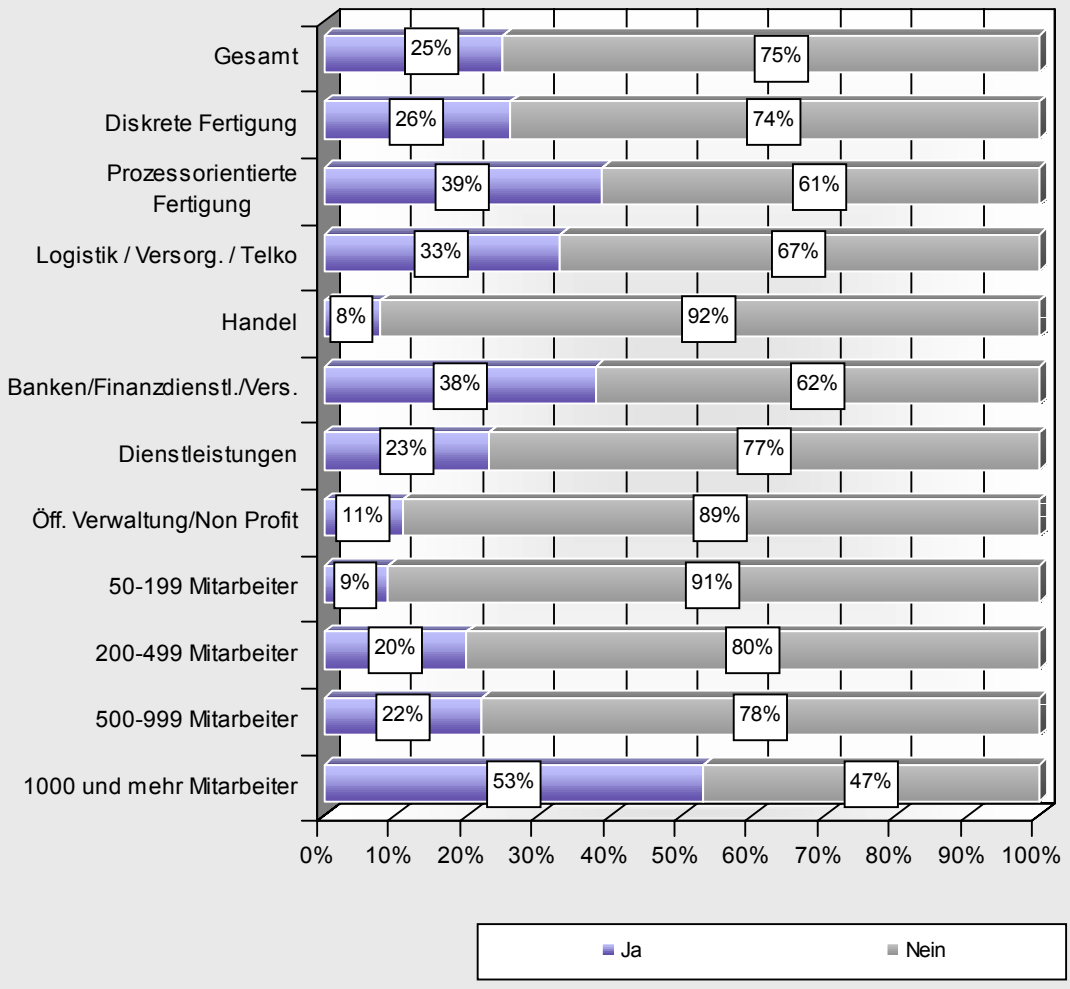


Abbildung 27: Anteil der Unternehmen mit IT-Sicherheitsorganisation

Der Anteil der Unternehmen mit dedizierten Security-Teams variiert nicht nur entsprechend der Unternehmensgröße, sondern hängt auch von der Branche ab. So sind Banken, Finanzdienstleister und Versicherungen sowie die prozessorientierte Fertigung und die Gruppe der Logistikunternehmen, Telekommunikationsdienstleister und (Energie-) Versorger in Bezug auf dieses Thema relativ weit fortgeschritten. Erheblichen Nachholbedarf haben hingegen der Handel und die öffentliche Hand.

Gibt es in Ihrem Unternehmen eine IT-Sicherheitsorganisation, d.h. ein dediziertes Security-Team?



Quelle: META Group Deutschland *Basis: 209 Unternehmen*

Abbildung 28: Anteil der Unternehmen mit IT-Sicherheitsorganisation – nach Branchen

Im Durchschnitt beschäftigen sich pro Unternehmen acht (Vollzeit-)Mitarbeiter (Full-Time Equivalents – FTEs) mit Fragen der IT-Security. Der Median* liegt bei 3 FTEs – damit wird deutlich, dass das Gros der Befragten deutlich weniger als 8 FTEs im Einsatz hat und das hohe arithmetische Mittel durch einzelne, typischerweise große Unternehmen zustande kommt. Nur 49 der im Rahmen der Studie befragten Anwenderunternehmen konnten Aussagen zur Anzahl der FTEs tätigen.

Als Best Practice für die großen Global-2000-Unternehmen geht die META Group von einer (1) Security-Fachkraft pro 600 bis 1.000 Mitarbeiter aus. Ein Vergleich der Mitarbeiterzahlen der oben genannten Anwenderunternehmen mit der Anzahl der Security-Fachkräfte im Unternehmen zeigt exemplarisch, dass bei großen deutschen Unternehmen mit mindestens 1.000 Mitarbeitern im Durchschnitt nur eine Security-Fachkraft auf 2.050 Mitarbeitern kommt. Damit sind diese Unternehmen weit von der Best Practice entfernt.

Der kleine und gehobene Mittelstand mit weniger als 1.000 Mitarbeitern hat ein Größenverhältnis von etwa 230 Beschäftigten pro Sicherheits-Fachkraft. Beobachtungen der META Group im Mittelstand sowie der geringe Anteil an Mittelständlern mit dedizierten Security-Organisationen sprechen dafür, dass es sich hier um einzelne IT-Mitarbeiter handelt, die mehrere Aufgaben auf sich vereinen – unter anderem auch IT-Sicherheit. Aufgrund der speziellen Voraussetzungen bei mittelständischen Unternehmen kann der Best-Practice-Wert für die G2000-Unternehmen hier nicht angewandt werden.

Insgesamt, das heißt bei Betrachtung aller Unternehmensgrößen, ergibt sich ein Verhältnis von 1.260 Mitarbeitern pro Security-Fachkraft.

* Der Median ist als der mittlere aller der Größe nach sortierten Variablenwerte definiert. Er teilt also die Verteilung in zwei Teile, die idealerweise gleichviel Daten enthalten sollen.

48 Prozent der Befragten haben eine schriftlich fixierte Security Policy im Unternehmen. Ernüchternd ist die Erkenntnis, dass 37 Prozent der befragten Unternehmen weder eine schriftliche Security Policy haben noch dies in Zukunft planen. Dabei ist die Security Policy die Grundlage ein jeder Informationssicherheits-Infrastruktur. Die Security Policy ist als eine Menge von „Sicherheitsgesetzen" zu betrachten, die zum Schutz der IT umzusetzen sind. Eine Implementierung von Sicherheits-lösungen, die nicht auf Policies basiert, lässt sich mit dem Aufbau von Polizei, Gerichten und Gefängnissen ohne jede Gesetzesgrundlage vergleichen. Security Policies sind insbesondere deshalb wichtig, weil sie konkrete Regelwerke sowohl für technische Maßnahmen (Zielgruppe IT-Mitarbeiter) als auch für Verhaltensweisen (alle Mitarbeiter im Unternehmen) darstellen. Sie muss schriftlich niedergelegt sein, da nur schriftliche Dokumente verbindlichen Charakter haben, sauber kommuniziert und permanent weiter entwickelt werden können – auch bei personeller Fluktuation in der Organisation. Unternehmen ohne schriftlich niedergelegte Security-Policy laufen daher Gefahr, Sicherheitslücken nur unzureichend vorzubeugen beziehungsweise erkennen und beseitigen zu können.

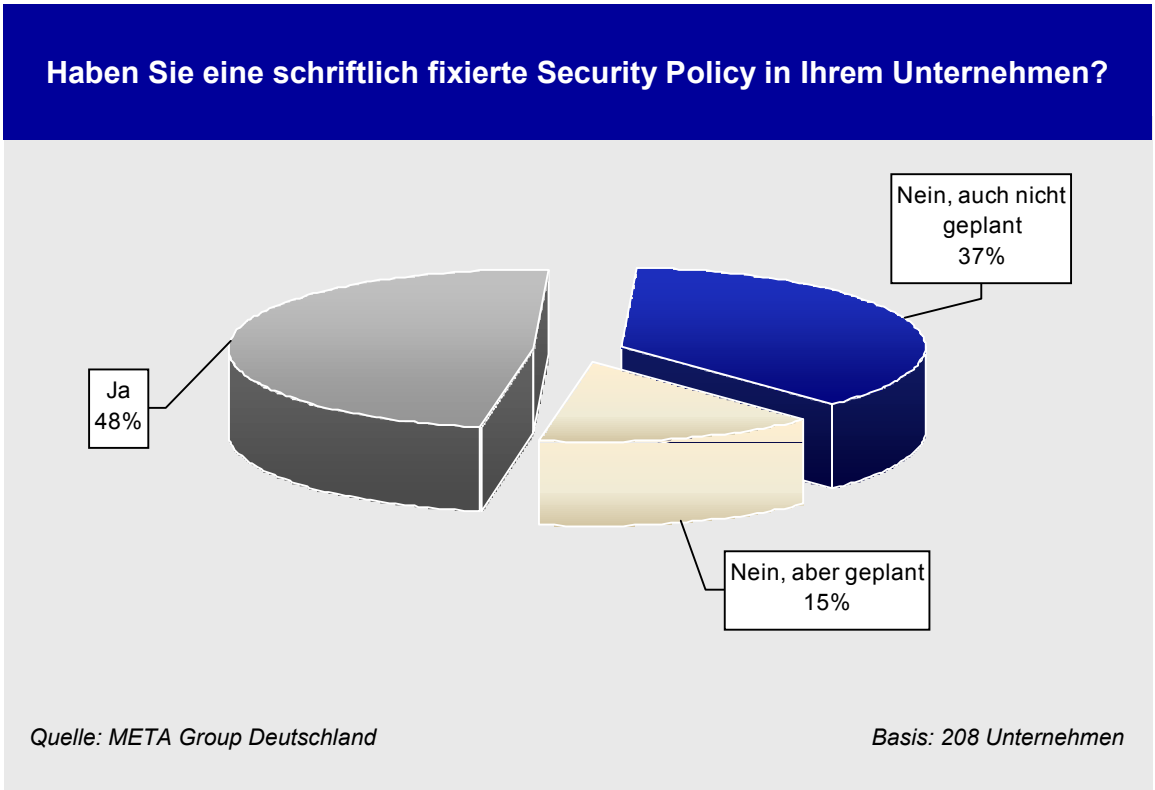
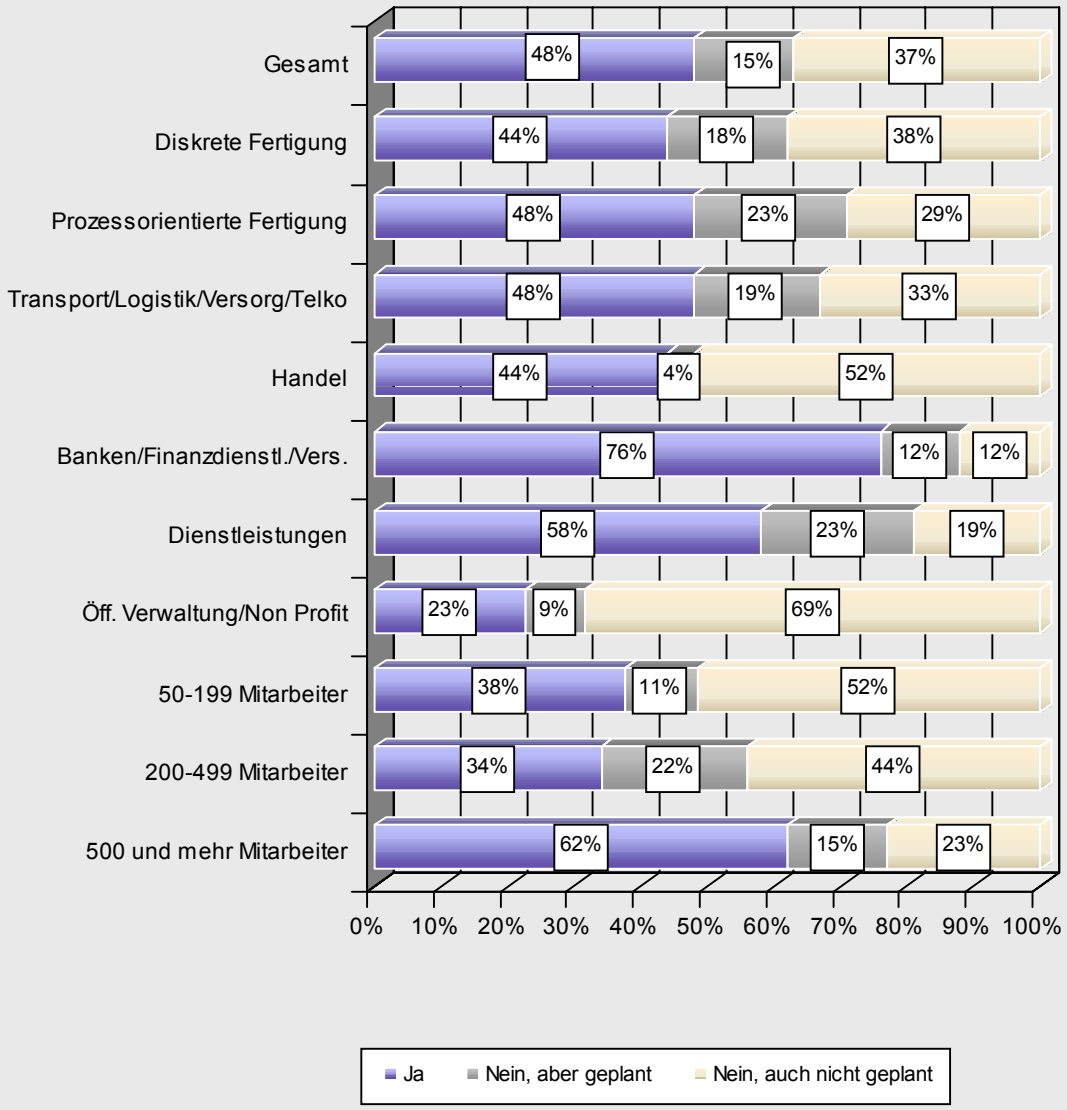


Abbildung 29: Anteil der Unternehmen mit schriftlich fixierter Security Policy

Große Mittelständler mit mindestens 500 Mitarbeitern und Großunternehmen haben mit 62 Prozent der befragten Unternehmen wesentlich häufiger eine Security Policy als kleinere Anwender. Die Analyse nach Branchen zeigt zudem, dass in diesem Punkt ganz eindeutig der Sektor Banken, Finanzdienstleistungen und Versicherungen führt: Dort verfügen 76 Prozent der Anwenderunternehmen über eine schriftlich niedergelegte Policy.

Haben Sie eine schriftlich fixierte Security Policy in Ihrem Unternehmen?



Quelle: META Group Deutschland

Basis: 208 Unternehmen

Abbildung 30: Anteil der Unternehmen mit schriftlich fixierter Security Policy – nach Branchen

Die von den befragten Unternehmen festgelegten Security Policies beziehen sich in erster Linie auf die Nutzung von Email und Web. Weitere sekundäre Bereiche sind vor allem spezifische Policies für PCs, Notebooks und PDAs, gefolgt von Policies für das Thema Zugriffsschutz im allgemeinen.

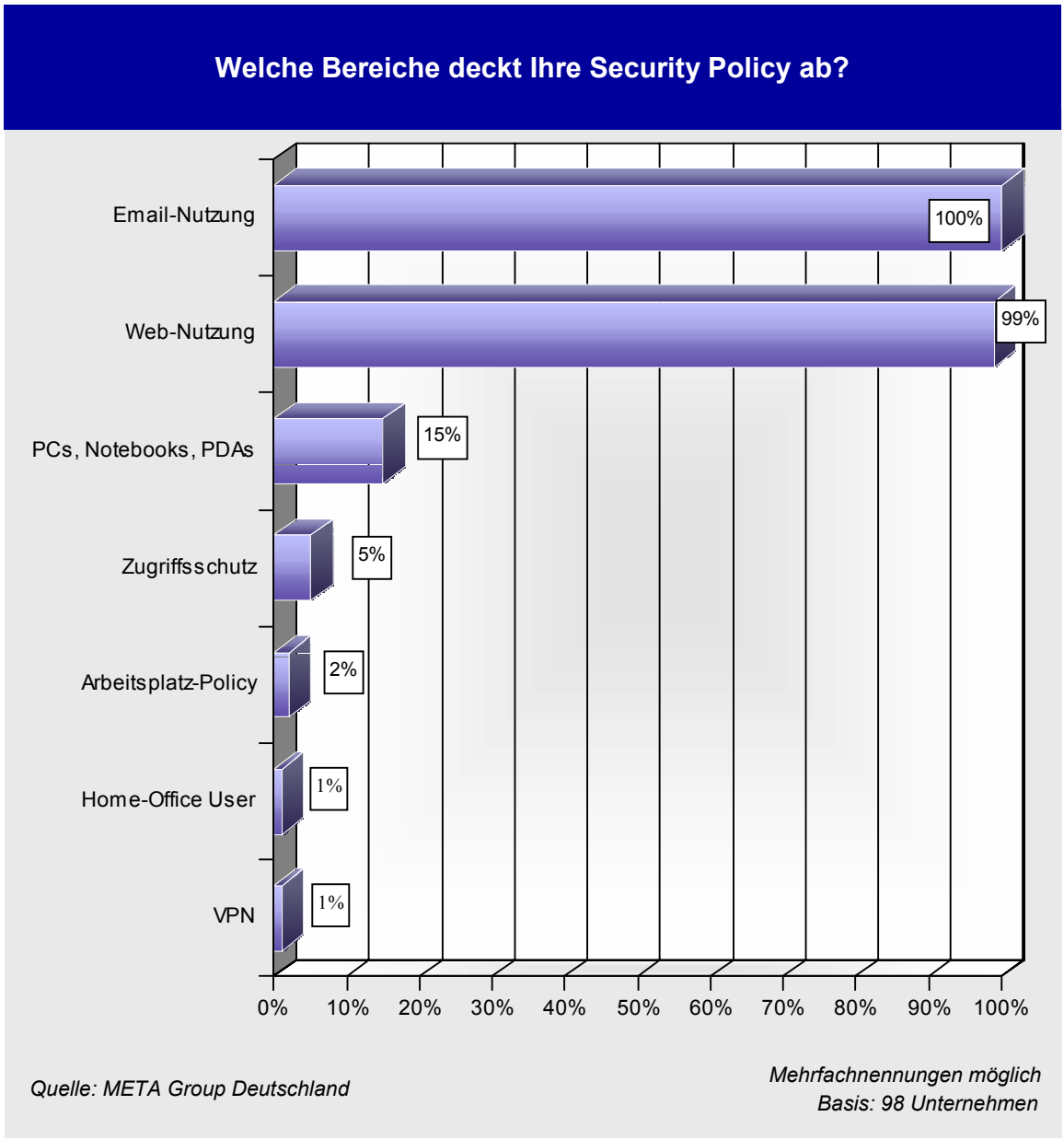


Abbildung 31: Durch die Security Policy abgedeckte Bereiche

Nach Meinung der META Group muss auf die Umsetzung der Security Policy mindestens genauso viel Augenmerk gelegt werden wie auf die bloße Definition. Die Umsetzung erfolgt dabei nicht nur technologisch, sondern vor allem auch auf Ebene von Prozessen und Verhaltensweisen.

Die befragten Unternehmen setzen ihre Security Policies – sofern solche im Unternehmen vorhanden sind – primär mittels schriftlicher Anweisungen durch, die an die Mitarbeiter verteilt werden (90 Prozent der Anwender mit Policy). Jeweils 59 Prozent der Unternehmen mit Security Policy verlassen sich zudem auf die Durchsetzung mit Hilfe fest vorkonfigurierter Systeme (auf Desktop / Server) und Informationen, die im Intranet zur Verfügung gestellt werden. Obligatorisches Training oder Web-Seminare als proaktive Mittel werden seltener eingesetzt – dasselbe gilt auch für Mitarbeiterzeitungen als Medium.

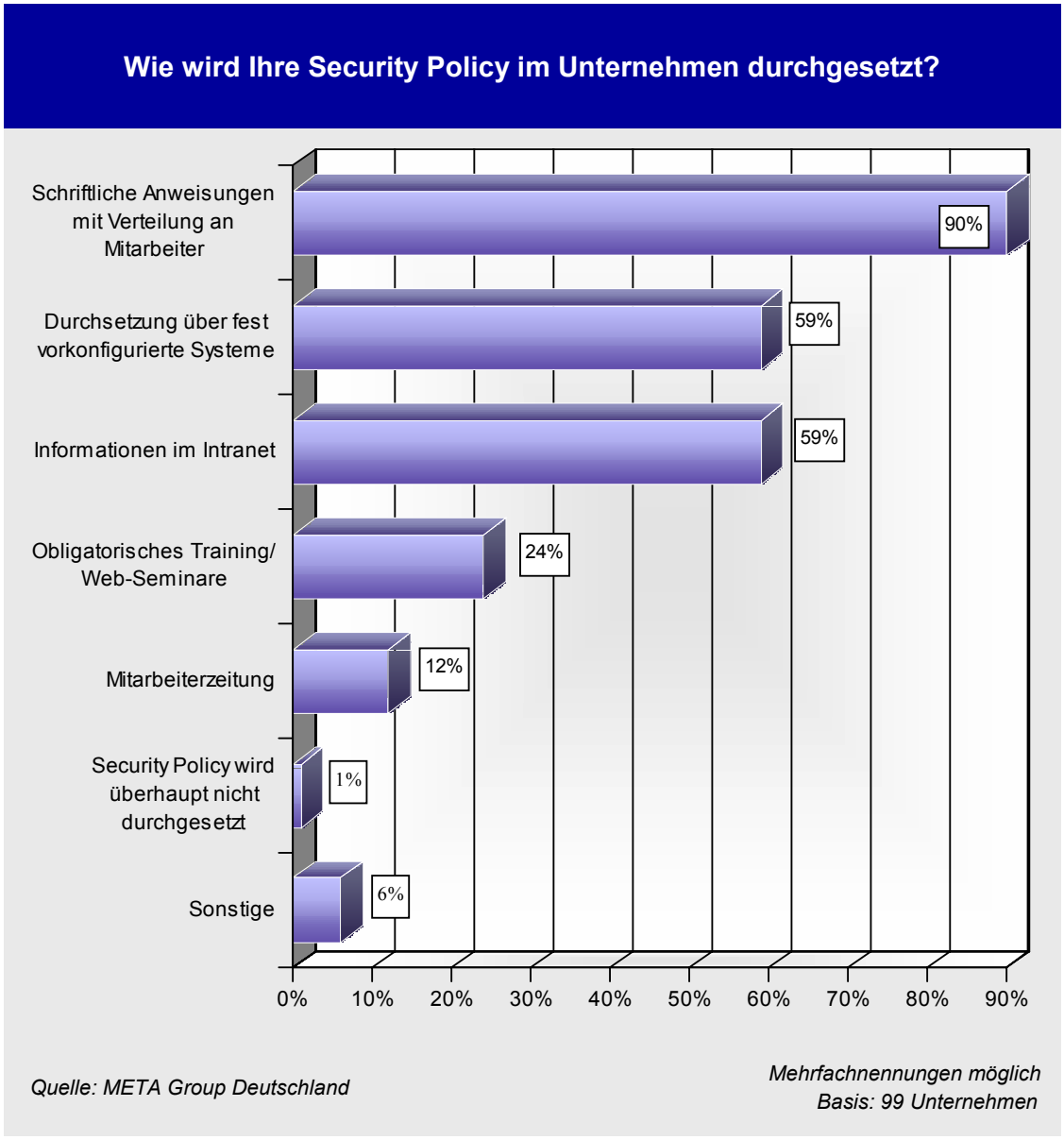


Abbildung 32: Methoden zur Durchsetzung der Security Policy

Zertifizierungen nach Security-Standards scheinen für die deutschen Anwenderunternehmen derzeit noch keine größere Bedeutung zu haben. Nur neun Prozent geben an, über eine Zertifizierung zu verfügen; 84 Prozent planen auch in Zukunft keine derartigen Aktivitäten ein.

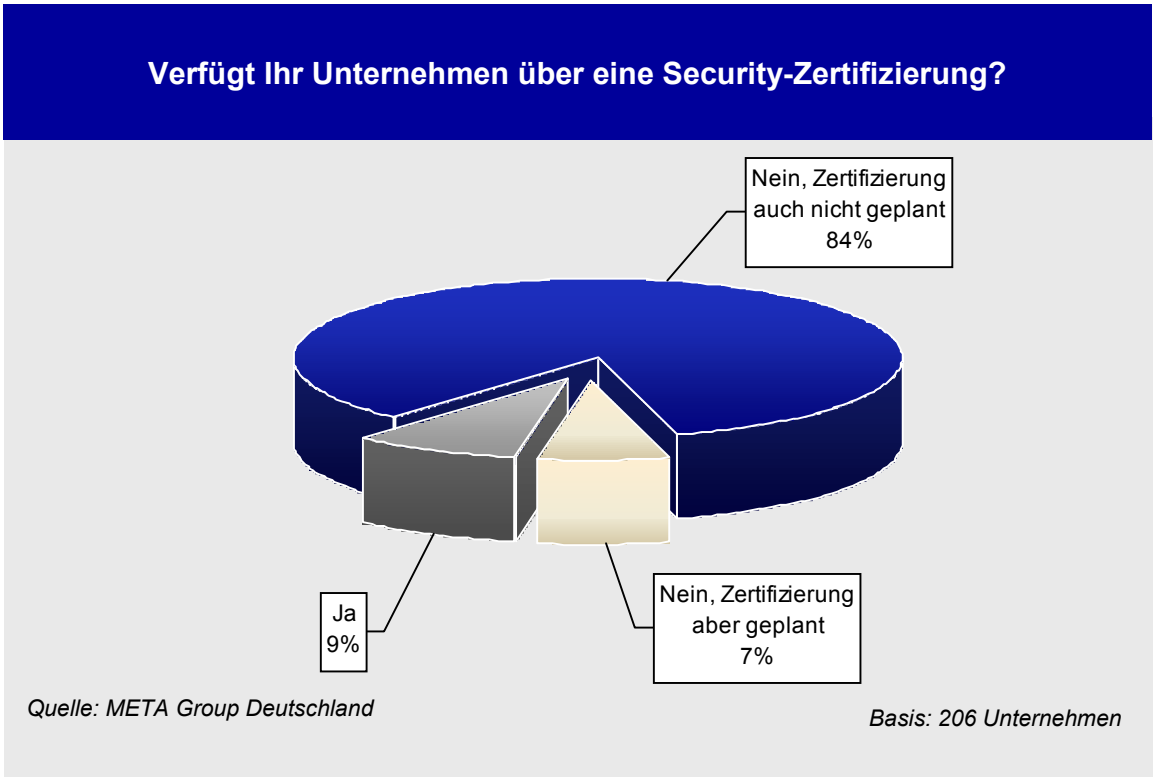


Abbildung 33: Unternehmen mit Security-Zertifizierungen

Beim Thema der Security-Zertifizierungen scheint noch viel Konfusion auf Anwenderseite zu herrschen. Nur 13 der befragten Unternehmen waren überhaupt in der Lage beziehungsweise bereit, hierzu Auskunft zu geben. 46 Prozent dieser Unternehmen geben an, nach ISO 9001 zertifiziert zu sein – einem Standard, der zunächst keinen direkten Bezug zu IT-Security hat. Über eine Zertifizierung des BSI (Bundesamt für Sicherheit in der Informationstechnik) verfügen nur drei dieser Anwender.

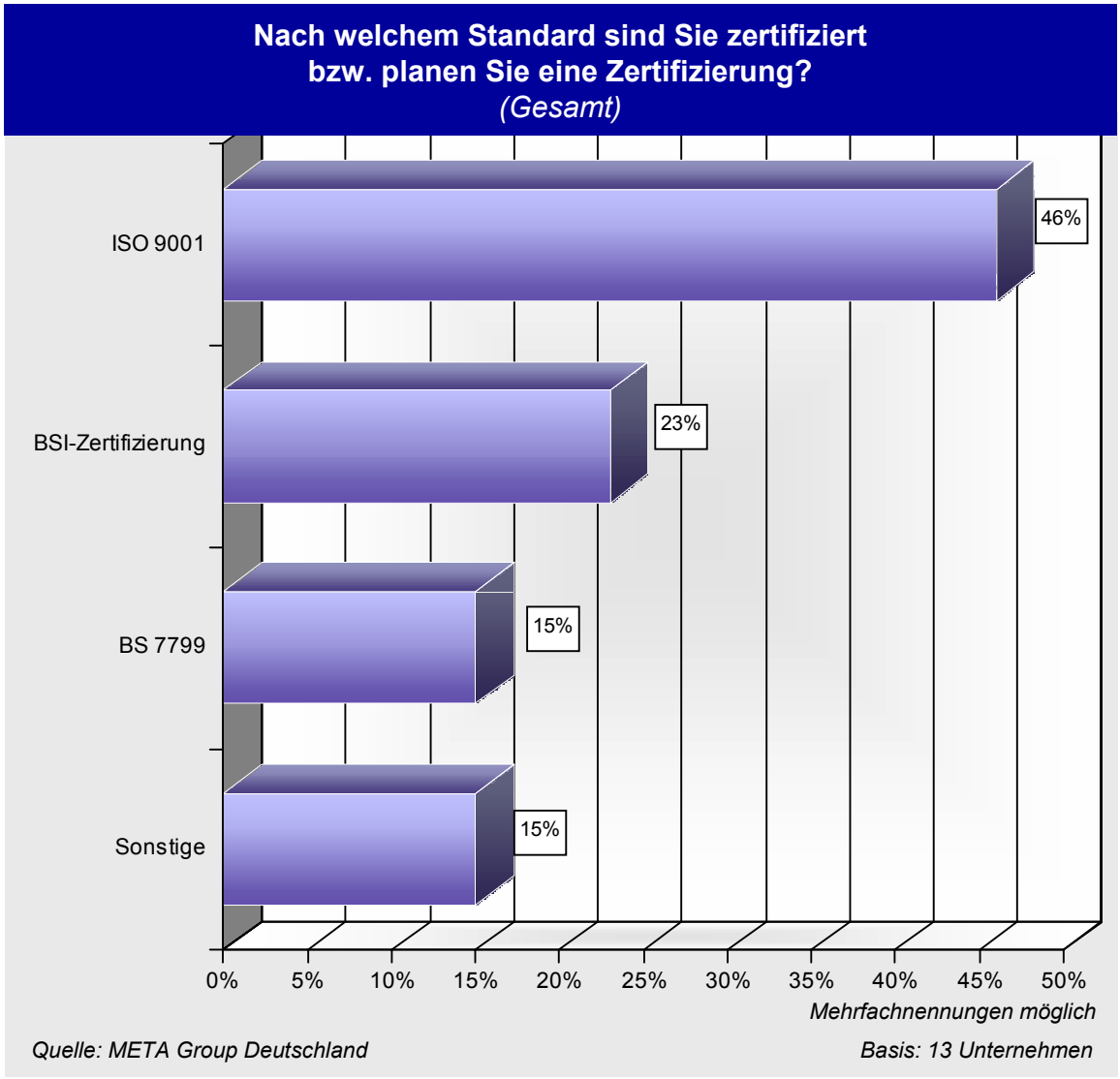


Abbildung 34: Genutzte Zertifizierungsstandards

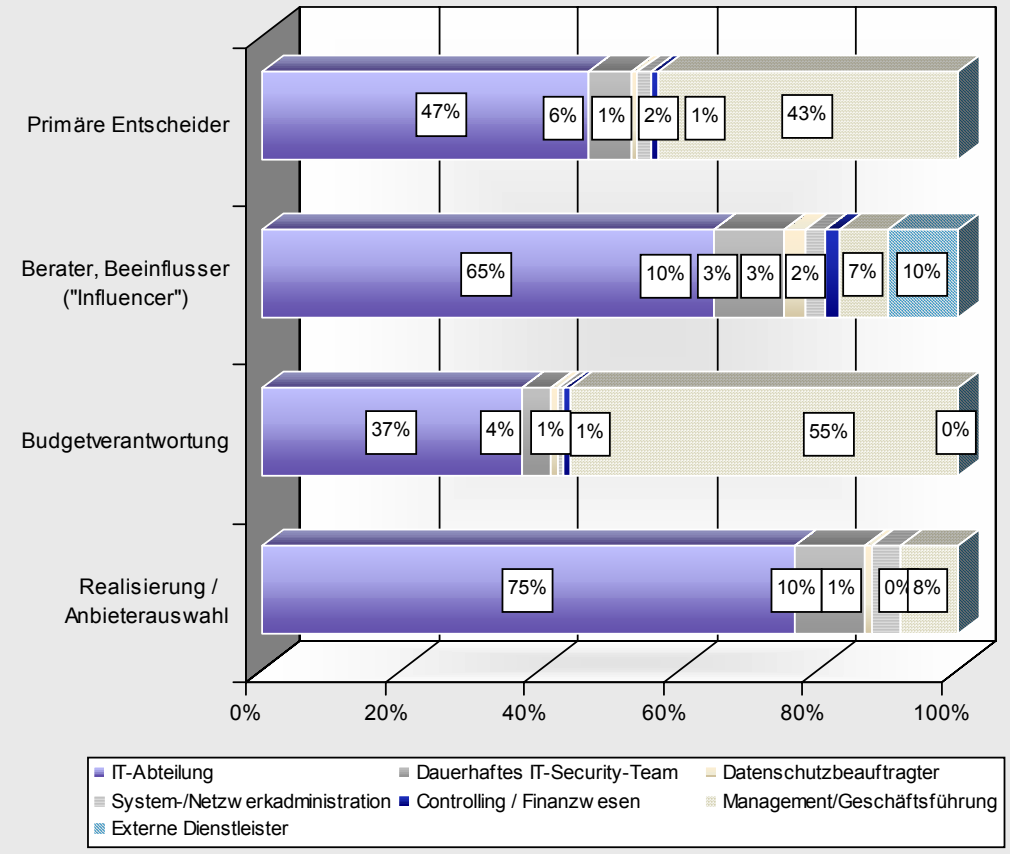
Grundsätzlich gilt es, nach Zertifizierungen von Technologien und Prozessen einerseits und Mitarbeitern andererseits zu unterscheiden. Viele der Global-2000-Unternehmen suchen eine unabhängige Bestätigung von Qualitäts- und Sicherheits-Niveaus und informieren sich in diesem Zusammenhang über technologieorientierte IT-Security-Zertifizierungen. Rein technologische Zertifizierungen (z.B. ISO 15408/Common Criteria, ITSec) gehen zwar mit einem neutralen Review einher, geben jedoch oft nur einen Anhaltspunkt für die Tiefe der Untersuchung, weniger aber für die tatsächliche "Stärke" in Bezug auf Sicherheit (ISO 15408). Außerdem gelten Zertifizierungen gewöhnlich für eine bestimmte Konfiguration, während manche üblicherweise genutzten Technologie-Features ausgeblendet werden. Implementierungs-Zertifizierungen (SysTrust/WebTrust etc.) sind punktuelle "Rückversicherungen" für die Unternehmen, welche einen akzeptablen Sicherheitsstandard im Unternehmen bestätigen sollen. Sie sind aber keinesfalls eine Garantie dafür, dass die Sicherheit auch in Zukunft fortbesteht. Damit lassen sich Technologie-Zertifizierungen zwar als grobes Security-Review nutzen, sie bieten aber keine umfassende Garantie für IT-Sicherheit. IT-Dienstleister sollten nach Meinung der META Group nichtsdestotrotz aktuelle Implementierungs-Zertifizierungen vorweisen können.

Ein weiterer Gesichtspunkt ist die Zertifizierung von Mitarbeitern. Nach Ansicht der META Group stellt bei der Einstellung neuer Security-Mitarbeiter deren Zertifizierung einen guten Anhaltspunkt dar, weist sie doch auf die Erfahrung des Bewerbers hin. Die Zertifizierung sollte dennoch nicht als primäres Auswahlkriterium dienen. Sie ist vielmehr ein gutes Mittel für die ständige Weiterentwicklung der Mitarbeiter. Es ist darauf zu achten, dass Zertifizierungen anbieterunabhängig sind und durch geeignete Organisationen unterstützt werden. Die META Group schlägt für technische Security-Fachkräfte die SANS Institute GIAC Zertifizierung vor und rät im Zusammenhang mit Policy Management und konzeptionellen Aspekten zur CISSP des International Information Systems Security Certifications Consortium. Das kürzlich angekündigte ISACA CISM Programm ist vielversprechend als Zertifizierungsprogramm für Chief Security Officers (CSO), braucht aber noch etwas Zeit, um heranzureifen.

3.2 Verteilung der Verantwortlichkeiten

Die Anwenderunternehmen wurden im Rahmen der Untersuchung zur **Verteilung der Verantwortlichkeiten** hinsichtlich einzelner Rollen im Entscheidungsprozess befragt. Als primäre Entscheider agieren mit deutlicher Mehrheit die IT-Abteilung (in 47 Prozent der Unternehmen) und das Management beziehungsweise die Geschäftsführung (in 43 Prozent der Unternehmen). Eine beratende und die Entscheidung beeinflussende Position nehmen neben der IT-Abteilung mit jeweils zehn Prozent Anteil auch dedizierte IT-Security-Teams und externe Dienstleister ein. Die Budgetverantwortung liegt hingegen wieder beim Management (in 55 Prozent der befragten Unternehmen) und bei der IT-Abteilung (37 Prozent). Geht es um die konkrete Realisierung von Maßnahmen und die Auswahl von Anbietern, liegt die Verantwortlichkeit in 75 Prozent der Unternehmen primär in der IT-Abteilung, teilweise – aber seltener – auch beim IT-Security-Team oder im Management.

Wo ist die Verantwortlichkeit des Aufgabenkomplexes IT-Security hinsichtlich Initiative, Budgetverantwortung und Realisierung angesiedelt?
(Gesamt)



Quelle: META Group Deutschland

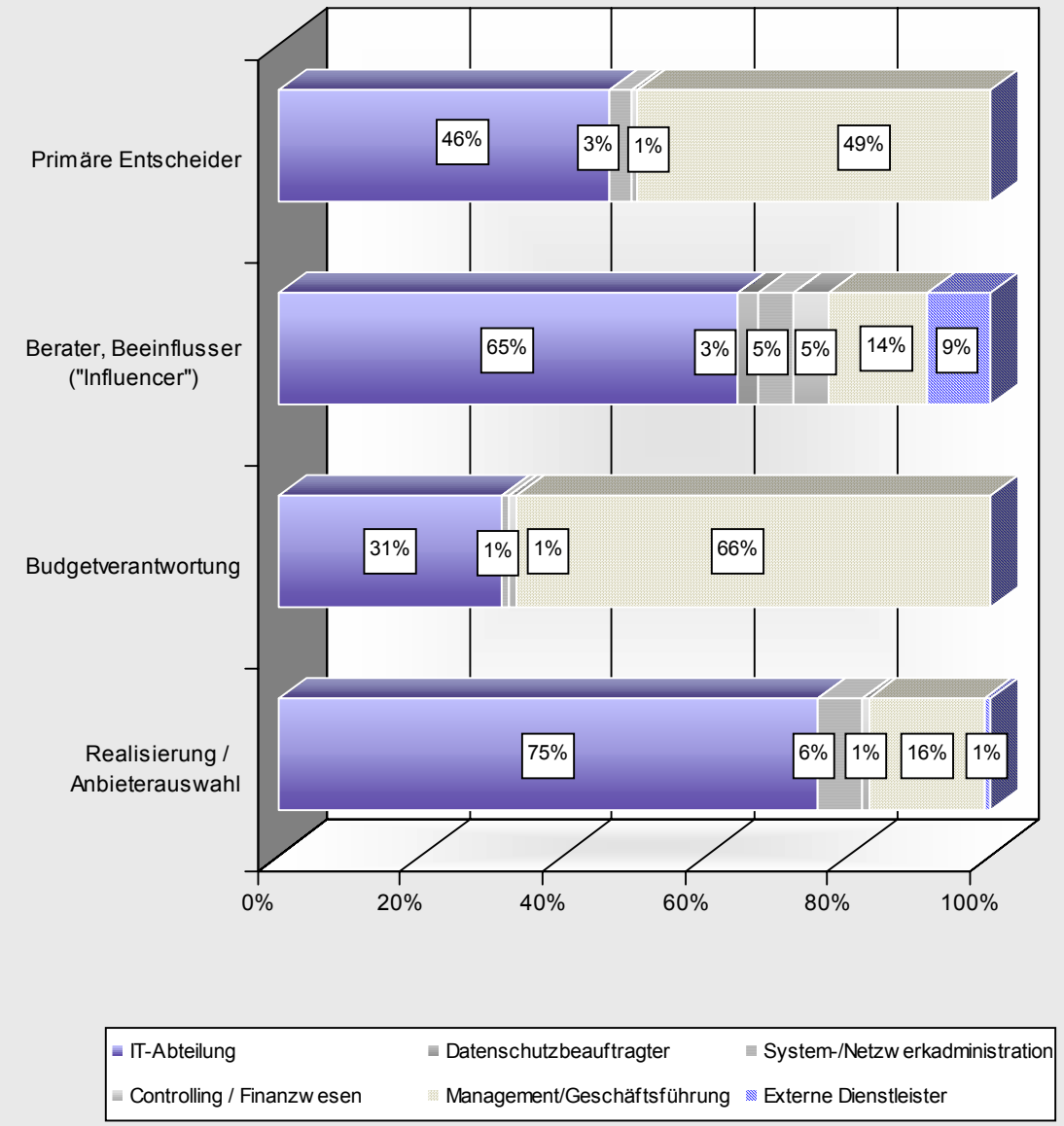
Basis: 208 Unternehmen

Abbildung 35: Verteilung der Verantwortlichkeiten im Security-Entscheidungsprozess

Die Ergebnisse zeigen, dass Anbieter von IT-Security-Lösungen oder –Dienstleistungen grundsätzlich ein „Buying Center“ adressieren müssen: Die IT-Abteilung, das IT-Security-Team sowie das Management und die Geschäftsführung sollten jeweils mit auf diese Zielgruppen maßgeschneiderten „Botschaften“ versorgt werden. Obgleich die Entscheidungsgewalt ganz in der Hand der IT- und Management-Entscheider zu liegen scheint, sind in einzelnen Lösungssegmenten auch weitere Business-Entscheider einzubeziehen. So bedürfen etwa Investitionen in Content-Security-Lösungen gegebenenfalls der Zustimmung des Betriebsrats; außerdem kommen hier Verkaufsargumente ins Spiel, die für die Rechtsabteilung von Interesse sein könnten. Zudem zeigte eine 2001 durchgeführte Untersuchung der META Group Deutschland, dass die Absicherung von spezifischen e-Business-Lösungen oftmals auch von den betreffenden „Lines of Business“ (LOBs) eingefordert wird.

Auf den folgenden Seiten ist die Verteilung der Verantwortlichkeiten in einzelnen Unternehmensgrößenklassen (Mitarbeiter) dargelegt. Hier wird deutlich, dass dedizierte IT-Security-Teams nur im gehobenem Mittelstand und bei Großunternehmen eine Rolle spielen. Kleine Unternehmen und der klassische Mittelstand verfügen typischerweise nicht über ausreichende Personalressourcen, um IT-Sicherheitsorganisationen aufzubauen. Im Mittelstand spielt dagegen die Geschäftsführung mit ihrer Entscheidungsgewalt eine ausgeprägte Rolle.

Wo ist die Verantwortlichkeit des Aufgabenkomplexes IT-Security hinsichtlich Initiative, Budgetverantwortung und Realisierung angesiedelt?
(50 bis 199 Mitarbeiter)

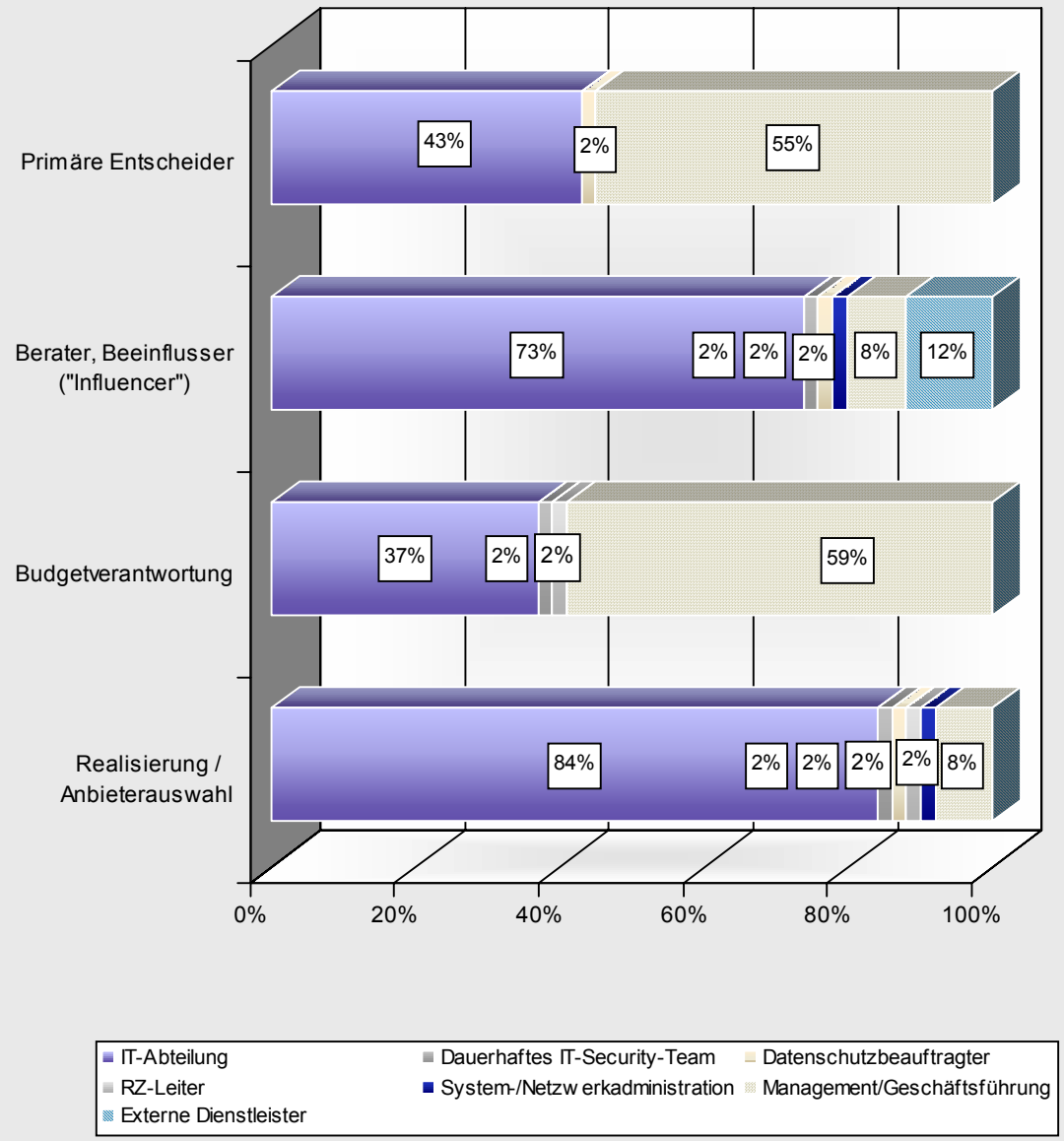


Quelle: META Group Deutschland

Basis: 67 Unternehmen

Abbildung 36: Verteilung der Verantwortlichkeiten im Entscheidungsprozess – 50-199 Mitarbeiter

Wo ist die Verantwortlichkeit des Aufgabenkomplexes IT-Security hinsichtlich Initiative, Budgetverantwortung und Realisierung angesiedelt?
(200 bis 499 Mitarbeiter)

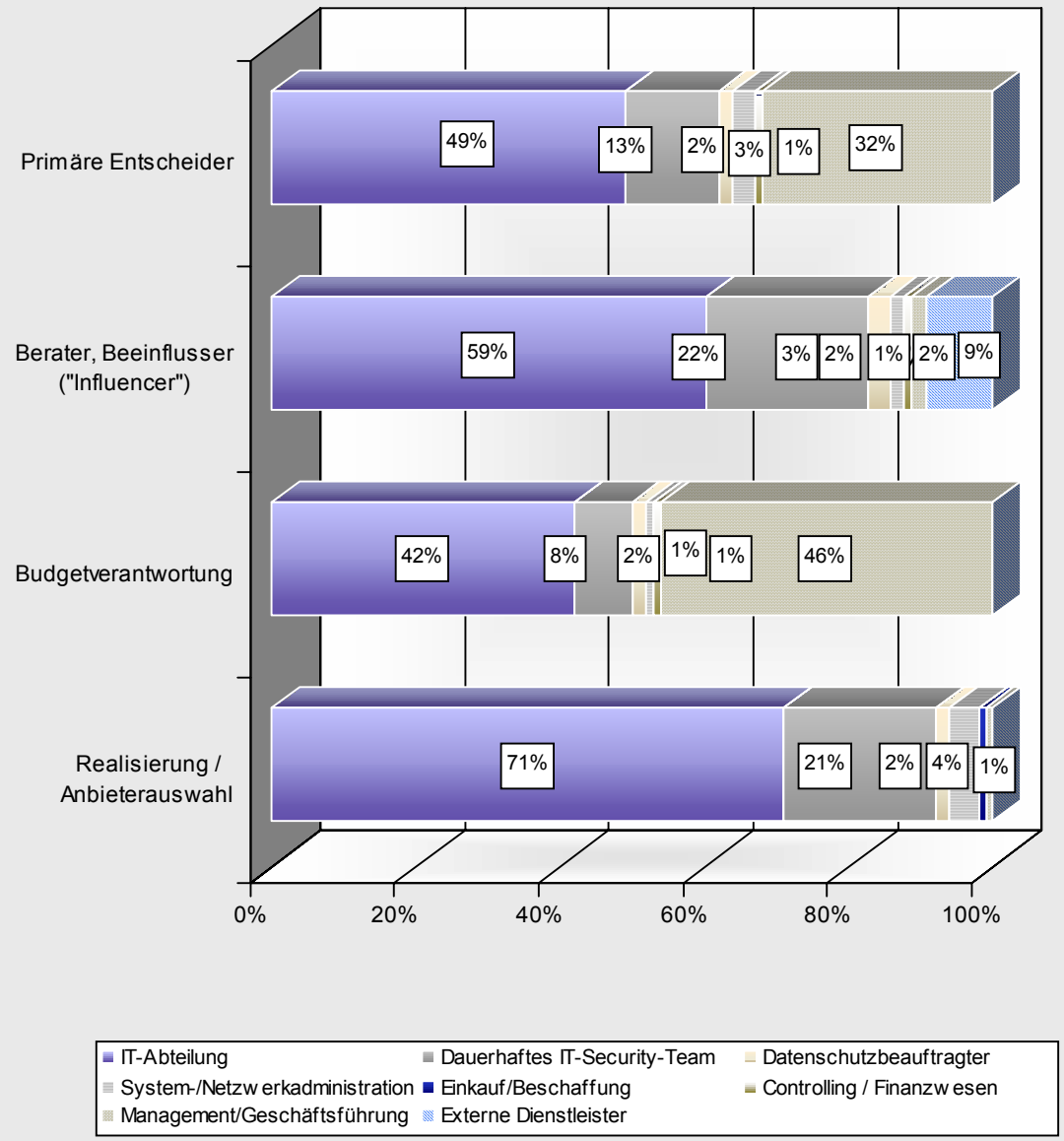


Quelle: META Group Deutschland

Basis: 49 Unternehmen

Abbildung 37: Verteilung der Verantwortlichkeiten im Entscheidungsprozess – 200-499 Mitarbeiter

Wo ist die Verantwortlichkeit des Aufgabenkomplexes IT-Security hinsichtlich Initiative, Budgetverantwortung und Realisierung angesiedelt?
(500 und mehr Mitarbeiter)



Quelle: META Group Deutschland

Basis: 92 Unternehmen

Abbildung 38: Verteilung der Verantwortlichkeiten im Entscheidungsprozess – ab 500 Mitarbeitern

3.3 Empfehlungen für Anwender

3.3.1 Strategisches Programm für Informationssicherheit

Die META Group rät Anwenderunternehmen, ein strategisches Programm für Informationssicherheit aufzusetzen. Hierdurch wird Informationssicherheit ganzheitlich adressiert und von den bislang verbreiteten Insellösungen und technologisch orientierten Projekten Abstand genommen.

Ein solches strategisches Programm für Informationssicherheit ist zunächst auf zwei bis drei Jahre angelegt. Im Vordergrund steht die Ausrichtung sämtlicher Maßnahmen der Informationssicherheit an den geschäftlichen Anforderungen. Jede Fachabteilung trägt die Verantwortung für ihren Bereich und leitet zusammen mit der Abteilung Informationssicherheit spezifische Richtlinien ab. Diese sind eingeordnet in ein Rahmenwerk für Sicherheitsrichtlinien im Unternehmen insgesamt. Weiterhin wird die Infrastruktur des Unternehmens in so genannte Domains unterteilt. Jeder Domain wird nur bis zu einem gewissen Grad vertraut. Die Fachabteilung muss entscheiden, auf welchem “Trustlevel” ihre Applikationen zu laufen haben, und muss auch die dadurch entstehenden Kosten verantworten. Die zentrale Infrastruktur wird im Allgemeinen der IT-Abteilung zugerechnet.

Entscheidend ist es, im Unternehmen nicht nur ein einziges Niveau für Informationssicherheit zu definieren, sondern abhängig von den geschäftlichen Anforderungen verschiedene Abstufungen vorzuhalten. Diese Abstufungen spiegeln sich in spezifischen Richtlinien und Technologien wider. Zusammengehalten werden die verschiedenen Komponenten durch strategische und operative Prozesse und eine Sicherheitsorganisation, die Verantwortliche auf allen Ebenen einbezieht. Entscheidend ist dabei die Kommunikation untereinander. Nicht nur müssen Maßnahmen zur Informationssicherheit umgesetzt werden, es muss auch allen klar sein, welcher Wert für das Unternehmen mit diesen Investitionen entsteht.

3.3.2 Das META Group Information Security Services Framework

Aufgaben der IT-Sicherheit können nicht einfach von heute auf morgen erledigt werden. Anwenderunternehmen sollten konkrete Maßnahmen anvisieren, die die auf einen Planungshorizont von rund drei Jahren ausgerichteten strategischen Pläne mit Leben füllen und durch geeignete „nächste Schritte“ ergänzen.

Anwenderunternehmen müssen – unabhängig von der später entwickelten Sicherheitsarchitektur – zunächst eine grundlegende Abgrenzung der Sicherheitsthematik vornehmen. Die META Group empfiehlt in diesem Zusammenhang das META Group Information Security Services Framework, das sich aus drei übergeordneten Kategorien von Sicherheitsmaßnahmen zusammensetzt: Führung und Management, operative und technische Maßnahmen sowie bereichs- beziehungsweise anwendungsspezifische Themen.

Governance und Management Services. Diese bestehen in erster Linie aus übergeordneten Prozessen, die im Verantwortungsbereich des Chief Information Security Officers (CISO) und seines

Teams liegen. Führung und Management betrifft die Entwicklung von Frameworks und Strategien, Sourcing-Strategien, Marketing in eigener Sache, Budgetplanung, Awareness und Training, formale Audits, Risk Management und Policy Management. Obgleich der CISO für viele dieser Maßnahmen voll verantwortlich ist, hat er in manchen Bereichen doch nur eingeschränkten Einfluss (zum Beispiel Risk Management). Hier beschränken sich die Aktivitäten auf die Entwicklung von Standards und Methodologien sowie die Unterstützung, wenn es um die Umsetzung von Maßnahmen seitens der „Eigentümer" von Ressourcen geht (beispielsweise Fachbereichsleiter).

Operative und technische Services. Sicherheitsarchitekturen haben bislang oftmals einen starken Fokus auf technologische Elemente, wobei die operative Umsetzung und das Management zu kurz kommen. Das META Group Information Security Services Framework unterscheidet zwischen technologischen und operativen Elementen einerseits und den Subkategorien *protect*, *detect* und *response* andererseits (siehe Abbildung 39). In die *protect*-Kategorie, wo es um den Schutz von Ressourcen geht, fallen Vertraulichkeit, Integrität und Verfügbarkeit. Sie beinhaltet Maßnahmen für das Management von Identitäten und Zugriffsrechten („Identity and Permissions Management"), Zugriffskontrolle („Isolation"), Vertraulichkeit und Integrität („Privacy and Integrity") sowie die Verfügbarkeit („Availability"). Die Kategorien *detect* und *response* schließen unter anderem Filter- und Scanning-Technologien ein und haben zudem eine starke Monitoring- und Management-Komponente.

Angewandte und domain-spezifische Sicherheits-Services. Diese „Applied Security Services" berücksichtigen einzelne Business-Anwendungen und spezifische Formen von Client-Plattformen, Netzwerken und Systemen. Die Bedeutung dieser Kategorie wird künftig stark zunehmen. Sicherheit für PDAs, drahtlose Netzwerke, Messaging und langfristig auch für kollaborative Anwendungen, Konvergenzthemen und Web Services sind Beispiele für spezifische Bereiche, auf die besonderer Fokus gelegt werden muss. Angewandte Security-Services sorgen für die Übertragung von Kernaufgaben im Bereich Security in die Praxis.

META Group Information Security Services Framework – Operational & Technical Services			
		Technical Elements	**Operational Elements**
Protection	**Identity and Permissions Management Services**	▪ **Authentication**: Radius, Certificates, Kerberos, Tokens, SmartCards, Biometrics ▪ **Authorization**: Role-based, rule-based, Web Access Control, Legacy (C/S), Single Sign-On, Attribute Certificates ▪ **Directory Services:** Enterprise, Extranet, Metadirectory	▪ **User Administration**
	Isolation Services	▪ **Access Control (Logical):** Access Control Lists, Firewalls, DMZ, Proxy/Reverse Proxy, URL Filters ▪ **Access Control (Physical):** Physical Security	▪ **Secure Management** ▪ **Configuration Management:** Secure Configuration, Configuration Maintenance ▪ **Data/Information Management**
	Privacy and Integrity Services	▪ **Encryption:** Cryptographic Protocols, Algorithms, and Methods; VPNs, PKI ▪ **Non-Repudiation:** Digital Signatures, Secure Time Stamp	▪ **Certificate/Key Life-Cycle Management:** Registration, Distribution, Revocation, Verification, Backup, Recovery
	Availability Services	▪ **Reliability:** Failover/Hot Standby, Clustering	▪ **Backup, Recovery:** Data and Configuration Backup ▪ **Business Continuity:** Alternative Methods for Conducting Business
Detection and Response	**Detection Services**	▪ **Filtering:** Antivirus, Antivandal; Intrusion Detection ▪ **Scanning:** Vulnerability Scanners, Configuration Scanners	Research, Monitoring, Logging and Log Analysis
	Response Services	▪ **Notification**	▪ **Incident Response** ▪ **Reporting** ▪ **Forensics**

Quelle: META Group

Abbildung 39: META Group Information Security Services Framework: operative / technische Services

4 Wahrnehmung von Risiken, Hemmnissen und Schäden

4.1 Sicherheits-Risiken aus Sicht der Anwenderunternehmen

Im Rahmen der vorliegenden Untersuchung wurden die Anwenderunternehmen zur Bedeutung einzelner Sicherheits-Risiken beziehungsweise Gefahrenquellen befragt, die zu entsprechendem Handlungsbedarf führen (siehe Abbildung 40). Im Vergleich zur bereits 2001 durchgeführten META Group Studie zum Thema „e-Security“ hat sich die Wahrnehmung des größten Risikofaktors nicht verändert: Auch im Jahr 2003 schätzen die Unternehmen die Gefahr durch Virenbefall und „bösartigen“ Code als eindeutig höchstes Risiko ein. Ausschlaggebend hierfür dürften unter anderem die anhaltende Präsenz entsprechender Zwischenfälle in den Medien und nicht zuletzt auch eigene nachvollziehbare negative Erfahrungen sein.

Als zweithöchstes Risiko werten die Anwender das unautorisierte Eindringen Fremder ins Unternehmensnetzwerk. Dabei denken die Befragten in erster Linie an Hacker ohne wirtschaftliche Interessen, weniger aber an gezielte Industriespionage. Zu den weiteren Risiken, die mittelmäßig bis hoch eingestuft werden, zählen die Manipulation oder Offenlegung von Transaktionen im Web und über Email sowie der Missbrauch von Benutzerrechten durch eigene Mitarbeiter („Innentäter“).

Am anderen Ende der Skala, das heißt nur als mäßiges Risiko eingestuft, befinden sich die Verbreitung illegaler oder „politisch unkorrekter“ Inhalte im Unternehmensnetzwerk und der physische Einbruch beziehungsweise Diebstahl von Hardware. Auch über neue Sicherheitsfragen, die sich durch die Nutzung drahtloser Technologien (WLAN, UMTS etc.) ergeben könnten, zerbrechen sich die Anwenderunternehmen derzeit weniger den Kopf. Neue Sicherheitsfragen durch die Nutzung von Web Services spielen noch eine mäßige Rolle, werden nach Einschätzung der META Group aber künftig – mit der Verbreitung von Web Services – zunehmend wichtiger.

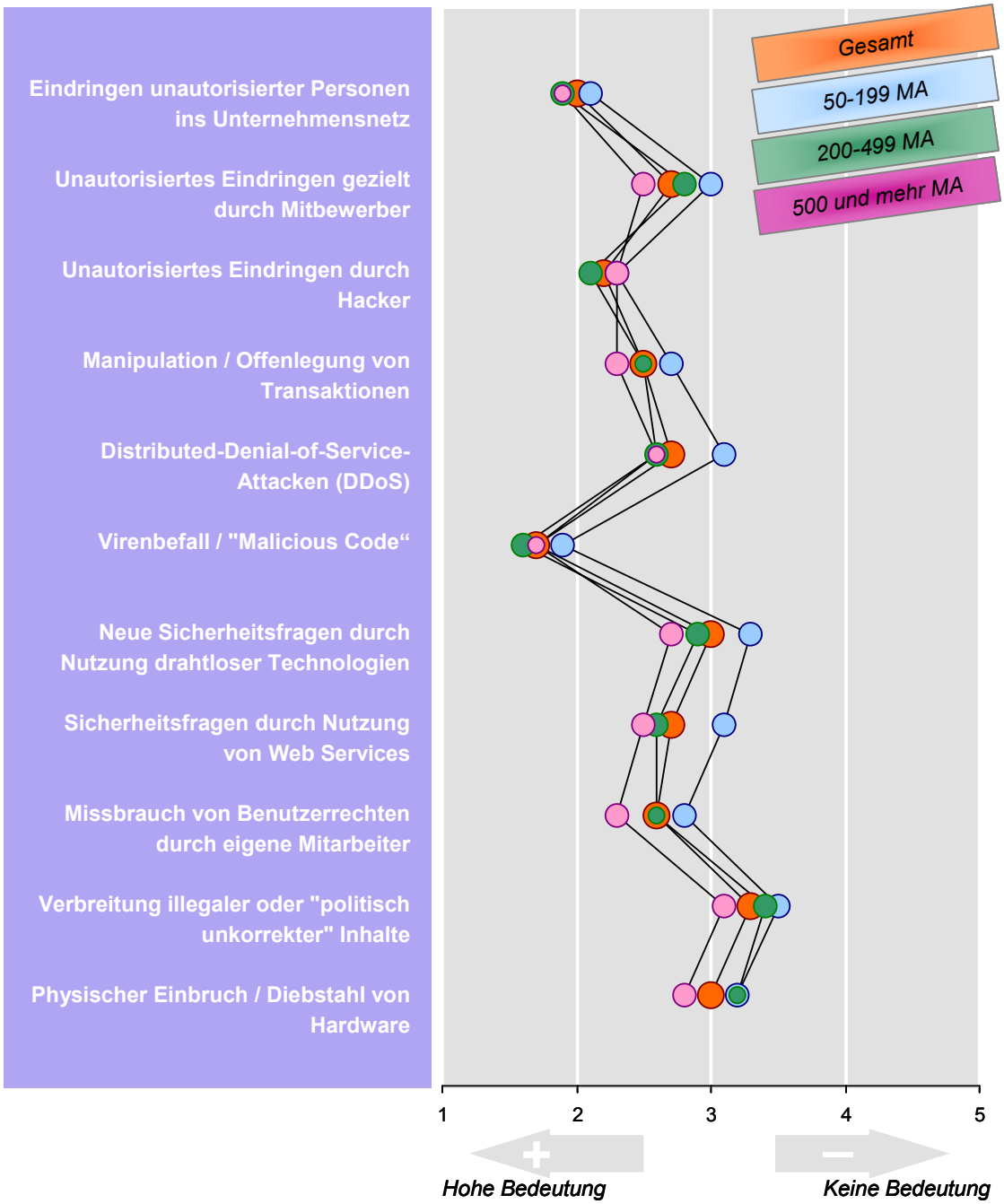
Die Analyse nach Unternehmensgröße zeigt, dass das „Ranking“ der einzelnen Risikofaktoren über alle Größenklassen hinweg identisch ist (siehe Abbildung 40). Allerdings erweisen sich kleine Mittelständler als weniger risikobewusst. Abgesehen von den Top 2-Themen – Virenbefall und Hacker – bewegt sich die durchschnittliche Risikobewertung um den Wert 3, das heißt „mittelmäßig“.

Auch im Branchenvergleich gibt es keine gravierenden Unterschiede in der Reihenfolge der wichtigsten Risiken (siehe Abbildung 41ff). Nur im Mittelfeld und auf den hinteren Rängen verschiebt sich die Gewichtung einzelner Faktoren. So macht sich die prozessorientierte Fertigung verhältnismäßig viele Sorgen um den physischen Diebstahl von Hardware, während sich Telekommunikationsdienstleister, Logistikunternehmen und die Utility-Branche überdurchschnittlich vor Distributed-Denial-of-Service-Attacken (DDoS) fürchten. Der Dienstleistungssektor erweist sich generell als sehr sensibel in punkto Risiken, im Gegensatz zum Handel. In der Natur der Finanzdienstleistungsbranche liegt die hohe Sorge um die Manipulation oder Offenlegung von Transaktionen sowie um potenzielle “Innentäter”. Etwas aus dem Rahmen fällt die öffentliche Hand: Dort werden zwar Hacker und Virenbefall ebenfalls

als gefährlich eingestuft, unsichere drahtlose Technologien spielen hingegen fast gar keine Rolle – ebenso Industriespionage, die für Behörden im engeren Sinne ohnehin nicht relevant ist.

Insgesamt lässt sich eine Korrelation zwischen der Bewertung einzelner Risiken, den tatsächlich entstandenen Schäden (siehe 4.3) und den Entscheidungsgrundlagen für IT-Security-Investitionen (siehe Kapitel 5.1) feststellen. So führen etwa Virenattacken typischerweise zu Systemausfällen und Datenverlust - den besonders häufig aufgetretenen Schäden bei den befragten Unternehmen – und in der Vergangenheit aufgetretene Schäden wiederum stellen eine wichtige Entscheidungsgrundlage für künftige Security-Investitionen dar. Nach Meinung der META Group muss bei der Betrachtung des Sicherheits-Bewusstseins der deutschen Unternehmen zwischen einzelnen Themenbereichen differenziert werden. So liegt hinsichtlich der “Mainstream”-Themen (z.B. Viren) heute bereits ein hohes Bewusstsein vor. Bei neueren Themen wie etwa der Sicherheit von Web Services oder mobilen Systemen ist die “Drohkulisse” noch nicht so stark durch entsprechende Erfahrungswerte untermauert. Entsprechend gering ist hier auch die “Awareness”. Dennoch stellen dortige Sicherheitslücken eine erhebliche Gefahr für die Anwenderunternehmen dar. Anbieter stehen damit auch in Zukunft vor der Herausforderung, für neue Themen geeignete Maßnahmen zur Erhöhung des Sicherheitsbewusstseins bei Anwenderunternehmen durchzuführen.

Wie hoch schätzen Sie die Bedeutung folgender Sicherheits-Risiken als treibende Faktoren für künftige Security-Investitionen (Datenschutz) ein?

