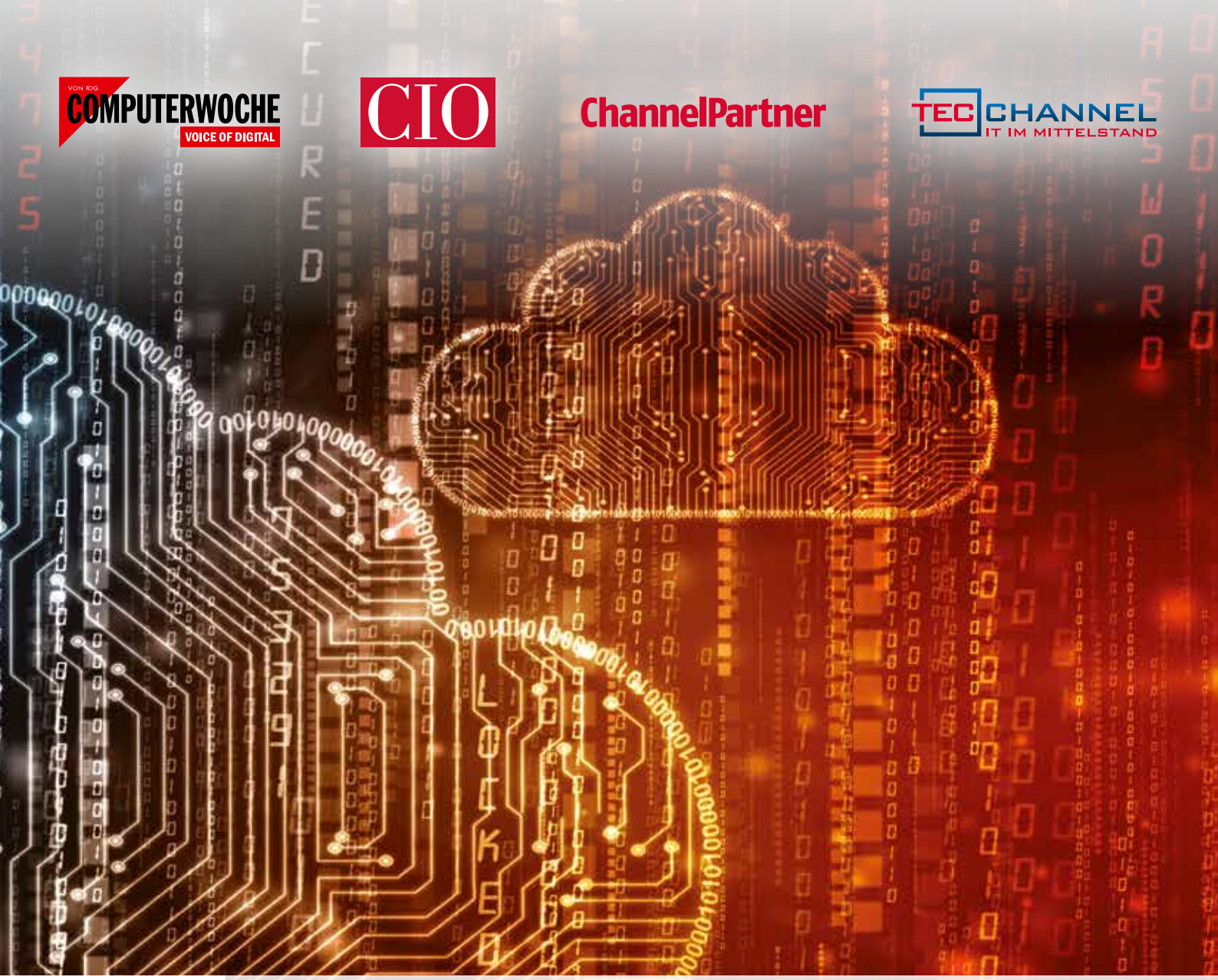


COMPUTERWOCHE VOICE OF DIGITAL

CIO

ChannelPartner

TECCHANNEL IT IM MITTELSTAND

IDG RESEARCH SERVICES

STUDIE CLOUD SECURITY 2019

PLATIN-PARTNER

cisco

GOLD-PARTNER

Akamai Experience the Edge

MICRO FOCUS

plusserver

SILBER-PARTNER

NTT Security

BRONZE-PARTNER

genua Ein Unternehmen der Bundesdruckerei

SecurEnvoy A Shearwater Group plc Company

Denn sie wissen, was sie wollen

Wenn das kein eindeutiges Ergebnis ist: Fast 92 Prozent der deutschen Unternehmen nutzen bereits Cloud-Services, planen die Nutzung binnen Jahresfrist oder prüfen zumindest konkret einen Einsatz. Wichtig ist einem großen Teil von ihnen, dass die Cloud-Services sicher sind und den Anbietern vertraut werden kann. Auch die Einhaltung moderner Datenschutzstandards spielt eine übergeordnete Rolle – kein Wunder, im Fahrtwind der EU-DSGVO steht dieses Thema nach wie vor ganz oben auf der Agenda vieler.

Heißt: Die Cloud drängt nach jahrelanger, meist durch Sicherheitsbedenken verursachter Zurückhaltung nun mit aller Macht in die Unternehmen – und sie scheint sicherer als je zuvor. Das ist mehr als ein Gefühl – die Cloud-Anbieter haben viel dafür getan, dass längst nicht mehr nur der Kostendruck, sondern auch die Sicherheit ihrer Dienste die Unternehmen zu einer Nutzung veranlassen.

Bei aller Cloud-Euphorie dürfen wir natürlich nicht vergessen, dass es heute mehr Sicherheitsvorfälle mit Cloud-Diensten gibt als je zuvor. Das ist aber nur logisch: Je mehr Cloud-Nutzer es gibt, desto mehr Incidents. Ein Grund, die Cloud als Unsicherheitsfaktor pauschal abzulehnen, ist diese Entwicklung schon lange nicht mehr.

