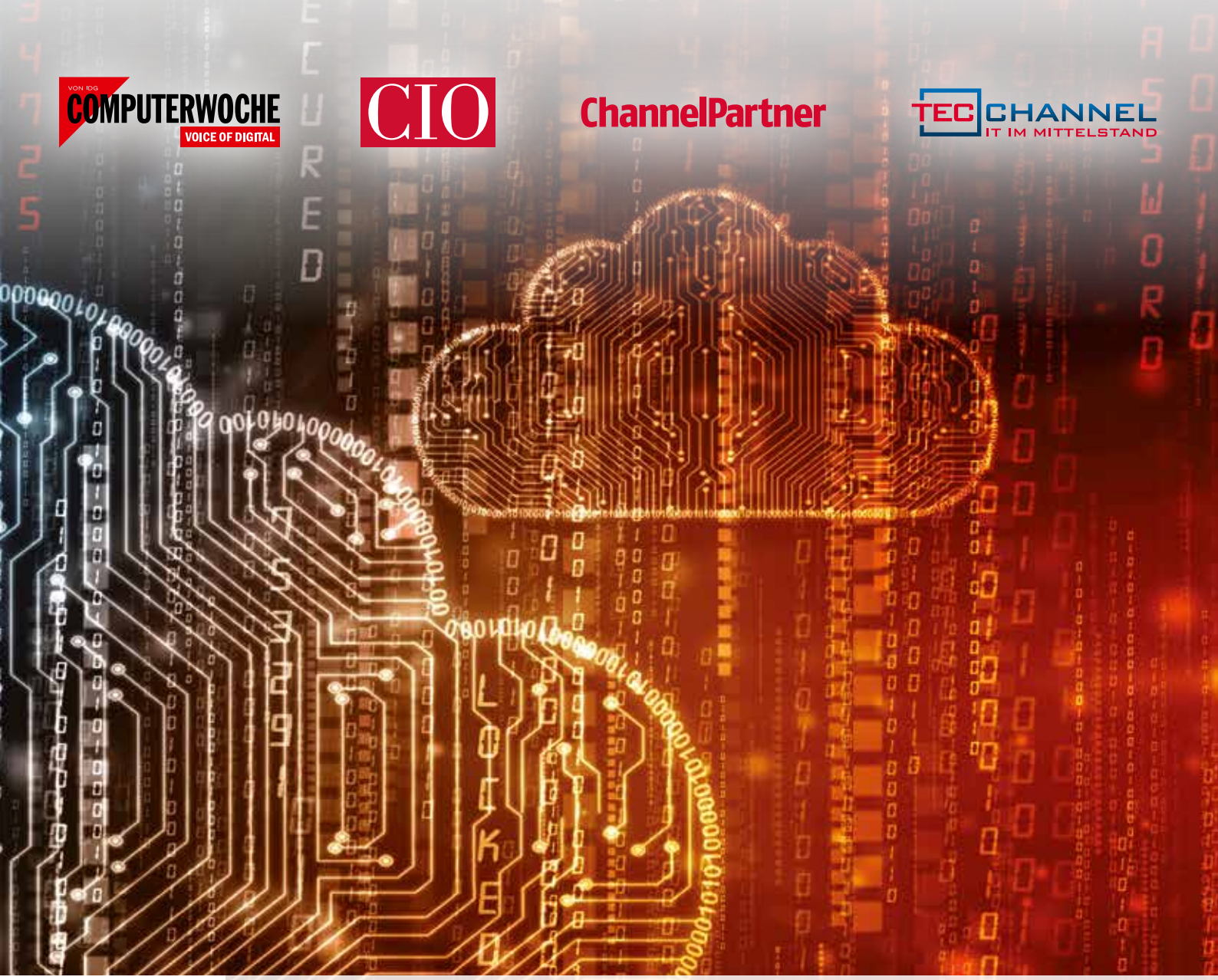


COMPUTERWOCHE VOICE OF DIGITAL

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

Ein aktuelles Studienprojekt von

IDG
RESEARCH SERVICES

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

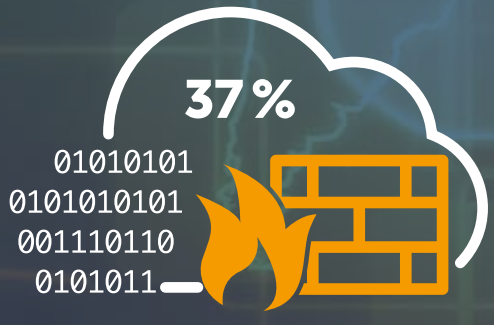
Jedes dritte Unternehmen sagt, dass die Datenschutz-Grundverordnung einen Einfluss auf die Auswahl des Cloud-Anbieters und des Speicherortes für die Cloud-Daten hat. Auch die Cloud-Zertifizierung bekommt einen neuen Stellenwert.

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.

EU-Datenschutz ist ein Vorteil, US-Vertrag eher nicht

Die Einhaltung der Datenschutz-Grundverordnung (DSGVO) durch den Anbieter ist den Unternehmen wichtiger als ein Standort oder eine Niederlassung in Deutschland. US-Verträge sind weniger auf der Wunschliste bei der Anbietersuche.

Provider sollen für Backup und Zugangsschutz sorgen

Weniger die Herkunft der Servertechnik ist den Cloud-Nutzern wichtig, sondern zentrale Schutzmaßnahmen wie Backup und Zugangskontrolle durch den Cloud-Anbieter. Dabei spielt Single-Sign-On (SSO) eine geringere Rolle.

Management Summary

Die Key Findings im Überblick

Unternehmen fürchten Hacker und Datendiebe

DDoS-Attacken werden kaum als Sicherheitsrisiko für Cloud-Services gesehen, obwohl viele Unternehmen solche Angriffe bereits erlebt haben. Auch Innentäter werden kaum als Cloud-Risiko eingestuft.

On-Premises mit weniger Datenschutz und Verfügbarkeit

Intern betriebene IT-Services bieten weniger Schutz für die Daten als Cloud-Services, meinen 18 Prozent der Unternehmen. Die Rechenzentren der Provider sind sicherer als interne, sagen zwölf 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

2. Die DSGVO beeinflusst stark den Umgang mit den Daten in der Cloud

Für fast 60 Prozent der Unternehmen hat die Datenschutz-Grundverordnung (DSGVO) einen starken oder sehr starken Einfluss darauf, wie sie mit Daten umgehen, die in einer Cloud verarbeitet werden. Keine Auswirkung der DSGVO sehen gerade einmal zwei Prozent der befragten Unternehmen.

Während 16 Prozent der befragten Unternehmen meinen, die DSGVO hat nur einen sehr schwachen bis eher schwachen Einfluss auf ihren Umgang mit Daten in der Cloud, berichten 82 Prozent von einer eher starken bis sehr starken Wirkung des neuen EU-Datenschutzrechts.

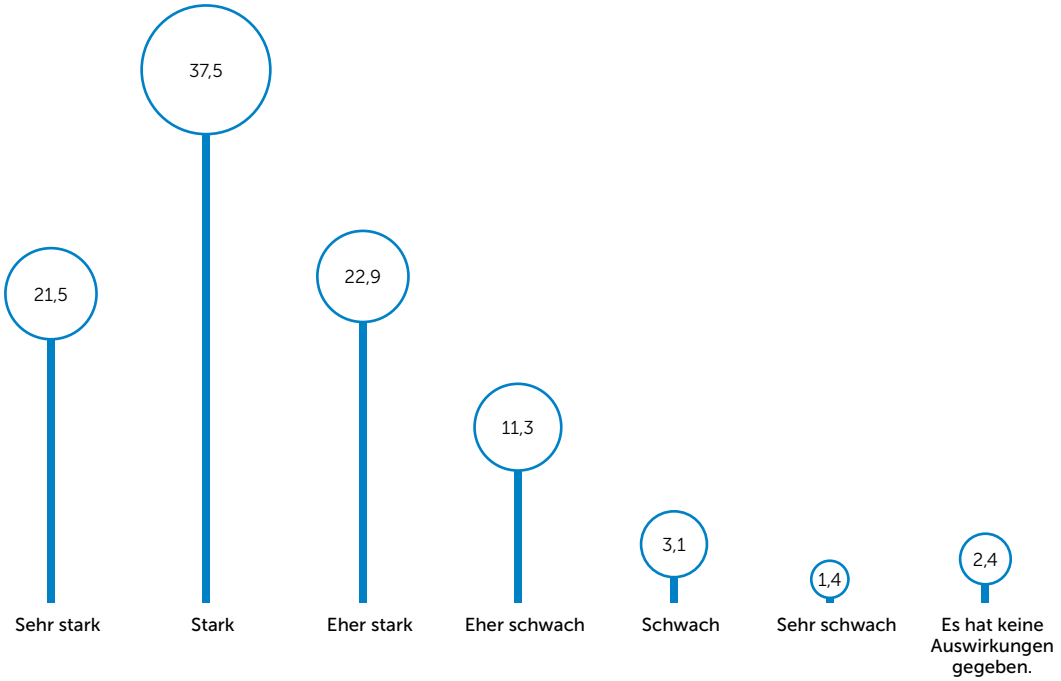
Ob der Einfluss der DSGVO als sehr stark angesehen wird, hängt weniger von der Mitarbeiterzahl der Unternehmen in Deutschland ab als vielmehr von der Höhe der jährlichen Investitionen in Cloud-Services.

Betragen die Aufwendungen für Cloud-Dienste weniger als eine Million Euro pro Jahr, sind es nur 15 Prozent der Unternehmen, die einen sehr starken Einfluss der DSGVO sehen, bei einer bis 100 Millionen Euro pro Jahr 21 Prozent, bei mehr als 100 Millionen Euro jährlicher Aufwendungen für Cloud-Services sogar 36 Prozent.

Den sehr starken Einfluss der DSGVO sehen dabei insbesondere die Geschäftsführer mit 34 Prozent Zustimmung; bei der IT-Leitung sind es noch 22 Prozent, in den Fachbereichen 19 Prozent und beim CIO sogar nur 13 Prozent.

Wie stark sind die Auswirkungen der EU-DSGVO (EU-Datenschutz-Grundverordnung) bezogen auf den Umgang Ihres Unternehmens mit Daten in der Cloud?

Angaben in Prozent. Filter: Nur Unternehmen, die Cloud-Services bereits eingeführt haben oder es konkret planen. Basis: n = 300



3. Der Datenschutz verändert die Auswahl von Cloud-Services

Ob Speicherort, Zertifizierung oder Verschlüsselung der Cloud-Daten: Kaum ein Kriterium bei der Auswahl eines Cloud-Services ist nicht betroffen von der erhöhten Aufmerksamkeit für den Datenschutz, die seit der Anwendung der Datenschutz-Grundverordnung (DSGVO) zu spüren ist.

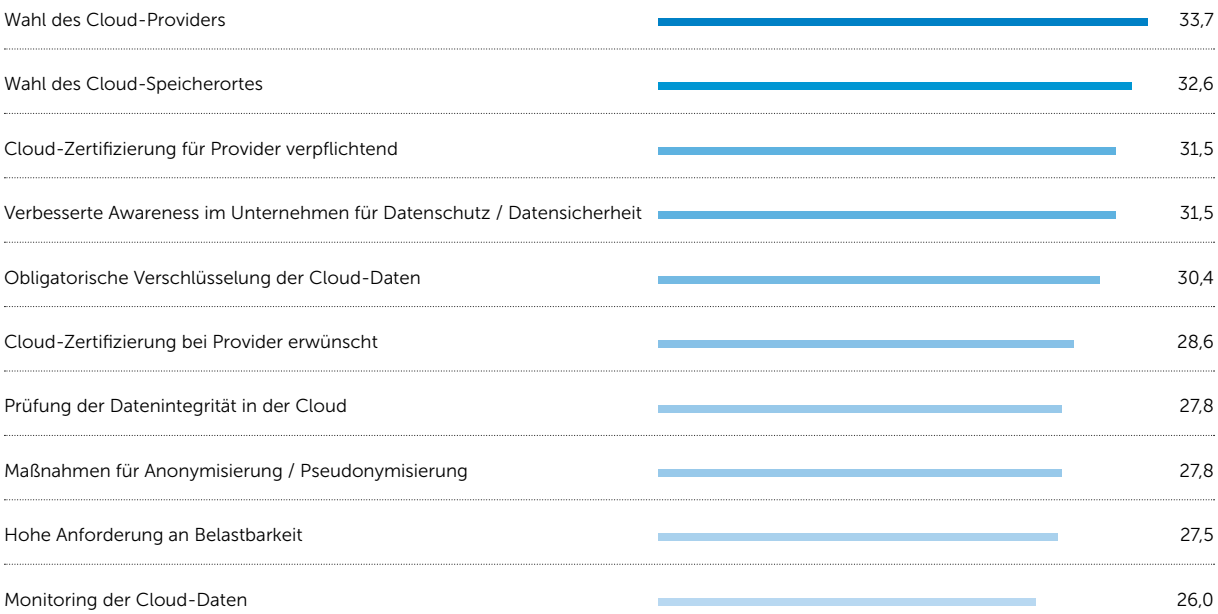
Die DSGVO hat besonderen Einfluss auf die Wahl des Cloud-Providers und den Speicherort für die Cloud-Daten. Als weitere Folgen nennen Unternehmen, dass sie eine Cloud-Zertifizierung nun als verpflichtend ansehen und die Verschlüsselung der Cloud-Daten vom Provider fordern. Die Unternehmen berichten von einer gesteigerten Sensibilisierung für Datenschutz und Datensicherheit im eigenen Betrieb.

Dies wird dadurch bestätigt, dass die Unternehmen viele weitere Faktoren für die Anbietersuche nennen, die durch die DSGVO an Gewicht gewonnen haben, darunter die Prüfung der Datenintegrität in der Cloud, Maßnahmen für Anonymisierung und Pseudonymisierung, hohe Anforderungen an die Belastbarkeit der Cloud-Services und das Monitoring der Cloud-Daten.

Bezeichnend ist dabei, dass die Zustimmung zu den wichtigsten Auswirkungen der DSGVO relativ einheitlich ist; sie variiert zwischen 34 Prozent und 26 Prozent. Die meisten der Kriterien werden als nahezu gleich wichtig gesehen, was für ein breites und hohes Anforderungsspektrum bei der Suche nach Cloud-Services spricht.

Welche Auswirkungen hat die EU-DSGVO (EU-Datenschutz-Grundverordnung) bezogen auf den Umgang Ihres Unternehmens mit Daten in der Cloud?

Angaben in Prozent. Auflistung der Top 10. Mehrfachnennungen möglich. Filter: Es gab Auswirkungen durch EU-DSGVO. Basis: n=273.



4. Sicherheit und Vertrauen sind die wichtigsten Auswahlkriterien bei Cloud-Diensten

Weder der Preis noch Open Source schaffen es in die Liste der zehn wichtigsten Kriterien bei der Auswahl von Cloud-Diensten. Ganz oben steht die Sicherheit des Datenzugriffs, die gute Usability bringt es nur auf den sechsten Platz der führenden Auswahlkriterien.

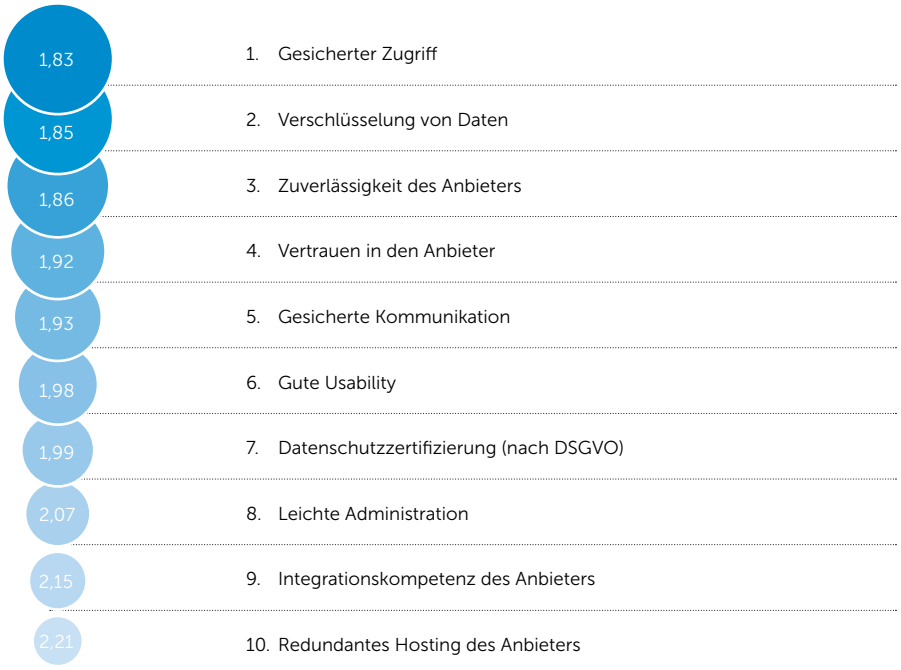
Wenn Unternehmen nach einem geeigneten Cloud-Dienst Ausschau halten, spielen viele Faktoren eine Rolle.

