

Strategie, Organisation, Prozesse und Systeme

Cloud Computing

Navigation in der Wolke

Cloud Computing

Navigation in der Wolke

Cloud Computing

Navigation in der Wolke

Herausgegeben von PricewaterhouseCoopers AG

Von Markus Vehlow und Cordula Golkowsky

Unter Mitarbeit von Eiko Ermold, Marius Fetzberger, Juri Frommer, Martin Glaser, Andreas Gorholt, Joachim Mohs, Dirk Nippert, Christian Schmidt, Alexia Spieler, Konrad Wachowiak und Falko Wendt.

Gesamtkonzeption, Durchsteuerung und Auswertung der telefonischen Befragung
denkstelle hamburg

Unabhängiges Marktforschungsinstitut für die telefonische Befragung
C.M.R. Institut für Communication- & Marketing-Research

Layout
Schölzel, Möhring GmbH, Frankfurt am Main

Druck
Kohlhammer und Wallishauser GmbH, Hechingen

Alle Rechte vorbehalten. Vervielfältigungen, Mikroverfilmung, die Einspeicherung und Verarbeitung in elektronischen Medien sind ohne Zustimmung des Verlags nicht gestattet.

Die Ergebnisse der Umfrage und Expertenbeiträge sind als Hinweis für unsere Mandanten bestimmt. Für die Lösung einschlägiger Probleme greifen Sie bitte auf die angegebenen Quellen und die Unterstützung der in dieser Publikation genannten Ansprechpartner zurück.

Meinungsbeiträge geben die Auffassung der Autoren wieder.

Printed in Germany

Vorwort

Sehr geehrte Leserinnen und Leser,

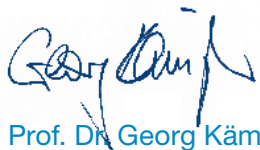
Technik und Innovation bewirken einen stetigen Wandel unserer Gesellschaft und bestimmen den Alltag in einer zunehmend digitalisierten Lebenswelt. Technische Entwicklungen bilden dabei eine unverzichtbare Basis für private und geschäftliche Aktivitäten. Darüber hinaus sind sie elementare Bestandteile heutiger Kommunikation und helfen dabei, Arbeitsabläufe effizienter und wirtschaftlicher zu gestalten. Kürzlich hat ein neuer Akteur das Parkett unserer Geschäftswelt betreten, der Unternehmen dabei unterstützt, diese Aufgabe erfolgreich zu lösen. Es handelt sich um Cloud Computing.

Mittels Cloud Computing sind Unternehmen in der Lage, IT-Leistungen bedarfsorientiert und flexibel zu beziehen, um damit den dynamischen Anforderungen ihrer Märkte optimal zu begegnen. Die IT wird dazu befähigt, auf Anforderungen der Unternehmenswelt schnell und flexibel zu reagieren. So lassen sich Kosten einsparen und Kapazitäten effektiver nutzen. Diese lukrativen Möglichkeiten bergen jedoch auch eine Vielzahl von Risiken und Herausforderungen. Nur wer diese kennt und beachtet, profitiert von Cloud Computing in vollem Umfang.

In dieser Studie hat PricewaterhouseCoopers (PwC) die wesentlichen Herausforderungen für Cloud Computing in Deutschland identifiziert. Sie reichen von Vertragsgestaltung, Datenmigration, Risiken und Compliance über einen ausreichenden Datenschutz bis hin zur Informationssicherheit.

Die Ergebnisse veranschaulichen, wie Cloud-Anbieter den aktuellen Anforderungen des Marktes begegnen. Sie bieten einen Überblick darüber, welche Risiken und Herausforderungen Cloud-Provider zu meistern haben und zeigen, was sie tun müssen, um ihren Kunden eine erfolgreiche und gewinnbringende Nutzung von Cloud-Services zu ermöglichen.

Eine erkenntnisreiche und informative Lektüre wünschen Ihnen



Prof. Dr. Georg Kämpfer



Markus Vehlow



Cordula Golkowsky

Inhalt

Vorwort.....	5
Abbildungsverzeichnis	8
Abkürzungsverzeichnis	11
Zusammenfassung.....	12
Methodik der Studie.....	15
Informationen zu den Anbietern.....	16
A Ausgangssituation.....	22
B Vorstellung der Studienergebnisse	27
1 Vertragsgestaltung	27
2 Datenmigration.....	32
3 Risiken und Compliance.....	36
4 Datenschutz	40
5 Informationssicherheit.....	45
6 Ausblick.....	50
Stichwortverzeichnis	54
Ansprechpartner	58

Abbildungsverzeichnis

Abb. 1	Funktion der Befragten im Unternehmen.....	16
Abb. 2	Anzahl der Mitarbeitenden in Deutschland.....	16
Abb. 3	Mitarbeitende im Cloud-Service-Bereich	17
Abb. 4	Nettogesamtumsatz im letzten Geschäftsjahr.....	17
Abb. 5	Anteil der Cloud-Services am Gesamtgeschäft in Deutschland	18
Abb. 6	Differenzierung nach Kundengruppen in Deutschland	18
Abb. 7	Branchenzugehörigkeit der Kunden.....	19
Abb. 8	Arten von Cloud-Computing-Services im Angebot der befragten Provider	19
Abb. 9	SaaS-Lösungen im Angebot der befragten Unternehmen	20
Abb. 10	Unterstützte Cloud-Formen	21
Abb. 11	Einschätzung der Cloud-Strategie der Kunden	24
Abb. 12	Wesentliche Faktoren für die Kundenzufriedenheit	24
Abb. 13	Herausforderungen des Cloud-Computing-Marktes.....	25
Abb. 14	Kündigungsfristen	29
Abb. 15	Zusatzkosten nach Vertragsende.....	29
Abb. 16	Zugesicherte Serviceverfügbarkeit	30
Abb. 17	Cloud-Chaining – Inanspruchnahme von Unterauftragnehmern	30
Abb. 18	Unterstützung der Datenmigration bei Neukunden	34
Abb. 19	Unterstützung der Datenmigration bei Kündigung.....	34
Abb. 20	Compliance-Management.....	38
Abb. 21	Herausforderungen bei der Erfüllung der Compliance- Anforderungen.....	38
Abb. 22	Lokation der Daten	43
Abb. 23	Kundenanfragen zum Datenschutz und Reaktion der Anbieter	43

Abb. 24	Gewährleistung der Informationssicherheit für den Nutzer	47
Abb. 25	Aspekte der Informationssicherheit	48
Abb. 26	Vereinbarung von Notfallplänen	49
Abb. 27	Umsatztendenz mit Cloud-Services	51
Abb. 28	Einschätzungen der Markttrends	52

Abkürzungsverzeichnis

BDSG	Bundesdatenschutzgesetz
IEC	International Electrotechnical Commission
ISMS	Information Security Management System
ISO	International Organization for Standardization
MuK	Medien und Kommunikation
SaaS	Software as a Service
SLA	Service Level Agreement

Zusammenfassung

Motivation und Vorgehensweise

Was vor wenigen Jahren noch undenkbar erschien, bildet heute ein attraktives Implementierungs- und Betriebsmodell für viele Unternehmen und deren IT: Cloud Computing – auch als „IT aus der Steckdose“ bezeichnet. Die Vorteile, wie beispielsweise erhöhte Flexibilität, Business-Agilität, Komplexitätsreduktion, verbrauchsabhängige Bezahlung und hohe Skalierbarkeit, liegen klar auf der Hand. Allerdings stehen Provider und Nutzer noch vor einer Vielzahl von Fragen. Zu den Ansichten der Nutzer gibt es bereits eine Reihe nationaler und internationaler Studien. Die Perspektive der Provider wurde bisher selten aufgegriffen.

Um ein aktuelles Stimmungsbild der Provider in Deutschland zu zeigen, haben wir diese zu den derzeitigen Herausforderungen von Cloud Computing befragt. Die in der Studie dargelegten Kernthemen hatten wir zuvor im Rahmen einer Marktrecherche ermittelt. Mittels einer Vielzahl von Vorgesprächen mit Vertretern ausgewählter Provider wurden diese Schwerpunktthemen in unserem Fragebogen verprobt und verifiziert. Die 51 Befragten sind vornehmlich strategisch (mit-)verantwortliche Führungskräfte in den Anbieterunternehmen.

Informationen zu den Anbietern

An unserer Studie haben sowohl kleine und mittlere als auch große Anbieter teilgenommen. Das Verhältnis der Cloud-Services zum Gesamtgeschäft unterscheidet sich stark von Anbieter zu Anbieter. Einige, überwiegend junge Unternehmen, sind ganz auf Cloud-Services spezialisiert. Dabei handelt es sich überwiegend um kleinere Provider. Größere Unternehmen hingegen haben im Verhältnis zum gesamten Lösungsspektrum oft nur einen geringen Anteil an Cloud-Services in ihrem Portfolio.

Durchschnittlich bietet jeder der befragten Anbieter drei Cloud-Dienstleistungen im deutschen Markt an. Mehr als drei Viertel der Befragten bieten Software as a Service (SaaS), jedes zweite Unternehmen Infrastructure as a Service (IaaS) und zwei von fünf Platform as a Service (PaaS) an. Dabei fällt auf, dass vor allem die klassischen Unterstützungsprozesse (Einkauf, Verkauf, Personal, Rechnungswesen etc.) durch SaaS-Lösungen bereits abgebildet werden. Eine kaufmännische Relevanz ist bei der überwiegenden Mehrzahl der Lösungen gegeben. Business Process as a Service (BPaaS) spielt die kleinste Rolle und wird nur von einem Viertel der Befragten angeboten.

Die Hälfte der Befragten bietet ihre Lösungen ausschließlich in Private-Cloud-Umgebungen an, ein weiteres Viertel bietet sie in Public-Cloud-Umgebungen. Wiederum ein Viertel der Befragten offeriert beide Formen der Implementierung.

Informationen zu den Kunden der Anbieter

Auffällig ist, dass Nutzer aller Unternehmensgrößen in nahezu gleichem Ausmaß Cloud-Services von den befragten Anbietern beziehen. Diese scheinen aktuell in allen Branchen gefragt. Dies erklärt sich dadurch, dass die bestehenden Cloud-Services auf Grund ihrer Ausrichtung auf Sekundärprozesse größtenteils branchenunabhängig eingesetzt werden können.

Nach Einschätzung der befragten Provider sind umfassende Cloud-Strategien bei den Nutzern trotz hohem Interesse noch nicht sehr

ausgereift. Nutzer suchen vielmehr nach Lösungen für einzelne, konkrete Probleme, und schaffen somit Referenzen bzw. Pilotanwendungen. Eine umfassende Cloud-Strategie, die mit der IT-Strategie harmonisiert ist, haben bisher nur wenige Nutzer etabliert.

In der Befragung stechen drei Themenblöcke besonders hervor: Die Informationssicherheit muss garantiert, der Datenschutz gewährleistet und die Compliance erreicht werden. Die Lösungen für diese Aufgaben sind nach Angabe der Befragten sowohl wichtige Faktoren für die Kundenzufriedenheit als auch große Herausforderungen für die Provider.

Informationssicherheit, Datenschutz und Compliance sind wichtig für Nutzer und Provider

Als wichtigste Aufgabe, um die Informationssicherheit der Kundendaten zu gewährleisten, nannten die Anbieter die Durchführung detaillierter Risikoanalysen und an zweiter Stelle die Zertifizierung der eigenen Informationssicherheit. Knapp dahinter rangierten Security Penetration Tests, die Anpassung der Sicherheitskonzepte sowie Nutzer-Audits durch externe Dritte. Über die Hälfte der Befragten vereinbart mit den Nutzern Notfallpläne für den Katastrophenfall bzw. für Vorkommnisse im Sicherheits- oder Datenschutzbereich. Knapp ein Drittel vereinbaren keine Notfallpläne.

Auch über die zweite genannte Herausforderung – den Datenschutz – haben wir mit den Anbietern gesprochen. Wir fragten, an welchen Standorten sie die ihnen anvertrauten Kundendaten speichern und verarbeiten und welche Maßnahmen sie zu deren Schutz ergreifen. Gut jeder Zweite nutzt Rechenzentren in Deutschland. Allerdings speichert nur knapp ein Drittel der Anbieter seine Daten ausschließlich in Deutschland, was die Gewährleistung des Datenschutzes vereinfachen würde. Die großen Anbieter überlassen ihren Kunden häufiger als kleinere Anbieter die Entscheidung, ob ihre Daten ausschließlich in Deutschland oder auch im Ausland gespeichert werden dürfen. Etwas über die Hälfte aller Provider wurde bereits von ihren Kunden gefragt, welche technischen und organisatorischen Maßnahmen zum Datenschutz sie getroffen haben (Anfragen zum § 11 des Bundesdatenschutzgesetzes). Ebenso viele Provider besitzen nach eigenen Angaben ein formalisiertes Standardverfahren, um auf Datenschutzanfragen dieser Art zu reagieren.

Um Risiken und Compliance im Griff zu haben, wurde bei vier von fünf Anbietern ein eigenes Compliance-Managementsystem etabliert. Als wichtigste Herausforderung bei der Compliance nennen die Befragten das Problem, die Compliance-Anforderungen der Nutzer überhaupt zu identifizieren. Fast ebenso große Herausforderungen liegen darin, branchenspezifische Erfordernisse zu erfüllen, Compliance-Nachweise zu erbringen oder ein internes Kontrollsystem zu implementieren.

Um Kundendaten sicher und reibungslos in die Cloud zu überführen, bieten zwei von fünf Providern ihren Nutzern kostenpflichtige Zusatzservices an. Kostenlose Migrationstools oder Funktionen hierzu bietet nur ein Fünftel der Befragten an. Nur drei von fünf Befragten regeln die Datenrückgabe per Vertrag. Hierbei sind die kleineren Anbieter in der Mehrzahl.

Rein in die Cloud, raus aus der Cloud

Zur Vertragsgestaltung in der Cloud ergibt die Befragung folgendes Bild: Jeder zweite Anbieter bietet Verträge mit fester Monatslaufzeit und entsprechender Kündigungsfrist. Nur ein Anbieter entlässt Kunden innerhalb von 24 Stunden aus einem bestehenden Vertrag. Trotz der angepriesenen Flexibilität von Cloud Computing haben die Provider noch

Augen auf bei der Vertragsgestaltung!

häufig lange Kündigungsfristen. Allerdings ist zu berücksichtigen, dass gut ein Drittel der Befragten eine Public-Cloud-Lösung anbietet. Hier sind die technischen Möglichkeiten am größten, kurze Kündigungsfristen zu realisieren.

Ein Viertel der Befragten stellen ihren Kunden nach der Kündigung des Vertrags Zusatzkosten in Rechnung. In puncto Serviceverfügbarkeit ist es erstaunlich, dass ein Viertel der Befragten die Serviceverfügbarkeit nicht vertraglich festlegt. Insgesamt garantieren kleinere Anbieter eine geringere Serviceverfügbarkeit als größere Anbieter.

Rund zwei von fünf Providern nutzen Unterauftragnehmer. Weniger als ein Zehntel besitzt keine eigenen Ressourcen für Cloud-Dienstleistungen und nutzt ausschließlich Unterauftragnehmer zur eigenen Service-Erbringung. Praktisch alle Anbieter, die Unterauftragnehmer nutzen, informieren ihre Kunden darüber. Wir haben die Teilnehmer auch gefragt, wie flexibel sie bei der Vereinbarung von Service Level Agreements (SLAs) agieren. Die große Mehrheit der Unternehmen bieten ihren Kunden neben den Standard-services auch individuell konfigurierte Services an.

Cloud Computing ist stark im Aufwind

Knapp drei Viertel der Anbieter gehen davon aus, dass der Anteil der Cloud-Services an ihrem Gesamtgeschäft in Deutschland mittelfristig steigen wird. Keiner der Befragten erwartet, dass dieser Anteil sinkt. Die Mehrheit der Anbieter erwartet, dass Cloud Computing das Vendor-Management und die damit verbundene Providersteuerung vor neue Herausforderungen stellen wird. Insbesondere die stärker spezialisierten Provider glauben, dass das internetbasierte Arbeiten zur Regel wird und dass die Integrierbarkeit und Kombinierbarkeit der Cloud-Angebote immer wichtiger werden. Um einzelne Cloud-Dienstleistungen miteinander zu integrieren, ist eine Standardisierung der verschiedenen Services unbedingt erforderlich.