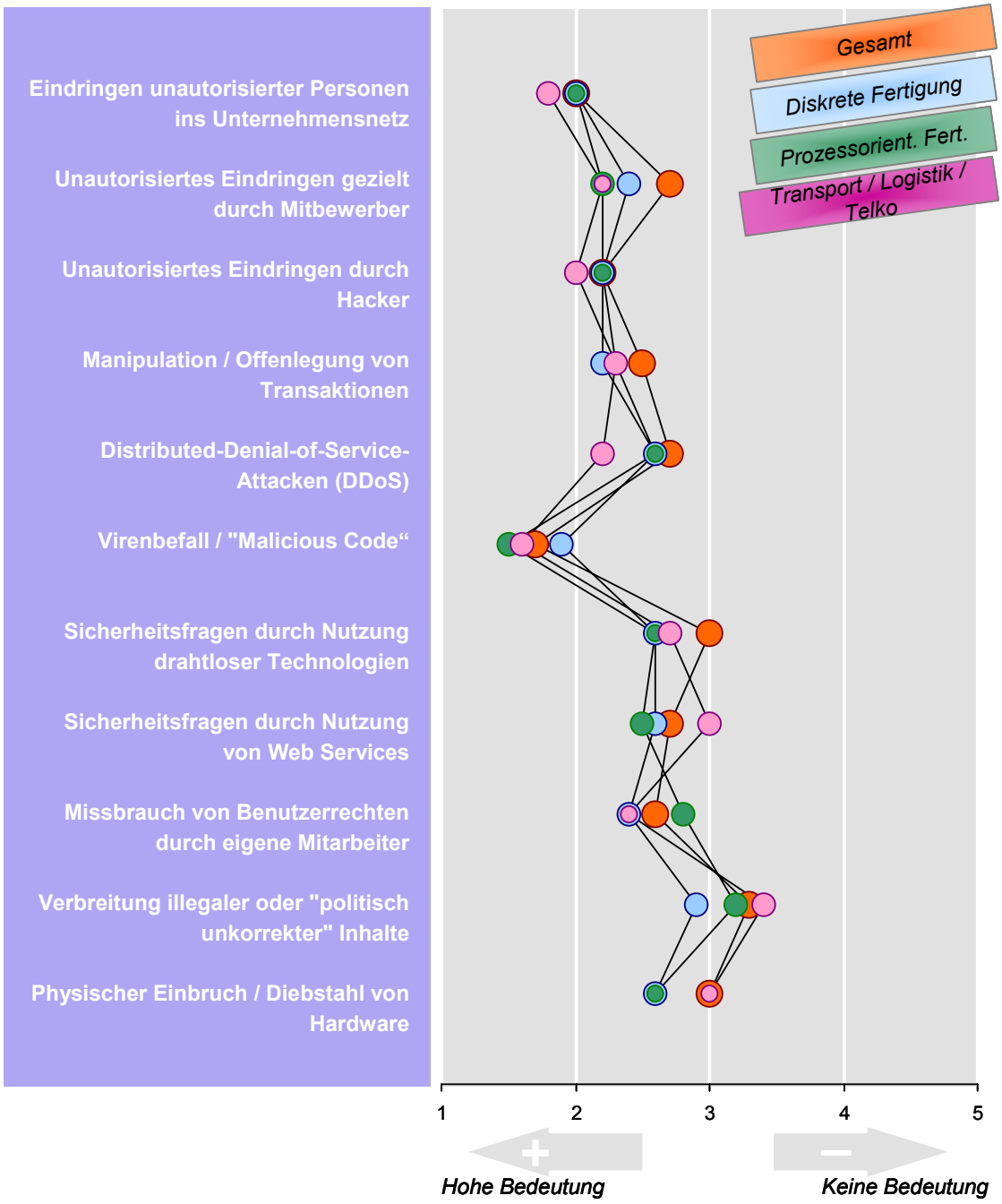


Quelle: META Group Deutschland

Basis: Gesamt: 209; 50-199: 67; 200-499: 50; 500 und mehr: 92 Unternehmen

Abbildung 40: Einschätzung von Sicherheitsrisiken (nach Unternehmensgröße)

Wie hoch schätzen Sie die Bedeutung folgender Sicherheits-Risiken als treibende Faktoren für künftige Security-Investitionen (Datenschutz) ein? [1]

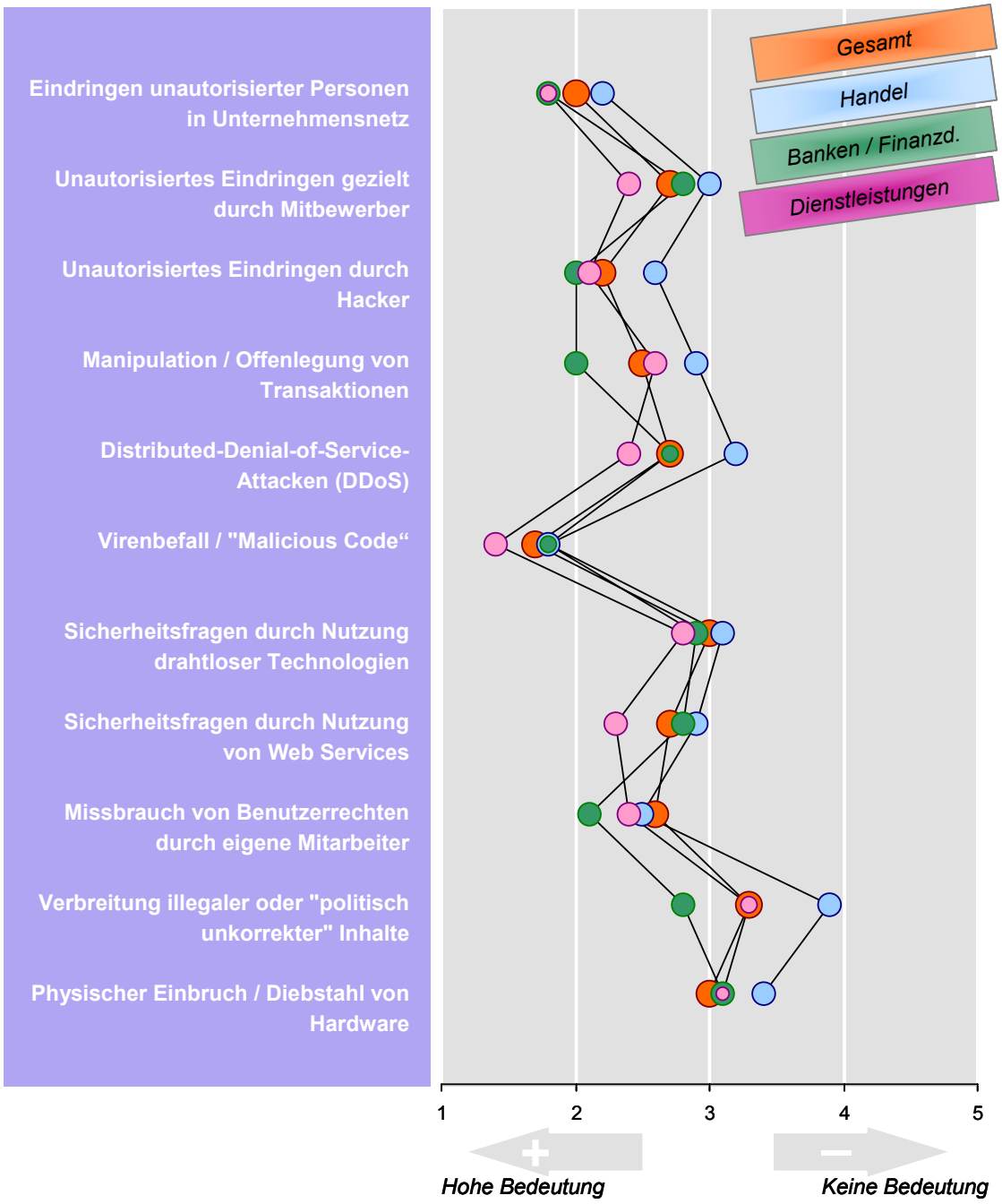


Quelle: META Group Deutschland

Basis: Gesamt: 209; Diskrete F.: 34; Prozess: 31; Transport: 27 Unternehmen

Abbildung 41: Einschätzung von Sicherheitsrisiken - nach Branchen (1)

Wie hoch schätzen Sie die Bedeutung folgender Sicherheits-Risiken als treibende Faktoren für künftige Security-Investitionen (Datenschutz) ein? [2]

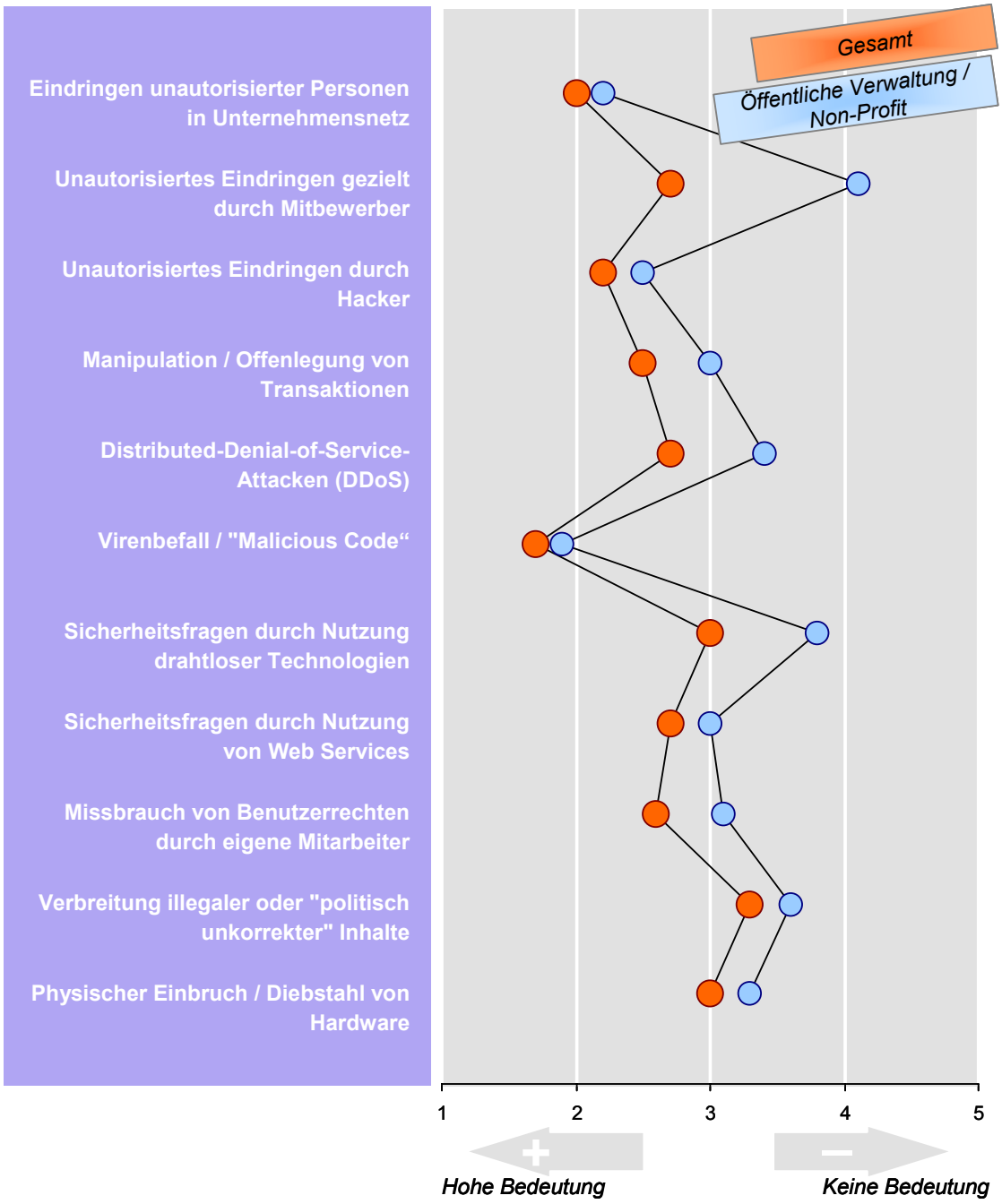


Quelle: META Group Deutschland

Basis: Gesamt: 209; Handel: 25; Banken: 26; Dienstleistungen: 31 Unternehmen

Abbildung 42: Einschätzung von Sicherheitsrisiken - nach Branchen (2)

Wie hoch schätzen Sie die Bedeutung folgender Sicherheits-Risiken als treibende Faktoren für künftige Security-Investitionen (Datenschutz) ein? [3]



Quelle: META Group Deutschland

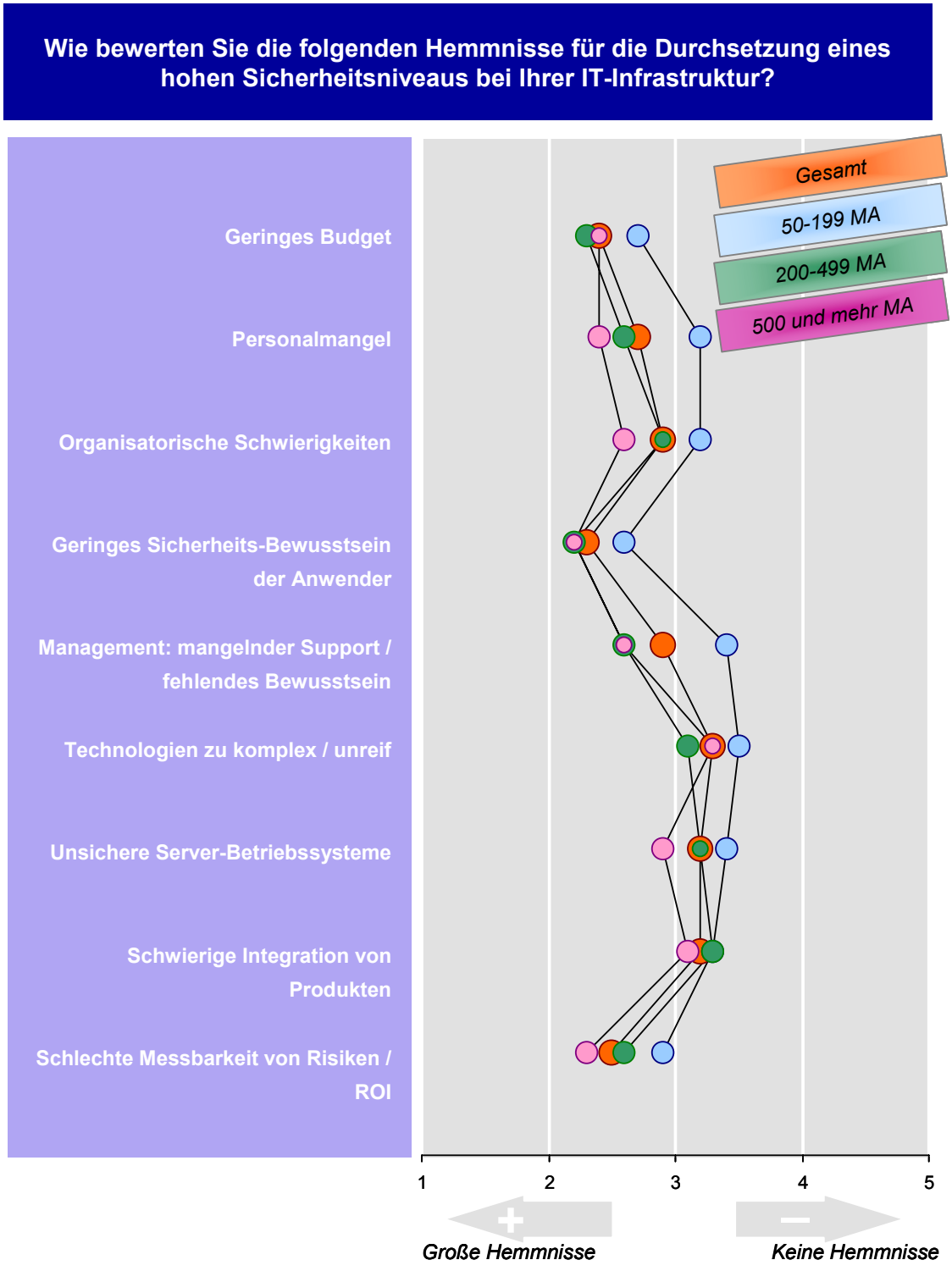
Basis: Gesamt: 209; Öffentl.: 35 Unternehmen

Abbildung 43: Einschätzung von Sicherheitsrisiken - nach Branchen (3)

4.2 Hemmnisse für IT-Sicherheit

Nach Einschätzung der befragten Unternehmen stellt das geringe Sicherheitsbewusstsein der Anwender im Unternehmen das größte Hemmnis für IT-Sicherheit dar. Außerdem fühlen sich die Verantwortlichen durch geringe Security-Budgets und die schlechte Messbarkeit von Risiken beziehungsweise des Return on Investment (ROI) behindert, gefolgt vom klassischen Thema „Personalmangel“. Als weniger ausschlaggebend werden hingegen unreife Sicherheitstechnologien, unsichere Server-Betriebssysteme und die gegebenenfalls schwierige Integration von unterschiedlichen Produkten erachtet. Damit wird deutlich, dass die wahren Hemmnisse aus Sicht der Anwenderunternehmen nicht in erster Linie im technischen Bereich liegen, sondern vielmehr im Umfeld von Ressourcen, Prozessen und „weichen“ Faktoren.

Erwähnenswert ist, dass kein Hemmfaktor als „sehr hoch“ eingestuft wurde. Nach Einschätzung der META Group liegt dies unter anderem daran, dass rechtliche Rahmenbedingungen die wichtigste Entscheidungsgrundlage für Investitionen in IT-Sicherheit darstellen (siehe auch Kapitel 5.1). Damit handelt es sich beim IT-Security-Budget um einen Posten, der auch bei angespannten wirtschaftlichen Gegebenheiten nicht beliebig gekürzt werden kann – auch die primären Hemmnisse scheinen nicht so gravierend zu sein, dass sie Maßnahmen der IT-Sicherheit in hohem Umfang gefährden.



Quelle: META Group Deutschland

Basis: Gesamt: 208; 50-199 MA: 67; 200-499 MA: 49; 500 und mehr MA: 92 Unternehmen

Abbildung 44: Hemmnisse für IT-Security

4.3 Schäden durch sicherheitsrelevante Zwischenfälle

Im Rahmen der vorliegenden Untersuchung wurden die Anwenderunternehmen dazu befragt, welche **Schadensarten** im eigenen oder bei bekannten Unternehmen – insbesondere in der eigenen Branche - in den letzten 24 Monaten entstanden waren. Lediglich 26 Prozent der Unternehmen geben dabei an, dass keine Schäden entstanden beziehungsweise bekannt sind (vergleiche Abbildung 45).

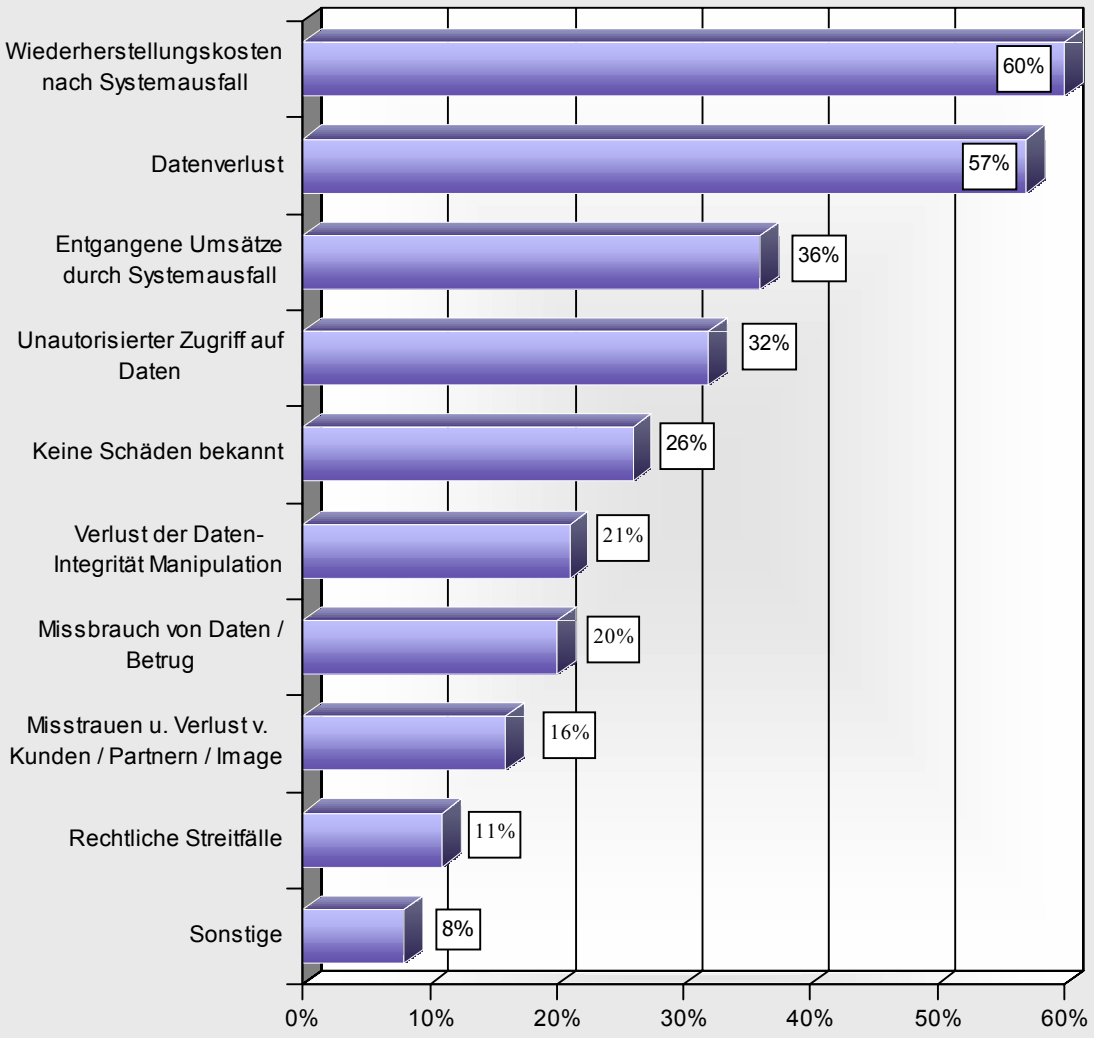
Über die Hälfte der Unternehmen berichtet hingegen von Zwischenfällen, die Wiederherstellungskosten nach einem Systemausfall oder den Verlust von Daten verursachten. Dies sind in der Regel Schäden, die vergleichsweise schnell erkennbar und messbar sind.

Jeweils rund ein Drittel der Befragten klagt über entgangene Umsätze durch Systemausfälle und den unautorisierten Zugriff auf Daten (Vertraulichkeitsverlust). Rund ein Fünftel der Unternehmen litt unter der Manipulation oder dem Missbrauch von Daten (Betrug). Der potenzielle Verlust von Partnern und Kunden bzw. Imageschädigung sowie rechtliche Streitfälle wurden seltener registriert.

Diese „Rangfolge“ der Schadensarten darf nicht darüber hinwegtäuschen, dass in einzelnen Bereichen mit einer erheblichen Dunkelziffer zu rechnen ist. So sind manche der seltener genannten Schäden vom betroffenen Unternehmen schwer zu registrieren. Andere Schäden wiederum, wie etwa ein Imageverlust, lassen sich kaum monetär bewerten. Nicht zuletzt liegen hier Aussagen zur Häufigkeit unterschiedlicher Schadensarten vor, nicht aber zur Relevanz beziehungsweise Höhe der entstandenen Schäden.

Insgesamt lässt sich feststellen, dass trotz aller Vorkehrungen ein hoher Anteil an Unternehmen von sicherheitsrelevanten Zwischenfällen betroffen ist. Eine zusätzliche Analyse zeigt, dass selbst bei Banken, Finanzdienstleistern und Versicherungen, wo teilweise mit sehr sensitiven Daten umgegangen wird, in 31 Prozent der Fälle ein unautorisierter Zugriff auf Daten festgestellt wurde.

Welche Schadensarten sind Ihrem Wissen nach in Ihrem eigenen oder Ihnen bekannten Unternehmen in den letzten 24 Monaten entstanden?
(Gesamt)



Mehrfachnennungen möglich

Quelle: META Group Deutschland

Basis: 209 Unternehmen

Abbildung 45: Entstandene Schäden durch sicherheitsrelevante Zwischenfälle

5 Investitionsplanung für IT-Security

5.1 Entscheidungsgrundlagen

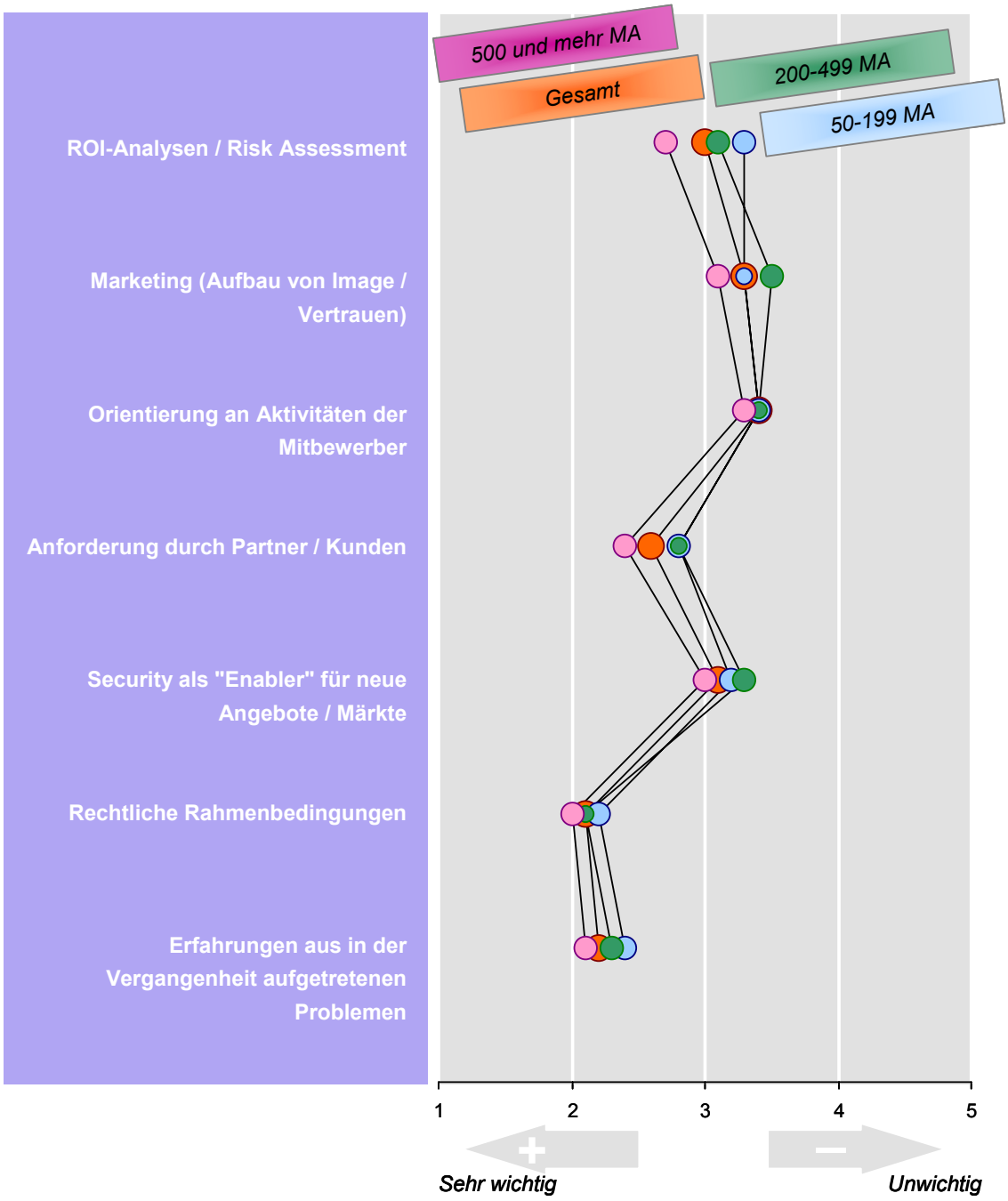
Die befragten Anwenderunternehmen nennen rechtliche Rahmenbedingungen als wichtigste Entscheidungsgrundlage für die Höhe der IT-Security-Investitionen, dicht gefolgt von Erfahrungswerten aus vergangenen Sicherheitsproblemen im Unternehmen. Außerdem orientieren sich die Unternehmen an den Anforderungen der Partner und Kunden an IT-Sicherheit. ROI-Analysen und Risk Assessment werden primär durch Unternehmen mit mindestens 500 Mitarbeitern als Entscheidungsgrundlage herangezogen (siehe Abbildung 46 ff).

Damit stellt sich das IT-Security-Budget als relativ fixe Größe dar, die nur in begrenztem Umfang Gegenstand von Kürzungen sein kann. Es wird gleichzeitig deutlich, dass die Anwender bei der Entscheidungsfindung in der Regel keinen proaktiven Ansatz verfolgen. IT-Security wird seltener als „Enabler“ für neue Angebote oder die Erschließung neuer Märkte gesehen, sondern vielmehr als Zwang, der aus Anforderungen von Institutionen, Partnern und Kunden resultiert. Der hohe Stellenwert rechtlicher Rahmenbedingungen, wie etwa Basel II, KonTraG, das Bundesdatenschutzgesetz und diverse EU-Direktiven, wird nach Meinung der META Group mittelfristig dazu führen, dass auch die Bedeutung des Risk Assessments steigen wird. Dieses dürfte künftig eine wichtige Komponente für die Umsetzung etwa von Basel II bilden. Kernelemente sind die Erfassung aller potenziell betroffenen “Assets” im Unternehmen, die Wahrscheinlichkeit, dass sie durch sicherheitsrelevante Zwischenfälle bedroht beziehungsweise getroffen werden, sowie die Höhe des im Ernstfall resultierenden Schadens. Für die “exakte” Messung sowohl der Risiken als auch der potenziellen Schäden besteht heute jedoch in der Regel keine ausreichende Datengrundlage. Die Anwenderunternehmen haben dies erkannt und sehen die schlechte Messbarkeit von Risiken und ROI als wesentliches Hemmnis an (siehe Kapitel 4.2). Anwenderunternehmen sollten dennoch Ansätze wie Risk Assessment nutzen, um die Sicherheitsprioritäten und –anforderungen in einzelnen Unternehmensbereichen auszuloten.

Die monetäre Bewertung des Nutzens von IT-Sicherheit ist zumeist schwierig. Für viele Bereiche der IT-Security ist der Return on Investment (ROI) schwer quantitativ nachweisbar. Daher wird der ROI durch Sicherheitslösungen auch nicht als primäre Entscheidungsgrundlage herangezogen – vor allem nicht beim Mittelstand. Dennoch macht es für Anbieter von Lösungen Sinn, den ROI im Sinne des „Nutzens“ dem Kunden gegenüber zu kommunizieren. Die ROI-Analyse sollte aber glaubwürdig und für den Kunden leicht nachvollziehbar sein; die ROI-Argumentation allein reicht für die Kaufentscheidung selten aus und sollte daher primär als zusätzliches Verkaufsargument des Anbieters dienen. Den Anwenderunternehmen sei in diesem Zusammenhang geraten, ROI-Berechnungen nicht zur Beruhigung des Gewissens zu „missbrauchen“. IT-Security ist keine Kostenstelle mit „Nice-to-Have“-Charakter, sondern sie ist vielmehr Garant für die Sicherung wichtiger Unternehmensprozesse. Der Nutzen lässt sich weniger in Form einer mathematisch exakten Zahl berechnen, sondern sollte vielmehr als eine Kombination aus quantifizierbarem Nutzen (Einsparungen, Prozessverbesserungen),

quantifizierbarer Risikominimierung (sofern zuvor eine Risikoanalyse erfolgte) und eher subjektiv wahrgenommener Verbesserungen der Informationssicherheit betrachtet werden.

Wie wichtig sind die folgenden Entscheidungsgrundlagen bzw. Faktoren für die Höhe der IT-Security-Investitionen in Ihrem Unternehmen?



Quelle: META Group Deutschland

Basis: Gesamt: 207; 50-199 MA: 67; 200-499 MA: 49; 500 und mehr MA: 91 Unternehmen

Abbildung 46: Entscheidungsgrundlagen für die Höhe der IT-Security-Investitionen

Während sich die Branche der prozessorientierten Fertigungsunternehmen bei der Budgetplanung relativ stark an Erfahrungswerten aus der Vergangenheit orientiert, kommen bei Logistikern, bei Telekommunikationsdienstleistern und bei Energieversorgern die Kundenanforderungen stärker zum Tragen. Hier wird IT-Sicherheit in gewissem Umfang auch als „Enabler“ für das Geschäft wahrgenommen.

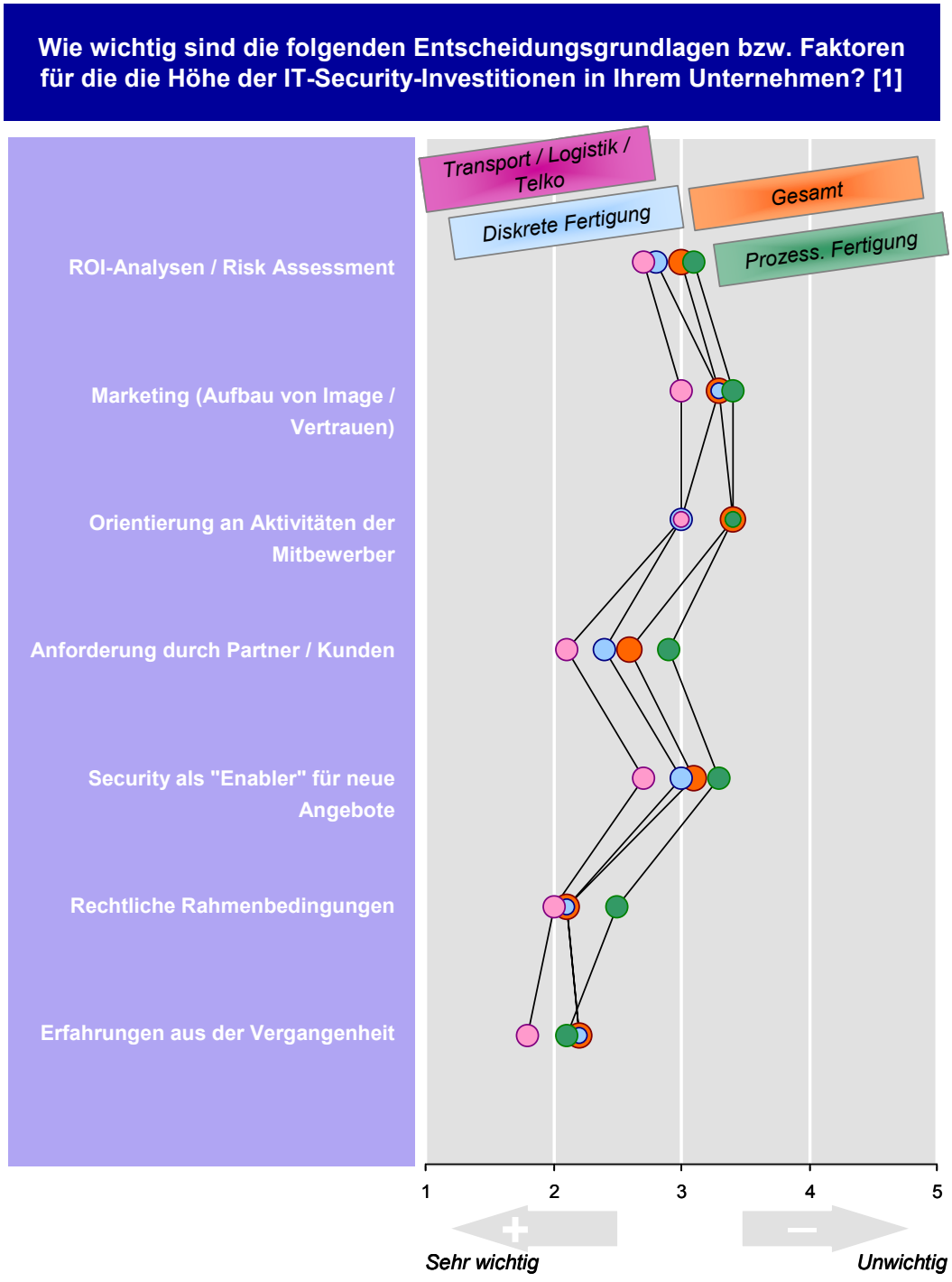


Abbildung 47: Entscheidungsgrundlagen für die Höhe der IT-Security-Investitionen – Branchen (1)

Für Banken spielen der Aufbau von Image und Vertrauen, resultierend auch aus den Anforderungen der Partner und Kunden, sowie die rechtlichen Rahmenbedingungen eine überdurchschnittlich große Rolle.

Abbildung 48: Entscheidungsgrundlagen für die Höhe der IT-Security-Investitionen – Branchen (2)

In der Natur der öffentlichen Hand liegt es, dass vor allem rechtliche Rahmenbedingungen das Fundament für Entscheidungen über Security-Investitionen bilden. Während vergangene Erfahrungen mit sicherheitsrelevanten Zwischenfällen ebenfalls noch eine Rolle spielen, erachten die befragten Institutionen alle anderen Faktoren als relativ unwichtig – einschließlich der ROI- und Risiko-Analysen.

Wie wichtig sind die folgenden Entscheidungsgrundlagen bzw. Faktoren für die die Höhe der IT-Security-Investitionen in Ihrem Unternehmen? [3]

Quelle: META Group Deutschland

Basis: Gesamt: 207; Öffentl. Verw.: 35 Unternehmen

Abbildung 49: Entscheidungsgrundlagen für die Höhe der IT-Security-Investitionen – Branchen (3)

5.2 Budgetplanung

Die durchschnittlichen IT-Budgets der befragten Unternehmen sind 2003 im Vergleich zum Vorjahr um rund sechs Prozent gesunken. Sollte an der aktuellen Planung für 2004 festgehalten werden, werden die IT-Budgets im kommenden Jahr nahezu konstant bleiben.

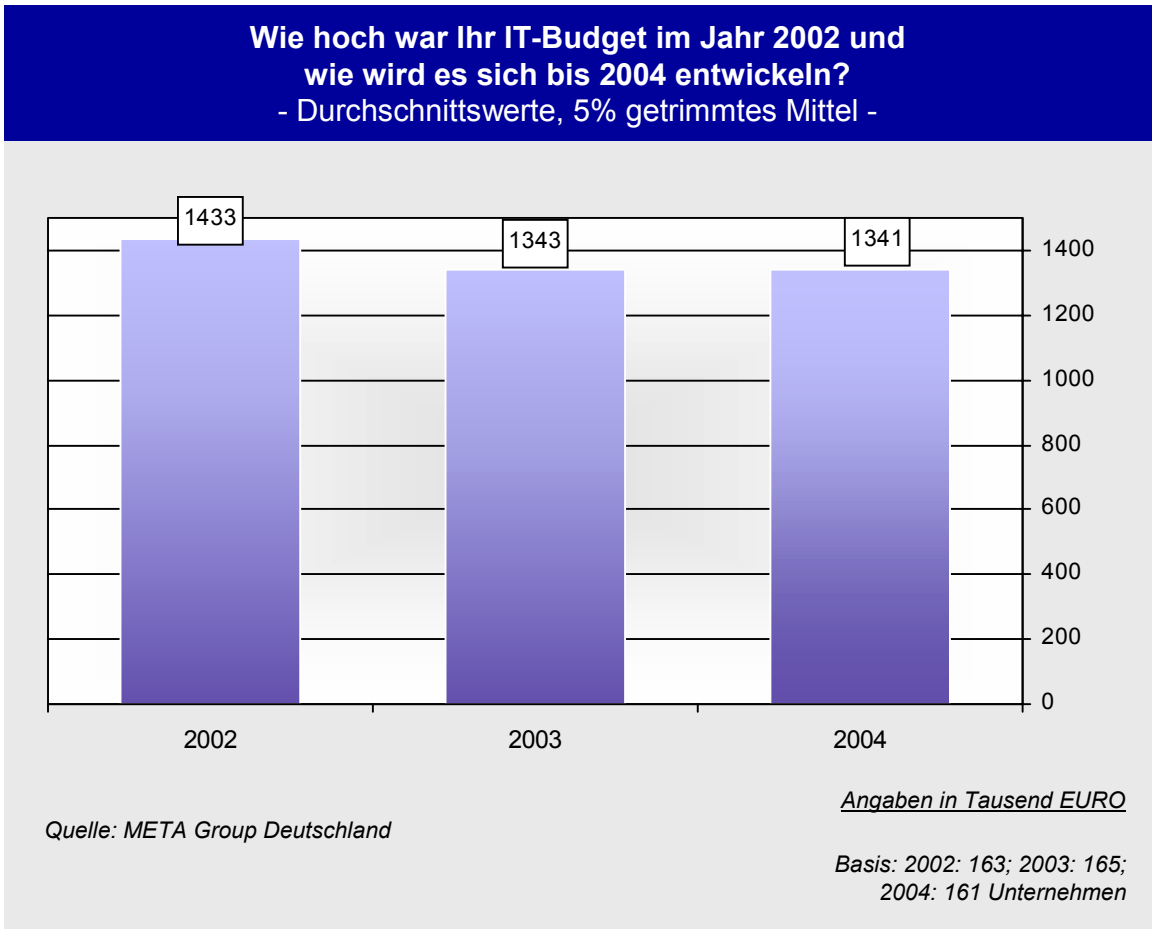


Abbildung 50: Entwicklung der IT-Budgets der Unternehmen – Mittelwerte 2002 bis 2004

Näheren Aufschluss über die Streuung der IT-Budget-Werte innerhalb der untersuchten Befragungsstichprobe gibt die Abbildung 51. 57 Prozent der Unternehmen investieren 2003 weniger als 0,5 Millionen EURO in IT und bleiben damit deutlich unter dem Durchschnittswert von rund 1,3 Millionen EUR. Immerhin gut ein Viertel der Unternehmen gibt 2003 mindestens fünf Millionen EUR für IT aus.

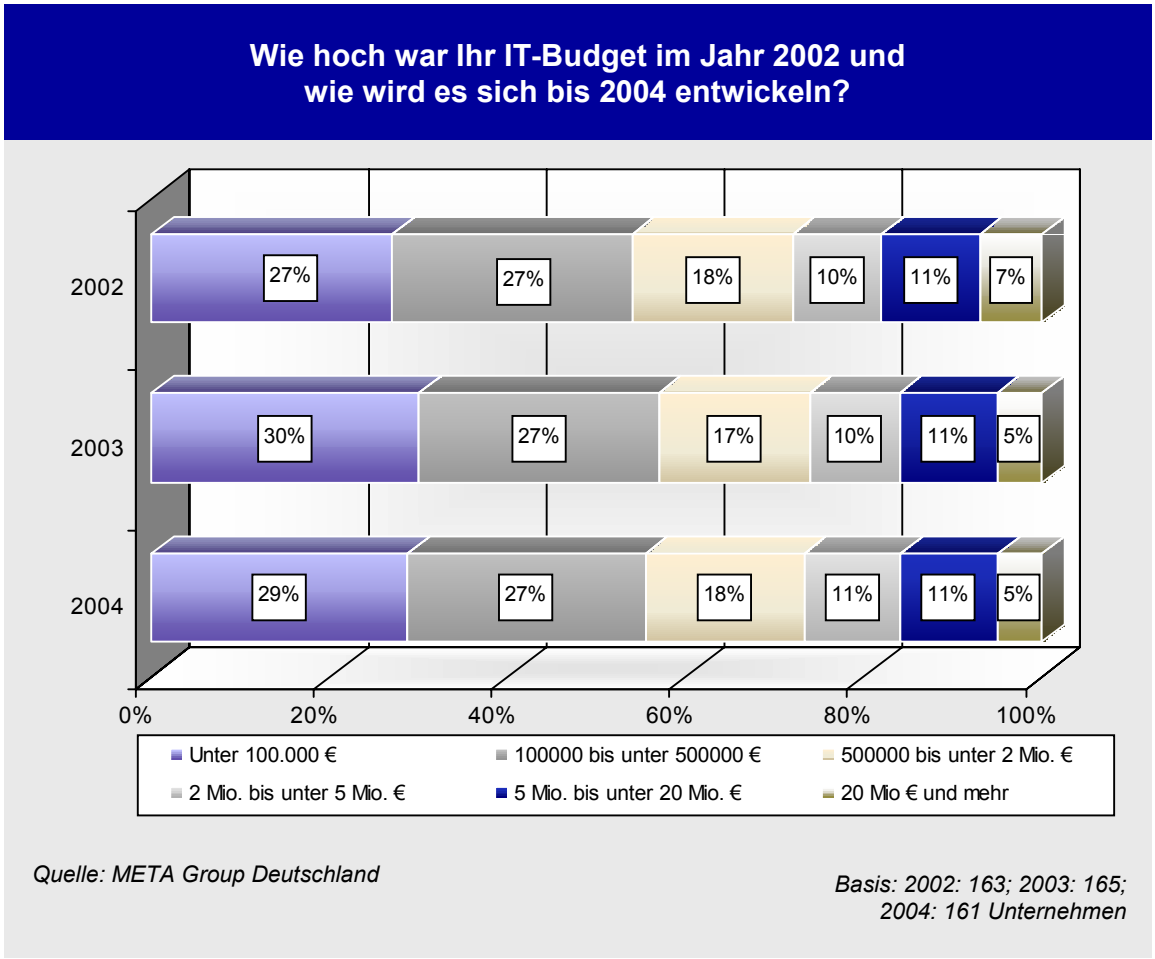


Abbildung 51: Entwicklung der IT-Budgets – 2002 bis 2004 (nach Budget-Größenklassen)

79 Prozent der befragten Unternehmen investieren mindestens vier Prozent ihres IT-Budgets in IT-Security – gut ein Drittel gibt sogar an, über zehn Prozent des IT-Budgets für IT-Sicherheit auszugeben. Die Untersuchung zeigt, dass sich die Security-Ausgaben der Unternehmen insbesondere im Bereich von vier bis fünf Prozent des IT-Budgets häufen (14 Prozent der Befragten), des Weiteren zwischen sechs und zehn Prozent (23 Prozent der Befragten) sowie oberhalb der erwähnten 10-Prozent-Schwelle (33 Prozent der Befragten). Die META Group geht davon aus, dass sich der Security-„Kostenblock“ in den IT-Budgets in den vergangenen 18 Monaten prozentual deutlich erhöht hat – teils wegen steigender Sicherheitsbudgets, vor allem aber auch aufgrund stagnierender oder fallender Werte bei der „Bezugsgröße“ IT-Budget. Die IT-Security-Ausgaben erweisen sich damit als „feste Größe“, die weniger anfällig für Kürzungen ist als manche anderen IT-Themen. Hintergrund ist unter anderem die hohe Bedeutung rechtlicher Rahmenbedingungen und der Anforderungen von Kunden und Partnern, die als Entscheidungsgrundlage dienen (siehe auch Kapitel 5.1).

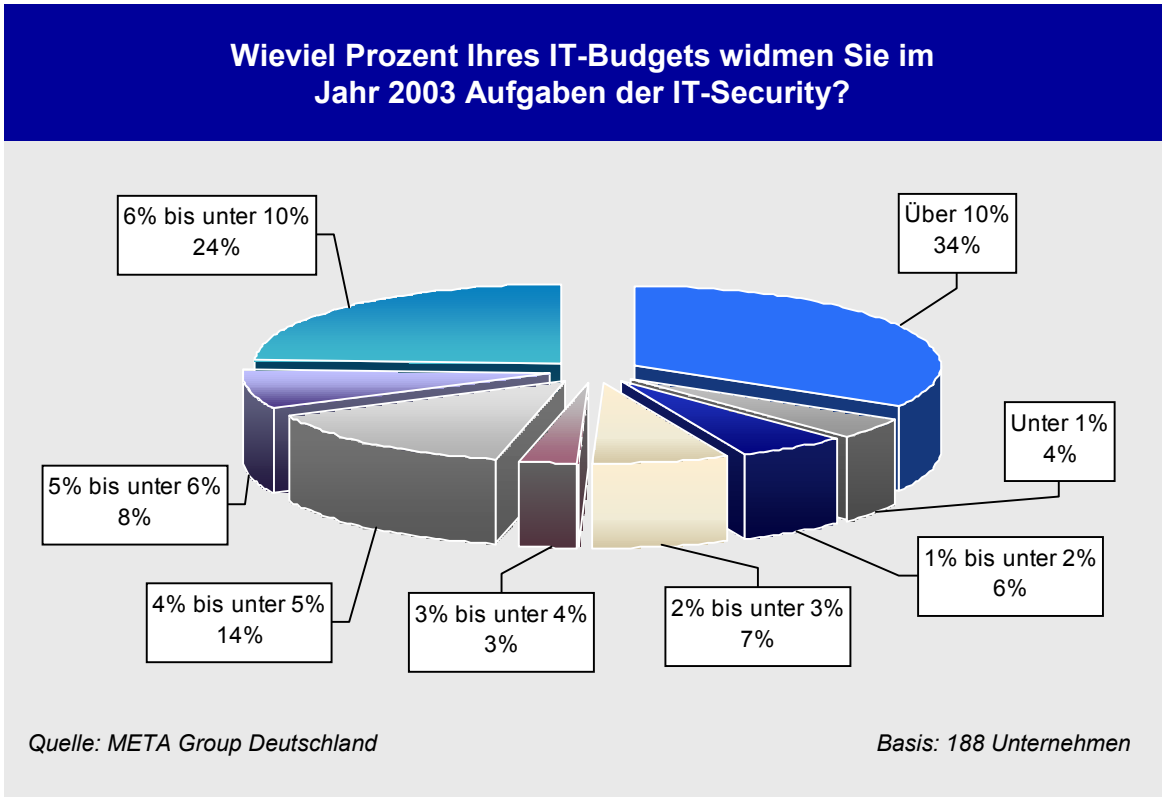


Abbildung 52: Anteil der IT-Security-Ausgaben am IT-Budget

Nach Einschätzung der META Group geben die Befragungsteilnehmer durchschnittlich zwischen 6 und 7,5 Prozent des IT-Budgets für IT-Security (Datenschutz *und* Verfügbarkeit) aus. Davon entfallen 41 Prozent auf Datenschutz-Maßnahmen und 59 Prozent auf die Sicherung der Verfügbarkeit der IT-Systeme (vergleiche Abbildung 59). Damit liegt der Anteil der Ausgaben allein für Datenschutz bei den befragten Unternehmen in einem Bereich von 2,5 bis 3 Prozent des IT-Budgets. Nach Schätzungen der META Group haben die großen Global-2000-Unternehmen für den Bereich des Datenschutzes

bislang rund zwei bis drei Prozent ihres IT-Budgets ausgegeben, wobei erwartet wird, dass dieser Anteil künftig auf vier Prozent steigen wird.

Die Investitionen der befragten deutschen Unternehmen entsprechen demnach weitestgehend diesem internationalen Richtwert. Allerdings gibt es Unterschiede zwischen einzelnen Branchen. Die im Rahmen dieser Befragung vorgebrachten Klagen der Unternehmen über Budgetmangel, über Risiken und über entstandene Schäden lassen jedoch den Verdacht aufkommen, dass die vorhandenen Gelder nicht immer sinnvoll investiert werden. Zudem ist die Beschaffung von Sicherheits-*Produkten* nicht ausreichend für den Schutz des Unternehmens. Wichtig ist auch die Gestaltung von Prozessen, Policies und anderen organisatorischen Maßnahmen. Genau hier wurden an früherer Stelle aber bei vielen Unternehmen offensichtliche Mängel festgestellt.

Schätzungen der META Group zum durchschnittlichen Anteil der Security-Ausgaben am IT-Budget zeigen zwischen den einzelnen befragten Branchen keine gravierenden Unterschiede auf. Beim Vergleich nach Unternehmensgrößen wird deutlich, dass der Security-Anteil bei großen Unternehmen mit mindestens 1.000 Mitarbeitern geringfügig kleiner ist als im Mittelstand.

Anteil der IT-Security-Ausgaben am IT-Budget
- Nach Branchen / Unternehmensgrößen -

	IT-Security	Nur „Datenschutz“*	META Group Empfehlung - weltweit, G2000-
GESAMT	**6,0% - 7,5%**	**2,5% - 3,0%**	**-**
Diskrete Fertigung	6,0% - 7,5%	2,5% - 3,0%	3%
Prozessorientierte Fertigung	6,5% - 7,5%	2,5% - 3,0%	
Transport/Logistik/Versorger/Telko	5,5% - 7,0%	2,0% - 3,0%	-
Handel	6,5% - 8,5%	2,5% - 3,5%	5%
Banken/Finanzdienstleister/Versicherungen	6,5% - 8,5%	2,5% - 3,5%	8%
Dienstleistungen	5,0% - 7,0%	2,0% - 3,0%	-
Öffentliche Hand / Non-Profit-Organisationen	6,5% - 8,0%	2,5% - 3,5%	-
50-199 Mitarbeiter	6,0% - 8,0%	2,5% - 3,5%	-
200-499 Mitarbeiter	6,5% - 8,0%	2,5% - 3,5%	-
500-999 Mitarbeiter	6,5% - 8,5%	2,5% - 3,5%	-
1.000 und mehr Mitarbeiter	5,0% - 7,0%	2,0% - 3,0%	-

Quelle: META Group Deutschland, 2003 (Schätzwerte auf Basis von 188 Anwenderaussagen); Empfehlungen der META Group auf Basis von Best Practices

* Datenschutz: Maßnahmen für zur Sicherung von Integrität, Vertraulichkeit und Authentizität (nicht Verfügbarkeit).

Abbildung 53: Anteil der IT-Security-Ausgaben am IT-Budget – Schätzwerte nach Branche / Größe

Obgleich die IT-Budgets der befragten Unternehmen insgesamt in den Jahren 2003/04 weitestgehend stagnieren, sehen die Aussichten im Bereich der IT-Sicherheit erfreulicher aus: 37 Prozent der befragten Unternehmen geben an, im Jahr 2004 ihr Sicherheits-Budget gegenüber 2003 erhöhen zu wollen; immerhin 40 Prozent rechnen mit konstanten Ausgaben. Nur knapp ein Viertel der Studienteilnehmer rechnet mit abnehmenden Investitionen in IT-Security beziehungsweise hat die Budgets für 2004 noch nicht festgelegt. Diese Werte schließen auch interne Personalkosten ein.

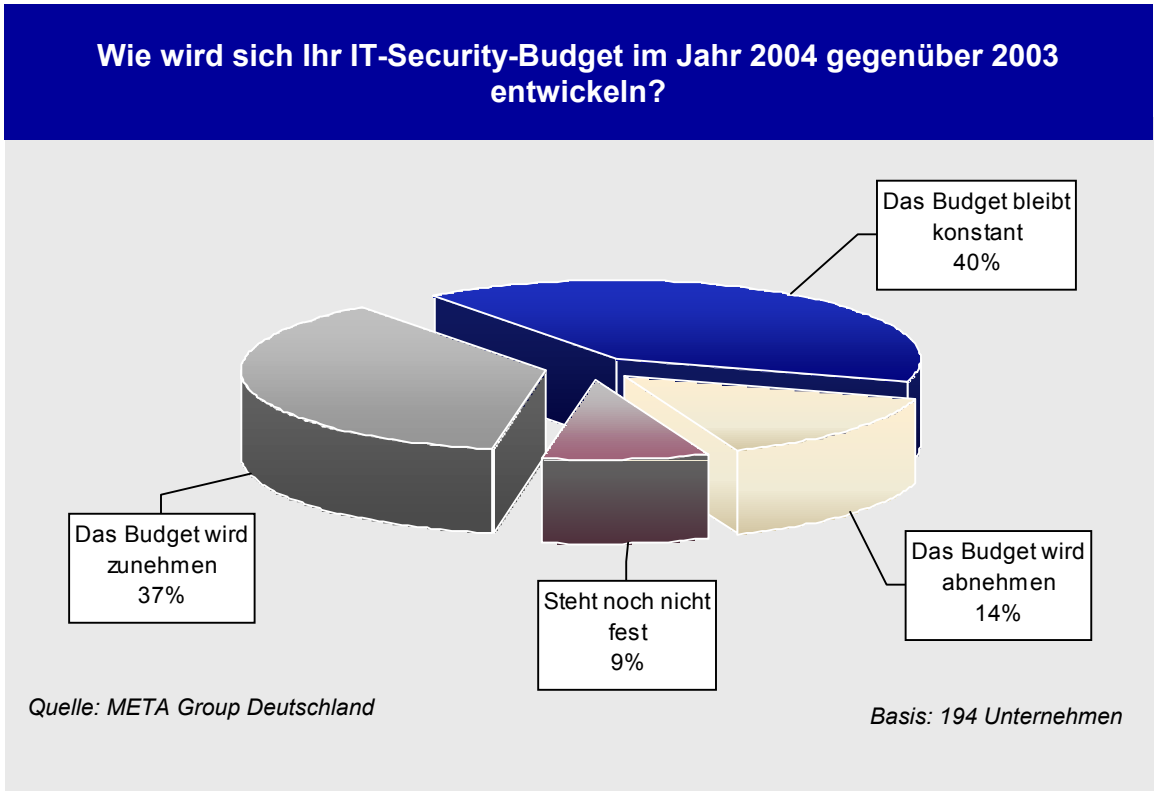


Abbildung 54: Geplante Entwicklung des IT-Security-Budgets von 2003 auf 2004

Die Budgetpläne der einzelnen Anwenderunternehmen fallen sehr unterschiedlich aus. Während 37 Prozent im Jahr 2004 mit einer Zunahme der IT-Security-Ausgaben gegenüber dem Vorjahr um durchschnittlich 28 Prozent rechnen, geben 14 Prozent an, 2004 ihre Sicherheitsbudgets um durchschnittlich 27 Prozent zu senken (vergleiche auch vorige Abbildung). Insgesamt ergibt sich für 2004 eine durchschnittliche Wachstumsrate der IT-Security-Budgets von sieben Prozent.

Eine nähere Analyse zeigt, dass abnehmende Budgets vor allem bei Unternehmen mit ursprünglich hohem Anteil der Security-Ausgaben am gesamten IT-Budget vorliegen. Unternehmen mit IT-Security-Budgets in Höhe von weniger als vier Prozent des IT-Budgets kürzen ihre Ausgaben nicht weiter. Der Grund dafür ist nach Einschätzung der META Group nicht nur der wirtschaftliche Druck, insbesondere die hohen Budgets zu kürzen. Typischerweise investieren Unternehmen in den ersten Jahren massiv, wenn ihnen ihr Rückstand im Bereich IT-Sicherheit bewusst wird. Einige Unternehmen meinen nun, diese erste Hürde genommen zu haben und aus diesem Grund diese Ausgaben reduzieren zu können.

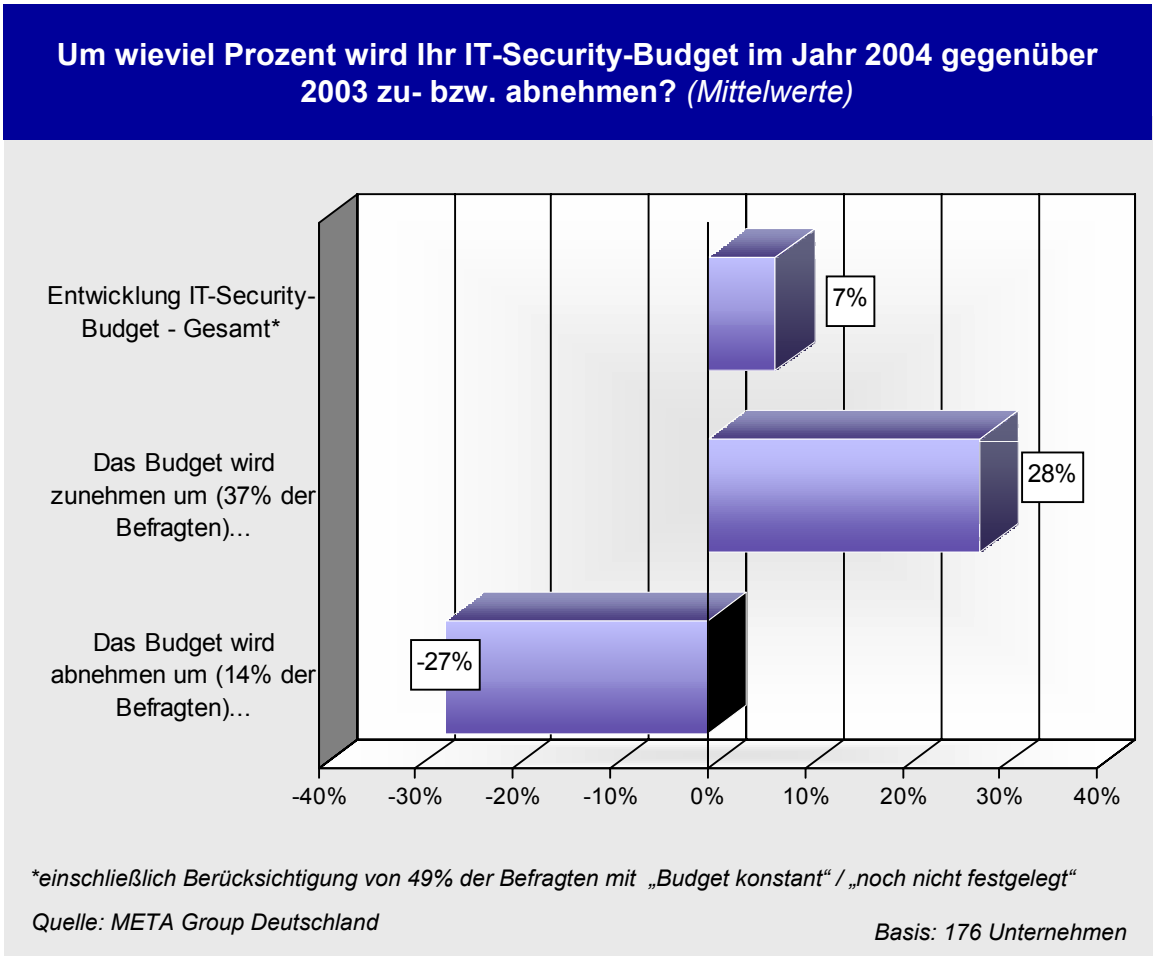
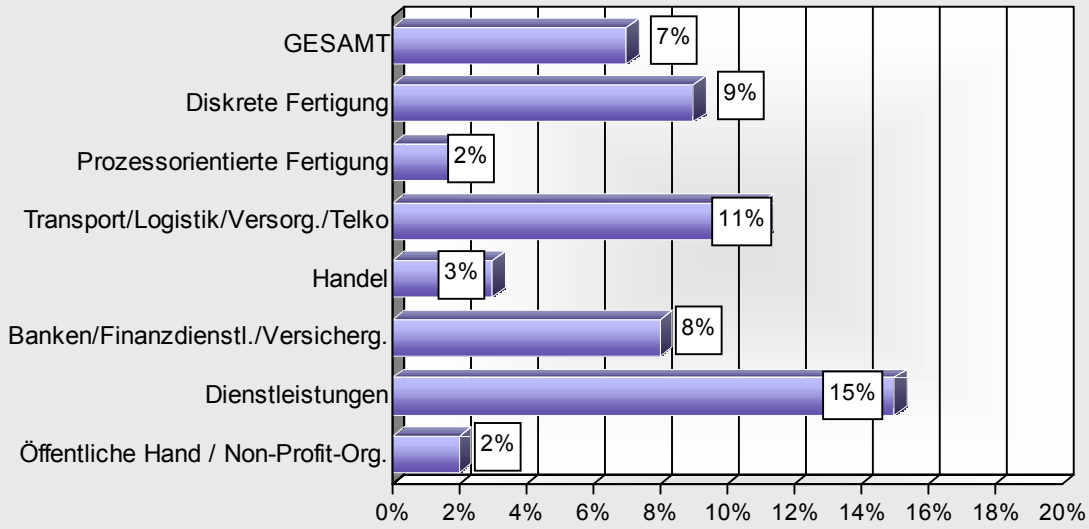


Abbildung 55: Relative Veränderung der Security-Budgets (2003-04)

Überdurchschnittliche Wachstumsraten bei den IT-Security-Budgets zeigen Unternehmen aus den Branchen diskrete Fertigung, Transport-, Logistik- und Versorgungsunternehmen, Banken, Finanzdienstleister und Versicherungen, sowie der Dienstleistungssektor. Die prozessorientierte Fertigung, der Handel und die öffentliche Hand planen deutlich geringere Zuwächse der Security-Budgets.

Um wieviel Prozent wird sich Ihr IT-Security-Budget im Jahr 2004 gegenüber 2003 verändern? *(Mittelwerte – nach Branchen)*



Basis: Diskr. Fert.: 30; Prozessor. Fert.: 25; Transport/Vers./Telko: 26; Handel :19; Banken/Finanz./Vers.: 21; Dienstl.: 25; Öff. Hand: 30 Unternehmen

Quelle: META Group Deutschland

Abbildung 56: Relative Veränderung der Security-Budgets (2003-04) – nach Branchen

Die höchsten durchschnittlichen Zuwachsraten von 2003 auf 2004 sind beim gehobenen Mittelstand (Unternehmen mit 500-999 Mitarbeitern, Wachstum um 24 Prozent) sowie bei großen Unternehmen mit mindestens 1.000 Mitarbeitern zu verzeichnen (durchschnittlich neun Prozent Zuwachs). Der klassische Mittelstand mit weniger als 500 Mitarbeitern weist bis Ende 2004 mehr oder weniger ein "Nullwachstum" bei den IT-Security-Budgets auf.

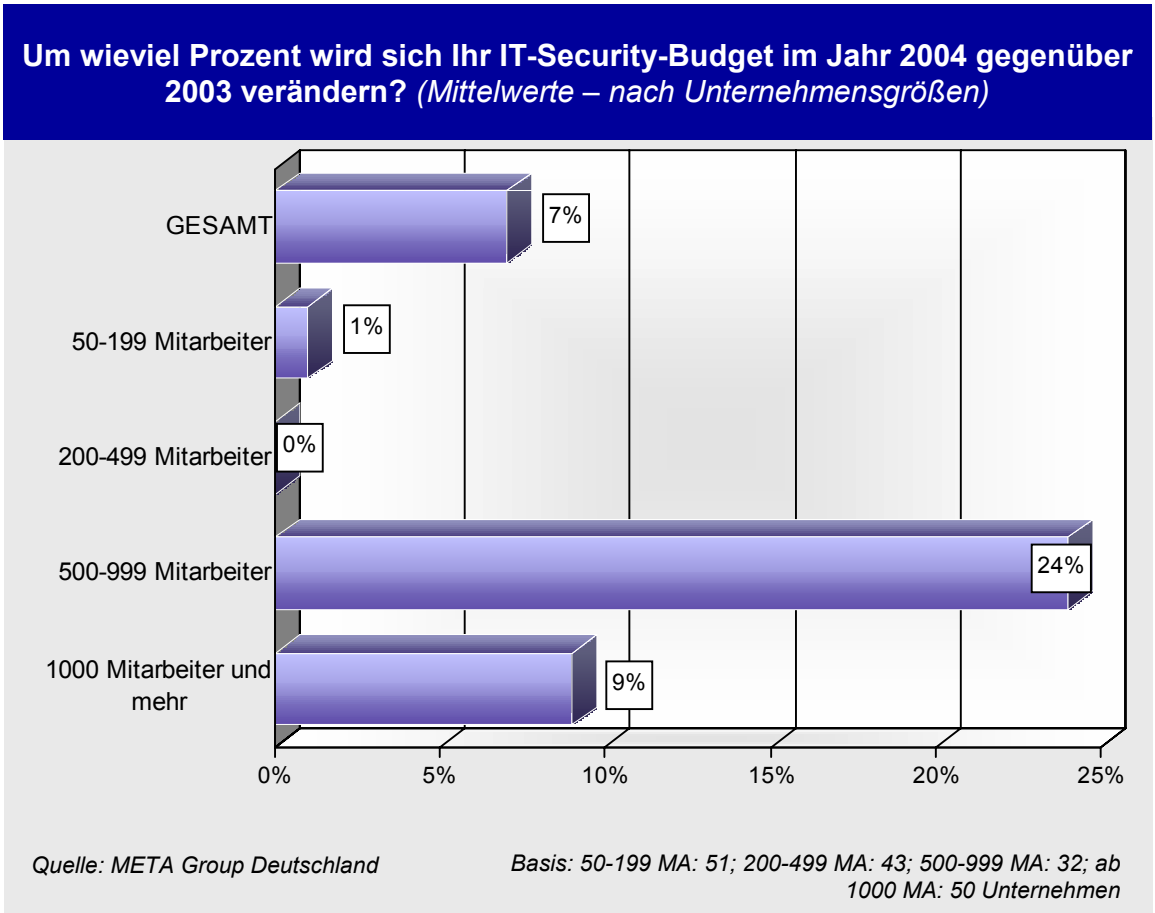


Abbildung 57: Relative Veränderung der Security-Budgets (2003-04) – nach Unternehmensgröße

Die Ausgaben für IT-Security verteilen sich auf 33 Prozent interne Personalkosten, 37 Prozent extern bezogene Sicherheitsprodukte (Hardware / Software) und 30 Prozent externe Dienstleistungen. Der Anteil der extern bezogenen Dienstleistungen am Security-Budget erweist sich damit als sehr hoch. Dies deutet auf eine grundsätzlich hohe Bereitschaft zur Vergabe von Aufgaben an externe Service Provider hin. Bemerkenswert ist, dass bei mittelständischen Unternehmen mit unter 500 Mitarbeitern der Anteil interner Personalkosten etwas geringer ausfällt als bei großen Unternehmen mit mindestens 1.000 Mitarbeitern. Dafür wird anteilig etwas mehr für externe Dienstleistungen ausgegeben. Der Mittelstand mit seinen begrenzten Personalressourcen erweist sich damit als potenziell interessante Zielgruppe für Security-Dienstleister – allerdings sind die Zuwachsraten der vorliegenden Budgets beim klassischen Mittelständler derzeit gering.

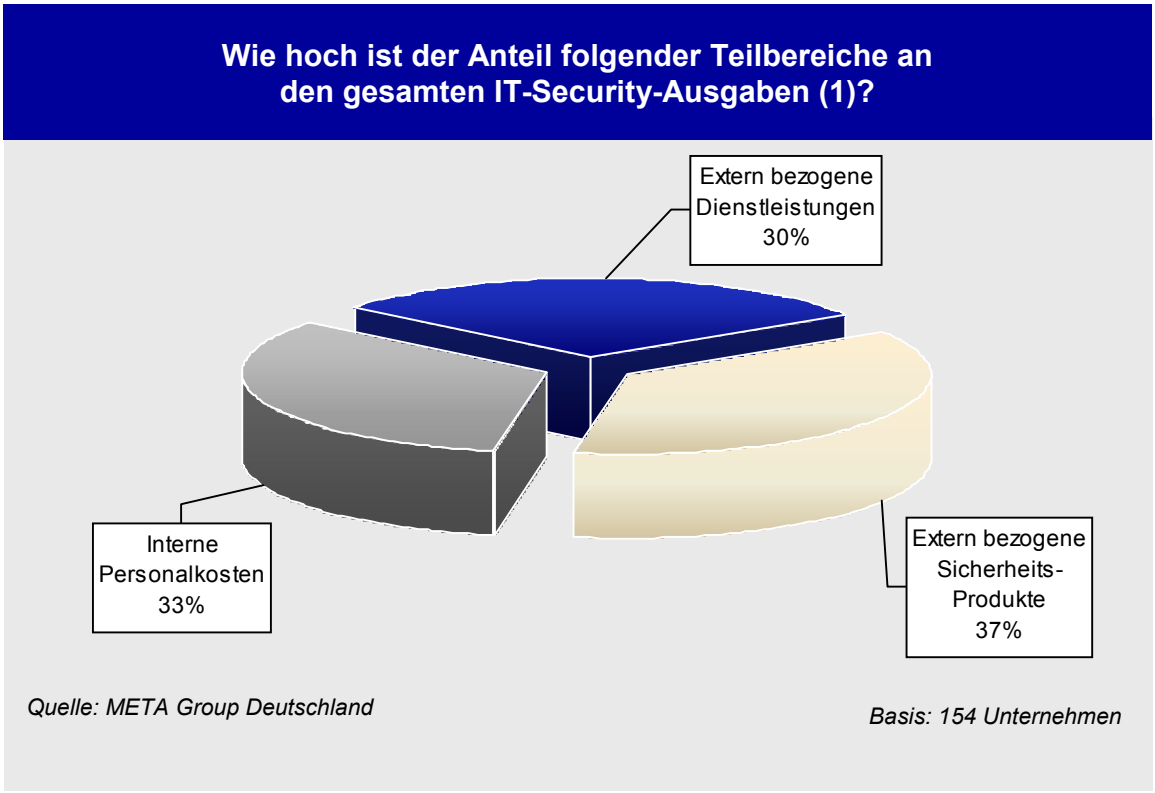


Abbildung 58: Anteil einzelner Teilbereiche an den gesamten IT-Security-Ausgaben (1)

Die META Group unterscheidet im Zusammenhang mit IT-Security grundsätzlich zwischen „Datensicherheit“ und „Datenschutz“. Unter dem Begriff Datensicherheit sind alle Disziplinen zusammengefasst, die sich mit der Verfügbarkeit bzw. mit der Wiederherstellung von Daten beschäftigen. Der Datenschutz fasst die Disziplinen zusammen, die notwendig sind, um sicherzustellen, dass Daten nicht von Unbefugten genutzt oder manipuliert werden können (Integrität, Vertraulichkeit und Authentizität).

Die befragten Anwenderunternehmen investieren 59 Prozent ihres IT-Security-Budgets in Datensicherheit beziehungsweise Lösungen und Services, die der Verfügbarkeit von IT-Systemen dienlich sind. Die restlichen 41 Prozent fließen in den Datenschutz-Komplex. Verfügbarkeitsthemen haben sich vor allem bei größeren Unternehmen bereits seit langer Zeit etabliert. Erst in den letzten Jahren haben die Anwenderunternehmen begonnen, auch verstärktes Augenmerk auf den Schutz von Daten zu legen.