Die vorliegende Studie zeigt vor allem eins: Die von uns befragten deutschen Unternehmen wissen vor dem Hintergrund von Klassikern wie Datenschutz- und Compliance-Vorgaben, Policies, Audits und Zertifikaten schon lange, was sie wollen. Mit Sicht auf eine sinnvolle und entlastende Nutzung von Cloud-Diensten wissen sie seit geraumer Zeit auch, was sie brauchen. Neu scheint, dass sie mittlerweile auch verstanden haben, wie sie es bekommen.

Simon Hülsbömer, Senior Project Manager Research

Was die Anbieter angeht, dürfen diese sich auf ihren derzeitigen Erfolgen nicht ausruhen. Sie sollten auch künftig den steigenden Kundenerwartungen nachkommen, um ihre Produkte dauerhaft vermarkten zu können. Obacht ist durchaus geboten, wie bereits Fußball-Trainerlegende Otto Rehhagel wusste: „Im Erfolg macht man die größten Fehler."

Ich wünsche Ihnen eine spannende und erkenntnisreiche Lektüre!

Inhalt

Weitere Studienergebnisse

20

Unsere Studienpartner stellen sich vor

41

Blick in die Zukunft

Die Cloud Security braucht und bekommt ein neues Verständnis

35

Kontakt/ Impressum

55

Cloud-Dienste sind von DDoS-Attacken betroffen

47 Prozent der Unternehmen berichten von Cyber-Angriffen auf ihre Cloud-Services; mehr als die Hälfte der Angriffe sind DDoS-Attacken.

DSGVO hat hohen Einfluss auf Umgang mit Cloud-Daten

Acht von zehn Unternehmen berichten von einer eher starken bis sehr starken Auswirkung der Datenschutz-Grundverordnung (DSGVO), wenn es um die Verarbeitung von Daten in der Cloud geht.

