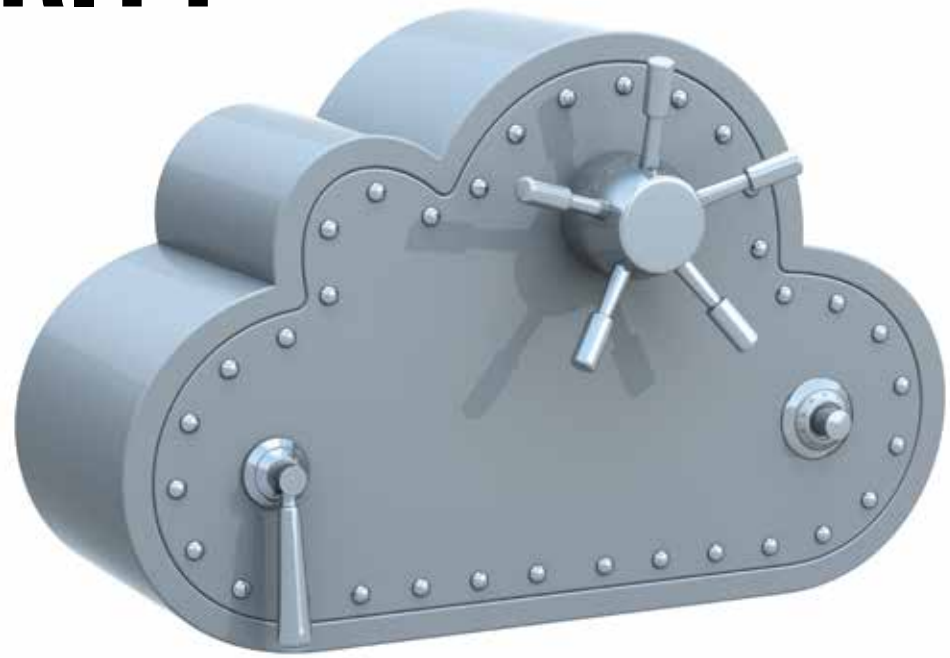
VON IDG COMPUTERWOCHE VOICE OF DIGITAL

CIO

STUDIE CLOUD SECURITY 2021



plusserver

arvato BERTELSMANN Arvato Systems

AIRLOCK® SECURE ACCESS HUB

TÜV SÜD

uniscon SEALED CLOUD TECHNOLOGIES

A member of TÜV SÜD

Ein aktuelles Studienprojekt von

IDG
RESEARCH SERVICES

Gold-Partner

plusserver

Silber-Partner

arvato
BERTELSMANN
Arvato Systems

AIRLOCK®
SECURE ACCESS HUB

TÜV SÜD

uniscon
SEALED CLOUD TECHNOLOGIES
A member of TÜV SÜD

Lassen Sie die Profis ran

Simon Hülsbömer,
Senior Project Manager

Mehr als jedes zweite Unternehmen plant für Cloud-Sicherheit kein eigenes beziehungsweise zusätzliches Budget. Das ist durchaus verwunderlich, wo doch der überwiegende Teil der Unternehmen Cloud-Dienste nutzt, zumindest im Private-Cloud-Modell. Und wobei viele von ihnen bereits Cyberangriffe auf diese Services erlitten haben, die mehr oder weniger schlimme Folgen nach sich zogen.

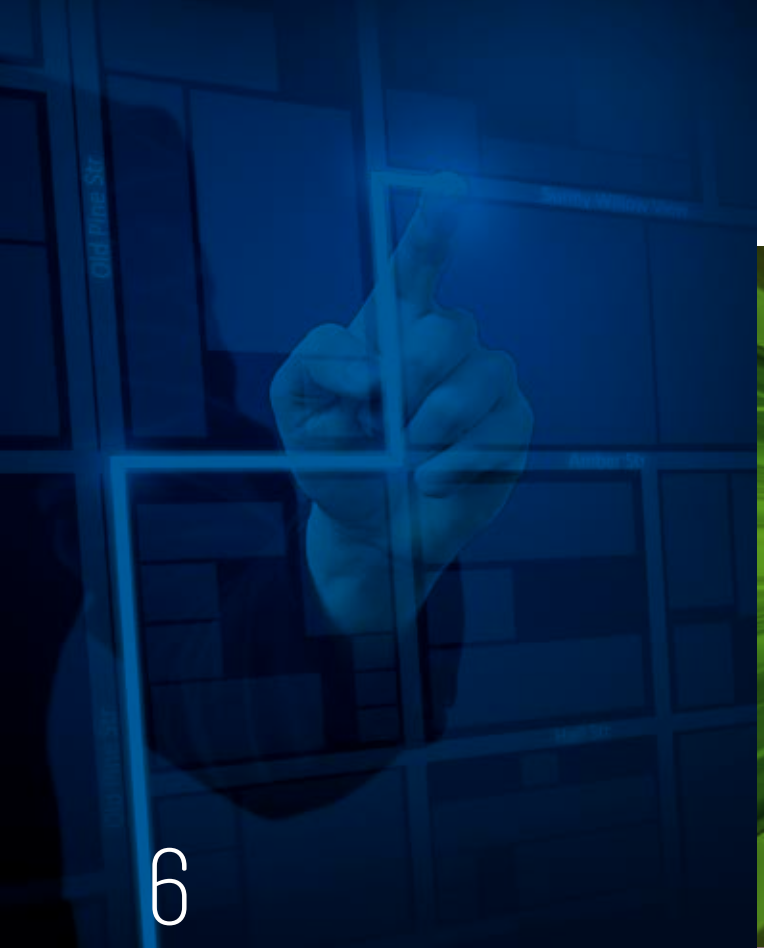
Das herrschende Motto lautet: „Der Cloud Provider wird es schon richten, ohne dass ich extra dafür zahle." Es ist zwar richtig, dass der Service Provider ein wichtiger Partner für die Cloud Security ist – aber um alles kann und wird er sich nicht kümmern. Dafür braucht es zusätzliche sichere und sichernde Lösungen von Drittanbietern – sei es für den Datentransfer in, aus und innerhalb der Cloud, oder für die Klassifizierung von Cloud-Daten und deren Schutzbedarfen. Oder für weitere Backups, wenn einmal wieder ein Cloud-Rechenzentrum samt Backup-Servern in Flammen stehen sollte (wie unlängst in Straßburg geschehen).

Cloud Security ist komplex, in ihrer Gänze manchmal gar etwas intransparent. Das sollte aber nicht als Entschuldigung dienen, das Thema komplett in die Hände eines einzigen (womöglich nicht Security-affinen) Dienstleisters zu legen. Es wäre ratsamer, zum einen auf die ergänzende Expertise von Spezialisten zu setzen. Zum anderen schadet es bestimmt nicht, darüber hinaus internes Spezial-Know-how einzubringen, um der Cloud Security das Gewicht und Gesicht zu geben, das sie benötigt.

Sollten Sie bereits Security-Experten in Ihrem Unternehmen haben: Trauen Sie ihnen mehr zu, geben Sie ihnen mehr Verantwortung, beziehen Sie sie früher ein. Noch wird viel zu wenig auf die schon im Unternehmen vorhandenen Spezialisten gesetzt: Gerade strategisch wichtige IT-Entscheidungen fallen meist woanders. Dass es im Kern um Security-bezogene Themen geht, wird dadurch häufig gar nicht oder zumindest viel zu spät erkannt.

Die Cloud ist die technische Grundlage für viele neue, zukunftsträchtige und innovative Geschäftsmodelle – geben wir ihr deshalb auch den Schutz und die Sicherheit, die sie verdient.

Ich wünsche Ihnen eine aufschlussreiche Lektüre.

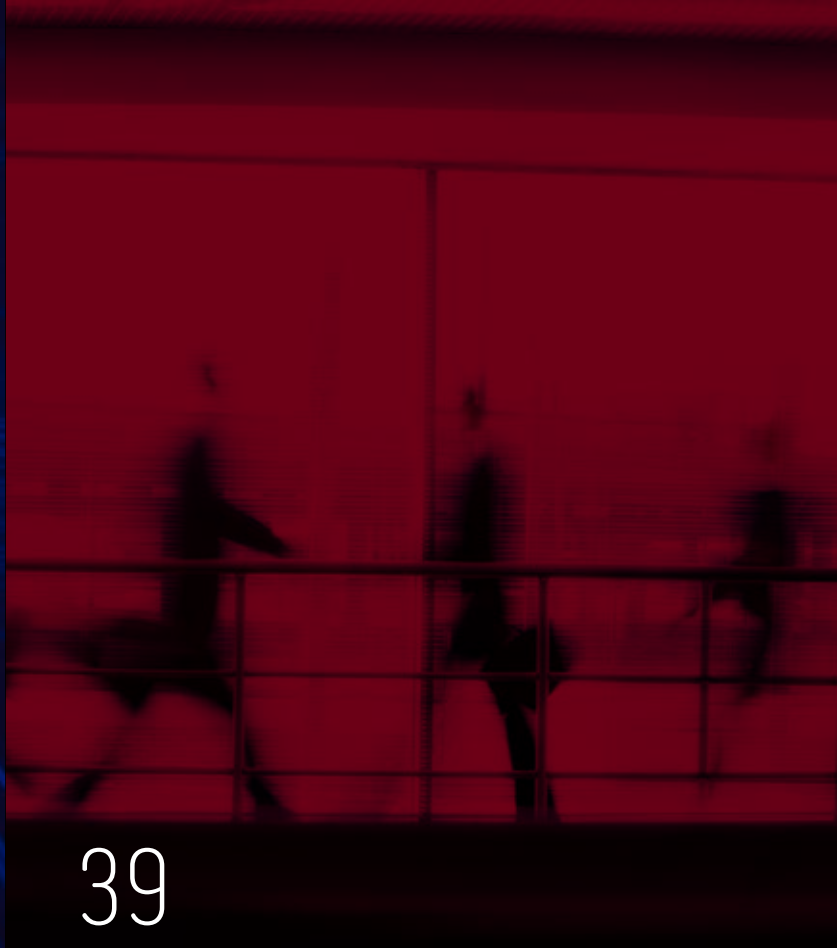


Inhalt

Die wichtigsten Ergebnisse

Weitere Studienergebnisse

Studiendesign



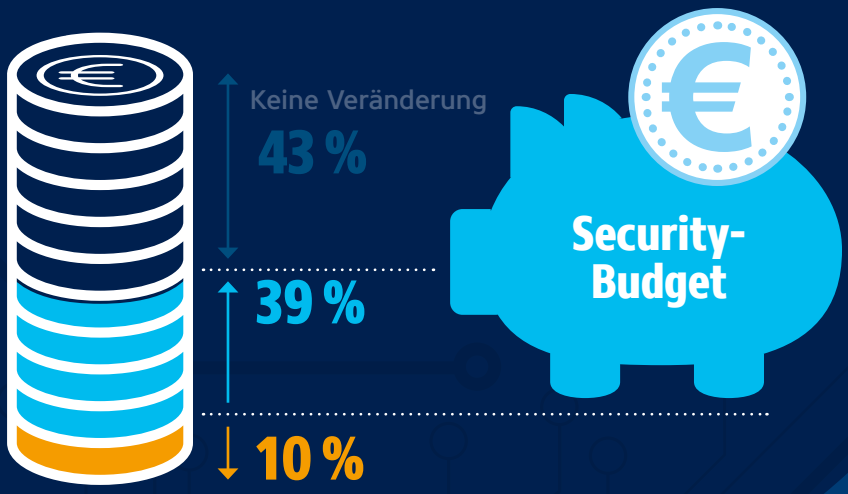
Blick in die Zukunft

CIO-Agenda 2021

Studienpartner stellen sich vor

Die Mehrheit der Unternehmen hat kein zusätzliches Budget für Cloud-Sicherheit

Nur **39 Prozent** erhöhen das Security-Budget, wenn IT-Lösungen von On-Premises in die Cloud übertragen werden. **Zehn Prozent** senken sogar das Security-Budget ab, wenn in die Cloud migriert wird.

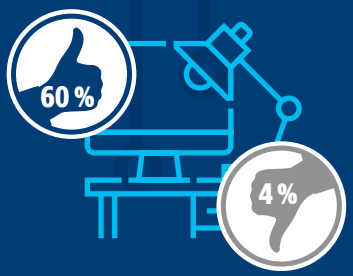


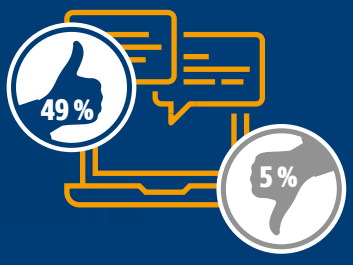
Cloud-Angriffe führen zu Betriebsunterbrechungen

Jedes dritte Unternehmen hat in den letzten zwölf Monaten einen Schaden durch Cloud-Attacken erlitten. Besonders häufig kam es zu Betriebsunterbrechungen und Stillstand im Unternehmen.

Büros gelten als sicherer als Remote-Arbeitsplätze

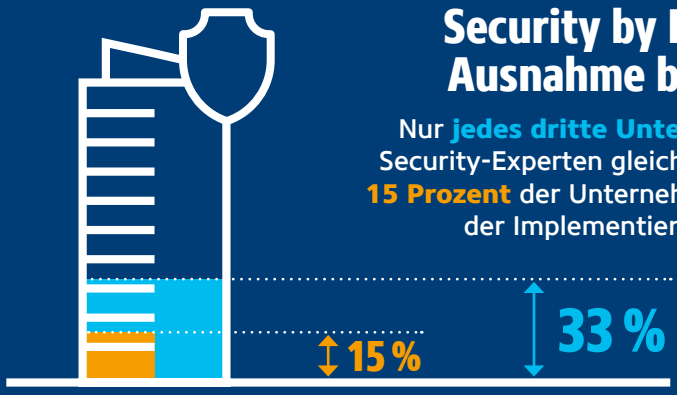
60 Prozent der Unternehmen halten Büroarbeitsplätze für sicher oder sehr sicher, bei Remote-Arbeitsplätzen sinkt diese Einschätzung auf **49 Prozent**. **Fünf Prozent** halten Remote Work für unsicher oder sehr unsicher, bei Büroarbeitsplätzen sind es **vier Prozent**.





Administration bei Clouds wichtiger als Datenschutz

Für **91 Prozent** ist die leichte Administrierbarkeit bei Cloud-Diensten wichtig oder sehr wichtig. Die Konformität der Cloud mit der EU-DSGVO stufen **79 Prozent** entsprechend ein, den Cloud-Standort Deutschland nur **75 Prozent**.



Security by Default ist noch die Ausnahme bei Cloud-Projekten

Nur **jedes dritte Unternehmen** involviert die internen Security-Experten gleich zu Beginn eines Cloud-Projektes. **15 Prozent** der Unternehmen beziehen die Security erst bei der Implementierung der Cloud Services ein.

Verschlüsselung und Policies sollen für Cloud-Sicherheit sorgen

39 Prozent der Unternehmen achten besonders auf die verschlüsselte Datenübertragung vom und zum Cloud Provider, **38 Prozent** auf Cloud Policies für die Nutzung von Cloud-Lösungen und Zugangsgeräten, wenn es um Cloud Security geht.

Cloud Provider gilt als wichtigster Security-Partner

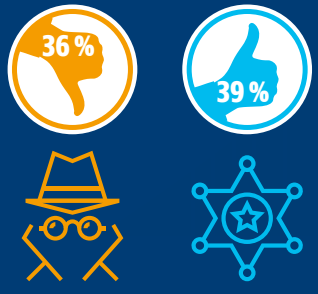
43 Prozent der Unternehmen arbeiten mit ihrem Cloud Provider in Sicherheitsfragen zusammen. Externe SOCs nutzen **34 Prozent** für Maßnahmen der Cloud-Sicherheit, **30 Prozent** setzen auf Managed Security Service Provider (MSSP).

Management Summary

Die Key Findings im Überblick

Datendiebstahl ist größtes Cloud-Risiko, Datenschutz größter Cloud-Vorteil

Für **36 Prozent** der Unternehmen ist Datendiebstahl das größte Sicherheitsrisiko im Cloud Computing, während **39 Prozent** sagen, der höhere Datenschutz ist der größte Vorteil der Cloud im Vergleich zu On-Premises-IT.



Das zentrale Ergebnis

Mehr als die Hälfte der Unternehmen sehen kein zusätzliches Budget für die Cloud-Sicherheit vor

Obwohl spezielle Maßnahmen für die Cloud-Sicherheit ergriffen werden, gibt es bei 43 Prozent der Unternehmen keine Veränderung beim Security-Budget. Zehn Prozent senken das Budget sogar, wenn Anwendungen von On-Premises in die Cloud wandern. Ein erhöhtes Security-Budget bei Cloud-Migrations-Projekten bestätigen nur 39 Prozent.

Kein zusätzliches Budget für Cloud-Sicherheit gibt es insbesondere bei Unternehmen mit 500 bis 999 Beschäftigten. Hier sagen 49 Prozent, dass es keine Veränderung im Security-Budget gibt, 15 Prozent berichten sogar von einer Absenkung. Bei größeren Unternehmen bleibt das Budget bei 44 Prozent unverändert, aber nur sechs Prozent sprechen von einem sinkenden Security-Budget, wenn in die Cloud migriert wird.

Auch die generellen IT-Aufwendungen haben einen Einfluss darauf, ob zusätzliches Budget für die Sicherheit in der Cloud vorgesehen ist. Betragen die jährlichen IT-Aufwendungen unter zehn Millionen Euro, erhöhen 39 Prozent der befragten Unternehmen das Security-Budget für die Cloud. Bei höheren jährlichen IT-Ausgaben steigt dieser Anteil erwartungsgemäß und beträgt dann 46 Prozent. Doch selbst bei höheren IT-Kosten von mindestens zehn Millionen Euro im Jahr erklären elf Prozent, dass sie das Security-Budget bei einer Cloud-Migration absenken.

Da viele Unternehmen Cloud-Lösungen und **→ On-Premises-IT *** parallel und damit hybrides Cloud Computing nutzen, kann man nicht automatisch davon ausgehen, dass die Ausgaben für die On-Premises-Sicherheit sinken, wenn man Anwendungen in die Cloud überführt. Es gibt also nicht unbedingt Ersparnisse in der bisherigen Security, die man für die Cloud-Sicherheit nutzen könnte.

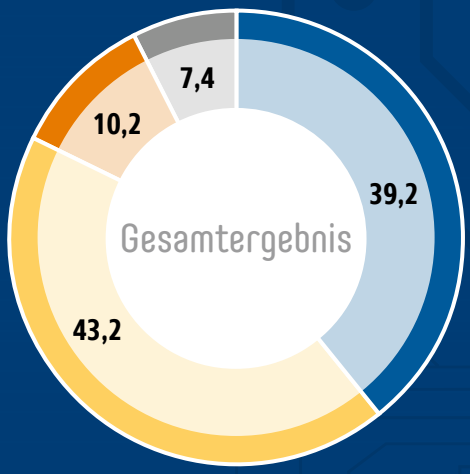
Wenn aber im Durchschnitt 43 Prozent der Unternehmen ihr Security-Budget nicht verändern und zehn Prozent sogar eine Reduzierung vornehmen, stellt sich die Frage, wie die technischen und organisatorischen Maßnahmen, die speziell für die Cloud-Sicherheit umgesetzt werden, finanziert werden. Unternehmen sollten also genau ihr Security-Budget überdenken, damit die Maßnahmen für die Cloud-Sicherheit nicht in der Planung stecken bleiben.

» Es gibt nicht unbedingt Ersparnisse in der bisherigen Security, die man für die Cloud-Sicherheit nutzen könnte. «

*** Mit → markierte Begriffe werden im Glossar (Seite 53) erläutert.**

Welche Auswirkung auf das IT-Security-Budget hat es, wenn in Ihrem Unternehmen eine On-Premises-Lösung durch einen Cloud Service ersetzt wird?