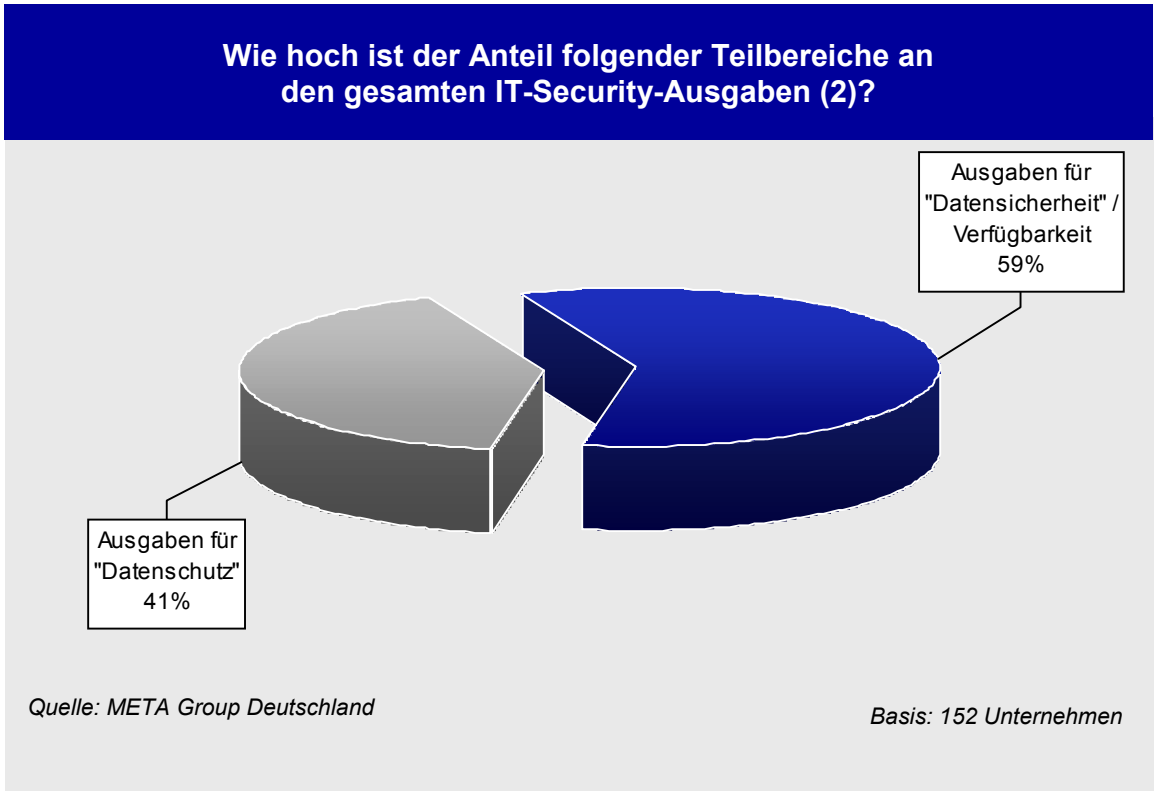


Abbildung 59: Anteil einzelner Teilbereiche an den gesamten IT-Security-Ausgaben (2)

6 Gegenwärtiger und geplanter Einsatz von IT-Security-Lösungen

6.1 IT-Security im Überblick

Haben Sie folgende IT-Sicherheitslösungen implementiert oder planen Sie deren Evaluierung oder Realisierung? *(Überblick)*

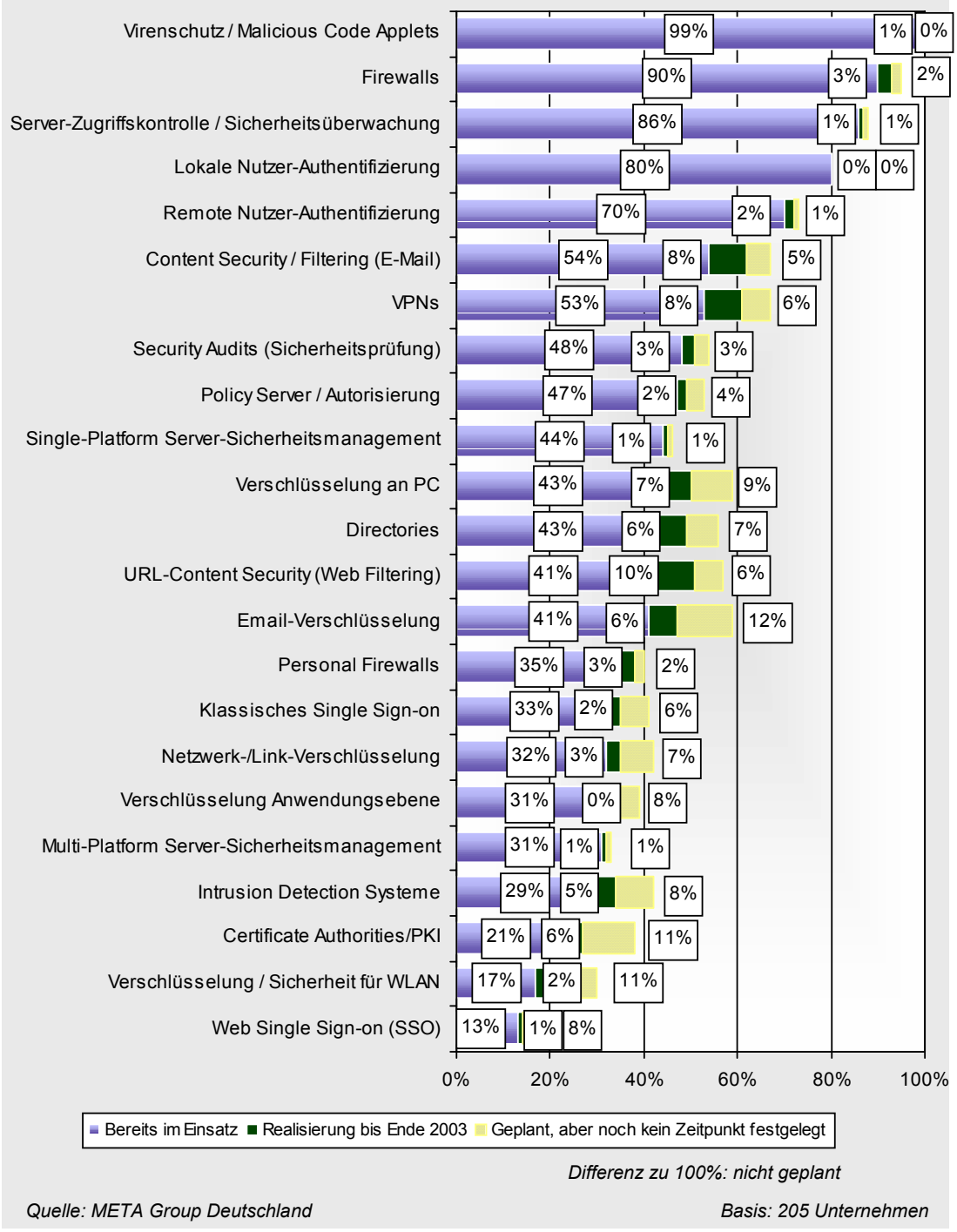


Abbildung 60: Gegenwärtiger und geplanter Einsatz ausgewählter Security-Technologien (Überblick)

Auf Basis der Anwenderaussagen lassen sich die folgenden Rankings in Bezug auf die geplanten Investitionen aufstellen. Zu beachten ist, dass diese Rankings zwar Aufschluss über die Einsatzplanung der Unternehmen in einzelnen Lösungsbereichen geben; das tatsächlich realisierte Marktvolumen auf der Anbieterseite kann aber davon abweichen, da die Preisentwicklung für einzelne Technologien zu berücksichtigen ist und die tatsächliche Umsetzung der geplanten Vorhaben umso unsicherer wird, je weiter der geplante Realisierungstermin in der Ferne liegt.

Top-5-Ranking nach Einsatzgrad – Anfang 2003:

1. Virenschutz / Malicious Code Applets
2. Firewalls
3. Server-Zugriffskontrolle u. Sicherheitsüberwachung
4. Lokale Nutzer-Authentifizierung
5. Remote Nutzer-Authentifizierung

Top-5-Ranking nach absolutem Wachstum bis Ende 2003:

1. URL Content Security (Web Filtering)
2. VPNs
3. Content Security / Filtering (Email)
4. Verschlüsselung an PC
5. Email-Verschlüsselung, Certificate Authorities/PKI, Directories

ToP-5-Ranking nach relativem Wachstum bis Ende 2003 (Einsatzgrad 2002 vs. 2003):

1. Certificate Authorities/PKI
2. URL Content Security (Web Filtering)
3. Intrusion Detection Systeme
4. Verschlüsselung an PC
5. VPNs; Content Security / Filtering (Email); Email-Verschlüsselung

Top-5-Ranking nach langfristigem relativem Wachstum (2002 vs. 2003 / später):

1. Certificate Authorities/PKI
2. Verschlüsselung / Sicherheit für WLAN
3. Web Single Sign-on (SSO)
4. Intrusion Detection Systeme
5. Email-Verschlüsselung

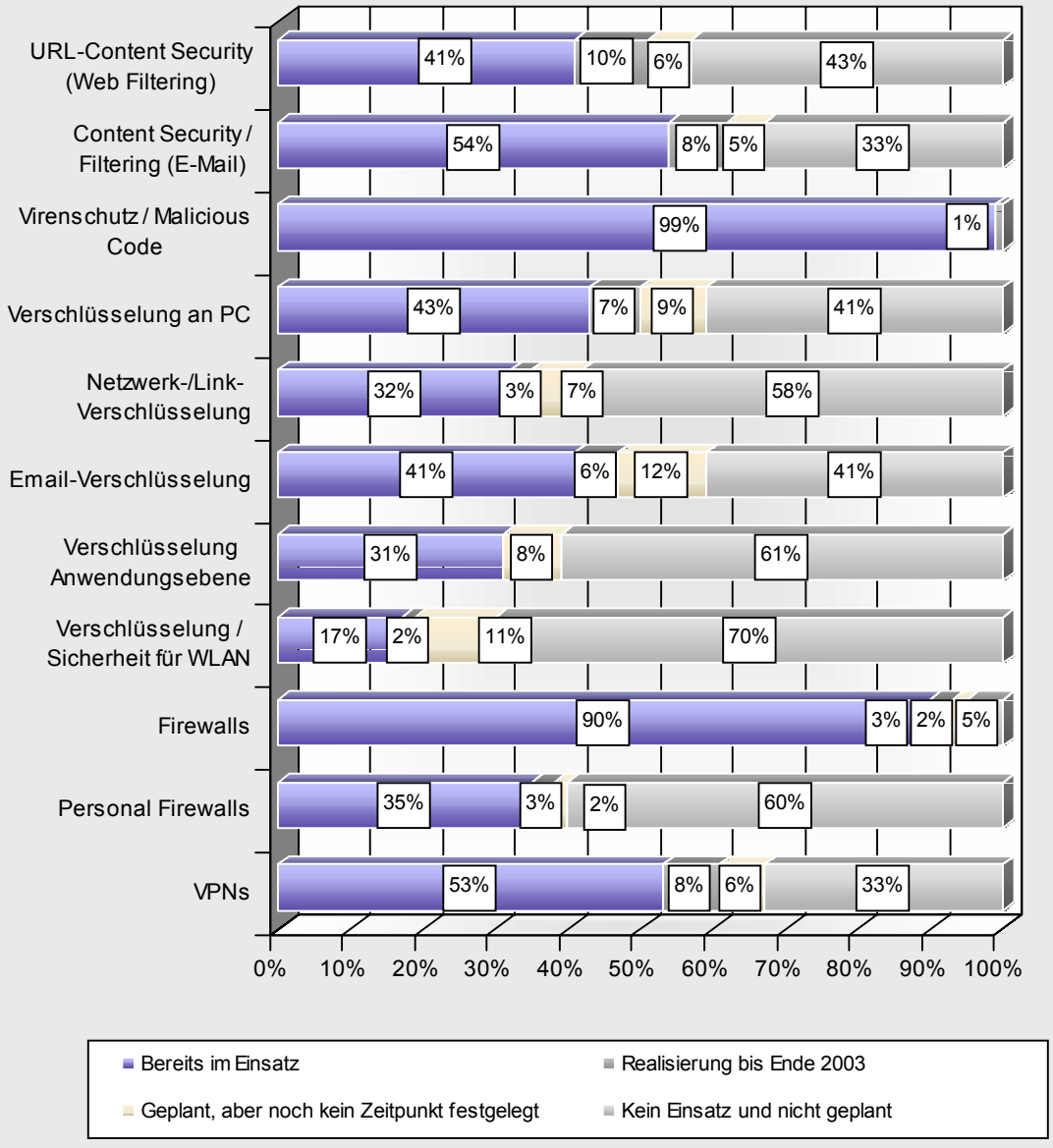
6.1.1 Einsatz und Planung: Virenschutz, Zugriffskontrolle und Verschlüsselung

Virenschutzlösungen und Firewalls haben in dieser Kategorie mit Abstand den höchsten Einsatzgrad (99 bzw. 90 Prozent). Immerhin gut die Hälfte der befragten Anwender gibt an, Content-Security-Lösungen für Email-Systeme und Virtual Private Networks (VPNs) einzusetzen. Bis Ende 2003 sind vor allem der Einsatz von Lösungen im Bereich Web Filtering (zehn Prozent der Befragten), Email-Content-Security und VPN (jeweils acht Prozent) geplant.

Verschlüsselungstechnologien sind vielfach im Gespräch, wobei sich die Anwender in Bezug auf die Planung wenig konkret äußern. Insbesondere bei der Verschlüsselung von Emails, Wireless LAN (WLAN) und auf Anwendungsebene sind die befragten Unternehmen vielfach nicht in der Lage, einen genauen Realisierungszeitraum zu nennen. Dies deutet darauf hin, dass die Anwender zunächst die weitere Entwicklung des Marktes beobachten und gleichzeitig noch untersuchen möchten, wo genau Bedarf an entsprechenden Lösungen besteht.

Die Analyse nach Branchen zeigt erwartungsgemäß, dass der gehobene Mittelstand und große Unternehmen über nahezu alle Lösungskategorien hinweg höhere Einsatzgrade aufweisen als der Mittelstand. Vor allem VPNs werden mit 70 Prozent bei den befragten Unternehmen mit mindestens 500 Mitarbeitern wesentlich häufiger eingesetzt als bei kleineren Marktteilnehmern (vergleiche Abbildungen auf den folgenden Seiten).

Haben Sie folgende IT-Sicherheitslösungen im Bereich Virenschutz, Zugriffskontrolle und Verschlüsselung implementiert oder planen Sie deren Evaluierung oder Realisierung? *(Gesamt)*

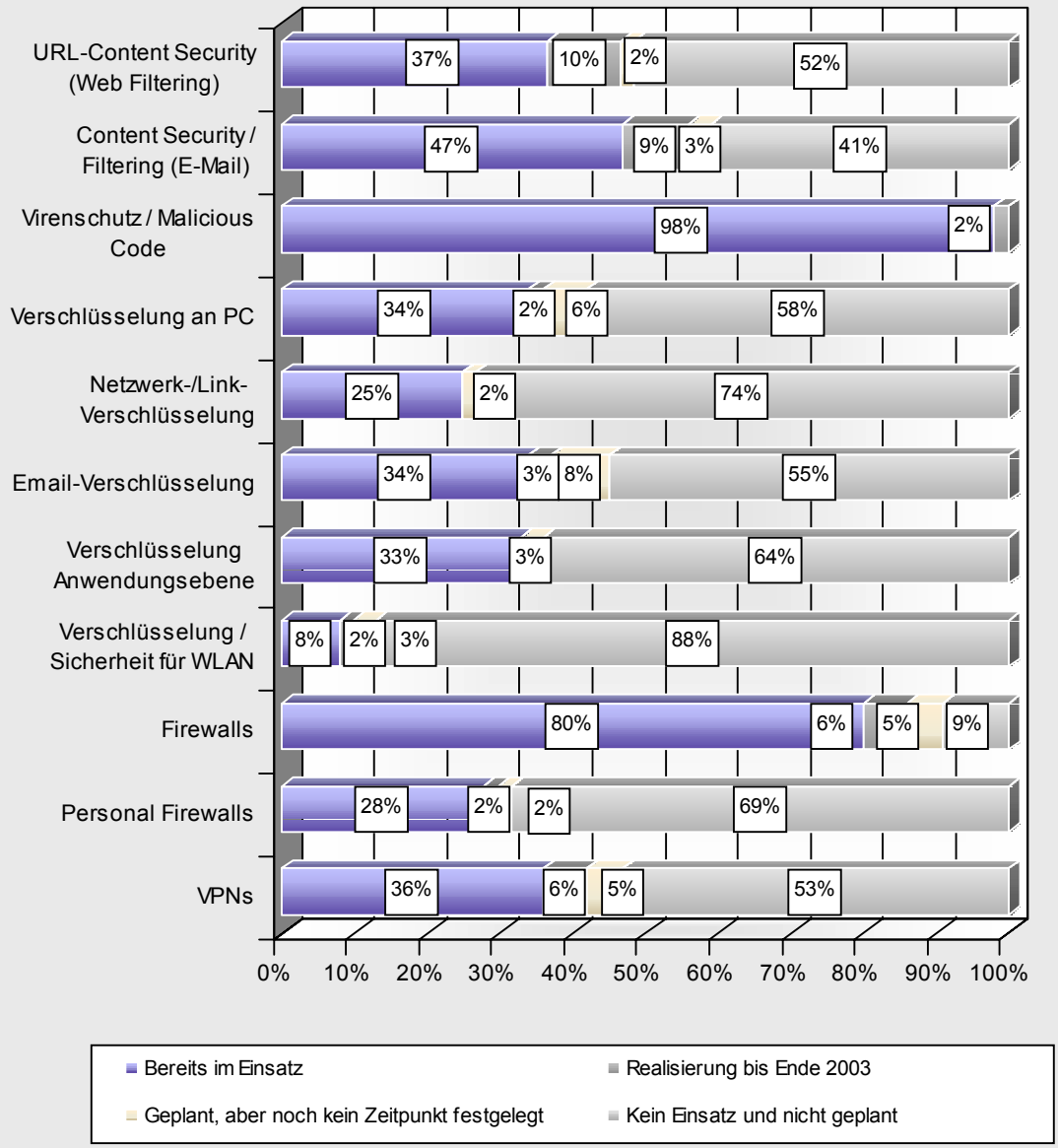


Quelle: META Group Deutschland

Basis: 207 Unternehmen

Abbildung 61: Einsatz und Planung bei Virenschutz, Zugriffskontrolle und Verschlüsselung

Haben Sie folgende IT-Sicherheitslösungen im Bereich Virenschutz, Zugriffskontrolle und Verschlüsselung implementiert oder planen Sie deren Evaluierung oder Realisierung? *(50-199 Mitarbeiter)*

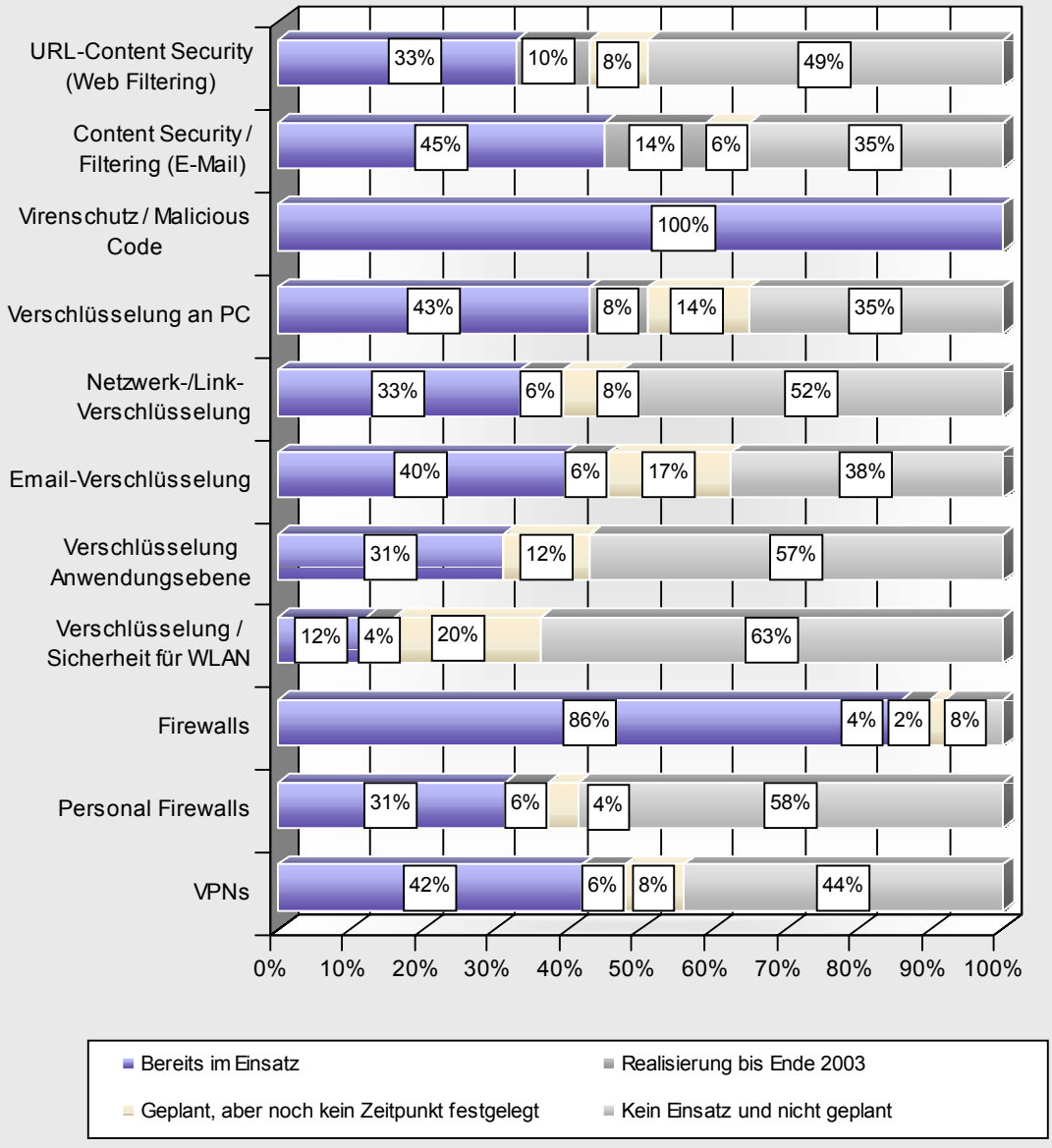


Quelle: META Group Deutschland

Basis: 65 Unternehmen

Abbildung 62: Einsatz/Planung - Virenschutz, Zugriffskontrolle, Verschlüsselung (50-199 Mitarbeiter)

Haben Sie folgende IT-Sicherheitslösungen im Bereich Virenschutz, Zugriffskontrolle und Verschlüsselung implementiert oder planen Sie deren Evaluierung oder Realisierung? *(200-499 Mitarbeiter)*

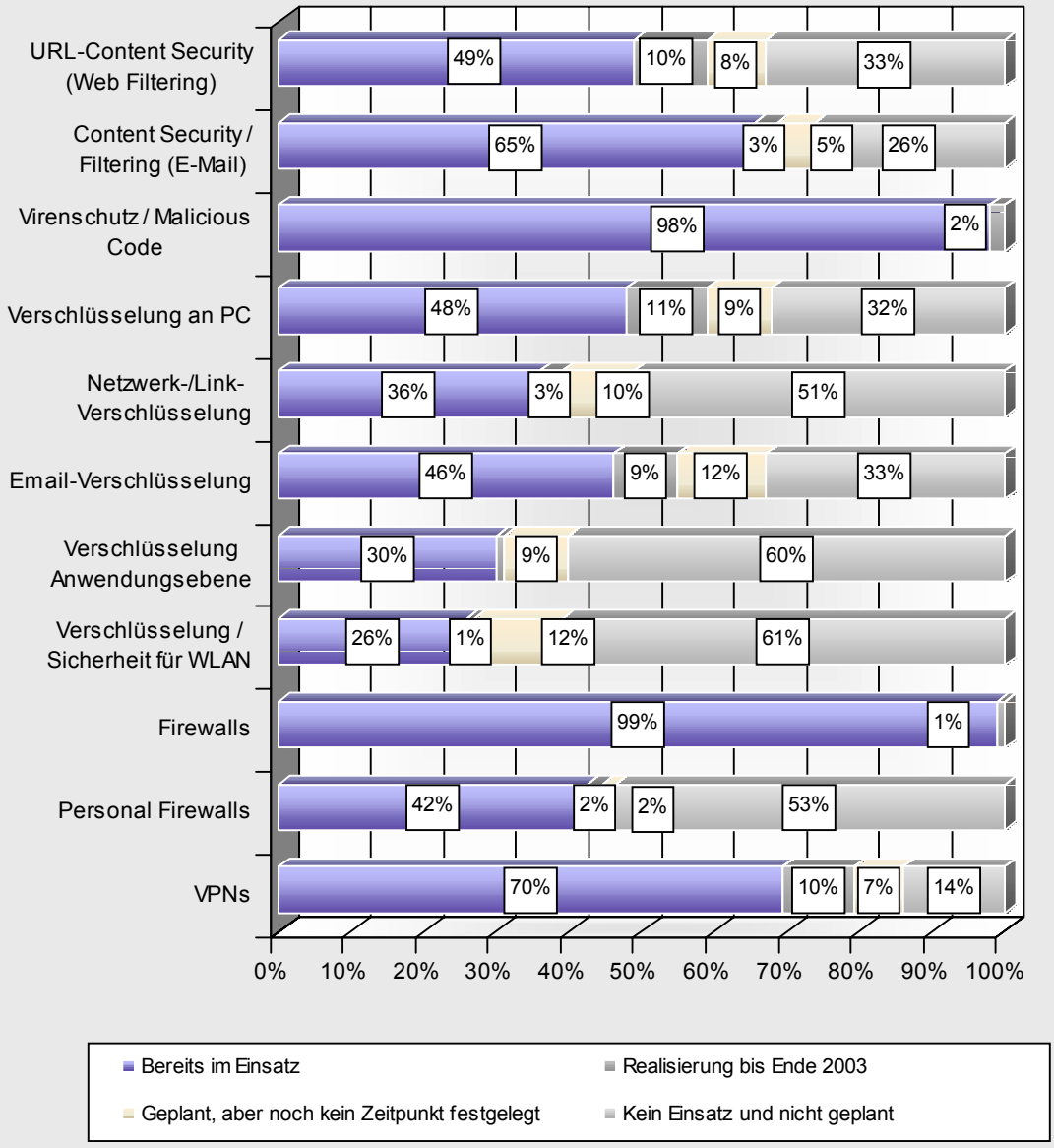


Quelle: META Group Deutschland

Basis: 49 Unternehmen

Abbildung 63: Einsatz/Planung - Virenschutz, Zugriffskontrolle, Verschlüsselung (200-499 Mitarbeiter)

Haben Sie folgende IT-Sicherheitslösungen im Bereich Virenschutz, Zugriffskontrolle und Verschlüsselung implementiert oder planen Sie deren Evaluierung oder Realisierung? *(500 und mehr Mitarbeiter)*



Quelle: META Group Deutschland

Basis: 92 Unternehmen

Abbildung 64: Einsatz/Planung - Virenschutz, Zugriffskontrolle, Verschlüsselung (ab 500 Mitarbeiter)

6.1.2 Einsatz und Planung: Authentifizierung und Autorisierung

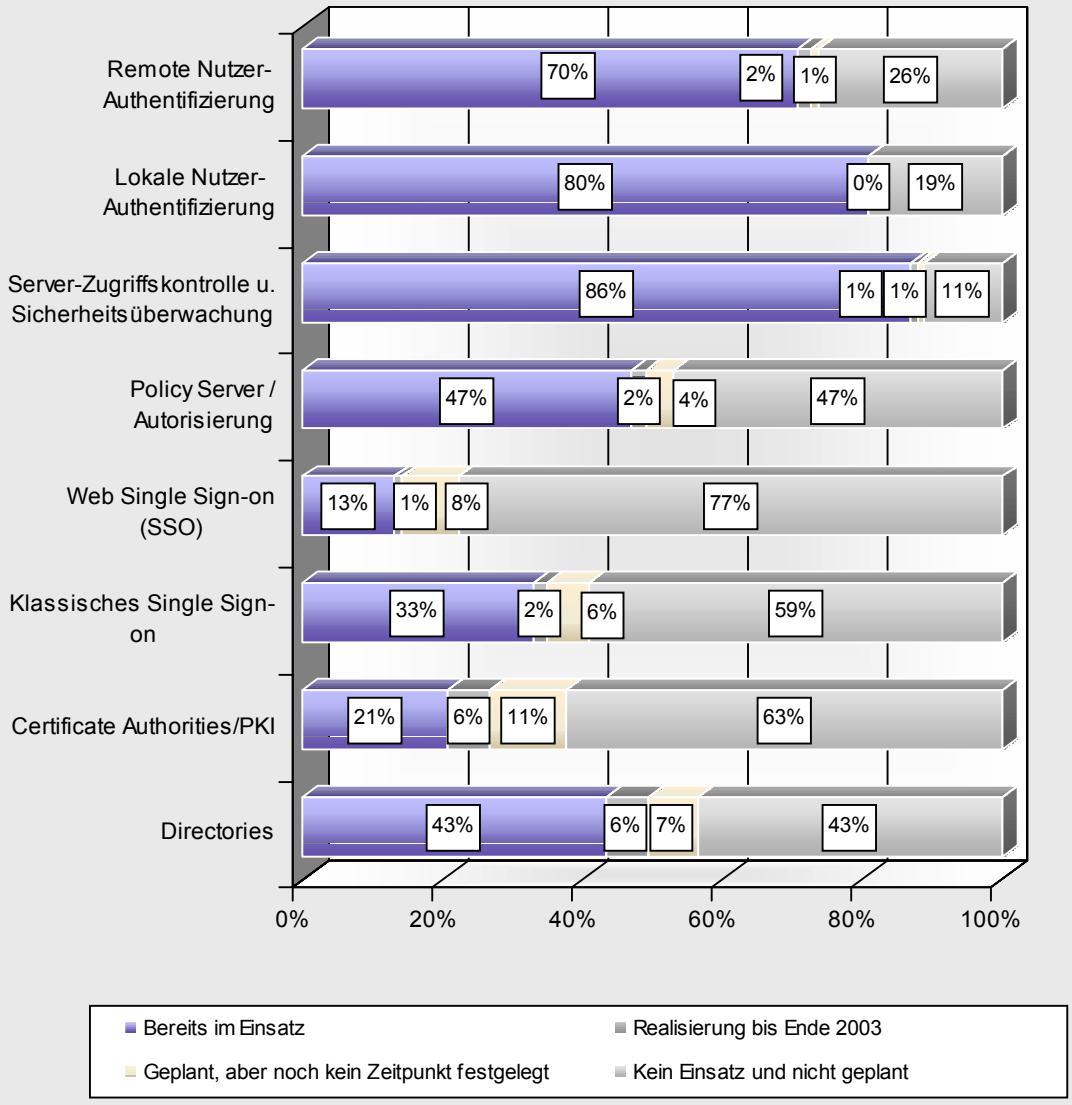
Die am häufigsten eingesetzten Lösungen aus dieser Kategorie sind Server-Zugriffskontrolle und Sicherheitsüberwachung (86 Prozent Einsatzgrad) sowie lokale Nutzer-Authentifizierung (80 Prozent) und „Remote“ Nutzer-Authentifizierung (70 Prozent). Diese Lösungen sind damit mehr oder weniger Standard in deutschen Unternehmen. Immerhin nahezu die Hälfte der befragten Anwender setzt auch Policy Server, die die Autorisierungsprozesse unterstützen sollen, sowie Verzeichnisdienste (Directories) ein.

Jeweils weitere sechs Prozent der Unternehmen planen den Einsatz von Certificate Authorities im Zusammenhang mit Public Key Infrastrukturen (digitale Signatur) sowie von Verzeichnisdiensten bis Ende 2003. Erwähnenswert ist, dass ein weiterer signifikanter Anteil der Befragten diese beiden Themenkomplexe sowie auch (Web) Single Sign-On künftig irgendwann einsetzen möchte, ohne dass ein konkreter Realisierungszeitraum bekannt wäre. Wie bereits an früherer Stelle angemerkt, deutet dies darauf hin, dass diese Anwender zunächst die weitere Entwicklung des Marktes beobachten und dann eine abschließende Bewertung des Einsatzes vornehmen möchten

Bei den anderen Themen rund um Authentifizierung und Autorisierung plant ein relativ geringer Anteil der Befragten, künftig erste Investitionen zu tätigen. Dies schließt jedoch nicht aus, dass die Bestandskunden im Jahr 2003 Folge- oder Erweiterungsprojekte starten.

Die Analyse nach Unternehmensgrößen zeigt, dass der Einsatzgrad einzelner Lösungen auch hier tendenziell mit der Unternehmensgröße wächst. Dies gilt besonders für PKI, wo sowohl der Einsatzgrad als auch die zukünftige Planung bei Unternehmen mit mindestens 500 Mitarbeitern wesentlich höher ausfallen als bei kleineren Organisationen. Eine Ausnahme bildet das klassische Single Sign-On: Mit 47 Prozent der mittelständischen Unternehmen mit 200 bis unter 500 Mitarbeitern lag hier Anfang 2003 ein beachtlich hoher Einsatzgrad vor (siehe auch Abbildung 65ff).

Haben Sie folgende IT-Sicherheitslösungen im Bereich Authentifizierung und Autorisierung implementiert oder planen Sie in den kommenden 12 Monaten deren Evaluierung oder Realisierung? *(Gesamt)*

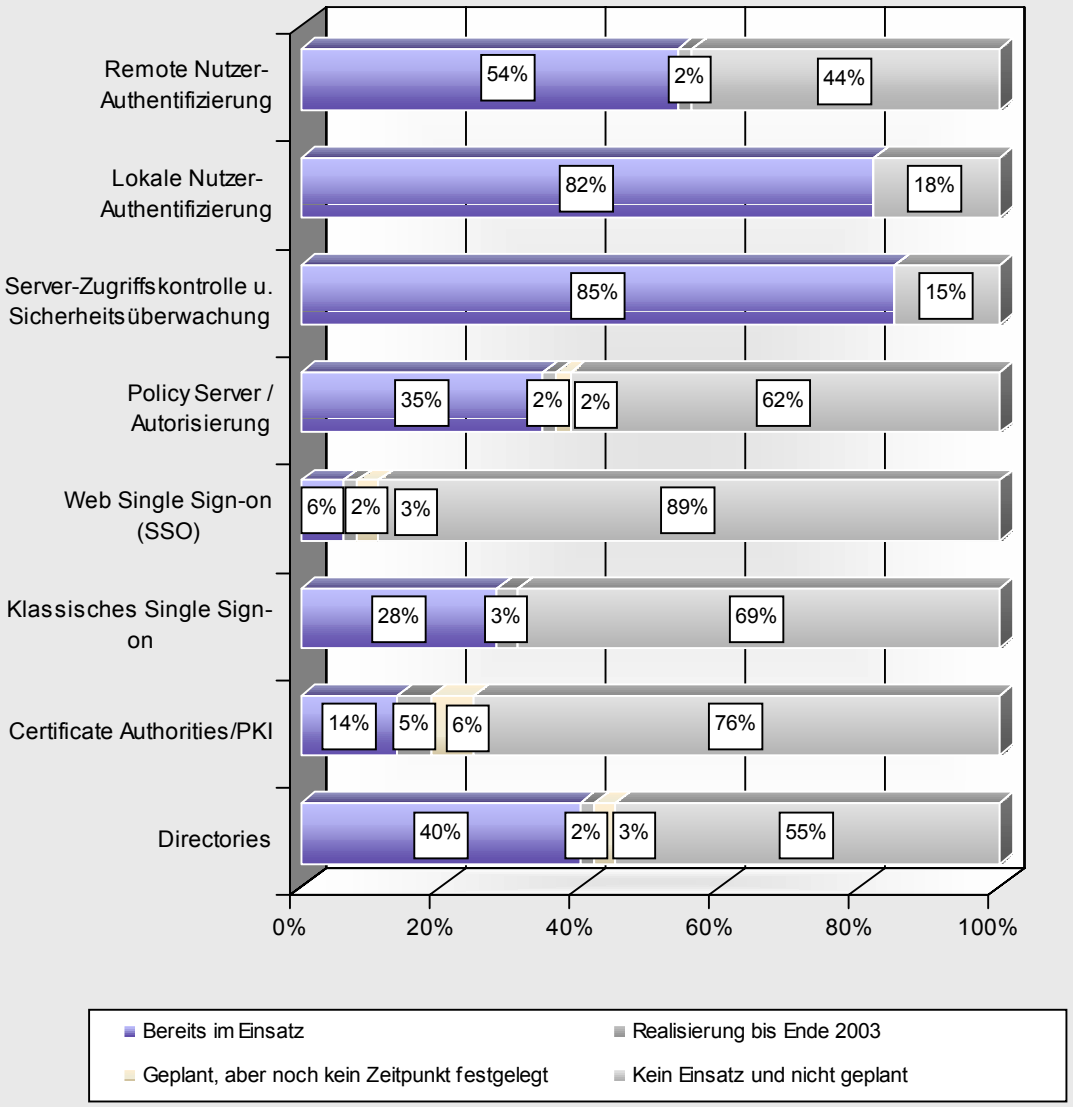


Quelle: META Group Deutschland

Basis: 207 Unternehmen

Abbildung 65: Einsatz und Planung bei Authentifizierung und Autorisierung

Haben Sie folgende IT-Sicherheitslösungen im Bereich Authentifizierung und Autorisierung implementiert oder planen Sie in den kommenden 12 Monaten deren Evaluierung oder Realisierung? *(50-199 Mitarbeiter)*

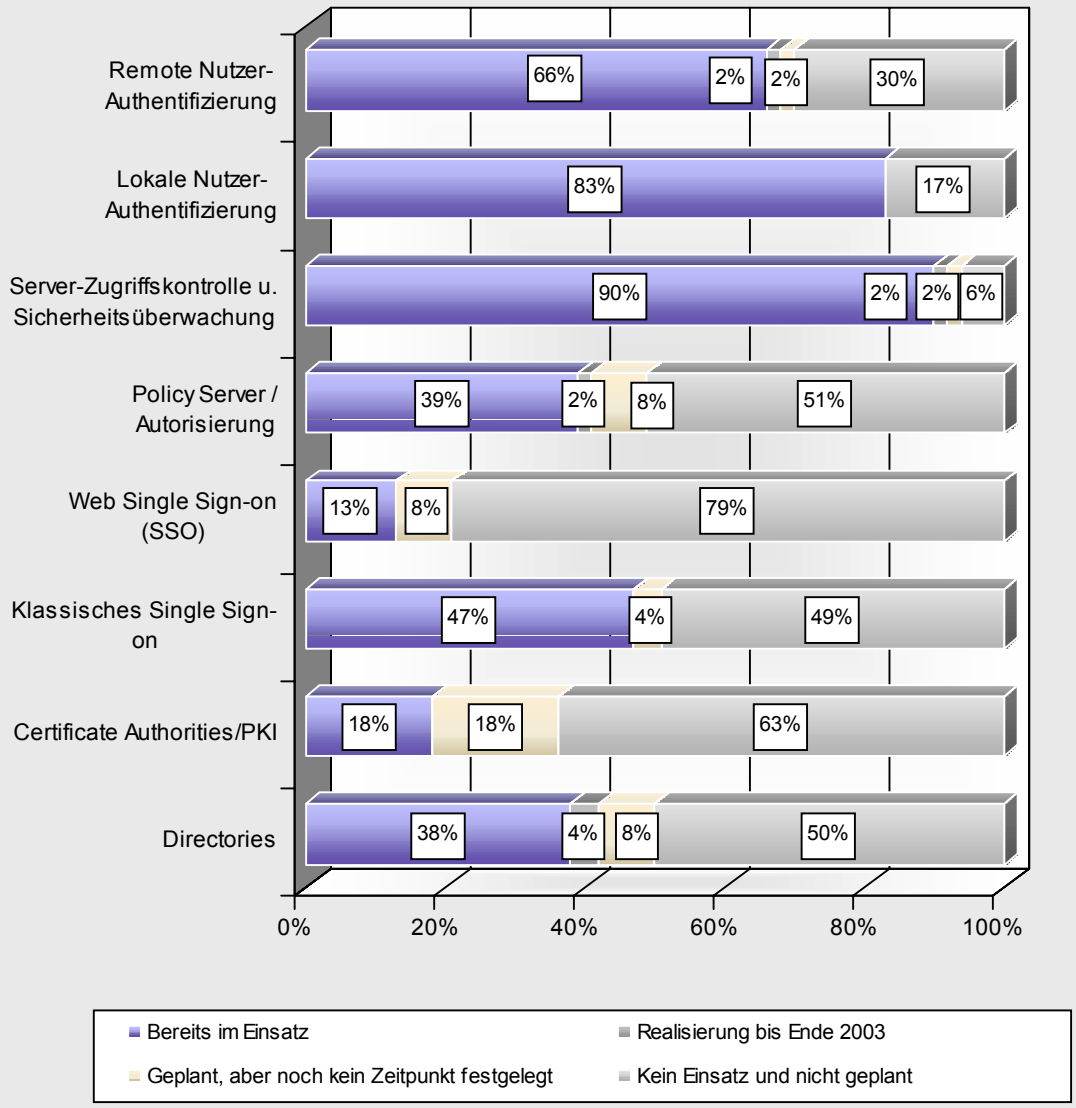


Quelle: META Group Deutschland

Basis: 66 Unternehmen

Abbildung 66: Einsatz und Planung bei Authentifizierung und Autorisierung (50-199 Mitarbeiter)

Haben Sie folgende IT-Sicherheitslösungen im Bereich Authentifizierung und Autorisierung implementiert oder planen Sie in den kommenden 12 Monaten deren Evaluierung oder Realisierung? *(200-499 Mitarbeiter)*

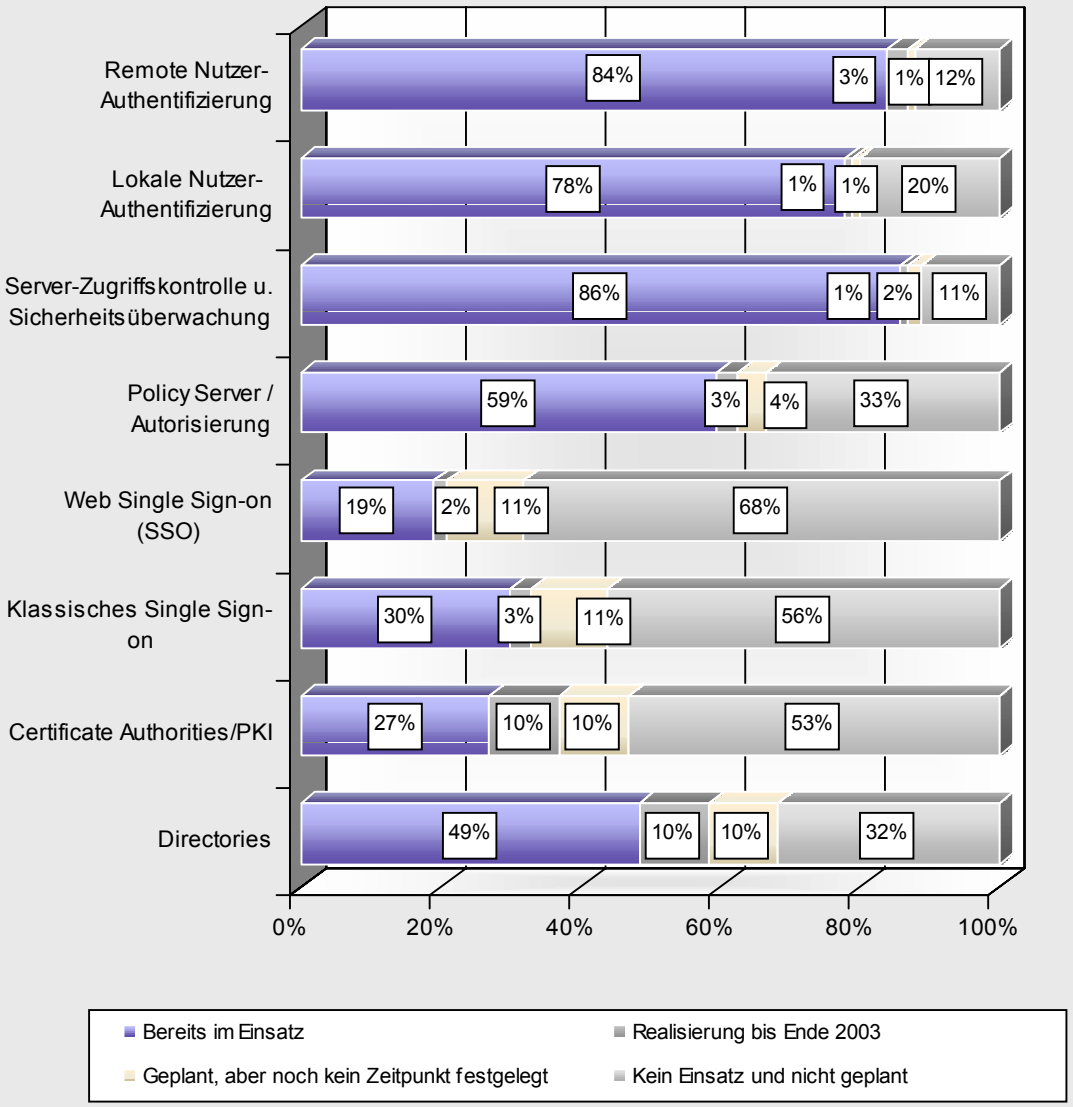


Quelle: META Group Deutschland

Basis: 49 Unternehmen

Abbildung 67: Einsatz und Planung bei Authentifizierung und Autorisierung (200-499 Mitarbeiter)

Haben Sie folgende IT-Sicherheitslösungen im Bereich Authentifizierung und Autorisierung implementiert oder planen Sie in den kommenden 12 Monaten deren Evaluierung oder Realisierung? *(500 und mehr Mitarbeiter)*



Quelle: META Group Deutschland

Basis: 92 Unternehmen

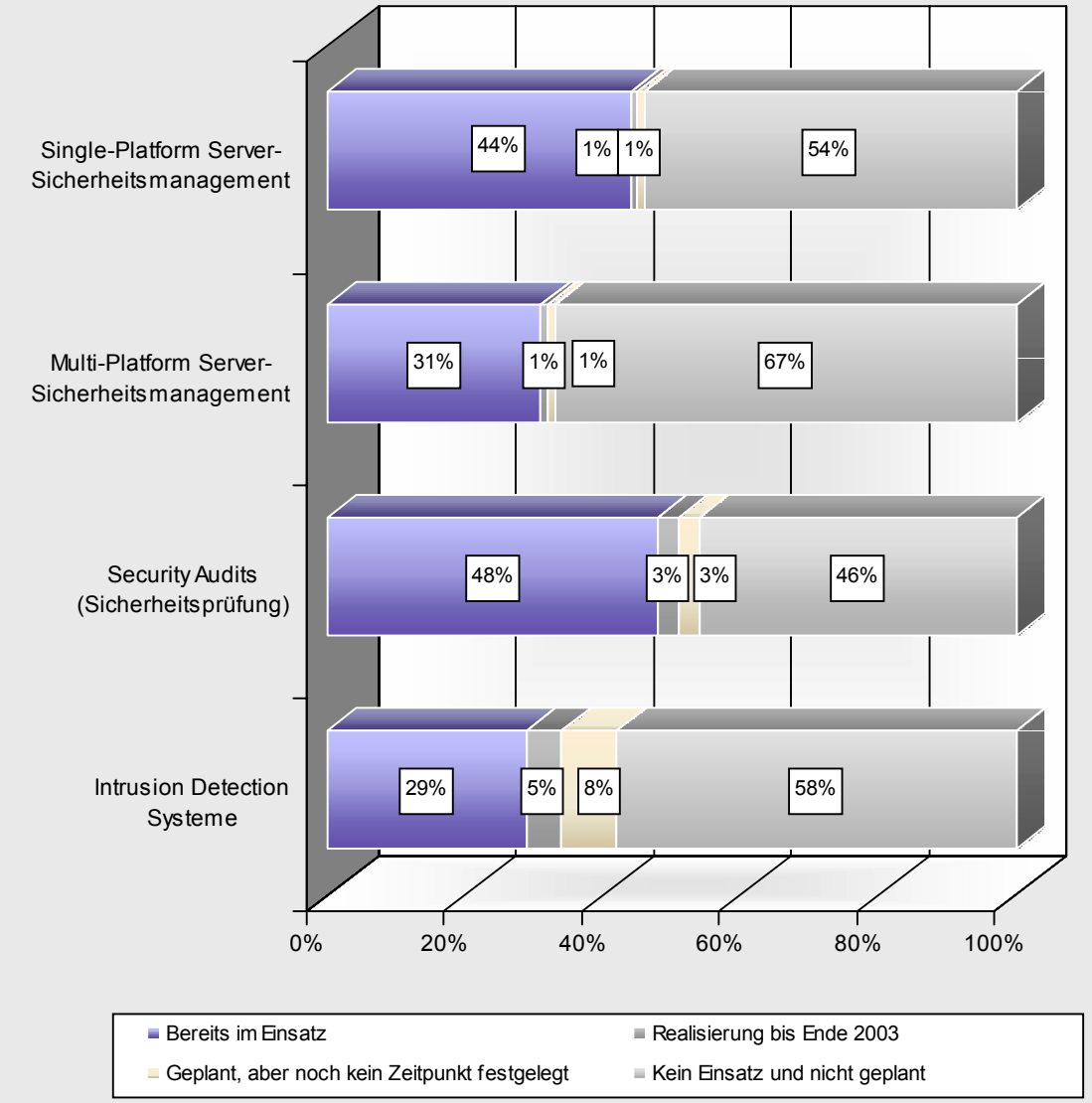
Abbildung 68: Einsatz und Planung bei Authentifizierung und Autorisierung (ab 500 Mitarbeitern)

6.1.3 Einsatz und Planung: Administration, Monitoring und Audit

Befragt zu den Bereichen Administration, Monitoring und Audit, geben 48 Prozent der Anwenderunternehmen an, Lösungen zur Sicherheitsprüfung (Security Audit) einzusetzen. Solche Werkzeuge helfen unter anderem bei der Umsetzung von Security Policies. Der Trend geht hin zu integrierten Audit-Werkzeugen, welche durch Konsolidierung verschiedener Tools in eine zentrale Konsole entstehen. Diese zentrale Konsole konsolidiert typischerweise Werkzeuge wie Scanner, Intrusion Detection Systeme für Netzwerke und Hosts, Audit-Log-Consolidators oder Systeme für die Zugriffskontrolle bzw. Firewalls. Solche Konsolen stehen als Server-Sicherheitsmanagement-Werkzeuge für einzelne Plattformen oder als plattformübergreifende Werkzeuge zur Verfügung. 44 Prozent der befragten Unternehmen haben “Single-Platform” Server-Sicherheitsmanagement-Werkzeuge im Einsatz, gegenüber 31 Prozent mit “Multi-Platform” Server-Sicherheitsmanagement-Werkzeugen. Die künftige Einsatzplanung fällt hingegen eher zurückhaltend aus.

Eine relativ geringe Verbreitung haben mit 29 Prozent Einsatzgrad Intrusion Detection Systeme (IDS). Allerdings liegt hier erhebliches Wachstumspotenzial vor: 13 Prozent der Unternehmen planen den künftigen Einsatz - fünf Prozent bis Ende 2003 und acht Prozent zu einem noch festzulegenden Zeitpunkt. Die Analyse nach Unternehmensgrößen zeigt eine besonders starke Nachfrage seitens Unternehmen mit mindestens 500 Mitarbeitern auf (siehe Abbildung 69ff).

Haben Sie folgende IT-Sicherheitslösungen im Bereich Administration, Monitoring und Audit implementiert oder planen Sie in den kommenden 12 Monaten deren Evaluierung oder Realisierung? *(Gesamt)*

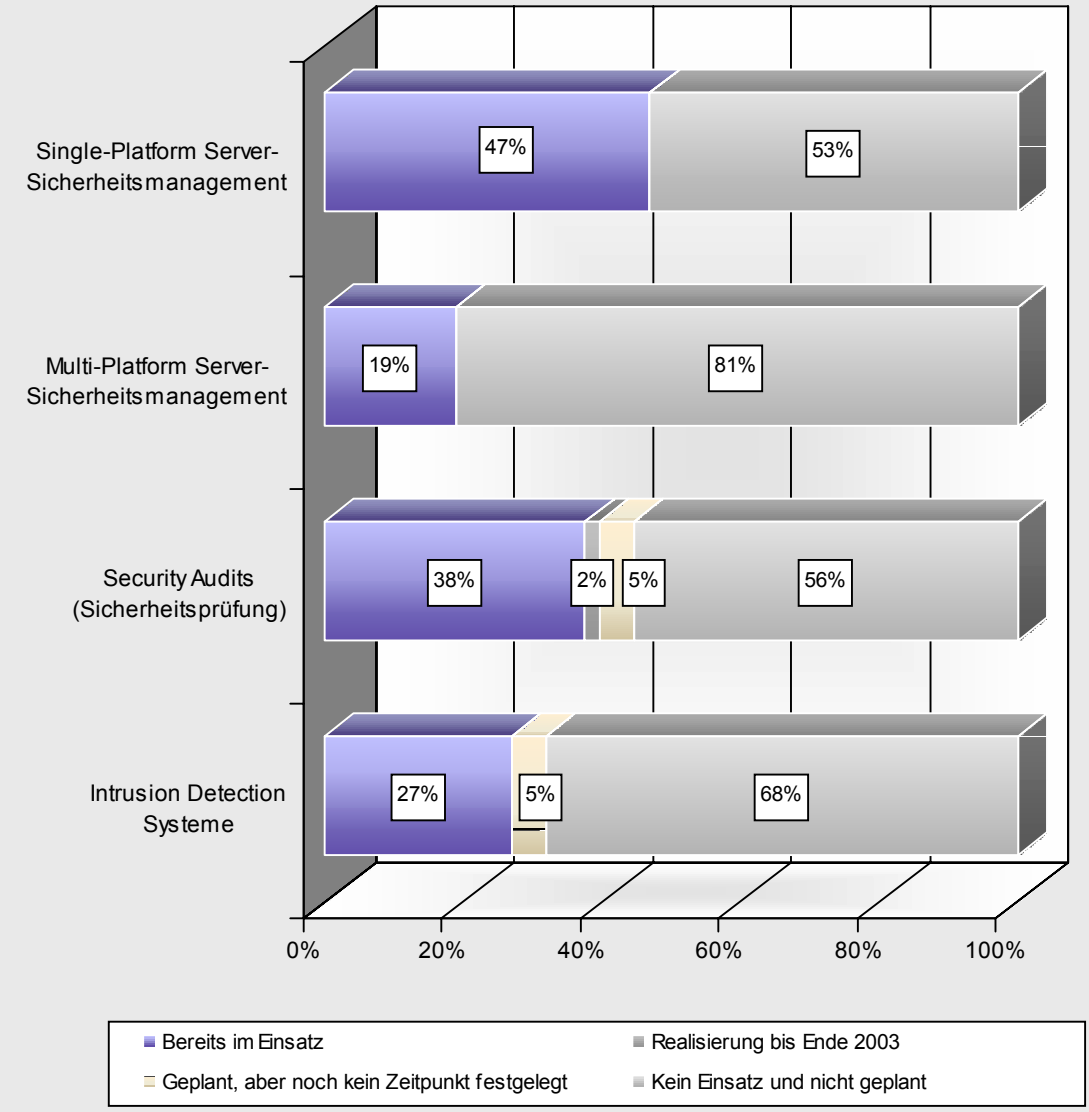


Quelle: META Group Deutschland

Basis: 204 Unternehmen

Abbildung 69: Einsatz und Planung bei Administration, Monitoring und Audit

Haben Sie folgende IT-Sicherheitslösungen im Bereich Administration, Monitoring und Audit implementiert oder planen Sie in den kommenden 12 Monaten deren Evaluierung oder Realisierung? *(50-199 MA)*

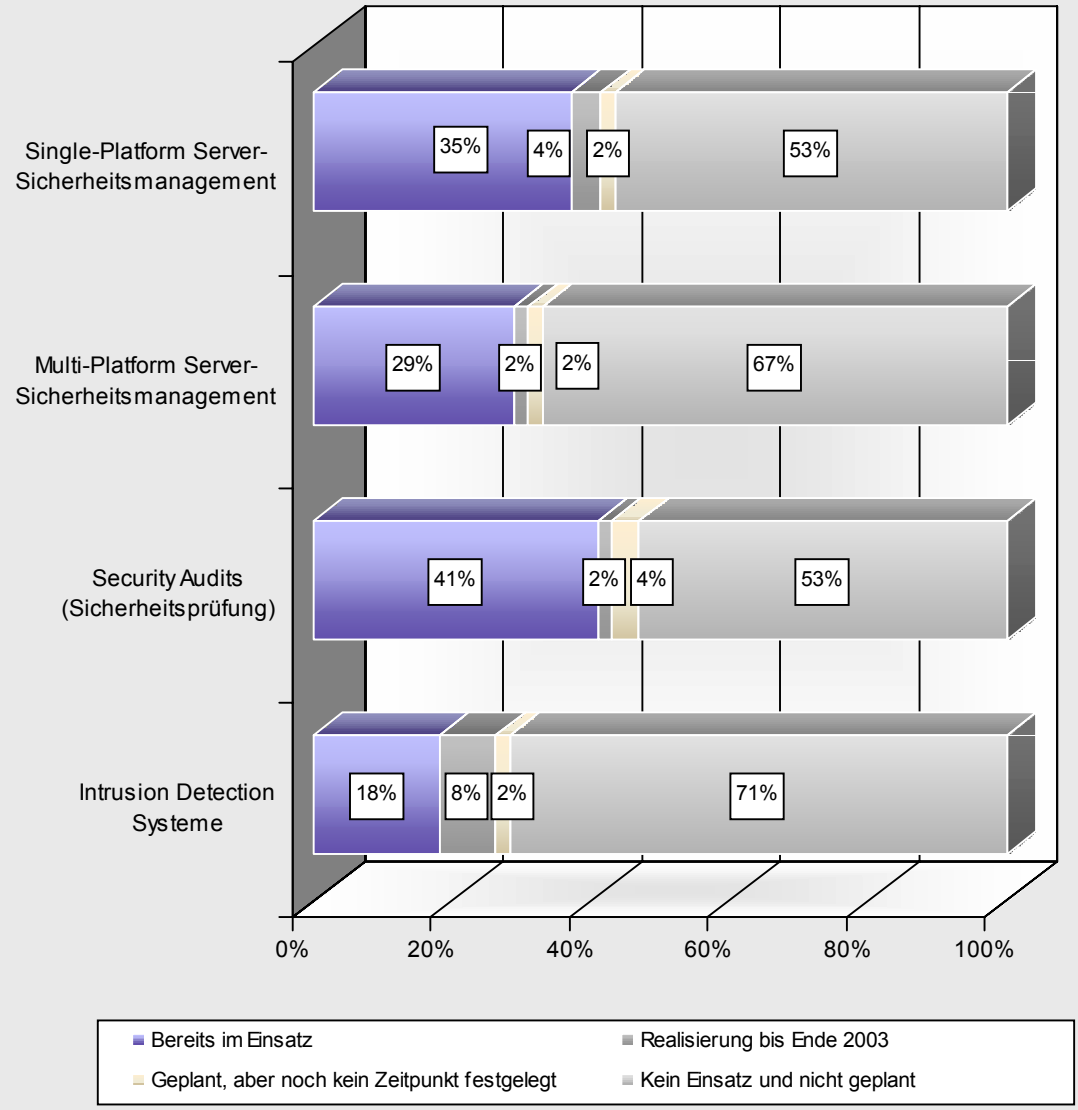


Quelle: META Group Deutschland

Basis: 66 Unternehmen

Abbildung 70: Einsatz und Planung bei Administration, Monitoring und Audit (50–199 Mitarbeiter)

Haben Sie folgende IT-Sicherheitslösungen im Bereich Administration, Monitoring und Audit implementiert oder planen Sie in den kommenden 12 Monaten deren Evaluierung oder Realisierung? *(200-499 MA)*

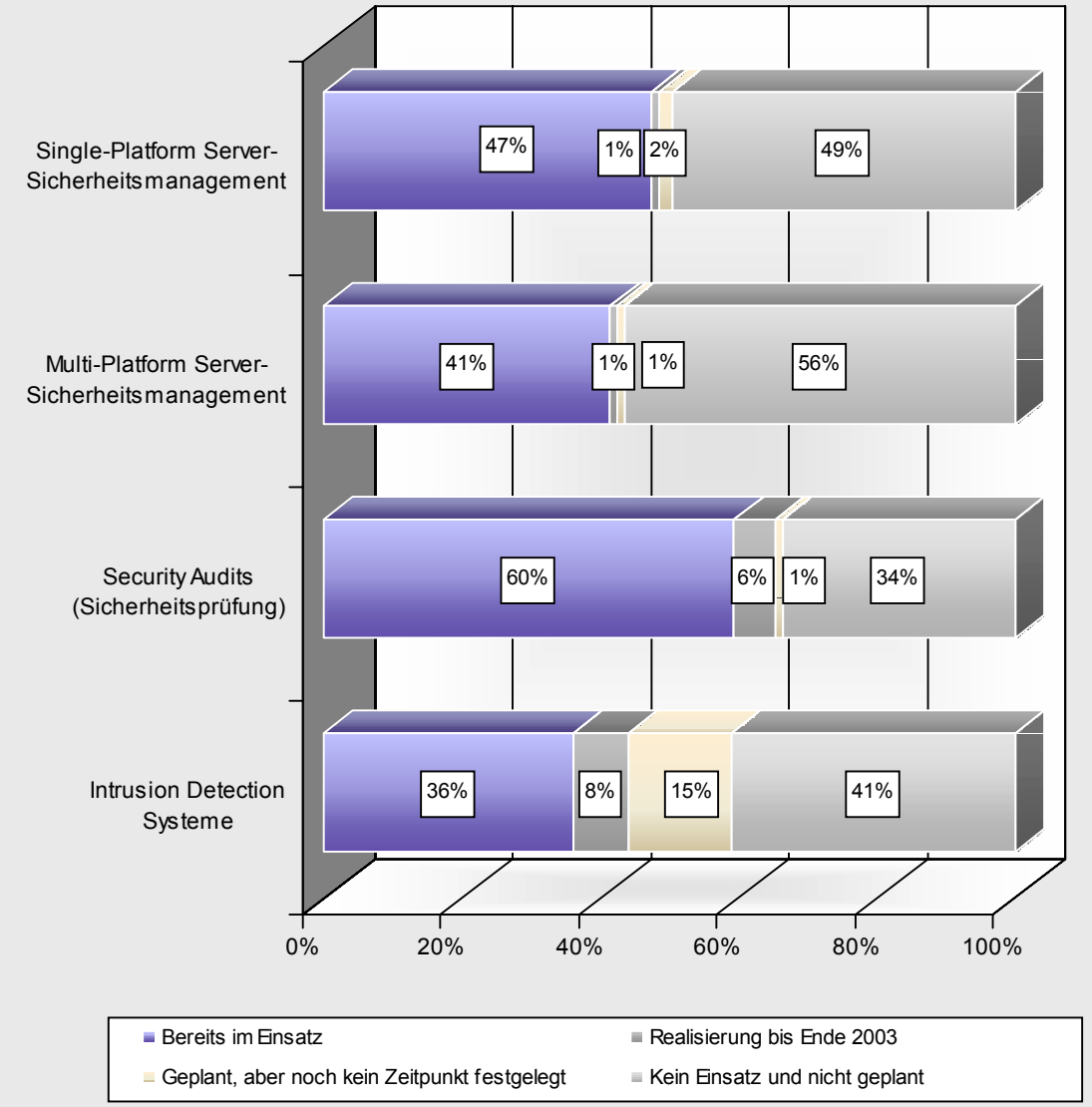


Quelle: META Group Deutschland

Basis: 48 Unternehmen

Abbildung 71: Einsatz und Planung bei Administration, Monitoring und Audit (200-499 Mitarbeiter)

Haben Sie folgende IT-Sicherheitslösungen im Bereich Administration, Monitoring und Audit implementiert oder planen Sie in den kommenden 12 Monaten deren Evaluierung oder Realisierung? *(500 und mehr MA)*



Quelle: META Group Deutschland

Basis: 89 Unternehmen

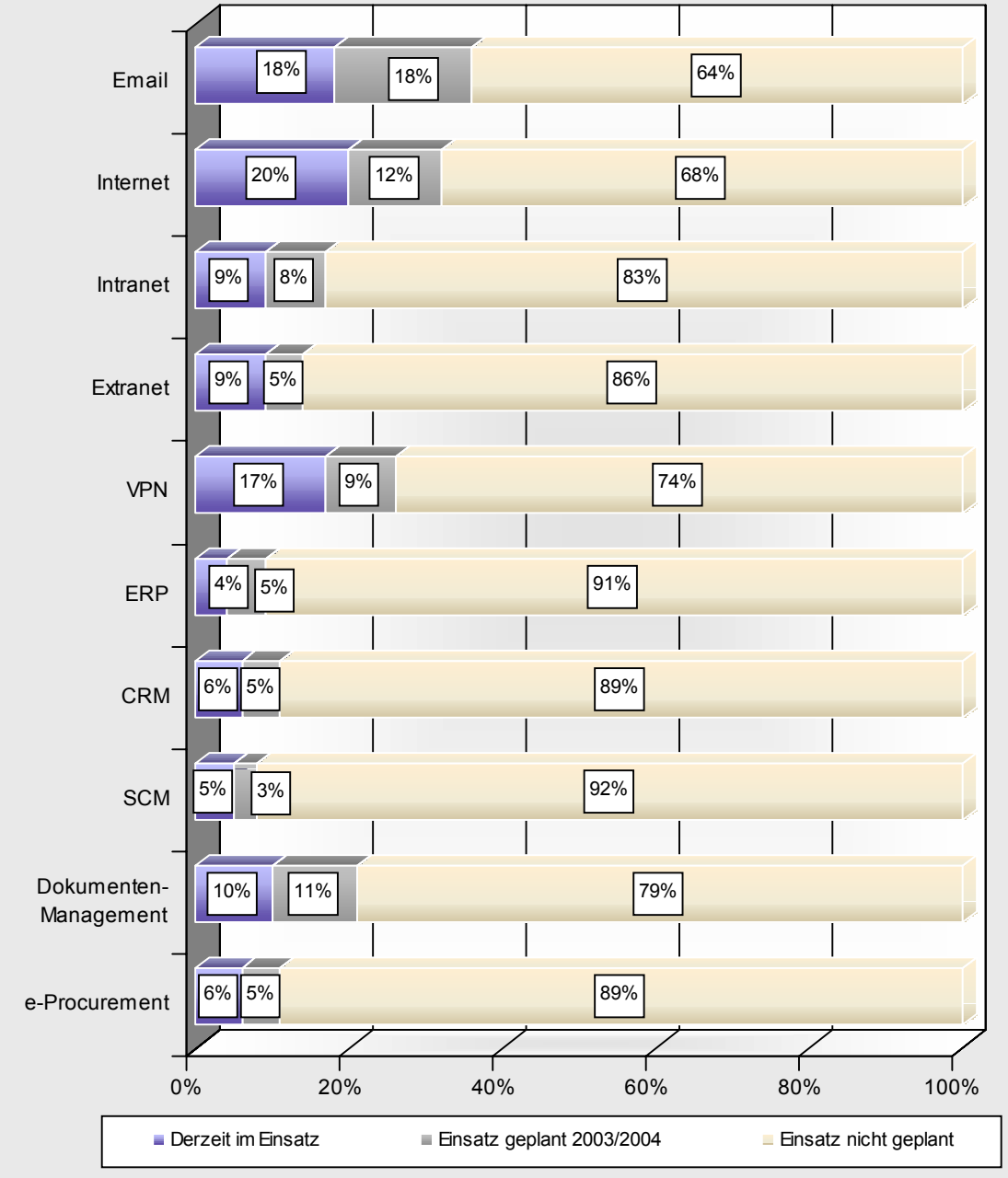
Abbildung 72: Einsatz und Planung bei Administration, Monitoring und Audit (ab 500 Mitarbeiter)

6.2 Vorhaben in spezifischen Bereichen

6.2.1 Digitale Signatur

Der Einsatz digitaler Zertifikate erfolgte bei den befragten Anwenderunternehmen bislang primär im Zusammenhang mit Internetanwendungen (20 Prozent der Befragten), Email (18 Prozent) und VPN (17 Prozent). Etwa jedes zehnte Unternehmen setzte digitale Zertifikate für Dokumentenmanagement, Extranet und Intranet ein. ERP-Software, CRM, SCM und e-Procurement werden seltener mittels elektronischer Zertifikate abgesichert. Bei der Planung für 2003/04 ziehen die Unternehmen primär in den Bereichen Email, Internet und Dokumentenmanagement digitale Zertifikate in Betracht. Betrachtet man aber den geplanten prozentualen Zuwachs des Einsatzgrades in den einzelnen Anwendungsbereichen, so ergibt sich durchweg eine Wachstumsrate von deutlich über 50 Prozent bis spätestens Ende 2004.

In welchen der folgenden Bereiche werden digitale Zertifikate eingesetzt bzw. wo ist in den kommenden 24 Monaten der Einsatz geplant?



Quelle: META Group Deutschland

Basis: 203 Unternehmen

Abbildung 73: Einsatz digitaler Zertifikate in einzelnen Anwendungsbereichen

6.2.2 Virtual Private Networks

Die Unternehmen wurden im Rahmen der vorliegenden Untersuchung gefragt, welche VPN-Technologien ihre Anforderungen am besten abdecken. Eine klare Mehrheit von 73 Prozent der Unternehmen ist der Meinung, dass dies auf das Internet-VPN zutrifft. Die anderen VPN-Technologien folgen in der Rangliste mit großem Abstand, wobei das ATM-basierte VPN mittlerweile das Schlusslicht bildet.