Methodik der Studie

Bei dieser Studie kam ein Drei-Stufen-Modell zum Einsatz: Im ersten Schritt wurden acht Telefoninterviews durchgeführt, um den Fragebogen im Hinblick auf eine Optimierung zu verproben. Die anschließende Feldphase bestand aus 51 Telefoninterviews. Sie wurden von einem unabhängigen Marktforschungsinstitut als CATI-Befragung (Computer Aided Telephone Interviews) durchgeführt. Das Marktforschungsinstitut stellt den Datenschutz und die Anonymität der Befragten sicher. Die Feldphase fand vom 25. August bis zum 7. September 2010 statt.

Ergänzend zur telefonischen Erhebung führte PwC zehn Experten-gespräche mit Anbietern im deutschen Cloud-Computing-Markt. Passagen aus diesen Gesprächen werden im Kapitel „Vorstellung der Studienergebnisse“ zur Illustration der Ergebnisse zitiert.

Die Expertengespräche wurden in der Zeit vom 22. September bis zum 5. Oktober 2010 geführt.

Die Gruppe der Befragten setzte sich vornehmlich aus strategisch (mit-) verantwortlichen Führungskräften in den Anbieterunternehmen zusammen.

Die erhobenen Daten wurden für grobe qualitative Trendaussagen unter anderem nach folgenden Aspekten analysiert:

- Den Anbietern mit bis zu 499 Mitarbeitenden in Deutschland wurden Anbieter mit 500 und mehr Mitarbeitenden gegenübergestellt. Diese Vergleichsgruppen werden in der Ergebnisdarstellung als „kleinere Anbieter“ und „größere Anbieter“ bezeichnet.
- Auch die Antworten nach der Kundenstruktur der Anbieter wurden ausgewertet. Anbieter, die hauptsächlich kleinere Unternehmen als Kunden haben, wurden gesondert von jenen betrachtet, zu deren Kunden hauptsächlich Großunternehmen mit mehr als 2.000 Mitarbeitenden in Deutschland zählen.
- Bei der Betrachtung des Anteils der Cloud-Services am Gesamtgeschäft der Anbieter werden größere Anbieter, deren Cloud-Anteil am Gesamtgeschäft weniger als 10 % beträgt, kleineren Anbietern gegenübergestellt, die einen höheren Anteil an Cloud-Services in ihrem Portfolio haben.

Die Grundgesamtheit der Studie bilden Anbieter im deutschen Cloud-Computing-Markt. Im Rahmen unserer Befragung ergab sich eine Ausschöpfungsquote von 71 %.

Die nachfolgenden grafischen Darstellungen beziehen sich auf das Stichprobentotal von $n=51$, sofern nicht explizit anders erwähnt.

Informationen zu den Anbietern

In welcher Funktion sind Sie tätig?

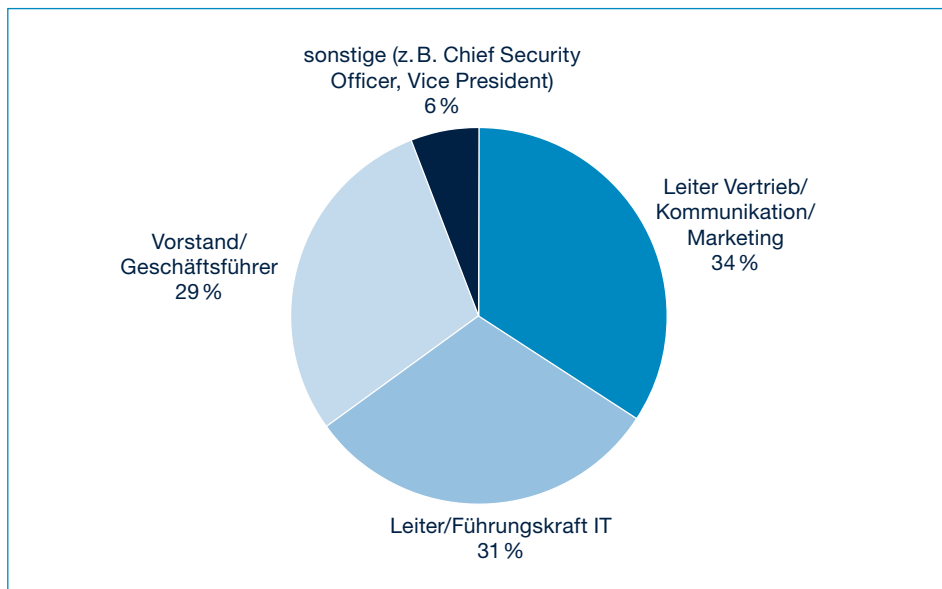


Abb. 1 Funktion der Befragten im Unternehmen

Bei den 51 Gesprächspartnern handelt es sich um strategisch (mit-) verantwortliche Führungskräfte von Cloud-Computing-Providern im deutschen Markt.

Wie viele Mitarbeitende beschäftigt Ihr Unternehmen in Deutschland?

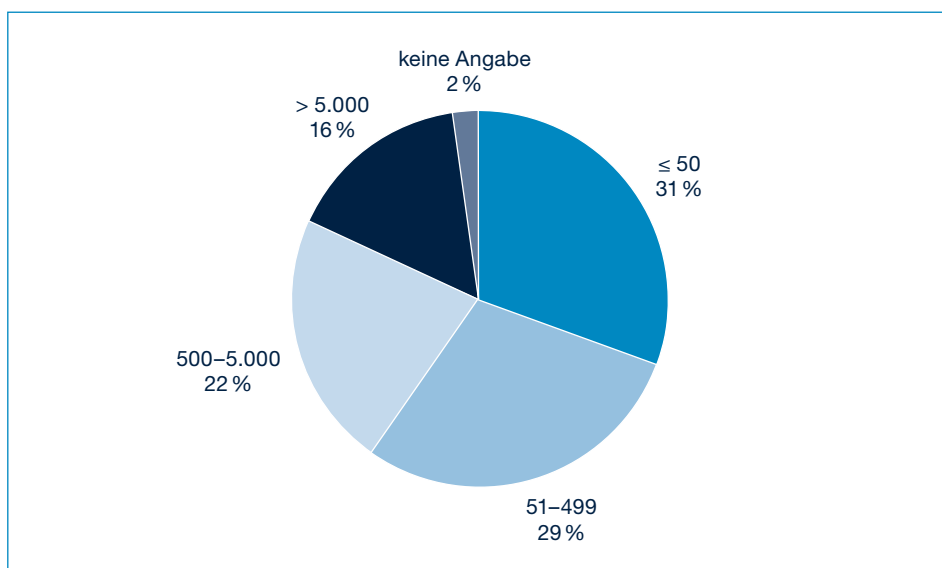
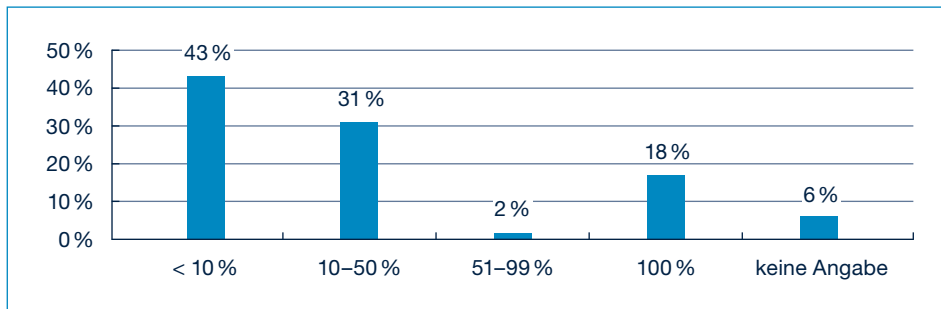


Abb. 2 Anzahl der Mitarbeitenden in Deutschland

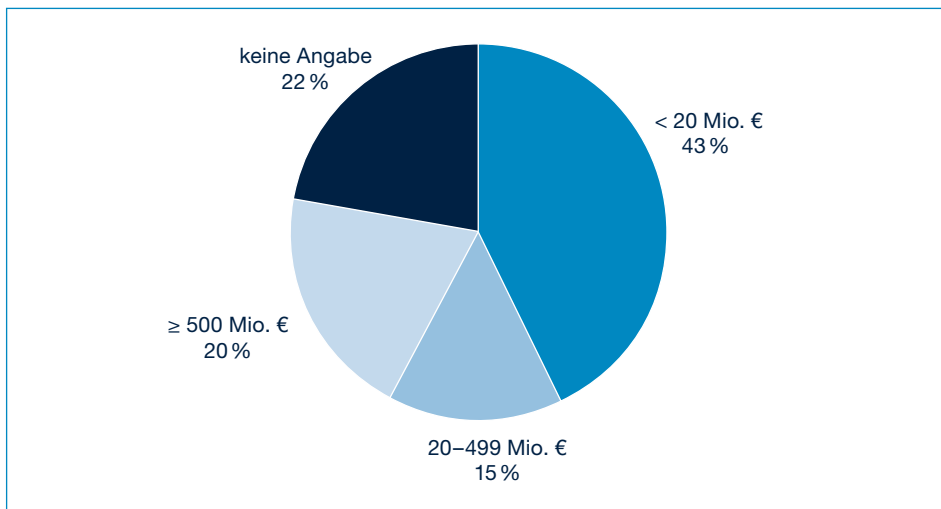
Um die Unternehmensgröße zu schätzen, wurde die Mitarbeiterzahl in Deutschland erfragt. 60 % der Cloud-Anbieter beschäftigen weniger als 500 Mitarbeitende in Deutschland. Knapp 40 % der Befragten beschäftigen mehr als 500 Mitarbeitende.



Wie viele Mitarbeitende beschäftigt Ihr Unternehmen in Deutschland in Cloud-Service-Bereichen?

Abb. 3 Mitarbeitende im Cloud-Service-Bereich

Zusätzlich fragten wir nach dem Anteil der Mitarbeitenden, die in Cloud-Service-Bereichen in Deutschland arbeiten. Hier ergibt sich ein sehr differenziertes Bild. Bei 43 % der Anbieter liegt dieser Anteil derzeit noch unter 10 %. Ein knappes Drittel der Anbieter beschäftigt 10 bis 50 % ihrer Mitarbeitenden in Cloud-Service-Bereichen. Nicht verwunderlich ist, dass kleinere Anbieter proportional mehr Mitarbeitende im Bereich Cloud Computing beschäftigen als größere Anbieter. Derzeit hat sich keiner der größeren Anbieter zu 100 % auf Cloud-Services spezialisiert.



Wie hoch war der Nettogeschäftsumsatz Ihres Unternehmens in Deutschland im letzten Geschäftsjahr?

Abb. 4 Nettogeschäftsumsatz im letzten Geschäftsjahr

Ein Fünftel der Anbieter erreichte im letzten Jahr mehr als 500 Millionen Euro Gesamtumsatz in Deutschland. 15 % gaben einen Umsatz von 20 bis unter 500 Millionen Euro an. Bei 43 % lag der Umsatz unter 20 Millionen Euro. Es waren hauptsächlich kleinere Anbieter, die keine Angaben zur Frage nach ihrem Nettoumsatz machten. Welche Anteile Cloud-Services am Nettogeschäftsumsatz der Anbieter ausmachten, zeigt die folgende Grafik.

Wie hoch ist der Anteil Ihrer Cloud-Services am Gesamtgeschäft in Deutschland?

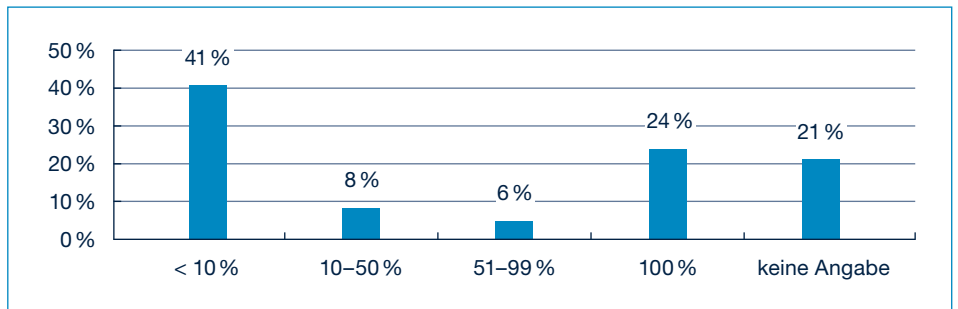


Abb. 5 Anteil der Cloud-Services am Gesamtgeschäft in Deutschland

Auch beim Anteil der Cloud-Services am Gesamtgeschäft der Befragten in Deutschland ergibt sich ein sehr differenziertes Bild. Einige Befragte bieten zu 100 % Cloud-Services an, bei anderen beträgt deren Anteil im Geschäftsportfolio weniger als 10 %. Einen Anteil zwischen 10 und 99 % geben nur sieben Befragte an. Bei einem knappen Viertel der Anbieter machen Cloud-Services 100 % des Geschäftsportfolios aus. Nur kleinere Anbieter fokussieren sich ausschließlich auf Cloud Computing.

Kunden welcher Größe beziehen vorwiegend Cloud-Dienstleistungen?

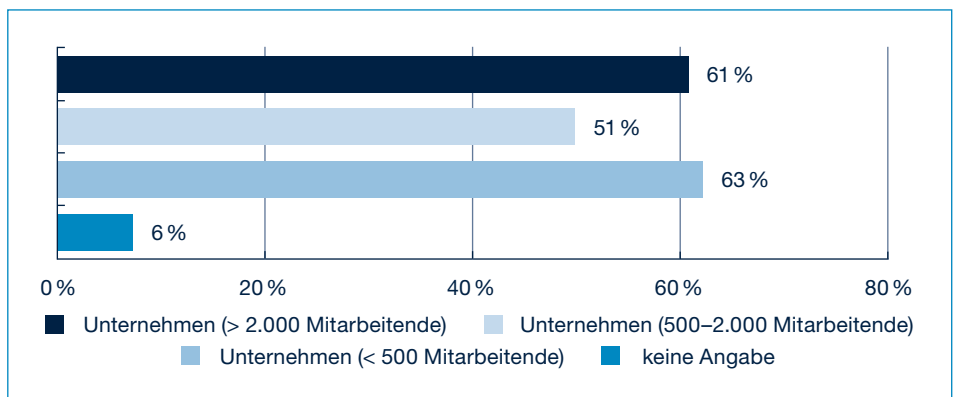
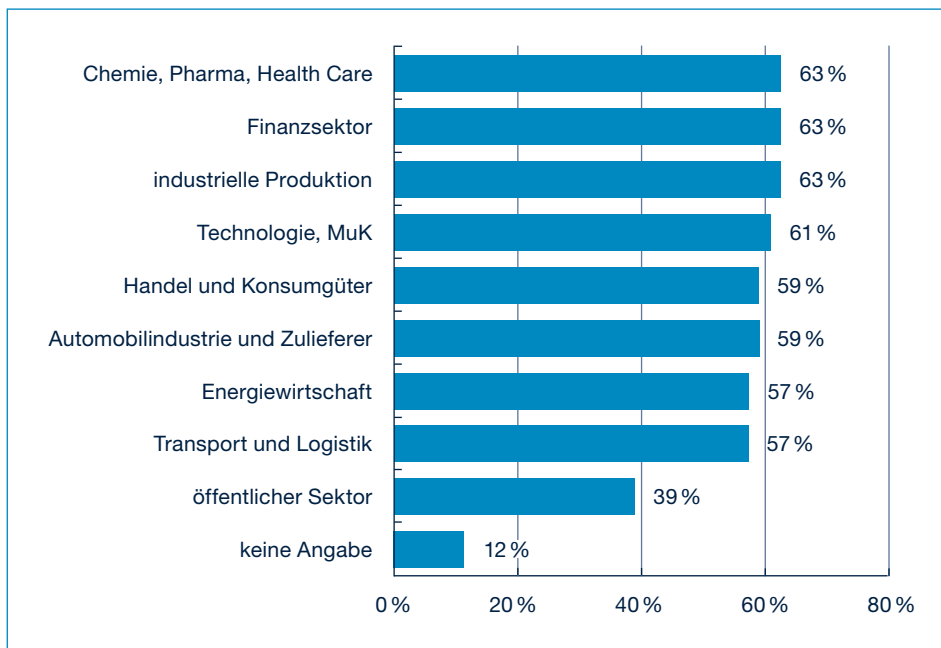


Abb. 6 Differenzierung nach Kundengruppen in Deutschland

Es fällt auf, dass Unternehmen aller Größenordnungen in nahezu gleichem Maße Cloud-Services beziehen. Dies überrascht, da Cloud Computing oft nachgesagt wird, es rechne sich besonders für den Mittelstand und größere Unternehmen würden erst später nachziehen.

