COMPUTERWOCHE CIO ChannelPartner TECCHANNEL IT IM MITTELSTAND

IDG RESEARCH SERVICES

STUDIE CLOUD SECURITY 2016

PLATINPARTNER

FIT IT Solutions. Simplified.

GOLDPARTNER

Microsoft

TREND MICRO™ Securing Your Journey to the Cloud

Ein aktuelles Studienprojekt von

IDG
RESEARCH SERVICES

durchgeführt in Kooperation mit

Freudenberg IT
(Platinpartner)

und

Microsoft Deutschland
(Goldpartner)

Trend Micro Deutschland
(Goldpartner)

Alle Angaben in diesem Ergebnisband wurden mit größter Sorgfalt zusammengestellt. Trotzdem sind Fehler nicht ausgeschlossen. Verlag, Redaktion und Herausgeber weisen darauf hin, dass sie weder eine Garantie noch eine juristische Verantwortung oder jegliche Haftung für Folgen, die auf fehlerhafte Informationen zurückzuführen sind, übernehmen.

Die Cloud ist Vertrauenssache

Eines zeigt unsere Cloud-Studie deutlich: Die Cloud ist in den deutschen Unternehmen angekommen. Und beim Thema Cloud Security glaubt niemand, er könne einfach den Kopf in den Sand stecken und mit bester Vogel-Strauß-Politik die Herausforderungen verdrängen. Doch die Ergebnisse unserer Cloud-Studie bieten nicht nur Anlass zum Jubeln. So ist es geradezu erschreckend, wie langsam der deutsche Mittelstand das Thema Cloud angeht.

Ebenso schockierend ist der fast blauäugige Umgang mit Datenschutz und Datensicherung. Okay – das heißt nicht, dass sich deutsche Unternehmen nicht um die Security ihrer Daten kümmern. Eher das Gegenteil ist der Fall: Es wird zu viel und ohne Strategie geschützt. Und damit womöglich erst recht das eigene Unternehmen gefährdet, denn unter Experten ist unumstritten, dass diese Datenberge ökonomisch sinnvoll und effizient nicht mehr zu schützen sind.

Warum überlegen wir uns nicht, welche Daten wirklich schützenswert sind? Und für die anderen Informationen erlauben wir eine flexiblere Nutzung. Dabei handelt es sich um einen Punkt, der gerade im Cloud-Zeitalter und in unserer mobilen Gesellschaft immer wichtiger wird. Denn wenn wir unsere Daten nicht klassifizieren können, werden wir spätestens bei der Digitalisierung oder im Internet of Things in der Datenflut untergehen.

Zu einem entspannteren Umgang mit den Daten könnte auch mehr Transparenz der Provider führen. Denn die Cloud ist, wie unsere Studie zeigt, Vertrauenssache. Dabei sind Zertifikate und Audits nur ein

Jürgen Hill
Team-Leiter Technologie,
Leitender Redakteur
COMPUTERWOCHE

Aspekt, fast noch wichtiger sind vertrauensbildende Maßnahmen, damit sich der Anwender vor Ort im Rechenzentrum von den Sicherheitsmaßnahmen überzeugen kann.

Ich wünsche Ihnen eine spannende und anregende Lektüre mit unserer COMPUTERWOCHE-Studie „Cloud Security“.

Inhalt

Studien-steckbrief 6

Management Summary

Die Key Findings im Überblick 8

Die Key Findings im Einzelnen

1. Die Cloud ist angekommen 11
2. SaaS besonders beliebt 12
   SaaS-Nutzung nach Branchen 13
3. Datenschutz und Sicherheit 14
4. Datensicherheit 15
5. Sicherheits-Policies 16
   Sicherheits-Policies nach Branchen 17
6. Bring your own device (Byod) 18
7. Sicherheitsmaßnahmen in der Cloud 19
8. Wahl des Cloud-Partners 20
   Wahl des Cloud-Providers nach Branchen 21

8

Unsere Autoren / Vorschau Studienreihe 42

Kontakt / Impressum 43

Stichproben-statistik

7

Die Round Tables

Cloud Security ist kein Thema der Technik, sondern der Compliance 32
Das Cloud-Security-Studienprojekt 34
Ist die Cloud per se unsicher? 35

31

Weitere Studienergebnisse

Cloud Security ist Chefsache 23
Große Bedeutung von Audits und Zertifikaten 24
Wenig spezielle SLAs für Cloud-Services 25
Erwartungen an den Cloud-Provider 26
Erwartungen an das Cloud-Rechenzentrum 27
Sicherheit per Technik 28
Schatten-IT und Security 29
Schatten-IT in der Praxis 30

22

Unser Platinpartner Freudenberg IT stellt sich vor

39

Studiensteckbrief Cloud Security 2016

Herausgeber	COMPUTERWOCHE, CIO, TecChannel und ChannelPartner
Studienpartner	Freudenberg IT (Platin) Microsoft Deutschland (Gold) Trend Micro Deutschland (Gold)
Grundgesamtheit	Oberste (IT-)Verantwortliche von Unternehmen in der D-A-CH-Region: strategische (IT-)Entscheider im C-Level-Bereich, IT-Entscheider und IT-Spezialisten aus dem IT-Bereich
Teilnehmergenerierung	Stichprobenziehung in der IT-Entscheider-Datenbank von IDG Business Media. Persönliche E-Mail-Einladungen zur Umfrage
Gesamtstichprobe	517 Teilnehmer, die auf den Online-Fragebogen zugegriffen und die Fragen zumindest teilweise beantwortet haben. Nur die 335 abgeschlossenen und qualifizierten Interviews sind in die Ergebnisanalyse eingegangen.
Untersuchungszeitraum	10. Mai bis 27. Juni 2016
Methode	Online-Umfrage (CAWI)
Fragebogenentwicklung	IDG Research Services in enger Abstimmung mit den drei Studienpartnern
Durchführung	IDG Research Services
Technologischer Partner	Questback GmbH, Köln
Umfragesoftware	EFS Survey Spring 2016

Stichprobenstatistik

Branchenverteilung*	Energie- und Wasserversorgung	7,8 %
	Chemische und pharmazeutische Industrie	6,0 %
	Metallerzeugende und -verarbeitende Industrie, Maschinenbau, Fahrzeugbau	11,3 %
	Herstellung von elektrotechnischen Gütern, IT-Industrie	21,2 %
	Medienbranche	2,4 %
	Baugewerbe	3,9 %
	Handel	9,0 %
	Banken und Versicherungen	10,4 %
	Dienstleistungen für Unternehmen	22,7 %
	Öffentliche Verwaltung, Gebietskörperschaften, Sozialversicherung	7,5 %
	Schule, Universität, Hochschule	1,8 %
	Gesundheits- und Sozialwesen	3,6 %
	Andere Branchengruppe	15,3 %
Unternehmensgröße	Weniger als 100 Beschäftigte	25,6 %
	100 bis 499 Beschäftigte	23,3 %
	500 bis 999 Beschäftigte	17,6 %
	1.000 Beschäftigte und mehr	33,5 %
Umsatzklasse	Weniger als 100 Millionen Euro	49,8 %
	100 bis 999 Millionen Euro	33,2 %
	1 Milliarde Euro und mehr	16,9 %
Jährliche Aufwendungen für IT-Systeme	Weniger als 1 Million Euro	43,6 %
	1 bis 10 Millionen Euro	30,3 %
	10 bis 100 Millionen Euro	17,5 %
	100 Millionen Euro und mehr	8,6 %

** Mehrfachnennungen möglich*

Management Summary

Die Key Findings im Überblick

Cloud? Ja bitte!

Jedes **2.** Unternehmen nutzt bereits Cloud-Services.

15 % planen die Einführung.

Angst um die Daten

Spricht sich ein größeres mittelständisches Unternehmen gegen die Cloud aus, dann werden zu

77 %

Datenschutzgründe angeführt.

SaaS beliebt

Sechs von zehn Befragten sagen, dass ihre Unternehmen bereits Software-as-a-Service (SaaS) nutzen. Weniger hoch im Kurs stehen Dienste wie PaaS, IaaS oder CaaS.

Umfassende Security Policies

2/3 der Enterprise Player geben an, umfassende Sicherheitsrichtlinien erlassen zu haben.

Byod – weit verbreitet

60 %

der Unternehmen erlauben die Nutzung privater Smartphones im Berufsalltag.

Cloud Security

Die Hälfte der Unternehmen setzt beim Datentransport vom und zum Cloud-Provider auf eine verschlüsselte Datenübertragung.

Hohe Sicherheitsansprüche

der Unternehmen haben in Bezug auf ihre Daten hohe bis sehr hohe Sicherheitsansprüche.

Provider-Wahl ist Vertrauenssache

Mit **57 %**

ist das Vertrauen in den Cloud-Provider das meistgenannte Entscheidungskriterium bei der Wahl des passenden Cloud-Providers.

Die Key Findings im Einzelnen

Cloud Security 2016

1

Die Cloud ist angekommen

Die Frage, ob Cloud-Services im Unternehmen eingesetzt werden, stellt sich für das Gros der Befragten nicht mehr. Sie nutzen bereits heute die Cloud im täglichen Business.

- Etwas mehr als die Hälfte der Befragten sagt, dass ihre Unternehmen bereits jetzt Cloud-Dienste nutzen.
- Weitere 15 Prozent – also fast jedes dritte Unternehmen, das bis dato noch keine Cloud-Services bezieht – wollen Cloud-Services innerhalb der nächsten zwölf Monate einführen.
- In der Prüfungsphase, ob Cloud-Services für sie infrage kommen, befinden sich fast 20 Prozent der Befragten.
- Lediglich eine kleine Minderheit (rund zehn Prozent) schließt für sich eine Cloud-Nutzung kategorisch aus.
- Kaum eine Rolle spielen bei den Überlegungen in Sachen Cloud das gekündigte Safe-Harbor-Abkommen und sein Nachfolger, der Privacy-Shield. Lediglich etwas über 2 Prozent gaben zu Protokoll, deshalb von einer Cloud-Nutzung abzusehen.

Nutzt Ihr Unternehmen bereits Cloud-Services? Plant Ihr Unternehmen, in näherer Zukunft Cloud-Services in Anspruch zu nehmen?

	Prozent
Unser Unternehmen nutzt bereits Cloud-Services.	53,5
Unser Unternehmen plant konkret die Nutzung von Cloud-Services in den nächsten zwölf Monaten.	15,0
Die Nutzung von Cloud-Services wird in unserem Unternehmen geprüft.	18,9
Eine Entscheidung zur Nutzung von Cloud-Services liegt bis zur verbindlichen Nachfolgeregelung zum Safe-Harbor-Abkommen auf Eis.	2,4
Die Nutzung von Cloud-Services kommt für unser Unternehmen generell nicht infrage.	10,2

Basis: n = 460

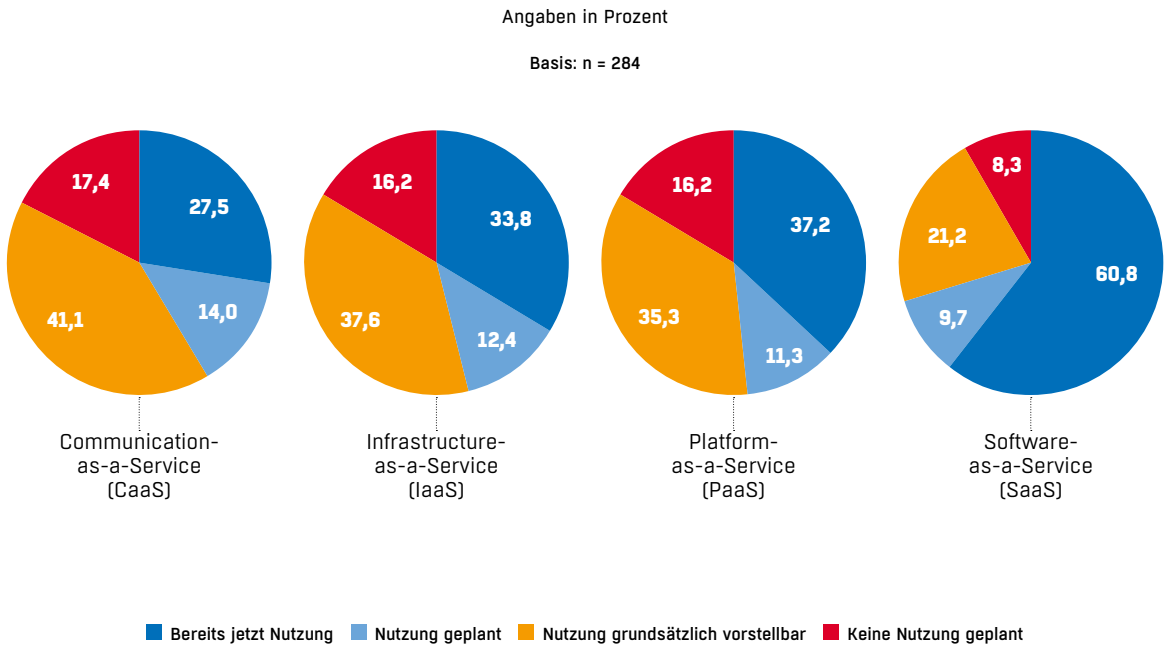
2

SaaS besonders beliebt

Zu den beliebtesten Cloud-Diensten zählt in den Unternehmen die Nutzung von Software-as-a-Service (SaaS). Dagegen steckt der Bezug von Kommunikations-Services aus der Cloud noch in den Kinderschuhen.