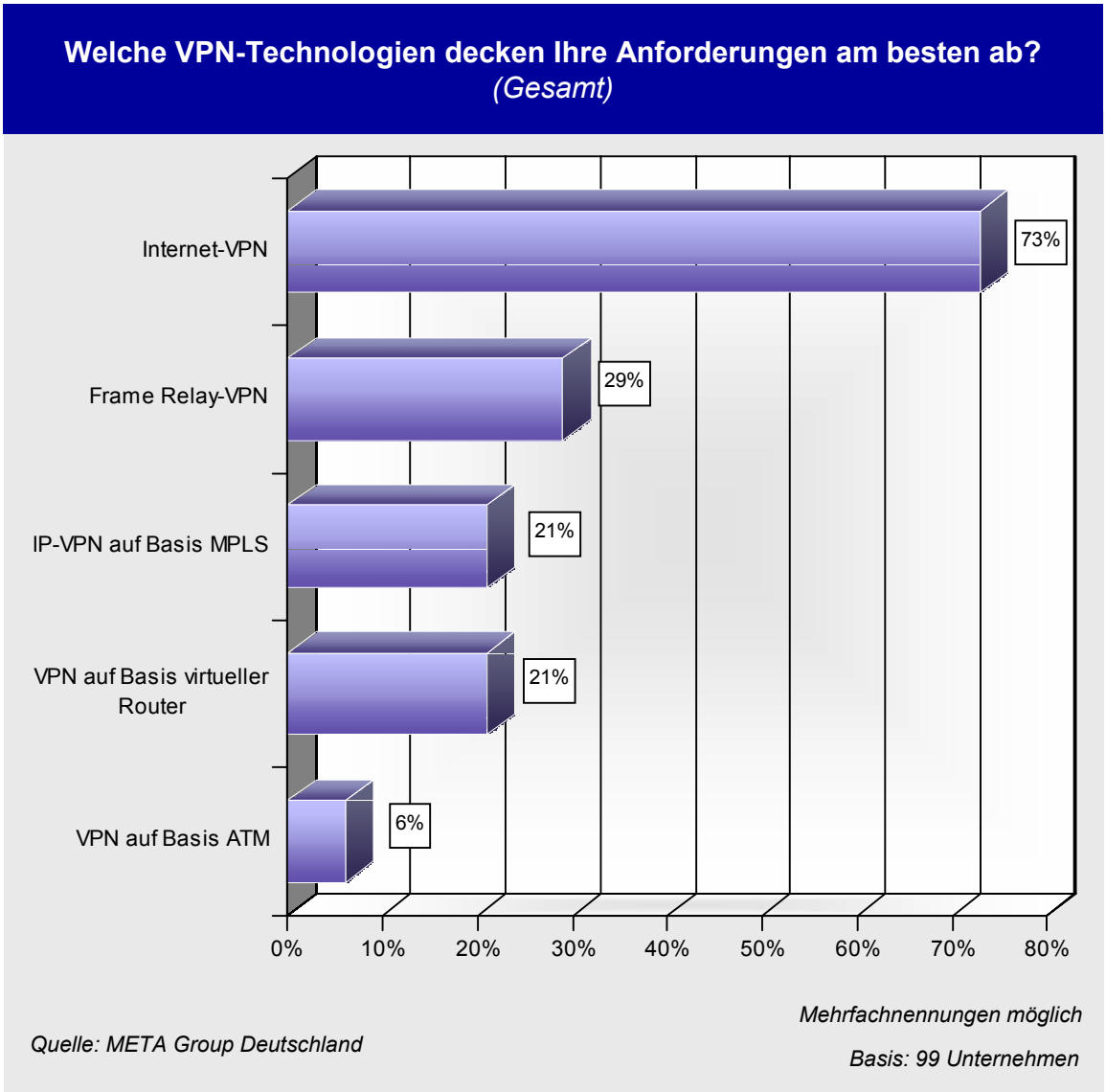


Abbildung 74: Abdeckung von Anforderungen durch einzelne VPN-Technologien

6.2.3 Email- und Content-Security

Die primäre Zielsetzung der deutschen Unternehmen beim Einsatz von Lösungen für Content-Security-Management (einschließlich Web-Filtering) ist der Schutz der Netzwerkinfrastruktur vor Virenattacken. Rechtliche Aspekte der Web-Nutzung, etwa im Zusammenhang mit der Verbreitung illegaler oder „politisch unkorrekter" Inhalte, spielen noch eine kleinere Rolle. Auch die Erhöhung der Mitarbeiterproduktivität und der Netzwerkbandbreite durch die Kontrolle der Internet-Nutzung stehen nicht im Vordergrund der Zielsetzungen. Dies korreliert zu der an früherer Stelle beobachteten Bewertung der Anwender zu allgemeinen Sicherheitsrisiken: Auch dort wurden Virenattacken und Hacker als höchstes Risiko eingeschätzt, während „political correctness" eine kleinere Rolle spielte. Damit treffen die Marketingbotschaften und Kaufargumente der führenden Anbieter zu einem gewissen Teil ins Leere. Es sind nach Einschätzung der META Group noch große Anstrengungen notwendig, um die deutschen Unternehmen für das Thema zu sensibilisieren. Dies ist für die Anbieter in diesem Marktsegment von hoher Bedeutung, müssen sich diese doch von klassischen Virenschutz-Anbietern differenzieren können. Ansatzpunkte für Awareness-Kampagnen gibt es durchaus, beispielsweise über den Hinweis auf allgemeine rechtliche Rahmenbedingungen, die ja im Rahmen der vorliegenden Untersuchung als wichtige Entscheidungsgrundlage für IT-Security insgesamt genannt wurden. Derzeit allerdings sind in Deutschland die potenziellen rechtlichen Implikationen beim Missbrauch von Email und Internet durch Mitarbeiter etwas unklarer als in den USA. „Wo kein Kläger, da kein Richter" ist das Motto, nach dem in Deutschland derzeit verfahren wird. Im Gegenteil: Das Misstrauen gegenüber Maßnahmen, die als Überwachung der Mitarbeiter interpretiert werden können, ist erheblich, und Entscheidungen über den Einsatz entsprechender Lösungen bedürfen der Mitsprache des Betriebsrats.

Nichtsdestotrotz gibt es Unterschiede zwischen einzelnen Branchen und Unternehmensgrößen. So misst der Mittelstand Gesichtspunkten der Produktivitätserhöhung durch Web- und Email-Filtering überdurchschnittliche Bedeutung bei, und auch die prozessorientierte Fertigung ist diesbezüglich sensibler – im Gegensatz insbesondere zum Banken- und Versicherungssektor. Die Vermeidung rechtlicher Risiken hingegen spielt für Banken und Versicherungen, für die diskrete Fertigung und die öffentliche Hand eine überdurchschnittliche Rolle.

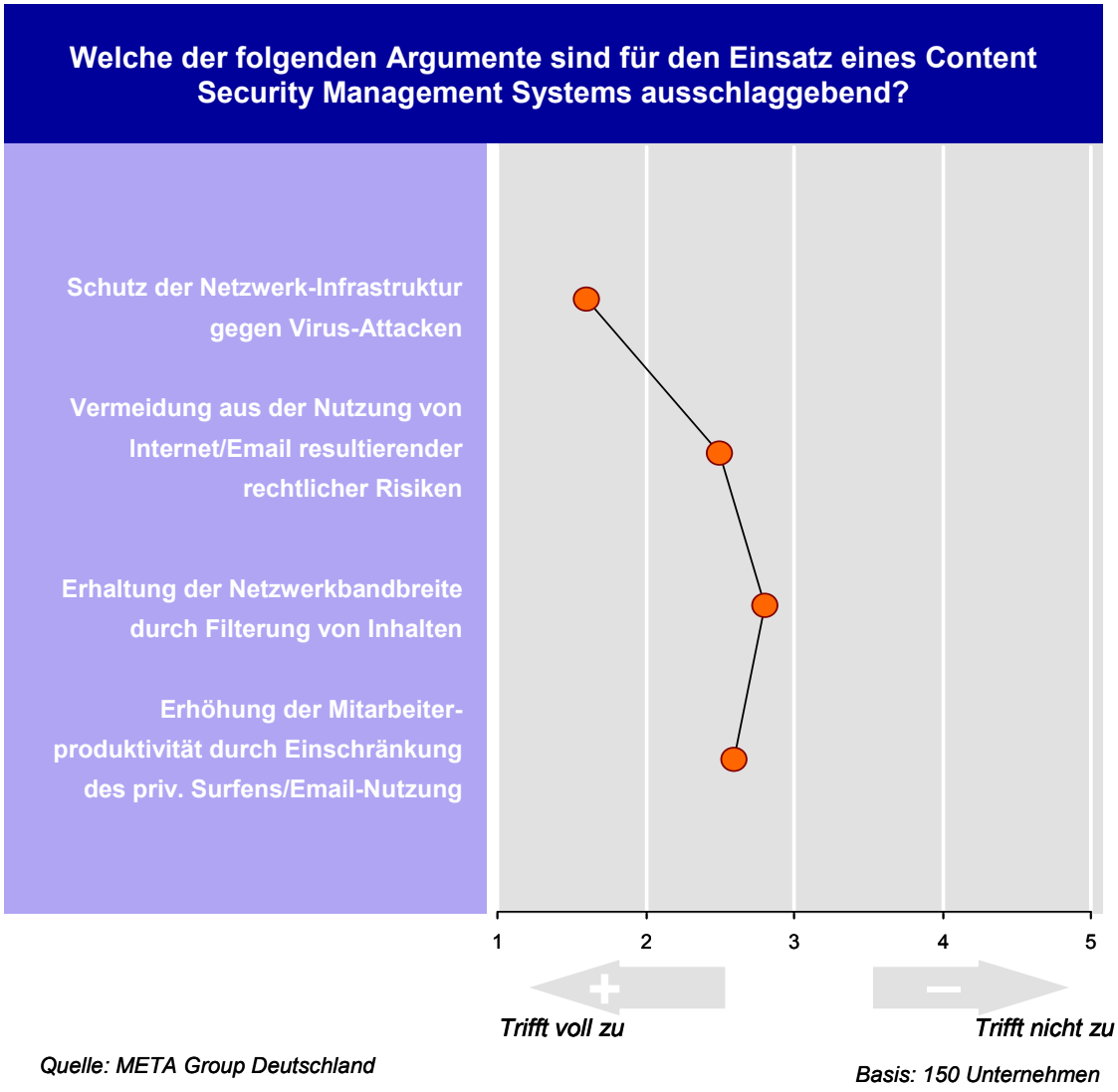
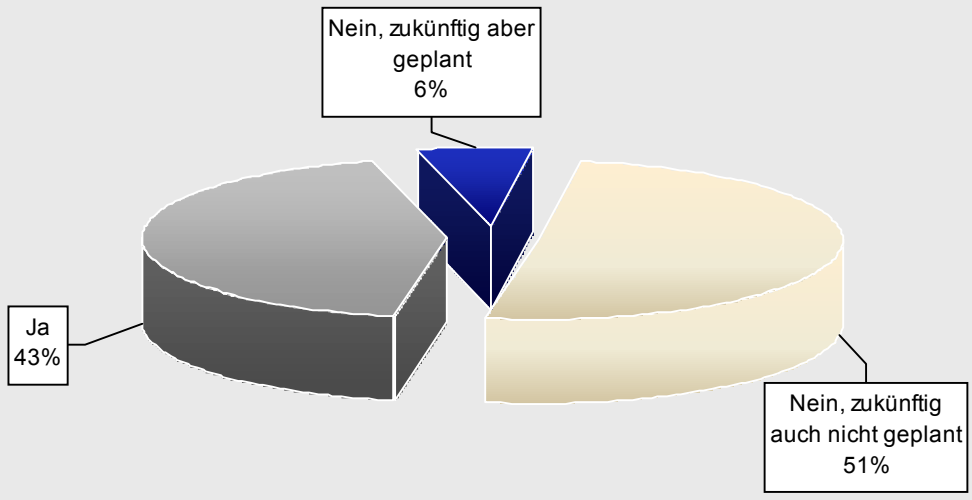


Abbildung 75: Argumente für den Einsatz eines Content-Security-Management-Systems

43 Prozent der befragten Unternehmen geben an, für Virenschutz beziehungsweise Content Filtering eine E-Mail Appliance einzusetzen. Weitere sechs Prozent planen den künftigen Einsatz einer derartigen Appliance (siehe Abbildung 76). Im Branchenvergleich sind Banken und Versicherungen führend beim Einsatz von Appliances, im Gegensatz zur öffentlichen Hand, die diesbezüglich bislang zurückhaltend war. Immerhin planen mit Ausnahme des Dienstleistungssektors vier bis neun Prozent der befragten Unternehmen in allen anderen Branchen den zukünftigen Einsatz.

Bei E-Mail Appliances handelt es sich um kombinierte Hardware-Software-Lösungen, zum Beispiel E-Mail Appliances am Gateway beziehungsweise als Messaging Routing Hub. Die Anbieter solcher Lösungen umwerben ihre Zielgruppen vor allem mit dem Argument einer schnellen Einsetzbarkeit und kalkulierbarer Kosten. Die Ergebnisse der Anwenderbefragung zeigen zwar, dass im Mittelstand aktuell nur jedes dritte Unternehme eine Email Appliance einsetzt, aber künftig werden die Einsatzgrade im Mittelstand in ähnlichen Größenordungen ansteigen wie bei Großunternehmen.

Wenn Virenschutz / Content Security im Einsatz oder geplant:
Nutzen Sie so genannte „E-Mail Appliances“ für Virenschutz bzw. Content Security, oder haben Sie deren Einsatz geplant?



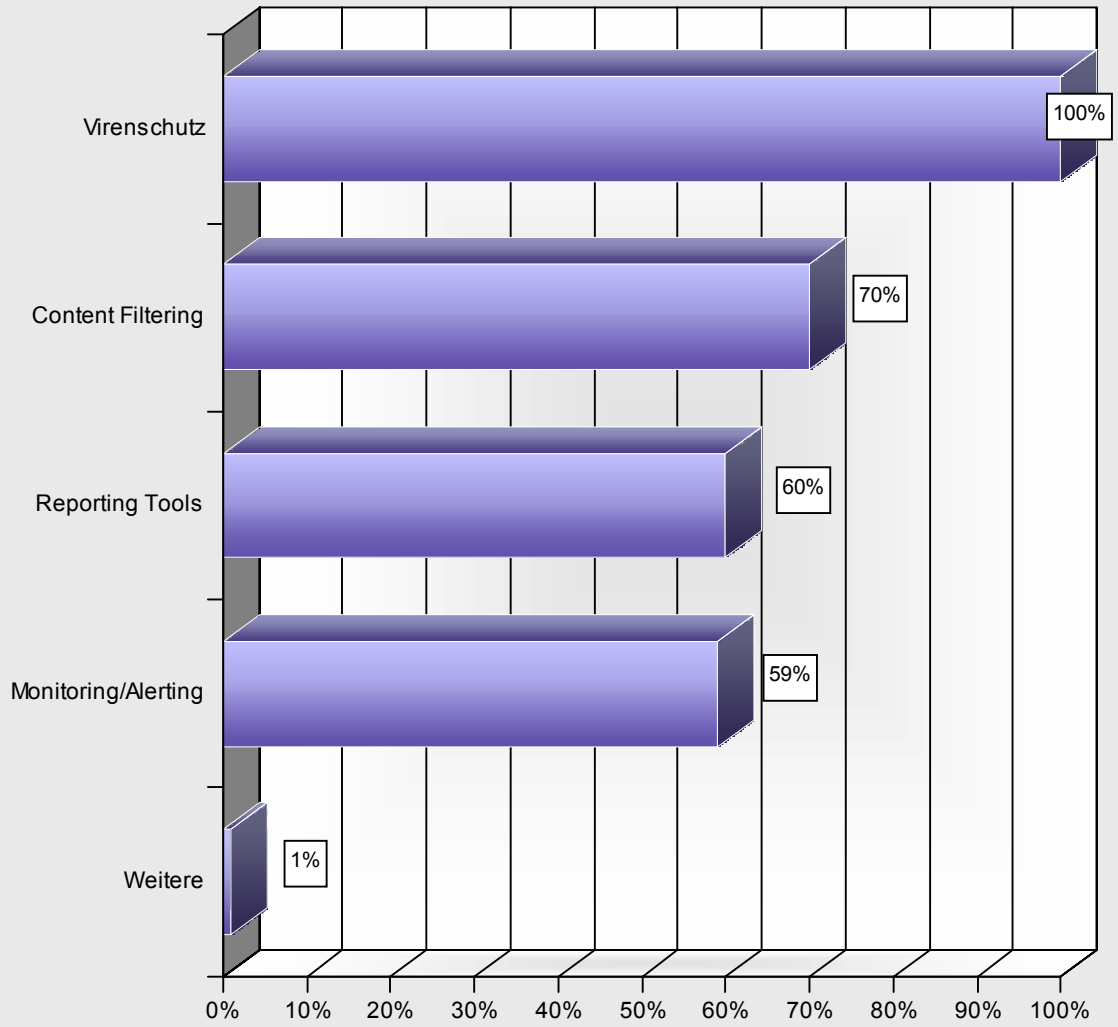
Quelle: META Group Deutschland

Basis: 204 Unternehmen

Abbildung 76: Einsatzplanung von E-Mail Appliances für Virenschutz / Content Filtering

Im Vordergrund der gewünschten Funktionalitäten einer E-Mail Appliance steht bei den befragten Anwendern generell der Virenschutz, gefolgt von Content Filtering. Mehr als die Hälfte der Anwenderunternehmen wünscht sich auch Reporting Tools und Monitoring-/Alerting-Features.

Falls eine E-Mail-Appliance im Einsatz oder geplant ist:
Welche Funktionalitäten erwarten Sie von einer E-Mail Appliance?



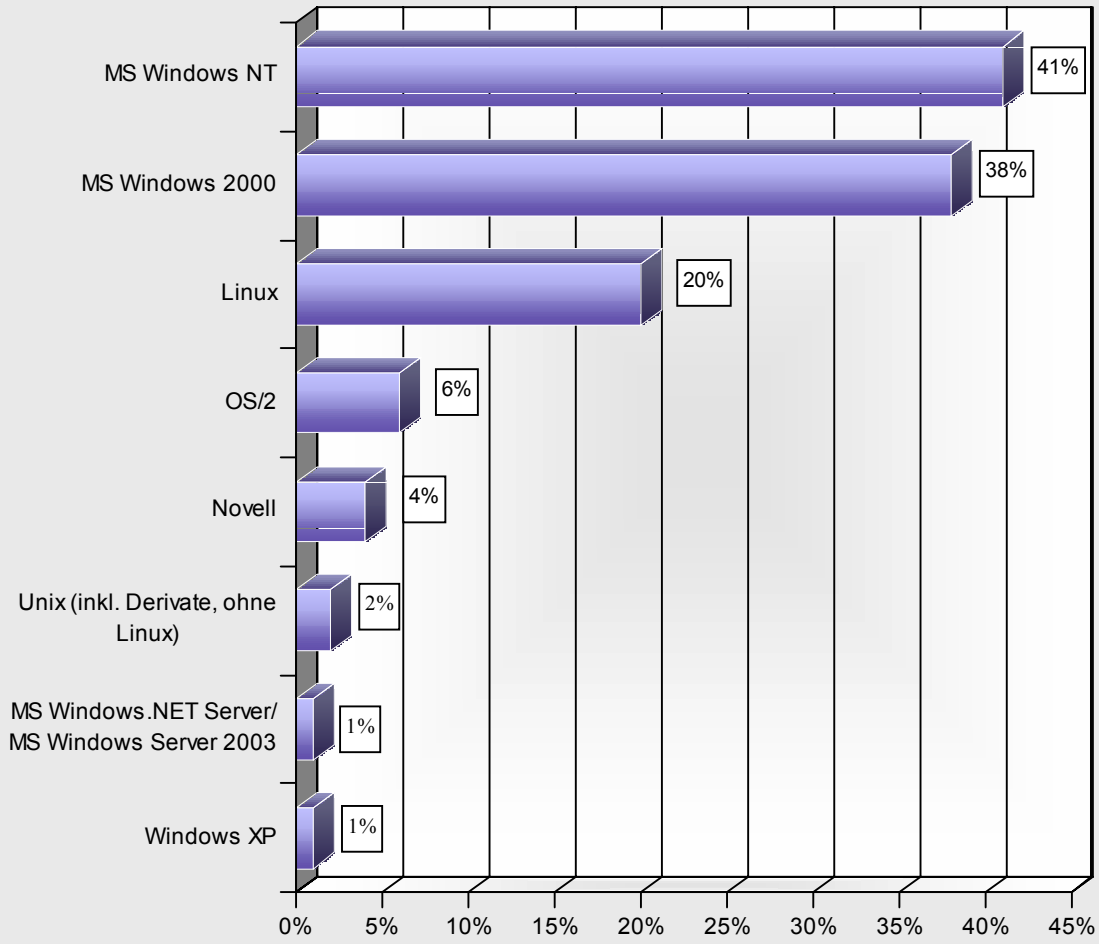
Quelle: META Group Deutschland

Mehrfachnennungen möglich
Basis: 97 Unternehmen

Abbildung 77: Erwartete Funktionalitäten einer Email Appliance

Am häufigsten sollen E-Mail Appliances auf Microsoft Windows NT (41 Prozent der Befragten) oder Windows 2000 (38 Prozent) aufsetzen. Auch Linux ist mit 20 Prozent der Nennungen relativ stark als Server-Betriebssystem im Gespräch. Daher ist es auch nicht verwunderlich, dass einige Anbieter ihre Appliances auf Linux portieren. Erstaunlich gering ist bei dieser offen gestellten Frage der Anteil der anderen möglichen Betriebssysteme.

Falls eine E-Mail-Appliance im Einsatz oder geplant ist:
Auf welchem (Server)-Betriebssystem setzt die E-Mail Appliance auf bzw. soll sie aufsetzen?



Quelle: META Group Deutschland

Mehrfachnennungen möglich
Basis: 96 Unternehmen

Abbildung 78: Bevorzugte (Server-) Betriebssysteme für E-Mail Appliances

In Rahmen der Studie wurden die Anwenderunternehmen zur Anzahl der Emails befragt, die pro Mitarbeiter täglich empfangen werden, sowie zum Anteil der nicht geschäftsrelevanten beziehungsweise Werbemails. Es wird an dieser Stelle ausdrücklich darauf hingewiesen, dass es sich bei den folgenden Angaben um exemplarische Werte der direkten oder indirekten Entscheidungsträger im Bereich der IT-Sicherheit handelt. Diese erhalten täglich durchschnittlich 37 Emails. 20 Prozent dieser Emails sind nach eigenem Bekunden nicht geschäftsrelevant oder Werbemails. Zahlen zu Anwendern in anderen Unternehmensbereichen liegen nicht vor. Dennoch sind die prozentualen Werte als guter Anhaltspunkt auch für andere Nutzergruppen zu betrachten.

Die META Group schätzt, dass 2002 bei global aufgestellten Unternehmen allein SPAM im engeren Sinne einen Anteil von zwei bis zehn Prozent der eingehenden Kommunikation ausmachte. Dieser Anteil wird in den nächsten Jahren auf 10 bis 20 Prozent wachsen. Bei manchen Unternehmen liegt bereits heute der Anteil an eingehenden Mails, die als SPAM zu klassifizieren sind, bei bis zu 40 Prozent.

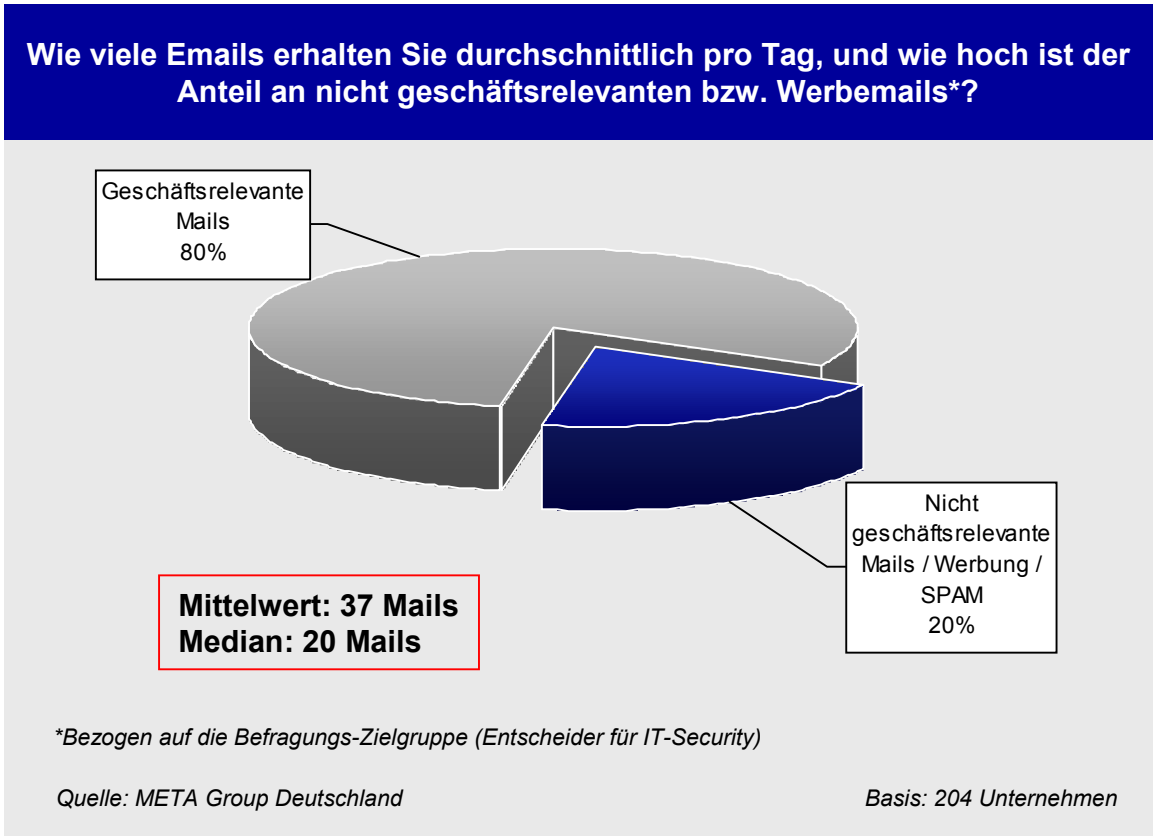


Abbildung 79: Anteil nicht geschäftsrelevanter Mails / SPAM / Werbung

Virenschutzlösungen und Email-Verschlüsselung sind in gewissem Umfang konträre Maßnahmen; das heißt es besteht die Gefahr, dass sie sich gegenseitig in ihrer Wirkung behindern, da verschlüsselte Emails nicht ohne weiteres durch AV-Tools geprüft werden können. Eine Koordination von Virenschutz-Maßnahmen und Verschlüsselung ist jedoch unabdingbar. Von der technischen Seite betrachtet können Emails am Gateway auf Viren gescannt werden, wenn bereits dort die Entschlüsselung erfolgt. Sollte eine End-to-End-Verschlüsselung geplant sein, ist eine Client-Virenschutzlösung notwendig. Anbieter von Email-Sicherheitslösungen adressieren teilweise diesen Aspekt mit integrierten Lösungen beziehungsweise Frameworks.

42 Prozent der befragten Unternehmen, die Virenschutz- und Verschlüsselungslösungen für Email-Systeme im Einsatz haben, setzen diese bereits gleichzeitig ein, das heißt verschlüsselte Emails werden auch auf Viren untersucht. Offen bleibt allerdings die Frage, ob die Wirkung und Effizienz dieser Maßnahmen ausreichend sind.

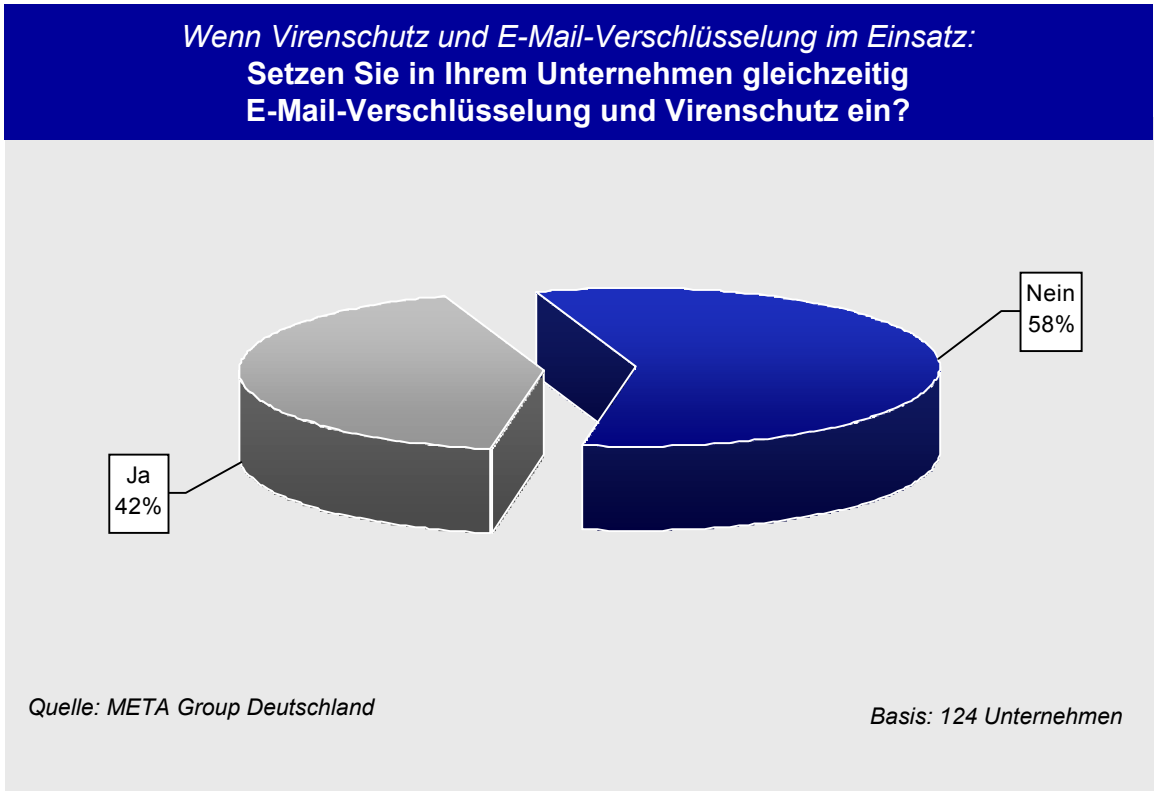


Abbildung 80: Paralleler Einsatz von Email-Verschlüsselung und Virenschutz

Ergänzend zur Frage, ob der gleichzeitige Einsatz von Virenschutz und Verschlüsselung erfolgt, geben die Anwenderunternehmen nähere Auskunft zur konkreten Integration dieser beiden Funktionalitäten. 96 Prozent der Befragten greifen in diesem Zusammenhang auf Standardlösungen zurück, nur vier Prozent haben eigenentwickelte „Custom"-Lösungen im Einsatz.

Eine nähere Analyse dieser Daten zeigt, dass die eigenentwickelten Individuallösungen im Wesentlichen bei kleineren und mittelgroßen Institutionen im Banken-, Versicherungs- und Finanzdienstleistungssektor im Einsatz sind (siehe Abbildung auf der folgenden Seite). Es wird darauf hingewiesen, dass dieser Analyse eine kleine Stichprobe zugrunde liegt und die Werte nur als Trendaussagen gelten können.

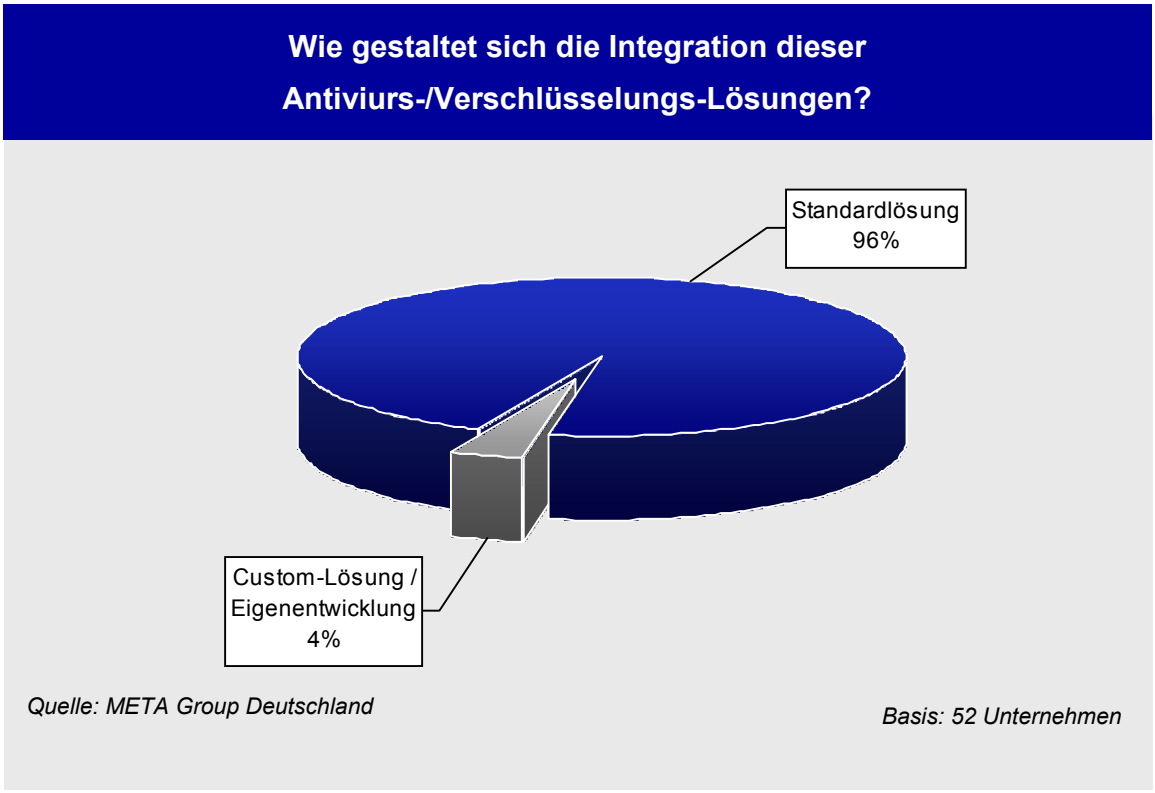
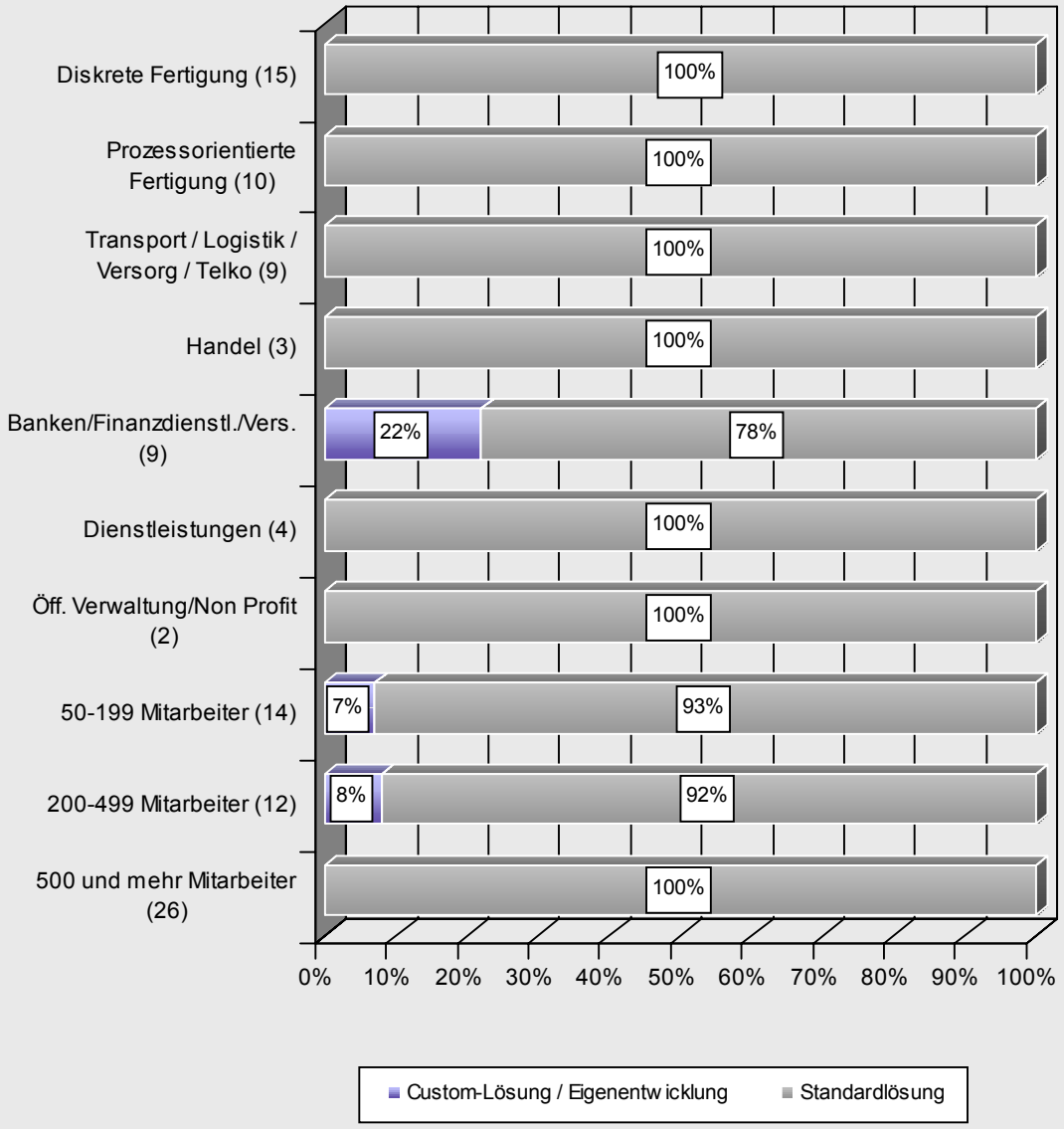


Abbildung 81: Integration von AV- und Verschlüsselung – Standard- vs. Custom-Lösung

Wie gestaltet sich die Integration dieser AV-/Verschlüsselungs-Lösungen?



Quelle: META Group Deutschland

(X): Anzahl der Nennungen

Abbildung 82: Integration von AV- und Verschlüsselung – nach Branche/Unternehmensgröße

Bei 48 Prozent der befragten Unternehmen erfolgt eine zentrale Archivierung der ein- und ausgehenden Emails. Damit soll der zunehmenden Bedeutung von Emails in Hinsicht auf geschäftsrelevante Kommunikation Rechnung getragen werden. Der Anteil zentraler Archivierung ist nach Einschätzung der META Group relativ hoch. Es ist nicht auszuschließen, dass eine Vermischung der Begriffe „zentrale Archivierung“ und „zentraler Server“ vorliegt.

IT-Verantwortliche plädieren typischerweise für eine Beschränkung des gespeicherten Posteingangs- und Ausgangsvolumens, um Kosten zu reduzieren, die Email-Server-Recovery-Zeit niedrig zu halten und das Backup zu vereinfachen. Archivierungssysteme bieten einen Kompromiss, indem Nachrichten vom Email-Server auf alternative Server heruntergeladen werden und somit den Nutzern sofort zur Verfügung stehen, ohne den Email-Server zu belasten.

Die META Group rät, möglichst nur Emails zu archivieren, wenn entsprechende rechtliche Anforderungen bestehen. Die Archivierungszeit sollte sich auf die rechtlich notwendige beschränken. IT-Abteilungen sollten zusammen mit der Rechtsabteilung, der Personalabteilung (HR) und dem Management entsprechende Email-Archivierungs-Policies auf- und umsetzen.

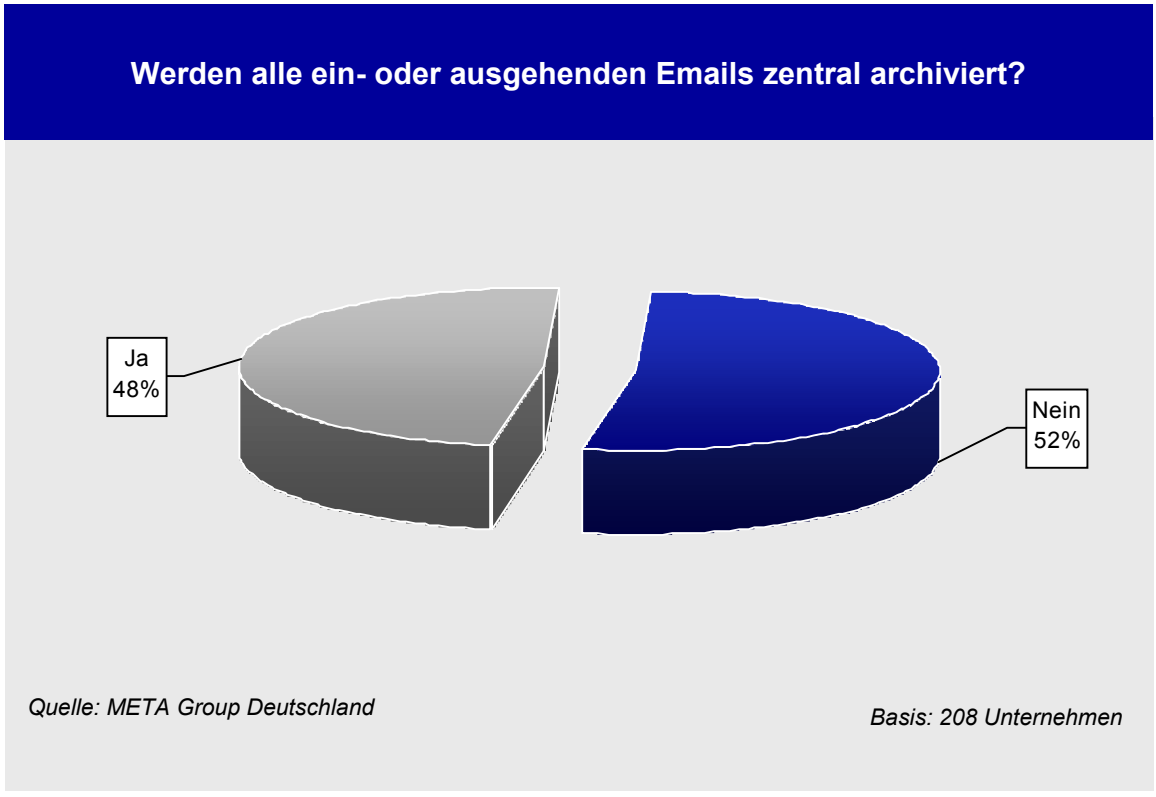


Abbildung 83: Archivierung von Emails

63 Prozent der befragten Anwenderunternehmen setzen Emails primär „informativ“ ein, bei den restlichen 37 Prozent der Befragten haben Emails teilweise auch den Charakter einer rechtsverbindlichen Willenserklärung, beispielweise im Zusammenhang mit der Bestellung von Waren oder der Abgabe von Angeboten.

Die Analyse nach Branchen und Unternehmensgröße zeigt, dass vor allem große Mittelständler und Großunternehmen sowie die Gruppe der Logistik-, Telekommunikations- und Versorgungsunternehmen Emails rechtsverbindlich einsetzen (siehe Abbildung 85).

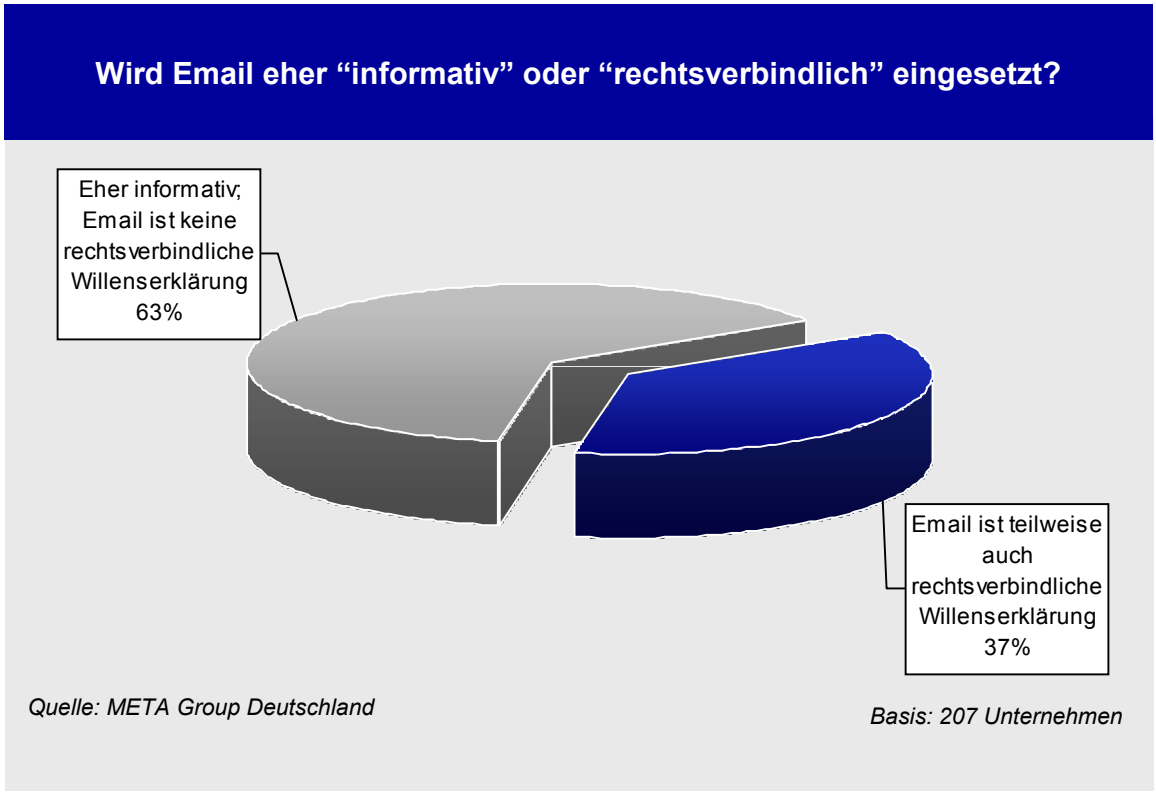
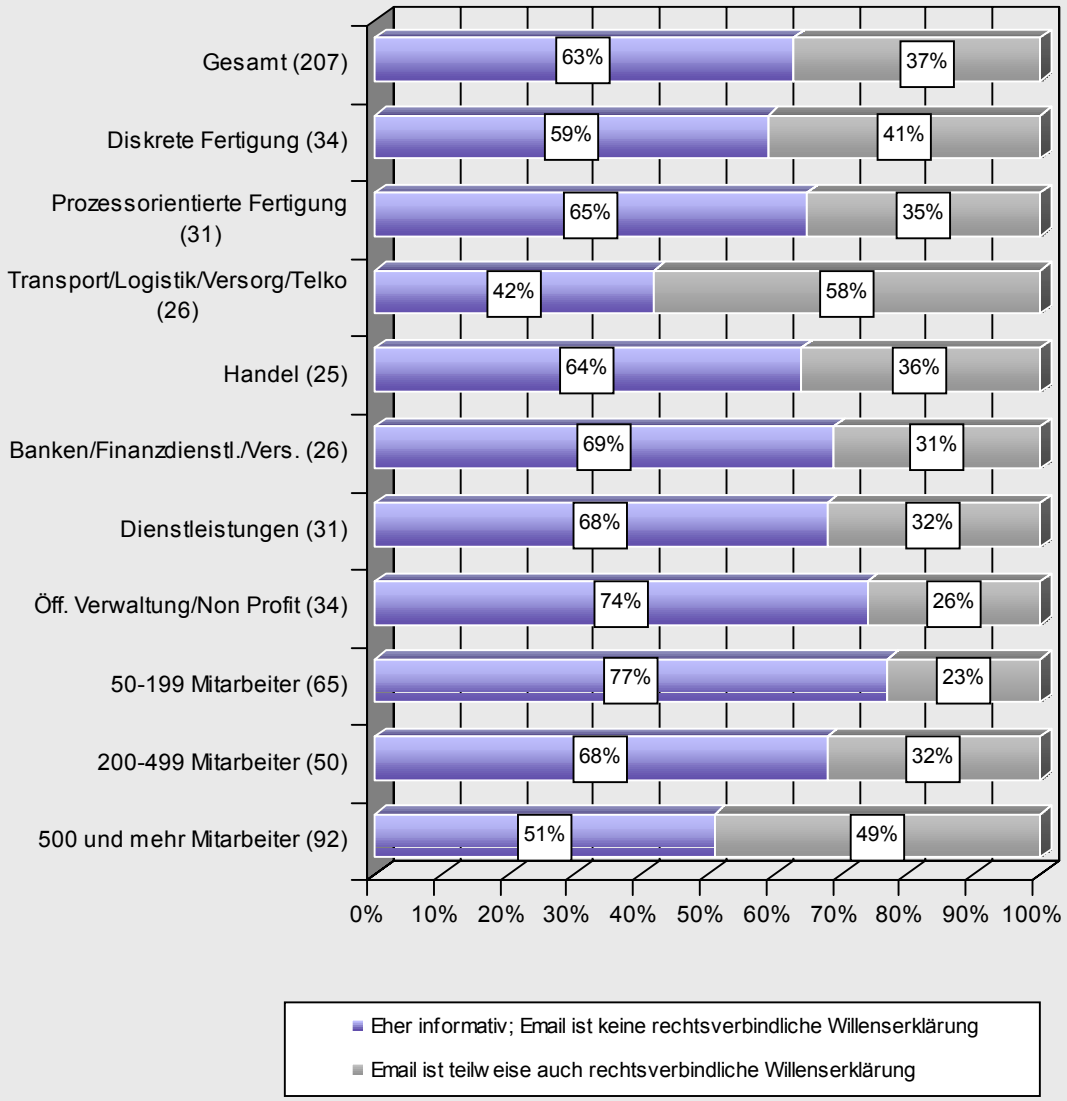


Abbildung 84 „Informativer“ vs. „rechtsverbindlicher“ Einsatz von Emails

Wird Email eher “informativ” oder “rechtsverbindlich” eingesetzt?



Quelle: META Group Deutschland

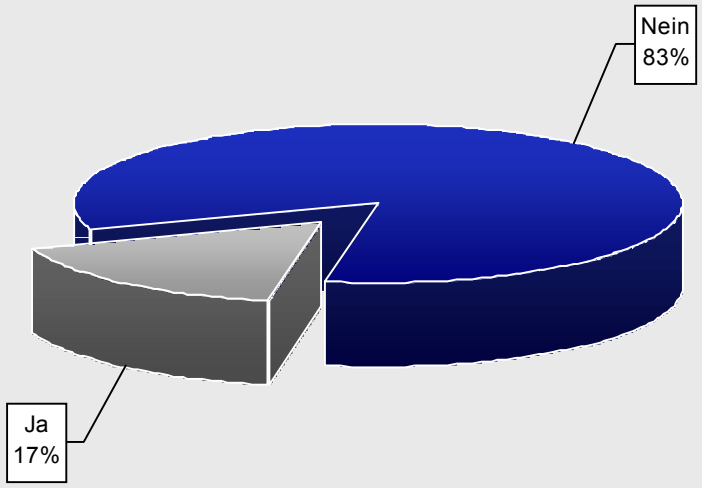
(X): Anzahl der Nennungen

Abbildung 85: „Informativer“ vs. „rechtsverbindlicher“ Einsatz von Emails – nach Branchen und Unternehmensgrößenklassen

Ein Legal Disclaimer (Haftungsausschlusserklärung) als Zusatz zur Email bietet die Möglichkeit, mehr Rechtssicherheit im Umgang mit Emails zu schaffen und gegebenenfalls Haftungsansprüche abzuwehren. Die Rechtslage besagt, dass eine so genannte Willenserklärung in jeder Gestalt angenommen werden kann, sofern keine Schriftform vorgeschrieben ist und man dem Verhalten nach dem Empfängerhorizont einen Erklärungswert mit Rechtsbindungswillen beimessen kann. Dies gilt auch für Emails. Der elektronischen Signatur bedarf eine Email nur dann zur Rechtsverbindlichkeit, wenn die in ihr wiedergegebene Willenserklärung gesetzlich vorgeschrieben der Schriftform bedarf.

Dennoch nutzen nur 17 Prozent der befragten Anwender einen Legal Disclaimer. Dies deckt eine klare Diskrepanz in Bezug auf den Charakter der Email-Nutzung auf: Obgleich 63 Prozent der Unternehmen Emails eher informativ, das heißt nicht rechtsverbindlich einsetzen, stellt weniger als jedes fünfte Unternehmen sicher, dass die Haftung über einen Legal Disclaimer ausgeschlossen wird. Nur die Banken, Versicherungen und Finanzdienstleister erweisen sich in dieser Hinsicht als nahezu mustergültig: 50 Prozent verwenden Haftungsausschlusserklärungen (siehe Abbildung 87).

Ist die Rechtssicherheit Ihrer Email-Kommunikation durch Verwendung eines Legal Disclaimer (Haftungsausschlusserklärung) als Zusatz zur Email gewährleistet?

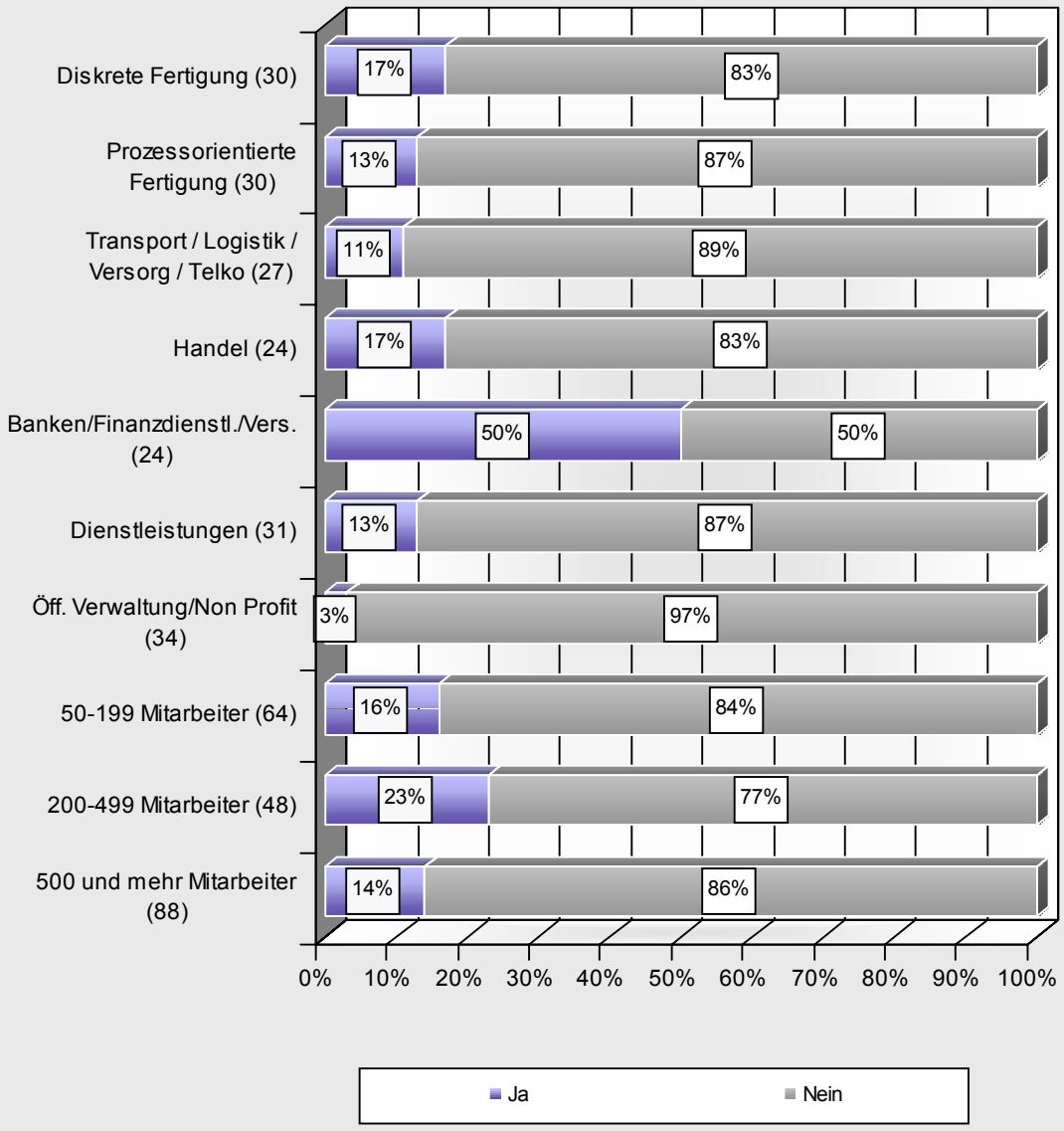


Quelle: META Group Deutschland

Basis: 200 Unternehmen

Abbildung 86: Verwendung eines Legal Disclaimer bei der Email-Kommunikation

Ist die Rechtssicherheit Ihrer Email-Kommunikation durch Verwendung eines Legal Disclaimer (Haftungsausschlusserklärung) als Zusatz zur Email gewährleistet?



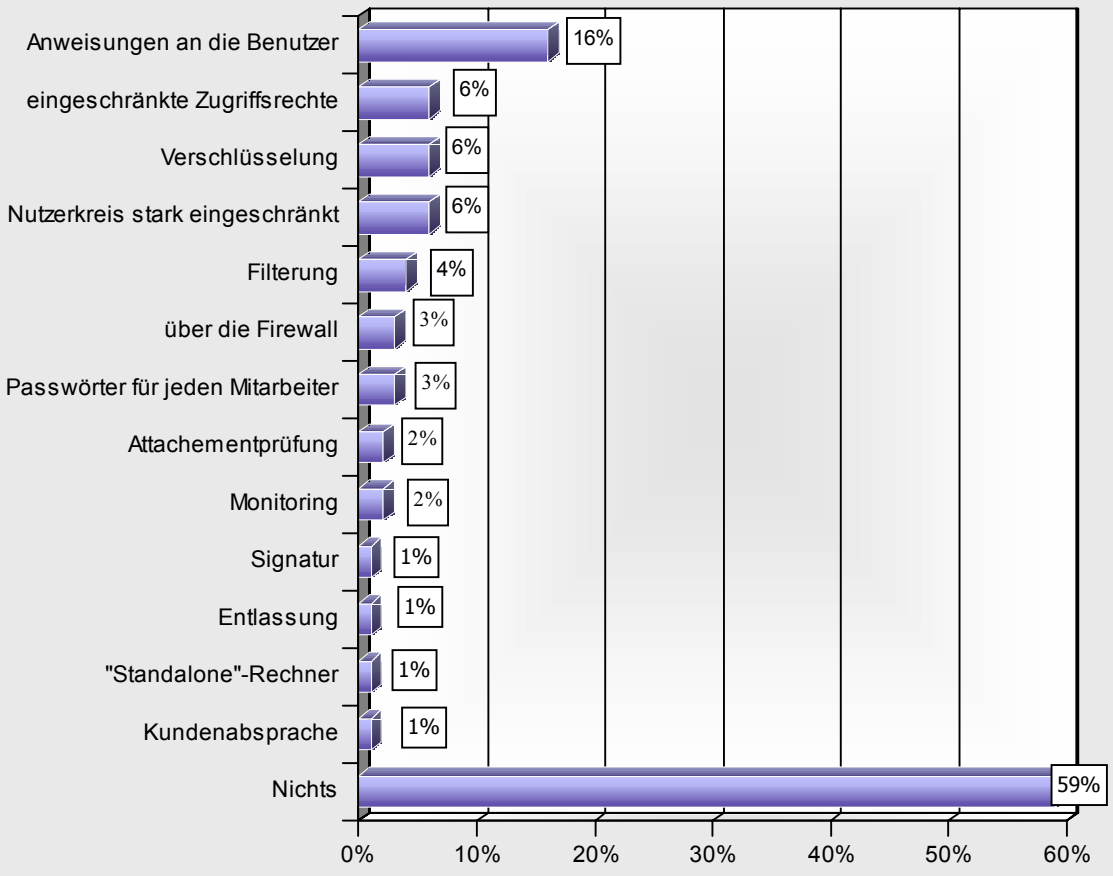
Quelle: META Group Deutschland

(X): Anzahl der Nennungen

Abbildung 87: Verwendung eines Legal Disclaimer – nach Branchen / Unternehmensgrößen

Befragt zu den Maßnahmen, die den Missbrauch von Emails zur Betriebsspionage verhindern sollen, geben 16 Prozent der Anwenderunternehmen an, den Nutzern entsprechende Anweisungen zu erteilen. Weitere relativ häufig genannte Maßnahmen sind die Einschränkung von Zugriffsrechten und Nutzerkreisen sowie die Verschlüsselung der Email-Kommunikation. Erst an fünfter Stelle der Maßnahmen steht die Filterung ein- und ausgehender Nachrichten. Dies ist erstaunlich, behaupten doch 54 Prozent der Befragten, grundsätzlich Content-Security-Produkte für Email einzusetzen. Dies legt den Schluss nahe, dass das Bewusstsein für Sicherheitsrisiken durch Industriespionage beziehungsweise für entsprechende Gegenmaßnahmen bei den Anwenderunternehmen noch nicht weit gediehen ist. Der mit 59 Prozent hohe Anteil an Unternehmen, die überhaupt keine technischen oder organisatorischen Maßnahmen gegen Industriespionage einleiten, bestätigt diese Annahme.

Welche Maßnahmen haben Sie ergriffen, um den Missbrauch von Emails zur Betriebsspionage zu unterbinden?
(Gesamt)



Mehrfachnennungen möglich

Quelle: META Group Deutschland

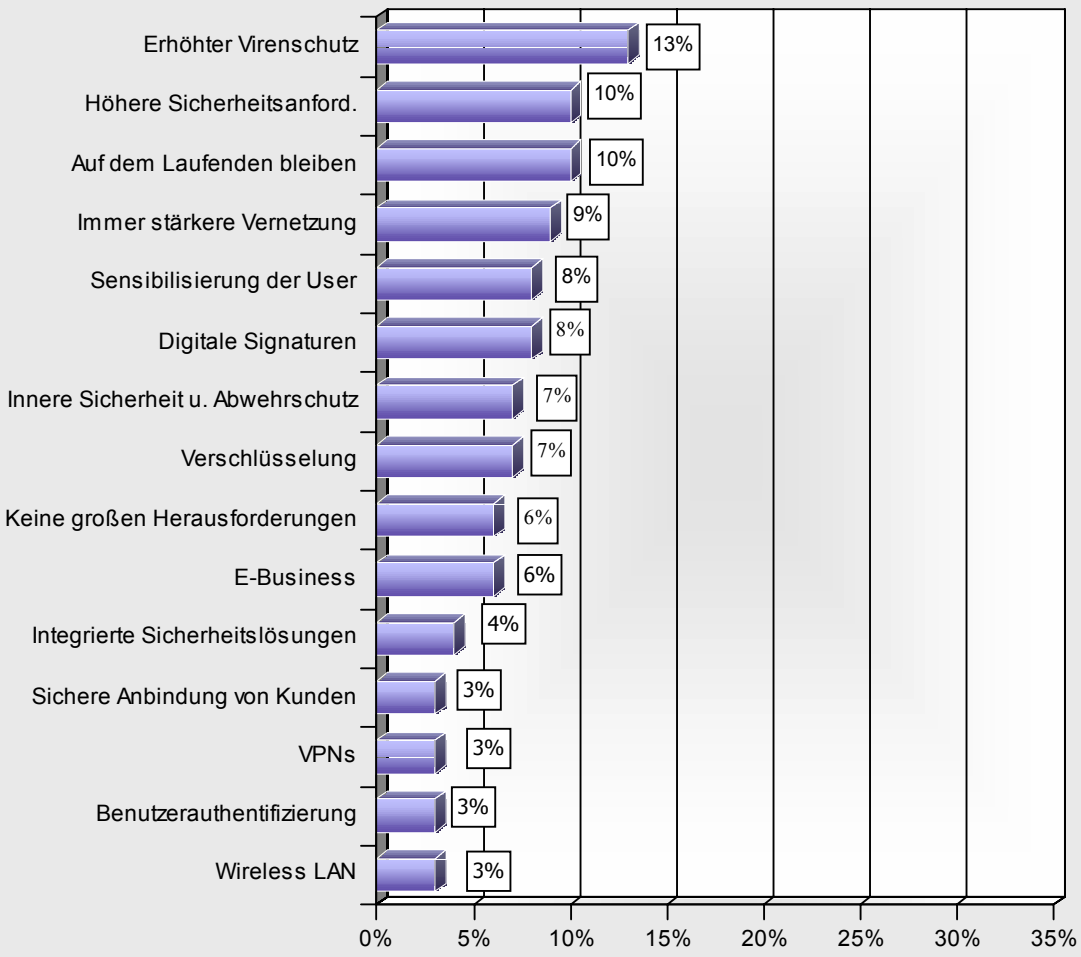
Basis: 198 Unternehmen

Abbildung 88: Maßnahmen gegen den Missbrauch von Emails zur Industriespionage

6.3 Zukünftige Herausforderungen

Als größte zukünftige Herausforderungen sehen die befragten Unternehmen den erhöhten Virenschutz, gefolgt von steigenden Sicherheitsanforderungen im Allgemeinen, dem Zwang, immer auf dem Laufenden bleiben zu müssen, der zunehmenden Vernetzung in der IT sowie der notwendigen Sensibilisierung der Nutzer und dem Einsatz digitaler Signaturen (vergleiche Abbildung 89 und Abbildung 90). Diese Rangliste variiert in Abhängigkeit von der Unternehmensgröße. Während bei Mittelständlern das Augenmerk stark auf Virenschutz liegt, sehen sich die größeren Unternehmen in weitaus höherem Ausmaß mit der nötigen Sensibilisierung der Nutzer im Unternehmen konfrontiert. Auch Unterschiede zwischen den Branchen sind zu verzeichnen: Banken und Versicherungen sowie die öffentliche Hand sehen die digitale Signatur als überdurchschnittlich große Herausforderung, die diskrete Fertigung sieht sich mit hohen Sicherheits-Anforderungen aus e-Business-Vorhaben konfrontiert, und bei der Kategorie der Logistik-, Telekommunikations- und Versorgungsunternehmen spielt die immer größere Vernetzung und Anbindung von Kunden eine wesentliche Rolle.

Welche Herausforderungen sehen Sie im Zusammenhang mit dem Thema IT-Security für die Unternehmen Ihrer Branche in den nächsten Jahren? [1]
(Gesamt)

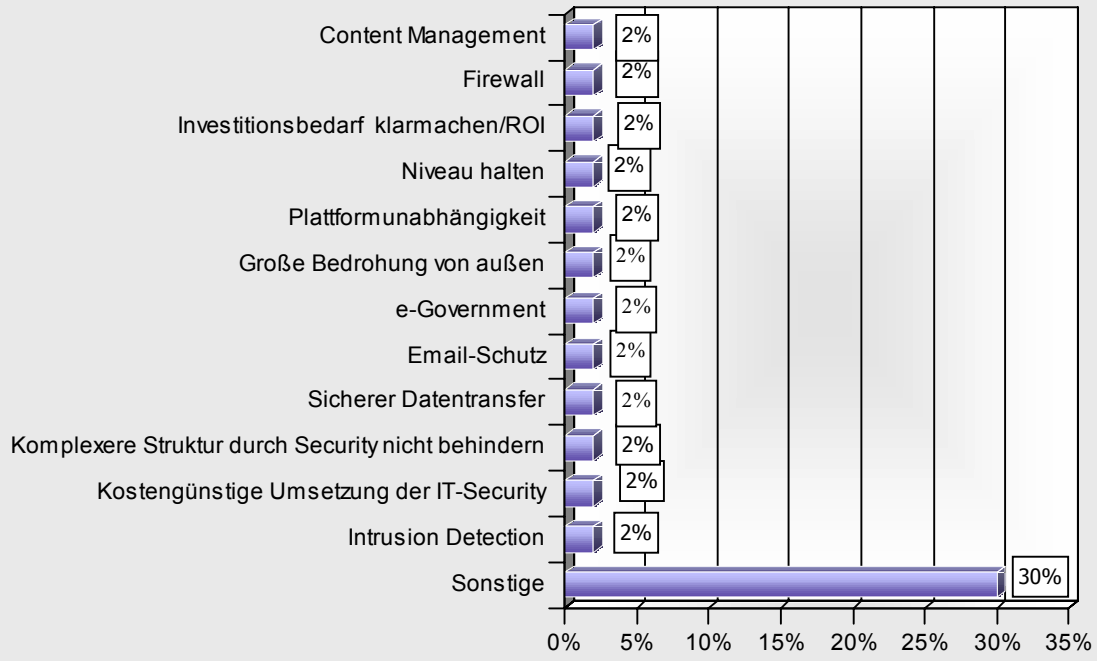


Quelle: META Group Deutschland

Mehrfachnennungen möglich
Basis: 186 Unternehmen

Abbildung 89: Zukünftige Herausforderungen im Bereich der IT-Security (1)

Welche Herausforderungen sehen Sie im Zusammenhang mit dem Thema IT-Security für die Unternehmen Ihrer Branche in den nächsten Jahren? [2]
(Gesamt)



Quelle: META Group Deutschland

Mehrfachnennungen möglich
Basis: 186 Unternehmen

Abbildung 90: Zukünftige Herausforderungen im Bereich der IT-Security (2)

7 Zusammenarbeit mit externen Dienstleistern und Produktanbietern

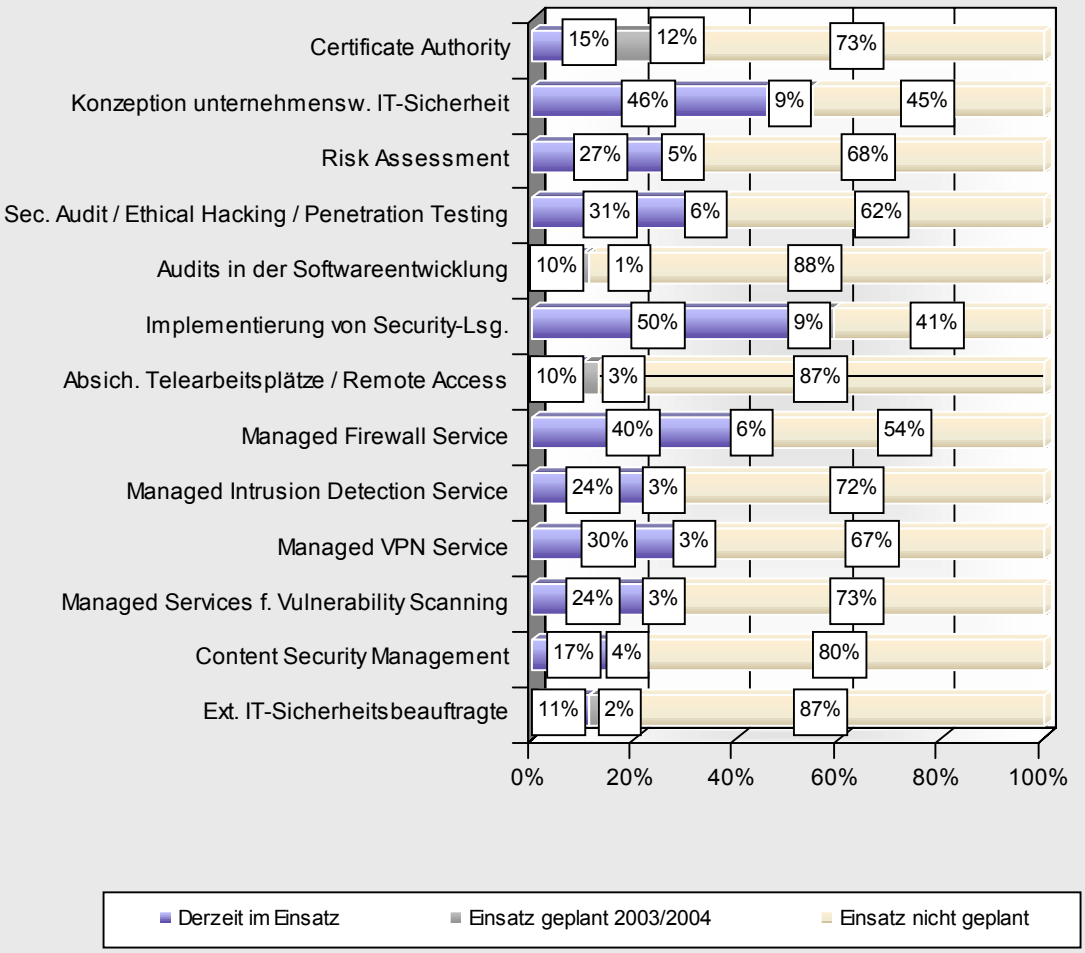
7.1 Einsatzbereiche für externe Dienstleister

Die drei führenden Themen für den Einbezug externer Dienstleister waren bislang die Implementierung von Security-Lösungen, die Konzeption unternehmensweiter IT-Sicherheit sowie Managed Firewall Services. Diese Bereiche werden auch bei künftigen Planungsvorhaben der Anwenderunternehmen in Bezug auf das realisierte Volumen (Einsatzgrad) eine wichtige Rolle spielen. Eine Zusatzanalyse zeigt überdies, dass in Zukunft vor allem der Mittelstand in Managed Services für Firewalls investieren möchte.