DSGVO beeinflusst Wahl des Cloud-Providers

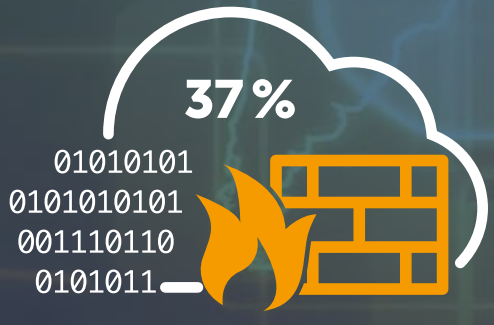
Jedes dritte Unternehmen sagt, dass die Datenschutz-Grundverordnung einen Einfluss auf die Auswahl des Cloud-Anbieters und des Speicherortes für die Cloud-Daten hat. Auch die Cloud-Zertifizierung bekommt einen neuen Stellenwert.

Sicherer Datenzugriff ist wichtiger als Open Source

Sicherheitskriterien liegen klar vor Usability, Preis und Open Source, wenn es um die Auswahl eines Cloud-Dienstes geht. Dabei spielen auch weiche Kriterien wie Vertrauen in den Anbieter eine große Rolle.

Cloud-Zertifikate für die organisatorische Sicherheit

Ein Drittel der Unternehmen achtet auf Cloud-Zertifikate. Fehlen diese Zertifikate, werden Datenschutz-Audits bei dem Provider verlangt. Intern regeln Policies die Nutzung von Clouds und Zugangsgeräten.



Verschlüsselung und Firewall als Cloud-Schutz

37 Prozent der Unternehmen setzen auf klassische Sicherheitsmaßnahmen wie Datenverschlüsselung und VPN. Neue Schutzlösungen wie CASB (Cloud Access Security Broker) gibt es erst bei 18 Prozent.

Die Key Findings im Einzelnen

1. Cyber-Attacken belasten Cloud-Services der Unternehmen

Fast die Hälfte (47 Prozent) der Unternehmen hat bereits Cyber-Angriffe auf ihre Cloud-Services festgestellt, zwölf Prozent wissen nicht, ob bereits eine Online-Attacke auf ihre Cloud-Dienste erfolgt ist. Unter den beobachteten Cyber-Angriffen dominieren die DDoS-Attacken, mit denen Cloud-Dienste überlastet werden sollen.

42 Prozent der befragten Unternehmen sagen, dass die von ihnen genutzten Cloud-Dienste noch von keinem Cyber-Angriff getroffen wurden. Die Mehrheit der Unternehmen berichtet von einer solchen Attacke oder ist sich nicht sicher, ob ein entsprechender Angriff erfolgt ist.

Besonders häufig erfolgen DDoS-Attacken (Distributed Denial of Service Attacken). Diese Angriffe haben das Ziel, einen Ausfall des Cloud-Services zu verursachen.

Besonders betroffen von DDoS-Attacken sind die Unternehmen, die mehr als 100 Millionen Euro pro Jahr in Cloud-Dienste investieren. Hier klagen 55 Prozent der Unternehmen über DDoS-Angriffe. Bei den Unternehmen mit einer Investition von weniger als einer Million Euro jährlich in Cloud-Dienste berichten dagegen nur neun Prozent von DDoS-Attacken.

Interessant ist auch, dass Fachbereiche wie der Vertrieb wenig von den DDoS-Angriffen auf die Cloud-Dienste wissen: Nur sechs Prozent nennen diese Attacken, unter den CIOs sind es 43 Prozent, bei den Geschäftsführern 36 Prozent und bei den IT-Leitern immer noch 16 Prozent.