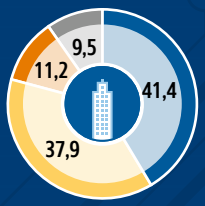
Angaben in Prozent. Basis: n = 352



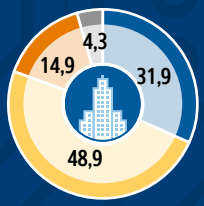
Erhöhung | Keine Veränderung | Absenkung | Weiß nicht

Ergebnis-Splits

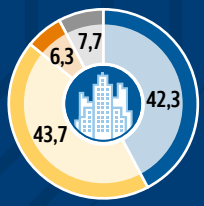
Mitarbeiterzahl



bis 499 Beschäftigte

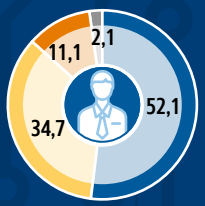


500 bis 999 Beschäftigte

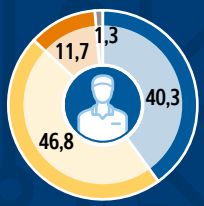


1.000 Beschäftigte und mehr

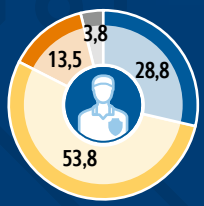
Funktion im Unternehmen



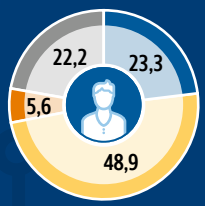
C-Level



IT-Leiter / IT-Bereich

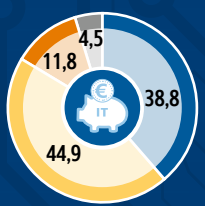


IT-Security

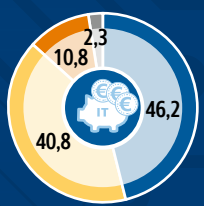


Fachbereiche

Jährliche IT-Aufwendungen



< 10 Mio. Euro



10 Mio. Euro und mehr

Die weiteren Key Findings

Zahlen und Analysen, die aus Sicht des IDG-Marktforschungs-teams besonders wichtig sind

Jedes dritte Unternehmen hat wirtschaftlichen Schaden durch Cloud-Angriffe erlitten

39 Prozent der Unternehmen mit 500 bis 999 Beschäftigten mussten in den letzten zwölf Monaten wirtschaftliche Schäden durch Attacken auf die von ihnen genutzten Cloud-Dienste hinnehmen. Bei Unternehmen mit weniger als 500 oder mindestens 1.000 Beschäftigten waren es immer noch 32 Prozent.

Unternehmen mit jährlichen IT-Aufwendungen von mindestens zehn Millionen Euro wurden besonders stark getroffen: Hier berichten 51 Prozent von einem wirtschaftlichen Schaden durch Cloud-Attacken in den letzten zwölf Monaten, bei geringeren IT-Aufwendungen sinkt der Anteil der betroffenen Unternehmen auf 29 Prozent.

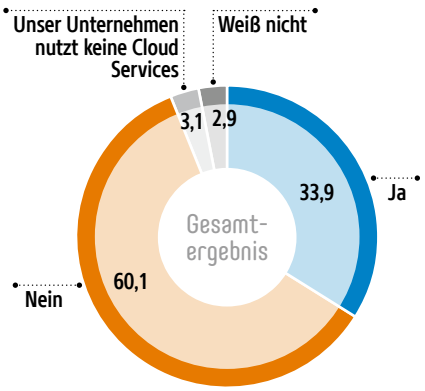
Das Wissen um die wirtschaftlichen Folgeschäden ist abhängig von der Position der Befragten. So gehen in den Fachbereichen nur elf Prozent davon aus, dass es einen wirtschaftlichen Schaden durch Cloud-Attacken gab, in der Geschäftsführung hingegen sind es 50 Prozent. Bemerkenswert ist zudem, dass in der Security-Abteilung immerhin drei Prozent nicht wissen, ob es einen solchen Schaden gab oder nicht.

Auch die Art des Schadens wurde untersucht: Die geschädigten Unternehmen berichten zu 43 Prozent von einer Unterbrechung der Arbeits- und Produktionsprozesse im gesamten Unternehmen oder in einzelnen Abteilungen. 34 Prozent beklagten einen kompletten Stillstand im Unternehmen, 31 Prozent Datenverlust.

Diese Folgeschäden durch Cloud-Attacken unterstreichen, wie wichtig Cloud Computing inzwischen für die Unternehmensabläufe ist – aber auch, wie anfällig die Cloud-Dienste für Attacken noch sind.

Hat Ihr Unternehmen innerhalb der vergangenen zwölf Monate einen wirtschaftlichen Schaden durch eine Cyberattacke auf Cloud Services erlitten?

Angaben in Prozent. Basis: n = 383



Welcher Art war der Schaden genau?

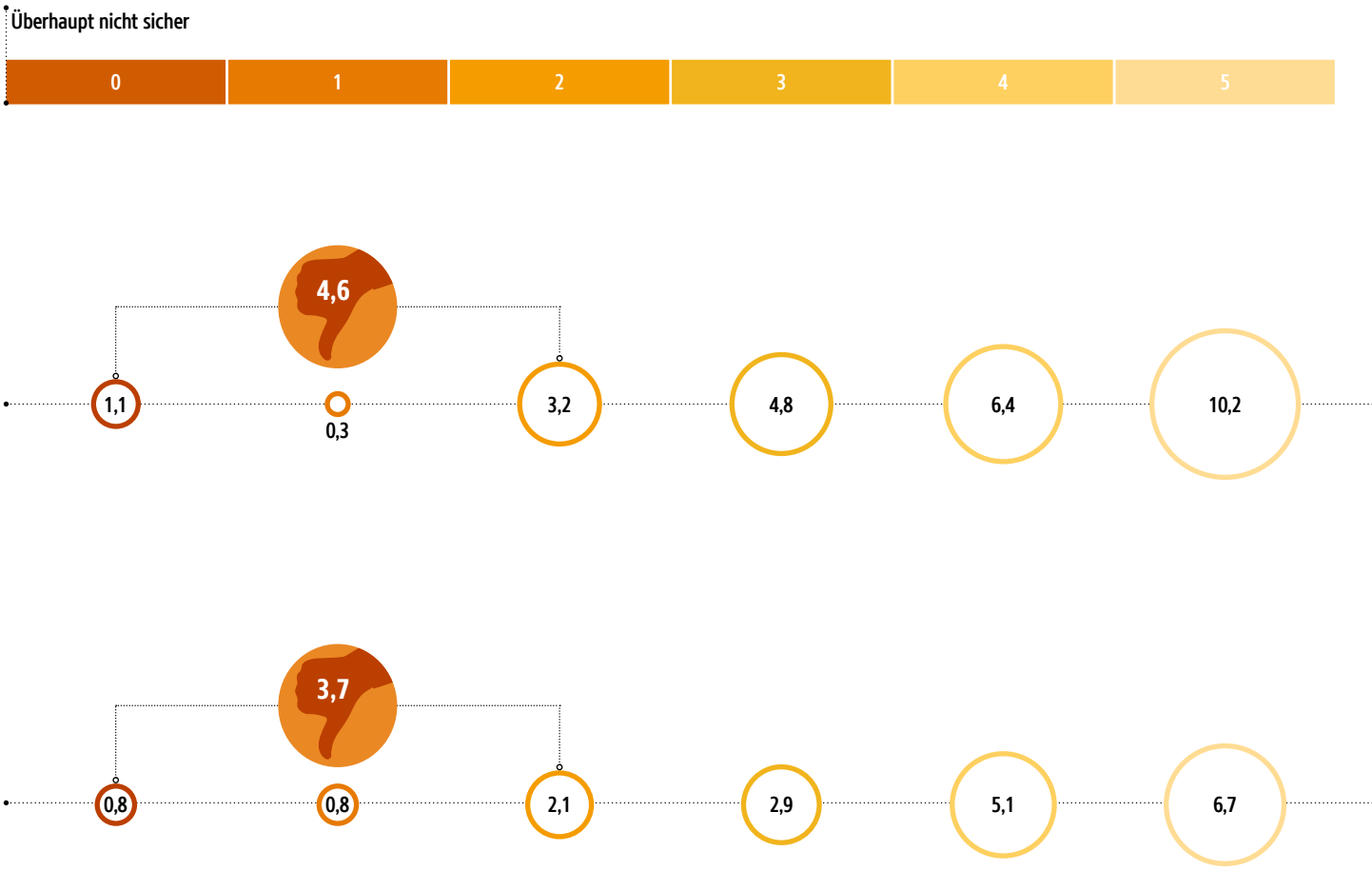
Angaben in Prozent. Mehrfachantworten möglich. Filter: Unternehmen, die innerhalb der vergangenen zwölf Monate einen wirtschaftlichen Schaden durch eine Cyberattacke auf Cloud Services erlitten haben. Basis: n = 130

43,1	Unterbrechung der Arbeits-/Produktionsprozesse (im gesamten Unternehmen oder in einzelnen Abteilungen)
33,8	Kompletter Stillstand des Unternehmens
30,8	Verlust geschäftskritischer Daten
25,4	Umsatzverlust
24,6	Produktivitätsverlust
20,8	Kundenverlust
16,9	Zusätzliche Troubleshooting-Kosten (intern und / oder extern)
13,1	Imageschaden / zusätzliche PR-Kosten
10,8	Regulatorische Kosten / Zahlung von Buß- und / oder Strafgeldern

2

Wie bewerten Sie die Sicherheit der Remote-Arbeitsplätze und der Büro-Arbeitsplätze (d.h. der Nicht-Remote-Arbeitsplätze) Ihres Unternehmens?

Angaben in Prozent. Bewertung des Grades der IT-Security auf einer Skala von 0 (Überhaupt nicht sicher) bis 10 (Vollkommen sicher). Basis: n = 383

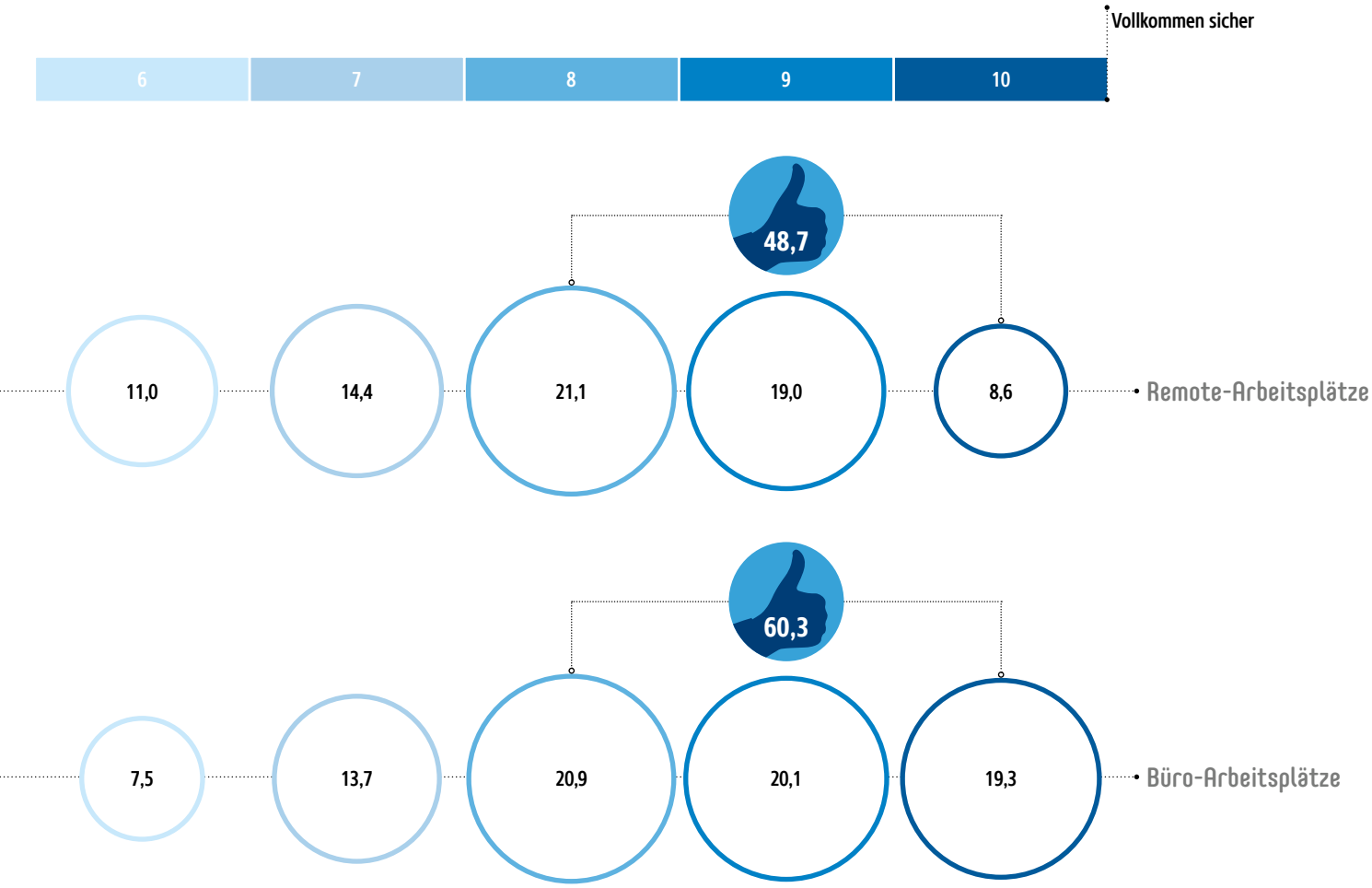


Nur 42 Prozent der Fachbereiche halten Remote Work für (sehr) sicher

Fast die Hälfte der Befragten stufen Remote-Arbeitsplätze als sicher oder sehr sicher ein, bei den „klassischen" Büroarbeitsplätzen liegt dieser Wert noch deutlich höher. Die Fachbereiche sind von der Sicherheit der Remote-Arbeitsplätze deutlich weniger überzeugt als Geschäftsführer oder IT-Security-Verantwortliche.

Die Sicherheit bei Remote-Arbeitsplätzen wird kritischer gesehen als diejenige, die bei Büroarbeitsplätzen angenommen wird. So meinen 49 Prozent der befragten Unternehmen, Arbeitsplätze für Remote Work seien sicher oder sehr sicher. Bei Büroarbeitsplätzen teilen 60 Prozent diese Einschätzung.

Befragte aus Unternehmen mit mehr als 1.000 Beschäftigten jedoch sind zu 56 Prozent der Meinung, Remote Work sei sicher oder sehr sicher. Bei der klassischen Büroarbeit sind es sogar 66 Prozent der Unternehmen mit vielen Beschäftigten, die keine Sicherheitsprobleme sehen.



Interessant ist zudem, dass die befragten Security-Verantwortlichen die Remote-Arbeitsplätze sicherer einschätzen, als es die Fachbereiche tun. Von den Security-Verantwortlichen sagen 52 Prozent, Remote Work ist sicher oder sehr sicher, in den Fachbereichen denken dies dagegen nur 42 Prozent.

Die Beurteilung der Sicherheit bei Büroarbeitsplätzen hingegen weicht bei den Security-Verantwortlichen nicht von dem Unternehmensdurchschnitt von 60 Prozent ab, die die klassische Büroarbeit als sicher oder sehr sicher bezeichnen.

Dies könnte bedeuten, dass das gefühlte Sicherheitsniveau bei der klassischen Büroarbeit inzwischen relativ hoch ist. Bei Remote-Arbeitsplätzen hingegen mangelt es an Erfahrung, sodass die Fachbereiche weniger Sicherheit bei Remote Work wahrnehmen als die Security-Experten im Unternehmen. Hier könnte es ratsam sein, mehr über die Sicherheit im Büro und bei Remote Work aufzuklären. So werden in beiden Fällen oftmals die gleichen Cloud-Dienste (wie Office-Lösungen) genutzt. Die Sicherheitsbewertung hängt also nicht nur mit der Cloud-Nutzung bei Remote Work zusammen.

3

EU-Datenschutz ist als Cloud-Kriterium nicht so wichtig wie leichte Administrierbarkeit

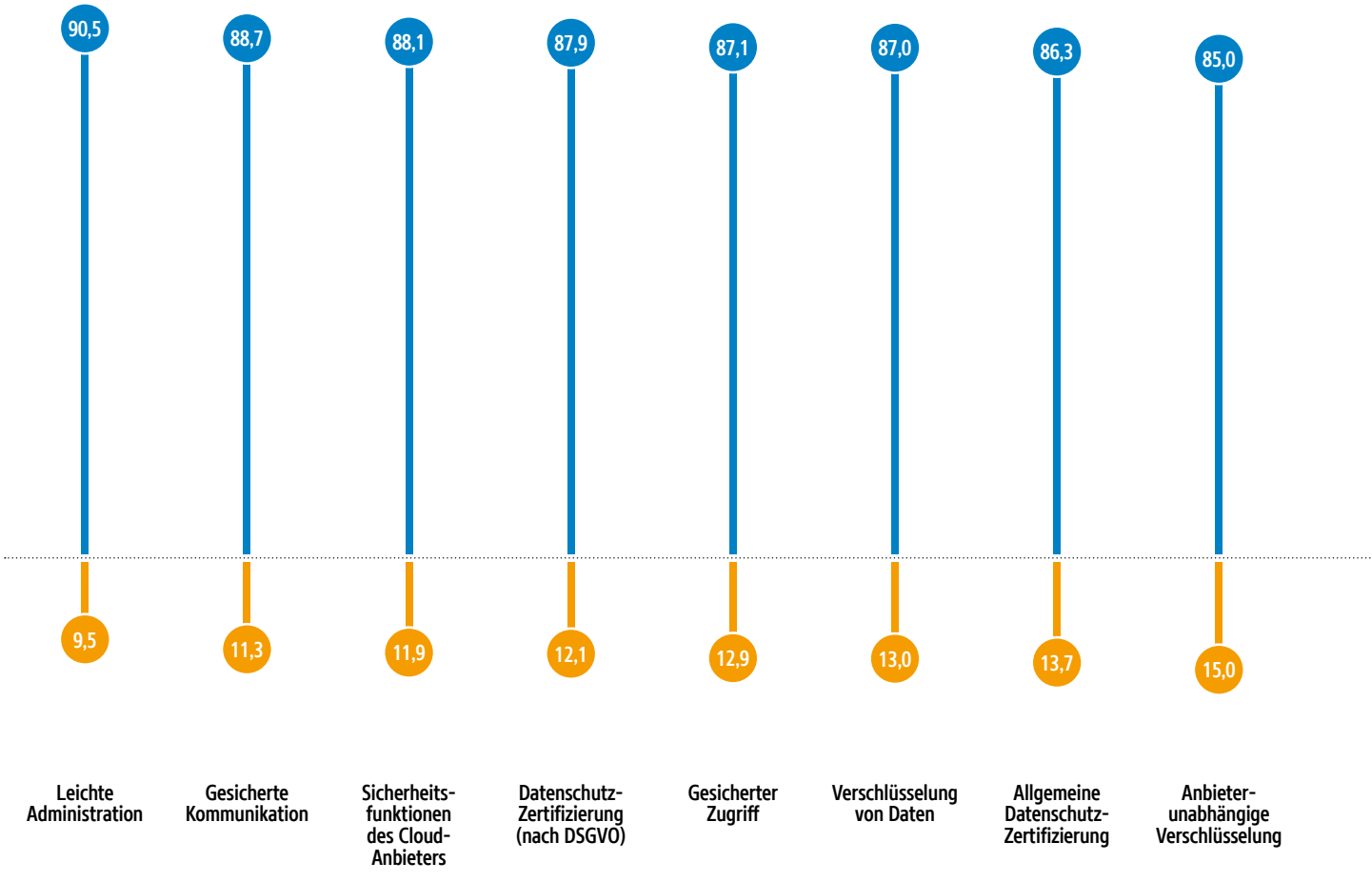
Die wichtigsten Auswahlkriterien bei Cloud-Diensten sind die leichte Administration (91 Prozent der Nennungen), die gesicherte Kommunikation (89 Prozent) und die Sicherheitsfunktionen des Cloud-Anbieters (88 Prozent). Datenschutzkriterien spielen eher eine nachgelagerte Rolle.