Sehr hohe relative Zuwächse - bezogen auf den künftigen Einsatz externer Dienstleister – planen die Unternehmen bei Certificate Authorities (CA, als Komponente von PKIs), bei der Absicherung von Telearbeitsplätzen und bei Content Security Management als Service. Abgesehen von CA-Dienstleistungen nehmen aber auch künftig kaum mehr als 20 Prozent der Nutzer diese Services in Anspruch. Auch Managed Services für Intrusion Detection und Vulnerability Scanning fristen nach Planung der Anwender zunächst ein Nischendasein. Populärer ist hingegen neben dem Managed Firewall Service auch der Managed VPN Service.

Dienstleistungen rund um Penetration Testing, Ethical Hacking, Sicherheits-Audits und Risk Assessment sind allmählich im Kommen. Dies zeigt, dass das Sicherheitsbewusstsein - aber auch die Unsicherheit ob der Verlässlichkeit der eigenen Security-Infrastrukturen und -Prozesse - in den vergangenen Jahren zugenommen hat. Externe Sicherheitsbeauftragte werden hingegen auch weiterhin ein Nischendasein fristen.

In welchen Bereichen nehmen Sie heute externe Dienstleister in Anspruch und wo planen Sie dies zukünftig?



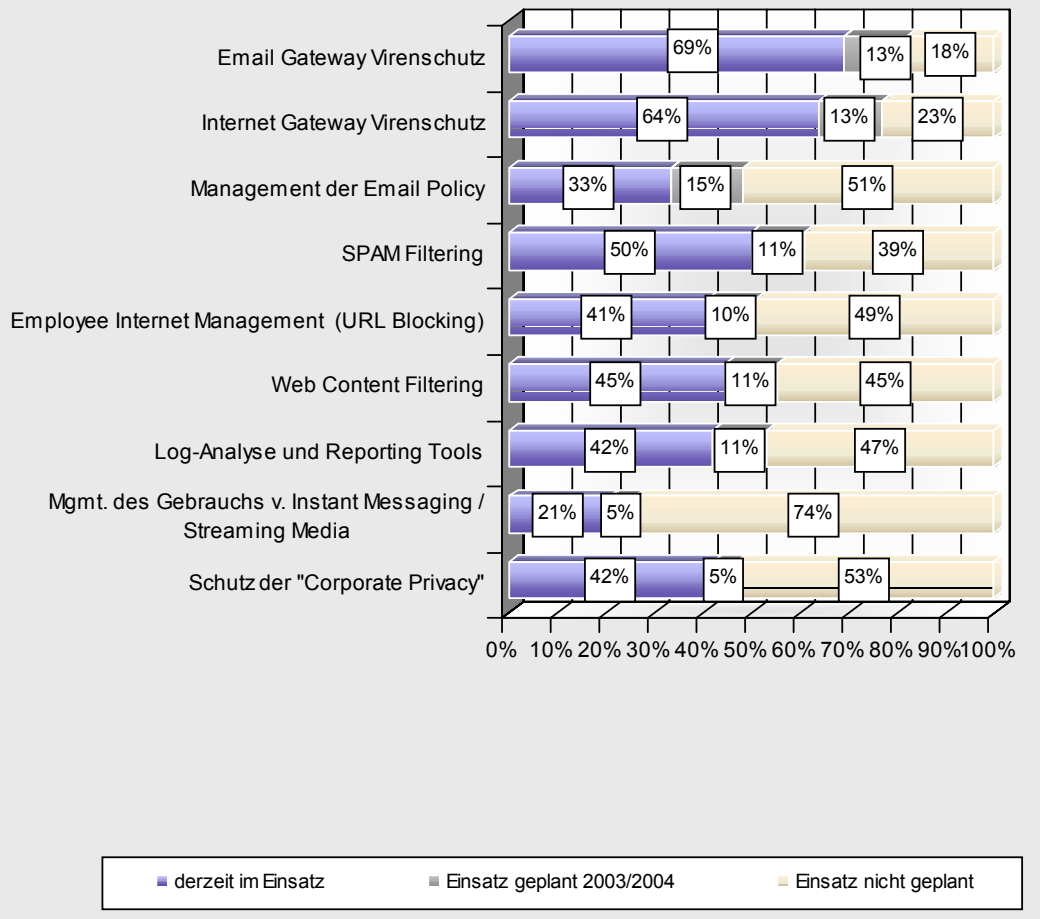
Quelle: META Group Deutschland

Basis: 207 Unternehmen

Abbildung 91: Inanspruchnahme externer Dienstleister nach Bereichen

Sofern die befragten Unternehmen für Content Security Management externe Dienstleister einbeziehen, geht es vor allem um Email- und Internet-Gateway-Virenschutz. Aber auch in anderen Bereichen des Content Security Managements erfolgt der Einbezug von Dienstleistern, beziehungsweise es liegen entsprechende Planungen vor. Allein das Management des Gebrauchs von Instant Messaging und Streaming Media fällt noch nicht stark ins Gewicht. Diese Aspekte sind sowohl für die Anwenderunternehmen als auch für die Anbieter von Sicherheitslösungen noch relativ neu – entsprechend niedrig ist das Bewusstsein für die damit verbundenen potenziellen Risiken für Sicherheit und Produktivität im Unternehmen.

In welchen Bereichen des Content Security Management nehmen Sie heute Dienstleister in Anspruch und wo planen Sie dies zukünftig?



Quelle: META Group Deutschland

Basis: 39 Unternehmen

Abbildung 92: Einbezug von Dienstleistern für Content Security Management

7.2 Auswahlprozess

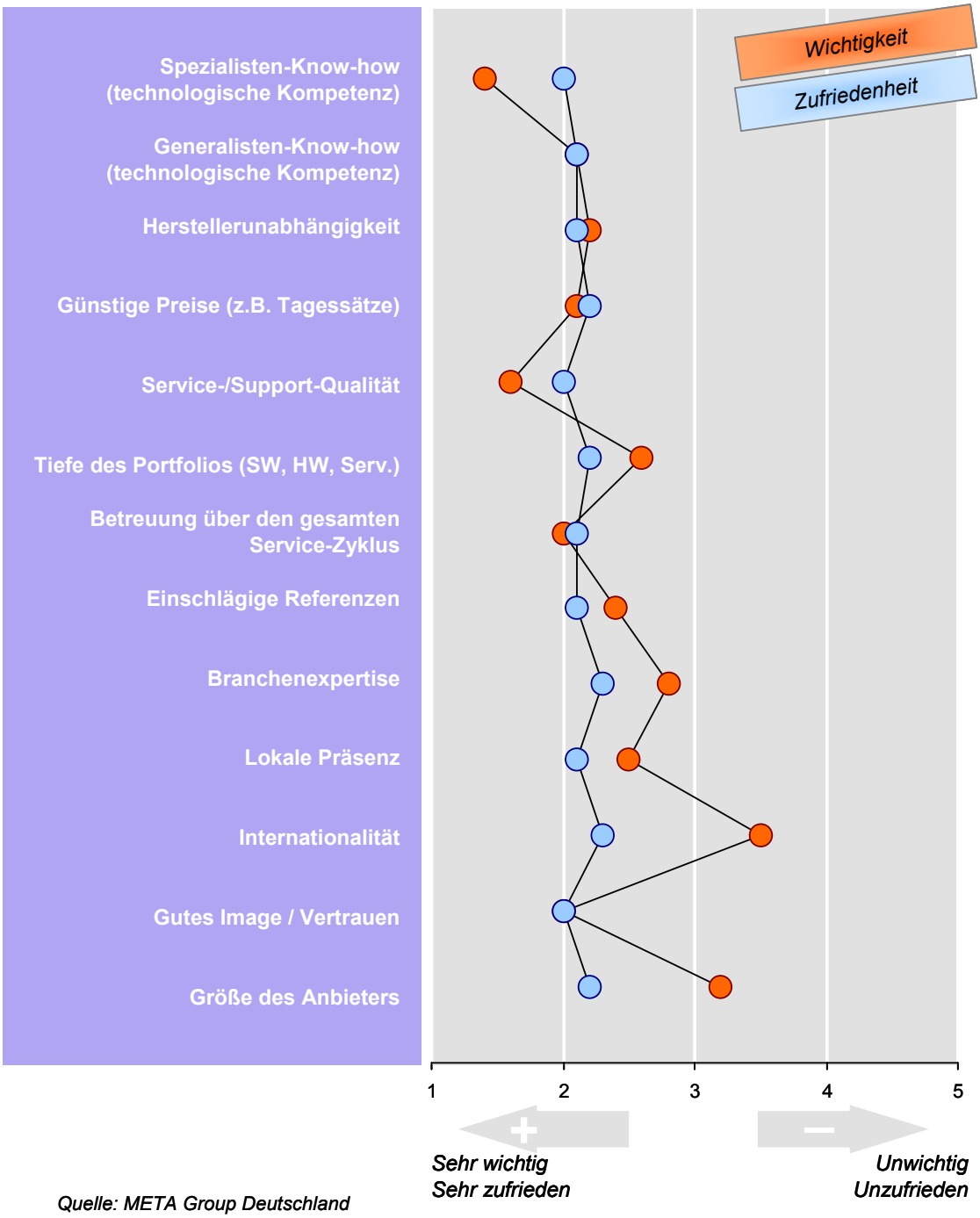
Bei der Auswahl eines Anbieters von Dienstleistungen im IT-Security-Umfeld legen die befragten Unternehmen vor allem großen Wert auf technologisches Spezialisten-Know-how sowie auf die Qualität von Service und Support. Weitere wichtige Auswahlkriterien sind die Betreuung des Kunden über den gesamten Service-Zyklus („PLAN-BUILD-RUN"), die Vertrauenswürdigkeit und das Image des Dienstleisters. Letzteres ist sehr gut nachvollziehbar, handelt es sich bei IT-Sicherheit doch um ein außerordentlich sensibles Thema. Ferner ist auch technologisches Generalisten-Know-how beim Dienstleister gefordert, wobei der Anbieter nach Meinung der Anwender herstellerunabhängig und zu günstigen Preisen agieren sollte.

Nach Meinung der META Group hängt die Gewichtung im „Kritieren-Mix" bei der Anbieterauswahl erheblich von den spezifischen Anforderungen beim Kunden oder im Projekt ab. So dürfte etwa die Herstellerneutralität insbesondere in frühen Phasen des Entscheidungsprozesses beim Anwenderunternehmen relevant sein. Ist aber die Produktauswahl einmal vollzogen, liegt das Augenmerk vor allem auf einer sauberen Implementierung und Integration.

Ähnliches gilt für die Größe und Internationalität des Dienstleisters: Diese spielen nach Aussage der befragten Unternehmen zunächst eine geringere Rolle. Dennoch können diese Faktoren nach Einschätzung der META Group in spezifischen Projekten ausschlaggebend sein. Relevant werden sie beispielsweise bei der Realisierung und Betreuung der globalen Sicherheits-Infrastruktur eines international tätigen Unternehmens. Nähere Untersuchungen der META Group zeigen in diesem Zusammenhang, dass die Forderung nach Internationalität des Dienstleisters bei typischerweise international ausgerichteten Großunternehmen etwas stärker formuliert wird als im Mittelstand (für Details siehe auch Abbildung 95).

Die Anwenderunternehmen sind in Bezug auf fast alle Kriterien zufrieden mit den Dienstleistern. Allein in Hinsicht auf Spezialisten-Kenntnisse und die Qualität von Service und Support erwarten sich die Kunden mehr: Hier gibt es noch eine auffallende Diskrepanz zwischen der Relevanz der beiden Kriterien und der Zufriedenheit der Anwenderschaft.

Wie wichtig sind / waren Ihnen die folgenden Kriterien bei der Auswahl eines Anbieters von Dienstleistungen im IT-Security-Umfeld und wie zufrieden sind Sie mit Ihrem Dienstleister? *(Gesamt)*



Quelle: META Group Deutschland

Basis: Wichtigkeit: 160; Zufreidenheit: 132 Unternehmen

Abbildung 93: Kriterien und Zufriedenheit bei der Auswahl von Security-Dienstleistern

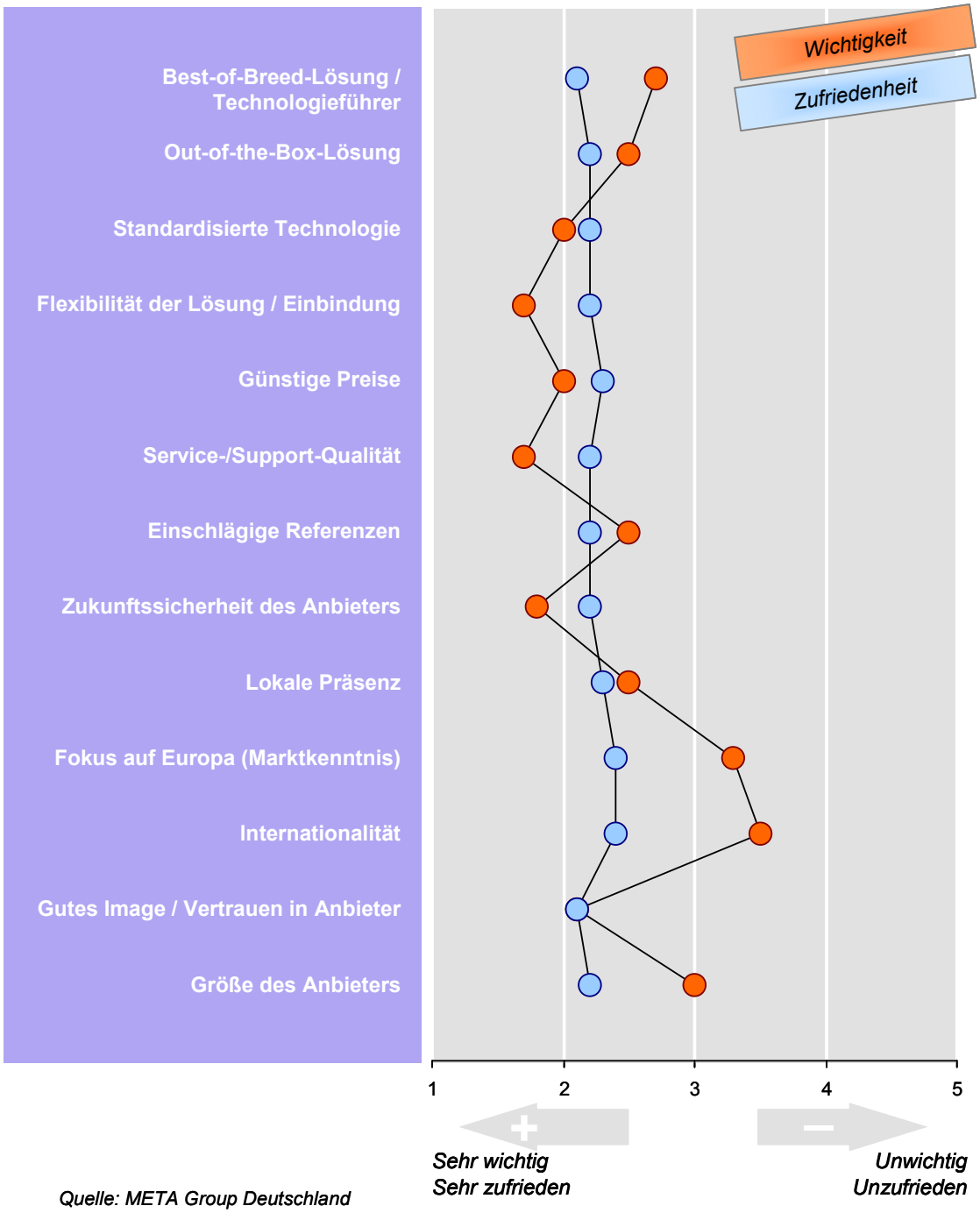
Bei der Auswahl eines Anbieters von Lösungen und Produkten im IT-Security-Umfeld legen die befragten Unternehmen vor allem großen Wert auf die Flexibilität der Lösung, das heißt die Integrierbarkeit in bestehende Systemlandschaften, sowie auf die Service- und Support-Qualität und die Zukunftssicherheit des Anbieters. Weitere wichtige Auswahlkriterien sind standardisierte Technologien, günstige Preise sowie nicht zuletzt auch eine durch Vertrauen geprägte Beziehung zwischen Kunde und Anbieter.

Weniger wichtig sind die Größe des Anbieters und die internationale Ausrichtung, aber auch ein spezieller Fokus auf Europa einschließlich entsprechender lokaler Marktkenntnisse spielt nach Aussagen der Anwender eine kleine Rolle. Allerdings muss hier nach Zielgruppe und Thema differenziert werden. Eine Zusatzauswertung der Daten nach Unternehmensgrößen zeigt, dass Größe und Internationalität des Anbieters für große Unternehmen eine höhere Bedeutung haben als für den Mittelstand (siehe auch Abbildung 96 bis Abbildung 98). Außerdem ist davon auszugehen, dass Kenntnisse in Bezug auf spezifische europäische Marktgegebenheiten und Mentalitäten dem Anbieter vertriebliche Wettbewerbsvorteile verschaffen. Erwähnenswert ist insgesamt, dass diese Anforderungen durch die Anbieter in einem hohen Maß übererfüllt werden, das heißt sie bieten mehr als von den Anwendern erwartet wird.

Ob nun „Best-of-Breed"-Lösungen der Technologieführer oder schlüsselfertige „Out-of-the-Box"-Lösungen bevorzugt werden, dürfte von den jeweiligen situationsbezogenen Anforderungen des Unternehmens abhängen. Hohe Priorität genießen preisliche Aspekte und die Flexibilität der Lösung. Best-of-Breed-Lösungen mögen gegebenenfalls skalierbarer und flexibler hinsichtlich der Einbindung in heterogene IT-Infrastrukturen sein und mehr Funktionalität bieten, dafür punkten schlüsselfertige Lösungen aus einer Hand oftmals beim Preis. Out-of-the-Box-Lösungen sind daher besonders für den Mittelstand interessant. Tatsächlich zeigt eine Analyse nach Unternehmensgrößen, dass die Forderung nach Best-of-Breed-Lösungen bei Großunternehmen deutlich stärker formuliert wird.

Die Anwenderunternehmen sind in Bezug auf alle Kriterien einigermaßen zufrieden mit den Anbietern. Kritische Punkte bleiben aber die Flexibilität der gebotenen Lösungen, die Service- und Support-Qualität und die Zukunftssicherheit der Anbieter: Hier hinkt der Zufriedenheitsgrad der Kunden hinter den hochgesteckten Erwartungen hinterher.

Wie wichtig sind / waren Ihnen die folgenden Kriterien bei der Auswahl eines Anbieters von Lösungen im IT-Security-Umfeld und wie zufrieden sind Sie mit Ihrem Anbieter? *(Gesamt)*



Quelle: META Group Deutschland

Basis: Wichtigkeit: 203; Zufriedenheit: 188

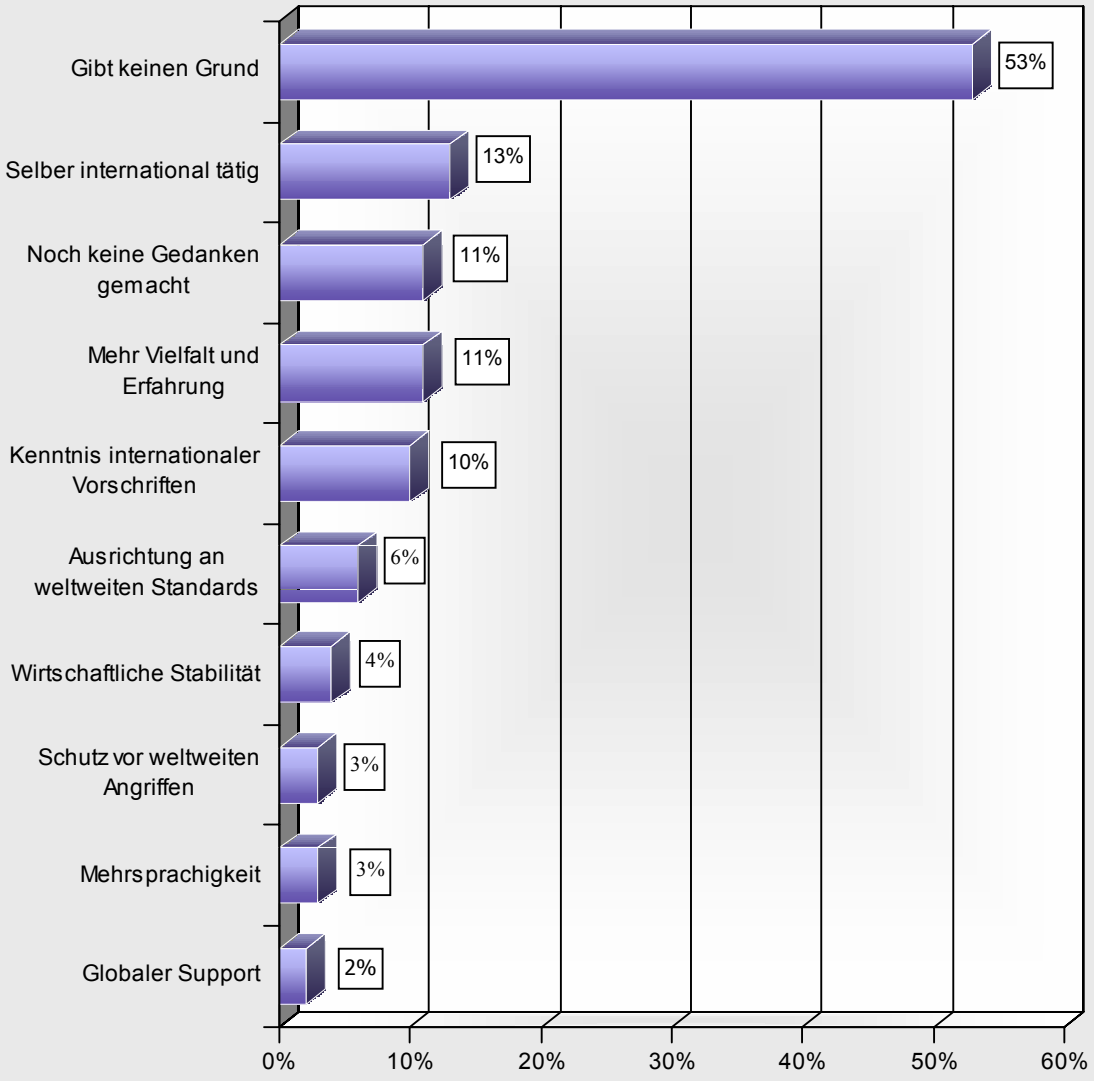
Abbildung 94: Kriterien für die Auswahl von Security-Lösungsanbietern

Ergänzend zur Frage nach den Kriterien bei der Auswahl von Anbietern wurde genauer untersucht, welche Rolle der Aspekt der „Internationalität“ für die Anwenderunternehmen spielt. Über die Hälfte der Befragten ist der Meinung, dass es überhaupt kein Argument für den Einbezug eines international präsenten Security-Anbieters gibt. Für die restlichen Unternehmen ist insbesondere ausschlaggebend, dass sie selbst international tätig sind und damit globalen Supports und Schutzes bedürfen. Außerdem erwarten sie sich von einem internationalen Anbieter mehr Vielfalt und Erfahrung, auch in Bezug auf weltweite Vorschriften und Standards. Manche Anwender sehen die globale Präsenz auch als Indikator für wirtschaftliche Stabilität.

Wie bereits zuvor angedeutet, ist die Internationalität vor dem Hintergrund der Größe des Kunden näher zu beleuchten (siehe Abbildung 96bis Abbildung 98). Während die Mehrheit der Großunternehmen detailliert Argumente für den Einsatz eines international ausgerichteten Dienstleisters nennen kann, sehen über zwei Drittel des Mittelstands entweder überhaupt keinen Grund dafür oder haben sich noch keine Gedanken darüber gemacht.

Interessant ist zudem die Betrachtung nach Branchen. Fertigungsunternehmen sehen insbesondere die eigene internationale Tätigkeit als Argument, für die Gruppe der Logistik-, Versorgungs- und Telekommunikationsdienstleister spielt die Kenntnis der internationalen Vorschriften eine tragende Rolle. Handelsunternehmen versprechen sich von einem internationalen Dienstleister mehr Erfahrung und Vielfalt, und die prozessorientierte Fertigungsindustrie argumentiert mit der Ausrichtung an weltweiten Standards, die etwa in den Bereichen Chemie und Pharma erforderlich sind.

Welche drei Argumente sprechen aus Ihrer Sicht für den Einbezug eines international präsenten Security-Dienstleisters oder -Produktanbieters?
(Gesamt)

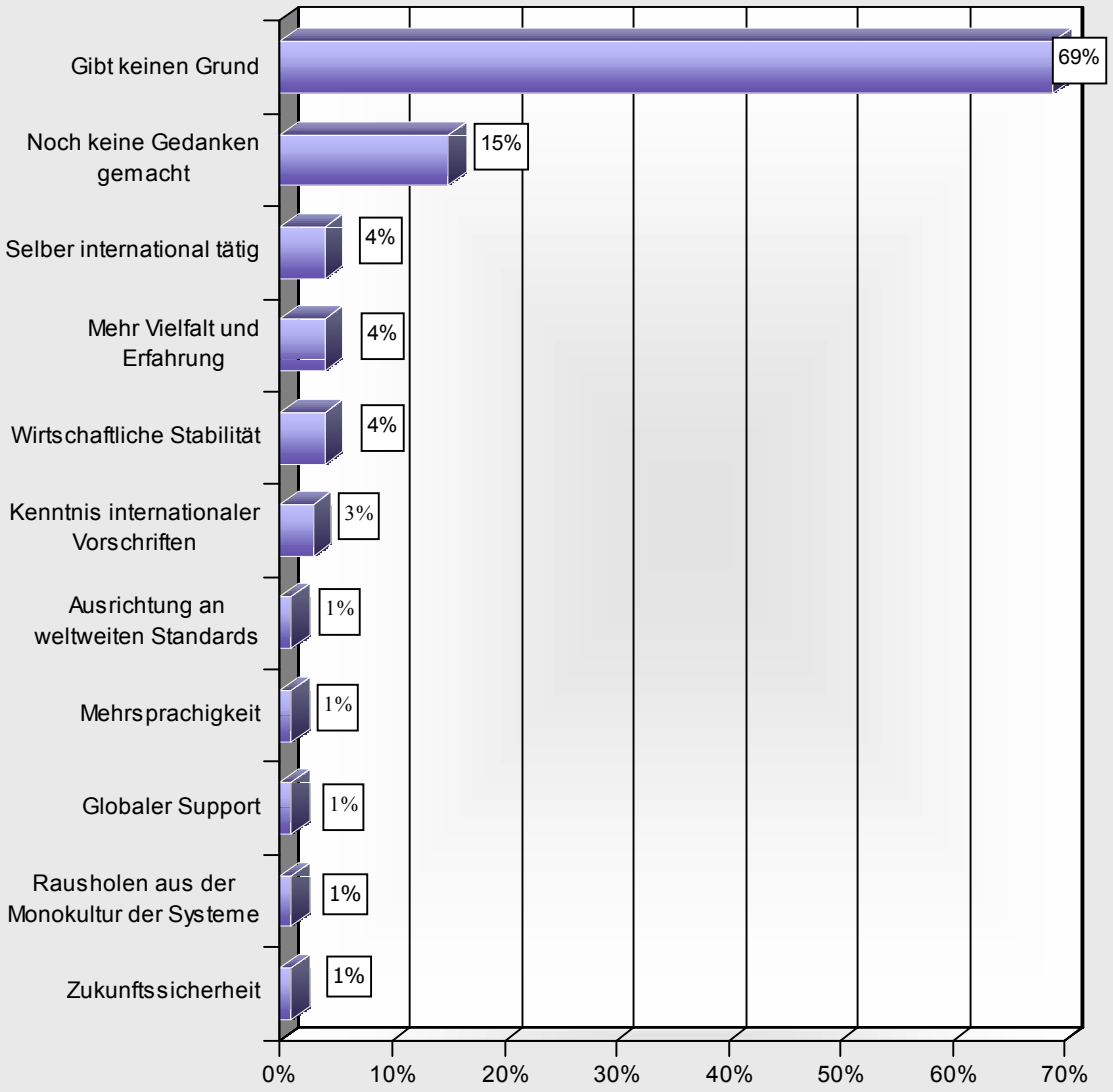


Quelle: META Group Deutschland

Mehrfachnennungen möglich
Basis: 206 Unternehmen

Abbildung 95: Argumente für den Einbezug international präsenter Security-Anbieter

Welche drei Argumente sprechen aus Ihrer Sicht für den Einbezug eines international präsenten Security-Dienstleisters oder -Produktanbieters?
(50-199 Mitarbeiter)



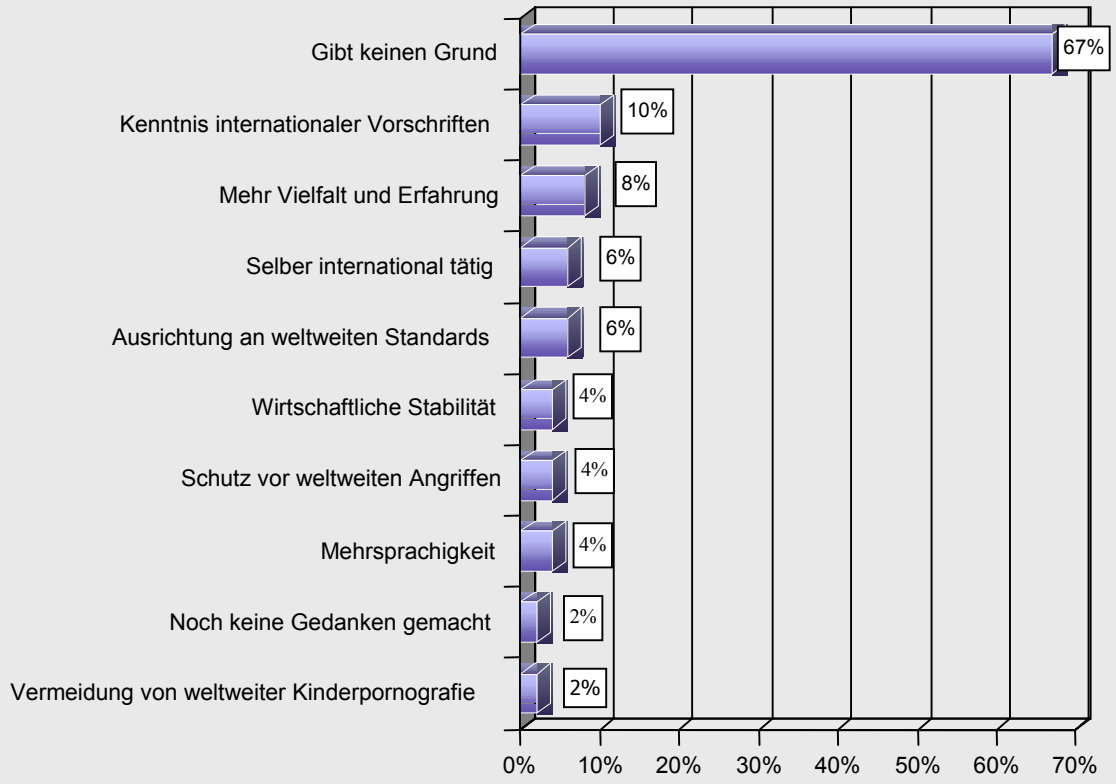
Mehrfachnennungen möglich

Quelle: META Group Deutschland

Basis: 67 Unternehmen

Abbildung 96: Argumente für den Einbezug internationaler Security-Anbieter (50-199 Mitarbeiter)

Welche drei Argumente sprechen aus Ihrer Sicht für den Einbezug eines international präsenten Security-Dienstleisters oder -Produktanbieters?
(200-499 Mitarbeiter)

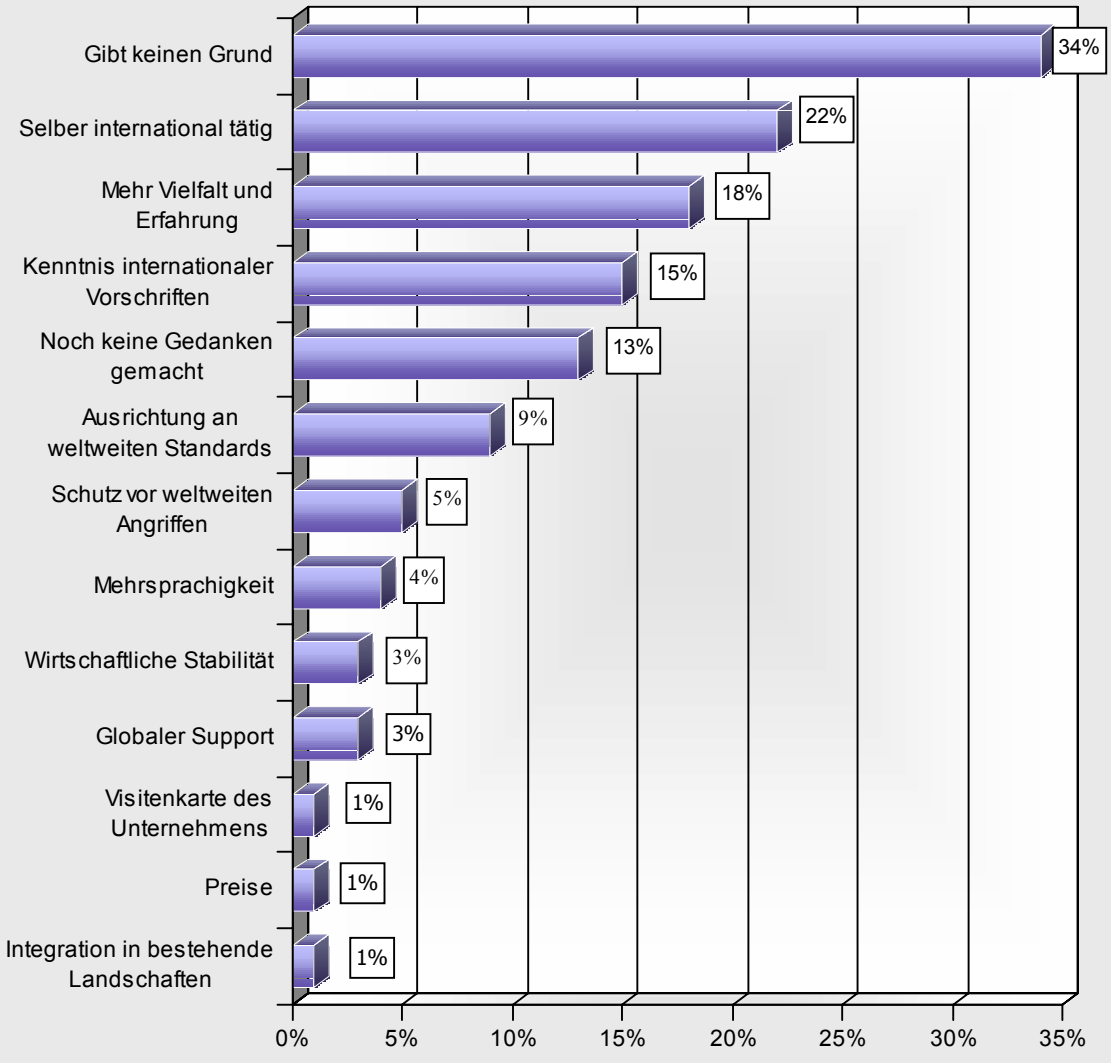


Quelle: META Group Deutschland

Mehrfachnennungen möglich
Basis: 48 Unternehmen

Abbildung 97: Argumente für den Einbezug internationaler Security-Anbieter (200-499 Mitarbeiter)

Welche drei Argumente sprechen aus Ihrer Sicht für den Einbezug eines international präsenten Security-Dienstleisters oder -Produktanbieters?
(500 und mehr Mitarbeiter)



Quelle: META Group Deutschland

Mehrfachnennungen möglich
Basis: 91 Unternehmen

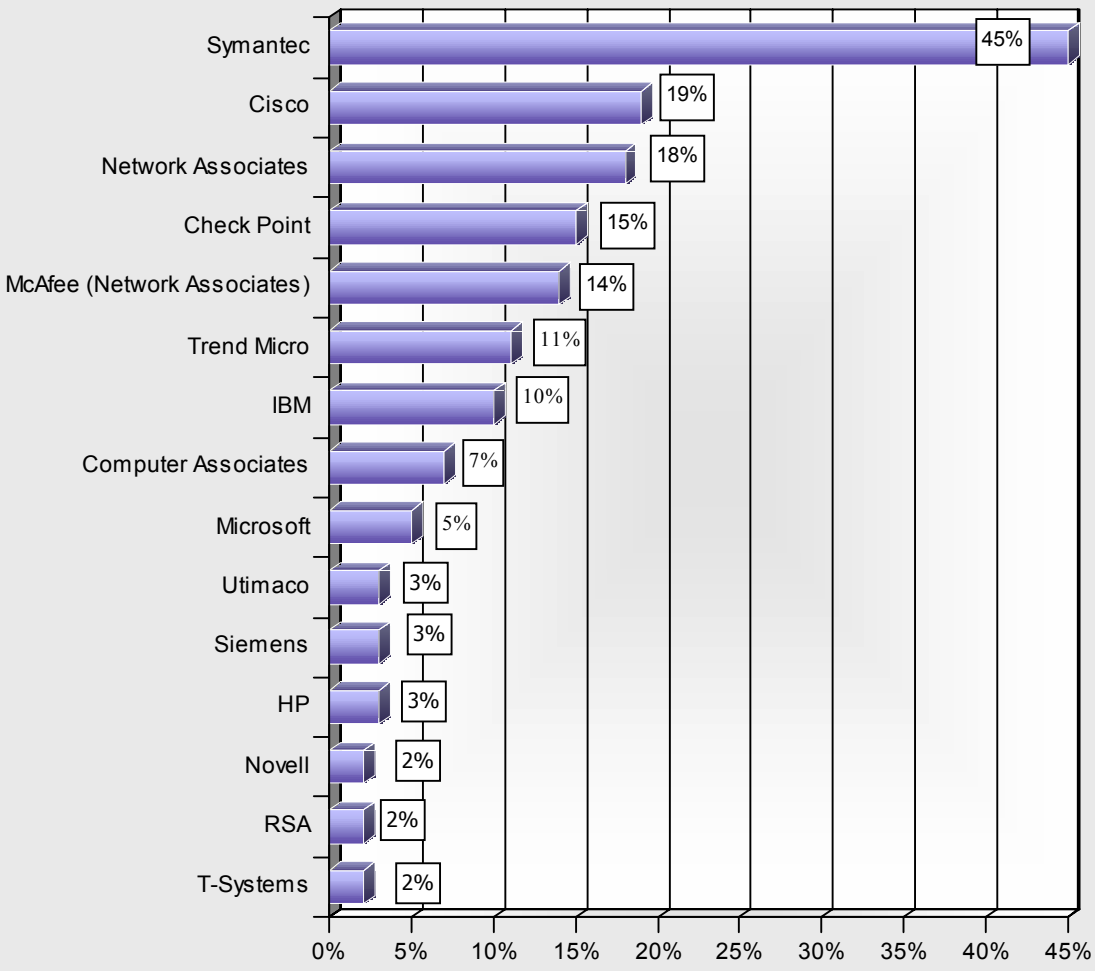
Abbildung 98: Argumente für den Einbezug internationaler Security-Anbieter (ab 500 Mitarbeiter)

7.3 Bewertung von Anbietern

7.3.1 Ungestützter Bekanntheitsgrad von Security-Anbietern und -Dienstleistern

Wenn es um IT-Security-Produkte geht, fällt deutschen Anwenderunternehmen zuerst Symantec ein. Zu den fünf am häufigsten genannten Anbietern gehören ferner Network Associates / McAfee, Cisco, Check Point und Trend Micro. Das Ranking verschiebt sich zugunsten von Cisco, wenn zwischen den Marken „Network Associates“ und „McAfee“ differenziert wird. Dies zeigt die Untersuchung des ungestützten (das heißt ohne Vorgabe einer festen Anbieterliste ermittelten) Bekanntheitsgrades von Security-Produktanbietern durch die META Group. Damit wird gleichzeitig allzu deutlich, dass die Unternehmen beim Thema IT-Sicherheit auf technologischer Ebene primär an Virenschutz und Netzwerksicherheit (v.a. Firewalls und VPNs) denken. Es wird darauf hingewiesen, dass das Kerngeschäft mancher als Produktanbieter genannten Unternehmen eigentlich im Service-Bereich liegt.

Welche Anbieter von Sicherheitslösungen (Produkten) fallen Ihnen spontan ein? [1]
(Gesamt)

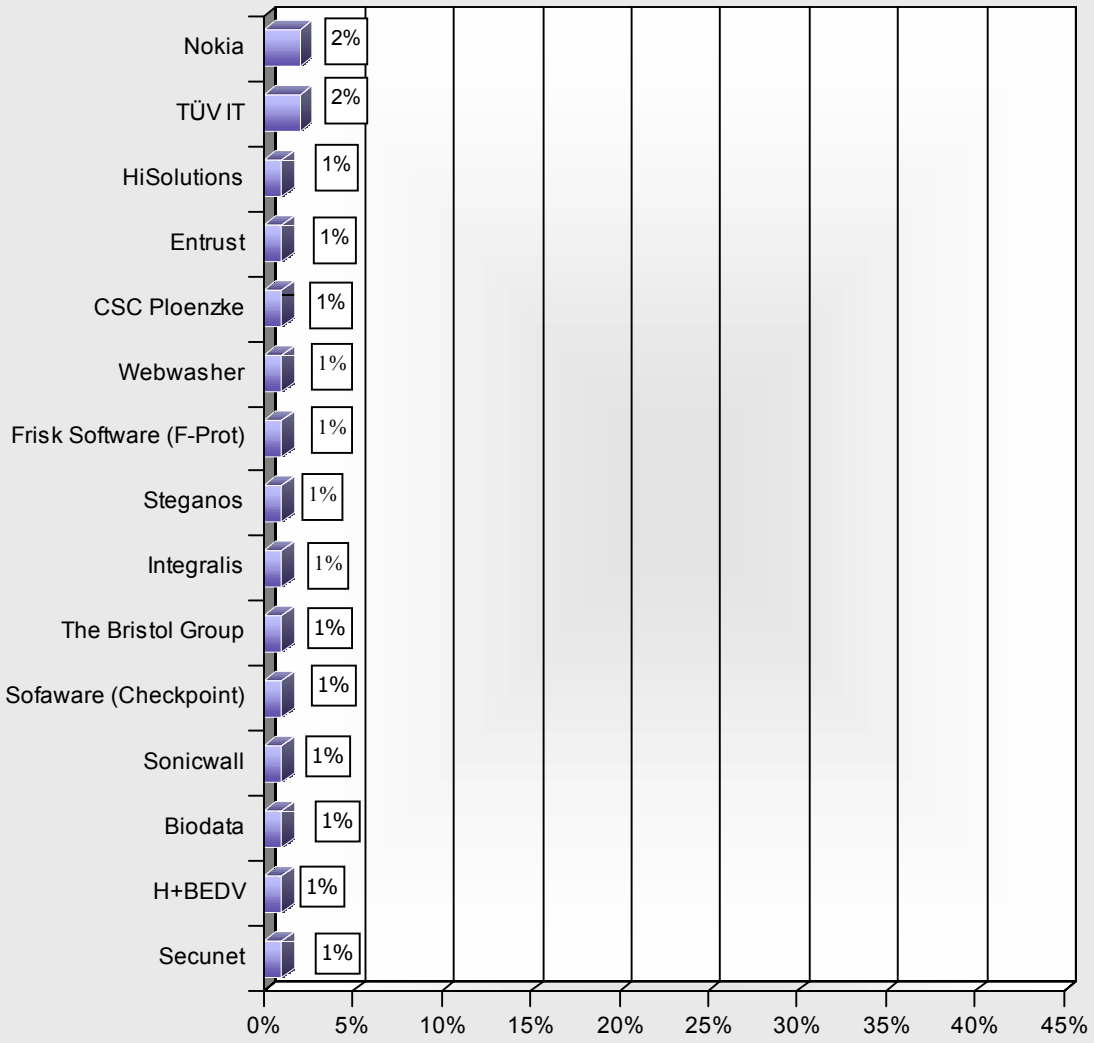


Quelle: META Group Deutschland

Mehrfachnennungen möglich
Basis: 166 Unternehmen

Abbildung 99: Ungestützter Bekanntheitsgrad von Security-Produktanbietern (1)

Welche Anbieter von Sicherheitslösungen (Produkten) fallen Ihnen spontan ein? [2]
(Gesamt)



Quelle: META Group Deutschland

Mehrfachnennungen möglich
Basis: 166 Unternehmen

Abbildung 100: Ungestützter Bekanntheitsgrad von Security-Produktanbietern (2)

Auch bei der spontanen Nennung von Sicherheits-Dienstleistern durch die befragten Anwenderunternehmen nimmt Symantec den ersten Platz ein, noch vor IBM Global Services, Siemens, Secunet, T-Systems und dem TÜV – wobei unklar bleibt, ob damit die TÜV Secure iT GmbH oder der TÜV IT gemeint ist. Dass sich Symantec als Produktanbieter auch bei Services ganz vorne platzieren kann, lässt darauf schließen, wie wichtig den Anwenderunternehmen heute Support- und weitere Dienstleistungen sind. Auf der „Mindshare"-Liste tauchen auch weitere Produktanbieter auf. Es wird hier deutlich, dass das Branding der führenden Produktanbieter sehr fest im Markt verankert ist. Dennoch schaffen es auch kleinere, primär auf den deutschsprachigen Markt fokussierte Dienstleister, in die Wahrnehmung der Anwender Eingang zu finden, so beispielsweise Secorvo, Controlware und Cirosec.

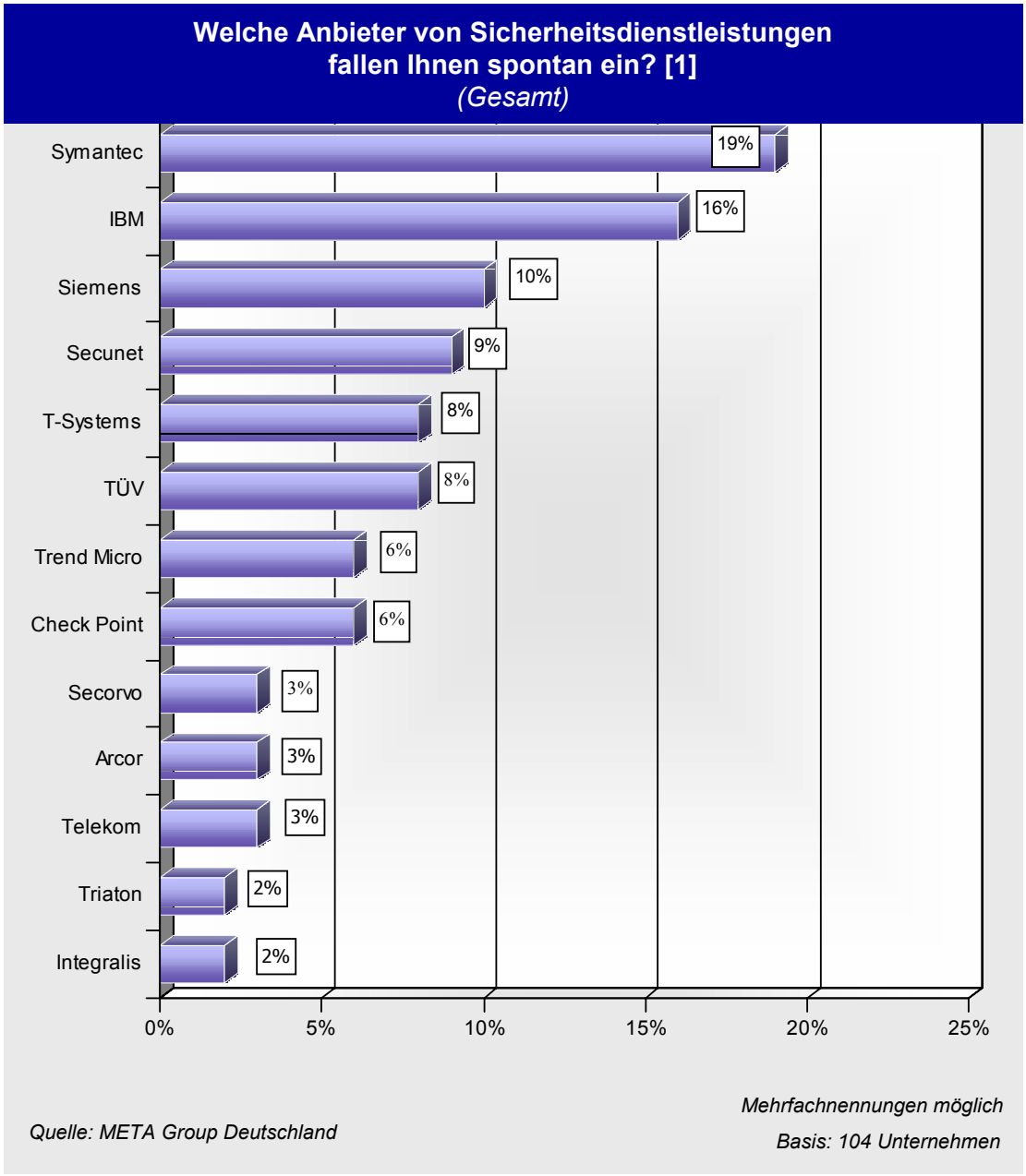


Abbildung 101: Ungestützter Bekanntheitsgrad von Security-Dienstleistern (1)

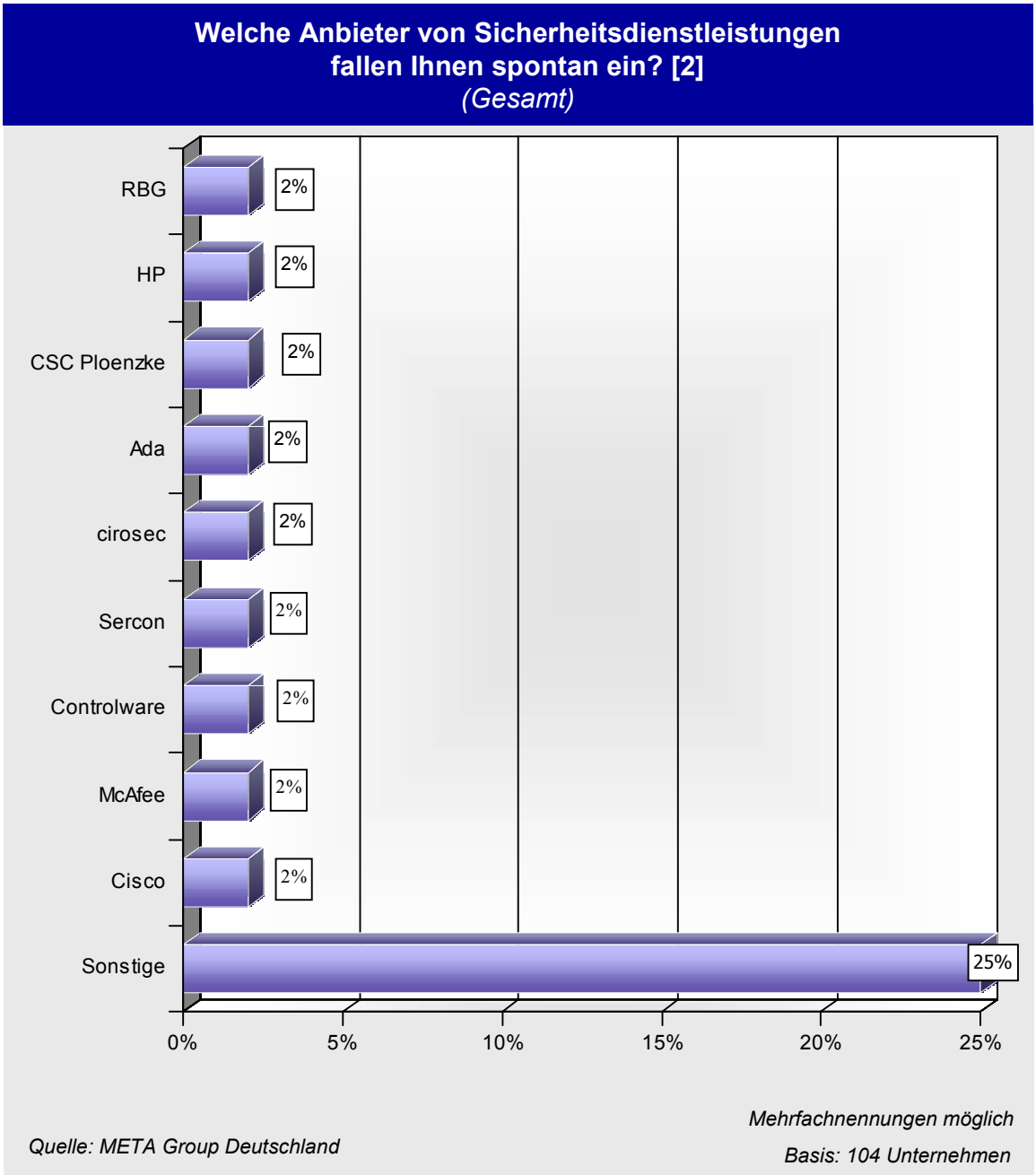


Abbildung 102: Ungestützter Bekanntheitsgrad von Security-Dienstleistern (2)

7.3.2 Gestützter Bekanntheitsgrad und Leistungsfähigkeit ausgewählter Anbieter

Im Folgenden werden die Einschätzung der Leistungsfähigkeit einzelner Security-Dienstleister und Produktanbieter durch die befragten Anwender sowie der Bekanntheitsgrad im Überblick aufgeführt. Die Leistungsfähigkeit ist sowohl auf einer Skala von 1 bis 5 als auch in Prozent angegeben, wobei der Maximalwert von 100% einer Bewertung von „1“ (=sehr gut) und der Minimalwert von 20% einer Bewertung von „5“ (=sehr schlecht) entspricht.

Es wurde entlang folgender Fragenkomplexe vorgegangen:

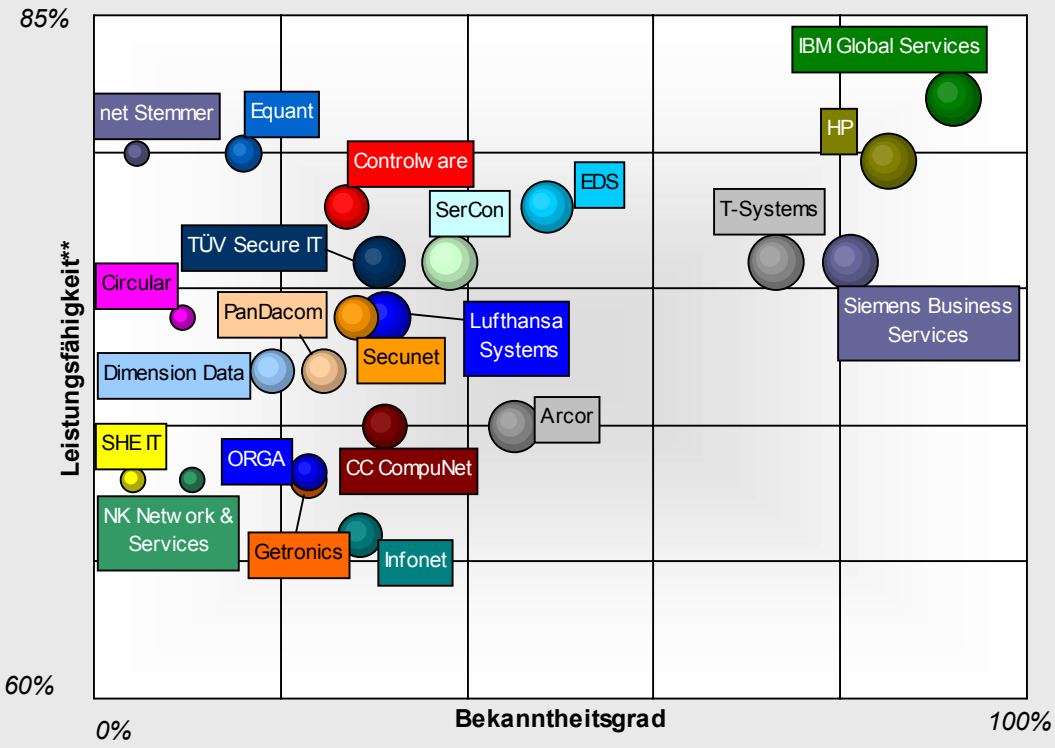
- Gestützter Bekanntheitsgrad von Dienstleistern und Lösungsanbietern im Bereich IT-Security
- Einschätzung der Leistungsfähigkeit von Anbietern durch Anwender im Hinblick auf IT-Security
- Sicherheits-Dienstleister und -Lösungsanbieter auf der „Short-List“ im Auswahlprozess bei den Anwendern

7.3.2.1 Einschätzung von IT-Security-Dienstleistern

Die folgende Abbildung zeigt eine Auswahl von Security-Dienstleistern sowie den gestützten Bekanntheitsgrad und die Bewertung der Leistungsfähigkeit durch die befragten Anwender im Überblick. Es wird darauf hingewiesen, dass diese Anbieterübersicht aufgrund des fragmentierten Security-Marktes keinen Anspruch auf Vollständigkeit erhebt. Die fünf bekanntesten Dienstleister innerhalb dieser Übersicht sind IBM Global Services, HP, Siemens Business Services, T-Systems sowie EDS. Auch bei der Bewertung der Leistungsfähigkeit durch die Anwender landet IBM Global Services auf dem ersten Platz, in geringem Abstand gefolgt von Equant, HP, net Stemmer, Controlware und EDS. Zu beachten ist allerdings, dass für die Bewertungen von net Stemmer und Equant nur geringe Stichprobengrößen zugrunde liegen, sodass die Aussagekraft mit Unsicherheiten behaftet ist. Die Streuung der Bewertungen ist insgesamt gering – die Leistungsfähigkeit wird bei den meisten Dienstleistern als „gut“ bis „befriedigend“ eingeschätzt. Kein Anbieter wird als „schlecht“ bewertet.

Bekanntheitsgrad und Leistungsfähigkeit ausgewählter Security-Dienstleister*

*- Perception Survey Chart / Anwendermeinungsbild*** -*



Quelle: META Group Deutschland *Basis: 200 Unternehmen*

**Die Größe der Kreise entspricht der Anzahl der Bewertungen zur Leistungsfähigkeit.*
***Transformierte Skala (100% entspricht sehr gut = 1 und 20% entspricht sehr schlecht = 5)*
****Die von der META Group getroffene Auswahl und Positionierung der Anbieterunternehmen reflektiert die Recherche der META Group durch Stichproben von Einschätzungen Dritter. Die Ergebnisse geben daher keinen Aufschluss über die tatsächliche Leistungsfähigkeit und/oder die tatsächliche Bekanntheit im Gesamtmarkt, weder absolut noch relativ zueinander.*

Abbildung 103: Bekanntheitsgrad und Leistungsfähigkeit von Security-Dienstleistern

Eine Auswertung auf Basis der Aussagen aus verschiedenen Unternehmensgrößenklassen ist Abbildung 108 bis Abbildung 111 zu entnehmen. Im Folgenden werden der Bekanntheitsgrad und die Leistungsfähigkeit der Anbieter gesondert dargestellt.

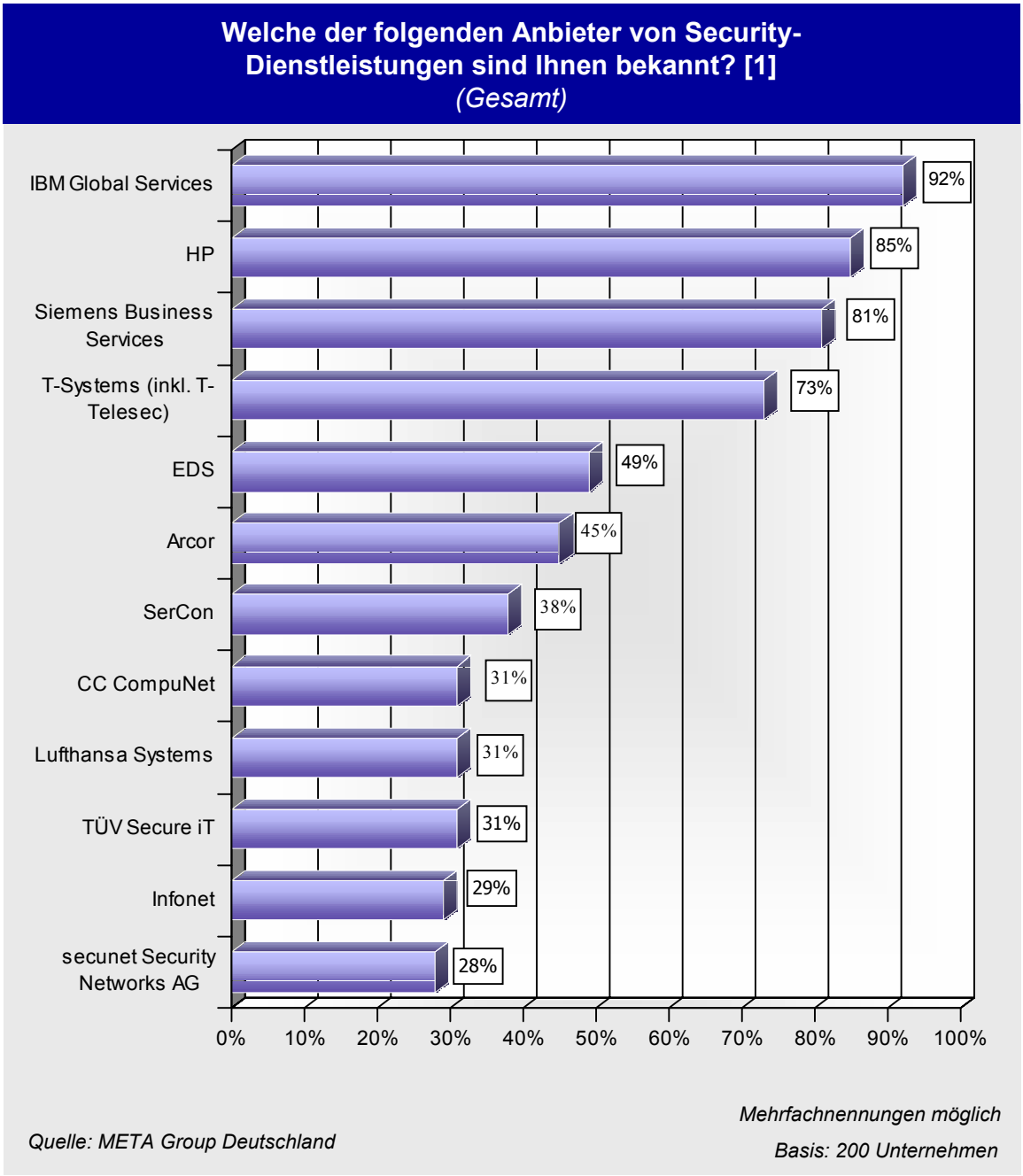
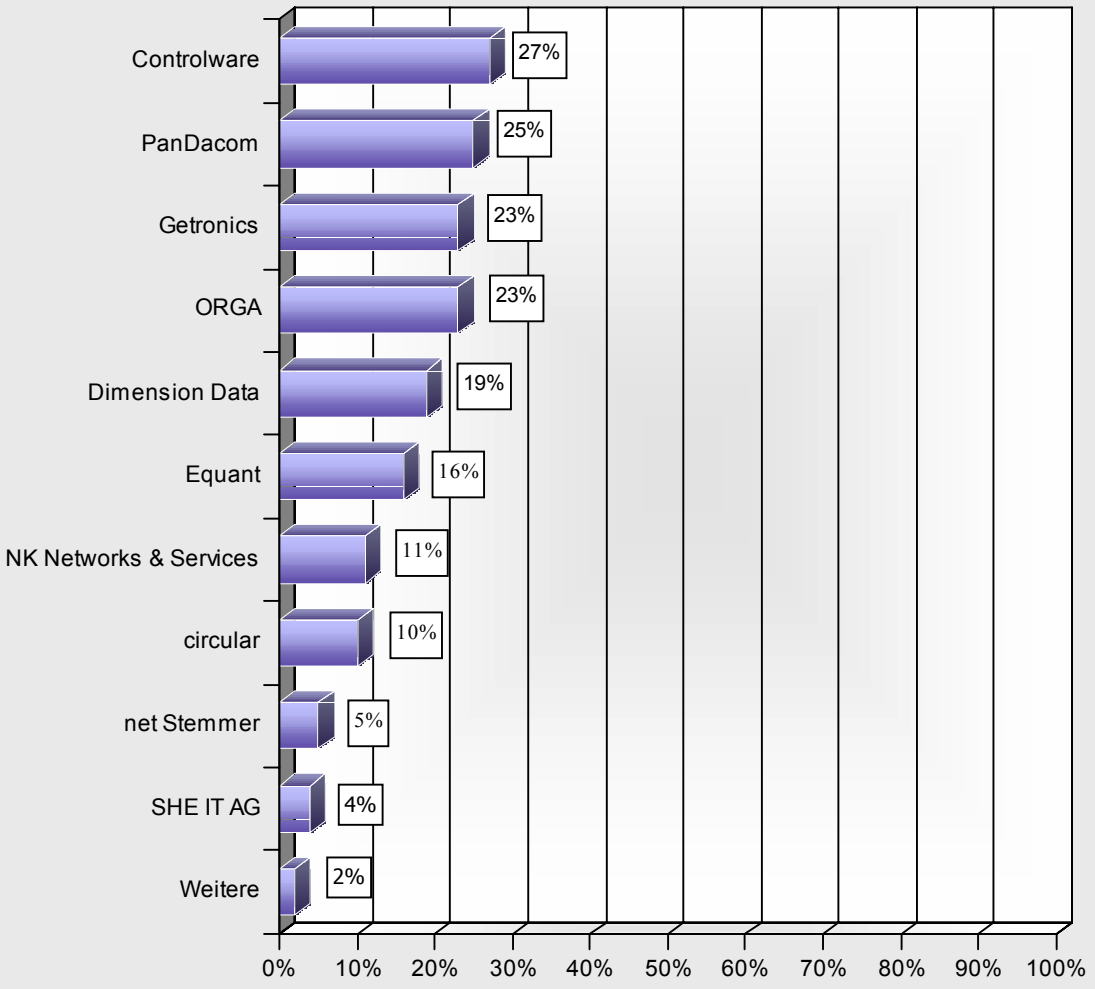


Abbildung 104: Gestützter Bekanntheitsgrad ausgewählter Security-Dienstleister (1)

Welche der folgenden Anbieter von Security-Dienstleistungen sind Ihnen bekannt? [2]
(Gesamt)



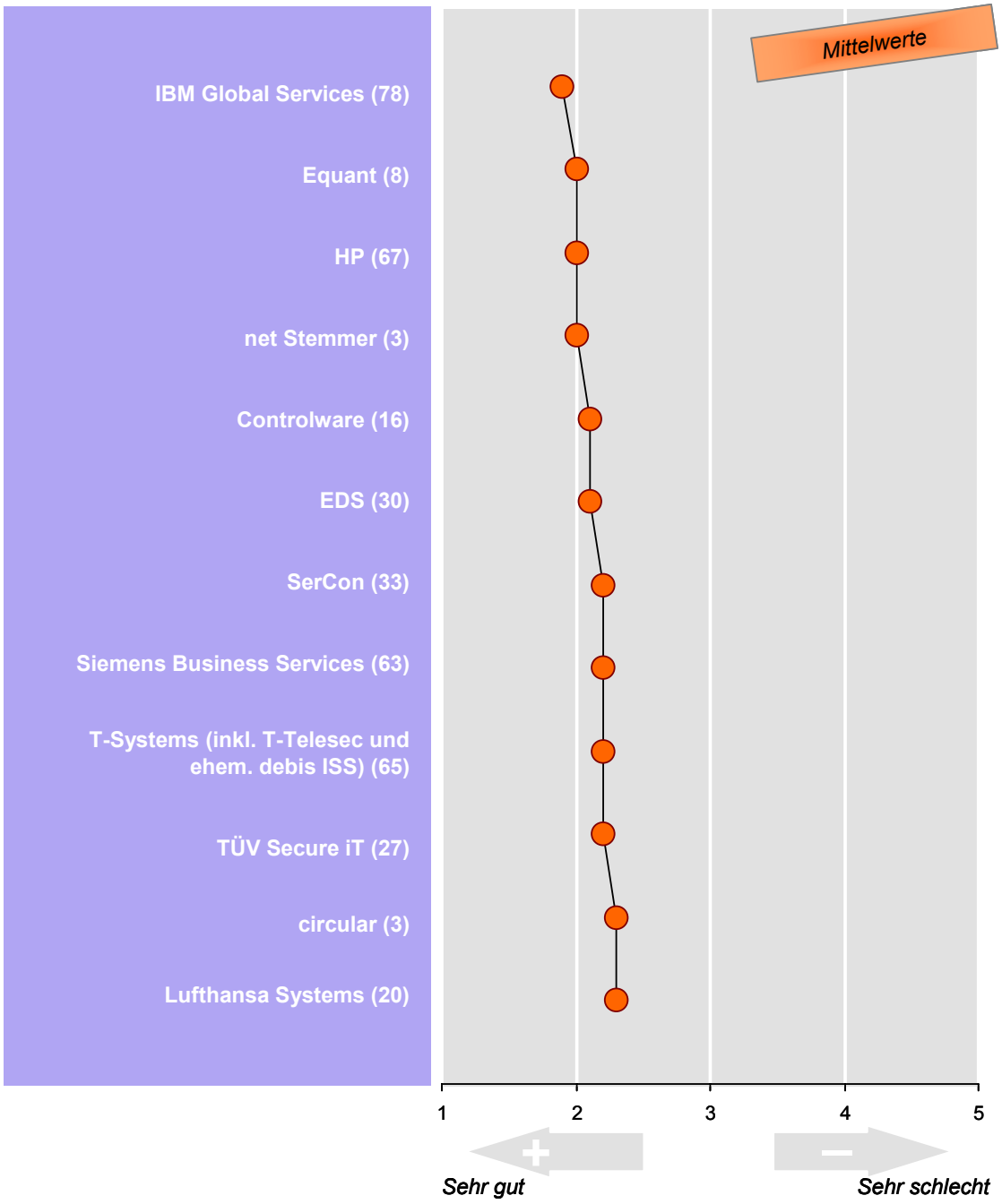
Quelle: META Group Deutschland

Mehrfachnennungen möglich
Basis: 200 Unternehmen

Abbildung 105: Gestützter Bekanntheitsgrad ausgewählter Security-Dienstleister (2)

Ergänzend zur Dienstleisterübersicht wird im Folgenden die Leistungsfähigkeit der einzelnen Anbieter – nach Einschätzung der befragten Anwenderunternehmen - gesondert dargestellt.