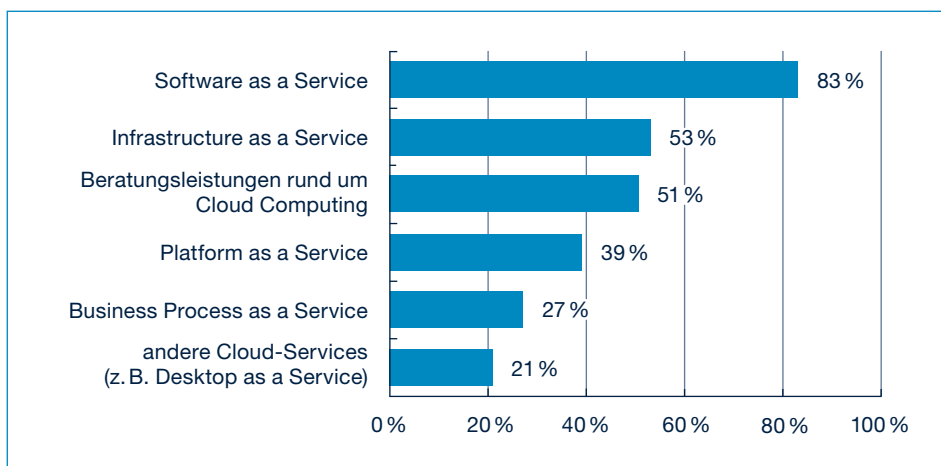
Auf die Frage nach der hauptsächlichen Kundengruppe gaben 42 % der Provider an, dass sie Unternehmen mit mehr als 2.000 Mitarbeitenden bedienen. 23 % der Teilnehmer gaben an, dass zu ihrer hauptsächlichen Kundengruppe Unternehmen zwischen 500 und 2.000 Mitarbeitenden zählen. Ein Drittel der Befragten versorgt Unternehmen mit weniger als 500 Beschäftigten mit Cloud-Dienstleistungen.



Aus welchen Branchen kommen Ihre Cloud-Kunden hauptsächlich?

Abb. 7 Branchenzugehörigkeit der Kunden

Durchschnittlich gaben die Befragten fünf Branchen an, für die ihr Haus tätig ist. Dies liegt im Wesentlichen daran, dass zahlreiche Cloud-Services branchenübergreifend eingesetzt werden können (hauptsächlich im Bereich von Unterstützungsprozessen – vgl. hierzu auch Abbildung 9). Die nahezu gleiche Verteilung der Nennungen über alle Branchen hinweg stützt diese Einschätzung. Unsere Stichprobe zeigt, dass es derzeit offensichtlich nur wenige rein branchenorientierte Lösungen am Markt gibt.



Welche Art von Cloud-Computing-Services erbringt Ihr Unternehmen?

Abb. 8 Arten von Cloud-Computing-Services im Angebot der befragten Provider

Jeder der befragten Anbieter bietet durchschnittlich drei Cloud-Dienstleistungen im deutschen Markt an. Der Schwerpunkt liegt deutlich auf Software as a Service. Jeder zweite Befragte bietet Infrastructure-as-a-Service-Leistungen an. Ebenfalls die Hälfte der Befragten bietet allgemeine Beratungsleistungen rund um das Thema Cloud Computing an. Business Process as a Service hat dagegen nur jeder vierte Anbieter im Portfolio.

Software, Platform und Infrastructure as a Service spielen erwartungsgemäß unter Umsatzgesichtspunkten die wichtigsten Rollen. Business Process as a Service stellt bisher bei keinem der Befragten die umsatzstärkste Dienstleistung dar. Hier wird aber mit einem Anstieg in den nächsten Jahren gerechnet.

Welche SaaS-Lösungen bietet Ihr Unternehmen an?

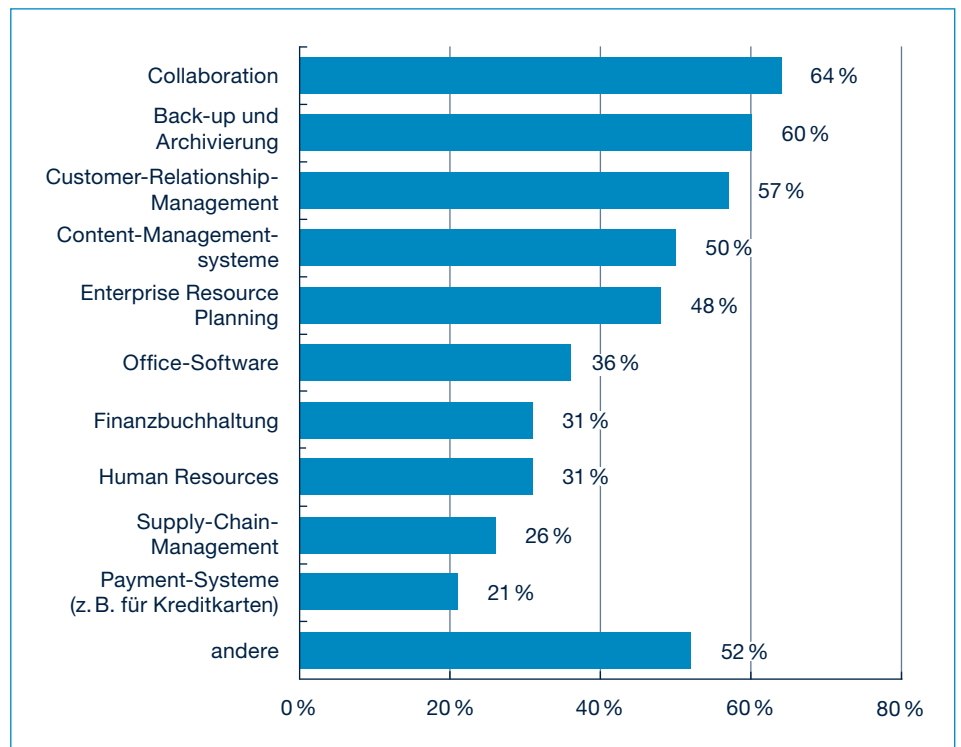
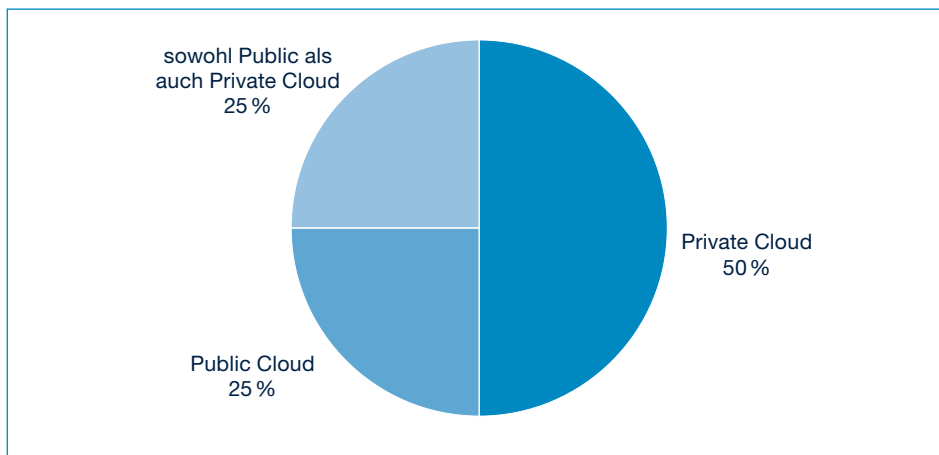


Abb. 9 SaaS-Lösungen im Angebot der befragten Unternehmen

Die Anbieter, die Software-as-a-Service-Dienstleistungen erbringen, bieten durchschnittlich fünf verschiedene Lösungen an. Auffällig ist, dass eine Vielzahl der klassischen Unterstützungsprozesse (Einkauf, Verkauf, Personal, Rechnungswesen, etc.) bereits durch SaaS-Lösungen abgebildet werden kann. Über die Hälfte der SaaS-Provider hat noch andere Dienstleistungen im Portfolio. Dabei handelt es sich im Wesentlichen um Unified Communication (rund 29 %), Business Intelligence (rund 23 %), Security (rund 18 %) und E-Commerce (rund 11 %). In Einzelnennungen wurden Marketing, Dokumentenerkennung (OCR), Disaster Recovery und Compliance angeführt. Es ist zu beobachten, dass vor allem kleinere Anbieter eine Nischenstrategie verfolgen.



In welcher Form bietet Ihr Unternehmen Cloud-Lösungen an?

Abb. 10 Unterstützte Cloud-Formen

Ein Viertel der Cloud-Lösungen wird über das Internet angeboten (Public Cloud). Die Hälfte der bezogenen Cloud-Services wird entweder von den Kunden selbst oder von einem Provider in einer für den Kunden exklusiv bereitgestellten Umgebung implementiert und betrieben (Private Cloud). Die restlichen Lösungen werden sowohl in Form von Private Clouds als auch in Form von Public Clouds angeboten.



Ausgangssituation

Cloud Computing ermöglicht Unternehmen den Bezug von IT-Ressourcen per Internet – flexibel, wirtschaftlich, nahezu unbegrenzt und effizient bei verbrauchsabhängiger Bezahlung. Dadurch müssen Rechnerkapazitäten, Datenspeicher und Anwendungen nicht mehr ständig bzw. in vollem Umfang von den Unternehmen vorgehalten und betrieben werden. Dies bietet, neben Kapazitäts-, Investitions- und Kostenreduktionen, vor allem neue Gestaltungsmöglichkeiten für die Fachabteilungen.

Cloud Computing ist ein Paradigma, das die Geschäftsmodelle, Prozesse und IT der Unternehmen nachhaltig verändern wird

Auch wenn die zugrundeliegenden Technologien nicht neu sind, werden die Auswirkungen der Weiterentwicklung sowohl für die Anbieter als auch die Anwender von IT-Dienstleistungen voraussichtlich immens sein. Cloud Computing kann nicht nur die Basis für völlig neue Vertriebs- und Nutzungswege von IT-Leistungen schaffen, sondern auch den Boden bereiten für völlig neue Prozesse und Geschäftsmodelle. Unbestritten scheinen diese Zukunftsaussichten äußerst lukrativ zu sein. Allerdings stehen sowohl Nutzer als auch Provider vor diversen Herausforderungen, um Cloud Computing erfolgreich anzubieten oder zu nutzen. Dabei gestalten sich diese Fragen unterschiedlich für Nutzer und Provider.

Nutzer müssen sich folgende Fragen stellen:

- Für welche Zwecke, Prozesse oder Anwendungen lohnen sich Cloud-Services im Unternehmen?
- Sind dem Unternehmen alle potenziellen Risiken der Services bekannt?
- Wie soll der Cloud-Anbieter gesteuert und überwacht werden (Sourcing Governance)?
- Welche Voraussetzungen müssen gegeben sein, um Cloud-Leistungen in die bestehende IT-Landschaft zu integrieren?
- Welche Kriterien sind entscheidend für die optimale Auswahl eines Cloud-Anbieters?

Für Anbieter ergeben sich die folgenden Kernfragen:

- Welche Compliance- und Sicherheitsanforderungen der Nutzer sollten Anbieter erfüllen?
- Wie ist der Datenschutz bei länderübergreifender Datenspeicherung zu gewährleisten?
- Wie sind Datenmigration, Archivierung und Rückgabe der Kundendaten zu regeln?
- Welche vertraglichen Implikationen ergeben sich aus den eigenen Vorgehensweisen und Geschäftsmodellen?

Kurz: Anbieter und Nutzer haben das Potenzial, aber auch die Herausforderungen von Cloud Computing erkannt und arbeiten derzeit an Integrationskonzepten und Lösungsstrategien. Um zu erfahren, wie gut die Nutzer für den Einsatz von Cloud-Services gerüstet sind, haben wir die Provider gefragt, welche Schlüsse sie aus Kundenanfragen ziehen konnten.

Wie ausgereift ist die Cloud-Strategie Ihrer Kunden? Welches Bild bietet sich Ihnen in der Regel?

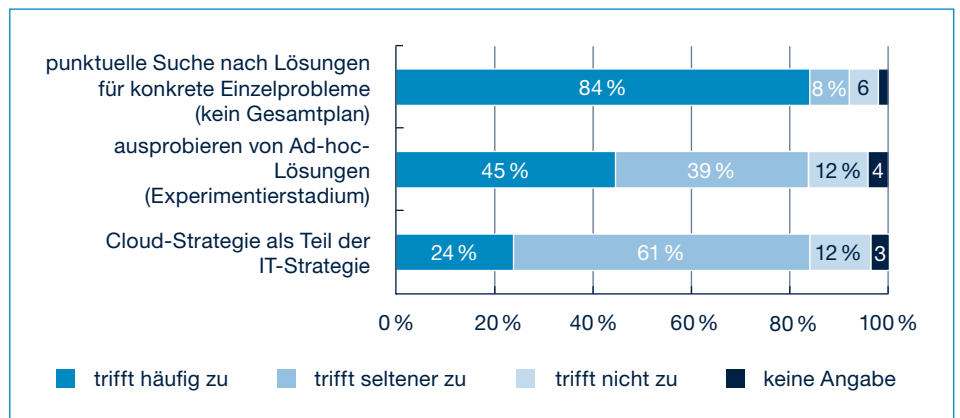


Abb. 11 Einschätzung der Cloud-Strategie der Kunden

Die Provider schätzen die Cloud-Strategie ihrer Kunden als nicht sehr ausgereift ein. Besonders häufig gehe es den Nutzern um die punktuelle Suche nach Lösungen für konkrete Einzelprobleme. Dieses Verhalten erleben die größeren Cloud-Provider tendenziell häufiger als die kleineren. Lediglich die Provider, die hauptsächlich für Großunternehmen arbeiten, erleben häufiger, dass ihre Kunden bereits eine Cloud-Strategie erarbeitet haben.

Was sind die wesentlichen Erfolgsfaktoren für die Zufriedenheit Ihrer Kunden?

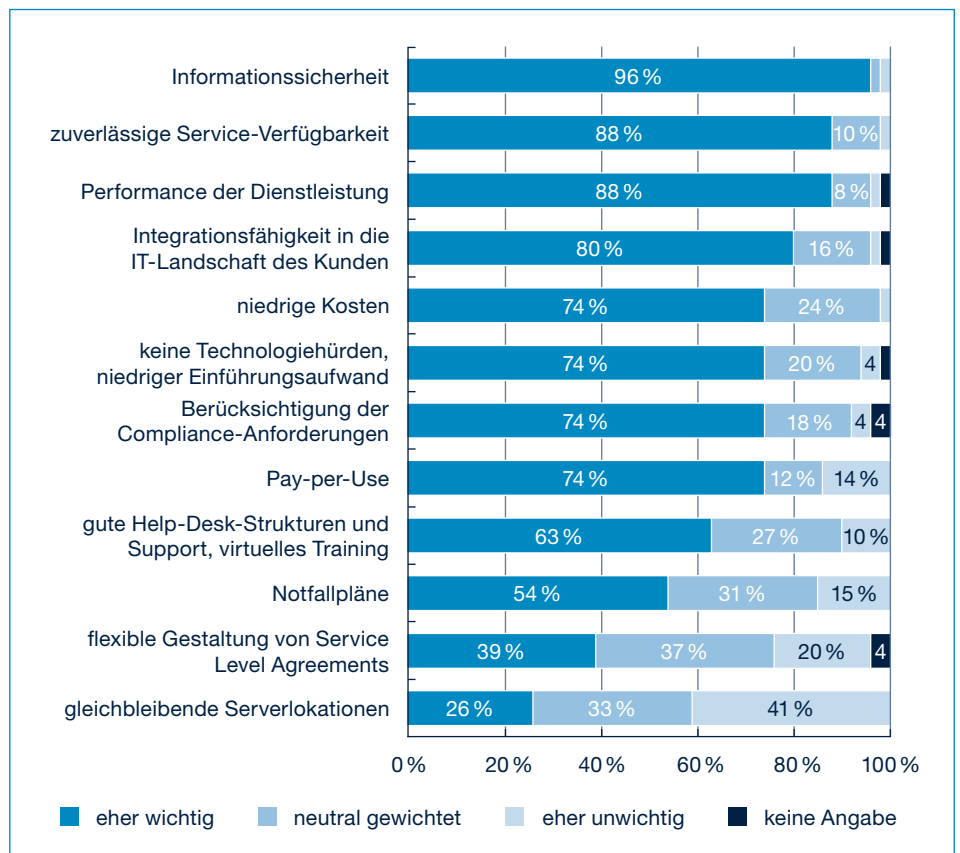


Abb. 12 Wesentliche Faktoren für die Kundenzufriedenheit

Informationssicherheit und zuverlässige Serviceverfügbarkeit sind aus Anbietersicht die wesentlichen Erfolgsfaktoren für die Kundenzufriedenheit. Wichtig sind außerdem die Performance der Dienstleistung, niedrige Kosten, geringer Einführungsaufwand und die Integrationsfähigkeit der Cloud-Dienstleistung in die IT-Landschaft des Nutzers, einhergehend mit Compliance und einer verbrauchsabhängigen Abrechnung. Notfallpläne, die flexible Gestaltung von SLAs und gleichbleibende Serverlokationen gelten als die am wenigsten wichtigen Kriterien. Aspekte, die oftmals mit den Vorteilen von Cloud Computing in Verbindung gebracht werden, wie etwa niedrige Kosten oder Pay-per-Use, zählen hier nicht zu den wichtigsten Aspekten der Kundenzufriedenheit. Des Weiteren fällt auf, dass die Aspekte „Notfallpläne“ und „gleichbleibende Serverlokationen“ an hinterer Stelle stehen. Allerdings stehen diese Faktoren in Relation zum Thema Informationssicherheit, welches an erster Stelle rangiert.