- Für 60 Prozent gehört die Nutzung von Software-as-a-Service bereits zum IT-Alltag.
- 30 Prozent planen bereits eine SaaS-Nutzung oder können sich dies grundsätzlich vorstellen.
- Verschwindend gering (rund 8 Prozent) ist der Anteil derer, die sich eine Verwendung von SaaS-Diensten nicht vorstellen können.
- Besonders fleißige SaaS-Nutzer sind dabei Kleinunternehmen und große Enterprise-Anwender, während sich der deutsche Mittelstand (100 bis 999 Beschäftigte) bei der Cloud-Nutzung zurückhaltender zeigt.
- Weniger hoch im Kurs stehen bei den Unternehmen Cloud-Dienste wie Platform-as-a-Service, Infrastructure-as-a-Service oder Communication-as-a-Service.

Welche der folgenden Arten von Cloud-Services nutzt Ihr Unternehmen bereits, welche kommen für Ihr Unternehmen grundsätzlich infrage, und welche sind für die Nutzung konkret geplant?



SaaS-Nutzung nach Branchen

Die Nutzung von Cloud-Services ist eine Sache der Unternehmensgröße? Ja! Aber die Unterschiede, die sich bei Auswertungen nach Unternehmensbranchen auftun, sind weitaus signifikanter.

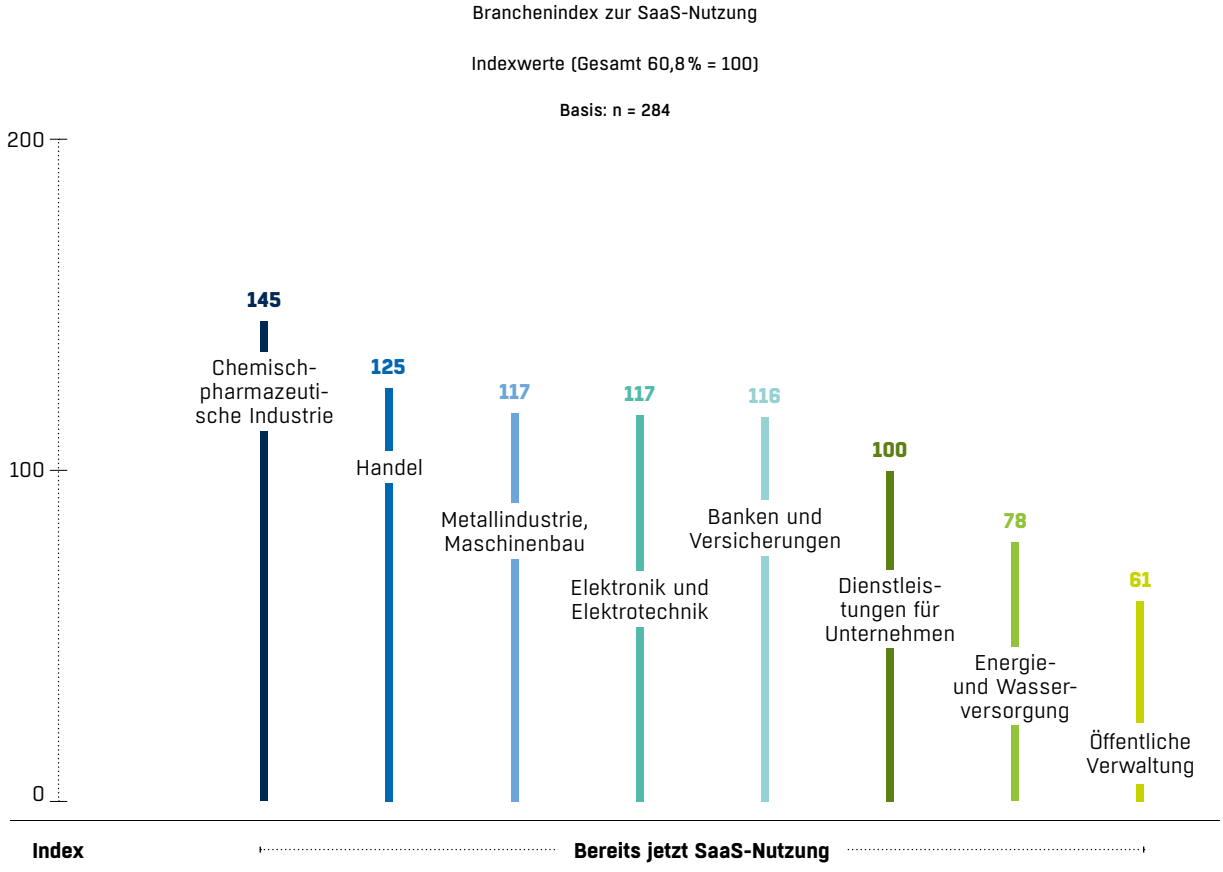
— 88 Prozent der chemisch-pharmazeutischen Industrie nutzen bereits SaaS. Auch beim Thema PaaS nimmt diese Branche mit knapp 63 Prozent eine Vorreiterrolle ein.

— Dagegen setzt nicht einmal jeder zweite Energie- und Wasserversorger SaaS ein. Noch zurückhaltender ist die öffentliche Verwaltung mit rund 37 Prozent. Tatsächliche Vorbehalte – oder mahlen dort die Mühlen einfach nur langsamer? Der Public Sector hat mit 21 Prozent den höchsten Anteil an geplanter SaaS-Nutzung.

— Beim Thema IaaS zeigen sich alle Branchen eher zurückhaltend.

— Communication-as-a-Service (CaaS) – also etwa Cloud-Telefonie – nutzen Pharma- und Chemie-Industrie (41 Prozent) sowie Banken und Versicherungen (knapp 39 Prozent) überdurchschnittlich häufig (Durchschnitt bei 28 Prozent).

Welche der folgenden Arten von Cloud-Services nutzt Ihr Unternehmen bereits, welche kommen für Ihr Unternehmen grundsätzlich infrage, und welche sind für die Nutzung konkret geplant?



3

Datenschutz und Sicherheit

Vor allem Sicherheitsbedenken und Datenschutzgründe halten Unternehmen von der Cloud-Nutzung ab. Erst mit weitem Abstand folgen Punkte wie ungeklärte Rechtsfragen, der noch nicht erkannte Business-Zweck oder die Angst vor einem Vendor-Lock-in.

— Datenschutzgründe sind für den gehobenen Mittelstand (500 bis 999 Mitarbeiter – 100 Prozent) der Hinderungsgrund Nummer eins, wenn sie sich gegen eine Cloud-Nutzung aussprechen.
— Des Weiteren führen sowohl Kleinstunternehmen als auch der Mittelstand Sicherheitsbedenken (rund 85 Prozent der Nennungen) an, während die Enterprise-Anwender dies nur zu 70 Prozent kritisch sehen.
— Die Befürchtungen in Sachen Datenschutz und Sicherheit ziehen sich quer durch alle Branchen, wenn man davon absieht, dass Datenschutzgründe lediglich von einem Viertel des Handels angeführt werden. Und interessanterweise haben nur 60 Prozent der Befragten aus der öffentlichen Verwaltung Sicherheitsbedenken.
— Den Großunternehmen scheint auch der Business-Nutzen der Cloud eher klar zu sein als den kleineren Unternehmen. Lediglich 14 Prozent erkennen keinen Business-Nutzen. Bei den Kleinunternehmen liegt dieser Wert um die 40 Prozent.

Warum Unternehmen ungern auslagern …

Mehrfachnennungen möglich

Basis: n = 46

	Prozent
Sicherheitsbedenken	82,6
Datenschutzgründe	73,9
Ungeklärte Rechtsfragen	39,1
Business-Nutzen von Cloud-Services nicht klar erkennbar	34,8
Befürchtete Abhängigkeit von einem Anbieter (Vendor-Lock-in)	30,4
Unklare Ziele einer Cloud-Nutzung	28,3
Schwierige Integration von Cloud-Services in die vorhandene IT-Infrastruktur	23,9
Interne Widerstände aus einzelnen Abteilungen (z.B. IT-Abteilung)	13,0
Bedenken / Abraten des IT-Dienstleisters	13,0
Fehlendes technisches Know-how (Cloud Skills)	8,7
Bedenken des Betriebsrats	8,7
Intransparentes Preisgefüge des Cloud-Anbieters	6,5
Wegen spezifischer Anwendungen, für die es derzeit keine Cloud-Lösung gibt	2,2
Unterschiedliche Anforderungen/Ziele von Fachabteilungen und IT	2,2
Andere Gründe	10,9

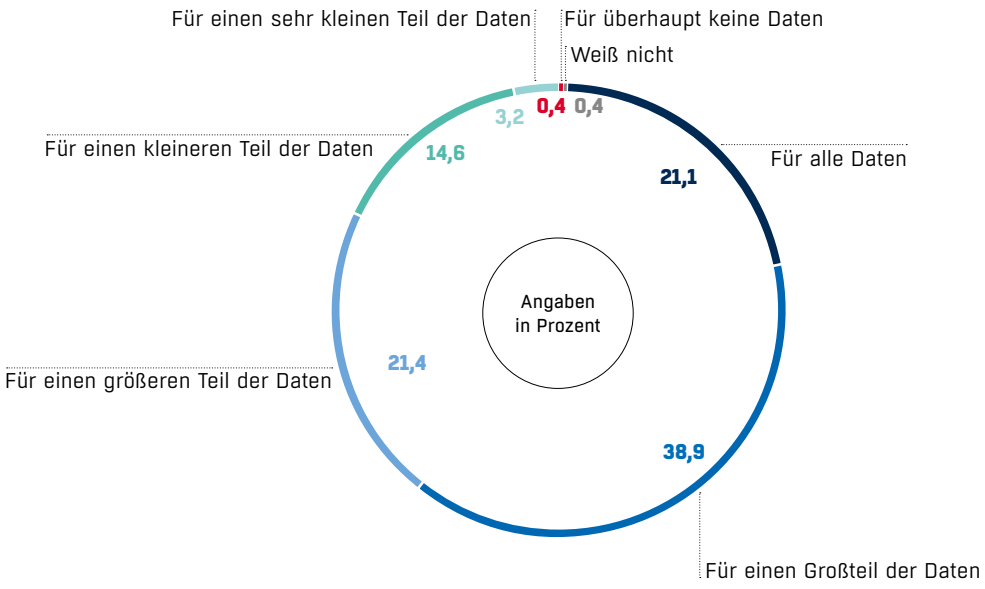
4 Datensicherheit

100 Prozent Sicherheit gibt es nicht. Deshalb ist es umso wichtiger, zu entscheiden, welche Daten schützenswert sind. Speziell für diese Daten sollten dann hohe Sicherheitsansprüche gelten.

- 60 Prozent der Befragten geben an, dass für einen Großteil bzw. alle Daten hohe bis sehr hohe Sicherheitsansprüche gelten.
- Auf der einen Seite ist diese Sensibilität in Sachen Sicherheit durchaus zu begrüßen, auf der anderen Seite liegt der Verdacht nahe, dass viele Unternehmen den Sensibilitätsgrad ihrer eigenen Daten nur unzureichend einstufen können, weil sie pauschal alles für schützenswert halten.
- Besonders hoch ist mit 40 Prozent im Handel der Anteil der Unternehmen, bei denen für alle Daten hohe Sicherheitsansprüche gelten.
- Wenn hohe Sicherheitsansprüche für die Daten gelten, dann ist dies eher in Großunternehmen (69 Prozent) der Fall als in kleinen Firmen (47 Prozent).

Wenn Sie einmal an die unterschiedlichen Arten und Kategorien von Daten in Ihrem Unternehmen denken: Für welchen Anteil der Daten gelten hohe bis sehr hohe Sicherheitsansprüche?

Basis: n = 280



5

Sicherheits-Policies

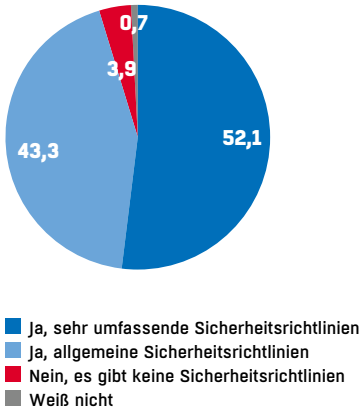
In Sachen Security zeigen sich die befragten Unternehmen vorbildlich. Fast 95 Prozent haben für ihre Mitarbeiter Sicherheitsrichtlinien für den Umgang mit der IT im Berufsalltag erlassen.