Die Bedeutung der leichten Administration beim Cloud-Dienst der Wahl wird eher von den Unternehmen mit mehr Beschäftigten gesehen. In Unternehmen mit weniger als 500 Beschäftigten sagen 88 Prozent, die leichte Cloud-Administration sei ein wichtiges oder sehr wichtiges Auswahlkriterium. Bei 500 bis 999 Beschäftigten sind es sogar 93 Prozent, die dies sagen – ab 1.000 Beschäftigten 91 Prozent.

In den Fachbereichen ist es 93 Prozent der Befragten wichtig, eine einfach zu administrierende Cloud zu haben, die Geschäftsführung hingegen sagt dies nur in 88 Prozent der Fälle. Offensichtlich

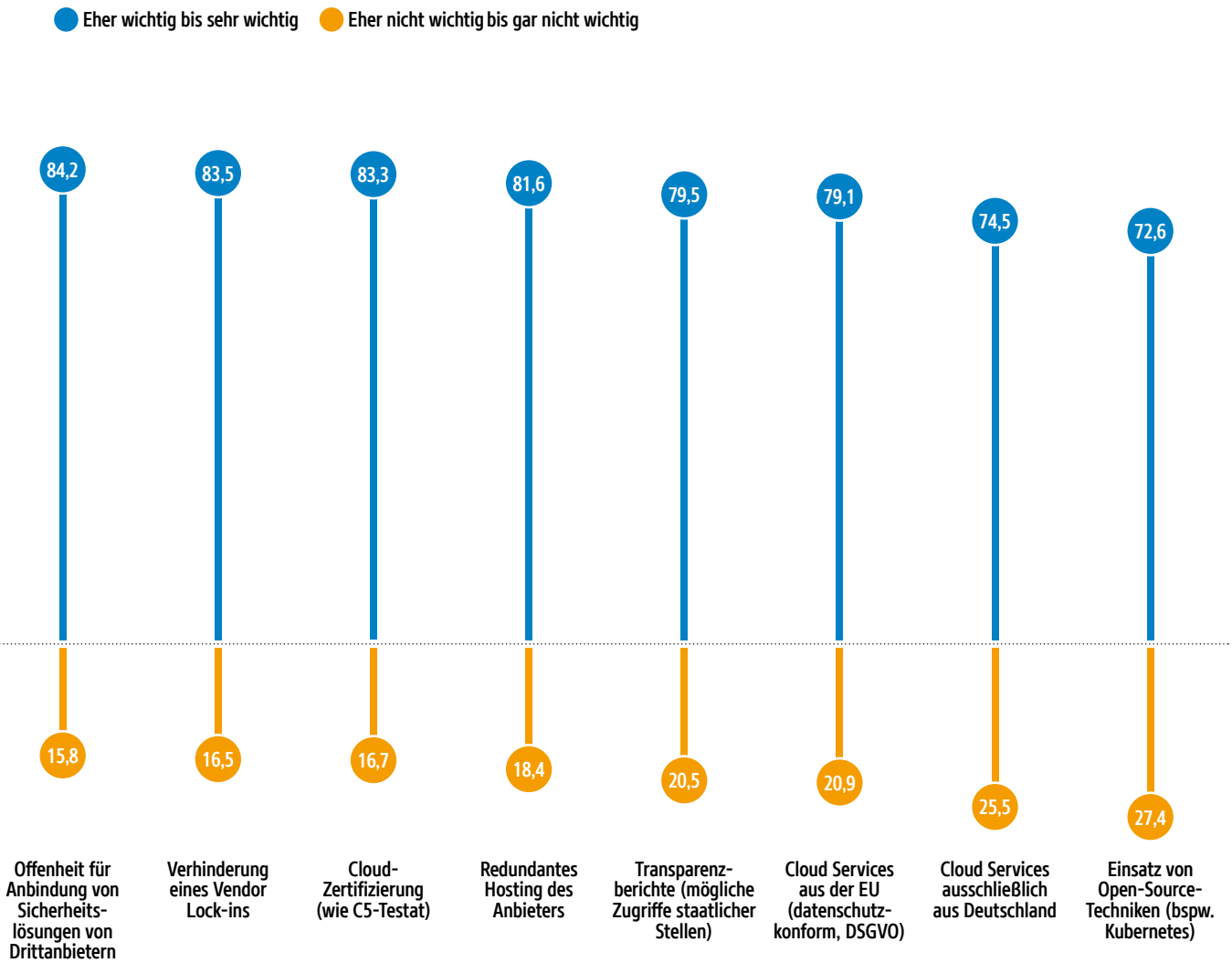
Wie wichtig sind Ihnen in Bezug auf Cloud Services die folgenden Kriterien?

Angaben in Prozent. Basis: n = 352



sind die Fachbereiche selbst in die Cloud-Administration involviert.

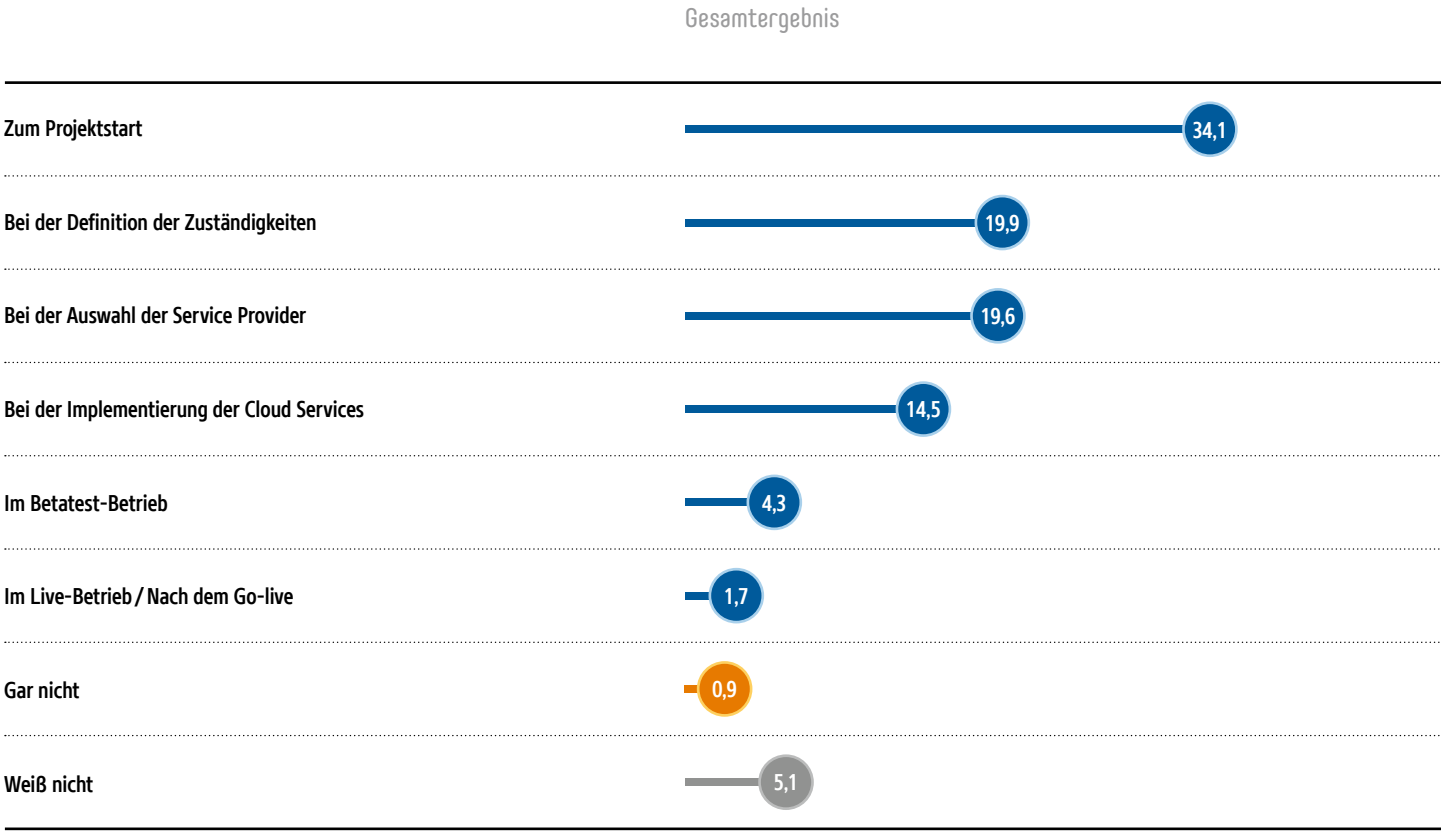
Explizite Datenschutzkriterien wie datenschutzkonforme Cloud-Dienste aus der EU bringen es auf 79 Prozent, die allgemeine Datenschutz-Zertifizierung auf 86 Prozent, die DSGVO-Zertifizierung auf 88 Prozent. Damit bleiben Datenschutzkriterien entscheidend für die Wahl eines Cloud-Dienstes, doch Fragen nach der Administration und den Sicherheitsfunktionen stehen stärker im Vordergrund. Betrachtet man jedoch die Folgen einer komplizierten Cloud-Administration, wird schnell klar, dass auch das Kriterium einer einfachen Administration für Cloud-Sicherheit und Cloud-Datenschutz eine wichtige Rolle spielt. So sind es Fehler bei der Cloud-Konfiguration und -Administration, die die meisten Cloud-Angriffe ermöglichen, da sie ungewollt zu Schwachstellen führen, die Angreifer ausnutzen können.



4

Wie frühzeitig werden bei den Cloud-Projekten Ihres Unternehmens die internen IT-Security-Spezialisten ins Boot geholt?

Angaben in Prozent. Basis: n = 352

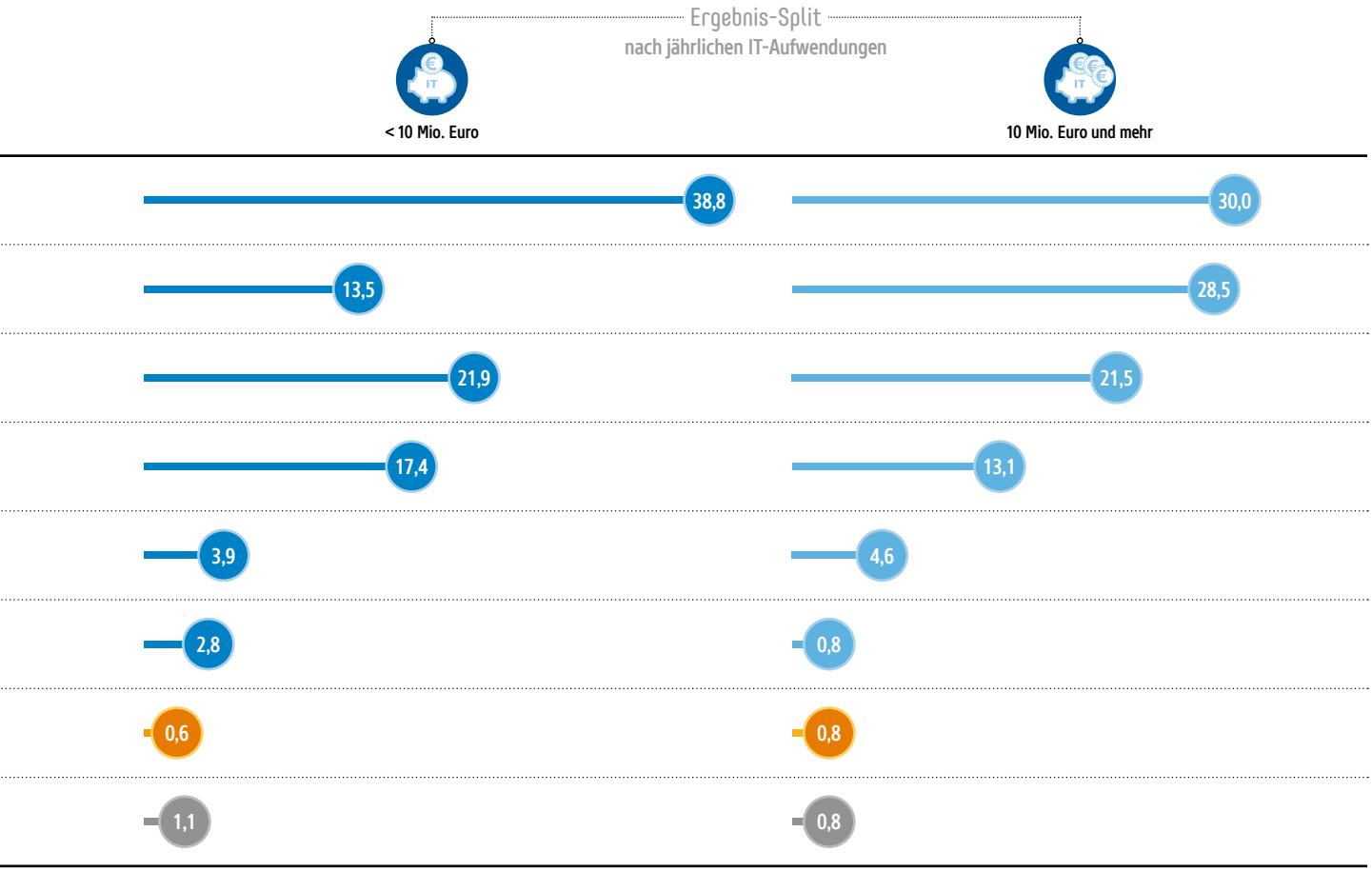


Nur 28 Prozent der kleineren Unternehmen starten Cloud-Projekte mit der Security

Fünf Prozent der Unternehmen wissen nicht, zu welchem Zeitpunkt die interne Security bei Cloud-Projekten einbezogen wird. Zwei Prozent involvieren die Security erst im Live-Betrieb. Nur 34 Prozent der befragten Unternehmen denken an die internen Security-Experten, wenn Cloud-Projekte begonnen werden.

Nur jedes fünfte Unternehmen holt die Security ins Boot, wenn der Cloud Provider ausgewählt wird. Das sind überraschend wenige Unternehmen, da zum Beispiel die Sicherheitsfunktionen des Cloud-Anbieters zu den drei wichtigsten Auswahlkriterien gezählt werden. Dabei stellt sich die Frage, wer die Sicherheitsfunktionen des Cloud-Providers bei den restlichen Unternehmen beurteilt.

Unternehmen mit mehr Beschäftigten achten eher auf Security von Beginn an als kleinere



Unternehmen. So sagen 38 Prozent der Unternehmen mit mindestens 1.000 Beschäftigten, dass die interne Security gleich zu Beginn eingeschaltet wird, bei den kleineren Unternehmen sind es zehn Prozentpunkte weniger.

Höhere jährliche IT-Aufwendungen hingegen sorgen nicht dafür, in Cloud-Projekten so früh wie möglich an die Security zu denken. Von den Unternehmen mit mehr als zehn Millionen Euro IT-Ausgaben pro Jahr beziehen nur 30 Prozent die Security von Anfang an mit ein. Sind die IT-Kosten geringer, steigt dieser Anteil auf 39 Prozent.

Interessant ist auch, dass 41 Prozent der befragten Geschäftsführer meinen, die Security werde bei Cloud-Projekten gleich zu Beginn mit einbezogen, die Security selbst dies aber nur zu 29 Prozent bestätigt. Offensichtlich besteht beim Thema **→ Security by Default** in Cloud-Projekten einiges an Nachholbedarf.

5

Verschlüsselte Cloud-Übertragung ist kleinen Unternehmen wichtiger als größeren

39 Prozent der Unternehmen denken bei Cloud-Sicherheit besonders an die verschlüsselte Datenübertragung vom und zum Cloud-Provider. Unter den Unternehmen mit weniger als 500 Beschäftigten steigt dieser Anteil auf 41 Prozent, bei Unternehmen mit mehr Beschäftigten betonen dagegen nur 38 Prozent die Bedeutung der Datenverschlüsselung.

Besonders häufig wird die verschlüsselte Übertragung in die Cloud mit 44 Prozent von den Unternehmen genannt, die IT-Aufwendungen von weniger als zehn Millionen Euro im Jahr haben. Bei höheren IT-Aufwendungen sinkt der Anteil auf 37 Prozent.

Je nach Rolle der Befragten sind es insbesondere die Security-Verantwortlichen, die zu 42 Prozent die verschlüsselte Datenübertragung nennen. Im Vergleich dazu sagen dies nur 36 Prozent der Befragten aus den Fachbereichen.

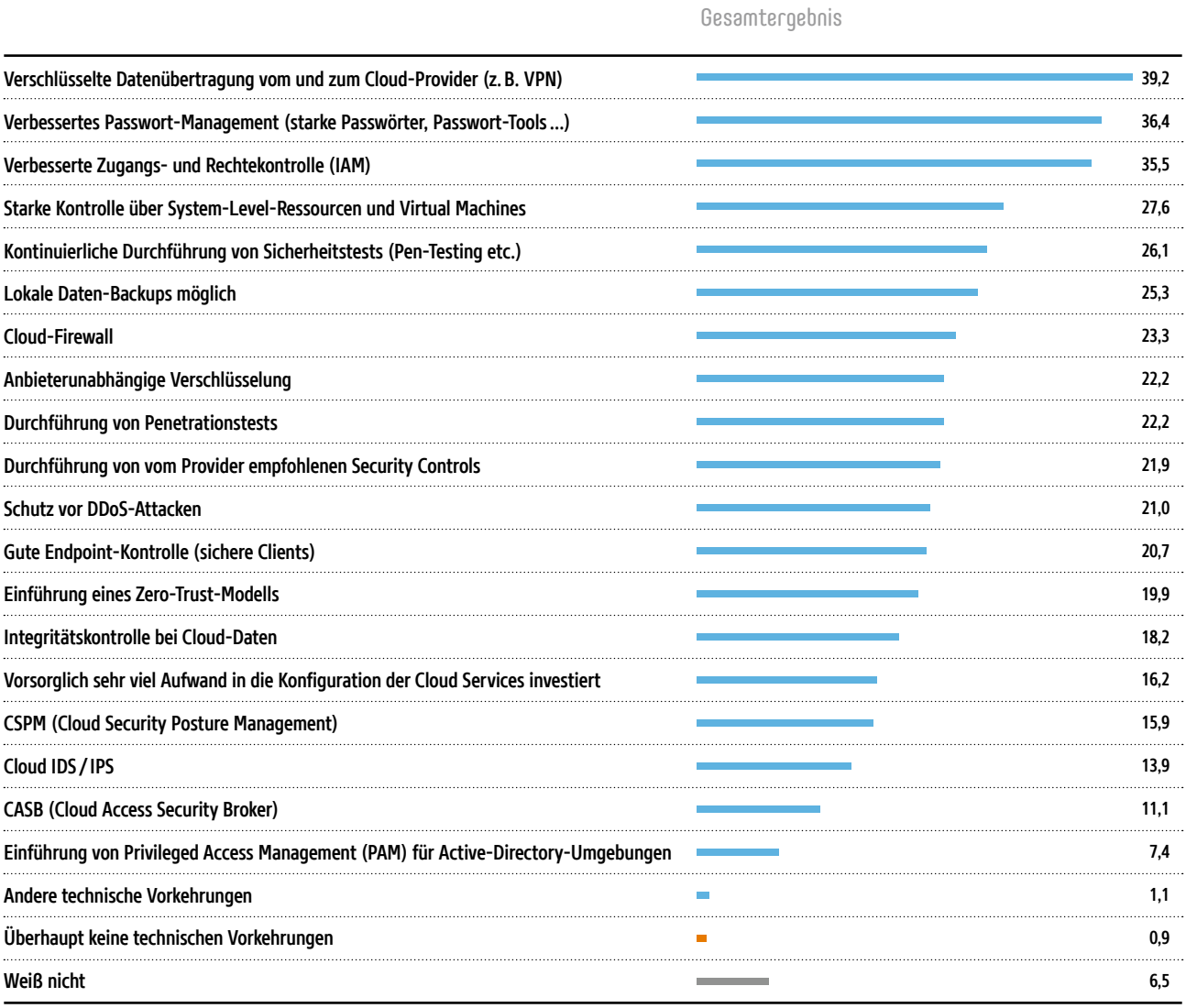
Welche organisatorischen Vorkehrungen sind in Ihrem Unternehmen in Bezug auf Cloud Security getroffen worden?