Was sind aus Sicht eines Anbieters momentan die größten Herausforderungen?

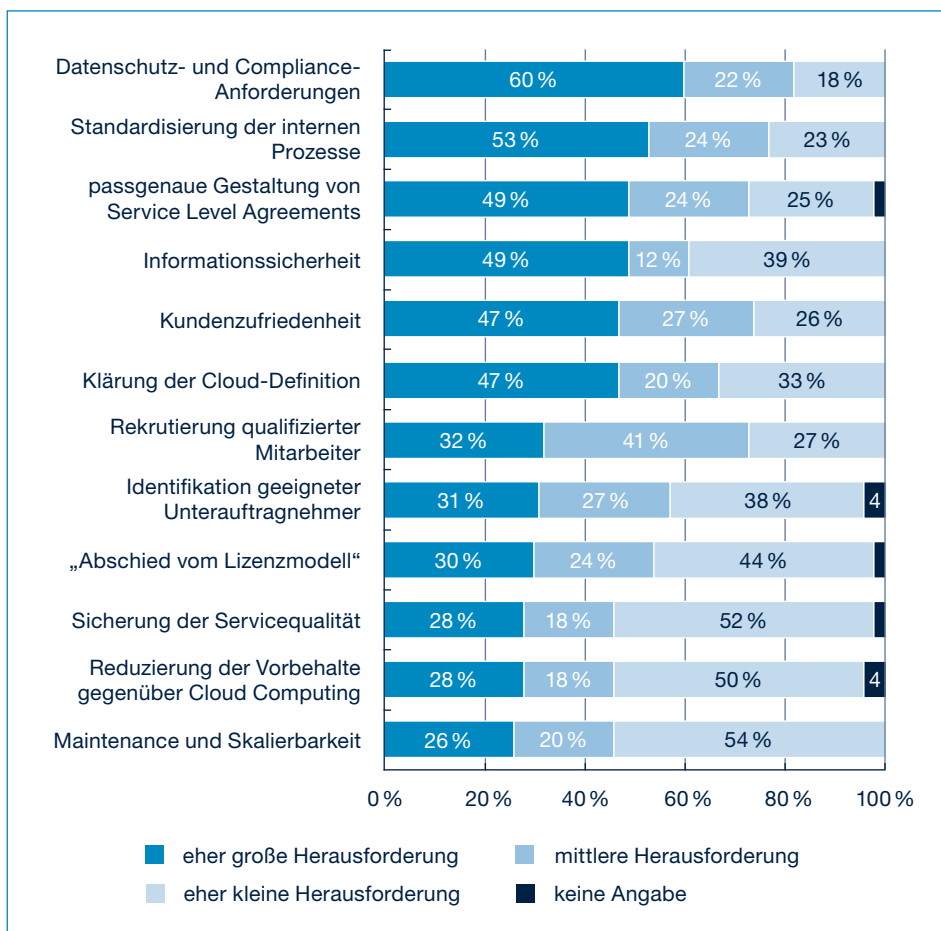


Abb. 13 Herausforderungen des Cloud-Computing-Marktes

Als die beiden größten Herausforderungen im deutschen Cloud-Computing-Markt gelten Datenschutz und Compliance sowie die Standardisierung der internen Prozesse. Letzteres überrascht angesichts der mit Cloud Computing verbundenen Skaleneffekte aufseiten der Provider. An dritter Stelle der identifizierten Herausforderungen stehen fast gleichauf die Themen: Ausgestaltung der Service Level Agreements, Informationssicherheit der Daten sowie mit leichtem Abstand die Themen Kundenzufriedenheit sowie, etwas überraschend, die Klärung der Definition von Cloud Computing. Dies liegt sicher daran, dass aktuell

außergewöhnlich viele und sich teils widersprechende Definitionen im Internet und den Fachmedien kursieren. Fehlende Standards im Markt sowie die Komplexität des Themas erschweren es den Anbietern zusätzlich, das Thema den Nutzern klar darzustellen.

Als weniger große Herausforderungen werden der „Abschied vom Lizenzmodell“, die Sicherung der Servicequalität und die Cloud-Zurückhaltung der Kunden in Deutschland empfunden. Die Aspekte Maintenance und Skalierbarkeit bilden die Schlusslichter unter den Herausforderungen. Dies spricht dafür, dass die Anbieter die technologischen Herausforderungen offenbar im Griff haben.

Es fällt auf, dass die wesentlichen Erfolgsfaktoren für die Kundenzufriedenheit (vgl. Abbildung 12) nicht identisch mit den eigenen Herausforderungen sind. So ist beispielsweise eine flexible Gestaltung der SLAs weniger wichtig für die Kundenzufriedenheit, wohl aber stellt sie eine große Herausforderung dar. Gleiches gilt für die Zuverlässigkeit der Serviceverfügbarkeit versus die Sicherung der Servicequalität. Die Themen Informationssicherheit, Datenschutz und Compliance sind sowohl wichtige Erfolgsfaktoren für die Kundenzufriedenheit als auch große Herausforderungen. Die Provider sollten sie daher mit höchster Priorität behandeln.



Vorstellung der Studienergebnisse

1 Vertragsgestaltung

Vertragsmanagement als Erfolgsfaktor

Vertragsmanagement als Grundlage des betriebswirtschaftlichen Handelns ist eine vielschichtige und komplexe Unternehmensaufgabe. Das Vertragsmanagement folgt in der Regel einem Vertragslebenszyklus: Entscheidung und Ausschreibung, Vertragsgestaltung und -verhandlung sowie Vertragsänderung und -beendigung. Die Erfahrung zeigt, dass die Vertragsgestaltung in der Praxis oft erhebliche Schwächen aufweist. Die Konsequenzen können drastisch sein. Regelungslücken führen zu Rechtsunsicherheit, unwirksame Klauseln zu erhöhtem Risiko, Verletzungen der Rechte Dritter gegebenenfalls zu Ansprüchen oder gerichtlichen Auseinandersetzungen. Verstöße gegen ordnungsrechtliche Vorschriften können zu Ordnungsmitteln und behördlichen Sanktionen führen.

Wie ich es sehe

„Ein Provider sollte zwei wesentliche Kriterien beachten, um erfolgreich zu agieren: erstens passgenaue Services gestalten nach Unternehmensgröße und Branche; und zweitens ein funktionierendes Ecosystem von Branchenpartnern aufbauen, die im Einzelfall komplementär Dienste und Services zu einer passgenauen Gesamtlösung ergänzen.“

Michael Rosbach, Vorstand, Scopevisio AG

1.1 Vertragsgestaltung und Cloud Computing

Viele Fehler werden am Anfang gemacht

Im Rahmen von Cloud Computing gestaltet sich die Vertragsgestaltung aufgrund der zugrunde liegenden innovativen Technologie als schwierig. Die Definition der Rechte und Pflichten der Vertragspartner ist im Detail anspruchsvoll. Wichtige Aspekte der Vertragsgestaltung für eine Cloud-Computing-Leistung sind unter anderem: Kündigungskonditionen, Sicherstellung der Leistungserbringung sowie die Einbeziehung von Unterauftragnehmern. Versäumt ein Cloud-Nutzer im Vorfeld des Vertragsabschlusses die Identifikation der cloud-spezifischen Risiken der Vertragsgestaltung, zum Beispiel bezüglich der lizenzrechtlichen Situation, und lässt sich allein durch die Kosteneinspareffekte treiben, so besteht die Möglichkeit, dass am Ende erheblich höhere Kosten entstehen als geplant. Die Gefahr der reinen Kostenfokussierung ist aus IT-Outsourcing-Verträgen bekannt. Beachten müssen dies sowohl die Anbieter, die ihre Standardverträge für Cloud-Computing-Leistungen AGB-konform gestalten und gegebenenfalls verhandeln müssen, als auch die potenziellen Kunden, die die vertraglichen Risiken kennen müssen, um sie bewerten zu können.

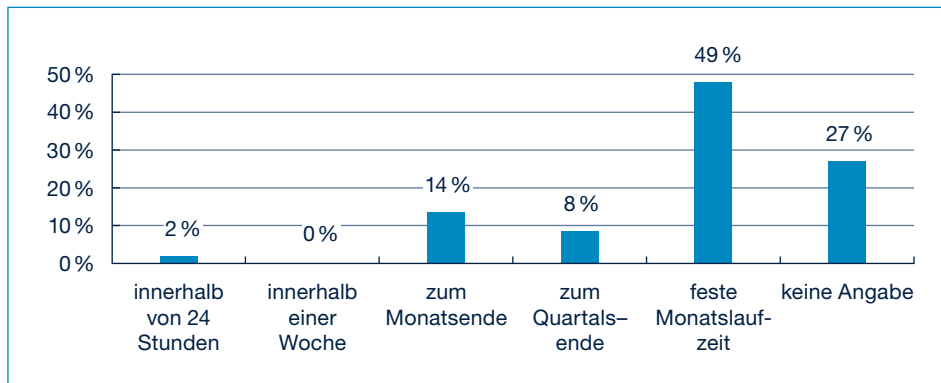
Wie ich es sehe

„Cloud ist nicht gleich Cloud: Private Cloud und Public Cloud unterscheiden sich deutlich: Pay-per-Use und Multi-Tenancy sind beispielsweise wesentliche Kennzeichen von Cloud Computing. Beides ist ausschließlich in einer Public Cloud gegeben.“

Mani Pirouz, Leiter Produktmarketing, salesforce.com Germany GmbH

PwC hat die teilnehmenden Provider hinsichtlich der Vertragsgestaltung befragt. Im Folgenden werden die Ergebnisse der Befragung dargestellt.

1.2 Umfrageergebnisse

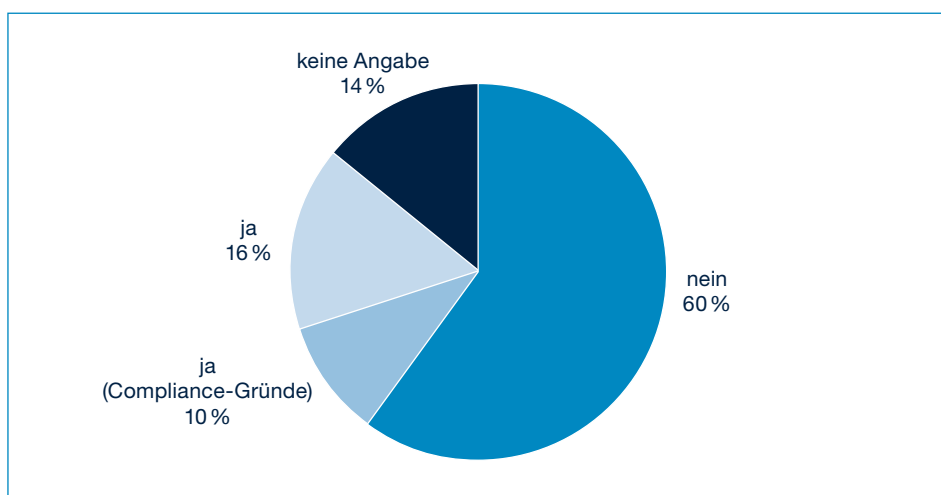


Welche Kündigungsfristen bieten Sie Ihren Kunden?

Abb. 14 Kündigungsfristen

Jeder zweite Anbieter hat Verträge mit fester Monatslaufzeit und entsprechender Kündigungsfrist. Nur ein Anbieter entlässt die Kunden innerhalb von 24 Stunden aus einem bestehenden Vertrag. Kein Provider bietet eine wöchentliche Kündigungsfrist. Trotz der angepriesenen Flexibilität von Cloud Computing bieten Provider größtenteils noch immer Kündigungsfristen aus dem Zeitalter vor Cloud Computing an. 27 % der Anbieter machten keine Angabe zu dieser Frage.

Einschränkend muss man anmerken, dass knapp 38 % der Befragten eine Public-Cloud-Lösung anbieten. Hier sind die technischen Möglichkeiten sowie die Aussichten auf kurze Kündigungsfristen am größten, insbesondere bei IaaS.



Entstehen Ihren Kunden nach der Kündigung Zusatzkosten?

Abb. 15 Zusatzkosten nach Vertragsende

Die meisten Cloud-Anbieter (60 %) geben an, dass für ihre Kunden nach der Kündigung des Vertrags keine Zusatzkosten entstehen. Kosten entstehen nur bei etwa einem Viertel der Unternehmen. Knapp 40 % der Unternehmen, bei denen nach Vertragsauflösung Kosten entstehen, betonen, dass dies hauptsächlich die Kosten seien, die aus der

Welche Serviceverfügbarkeit sichern Sie Ihren Kunden vertraglich zu?

gesetzlichen Datenaufbewahrungsfrist resultieren. Kleinere Anbieter und Anbieter mit kleineren Kunden machen wesentlich seltener Zusatzkosten geltend als die größeren Provider und Anbieter, die Cloud-Services hauptsächlich für Großunternehmen anbieten.

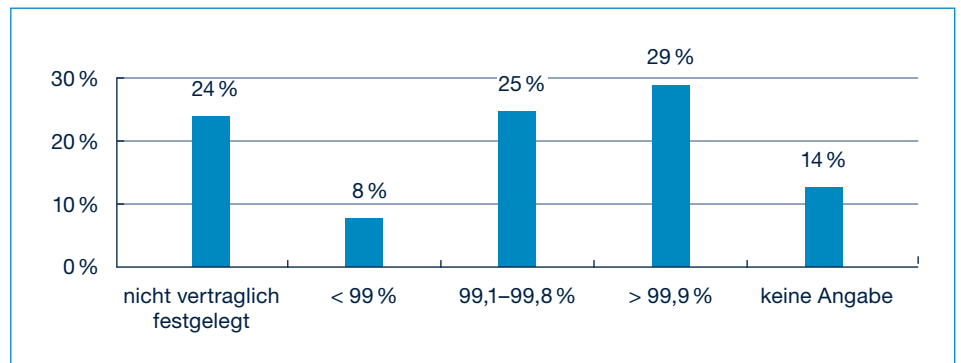


Abb. 16 Zugesicherte Serviceverfügbarkeit

29 % der Anbieter sichern ihren Nutzern vertraglich eine Serviceverfügbarkeit von mindestens 99,9 % zu. Weniger als 99 % Serviceverfügbarkeit garantieren lediglich 8 % der Anbieter; dabei handelt es sich um kleinere Unternehmen mit weniger als 500 Mitarbeitenden in Deutschland, die hauptsächlich für mittelständische Kunden arbeiten. Die größeren und spezialisierten Cloud-Anbieter sichern ihren Kunden tendenziell eine höhere Serviceverfügbarkeit zu als die kleineren Anbieter und diejenigen, bei denen das Cloud-Geschäft nur einen geringen Anteil am Gesamtgeschäft hat. Letztere liegen häufiger zwischen 99,1 und 99,8 % Serviceverfügbarkeit als die großen und spezialisierten Anbieter, die meist 99,9 % Serviceverfügbarkeit und mehr zusichern. Erstaunlich ist, dass ein Viertel der Befragten die Serviceverfügbarkeit nicht vertraglich festlegt.

Nutzen Sie die Services von anderen Cloud-Anbietern, um Ihre Dienstleistung sicherzustellen?