— Sehr umfassende Sicherheitsrichtlinien sind primär eine Domäne der großen Unternehmen. Zwei von drei Enterprises haben entsprechende Policies formuliert, während man sich nur in einem Drittel der Unternehmen mit bis zu 499 Mitarbeitern diese Mühe macht.
— Über die Hälfte dieser Unternehmen gibt allerdings zu Protokoll, zumindest allgemeine Sicherheitsrichtlinien zu erlassen.
— Jedes Zehnte der Kleinunternehmen mit weniger als 100 Mitarbeitern zeigt sich in Sachen Sicherheit gar ganz unbedarft: Es gibt keine Sicherheitsrichtlinien. Ein Unbedarftheit, die in dieser Form bei Großunternehmen nicht anzutreffen ist.

Gibt es in Ihrem Unternehmen Sicherheitsrichtlinien/-Policies?

Angaben in Prozent

Basis: n = 284

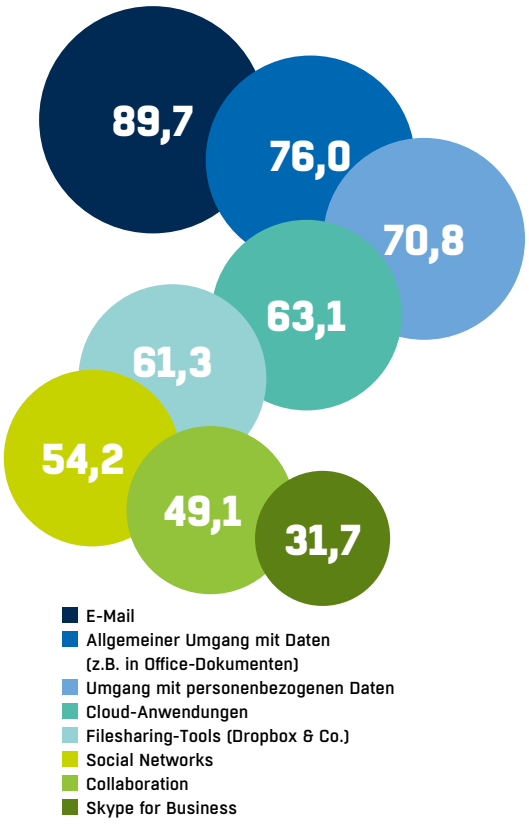


Auf welche der folgenden Anwendungsbereiche beziehen sich die Sicherheitsrichtlinien Ihres Unternehmens?

Mehrfachnennungen möglich

Angaben in Prozent

Basis: n = 271



Sicherheits-Policies nach Branchen

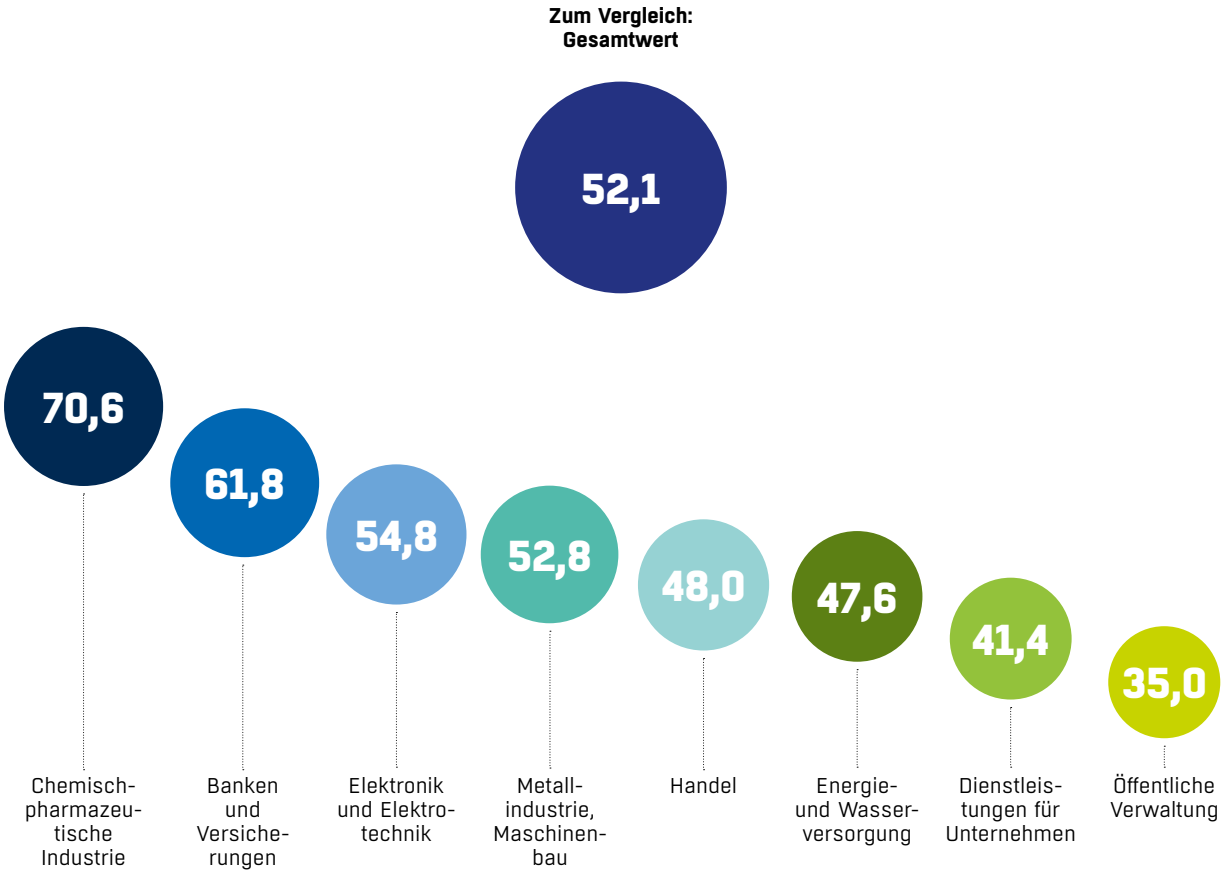
Auffallend ist, dass gerade die Branchen, die sich gegenüber der SaaS-Nutzung sehr offen zeigen, angeben, dass sie sehr umfassende Sicherheitsrichtlinien haben.

— Es scheint einen Zusammenhang zwischen Cloud-Nutzung und dem Vorhandensein von sehr umfassenden Sicherheitsrichtlinien zu geben.
— So geben über 70 Prozent der chemischen und pharmazeutischen Industrie sowie fast 62 Prozent der Banken und Versicherungen zu Protokoll, entsprechende Richtlinien erlassen zu haben.
— Dagegen gibt es nicht einmal bei jedem zweiten Energie- und Wasserversorger sehr umfassende Sicherheitsrichtlinien.
— Sehr gering ist dieser Anteil auch bei der öffentlichen Verwaltung mit 35 Prozent.

Gibt es in Ihrem Unternehmen Sicherheitsrichtlinien/-Policies?

Anteil der Nennungen „Ja, sehr umfassende Sicherheitsrichtlinien" nach Branchen; Angaben in Prozent

Basis: n = 284



6

Bring your own device (Byod)

Das eigene Smartphone, Tablet oder Notebook für die Arbeit nutzen? Was vor einigen Jahren lediglich ein Hype-Thema für Analysten und Berater war, ist mittlerweile im Alltag deutscher Unternehmen angekommen. Byod wird dabei vor allem in kleineren Unternehmen gelebt.

- Mit fast 65 Prozent ist das Smartphone das meistgenutzte private Device im Arbeitsalltag. Ebenso ist die Nutzung des eigenen Tablets im Beruf mit rund 60 Prozent sehr häufig. Etwas seltener ist mit 56 Prozent dagegen der Einsatz des eigenen Notebooks.
- Sehr offen in Bezug auf die Nutzung privater Endgeräte zeigen sich interessanterweise vor allem die kleinen und wiederum die ganz großen Unternehmen. Vor allem für kleinere Unternehmen ist Byod sicherlich auch eine Budgetfrage: Durch die Duldung privater Tablets und Smartphones im Business sparen sie einiges an Geld.
- Zurückhaltender agiert diesbezüglich der Mittelstand.
- Die Offenheit großer Unternehmen lässt sich unter anderem damit erklären, dass diese auch häufiger Sicherheitsrichtlinien erlassen. Zudem dürften sie sich eher die erforderlichen technischen Schutzmaßnahmen leisten können.
- Analysiert man die Byod-Nutzung nach Branchen, so zeigt sich, dass in der öffentlichen Verwaltung die Nutzung privater Endgeräte wie Tablets, Smartphones oder Notebooks eher unüblich ist.
- Überdurchschnittlich häufig ist dagegen die Verwendung im Handel.

Ist den Mitarbeitern in Ihrem Unternehmen die Nutzung privater Endgeräte erlaubt, die in die Firmen-IT-Umgebung eingebunden werden können (Bring your own device)?

Angaben in Prozent (Differenz zu 100 % = Weiß-nicht-Nennungen)

Basis: n = 269

	Smartphones	Tablets	Notebooks
Ja	41,3	36,2	37,3
Nur für ausgewählten Personenkreis	23,4	23,1	19,0
Nein	34,2	38,8	42,5

7

Sicherheitsmaßnahmen in der Cloud

Unternehmen stehen eine Reihe von technischen und organisatorischen Maßnahmen zur Verfügung, um ihre Daten in der Cloud zu schützen. So gehört eine verschlüsselte Datenübertragung vom und zum Cloud-Provider für die Hälfte der Unternehmen zum guten Ton.

- Verschlüsselte Datenübertragung, Compliance-Vorgaben, eine spezielle Cloud-Policy, ein verbessertes Passwortmanagement sowie eine verbesserte Zugangs- und Rechtekontrolle, das sind die Maßnahmen, die bei den Unternehmen besonders populär sind, um ihre Daten in der Cloud zu schützen.
- Auffallend ist, dass nur wenige Unternehmen (13 Prozent) einen Joiner-Mover-Leaver-Prozess etabliert haben. Gerade mit Blick auf die Cloud-Services verwundert dies, ist doch ein Zugriff auf diese Dienste in der Regel überall und auf jedem Endgerät möglich.
- Besondere organisatorische Maßnahmen wie etwa ein Vendor-Management etc. sind vor allem bei größeren Unternehmen anzutreffen, während die Verbreitung der technischen Maßnahmen nicht mit der Unternehmensgröße skaliert.
- Ein ebenso signifikantes wie nachvollziehbares Ergebnis ist, dass vor allem die öffentliche Verwaltung (75 Prozent) Wert auf eine verschlüsselte Datenübertragung legt.
- Ebenso spielen dort Compliance-Aspekte eine große Rolle. Dies wird lediglich noch von der Chemie- und Pharmaindustrie (66 Prozent) übertroffen.

Welche organisatorischen wie auch technischen Vorkehrungen sind in Ihrem Unternehmen in Bezug auf Cloud Security getroffen worden?

Mehrfachnennungen möglich

Basis: n = 289

	Prozent
Verschlüsselte Datenübertragung vom und zum Cloud-Provider	51,9
Vorkehrungen für Compliance (in welchem Land liegen welche Daten?)	48,8
Cloud-Policy für die Nutzung von Cloud-Lösungen und Zugangsgeräten	42,9
Verbessertes Passwortmanagement (starke Passwörter, kurze Wechselzyklen)	36,0
Verbesserte Zugangs- und Rechtekontrolle (IAM)	38,8
Lokale Daten-Backups möglich	26,0
Detailliertes Konzept für das Vendor-Management	22,5
Gute Endpoint-Kontrolle (sichere Clients)	22,5
Starke Kontrolle über System-Level-Ressourcen und Virtual Machines	20,8
Person, die für die Steuerung der Cloud-Services-Anbieter zuständig ist	20,1
Neue Security-Stellen	18,7
Joiner-Mover-Leaver-Prozess (Prozedere bei Mitarbeiterwechsel)	12,8
Andere organisatorische Vorkehrungen	2,4
Andere technische Vorkehrungen	2,1

8

Wahl des Cloud-Partners

Die Wahl des Cloud-Providers ist derzeit primär Vertrauenssache. Für 57 Prozent der Befragten ist dies das wichtigste Kriterium bei der Wahl eines Cloud-Anbieters. Andere Kriterien folgen erst mit deutlichem Abstand.

- Ein weiteres wichtiges Entscheidungskriterium bei der Auswahl des Cloud-Providers ist das Preis-Leistungs-Verhältnis.
- Günstig allein reicht dabei allerdings nicht. Über ein Drittel erwartet von seinem künftigen Partner auch ein transparentes Preisgefüge. Dieser Punkt ist damit für die Befragten fast genauso wichtig wie die Lokation des Rechenzentrums, in dem die Cloud-Anwendungen gehostet werden.
- Zwei weitere wichtige Entscheidungskriterien sind für rund 40 Prozent der Unternehmen die Skalierbarkeit des Dienstes sowie das technologische Know-how des Cloud-Partners.
- Auffallend ist, dass die Bedeutung des Entscheidungskriteriums „Vertrauen in den Anbieter" in kleinen Unternehmen deutlich stärker ausgeprägt ist. Bei Großunternehmen hingegen ist die Skalierbarkeit der Dienste deutlich relevanter.