Wie hoch schätzen Sie die Leistungsfähigkeit der Ihnen bekannten Anbieter von Security-Dienstleistungen ein? [1]

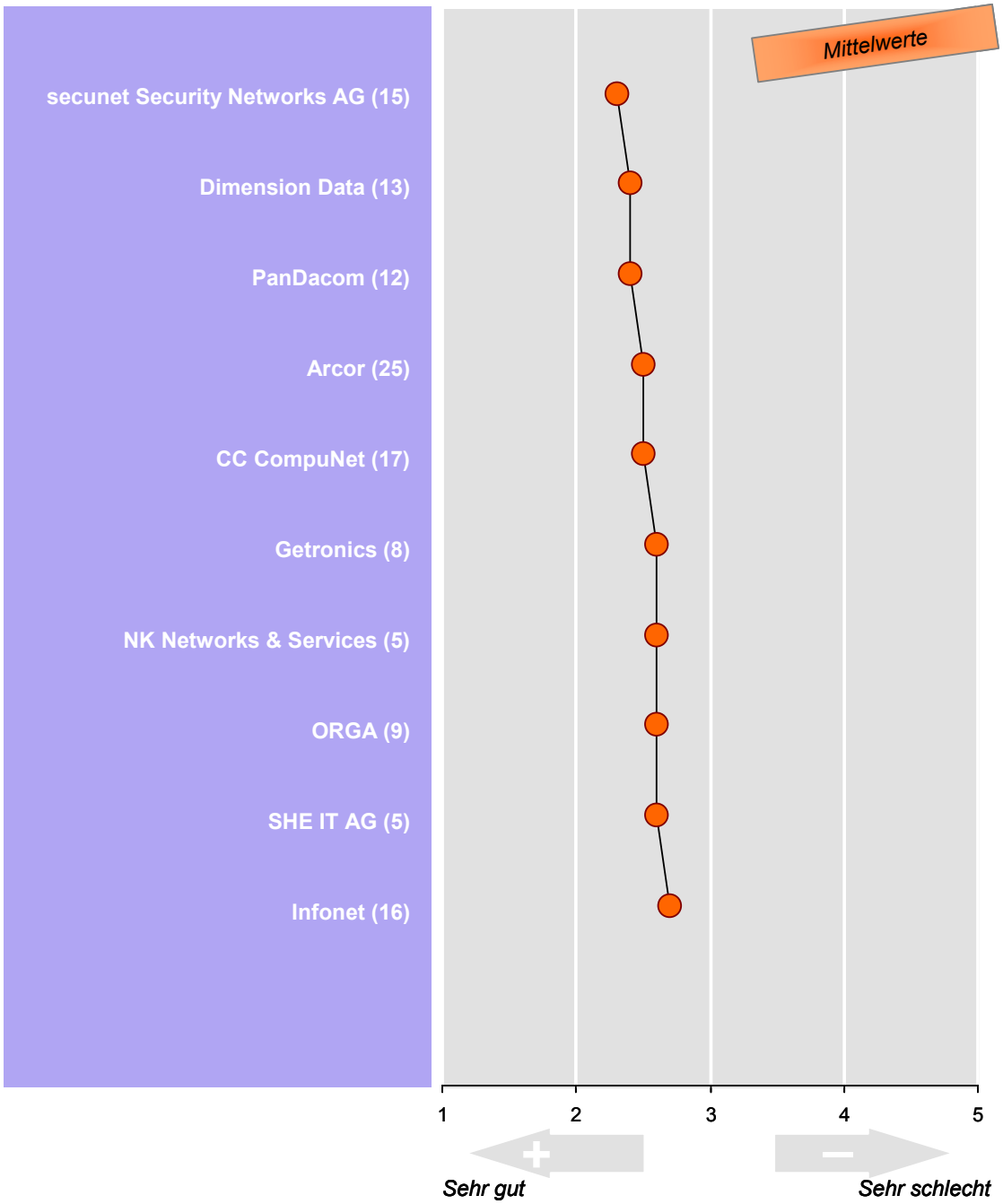


Quelle: META Group Deutschland

(x): Anzahl der Nennungen

Abbildung 106: Leistungsfähigkeit ausgewählter Security-Dienstleister (1)

Wie hoch schätzen Sie die Leistungsfähigkeit der Ihnen bekannten Anbieter von Security-Dienstleistungen ein? [2]



Quelle: META Group Deutschland

(x): Anzahl der Nennungen

Abbildung 107: Leistungsfähigkeit ausgewählter Security-Dienstleister (2)

7.3.2.1.1 IT-Security-Dienstleistungen – Auswertung nach Unternehmensgröße

Die einzelnen Dienstleister werden von Anwendern verschiedener Unternehmensgrößenklassen in der Regel unterschiedlich bewertet. Näheren Aufschluss geben die folgenden Auswertungen. Es wird darauf hingewiesen, dass vor allem bei den weniger bekannten Dienstleistern teilweise kleine Stichprobengrößen zugrunde liegen.

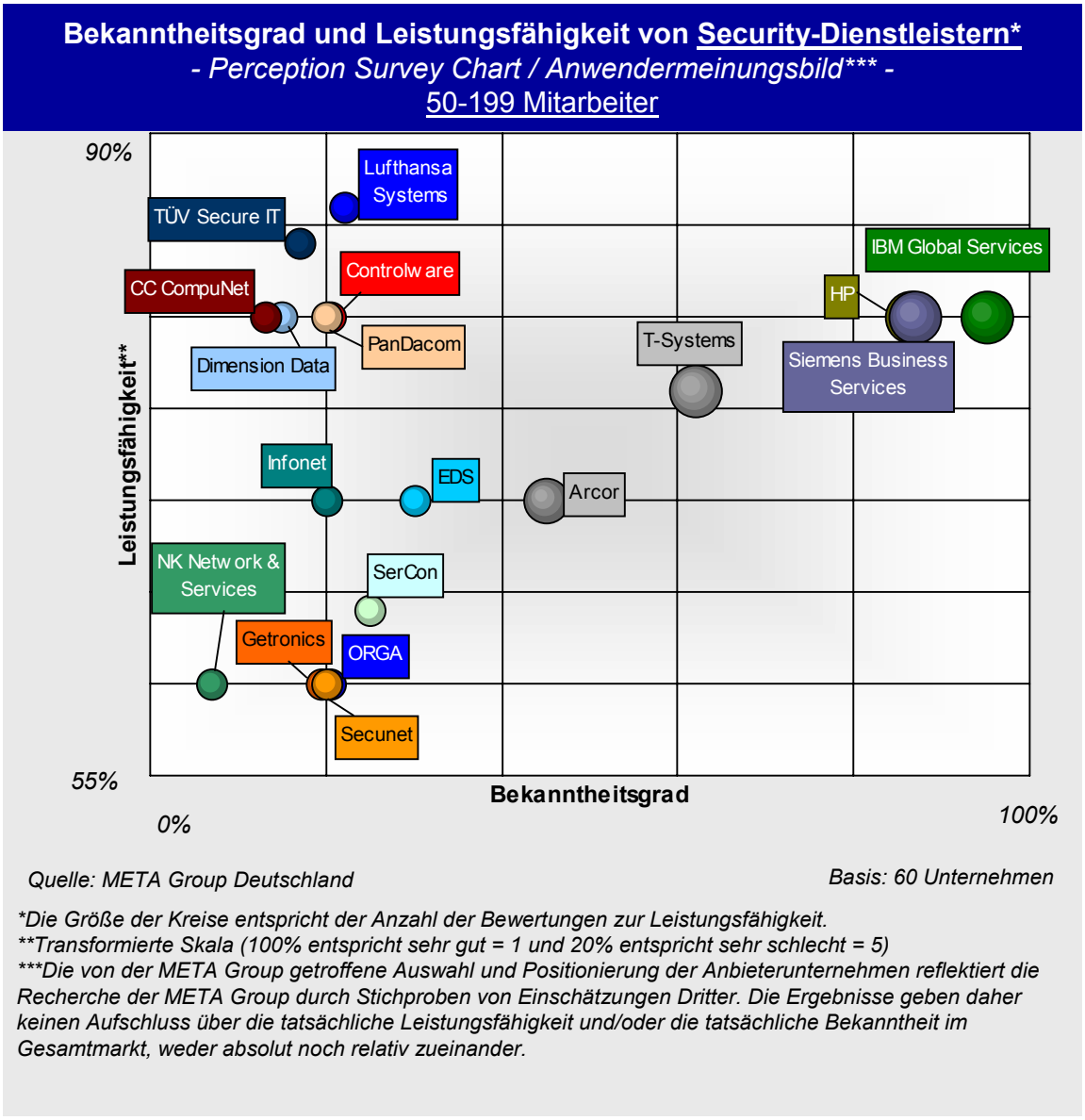
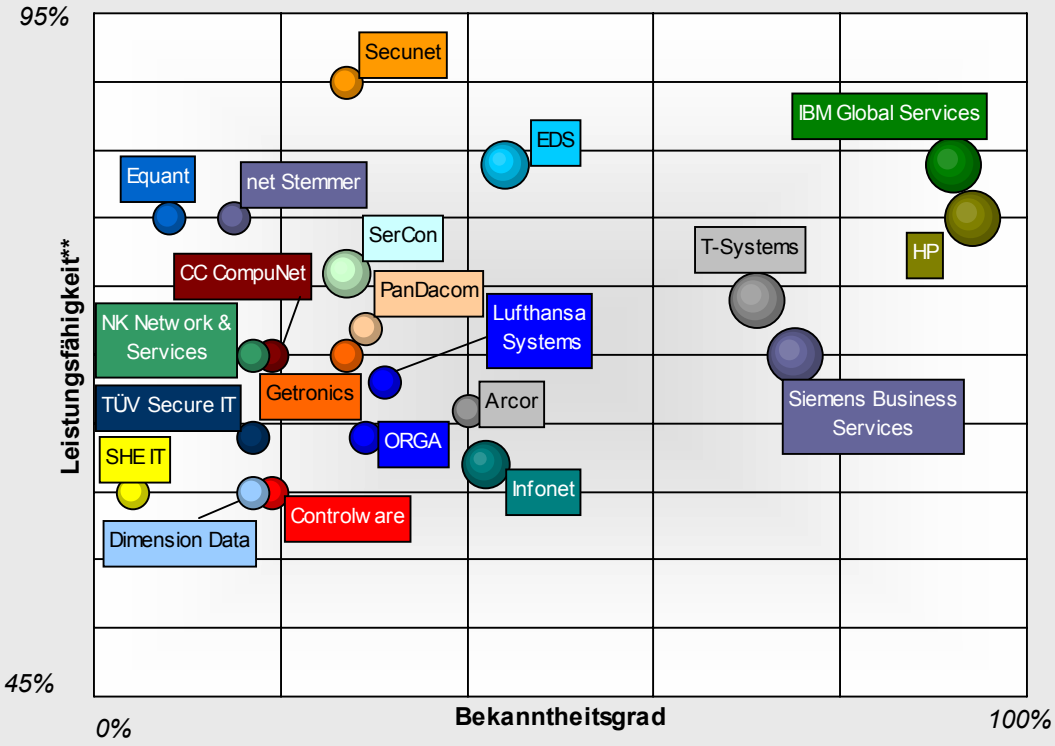


Abbildung 108: Bekanntheitsgrad/Leistungsfähigkeit von Security-Dienstleistern (50-199 Mitarbeiter)

Bekanntheitsgrad und Leistungsfähigkeit von Security-Dienstleistern*
*- Perception Survey Chart / Anwendermeinungsbild*** -*
200-499 Mitarbeiter



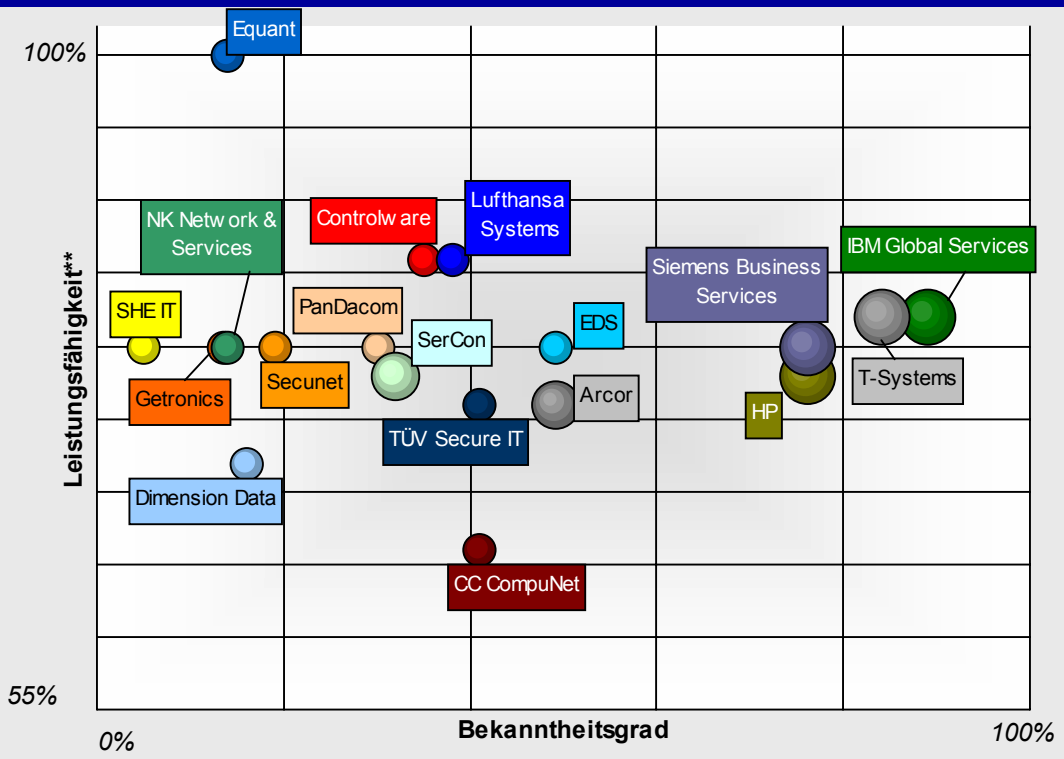
Quelle: META Group Deutschland

Basis: 48 Unternehmen

**Die Größe der Kreise entspricht der Anzahl der Bewertungen zur Leistungsfähigkeit.*
***Transformierte Skala (100% entspricht sehr gut = 1 und 20% entspricht sehr schlecht = 5)*
****Die von der META Group getroffene Auswahl und Positionierung der Anbieterunternehmen reflektiert die Recherche der META Group durch Stichproben von Einschätzungen Dritter. Die Ergebnisse geben daher keinen Aufschluss über die tatsächliche Leistungsfähigkeit und/oder die tatsächliche Bekanntheit im Gesamtmarkt, weder absolut noch relativ zueinander.*

Abbildung 109: Bekanntheitsgrad/Leistungsfähigkeit von Security-Dienstleistern (200-499 Mitarbeiter)

Bekanntheitsgrad und Leistungsfähigkeit von Security-Dienstleistern*
*- Perception Survey Chart / Anwendermeinungsbild*** -*
500-999 Mitarbeiter



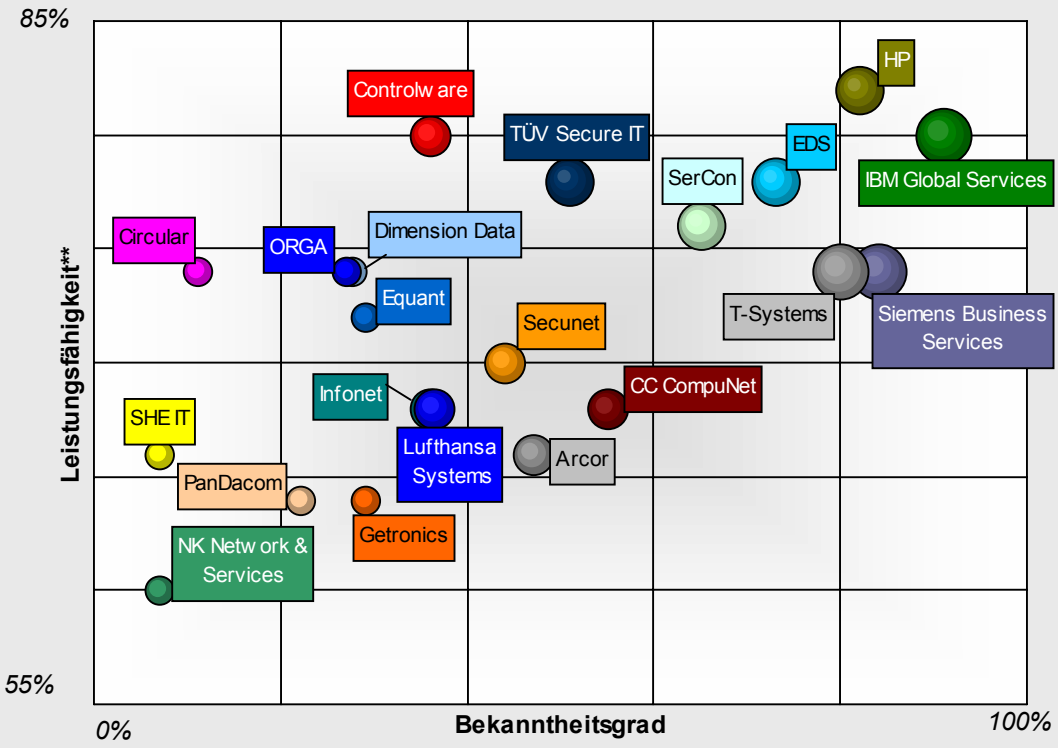
Quelle: META Group Deutschland

Basis: 37 Unternehmen

**Die Größe der Kreise entspricht der Anzahl der Bewertungen zur Leistungsfähigkeit.*
***Transformierte Skala (100% entspricht sehr gut = 1 und 20% entspricht sehr schlecht = 5)*
****Die von der META Group getroffene Auswahl und Positionierung der Anbieterunternehmen reflektiert die Recherche der META Group durch Stichproben von Einschätzungen Dritter. Die Ergebnisse geben daher keinen Aufschluss über die tatsächliche Leistungsfähigkeit und/oder die tatsächliche Bekanntheit im Gesamtmarkt, weder absolut noch relativ zueinander.*

Abbildung 110: Bekanntheitsgrad/Leistungsfähigkeit von Security-Dienstleistern (500-999 Mitarbeiter)

Bekanntheitsgrad und Leistungsfähigkeit von Security-Dienstleistern*
*- Perception Survey Chart / Anwendermeinungsbild*** -*
ab 1.000 Mitarbeiter



Quelle: META Group Deutschland

Basis: 55 Unternehmen

**Die Größe der Kreise entspricht der Anzahl der Bewertungen zur Leistungsfähigkeit.*
***Transformierte Skala (100% entspricht sehr gut = 1 und 20% entspricht sehr schlecht = 5)*
****Die von der META Group getroffene Auswahl und Positionierung der Anbieterunternehmen reflektiert die Recherche der META Group durch Stichproben von Einschätzungen Dritter. Die Ergebnisse geben daher keinen Aufschluss über die tatsächliche Leistungsfähigkeit und/oder die tatsächliche Bekanntheit im Gesamtmarkt, weder absolut noch relativ zueinander.*

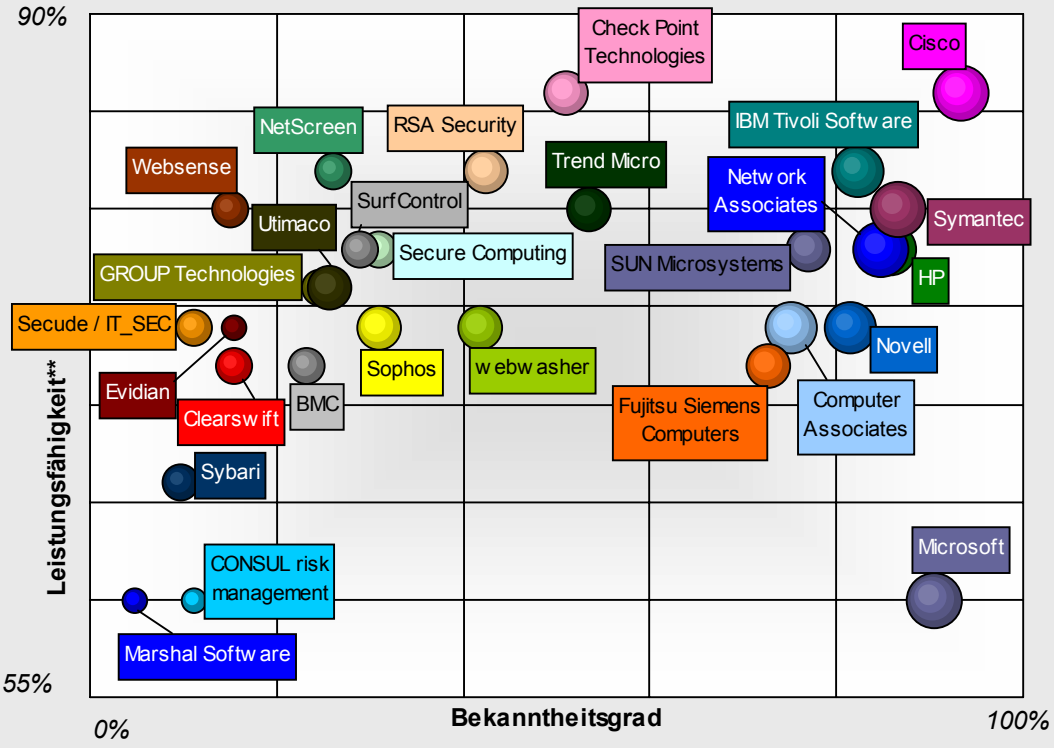
Abbildung 111: Bekanntheitsgrad/Leistungsfähigkeit von Security-Dienstleistern (ab 1.000 Mitarbeiter)

7.3.2.2 Einschätzung von IT-Security-Produktanbietern

Die folgende Abbildung zeigt eine Auswahl von Security-Produktanbietern sowie den gestützten Bekanntheitsgrad und die Bewertung der Leistungsfähigkeit durch die befragten Anwender im Überblick. Es wird darauf hingewiesen, dass diese Anbieterübersicht aufgrund des fragmentierten Security-Marktes keinen Anspruch auf Vollständigkeit erhebt. Die fünf bekanntesten Anbieter innerhalb dieser Übersicht sind Cisco, Microsoft, Symantec, HP und Network Associates. Bei der Bewertung der Leistungsfähigkeit durch die Anwender führen Check Point Technologies und Cisco - jeweils mit der Note „1,7“. Darauf folgen IBM Tivoli Software, NetScreen und RSA Security. Die Streuung der Bewertungen ist insgesamt gering – die Leistungsfähigkeit wird bei den meisten Anbietern zwischen „2“ (gut) und „2,5“ („gut bis befriedigend“) eingeschätzt. Kein Anbieter schneidet „schlecht“ ab.

Bekanntheitsgrad und Leistungsfähigkeit ausgewählter Anbieter von Security-Lösungen*

*- Perception Survey Chart / Anwendermeinungsbild*** -*



Quelle: META Group Deutschland

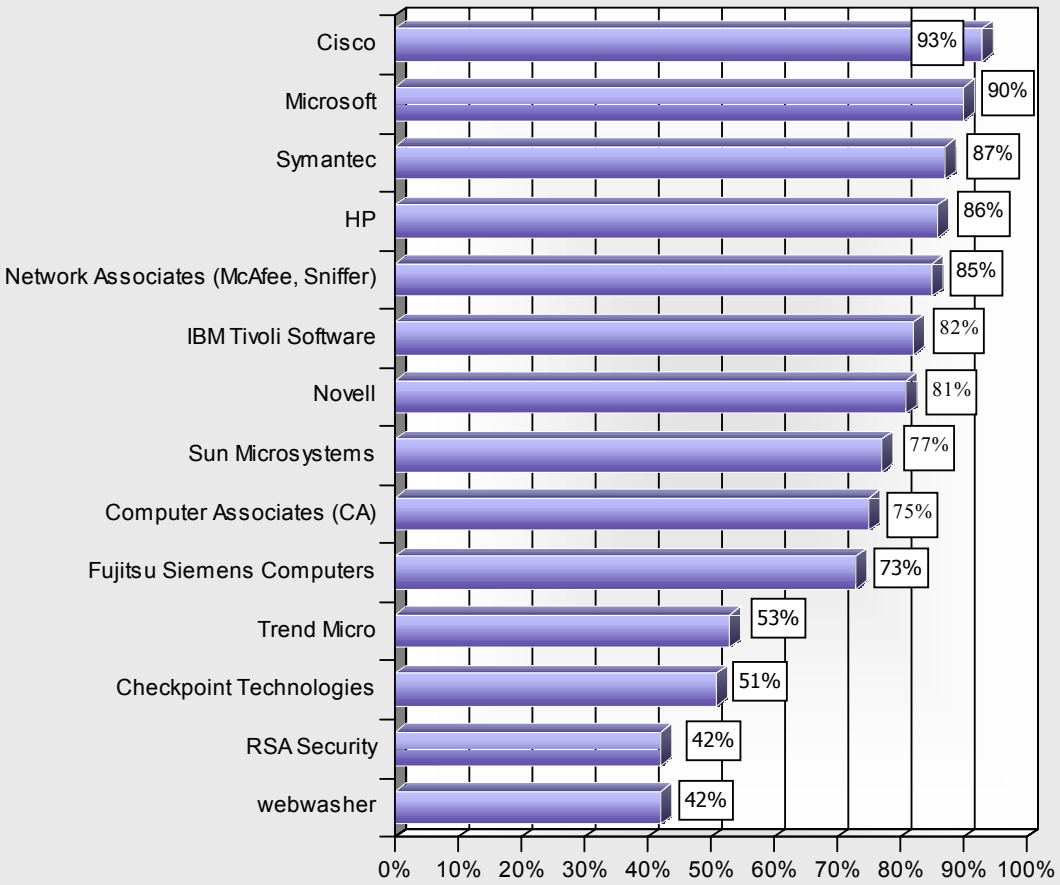
Basis: 208 Unternehmen

**Die Größe der Kreise entspricht der Anzahl der Bewertungen zur Leistungsfähigkeit.*
***Transformierte Skala (100% entspricht sehr gut = 1 und 20% entspricht sehr schlecht = 5)*
****Die von der META Group getroffene Auswahl und Positionierung der Anbieterunternehmen reflektiert die Recherche der META Group durch Stichproben von Einschätzungen Dritter. Die Ergebnisse geben daher keinen Aufschluss über die tatsächliche Leistungsfähigkeit und/oder die tatsächliche Bekanntheit im Gesamtmarkt, weder absolut noch relativ zueinander.*

Abbildung 112: Bekanntheitsgrad und Leistungsfähigkeit von Security-Produktanbietern

Eine Auswertung auf Basis der Aussagen aus verschiedenen Unternehmensgrößenklassen ist Abbildung 117 bis Abbildung 120 zu entnehmen. Ergänzend zur Anbieterübersicht auf der vorigen Seite werden im Folgenden der Bekanntheitsgrad und die Leistungsfähigkeit der einzelnen Anbieter gesondert dargestellt.

Welche der folgenden Anbieter von Security-Lösungen sind Ihnen bekannt? [1]
(Gesamt)

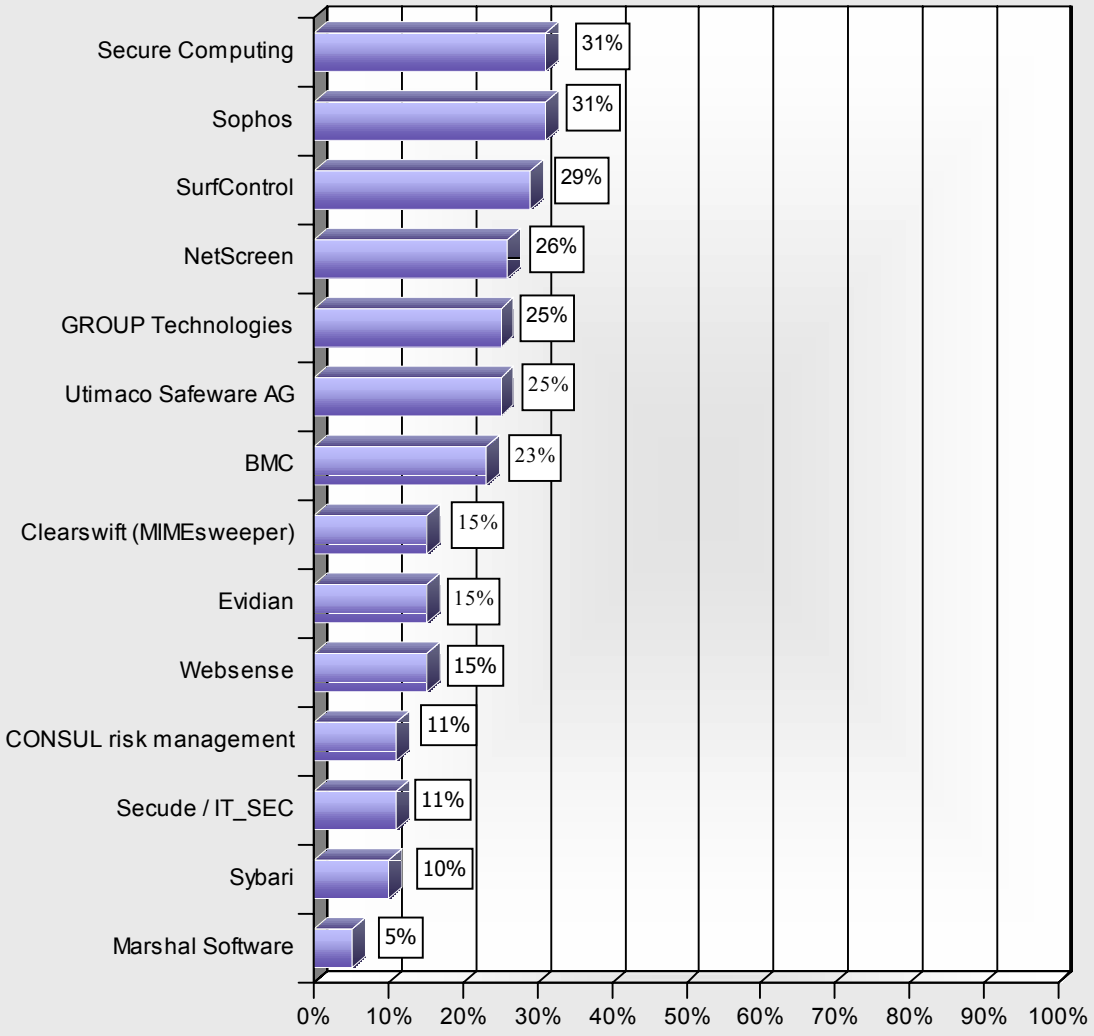


Quelle: META Group Deutschland

Mehrfachnennungen möglich
Basis: 208 Unternehmen

Abbildung 113: Ungestützter Bekanntheitsgrad ausgewählter Security-Produktanbieter (1)

Welche der folgenden Anbieter von Security-Lösungen sind Ihnen bekannt? [2]
(Gesamt)



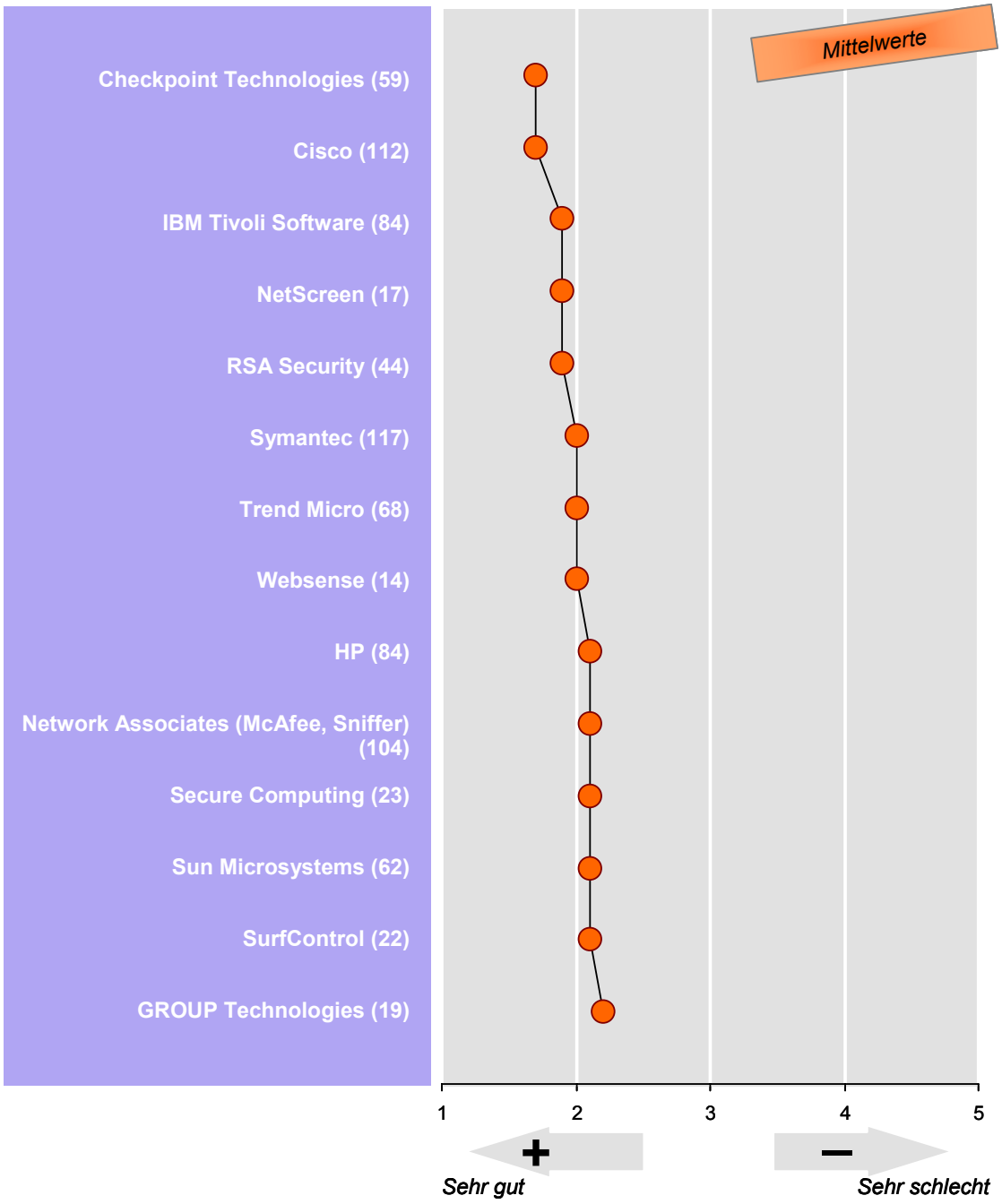
Quelle: META Group Deutschland

Mehrfachnennungen möglich
Basis: 208 Unternehmen

Abbildung 114: Ungestützter Bekanntheitsgrad ausgewählter Security-Produktanbieter (2)

Ergänzend zur Anbieterübersicht wird im Folgenden die Leistungsfähigkeit der einzelnen Anbieter – nach Einschätzung der befragten Anwenderunternehmen - gesondert dargestellt.

Wie hoch schätzen Sie die Leistungsfähigkeit der Ihnen bekannten Anbieter von Security-Lösungen ein? [1]

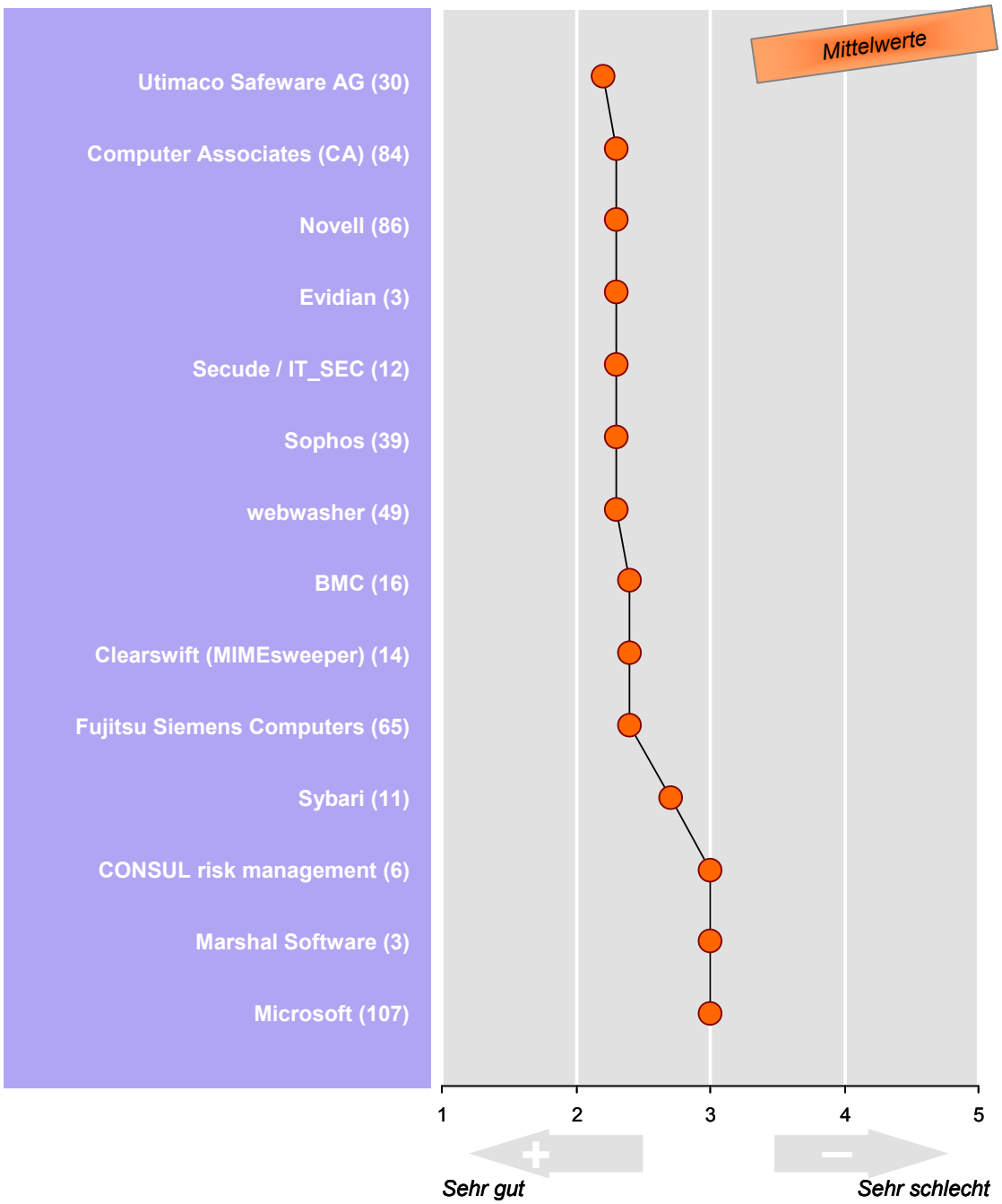


Quelle: META Group Deutschland

(x): Anzahl der Nennungen

Abbildung 115: Leistungsfähigkeit ausgewählter Security-Produktanbieter (1)

Wie hoch schätzen Sie die Leistungsfähigkeit der Ihnen bekannten Anbieter von Security-Lösungen ein? [2]



Quelle: META Group Deutschland

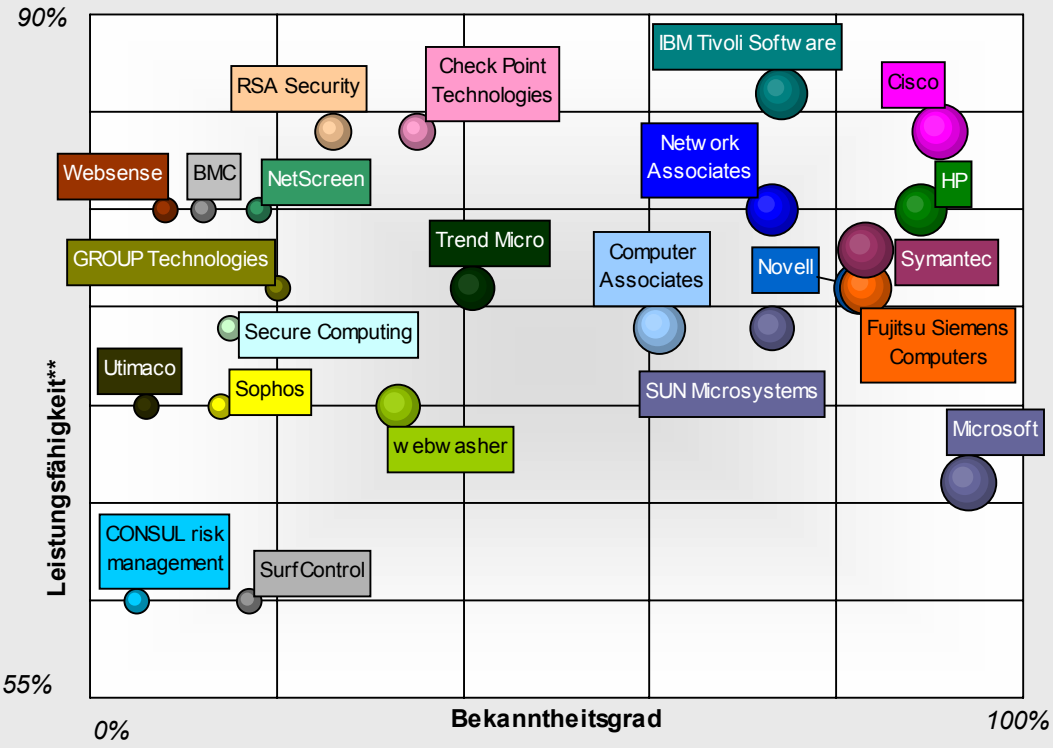
(x): Anzahl der Nennungen

Abbildung 116: Leistungsfähigkeit ausgewählter Security-Produktanbieter (2)

7.3.2.2.1 IT-Security-Lösungen – Auswertung nach Unternehmensgröße

Die einzelnen Produktanbieter werden von Anwendern verschiedener Unternehmensgrößenklassen in der Regel unterschiedlich bewertet. Näheren Aufschluss geben die folgenden Auswertungen. Es wird darauf hingewiesen, dass vor allem bei den weniger bekannten Anbietern teilweise kleine Stichprobengrößen zugrunde liegen.

Bekanntheitsgrad und Leistungsfähigkeit von Security-Lösungs-Anbietern*
*- Perception Survey Chart / Anwendermeinungsbild*** -*
50-199 Mitarbeiter



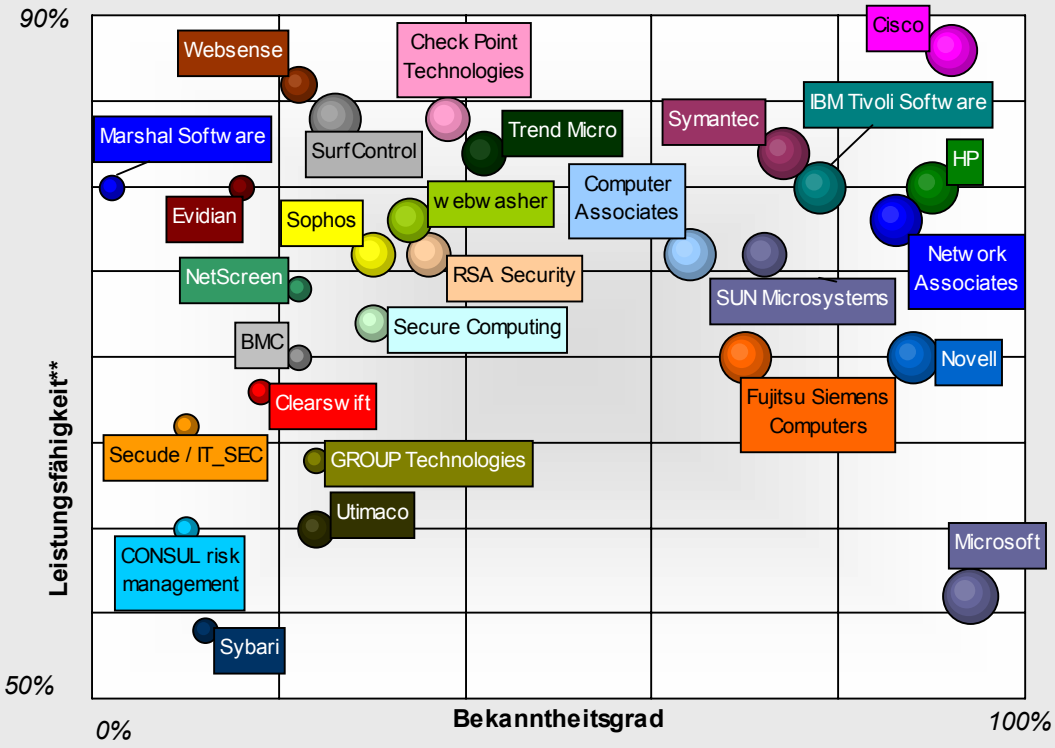
Quelle: META Group Deutschland

Basis: 66 Unternehmen

**Die Größe der Kreise entspricht der Anzahl der Bewertungen zur Leistungsfähigkeit.*
***Transformierte Skala (100% entspricht sehr gut = 1 und 20% entspricht sehr schlecht = 5)*
****Die von der META Group getroffene Auswahl und Positionierung der Anbieterunternehmen reflektiert die Recherche der META Group durch Stichproben von Einschätzungen Dritter. Die Ergebnisse geben daher keinen Aufschluss über die tatsächliche Leistungsfähigkeit und/oder die tatsächliche Bekanntheit im Gesamtmarkt, weder absolut noch relativ zueinander.*

Abbildung 117: Bekanntheitsgrad/Leistungsfähigkeit von Security-Produktanbietern (50-199 Mitarbeiter)

Bekanntheitsgrad und Leistungsfähigkeit von Security-Lösungs-Anbietern*
*- Perception Survey Chart / Anwendermeinungsbild*** -*
200-499 Mitarbeiter



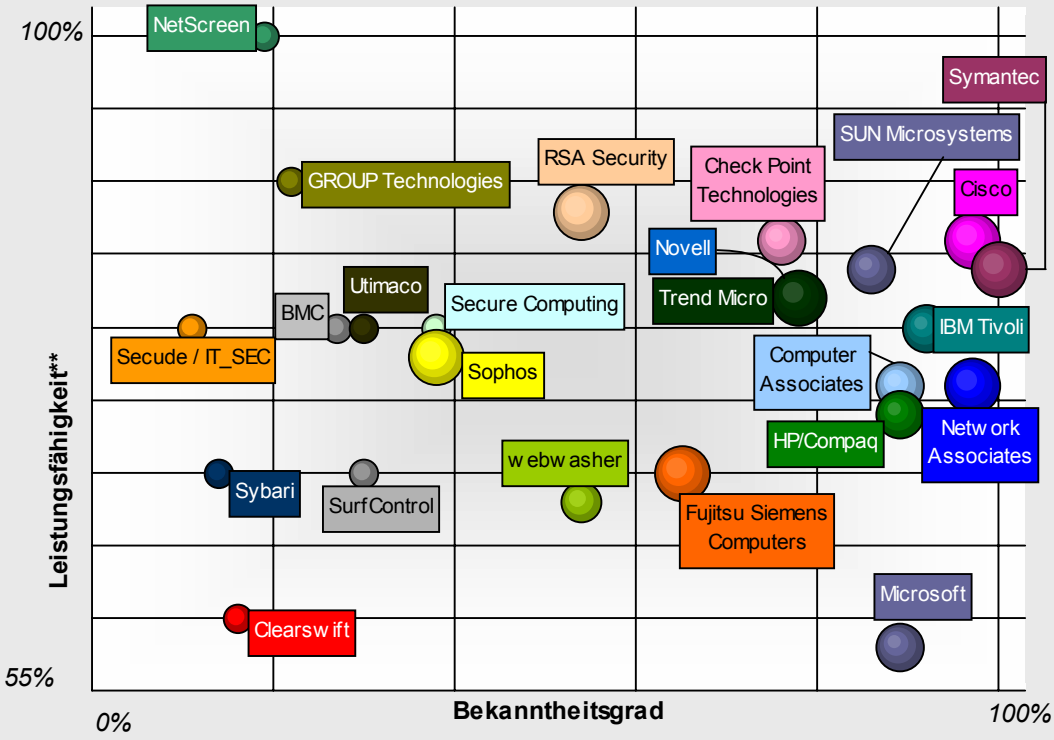
Quelle: META Group Deutschland

Basis: 50 Unternehmen

**Die Größe der Kreise entspricht der Anzahl der Bewertungen zur Leistungsfähigkeit.*
***Transformierte Skala (100% entspricht sehr gut = 1 und 20% entspricht sehr schlecht = 5)*
****Die von der META Group getroffene Auswahl und Positionierung der Anbieterunternehmen reflektiert die Recherche der META Group durch Stichproben von Einschätzungen Dritter. Die Ergebnisse geben daher keinen Aufschluss über die tatsächliche Leistungsfähigkeit und/oder die tatsächliche Bekanntheit im Gesamtmarkt, weder absolut noch relativ zueinander.*

Abbildung 118: Bekanntheitsgrad/Leistungsfähigkeit von Security-Produktanbietern (200-499 Mitarbeiter)

Bekanntheitsgrad und Leistungsfähigkeit von Security-Lösungs-Anbietern*
*- Perception Survey Chart / Anwendermeinungsbild***-*
500-999 Mitarbeiter



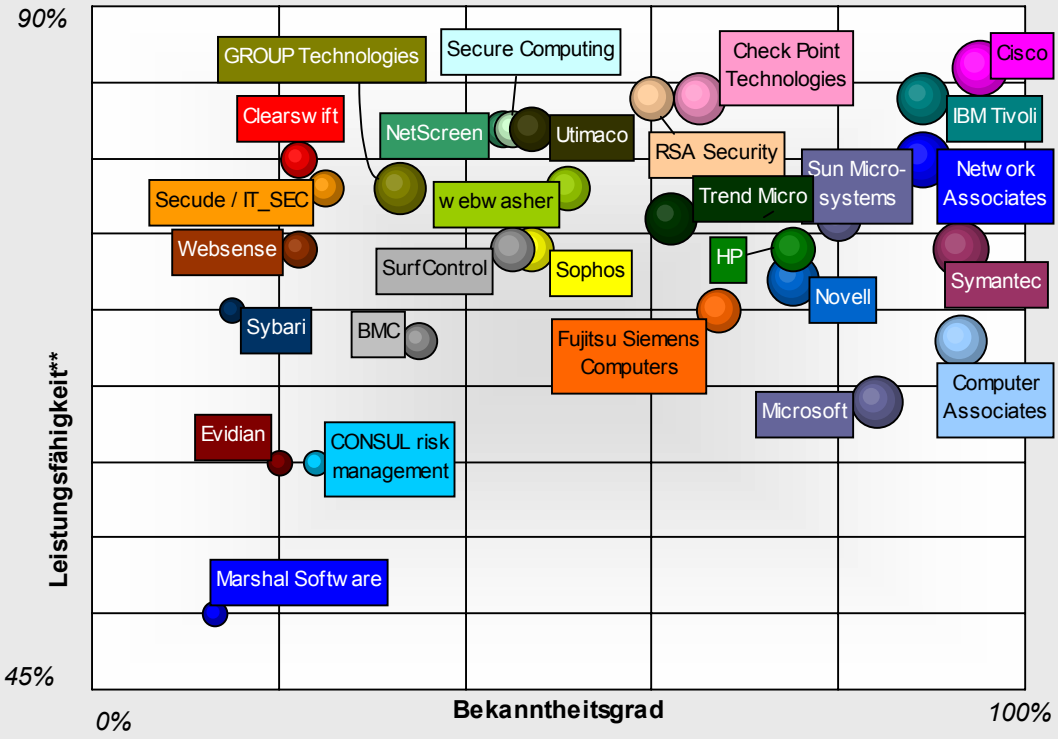
Quelle: META Group Deutschland

Basis: 37 Unternehmen

**Die Größe der Kreise entspricht der Anzahl der Bewertungen zur Leistungsfähigkeit.*
***Transformierte Skala (100% entspricht sehr gut = 1 und 20% entspricht sehr schlecht = 5)*
****Die von der META Group getroffene Auswahl und Positionierung der Anbieterunternehmen reflektiert die Recherche der META Group durch Stichproben von Einschätzungen Dritter. Die Ergebnisse geben daher keinen Aufschluss über die tatsächliche Leistungsfähigkeit und/oder die tatsächliche Bekanntheit im Gesamtmarkt, weder absolut noch relativ zueinander.*

Abbildung 119: Bekanntheitsgrad/Leistungsfähigkeit von Security-Produktanbietern (500-999 Mitarbeiter)

Bekanntheitsgrad und Leistungsfähigkeit von Security-Lösungs-Anbietern*
*- Perception Survey Chart/ Anwendermeinungsbild*** -*
ab 1.000 Mitarbeiter



Quelle: META Group Deutschland

Basis: 55 Unternehmen

**Die Größe der Kreise entspricht der Anzahl der Bewertungen zur Leistungsfähigkeit.*
***Transformierte Skala (100% entspricht sehr gut = 1 und 20% entspricht sehr schlecht = 5)*
****Die von der META Group getroffene Auswahl und Positionierung der Anbieterunternehmen reflektiert die Recherche der META Group durch Stichproben von Einschätzungen Dritter. Die Ergebnisse geben daher keinen Aufschluss über die tatsächliche Leistungsfähigkeit und/oder die tatsächliche Bekanntheit im Gesamtmarkt, weder absolut noch relativ zueinander.*

Abbildung 120: Bekanntheitsgrad/Leistungsfähigkeit von Security-Produktanbietern (ab 1.000 Mitarbeiter)

7.3.3 Anbieter auf der „Short List“ der Anwenderunternehmen

Ein hoher Bekanntheitsgrad ist für Anbieter eine gute Voraussetzung, um in den engeren Auswahlprozess bei Investitionsentscheidungen einbezogen zu werden. Im Rahmen der vorliegenden Untersuchung wurde hinterfragt, welche der den Anwenderunternehmen bekannten Anbieter auch tatsächlich auf der „Short List“ stehen. Den höchsten Prozentsatz bei **IT-Security-Services** erreicht IBM Global Services: dort ist der Anteil der Befragten, die den Dienstleister nicht nur kennen, sondern auch auf der Short List stehen haben, am größten. Zu den „Top 5“ gehören in diesem Zusammenhang ferner T-Systems, HP, Siemens Business Services sowie mit gleichen Anteilen SerCon und secunet.

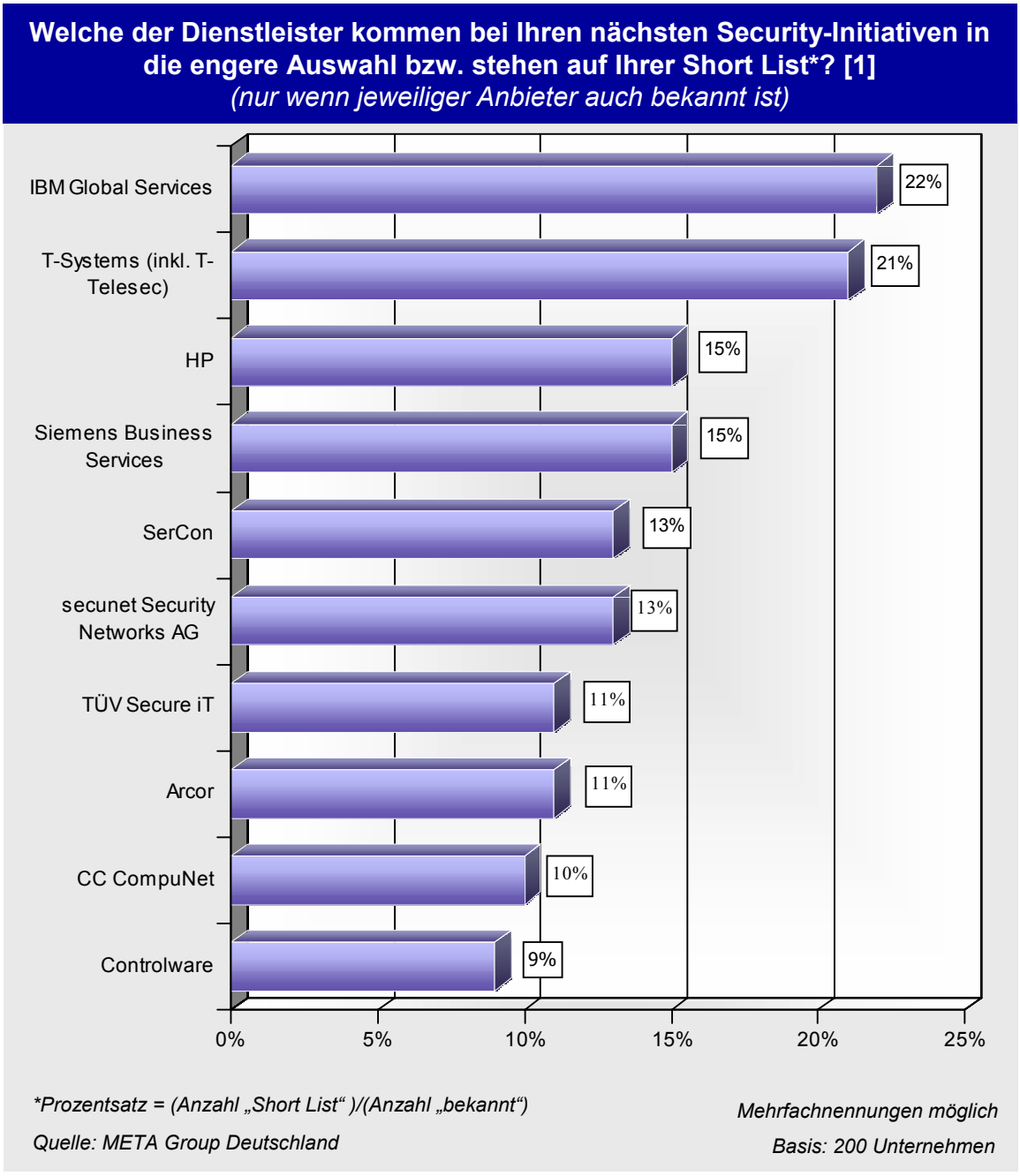
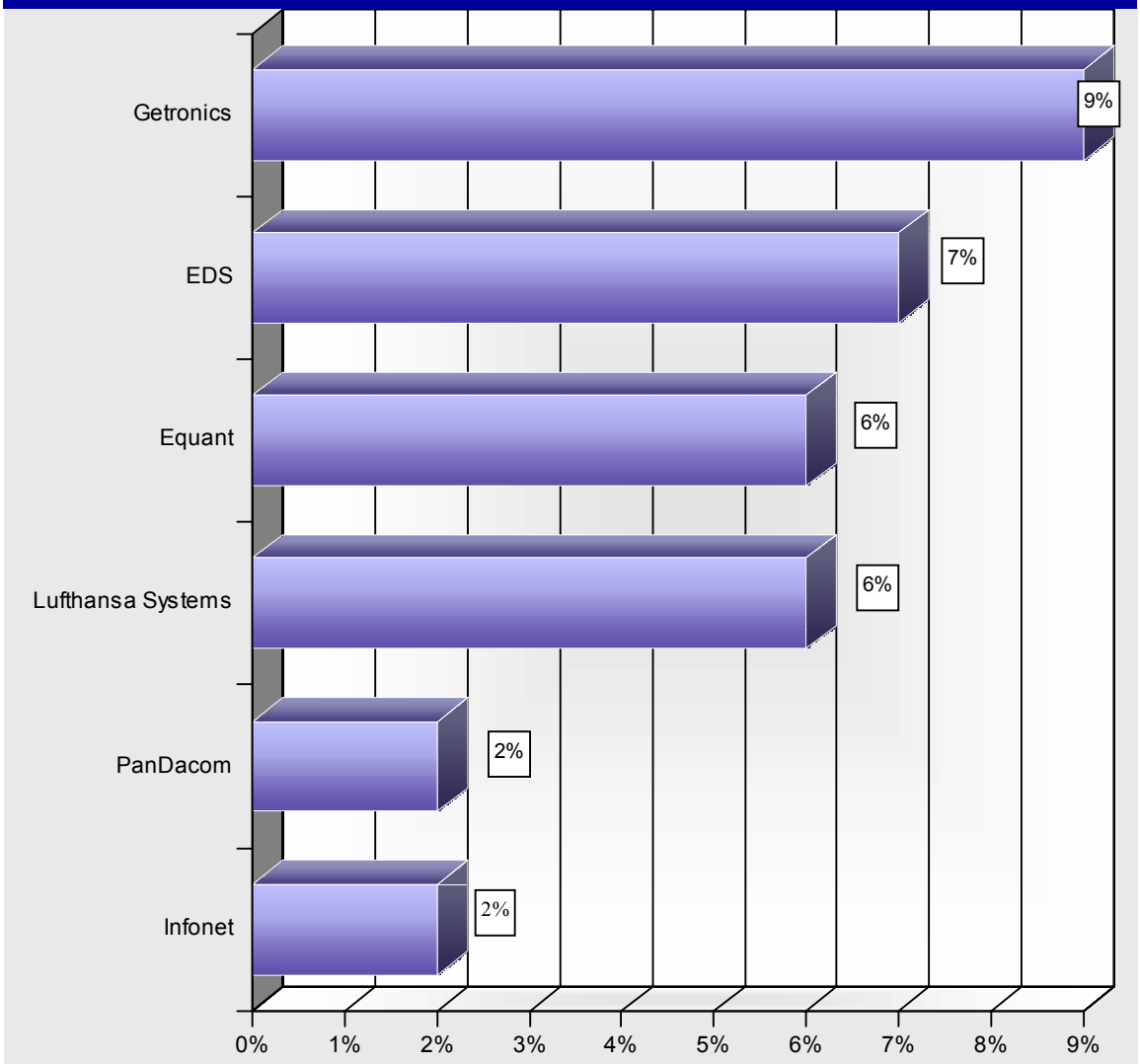


Abbildung 121: Ausgewählte Security-Dienstleister auf der Short List der Anwenderunternehmen (1)

Welche der Dienstleister kommen bei Ihren nächsten Security-Initiativen in die engere Auswahl bzw. stehen auf Ihrer Short List*? [2]
(nur wenn jeweiliger Anbieter auch bekannt ist)



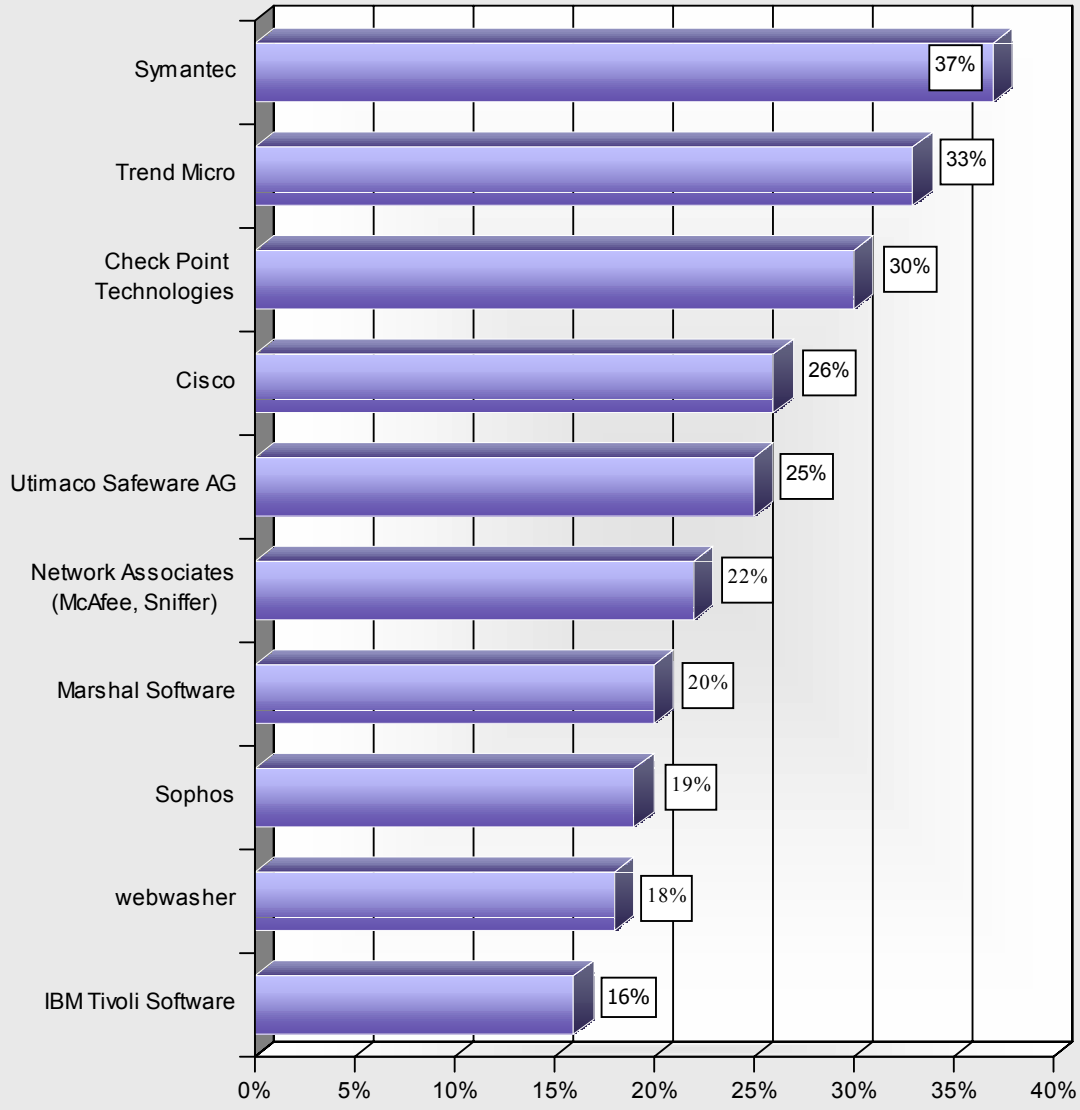
*Prozentsatz = (Anzahl „Short List“)/(Anzahl „bekannt“)
Quelle: META Group Deutschland

*Mehrfachnennungen möglich
Basis: 200 Unternehmen*

Abbildung 122: Ausgewählte Security-Dienstleister auf der Short List der Anwenderunternehmen (2)

Bei den Produktanbietern im IT-Security-Umfeld erreicht Symantec die höchste „Durchdringungsrate“, was den Anteil der Befragten anbetrifft, die den Anbieter in die engere Auswahl einbeziehen – bezogen auf die Anzahl der Unternehmen, die den Anbieter kennen. Im „Ranking“ folgen Trend Micro, Check Point Technologies, Cisco und Utimaco.

Welche Lösungs-Anbieter kommen bei Ihren nächsten Security-Initiativen in die engere Auswahl bzw. stehen auf Ihrer Short List*? [1]
(nur wenn jeweiliger Anbieter auch bekannt ist)

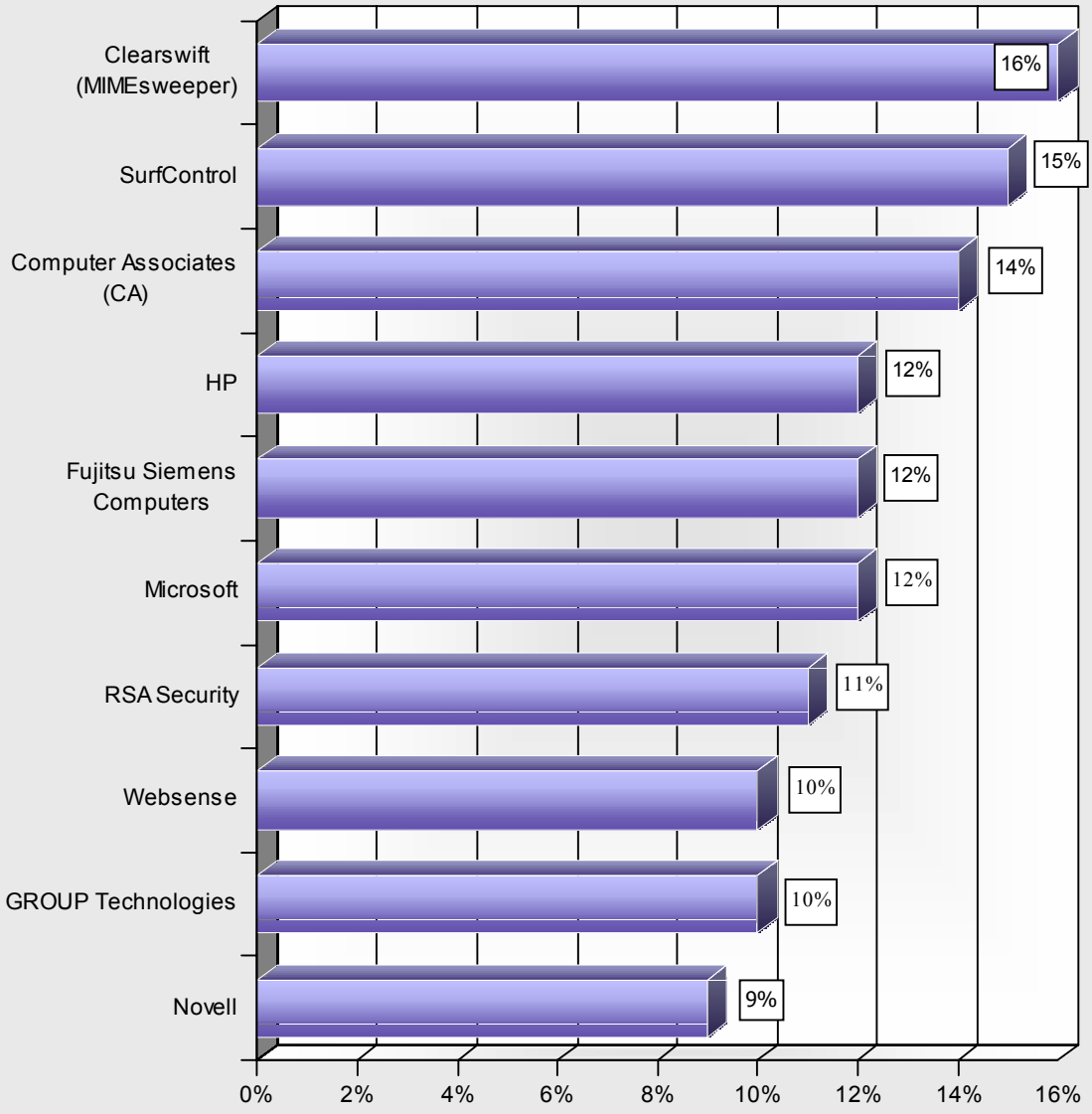


**Prozentsatz = (Anzahl „Short List“)/(Anzahl „bekannt“)*
Quelle: META Group Deutschland

Mehrfachnennungen möglich
Basis: 208 Unternehmen

Abbildung 123: Ausgewählte Security-Produktanbieter auf der Short List der Anwenderunternehmen (1)

Welche Lösungs-Anbieter kommen bei Ihren nächsten Security-Initiativen in die engere Auswahl bzw. stehen auf Ihrer Short List*? [2]
(nur wenn jeweiliger Anbieter auch bekannt ist)

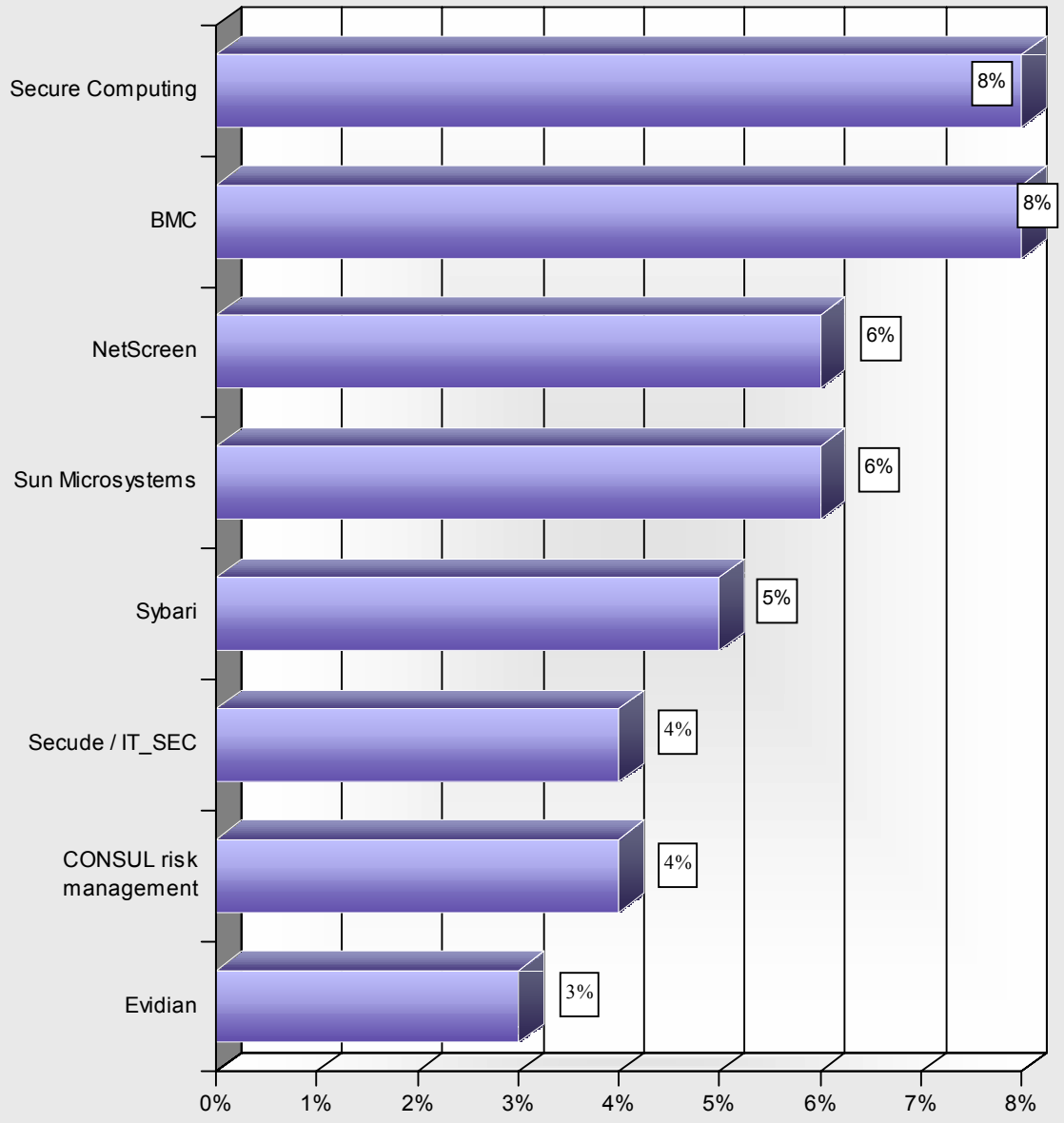


Prozentsatz = (Anzahl „Short List“)/(Anzahl „bekannt“)
Quelle: META Group Deutschland

Mehrfachnennungen möglich
Basis: 208 Unternehmen

Abbildung 124: Ausgewählte Security-Produktanbieter auf der Short List der Anwenderunternehmen (2)

Welche Lösungs-Anbieter kommen bei Ihren nächsten Security-Initiativen in die engere Auswahl bzw. stehen auf Ihrer Short List*? [3]
(nur wenn jeweiliger Anbieter auch bekannt ist)



**Prozentsatz = (Anzahl „Short List“)/(Anzahl „bekannt“)*
Quelle: META Group Deutschland

Mehrfachnennungen möglich
Basis: 208 Unternehmen

Abbildung 125: Ausgewählte Security-Produktanbieter auf der Short List der Anwenderunternehmen (3)

8 Marktentwicklung

8.1 Marktentwicklung in Deutschland

Der Markt für IT-Security-Produkte und –Dienstleistungen befand sich Anfang 2003 im Spannungsfeld zwischen steigenden Sicherheitsanforderungen und angespannten IT-Budgets. Jährliche Wachstumsraten in Höhe von 20 bis 30 Prozent, wie sie bis vor zwei Jahren noch zu beobachten waren, sind heute passé. Der Stellenwert der IT-Sicherheit wächst jedoch unvermindert weiter. Durchschnittlich über sechs Prozent des IT-Budgets geben deutsche Unternehmen mit mindestens 50 Mitarbeitern heute für IT-Sicherheit aus. Rund 40 Prozent der Ausgaben beziehen sich dabei auf Maßnahmen für „Datenschutz“ und Vertraulichkeit, der Rest auf Verfügbarkeitsthemen beziehungsweise „Datensicherheit“. Trotz nahezu stagnierender IT-Ausgaben wird der Security-Markt im Jahr 2003 immerhin um sieben Prozent auf knapp 3 Milliarden EURO wachsen. Die Umsätze im Service-Bereich werden dank des anhaltenden Know-how- und Personalmangels bei Anwendern mit acht Prozent etwas stärker zunehmen als bei Hardware- und Software-Produkten (sechs Prozent).