Angaben in Prozent. Mehrfachantworten möglich. Basis: n = 352

	Gesamtergebnis
Cloud-Policy für die Nutzung von Cloud-Lösungen und Zugangsgeräten	37,5
Klare Definition von Zuständigkeiten im neuen Cloud-Umfeld	33,5
Vorkehrungen für Compliance (z.B. in welchem Land liegen welche Daten?)	33,0
Prüfung der Cloud-Zertifikate	32,1
Neue Security-Stellen	30,1
Person, welche die Cloud-Serviceanbieter im Sinne eines Vendor-Managements steuert	27,8
Prüfung der Transparenzberichte (Zugriffe staatlicher Stellen)	27,3
Datenschutz-Audits bei Provider (bei fehlender Zertifizierung)	25,3
Detailliertes Konzept für das Vendor-Management	19,9
Verpflichtendes Security Awareness Programm für alle Mitarbeiter (inklusive Geschäftsführung und Vorstand)	18,2
Joiner-Mover-Leaver-Prozess (Behandlung von Daten nach Wechsel oder Austritt eines Mitarbeiters)	15,9
Andere organisatorische Vorkehrungen	0,3
Überhaupt keine organisatorischen Vorkehrungen	0,9
Weiß nicht	6,5

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

Angaben in Prozent. Mehrfachantworten möglich. Basis: n = 352



Größere Unternehmen mit mindestens 1.000 Beschäftigten nennen zu 40 Prozent eine verbesserte Zugangs- und Rechtekontrolle (IAM) als Maßnahme für mehr Cloud-Sicherheit. Auch ein verbessertes Passwort-Management (starke Passwörter, Passwort-Tools) wird mit 39 Prozent bei diesen Unternehmen häufiger genannt als die verschlüsselte Datenübertragung in die und aus der Cloud.

Auf gegenwärtig stark diskutierte Maßnahmen wie eine möglichst genaue Cloud-Konfiguration, **→ CSPM (Cloud Security Posture Management)**, **→ Cloud IDS / IPS** und **→ CASB (Cloud Access Security Broker)** setzen nur elf bis 16 Prozent der Befragten.

Bei den organisatorischen Maßnahmen dominieren Cloud Policies für die Nutzung von Cloud-Lösungen und Zugangsgeräten mit 38 Prozent, klare Definition von Zuständigkeiten im neuen Cloud-Umfeld mit 34 Prozent, Vorkehrungen für die Compliance (wie Cloud-Standort) mit 33 Prozent, Prüfung von Cloud-Zertifikaten mit 32 Prozent und neue Security-Stellen mit immerhin 30 Prozent.

6

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

Angaben in Prozent. Mehrfachantworten möglich. Basis: n = 352

Gesamtergebnis

Cloud Provider sind erste Ansprechpartner für die Cloud-Sicherheit

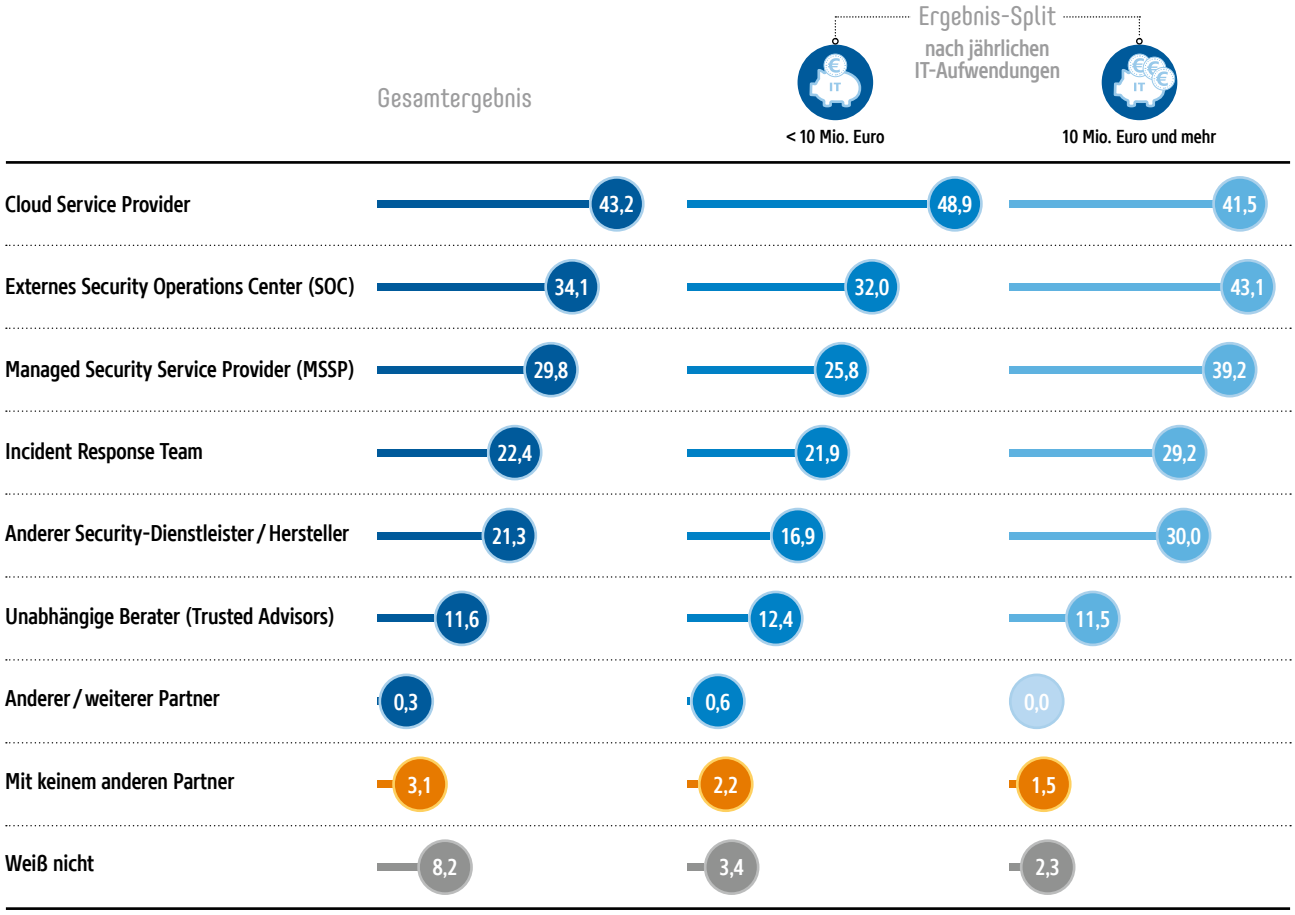
43 Prozent der Unternehmen arbeiten mit ihrem Cloud Provider zusammen, wenn es um die Cloud-Sicherheit geht. Wichtigstes Auswahlkriterium bei der Suche nach einem Cloud-Anbieter ist für 36 Prozent der Unternehmen das Preis-Leistungs-Verhältnis. Nur 28 Prozent achten besonders auf das Know-how ihres Cloud Providers.

Unternehmen mit IT-Aufwendungen von weniger als zehn Millionen Euro jährlich und solche mit mindestens 1.000 Beschäftigten nennen zu 49 Prozent ihre Cloud Provider als Partner in der Cloud-Sicherheit. Der Anteil sinkt auf 42 Prozent, wenn die IT-Aufwendungen höher werden, und sogar auf 37 Prozent, wenn die Mitarbeiterzahl mit 500 bis 999 geringer ist.

Bei höheren jährlichen IT-Aufwendungen sind es für 43 Prozent eher externe **→ SOCs (Security Operations Center)**, die die Partner der Wahl für Cloud-Sicherheit sind. 39 Prozent wenden sich an **→ Managed Security Service Provider (MSSP)**, 30 Prozent an andere Security-Hersteller und 29 Prozent an ein Incident-Response-Team. Unabhängige Berater (Trusted Advisors) spielen mit 13 Pro-

Mit welchen Partnern arbeitet Ihr Unternehmen zusammen, wenn es um Cloud Security geht?

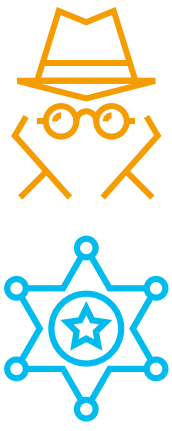
Angaben in Prozent. Mehrfachantworten möglich. Basis: n = 352



zent der Nennungen selbst bei Unternehmen mit weniger als 500 Beschäftigten eher eine untergeordnete Rolle.

Obwohl die Cloud Provider in den meisten Fällen an erster Stelle stehen, wenn es um einen Partner für die Cloud-Sicherheit geht, ist es das gute Preis-Leistungs-Verhältnis, das bei 36 Prozent der Unternehmen als wichtigstes Auswahlkriterium für einen Cloud Provider zählt. Die Datenschutz-Zertifizierung folgt mit 33 Prozent der Nennungen, Vertrauen in den Cloud Provider mit 30 Prozent und technologisches Know-how des Providers mit 28 Prozent. Erwartungsgemäß ist das gute Preis-Leistungs-Verhältnis mit 42 Prozent der Nennungen besonders wichtig, wenn die jährlichen IT-Aufwendungen unter zehn Millionen Euro liegen.

» Datendiebstahl ist größtes Cloud-Risiko, Datenschutz größter Cloud-Vorteil. «



Cloud-Nutzer fürchten Datendiebstahl und erhoffen Datenschutz bei Cloud Computing

Verletzungen des Datenschutzes wie Datendiebstahl, mangelhafte Datenverfügbarkeit und eine zu geringe Belastbarkeit sind für 25 bis 36 Prozent der Unternehmen die größten Sicherheitsrisiken bei der Nutzung von Cloud-Diensten. Gleichzeitig sehen aber 39 Prozent einen Vorteil für den Datenschutz in der Cloud im Vergleich zur On-Premises-IT.

Risiken wie unerlaubte Cloud-Zugriffe durch Innentäter oder Angriffe mit APTs (Advanced Persistent Threats) werden zwar häufig diskutiert, doch nur vier bis fünf Prozent der befragten Unternehmen sehen sie als größte Cloud-Risiken. Auch Konfigurationsfehler in der Cloud nennen nur neun Prozent als dominantes Cloud-Risiko.

Alle als führend eingestuften Sicherheitsrisiken der Cloud drehen sich um den Datenschutz, um Datenverlust, um Cloud-Ausfall und um unzureichende Datenintegrität. Diese Risiken nennen 24 bis 36 Prozent der befragten Unternehmen.

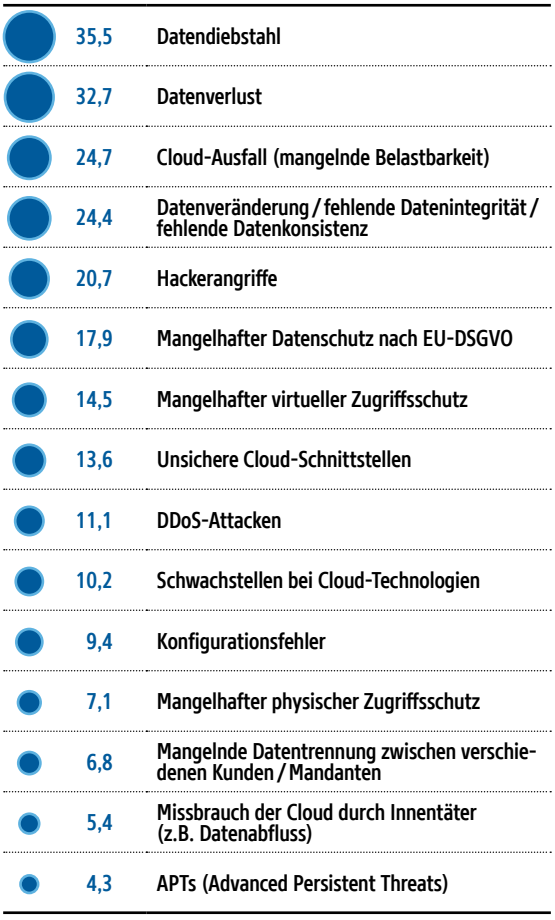
Interessanterweise sind es genau die Datenschutzaspekte, deren Verletzung man fürchtet, die umgekehrt auch als Vorteile einer Cloud gesehen werden, wenn man einen Vergleich zur On-Premises-IT anstellt. 39 Prozent der Befragten sehen den Datenschutz als Cloud-Vorteil, 37 Prozent die Datenverfügbarkeit und 28 Prozent die Belastbarkeit eines Cloud-Dienstes. Die Datenintegrität in der Cloud ist für 20 Prozent vorteilhaft.

Dies unterstreicht, wie wichtig zum einen der Datenschutz gesehen wird und wie groß die Hoffnung ist, dem Datenschutz durch Cloud Computing besser gerecht zu werden. Möglich wird dies aber nur durch weitere Anstrengungen in der Cloud-Sicherheit.

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

Angaben in Prozent. Top 15. Mehrfachantworten möglich. Basis: n = 352

Gesamtergebnis



35,5	Datendiebstahl
32,7	Datenverlust
24,7	Cloud-Ausfall (mangelnde Belastbarkeit)
24,4	Datenveränderung / fehlende Datenintegrität / fehlende Datenkonsistenz
20,7	Hackerangriffe
17,9	Mangelhafter Datenschutz nach EU-DSGVO
14,5	Mangelhafter virtueller Zugriffsschutz
13,6	Unsichere Cloud-Schnittstellen
11,1	DDoS-Attacken
10,2	Schwachstellen bei Cloud-Technologien
9,4	Konfigurationsfehler
7,1	Mangelhafter physischer Zugriffsschutz
6,8	Mangelnde Datentrennung zwischen verschiedenen Kunden / Mandanten
5,4	Missbrauch der Cloud durch Innentäter (z.B. Datenabfluss)
4,3	APTs (Advanced Persistent Threats)

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

Angaben in Prozent. Top 10. Mehrfachantworten möglich. Basis: n = 352

Gesamtergebnis

38,9	Datenschutz
36,9	Datenverfügbarkeit
28,1	Belastbarkeit
20,5	Sicheres Rechenzentrum
20,2	Datenintegrität / Datenkonsistenz
19,0	Virtueller Zugriffsschutz
14,5	Automatisches Patchmanagement
13,4	Physischer Zugriffsschutz
11,9	Cloud Monitoring durch Provider
11,9	Cloud Security durch Provider

Weitere Studienergebnisse

Zahlen und Analysen, die aus Sicht des IDG-Marktforschungsteams ebenfalls wichtig sind

Security-Verantwortliche halten private Cloud-Daten für sicherer als betriebliche

18 Prozent der Befragten glauben, dass ihre privaten Daten in der Cloud nicht sicher sind. Die betrieblichen Daten sind in der Cloud sogar aus Sicht von 20 Prozent unsicher. Mitglieder der Geschäftsführungen sind zuversichtlicher. Hier denken nur 13 Prozent, dass private wie auch betriebliche Daten in der Cloud nicht sicher sind.

An die Sicherheit betrieblicher Daten in der Cloud glauben Unternehmen mit weniger als 500 Beschäftigten zu 67 Prozent, bei 500 bis 999 Beschäftigten steigt dieser Anteil auf 74 Prozent, bei mindestens 1.000 Beschäftigten auf 77 Prozent. Auch die Sicherheit privater Daten in der Cloud wird ähnlich eingeschätzt.

Unterschiede zeigen sich aber bei den verschiedenen Rollen der Befragten. Bei betrieblichen Daten in der Cloud sind sich 82 Prozent der C-Level-Entscheider der Sicherheit gewiss, für private Daten in der Cloud sagen dies aber nur noch 77 Prozent. Offensichtlich vertraut die Geschäftsführung den betrieblichen Cloud-Diensten und der betrieblichen Sicherheit mehr als den privaten Entsprechungen.

Interessant ist auch die Einschätzung der Security-Verantwortlichen, die sich nicht mit der Auffassung der Geschäftsführung deckt. Hier sagen 67 Prozent, dass ihre privaten Cloud-Daten sicher sind, im Fall der betrieblichen Daten in der Cloud liegt der Anteil fast gleichauf bei 66 Prozent. Trotzdem bleibt festzustellen, dass die interne Security nicht davon ausgeht, dass die betriebliche Cloud-Sicherheit höher sei als die private – eher das Gegenteil ist der Fall.

Glauben Sie, dass Ihre persönlichen (privaten) Daten / die Daten Ihres Unternehmens in der Cloud sicher sind?
Angaben in Prozent. Basis: n = 383

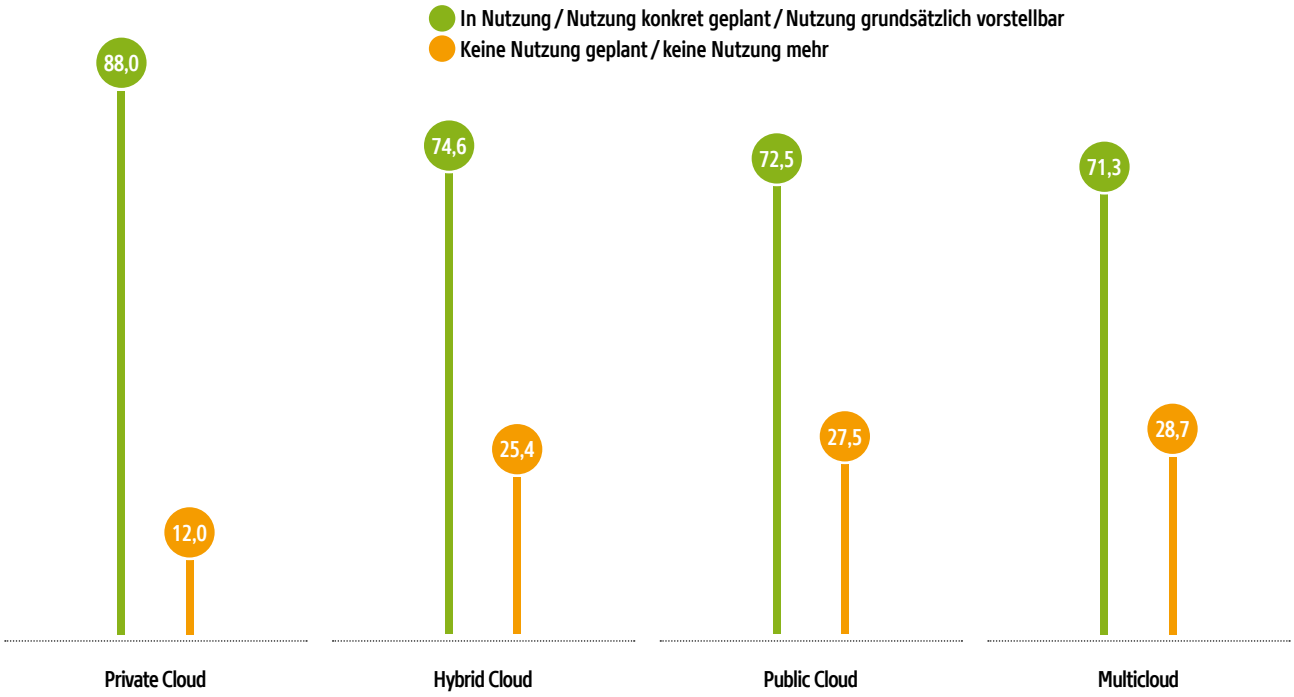
Ergebnis-Split nach Unternehmensbereich

	Gesamtergebnis	C-Level	IT-Leiter / IT-Bereich	IT-Security	Fachbereiche
Ja	72,3 / 72,8	77,1 / 82,4	80,0 / 77,5	67,2 / 65,5	63,8 / 61,9
Nein	18,0 / 20,1	13,1 / 13,1	12,5 / 18,8	22,4 / 25,9	25,7 / 26,7
Kann ich nicht einschätzen	9,7 / 7,0	9,8 / 4,6	7,5 / 3,8	10,3 / 8,6	10,5 / 11,4

Persönliche Daten | Unternehmensdaten

Welches Cloud-Bezugsmodell nutzt Ihr Unternehmen, welches kommt für Ihr Unternehmen grundsätzlich infrage und welches ist für die Nutzung konkret geplant?