Was sind für Ihr Unternehmen zunächst einmal die maßgeblichen Kriterien bei der Auswahl eines geeigneten Cloud-Providers?

Ranking der Top-15-Antworten (von insgesamt 23 gestützt vorgegebenen Antwortmöglichkeiten)

Basis: n = 289

	Prozent
Vertrauen in den Anbieter	57,1
Gutes Preis-Leistungs-Verhältnis	50,9
Technologisches Know-how	40,5
Skalierbarkeit	40,1
Lokation des Rechenzentrums	36,7
Transparentes Preisgefüge	35,6
Branchenkompetenz	31,5
Gute Zusammenarbeit bei anderem IT-Projekt	26,6
Fester Ansprechpartner	26,0
Prozess-Know-how	25,6
1st-/2nd-Level-Support	23,9
Persönlicher Kontakt	21,8
Internationale / globale Ausrichtung des Partners	21,1
Serviceerbringung nach ISO 20000 (ITIL-Prozesse)	21,1
Innovationskraft	20,8

Wahl des Cloud-Providers nach Branchen

Allerdings spielen die einzelnen Auswahlkriterien je nach Branche eine unterschiedliche Rolle. Dies zeigt sich beispielsweise deutlich beim Kriterium „Vertrauen in den Anbieter".

- Während etwa 62 Prozent der Dienstleister oder 58 Prozent der IT-Industrie/Hersteller elektrotechnischer Güter dieses Kriterium nennen, spielt es nur bei rund 38 Prozent der Energie- und Wasserversorger sowie in der Chemie- und-Pharmaindustrie eine Rolle.
- Dagegen achten Energie- und Wasserversorger überdurchschnittlich auf Aspekte wie 1st-/2nd-Level-Support (24 Prozent) oder Helpdesk-Funktion (38 Prozent).
- Auf eine Skalierbarkeit des Cloud-Angebots legt jedes zweite Unternehmen der metallverarbeitenden und -erzeugenden Industrie sowie im Banken- und Versicherungssektor Wert, während dies bei der Gesamtheit der Stichprobe nur zu 40 Prozent der Fall ist.
- Sehr wichtig ist Banken und Versicherungen sowie Chemie- und Pharmaunternehmen auch die Branchenkompetenz – für die Gesamtheit der Befragten gilt dies nur für 31 Prozent.

Was sind für Ihr Unternehmen zunächst einmal die maßgeblichen Kriterien bei der Auswahl eines geeigneten Cloud-Providers?

Mehrfachnennungen möglich

Angaben in Prozent

Basis: n = 269

	Vertrauen in den Anbieter	Skalierbarkeit	Branchenkompetenz	Wichtigstes Kriterium
Gesamt	**57,1**	**40,1**	**31,5**	**Vertrauen in den Anbieter**
Energie- und Wasserversorgung	38,1	28,6	28,6	u.a. Vertrauen in den Anbieter (38,1 %)
Chemisch-pharmazeutische Industrie	38,9	44,4	50,0	Prozess-Know-how (61,1 %)
Metallindustrie, Maschinenbau	44,4	50,0	19,4	Gutes Preis-Leistungs-Verhältnis (55,6 %)
Elektronik und Elektrotechnik	58,1	46,8	30,6	Vertrauen in den Anbieter (58,1 %)
Handel	57,7	30,8	34,6	Gutes Preis-Leistungs-Verhältnis (61,5 %)
Banken und Versicherungen	44,1	52,9	47,1	Skalierbarkeit (52,9 %)
Dienstleistungen für Unternehmen	62,3	34,4	37,7	Vertrauen in den Anbieter und gutes Preis-Leistungs-Verhältnis (jeweils 62,3 %)
Öffentliche Verwaltung	55,0	35,0	35,0	Lokation des Rechenzentrums (70,0 %)

Weitere Studienergebnisse

Cloud Security 2016

Cloud Security ist Chefsache

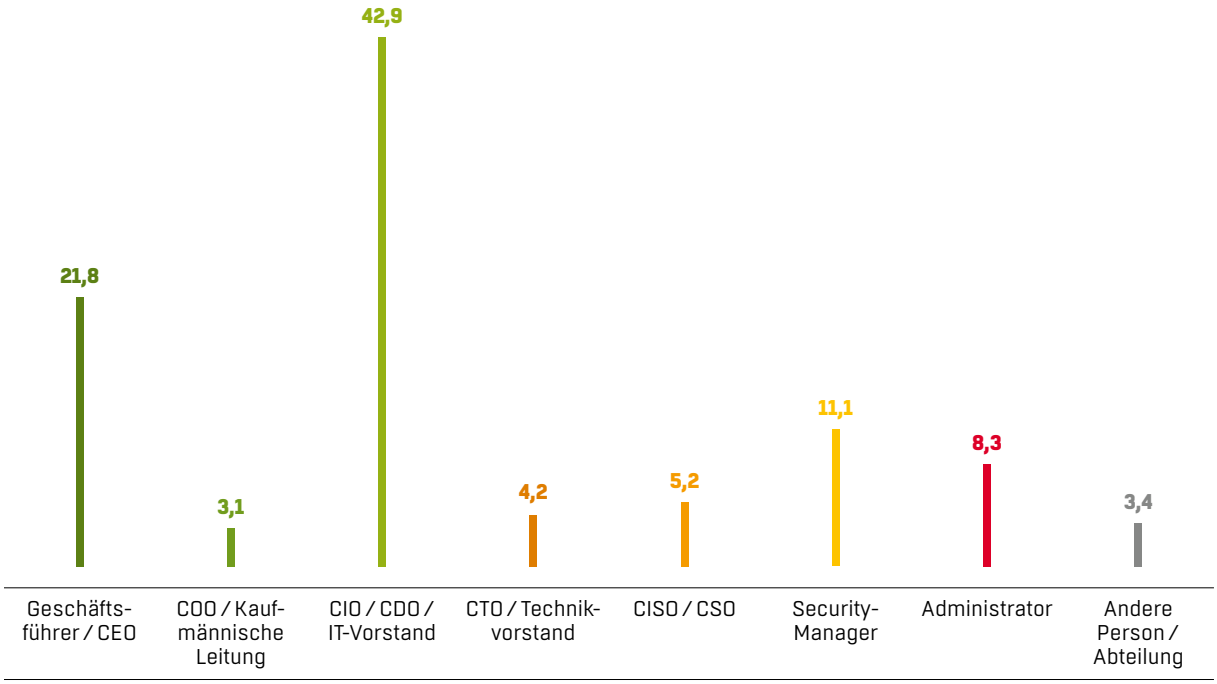
Geht es um Cloud Security, so ist dieses Thema eindeutig Chefsache und auf der C-Level-Ebene angesiedelt. In über 60 Prozent der Unternehmen fallen dort die Entscheidungen zu Cloud-Security-Fragen.

- Überraschend ist vor allem, dass die Security-Verantwortung nur selten an dedizierte Security-Manager (11 Prozent) oder den CISO / CSO (5 Prozent) delegiert wird. Selbst bei größeren Unternehmen mit mehr als 500 Mitarbeitern ist das nur geringfügig häufiger der Fall.
- Durch die Bank haben CTO beziehungsweise Technikvorstand kaum Verantwortung für die Cloud Security.
- Deutliche Unterschiede hinsichtlich der Verantwortung zeigen sich in Korrelation zur Unternehmensgröße. Während bei den Kleinunternehmen bei rund 52 Prozent das Thema beim Geschäftsführer / CEO angesiedelt ist, ist bei den Enterprise-Unternehmen lediglich jeder zehnte Geschäftsführer / CEO damit befasst.
- In Großunternehmen ist Security ganz klar eine Domäne von CIO / CDO / IT-Vorstand (56 Prozent). Bei Kleinunternehmen sind es dagegen nur 11 Prozent. Eine Erklärung hierfür ist sicher, dass bei diesen Unternehmen häufig keine solche Position existiert.
- Besonders stark sind CIO / CDO / IT-Vorstand in den Branchen Metallindustrie (50 Prozent) sowie Banken und Versicherungen (fast 60 Prozent) für die Cloud Security verantwortlich.

Wer in Ihrem Unternehmen ist federführend verantwortlich für Cloud Security?

Angaben in Prozent

Basis: n = 289



Große Bedeutung von Audits und Zertifikaten

Bei der Wahl ihres Cloud-Providers legen die deutschen Unternehmen viel Wert auf das Vorhandensein von ISO-Zertifizierungen, Siegeln und Prüfungen. Wer als Cloud-Anbieter bei einer Entscheidung in die engere Wahl kommen will, ist zudem gut beraten, sich auch Audits zu unterziehen.

- Spricht sich ein Unternehmen für Audits aus, dann werden in diesem Zusammenhang ebenfalls primär Zertifizierungen überprüft.
- Ganz oben steht auf der Checkliste zudem der Ort der Datenspeicherung.
- Weitere Kriterien, die im Zuge eines Audits überprüft werden, sind die SLAs, die Finanzkraft eines Anbieters sowie die Erfahrungen, die andere Kunden mit dem Cloud-Provider gemacht haben.
- Fast 70 Prozent der Entscheider legen Wert auf das Vorhandensein von (ISO-)Zertifikaten etc.
- Noch höher ist dieser Wert mit 94 Prozent in der Chemie-und Pharmaindustrie sowie bei Banken und Versicherungen mit fast 80 Prozent.
- Die Bedeutung dieser Nachweise korreliert mit der Unternehmensgröße. Während lediglich etwa die Hälfte der Kleinunternehmen auf solche Zertifikate Wert legt, achten über 80 Prozent der Enterprise-Anwender auf entsprechende Nachweise.

Was beinhaltet ein Audit, in dessen Rahmen Ihr Unternehmen einen Cloud-Provider überprüft?

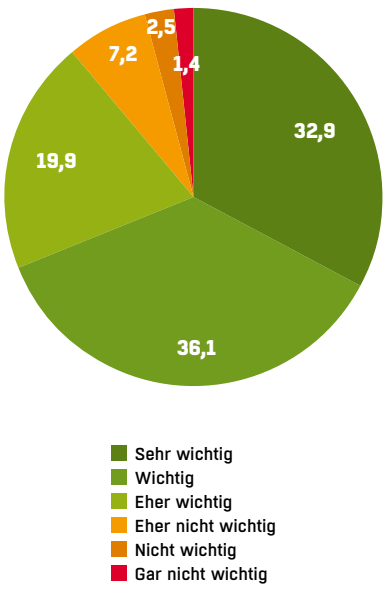
Mehrfachnennungen möglich

	Prozent
Zertifizierungen	56,7
Orte / Lokationen der Datenspeicherung	49,1
Service-Level-Agreements (SLA)	39,1
Größe und Finanzkraft des Anbieters	34,9
Erfahrungen anderer Kunden	32,5
Internationale Präsenz des Anbieters	27,3
Andere Prüfkriterien	1,4
Wir führen keine Audits von Cloud-Providern durch	15,9

Basis: n = 289

Wie wichtig sind Ihnen (ISO-)Zertifizierungen, Nachweise, Siegel und Prüfungen?

Angaben in Prozent



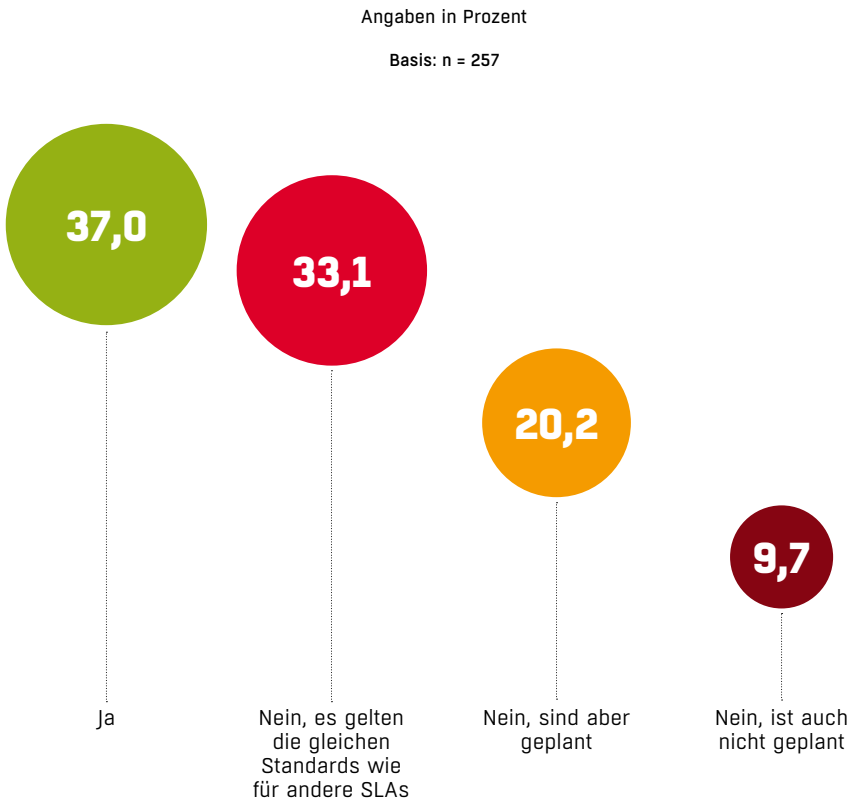
Basis: n = 277

Wenig spezielle SLAs für Cloud-Services

Fast zwei Drittel der deutschen Unternehmen definieren für Cloud-Dienste keine speziellen Service Level Agreements (SLAs). Allerdings zeigt eine detaillierte Betrachtung der Ergebnisse teilweise beträchtliche Unterschiede in der Sichtweise – je nach Unternehmensgröße und nach Branche.