Die META Group geht davon aus, dass die Talsohle im Markt für IT-Sicherheit im Jahr 2003 durchschritten wird – eine halbwegs stabile weltweite politische und gesamtwirtschaftliche Situation vorausgesetzt. Das durchschnittliche jährliche Wachstum (CAGR) im IT-Sicherheits-Markt wird zwischen 2002 und 2005 rund 9,5 Prozent betragen. Damit gehört IT-Sicherheit zu den wichtigen Wachstumssegmenten im Bereich der Informationstechnologie.

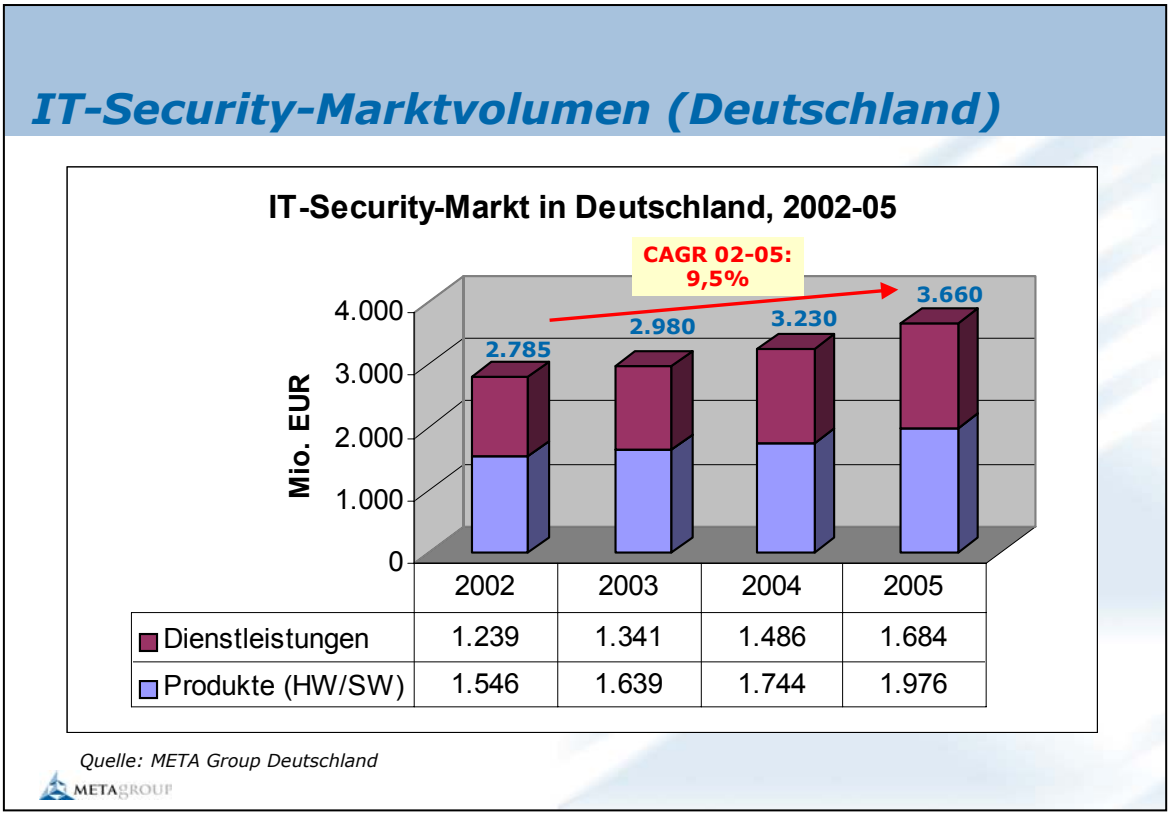


Abbildung 126: Marktentwicklung in Deutschland – IT-Security

Wachstumsimpulse werden bis Ende 2004 vor allem aus dem Dienstleistungssektor, der diskreten Fertigungsbranche, von Banken, Versicherungen und Finanzdienstleistungen sowie aus der Gruppe der Logistikunternehmen, Telekommunikationsdienstleister und Energieversorger kommen. Zurückhaltend bei den Investitionen in IT-Sicherheit sind hingegen die öffentliche Hand, die prozessorientierte Fertigung und der Handel.

Der klassische Mittelstand als Segment der Unternehmen mit weniger als 500 Mitarbeitern wird sich erst allmählich über die Risiken mangelnder IT-Sicherheit bewusst. Rechtliche Rahmenbedingungen wie Basel II werden langfristig entsprechende Maßnahmen zur Schadensverhütung mit anstoßen. Der Weg vom Bewusstsein zur Investition ist jedoch steinig und durch Budgetmangel gekennzeichnet. Mittelfristig, das heißt bis Ende 2004, sind aus dem Mittelstand deshalb keine besonderen Wachstumsimpulse für den IT-Security-Markt zu erwarten. Das Marktwachstum wird weitestgehend von großen Unternehmen und vom gehobenen Mittelstand mit 500 bis unter 1000 Mitarbeitern getragen. Letzterer zeigt aktuell sehr aggressive Investitionspläne für IT-Sicherheit.

8.1.1 Lösungen

Virenattacken werden von den Anwenderunternehmen in Deutschland als höchstes Sicherheitsrisiko eingestuft, und so ist es auch nicht weiter verwunderlich, dass der Einsatzgrad von Virenschutzlösungen heute nah an der 100%-Marke liegt. Auch Firewalls sind mittlerweile in den meisten Unternehmen Standard. Dennoch kann man von keiner Marktsättigung im eigentlichen Sinne sprechen. Die Anforderungen in den Bereichen Virenschutz und Firewall sind einer starken Dynamik unterworfen. So wird auch zukünftig eine stabile Nachfrage nach um neue Funktionalitäten erweiterten AV- und Firewall-Lösungen herrschen. Für eine hohe Grundaktivität bei den Sicherheits-Investitionen sorgen darüber hinaus Technologien für die Server-Zugriffskontrolle und Sicherheitsüberwachung sowie für die Nutzer-Authentifizierung (lokal und „remote“).

Im Jahr 2003 legen die Anwenderunternehmen verstärktes Augenmerk auf Content Security (Email- und Web-Filtering, SPAM-Filter). Der Wissensstand der Anwender über Ziele, Nutzen und Ausrichtung der einzelnen Lösungen ist jedoch derzeit noch sehr „durchwachsen“. Es ist nach Einschätzung der META Group nicht auszuschließen, dass zunächst in kleinerem Umfang investiert wird und sich erst nach umfassenden Bewusstseinskampagnen der Anbieter ab 2004 Content-Security-Lösungen in der Breite durchsetzen werden. Stetiges Wachstum hingegen ist bei Virtual Private Networks (VPN) zu verzeichnen. VPNs verknüpfen konkret nachweisbaren Nutzen mit IT-Sicherheit und ermöglichen damit eine einfachere Verkaufsargumentation gegenüber den Budgetverantwortlichen.

Etwas längerfristiger sehen die Planungen der Anwender in Bezug auf die Verschlüsselung von Emails und PCs sowie bei Public-Key-Infrastrukturen (PKI) aus. Nach dem Scheitern vieler PKI-Projekte in der Vergangenheit sind die Unternehmen nunmehr zurückhaltender geworden. Neue Vorhaben werden heute selektiv und vorsichtig angegangen. Die META Group geht in Deutschland

von einem geringen, aber stetigen Wachstum der PKI-Investitionen aus. Damit entwickelt sich das Thema zwar langsamer als vor zwei Jahren noch weitläufig vermutet, aber es ist nicht „tot“.

Weitere langfristig orientierte Themen sind WLAN-Sicherheit bzw. –Verschlüsselung, Intrusion Detection Systeme (IDS), die Verschlüsselung auf Anwendungsebene (z.B. Internetanwendungen), Web Single Sign-On, Directories sowie generell Identity Management als übergreifender Ansatz. Auch die Sicherheit von Web Services wird zunehmend ins Blickfeld rücken.

8.1.2 Dienstleistungen

Trotz der mittlerweile vergleichsweise entspannten Lage am IT-Arbeitsmarkt wirkt der Personalmangel bei deutschen Anwenderunternehmen immer noch als Hemmnis für IT-Security. Wo Budgets knapp sind, fehlt auch Geld für qualifizierte Security-Fachkräfte beziehungsweise internes Know-how. Es muss zudem davon ausgegangen werden, dass in wirtschaftlich unsicheren Zeiten die Unternehmen der Anstellung neuer Mitarbeiter vorsichtig gegenüberstehen. Externe Dienstleister unterstützen Anwenderunternehmen bei der Umsetzung von Maßnahmen, ohne dass sich das Unternehmen an neue Mitarbeiter „binden“ muss.

Deutsche Unternehmen nehmen in den Jahren 2003 und 2004 Sicherheitsdienstleister vor allem bei der Implementierung von Security-Lösungen, der Konzeption unternehmensweiter IT-Sicherheit und –Architekturen sowie für Managed Firewall Services in Anspruch. Managed Services für Firewalls gehören zu den wenigen Bereichen, auf die vor allem auch der klassische Mittelstand künftig verstärkt zugreifen wird.

Dienstleistungen rund um Penetration Testing, Ethical Hacking, Sicherheits-Audits und Risk Assessment sind allmählich im Kommen. Dies zeigt, dass das Sicherheitsbewusstsein in den vergangenen Jahren zugenommen hat, aber auch die Unsicherheit in Hinsicht auf die Verlässlichkeit der eigenen Security-Infrastrukturen und –Prozesse. Methoden des Risk Assessments müssen jedoch noch heranreifen. Sie werden mittelfristig vorwiegend in großen Unternehmen zum Einsatz kommen.

Das Outsourcing der Certificate Authority im Rahmen von PKI-Projekten wird künftig langsam zunehmen. Die META Group geht davon aus, dass es sich zunächst um begrenzte Implementierungen für spezielle Bereiche oder Nutzergruppen handelt und erst später teilweise um einen kompletten Roll-Out im ganzen Unternehmen.

Managed Services für Intrusion Detection und Vulnerability Scanning fristen mittelfristig noch ein Nischendasein. Populär ist hingegen neben dem Managed Firewall Service auch der Managed VPN Service. Nach Einschätzung der META Group ist die Reife von Managed VPN und Firewall Services bereits heute relativ weit gediehen. Entsprechende Dienste für Vulnerability Scanning werden weltweit erst bis Ende 2003 heranreifen, gefolgt von Managed Services für Intrusion Detection (2003/2004), Security Monitoring und Response (2004) sowie für Authentifizierung und Administration (2004/2005). Der deutsche Markt wird nach Einschätzung der META Group dieser Entwicklung um etwa ein Jahr hinterherhinken.

Die META Group ist der Meinung, dass die Anwenderunternehmen noch viel Bedarf an Unterstützung im Zusammenhang mit organisatorischen Sicherheitsaspekten haben. Bislang war dort IT-Sicherheit eng verknüpft mit technologischen und produktlastigen Aspekten. Doch nicht etwa in erster Linie Probleme mit Sicherheitstechnologien, sondern mangelndes Sicherheitsbewusstsein bei internen Anwendern im Unternehmen, Ressourcenmangel und die Unfähigkeit, verschiedene Risiken einzuschätzen, wirken heute hemmend für die IT-Sicherheit im Unternehmen. Eine weitere Herausforderung besteht auch im Management der Beziehung zwischen Kunde und Security-Dienstleister. Anwenderunternehmen sollten niemals die Verantwortung für IT-Sicherheit komplett outsourcen. Wichtig ist ein straffes Management der Outsourcing-Beziehung und umfassendes Verständnis des Anwenders für die Funktionen, die nach außen vergeben werden. Diese Voraussetzung dürfte bei vielen Anwenderunternehmen nicht gegeben sein: Nur ein Viertel der Unternehmen verfügt über ein dediziertes Security-Team, und weniger als die Hälfte hat irgendeine Form von schriftlich festgelegten Security Policies.

8.2 Entwicklungen in spezifischen Lösungsbereichen (Produkte)

8.2.1 Anbieterlandschaft Produkte

Die Anbieterlandschaft im Bereich IT-Security ist nach wie vor sehr fragmentiert. Hier tummeln sich spezialisierte Anbieter von Punktlösungen und von kompletten Security Suites, Anbieter aus dem Bereich Systems Management, die großen Systemhersteller sowie Plattformanbieter aus den Bereichen Netzwerke und Betriebssysteme. Die IT-Sicherheit als Querschnittsthema durchlebt einen permanenten Wandel, angetrieben durch ständig neue Anforderungen aus dem IT- und Business-Umfeld, wie beispielsweise die Absicherung von WLANs und Web Services. Die Konsolidierung von Anbieterlandschaften bleibt dabei nicht aus. Sie erfolgt in der Regel aber nur in einzelnen Marktsegmenten – insbesondere dann, wenn die Pionier- und „Early-Adopter“-Phase im betreffenden Marktsegment vorüber ist und die breite Wachstumsphase beginnt.

Die einzelnen Anbieter positionieren sich mit einzelnen oder gleich mehreren technologischen Themen, wobei teilweise erhebliche Überlappungen bestehen. Eine Auswahl von Security-Anbietern und ihre Positionierung in den jeweiligen Marktsegmenten zeigt folgende Grafik. Es wird darauf hingewiesen, dass der Schwerpunkt dieser Betrachtung auf dem „Datenschutz“ liegt, während Verfügbarkeitsthemen an dieser Stelle außen vor gelassen werden.

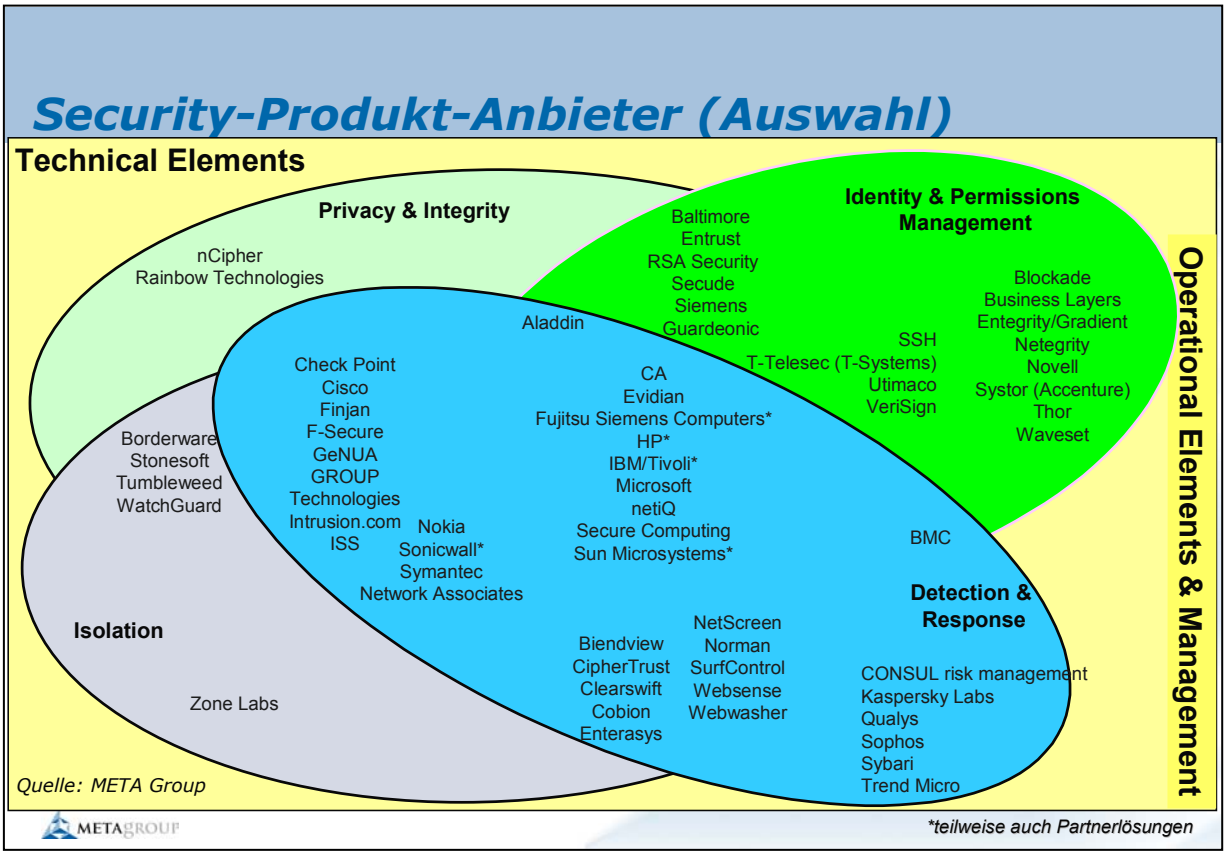


Abbildung 127: Anbieterlandschaft IT-Security (Auswahl)

Die **Marktsegmente** sind im Einzelnen (für Details siehe auch Abbildung 39).

- Identity & Permissions Management: Authentifizierung, Autorisierung und Directory Services
- Isolation: Access Control (logische und physische Zugriffskontrolle)
- Privacy & Integrity: Verschlüsselung und „Unwiederrufbarkeit“ (Non-Repudiation)
- Detection & Response: Filtering und Scanning, Benachrichtigung

Eine weitere Charakterisierung von Sicherheitsproduktanbietern, die bereits oben angesprochen wurde, ist die Kategorisierung entlang des Kerngeschäfts beziehungsweise der Strategie. Typische **Strategien** von Lösungsanbietern im Security-Umfeld sind:

- **Punktlösungen:** Diese Anbieter sind oftmals Technologieführer in jungen Märkten oder in Marktnischen. Sie stehen vor der Herausforderung, ihren technologischen Vorsprung auf Dauer zu halten oder eine Marktnische zu besetzen, um nicht langfristig von größeren Playern verdrängt zu werden.
- Anbieter von kompletten **Security-Suites** nutzen ihre breite installierte Basis und ihr Branding aktiv für Neugeschäft. Sie sind nicht immer in allen Bereichen auf Anhieb technologieführend, adaptieren aber oftmals neue Technologien durch Zukauf von kleineren Anbietern. Integrierte

Lösungen und Zukunftssicherheit sind Schlagworte, die typischerweise als Differenzierungsmerkmale kommuniziert werden. Weltweit führende Anbieter von Security Suites – sofern sie nicht in die Kategorie des Systems Management fallen – sind Network Associates und Symantec.

- **Systems-Management-Anbieter** gehen von einer wichtigen Komponente der IT-Sicherheit aus: dem Security Management. Sie haben gleichwohl damit eine vielversprechende Umsatzquelle erschlossen und mittlerweile ihr Portfolio um mehr oder weniger umfassende Security Suites erweitert. Neue Funktionalitäten werden über Akquisitionen, Eigenentwicklungen oder Partner integriert. Zur Kategorie der Systems-Management-Anbieter mit Security Suites gehören unter anderem BMC, Computer Associates (CA) und IBM Tivoli Software.
- **Systemhersteller bzw. Hardware-Plattform-Anbieter** sind darauf bedacht, dem Kunden sehr sichere und verlässliche Produkte bereitzustellen, sind diese doch Grundlage für sichere und verfügbare Geschäftsprozesse. Der Umsatz mit IT-Sicherheit fällt bei diesen Anbietern nicht so stark ins Gewicht, vielmehr dagegen der Gewinn an Vertrauen bei der Kundschaft. Zudem werden immer häufiger schlüsselfertige und vorintegrierte Systeme mit standardisierten Modulen angeboten, die dem Kunden mit relativ wenig Aufwand ein hohes Maß an Sicherheit bringen. Die Sicherheitslösungen stammen teils aus dem eigenen Hause, teils werden sie zusammen mit Partnern gebündelt. Zur Kategorie der Systemhersteller gehören Fujitsu Siemens Computers, HP, IBM und Sun Microsystems.
- **Plattformanbieter (Netzwerke):** Diese adressieren traditionell das Thema Netzwerksicherheit. Die Motivation zur Erweiterung des Produktportfolios um IT-Security-Funktionalitäten ist ähnlich wie bei Systems-Management-Anbietern. Netzwerkhersteller bieten insbesondere VPN-, Firewall- und Intrusion Detection Lösungen sowie Produkte für Netzwerkmanagement und Vulnerability Scanning an. Zu dieser Anbieterkategorie gehören Cisco, Nokia und weitere Anbieter.
- **Anbieter von Betriebsumgebungen** legen verstärktes Augenmerk auf die Sicherheit ihrer Plattformen. In diese Kategorie fällt neben den Systemherstellern vor allem auch Microsoft.

Im Folgenden sind Kurzprofile ausgewählter Anbieter von IT-Sicherheits-Lösungen aufgeführt.

BMC Software

BMC Software ist einer der weltweit führenden Anbieter von Enterprise Management Lösungen. Assuring Business Availability - also die gesicherte Verfügbarkeit sämtlicher unternehmenskritischer Anwendungen und Prozesse im Unternehmen - ist eines der Kernthemen der Geschäftstätigkeit von BMC. Für eine kontinuierliche Steigerung des Unternehmenswertes unterstützt BMC Kunden mit einem proaktiven Ansatz vor allem bei der Verbesserung der bereitgestellten IT-Dienste und gleichzeitigen Minimierung der anfallenden Kosten. BMC Software gliedert sein Produkt- und Service-Portfolio in die Geschäftsbereiche Enterprise Systems Management und Enterprise Data Management. Dazu kommen strategische Initiativen wie Storage Management, Security Management, SAP Management, Linux und Service-Provider-Lösungen. Auf diese Weise stellt BMC Software für jeden

Kunden ein individuelles Lösungspaket zusammen, das eine globale Sicht auf komplexe IT-Landschaften erlaubt. Gegründet im Jahr 1980, beschäftigt BMC Software heute weltweit über 6.400 Mitarbeiter. Der Gesamtumsatz des Unternehmens im Geschäftsjahr 2002 betrug ca. 1,3 Milliarden US$.

Cisco Systems

Ciscos Produktpalette für die Daten-, Sprach- und Videokommunikation reicht von Multiprotokoll-Routern und Workgroup-Systemen über ATM- und Ethernet-Switches bis hin zu Dial-up Access-Servern und Software-Routern sowie der entsprechenden Netzwerkmanagement-Software (Cisco IOS: Internet Operating System). Cisco liefert durchgängige „End-to-End"-Lösungen für alle Bereiche des Internetworking: LAN, Campus, WAN und Remote Access. Intelligentes Netzwerkmanagement und eine optimale Ressourcennutzung wird mit Systemen wie Content Delivery Networking und der Paketpriorisierung in Netzen möglich. Im Bereich der IT-Sicherheit bietet Cisco mit SAFE eine integrierte Sicherheitslösung, die auf die vielschichtigen Anforderungen moderner Netzwerke abgestimmt ist. Die zugrundeliegenden technischen Komponenten reichen von Firewalls, Routern und Intrusion Detection Systemen bis hin zu Lösungen für VPN und Policy-Management. Gegründet 1984, erzielte Cisco im Geschäftsjahr 2002 mit rund 36.000 Mitarbeitern weltweit einen Umsatz von rund 18,9 Milliarden US-Dollar. Die europäische Unternehmenszentrale von Cisco ist in London. Die deutsche Niederlassung Cisco Systems GmbH hat ihren Sitz in Hallbergmoos bei München.

Clearswift

Clearswift gehört weltweit zu den führenden Software-Anbietern für das Management und die Absicherung elektronischer Kommunikation. Clearswift unterstützt Unternehmen beim Schutz gegen Email- und web-basierte Bedrohungen, bei der Erfüllung von rechtlichen Vorgaben und bei der Umsetzung produktivitätssteigernder Policies. Außerdem sorgt Clearswift für das Management und den Schutz von geistigem Eigentum im Unternehmensnetzwerk. Das Produktportfolio des Anbieters umfasst Clearswift MIMEsweeper und Clearswift ENTERPRISEsuite. Die Produktfamilie Clearswift MIMEsweeper (MSW) unterstützt bei der Implementierung von Policies für die Kommunikation über Web und Email. Die Clearswift ENTERPRISEsuite (ES) stellt die e-Policy-Infrastruktur und Technologie bereit, die es komplexen Organisationen ermöglicht, umfassende Management- und Sicherheitslösungen zu realisieren. Die Wurzeln des Unternehmens reichen bis ins Jahr 1998 zurück. Clearswift hat heute 12.200 Kunden und 11 Millionen Nutzer weltweit. Die Firmenzentrale befindet sich in Theale (UK); die deutsche Niederlassung ist in Hamburg.

CA Computer Associates

Computer Associates International, Inc. (NYSE: CA), entwickelt anspruchsvolle Software-Lösungen für das eBusiness-Management: Unicenter für Infrastrukturmanagement, BrightStor für Speicher-management, *e*Trust für Sicherheitsmanagement, CleverPath für Portal- und Business Intelligence-Lösungen, AllFusion für Application Life Cycle Management, Advantage für Datenverwaltung und Anwendungsentwicklung sowie Jasmine für objektorientierte Datenbanktechnologie. CA bietet mit *e*Trust ein umfassendes Portfolio von Sicherheitslösungen, die durch den Schutz vorhandener

Technologien das eBusiness unterstützen und ermöglichen. Um diesen Anforderungen gerecht zu werden, hat CA seine Lösungen in die Kategorien *e*Trust Internet Access Solution Set, *e*Trust Defense Solution Set und *e*Trust Management Solution Set eingeteilt. CA wurde 1976 gegründet und betreut heute Kunden in über 100 Ländern. Mit 16.000 Mitarbeitern wurden im Geschäftsjahr 2002 weltweit 2,96 Milliarden US$ Umsatz erbracht. In Deutschland sind 580 Mitarbeiter tätig; der Hauptsitz der CA Computer Associates GmbH liegt in Darmstadt.

CONSUL risk management

CONSUL risk management ist ein Anbieter von IT-Security-Software mit Schwerpunkt auf Audit- und Administrations-Werkzeugen für unternehmensweites Sicherheitsmanagement. CONSUL wurde 1986 gegründet und hat seinen Hauptsitz in Delft / Niederlande. Heute gehört CONSUL in den Niederlanden zu den größten unabhängigen Anbietern von Sicherheitssoftware. Das Unternehmen ist international mit Niederlassungen in den USA und in Deutschland vertreten und verfügt weltweit über ein Partnernetzwerk. Das Produktportfolio umfasst das plattformübergreifende Consul/eAudit für die Konsolidierung und Korrelation von Sicherheitsbedrohungen und die CONSUL zSecure Pro Suite für Mainframe-Umgebungen. Neben der Entwicklung von Sicherheitssoftware bietet CONSUL auch Consulting-Dienstleistungen im Umfeld des Security-Managements an, beispielsweise in Form von schnellen und genauen Audits hinsichtlich der Angreifbarkeit von IT-Systemen.

Fujitsu Siemens Computers

Fujitsu Siemens Computers bedient den Endkunden- und Geschäftskundenmarkt in 25 Ländern in Europa mit einer kompletten Palette von Computerprodukten, angefangen bei PDAs und Notebooks, PCs und Workstations über Intel- und Unix-Server bis hin zu Großrechnern und Speicherlösungen. Im Rahmen seiner strategischen Ausrichtung legt Fujitsu Siemens Computers seinen Fokus auf die Zukunftsthemen "Business Critical Computing" und "Mobilität" und bietet seinen Kunden Produkte und Lösungen, die diese Schlüsselbereiche des Internet-Zeitalters, der mobilen Welt und des e-Business unterstützen. Fujitsu Siemens offeriert in diesem Zusammenhang ein breites Produktportfolio für IT-Security im Server- und Client-Bereich, sowohl für den Datenschutz als auch für Hochverfügbarkeit. Dabei greift das Unternehmen neben eigenen Lösungen vor allem auch auf Produkte führender Anbieter zurück, die als Partner im Global Alliance Programm mit integrationsfähigen und skalierbaren Security-Lösungen vertreten sind. Überdies unterstützt Fujitsu-Siemens seine Kunden durch Beratungs- und Implementierungsleistungen im Umfeld der IT-Security. Realisiert wird dies durch ein Security Competence Center als internem Querschnittsbereich sowie in Zusammenarbeit mit IT-Dienstleistern. Die deutsche Vertriebsorganisation von Fujitsu Siemens Computers hat rund 2.000 Mitarbeiter und erwirtschaftete im Geschäftsjahr 2001/02 (1.4.2001 bis 31.3.2002) einen Umsatz von 2,6 Milliarden EUR (weltweit: 5,4 Mrd. EUR).

GROUP Technologies

Die GROUP Technologies AG ist ein Hersteller von Email-Sicherheitssoftware und agiert im wachstumsstarken Markt für Content Security. GROUP positioniert sich mit zukunftsweisenden Produkten als Technologie- und Innovationsführer in den Bereichen Sicherheit, Organisation und Management von Emails. Die aufeinander abgestimmten Produkte sind für die Plattformen Microsoft Exchange und Lotus Notes Domino erhältlich. Das Leistungsspektrum der iQ.Suite reicht von Kryptografie über Virenschutz und Content Filtering bis zur revisionssicheren Ablage von Emails. Ein besonderes Feature der iQ.Suite ist der Schutz vor Industriespionage per Email. Die Standard-softwaremodule der Produktlinien umfassen securiQ, organiziQ und managiQ. securiQ gewährleistet einen regelbasierten Informationsschutz sowie die Sicherstellung der Datenintegrität. organiziQ ist das regelbasierte Organisationstool zur Verwaltung und Zuordnung eingehender und ausgehender sowie im System befindlicher Informationen. managiQ stellt die quantitative Transparenz des Email-Verkehrs her und liefert unter anderem konsolidierte Informationen über Menge, Größe und Häufigkeiten der Email-Kommunikation. Das Unternehmen bietet seine Produkte sowohl im Direktvertrieb als auch über OEM- und Handels-Partner an. Die Zentrale der GROUP Technologies AG befindet sich in Karlsruhe. Die GROUP Technologies AG beschäftigt aktuell rund 100 Mitarbeiter. Im Jahr 2001 wurde ein Umsatz von rund 8,9 Mio. EUR erwirtschaftet.

IBM Tivoli Software

Tivoli Software von IBM richtet sich an Mittelstands- und Großunternehmen zum Management der e-infrastructure. Tivoli Software erlaubt, das Netzwerk- und Systemmanagement durchgängig zu organisieren, vom Rechenzentrum bis ins Internet, vom Desktop bis zu intelligenten Endgeräten. Das modulare Tivoli Softwareportfolio umfasst unter anderem Netzwerkkontrolle, Inventarisierung, Softwareverteilung, Benutzerverwaltung, Fernwartung u.v.m. Vom Sicherheits-, Speicher-, und SAN-Management bis hin zum Management virtueller Marktplätze und mobiler Geräte werden zuverlässige Lösungen für eine schnell wachsende IT geboten. Bei IBM Tivoli Software ist gleichzeitig die technische Security-Expertise von IBM konzentriert. Die IBM Tivoli Security Management Lösungen adressieren zwei kritische e-Business-Herausforderungen: automatisiertes Identity Management und Security Event Management. Die IBM Tivoli Identity Management Lösung zielt auf einen schnell realisierbaren ROI ab, indem Nutzer, Systeme und Anwendungen zügig „online“ gebracht werden, während die Nutzer, Zugriffsrechte und Privacy-Einstellungen auf effiziente Weise über den gesamten Identity-Lebenszyklus gemanagt werden. Die IBM Tivoli Security Event Lösung unterstützt beim aktiven Monitoring, der Korrelation von Sicherheitszwischenfällen und einer schnellen Reaktion auf solche Zwischenfälle. Gegründet im Jahr 1989, ist Tivoli seit 1996 ein hundertprozentiges Tochterunternehmen der IBM. Tivoli beschäftigt heute weltweit rund 5.000 Mitarbeiter.

Microsoft

Microsoft ist der weltweit führende Hersteller von PC-Software. Die Produktpalette von Microsoft erstreckt sich von Betriebssystemen für PCs und Netzwerke über Serversoftware für Client-Server-Umgebungen, Anwendungsprogramme und Desktop-Applikationen für Unternehmen und den privaten

Nutzer und Multimedia-Anwendungen bis hin zu Internet-Plattformen und Entwickler-Tools. Anfang 2002 hat Microsoft unter der Bezeichnung „Trustworthy Computing“ eine unternehmensweite Initiative gestartet, die die Sicherheit beim Einsatz von Microsoft-Lösungen langfristig erhöhen soll. Trustworthy Computing stützt sich auf vier Pfeiler: IT-Sicherheit, Privacy, Zuverlässigkeit und Geschäftsintegrität. Im Rahmen der Initiative werden die Kunden unter anderem durch Richtlinien und Werkzeuge sowie Update- und Patch-Services unterstützt. Außerdem möchte Microsoft der Überprüfung der Produkte in Hinsicht auf Sicherheitsaspekte höchste Priorität einräumen – auch gegenüber der Weiterentwicklung seiner Produkte. Microsoft bietet ein umfassendes Portfolio an IT-Security-Produkten und –Dienstleistungen in den Bereichen "Prozesse und Technologien", "Desktopsicherheit" sowie "Server- und Applikationssicherheit". Weltweit erwirtschaftete Microsoft im Geschäftsjahr 2002 28,4 Mrd. US$. Microsoft Deutschland ist die größte europäische Auslandstochter der amerikanischen Microsoft Corp. Sie wurde 1983 gegründet und beschäftigt heute 1.300 Mitarbeiter.

Network Associates

Network Associates Inc. mit Firmenzentrale in Santa Clara, Kalifornien, ist ein führender Hersteller von Softwarelösungen im Bereich Netzwerksicherheit und –verfügbarkeit. Network Associates besteht aus drei Marken: McAfee Security (Virenschutzprodukte), Sniffer Technologies (Netzwerk- und Anwendungsmanagement), und Magic Solutions (Anbieter von Service Desk Lösungen). Entstanden ist das Unternehmen im Dezember 1997 aus der Fusion von Network General und der 1989 gegründeten McAfee Associates. Seitdem wurden insgesamt zehn Unternehmen akquiriert, deren Produkte und Entwicklungskompetenzen die Position von NAI im Markt weiter gestärkt haben. Die Produktlinien zur Datenverschlüsselung - PGP desktop und wireless – wurden im August 2002 an das neu gegründete Venture-Capital-Unternehmen PGP Corporation verkauft. Die bislang börsennotierte Tochtergesellschaft McAfee.com, ein Anbieter von Sicherheitslösungen für PCs von Heimanwendern, wurde Ende 2002 wieder in das Unternehmen Network Associates integriert. Weltweit beschäftigt Network Associates mehr als 3.800 Mitarbeiter in 65 Ländern, davon rund 150 in Deutschland. Im Geschäftsjahr 2002 erwirtschaftete das Unternehmen einen weltweiten Umsatz von 942 Mio. US$.

RSA Security

Mit mehr als 9.000 Kunden positioniert sich RSA Security als strategischer e-Security-Partner zahlreicher erfolgreicher Unternehmen weltweit. Mit einem breiten Produktangebot, das aus Authentifizierungs- und Web-Access-Management-Lösungen sowie Werkzeugen für Entwickler besteht, unterstützt RSA Security Unternehmen bei der Umsatzgenerierung, indem kritische Informationen gegen unerlaubten Zugriff und böswillige Absichten geschützt werden. Seine Position am Markt stützt sich unter anderem auf die langjährige Innovation und Führerschaft auf dem Gebiet der IT-Sicherheit und die intensiven Beziehungen mit mehr als 1.000 Technologie-Partnern. Das Angebot umfasst die Produktfamilien RSA SecurID Zwei-Faktor Authentifizierung, RSA BSAFE Datenverschlüsselung, RSA ClearTrust Web-Zugangsmanagement, RSA Keon Zertifikatsmanagement und RSA Mobile Zwei-Faktor Authentifizierung für drahtlose Kommunikation. RSA Security erwirtschaftete im Jahr 2002 einen Umsatz in Höhe von 232,1 Millionen US$.

Sun Microsystems

Seit seiner Gründung 1982 bildet Network Computing das Fundament der Unternehmensphilosophie von Sun, denn Ziel von Sun ist es, auf Standards basierende, offene, vernetzbare Computersysteme zu fertigen. „The Network Is The Computer", Suns seit langen Jahren propagiertes Motto, wird heute in der Industrie gelebt. In zahlreichen Anwendungsbereichen wie in der Elektronikentwicklung, der mechanischen Konstruktion, im Software Engineering, bei den Druck- und elektronischen Medien sowie im Telekommunikationsbereich und der Finanzwirtschaft ist Sun Technologie-Anbieter. IT-Security ist genereller Bestandteil der Produkte und Services von Sun Microsystems. Sun adressiert das Thema IT-Security zum einen über die Solaris-Basisfunktionalitäten und die erweiterten Security-Funktionalitäten von Solaris, z.B. das Solaris Security Toolkit. Mit der iForce Sicherheitslösung bietet Sun zusammen mit Partnern zudem eine umfangreich getestete Lösung mit sieben Sicherheits-komponenten. Weitere Bestandteile des Sicherheits-Portfolios sind die Sun ONE Network Identity Lösungen sowie Secure Web Server. Schließlich unterstützt Sun Professional Services den Kunden bei der Analyse der Sicherheitsumgebung, der Prozesse und der Technologien sowie bei der Implementierung umfassender Sicherheitslösungen. Sun Deutschland beschäftigt rund 1.500 Mitarbeiter. Im Geschäftsjahr 2002 erzielte die GmbH einen Umsatz von 862 Millionen EUR.

SurfControl

SurfControl gehört weltweit zu den führenden Internet Filtering Anbietern im Markt für IT-Sicherheit. Die Produktfamilie von SurfControl wendet Experten-Filterung, Pass-Through- und Pass-By-Technologien an, um eine produktive Internet-Umgebung am Arbeitsplatz zu schaffen und die Sicherheit für Kinder bei der Nutzung des Internets zu erhöhen, sei es zu Hause oder in der Schule. Nach seinem Börsengang am Alternative Investment Market (AIM) in London im Juni 1998 wurde SurfControl 1999 in den Nasdaq Europe aufgenommen. Seit Februar 2000 notiert SurfControl auch an der Londoner Börse. SurfControl ist weiterhin an beiden Märkten gelistet und ein „techMARK Constituent". SurfControl beschäftigt über 400 Mitarbeiter weltweit und verfügt über acht Nieder-lassungen. Im deutschsprachigen Raum ist das Unternehmen seit der Übernahme der öster-reichischen CSM Security Management AG im August 2000 vertreten, heute mit Niederlassungen in Wien und Frankfurt. Im Jahr 2002 wurde weltweit ein Umsatz von 54,2 Millionen US-Dollar erzielt.

Sybari Software

Sybari ist Anbieter hochwertiger Antiviren- und Sicherheitslösungen für Groupware. Sybari Software wurde 1995 mit der Zielsetzung gegründet, dringend notwendige und auf den Schutz von Microsoft Exchange und Lotus Domino Communities zugeschnittene Antiviren- und Sicherheitslösungen zu liefern. Heute nimmt Sybari mit über fünf Millionen sicheren und virenfreien Groupware-Arbeitsplätzen eine wichtige Stellung am Markt ein. Mit Sybari-Produkten können Unternehmen ihre ein- und ausgehenden Email-Nachrichten effektiver verwalten und potenziell bedrohliche Anhänge unschädlich machen. Die Produkte wie beispielsweise Antigen für Microsoft Exchange und Lotus Domino/Notes sind mit einer Scan-Technologie ausgestattet, mit der auf eingehende Email-Nachrichten und Daten zugegriffen wird und diese gescannt und verwaltet werden, bevor sie empfindliche Teile des

Groupware-Netzwerkes erreichen können. Der Hauptsitz von Sybari ist in East Northport (USA); die deutsche Niederlassung befindet sich in München. Im Jahr 2002 erzielte Sybari mit rund 200 Mitarbeitern einen weltweiten Umsatz von 34 Millionen US$.

Symantec

Symantec gehört zu den weltweit marktführenden Anbietern auf dem Gebiet der Internet-Sicherheit. Die umfangreiche Palette an Software- und Appliance-Lösungen umfasst Produkte in den Bereichen Content- und Netzwerk-Sicherheit für Privatanwender, Unternehmen und Internet-Dienstleister. Zu den Produkten gehören Client-, Gateway- und Serverlösungen für die Bereiche Virenschutz, Firewalls, Virtual Private Networks, Schwachstellen-Management, Intrusion Detection, Internet- und Email-Filter, Technologien für die Fernverwaltung sowie Sicherheitsdienstleistungen für Unternehmen und Internet-Dienstleister. Die Konsumentenmarke für Sicherheitsprodukte, Norton, nimmt weltweit eine marktführende Position im Einzelhandel ein und hat zahlreiche Auszeichnungen der Branche bekommen. Das Unternehmen ist in Cupertino, Kalifornien, beheimatet und vertreibt seine Produkte in 38 Ländern. Symantec beschäftigt insgesamt über 4.000 Mitarbeiter und erwirtschaftete im Geschäftsjahr 2002 einen Umsatz in Höhe von 1,071 Milliarden US-Dollar.

Trend Micro

Trend Micro Incorporated gehört zu den weltweit führenden Anbietern von Software und Services im Bereich Antiviren und Content Security. Als Spezialist für serverbasierten Virenschutz stellt Trend Micro leistungsfähige Antiviren-Produkte mit erweiterten administrativen Funktionen und hoher Skalierbarkeit bereit, die für den Einsatz in kleinen Betrieben und in Großunternehmen gleichermaßen geeignet sind. Das Angebot umfasst darüber hinaus Antiviren-Software für den privaten Endanwender. Trend Micro wurde 1988 von Steve Chang gegründet. Innerhalb von gut zehn Jahren hat sich Trend Micro, mit Hauptfirmensitz in Tokio, Japan, zu einem globalen Unternehmen entwickelt, mit über 1.600 Angestellten in 23 Ländern. Für das gesamte Jahr 2002 erzielte Trend Micro beim Nettoabsatz ein Ergebnis von 364 Mio. US-Dollar und eine Steigerungsrate von 37 Prozent gegenüber 2001. Die Firmenaktien werden an der Börse in Tokio gehandelt und sind im Nikkei225-Index notiert. Zusätzlich werden die American Depository Receipts der Firma an der Technologiebörse NASDAQ gehandelt. Sitz der deutschen Niederlassung Trend Micro Deutschland GmbH ist Unterschleißheim bei München. Trend Micro vertreibt seine Produkte über autorisierte Systemhäuser und Distributoren.

webwasher AG

Die webwasher AG zählt zu den führenden Anbietern von Internet Content Security Software für Unternehmen und Behörden. Auf der Basis selbst entwickelter Technologien sowie durch Kooperationen mit führenden Technologiepartnern entwickelt und vermarktet das Unternehmen innovative Produkte für den wachsenden Markt des Content Security Management. Mittels Internet Access Management, Internet Content Filtering, E-Mail- und Spam-Filterung, Virenschutz und Reporting können Unternehmen ihre Internet-Nutzung optimieren und sich wirksam und effizient vor Gefährdungen und Belästigungen aus dem Internet schützen. Die server-basierten WebWasher-Lösungen sind weltweit bei über 4.000 Unternehmen im Einsatz – darunter in Europa die

HypoVereinsbank, UBS und Wincor Nixdorf, in den USA 17 Unternehmen der Fortune 500. Die webwasher AG unterhält strategische Partnerschaften mit Network Appliance, Check Point, Computer Associates und Network Associates. Derzeit beschäftigt die webwasher AG 100 Mitarbeiter in Deutschland und den USA sowie in weiteren europäischen Ländern.

8.2.2 Trends weltweit / Deutschland

Im Folgenden werden die Trends in einzelnen Lösungsbereichen skizziert.

Virenschutz

Der weltweite Markt für Virenschutz-Produkte wird künftig um 10 bis 20 Prozent jährlich wachsen. Anbieter mit soliden Lösungen in den führenden Wachstumsbereichen – Storage-Area Networking (SAN), Linux, Email und Web Gateways – werden zunehmend erfolgreich sein. Kurzfristig (2003-05) müssen die Anbieter die zentralen Management-Werkzeuge für die Implementierung, Policy Compliance und Notfall-Management weiter verbessern.

Die Attraktivität von Virenschutz-Suites gegenüber Punktlösungen wird proportional zur Vollständigkeit der Management-Tools zunehmen. Dennoch werden sich risiko-averse Unternehmen (20 bis 30 Prozent der G2000) aufgrund des technologischen Vorsprungs auch in Zukunft für multiple Scan-Engines entscheiden. Anwender müssen die Vorteile des Managements und die geringeren Kosten von AV-Suites gegenüber der zusätzlichen Sicherheit bei multiplen Scan-Engines abwägen. Anbieter stehen außerdem vor der Herausforderung, die Transparenz und Performance von Scan-Engines zu erhöhen – vor allem im Web-Gateway- und SAN-Markt sowie bei Highend-Server-Plattformen. Im Email-Gateway-Markt werden die Anbieter zusätzliche Werkzeuge für Email-Sicherheit und Produktivität integrieren.

Die META Group erwartet, dass bis Ende 2004 die führenden Virenschutz-Anbieter durch Akquisition oder Integration umfassende Antispam-Software offerieren werden. Langfristig (2006/07) werden die Anbieter vor der Aufgabe stehen, die richtige Mischung aus eigenen Komponenten und der Integration mit Best-of-Breed-Tools für IT-Sicherheit zu finden. Erfolgreiche Anbieter werden andere Formen von Content Management (z.B. SPAM-Schutz und Filterung von URLs und mobilem Code) am Gateway aufgreifen, außerdem auch integrierte Personal Firewalls und persönliche Intrusion Detection am Client. Ziel ist es, eine höherwertige Lösung zu günstigeren Kosten anzubieten. Die Best-of-Breed-Integration wird jedoch erfolgreicher mit Unternehmens-Firewalls, Intrusion Detection Systemen und Sicherheitsmanagement-Werkzeugen vonstatten gehen.

Die weltweit führenden Anbieter im Markt für Virenschutz-Lösungen sind Trend Micro, Symantec und Network Associates/McAfee. Die „Herausforderer“ Computer Associates (CA) und Sophos sind den Marktführern dicht auf den Fersen.

- **Content Security:** Die Implementierung von Content Security Lösungen, die den Verkehr in den Bereichen Web/Email/Sprache/Instant Messaging nach Viren, mobilem Code und unerwünschter Nutzung filtern, wird weltweit durch rechtliche Bedenken und die Sorge um Verluste und Schäden

vorangetrieben (2003/05). Die Effektivität wird jedoch durch die Diversifikation der Client-Plattformen und Kommunikationskanäle behindert, trotz allmählicher Verbesserungen der Detection-Genauigkeit (2004-07). Zukünftige Schwerpunkte umfassen die Bereitstellung von Management-Funktionalitäten auf Unternehmensebene und umfassende Suites (das heißt für alle Formen von Inhalten und Kanälen: 2004-06).

- Im **Web-Filtering-Markt in Deutschland** steckt derzeit viel Dynamik. Die META Group geht davon aus, dass dieses Segment in Deutschland zwischen 2002 und 2004 mit durchschnittlich über 25 Prozent pro Jahr wachsen wird - allerdings mit einem vergleichsweise geringen Marktvolumen in Höhe von rund 20 Millionen Euro im Jahr 2003. Die primäre Zielsetzung der deutschen Unternehmen beim Einsatz von Web-Filtering-Lösungen ist der Schutz der Netzwerkinfrastruktur vor Virenattacken. Rechtliche Aspekte, etwa im Zusammenhang mit der Verbreitung illegaler oder "politisch unkorrekter" Inhalte, spielen eine kleinere Rolle. Auch die Erhöhung der Mitarbeiterproduktivität und der Netzwerkbandbreite durch die Kontrolle der Internet-Nutzung stehen nicht im Vordergrund der Zielsetzungen. Damit treffen die Marketingbotschaften und Kaufargumente der führenden Anbieter zu einem gewissen Teil ins Leere. Es sind noch große Anstrengungen notwendig, um die deutschen Unternehmen für das Thema zu sensibilisieren und sich gleichzeitig gegenüber klassischen Anbietern von Virenschutz-Lösungen zu differenzieren. **Führender Anbieter nach Umsatz in Deutschland ist webwasher, gefolgt von SurfControl, Websense, Secure Computing und Symantec. Weitere Anbieter sind die primär international aktiven Unternehmen Elron Software und N2H2 sowie diverse Email-Filtering-Anbieter, die zunehmend auch das Thema Web-Filtering adressieren.**

Firewalls

Firewalls werden künftig weitere Funktionalitäten aufnehmen (z.B. höhere Intrusion Awareness, dynamische Policy-Definition und –Umsetzung: 2004/05), da sie um anwendungsspezifische Security-Gateways erweitert werden (für Web und Email: 2003; für konvergierte Sprache/Daten, Web Services: 2004/05). Persönliche und „Node“-Abwehrsysteme (z.B. Firewall + Virenschutz + Policy Enforcement), die ursprünglich auf die Absicherung von Remote-Nutzern ausgerichtet waren (2003/04), werden zusammen mit Security Services vorangetrieben, die in die Infrastruktur eingebettet sind und die vielfach vernachlässigte „interne“ Bedrohung adressieren (2004-07).

Identity Management

Identity Management und Sicherheitsbedürfnisse werden bis 2004 eine Zunahme des Einsatzes von Verzeichnisdiensten (Directory Services) im Unternehmen bewirken, wobei bestehende gebündelte Directories die Nutzung von Werkzeugen für das Provisioning und die Directory-Integration vorantreiben werden. Die Grenzen zwischen Unternehmens- und Extranet-Verzeichnisdiensten werden bis 2005 und darüber hinaus verschwimmen, da interne und externe Identities zusammenzufügen sind. Die Nutzung von Directories für manche Autorisierungsrollen bei Anwendungen wird aufgrund der erweiterten Funktionalität von Directories zunehmen. XML wird für

Komponenten-Datenbanken (als Directory der nächsten Generation) und bessere Integrationsfähigkeit sorgen (2006-08).

Identity Management und Sicherheitsanforderungen werden bis 2006 in beschränktem Ausmaß zu umfassenden SSO-Realisierungen (Legacy + Web) führen. Wirkliche Fortschritte bei der Implementierung von ganzheitlichen SSO-Services werden erst dann gemacht werden, wenn sich ein Standard-Ansatz für multiple Anwendungs- und Plattform-Umgebungen entwickelt. Es ist unwahrscheinlich, dass dieser Fall vor der verbreiteten Nutzung von Web-Services-Sicherheitsstandards (z.B. SAML, XACML) bei der Bereitstellung von Anwendungs- und Infrastrukturdiensten (2006+) eintritt. Pragmatische Fortschritte können mittelfristig nur über die Reduzierung der benötigten Anzahl an Authentifizierungsumgebungen erzielt werden.

Secure Access und Authentifizierung

Der Bedarf an sicherem Zugriff und Identifikation wird bis 2006 die Implementierung von stärkerer Authentifizierung mittels Tokens (Mainstream), Smart Cards (zunehmender Einsatz) und Biometrie (Nischenmarkt) vorantreiben. Der Bedarf an externalisierter Anwendungs-Authentifizierung wird für verbesserte Verzeichnisfunktionalitäten sorgen, während die Anforderungen aus drahtlosen und mobilen Systemen die standardisierte (z.B. 802.1x) verteilte Netzwerk-Authentifizierung vorantreiben (2004/05) und dabei schließlich interne Bedrohungen adressieren werden.

Privacy und Verschlüsselung

Die Regelungen für Vertraulichkeit (Privacy) werden weiterhin bis 2004/05 besonderes Augenmerk auf die Verschlüsselung von Informationen auf der Daten-, Datei-, Datenbank- und Transportebene legen (für transaktionsorientierte und kollaborative Anwendungen, „wireline“ und „wireless“). Ab 2005/06 werden die Reife und die Transparenz von PKI-Komponenten (das heißt eingebettet im NOS, in Directories und File-Systeme) den verbreiteten Einsatz von Verschlüsselung beschleunigen. Bis 2007 werden PKI-basierte Sicherheitsfunktionen (z.B. Verschlüsselung, digitale Signaturen) bereits während des Entwicklungsprozesses direkt in die Anwendungen integriert. Dabei wird unter anderem Microsoft eine wichtige Rolle als Anbieter spielen.

Security Management

Security Management wird sich in drei funktionellen Bereichen entwickeln: Nutzer-, Event- und Konfigurations-Management. Die Aggregation des Nutzermanagements (Identity Management, Provisioning) wird schnell heranreifen (2004). Management-Konsolen für Security-Events, die Ereignisse aus Intrusion Detection Systemen, Firewalls und Hosts sammeln, werden bis 2005 außerhalb des Mainstreams bleiben. Security-Konfigurations-Konsolen (zentrale Verteilpunkte für Firewall, Personal Firewall und schließlich Server-Konfiguration/Policies) sind am unreifsten. Ausgereifte und integrierte Produkte werden erst 2006/07 am Markt erscheinen.

Threat und Vulnerability Management

Die Integration von Threat und Vulnerability Management, also dem Management von Bedrohungen und Schwachstellen, wird sich beschleunigen. Dabei wird Intrusion Detection (unter dem Begriff „Intrusion Prevention“) immer mehr Informationen über Schwachstellen und Assets erfassen. Obgleich die automatisierte Beantwortung von Alarmen allgemein verfügbar sein wird, werden die Unternehmen bis 2005/06 nur begrenzten Gebrauch davon machen. Auch verschiedene Formen von Managed Services (z.B. Alarmierung über Schwachstellen, Intrusion Detection Systeme) werden zunehmend nachgefragt. Dennoch wird bis zum Jahr 2007 die Reife vieler Disziplinen in diesem Bereich trotz der Konsolidierung des Anbietermarktes zu wünschen übrig lassen.

8.3 Entwicklungen bei Anbietern von Security-Services

8.3.1 Anbieterlandschaft

IT-Security ist heute nicht mehr eine reine Domäne großer oder spezialisierter IT-Dienstleister, sondern wird aus vielen Service-Segmenten heraus als „Querschnittsthema“ oder „Enabler“ adressiert. Einen Überblick über die Anbieterlandschaft zeigt die folgende Grafik.

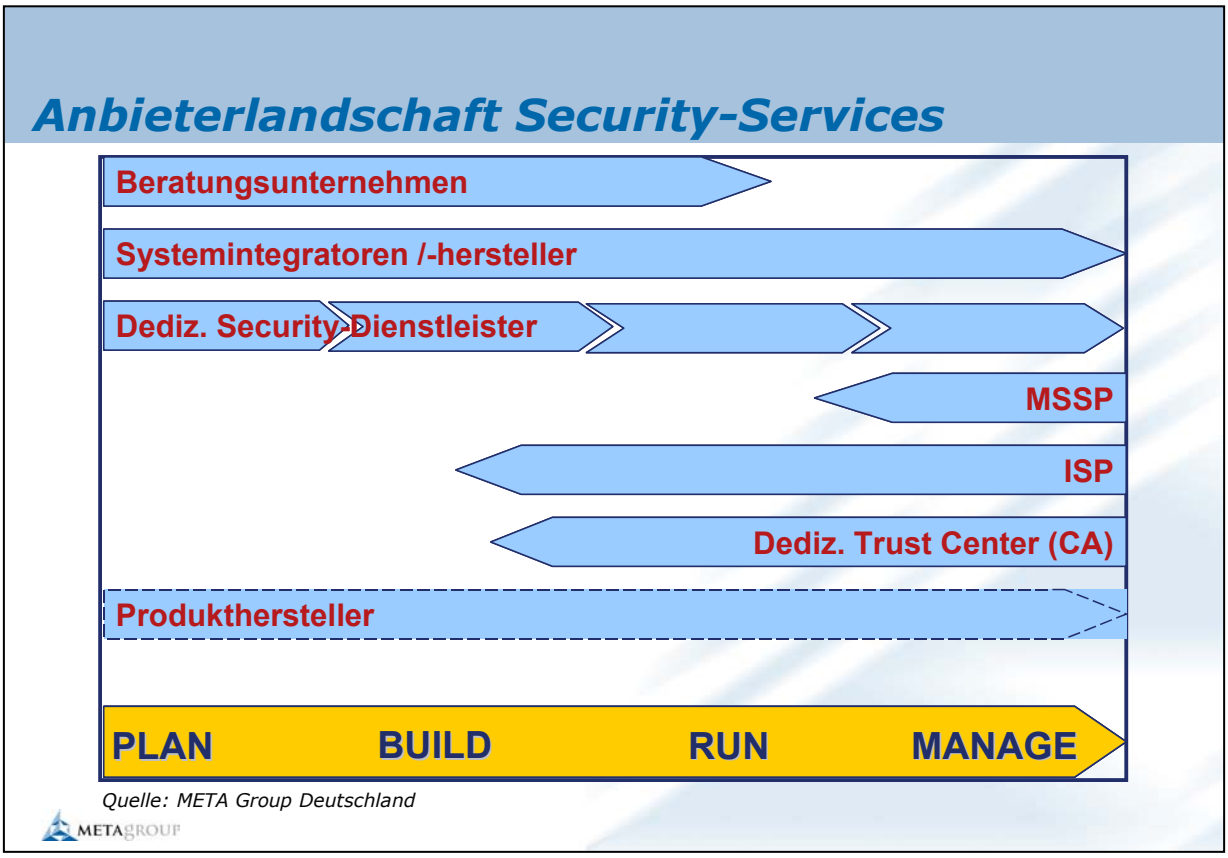


Abbildung 128: Anbieterlandschaft Security Services

Entwicklung in den einzelnen Kategorien:

- **Beratungsunternehmen:** Accenture, Bearing Point (ehemals KPMG), Deloitte Consulting, Ernst & Young IT-Security, Mummert Consulting, Plaut etc. Die Leistungen konzentrieren sich vorwiegend, aber nicht ausschließlich auf den „Plan"-Bereich, unter anderem auf Security-Strategie, -Organisation und –Prozesse sowie Audit, Risk Assessment und Produktevaluierung. Ursprünglich auf Consulting ausgerichtet, adressieren einzelne Beratungsunternehmen heute auch zunehmend die Implementierung und den Betrieb von Lösungen.
- **Systemintegratoren** (auch Netzwerke) und Service-Bereiche der Systemhersteller: Atos-Origin, circular, Controlware, CSC, Dimension Data, EDS, CC CompuNet, Getronics, HP, IBM Global Services (einschließlich der Beratungssparte BSS), INFO AG, infodas, LogicaCMG, Lufthansa Systems, net Stemmer, NK Networks & Services, ORGA, PanDacom, SAP SI, SerCon, Siemens Business Services, Softlab, Sun Microsystems, Syskoplan, TDS, ThyssenKrupp IS/Triaton, T-Systems (ITC Security), taskarena, Unisys etc. Manche der Systemintegratoren bieten das komplette Portfolio aus einer Hand, andere wiederum konzentrieren sich auf bestimmte Delivery Modes im Zyklus PLAN-BUILD-RUN. Vor allem bei Integratoren im Netzwerkbereich sind immer häufiger Managed Security Services Bestandteil des Angebots.
- **Dedizierte Security-Dienstleister**: cirosec, Integralis, Secorvo, secunet, TÜV Secure iT etc. Dienstleister dieser Kategorie konzentrieren sich meistens auf bestimmte Themen oder Phasen im PLAN-BUILD-RUN-Zyklus und positionieren sich dort als Spezialisten. Als dedizierte Security-Dienstleister können des Weiteren auch „semi-unabhängige" Einheiten größerer Dienstleister und Konzerne aufgefasst werden, so etwa T-Systems mit dem Geschäftsbereich ITC-Security oder Giesecke&Devrient mit der Tochter Secartis.
- **Managed Security Service Provider:** Hierbei handelt es sich eigentlich in erster Linie um eine Service-Kategorie, die sich in einem frühen Stadium befindet. Zu den dedizierten MSSPs gehören weltweit ISS, Counterpane, Riptech und Ubizen und in Deutschland unter anderem die Integralis-Tochter Activis sowie die SHE IT AG. Managed Security Services werden aber auch von anderen Dienstleistern angeboten, insbesondere von ISPs und Systemintegratoren. Auch Anbieter von Sicherheitsprodukten beginnen teilweise, ihre Lösung in Form eines MSS zu offerieren. Bei Managed Security Services handelt es sich allerdings derzeit noch um einen kleinen Markt, in dem sich viele Anbieter tummeln. Es ist von einer Konsolidierung des Marktes auszugehen.
- **Internet Service Provider (ISPs)** und Carrier: Arcor, Equant, infonet, PSInet etc. Der Schwerpunkt dieser Unternehmen liegt auf Security im Betrieb und Management der IT-Infrastrukturen (vor allem Netzwerke: VPN, Firewalls, IDS). Die konkrete Implementierung erfolgt gegebenenfalls in Zusammenarbeit mit IT-Dienstleistern.
- **Dedizierte Trust Center:** AuthentiDate International, Datev, D-Trust, TC Trust Center, T-Telesec, SchlumbergerSema CCI, S-Trust etc. Diese Anbieter übernehmen für den Kunden den Betrieb von Trust Centern beziehungsweise einzelne Funktionen wie die Ausgabe von digitalen

Zertifikaten, Registrierung neuer Nutzer oder Verzeichnisdienste. Dies ist auch mit einem gewissen Anteil an Beratungs- und Implementierungsleistungen verbunden. Außerdem werden Komplettsysteme wie Chipkarten und Lesegeräte angeboten. Der Betrieb von Trust Centern wird auch oftmals von den klassischen IT-Dienstleistern übernommen. Dies geschieht aber eher im Kontext von einzelnen Projekten. Um kommerzielle Trust Center ist es seit dem Ende des PKI-„Hypes“ und dem Rückzug der Deutsche Post Signtrust 2002 stiller geworden. Die Zukunft der Trust Center wird maßgeblich davon abhängen, ob es ihnen gelingt, eine kritische Größe zu erreichen und sich in erfolgsversprechenden Marktnischen oder Branchen zu positionieren.

- **Security-Produktanbieter** lassen in der Regel einen Großteil der Services (Beratung, Implementierung, Betrieb) durch Partner erbringen. Dennoch liegt der Dienstleistungsanteil am Gesamtumsatz bei Produktanbietern in der Regel zwischen 10 und 40 Prozent – je nach Lösungskategorie. Schwerpunkte neben dem sehr wichtigen Support und der Wartung sind typischerweise produktorientierte Beratungs- und Trainingsleistungen. Einige Produkthersteller haben außerdem begonnen, Managed Security Services auf Basis ihrer Lösungen anzubieten.

Im Folgenden sind Kurzprofile ausgewählter Anbieter von IT-Sicherheits-Dienstleistungen aufgeführt.

Arcor

Die Arcor AG & Co. positioniert sich als Komplettanbieter für Geschäftskunden vom Mittelstand aufwärts und viel telefonierende Privatkunden. Mit seinem eigenen, bundesweit flächendeckenden Sprach- und Datennetz von über 50.000 Kilometern Länge bietet Arcor seinen Kunden das volle Spektrum an Sprach-, Daten- und Mehrwertdiensten sowie Internet-, Multimedia-Services und e-Business-Lösungen. Im Bereich der IT-Sicherheit bietet Arcor eine Reihe von Dienstleistungen für Geschäftskunden, die insbesondere die Themen VPN und Managed Firewall abdecken. Die Dienstleistungen im VPN-Umfeld sind im Bereich „Datendienste“ angesiedelt und umfassen sowohl ATM- (Arcor – ATM) und Frame Relay- (Arcor – Frame Relay) als auch IP-basierte VPN-Lösungen (Arcor – Company Net). Die Arcor-Managed Firewall bietet Sicherheitsmanagement für Firmennetze mit permanentem Monitoring und laufender Softwareaktualisierung. Zu den Unternehmen der Arcor-Gruppe gehören neben der Arcor AG & Co. die Arcor Online GmbH, die Arcor Kundenservice GmbH, die ISIS Multimedia Net GmbH & Co. KG und die Netcom Kassel Gesellschaft für Telekommunikation mbH. Im Jahr 2000 erwirtschaftete die Gruppe einen Umsatz von ca. 1,6 Milliarden Euro.

Controlware

Als deutscher Systemintegrator bietet die Controlware GmbH seit der Gründung im Jahr 1980 komplette Dienstleistungen rund um das Netzwerk an. Das Portfolio reicht dabei von Beratung und Planung über Installation und Wartung bis hin zum Betrieb von Netzwerken über das firmeneigene Network Control Center. Im Mittelpunkt stehen "Kommunikationslösungen", "Informationssicherheit", "IT-Management-Lösungen" sowie "Storage Networking". Darüber hinaus hat sich Controlware weltweit einen Namen als Hersteller von ISDN-, Videoüberwachungs-, Multimedia- und Fiber Optic-

Produkten gemacht. Mehr als 800 Mitarbeiter an zehn Standorten in Deutschland und in zwölf Niederlassungen auf allen fünf Kontinenten sichern ein flächendeckendes Vertriebs- und Service-Netz, das durch zahlreiche Distributoren in aller Welt komplettiert wird. Im Jahr 2001 betrug der Umsatz der Controlware GmbH 105 Millionen EUR. Weitere Aktivitäten entfaltet Controlware in vier Tochtergesellschaften und mehreren Beteiligungen, unter anderem in einem Joint Venture mit dem größten Internet-Service-Provider der Ukraine, Infocom. Es bestehen langfristige Partnerschaften mit führenden IT-Herstellern wie Brocade, Check Point, Cisco, ISS, Marconi, Micromuse, Nokia, Nortel Networks u.a.

Dimension Data

Dimension Data Germany AG & Co. ist einer der führenden Netzwerkintegratoren für LAN und WAN, Corporate Networks, Citynetze, Intranet/Internet und Telekommunikation sowie Dienstleister für Multi-Channel e-Commerce-Lösungen. Eine Kernkompetenz des Unternehmens liegt im Aufbau von IP basierten, konvergenten Netzen sowie im Netzwerkmanagement und in der Netzwerksicherheit. Mit umfassenden Dienstleistungen und Services in den Bereichen Content Delivery Networks, Multiservice Networks, Interactive Solutions mit Customer Contact Center-Lösungen, integrierte BSS/OSS Service Provider-Lösungen sowie Managed Services z.B. im Security-Bereich unterstützt Dimension Data ihre Kunden mit e-Commerce-Infrastrukturen für zuverlässige und kalkulierbare Business-Services. Komplette Dienstleistungen rund um Netzwerk-Lösungen fasst Dimension Data in den Service-Paketen PRIMER, UPTIME, INSITE, SURVEYOR und OPTIMISER zusammen und sichert so die Verfügbarkeit von e-Business Lösungen. Weltweit ist die Dimension Data Gruppe mit rund 11.000 Mitarbeitern in über 30 Ländern vertreten. 2001 wurde eine Umsatzgröße von rund 2,5 Milliarden US-Dollar erreicht; der Konzern ist an der Johannesburger Börse und seit Juli 2000 an der Londoner Börse notiert. Darüber hinaus ist Dimension Data Global Cisco Gold Partner auf fünf Kontinenten und Global Support Partner von Cisco.