Angaben in Prozent. Basis: n = 383



Private Cloud dominiert bei allen Unternehmensgrößen

88 Prozent der Unternehmen nutzen Private Clouds, planen dies konkret oder können es sich zumindest grundsätzlich vorstellen. Dabei variiert der Anteil nur gering mit der Höhe der jährlichen IT-Aufwendungen. Public Clouds stoßen in 73 Prozent der Unternehmen auf Zustimmung. Unternehmen mit 500 oder mehr Beschäftigten sind hier mit jeweils 75 Prozent offener für die Public Cloud, bei weniger als 500 Beschäftigten sinkt der Anteil auf 68 Prozent.

75 Prozent der Unternehmen nutzen hybrides Cloud Computing, planen dessen Einsatz bereits konkret oder können sich eine Nutzung zumindest vorstellen. Multiclouds werden von 20 Prozent eingesetzt, 16 Prozent planen den Einsatz. 29 Prozent verwenden keine Multiclouds (mehr), 25 Prozent sagen, dass sie keine hybriden Clouds (mehr) einsetzen.

21 Prozent der Unternehmen setzen keine Public Clouds ein und haben dies auch nicht geplant, bei Private Clouds beträgt dieser Anteil nur zehn Prozent. Damit ist der Zuspruch für Private Clouds weiterhin deutlich höher als für Public Clouds.

Ob Public Clouds, hybride Clouds oder Multiclouds abgelehnt werden, hängt insbesondere auch von den jährlichen IT-Aufwendungen ab. Betragen diese Aufwendungen mindestens zehn Millionen Euro pro Jahr, liegt der Anteil der Nichtnutzer und Ex-Nutzer von Public Clouds nur noch bei 21 Prozent, von hybriden Clouds bei 17 Prozent und von Multiclouds bei 22 Prozent.

Ob eine bestimmte Form der Cloud-Bereitstellung gar nicht erst geplant ist, hängt auch von der Anzahl der Beschäftigten ab. Bei weniger als 500 Beschäftigten beträgt der Anteil der Nichtnutzer von Public Clouds 23 Prozent, bei mindestens 1.000 Beschäftigten sinkt dieser Anteil auf 19 Prozent.

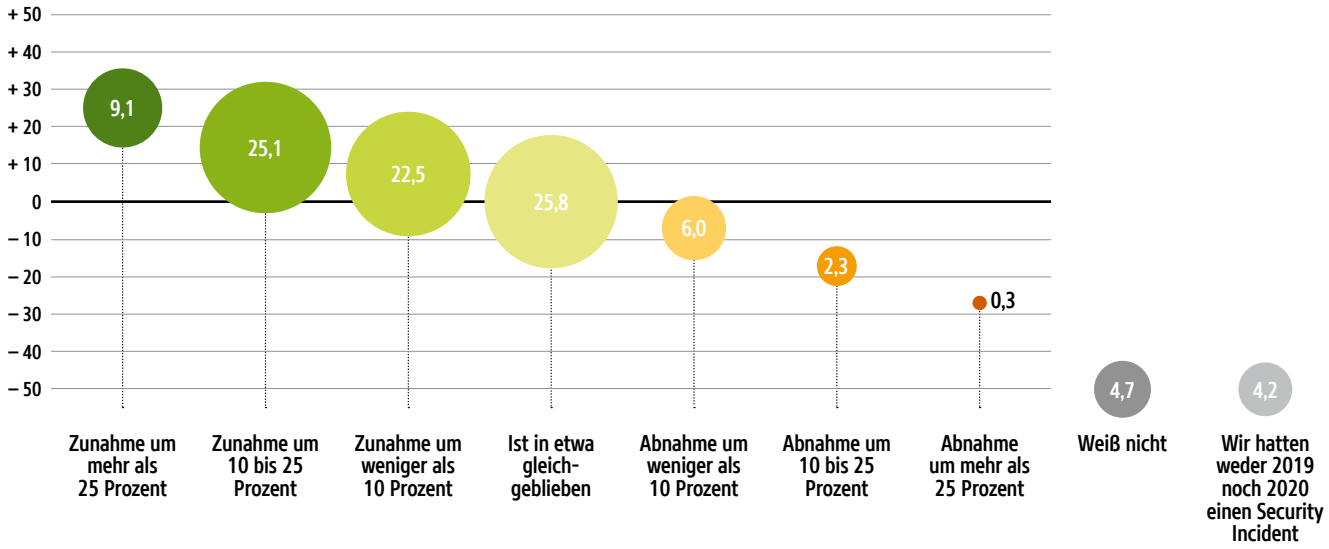
3

57 Prozent der Unternehmen berichten von einer Zunahme der Security-Vorfälle

Die Zahl der Security-Vorfälle hat sich 2020 im Vergleich zum Vorjahr bei jedem vierten Unternehmen um zehn bis 25 Prozent erhöht. Neun Prozent der Befragten berichten gar von einer noch stärkeren Zunahme. Der Anteil der Unternehmen, die von einem Rückgang der Incidents ausgehen, ist derweil ebenso hoch, während vier Prozent meinen, in den vergangenen beiden Jahren überhaupt keinen Security-Vorfall gehabt zu haben.

Wie hat sich, verglichen mit 2019, die Häufigkeit von Security Incidents insgesamt in Ihrem Unternehmen im Jahr 2020 entwickelt?

Angaben in Prozent. Basis: n = 383



Während 26 Prozent der Unternehmen glauben, die Zahl der Security-Vorfälle wäre in 2019 und 2020 etwa gleich geblieben, geht über die Hälfte der Befragten von einer Zunahme aus. Ein besonders starkes Wachstum von mehr als 25 Prozent bei den IT-Sicherheitsvorkommnissen haben elf Prozent der Unternehmen mit mindestens 1.000 Beschäftigten und 13 Prozent der Unternehmen, die jährlich mehr als zehn Millionen Euro für die IT aufwenden.

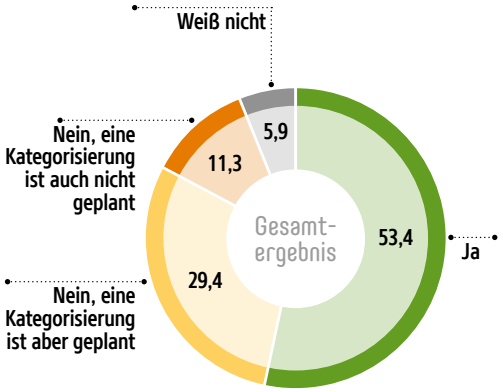
Keinen Security-Vorfall in 2019 und 2020 vermuten sechs Prozent der Unternehmen mit jährlichen IT-Aufwendungen von unter zehn Millionen Euro, bei höheren IT-Aufwendungen geht kein Unternehmen davon aus.

Die Unkenntnis über IT-Sicherheitsvorfälle ist mit acht Prozent bei den Unternehmen mit weniger als 500 Beschäftigten stärker vorhanden als bei Unternehmen mit 500 bis 999 Beschäftigten, bei denen nur ein Prozent sagt, nicht zu wissen, wie es um die Security-Vorfälle in 2019 und 2020 stand.

Nichts über die Entwicklung der Sicherheitsvorfälle wissen insbesondere die Vertreter aus den Fachbereichen (14 Prozent). Unter den Security-Verantwortlichen sind es immer noch drei Prozent.

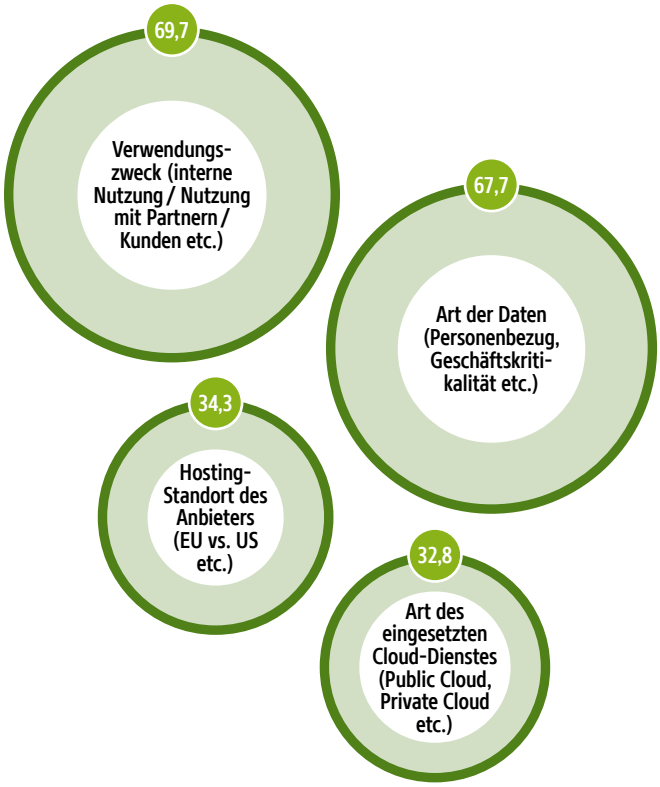
Erfolgt in Ihrem Unternehmen eine Kategorisierung, welche Art von Daten bzw. Dokumenten mit welchen Cloud-Diensten verarbeitet werden darf?

Angaben in Prozent. Basis: n = 371



Nach welchen Kriterien wird kategorisiert?

Angaben in Prozent. Mehrfachantworten möglich. Filter: Unternehmen, die Daten für die Cloud-Verarbeitung kategorisieren. Basis: n = 198



53 Prozent kategorisieren ihre Daten vor der Cloud-Migration

Nur elf Prozent der Unternehmen sagen, dass sie nicht planen, ihre Daten zu kategorisieren, bevor diese in eine Cloud übertragen werden. 29 Prozent planen eine solche Kategorisierung, sechs Prozent sind darüber nicht informiert, ob die Daten kategorisiert werden. Dabei ist das Kategorisieren bei Unternehmen mit mehr Beschäftigten weiter verbreitet.

61 Prozent der Unternehmen mit mindestens 1.000 Beschäftigten achten darauf, welche Datenkategorien in einen Cloud-Dienst übertragen werden. Bei unter 500 Beschäftigten sinkt der Anteil auf 44 Prozent. Auch die Höhe der IT-Aufwendungen hat einen Einfluss. Werden pro Jahr mindestens zehn Millionen Euro für IT ausgegeben, sind es 64 Prozent der Unternehmen, die die Daten kategorisieren. Auffällig sind auch die Unternehmen mit weniger als 500 Beschäftigten: Mit 17 Prozent besonders hoch ist hier der Anteil der Unternehmen, die die Daten nicht kategorisieren.

Befragt wurden die Unternehmen auch, wie sie die Daten kategorisieren, bevor sie in eine Cloud übermittelt werden. 70 Prozent achten dabei auf den Verwendungszweck der Daten, also darauf, ob die Daten zum Beispiel nur intern verwendet werden. 68 Prozent achten auf einen Personenbezug oder die Bedeutung für das Unternehmen.

34 Prozent machen einen Unterschied, wenn eine Cloud in der EU oder zum Beispiel in den USA betrieben wird. 33 Prozent unterscheiden danach, ob es sich um eine Private Cloud oder Public Cloud handelt.

5

Sehr umfassende Sicherheitsrichtlinien zu einzelnen Cloud-Diensten

51 Prozent der Unternehmen bezeichnen ihre Sicherheits-Policies als sehr umfassend, nur vier Prozent sagen, sie hätten keine Sicherheitsrichtlinien. In zwei von drei Unternehmen beziehen sich diese Richtlinien auf den Umgang mit E-Mails. Die Sicherheitsmaßnahmen für Office aus der Cloud haben dagegen nur 46 Prozent geregelt, Cloud-Anwendungen generell 37 Prozent.

Während Sicherheitsrichtlinien im Rahmen der Umfrage als wichtigste organisatorische Maßnahme der Cloud-Sicherheit bezeichnet werden, setzen 43 Prozent der Unternehmen nur auf allgemeine Security-Policies. Das gilt insbesondere für Unternehmen mit 500 bis 999 Beschäftigten (52 Prozent). Unternehmen mit mindestens 1.000 Beschäftigten sagen zu 61 Prozent, dass sie sehr umfassende Sicherheitsrichtlinien haben.

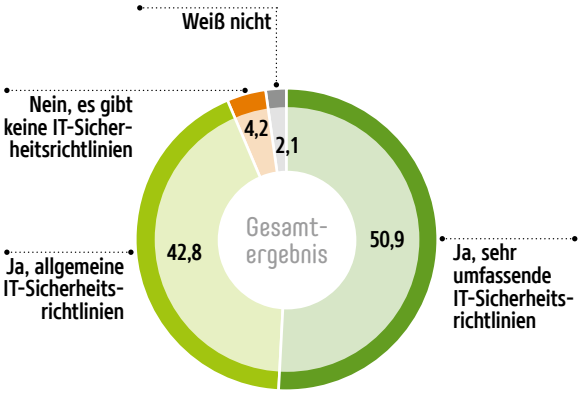
Ob ein Unternehmen allgemeine oder spezielle umfassende Sicherheitsrichtlinien hat, hängt auch von der Höhe der jährlichen IT-Aufwendungen ab. Liegen diese mindestens bei zehn Millionen Euro, berichten 58 Prozent von sehr umfassenden Security-Policies, bei weniger als zehn Millionen Euro sind es nur noch 48 Prozent.

Unternehmen mit Sicherheitsrichtlinien haben zu 42 Prozent Regeln für Videokonferenz-Tools aufgestellt, Datenschutzregeln haben 43 Prozent, für die digitale Zusammenarbeit sind es 29 Prozent, für Edge Computing hingegen erst 17 Prozent.

Generell besteht jedoch noch deutlicher Bedarf an weiteren Sicherheitsrichtlinien, damit auch alle genutzten Cloud-Dienste hinsichtlich der notwendigen Sicherheitsmaßnahmen geregelt sind.

Gibt es in Ihrem Unternehmen IT-Sicherheitsrichtlinien / -Policies?

Angaben in Prozent. Basis: n = 383



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

Angaben in Prozent. Mehrfachantworten möglich. Top 12. Filter: Unternehmen, in denen es IT-Sicherheitsrichtlinien gibt. Basis: n = 359

Gesamtergebnis

65,7	E-Mail
46,5	Allgemeiner Umgang mit Daten (z. B. in Office-Dokumenten)
46,0	Office aus der Cloud
43,2	Umgang mit personenbezogenen Daten
42,1	Video Conferencing Tools
38,2	IT-Plattformen (z. B. ESM, IIoT)
37,3	Cloud-Anwendungen generell (SaaS)
35,1	Umgang mit Geschäftsgeheimnissen
32,6	Social Networks
31,8	Filesharing-Tools (Dropbox etc.)
28,7	Collaboration
17,3	Edge Computing

30 Prozent der Unternehmen erwarten eine Cloud-Zertifizierung nach ISO / IEC 27701

Cloud-Zertifizierungen gehören zu den wichtigen Auswahlkriterien. Dabei erwarten nur zwölf Prozent ein C5-Testat nach Vorgaben des **→ Bundesamtes für Sicherheit in der Informationstechnik (BSI)**. 25 Prozent hingegen achten auf eine Zertifizierung nach ISO / IEC 27001. 28 Prozent wünschen sich eine Datenschutz-Zertifizierung nach EU-DSGVO.

Es gibt verschiedene Cloud-Zertifizierungen, die für die Sicherheit des Cloud-Dienstes oder des Cloud-Anbieters eine Rolle spielen. Neben allgemeineren Zertifizierungen, die sich nicht auf den Cloud-Bereich konzentrieren, gibt es auch solche, die speziell auf Cloud-Dienste zugeschnitten sind.

Die Unternehmen wurden befragt, welche Zertifizierungen sie von ihrem Cloud-Dienstleister erwarten: Dabei achten zum Beispiel 30 Prozent auf eine Zertifizierung nach **→ ISO / IEC 27701**, 28 Prozent auf eine **→ EU-DSGVO**-Zertifizierung (sobald diese verfügbar ist), 25 Prozent auf **→ ISO / IEC 20000-1**, 22 Prozent auf **→ ISO / IEC 27017**, 21 Prozent auf **→ ISO / IEC 27018** und 16 Prozent auf das geplante **→ EU Cloud Scheme**. Nur ein Prozent interessiert sich nicht für eine Zertifizierung.

Bei Unternehmen mit mindestens 1.000 Beschäftigten dominiert mit 37 Prozent der Wunsch nach einer Zertifizierung nach ISO / IEC 27001, Geschäftsführungsmitglieder halten diese zu 35 Prozent für genauso wichtig wie die Zertifizierung nach ISO / IEC 27701.

Welche Zertifizierung(en) erwarten Sie von Ihrem Cloud-Dienstleister?

Angaben in Prozent. Mehrfachantworten möglich. Basis: n = 352

Gesamtergebnis

30,1	ISO / IEC 27701
28,4	EU-DSGVO-Zertifizierung
25,0	ISO / IEC 27001
24,7	ISO / IEC 20000-1
22,2	ISO / IEC 27017
20,7	ISO / IEC 27018
15,6	EU Cloud Scheme
11,9	C5
0,6	Andere Zertifizierung
1,4	Keine Zertifizierung
12,5	Weiß nicht

OpenShift und Managed Services für Container-Plattformen sind besonders beliebt

Nur acht Prozent der Unternehmen haben keine Container-Plattform im Einsatz und planen dies auch nicht. 37 Prozent betreiben eine Container-Plattform selbst, 47 Prozent nutzen einen Managed Service dafür. Nicht über Container-Plattformen informiert sind acht Prozent. OpenShift führt dabei mit 48 Prozent, Kubernetes erreicht 44 Prozent.

Wenn auf Container-Plattformen verzichtet wird, hängt dies zum einen mit den jährlichen IT-Aufwendungen zusammen: Von den Unternehmen, die weniger als zehn Millionen Euro pro Jahr für IT ausgeben, verzichten acht Prozent auf eine Container-Plattform, bei höheren IT-Aufwendungen lediglich fünf Prozent.

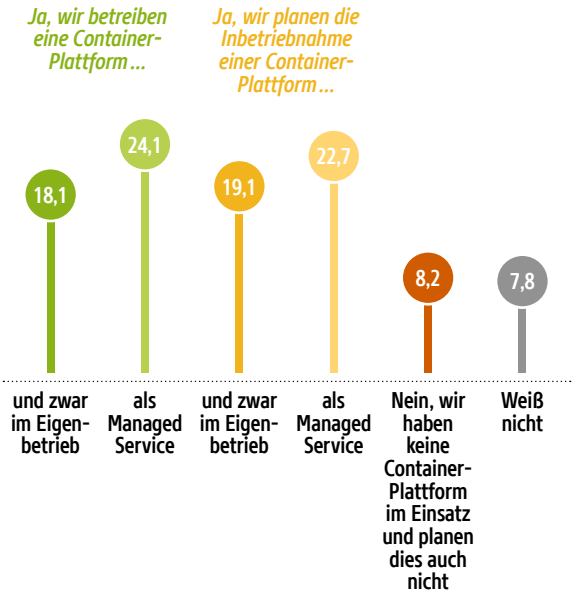
Auch die Zahl der Mitarbeiterinnen und Mitarbeiter hat darauf einen Einfluss. Ab 1.000 Beschäftigten verzichten sechs Prozent auf Container-Plattformen, bei 500 bis 999 Beschäftigten sind es sogar elf Prozent, bei unter 500 Beschäftigten dagegen nur neun Prozent.