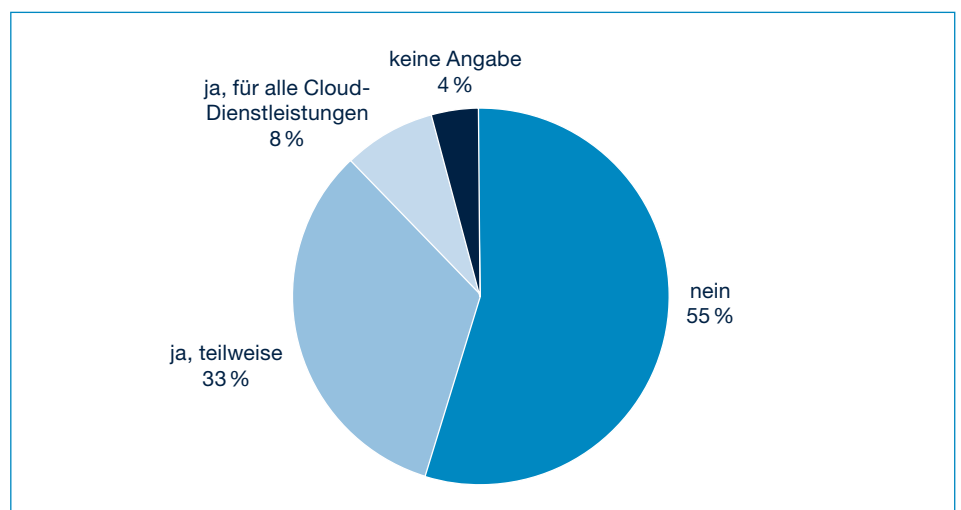
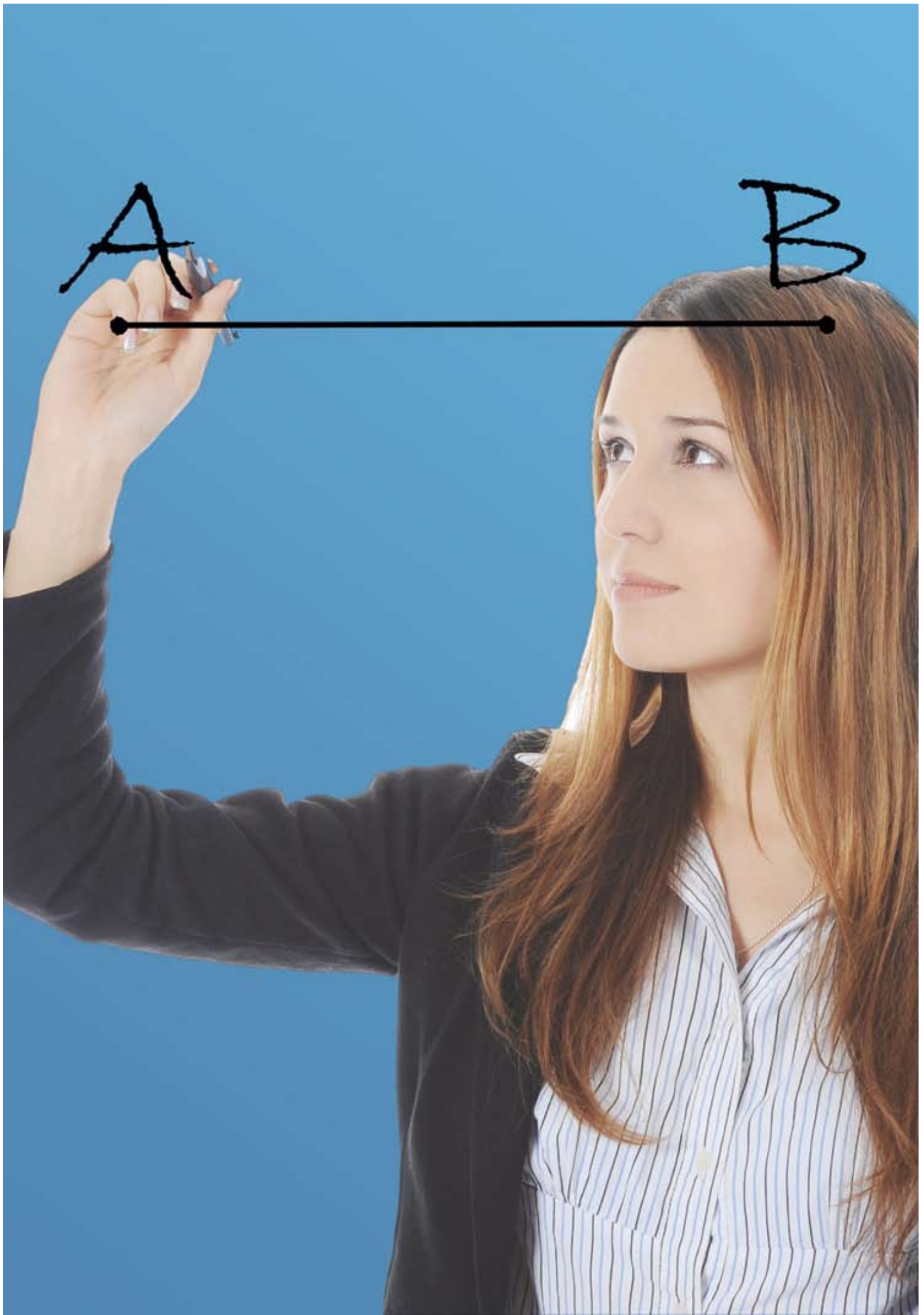


Abb. 17 Cloud-Chaining – Inanspruchnahme von Unterauftragnehmern

Über die Hälfte der Provider bietet alle Dienste aus eigener Hand an. Knapp über 40 % der Provider nutzen Unterauftragnehmer, um ihre Dienstleistung anbieten zu können. 8 % bieten ihre Dienstleistungen an, ohne eigene Ressourcen zu besitzen. Hierbei könnte es sich um erste Vorboten von Integration as a Service handeln. Dies ist eine Disziplin, bei der die eigentliche Leistung in der Kombination von unterschiedlichen Services

besteht. Integration as a Service wird nach Einschätzung der Provider in den nächsten Jahren zunehmen. Bei diesen Anbietern müssen die Nutzer aufgrund der mehrfachen Abhängigkeit bei der Vertragsgestaltung besonders auf Governance-Aspekte achten, wie die Überwachung, Kontrolle und Steuerung des Providers. Positiv hervorzuheben ist die Auskunft, dass praktisch alle Provider, die Unterauftragnehmer einbeziehen, ihre Kunden auch darüber informieren.

Wir haben die Teilnehmer auch gefragt, wie flexibel sie bei der Vereinbarung von SLAs agieren. Einerseits generieren Anbieter hohe Skaleneffekte durch die Standardisierung von SLAs, andererseits erhöhen sie ihre Attraktivität, wenn sie auf individuelle Vertragsvereinbarungen mit ihren Kunden eingehen. Drei von vier Unternehmen bieten ihren Kunden neben den Standardservices auch individuell konfigurierte Services an. Anbieter, die vorrangig Großunternehmen betreuen, bieten tendenziell häufiger individuell konfigurierte Services an als die Anbieter, die kleinere Unternehmen als Kunden bedienen. Hier ist offensichtlich die Abnahme bzw. das Volumen entscheidend. Nur knapp jedes fünfte Unternehmen bietet keine eigenen vom Standard abweichenden SLAs an.



2 Datenmigration

Die Einführung neuer Technologien, Architekturen und Systeme oder organisatorische Umstrukturierungen erfordern oft eine Neuorganisation der Datenbestände eines Unternehmens. Unternehmen übertragen dabei ihre Datenbestände aus bisherigen Anwendungen in neue Anwendungen oder ordnen ihre Daten innerhalb einer Anwendung neuen Organisationsstrukturen zu. Letzteres muss beispielsweise bei einer Fusion geschehen. Die Herausforderung bei allen genannten Fällen ist es, eine vollständige und inhaltlich korrekte Migration der Daten zu gewährleisten, das heißt, ohne dass Daten verloren gehen, bei der Übertragung falsch zugeordnet oder im Verlauf des Migrationsvorgangs manipuliert werden.

Daten folgen den Veränderungen im Unternehmen

Wie ich es sehe

„Cloud Computing ist keine Revolution in der IT-Nutzung und -Bereitstellung, sondern eine Evolution, die auf der Weiterentwicklung und Kombination bekannter Technologien basiert. Trotzdem bin ich überzeugt, dass es sich dabei um einen Paradigmenwechsel handelt, vergleichbar der Entwicklung vom Mainframe zur Client-Server-Nutzung oder dem Entstehen des Internets.“

Frank Strecker, Director of Cloud Computing, IBM Deutschland GmbH

2.1 Datenmigration und Cloud Computing

Für Nutzer von Cloud Computing-Lösungen ist es eine große Herausforderung, Anwendungen auszulagern, die bisher unternehmensintern genutzt und betrieben worden sind. Die Auslagerung wird in der Regel von einer Migration der Daten aus der unternehmensinternen IT in die Cloud begleitet. Die einheitliche Übertragung der Daten an den Provider erfordert technisch standardisierte Überleitungsverfahren, Schnittstellen und Datenformate. Ohne derartige Verfahren besteht das Risiko, dass die Daten bei der Migration aufwendig nachbereitet werden müssen, wodurch ein erheblicher Mehraufwand für den Nutzer, aber auch für den Provider entstehen kann. Insbesondere für Daten mit Bezug zur Rechnungslegung müssen bei der Datenmigration Aspekte wie Vollständigkeit, Nachvollziehbarkeit und Richtigkeit sichergestellt werden.

Ordnungsgemäß in die Cloud und aus der Cloud

Wie ich es sehe

„Cloud Computing führt die EDV zu neuer Nützlichkeit, indem elektronische Geschäftsprozesse per Mausklick verglichen und ausgetauscht werden können. Voraussetzung dafür ist, dass der CIO den Anwendungsfokus durch offenes Informationsmanagement erweitert.“

Stephan Haux, Senior Product Manager – International, Iron Mountain Digital GmbH

Bei einer Kündigung von Cloud-Services stellt sich für den Nutzer die Frage, wie er seine Daten zurückbekommt oder sie ordnungsgemäß in die Cloud eines anderen Providers migrieren kann. Hierbei gelten prinzipiell die gleichen Anforderungen wie bei der Auslagerung in die Cloud. Hinzu kommt die Sicherstellung der Vertraulichkeit der Daten durch eine nachhaltige, rückstandslose Löschung, nach der keine Daten in der ursprünglichen Cloud zurückbleiben dürfen oder zu rekonstruieren sind.

Allgemein sehen Nutzer die Gefahr, dass es zu dem sogenannten Vendor-Lock-In-Effekt kommen kann, bei dem der Cloud-Provider die Rückgabe der Daten nach einer Kündigung möglicherweise verzögert.

Auf die Unterstützung des Anbieters kommt es an

Die obigen Ausführungen verdeutlichen, dass eine erfolgreiche Migration der Daten in die Cloud oder aus der Cloud heraus entscheidend von der Unterstützung des Providers und den von ihm getroffenen Maßnahmen abhängt. Doch inwieweit unterstützen Provider ihre Kunden tatsächlich bei der Überführung von Daten in die Cloud und der Rückführung von Daten aus der Cloud? PwC bat die befragten Provider um ihre Antwort hierzu.

2.2 Umfrageergebnisse

Wie unterstützen Sie Ihre Neukunden bei der Datenübernahme?

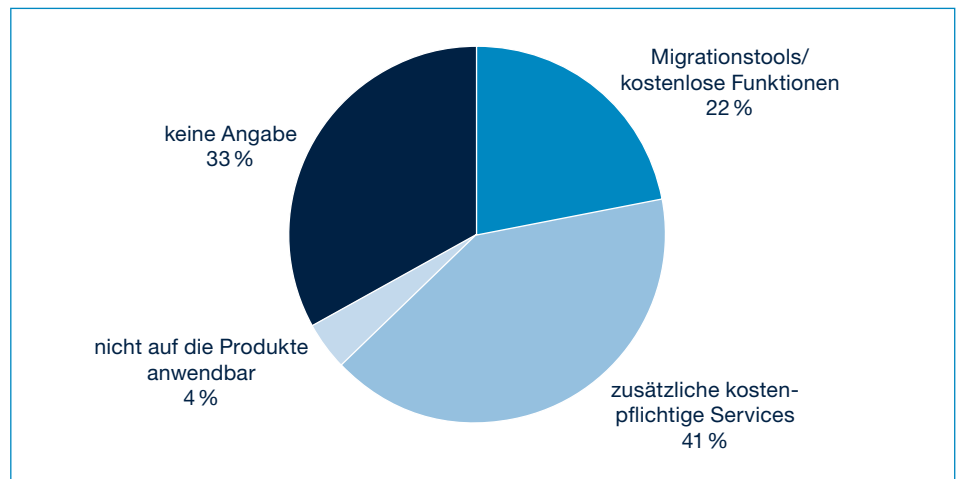


Abb. 18 Unterstützung der Datenmigration bei Neukunden

Gut 20 % der Anbieter stellen Migrationstools bereit oder bieten im Rahmen des Produkts Unterstützung durch kostenlose Funktionen an. Ungefähr 40 % der Anbieter unterstützen ihre Neukunden bei der Datenübergabe mit zusätzlichem kostenpflichtigem Service. Solche Unterstützung bieten große und kleine Anbieter gleichermaßen an. Keine Angaben zu dieser Frage haben 33 % der Befragten gemacht.

Ist im Vertrag geregelt, zu welchem Zeitpunkt und wie die Datenrückgabe bei Vertragsende erfolgt?

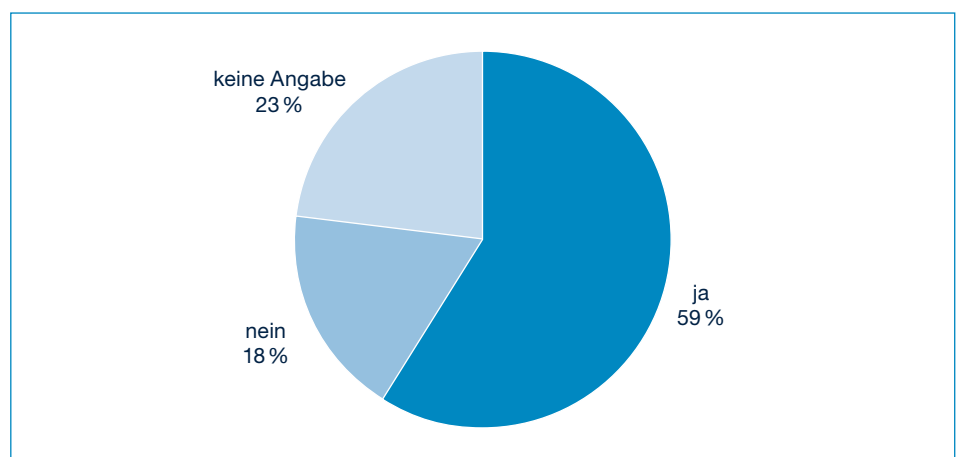
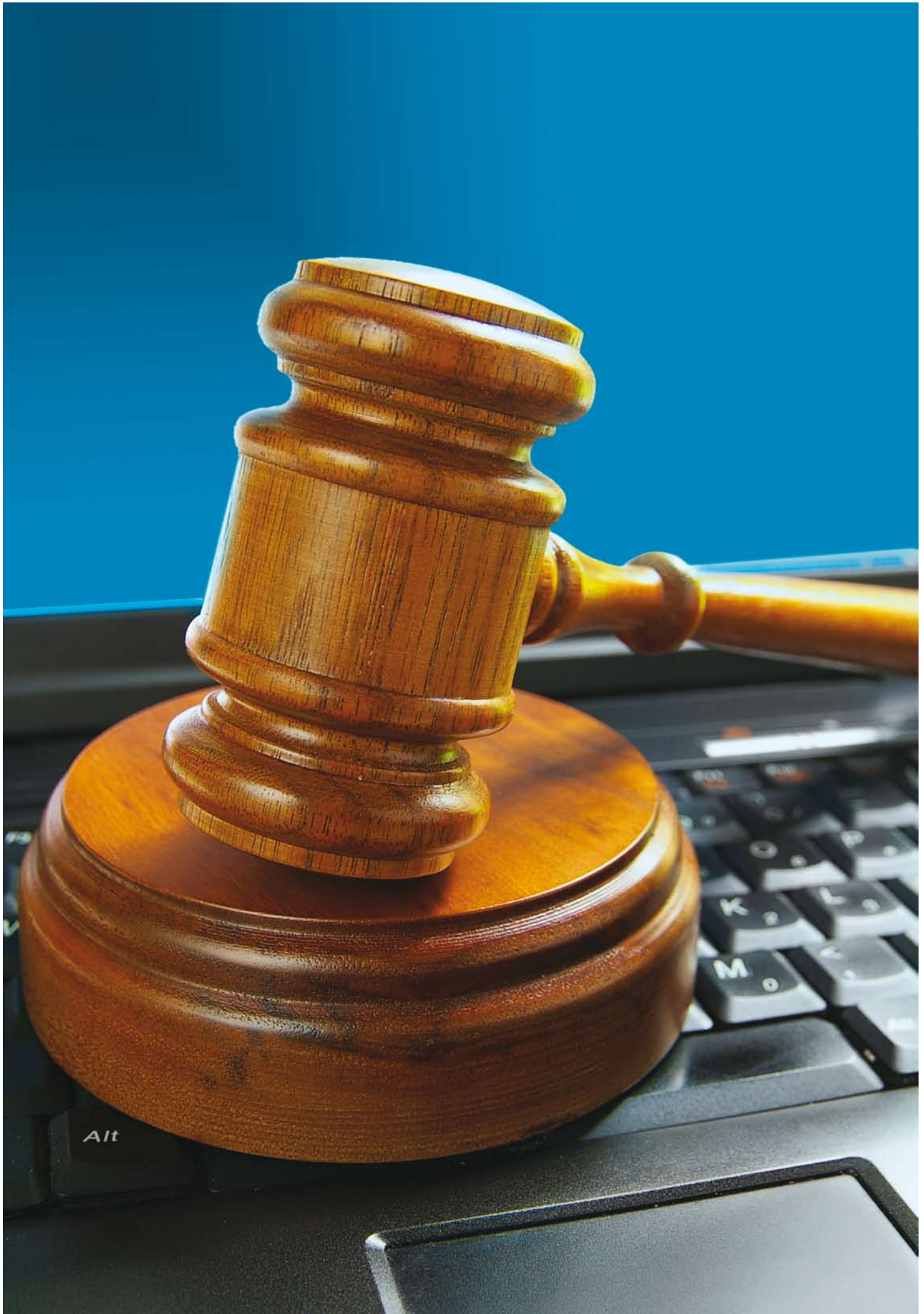