Die befragten Unternehmen wünschen sich einen gesicherten Zugriff auf ihre Daten, eine Verschlüsselung der Daten und einen zuverlässigen, vertrauenswürdigen Anbieter. Da die zuletzt genannten Kriterien Vertrauen und Zuverlässigkeit nicht so einfach greifbar sind, ist es nicht überraschend, dass sich die Unternehmen neben der Kommunikationssicherheit und der guten Bedienbarkeit eine Datenschutzzertifizierung nach der Datenschutz-Grundverordnung (DSGVO) vom Cloud-Dienst der Wahl wünschen, als Nachweis der Vertrauenswürdigkeit. Es folgen die leichte Administration des Cloud-Services, die Integrationskompetenz des Anbieters und ein redundantes Hosting durch den Anbieter.

Nicht in die Top 10 der Auswahlkriterien geschafft haben es Flexibilität im Deployment, Cloud-Zertifizierung (wie C5-Testat), Preis, Transparenzberichte (über mögliche Zugriffe staatlicher Stellen), ein bevorzugter Cloud-Standort in der EU oder in Deutschland oder der Einsatz von Open-Source-Techniken.

Wie wichtig sind Ihnen die folgenden Kriterien in Bezug auf Cloud-Services?

Top 10 aus arithmetischen Mittelwerten auf einer Schulnotenskala von 1 „Sehr wichtig" bis 6 „Gar nicht wichtig". Basis: n = 351



5. Zertifikate, Audits und Policies sind die Basis der Sicherheitsorganisation

Die organisatorische Sicherheit bei Nutzung von Cloud-Services ist breit aufgestellt, darunter befinden sich auch personelle Maßnahmen. 30 Prozent der Unternehmen haben einen Verantwortlichen zur Steuerung der Cloud-Provider bestimmt. 27 Prozent haben zusätzliche Security-Stellen geschaffen.

Datenschutz wird nicht nur als Kriterium bei der Auswahl von Cloud-Providern genannt, sondern findet konkreten Niederschlag in den organisatorischen Maßnahmen für die Cloud-Sicherheit. 34 Prozent der befragten Unternehmen prüfen die Cloud-Zertifikate der Anbieter. Fehlen die Zertifikate, achten sie auf Datenschutzaudits bei den Providern.

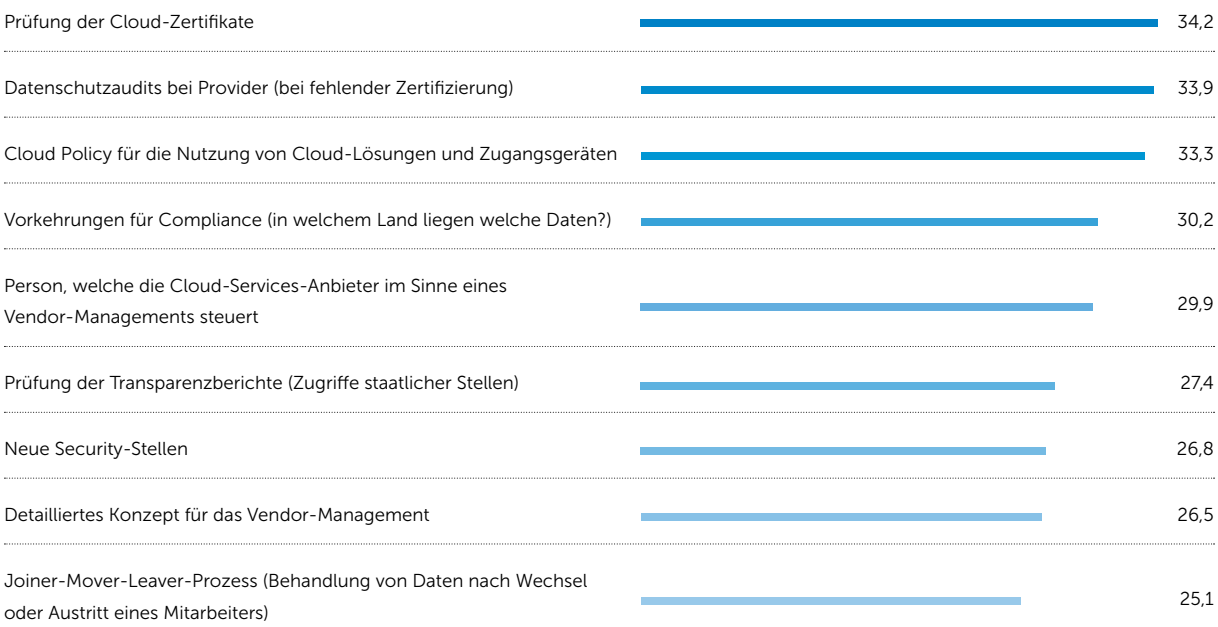
Intern werden bei jedem dritten Unternehmen Richtlinien für die Nutzung von Cloud-Diensten und Zugangsgeräten erlassen. 30 Prozent treffen Vorkehrungen, um feststellen zu können, in welchem Land die Cloud-Daten gespeichert werden. Bei 27 Prozent spielen auch die Transparenzberichte eine Rolle, die Auskunft über mögliche staatliche Zugriffe auf Cloud-Daten geben.

Weitere Maßnahmen sind Konzepte für das Vendor-Management (27 Prozent) und für Prozesse, wie mit den Daten ausscheidender Mitarbeiter umzugehen ist (25 Prozent).

Die Prüfung der Cloud-Zertifikate spielt bei Unternehmen mit weniger als 1.000 Mitarbeitern in Deutschland eine größere Rolle: Hier nennen 40 Prozent diese Maßnahme im Vergleich zu 29 Prozent bei den Firmen, die mehr als 1.000 Mitarbeiter in Deutschland haben.

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

Angaben in Prozent. Mehrfachnennungen möglich. Basis: n = 351



6. Neue Security-Ansätze kommen eher bei hohen Cloud-Investitionen zum Einsatz

Wenn es um die technische Cloud-Sicherheit geht, setzen viele Unternehmen auf vertraute Security-Konzepte wie Verschlüsselung, Firewall und lokale Backups. Trotz der zahlreichen DDoS-Attacken landet der DDoS-Schutz nur auf Platz vier der Security-Maßnahmen.

Gute Endpoint-Kontrolle, verbesserte Zugangs- und Rechtekontrolle (IAM) und ein verbessertes Passwortmanagement gehören bei 31 Prozent der Unternehmen zum technischen Schutz ihrer Cloud-Nutzung. Für 29 Prozent gehört auch die Integritätskontrolle bei Cloud-Daten dazu.

Bei 35 bis 37 Prozent der Unternehmen geht es in der Cloud-Sicherheit klassisch zu, sie vertrauen auf Maßnahmen wie Verschlüsselung, Firewall und Backups.

Eine starke Kontrolle über System-Level-Ressourcen und Virtual Machines, Cloud IDS / IPS und CASB (Cloud Access Security Broker) nutzt maximal ein Viertel der Unternehmen. Dabei ist die Umsetzung dieser neueren Ansätze für Cloud-Sicherheit abhängig davon, wie hoch die jährlichen Aufwendungen für Cloud-Services sind. Bei bis zu einer Million pro Jahr sind es bis zu 16 Prozent der Unternehmen, bei mehr als 100 Millionen Aufwendungen pro Jahr aber schon bis zu 34 Prozent.

Offensichtlich steigt das Interesse an neuen Security-Verfahren bei höheren Investitionen in die Cloud.

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

Angaben in Prozent. Mehrfachnennungen möglich. Basis: n = 351

	Gesamt	Jährliche Aufwendungen in Cloud Services		
		< 1 Mio.	1-100 Mio	100 Mio. +
Verschlüsselte Datenübertragung vom und zum Cloud-Provider (z.B. VPN)	36,8	42,4	34,6	40,0
Cloud-Firewall	36,5	32,3	39,7	28,0
Lokale Daten-Backups möglich	35,0	33,3	35,3	38,0
Schutz vor DDoS-Attacken	32,5	22,2	33,1	40,0
Gute Endpoint-Kontrolle (sichere Clients)	30,8	35,4	33,1	18,0
Verbesserte Zugangs- und Rechtekontrolle (IAM)	31,1	33,3	29,4	28,0
Verbessertes Passwortmanagement (starke Passwörter, kurze Wechselzyklen, Passwort-Tools ...)	31,1	32,3	30,9	20,0
Integritätskontrolle bei Cloud-Daten	28,2	24,2	33,1	30,0
Starke Kontrolle über System-Level-Ressourcen und Virtual Machines	25,1	16,2	26,5	34,0
Cloud IDS / IPS	24,2	14,1	33,8	30,0
CASB (Cloud Access Security Broker)	17,9	12,1	19,9	34,0

7. Der einheitliche EU-Datenschutz ist in den Köpfen der Cloud-Nutzer angekommen

Es muss nicht ein Cloud-Dienst aus Deutschland sein, entscheidend für die Unternehmen ist die Einhaltung des EU-Datenschutzes, wenn sie einen Cloud-Anbieter auswählen. Ein Vertrag nach deutschem Recht ist aber besser als ein US-Vertrag.

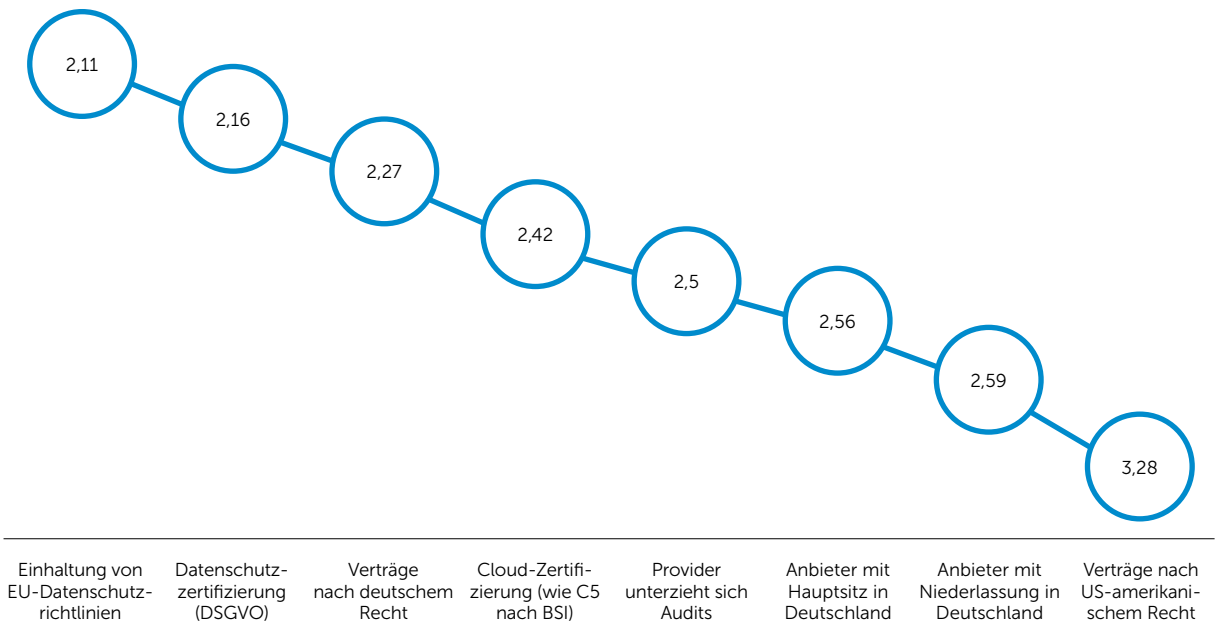
Die Harmonisierung des Datenschutzes in der EU hat bereits Früchte getragen, wenn es um die Suche nach einem Cloud-Anbieter geht. Verträge nach deutschem Recht und ein deutsches Cloud-Testat wie C5 (nach den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik, BSI) spielen eine geringere Rolle als die Einhaltung der EU-Datenschutzrichtlinien und eine Datenschutzzertifizierung nach Datenschutz-Grundverordnung (DSGVO).

Auch ein Standort oder eine Niederlassung in Deutschland sind im Vergleich zum EU-Datenschutz nachrangig. Abgeschlagen sind Verträge nach US-Recht, das gilt im Vergleich zu Verträgen nach deutschem Recht und erst recht im Vergleich zur Einhaltung der DSGVO.

Cloud-Anbieter sollten also stärker auf eine Zertifizierung nach DSGVO setzen. Bis es entsprechend akkreditierte Zertifizierungsstellen nach DSGVO gibt und die ersten echten DSGVO-Zertifikate auf den Markt kommen, empfiehlt sich die Durchführung eines Datenschutz-Audits, denn auch darauf achten die Cloud-Nutzer in Deutschland.

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

Arithmetische Mittelwerte auf einer Schulnotenskala von 1 „Absolut geschäftskritisch" bis 6 „Absolut geschäftsunkritisch". Basis: n = 350



8. Backup der Cloud-Daten sehen viele Nutzer als Aufgabe des Providers

Die Unternehmen erwarten vom Cloud-Anbieter ähnliche Schutzmaßnahmen, wie sie auf ihrer Seite selbst durchführen. Neben der Datensicherung wünschen sich die Nutzer insbesondere die Authentifizierung und Verschlüsselung bei Übertragung und Speicherung vom Anbieter der Wahl.

Anforderungen wie eine provider-unabhängige Verschlüsselung (25 Prozent) und die Zugangskontrolle über SSO (Single-Sign-On, 19 Prozent) gehören ebenso wenig zu den Top 10 der gewünschten Sicherheitsmaßnahmen wie der Ausschluss von Servertechnik aus den USA (21 Prozent) oder China (19 Prozent).

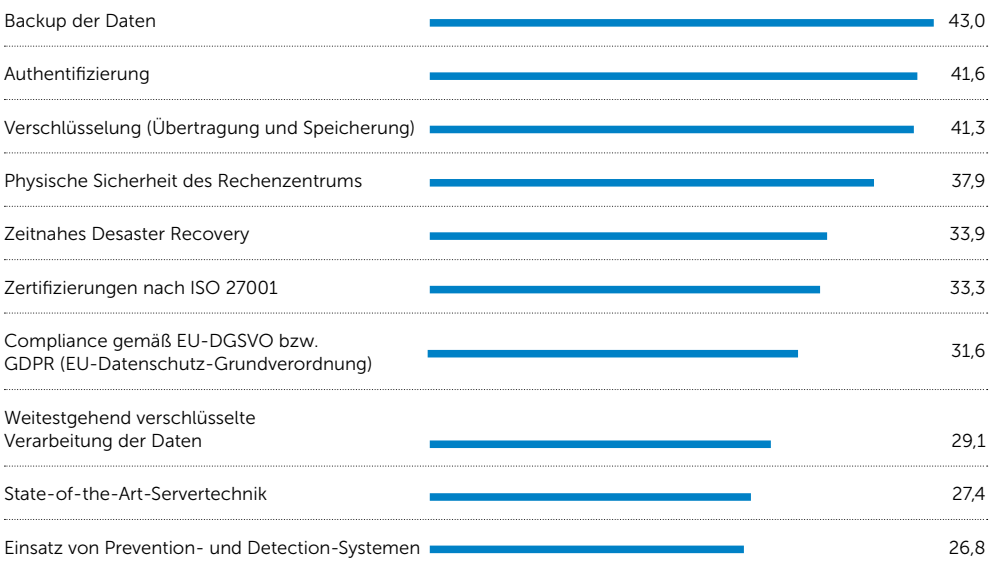
Forderungen an technische Maßnahmen des Cloud-Providers wie Backup der Daten werden von 43 Prozent der Unternehmen genannt, das Schlusslicht der Top-10-Forderungen ist der Einsatz von Prevention- und Detection-Systemen mit 27 Prozent.