Kubernetes wird eher bevorzugt, wenn ein Unternehmen höhere jährliche IT-Aufwendungen hat – hier liegt der Anteil bei 50 Prozent im Vergleich zu 39 Prozent bei geringeren IT-Aufwendungen. Bei OpenShift verhält es sich umgekehrt: 53 Prozent der Unternehmen mit jährlichen IT-Aufwendungen von weniger als zehn Millionen Euro nutzen OpenShift, dagegen sind es 47 Prozent bei höheren IT-Aufwendungen.

Bestehende Applikationen werden in 28 Prozent der befragten Unternehmen für Microservice-Architekturen umgebaut, weitere 48 Prozent planen dies.

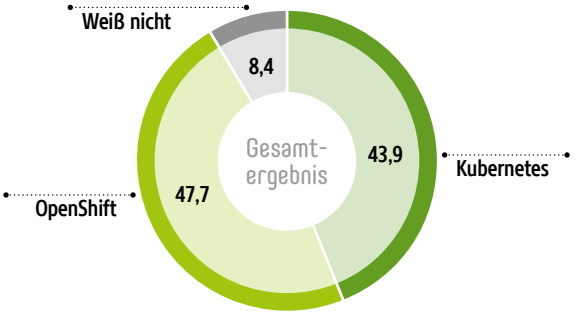
Gibt es in Ihrem Unternehmen eine Container-Plattform, und wie betreiben Sie diese? Betreiben Sie diese selbst oder greifen Sie auf ein Managed-Kubernetes-System zurück, z.B. in einer Public Cloud (Google, AWS, Azure)?

Angaben in Prozent. Filter: Unternehmen, die Cloud-Services nutzen. Basis: n = 282



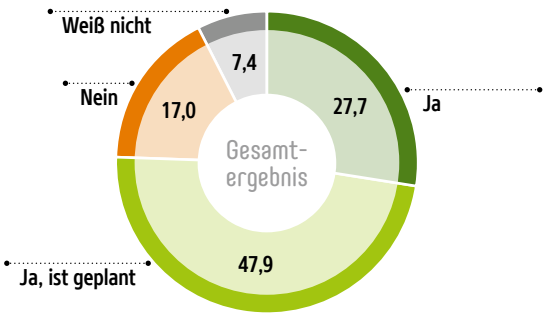
Welche Containerplattform setzt Ihr Unternehmen ein (bzw. plant Ihr Unternehmen einzusetzen)?

Angaben in Prozent. Filter: Unternehmen, die Cloud-Services nutzen und eine Container-Plattform betreiben oder deren Inbetriebnahme planen. Basis: n = 237



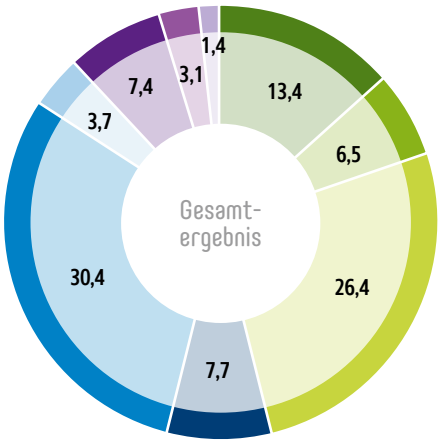
Werden bestehende Applikationen für Microservice-Architekturen umgebaut?

Angaben in Prozent. Filter: Unternehmen, die Cloud-Services nutzen. Basis: n = 282



Wer in Ihrem Unternehmen ist federführend verantwortlich für Cloud Security?

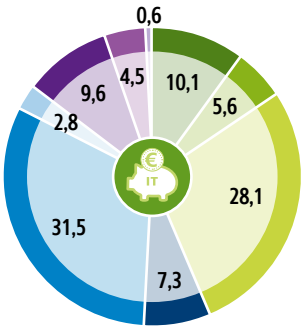
Angaben in Prozent. Basis: n = 352



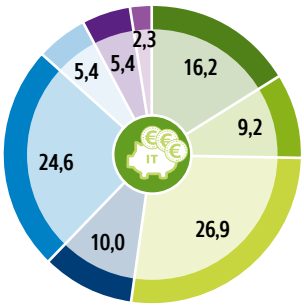
Interne Security verantwortet Cloud-Sicherheit bei nur elf Prozent der Unternehmen

Trotz der Komplexität der Cloud Security sind es nicht die CISOs oder Security-Managerinnen und -Manager, die über die Cloud-Sicherheit entscheiden. In 30 Prozent der Unternehmen macht dies die IT-Leitung, in 26 Prozent die IT-Vorstände, in 13 Prozent die Geschäftsführung.

Ergebnis-Split
nach jährlichen IT-Aufwendungen



< 10 Mio. Euro



10 Mio. Euro und mehr

- Geschäftsführer / CEO
- COO / CFO / Kaufmännische Leitung
- CIO / CDO / IT-Vorstand
- CTO / Technik-Vorstand
- IT-Leiter / IT-Manager
- CISO / CSO
- Security-Manager
- Administrator
- Andere Person / Abteilung

Selbst in Unternehmen, die höhere IT-Aufwendungen von mindestens zehn Millionen Euro im Jahr haben, sind es vor allem die IT-Vorstände oder IT-Leitungen, die die Cloud-Sicherheit in ihrem direkten Verantwortungsbereich haben. Beide Gruppen zusammen machen 52 Prozent der Entscheider im Bereich Cloud-Sicherheit aus. Bei geringeren jährlichen IT-Aufwendungen beträgt der Anteil der IT-Leitungen und IT-Vorstände bei den Cloud-Security-Entscheidern sogar 60 Prozent. Je mehr Beschäftigte ein Unternehmen hat, desto höher ist dieser Anteil: Bei weniger als 500 Beschäftigten sind es 49 Prozent, bei 500 bis 999 Beschäftigten sind es 60 Prozent und ab 1.000 Beschäftigten sogar 61 Prozent.

CISOs, Security-Verantwortliche und Security-Manager hingegen sind nur in elf bis zwölf Prozent der befragten Unternehmen die Cloud-Security-Entscheider.

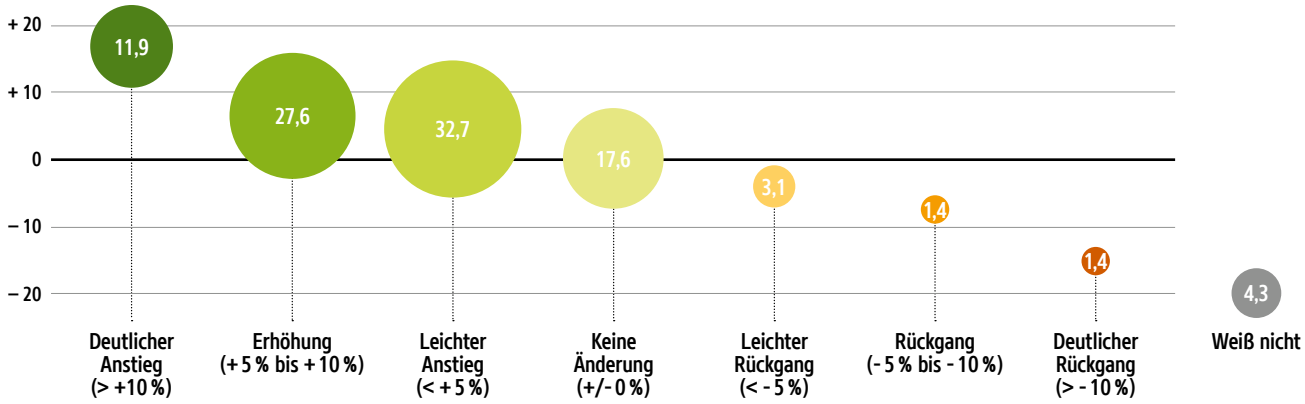
Offensichtlich sind die internen Security-Experten mehrheitlich nicht in der Position, über die Cloud-Sicherheit zu entscheiden. Dies sollte überdacht werden, da Cloud-Sicherheit anspruchsvoll und dynamisch ist. Somit ist viel Fachwissen für die Entscheidungen erforderlich, selbst bei Nutzung von Security-Services.

9

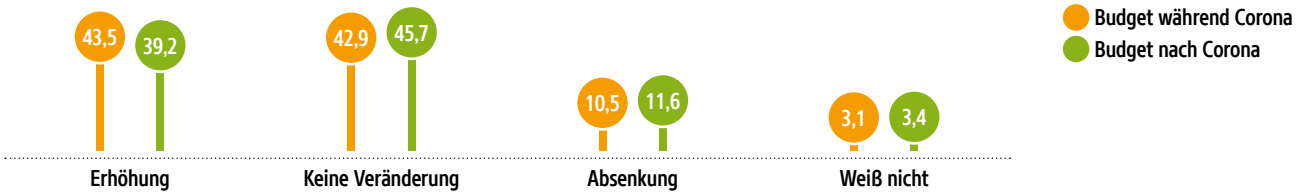
Security-Budget steigt bei 72 Prozent der Unternehmen, nicht nur wegen Corona

In zwölf Prozent der Unternehmen steigt in 2021 das Security-Budget deutlich um mehr als zehn Prozent an. Bei 28 Prozent wächst das Security-Budget um fünf bis zehn Prozent. Bei 33 Prozent ist die Erhöhung mit weniger als fünf Prozent eher gering. 18 Prozent berichten von keiner Änderung. Einen Rückgang sehen dagegen nur sechs Prozent.

Wie entwickelt sich das IT-Security-Budget Ihres Unternehmens in 2021 (im Vergleich zum Vorjahr)?
Angaben in Prozent. Basis: n = 352



Wie hat sich die Coronapandemie bisher auf das IT-Security-Budget ausgewirkt und wie wird es sich nach Ende der Pandemie verändern?
Angaben in Prozent. Basis: n = 352



Die Gründe für die Veränderungen bei den Security-Budgets in 2021 liegen nicht nur in der Coronakrise. 44 Prozent sagen zwar, sie erhöhten wegen der Pandemie das Security-Budget, doch bei 43 Prozent habe dies keinen Einfluss, während elf Prozent berichten, dass sie das Security-Budget wegen der Pandemie sogar absenkten.

Für die Zeit nach der Krise sehen 39 Prozent weiterhin eine Erhöhung des Security-Budgets. Keine Veränderung erwarten 46 Prozent, dagegen gehen zwölf Prozent von einer Reduzierung aus. Die weitere Erhöhung wird mit 46 Prozent vermehrt von den Unternehmen genannt, deren jährliche IT-Aufwendungen bei mindestens zehn Millionen Euro liegen. Bei geringeren IT-Ausgaben sinkt der Anteil auf 35 Prozent. Diese Unternehmen sehen mit 52 Prozent der Nennungen keine Veränderungen bei ihrem Security-Budget nach der Pandemie.

Im Security-Budget sind bei 64 Prozent der Firmen auch die Maßnahmen für Schulungen in der IT-Sicherheit enthalten. So sagen beispielsweise 15 Prozent der Befragten, dass es dafür ein eigenes Weiterbildungsbudget gebe.

Was Unternehmen über Cloud-Sicherheit denken

Über Cloud-Sicherheit wird viel diskutiert. Dabei sollte aber berücksichtigt werden, wie bestimmte Botschaften und Informationen zur Cloud-Sicherheit aufgenommen werden, welche Einstellungen also bei den Unternehmen vorherrschen. Hierzu wurden den Unternehmen fünf Statements vorgelegt und die Zustimmung abgefragt – mit spannenden Resultaten.

„So wie gute Bremsen absolut notwendige Voraussetzung für schnelles, aber sicheres Fahren sind, ist IT-Security Voraussetzung dafür, Cloud Services optimal und gewinnbringend zu nutzen. IT-Security wird hier zum Business Enabler!"

Kommentar des Autors:
Fast drei Viertel der Unternehmen sehen Cloud-Sicherheit als Business-Enabler. Trotzdem planen viele Firmen kein spezielles Budget für die Cloud-Sicherheit ein. Offensichtlich wird das Budget für Cloud-Sicherheit nicht wirklich als Investition für das Cloud-Business und damit die Digitalisierung an sich gesehen.

„Unser Unternehmen setzt bei seiner IT-Security-Strategie bevorzugt auf Bordmittel von Microsoft (z. B. M365 / Azure Defender) und nicht auf andere Security ISVs."

Kommentar des Autors:
Cloud Provider gelten als wichtigste Partner für die Cloud-Sicherheit. Dies zeigt sich auch daran, dass die Bordmittel von Microsoft gegenüber Security-Lösungen von Dritten von fast der Hälfte der Unternehmen bevorzugt werden.

„Bei Cloud Security geht es um Prozesse, es geht aber vor allem auch um Menschen."

Kommentar des Autors:
Über die Hälfte der Unternehmen erkennt die Bedeutung des Menschen für die Cloud-Sicherheit. Bedenkt man aber, dass fehlerhafte Cloud-Konfigurationen als Ursache für die meisten Cloud-Sicherheitsvorfälle gesehen werden, muss es noch deutlicher werden, dass Technik allein die Cloud nicht sicherer machen kann.

„Drei Handlungsempfehlungen in puncto Cloud Security: Backup, Backup, Backup!"

Kommentar des Autors:
62 Prozent messen Backups eine zentrale Bedeutung für die Cloud-Sicherheit zu. Auch wenn Datensicherungen natürlich ein wichtiger Bestandteil sind, sollte sich niemand in Sicherheit wiegen, weil es Backups für die Cloud-Daten gibt. Allein schon die Ransomware-Attacken auf Backups zeigen, dass dies zu kurz gedacht wäre.

„Die Cloud hat das Potenzial, die Sicherheit zu erhöhen."

Kommentar des Autors:
Rund 60 Prozent der Unternehmen sehen die Cloud als Chance, die Sicherheit zu verbessern. Trotzdem sollte nicht vergessen werden, dass mit der Cloud auch klare Risiken verbunden sein können. Nur so kann die Cloud wirklich zum Sicherheitsgewinn werden.

Stimme voll und ganz zu / stimme zu
Stimme gar nicht zu / stimme nicht zu

Was tun? Experten empfehlen

© stock.adobe.com / Sergey Nivens (auch S. 5)

„Lessons learned“ und Best Practices von denen, die es wissen müssen

Cloud Security 2021

Timo Schlüter,
Business Consultant Cyber Security, Arvato Systems

Unternehmen sollten sich darüber klar werden, **welches Security-Level** für sie sinnvoll ist, und in diesem Rahmen auf einen ganzheitlichen Ansatz setzen: Prevention-, Detection- und Response-Maßnahmen kombiniert mit den drei Ebenen Compliance, technische Security und Security Operations.

Jörg Marcus Horn,
Chief Product Officer, uniscon GmbH

Unternehmen sollten bei der Wahl eines Cloud-Dienstes darauf achten, dass ihre Daten nicht nur bei der Übertragung („in transit“) und Speicherung („at rest“), sondern auch **während der Verarbeitung** („in use“) stets geschützt sind. Confidential Computing kann hier Abhilfe schaffen.

Dr. Martin Burkhart,
Head of Product Management Airlock, Ergon Informatik AG

Bei Cloud Security dürfen keine Kompromisse gemacht werden. Handlungsbedarf besteht an den Schnittstellen zwischen Zonen und Services. Da es keine internen Zonen mehr gibt, wird eine **Zero Trust Architektur** Pflicht, die über Micro-gateways einzelne Services schützt. Ein Vendor Lock-in sollte möglichst vermieden werden.

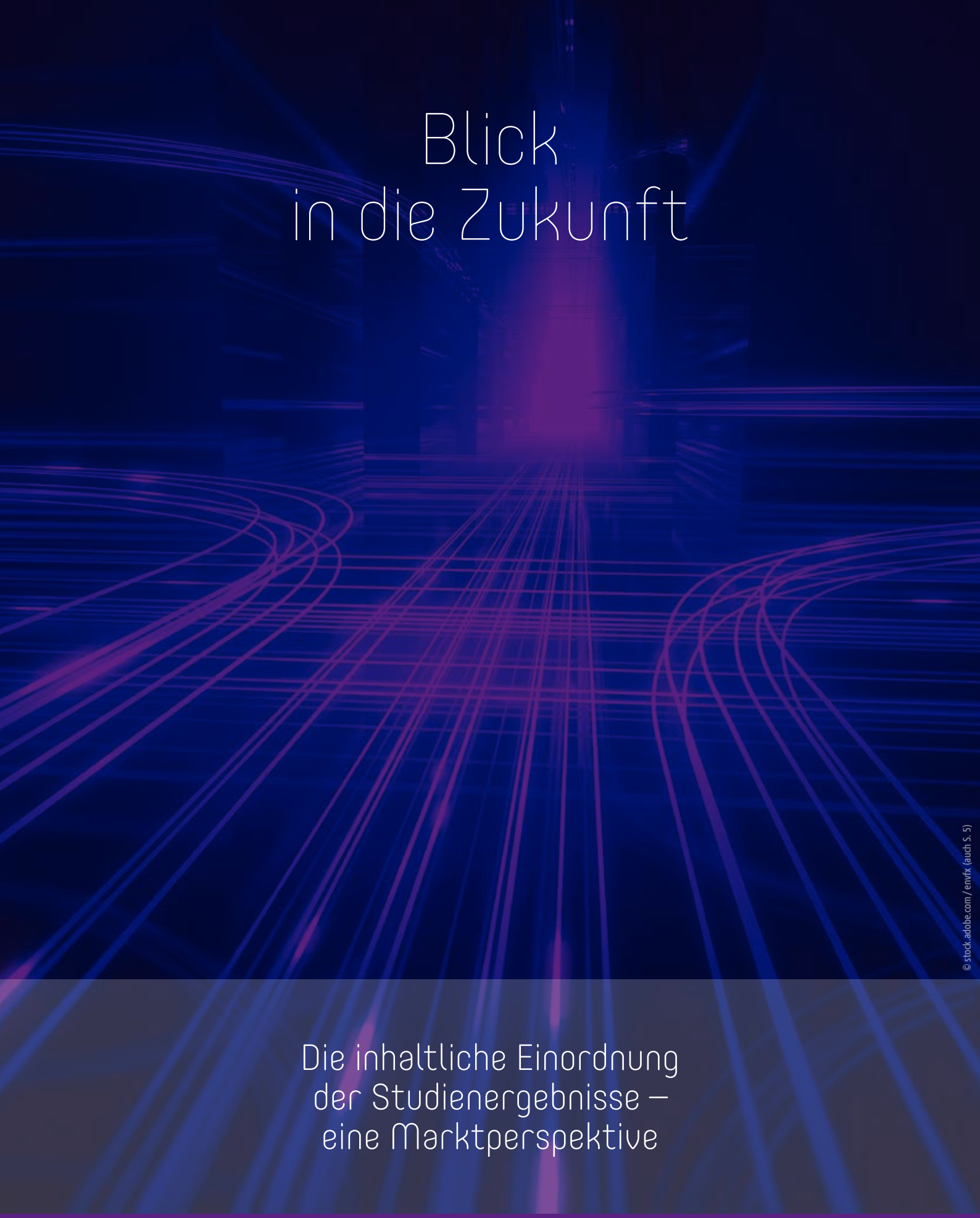
Alexander Häußler,
Product Compliance Manager ISO/IEC 27001 TÜV SÜD

Informationen, von Kundendaten bis zu Produktinformationen, sind das **höchste Gut von Unternehmen** und müssen geschützt werden. Die Qualität dieses Schutzes kann durch unabhängige Prüforganisationen wie TÜV SÜD nach der Normenreihe ISO/IEC 2700x überprüft und zertifiziert werden.

Florian Weigmann,
Chief Product Officer, PlusServer GmbH

Für Multiclouds empfiehlt sich ein einheitliches Sicherheitskonzept mit einem **zentralen Security Layer** für alle im Unternehmen genutzten Cloud-Lösungen. So muss für jede einzelne Cloud des Kunden nur noch ein Grundlevel an Security sowie ein sicherer Kanal zwischen Cloud-Plattform und Security Layer betrieben werden.