Ebenso fällt auf, dass das generelle Wissen um Attacken auf die Cloud-Dienste je nach Funktion im Unternehmen unterschiedlich ausgeprägt ist. Nur jeweils sieben Prozent der Geschäftsführer und CIOs sagten, sie wissen nicht, ob es Angriffe auf die Cloud-Services gab, in der IT-Leitung neun Prozent, in den Fachbereichen aber 22 Prozent. Dort besteht offensichtlich ein höherer Informationsbedarf.

Waren die Cloud-Services Ihres Unternehmens schon einmal Ziel eines Cyber-Angriffs?

Angaben in Prozent. Filter: Nur Unternehmen, die Cloud-Services bereits eingeführt haben oder es konkret planen. Basis: n = 322

	Gesamt	Ergebnis-Split nach Funktion im Unternehmen			
		Geschäftsführung/ COO/CFO/ sonst. Vorstand	CIO/IT-Vorstand/ CDO/CTO/ Technikvorstand	IT-Leiter	Fachbereiche (Vertrieb, Marketing, Produktion, Einkauf, anderer FB)
Ja, DDoS-Attacke	24,8	36,2	43,0	15,8	5,7
Ja, anderer Angriff	21,7	17,4	22,1	21,1	25,0
Nein	41,9	39,1	27,9	53,9	47,7
Weiß nicht / keine Angabe	11,5	7,2	7,0	9,2	21,6

Weitere Studienergebnisse

1. Private Clouds und Software as a Service (SaaS) sind führend

65 Prozent der Unternehmen nutzen bereits Cloud-Services. Dabei dominiert die Private Cloud als Bezugsmodell mit 61 Prozent. 57 Prozent der Unternehmen haben eine SaaS-Lösung im Einsatz. Häufig diskutierte Cloud-Modelle wie Hybrid Clouds und Multi-Clouds sind noch weniger stark verbreitet, als oftmals vermutet wird.

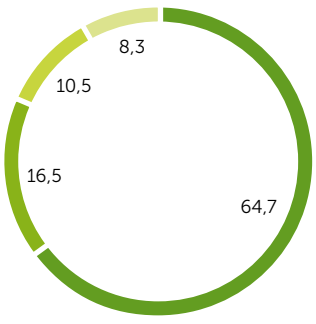
Cloud-Services sind in den Unternehmen in Deutschland angekommen und kaum noch wegzudenken. Nur für acht Prozent der Unternehmen kommen Cloud-Services nicht infrage. 92 Prozent der Unternehmen nutzen bereits Cloud-Dienste, sie planen es in den nächsten zwölf Monaten (17 Prozent) oder prüfen es intern (elf Prozent).

Als Bezugsmodell für Cloud-Dienste liegt die Private Cloud mit 61 Prozent der Antworten vorne, Virtual Private Clouds werden von 24 Prozent der Unternehmen genutzt. Public Clouds nutzen 45 Prozent der befragten Unternehmen. Hybrid Clouds sind bei 32 Prozent im Einsatz, Community Clouds und Multi-Clouds bei 20 Prozent.

Bei den genutzten Cloud-Services handelt es sich bei 57 Prozent der Unternehmen um SaaS-Dienste, bei 43 Prozent sind es PaaS-Lösungen, und bei 38 Prozent geht es um IaaS. Für Security-Services nutzen 23 Prozent der Unternehmen die Cloud, im Fall von IAMaaS sind es 20 Prozent.

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

Angaben in Prozent. Basis: n = 351



- Unser Unternehmen nutzt bereits Cloud-Services.
- Unser Unternehmen plant konkret die Nutzung von Cloud-Services in den nächsten zwölf Monaten.
- Die Nutzung von Cloud-Services wird in unserem Unternehmen geprüft.
- Die Nutzung von Cloud-Services kommt für unser Unternehmen generell nicht infrage.

Welches Cloud-Bezugsmodell nutzt Ihr Unternehmen bereits?