Die Zertifizierung nach ISO 27001 liegt mit 33 Prozent knapp vor der Compliance mit der Datenschutz-Grundverordnung (32 Prozent). Dabei sollte aber nicht vergessen werden, dass viele der technischen Maßnahmen, die als wichtiger eingestuft werden als die DSGVO-Compliance, grundsätzlich notwendig sind, um die DSGVO einzuhalten. Nur dann kann der Provider auch die Vorgaben an eine Auftragsverarbeitung (Artikel 28 DSGVO) nach EU-Datenschutz erfüllen.

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

Angaben in Prozent. Mehrfachnennungen möglich. Auflistung der Top 10. Basis: n = 351

Gesamt



Die zehn technischen Maßnahmen der Cloud-Provider, die insgesamt als besonders wichtig angesehen werden, betrachten die verschiedenen Funktionen im Unternehmen aber durchaus unterschiedlich.

Geschäftsführer stufen die Authentifizierung (42 Prozent) als wichtiger ein als die Backups (38 Prozent). Backups landen bei den Geschäftsführern auf Platz zwei unter den Top-10-Maßnahmen der Cloud-Provider für den technischen Schutz der Daten.

Die CIOs sehen ebenfalls die Authentifizierung (41 Prozent) als besonders wichtig an, gleichzeitig aber auch die physische Sicherheit im Rechenzentrum des Cloud-Anbieters (ebenfalls 41 Prozent). Das Backup der Daten nennen unter den CIOs nur 28 Prozent.

Ganz anders sehen dies die Fachbereiche: 53 Prozent halten die Backups für die zentrale technische Maßnahme des Cloud-Anbieters, 45 Prozent nennen die Verschlüsselung der Daten bei Übertragung und Speicherung, die Authentifizierung kommt bei den Fachbereichen auf 40 Prozent.

Ergebnis-Split nach Funktion im Unternehmen

	Geschäftsführung/ COO/CFO/ sonst. Vorstand	CIO/IT-Vorstand/ CDO/CTO/ Technikvorstand	Fachbereiche (Vertrieb, Marketing, Produktion, Einkauf, anderer FB)
Backup der Daten	37,8	28,4	52,8
Authentifizierung	41,9	40,9	39,8
Verschlüsselung (Übertragung und Speicherung)	31,1	39,8	45,4
Physische Sicherheit des Rechenzentrums	28,4	40,9	36,1
Zeitnahes Desaster Recovery	23,0	37,5	31,5
Zertifizierungen nach ISO 27001	32,4	34,1	28,7
Compliance gemäß EU-DGSVO bzw. GDPR (EU-Datenschutz-Grundverordnung)	25,7	29,5	29,6
Weitestgehend verschlüsselte Verarbeitung der Daten	28,4	26,1	30,6
State-of-the-Art-Servertechnik	21,6	29,5	17,6
Einsatz von Prevention- und Detection-Systemen	21,6	23,9	31,5

9. Sicherheitsrisiken der Cloud-Dienste werden zu einseitig gesehen

Obwohl von DDoS-Attacken berichtet wird und die Forderung nach einer Datensicherung durch den Cloud-Anbieter vorherrscht, stehen bei den Unternehmen andere Risiken im Fokus als DDoS-Angriffe und Datenverlust. Insbesondere Hacker-Angriffe und der Diebstahl von Daten werden gefürchtet, weniger Gefahren durch Innentäter.

Nur drei bis fünf Prozent der Unternehmen sehen große Risiken für Cloud-Dienste, wenn die Datenintegrität fehlt, der virtuelle Zugriffsschutz mangelhaft ist oder Daten aus der Cloud durch Insider-Attacken abfließen. Auch APTs (Advanced Persistent Threats) und mangelhafter physischer Zugriffsschutz gehören nicht zu den Top-Risiken in den Augen der Cloud-Nutzer.

Als besonders riskant dagegen bezeichnen 16 Prozent der Unternehmen Angriffe von Hackern, zwölf Prozent fürchten Datendiebstahl. DDoS-Attacken und Datenverlust nennen nur sechs Prozent der Unternehmen als große Bedrohung.

Interessant ist auch, dass der Datenschutz grundsätzlich als sehr wichtig erachtet wird, ein Mangel an Datenschutz jedoch nur für acht Prozent ein großes Risiko darstellt. Offensichtlich wird nicht der Zusammenhang gesehen zwischen Sicherheitsrisiken und Datenschutzmängeln. Das zeigt sich auch daran, dass mangelnde Belastbarkeit und fehlende Datentrennung nach Mandanten in der Rangfolge der Sicherheitsrisiken weiter unten stehen. Beide Risiken führen zu Problemen bei der Einhaltung der Datenschutz-Grundverordnung, die eigentlich einen hohen Stellenwert bei den Cloud-Nutzern hat.

Was schätzen Sie ganz allgemein als größtes Security-Risiko bei Cloud-Services ein?

Angaben in Prozent. Auflistung der Top 10. Basis: n = 347

10. Der Cloud-Datenschutz wird teils besser bewertet als der interne Datenschutz

Die Forderungen an den Datenschutz des Cloud-Anbieters sind hoch. 13 Prozent der Unternehmen denken trotzdem, dass der Cloud-Datenschutz besser ist als der Datenschutz bei intern betriebenen IT-Diensten. Die Datenverfügbarkeit in der Cloud sehen sogar 18 Prozent als besser an, wenn sie sie mit der Verfügbarkeit bei On-Premise-Lösungen vergleichen.

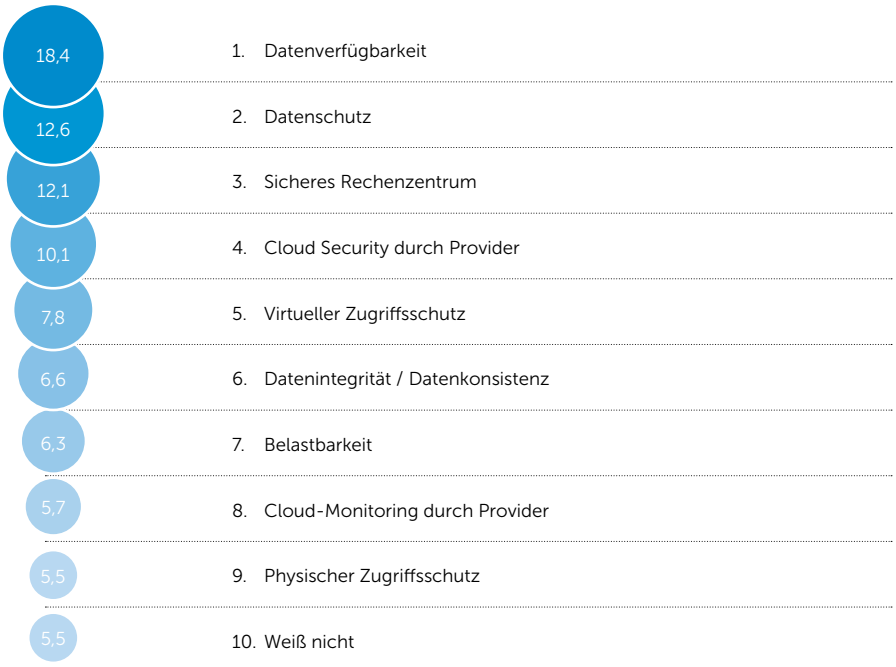
Cloud-Anbieter sind erfolgreicher als die Unternehmen selbst, wenn es um Datenschutz und Sicherheit geht; das denken immerhin zwischen zehn und 18 Prozent der Unternehmen. Eine höhere Verfügbarkeit der Daten, ein besserer Datenschutz, ein sicheres Rechenzentrum und die Maßnahmen für die Cloud-Sicherheit, das sind die wesentlichen Vorzüge für die Sicherheit, wenn man Cloud-Dienste und On-Premise-Services vergleicht.

Selbst das Cloud-Monitoring durch den Provider wird von sechs Prozent der Unternehmen als Vorteil gesehen. Dabei wird jedoch vergessen, dass ein Monitoring der Cloud-Dienste auch der Kontrolle des Providers dienen soll. Macht er dieses Monitoring selbst, kann die Aufgabe der Kontrolle, die auch aus der Datenschutz-Grundverordnung (DSGVO) erwächst, gar nicht erfüllt werden.

Die Unternehmen schätzen offensichtlich ihre bestehenden Security-Probleme im eigenen Unternehmen als höher ein als die des Cloud-Anbieters. Automatisch kann man jedoch nicht von diesen Vorteilen des Cloud-Anbieters ausgehen, wie zahlreiche Vorfälle bei Providern zeigen, etwa Cloud-Ausfälle, die die Datenverfügbarkeit bedrohen.

Was schätzen Sie als größten Security-Vorteil von Cloud-Services im Vergleich zu On-Premise-Lösungen ein?

Angaben in Prozent. Auflistung der TOP 10. Basis: n = 348



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.

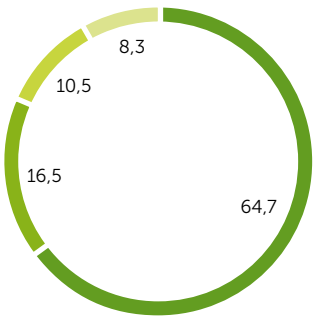
Cloud-Services sind in den Unternehmen in Deutschland angekommen und kaum noch wegzudenken. Nur für acht Prozent der Unternehmen kommen Cloud-Services nicht infrage. 92 Prozent der Unternehmen nutzen bereits Cloud-Dienste, sie planen es in den nächsten zwölf Monaten (17 Prozent) oder prüfen es intern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

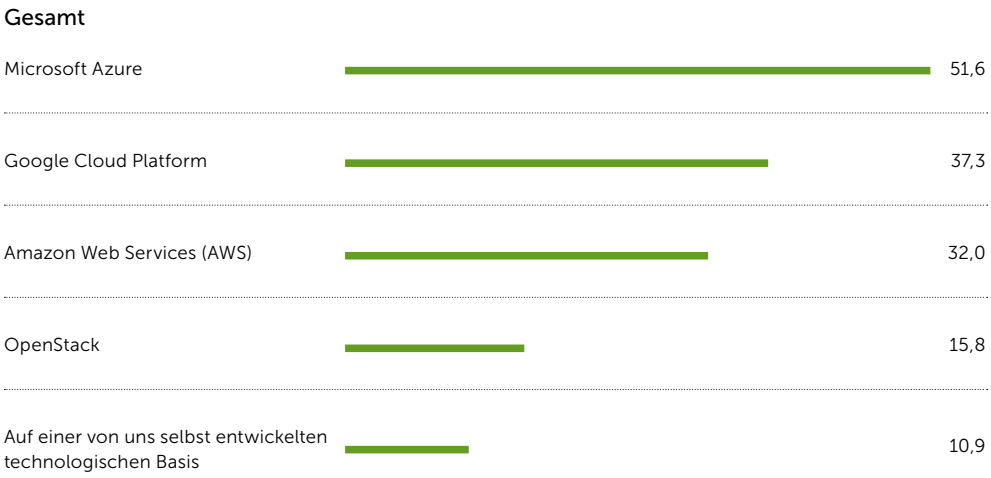
2. Microsoft Azure ist weit verbreitet und beliebt

Die genutzten Cloud-Infrastrukturen laufen bei 52 Prozent der Unternehmen auf Microsoft Azure. Bei 37 Prozent handelt es sich um die Google Cloud Platform. Auf Platz drei liegt AWS (Amazon Web Services) mit 32 Prozent. OpenStack ist die Basis bei 16 Prozent der befragten Unternehmen. Elf Prozent haben eine eigene technologische Basis entwickelt.

Die Verbreitung der Cloud-Plattformen bei den befragten Unternehmen deckt sich allerdings nicht mit der Zufriedenheit. In dem Ranking, wie zufrieden die Unternehmen mit der von ihnen genutzten Cloud-Plattform sind, dominiert ebenfalls Microsoft Azure, gefolgt von Amazon Web Services (AWS). Die bei der Verbreitung auf Platz vier liegende OpenStack-Plattform ist die Nummer drei bei der Zufriedenheit. Google Cloud Platform rutscht bei der Zufriedenheit dagegen auf Platz vier. Den letzten Platz bei der Zufriedenheit belegen die selbst entwickelten Plattformen.

Auf welcher technologischen Basis läuft Ihre Cloud-Infrastruktur?

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

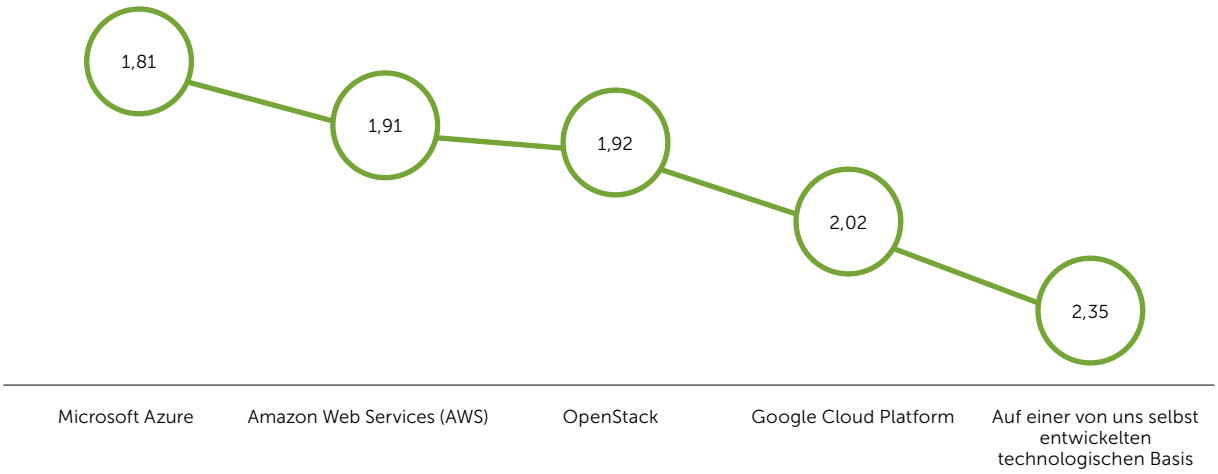


Folgen die Unternehmen ihrer Erfahrung und Zufriedenheit, könnte ein Wechsel von Google Cloud Platform zu einer besser bewerteten Cloud-Infrastruktur erfolgen. Die Idee, eine eigene Cloud-Plattform zu entwickeln, dürfte keine große Zukunft haben, da die Zufriedenheitswerte im Vergleich zu den auf dem Markt verfügbaren Plattformen eher gering sind.

Für die Cloud-Sicherheit könnte sich die Entwicklung hin zu wenigen, standardisierten Cloud-Plattformen als positiv erweisen, da sich dann auch eher die Cloud-Sicherheitslösungen konzentrieren und standardisieren lassen.

Wie zufrieden sind Sie damit?

Arithmetische Mittelwerte in Ø-Schulnoten (1 „Sehr gut" bis 6 „Ungenügend"). Filter: Nur Unternehmen, denen die technologische Basis namentlich bekannt ist. Basis: n = 297



3. Standarisierung der IT versus Sicherheitsbedenken

Unternehmen sehen einerseits ein höheres Niveau für Datenschutz und IT-Sicherheit als Vorteil einer Cloud-Nutzung. Andererseits sind es Sicherheitsbedenken und Datenschutzgründe, die gegen den Einsatz von Cloud-Services sprechen. Ebenso möchten Unternehmen IT-Standards nutzen, aber nicht von bestimmten Anbietern und Plattformen abhängig sein.

Auch wenn die Verbreitung von Cloud-Services bei den Unternehmen in Deutschland bereits hoch ist, die Entscheidung für Cloud-Dienste fällt den Unternehmen nicht immer leicht. Argumente für die Cloud widersprechen teilweise den Gründen, warum ein Cloud-Einsatz nicht infrage kommt.

Das beste Beispiel sind die Cloud-Sicherheit und der Cloud-Datenschutz. Beide gehören zu den Top 5 der Gründe für die Cloud und zu den Top 5 der Argumente gegen die Cloud. So erwarten sich die Unternehmen ein höheres Sicherheits- und Datenschutzniveau (34 Prozent und 32 Prozent). Allerdings nennen 35 Prozent Sicherheitsbedenken und 29 Prozent Datenschutzfragen als Gründe gegen die Cloud-Nutzung.

Offensichtlich besteht ein erhöhter Bedarf an Aufklärung, wie es wirklich um den Datenschutz und die Sicherheit bei Cloud-Diensten bestellt ist.

Was sind in Ihrem Unternehmen die entscheidenden Argumente für die Nutzung von Cloud-Services?