Blick in die Zukunft



Die inhaltliche Einordnung der Studienergebnisse – eine Marktperspektive

Cloud Security 2021

Viele Unternehmen müssen noch den wahren Wert der Cloud Security erkennen

Von der Cloud erhoffen sich Unternehmen Kosteneinsparungen. Diese sollten aber nicht gerade in der Security gesucht werden. Stattdessen gilt es, die Cloud-Sicherheit auf ein festeres Fundament zu stellen – mit Security-Prozessen, die Cloud-Projekte von Beginn an begleiten. Andernfalls drohen weiterhin Betriebsunterbrechungen und Datenverlust.

Von Oliver Schonschek

Jedes dritte Unternehmen hat in den letzten zwölf Monaten bereits einen wirtschaftlichen Schaden durch Cloud-Angriffe erlitten. Dabei sind die betroffenen Cloud-Dienste für die Produktivität der Unternehmen so wichtig, dass die Cloud-Vorfälle oftmals zu Betriebsunterbrechung und Stillstand geführt haben.

Wie zum Beispiel das Allianz Risk Barometer 2021 zeigt, fürchten sich Unternehmen derzeit besonders vor den Folgen der Coronapandemie, vor der Unterbrechung ihrer Geschäftstätigkeit und vor Cyberattacken. Wenn dann trotzdem das Security-Budget zur Absicherung der Cloud während der Coronakrise unverändert bleibt oder sogar abgesenkt wird, wenn es kein spezielles Budget für die Cloud-Sicherheit gibt, dann spricht dies dafür, dass die Bedeutung und die Komplexität der Cloud-Sicherheit unterschätzt werden.

Cloud-Sicherheit muss man sich erarbeiten

Die Nutzung der Cloud wird von fast 40 Prozent der Unternehmen als Vorteil für den Datenschutz gesehen. Man verspricht sich davon also, dass der Datenschutz besser eingehalten werden kann, wenn man die zu schützenden Daten von **→ On-Premises** in die Cloud überträgt. Allein die Migration in die Cloud erhöht den Datenschutz aber nicht. Aus gutem Grund fürchten sich die Unternehmen vor Datendiebstahl, mangelhafter Datenverfügbarkeit und einer zu geringen Belastbarkeit bei der Nutzung von Cloud-Diensten.

Auch wenn die Cloud Provider viel für die Security tun, gibt es das Modell der geteilten Verantwortung in der Cloud-Sicherheit. So ist es richtig, den Cloud Provider als wichtigen Partner in der Cloud Security zu sehen. Doch er übernimmt nicht alle Sicherheitsaufgaben. Ein Verzicht auf weitere Sicherheitslösungen, die Dritte anbieten und erbringen, ist durchaus riskant. So muss der Cloud-Nutzer zum Beispiel entscheiden, welche Daten in die Cloud übermittelt werden und wie der Nutzer sie dort dem Schutzbedarf entsprechend absichern will.

Cloud-Sicherheit muss am Anfang jedes Cloud-Projektes stehen

Nicht nur die noch unzureichende Berücksichtigung der Cloud im Security Budget ist ein Anzeichen dafür, dass die Bedeutung der

Cloud Security noch unterschätzt wird, trotz aller Beteuerungen, wie wichtig Datenschutz und Datensicherheit für die Entscheidung „pro Cloud“ sind.

Nur jedes dritte Unternehmen denkt an die eigenen Security-Maßnahmen, wenn ein neues Cloud-Projekt beginnt. **→ Security by Default** und **→ Security by Design** müssen deutlich stärker in das Bewusstsein aller Unternehmen rücken, die von den Vorteilen der Cloud profitieren wollen – erst recht, wenn Sicherheit und Datenschutz als Cloud-Vorteile gewertet werden.

Aufgabe für die Zukunft: Zusammenhänge in der Cloud-Sicherheit besser verstehen

Security-Experten sehen in Fehlern bei der Cloud-Administration und Cloud-Konfiguration die Basis für die meisten Cloud-Sicherheitsvorfälle. Wenn Unternehmen also die leichte Administration als wichtigstes Kriterium bei der Wahl eines Cloud-Dienstes und Cloud Providers identifizieren, hilft dies auch der Cloud-Sicherheit. Allerdings geschieht dies nicht bewusst, denn fehlerhafte Cloud-Konfigurationen werden laut Studie nicht als größtes Cloud-Risiko eingeschätzt.

Offensichtlich sehen viele Unternehmen noch nicht alle Abhängigkeiten in der Cloud und die Folgen für die Cloud-Sicherheit. Wäre ihnen dies bewusster, würden sie auch besser verstehen, warum Cloud-Sicherheit so umfangreich und komplex ist. Dann wäre auch der Wert einer sicheren Cloud deutlicher sichtbar.

Für die Zukunft wäre es wünschenswert, die Cloud-Sicherheit umfassender anzugehen und ihr das notwendige Gewicht und Budget zu geben. Dazu sollten die internen Security-Kräfte stärker in die Verantwortung für die Cloud-Sicherheit kommen. Die Geschäftsführung, die IT-Vorstände und die IT-Leitungen allein werden hier die notwendigen Entscheidungen nicht treffen können.

Fehlen die internen Security-Experten, könnten die sogenannten Trusted Advisors helfen, die anbieterübergreifend bei der Auswahl und Implementierung der erforderlichen Cloud-Sicherheit unterstützen. Noch aber werden sie am unteren Ende der wichtigen Partner in der Cloud Security einsortiert.

Das sollte sich in naher Zukunft ändern, denn nur der Cloud Provider allein reicht nicht als Sicherheitspartner im Cloud Computing – schon gar nicht, wenn die Multicloud und die hybride Cloud in Zukunft noch wichtiger werden.

CIO-Agenda 2021

Daten zur allgemeinen Einschätzung der Marktlage

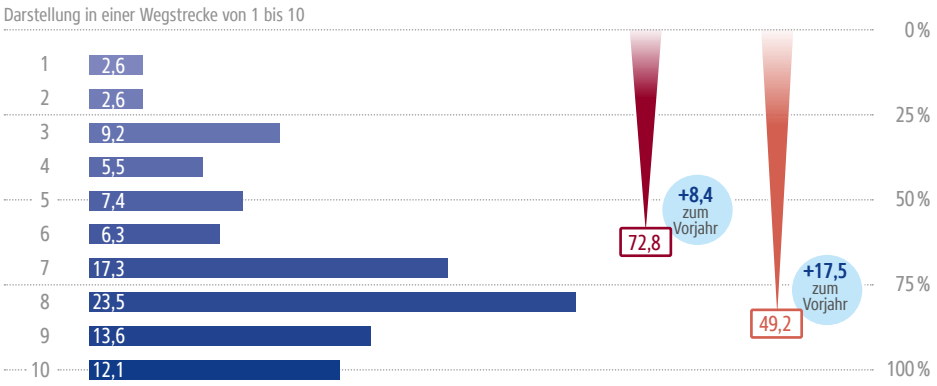
Exklusive Einblicke: Wie IT-Entscheider das Business in Gegenwart und Zukunft gestalten

Cloud Security 2021

CIO-Agenda 2021

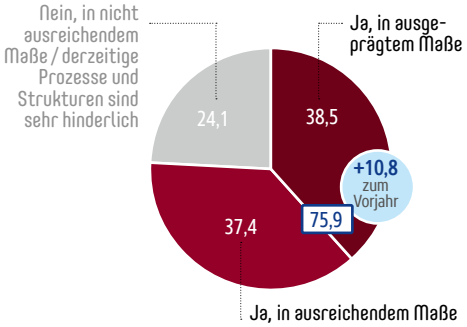
Mit Siebenmeilenstiefeln auf dem Weg der digitalen Transformation

Fast 73 Prozent der befragten CIOs sehen sich und ihre Unternehmen bereits auf der zweiten Hälfte des Weges, **knapp die Hälfte der Befragten (49 Prozent)** sogar auf dem letzten Viertel. Das ist teils deutlich mehr als im Vorjahr (+8 bzw. +18 Prozentpunkte).



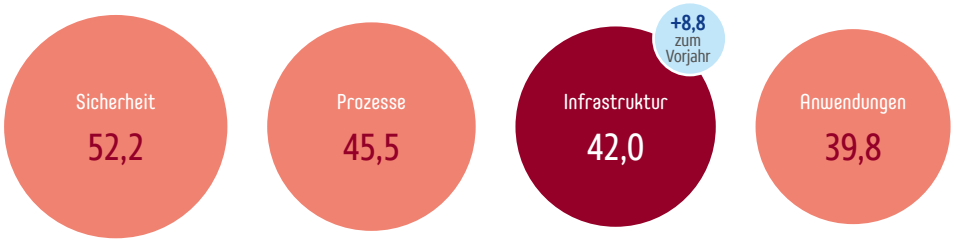
Entwicklung neuer digitaler Geschäftsmodelle

76 Prozent der Unternehmen verfügen über grundlegende **Prozesse und Strukturen** dafür – elf Prozentpunkte mehr als im Vorjahr. In den Unternehmen mit mehr als 10 Millionen Euro jährlichem IT-Budget liegt der Wert heute sogar bei fast 92 Prozent (+13).



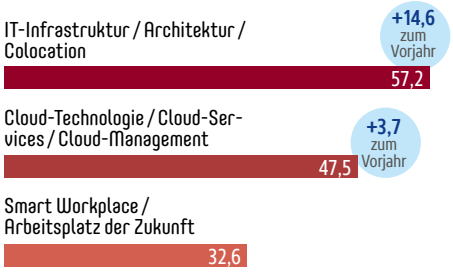
Starkes „Brot- und Buttergeschäft“

Die **substanziellsten Investments** der kommenden drei Jahre wollen die CIOs in den Bereichen Sicherheit, Prozesse, Infrastruktur und Anwendungen tätigen. Vor allem die **Infrastrukturthemen** erfahren neue Auferksamkeit (+9 Prozentpunkte im Vergleich zum Vorjahr).



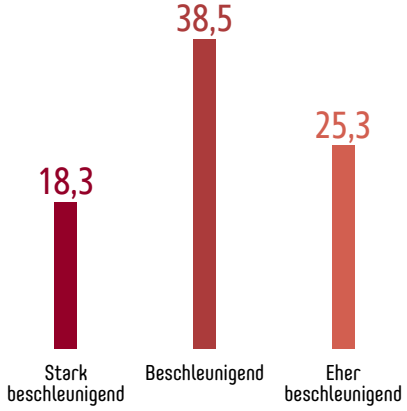
Cloud nicht mehr Nummer eins

Knapp 57 Prozent der Unternehmen wollen mittelfristig zunächst in Infrastrukturthemen **investieren** (+15 Prozentpunkte im Vorjahresvergleich). Damit verlieren die Cloud-Investments trotz Steigerung zum Vorjahr (+4) ihren Spitzenplatz deutlich.



Corona beschleunigt

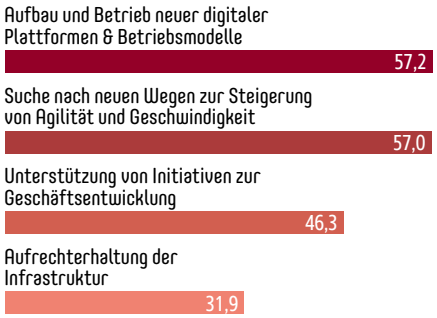
82 Prozent der Unternehmen schätzen den mittel- bis langfristigen **Einfluss der Pandemie** auf den digitalen Wandel in den Unternehmen als beschleunigend ein.



Innovator, kein „Bewahrer“

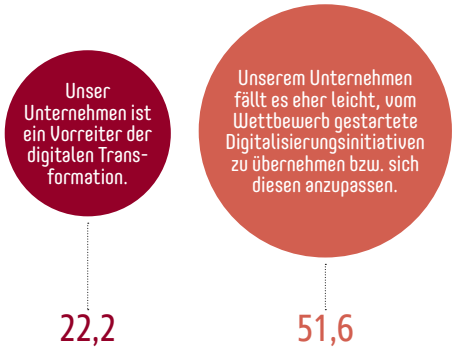
Die meisten CIOs / IT-Leiter sehen sich langfristig als Schaffer und Betreiber neuer digitaler Plattformen und Betriebsmodelle sowie als Wegbereiter von mehr Agilität und Geschwindigkeit in ihren Unternehmen.

Fokus des CIOs / IT-Leiters in 5 Jahren:



Pioniere und Fast Follower

Fast drei Viertel der CIOs sieht sich als **Vorreiter** (22 Prozent) oder **Fast Follower** (52 Prozent) für Digitalisierungsinitiativen.

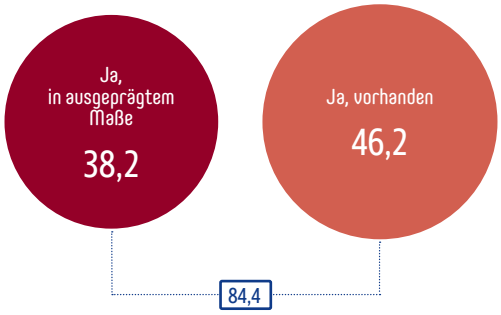


Ein Studienprojekt von IDG Research Services in Kooperation mit der WHU – Otto Beisheim School of Management.

Alle Angaben in Prozent

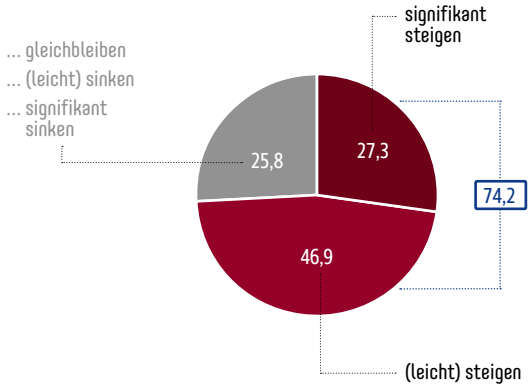
Digitalisierungsstrategie

Fast 85 Prozent der deutschen Unternehmen haben mittlerweile eine, bei den großen mit mehr als 100 Mitarbeitern sind es sogar 90 Prozent, bei denen mit mehr als 1 Mrd. Euro Jahresumsatz mehr als 95 Prozent.



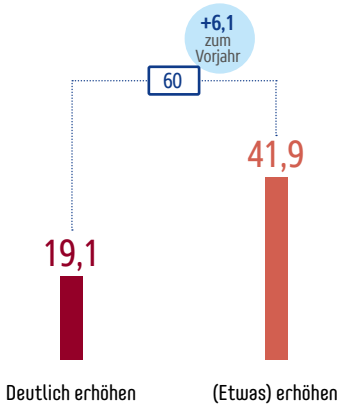
Weiter steigende Investitionen in die digitale Zukunft

Das **Gesamt-IT-Budget** wird bei **74 Prozent** der Befragten (signifikant) steigen. Im Vorjahr lag dieser Wert noch bei knapp 66 Prozent.



Mehr IT-Mitarbeiter für den Erfolg

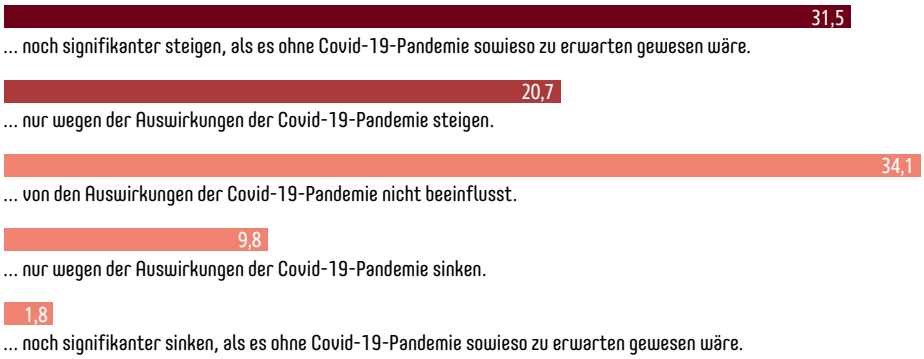
Die **Zahl der IT-Mitarbeiter** soll in über **60 Prozent** der Unternehmen (deutlich) erhöht werden. Das sind 6 Prozentpunkte mehr als im Vorjahr.



Corona sorgt für mehr Geld

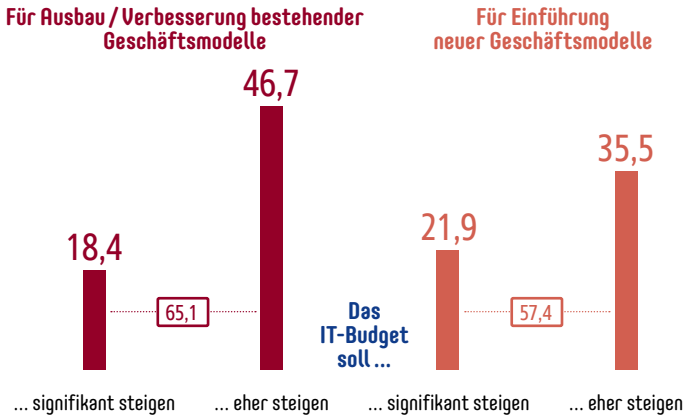
In mehr als einem Fünftel der befragten Unternehmen werden die IT-Budgets nur wegen der Auswirkungen durch die Coronapandemie steigen; **in fast einem weiteren Drittel** trägt die Pandemie zu einer noch stärkeren Budget-Steigerung bei.

Das IT-Budget wird ...



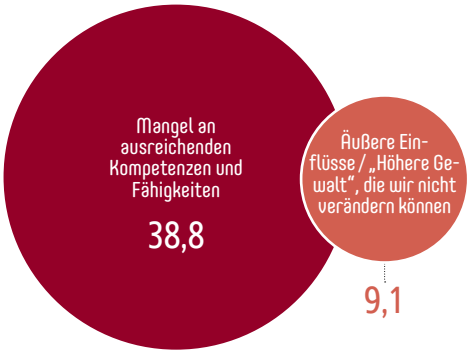
IT-Investitionen fürs Business

Um bestehende Geschäftsmodelle auszubauen oder zu verbessern, werden **zwei Drittel** der Unternehmen ihre **dafür nötigen IT-Investitionen** erhöhen. Deutlich **mehr als die Hälfte** der Befragten will auch mittels IT-Gelder ganz neue Geschäftsmodelle einführen.



Es mangelt an Know-how

Fragt man nach **Widerständen und Hindernissen**, die die digitalen Ambitionen ihrer Unternehmen behindern, antworten 39 Prozent der CIOs zuerst mit dem **Mangel an ausreichenden Kompetenzen und Fähigkeiten**. **Äußere Einflüsse / „Höhere Gewalt“** (wie beispielsweise eine Pandemie) wird indes kaum als Hindernis gesehen.



Grundgesamtheit:
Oberste (IT-)Verantwortliche von Unternehmen in der D-A-CH-Region: strategische (IT-)Entscheider im C-Level-Bereich und in den Fachbereichen (LoBs), IT-Entscheider & IT-Spezialisten aus dem IT-Bereich

Gesamtstichprobe:
276 abgeschlossene und qualifizierte Interviews

Untersuchungszeitraum:
17. November bis 10. Dezember 2020

Methode:
Online-Umfrage (CAWI)

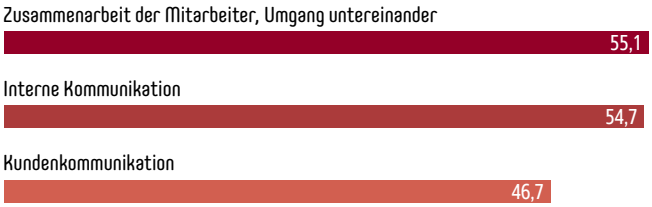
CIO-Agenda 2021

Alle Angaben in Prozent

Umgang und Kommunikation verändern sich

Die Pandemie beeinflusst die Menschen noch einmal deutlich stärker, als sie das mit den Unternehmensprozessen tut.