Abb. 19 Unterstützung der Datenmigration bei Kündigung

Rund 60 % der Anbieter geben zu Protokoll, dass sie mit den Kunden vertraglich regeln, wie die Datenrückgabe bei Vertragsende erfolgt. Die kleineren Anbieter sind dabei in der Mehrzahl. Immerhin knapp 20 % der Anbieter erklären überraschenderweise, dass es dazu keine vertragliche Regelung gibt. In diesem Fall ist nicht nur die Gefahr des zuvor genannten Vendor-Lock-In naturgemäß besonders groß, sondern auch das Risiko von Verstößen gegen den Datenschutz. Überraschend ist, dass der Rest der Befragten, knapp ein Viertel, keine Angabe dazu machen konnte oder wollte.



3 Risiken und Compliance

Compliance soll sicherstellen, dass das unternehmerische Handeln nicht gegen Gesetze, gesellschaftliche Wertvorstellungen, gegen Moral oder Ethik verstößt. Ergänzt um die Einhaltung und Umsetzung von internen Bestimmungen, Anweisungen und Regularien. Welche Maßnahmen im Einzelnen ergriffen werden müssen, ist unter anderem abhängig von der Art und dem Umfang des Geschäfts, sowie von Vertriebswegen und Kundenstrukturen. Ein Compliance-Ansatz ist also individuell auf jedes Unternehmen abzustimmen, damit alle Anforderungen im Interesse der Beteiligten erfüllt werden können.

Compliance

Wie ich es sehe

„Neue Herausforderungen durch Cloud Computing bedingen eine intelligente Data-Center-Architektur mit dem Netzwerk als Plattform für Transparenz, Management und Sicherheit.“

Viktor Hagen, Data Center Architect, Cisco Systems GmbH

3.1 Risiken, Compliance und Cloud Computing

Hat ein Unternehmen seine IT-Leistungen bisher mittels interner Kontrollmaßnahmen überwacht, so verliert es einerseits durch die Auslagerung der IT-Leistungen in eine Cloud-Computing-Lösung die Möglichkeit dazu. Andererseits bleibt der Nutzer trotz der Auslagerung von unternehmens-internen IT-Leistungen in die Cloud weiterhin für die Erfüllung seiner Compliance-Anforderungen verantwortlich. In dieser Situation muss der Nutzer sicherstellen, dass alle Risiken frühzeitig erkannt werden und die IT-Leistungen einer geeigneten Überwachung unterliegen. Die Herausforderung besteht darin zu überprüfen, ob der Provider geeignete Maßnahmen zur Risikoeinschätzung sowie Kontrollmaßnahmen implementiert hat, mit denen er die Risiken adäquat im Interesse des Nutzers behandeln kann. Dies gestaltet sich schwierig, da sich beispielsweise aus der Virtualisierungstechnologie, die dem Cloud Computing zugrunde liegt, eine Vielzahl neuer und geänderter IT-Risiken ergeben. Wie viele Provider unterstützen die Erfüllung der Compliance-Anforderungen für sich und ihre Nutzer durch ein entsprechendes Compliance-Management? Und welche Aspekte sind dabei besonders wichtig? PwC bat die befragten Provider um ihre Antwort hierzu.

Compliance in der Wolke

Wie ich es sehe

„IT-Verantwortliche sollten die Cloud als eine Chance zur Komplexitätsreduzierung und Fokussierung auf die Weiterentwicklung von Business-Technologien sehen. Bereits jetzt sollte an Cloud Readiness und Pilotprojekten gearbeitet werden. In vielen Bereichen fehlen noch Integrationstechnologien und wegweisende Standards sowie Best Practices. Wir erleben, dass sowohl Nutzer als auch Provider intensiv daran arbeiten, solche zu entwickeln.“

Jörg Hastreiter, Leiter Business Technology,
T-Systems Multimedia Solutions GmbH

3.2 Umfrageergebnisse

Gibt es in Ihrem Unternehmen ein Compliance-Management?

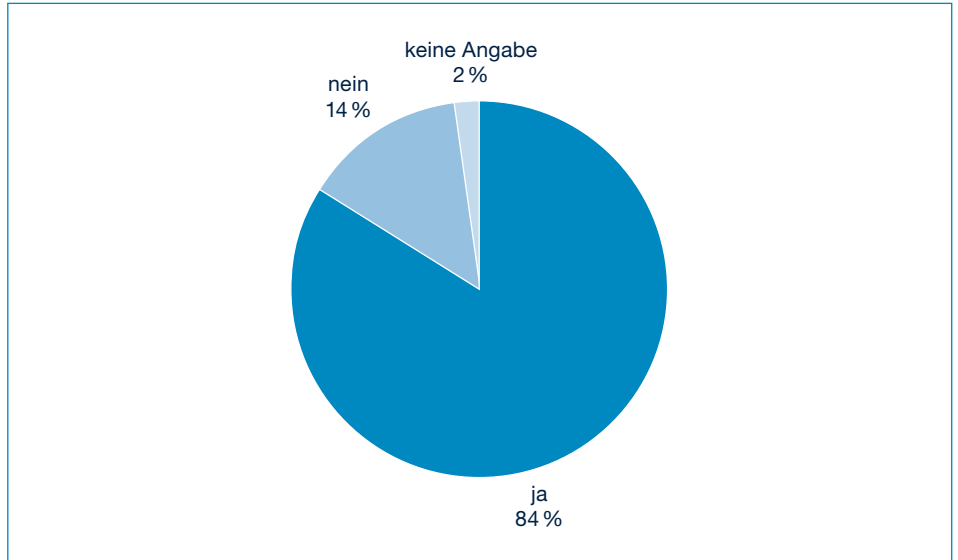


Abb. 20 Compliance-Management

Um die unternehmensspezifischen Compliance-Anforderungen optimal zu erfüllen, bietet sich ein Compliance-Managementsystem an. Als Teil des unternehmensweiten Risikomanagements fasst ein Compliance-Managementsystem die Grundsätze und Maßnahmen zusammen, durch die das regelkonforme Verhalten der gesetzlichen Vertreter und der Mitarbeitenden des Unternehmens sichergestellt werden soll.

Lediglich 14 % der befragten Anbieter geben an, dass bei ihnen kein Compliance-Management existiert. Es handelt sich dabei fast ausschließlich um kleinere Anbieter.

Welche Herausforderungen spielen in Ihrem Unternehmen bei der Erfüllung der Compliance-Anforderungen Ihrer Kunden momentan eine Rolle?

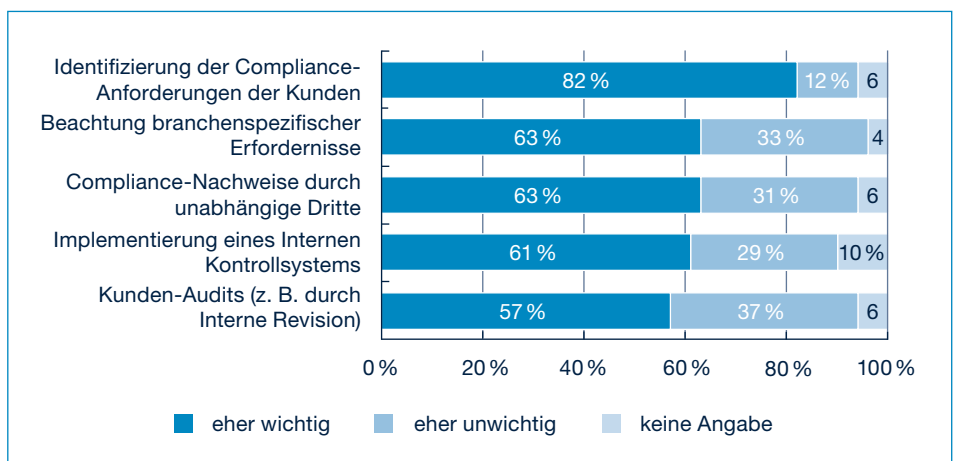


Abb. 21 Herausforderungen bei der Erfüllung der Compliance-Anforderungen

Da 84 % der Anbieter zuvor angegeben haben, über ein Compliance-Managementsystem zu verfügen, überrascht besonders, dass mehr als drei Viertel der Befragten die Identifizierung der Compliance-Anforderungen der Kunden als wichtigste Herausforderung erachten. Denn die Identifizierung der Compliance-Anforderungen der Kunden ist ein elementarer Bestandteil eines Compliance-Managementsystems

und steht zumeist an erster Stelle. Auffällig ist zudem, dass alle weiteren Herausforderungen von ähnlich hoher Wichtigkeit sind.

Es werden mehrere Tendenzen deutlich: Der Nachweis durch unabhängige Dritte, dass die Kundenforderungen erfüllt werden, scheint bei Providern mit Großkunden wichtiger zu sein als bei Anbietern mit vorwiegend mittelständischen Kunden. Das Gleiche gilt auch für Nutzer-Audits, Interne Kontrollsysteme und die Beachtung branchenspezifischer Erfordernisse. Dies sind drei Compliance-Aspekte, die in den größeren Anbieterunternehmen wichtiger genommen werden als von den kleineren Anbietern.



4 Datenschutz

Die als Skandale empfundenen Vorfälle der jüngsten Vergangenheit haben das Thema Datenschutz in Deutschland verstärkt in den Fokus gerückt. Die Öffentlichkeit und Führungskräfte aus der Wirtschaft widmen dem Datenschutz mehr Aufmerksamkeit als noch vor ein paar Jahren. Bei Verletzungen drohen Sanktionen, Bußgelder und nachhaltige Reputationschäden. Daher müssen die Verantwortlichen mehr denn je sicherstellen, dass ihre Unternehmen den gesetzlichen Anforderungen entsprechen. Das Datenschutzrecht soll natürliche Personen vor Missbrauch ihrer persönlichen Daten schützen und ihr Grundrecht auf informationelle Selbstbestimmung sichern. In den Schutzbereich fällt beispielsweise der Nutzer als natürliche Person oder ein Arbeitnehmer des Nutzers. In Deutschland regelt insbesondere das Bundesdatenschutzgesetz (BDSG) den Umgang mit personenbezogenen Daten im nicht öffentlichen Bereich. Ergänzt wird das BDSG durch weitere Gesetze, wie beispielsweise das Telemediengesetz (TMG), das Telekommunikationsgesetz (TKG) und das Sozialgesetzbuch (SGB). Diese müssen Nutzer ebenso wie Provider beachten.

Datenschutz in Deutschland

Wie ich es sehe

„Eine wesentliche Aufgabe der Provider ist es, durch Transparenz und Nachhaltigkeit sowie durch entsprechende Maßnahmen und Zertifizierungen die Dienste nachvollziehbar darzustellen und somit bei ihren Kunden Vertrauen zu schaffen. Das beginnt bei der Vertragsgestaltung und zieht sich über das ganze Vertragsverhältnis durch unterschiedliche Bereiche bis hin zu Informationssicherheits- und Datenschutzthemen.“

Michael Kranawetter, Chief Security Advisor, Microsoft Deutschland GmbH

Die Europäische Gemeinschaft (EG) hat die Notwendigkeit eines einheitlichen Datenschutzniveaus erkannt. Die entsprechende Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr wurde am 24. Oktober 1995 erlassen. Inzwischen haben alle Mitgliedsstaaten sie in nationales Recht umgesetzt.

Datenschutz innerhalb und außerhalb der EU sowie in den USA

Ein Grundsatz des europäischen Datenschutzrechts ist es, dass personenbezogene Daten nur dann aus dem Europäischen Wirtschaftsraum (EWR) heraus übermittelt werden dürfen, wenn bei dem Empfänger ein angemessenes, gesetzlich festgelegtes Datenschutzniveau besteht. Diese Bedingung kann dadurch erfüllt sein, dass das Land, in dem der Empfänger ansässig ist, ein solches Datenschutzniveau aufweist, wie es zum Beispiel die Schweiz tut. Die USA verfügen nicht über ein angemessenes, gesetzlich festgelegtes Datenschutzniveau. Der Empfänger kann diese Bedingung in seinem Unternehmen jedoch dadurch herstellen, dass er sich dem sogenannten Safe-Harbor-Regelwerk des US-Handelsministeriums unterwirft. Dadurch verpflichtet sich der Empfänger zur Einhaltung von Standards, die den europäischen Datenschutzstandards entsprechen. Der Empfänger wird somit in den datenschutzrechtlich unsicheren USA zu einem sicheren Hafen (Safe Harbor) für die Daten. Auch vertraglich kann ein angemessenes Datenschutzniveau geschaffen werden, zum Beispiel durch die sogenannten Standardvertragsklauseln. Ungeachtet des Empfängerlandes, eines sicheren Hafens oder der

Standardvertragsklauseln muss der europäische Datenexporteur jedoch stets prüfen, ob er die Daten überhaupt an einen Dritten weitergeben darf.

4.1 Datenschutz und Cloud Computing

Grenzenloser Datenverkehr

Im Rahmen der Cloud-Computing-Angebote in Deutschland verarbeiten Provider auch personenbezogene Daten (z. B. Kunden-, Personal-, Lieferanten- und Vertragsdaten etc.) in der Cloud. Um Daten möglichst effizient zu verarbeiten, können Provider die personenbezogenen Daten lastenorientiert standort- und länderübergreifend auf viele verschiedene Serversysteme in unterschiedlichen Rechenzentren verteilen. Normalerweise verarbeitet der Provider die Daten dabei im Auftrag des Nutzers (Auftragsdatenverarbeitung). In diesem Fall muss der Nutzer im nicht öffentlichen Bereich die Anforderungen des § 11 BDSG erfüllen. Als „Herr der Daten“ bleibt er für die Verarbeitung der von ihm in die Cloud gegebenen Daten verantwortlich. Er darf die Daten nur dann dem Provider zur Verfügung stellen, wenn bei einer Verarbeitung außerhalb des EWR ein angemessenes Datenschutzniveau besteht. Der Provider seinerseits darf die Daten nur nach den Weisungen des Nutzers verarbeiten.