Angaben in Prozent. Mehrfachnennungen möglich. Auflistung der Top 5. Basis: n = 351

Standardisierung der IT	38,5
Arbeiten von überall und mit jedem Endgerät	34,5
Flexiblere Ressourcennutzung	34,5
Höheres Sicherheitsniveau	34,2
Höheres Datenschutzniveau	32,2

Was sind in Ihrem Unternehmen die größten Hindernisse für die Nutzung von Cloud-Services?

Angaben in Prozent. Mehrfachnennungen möglich. Auflistung der Top 5. Basis: n = 351

Sicherheitsbedenken	35,9
Datenschutzgründe	29,1
Ungeklärte Rechtsfragen	27,6
Befürchtete Abhängigkeit von einem Anbieter (Vendor Lock-in)	23,6
Bedenken bezüglich der Einhaltung von IT-Compliance-Vorgaben	19,9

4. Cloud Security ist meist nicht in Händen der Security-Manager oder CISOs

Obwohl Cloud-Sicherheit sowohl technisch als auch rechtlich und organisatorisch anspruchsvoll sein kann, legen die Unternehmen die Verantwortung dafür nicht in die Hände der eigenen Security-Experten. Bei 36 Prozent der Unternehmen kümmert sich der CIO selbst darum.

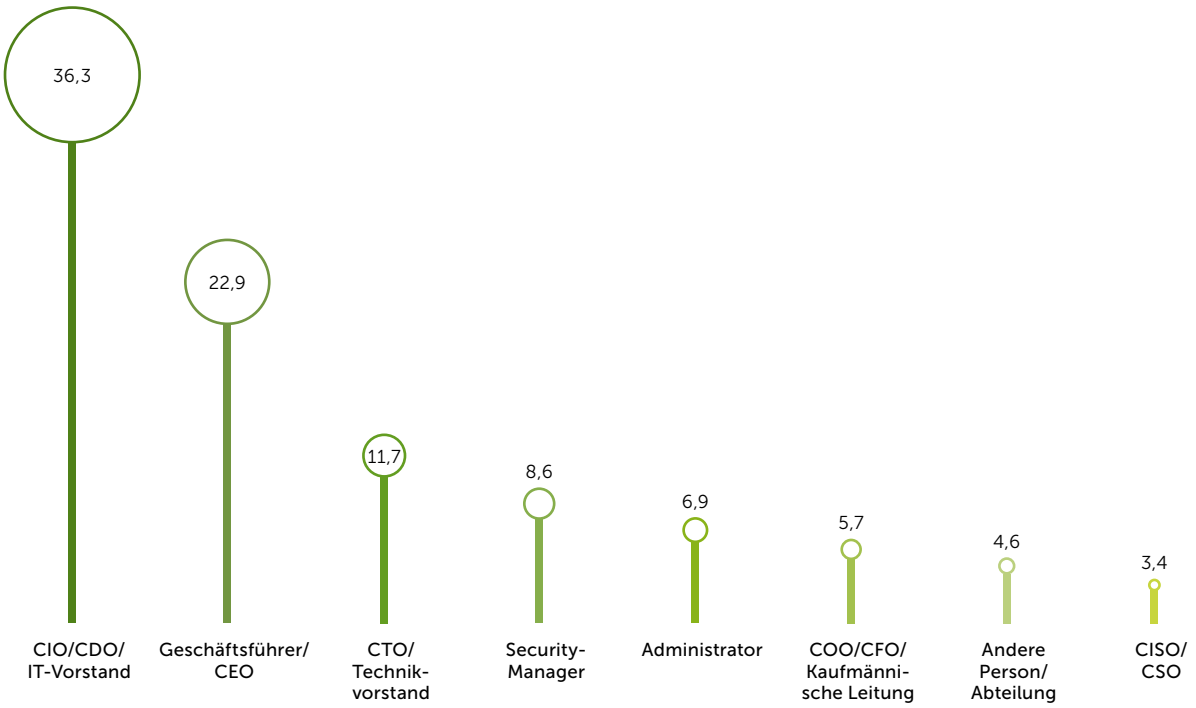
Federführend zuständig für die Cloud-Sicherheit sind die Stellen, die auch generell das Thema Cloud Computing im Unternehmen verantworten. Neben dem CIO kommen als Verantwortliche der Geschäftsführer oder CEO (23 Prozent), der CTO oder Technikvorstand (zwölf Prozent), der Administrator (sieben Prozent), die Kaufmännische Leitung oder der CFO oder COO (sechs Prozent) oder eine andere Abteilung (fünf Prozent) in Betracht.

Security-Manager und CISOs erreichen gemeinsam nur zwölf Prozent Zustimmung, wenn es um die Wahl des Verantwortlichen für Cloud-Sicherheit geht.

Diese Zuordnung der Verantwortlichkeit für die Sicherheit der Cloud-Dienste ist zwiespältig zu bewerten. Einerseits ist es positiv, wenn die Cloud-Sicherheit nicht abgekapselt von anderen Cloud-Entscheidungen behandelt wird. Andererseits bedarf die Cloud-Sicherheit einer hohen und speziellen Kompetenz. Es ist deshalb immer anzuraten, den CISO oder Security-Manager in die Fragen rund um die Cloud-Sicherheit einzubeziehen.

Wer in Ihrem Unternehmen ist federführend verantwortlich für Cloud Security?

Angaben in Prozent. Basis: n = 350



5. Preis-Leistungs-Verhältnis und Ausfallsicherheit sind Trumpf

Zu den wichtigsten Kriterien bei der Auswahl eines Cloud-Providers zählen neben Vertrauen und Datenschutz auch das Verhältnis von Preis und Leistung. Bei den Leistungen des Rechenzentrums, das die Cloud-Dienste betreibt, geht es den befragten Unternehmen insbesondere um Sicherheit, Compliance und Support.

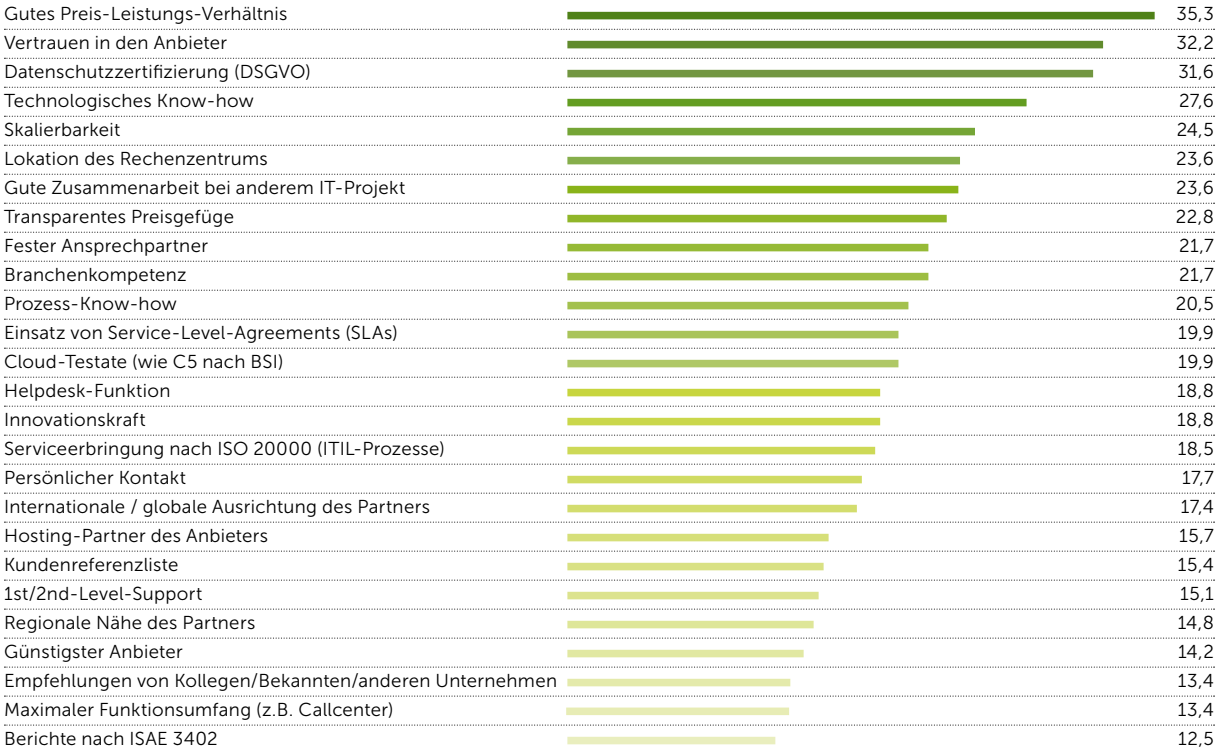
Die zehn wichtigsten Kriterien, die ein Cloud-Anbieter nach Meinung der befragten Unternehmen erfüllen sollte, reichen von preiswerten Leistungen (35 Prozent) und Vertrauenswürdigkeit (32 Prozent) bis hin zu einem festen Ansprechpartner und der notwendigen Branchenkompetenz (jeweils 22 Prozent).

Interessant ist, dass Kriterien wie Kundenreferenzliste, 1st/2nd-Level-Support, regionale Nähe des Partners und günstigster Anbieter nur von jeweils 14 bis 15 Prozent der Unternehmen genannt werden, obwohl diesen Kriterien bisher in Marktanalysen eine hohe Relevanz zugestanden wurde. Dies wird bei den verschiedenen Funktionen im Unternehmen, vom Geschäftsführer bis hin zu den Fachbereichen, sehr ähnlich gesehen. Der „günstigste Anbieter" spielt in der Geschäftsführung sogar eine noch geringere Rolle: Nur zehn Prozent der Geschäftsführer nannten dieses Kriterium.

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

Angaben in Prozent. Mehrfachnennungen möglich. Basis: n = 351

Gesamt



Betrachtet man das Rechenzentrum, in dem die Cloud-Dienste erbracht werden sollen, stehen insbesondere Sicherheit und Datenschutz im Fokus. Ein Rechenzentrumsstandort in Deutschland wurde hier als besser eingestuft als ein Standort innerhalb der EU. Hier geht es den Unternehmen offensichtlich weniger um Compliance-Fragen als um die Erreichbarkeit und räumliche Nähe.

Das Kriterium „Abstand zwischen RZ und Recovery-RZ mehr als 100 Kilometer" kommt hier auf den letzten Platz, auch bei den IT-Leitern und bei den Fachbereichen. Dies ist insofern interessant, als das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Kriterien für die Standortwahl höchstverfügbarer und georedundanter Rechenzentren im Dezember 2018 so festgelegt hat, dass sich „einander Georedundanz gebende RZ einen Mindestabstand von ca. 200 km haben sollen".

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

Arithmetische Mittelwerte auf einer Schulnotenskala von 1 „Absolut geschäftskritisch" bis 6 „Absolut geschäftsunkritisch". Basis: n = 348

Ausfallsicherheit: Provider bietet SLAs für die Datenwiederherstellung	2,11
Provider hat Prozesse zur Einhaltung der Meldepflichten nach DSGVO etabliert	2,17
Rechenzentrum in Deutschland mit deutschem Rechenzentrumsbetrieb und deutschem Support	2,20
Provider unterstützt Untersuchungen bzgl. Vorfällen und Anwenderaktivitäten in der Cloud	2,23
Backup-Rechenzentrum	2,29
Provider garantiert Mandantenfähigkeit	2,29
RZ gemäß Qualitätsstufe Tier IV	2,32
Rechenzentrum in EU	2,35
RZ gemäß Qualitätsstufe Tier III	2,40
Rechenzentrum in Deutschland mit globalem Rechenzentrumsbetrieb und Support	2,42
Hardware namhafter Hersteller	2,54
Abstand zwischen RZ und Backup-RZ mehr als 10 Kilometer	2,63
Begehbares Rechenzentrum (mögliches Audit vor Ort)	2,64
Abstand zwischen RZ und Recovery-RZ mehr als 100 Kilometer	2,67

6. Die Risiken für Cloud-Dienste haben viele Gesichter

Die Unternehmen wurden nicht nur gefragt, welche Risiken sie für die von ihnen genutzten Cloud-Dienste sehen, sondern auch, warum. Die Statements der Unternehmen geben einen beispielhaften Einblick, wie die Risikowahrnehmung in der Praxis aussieht und warum bestimmte Risiken nicht so von den Unternehmen erkannt werden, wie die Bedrohungslage nach Meinung von IT-Sicherheitsforschern in Wirklichkeit ist.
In den grünen Kästen lesen Sie jeweils die Einschätzung des Studienautors.

„Der Anbieter hat viele Kunden, daher besteht immer die Gefahr der Vermischung von Daten verschiedener Kunden."

Die Sorge, die Mandantentrennung könne unvollständig sein, ist ein wesentlicher Grund, warum Unternehmen auf eine Public Cloud verzichten. Eine Cloud, die der DSGVO entspricht, muss aber eine funktionierende Mandantentrennung vorweisen können. DSGVO-Zertifikate können also helfen, die Sorge zu entkräften.

„Selbst die besten Verschlüsselungen sind zu knacken."

Sicherheitskonzepte, die mehrstufig sind und nicht nur auf Verschlüsselung vertrauen, können die Risiken reduzieren. Cloud-Sicherheit sollte immer mehrstufig sein.

„Cloud-Systeme sind noch nicht so lange auf dem Markt. Die Möglichkeiten bestehen, dass evtl. Sicherheitslücken Hacker-Angriffen ausgesetzt sind."

Sicherheitslücken gibt es auch bei Technologien, die schon sehr lange auf dem Markt sind. Wichtig ist der Nachweis eines funktionierenden Patch-Managements.

„Die Priorität des Restaurierens bei Datenverlust hängt von der Größe des Kunden ab. Als kleiner Kunde hat man praktisch kaum Druckmittel, auch wenn kritische Unternehmensdaten in der Cloud liegen. Will ich mein Geschäft zu jemandem auslagern, über den ich praktisch keine Kontrolle habe und der doch nur sehr eingeschränkt Schadensersatz im Falle eines Datenverlusts leisten wird? Wohl kaum …"

Cloud-Anbieter müssen auch kleine Kunden umfassend schützen. Hier ist eine bessere Kundenkommunikation gefragt, damit sich kein Kunde unwichtig vorkommt. Die Forderungen der DSGVO müssen erfüllt werden, unabhängig vom Umsatz mit dem Kunden.

„Weil in letzter Zeit selbst Daten von Bundestagsabgeordneten in die Öffentlichkeit gelangten. Weil E-Mails und Passwörter aus Servern geklaut wurden."

Hier zeigt sich beispielhaft, wie die Meldungen in den Medien die Risikowahrnehmung prägen und beeinflussen können.

„Wenn unsere Daten in fremde Hände kommen, ist dies massiv geschäftsschädigend und ein sehr großer Vertrauensverlust in der Öffentlichkeit."

Datenschutz ist tatsächlich Kundenschutz und Schutz gegen Verlust an Image und den Umsatzfolgen.

7. Cloud-Sicherheit ist auch eine Bauchentscheidung

Trotz aller Planung erfolgt die Entscheidung für oder gegen einen Cloud-Dienst nicht nur auf Basis harter Fakten. Die Unternehmen wurden auch nach ihrem Empfinden befragt, wie sie bestimmte Bezugsmodelle für Cloud-Services sehen. Dabei werden auch die Cloud-Modelle weniger gut bewertet, die als die Zukunft des Cloud Computing gesehen werden.

Private Clouds und Virtual Private Clouds werden von den Unternehmen im Durchschnitt als sicherer empfunden als On-Premise-Umgebungen. Das kann als gutes Zeichen für die weitere Entwicklung des Cloud Computing gewertet werden.