- Ein Drittel der befragten Unternehmen sagt, dass die gleichen Standards wie für andere SLAs gelten.
- Dass es im Unternehmen spezielle Service Level Agreements (SLAs) für Cloud-bezogene Dienste gibt, sagen 37 Prozent. Hier gibt es aber sehr unterschiedliche Ergebnisse. Es besteht eine starke Korrelation mit der Unternehmensgröße. So existieren in zwei Dritteln der sehr großen Unternehmen (mit über einer Mrd. Euro Umsatz) spezielle SLAs.
- In jedem fünften Unternehmen sind solche SLAs geplant, in zehn Prozent gibt es keine speziellen SLAs und sind auch nicht geplant.
- Wenig überraschend ist das Ergebnis, dass der Anteil der Unternehmen im Finanzsektor überdurchschnittlich häufig über spezielle Service Level Agreements bezüglich der Cloud verfügt: Er liegt bei knapp 60 Prozent. Es erstaunt vielleicht sogar eher noch, dass der Wert nicht noch höher ausfällt.

Gibt es in Ihrem Unternehmen spezielle Service Level Agreements (SLAs) für Cloud-bezogene Dienste?



Erwartungen an den Cloud-Provider

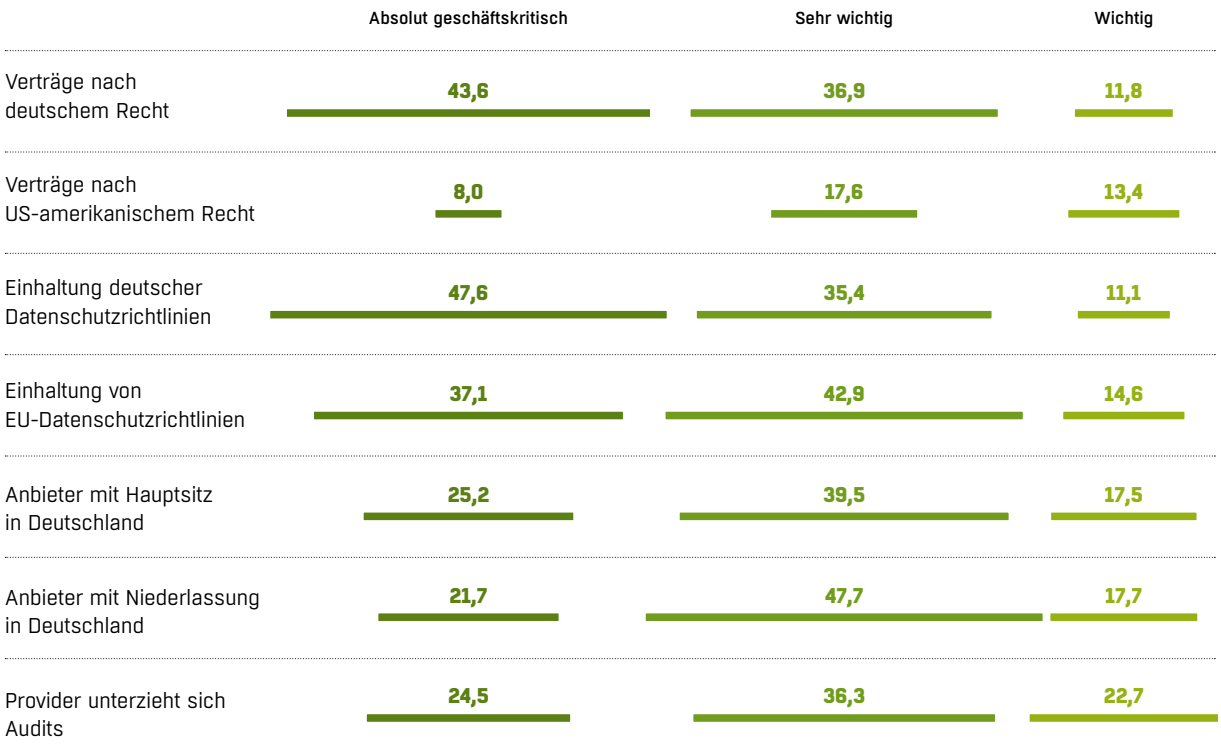
Hält ein Cloud-Anbieter deutsche oder EU-Datenschutzrichtlinien nicht ein, so braucht er bei den Unternehmen dieser Studie erst gar nicht antreten. Jeweils deutlich über 90 Prozent werteten diese Punkte als wichtig bezüglich Standort und Compliance.

- Ein weiteres Must-have (über 90 Prozent) ist für die Unternehmen ein Vertrag, der nach deutschem Recht abgeschlossen wird. Verträge nach US-amerikanischem Recht sind hingegen nur für ein Drittel ein wichtiges Kriterium.
- Ein Punkt, auf den alle Befragten aus der öffentlichen Verwaltung (100 Prozent) achten.
- Mehr als 80 Prozent achten zudem darauf, dass der Cloud-Partner seinen Hauptsitz in Deutschland hat beziehungsweise hier zumindest mit einer Niederlassung vertreten ist.
- Auch hier achtet besonders die öffentliche Hand auf eine Cloud-Datenverarbeitung in Deutschland. Lediglich bei den Dienstleistungsunternehmen spielt dies ein untergeordnete Rolle.
- Ebenso legen über 80 Prozent auf die bereits angesprochenen Audits Wert.

Wie wichtig ist es Ihrem Unternehmen, dass der Cloud-Provider den folgenden Kriterien bezüglich Standort und Compliance entspricht?

Bewertung auf siebenstufiger Skala von 1 (Absolut geschäftskritisch) bis 7 (Gar nicht wichtig)

Angaben in Prozent
Basis: n = 289



Erwartungen an das Cloud-Rechenzentrum

Sicher, transparent und deutsch – mit diesen drei Schlagworten lassen sich die Kriterien zusammenfassen, auf die Unternehmen achten, wenn es um das Rechenzentrum des Cloud-Providers geht.

— Ein absolutes Muss ist für über 95 Prozent der Unternehmen die Ausfallsicherheit. Und im Falle eines Desasters sollte der Provider die Datenwiederherstellung garantieren können.
— Gerade Energie- und Wasserversorger sind bei diesem Punkt sehr sensibel.
— Sehr wichtig ist für etwas über 90 Prozent der Unternehmen die Transparenz. Sie erwarten, dass der Provider sie bei Untersuchungen bezüglich Vorfällen und Anwenderaktivitäten unterstützt.
— Genauso wichtig ist den Unternehmen, dass ihre Daten abgeschottet von den Daten anderer Kunden behandelt werden.
— Dieser Aspekt gilt besonders für 90 Prozent der öffentlichen Verwaltung.
— Wichtig ist den Anwendern zudem, dass das Rechenzentrum in Deutschland steht und ein deutscher Support erhältlich ist.

Wie wichtig sind Ihrem Unternehmen die folgenden Kriterien bezüglich des Rechenzentrums?

Bewertung auf siebenstufiger Skala von 1 (Absolut geschäftskritisch) bis 7 (Gar nicht wichtig)

Angaben in Prozent
Basis: n = 289

	Absolut geschäftskritisch	Sehr wichtig	Wichtig
Rechenzentrum in Deutschland mit deutschem Rechenzentrumsbetrieb und deutschem Support	31,1	43,6	13,6
Rechenzentrum in Deutschland mit globalem Rechenzentrumsbetrieb und Support	13,3	36,3	24,4
Rechenzentrum in EU	15,8	35,7	23,7
Begehbares Rechenzentrum	11,3	26,7	19,9
Backup-Rechenzentrum	22,3	37,8	23,4
Abstand zwischen RZ und Backup-RZ mehr als 10 Kilometer	13,7	23,3	25,6
Abstand zwischen RZ und Recovery-RZ mehr als 100 Kilometer	8,0	25,5	18,3
Hardware namhafter Hersteller	10,8	36,1	23,8
Provider behandelt meine Daten abgeschottet von denen anderer Kunden	30,8	42,3	17,6
Ausfallsicherheit: Provider kann Datenwiederherstellung im Falle eines Desasters garantieren	43,4	37,4	12,5
Provider unterstützt Untersuchungen bzgl. Vorfällen und Anwenderaktivitäten in der Cloud	23,6	45,7	20,6
RZ gemäß Qualitätsstufe Tier III	15,6	36,6	27,9
RZ gemäß Qualitätsstufe Tier IV	14,5	37,4	27,5

Sicherheit per Technik

Bei den technischen Maßnahmen, die Unternehmen vom Cloud-Provider erwarten, kristallisieren sich zwei Felder heraus: Daten sollten verschlüsselt verarbeitet werden, und der Provider sollte über entsprechende Backup- und Recovery-Funktionen verfügen.

- Drei Viertel der Unternehmen legen Wert darauf, dass ihre Daten in der Cloud verschlüsselt übertragen und gespeichert werden. Fast 40 Prozent wünschen sich dies auch bei der Verarbeitung ihrer Daten.
- Knapp 70 Prozent der Befragten erwarten von ihrem Provider, dass er Authentifizierungssysteme einsetzt. Überdurchschnittlich häufig (über 80 Prozent) nennen Unternehmen aus dem Energiesektor, der chemischen Industrie sowie der öffentlichen Verwaltung diesen Punkt.
- Im Fall der Fälle legen Unternehmen großen Wert auf Datensicherheit: Über 60 Prozent setzen ein Backup durch den Provider voraus, über die Hälfte der Unternehmen auch ein zeitnahes Desaster-Recovery. Hierauf legen speziell Chemieunternehmen, Dienstleister und die öffentliche Hand besonderen Wert.
- Die NSA-Affäre scheint auch bei den deutschen Anwendern ihre Spuren hinterlassen zu haben: Fast 20 Prozent erwarten, dass die Servertechnik nicht aus den USA stammt. Noch größer ist der Argwohn gegenüber Technik aus China.
- Besonders groß ist das Misstrauen gegenüber Servertechnik made in USA in der chemischen und elektrotechnischen Industrie (über 27 Prozent). Das Misstrauen gegenüber chinesischer Technik ist dagegen fast durchweg über alle Branchen gleich verteilt.

Welche technischen Maßnahmen erwarten Sie von einem Cloud-Provider zum Schutz der Daten?

Mehrfachnennungen möglich

Basis: n = 289

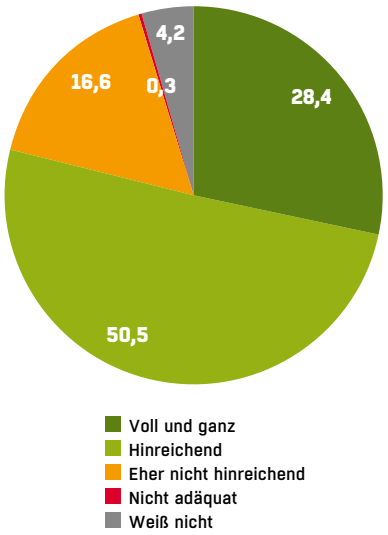
	Prozent
Verschlüsselung (Übertragung und Speicherung)	76,5
Authentifizierung	69,2
Backup der Daten	60,6
Zeitnahes Desaster-Recovery	54,3
Einsatz von Prevention- und Detection-Systemen	43,6
Weitestgehend verschlüsselte Verarbeitung der Daten	38,4
Single-Sign-On	37,0
State-of-the-Art-Servertechnik	36,7
Zertifizierungen nach ISO 27001	36,3
Servertechnik nicht aus China	24,2
Servertechnik nicht aus den USA	19,0
Compliance gemäß Vorgabe der FDA / GxP	13,8
Compliance gemäß Vorgabe der US-Börsenaufsicht	9,7

Schatten-IT und Security

Die Ergebnisse rund um das Thema Schatten-IT vermitteln einen zwiespältigen Eindruck: Auf der einen Seite scheinen Unternehmen das Thema erkannt zu haben und anzugehen – auf der anderen Seite liegt der Verdacht einer gewissen Blauäugigkeit nahe.