Wie ich es sehe

„Die Integration und Orchestrierung einer Lösungslandschaft aus On-Premise-Komponenten und verschiedenen Cloud-Services muss in Zukunft eine Kernkompetenz der IT-Abteilungen sein. Die Rolle der IT-Abteilungen wird sich dadurch definitiv verändern und gleichzeitig an Bedeutung – auch für das Business – gewinnen.“

Dr. Bernd Welz, Senior Vice President OnDemand Services Unit, SAP AG

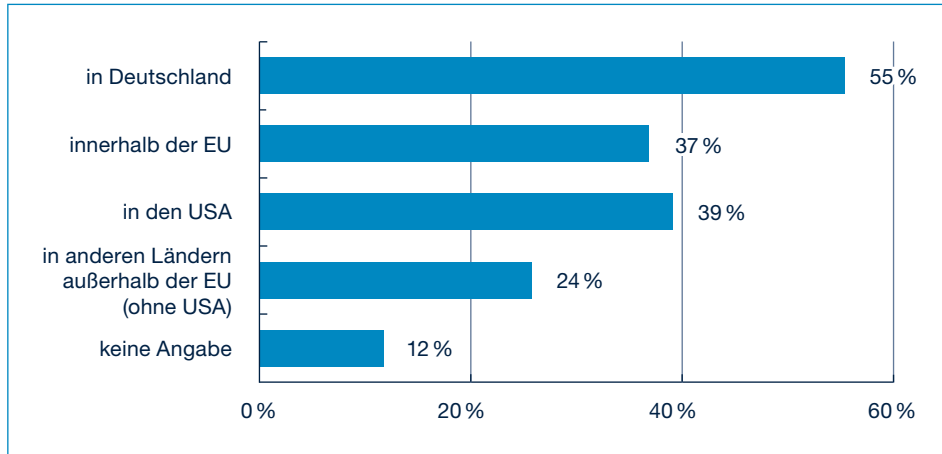
Die Verantwortung bleibt beim Besitzer der Daten. Die Sicherheit muss der Provider gewährleisten.

Wesentlich für den Schutz der personenbezogenen Daten sind angemessene technische und organisatorische Maßnahmen, die der Provider gemäß § 9 BDSG ergreifen muss. Die Schutzziele hat der Gesetzgeber in einer Anlage zu § 9 BDSG konkretisiert. Zu ihnen gehören insbesondere Vertraulichkeit, Verfügbarkeit und Integrität der personenbezogenen Daten. Schutzmaßnahmen sind beispielsweise Zutrittskontrollen zum physischen Schutz der Systeme oder Eingabekontrollen zur Überwachung und Protokollierung von Änderungen, Löschungen oder Speicherungen personenbezogener Daten.

BDSG-Novellierung konkretisiert Anforderungen

Seit der Novellierung des § 11 BDSG zum 1. September 2009 muss ein Nutzer prüfen, ob die technischen und organisatorischen Maßnahmen des Providers zum Schutz der Daten ausreichen, bevor er ihm anvertraute personenbezogene Daten in die Cloud übermittelt. Auch muss der Auftrag an den Provider zur Auftragsdatenverarbeitung Mindestinhalte aufweisen, zum Beispiel zum Einsatz von Unterauftragnehmern. Solange das Vertragsverhältnis besteht, muss sich der Nutzer fortwährend von der Sicherheit der Daten beim Provider überzeugen und das Ergebnis der Prüfung dokumentieren. Doch wie organisieren die Provider aktuell ihre Datenverarbeitung und an welchen Standorten verarbeiten sie die ihnen anvertrauten Nutzerdaten? Überprüfen Cloud-Nutzer in der Praxis, ob ihr Provider die Voraussetzungen zum Schutz der Daten geschaffen hat? Falls ja, in welcher Form reagiert der Provider auf solche Anfragen? PwC bat die befragten Provider um ihre Antwort hierzu.

4.2 Umfrageergebnisse



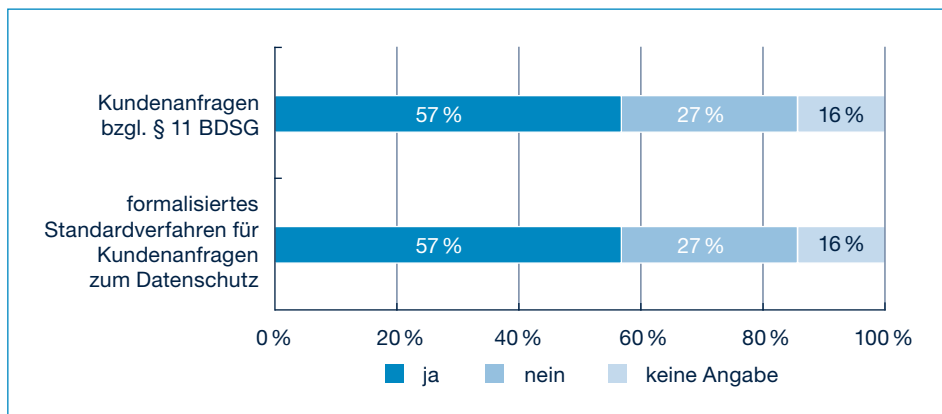
In welchen Ländern befinden sich Ihre Rechenzentren bzw. die Server, auf denen die Nutzerdaten gespeichert sind?

Abb. 22 Lokation der Daten

Gut jeder zweite Anbieter nutzt Server bzw. Rechenzentren in Deutschland. Dabei zeigt sich erwartungsgemäß, dass größere Anbieter tendenziell über mehr Datenstandorte verfügen als kleinere.

Nur 30 % der Anbieter speichern Nutzerdaten ausschließlich in Deutschland. Bei 25 % der Anbieter ist es also nicht ausgeschlossen, dass die Nutzerdaten Deutschland verlassen. Große Anbieter überlassen häufiger ihren Kunden die Entscheidung darüber, ob ihre Daten ausschließlich in Deutschland gespeichert werden sollen, als die kleineren Unternehmen mit einem stärkeren Cloud-Schwerpunkt im Portfolio. Möglicherweise kommen bei diesen mehr Unterauftragnehmer zum Zuge, bei denen der Standort nicht frei wählbar ist.

Jeder dritte kleine Cloud-Anbieter und jeder zweite große Anbieter speichert Nutzerdaten in anderen Ländern als Deutschland, den EU-Ländern und den USA. Unter den befragten Anbietern sind auch große Provider, die Kundendaten ausschließlich in außereuropäischen Regionen speichern lassen.



Sind Kunden bereits mit der Frage an Sie herangetreten, welche Maßnahmen gemäß § 11 BDSG Ihrerseits getroffen wurden?

Hat Ihr Unternehmen ein formalisiertes Standardverfahren, um auf solche Kundenanfragen zu reagieren?

Abb. 23 Kundenanfragen zum Datenschutz und Reaktion der Anbieter

PASSWORD



5 Informationssicherheit

Informationssicherheit ist nur so gut wie ihr schwächstes Glied

Ein Unternehmen ohne IT ist in der heutigen Zeit nahezu undenkbar. IT-Systeme sind eine wesentliche Voraussetzung für den erfolgreichen Geschäftsbetrieb von Unternehmen und öffentlichen Institutionen. In manchen Unternehmen hängen Teile der Produktion oder andere unmittelbar wertschöpfende Bereiche direkt von der Verfügbarkeit der IT ab. Bei Unternehmen, deren Wettbewerbsvorteil auf einem Informationsvorsprung (z. B. Forschung und Entwicklung) basiert, muss die Vertraulichkeit und Integrität der elektronisch verarbeiteten Informationen gewährleistet sein. Der Verlust der IT-Sicherheit kann erhebliche wirtschaftliche Schäden nach sich ziehen. Daher sollten IT-Systeme, die sensible Daten beinhalten, auf allen Ebenen geschützt werden.

Wie ich es sehe

„Cloud Computing bietet die Möglichkeit, das Management der dezentralen IT handhabbar zu machen. Insbesondere Desktop as a Service mit der Eigenschaft der Hardwareunabhängigkeit trägt in global agierenden Unternehmen zur Verminderung der Heterogenität und zur Kosteneinsparung bei.“

Dr. Roland Schütz, Chief Operating Officer, Lufthansa Systems AG

Management von Informationssicherheit

Informationssicherheit ist kein Selbstzweck und muss unter wirtschaftlichen Gesichtspunkten behandelt werden. Es ist daher Aufgabe der Unternehmen, ein angemessenes Sicherheitsniveau herzustellen und es stetig an den Unternehmensbedürfnissen auszurichten. Diese Aufgabe hat das Informationssicherheitsmanagement (Information Security Management System, ISMS). Im Rahmen des ISMS werden Maßnahmen zum Schutz sensibler Daten vor potenziellen Bedrohungen und realen Gefahren ergriffen. Dadurch sollen Reputations- oder finanzielle Schäden vermieden und betriebliche Risiken minimiert werden. In der Praxis orientiert sich das Informationssicherheitsmanagement unter anderem an der ISO/IEC-Standard-Reihe 2700x, an ISO/IEC 15408 bzw. an nationalen Handlungsempfehlungen. Zu diesen zählen in Deutschland zum Beispiel die IT-Grundschrift-Kataloge des Bundesamts für Sicherheit in der Informationstechnik (BSI), in denen Maßnahmen zur Umsetzung eines effektiven Informationssicherheitsmanagementsystems beschrieben werden.

5.1 Informationssicherheit und Cloud Computing

Globales Management von Informationssicherheit

Bei der Auslagerung von Daten in die Cloud geben Unternehmen Kontrollmöglichkeiten ab. Vertraulichkeit, Integrität und Verfügbarkeit von Informationen müssen aber weiterhin gewährleistet sein. Im Vergleich zu herkömmlichen Outsourcing-Lösungen gilt es hier nicht nur, lokale Server oder Rechenzentren zu schützen, sondern den Schutz und die Kontrollmaßnahmen auf mehrere Serversysteme (logische Sicherheit) und Rechenzentren (physische Sicherheit) auszuweiten, die weltweit verteilt sind. Bisher haben Provider in ihren Rechenzentren Firewalls eingerichtet, um die Daten ihrer Nutzer in eigens eingerichteten Sicherheitszonen gegen unerlaubte Zugriffe und Angriffe von innen und außen zu schützen. Diese Maßnahme reicht in einer Cloud-Umgebung mit verteilten, länderübergreifenden Standorten und unterschiedlichen Providern nicht

Wie ich es sehe

„Die Cloud eröffnet neue Optionen zur Bewertung der Leistungskraft der IT und liefert den Anstoß für mehr Flexibilität und Effizienz. Das Fundament und die Zukunft der IT ist eine Shared Infrastructure, die durch Automatisierung und Vereinfachung mit dem Business Schritt halten hilft.“

Alexander Wallner, Area Vice President Germany, NetApp Deutschland GmbH

aus. Hier gewährleistet nur ein globales, umfassendes ISMS den Schutz der sensiblen Unternehmensdaten.

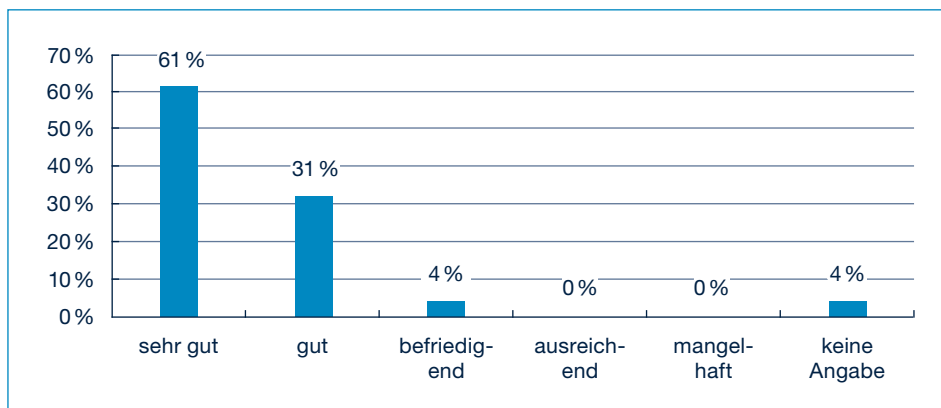
Viele Public-Cloud-Lösungen versorgen eine Vielzahl von Nutzern gleichzeitig mit IT-Leistungen. Um die Ressourcen eines physischen Systems möglichst effizient zu nutzen, werden die Anwendungen mehrerer Nutzer gleichzeitig darauf betrieben (Multi-Mandanten-Fähigkeit). Vertrauliche Daten, wie zum Beispiel Personaldaten, Produktinformationen oder Innovationsvorhaben, sind in einer solchen Umgebung bei Fehlfunktionen (unbeabsichtigte mandantenübergreifende Zugriffe) und Sicherheitslücken (Hackerangriffe) besonders gefährdet. Allein die Betrachtung dieses einen Cloud-Spezifikums verdeutlicht, wie wichtig eine Neubewertung der Sicherheitsrisiken im Rahmen einer Risikoanalyse ist.

Neue Risiken erfordern neue Maßnahmen

Auch das Katastrophenrisiko bzw. das Risiko unzureichender Kapazität ist in Cloud-Umgebungen nicht automatisch ausgeräumt. Denn wer garantiert, dass die physischen Ressourcen bei gleichzeitiger Nutzung durch mehrere, teilweise häufig wechselnde Mandanten immer ausreichen? Auch für den Katastrophenfall sollten mit dem Provider Ausweichmöglichkeiten festgelegt und Wiederanlaufzeiten vereinbart werden, damit der Geschäftsbetrieb aufrechterhalten werden kann.

PwC befragte die Studienteilnehmer, wie es um die Informationssicherheit der ihnen anvertrauten Daten bestellt ist und welche Aspekte sie dafür als besonders wichtig erachten. Außerdem wollten wir wissen, ob sie Notfallpläne mit ihren Kunden vereinbaren, damit diese für den Katastrophenfall gewappnet sind.

5.2 Umfrageergebnisse



Wie gelingt es Ihrem Unternehmen derzeit, die Informationssicherheit im Sinne Ihrer Kunden zu gewährleisten?

Abb. 24 Gewährleistung der Informationssicherheit für den Nutzer

Nahezu zwei Drittel der Befragten erklären, dass es ihnen im Unternehmen derzeit sehr gut gelinge, die Informationssicherheit für die Kunden zu gewährleisten. Man muss aber grundsätzlich davon ausgehen, dass in Antworten auf Fragen zur Datensicherheit normative Überlegungen zu Werthaltungen und Fremderwartungen hineinspielen. Positive Antworten auf Fragen nach sozial erwünschtem Verhalten liegen näher als negative. Ein klarer Trend ist, dass die Bewertungen der größeren Anbieter besser ausfallen als die der kleinen und dass sie in Firmen, die vorwiegend Großkunden betreuen, besser ausfallen als in Firmen mit kleineren Kunden.

Welche Rolle spielen die folgenden Aspekte bei der Gewährleistung der Informationssicherheit der Kundendaten?

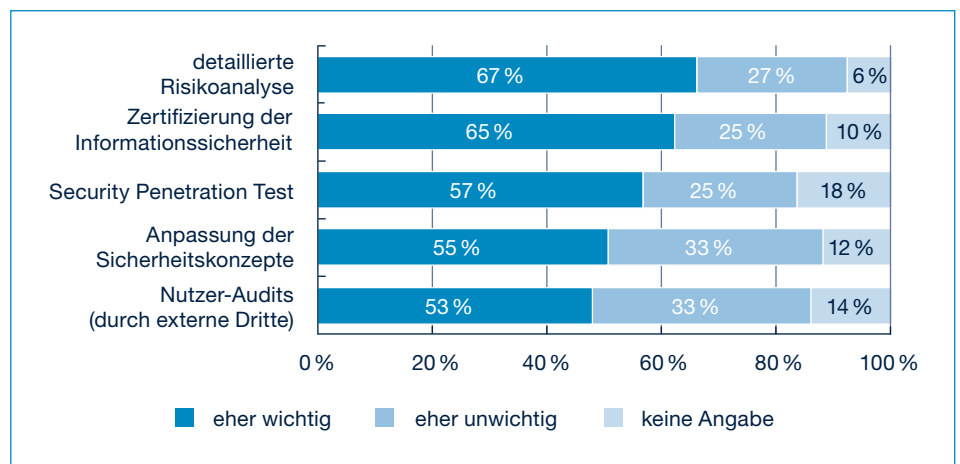


Abb. 25 Aspekte der Informationssicherheit

Für die Gewährleistung der Informationssicherheit spielen detaillierte Risikoanalysen als Basis der Maßnahmenplanung und die Zertifizierung der Informationssicherheit (z. B. durch ISO/IEC 2700x) die wichtigsten Rollen. Von nur wenig geringerer Bedeutung scheinen Security Penetration Tests (simulierte Hackerangriffe), die Anpassung der Sicherheitskonzepte und die Möglichkeit eines vom Kunden veranlassten Audits durch externe Dritte zu sein.