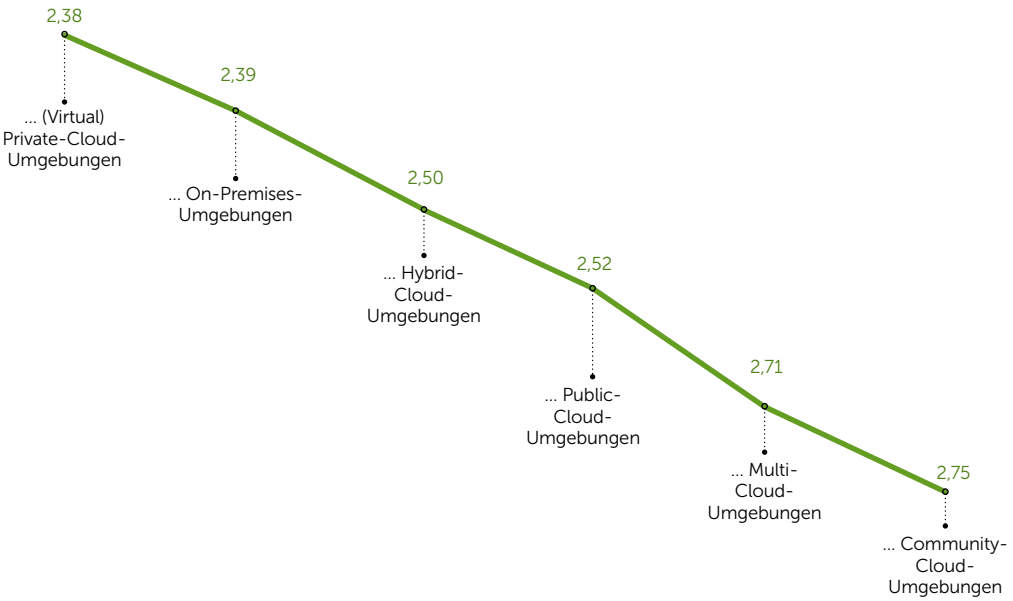
Hybride Clouds werden als weniger sicher angesehen als On-Premise-Umgebungen. Das ist insofern interessant, als hybride Clouds eine nicht weiter bestimmte Mischung aus Cloud-Diensten und lokalen Diensten sind. Es können sich große Anteile von On-Premise-Lösungen darunter befinden, aber auch Public Clouds und Private Clouds. Wie sicher eine hybride Cloud im Vergleich zu den anderen Bezugsmodellen ist, kommt auf die genaue Zusammensetzung an. Nicht allen Unternehmen ist dies jedoch bewusst.

Bemerkenswert ist, dass das Modell der Multi-Clouds hinsichtlich der Sicherheit relativ schlecht bewertet wird. Dabei kann Multi-Cloud auch für mehrere Private Clouds stehen. Auch sind die Bedeutung und die mögliche Zusammensetzung den Unternehmen nicht klar genug.

Community Clouds werden mit hoher Wahrscheinlichkeit deshalb eher als weniger sicher bewertet, weil dieses Bezugsmodell nicht sehr bekannt und verbreitet ist.

Wie sicher empfinden Sie ganz allgemein ...

Arithmetische Mittelwerte. Bewertung auf einer Schulnotenskala von 1 „Sehr sicher" bis 6 „Sehr unsicher". Basis: n = 348



8. Bedeutung der Cloud-Sicherheit für die Performance wird verkannt

Die Unternehmen wurden mit dem Statement konfrontiert, Performance sei wichtiger als Sicherheit. 18 Prozent der befragten Firmen stimmten voll und ganz zu. Dabei stellt sich die Frage, wie Performance und die Gewährleistung von Performance bei Cloud-Diensten verstanden werden. Die Rolle der Sicherheit dafür muss stärker kommuniziert werden.

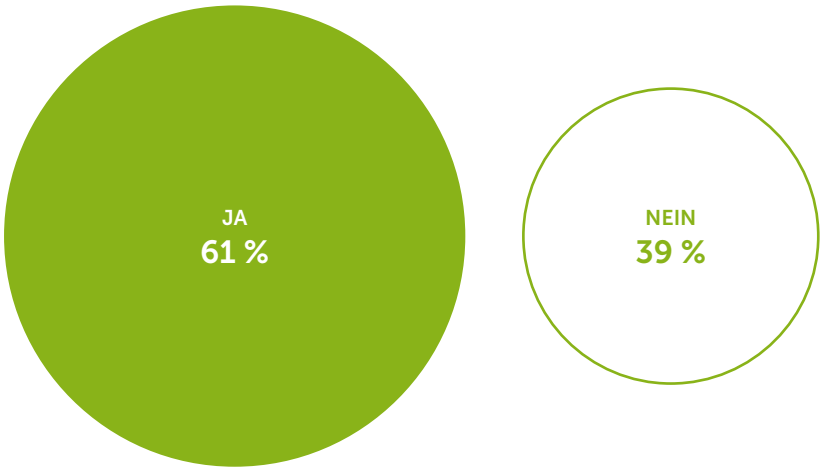
Wenn die Performance gegen die Sicherheit antritt, dann erreicht die Sicherheit 39 Prozent Zustimmung, die Performance 61 Prozent. Voll und ganz überzeugt von der größeren Bedeutung der Sicherheit sind neun Prozent im Vergleich zu 18 Prozent, die die Performance klar vor der Sicherheit sehen.

Dieses Stimmungsbild wird der Bedeutung der Cloud-Sicherheit nicht gerecht. Die scheinbar höhere Bedeutung der Performance macht deutlich, dass die Sicherheit nicht richtig wahrgenommen wird. Sicherheit ist bei Cloud-Diensten die Grundlage der Performance. Ohne Sicherheit kann keine Performance gewährleistet werden.

Die Überlastungsangriffe (DDoS-Attacken) auf Cloud-Dienste, von denen die Unternehmen berichten, sind das beste Beispiel dafür, dass eine mangelhafte Cloud-Sicherheit zum Problem für die Cloud-Performance werden kann. Selbst der komplette Ausfall des Cloud-Dienstes kann durch DDoS-Angriffe verursacht werden. Offensichtlich besteht hier noch Aufklärungsbedarf über die Leistungen der Cloud-Sicherheit.

Inwiefern stimmen Sie folgender Aussage zu oder nicht:
In der Cloud gilt für mich als Unternehmen: Performance vor Sicherheit?

Angaben in Prozent. Basis: n = 349



9. Richtlinien zur Cloud-Nutzung sind eher allgemein als speziell

Die Sicherheitsrichtlinien beziehen sich bei 68 Prozent der befragten Unternehmen auf E-Mail. Die Nutzung von Cloud-Diensten wird bei 57 Prozent der Unternehmen geregelt, genauso häufig ist der Umgang mit personenbezogenen Daten Gegenstand der Richtlinien. Filesharing-Lösungen wie Dropbox regeln dagegen nur 43 Prozent der Unternehmen.

Sicherheitsrichtlinien sind ein elementarer Bestandteil der organisatorischen IT-Sicherheit. Sie enthalten die Vorgaben, die die sichere Nutzung von IT-Diensten und Systemen gewährleisten sollen. Obwohl kaum ein Unternehmen auf E-Mail verzichtet, haben 32 Prozent der befragten Firmen keine Sicherheitsrichtlinie zur E-Mail-Nutzung.

Im Vergleich dazu liegt die Verbreitung von Sicherheitsrichtlinien zur Cloud-Nutzung hoch, allerdings nur für die allgemeine Anwendung der Cloud. Betrachtet man spezielle Cloud-Dienste wie Office aus der Cloud, sind es nur noch 42 Prozent, die Sicherheitsrichtlinien eingeführt haben, obwohl Office-Lösungen zu den besonders beliebten Cloud-Diensten bei den Unternehmen zählen.

Betrachtet man die Höhe der jährlichen Cloud-Aufwendungen, sind es die Unternehmen mit bis zu einer Million Euro Cloud-Budget, die besonders stark auf Sicherheitsrichtlinien setzen, bei E-Mail sind es 73 Prozent, die allgemeine Cloud-Nutzung jedoch wird mit 46 Prozent unterdurchschnittlich reguliert.

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

Angaben in Prozent. Mehrfachnennungen möglich. Filter: Es gibt im Unternehmen Sicherheitsrichtlinien / -Policies. Basis: n = 301

	Gesamt	Jährliche Aufwendungen in Cloud-Services		
		< 1 Mio.	1-100 Mio	100 Mio. +
E-Mail	68,1	72,8	61,9	57,4
Allgemeiner Umgang mit Daten (z.B. in Office-Dokumenten)	57,1	59,3	53,2	42,6
Cloud-Anwendungen generell	57,1	45,7	66,7	48,9
Umgang mit personenbezogenen Daten	56,1	69,1	46,8	31,9
Filesharing-Tools (Dropbox & Co.)	42,9	53,1	34,9	42,6
Office aus der Cloud	42,2	38,3	41,3	55,3
Social Networks	41,2	39,5	38,9	38,3
Skype for Business	35,2	28,4	35,7	42,6
Collaboration	32,2	25,9	36,5	29,8
Auf andere Bereiche	1,0	2,5	0,0	2,1

10. Für neun von zehn Unternehmen sind Zertifizierungen und Siegel wichtig

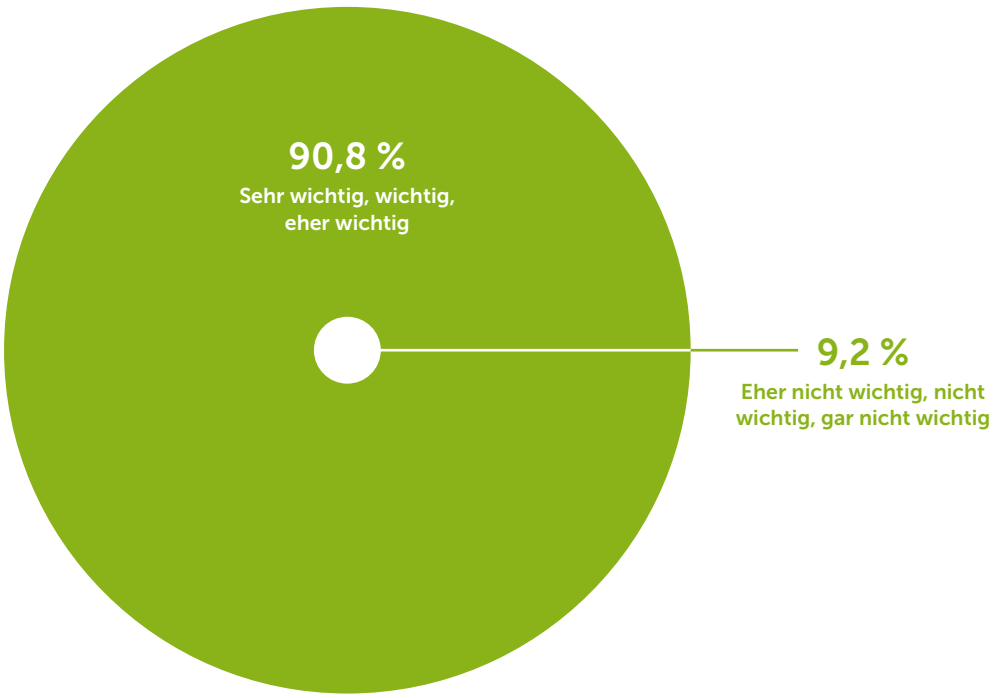
Nur ein Prozent der befragten Unternehmen meint, Siegel, Zertifizierungen und Prüfungen sind nicht wichtig, wenn es um Cloud-Sicherheit geht. Für 35 Prozent sind diese Nachweise dagegen sehr wichtig, für 41 Prozent sind sie wichtig. Cloud-Sicherheit braucht somit mehr als Vertrauen, die Cloud-Nutzer möchten Gewissheit über die Sicherheit haben.

Die Einschätzung, ob Prüfungen, Siegel und Zertifizierung zur Cloud-Sicherheit wichtig sind oder nicht, ist weniger eine Frage der Größe des Unternehmens, wenn man diese an der Mitarbeiterzahl festmacht. Die Unternehmen mit weniger oder mehr als 1.000 Mitarbeitern in Deutschland gaben hier recht ähnliche Antworten. Allein die Antwort, Siegel und Zertifizierungen seien eher wichtig, ist bei den Unternehmen mit weniger Mitarbeitern in Deutschland stärker vertreten als bei den Unternehmen mit mehr als 1.000 Mitarbeitern (22 Prozent im Vergleich zu neun Prozent).

Anders sieht ein Vergleich aus, wenn man die jährlichen Cloud-Aufwendungen betrachtet. Die Unternehmen, die mehr als 100 Millionen Euro für Cloud-Dienste pro Jahr aufwenden, halten zu 49 Prozent die Siegel und Zertifizierungen für sehr wichtig. Unternehmen mit bis zu einer Million Euro Aufwendungen für Cloud-Dienste dagegen gaben diese Antwort nur in 30 Prozent der Fälle. Offensichtlich möchten Unternehmen mit höheren Investitionen in die Cloud auch mehr Gewissheit bei der Cloud-Sicherheit.

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

Angaben in Prozent. Bewertung auf einer Schulnotenskala von 1 „Sehr wichtig" bis 6 „Gar nicht wichtig" Basis: n = 318



11. Die Nutzung von Managed Security Services steigt mit dem Cloud-Budget

68 Prozent der befragten Unternehmen nutzen Managed Security Services, 49 Prozent allerdings nur manchmal. 15 Prozent der Unternehmen verwenden keine Dienste von Managed Security Service Providern. 17 Prozent können allerdings nicht sagen, ob sie solche Dienste einsetzen oder nicht.

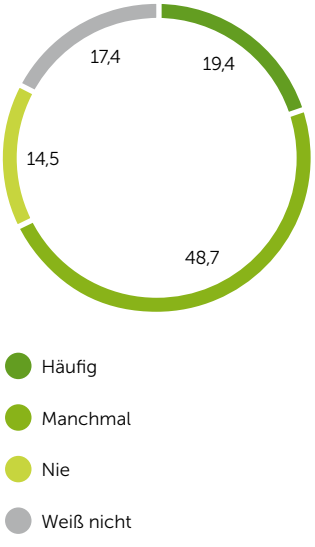
Die Antworten, ob Managed Security Services (MSS) eingesetzt werden, hängen stark von den jährlichen Aufwendungen für Cloud-Dienste ab. So ist die Unsicherheit, ob solche Security-Services eingesetzt werden oder nicht, bei den Unternehmen mit 24 Prozent am höchsten, die bis zu einer Million Euro pro Jahr für die Cloud aufwenden. Bei den Unternehmen, die zwischen einer und 100 Millionen Cloud-Budget pro Jahr haben, sind es nur noch sechs Prozent. Unternehmen, die mehr als 100 Millionen Euro jährlich für die Cloud-Dienste ausgeben, kennen diese Ungewissheit nicht, sie wissen genau, ob sie MSS nutzen oder nicht.

55 Prozent der Unternehmen mit einem Cloud-Budget von mehr als 100 Millionen Euro pro Jahr setzen Managed Security Services häufig ein, bei ein bis 100 Millionen jährlichen Cloud-Aufwendungen sinkt die Zahl der häufigen MSS-Nutzer auf 20 Prozent. Bei weniger als einer Million Euro pro Jahr für Cloud-Aufwendungen sind es nur noch 14 Prozent, die häufig zu Managed Security Services greifen.

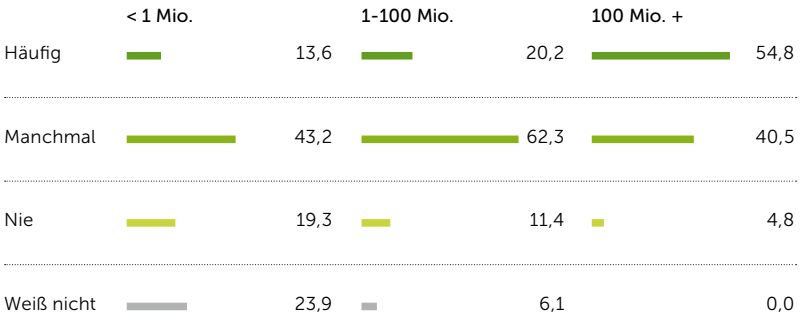
Greifen Sie im Hinblick auf die eingesetzten Cloud-Services auch auf dedizierte Managed Security Service Provider (MSSP) zurück?

Angaben in Prozent. Basis: n = 351

Gesamt



Ergebnis-Split nach jährliche Aufwendungen in Cloud-Services



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.

Zertifikate werden Cloud-Sicherheit transparenter machen
Mit der Datenschutz-Grundverordnung entstehen Instrumente, die die Transparenz in der Cloud-Sicherheit erhöhen werden. Im Rahmen der DSGVO-Zertifizierung werden die Sicherheitskriterien, die erfüllt werden, klar benannt. Dabei werden solche Zertifikate nicht nur für Security-Experten verständlich sein, sondern auch und gerade für den jeweiligen Cloud-Entscheider.

Unternehmen erfahren dann, welche Sicherheitsmaßnahmen der Cloud-Anbieter erbringt, ob also zum Beispiel der Wunsch nach einem Cloud-Backup durch den Provider erfüllt wird oder nicht. Mit der Übersicht über die erbrachten Leistungen für die Cloud-Sicherheit wird zudem sichtbar, welche Maßnahmen der Cloud Security durch das Unternehmen noch selbst zu erbringen sind. Zertifizierung und Auditierung helfen so dabei, dass es Cloud-Sicherheit gibt und nicht Cloud-Scheinsicherheit.