- Fast 80 Prozent der befragten Unternehmen glauben, dass sie mit den Risiken durch Schatten-IT adäquat umgehen.
- Lediglich in der öffentlichen Verwaltung und bei den Energie- und Wasserversorgern sind diesbezüglich gewisse Selbstzweifel zu bemerken, da hier nur rund 70 Prozent diese Frage positiv beantworten.
- Des Weiteren glauben etwa 62 Prozent, dass eine Nutzung von Public-Cloud-Diensten ohne Freigabe durch die IT nicht erfolgt.
- Zudem sind Dropbox und Co. in fast 65 Prozent der Unternehmen verboten.
- Allerdings ist es mehr als zweifelhaft, dass diese Verbote in der Praxis auch eingehalten werden, denn lediglich 55 Prozent unterbinden die Nutzung technisch. Knapp 40 Prozent setzen auf Arbeitsanweisungen und Ähnliches.

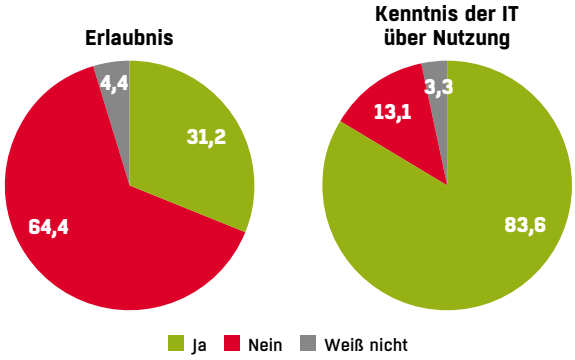
Glauben Sie, dass Ihr Unternehmen mit dem Phänomen Schatten-IT und den daraus resultierenden Sicherheitsrisiken insgesamt adäquat umgeht?



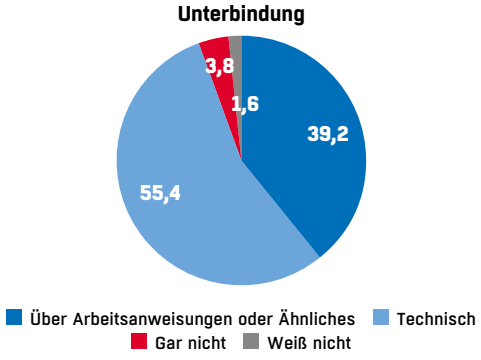
Angaben in Prozent

Basis: n = 277

Nutzung von Public-Cloud-Diensten



Unterbindung der Public-Cloud-Nutzung, wenn im Unternehmen untersagt



Basis:
n = 202; n = 130; n = 61 Befragte aus dem IT-Vorstand / IT-Bereich

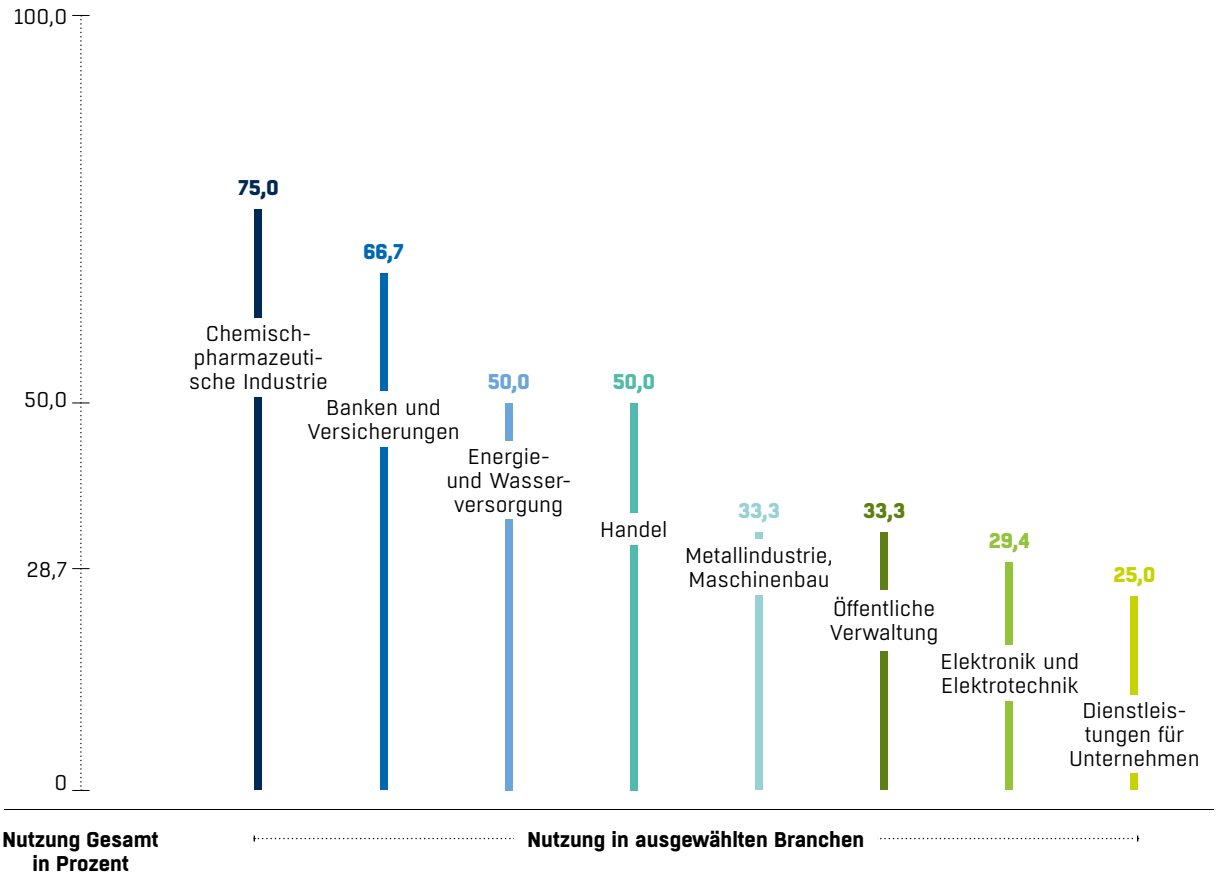
Schatten-IT in der Praxis

Während das Gros der Unternehmen glaubt, dass es das Phänomen der Schatten-IT gut im Griff hat, zeigt sich ein ganz anderes Bild, wenn man die Fachbereiche danach befragt, ob sie Public-Cloud-Services ohne Freigabe durch die IT nutzen.

- Ganz offensichtlich reicht es nicht, die Public-Cloud-Nutzung „nur" per Arbeitsanweisung zu unterbinden. Knapp 29 Prozent der Befragten aus den Fachbereichen geben zu, dass sie die Public Cloud ohne Freigabe der zentralen IT nutzen.
- In der Chemie- und Pharmaindustrie bejahen diese Frage sogar drei Viertel der Befragten. Und selbst im Bankenbereich, von dem eigentlich ein gewisses Sicherheitsbewusstsein erwartet wird, ist dieser Anteil mit 67 Prozent erstaunlich hoch.
- Auch interessant: Jeder zehnte Befragte aus den Fachbereichen kann nicht sagen, ob in seinem Bereich die Public Cloud genutzt wird.
- Wenn die Fachbereiche die Public Cloud nicht nutzen, dann vor allem deswegen, weil es Datenschutzvorbehalte gibt und die Public Cloud insgesamt als zu unsicher angesehen wird.

Nutzung von Public-Cloud-Diensten durch die Fachbereiche ohne Freigabe durch die zentrale IT

Angaben in Prozent
Basis: n = 87



Die Round Tables

Cloud Security 2016

Cloud Security ist kein Thema der Technik, sondern der Compliance

Mit dem Internet of Things (IoT) und der Digitalisierung der Wirtschaft gewinnt die Frage nach der Cloud Security immer mehr an Bedeutung. Am COMPUTERWOCHE-Round-Table „Cloud Security“ diskutierten CIOs kontrovers über das Thema.

Von Jürgen Hill

An der Cloud führt im Prinzip kein Weg mehr vorbei. Darüber waren sich die Teilnehmer des COMPUTERWOCHE-Round-Table „Cloud Security“, Dr. Werner Gutau, verantwortlich für die Sicherheit der Division Chip Card & Security der Infineon Technologies AG, Thomas Schott, ehemals CIO bei Rehau, Dr. Rolf Reinema, Head of Technology Field IT-Security bei der Siemens AG, sowie Gerald Götz, CIO beim Städtischen Klinikum München, einig. So sprach Thomas Schott, dessen Unternehmen seit 2007 auf eine Private Cloud setzt, für viele, wenn er meinte, die heute geforderte Agilität und Schnelligkeit im Geschäftsleben könne nur noch durch Cloud-Lösungen gewährleistet werden.

Ein differenzierteres Bild zeigt sich dagegen bei der Frage Private oder Public Cloud. Hier spielen gleich mehrere Aspekte eine Rolle. So war unter den Teilnehmern eine weitverbreitete Skepsis gegenüber den Public-Cloud-Angeboten hinsichtlich der Sicherheit zu spüren. „Für unsere sensiblen Daten kommt nur die Private Cloud infrage“, bekräftigte Götz, „zumal wir in der Public Cloud keinen deutlichen Vorteil sehen.“

Offen allerdings ist die Frage, ob sich diese Unterscheidung Private oder Public Cloud in der Praxis wirklich so eindeutig treffen lässt. Eventuell befinden sich viele Unternehmen bereits bewusst oder unbewusst in einer Hybrid Cloud, da ihre Mitarbeiter Public-Cloud-Dienste nutzen – und sei es nur auf dem eigenen Smartphone. Aber bekanntlich bestimmt ja das schwächste Glied einer Kette die Gesamtsicherheit.

CIO Götz drückt der Schuh in Sachen Cloud und Security an ganz anderer Stelle: „Uns lässt das bayerische Datenschutzgesetz keinen Spielraum“, klagt Götz. „Die Cloud könnte nämlich für die Patienten einen Quantensprung bei der Behandlung bringen“, schwärmt der IT-Verantwortliche. Gerade im medizinischen Umfeld lassen sich viele Anwendungsfälle finden, die von Cloud-Lösungen profitieren würden, wenn es denn die Gesetzeslage erlauben würde. „Die Sicherheitstechnik ist nicht das Problem“, so Götz. So ist für die Diskussionsteilnehmer am Security-Round-Table weniger die Sicherheitstechnik eine Frage, sondern eher das Thema Compliance und Recht ein Problemfeld, wenn nicht gar ein Minenfeld.

Angesichts solcher und anderer Unwägbarkeiten kann sich die Diskussionsrunde nur schwer mit dem Gedanken anfreunden, dass in einigen Jahren eine Erbringung von IT-Leistungen ohne Cloud-Services eventuell komplett unmöglich ist. So ist etwa Schott überzeugt, dass man künftig um gewisse Cloud-Anwendungen nicht herumkommen werde, nachdem er bereits heute dediziert Cloud-Anwendungen wie zum Beispiel Salesforce einsetzt. Deshalb sei es wichtig, die Cloud so kompatibel wie möglich zu den Standards der Anwenderunternehmen zu gestalten, um agil und flexibel handeln zu können. Gutau von Infineon unterstützt dies durchaus, weist aber darauf hin, dass sein Unternehmen Kundenbeziehungen pflege, die geschützt werden müssten.

Dies sei mit den momentan verfügbaren Sicherheitsmechanismen in der Public Cloud nicht gewährleis-

tet. „Und was machen Sie, wenn zwei Unternehmen fusionieren, die bei unterschiedlichen Cloud-Anbietern sind?“, fragt Gutau weiter und kommt zu dem Schluss: „Die Zusammenführung der Daten kann je nach vertraglicher Situation sehr problematisch sein.“ Letztlich, so sein Credo, müsse jedes Unternehmen für sich klären, wie es mit diesen Fragen umgeht.

Götz wirft die These in den Raum, dass, „wenn wir deutsches Recht umsetzen, die Sache eigentlich okay sein müsste, schließlich sind wir weltweit als die German Ängstler bekannt“. Allerdings hat er mit einer Besonderheit zu kämpfen: Obwohl das Gesundheitswesen als einer der Wachstumsmärkte der Zukunft gilt, sieht sich Götz immer wieder mit steinzeitlichen Vorstellungen konfrontiert, etwa einem Bayerischen Krankenhausgesetz Art 27, das im Jahr 2016 noch Vorschriften zur Verarbeitung vom Mikrofilmen enthält und nur die Datenverarbeitung in anderen Krankenhäusern erlaubt, oder wie es Götz formuliert: „Einen Cloud-Service, der Patientendaten verarbeitet, dürfte ich nur von einem anderen Krankenhaus beziehen.“

Götz sieht sich hier mit einem Spannungsbogen zwischen Datenschutz und Praktikabilität konfrontiert, die etwa seinen Medizinern eine Teilnahme an US-Studien unmöglich macht, da hier private Daten per Patriot Act in fremde Hände gelangen könnten. Schott plädiert deshalb dafür, dass Deutschland schnellstmöglich handlungsfähig wird und die Standards und Regeln setzt, wobei die 100 Prozent Sicherheit nicht zu erreichen seien – da der Mensch immer das schwächste Glied bleiben wird.