Equant

Equant gehört zur Gruppe der führenden Dienstleister in der weltweiten IP- und Datenkommunikation. Equant bietet multinationalen Unternehmen Netzwerk-, Integrations- und Applikationsdienstleistungen. Durch die Integration in die France Telecom Gruppe im Jahr 2001 kann Equant nunmehr auch integrierte Sprach-Daten-Lösungen anbieten. Sein Datennetzwerk verbindet heute wichtige Geschäftszentren in 220 Ländern und Regionen. Das Unternehmen bietet außerdem lokalen Support in 191 Ländern. Die Anforderungen internationaler Konzerne werden mit einem umfassenden Angebot an Managed Data Network Services bedient. Dazu gehört auch die Equant IP-VPN-Lösung, die heute von über 550 Equant-Kunden eingesetzt wird. Die Security-Services umfassen das Equant Secure Gateway mit gemanagten Firewall-, Anti-Virus-, Internet Accelerator-Lösungen und der Erkennung aller Angriffe auf das Netzwerk. Equant Secure Authentication Services bieten gemanagte Authentifizierung, digitale Signatur durch eine geprüfte Zertifizierungsstelle und die Integration dieser Security Services in die Netzinfrastruktur. Neben den gemanagten Lösungen bietet Equant begleitendes Security Consulting an. Equant erzielte im Jahr 2001 einen Pro-Forma-Umsatz von 3,1

Milliarden US-Dollar. Das Unternehmen beschäftigt weltweit mehr als 10.000 Mitarbeiter, davon über 500 in Deutschland.

Lufthansa Systems Group

Die Lufthansa Systems Group GmbH bildet das Geschäftsfeld IT Services des Lufthansa-Konzerns und wurde zum 01.01.2001 als Management-Holding gegründet. Mit rund 4.200 Mitarbeitern, mehreren Standorten in Deutschland und Auslandsniederlassungen in 13 Ländern ist das Unternehmen einer der führenden Aviation IT-Provider weltweit. Als Systemintegrator für den Airline- und Aviation-Markt deckt Lufthansa Systems das gesamte Spektrum an IT-Leistungen ab - von der Beratung über die Applikationsentwicklung und -implementierung bis hin zum zuverlässigen Betrieb. Darüber hinaus bietet das IT-Unternehmen seine Leistungen im Bereich IT-Infrastruktur und Betrieb branchenübergreifend an. Im Geschäftsjahr 2002 erwirtschaftete das Unternehmen einen Umsatz von 557,4 Millionen EUR. Das Thema IT-Sicherheit wird bei Lufthansa Systems in mehreren Geschäftssegmenten abgedeckt. Hierzu gehören unter anderem das Geschäftsfeld Web & Security Solutions sowie das Active Security Angebot. Active Security bietet weitreichende Consulting-Leistungen im Bereich Sicherheitsberatung und Systemlösung an. Wichtigste Aufgabe ist dabei der Schutz aller unternehmenskritischen Geschäftsprozesse durch eine intelligente und effiziente Sicherheitsarchitektur, bei der sich die einzelnen Systemkomponenten optimal ergänzen.

ORGA

Die ORGA GmbH mit Hauptsitz in Karlsruhe wurde 1970 als IT-Dienstleister für Lohn- und Gehaltsabrechnungen gegründet und hat seitdem ihr Produkt- und Dienstleistungsportfolio kontinuierlich erweitert. Bereits im Jahr 1979 wurde mit der strategischen Entscheidung, einen Schwerpunkt auf das Anbieten von Services im Umfeld von SAP-Standardlösungen zu setzen, der Grundstein gelegt, um sich im weiteren Verlauf bis heute zu einem Systemhaus für SAP R/3 (seit 1995 autorisiertes SAP-Systemhaus) weiterzuentwickeln. Die Hauptgeschäftsfelder der ORGA GmbH sind heute Beratung, das SAP-Systemhaus, das Outsourcing/ Application Service Provisioning, die Branchenlösungen sowie die Archivierung und das Dokumentenmanagement. Seit 1978 bietet ORGA im eigenen Hochverfügbarkeits-Rechenzentrum Hosting-Services für SAP an. Außerdem liegt ein Schwerpunkt des Unternehmens auf der Applikationssicherheit im SAP-Umfeld. Hier besteht unter anderem eine Technologiepartnerschaft mit der SECUDE Sicherheitstechnologie Informationssysteme GmbH. Die ORGA GmbH ist ein 100-prozentiges Tochterunternehmen der FIDUCIA AG, eines Rechenzentrums-Dienstleisters mit Fokus auf den Bankensektor, und beschäftigt heute ca. 200 Mitarbeiterinnen und Mitarbeiter. Im Geschäftsjahr 2001 erzielte die ORGA GmbH einen Umsatz von 36 Mio. EUR und ist neben ihrer Zentrale in Karlsruhe auch mit Geschäftsstellen in Berlin, Köln und Stuttgart in der Bundesrepublik Deutschland vertreten.

Siemens Business Services

Die Siemens Business Services GmbH & Co OHG (SBS) bietet Komplettlösungen und Dienstleistungen entlang der gesamten Wertschöpfungskette Consult - Design - Build - Operate - Maintain an. Im Bereich der IT-Sicherheit unterstützt Siemens Business Services Unternehmen bei

der Planung von individuell auf ihre Erfordernisse zugeschnittenen Lösungen, integriert sie in ein Gesamtkonzept und übernimmt auf Wunsch den Betrieb der Sicherheitsinfrastruktur. Durch Security Consulting und Management wird das Thema IT-Security auf Basis von Business-Security-Szenarien aus verschiedenen Perspektiven analysiert. Der integrierte Beratungsansatz reicht von der Sicherheitspolitik, über Risikoanalyse und -management von Geschäftsprozessen bis zum Design einer unternehmensweit standardisierten Sicherheits-Architektur. Neben der Beratung übernimmt Siemens Business Services auch den Aufbau der Sicherheitsinfrastruktur. Darüber hinaus bietet Siemens Business Services alle Komponenten für das Management moderner Informations- und Kommunikationsnetzwerke aus einer Hand: von der Bereitstellung und dem Betrieb des Netzes, über die benötigte Hard- und Software bis hin zu Telekommunikations-Services. Lösungen und Dienstleistungen für die Workplace Security runden das Angebot ab. SBS war im Geschäftsjahr 2002 mit rund 33.600 Mitarbeitern in 44 Ländern vertreten. Im letzten Geschäftsjahr erzielte SBS einen Umsatz von etwa 5,8 Milliarden EUR.

SerCon

SerCon, gegründet 1992, ist eine hundertprozentige Tochter der IBM Deutschland GmbH. SerCon positioniert sich als Beratungsgesellschaft für Informationssysteme, die als Komplettlösungsanbieter operiert und dabei die gesamte Leistungsbandbreite von der Beratung über die Konzeption bis zur Realisierung abdeckt. Das SerCon-Angebot ruht auf zwei Säulen. Das Consulting umfasst Strategie-, Organisations- und Potenzialberatung sowie Sicherheitsmanagement. Der Bereich Service konzentriert sich auf Integrationsdienstleistungen für Themen wie Buy&Supply, ERP, Sell&Support, e-Business Integration und e-Business Enabling. Hier ist auch die Geschäftseinheit Security & Privacy angesiedelt. Das Dienstleistungsportfolio von SerCon im Bereich IT-Security orientiert sich an Grundsätzen der Effektivität und Effizienz der Informationsverarbeitung, Vertraulichkeit und Integrität von Informationen sowie an der Verfügbarkeit von Ressourcen. Außerdem werden rechtliche Rahmenbedingen mit einbezogen, zum Beispiel KonTraG, BDSG, oder IuKDG. Das Angebot orientiert sich am Lebenszyklus des IT-Risikomanagement-Prozesses und umfasst unter anderem auch IT-Risikomanagement, Security Auditing und unternehmensweite Public-Key-Infrastrukturen. SerCon ist an 25 Standorten und mit rund 1.000 Mitarbeitern in ganz Deutschland vertreten.

SHE Informationstechnologie

Die SHE Informationstechnologie AG wurde 1987 in Ludwigshafen gegründet. Sie beschäftigt derzeit ca. 140 MitarbeiterInnen und hat ihren Firmensitz in der Rhein-Neckar-Main-Region. Mit bundesweiten Projekten, internationalen Kunden und Partnerschaften agiert die SHE IT AG inzwischen europaweit agiert als Komplettanbieter im e-Business Markt. Das Leistungsspektrum reicht vom Consulting über die Integration und den Betrieb kundenspezifischer Systeme in den Bereichen eSecurity, Information Management, Portal Solutions, Middleware, Process-IT und Research & Development. Vor allem durch die Operations Center (AOC, SOC,NOC), die 365 Tage im Jahr, 24 Stunden rund um die Uhr mit speziell geschultem Sicherheitspersonal besetzt sind, positioniert sich die SHE IT AG als Anbieter, der seinen Kunden komplexe e-Business Applikationen in Verbindung mit sehr hohen Sicherheits-

standards bieten kann. Wichtiges Element des Security-Portfolios ist in diesem Zusammenhang der Internet-Sicherheitsdienst MANAGED SECURITY MONITORING SERVICE. Zum Kundenkreis von SHE zählen Unternehmen wie BASF, ABB, Aral, Deutsche Bank, Rolls-Royce, Lufthansa Systems, Knoll, L'Oréal, Roche Diagnostics sowie die Städte Ludwigshafen, Mannheim und Heidelberg.

T-Systems International

T-Systems International GmbH ist eine Konzerndivision der Deutschen Telekom und bietet Unternehmen und Behörden in über 20 Ländern klassische IT- und TK-Leistungen aus einer Hand sowie integrierte Lösungen aus dem Konvergenzbereich beider Märkte. Die Telekom-Division bündelt das Know-how von rund 43.500 Mitarbeitern. Im Geschäftsjahr 2001 erzielte das Unternehmen einen Umsatz von rund 11,9 Milliarden EUR (restated). Kompetenz und technologisches Know-how beim Thema Security hat T-Systems in der Business Unit "Information Technology & Communication Security" (ITC Security) gebündelt. Diese entstand aus der Verschmelzung der T-Systems ISS GmbH (ehemals debis Systemhaus ISS GmbH), des Bereichs ES2 des Technologiezentrums der T-Systems Nova GmbH und des Geschäftsbereichs T-Telesec der Deutschen Telekom AG. T-Systems bietet für „Corporate, e-Business und Communication Security“ ein komplettes Leistungspaket an, von der Beratung über Konzepte bis hin zur Umsetzung. Hierzu gehören vorgefertigte Lösungen, beispielsweise für Firewall, VPN, Intrusion Detection, PKI und Virenschutz sowie Smart Card Lösungen und Trust Center Dienste. Darüber hinaus werden Integrationsleistungen für komplexere Lösungen erbracht. Das Angebotsportfolio von T-Systems umfasst im Bereich ITC Security ferner umfassende Beratungs- und Entwicklungsleistungen für verschiedenste Technologien und Anwendungsfelder (Security Engineering). Evaluierungen und sonstige Gutachten runden das Leistungsspektrum ab.

TÜV Secure iT

Die TÜV Secure iT GmbH erbringt Services in den Bereichen der technischen und organisatorischen IT-Sicherheit sowie für IT-Prozesse und –Usability. Als neutraler Dienstleister begleitet das Unternehmen den Kunden während des gesamten Verbesserungsprozesses – von der Identifizierung der IT-Herausforderungen und Risiken über die Optimierung bin hin zur Implementierung der richtigen Lösungen und deren Zertifizierung durch den TÜV. Die TÜV Secure iT GmbH, eine Tochtergesellschaft des TÜV Rheinland Berlin Brandenburg, entwickelt und nutzt international standardisierte Verfahren und Methoden. Das Unternehmen wurde 1999 gegründet und hat seinen Hauptsitz in Köln. Die TÜV Secure iT GmbH konzentriert sich auf Großunternehmen in den Branchen Finanzdienstleistungen, Automotive, Handel, Chemie/Pharma und Energie sowie dem „TIMES“-Segment. Die internationale Präsenz ist über die Muttergesellschaft gewährleistet: Der TÜV RBB ist weltweit an 200 Standorten in 50 Ländern vertreten. Mit knapp 7.500 Mitarbeitern weltweit erwirtschaftete der TÜV RBB 2002 einen Umsatz von 657 Millionen EUR. Nach Schätzungen der META Group entfallen etwa 10 Millionen EUR auf die TÜV Secure iT.

8.3.2 Trends in Deutschland

IT-Sicherheit ist mittlerweile nicht mehr eine reine Domäne spezialisierter oder großer IT-Dienstleister. Viele Dienstleister im IT-Umfeld – darunter auch kleinere Systemhäuser – adressieren heute dieses Thema in mehr oder weniger großem Umfang. Wer beim Kunden letztendlich „zum Zug“ kommt, hängt von verschiedenen Faktoren ab. Grundsätzlich wird vom Dienstleister technologisches Spezialisten-Know-how und eine hohe Service-Qualität erwartet. Zudem sind Herstellerneutralität und die Betreuung über den gesamten Service-Zyklus („PLAN-BUILD-RUN“) sowie insbesondere ein gutes Image als vertrauenswürdiger Anbieter gefragt. Nach Einschätzung der META Group spielt der Vertrauensaspekt eine Schlüsselrolle. Ein solches Image kann durch ein ausgeprägtes Branding am Markt oder durch bestehende Geschäftsbeziehungen transportiert werden. Damit kann je nach Projektanforderung auch ein kleinerer, nicht auf IT-Sicherheit spezialisierter Dienstleister zum Einsatz kommen. Dedizierte Security-Dienstleister greifen oftmals auf ihr Spezialisten-Image zurück und nutzen dies, um auch bei potenziellen Neukunden schneller auf der „Short List“ zu landen. Die großen IT-Dienstleister beziehungsweise Systemintegratoren profitieren in diesem Zusammenhang doppelt: Sie verkaufen Sicherheitsdienstleistungen in eine große bestehende Kundenbasis und haben in der Regel ein ausgeprägtes Branding.

Erklärungsbedürftig ist die Bedeutung der Herstellerneutralität. Diese ist insbesondere in frühen Phasen des Entscheidungsprozesses beim Anwenderunternehmen relevant. Ist aber die Produktauswahl einmal vollzogen, liegt das Augenmerk vor allem auf einer sauberen Implementierung und Integration. In der Realität ist das Security-Service-Thema in Deutschland immer noch eng verknüpft mit Produkten. Zur spontanen Nennung von Sicherheitsdienstleistern aufgefordert, tauchen auf der Top-10-Liste der Anwenderunternehmen drei Produktanbieter auf. Die Trennlinie zwischen Dienstleister und Produktanbieter ist unscharf, und einige Produkthersteller sind selbst auch im Service-Geschäft tätig, wenn auch zumeist in geringerem Umfang.

Dennoch werden Sicherheitsaspekte jenseits der bloßen Technologie zunehmend Bestandteil der Angebote der Sicherheitsdienstleister. Hierzu gehören etwa die Unterstützung bei der Aufstellung von Security Policies, Risikoanalysen und Sicherheits-Audits.

Ausschlaggebend ist unter anderem, dass sich gleichzeitig der Preisdruck insbesondere bei standardisierten Services wie beispielsweise im Netzwerkbereich erhöht hat. Die Akzeptanz der Angebote rund um organisatorische IT-Sicherheit variiert bei den Anwenderunternehmen nach Einschätzung der META Group allerdings erheblich – abhängig vom Sicherheitsbewusstsein der jeweiligen Verantwortlichen und von den vorhandenen Budgets.

Allgemein lässt sich beobachten, dass immer mehr Dienstleister auch verstärkt das Mittelstandssegment adressieren. Insbesondere im investitionsscheuen klassischen Mittelstand (Unternehmen unter 500 Mitarbeiter) wird es für die Dienstleister aufgrund der jeweils geringen Budgets nicht einfach sein, profitabel operieren können. Diese Zielgruppe ist daher mit geeigneten Lösungspaketen zu adressieren. Im gehobenen Mittelstand (Unternehmen mit 500 bis 999

Mitarbeitern) tummeln sich kleine wie große Anbieter, was nicht ohne Folgen für die Entwicklung der Preise bleiben wird.

Große Erwartungen hegen spezialisierte und klassische IT-Dienstleister an Managed Security Services (MSS). Die Gründe liegen auf der Hand: Immerhin sind nach Einschätzung der META Group 80 Prozent der heutigen Sicherheitsprobleme eine Folge von Unzulänglichkeiten im Betrieb der IT-Systeme und nicht notwendigerweise eine Konsequenz von Mängeln bei Design oder Implementierung der Lösungen. Systeme werden oftmals unzureichend konfiguriert, gepatcht und gewartet, mit entsprechenden Auswirkungen auf die IT-Sicherheit. Das benötigte umfassende Management von Sicherheitsinfrastrukturen wiederum ist aber sehr personalintensiv. Managed Security Service Provider (MSSP) könnten angesichts des Mangels an qualifizierten Fachkräften Abhilfe schaffen – nicht zuletzt im Mittelstand.

Allerdings tummeln sich in diesem Marktsegment zahlreiche Anbieter. Die Konsolidierung des Marktes ist derzeit im Gange. Trotz der zunehmenden Resonanz auf Managed Firewall und VPN Services sind die geringe Sensibilisierung der Anwender für das Thema sowie teilweise erhebliche Qualitätsunterschiede bei den Angeboten der einzelnen Managed Service Provider derzeit noch problematisch. Die überlebenden MSSPs werden jedoch gestärkt aus der Konsolidierungsphase hervorgehen.

9 Sponsoren der Studie

Die im Folgenden aufgeführten teilnehmenden Unternehmen traten bei der Erstellung dieser Studie als Sponsoren auf. Die Unternehmen konnten den der Studie zu Grunde liegenden Fragebogen mitgestalten und relevante Auswertungen diesbezüglich erstellen lassen.

Weiterhin werden von allen Sponsoren umfassende Firmenprofile erstellt, die im Internet unter www.metagroup.de eingesehen bzw. auf Anfrage als gebundene Version bezogen werden können.

▸ Arcor	▸ Network Associates
▸ BMC Software	▸ ORGA
▸ Cisco	▸ RSA Security
▸ Clearswift	▸ SerCon
▸ Computer Associates	▸ SHE Informationstechnologie
▸ CONSUL risk management	▸ Siemens Business Services
▸ Controlware	▸ Sun Microsystems
▸ Dimension Data	▸ SurfControl
▸ Equant	▸ Sybari
▸ Fujitsu Siemens Computers	▸ Symantec
▸ GROUP Technologies	▸ Trend Micro
▸ IBM Tivoli Software	▸ T-Systems ISS
▸ Lufthansa Systems	▸ TÜV Secure iT
▸ Microsoft	▸ webwasher

10 Anhang

10.1 Glossar

Der Begriff der **IT-Security** lässt sich in die zwei Bestandteile Datensicherheit und Datenschutz zerlegen. Unter dem Begriff Datensicherheit sind alle Disziplinen zusammengefasst, die sich mit der Verfügbarkeit bzw. mit der Wiederherstellung von Daten beschäftigen. Der Datenschutz fasst die Disziplinen zusammen, die notwendig sind, um sicherzustellen, dass Daten nicht von Unbefugten genutzt oder manipuliert werden können (Integrität, Vertraulichkeit und Authentizität).

Weitere Begrifflichkeiten werden nachfolgend alphabetisch und in Kurzform geklärt.

- **Authentifizierung:** Der Prozess oder die Fähigkeit, eine Person, Ressource oder System, das auf eine andere Person, Ressource oder ein anderes System zuzugreifen versucht, eindeutig zu identifizieren. Dazu gehört beispielsweise die Verifizierung einer gesicherten Rechner-Rechner-Kommunikation.
- **BDSG**: Bundesdatenschutzgesetz
- **Backup-Rechenzentren:** Deren Zielsetzung ist im Prinzip die gleiche wie bei Cluster Servern, mit dem Unterschied, dass die verschiedenen Server auch räumlich voneinander getrennt sind. Auf diese Art sollen Katastrophen wie Feuer, Überschwemmungen, Erdbeben und Sabotage in ihrem Schadensausmaß begrenzt bleiben.
- **Basel II:** Die neue Baseler Eigenkapitalvereinbarung, die unter anderem auch zu strengeren finanziellen Prüfmaßstäben für die Vergabe von Krediten führt (betrifft v.a. den Mittelstand).
- **Cluster Server** bestehen aus zwei oder mehr Rechnern, die durch geeignete Software-Tools so konfiguriert werden können, dass für den Fall eines Serverausfalls ein anderer Server dessen Dienste übernimmt und laufende Prozesse zurücksetzt bzw. neu startet.
- **Content Security** Lösungen sollen verhindern, dass im Unternehmen „politisch nicht korrekte“ Inhalte (z.B. Pornografie) genutzt oder verbreitet werden. Auch die Weitergabe firmeninterner sensitiver Informationen an Dritte (z.B. Mitbewerber) wird damit unterbunden. Ferner kann Content Security Technologie die private Nutzung des Webs werden der Arbeitszeit limitieren, um den Netzwerkverkehr zu reduzieren und die Arbeitsproduktivität zu erhöhen. Content Security umfasst im Wesentlichen die Disziplinen E-Mail Content Filtering, Malicious Code Management, Usage Tracking (Überwachung des Nutzerverhaltens im Web), und Site Blocking (Sperren von bestimmten URL für Nutzer). Die Integration aller Disziplinen wird unter dem Begriff Content Security Management (CSM) zusammengefasst.
- **Content Security Management (CSM)** → Content Security

- **Daten-Backup:** Backups dienen der Wiederherstellung von Daten. Zu diesem Zweck werden die Daten beispielsweise auf Bänder kopiert und diese an einem sicheren Ort, z.B. in einem feuerfesten Tresor, gelagert.
- **Datenschutz:** Fasst die Disziplinen zusammen, die notwendig sind, um sicherzustellen, dass Daten nicht von Unbefugten genutzt oder manipuliert werden können. Wesentliche Eckpunkte des Datenschutzes sind die Vertraulichkeit und Integrität (Schutz vor Veränderung durch Dritte) von Daten, die Zugriffskontrolle beispielsweise durch Firewalls sowie die Authentifizierung und Identifizierung von Nutzern.
- **Datensicherheit:** Alle Disziplinen, die sich mit der Verfügbarkeit bzw. mit der Wiederherstellung von Daten beschäftigen.
- **Distributed-Denial-of-Service-Attacken (DDoS):** Der Ablauf eines DDoS-Angriffs kann in zwei Phasen unterteilt werden. Während in Phase I mittelbar unter Einsatz automatisiert ablaufender Tools in kompletten Netzwerkbereichen versucht wird, DDoS-Agenten zu installieren, werden die erfolgreich hinterlassenen und aktiviert im Hintergrund laufenden DDoS-Agenten in Phase II von einem zentralen Master unmittelbar angewiesen, ein gemeinsames Zielsystem (Webserver) anzugreifen. Die Wirksamkeit des Angriffs ist durch die Vielzahl der gleichzeitig angreifenden Rechner stark erhöht und führt zur „Überlastung“ bzw. zum Ausfall des Zielsystems.
- **DMZ** - „demilitarisierte Zone“ – der Bereich des Netzwerks, der mit der „Außenwelt“ bzw. dem Internet verbunden ist.
- **e-Business:** Strategische Klammer, die Transaktionen des e-Commerce in den Gesamtprozess und seine Organisationsform integriert oder diese gegebenenfalls an ein neues „elektronisches“ Prozessmodell anpasst. e-Business bezeichnet demnach die strategische Einbeziehung der elektronischen Transaktionen in alle Aspekte der Geschäftstätigkeit (Strategien, Prozesse, Organisationsstrukturen, um sie zur Erreichung der Geschäftsziele einzusetzen.
- **e-Commerce:** Jede Art von geschäftlicher Transaktion, bei der die Beteiligten auf elektronischem Weg miteinander verkehren. Diese Transaktionen finden innerhalb von Unternehmen, zwischen Unternehmen und privaten Endverbrauchern und zwischen privaten Endverbrauchern / Unternehmen und öffentlichen Einrichtungen auf Basis verteilter Kommunikationsnetzwerke statt.
- **Enterprise Security** beschäftigt sich mit der Sicherstellung der einwandfreien Funktion DV-technischer Einrichtungen und Abläufe (→ Verfügbarkeit, Datensicherheit; → Datenschutz); wird an dieser Stelle als Synonym für IT-Security verwendet (→ IT-Security).
- **e-Security:** Alle Disziplinen der Enterprise Security (Datensicherheit und Datenschutz), die zum Ziel haben, die Sicherheit von e-Business-Lösungen und der damit verbundenen IT-Systeme im Unternehmen sicherzustellen.

- **Ethical Hacking:** Test der Sicherheit der IT-Systeme durch simulierten Hackerangriff. Unternehmensinterne Spezialisten oder externe Dienstleister versuchen dabei, in die IT-Systeme des Unternehmens einzudringen und eventuelle Sicherheitslücken aufzudecken.
- **Identifizierung:** Sichere Identifikation eines Nutzers gegenüber dem System, z.B. durch Smart Cards.
- **Integrität** (von Daten): Schutz von Daten gegen Manipulation durch unberechtigte Dritte.
- **Intrusion Detection Systeme (IDS):** Entdecken Eindringlinge bzw. Abnormalitäten in Netzwerken. Unterschieden werden netzwerkbasierte IDS und hostbasierte IDS. Netzwerkbasierte IDS sind typischerweise „Sniffer", die auf dem Netzwerk sitzen und eingehende Datenpakete prüfen. Sie betrachten dabei Muster oder Signaturen, die zu bekannten Attacken, verbotenen Aktionen oder verdächtigem Verhalten passen. - Hostbasierte IDS nutzen die host-/systembasierten Funktionalitäten wie Snap Shots, Event Log Monitoring oder Kernel-Level Detection, um entsprechende Muster zu überprüfen.
- **IT-Security:** → Enterprise Security; siehe auch explizite Definition am Anfang des Fragebogens.
- **KonTraG:** Gesetz zur Kontrolle und Transparenz im Unternehmensbereich.
- **Malicious Code:** „Trojanische Pferde", zum Beispiel in Form von Java Applets oder Visual Basic Scripts; d.h. bösartiger Code, der sich beim Öffnen von Emails oder Attachments oder beim Download von Dateien aus dem Internet als Virus entpuppt und Schäden an Systemen anrichtet. (siehe auch → Content Security)
- **Public Key Infrastructure (PKI):** Public Key Infrastrukturen bilden den Rahmen, um vier wesentliche Hauptsicherheitsfunktionen für kommerzielle Transaktionen im und zwischen Unternehmen zu verwirklichen:·1) Vertraulichkeit - für die Geheimhaltung von Daten; 2) Integrität - für den Nachweis, dass Daten nicht manipuliert wurden; 3) Authentifizierung - für den Nachweis der Identität einer Person oder Anwendung; 4) Nichtbestreitbarkeit - damit Informationen nicht geleugnet werden können. - Technologisch wird die PKI über eine Kombination aus Hardware- und Software-Produkten, Richtlinien und Prozeduren realisiert. Sie basiert auf "digitalen Zertifikaten", die als "elektronische Ausweise" fungieren. Zum Erstellen und Verifizieren von digitalen Signaturen werden so genannte öffentliche und private Schlüssel verwendet. Diese werden überdies zur Verschlüsselung von Informationen benutzt.
- **Security Policy:** Regeln zur Sicherstellung des Schutzes von Informationen im Unternehmen sowie für die Implementierung eines Security-Programms. Security Policies sind unabhängig von spezifischen Technologien und Lösungen.
- **Single Sign-On (SSO)** ermöglicht Nutzern, sich mit ein und demselben Passwort in mehrere verschiedene Applikationen (oder Web-Anwendungen → Web Single Sign-On) einzuloggen – reduziert Administrationsaufwand / Helpdesk-Aufwand.

- **SPAM:** umgangssprachlicher Begriff für unerwünschte, nicht geschäftsrelevante Emails (z.B. Werbung), die typischerweise an zahlreiche Empfänger verteilt werden.
- **Web Services:** Mittel, um im „Remote"-Modus eine Funktion aufzurufen oder einzubinden, wobei internet-basierende Protokolle genutzt werden.
- **WLAN**: Wireless Local-Area Network – Standard IEEE 802.11x.

10.2 META Group Research Notes

Vollständige Liste der verwendeten META Group Quellen:

META Deltas (Research Notes)

GNS 1023, 19.07.2002: Information Security Policy: Best Practices

GNS 970, 28.02.2002: META Group Information Security Services Framework

GNS 1054, 21.10.2002: Getting Serious About Antivirus

GNS 1066, 11.11.2002: Appropriate Investment in Information Security: Is Risk Assessment Enough?

GNS 1071, 27.11.2002: Controlling Internet Usage: Part 1 – Strategies

GNS 1081, 31.12.2002: Controlling Internet Usage: Part 2 – Selecting a Web Filtering Product

GNS 1086, 15.01.2003: An Information Security Road Map

WCS 1122, 01.05.2002: No Spam Shortage Here

WCS 1136, 31.05.2002: The Battle for Port 25

WCS 1205, 11.12.2002: The Future of Spam

SIS 1028, 08.10.2002: Storage Technologies

WCS 1183, 16.10.2002: E-Mail Off and On the Record: Part 1

WCS 1184, 16.10.2002: E-Mail Off and On the Record: Part 2

META Practice

ED 008, 23.10.2002: Information Security Technology for CIOs

METAspectrum Evaluation

Global Networking Strategies, Security & Risk Strategies, 20.3.2003: Antivirus METAspectrum Evaluation

10.3 Weitere Informationsquellen zum Thema IT-Security

Enterprise Security Desk Reference

Der Enterprise Security Desk Reference ist ein einzigartiges "Handbuch" für CIOs, CSOs und Führungskräfte im Bereich der Enterprise Security und des Risk Managements. Dieser Reference Guide erklärt die fundamentale Rolle und die Implikationen einer Security-Führungsfunktion im Unternehmen. Er zeigt Wege auf, wie ein Enterprise-Security-Programm richtig strukturiert wird, einschließlich der Integration von IT-Sicherheit, Risikomanagement und Privacy Governance.

SPEX Software Evaluation

Mit SPEX lässt sich der komplexe Auswahl-Prozess für unternehmensweite Softwareanwendungen vereinfachen und beschleunigen. SPEX bietet folgende Software-Analysen zum Thema:

- Essential Security Tools - 2002
- Web Single Sign-On - 2002

Subskriptions-Services: Security & Risk Strategies

Im Rahmen der META Group Subskriptions-Services kann auf das Wissen von Experten zugegriffen werden. Der META Group Service „Security & Risk Strategies“ stellt Kunden Research-Informationen und pragmatische Handlungsanleitungen zur Verfügung, damit zukünftigen Herausforderungen begegnet werden kann.

Structured Transformation (Security Infusion)

Die „Security Infusion“ der META Group als strukturiertes Transformationsprogramm unterstützt Kunden bei der Feinabstimmung der Security Policies, der Optimierung von Sicherheitsprozessen, bei der Ausbalancierung von Kosten und Risiken sowie der Kommunikation von „Value“. Kunden lernen, wie eine erprobte Methode zur Erreichung von Sicherheit umgesetzt werden kann, trotz komplexer interner organisatorischer Gegebenheiten oder konkurrierender Business-Prioritäten und Unternehmens-Policies.

Consulting

Das Consulting-Angebot der META Group kombiniert das Wissen über Märkte, Hersteller und Produkte. Kunden profitieren von der Erfahrung der META Group Berater und den Best Practices hunderter Unternehmen.

META IT-Service

Mit dem META IT-Service bietet die META Group einen auf zwölf Monate angelegten Marktforschungs- und Beratungs-Service für IT-Anbieter, der den Forderungen nach Berücksichtigung lokaler Aspekte in der Marktforschung und Beratung weitestgehend Rechnung trägt.

Weitere META Group Multi-Client Studien

MC-(Multi Client)-Studien sind umfassende Befragungen von Anwenderunternehmen zu aktuellen Themen aus dem Bereich IT-Software- und Servicemarkt. Die META Group Deutschland GmbH bietet hierbei IT-Anbietern und Dienstleistern des entsprechenden Marktsegments die Möglichkeit, an diesen MC-Studien teilzunehmen.

An dieser Stelle sei außerdem darauf hingewiesen, dass die META Group als neutrales Beratungsunternehmen weder Hardware und Software verkauft noch Implementierungs-Dienstleistungen anbietet.

10.4 Fragebogen zur Anwenderbefragung

I. Qualifizierung des Unternehmens / allgemeine Angaben

1. Welcher Branche gehört Ihr Unternehmen an?

ISIC Code		(**I**nternational **S**tandard **I**ndustrial **C**lassification)	
Diskrete Fertigung	❑	Bekleidungsindustrie und andere Endprodukte	❑
		Möbel und anderes unbewegliches Mobiliar	❑
		Druckindustrie, Publishing	❑
		Ledergewerbe und Lederprodukte	❑
		Metallerzeugnisse (keine Maschinen und Transporterzeugnisse)	❑
		Maschinenbau	❑
		Computer / Büromaschinen	❑
		Elektronik und elektrisches Equipment und Komponenten mit Ausnahme von Computer Equipment	❑
		Fahrzeugbau und Zulieferer	❑
		Mess- und Regelungstechnik	❑
		Instrumente: medizinische und optische Geräte sowie Uhren	❑
		Sonstige Erzeugnisse (Sportgeräte, Musikinstrumente, Spielwaren, Haushalt)	❑
Prozessorientierte Fertigung	❑	Eisen-, Erz- und Kohlebergbau	❑
		Öl- und Gasförderung	❑
		Metallerzeugung und –verarbeitung, Gießereien	❑
		Bergbau/ Steinbruch nichtmetallische Mineralien	❑
		Nahrungsmittel- und verwandte Produkte	❑
		Tabakprodukte	❑
		Textilindustrie	❑
		Bauholz und Holzprodukte / keine Möbel	❑
		Papierindustrie	❑
		Chemisch/pharmazeutische Produkte	❑
		Ölverarbeitende Industrie	❑
		Gummi- und weiterverarbeitete Kunststoffe	❑
		Steine, Ton, Glas, Keramik	❑
		Sonstige (Zement, Beton, Bau, Straßenbau etc.)	❑
Transport	❑	Schienenverkehr	❑

ISIC Code		(International Standard Industrial Classification)	
		Frachtverkehr Straße	❑
		Schifffahrt	❑
		Luftverkehr, Flughafen (einschl. Reservierungsservice)	❑
		Pipelines (Ausnahme Erdgas)	❑
		Sonstige Beförderungsdienstleistungen	❑
Telekommunikation	❑	Leitungsgebundene Kommunikation (Sprache, Text, Bild)	❑
		Nichtleitungsgebundene Kommunikation (Sprache, Text, Bild)	❑
		Sonstige Fernmeldedienstleistungen	❑
Medien	❑	Verlage (Bücher, Zeitschriften etc.)	❑
		Ton, Bild, Datenträger	❑
Versorgung	❑	Gas- und Wasser	❑
		Elektrizität	❑
Einzelhandel	❑	Baumaterial	❑
		Allg. Warenhäuser	❑
		Lebensmittelketten	❑
		Kfz-Handel / Tankstellen	❑
		Bekleidungsgeschäfte	❑
		Möbel, Mobiliar, Accessoires	❑
		Gaststätten, Trinkhallen	❑
		Sonstiger Handel	❑
Großhandel	❑	Gebrauchsgüter	❑
		Konsumgüter	❑
Versandhandel	❑	Versandhandel	❑
Banken und Finanz-dienstleistungen	❑	Kreditinstitute / Sparkassen / Bausparkassen	❑
		Broker, Händler, Börsen, Spezialkreditinstitute, Leasingfirmen, Hypothekenbanken etc.	❑
		Vermögensverwaltungen	❑
Versicherungen	❑	Versicherungen	❑
		Krankenversicherungen	
		Versicherungsmakler, -agenturen	❑
Gesundheitswesen	❑	Krankenhäuser, Hochschulkliniken	❑
		Praxen von Ärzten	❑
		Alten-/ Pflege-/ Wohnheime	❑
Bildung	❑	Schulen, Fachhochschulen, Universitäten	❑

ISIC Code		(**I**nternational **S**tandard **I**ndustrial **C**lassification)	
Business Services	❑	Immobilien, Grundbesitz (Erschließung, Bauträger)	❑
		Hotels und sonstiges Gastgewerbe	❑
		Beratung (Unternehmensberatung, DV-Beratung)	❑
		Steuerberatung	❑
		Hotelreservierung	❑
		Reparaturwerkstätten (Automotive)	❑
		Sonstige Reparaturwerkstätten	❑
		Kino	❑
		Entertainment, Werbung	❑
		Juristische Dienstleistungen	❑
		Vermietung (Immobilien, Mobilien)	❑
		Forschung und Entwicklung	❑
		Soziale Dienstleistungen	❑
		Museen, Kunstgalerien, botanische und zoologische Gärten	❑
		Vereine und ähnliches	❑
		Konstruktion, Buchführung, Marktforschung, Management, Reisebüro, DV und verwandte Dienstleistungen	❑
		Hoch- und Tiefbau – Generalunternehmen und Subkontraktoren	❑
		Sonstige Dienstleistungen (Reinigung, Detekteien, Arbeitsvermittlung, Entsorgung)	❑
Öffentliche Hand	❑	Kommunale Behörden und Verbände	❑
		Landesbehörden	❑
		Bundesbehörden	❑
Primärer Sektor	❑	Landwirtschaft Getreide und Viehzucht	❑
		Forstindustrie	❑
		Fischerei, Jagdindustrie	❑

2. Unternehmensgröße

2 a) Wie hoch war der Umsatz Ihres Unternehmens 2001 in Deutschland und weltweit?

Weltweit: _____ Millionen EUR in Deutschland: _____ Millionen EUR

(bei Banken: Bilanzsumme; bei Versicherungen: Beitragsvolumen; öffentliche Hand: Haushaltsvolumen o.ä.)

Oder Umsatz in Klassen für Deutschland:

❒	unter 2,5 Mio. EUR
❒	2,5 bis unter 5 Mio. EUR
❒	5 bis unter 10 Mio. EUR
❒	10 bis unter 50 Mio. EUR
❒	50 bis unter 100 Mio. EUR
❒	100 bis unter 500 Mio. EUR
❒	500 bis unter 1.000 Mio. EUR
❒	1 Mrd. bis unter 20 Mrd. EUR
❒	20 Mrd. bis unter 50 Mrd. EUR
❒	50 Mrd. EUR oder mehr

2 b) Wie viele Mitarbeiter waren Ende 2002 in Ihrem Unternehmen in Deutschland und weltweit beschäftigt?

Weltweit: _____ in Deutschland: _____ (*<50 MA=> Abbruch!!)*

Filter: Wenn Frage 2b Deutschland „keine Angabe“ oder „Weiß nicht“:

2 c) Wie viele Mitarbeiter waren Ende 2002 in Ihrem Unternehmen in Deutschland und weltweit beschäftigt (in Klassen)?

Mitarbeiter Deutschland		Mitarbeiter weltweit	
❒	50 bis 199	❒	50 bis 199
❒	200 bis 499	❒	200 bis 499
❒	500 bis 999	❒	500 bis 999
❒	1000 bis 4999	❒	1000 bis 4999
❒	5000 oder mehr	❒	5000 oder mehr

Filter: < 50 MA => Abbruch !!

3. Wie viele PCs, PDAs, Server und Mainframes gibt es in Ihrem Unternehmen (2002, nur Deutschland)?

Front-End / Desktop: _____ PCs

_____ Notebooks

_____ PDAs (Palm, Pocket PC…)

Back-End: _____ Server (Unix, Linux, Windows NT/2000…)

_____ Mainframes

4. Welche Position nehmen Sie in Ihrem Unternehmen ein?

- ❒ IT-Leiter / CIO
- ❒ Leiter IT Security (CISO)
- ❒ Vorstand / Geschäftsführung / CEO / COO
- ❒ Leiter Netzwerkplanung / Systemadministration
- ❒ Datenschutzbeauftragter
- ❒ Bereichsleiter / Fachabteilung
- ❒ Bereichsleiter E-Business
- ❒ Controlling / Finanzwesen / CFO
- ❒ Marketingleiter
- ❒ Leiter Einkauf
- ❒ Leiter Vertrieb
- ❒ Sonstige: _____

5. Wie hoch war Ihr IT-Budget im Jahr 2002 und wie wird es sich bis 2004 entwickeln?

IT-Budget in Tausend EURO	2002	2003	2004
Insgesamt:			

Filter: Wenn Frage 5 „Keine Angaben“:

5 a) IT-Budget 2003 in Klassen abfragen!

❒	unter 12.500 EUR	❒	1 Mio. bis unter 2 Mio. EUR
❒	12.500 bis unter 25.000 EUR	❒	2 Mio. bis unter 5 Mio. EUR
❒	25.000 bis unter 50.000 EUR	❒	5 Mio. bis unter 10 Mio. EUR
❒	50.000 bis unter 100.000 EUR	❒	10 Mio. bis unter 20 Mio. EUR
❒	100000 bis unter 200000 EUR	❒	20 Mio. bis unter 50 Mio. EUR
❒	200000 bis unter 500000 EUR	❒	50 Mio. bis unter 100 Mio. EUR
❒	500000 bis unter 1 Mio. EUR	❒	200 Mio. EUR oder mehr

II. Organisatorische Aspekte / Einschätzung des Bedrohungspotenzials

6. Personelle Ausstattung für IT-Sicherheit

6 a) Gibt es in Ihrem Unternehmen eine IT-Sicherheitsorganisation, d.h. ein dediziertes Security-Team?

- ❒ Ja
- ❒ Nein.
- ❒ Ich weiß nicht
- ❒ Keine Angabe

6 b) Wie groß ist Ihre personelle Ausstattung für IT Security (Full-Time Equivalents)?

Insgesamt sind _____ Mitarbeiter (Fulltime Equivalents[1]) mit IT-Security beschäftigt.

7. a) Haben Sie eine schriftlich fixierte Security Policy im Unternehmen?

- ❒ Ja
- ❒ Nein, auch nicht geplant => Weiter mit Frage 8
- ❒ Nein, aber geplant => Weiter mit Frage 8
- ❒ Ich weiß nicht => Weiter mit Frage 8
- ❒ Keine Angaben => Weiter mit Frage 8

7 b) Welche Bereiche deckt Ihre Security Policy ab?

- ❒ Email-Nutzung
- ❒ Web-Nutzung
- ❒ Weitere: _____
- ❒ Keine Angabe

7 c) Wie wird Ihre Security Policy im Unternehmen durchgesetzt?

(Mehrere Antworten möglich)

- ❒ Schriftliche Anweisungen, die an die Mitarbeiter verteilt werden
- ❒ Durchsetzung über fest vorkonfigurierte Systeme (Desktops, Server)
- ❒ Obligatorisches Training / Web-Seminare
- ❒ Informationen im Intranet
- ❒ Mitarbeiterzeitung
- ❒ Sonstige: _____
- ❒ Ich weiß nicht
- ❒ Security Policy wird überhaupt nicht durchgesetzt

[1] Full-Time Equivalents (FTE): Falls manche Mitarbeiter sich nur teilweise der IT-Security widmen, so bedeutet FTE die Summe der Kapazitäten, bezogen auf „Als-ob"-Vollzeitmitarbeiter: Bsp.: 4 Mitarbeiter, die zu 50% für Security eingesetzt werden, entsprechen 2 FTE.

❒ Keine Angabe

8. a) Verfügt Ihr Unternehmen über eine Security-Zertifizierung, z.B. nach BS 7799?

❒ Ja
❒ Nein, Zertifizierung auch nicht geplant => Weiter mit Frage 9
❒ Nein, Zertifizierung aber geplant
❒ Ich weiß nicht => Weiter mit Frage 9
❒ Keine Angabe => Weiter mit Frage 9

8 b) Nach welchem Standard sind Sie zertifiziert bzw. planen Sie eine Zertifizierung?

❒ _____
❒ Ich weiß nicht
❒ Keine Angabe

9. Wie hoch schätzen Sie die Bedeutung folgender Sicherheits-Risiken als treibende Faktoren für künftige Security-Investitionen (Datenschutz) auf einer Skala von 1=sehr hoch bis 5=sehr niedrig ein?

	1	2	3	4	5	Keine Angabe
Eindringen unautorisierter Personen in das Unternehmensnetzwerk:						
Unautorisiertes Eindringen gezielt durch Mitbewerber (Industriespionage)	❒	❒	❒	❒	❒	❒
Unautorisiertes Eindringen durch Hacker ohne wirtschaftl. Interessen	❒	❒	❒	❒	❒	❒
Manipulation / Offenlegung von Transaktionen (Web / Email)	❒	❒	❒	❒	❒	❒
Distributed-Denial-of-Service-Attacken (DDoS)	❒	❒	❒	❒	❒	❒
Virenbefall / „Malicious Code“	❒	❒	❒	❒	❒	❒
Neue Sicherheitsfragen durch Nutzung drahtloser Technologien (WLAN, UMTS etc.)	❒	❒	❒	❒	❒	❒
Neue Sicherheitsfragen durch Nutzung von Web Services	❒	❒	❒	❒	❒	❒
Missbrauch von Benutzerrechten durch eigene Mitarbeiter - „Innentäter“	❒	❒	❒	❒	❒	❒
Verbreitung illegaler oder „politisch unkorrekter“ Inhalte im Unternehmensnetzwerk	❒	❒	❒	❒	❒	❒
Physischer Einbruch / Diebstahl von Hardware	❒	❒	❒	❒	❒	❒
Sonstige, und zwar: _____	❒	❒	❒	❒	❒	❒

10. Wo ist die Verantwortlichkeit des Aufgabenkomplexes IT-Security hinsichtlich Initiative, Budgetverantwortung und Realisierung angesiedelt?

(Mehrfachantworten sind möglich)

	IT-Abteilung	Dauerhaftes IT-Security-Team	Datenschutzbeauftragter	RZ-Leiter	System-/Netzwerkadministration	Fachabteilung	Marketing	Einkauf/Beschaffung	Controlling / Finanzwesen	Management/Geschäftsführung	Externe Dienstleister	Sonstige (bitte spezifizieren): _____
Primärer Entscheider	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Berater, Beeinflusser („Influencer“)	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Budgetverantwortung	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Realisierung/Anbieterauswahl	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒

III. Investitionsplanung für IT-Security

11. Wie viel Prozent Ihres IT-Budgets widmen Sie im Jahr 2003 Aufgaben der IT-Security (inklusive direkt zuordenbarer Personalkosten)?
(Auf Definition von IT-Security achten: Datenschutz und Datensicherheit!)

- ❒ Unter 1%
- ❒ 1% bis unter 2%
- ❒ 2% bis unter 3%
- ❒ 3% bis unter 4%
- ❒ 4% bis unter 5%
- ❒ 5% bis unter 6%
- ❒ 6% bis unter 10%
- ❒ Über 10%
- ❒ Keine Angabe

12. Entwicklung und Verteilung der Ausgaben für IT Security

12 a) Wie wird sich Ihr IT-Security-Budget im Jahr 2004 gegenüber 2003 entwickeln?

- ❒ Das Budget wird zunehmen
- ❒ Das Budget bleibt konstant
- ❒ Das Budget wird abnehmen
- ❒ Steht noch nicht fest
- ❒ Keine Angabe.

Filter: Frage 12a → 12b:

12 b) Um wie viel % wird Ihr IT-Security-Budget im Jahr 2004 gegenüber 2003 zu- bzw. abnehmen?

Zunahme um _____ %; Abnahme um _____ %.

12 c) Wie hoch ist der Anteil folgender Teilbereiche an den gesamten IT-Security-Ausgaben?

Interne Personalkosten: _____ % vom IT-Security-Budget

Extern bezogene Dienstleistungen: _____ % vom IT-Security-Budget

Extern bezogene Sicherheits-Produkte: _____ % vom IT-Security-Budget

Summe = 100%

12 d) Wie hoch ist der Anteil folgender Teilbereiche an den gesamten IT-Security-Ausgaben?

Ausgaben für „Datenschutz“: _____ % vom IT-Security-Budget

Ausgaben für „Datensicherheit“ / Verfügbarkeit: _____ % vom IT-Security-Budget

Summe = 100%

13. Wie bewerten Sie die folgenden Hemmnisse für die Durchsetzung eines hohen Sicherheitsniveaus bei Ihrer IT-Infrastruktur auf einer Skala von 1 (sehr hohes Hemmnis) bis 5 (sehr geringes Hemmnis)?

Hemmnis:	1	2	3	4	5	Keine Angabe
Geringes Budget	❒	❒	❒	❒	❒	❒
Personalmangel	❒	❒	❒	❒	❒	❒
Organisatorische Schwierigkeiten (Security Policy, Integration von Sicherheitsfragen in Geschäftsprozesse, unklare Zuständigkeiten...)	❒	❒	❒	❒	❒	❒
Geringes Sicherheitsbewusstsein der Anwender	❒	❒	❒	❒	❒	❒
Management: mangelnder Support / fehlendes Bewusstsein	❒	❒	❒	❒	❒	❒
Technologien zu komplex / unreif	❒	❒	❒	❒	❒	❒
Unsichere Server-Betriebssysteme	❒	❒	❒	❒	❒	❒
Schwierige Integration von Produkten (Standalone-Lösungen, keine Standards)	❒	❒	❒	❒	❒	❒
Schlechte Messbarkeit von Risiken / ROI	❒	❒	❒	❒	❒	❒
Sonstige: _____	❒	❒	❒	❒	❒	❒

14. Wie wichtig sind die folgenden Entscheidungsgrundlagen bzw. Faktoren für die Höhe der IT-Security-Investitionen in Ihrem Unternehmen? Bitte bewerten sie die Kriterien auf einer Skala von 1 (sehr wichtig) bis 5 (unwichtig).

	1	2	3	4	5	Keine Angabe
ROI-Analysen / Risk Assessment	❒	❒	❒	❒	❒	❒
Marketing[2] (Aufbau von Image / Vertrauen)	❒	❒	❒	❒	❒	❒
Orientierung an Aktivitäten der Mitbewerber	❒	❒	❒	❒	❒	❒
Anforderung durch Partner / Kunden	❒	❒	❒	❒	❒	❒
Security als „Enabler" für neue Angebote oder Erschließung neuer Märkte (v.a. e-Business)	❒	❒	❒	❒	❒	❒
Rechtliche Rahmenbedingungen, z.B. Basel II, KonTraG, BDSG	❒	❒	❒	❒	❒	❒
Erfahrungen aus in der Vergangenheit eingetretenen Sicherheitsproblemen	❒	❒	❒	❒	❒	❒
Sonstige: _____	❒	❒	❒	❒	❒	❒

15. a) Haben Sie folgende IT-Sicherheitslösungen im Bereich Virenschutz, Zugriffskontrolle und Verschlüsselung implementiert oder planen Sie in den kommenden 12 Monaten deren Evaluierung oder Realisierung?

Virenschutz, Zugriffskontrolle und Verschlüsselung	**Bereits im Einsatz**	**Realisierung bis Ende 2003**	**Geplant, aber noch kein Zeitpunkt festgelegt**	**Kein Einsatz und nicht geplant**
URL Content Security (Web Filtering)	❒	❒	❒	❒
Content Security / Filtering (Email)	❒	❒	❒	❒
Virenschutz / Malicious Code	❒	❒	❒	❒
Verschlüsselung an PC, Notebook oder Workstation	❒	❒	❒	❒
Netzwerk-/Link-Verschlüsselung	❒	❒	❒	❒
Email-Verschlüsselung	❒	❒	❒	❒
Verschlüsselung auf Anwendungsebene	❒	❒	❒	❒
Verschlüsselung/Sicherheit für WLAN (Wireless LAN)	❒	❒	❒	❒
Firewalls	❒	❒	❒	❒

[2] Marketing/Image in diesem Zusammenhang: das Anwenderunternehmen wirbt gegenüber seinen Kunden mit dem Einsatz von „sicheren IT-/E-Business-Lösungen". Beispiel: Ein Betreiber eines elektronischen Marktplatzes sichert den Teilnehmern hohe Verfügbarkeit des Marktplatzes (24 Stunden, 7 Tage pro Woche) und die Vertraulichkeit der Kundendaten zu.

Virenschutz, Zugriffskontrolle und Verschlüsselung	Bereits im Einsatz	Realisierung bis Ende 2003	Geplant, aber noch kein Zeitpunkt festgelegt	Kein Einsatz und nicht geplant
Personal Firewalls	❒	❒	❒	❒
VPNs (Virtual Private Networks)	❒	❒	❒	❒
Sonstige: _____	❒	❒	❒	❒

15 b) Haben Sie folgende IT-Sicherheitslösungen im Bereich Authentifizierung und Autorisierung implementiert oder planen Sie in den kommenden 12 Monaten deren Evaluierung oder Realisierung?

Authentifizierung und Autorisierung	Bereits im Einsatz	Realisierung bis Ende 2003	Geplant, aber noch kein Zeitpunkt festgelegt	Kein Einsatz und nicht geplant
Remote Nutzer-Authentifizierung	❒	❒	❒	❒
Lokale Nutzer-Authentifizierung	❒	❒	❒	❒
Server-Zugriffskontrolle und Sicherheitsüberwachung	❒	❒	❒	❒
Policy Server / Autorisierung	❒	❒	❒	❒
Web Single Sign-on (SSO)	❒	❒	❒	❒
Klassisches Single Sign-on	❒	❒	❒	❒
Certificate Authorities/PKI (Public Key Infrastructure)/ digitale Signatur	❒	❒	❒	❒
Directories	❒	❒	❒	❒
Sonstige: _____	❒	❒	❒	❒

15 c) Haben Sie folgende IT-Sicherheitslösungen im Bereich Administration, Monitoring und Audit implementiert oder planen Sie in den kommenden 12 Monaten deren Evaluierung oder Realisierung?

Administration, Monitoring und Audit	**Bereits im Einsatz**	**Realisierung bis Ende 2003**	**Geplant, aber noch kein Zeitpunkt festgelegt**	**Kein Einsatz und nicht geplant**
"Single-Platform" Server-Sicherheitsmanagement-Werkzeuge	❒	❒	❒	❒
"Multi-Platform" Server-Sicherheitsmanagement-Werkzeuge	❒	❒	❒	❒
Security Audits (Sicherheitsprüfung)	❒	❒	❒	❒
Intrusion Detection Systeme	❒	❒	❒	❒
Sonstige: _____	❒	❒	❒	❒

Filter: Frage 15a: Wenn Content Security / Virenschutz derzeit im Einsatz oder zukünftig geplant:

16. Welche der folgenden Argumente sind für den Einsatz eines Content Security Management-Systems ausschlaggebend? Bitte bewerten Sie die Kriterien auf einer Skala von 1 = "trifft voll zu", bis 5= „trifft überhaupt nicht zu".

	1	**2**	**3**	**4**	**5**	**Keine Angabe**
Schutz der Netzwerk-Infrastruktur gegen Virus-Attacken etc.	❒	❒	❒	❒	❒	❒
Vermeidung aus der Nutzung von Internet/Email resultierender rechtlicher Risiken / Streitfälle	❒	❒	❒	❒	❒	❒
Erhaltung der Netzwerkbandbreite durch Filterung von Inhalten	❒	❒	❒	❒	❒	❒
Erhöhung der Mitarbeiterproduktivität durch Einschränkung privaten „Surfens" und Email-Nutzung	❒	❒	❒	❒	❒	❒
Sonstige: _____	❒	❒	❒	❒	❒	❒

Filter: Wenn in Frage 15a Virenschutz/Content Security im Einsatz oder geplant:

17. Nutzen Sie so genannte „E-Mail Appliances" für Virenschutz bzw. Content Security oder haben Sie deren Einsatz geplant?

(Zum Beispiel E-Mail Appliances am Gateway bzw. als Messaging Routing Hub – als kombinierte Hardware-Software-Lösung im Bereich Virenschutz / Content Security.)

- ❒ Ja
- ❒ Nein, zukünftig aber geplant
- ❒ Nein, zukünftig auch nicht geplant
- ❒ Keine Angabe
- ❒ Ich weiß nicht

Filter: Wenn Frage 17 „Ja“ oder „Nein, zukünftig aber geplant“:

17 a) Welche Funktionalitäten erwarten Sie von einer solchen E-Mail Appliance?
(Mehrfachnennungen sind möglich)

- ❒ Virenschutz
- ❒ Content Filtering
- ❒ Reporting Tools
- ❒ Monitoring/Alerting
- ❒ Weitere: _____

Filter: Wenn Frage 17 „Ja“ oder „Nein, zukünftig aber geplant“:

17 b) Auf welchem Server-Betriebssystem setzt die E-Mail Appliance auf bzw. soll sie aufsetzen?

- ❒ MS Windows 2000
- ❒ MS Windows NT
- ❒ MS Windows.NET Server/ jetzt: MS Windows Server 2003
- ❒ Linux
- ❒ Unix (inkl. Derivate, ohne Linux)
- ❒ Novell
- ❒ Sonstige:_____

18. Wie viele Emails erhalten Sie durchschnittlich pro Tag, und wie hoch ist der Anteil an nicht geschäftsrelevanten bzw. Werbemails?

Durchschnittlich _____ **Emails** pro Tag.

Hiervon sind _____ % **Werbemails / nicht geschäftsrelevant**.

Filter: Frage 15a: Wenn Virenschutz und Email-Verschlüsselung derzeit im Einsatz:

18 a) Setzen Sie in Ihrem Unternehmen gleichzeitig Email-Verschlüsselung und Virenschutz ein?

- ❒ **Ja**
- ❒ Nein
- ❒ Ich weiß nicht
- ❒ Keine Angabe

Filter: Wenn Frage 18a: „Ja“

18 b) Wie gestaltet sich die Integration dieser Email/Verschlüsselungs-Lösungen?

- ❒ „Custom“-Lösung / Eigenentwicklung
- ❒ Standardlösung
- ❒ Keine Angabe

18 c) Werden alle ein- oder ausgehenden Emails zentral archiviert?

- ❒ Ja
- ❒ Nein
- ❒ Ich weiß nicht
- ❒ Keine Angabe

18 d) Wird Email eher „informativ“ oder „rechtsverbindlich“ eingesetzt?

(Mehrfachantworten möglich)

❒ Eher informativ; Email ist keine rechtsverbindliche Willenserklärung.

❒ Email ist teilweise auch rechtsverbindliche Willenserklärung
(z.B. zur Bestellung von Waren, Angebotsabgabe etc.).

❒ Ich weiß nicht. ❒ Keine Angabe.

18 e) Ist die Rechtssicherheit Ihrer Email-Kommunikation durch Verwendung eines Legal Disclaimer (Haftungsausschlusserklärung) als Zusatz zur Email gewährleistet?

❒ Ja ❒ Ich weiß nicht

❒ Nein ❒ Keine Angabe

18 f) Welche Maßnahmen haben Sie ergriffen, um den Missbrauch von Emails zur Betriebsspionage zu unterbinden?

_____

_____

_____

19. In welchen der folgenden Bereiche werden digitale Zertifikate eingesetzt bzw. wo ist in den kommenden 24 Monaten der Einsatz geplant?

(Mehrfachnennungen sind möglich)

	Bereits heute.	2003 / 2004	Nicht geplant
Email	❒	❒	❒
Internet	❒	❒	❒
Intranet	❒	❒	❒
Extranet	❒	❒	❒
VPN (Virtual Private Network)	❒	❒	❒
ERP (Enterprise Resource Planning)	❒	❒	❒
CRM (Customer Relationship Management)	❒	❒	❒
SCM (Supply Chain Management)	❒	❒	❒
Dokumenten-Management	❒	❒	❒
e-Procurement (elektronische Beschaffung)	❒	❒	❒
Sonstige: _____	❒	❒	❒

Filter: Wenn in Frage15 VPN im Einsatz:

20. Welche VPN-Technologien decken Ihre Anforderungen am besten ab?
(Mehrfachantworten möglich)

- ❒ Internet-VPN
- ❒ IP-VPN auf Basis MPLS
- ❒ VPN auf Basis virtueller Router
- ❒ Frame Relay-VPN
- ❒ VPN auf Basis ATM
- ❒ Weiß nicht
- ❒ Keine Angaben

IV. Erfahrungen mit IT-Security

21. Welche Schadensarten sind Ihrem Wissen nach in Ihrem eigenen oder bei Ihnen bekannten Unternehmen in den letzten 24 Monaten entstanden?
(Mehrfachantworten möglich)

- ❒ Datenverlust
- ❒ Verlust der Daten-Integrität / Manipulation von Daten
- ❒ Unautorisierter Zugriff auf Daten (Vertraulichkeitsverlust)
- ❒ Missbrauch von Daten / Betrug
- ❒ Rechtliche Streitfälle
- ❒ Entgangene Umsätze durch Systemausfall
- ❒ Wiederherstellungskosten nach Systemausfall
- ❒ Misstrauen und Verlust von Kunden/Partnern / Imageverlust
- ❒ Sonstige, und zwar: _____
- ❒ Keine Angabe

V. Zusammenarbeit mit Anbietern von Lösungen und Dienstleistungen

22. In welchen Bereichen nehmen Sie heute externe Dienstleister in Anspruch und wo planen Sie dies zukünftig?
(Mehrfachantworten möglich)

	Bereits heute	2003 / 2004	Nicht geplant
Certificate Authority (digitale Zertifikate und PKI)	❒	❒	❒
Konzeption und Entwicklung von unternehmensweiter IT-Sicherheit	❒	❒	❒
Risk Assessment, Analyse der Geschäftsprozesse	❒	❒	❒
Security Audit/ Ethical Hacking/Penetration Testing	❒	❒	❒
Spezifischer: Audits in der Softwareentwicklung / Sicherheitskonzepte für eigenentwickelte Software	❒	❒	❒
Implementierung von Security-Lösungen	❒	❒	❒
Absicherung von Telearbeitsplätzen / Remote Access Lösungen	❒	❒	❒
Managed Firewall Service	❒	❒	❒
Managed Intrusion Detection Service / Netzwerk-Monitoring	❒	❒	❒
Managed VPN Service	❒	❒	❒
Managed Services für Vulnerability Scanning / Netzwerkanalyse	❒	❒	❒
Content Security Management	❒	❒	❒
Externe IT-Sicherheitsbeauftragte	❒	❒	❒
Sonstige: _____	❒	❒	❒

Filter: Nur wenn in Frage 22 derzeit oder zukünftig Content Security Management in Anspruch genommen wird:

22 a) Nur falls Sie für Content Security Management externe Dienstleister einbeziehen: In welchen Bereichen des Content Security Management nehmen Sie heute Dienstleister in Anspruch, und wo planen Sie dies zukünftig?

	Bereits heute	2003 / 2004	Nicht geplant
Email Gateway Virenschutz	❒	❒	❒
Internet Gateway Virenschutz	❒	❒	❒
Management der Email Policy (Inhalte und Attachments)	❒	❒	❒
SPAM Filtering	❒	❒	❒
„Employee Internet Management“ (URL Blocking)	❒	❒	❒
Web Content Filtering (Werbung, Privacy, File Downloads)	❒	❒	❒
Log-Analyse und Reporting Tools	❒	❒	❒
Management des Gebrauchs von Instant Messaging / Streaming Media	❒	❒	❒
Schutz der „Corporate Privacy“ und vertraulichen Informationen	❒	❒	❒

	Bereits heute	2003 / 2004	Nicht geplant
Sonstige: _____	❒	❒	❒

Filter: Nur wenn in Frage 22 externe Dienstleister in Anspruch genommen oder geplant werden:

23. Wie wichtig sind bzw. waren Ihnen die folgenden Kriterien bei der Auswahl eines Anbieters von Dienstleistungen im IT-Security-Umfeld? Bitte bewerten Sie die Kriterien auf einer Skala von 1 = sehr wichtig bis 5 = unwichtig. Wie zufrieden waren / sind Sie mit Ihrem Dienstleister in Bezug auf diese Kriterien auf einer Skala von 1 = sehr zufrieden bis 5 = unzufrieden?

Kriterien	Anforderungen					Zufriedenheit				
	1	2	3	4	5	1	2	3	4	5
Spezialisten-Know-how (technologische Kompetenz)	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Generalisten-Know-how (technologische Kompetenz)	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Herstellerunabhängigkeit	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Günstige Preise (z.B. Tagessätze)	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Service-/Support-Qualität	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Tiefe des Portfolios (Software, Hardware, Service - „alles aus einer Hand“)	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Betreuung über den gesamten Service-Zyklus „PLAN-BUILD-RUN“ (einschl. Betrieb)	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Einschlägige Referenzen	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Branchenexpertise	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Lokale Präsenz	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Internationalität	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Gutes Image / Vertrauen	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Größe des Anbieters (groß=besser?)	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Sonstige: _____	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒

24. Wie wichtig sind bzw. waren Ihnen die folgenden Kriterien bei der Auswahl eines Anbieters von Lösungen im IT-Security-Umfeld? Bitte bewerten Sie die Kriterien auf einer Skala von 1 = sehr wichtig bis 5 = unwichtig. Wie zufrieden waren / sind Sie mit ihrem Anbieter in Bezug auf diese Kriterien auf einer Skala von 1 = sehr zufrieden bis 5 = unzufrieden?

Kriterien	Anforderungen					Zufriedenheit				
	1	2	3	4	5	1	2	3	4	5
„Best-of-Breed"-Lösung / Technologieführer	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
„Out-of-the-Box"-Lösung (schlüsselfertige Lösung *aus einer Hand*[3])	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Standardisierte Technologie	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Flexibilität der Lösung / Einbindung in bestehende Systemlandschaften	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Günstige Preise	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Service-/Support-Qualität	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Einschlägige Referenzen	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Zukunftssicherheit des Anbieters	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Lokale Präsenz	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Fokus auf Europa (Markt-Kenntnis, rechtliche Rahmenbedingungen)	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Internationalität	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Gutes Image / Vertrauen in Anbieter	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Größe des Anbieters (groß=besser?)	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒
Sonstige: _____	❒	❒	❒	❒	❒	❒	❒	❒	❒	❒

25. Welche (max. 3) **drei Argumente sprechen aus Ihrer Sicht für den Einbezug eines international präsenten Security-Dienstleisters oder –Produktanbieters?**

_____

26. Welche Anbieter von Sicherheitslösungen (Produkten) fallen Ihnen spontan ein?

_____

27. Welche Anbieter von Sicherheits-Dienstleistungen fallen Ihnen spontan ein?

_____

28. a) Welche der folgenden Anbieter von Security-Dienstleistungen sind Ihnen bekannt, wie hoch schätzen Sie die Leistungsfähigkeit des Anbieters unter dem Security-Dienst-eistungsaspekt ein? Bitte bewerten Sie die Leistungsfähigkeit der Anbieter auf einer Skala von 1= sehr gut bis 5= sehr schlecht.

28 b) Welche dieser Dienstleister kommen bei Ihren nächsten Security-Initiativen in die engere Auswahl bzw. stehen auf Ihrer Short List?

Anbieter	Bekannt?	1	2	3	4	5	Short List?
Arcor	❒	❒	❒	❒	❒	❒	❒
circular	❒	❒	❒	❒	❒	❒	❒
Controlware	❒	❒	❒	❒	❒	❒	❒
Dimension Data/Telemation	❒	❒	❒	❒	❒	❒	❒
EDS	❒	❒	❒	❒	❒	❒	❒
Equant	❒	❒	❒	❒	❒	❒	❒
GE Compunet	❒	❒	❒	❒	❒	❒	❒
Getronics	❒	❒	❒	❒	❒	❒	❒
Hewlett-Packard / Compaq	❒	❒	❒	❒	❒	❒	❒
IBM Global Services	❒	❒	❒	❒	❒	❒	❒
Infonet	❒	❒	❒	❒	❒	❒	❒
Lufthansa Systems[4]	❒	❒	❒	❒	❒	❒	❒
net Stemmer	❒	❒	❒	❒	❒	❒	❒
NK Networks & Services	❒	❒	❒	❒	❒	❒	❒
ORGA	❒	❒	❒	❒	❒	❒	❒
PanDacom	❒	❒	❒	❒	❒	❒	❒
secunet Security Networks AG	❒	❒	❒	❒	❒	❒	❒
SerCon	❒	❒	❒	❒	❒	❒	❒
SHE IT AG	❒	❒	❒	❒	❒	❒	❒
Siemens Business Services	❒	❒	❒	❒	❒	❒	❒
T-Systems (inkl. T-Telesec)[5]	❒	❒	❒	❒	❒	❒	❒
TÜV Secure iT	❒	❒	❒	❒	❒	❒	❒
Weitere: _____	❒	❒	❒	❒	❒	❒	❒

[3] Möglichst hohe Wertschöpfung durch Anbieter/Lieferant (z.B. durch Komplettpaket Smartcards/ Smartcard-Leser, Firewalls, PKI etc., wobei die einzelnen Komponenten für sich allein betrachtet nicht unbedingt die „beste“ Lösung darstellen) oder Best-of-Breed-Produkte von verschiedenen Herstellern?

[4] Lufthansa Systems einschließlich der Konzerngesellschaften, z.B. Lufthansa Systems AS, Lufthansa Systems Network, Lufthansa Systems Infratec etc.

[5] T-Systems: einschl. der ehemaligen debis ISS, heute integriert in ITC-Security

29. a) Welche der folgenden Anbieter von Security-Lösungen (Software, Hardware) sind Ihnen bekannt, wie hoch schätzen Sie die Leistungsfähigkeit des Anbieters ein? Bitte bewerten Sie die Leistungsfähigkeit der Anbieter auf einer Skala von 1= sehr gut bis 5= sehr schlecht.

29 b) Welche Lösungs-Anbieter kommen bei Ihren nächsten Security-Initiativen in die engere Auswahl bzw. stehen auf Ihrer Short List?

Anbieter	Bekannt?	1	2	3	4	5	Short List?
BMC	❒	❒	❒	❒	❒	❒	❒
Checkpoint Technologies	❒	❒	❒	❒	❒	❒	❒
Cisco	❒	❒	❒	❒	❒	❒	❒
Clearswift (MIMEsweeper)	❒	❒	❒	❒	❒	❒	❒
Computer Associates (CA)	❒	❒	❒	❒	❒	❒	❒
CONSUL risk management	❒	❒	❒	❒	❒	❒	❒
Evidian	❒	❒	❒	❒	❒	❒	❒
Fujitsu Siemens Computers	❒	❒	❒	❒	❒	❒	❒
GROUP Technologies	❒	❒	❒	❒	❒	❒	❒
HP	❒	❒	❒	❒	❒	❒	❒
IBM Tivoli Software	❒	❒	❒	❒	❒	❒	❒
Marshal Software	❒	❒	❒	❒	❒	❒	❒
Microsoft	❒	❒	❒	❒	❒	❒	❒
NetScreen	❒	❒	❒	❒	❒	❒	❒
Network Associates (McAfee, Sniffer)	❒	❒	❒	❒	❒	❒	❒
Novell	❒	❒	❒	❒	❒	❒	❒
RSA Security	❒	❒	❒	❒	❒	❒	❒
Secude / IT_SEC	❒	❒	❒	❒	❒	❒	❒
Secure Computing	❒	❒	❒	❒	❒	❒	❒
Sophos	❒	❒	❒	❒	❒	❒	❒
Sun Microsystems	❒	❒	❒	❒	❒	❒	❒
SurfControl	❒	❒	❒	❒	❒	❒	❒
Sybari	❒	❒	❒	❒	❒	❒	❒
Symantec	❒	❒	❒	❒	❒	❒	❒
Trend Micro	❒	❒	❒	❒	❒	❒	❒
Utimaco Safeware AG	❒	❒	❒	❒	❒	❒	❒
Websense	❒	❒	❒	❒	❒	❒	❒
webwasher	❒	❒	❒	❒	❒	❒	❒
Weitere: _____	❒	❒	❒	❒	❒	❒	❒

VI. Abschlussfrage

30. Welche Herausforderungen sehen Sie im Zusammenhang mit dem Thema IT-Security für die Unternehmen Ihrer Branche in den nächsten Jahren?

Herzlichen Dank für Ihre Teilnahme an der Befragung!