Cloud-Risiken müssen konkret bestimmt werden
Die Datenschutz-Grundverordnung hat einen weiteren positiven Effekt für die Cloud-Sicherheit: Cloud Computing gehört trotz der inzwischen hohen Verbreitung zu den neuen Technologien der Digitalisierung. Für den Einsatz solcher Technologien fordert die Datenschutz-Grundverordnung eine sogenannte Datenschutz-Folgenabschätzung (DSFA), zu finden in Artikel 35 der DSGVO.

In der DSFA müssen die Unternehmen vor dem Einsatz eines neuen Verfahrens die damit verbundenen Risiken ermitteln und bewerten und mit den notwendigen Schutzmaßnahmen abmildern. Die DSGVO sorgt also dafür, dass die Risiken der Cloud-Dienste weitaus genauer betrachtet und analysiert werden. Ebenso müssen die Maßnahmen der Cloud-Sicherheit zu den erkannten Cloud-Risiken passen.

Es ist deshalb zu erwarten, dass die Datenschutz-Grundverordnung für ein neues und scharfes Bild der Cloud-Sicherheit führen wird. Den Unternehmen ist die Einhaltung der DSGVO sehr wichtig, im eigenen Haus und beim Cloud-Anbieter.
Die Folge ist dann, dass die Cloud-Sicherheit transparent und besser strukturiert und geplant werden muss. Die DSGVO verändert damit nicht nur den Auswahlprozess für Cloud-Dienste, sondern die Cloud-Sicherheit selbst, indem das Bild von Cloud Security klarer werden wird.

Das betrifft sowohl die Cloud-Provider, die sich einer DSGVO-Zertifizierung unterziehen werden, als auch die Cloud-Nutzer, die selbst der DSGVO unterliegen und in Zukunft noch bessere Informationen über die Cloud-Sicherheit des Anbieters erhalten werden, dank der Datenschutz-Grundverordnung, die weitaus mehr für die Digitalisierung erreicht, als ihr die vielen Kritiker zugestehen wollen.

Studiendesign

Cloud Security 2019

Studiensteckbrief

Herausgeber	COMPUTERWOCHE, CIO, TecChannel und ChannelPartner
Studienpartner	**Platin-Partner:** Cisco Systems GmbH **Gold-Partner:** Akamai Technologies GmbH Micro Focus GmbH PlusServer GmbH **Silber-Partner:** NTT Security GmbH **Bronze-Partner:** genua GmbH SecurEnvoy GmbH
Grundgesamtheiten	Oberste (IT-) und IT-Security-Verantwortliche von Unternehmen in der D-A-CH-Region: strategische (IT-)Entscheider im C-Level-Bereich und in den Fachbereichen (LoBs), 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	351 abgeschlossene und qualifizierte Interviews
Untersuchungszeitraum	22. Januar bis 28. Januar 2019
Methode	Online-Umfrage (CAWI)
Fragebogenentwicklung	IDG Research Services in Abstimmung mit den Studienpartnern
Durchführung	IDG Research Services
Technologischer Partner	Questback GmbH, Köln
Umfragesoftware	EFS Survey Fall 2018

Stichprobenstatistik

Branchenverteilung*	Land- und Forstwirtschaft, Fischerei, Bergbau	4,6 %
	Energie- und Wasserversorgung	10,3 %
	Chemisch-pharmazeutische Industrie, Life-Science	14,0 %
	Metallerzeugende und -verarbeitende Industrie	10,8 %
	Maschinen- und Anlagenbau	8,5 %
	Automobilindustrie und Zulieferer	6,8 %
	Herstellung von elektronischen Gütern, IT-Industrie	12,8 %
	Konsumgüter-, Nahrungs- und Genussmittelindustrie	5,4 %
	Medien, Papier- und Druckgewerbe	3,4 %
	Baugewerbe, Handwerk	4,3 %
	Groß- und Einzelhandel (inkl. Online-Handel)	5,1 %
	Banken und Versicherungen	12,0 %
	Transport, Logistik und Verkehr	11,1 %
	Hotel- und Gastgewerbe, Tourismus	4,3 %
	Dienstleistungen für Unternehmen	16,5 %
	Öffentliche Verwaltung, Gebietskörperschaften, Sozialversicherungen	13,1 %
	Gesundheits- und Sozialwesen	5,4 %
	Schule, Universität, Hochschule	5,4 %
	Andere Branchengruppe	9,0 %
	Keine Angabe	1,1 %
Unternehmensgröße	Weniger als 100 Beschäftigte	5,1 %
	100 bis 999 Beschäftigte	30,2 %
	1.000 bis 9.999 Beschäftigte	37,0 %
	10.000 Beschäftigte und mehr	23,4 %
	Keine Angabe / Weiß nicht	4,3 %
Umsatzklasse deutschlandweit	Weniger als 100 Millionen Euro	16,2 %
	100 bis 999 Millionen Euro	27,9 %
	1 bis unter 2 Milliarden Euro	18,8 %
	2 bis unter 5 Milliarden Euro	15,4 %
	5 Milliarden Euro und mehr	8,5 %
	Keine Angabe / Weiß nicht	13,1 %
Umsatzklasse weltweit	Weniger als 100 Millionen Euro	13,4 %
	100 bis 999 Millionen Euro	21,1 %
	1 bis unter 2 Milliarden Euro	13,7 %
	2 bis unter 5 Milliarden Euro	17,7 %
	5 Milliarden Euro und mehr	18,8 %
	Keine Angabe / Weiß nicht	15,4 %
Jährliche Aufwendungen für IT-Systeme	Weniger als 1 Million Euro	18,2 %
	1 bis 10 Millionen Euro	28,5 %
	10 bis 100 Millionen Euro	25,4 %
	100 Millionen Euro und mehr	10,3 %
	Weiß nicht/keine Angabe	17,7 %

*** Mehrfachnennungen möglich**

Unsere Studienpartner stellen sich vor

Cloud Security 2019

Cisco (NASDAQ: CSCO) hilft als weltweit führender IT-Anbieter Unternehmen dabei, schon heute die Geschäftschancen von morgen zu nutzen. Durch die Vernetzung von Menschen, Prozessen, Daten und Dingen entstehen unvergleichliche Möglichkeiten. Unternehmen können damit Prozesse optimieren, Ressourcen effizienter nutzen und sich so Vorteile gegenüber Wettbewerbern verschaffen.

CISCO IN DEUTSCHLAND

Im Rahmen der Initiative „Deutschland Digital" investiert Cisco gezielt in die Beschleunigung der Digitalisierung in Deutschland – insbesondere in den drei Schwerpunkten Innovation, Cybersicherheit und Bildung. Die Investitionen umfassen Anschubfinanzierungen für konkrete Digitalisierungsprojekte, Forschungsgelder, den Ausbau des Cisco Networking Academy Programms, direkte Investitionen in einen Venture Fund sowie zusätzliche Personal- und Infrastrukturausgaben.

In Deutschland unterhält Cisco Standorte in Garching bei München, Berlin, Bonn, Düsseldorf, Eschborn, Hamburg, Mannheim und Stuttgart. Seit 2019 ist Uwe Peter Vice President und Vorsitzender der Geschäftsführung von Cisco Deutschland. Das Unternehmen setzt auf den indirekten Vertrieb über rund 2.200 zertifizierte Partner in Deutschland.

Das Unternehmen entwickelt und vertreibt Produkte auf Basis des IP-Protokolls in den Bereichen Security, Core Networking, Video und Collaboration, Access (Wired und Mobile), Unified Datacenter und Services. Dabei konzentriert sich das Unternehmen auf die Marktsegmente Enterprise (Großunternehmen, kleine und mittelständische Unternehmen sowie Öffentliche Hand) und Service Provider.

UMFASSENDE SICHERHEIT

Cisco ist ein seit Jahrzehnten erfolgreicher Anbieter und Experte für integrierte IT-Security-Lösungen. Im Jahr 2018 blockierte Cisco weltweit 20 Milliarden Cyber-Bedrohungen – pro Tag. Dabei baut es auf eine umfangreiche Erfahrung mit internen Netzwerken auf. Denn jeden Tag schützt Cisco 122.000 interne und externe Mitarbeiter, das eigene Netzwerk mit mehr als 40.000 Routern, 26.000 Büroanbindungen, 2.500 IT-Anwendungen, 1.350 Testlaboren sowie 500 Cloud-Anwendungen in 170 Ländern. Der ganzheitliche Security-Ansatz basiert auf drei Bereiche:

Das Security & Trust Office (STO) Deutschland ist Teil der weltweiten Security & Trust Organization, in der mehr als 650 Mitarbeiter tätig sind. Es unterstreicht Ciscos kontinuierliches Engagement für mehr Cybersicherheit. Das STO Deutschland dient als zentrale Kontaktstelle für Kunden zur Klärung

strategischer Anforderungen bei Cybersecurity, Datenschutz oder Datensicherheit. Zusätzlich unterstützt es die Cisco Networking Academy dabei, Trainings- und Schulungsmaterial zum Thema Cybersecurity zu entwickeln.

Das Intuitive Network lässt die Vision eines Netzes, das Aktionen vorhersieht und automatisiert, Sicherheitsgefahren abwehrt und sich durch Lernprozesse selbstständig weiterentwickelt, wahr werden. Das neue Netz baut auf der Cisco Digital Network Architecture (DNA) auf und bietet Software und Hardware mit neuen Technologien und Services. Damit verändert Cisco die Basis für Netzwerke von einem Hardware-zentrierten zu einem Software-getriebenen Ansatz. So profitieren Kunden von deutlich höherer Sicherheit, Agilität, Produktivität und Performance.

Die Cisco Talos Intelligence Group ist eines der weltweit größten kommerziellen Teams für Bedrohungsanalyse mit erstklassigen Forschern, Analysten und Entwicklern. Es wird durch führende Telemetrie und intelligente Systeme unterstützt, um genaue, schnelle und umsetzbare sicherheitsbezogene Informationen für Kunden, Produkte und Dienstleistungen von Cisco zu erstellen. Talos schützt sie vor bekannten und neuen Bedrohungen und entdeckt neue Schwachstellen in gängiger Software.

CISCO IN ZAHLEN

Im Geschäftsjahr 2018 erzielte Cisco einen Umsatz von 49,3 Milliarden US-Dollar mit mehr als 70.000 MitarbeiterInnen (Stand: Juli 2018) weltweit. CEO ist Chuck Robbins. Die Geschäftstätigkeiten von Cisco sind in die Regionen Americas, EMEAR (Europa, Naher Osten, Afrika und Russland) und Asia Pacific/Japan/Großchina gegliedert.

PRESSEKONTAKT:

Lars Gurow,
PR Manager Deutschland

Kurfürstendamm 22
10719 Berlin

Telefon: 030-9789-2203
Mobile: 0172-3898713
E-Mail: Lgurow@cisco.com

Cloud Security Solutions von Akamai

Wer online arbeitet, braucht sichere Cloud-Dienste – unabhängig von Standort oder Gerät: Dem hat sich Akamai seit inzwischen über zwei Jahrzehnten verschrieben.

Das Unternehmen aus Cambridge, MA, bietet Kunden die besten IT-Sicherheitsexperten, umfassende Informationen über die weltweite Bedrohungslage und neueste Sicherheitstechnologien, um ihnen im Netz die größtmögliche Sicherheit bei gleichzeitiger Flexibilität zu bieten. In der Bereitstellung und Beschleunigung von Cloud-Diensten ist Akamai führend und stellt seinen Nutzern nicht nur systemübergreifende Kompetenz, sondern auch eine leistungsfähige Infrastruktur zur Seite: die Akamai Intelligent Edge Platform sorgt mit mehr als 240.000 Servern in 130 Ländern für erstklassige Performance und einen umfassenden Schutz gegen Bedrohungen aus dem Internet.

Immer einen Schritt weiter

Ob in der Abwehr großer DDoS-Angriffe oder der Entwicklung der ersten cloudbasierten Web Application Firewall (WAF) und des ersten DDoS-Schutzservices: Akamai steht für Sicherheit. Mit seinen Security Operation Centern wehrt Akamai jeden Monat tausende DDoS-Attacken ab, erkennt neue Angriffsvektoren frühzeitig und kann dank der umfangreichen Erfahrung Angriffe noch schneller abwehren. Ziel ist es, Kunden bei der Bewältigung ihrer wachsenden Sicherheitsanforderungen und bei der Anpassung an die schnelllebige Bedrohungslandschaft zu unterstützen.

Branchenführende Firewall

Täglich finden Experten neue Schwachstellen an Websites und Webanwendungen. Akamai schützt seine Kunden mit einer branchenführenden Web Application Firewall (WAF)-Lösung. Gewonnene Erkenntnisse aus früheren Angriffen gegen Akamai-Kunden und neu entdeckte Schwachstellen helfen Akamai, seine WAF-Anwendungen stetig weiterzuentwickeln und so die Sicherheit für die Kunden auch zukünftig zu gewährleisten. So vertrauen beispielsweise alle weltweit führenden Commerce-Websites, 80 Prozent der weltweit führenden Banken und 70 Prozent der weltweit führenden Fluggesellschaften auf Akamai.

Elmar Witte
Product Marketing Manager Security EMEA, Akamai

„Immer mehr Geschäftsprozesse werden online abgewickelt. Websites und Infrastrukturen effektiv zu schützen gehört für Unternehmen deshalb heute zu einer der wichtigsten Herausforderungen."

„Akamai Sicherheitsexperten interagieren täglich mit 130 Terabytes an Daten, einer Milliarde Geräten und über 100 Millionen IP-Adressen, sie verfügen so über einzigartige Informationen und Einblicke, um Unternehmen zu schützen“

Akamai Technologies GmbH
Parkring 20-22
85748 Garching bei München
Telefon: +49 8994006308
www.akamai.com/de

Schutz vor Manipulation

Akamai hilft Kunden dabei, ihren autoritativen DNS-Service zu schützen und mit ihren Nutzern und Mitarbeitern in Verbindung zu bleiben. Die Lösung von Akamai ist auf Performance und Verfügbarkeit ausgelegt und gewährleistet selbst bei größten DDoS-Angriffen schnelle DNS-Ergebnisse. Außerdem schützt Akamai vor DNS-Fälschungen und Manipulationen.

Effektive Abwehr von Bots

Auch im Erkennen von Bots setzt Akamai Maßstäbe: Bots können bis zu 70 Prozent des Traffics auf einer Website ausmachen und die Performance der Seiten beeinträchtigen. Akamai entwickelt gemeinsam mit seinen Kunden effektive Strategien, um Angriffe durch Bots abzuwehren, um Scraper im Zaum zu halten und Angriffe auf relevante Systeme zu verhindern. Ständiges Weiterentwickeln der eigenen Sicherheitstechnik sorgt dafür, dass auch neue Bots erkannt werden können.

Flexibel und sicher auch im Remotezugriff

Für den Zugriff auf Unternehmensanwendungen durch Externe (Partner, Lieferanten), für Cloudanwendungen (SaaS) und wenn die Nutzer einer Anwendung an verschiedenen Standorten arbeiten, bietet Akamai eine sichere Verwaltung des Remotezugriffs an. Die von Akamai eingesetzten Techniken sind sicher, einfach und benutzerfreundlich. Damit stellt sich Akamai seinen Kunden als strategischer Sicherheitspartner zur Seite, der sicheren Zugriff auf Corporate Apps anbietet. Mit den Managed Security Services von Akamai profitieren die Kunden in ihrer täglichen Arbeit von den Sicherheitsmaßnahmen, vom Know-how und den Ressourcen Akamais und minimieren so das Geschäftsrisiko.

Gefahren proaktiv erkennen

Mit der Unterstützung von Akamai können Sicherheitsteams Malware, Ransomware, Phishing und Datenextraktion, die DNS-Schwachstellen ausnutzen, proaktiv erkennen, blockieren und abwehren. Die Enterprise Threat Protection von Akamai bietet Unternehmen Sicherheit, Kontrolle und Transparenz und lässt sich einfach in die bereits vorhandenen Verteidigungsmechanismen integrieren. Mit dem Einblick in mehr als zwei Billionen DNS-Anfragen täglich unterstützt Akamai seine Kunden proaktiv bei der Blockierung von Malware-Downloads oder CnC-Traffic (Command and Control) in ihren Netzwerken und sorgt somit für eine zusätzliche Sicherheitsebene.