Detaillierte Risikoanalysen, Zertifizierungen der Informationssicherheit und externe Audits scheinen den Providern, die hauptsächlich Großunternehmen betreuen, wichtiger zu sein als den Providern, die vorwiegend kleinere Unternehmen als Kunden haben.

Sowohl externe Audits als auch Zertifizierungen und Penetrationstests sind für größere Provider wichtiger als für die kleineren.

Nur ein Aspekt ist kleineren Provider wichtiger als den größeren Unternehmen: die Anpassung der Sicherheitskonzepte.

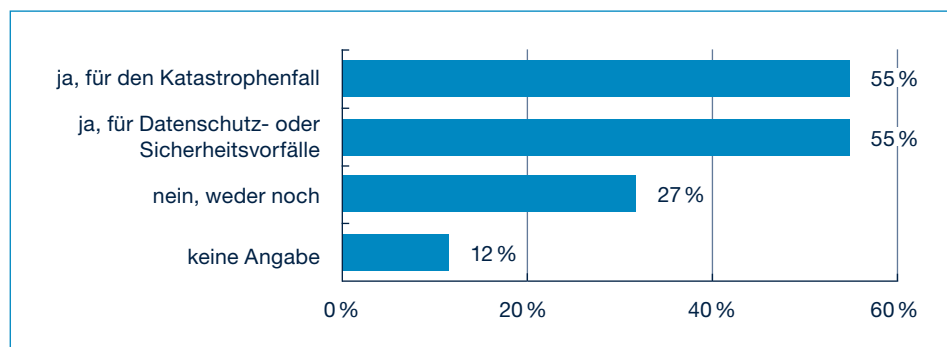


Abb. 26 Vereinbarung von Notfallplänen

Vereinbart Ihr Unternehmen mit den Kunden vertraglich Notfallpläne?

Über die Hälfte der Anbieter vereinbart mit ihren Kunden vertraglich Notfallpläne für den Katastrophenfall bzw. für Datenschutz- oder Sicherheitsvorfälle. Keine vertraglich vereinbarten Notfallpläne gibt es bei 27 % der Anbieter. Dabei handelt es sich praktisch ausschließlich um kleinere Cloud-Anbieter, die weniger als 500 Mitarbeitende in Deutschland beschäftigen.



6 Ausblick

Im Hinblick auf die künftige Entwicklung des Cloud-Computing-Marktes in Deutschland haben wir die Anbieter zu diversen Trends befragt. Wir wollten wissen, welche Umsatzentwicklung sie für die nächsten fünf Jahre prognostizieren und welche Entwicklungen sich im Cloud-Computing-Markt abzeichnen.

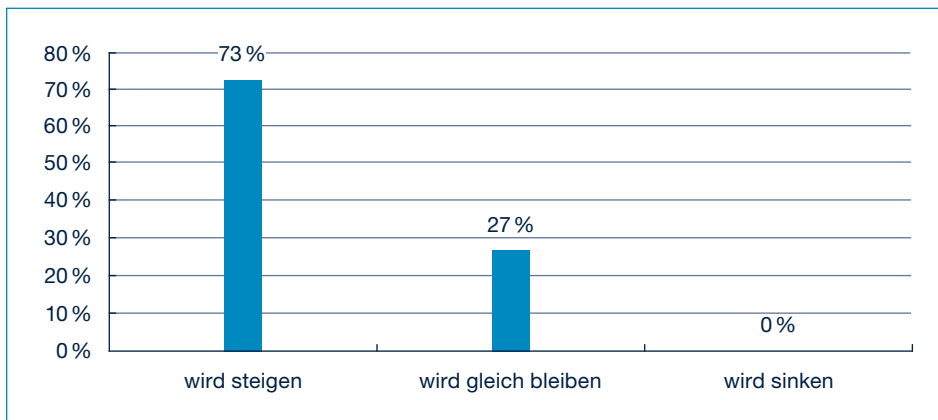


Abb. 27 Umsatztendenz mit Cloud-Services

Knapp drei Viertel der Anbieter gehen davon aus, dass der Anteil der Cloud-Services am Gesamtgeschäft in Deutschland steigen wird. Bei den Befragten, die keine Änderungen des Umsatzes erwarten, handelt es sich fast ausschließlich um kleinere Provider. Mit einem sinkenden Umsatz rechnet keines der befragten Unternehmen.

Wie wird sich der Umsatz mit Ihren Cloud-Services in den nächsten fünf Jahren entwickeln?

Wie wird sich der Markt Ihrer Meinung nach entwickeln?

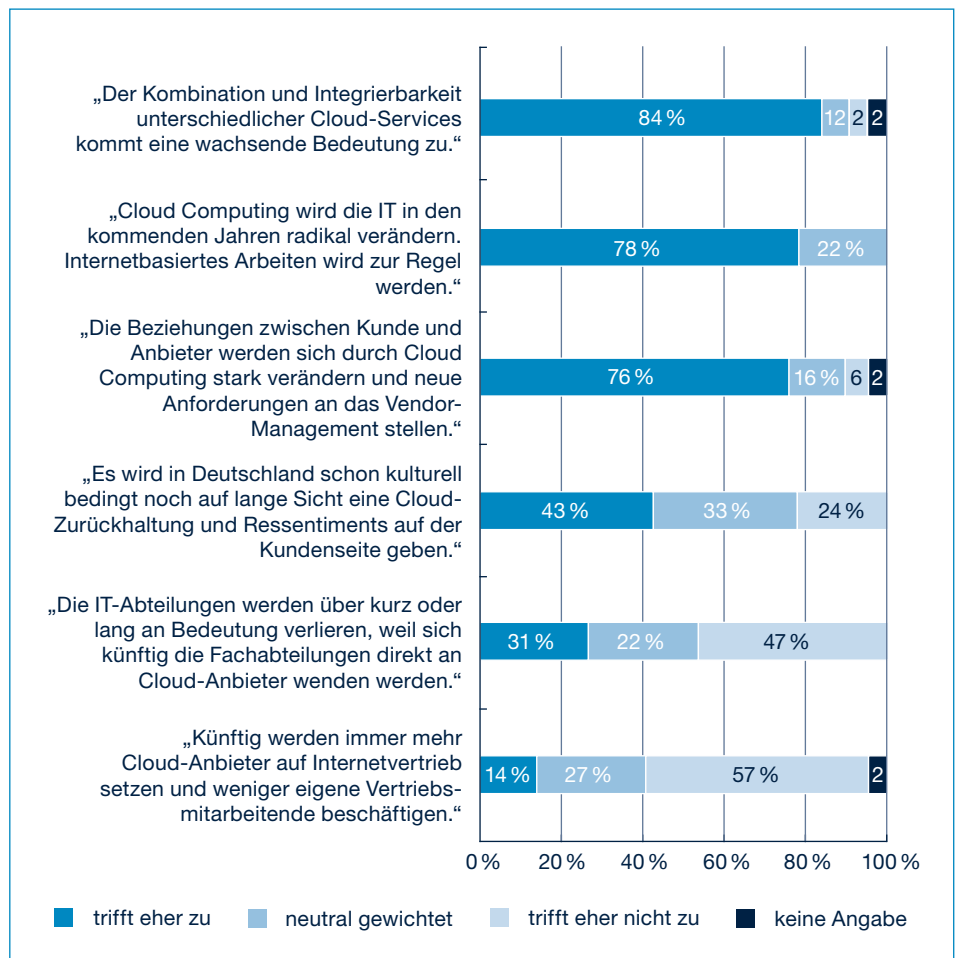


Abb. 28 Einschätzungen der Markttrends

Insbesondere die stärker spezialisierten Provider glauben, dass das internetbasierte Arbeiten zur Regel wird und dass in diesem Zukunftsszenario die Integrierbarkeit und Kombinierbarkeit der Cloud-Angebote immer wichtiger wird. Von Letzterem sind vor allem die Befragten bei den großen Anbietern überzeugt sowie diejenigen, die hauptsächlich Großkunden betreuen.

Wie ich es sehe

„Cloud Computing eröffnet ganz neue Chancen – für einzelne Unternehmen wie für den Standort Deutschland. Um diese Chancen zu ergreifen, müssen Industrie – Anbieter wie Anwender –, Politik und Wissenschaft zügig und gemeinsam handeln. Der BITKOM bringt seine Projekte in das Aktionsprogramm des Bundeswirtschaftsministeriums mit dem Ziel ein, die verstärkte Nutzung von Cloud Services anzuregen und zur Entwicklung einer wettbewerbsfähigen Industrie für Cloud Services am Standort Deutschland beizutragen.“

Dr. Mathias Weber, Bereichsleiter IT Services, BITKOM, Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.

Die Mehrheit der Anbieter geht davon aus, dass Cloud Computing das Vendor-Management und die damit verbundene Providersteuerung vor neue Herausforderungen stellen wird.

Hinsichtlich der Frage, ob es in Deutschland kulturell bedingt auf lange Sicht eine Cloud-Zurückhaltung geben wird, klaffen die Meinungen auseinander. Weniger als die Hälfte der Befragten glaubt, dass die Ressentiments noch lange bestehen bleiben.

Keine Einigkeit herrscht auch in der Frage nach einem etwaigen Bedeutungsverlust der IT-Abteilungen durch Cloud-Services sowie einer Veränderung der aktuellen Vertriebsmodelle. Dass künftig mehr Cloud-Provider auf Internetvertrieb setzen werden, glauben vor allem die Vertreter kleinerer Anbieter. Warum genau die Vertriebsmodelle keine Änderung erfahren sollen, bleibt allerdings offen. Verwunderlich ist es insofern, als über 80 % der Studienteilnehmer Software-as-a-Service-Lösungen anbieten. Durch den Wegfall des Lizenzgeschäfts sind gerade diese Unternehmen dazu gezwungen, den Internetvertrieb zu entdecken oder intensiver zu nutzen.

Die bisherigen Ausführungen haben gezeigt, dass Cloud Computing eine dynamische und an den Bedarf angepasste Form der IT-Dienstleistung ist. Hierbei werden unterschiedliche technische Entwicklungen zusammengefasst und faszinierende neue Möglichkeiten sowohl den Anbietern, als auch den Nutzern eröffnet. Zwar sind die zugrunde liegenden Technologien nicht neu, doch ergeben sich aus ihrer Weiterentwicklung für Anbieter und Anwender von IT-Dienstleistungen immense Innovationspotenziale. Cloud Computing schafft somit nicht nur die Basis für neue Vertriebs- und Nutzungswege von IT-Leistungen, sondern auch für ganz neue Prozesse und Geschäftsmodelle.

Stichwortverzeichnis

A

Archivierung	20
Auftragsdatenverarbeitung.....	42
Ausschöpfungsquote	15

B

Branche	19
BSI.....	46
Bundesdatenschutzgesetz (BDSG).....	41
Business Intelligence.....	20
Business Process as a Service.....	19
Bußgelder	41

C

CATI-Befragung (Computer Aided Telephone Interviews)	15
Cloud-Chaining	30
Cloud-Strategie	24
Compliance-Managementsystem	38

D

Datenformate.....	33
Datenmigration	23
Datenrückgabe	34
Datenschutz	15
Definition von Cloud Computing	25
Desaster Recovery	20
Deutschland	15
Dokumentenerkennung	20
Drei-Stufen-Modell.....	15

E

E-Commerce	20
Einkauf.....	20
Europäische Gemeinschaft (EG)	41
EWR	41
Expertengespräch.....	15

F

Fehlfunktionen.....	47
Feldphase.....	15
Fragebogen	15

G

Gesamtgeschäft.....	15
Geschäftsmodell	23
Geschäftsportfolio	18
Grundgesamtheit	15

H

Herr der Daten.....	42
---------------------	----

I

Information Security Management System – ISMS	46
Informationssicherheit.....	24
Infrastructure as a Service	19
Integrationsfähigkeit.....	24
Interne Kontrollsysteme.....	39
Internetvertrieb.....	52
ISO/IEC.....	46
IT-Outsourcing-Verträge	28
IT-Strategie.....	24

K

Katastrophenrisiko	47
Kosteneinspareffekt	28
kostenpflichtiger Service.....	34
Kostenreduktion	23
Kündigung	29
Kündigungsfrist	29
Kundenstruktur.....	15
Kundenzufriedenheit	23

L

Lizenzgeschäft	53
Lizenzmodell.....	25
Lokation.....	43

M

Maintenance.....	25
Marktforschungsinstitut	15
Markttrends.....	52
Migrationstool	34

N

Nettogesamtumsatz.....	17
Nischenstrategie	20
Notfallpläne	24
Novellierung.....	42
Nutzer-Audits	39

P

Personal	20
Platform as a Service	19
Private Cloud.....	21
Public Cloud.....	21

R

Rechnungswesen.....	20
Rechtsunsicherheit	28
Regelungslücken.....	28
Risikoanalyse	47
Rückführung.....	34

S

Safe Harbor	41
Sanktionen	28
Security Penetration Test	48
Serverlokationen	24
Service Level Agreement	24
Servicequalität	25
Serviceverfügbarkeit	25
Sicherheitskonzept.....	48
Sicherheitslücken.....	47
Skaleneffekte.....	25
Skalierbarkeit.....	25
Software as a Service	19
Sourcing Governance.....	23
Sozialgesetzbuch (SGB).....	41
Standardisierung	25
Standardservice	31

Standardverfahren	43
Stichprobentotal	15

T

Telefoninterview	15
Telekommunikationsgesetz (TKG)	41
Telemediengesetz (TMG)	41
Trendaussagen	15

U

Überwachung	31
Unified Communication	20
Unterauftragnehmer	25
Unterstützungsprozesse	19
USA	41
US-Handelsministerium	41

V

Vendor Management	52
Vendor-Lock-In	34
Verkauf	20
Vertragsauflösung	29
Vertragsgestaltung	28
Vertragslebenszyklus	28
Vertrauliche Daten	47

W

Wiederanlaufzeiten	47
--------------------------	----

Z

Zertifizierung	41
Zusatzkosten	29

57 % der Anbieter geben zu Protokoll, dass bereits Kunden mit der Frage nach datenschutzrechtlichen Maßnahmen gemäß § 11 BDSG an sie herangetreten sind. Ebenfalls 57 % haben ein formalisiertes Standardverfahren für den Umgang mit solchen Kundenanfragen. Die Zahlengleichheit für beide Fragen insgesamt lässt vermuten, dass diejenigen Anbieter ein solches Verfahren etabliert haben, die zuvor mit Kundenanfragen konfrontiert wurden. Die anderen Anbieter wären demnach noch nicht auf derartige Kundenanfragen vorbereitet.

Ansprechpartner

Markus Vehlow

Olof-Palme-Straße 35
60439 Frankfurt am Main
Tel.: +49 69 9585-2293
markus.vehlow@de.pwc.com

Cordula Golkowsky

Marie-Curie-Straße 24–28
60439 Frankfurt am Main
Tel.: +49 69 9585-5022
cordula.golkowsky@de.pwc.com

PricewaterhouseCoopers. Die Vorausdenker.

PricewaterhouseCoopers ist weltweit eines der führenden Netzwerke von Wirtschaftsprüfungs- und Beratungsgesellschaften und kann auf die Ressourcen von insgesamt 163.000 Mitarbeiterinnen und Mitarbeitern in 151 Ländern zugreifen. In Deutschland erwirtschaften fast 9.000 Mitarbeiterinnen und Mitarbeiter in den Bereichen Wirtschaftsprüfung und prüfungsnahe Dienstleistungen (Assurance), Steuerberatung (Tax) sowie Deals und Consulting (Advisory) an 29 Standorten einen Umsatz von rund 1,37 Milliarden Euro.

Seit vielen Jahren prüfen und beraten wir führende Industrie- und Dienstleistungsunternehmen jeder Größe. Stark ausgebaut wurde der Bereich „Familienunternehmen und Mittelstand“, der diese Unternehmen mit einem dichten Kontaktnetzwerk direkt vor Ort betreut. Auch Unternehmen der öffentlichen Hand, Verbände, kommunale Träger und andere Organisationen vertrauen unserem Wissen und unserer Erfahrung. Aus gutem Grund: Rund 440 Partner und 6.800 weitere Fachkräfte verfügen über umfassende Branchenkenntnisse in allen wichtigen Industrien.

Ergänzt wird unsere hohe Qualitätsorientierung durch den Anspruch, Mandanten vorausschauend zu betreuen: Wir antizipieren ihre Anliegen und führen sie einer zukunftsfähigen Lösung zu. Dadurch geben wir unseren Mandanten ein Höchstmaß an Handlungssicherheit in einem zunehmend komplexen Umfeld und helfen ihnen, auf den Märkten der Welt erfolgreich zu sein.