Eine Argumentation, der Infineon-Manager Gutau durchaus folgen kann, wobei dies für ihn weniger eine technische Frage ist als eine politische Diskussion verschiedener Interessengruppen. Hierbei lasse sich, so Reinema, eine Tendenz beobachten, nämlich alles totzuregulieren.

Der initiale redaktionelle Round Table zu Cloud Security im Münchner IDG Conference Center, moderiert von Heinrich Vaske (Editorial Director von COMPUTERWOCHE, links im Bild)
Foto: © Armin Weiler

Das Cloud-Security-Studienprojekt

Die Multi-Client-Studien von IDG Research Services, die es nun seit rund zwei Jahren gibt, sind weit mehr als nur einfache, isoliert zu betrachtende Befragungen einer speziellen Berufszielgruppe zu einem speziellen Thema. Es handelt sich vielmehr um ein in sich abgestimmtes nachhaltiges und integrales Studienkonzept. Ist die Idee für ein neues Studienprojekt geboren, steht zu Beginn ein initialer redaktioneller Round Table, zu dem wichtige Player im Markt und potenzielle Studienpartner eingeladen werden. Moderiert wird diese Veranstaltung durch den zuständigen Ressortleiter der COMPUTERWOCHE- oder CIO-Redaktion.

Die beim Round Table diskutierten Themen finden ihren Niederschlag in der Gestaltung des Studien- und Fragebogendesigns. Insbesondere die Studienpartner bekommen Gelegenheit, an der inhaltlichen Ausrichtung des Fragebogens mitzuwirken. Die Ergebnisse unserer Multi-Client-Studien münden immer in einen hochwertigen Survey Report, wie Sie ihn gerade in Händen halten. Wo die Studienergebnisse präsentiert werden, ist themen- und zeitpunktabhängig. Die Ergebnisse der Freiberuflerstudie werden alljährlich im Rahmen einer Podiumsdiskussion auf der CeBIT präsentiert, die Sourcing-Studie beispielsweise wurde in einem Vortrag auf dem Kölner Sourcing-Day dem Fachpublikum vorgestellt.

Die Ergebnisse der nun vorliegenden Cloud-Security-Studie 2016 münden nun in ein weiteres Round-Table-Gespräch mit Vertretern der drei Studienpartner Freudenberg IT, Microsoft und Trend Micro. Auch dieser Round Table ist wieder Gegenstand einer ausführlichen Ergebnisberichterstattung auf COMPUTERWOCHE, CIO, TecChannel und ChannelPartner und – wie in diesem Fall – Teil des Survey Reports.

Teilnehmer am Cloud-Security-Ergebnis-Round-Table:

Freudenberg IT	**Markus Becker**	Senior Management Consultant
Microsoft Deutschland	**Dana Behncke**	Product Marketing Manager EMS
Trend Micro	**Richard Werner**	Business Consultant

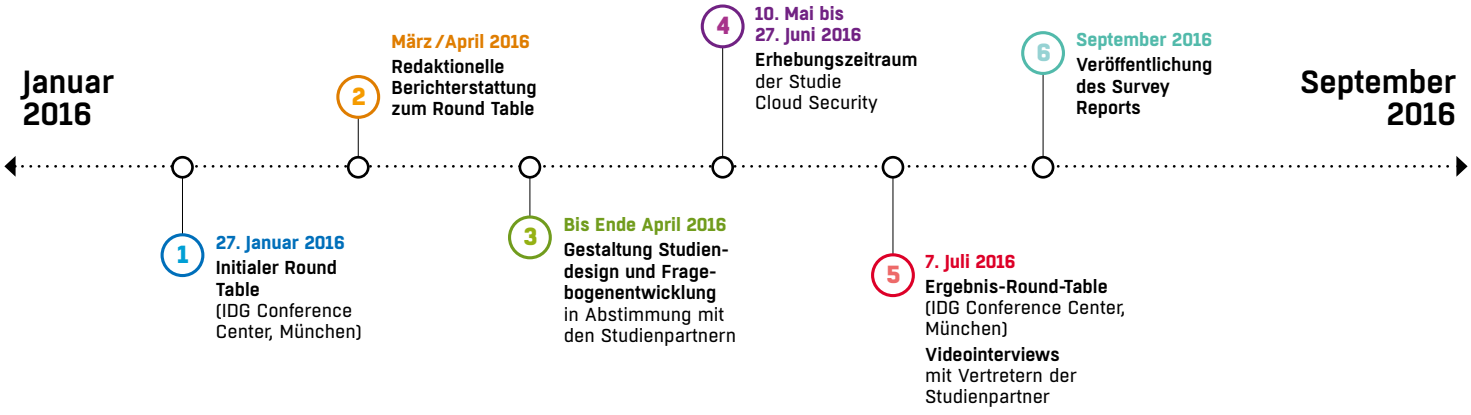


Foto © Patrick Hagn

Dana Behncke (Microsoft Deutschland), Richard Werner (Trend Micro Deutschland), Marcus Becker (Freudenberg IT) und Gastgeber Jürgen Hill (COMPUTERWOCHE) bei der Analyse der Ergebnisse der Cloud-Security-Studie 2016.

Ist die Cloud per se unsicher?

Cloud-Sicherheit und Byod lassen sich kaum voneinander trennen. Zudem kann die Cloud Security nur im Kontext der Gesamt-IT betrachtet werden. Dies wurde in einem Round Table der COMPUTERWOCHE in München zu den Ergebnissen der Cloud-Security-Studie deutlich.

Von Jürgen Hill und Florian Maier

Die Cloud ist in deutschen Unternehmen angekommen. Das ist ein Ergebnis der Cloud-Security-Studie, die die COMPUTERWOCHE gemeinsam mit den Studienpartnern Freudenberg IT, Microsoft sowie Trend Micro durchführte. Teilweise bieten die Ergebnisse reichlich Diskussionsstoff und offenbaren noch offene Baustellen rund um das Thema Cloud. Alarmierend ist beispielsweise, wie zögerlich der deutsche Mittelstand (100 bis 1.000 Beschäftigte) das Thema Cloud angeht. Er läuft Gefahr, hier gegenüber seinen globalen Konkurrenten ins Hintertreffen zu geraten und künftig womöglich in ein Kostenproblem zu laufen. Weiter in Sachen Cloud sind in Deutschland schon die Kleinunternehmen (unter 100 Mitarbeitern) sowie die Enterprise Player (mehr als 1.000 Mitarbeiter).

Eine andere Baustelle in Sachen Security ist die Zuständigkeit in den Unternehmen selbst. Dort ist das Thema Sicherheit häufig Chefsache und nicht

Foto © Patrick Hagn

Dana Behncke (Microsoft Deutschland)

bei der IT angesiedelt, wie man vermuten könnte. Eine Erfahrung, die auch Dana Behncke, Product Marketing Manager EMS bei Microsoft, gemacht hat: „Wir wollten Anfang des Jahres den Security-Ansprechpartner in Firmen finden – doch das ist bunt gemischt. So hatten wir auch gehofft, einen CISO zu finden, aber das ist nicht wirklich gelungen." Richard Werner, Business Consultant bei Trend Micro, kann das nur bestätigen. Er vermutet, dass der C-Level hier federführend ist, weil es eine Business-Entscheidung ist, in die Cloud zu gehen. Zudem würde hier über ganz andere Budget-Ebenen verhandelt. „Die Security-Leute werden dann vor vollendete Tatsachen gestellt", führt Werner weiter aus.

Mit dem Siegeszug der mobilen Devices müssen Unternehmen die Cloud nutzen

Zu den Erkenntnissen der Cloud-Security-Studie zählt auch, dass von den Unternehmen hierzulande das Thema Datenschutz und -sicherheit durchaus ernst genommen wird. Dabei haben die Anwender, wie Behncke erklärt, durchaus das Problem, ihre Daten nicht klassifizieren zu können. Erschwerend komme hinzu, dass die Sicherheitsstandards häufig eine flexible Nutzung mobiler Geräte nicht ermöglichen. Momentan würden viele alles schützen – was aber viel zu viel Aufwand für die IT sei. Letztlich sei zu überlegen, ob Unternehmen nur einen minimalen Teil schützen, der wirklich schützenswert ist. Das könnten etwa personenbezogene Daten oder Finanzdaten sein. Allerdings könnten die Anwender noch etwas „Guidance" brauchen. Werner geht noch einen kleinen Schritt weiter. Er vermutet, dass viele Unternehmen gar keinen Überblick darüber haben, welches die wichtigen Daten sind und wie sie sie differenzieren sollen.

Ein Thema, das noch an Dimension gewinnt, wenn der Aspekt Byod mit einbezogen wird. Fast schon als blauäugig kann man hier die Haltung vieler Unternehmen bezeichnen, wenn sie zu fast 80 Prozent glauben, dass sie das Thema Schatten-IT und eine potenzielle Nutzung von Public-Cloud-Diensten im Griff hätten. Und das, obwohl in vielen Unterneh-

Foto © Patrick Hagn

Marcus Becker (Freudenberg IT)

men die Nutzung privater Endgeräte wie Tablets und Smartphones erlaubt ist. „Das Thema Byod ist aktuell, denn der Arbeitsalltag hat sich stark gewandelt – heutzutage sitzt nicht mehr jeder acht Stunden im Office“, stellt Marcus Becker, Senior Management Consultant bei Freudenberg IT, fest. „Das Arbeiten der Zukunft läuft über mobile Devices wie Smartphones, Notebooks und Tablets ab. Für die nächste Generation, die jetzt in das Arbeitsleben einsteigt, stellt sich die Frage gar nicht mehr, ob Unternehmen die Cloud nutzen wollen oder nicht“, pflichtet ihm Werner bei. Allerdings mit der fatalen Konsequenz, dass die Unternehmen Gefahr laufen die Kontrolle zu verlieren.

IT-Sicherheit ist der Versuch der Unternehmen den User abzusichern

Denn das an sich sehr praxisorientierte Prinzip, das man etwa bei Freudenberg IT praktiziert – dort dürfen Mitarbeiter eigene Endgeräte nutzen, wenn sie per MDM administriert und im Zweifelsfall gelöscht werden dürfen – greift nur bedingt. So wirft etwa TrendMicro Consultant Werner ein: „So eine Einverständniserklärung können Sie jederzeit vor Gericht anfechten. Sie haben die Erlaubnis, auf dem Gerät private Daten zu speichern, und das zählt mehr als der Wunsch der Firma, die Inhalte zu löschen.“

Mit Blick auf die Generation Z meint Werner: „Die Arbeitgeber müssen sich auf eine neue Generation von Arbeitnehmern einstellen. Diese Generation hat mehr Loyalität zur eigenen Turnschuhmarke als zum Arbeitgeber. Es gibt so viele Apple-Jünger da draußen, die für ein Smartphone tagelang Schlange stehen. Wenn diese dann ihr Apple-Gerät nicht in der Firma nutzen dürfen, werden sie zu einer anderen Firma gehen. Für diese Generation ist das Internet eine Selbstverständlichkeit. Deshalb wird sich in Unternehmen, wo es heute heißt: ‚Wir werden niemals in die Cloud gehen‘, das Thema in fünf bis zehn Jahren von allein erledigt haben. Früher hieß IT-Sicherheit, dass das Unternehmen vorgibt, wie der Mitarbeiter zu arbeiten hat. Heute heißt IT-Sicherheit: Der Mitarbeiter sagt, wie er arbeiten will, und das Unternehmen versucht, ihn dabei abzusichern.“

Foto © Patrick Hagn

Richard Werner (Trend Micro Deutschland)

Vor diesem Hintergrund verwundert es, welche optimistische Meinung die Unternehmen von ihren Mitarbeitern in Sachen Cloud-Nutzung haben, wenn sie glauben dass Arbeitsanweisungen genügen. So ist etwa Becker davon überzeugt, dass sich das Ganze nur durch technische Vorkehrungen unterbinden lässt, denn organisatorische würden zu kurz greifen. In das gleiche Horn stößt Werner: „Eine technische Unterbindung ist die einzige Möglichkeit. Beispiel Dropbox und Co.: Hier hilft oft nur eine Steuerung, oder Sie bieten eine vernünftige Alternative, mit der die Mitarbeiter arbeiten können. Geschieht dies nicht, greifen die Mitarbeiter zum USB-Stick und nehmen die Daten mit nach Hause, um dort ihre privaten Dropbox-Accounts zu nutzen."