DATA& CLOUDSECURITY

by MICRO FOCUS

Untergehen oder Schwimmen:

Wie bewältigt man **Cloud Security?**

Die wachsende Akzeptanz von Cloud-Diensten und die Mobilität von Mitarbeitern mit unternehmenskritischem Wissen haben dazu geführt, dass gezielte Kontrollen zur Sicherung von Datenbeständen zu einer strategischen Notwendigkeit geworden sind – innerhalb und außerhalb der klassischen Unternehmensgrenzen in einer zunehmend hybriden Welt.

Alexander
NEFF
Vice President DACH
Micro Focus GmbH

Das führt zu einer steigenden Nachfrage nach Sicherheits- und Compliance-Lösungen, die sich schnell und problemlos in moderne IT-Umgebungen integrieren lassen und sowohl Altsystemen als auch neuen Technologien gerecht werden. Die marktführenden Sicherheits- und Compliance Lösungen von Micro Focus unterstützen Unternehmen hinsichtlich Riskominimierung in hybriden IT-Landschaften und dabei, sich gegen immer neue und komplexere Bedrohungsszenarien einzurichten. Ein ganzheitlicher, sowie analytisch orientierter Ansatz zur Absicherung Ihrer Identitäten, Anwendungen und Daten ist die Grundlage für eine erfolgreiche Transformation in das digitale Unternehmen der Zukunft.

„Die Flexibilität und Agilität, die Cloud-Lösungen mit sich bringen, sind für Business-Entscheider ein wichtiges Argument. Dieser Schritt in Richtung Digitalisierung zieht eine generelle und kulturelle Veränderung im Umgang mit der IT-Infrastruktur nach sich. Wir helfen Unternehmen auf dieser Reise in Bezug auf Datenschutz und Datensicherheit."
Alexander Neff

Unsere Cyber-Security Lösungen unterstützen Sie bei:

Der Verwaltung von Identitäten

Durch die immer weiter reichende Vernetzung über das Internet hat die Frage von bewusster Anonymität bzw. bewusstem Umgang mit Teilen der eigenen Identität eine neue und zuvor nie gekannte Komplexitätsstufe erreicht. Jeder potenzielle Akteur kann als Entität mit mehreren Identitäten verstanden werden. Sei es eine Person, Maschine, ein System, ein Prozess etc. Je größer ein Unternehmen ist, desto komplexer wird die Aufgabe, Identitäten und Ihre Zugriffsrechte zu verwalten. Regulieren Sie, wer Privilegien erhält, setzen Sie Zugangskontrollen durch und vereinheitlichen Sie die diversen Speicherorte all dieser Identitäten, indem Sie eine einheitliche, zentrale Sicht auf sie schaffen.

Hendrik
HAAS
Director Security
Business Germany
Micro Focus GmbH

Der Absicherung von Anwendungen

Der Einsatz agiler Methoden, kombiniert mit bewährten Sicherheitsmethoden im Softwareentwicklungsprozess bietet mehr Flexibilität und die Möglichkeit schneller Anpassung an neue Anforderungen. Codeentwicklung und -ausführung sollten eng miteinander verzahnt sein, damit Fehler zeitnah gefunden und behoben werden können. Auf diese Art entwickeln Sie nicht nur Applikationen höherer Qualität, sondern gestalten auch die Gesamtkostenbetrachtung Ihrer Anwendung über den gesamten Lebenszyklus positiv zu Ihren Gunsten.

„Unternehmen halten zunehmend auch ihre sensiblen Daten in der Public Cloud vor, ohne jedoch eine umfassende Sicherheitsstrategie für Daten in Cloud Umgebungen implementiert zu haben."
Hendrik Haas

DATA&CLOUDSECURITY

by MICRO FOCUS

Sicher in **die Cloud**

Wer Cloud-Dienste nutzen möchte, sollte sich der damit verbundenen Gefahren und Risiken bewusst sein. Da sich in einer Public Cloud oder in einer Hybrid Cloud die Daten außerhalb des klassischen, bekannten und gewohnten Einflussbereichs des Dateneigentümers befinden, nimmt der Schutz der Daten in der Cloud eine entscheidende Rolle ein. Oft ist der Datenschutz nicht mit den üblichen Mitteln zu realisieren, wie sie in eigenen, selbst betriebenen Infrastrukturen zum Einsatz kommen.

Datenschutz **und Datensicherheit**

Aufgrund von gesetzlichen Bestimmungen kann es zum Beispiel erforderlich sein, dass Daten sicher gelöscht werden. In einer Cloud-Umgebung besteht unter Umständen das Risiko, dass Daten unzureichend oder unvollständig gelöscht sind. Da sich die Speicherorte der Daten für den Dateneigentümer nicht lokalisieren lassen, ist die Löschung der Daten für ihn nicht vollständig nachvollziehbar. Nicht nur nach Kündigung eines Cloud-Services muss der Kunde darauf vertrauen, dass beim Cloud Provider funktionierende Prozesse und durchdachte Strategien zum Einsatz kommen, zum Beispiel bei der nachhaltigen Löschung von Daten. Des Weiteren bringt die Nutzung der Cloud-Services durch verschiedene Mandanten das Risiko mit sich, dass eine mangelnde Trennung von Kundeninstanzen Unbefugten das Einsehen oder Manipulieren der Daten Dritter ermöglicht. Ursache hierfür ist, dass in der Cloud meist keine physikalische, sondern eine virtuelle Trennung der Instanzen erfolgt.

Die Cloud Security beinhaltet sowohl technische als auch prozessuale Maßnahmen kombiniert mit vertraglichen Regelungen. Die technischen Maßnahmen umfassen die Sicherung und Verschlüsselung der Kommunikationsverbindungen, die geschützte und verschlüsselte Speicherung der Daten, die Sicherung der Cloud-Komponenten, die Authentifizierung von Usern und Administratoren und das Monitoring für das frühzeitige Erkennen von sicherheitsrelevanten Vorfällen oder Störungen.

Das **Herzstück**

Das Herzstück der Micro Focus Cloud Security Lösung stellt die Kombination von Datenverschlüsselung und einer starken Authentifikation darein umfassender und lückenloser Schutz Ihrer Daten auch in der Cloud.

Micro Focus®

Micro Focus gehört zu den zehn größten Software Unternehmen weltweit. Unsere Software bietet Ihnen die entscheidenden Werkzeuge, die Sie benötigen, um Ihr Unternehmen in einer sich ständig verändernden Welt weiter zu entwickeln, zu betreiben, zu sichern und zu analysieren. Dies bedeutet, Ihre digitale Transformation mit Lösungen zu unterstützen, die sich über vier Schlüsselbereiche erstrecken:

- **Enterprise DevOps -** Erstellen und liefern Sie bessere Software schneller.
- **Hybrid IT Management** - Betreiben Sie Ihre IT mit Agilität.
- **Security, Risk & Governance** - Schützen Sie das, was am wichtigsten ist.
- **Predictive Analytics** - Analysieren Sie Daten rechtzeitig, um schnell handeln zu können.

Micro Focus Lösungen schließen die Lücke zwischen bestehenden und neuen Technologiewelten - das bedeutet, dass Sie im Wettlauf um die digitale Transformation schneller und risikoärmer innovieren können.

Micro Focus GmbH Herrenberger Straße 140 71034 Böblingen

microfocus.com

MICRO FOCUS

Managed Cloud mit dem Plus an Security

Managed Cloud bedeutet für uns, dass wir Ihnen nicht nur die reine Infrastruktur zur Verfügung stellen. Wir möchten, dass Ihre geschäftskritischen Prozesse jederzeit mit hoher Performance verfügbar und Ihre wertvollen Daten stets gut geschützt sind. Daher berücksichtigt unser Sicherheitskonzept sowohl unsere internen Kontrollen und Verfahren als auch sämtliche Security-Services für unsere Kunden.

Diese **Cybersecurity-Services** bieten wir Ihnen:

- Führende Akamai DDoS-Mitigation-Lösungen
- Intrusion Detection und Protection (IDS/IPS)
- Zugangssicherung unserer Rechenzentren mittels modernster Maßnahmen
- Firewalls sowie Web Application Firewalls (WAF)
- Eigene Cybersecurity-Expertise im Unternehmen nicht erforderlich
- Individuelle Beratung und Sicherheitskonzept durch eigenes IT-Security-Team

Zu den Managed-Cloud-Services von PlusServer gehören Private- und Public-Cloud-Lösungen in unseren eigenen Rechenzentren in Deutschland sowie Lösungen bei unseren Public-Cloud-Partnern AWS, Azure und Google Cloud.

Security in der PlusServer-Cloud

Technische Störungen, Stromausfälle, Naturkatastrophen oder sogar Anschläge können die Verfügbarkeit Ihrer Daten gefährden. Wir garantieren Ihnen jedoch in unserem Service Level Agreement eine Verfügbarkeit unserer Rechenzentren sowie des Core-Netzwerks von 99,99 Prozent im Jahresmittel.

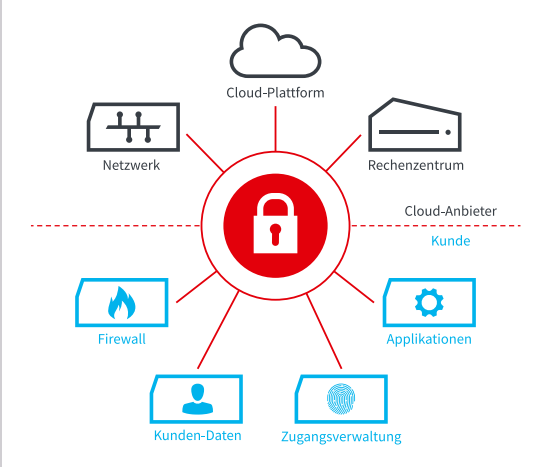
Unabhängige Institutionen haben die Sicherheit unserer Infrastruktur geprüft und bestätigt. Dazu gehört das Bundesamt für Sicherheit in der Informationstechnik, dessen IT-Grundschutz mit seinen Empfehlungen von Standard-Sicherheitsmaßnahmen einen Quasi-Standard für IT-Sicherheit darstellt.

„Wir unterstützen unsere Kunden ganzheitlich auf ihrem Weg in die Cloud. Dazu gehört natürlich auch auf Wunsch die Erstellung eines Sicherheitskonzepts sowie die Implementierung, das Monitoring und unser 24/7 Support."

Patric Czech
Head of Product Management

SECURITY IN DER PUBLIC CLOUD

In der Public Cloud gilt das Prinzip der geteilten Verantwortung (Shared Responsibility). Danach übernimmt der Public-Cloud-Anbieter die Verantwortung für die allgemeine Sicherheit der Infrastruktur – also der Rechenzentren, der Cloud-Plattform und der Netzwerkinfrastruktur. Doch auf der individuellen Cloud-Ebene ist der Kunde selbst bzw. der Cloud-Administrator für weitere Sicherheitsmaßnahmen zuständig. Der Public-Cloud-Anbieter liefert für deren Umsetzung zwar eine umfangreiche Auswahl an einzelnen „Security-Bausteinen". Doch die individuelle Zusammenstellung und Verwaltung dieser Bausteine obliegt dem Kunden selbst.



Möchten Sie beispielsweise Ihre sensiblen Kundendaten verschlüsselt übertragen und speichern, so ist der Cloud-Administrator auf Kundenseite für die Umsetzung der entsprechenden Maßnahmen zuständig. Gleiches gilt für das Aufsetzen von Software-Firewalls, Maßnahmen für Identifikations- und Zugangsverwaltung oder die Compliance-Überwachung.
Die wenigsten Unternehmen verfügen jedoch über das technische Know-how im eigenen Haus, um diese vielfältigen Anpassungen vornehmen zu können. Deshalb unterstützen wir Sie gerne im Bereich der Public Cloud Security.

Ein spezielles Redundanzkonzept, das auch eine Georedundanz zwischen unseren Rechenzentren in Köln und Düsseldorf umfasst, sorgt dafür, dass Ihre Businessprozesse nicht unterbrochen werden.

- Business-Continuity-Lösungen stellen den Betrieb auch im Ausnahmefall sicher (Georedundanz, Disaster Recovery)
- Mehrfach redundante Infrastruktur
- Redundante Anbindung
- 24/7-Überwachung aller Funktionen im Rechenzentrum
- Notstromversorgung inkl. USV-Anlagen und Dieselgeneratoren

Security Response Team: Unser dediziertes Team für Ihr Plus an Sicherheit

Mit unserem Security Response Team (SRT) eröffnen wir unseren Kunden umfassende Security-Leistungen, die über eine reine Netzwerk- und Security-Administration hinausgehen. Das SRT von PlusServer arbeitet mit einem Security Incident and Event Management (SIEM), das Verbindungen zwischen Logfiles verschiedener Systeme herstellt. So lassen sich mögliche Unregelmäßigkeiten im Betrieb aufdecken. Hinzu kommen weitere Informationsquellen über Schwachstellen bzw. Verwundbarkeiten in Systemen, aufkommende E-Mail-Attacken, Phishingszenarien oder DDoS-Angriffe, die innerhalb des SRT beobachtet und ausgewertet werden.

Zu den Services des SRT gehören:

- Frühzeitige Benachrichtigung bei Verwundbarkeiten (Vulnerabilities) in eingesetzten Softwareprodukten
- Logfileanalysen und Benachrichtigung bei Sicherheitsproblemen (via SIEM)
- Eingreifen bei laufenden Angriffen
- Sicherheitsscans und -beratung

plusserver

PlusServer GmbH
Hohenzollernring 72
50672 Köln
Telefon: +49 2203 1045 3500
E-Mail: beratung@plusserver.com
www.plusserver.com

NTT Security

SECURING YOUR DIGITAL TRANSFORMATION

NTT Security ist das auf Sicherheit spezialisierte Unternehmen und „Security Center of Excellence" der NTT Group. Mit „Embedded Security" bietet NTT Security Kunden zuverlässige Lösungen für ihre Anforderungen in der digitalen Transformation und sichert eine effiziente Ressourcennutzung, indem Kunden der richtige Mix an ganzheitlichen Managed Security Services, Security Consulting Services und Security-Technologie zur Verfügung gestellt wird – unter optimaler Kombination von lokalen und globalen Ressourcen. NTT Security ist Teil der NTT Group (Nippon Telegraph and Telephone Corporation), einem der größten IKT-Unternehmen weltweit.

DIE SICHERHEITS-EXPERTISE VON NTT SECURITY

- 1.500 Sicherheitsexperten weltweit, davon mehr als 250 allein in der DACH-Region
- Betrieb von zehn globalen SOCs (Security Operations Center) und sieben Forschungs- und Entwicklungszentren weltweit
- Mehr als 10.000 Kunden
- Fast 170.000 verwaltete, gesicherte und überwachte Endgeräte
- Analyse von jährlich rund 6,1 Billionen Log-Einträgen
- 150 Millionen entdeckte und abgewehrte Attacken pro Jahr

SECURITY-BERATUNG

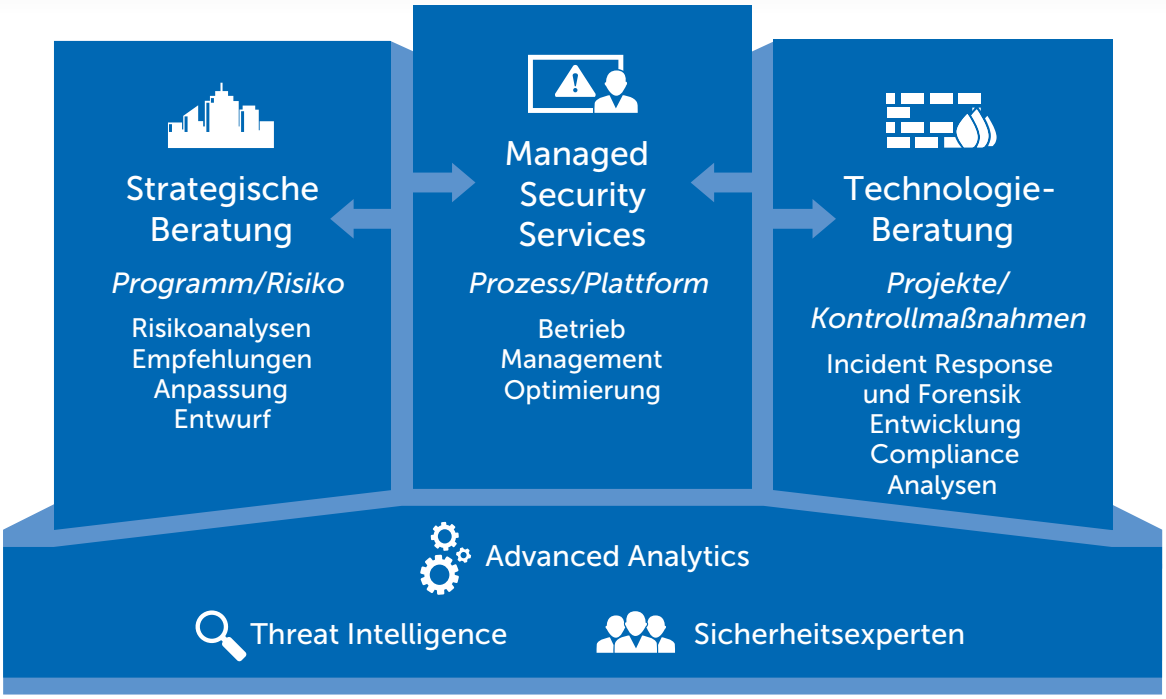
Mit langjährigen Erfahrungen und fundiertem Know-how unterstützen Sie unsere Fachleute bei der Definition und der Vermittlung Ihrer Risiko- und Sicherheitsstrategie. Als Grundlage dienen uns reale Daten, bewährte Frameworks und genaue Kenntnisse über Ihre Branche.