Angaben in Prozent. Filter: Nur Unternehmen, die Cloud-Services bereits eingeführt haben oder es konkret planen. Basis: n = 322

Gesamt

Private Cloud	60,9
Public Cloud	44,5
Hybrid Cloud	31,5
Virtual Private Cloud	24,2
Community Cloud	20,1
Multi-Cloud	19,9

Welche der folgenden Arten von Cloud-Services nutzt Ihr Unternehmen bereits?

Angaben in Prozent. Filter: Nur Unternehmen, die Cloud-Services bereits eingeführt haben oder es konkret planen. Basis: n = 320

Gesamt

Software as a Service (SaaS)	56,8
Platform as a Service (PaaS)	42,5
Infrastructure as a Service (IaaS)	38,1
Communication as a Service (CaaS)	24,8
Security as a Service (SecaaS)	22,9
Identity and Access Management as a Service (IAMaaS)	19,9

Blick in die Zukunft

Cloud Security 2019

Die Cloud Security braucht und bekommt ein neues Verständnis

Den Unternehmen in Deutschland ist Cloud-Sicherheit sehr wichtig. Die Datenschutz-Grundverordnung (DSGVO) hat dies noch verstärkt. Das Bild der sicheren Cloud ist in vielen Unternehmen aber noch unscharf. Das wird sich in Zukunft ändern. Dank der Zertifizierung von Cloud und Datenschutz erfahren die Unternehmen, was die Cloud Security umfasst.

Von Oliver Schonschek

Rund zwei Drittel der Unternehmen in Deutschland verwenden bereits Cloud-Dienste. Auch wenn Hybrid Cloud und Multi-Clouds in aller Munde sind, das vorherrschende Bezugsmodell ist weiterhin die Private Cloud. Wenn sich ein Unternehmen gegen Cloud-Services entscheidet, spielt die Sicherheit die entscheidende Rolle, genauer gesagt, das Bild von der Cloud-Sicherheit, das der jeweilige Entscheider hat.

Wie diese Studie zeigt, sind es in der Regel nicht die Sicherheitsexperten in den Unternehmen, die für die Cloud Security verantwortlich zeichnen. Welche Sicherheitsmaßnahmen für die genutzten Cloud-Dienste eingesetzt oder vom Anbieter eingefordert werden, hängt von der Risikowahrnehmung der Cloud-Entscheider ab, oftmals geprägt von aktuellen Medienberichten.

Cloud-Sicherheit wird oft noch missverstanden

Die Unklarheiten im Bereich Cloud-Sicherheit werden beispielhaft sichtbar, wenn man Performance gegen Sicherheit abwägen soll. Tatsächlich ist die Cloud-Sicherheit eine entscheidende Grundlage der Cloud-Performance, was jedoch noch in vielen Unternehmen nicht klar genug ist.

Dabei erleiden die befragten Unternehmen bereits DDoS-Angriffe auf ihre Cloud-Dienste. Unter den genannten Cloud-Risiken tauchen die DDoS-Attacken aber weit hinten auf. Bei Datendiebstahl denken die Unternehmen eher an Hacker als an mögliche Innentäter, die vertrauliche Daten über Cloud-Schnittstellen aus dem Unternehmen schleusen.

Die DSGVO sorgt für ein neues Bild

Die Zeichen stehen aber auf Veränderung. Die Datenschutz-Grundverordnung (DSGVO) beeinflusst deutlich die Entscheidungen bei der Auswahl von Cloud-Anbietern. Sowohl beim Cloud-Dienst als auch beim Cloud-Provider erwarten die befragten Unternehmen einen hohen Sicherheits- und Datenschutzstandard.

Cloud-Zertifikate und Datenschutzzertifizierungen gehören zu den wesentlichen Auswahlkriterien. Fehlt das Zertifikat, wünschen sich die Unternehmen eine Auditierung des Datenschutzes beim Provider. Zertifizierung und Auditierung helfen aber nicht nur im Auswahlprozess, sie schärfen auch den Blick für die Sicherheit der Cloud-Dienste.