Neben Zertifikaten und Audits ist die Transparenz der Cloud-Provider wichtig

Die pauschale Aussage der in der Studie befragten Unternehmen, dass die Public Cloud per se unsicher sei, wollten die Diskutanten des Round Tables so nicht stehen lassen. So erinnerte Werner daran, dass jeder Server mit Internetzugang auch unsicher sei und erst durch Sicherheitssoftware, Firewall und Netz-Security-Tools abgesichert werden könne. Letztlich müssten in der Cloud die gleichen Sicherheitsvorkehrungen wie im eigenen Data Center getroffen werden. Dabei stellt sich für Becker die Frage, wie der Cloud-Provider dies nachweist: „Zertifikate und Audits sind hier ein wichtiges Thema." Entsprechendes geben auch die Befragten der Studie zu Protokoll, wobei Werner allerdings bezweifelt, ob kleinere Unternehmen wirklich regelmäßige Audits durchführen, da ihnen hierzu meist die Manpower fehle.

Ein anderer wichtiger Aspekt ist für die Studienteilnehmer die Transparenz der Cloud-Provider, egal ob bezüglich Verträgen, Sicherheitsmaßnahmen oder des Rechenzentrums selbst. Letzteres können Behncke und Becker nur bestätigen. Ihre Unternehmen bieten den Kunden aktiv Führungen durch ihre Rechenzentren an – ein Angebot, das gut angenommen werde.

Unser Platinpartner stellt sich vor

Cloud Security 2016

Freudenberg IT (FIT): IT Solutions. Simplified.

Als weltweit aufgestellter IT-Full-Service-Anbieter deckt das Dienstleistungsspektrum von Freudenberg IT (FIT) sämtliche Facetten moderner SAP-Landschaften ab. Es reicht von verschiedenartigen Outsourcing-Angeboten über Systemoptimierung bis hin zu Betriebsservices und schließt hochkarätige Prozess- sowie SAP-Beratung ein. Als Value Added Reseller von SAP kann FIT Ihren Kunden zudem SAP-Softwarelizenzen und die dazugehörige Softwarepflege anbieten. Ein klares FIT-Alleinstellungsmerkmal ist die jahrelange Manufacturing-Execution-Solution-Erfahrung, die Kunden eine flexible Produktionssteuerung mit direkter SAP-Integration erlaubt. Wie kein zweites IT-Unternehmen kombiniert FIT profundes SAP-Know-how mit tiefem Verständnis für die spezifischen Bedürfnisse der mittelständischen Fertigungsindustrie. Schließlich ist das Unternehmen durch die eigene Herkunft, als ein Teil der familiengeführten Freudenberg-Gruppe, in eben dieser Branche verwurzelt. FIT erwirtschaftet 80 Prozent des eigenen Umsatzes außerhalb der Gruppe und gehört somit zu den erfolgreichsten IT-Ausgründungen in Deutschland. Bis heute wurden weit mehr als 1.000 SAP-Projekte für FIT-Kunden erfolgreich umgesetzt. Dabei stand immer im Vordergrund, effiziente IT-Lösungen anzubieten, die sich intuitiv vom Anwender bedienen lassen.

Ergänzend zur engen Partnerschaft mit SAP wurden in den vergangenen Jahren gezielt weitere Geschäftsfelder erschlossen, um Kunden überall auf der Welt – ganzheitlich und bedürfnisgerecht –

stets die Lösungen zu bieten, die im Rahmen der **Digitalen Transformation** konkret benötigt werden. Basierend auf der ebenfalls sehr intensiven Partnerschaft mit Microsoft bietet FIT heute beispielsweise ein sehr umfangreiches Serviceportfolio an, das Anwender in sämtlichen Digital-Enterprise-Bereichen des Arbeitsalltages praktisch unterstützt.

Auch der hoch entwickelte FIT Application Management Support (AMS) im globalen „Rund um die Uhr"-Betrieb wird branchenübergreifend intensiv genutzt.

FIT ist zudem Wegbereiter von Industrie 4.0 im Mittelstand und in allen wichtigen Innovationsfeldern wie Big Data / SAP HANA, Cloud Computing sowie Enterprise Mobility als Trusted Partner anerkannt.

Zahlreiche Standorte in Europa, Asien sowie in Nordamerika gewährleisten globale Kundennähe. Ein Aspekt, der gerade im Mittelstand sehr geschätzt wird. Als jüngster Standort wurde am 14. Juli 2016 das neue FIT Office im slowakischen Košice eingeweiht.

Lokal und global lautet die konsistente FIT-Mission: Komplexität in Nutzerfreundlichkeit zu wandeln, eben – **IT Solutions. Simplified.**

Hier finden Sie weitere Informationen über das Unternehmen FIT: www.freudenberg-it.com

FIT
IT Solutions.
Simplified.

Freudenberg IT GmbH & Co. KG
Höhnerweg 2 – 4
69469 Weinheim, Germany
Tel.: +49 (0)6201 80 – 8008
Fax: +49 (0)6201 88 – 8000
E-Mail: info-web@freudenberg-it.com
www.freudenberg-it.com

Unsere Autoren

Jürgen Hill begleitet die Entwicklung des deutschen und globalen IT-Markts seit 1992 von journalistischer Seite aus. Bevor er 1992 als Redakteur zur COMPUTERWOCHE kam, studierte er Diplom-Journalistik und Informatik in München. Mit dem Themenschwerpunkt Netzwerke verfolgt er die Liberalisierung des deutschen Telekommunikationsmarktes, schrieb über die ersten zarten Internet-Pflänzchen bis hin zum Siegeszug der IP-Welt. Der Leitende Redakteur hat jetzt seinen Fokus auf disruptiven Technologien wie IoT, Cloud und den neuen Business-Paradigmen Digitalisierung und Industrie 4.0.

Florian Maier arbeitet seit 2015 bei IDG. Er beschäftigt sich in erster Linie mit dem Themenbereich IT-Security. Daneben schreibt er auch über reichweitenstarke und populäre IT-Themen an der Schnittstelle zu B2C und ist für den Facebook-Auftritt der COMPUTERWOCHE zuständig. Er schreibt hauptsächlich für die Portale COMPUTERWOCHE und CIO.

Unsere Studienreihe

Erhältlich in unserem Studien-Shop auf ***www.computerwoche.de/studien***

Vorschau Studienreihe

Oktober 2016:
ANALYTICS READINESS

November 2016:
Internet of Things

Februar 2017:
Digitalisierung

März 2017:
IT-Freiberufler

April 2017:
Real Analytics

Juni 2017:
Sourcing 2017

Juli 2017:
Industrie 4.0

September 2017:
Workplace Security

Sales-Team

Franziska Kaufmann
Account Manager Research
IDG Research Services
Telefon: 089 36086 – 882
fkaufmann@idgbusiness.de

Carolin Beck
Marketing & Research Specialist
IDG Research Services
Telefon: 089 36086 – 122
cbeck@idgbusiness.de

Herausgeber:

IDG Business Media GmbH

Anschrift
Lyonel-Feininger-Str. 26
80807 München
Telefon (089) 360 86 – 0
Fax (089) 360 86 – 118
E-Mail info@idgbusiness.de

Vertretungsberechtigter
York von Heimburg
Geschäftsführer

Registergericht
Amtsgericht München
HRB 99187

Umsatzsteueridentifikations-nummer
DE 811 257 800

Weitere Informationen unter:
www.idgbusinessmedia.de

Partner:

Freudenberg IT GmbH & Co. KG
Höhnerweg 2 – 4
69469 Weinheim
Telefon: (06201) 80 8008
E-Mail:
info-web@freudenberg-it.com
Web: www.freudenberg-it.com

Microsoft Deutschland GmbH
Konrad-Zuse-Straße 1
85716 Unterschleißheim
Telefon: (01806) 67 22 55
E-Mail: kunden@microsoft.com
Web: www.microsoft.com/germany

Trend Micro Deutschland GmbH
Zeppelinstraße 1
85399 Hallbergmoos
Telefon: (0811) 88990 – 70
E-Mail: sales_info@trendmicro.de
Web: www.trendmicro.de/

Studienkonzept / Endredaktion / CvD-Survey Report:
Matthias Teichmann
IDG Research Services

Analysen / Kommentierungen:
Jürgen Hill (Team-Leiter Technologie und Leitender Redakteur COMPUTERWOCHE)

Umfrageprogrammierung:
Thamar Thomas-Ißbrücker
IDG Research Services
auf EFS Survey Spring 2016

Grafik:
Daniela Petrini, München

Umschlagkonzept:
Sandra Schmitt
IDG Research Services
(unter Verwendung eines Farbfotos für Vorder- und Rückseite von © shutterstock.com / prince_apple)

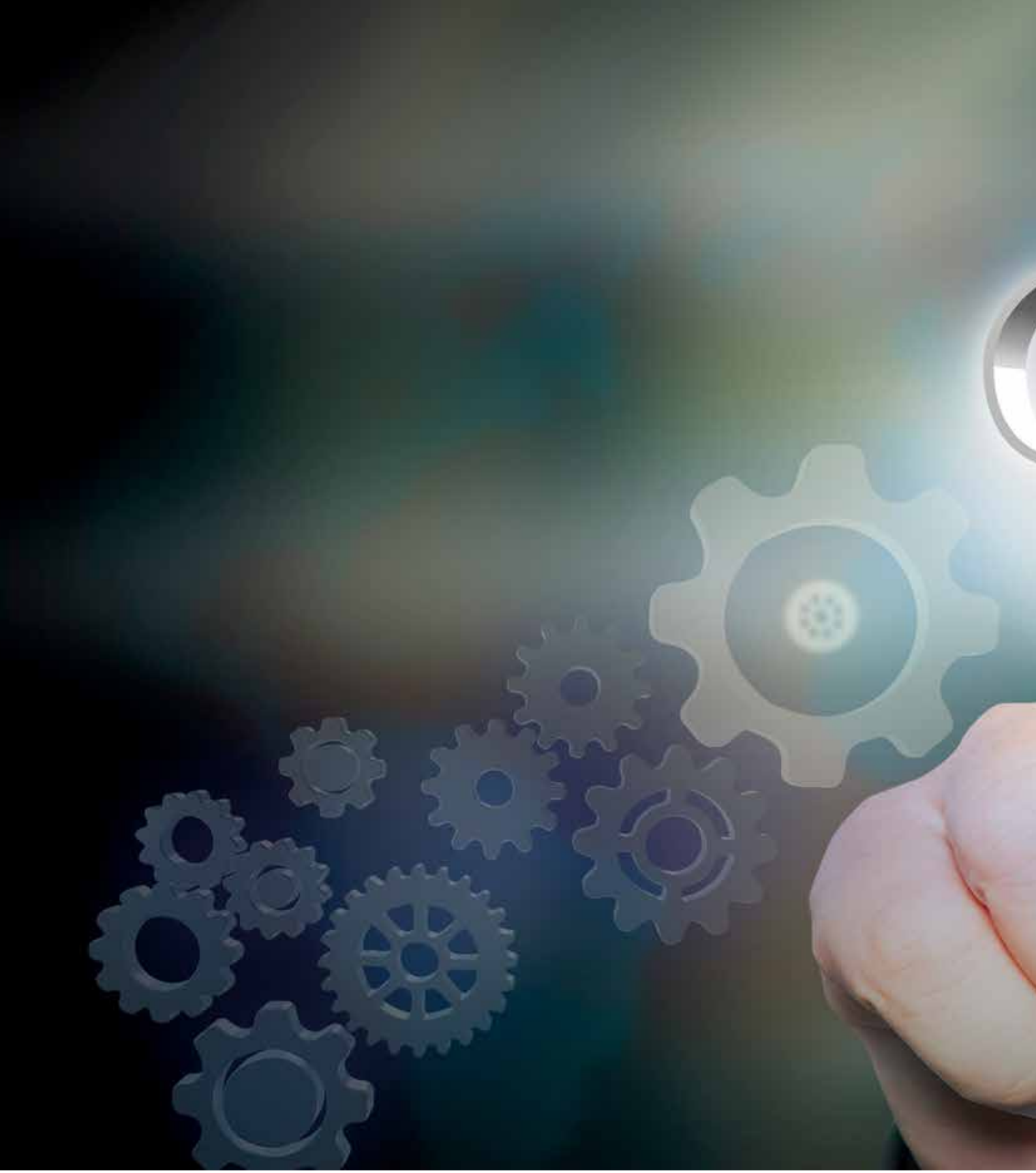
Lektorat:
Dr. Renate Oettinger, München

Druck:
Peradruck GmbH
Hofmannstr. 7 b
81379 München

Ansprechpartner:

Matthias Teichmann
Projektleitung und Leiter Marktforschung IDG Research Services
Telefon: 089 36086 – 131
mteichmann@idgbusiness.de

Carolin Beck
Marketing und Research Specialist
IDG Research Services
Telefon: 089 36086 – 122
cbeck@idgbusiness.de



PLATINPARTNER

FIT
IT Solutions.
Simplified.

GOLDPARTNER

Microsoft

TREND MICRO™
Securing Your Journey
to the Cloud