Für NTT Security arbeiten Berater, die früher auf CSO-Ebene in Unternehmen tätig waren und daher genau wissen, was bei der Erstellung eines Sicherheitsprogramms beachtet werden muss, damit das Unternehmen seine Ziele erreichen und das Risiko auf ein annehmbares Maß reduzieren kann.

Sie arbeiten mit Ihnen zusammen, um Ihre Cyber-Sicherheitsarchitektur aufzubauen bzw. zu stärken und die Änderungen einzuleiten, die für die digitale Transformation Ihres Unternehmens notwendig sind.

NTT Security

NTT Security GmbH
Robert-Bürkle-Str. 3, 85737 Ismaning
Telefon: 089 94573 – 0
E-Mail: de.info@nttsecurity.com
Web: www.nttsecurity.com



MANAGED SECURITY

Durch unsere enormen Investitionen in Bedrohungsermittlung, modernste Analyseverfahren und Security-Know-how können wir konsistente, wiederholbare und transparente Prozesse und Plattformen anbieten. Unsere MSS-Plattform erkennt und stoppt auch komplexe Angriffe und liefert gleichzeitig Informationen und Kennzahlen über die Sicherheitslage und aktuelle Trends.

Unsere geschulten und zertifizierten Sicherheitsexperten begleiten Sie durch einen effizienten Change-Management-Prozess für Ihre Netzwerk- und Sicherheitsgeräte, der die einschlägigen Vorschriften erfüllt und die relevanten Best Practices nutzt. In unseren Sicherheitszentren analysieren erfahrene Mitarbeiter Bedrohungen und Vorfälle mit der eigens von NTT Security entwickelten MSS-Plattform oder einem anderen SIEM-System, um Vorfälle zu erfassen, zu analysieren, zu identifizieren und abzuwehren.

TECHNOLOGIE-BERATUNG

Unsere Technologie-Beratung unterstützt Sie bei der Umsetzung von Projekten und der Implementierung von Sicherheitsmaßnahmen, die genau auf die in Ihrem Unternehmen vorhandene Kombination aus Technologie-Infrastruktur, IT-Nutzung und zu schützenden Daten zugeschnitten sind.

Unsere von Herstellern nach Branchenstandards zertifizierten Sicherheitsfachleute wissen genau, wie sich Ihre Infrastruktur und Ihre Investitionen in lokale und cloudgestützte Netzwerke, Plattformen und Kontrollen am besten einsetzen lassen, um Best Practices für die Sicherheit zu befolgen und Ihre Compliance-Ziele zu erreichen. Ob es darum geht, Cyber-Angriffe zu verhindern oder die Auswirkungen eines Vorfalls durch schnelle und effektive Maßnahmen zu minimieren – Ihnen stehen jederzeit die erforderlichen qualifizierten Spezialisten zur Seite.

Das Studienkonzept

Die Multi-Client-Studien von IDG Research Services sind mehr als nur Befragungen von C-Level-Entscheidern und IT-Spezialisten. Hinter den Marktforschungsprojekten steht ein nachhaltiges Studienkonzept, das auf eine Laufzeit von mindestens sechs Monaten ausgelegt ist.

Die Veranstaltung der initialen redaktionellen Round Tables, moderiert von leitenden Redakteuren der COMPUTERWOCHE, steht immer zu Beginn eines jeden Studienprojekts.

Über den Verlauf der Round-Table-Veranstaltungen wird ausführlich berichtet, und die Themen, die den Branchenexperten besonders „auf den Nägeln brennen", werden auch bei der Entwicklung des Studienfragebogens mitberücksichtigt. Die Unternehmen, die das Projekt als Partner begleiten, können eigene Ideen und Fragestellungen einbringen.

Etwa drei Monate nach der methodischen und inhaltlichen Ausgestaltung der Studie liegen die zentralen Ergebnisse in Form eines hochwertigen Survey Reports vor. Die Studienergebnisse werden auf Messen und Events, wie der CEBIT, Hannover Messe oder it-sa, präsentiert, zum Teil in Form von Podiumsdiskussionen, bei denen sich die Studienpartner einem interessierten Fachpublikum stellen können. Oder es wird zu einem Ergebnis-Round-Table ins IDG Conference Center eingeladen.

Begleitet wird das gesamte Studienprojekt durch kontinuierliche Berichterstattung von COMPUTERWOCHE und CIO, zum Thema im Allgemeinen und zur Studie im Speziellen. Fachwissen und Kompetenz unserer Autoren und Redakteure tragen maßgeblich dazu bei, dass die Ergebnisse der Multi-Client-Studien von IDG Research Services richtig eingeordnet werden können. Berichtet und kommentiert wird auf allen modernen Medienkanälen. Infografiken, Bildergalerien und Videointerviews tragen dazu bei, dass die IDG-Studien mittlerweile auf großes Interesse stoßen.

Das Redaktionsteam

Heinrich Vaske:
Chefredakteur

Heinrich Vaske ist Editorial Director von COMPUTERWOCHE und CIO. Seine wichtigste Aufgabe ist die inhaltliche Ausrichtung beider Medienmarken. Vaske verantwortet außerdem inhaltlich die Sonderpublikationen, Social-Web-Engagements und Mobile-Produkte und moderiert Veranstaltungen.

Wolfgang Herrmann:
Deputy Editorial Director

Wolfgang Herrmann ist Deputy Editorial Director der IDG-Publikationen COMPUTERWOCHE und CIO. Zu seinen thematischen Schwerpunkten gehören Cloud Computing, Big Data / Analytics und Digitale Transformation.

Manfred Bremmer:
Redakteur

Manfred Bremmer beschäftigt sich mit Mobile Computing und Communications. Er nimmt mobile Lösungen, Betriebssysteme, Apps und Endgeräte unter die Lupe und überprüft sie auf ihre Business-Tauglichkeit.

Alexandra Mesmer:
Redakteurin

Seit 18 Jahren ist „Karriere in der IT" ihr Leib- und Magenthema. Langweilig? Nein, sie entdeckt immer wieder neue Facetten in der IT-Arbeitswelt. Sie recherchiert, schreibt und moderiert.

Martin Bayer:
Stellvertretender Chefredakteur

Spezialgebiet Business-Software: Business Intelligence, Big Data, CRM, ECM und ERP; Betreuung von News und Titelstrecken in der Print-Ausgabe der COMPUTERWOCHE.

Jürgen Hill:
Teamleiter Technologie

Jürgen Hill ist Teamleiter Technologie. Thematisch ist der studierte Diplom-Journalist und Informatiker im Bereich Communications mit all seinen Facetten zu Hause.

Hans Königes:
Ressortleiter

Hans Königes ist Ressortleiter Jobs & Karriere und damit zuständig für alle Themen rund um Arbeitsmarkt, Jobs, Berufe, Gehälter, Personalmanagement, Recruiting sowie Social Media im Berufsleben.

Karen Funk:
Redakteurin

Ihre Schwerpunkte sind IT-Arbeitsmarkt, Recruiting, Freiberufler, Aus- und Weiterbildung, IT-Gehälter, Work-Life-Balance u. Ä. Wenn sie nicht gerade Projekte wie den „CIO des Jahres" betreut.

Der Autor dieser Studie

Oliver Schonschek
Oliver Schonschek ist freier Analyst und Fachjournalist und schreibt für führende Fachmedien über IT, Sicherheit und Datenschutz, darunter COMPUTERWOCHE und CIO. Er ist Herausgeber und Autor mehrerer Fachbücher und wurde in den USA mehrfach als Influencer und Media Leader für Technologien wie Blockchain, KI, VR / AR und Mobile Computing ausgezeichnet.

Unser Autorenteam

Alexander Jake Freimark
Alexander Jake Freimark wechselte 2009 von der Redaktion der COMPUTERWOCHE in die Freiberuflichkeit. Er schreibt für Medien und Unternehmen, sein Auftragsschwerpunkt liegt im Corporate Publishing. Dabei stehen technologische Innovationen im Fokus, aber auch der Wandel von Organisationen, Märkten und Menschen.

Christoph Lixenfeld
Christoph Lixenfeld schreibt seit 25 Jahren als Journalist und Autor für die Süddeutsche Zeitung, den Spiegel, Focus, den Tagesspiegel, das Handelsblatt, die Wirtschaftswoche, COMPUTERWOCHE und viele andere. Außerdem macht er Hörfunk, vor allem für DeutschlandRadio, und produziert TV-Beiträge, zum Beispiel für die ARD-Magazine Panorama und Plusminus. Inhaltlich geht es häufig um die Themen Wirtschaft und IT, aber nicht nur.

Jürgen Mauerer
Jürgen Mauerer arbeitet seit Oktober 2002 als freiberuflicher IT-Fachjournalist in München. Er schreibt vorwiegend über aktuelle Themen und Trends rund um IT und Wirtschaft für Publikationen wie COMPUTERWOCHE, com! professional oder ZD.NET. Darüber hinaus berät und unterstützt er PR-Agenturen sowie IT-Unternehmen bei der Erstellung von Anwenderberichten, Whitepapers, Fachartikeln oder Microsites und moderiert Podiumsdiskussionen und Veranstaltungen.

Bernd Reder
Bernd Reder ist seit rund 30 Jahren als Fachjournalist für Medien, PR-Agenturen und Unternehmen tätig. Zu seinen thematischen Schwerpunkten zählen die Informations- und Netzwerktechnik, Cloud Computing, IT-Security und Mobility. Bevor er sich selbstständig machte, war Reder in den Redaktionen führender Fachpublikationen tätig. Dazu zählen Elektronik, Network World, Digital World und Network Computing.

Michael Schweizer
Michael Schweizer ist freier Redakteur und Autor in München. Oft schreibt er über Menschen, Personal- und Karrierefragen mit IT-Bezug. Besonders interessiert ihn alles, was mit Wissenschaft zu tun hat, also zum Beispiel unabhängige Studien zu komplizierten Themen. Als freier Schlussredakteur ist er unter anderem für die Print-Ausgaben der IDG-Publikationen COMPUTERWOCHE, CIO und ChannelPartner zuständig. Er übernimmt auch Buchlektorate.

Sales-Team

Nicole Bruder
Account Manager Research
IDG Research Services
Telefon: 089 36086 – 137
nbruder@idg.de

Regina Hermann
Account Manager Research
IDG Research Services
Telefon: 089 36086 –384
rhermann@idgbusiness.de

Jessica Schmitz-Nellen
Account Manager Research
IDG Research Services
Telefon: 089 36086 – 745
jschmitz-nellen@idg.de

Projektmanagement

Simon Hülsbömer
Senior Project Manager
IDG Research Services
Telefon: 089 36086 – 177
shuelsboemer@idg.de

Thamar Thomas-Ißbrücker
Project Manager
IDG Research Services
Telefon: 089 36086 – 138
tthomas-issbruecker@idg.de

Armin Rozsa
Junior Project Manager
IDG Research Services
Telefon: 089 36086 – 184
arozsa@idg.de

Gesamtstudienleitung

Matthias Teichmann
Director Research
IDG Research Services
Telefon: 089 36086 – 131
mteichmann@idgbusiness.de

Unsere Studienreihe

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

Laufende Studienberichterstattung auf
computerwoche.de/p/research,3557

Vorschau Studienreihe

Oktober 2018 bis März 2019
IT-Freiberufler

November 2018 bis April 2019
Cloud Security

Dezember 2018 bis April 2019
Machine Learning / Deep Learning

Januar bis Mai 2019
Managed Services

Februar bis Mai 2019
Process Mining & Process Automation

März bis Juni 2019
Data Analytics & Data Protection

April bis September 2019
Digital Customer Experience

Mai bis September 2019
Augmented & Virtual Reality

Juni bis Oktober 2019
Endpoint Security Management

Juli bis November 2019
Internet of Things

September bis Dezember 2019
IT Service Management

September 2019 bis Januar 2020
Cloud Native

Oktober 2019 bis März 2020
DevOps

Oktober 2019 bis März 2020
IT-Freiberufler

November 2019 bis März 2020
Data Management / Data Quality

Dezember 2019 bis April 2020
Robotics

Die Studienprojekte beginnen mit initialen redaktionellen Round Tables jeweils rund drei bis vier Monate vor den angegebenen Veröffentlichungsterminen.

(Planungsstand 15.02.2019, Änderungen vorbehalten)

Für Rückfragen zum aktuellen Planungsstand: research@idg.de

Für regelmäßige Infos folgen Sie uns gerne auf Twitter: https://twitter.com/IDGResearch_DE

Herausgeber:

IDG Business Media GmbH

Anschrift
Lyonel-Feininger-Str. 26
80807 München
Telefon: 089 36086 – 0
Fax: 089 36086 – 118
E-Mail: info@idg.de

Vertretungsberechtigter
York von Heimburg
Geschäftsführer

Registergericht
Amtsgericht München
HRB 99187

Umsatzsteueridentifikations-
nummer: DE 811 257 800

Weitere Informationen unter:
www.idg.de

Platin-Partner:

Cisco Systems GmbH
Parkring 20
85748 Garching
Tel.: +49 89 51 65 71 000
Web: www.cisco.com

Gold-Partner:

Akamai Technologies GmbH
Parkring 20-22
85748 Garching bei München
Tel.: +49 89 94006308
Web: www.akamai.com/de

Micro Focus GmbH
Herrenberger Str. 140
71034 Böblingen
Tel.: +49 69 66308025
Web: www.microfocus.com/de

PlusServer GmbH
Hohenzollernring 72
50672 Köln
Tel.: +49 2203 1045 3500
E-Mail: beratung@plusserver.com
Web: www.plusserver.com

Silber-Partner:

NTT Security GmbH
Robert-Bürkle-Str. 3
85737 Ismaning
Tel.: +49 89 94573-0
E-Mail: de.info@nttsecurity.com
Web: www.nttcomsecurity.com

Bronze-Partner:

genua GmbH
Domagkstr. 7
85551 Kirchheim bei München
Tel.: +49 89 991950-0
E-Mail: info@genua.de
Web: www.genua.de

SecurEnvoy GmbH
Freibadstr. 30
81543 München
Tel.: +49 89 44 47 92 00
E-Mail: info@SecurEnvoy.com
Web: www.securenvoy.com

Studienkonzept / Fragebogenentwicklung
Simon Hülsbömer,
IDG Research Services

Endredaktion / CvD Studienberichtsband:
Simon Hülsbömer,
IDG Research Services

Analysen / Kommentierungen:
Oliver Schonschek,
Bad Ems

Umfrageprogrammierung und Ergebnisauswertungen:
Thamar Thomas-Ißbrücker,
IDG Research Services

Hosting / Koordination Feldarbeit:
Armin Rozsa,
IDG Research Services

Artdirector:
Daniela Petrini, Reutte

Umschlagkonzept:
Simon Hülsbömer,
IDG Research Services
(unter Verwendung eines Farbfotos für Vorder- und Rückseite von © Blackboard - shutterstock.com)

Grafik:
Jutta Weber-Vidal, Würzburg
www.erdenbuerger.de

Lektorat:
Dr. Renate Oettinger,
München

Druck:
Peradruck GmbH
Hofmannstr. 7b
81379 München

Ansprechpartner:
Matthias Teichmann
Director Research
IDG Research Services
Telefon: 089 36086 – 131
mteichmann@idgbusiness.de

Hintergrundbild © Blackboard - shutterstock.com

PLATIN-PARTNER

GOLD-PARTNER

SILBER-PARTNER

BRONZE-PARTNER