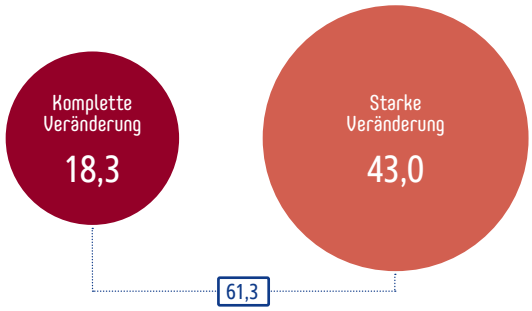
Was die Pandemie im Unternehmen am stärksten verändert:



Die Zukunft heißt Data Analytics

Mehr als sechs von zehn Unternehmen schätzt, dass Data Analytics / Big Data ihre Geschäftsmodelle langfristig – binnen fünf bis zehn Jahren – verändern werden.

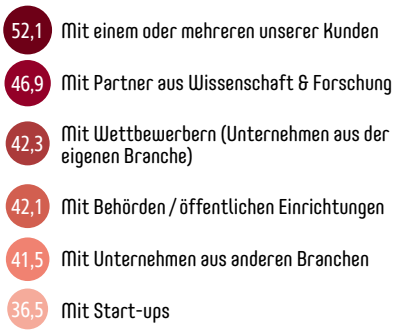
Veränderungseinfluss durch Data Analytics / Big Data binnen der kommenden drei Jahre:



Wenig Kooperation mit Start-ups

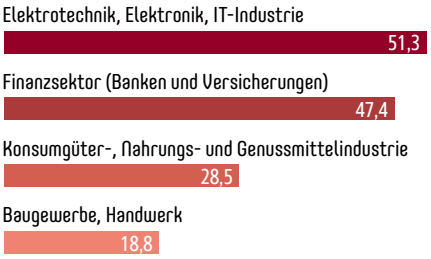
Unternehmen arbeiten bei Digitalisierungsprojekten vor allem **mit eigenen Kunden** oder Industriepartnern zusammen. Selbst Wettbewerber sind ihnen oft lieber als Start-ups.

Bestehende Partnerschaft ...



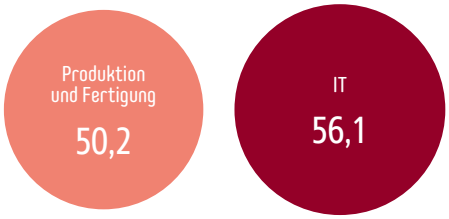
IT-Industrie und Banken / Versicherungen mit den größten Veränderungen

Die CIOs schätzen vor allem die Branchen Elektronik / IT und Banken / Versicherungen als **stark vom digitalen Wandel betroffen** ein.



Produktion, IT und Service wandeln sich stark

Fragt man nach den **einzelnen Unternehmensbereichen**, die vom digitalen Wandel **am stärksten beeinflusst und verändert** werden, so sehen die befragten CIOs hier ihren eigenen Bereich, **die IT**, deutlich betroffen.



CIO-Agenda 2021 – Executive Summary

Die Ergebnisse der „CIO-Agenda 2021" stehen zum Teil natürlich unter dem Eindruck der Coronapandemie. So shiften viele Unternehmen ihre Budgets, die sie vor Jahresfrist noch am ehesten in Cloud-Projekte gesteckt hätten, in Infrastrukturthemen um, um ihre bestehenden Systeme stabiler und sicherer zu machen. Insgesamt sorgt die Pandemie dafür, dass die digitale Transformation deutlich schneller voranschreitet und IT-Budgets oftmals signifikant erhöht werden. Letzteres ist auch deshalb nötig, weil neue Geschäftsmodelle entwickelt werden sollen oder gar müssen. Gerade der Bereich Data Analytics scheint hier langfristig ein aussichtsreicher Kandidat zu sein – die Zusammenarbeit mit Startups eher weniger. Wenig getan im Vergleich zum Vorjahr hat sich bei den Widerständen und Hindernissen, die die digitalen Ambitionen der Unternehmen einbremsen – hier schlägt insbesondere der Fachkräftemangel weiterhin voll durch.

Fragt man nach den grundsätzlichen Einflüssen der Pandemie in den Unternehmen, so sind es vor allem der Umgang der Mitarbeiter untereinander sowie die interne wie externe Kommunikation, die nach dem Eindruck der CIOs und IT-Leiter eine Veränderung erfahren haben – viel stärker noch als eher „technokratische" Themen wie (Vertriebs-)Prozesse oder Finanzen. Ihre eigenen Langfristaufgaben sehen die Befragten vornehmlich im innovativen Bereich – beispielsweise neue digitale Plattformen und Betriebsmodelle zu schaffen und zu betreiben sowie für mehr Agilität und Geschwindigkeit im Unternehmen zu sorgen. Die Aufrechterhaltung der bestehenden Infrastruktur zählte gerade im vergangenen Jahr zwar zu den Kernaufgaben der IT-Teams, ist aber nach einhelliger Meinung ein Zustand von nur kurzer Dauer. Spätestens wenn die Pandemie komplett überwunden ist, werden die innovativen Ärmel wieder richtig hochgekrempelt.

Studienpartner stellen sich vor

PlusServer,
Arvato Systems, Ergon Informatik/Airlock,
TÜV SÜD, uniscon

Cloud Security 2021

plusserver

plusserver managt Ihre Cloud Security

„Mit dem Plus an Sicherheit in die Cloud“

Was macht plusserver so erfolgreich?

Als deutscher Spezialist für Cloud Services unterstützen wir Unternehmen dabei, ihre digitalen Herausforderungen zu lösen. Dabei kümmern wir uns nicht nur um die Bereitstellung einer sicheren Infrastruktur, sondern bieten vollumfängliche Sicherheitslösungen, die individuell auf das jeweilige Unternehmen abgestimmt sind.

Wie gewährleistet plusserver Sicherheit und Datenschutz?

Auf Wunsch können unsere Kunden Cloud-Services ausschließlich aus unseren hochsicheren und zertifizierten Rechenzentren in Deutschland beziehen. Als Unternehmen mit Sitz in Deutschland unterliegen wir deutschem Recht und erfüllen auch die Anforderungen der EU-Datenschutz-Grundverordnung (DSGVO). Zusätzlich bieten wir mit plussecurity ganzheitliche Security-Konzepte sowie einzelne Lösungen wie DDoS-Mitigation und Firewalls, um Daten in der Cloud gegen Angriffe aus dem Internet bestmöglich abzusichern.

Warum sollten Kunden plusserver für ihre Cloud Security in Betracht ziehen?

Wir unterstützen unsere Kunden ganzheitlich auf ihrem Weg in die Cloud. Dazu gehört neben Implementierung, Monitoring und 24/7 Support auf Wunsch die Erstellung eines Sicherheitskonzepts. Um etwa eine Multi-Cloud-Lösung effizient im Unternehmen einzusetzen, braucht es eine umfassende Sicht und Kontrolle auf die Cloud-Security-Services und die IT-Infrastruktur. Durch unseren übergreifenden Security-Layer und zusammen mit führenden Partnern gewährleisten wir umfassenden Schutz und halten Aufwände und Kosten unserer Kunden gering.

plussecurity: Wir managen Ihre Cloud Security

Wir möchten, dass Ihre geschäftskritischen Prozesse jederzeit mit hoher Performance verfügbar und Ihre wertvollen Daten stets gut geschützt sind. Daher bietet plusserver ergänzend zu seinen Cloud-Lösungen umfassende Services rund um das Thema Sicherheit und Cybersecurity an. Von der Schwachstellenerkennung über DDoS, DNS- und Malwareschutz sowie Cloud Firewalls bis hin zur effizienten Echtzeitüberwachung.

Unsere Services für Ihre Datensicherheit:

- Führende Akamai DDoS-Mitigation-Lösungen
- Voll automatisierte Web Application Firewalls (WAF)
- Sicherer Applikationszugriff (Cloud/On-Premises)
- Malware- und Phishing-Schutz aus der Cloud
- Sichere IT-Infrastruktur durch 24/7 Überwachung und Analyse von Bedrohungen sowie Echtzeit-Reaktion durch Experten von Kudelski Security
- Container Security

Mit Sicherheit in der pluscloud

Die datensouveräne und DSGVO-konforme pluscloud ist Teil der modularen Multi-Cloud-Plattform plus.io. Die pluscloud ist in deutschen Rechenzentren zu Hause und bildet eine sichere Basis. Unternehmen mit sensiblen Daten und gesteigertem Interesse an Sicherheit finden hier ihre passende Sicherheitslösung inklusive der Anpassung an den spezifischen IT-Systembedarf, wie beispielsweise die Koordination vordefinierter Eskalationsketten. Bei Bedarf sorgt zudem eine Site-to-Site-Verbindung für Georedundanz und damit für Ausfallsicherheit von Anwendungen. Generell garantieren wir unseren Kunden in unserem Service Level Agreement eine Verfügbarkeit unserer Rechenzentren sowie des Core-Netzwerks von 99,99 Prozent im Jahresmittel.

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

Cyber Care
by Arvato Systems

Arvato Systems: Cyber Care ist mehr als SOC

IT-Security ist eine Frage des Vertrauens

IT-Sicherheit braucht Top-Technologie. Ebenso wichtig ist aber die enge und vertrauensvolle Zusammenarbeit von Kunden und Dienstleistern. Genau darauf setzt Arvato Systems.

Als international agierender IT-Spezialist unterstützt Arvato Systems namhafte Unternehmen bei der Digitalen Transformation. Ein Team von rund 3.000 Mitarbeiterinnen und Mitarbeitern entwickelt innovative IT-Lösungen, bringt Kunden in die Cloud, integriert digitale Prozesse und übernimmt den Betrieb sowie die Betreuung von IT-Systemen. Wir bieten umfassende IT-Lösungen für Branchen wie Handel, Medien, Gesundheitswesen sowie Energie- und Versorgungswirtschaft. Dabei setzen wir auf Kompetenz in Themen wie KI und Cloud Computing, Know-how in vielen starken Technologien, ein ausgeprägtes Partner-Ökosystem und eine große Bandbreite an Infrastructure Services wie beispielsweise Managed Services sowie ein darauf aufbauendes Application Management. All das kombinieren wir mit umfassendem IT-Security Know-how und unserem Cyber Care Angebot.

„Wir haben den Anspruch, ein verlässlicher Partner für unsere Kunden zu sein. Wir sind der Meinung: Nur in einer stabilen Partnerschaft können Cyber-Security-Konzepte nachhaltig erfolgreich sein."

Arne Wöhler
Head of Business Consulting and Development
Cyber Security bei Arvato Systems

Schutz für wertvolle Assets

Unsere Kunden können sich darauf verlassen, dass ihre Daten und Anwendungen in unseren Rechenzentren durch modernste Security-Lösungen geschützt werden. Dabei gehen die Arvato Systems Security Services mit Themen wie IT Security, Risk Management und Compliance weit über die physikalische Sicherung von IT Systemen hinaus. Es stehen umfassende IT Security Dienste zur Verfügung, um Informations- und Kommunikationsinhalte vor Missbrauch und unerlaubtem Zugriff Dritter zu schützen. Ergänzend bieten wir auch ein umfangreiches Security Consulting.

Ein Komplettpaket gegen Cyber-Attacken

Das Arvato Systems Cyber Care Angebot ist ein Komplettpaket gegen Cyber-Attacken und hilft unseren Kunden dabei, sich in punkto IT-Sicherheit professionell aufzustellen. Bei Arvato Systems gehen wir also weit hinaus über das klassische Kernangebot eines Security Operation Centers (SOC). Das Konzept von Arvato Systems Cyber Care beinhaltet Schutz durch Vorbeugung (Prevention), Systemüberwachung und Entdeckung konkreter Angriffe (Detection) und professionelle Reaktion auf diese Angriffe (Response). Dabei besteht stets die Wahl: Ob Komplettpaket oder einzelner Service - wir richten uns nach spezifischen Kundenbedürfnissen.

Managed Security Services

Das gilt auch für unsere Managed Security Services. So sorgen wir zum Beispiel mit Microsoft 365 Defender für den Schutz anwenderbezogener Assets wie Rechner, Nutzerprofile, Office-Anwendungen und Apps. Oder wir schützen mit dem Microsoft Azure Defender Server, Infrastruktur und Clouds für unsere Kunden. Dabei legen wir unsere eigenen Lösungen und Services über die vorhandenen Tools von Microsoft. So decken wir individuelle Anforderungen optimal ab: Wir konfigurieren mächtige Standard-Security-Lösungen nach bewährten Best Practices und passen sie unternehmensspezifisch an. Indem wir die dynamische Bedrohungslage fortlaufend monitoren, behalten wir den Secure Score jederzeit im Blick und sorgen für ein Höchstmaß an Cyber Security.

arvato
BERTELSMANN
Arvato Systems

Arvato Systems
An der Autobahn 200, 33333 Gütersloh
Telefon: 05241-80 70770
E-Mail: CyberCare@arvato-systems.de
Web: arvato-systems.de/security

INTEGRIERTE LÖSUNGEN STATT SPOT SOLUTIONS

Warum „gemeinsam stärker" auch in der IT-Security gilt

Die Anforderungen an die IT-Security steigen ständig. Darum sind heute integrierte Lösungen gefragt, die beides können: maximale Sicherheit gewährleisten und agile Entwicklungsprozesse ermöglichen.

Aus Ihrer Sicht als Security-Experte – was sind die großen Sicherheitsthemen, mit denen Unternehmen heute konfrontiert werden?

Vereinfach lässt sich sagen: Im Zuge der Digitalisierung werden Prozesse agiler. Damit steigt aber auch die Komplexität. Und mit dieser zunehmenden Komplexität muss die IT-Security heute umgehen können – sowohl aus sicherheitstechnischen als auch aus unternehmerischen Gründen.

Welche sind die sicherheitstechnischen Herausforderungen, die Sie ansprechen?

Immer mehr Applikationen, APIs, Microservices und Identitäten werden über die Grenzen der Unternehmens-IT hinaus exponiert. Darum reichen klassische WAF-Technologien, die für den Schutz von traditionellen HTML-Seiten gebaut wurden, heute einfach nicht mehr aus. Denn WAFs müssen heute auch APIs schützen, API Gateways müssen Web Security beherrschen, und APIs brauchen ein kohärentes Identity- und Access-Management.

Die Lösung ist also, statt einer WAF einfach einen API Gateway zu kaufen?

Ganz so einfach ist es leider nicht, denn traditionelle API Gateways können moderne Single-Page Applications (SPA) nur unvollständig absichern. Der Grund hierfür: Herkömmliche Gateways sind mit SOAP Webservices groß geworden, die Enterprise-Service-Busse benötigen und im Korsett komplexer Standards gefangen sind. Diese starre Struktur passt aber schlecht zur schönen neuen REST-Welt, die durch Agilität und Leichtgewichtigkeit geprägt ist.

Welche Lösung passt denn am besten zur REST-Welt?

Moderne APIs werden heute von ganz unterschiedlichen Clients genutzt – von herkömmlichen Webapplikationen, SPAs, Smartphone Apps, „Things" und anderen Softwaresystemen. Und diese Clients sind dort exponiert, wo heute das Leben spielt – im wilden, heterogenen Internet. Darum braucht es für APIs Schutzkonzepte, die WAFs schon lange bieten. Und es braucht ein leistungsstarkes Identity- und Access-Management, da immer mehre interne und externe User auf Applikationen zugreifen.

Das heißt ganz konkret?

Grundsätzlich gibt es zwei Lösungsansätze: Entweder man setzt auf Spot Solutions – also auf singuläre Lösungen für singuläre Herausforderungen. Oder man baut auf das, was immer mehr Experten bevorzugen: auf kohärente, integrierte Systeme.

„Mehr IT- und Investitions-Sicherheit in einem – der Secure Access Hub ist heute die effizienteste Lösung für die IT-Security."

ROMAN HUGELSHOFER,
Managing Director Application Security, Ergon Informatik AG

Integrierte Systeme – das klingt natürlich gut. Doch was sind die Vorteile?

Bildlich gesprochen werden bei integrierten Systemen vormals lose Enden zuverlässig miteinander verknüpft. So entsteht ein dichtes Sicherheitsnetz, das Unternehmen vor den aktuell größten Gefahren schützt: vor Angriffen auf Applikationen und Identitäten. Deshalb setzen wir bei unserem Secure Access Hub auf die drei Komponenten WAF, API Gateway und Customer IAM mit integrierter Zwei-Faktor-Authentifizierung aus einer Hand.

Neben dem Schutz von APIs haben Sie das Access-Management erwähnt. Warum ist dieser Aspekt so wichtig?

Neben dem Filtern von Inhalten über WAF und API Security wird die Verwaltung und Überprüfung von Identitäten und deren Berechtigungen heute immer wichtiger. Denn erstens greifen immer mehr externe Identitäten auf APIs zu. Und zweitens: Die Ansprüche an einen reibungslosen Authentisierungs-Flow werden immer größer, und Features wie Social Logins, Single Sign-on oder User Self-Services werden fast schon als Selbstverständlichkeit erwartet. Die Lösung für diese komplexen Herausforderungen sind Customer-IAM-Systeme (cIAM), da sie eine nahtlose User Experience garantieren und sich einfach skalieren lassen. Ein weiterer wichtiger Punkt: Mit cIAM-Lösungen lassen sich Zwei-Faktor-Authentifizierungen (2FA) implementieren – und an diesen kommen viele Unternehmen schon aus regulatorischen Gründen kaum mehr vorbei.

Sicherheitstechnische Anforderungen sind das eine, unternehmerischen Anforderungen das andere. Welche Benefits kann ein moderner Secure Access Hub hier bieten?

Die einfache Antwort: Intelligente und standardisierte Systeme lassen sich vorgelagert und zentralisiert über alle Applikationen und APIs hinweg an neue Aufgaben anpassen. So wird eine agile und flexible Softwareentwicklung ermöglicht, die eine schnelle Time-to-Market sicherstellt – mit allen Wettbewerbsvorteilen, die sich so für Unternehmen eröffnen. Zusätzlich ergeben sich geringere Betriebskosten oder auch eine effizientere Erfüllung von Compliance-Anforderungen.

Und die komplexe Antwort?

Egal ob von DevOps-Prozessen gesprochen wird oder der Einsatz von flexiblen Containern gefragt ist – der grundsätzliche Vorteil von integrierten Sicherheitslösungen ist derselbe: Sie basieren auf kohärenten Frameworks, sodass der Sicherheitsaspekt durchgängig in die Applikationsentwicklung integriert ist. Unternehmen profitieren so von All-in-One-Lösungen – z.B. für Authentisierung, Registrierung, die Anbindung von Directories, das Login sowie Single Sign-on und User Self-Services.

Das klingt ja alles sehr gut. Doch sehr gut – das heißt doch auch sehr teuer?

Unsere klare Antwort: Nein! Denn eine Vollkostenrechnung zeigt, dass ein integrierter Ansatz zu einem wesentlich tieferen TCO führt. Zudem steigern integrierte Ansätze nicht nur die IT-, sondern auch die Zukunfts- und Investitionssicherheit. So gesehen ermöglicht ein Secure Access Hub eine klassische Win-win-Situation – sowohl für die IT als auch für das Business.

AIRLOCK®
SECURE ACCESS HUB

Ergon Informatik AG
Merkurstraße 43, CH-8032 Zürich
Telefon: +41 44 268 89 00
E-Mail: info@ergon.ch

IT-Sicherheit von den Sicherheitsprofis

Seit 150 Jahren macht TÜV SÜD Technik sicher und garantiert Neutralität, Objektivität und Verlässlichkeit. Wir unterstützen Unternehmen dabei, die Chancen der Digitalisierung zu nutzen und ihre Risiken zu beherrschen. Als weltweit tätige Test-, Inspektions- und Zertifizierungsgesellschaft kennen wir die regulatorischen Anforderungen ebenso wie die aktuelle Bedrohungslandschaft. IT- und Informationssicherheit, Datensicherheit und Datenschutz zählen dabei zu unserer Kernkompetenz.

Wer die Chancen der Cloud nutzen will, muss sich auch mit ihren möglichen Sicherheitsrisiken auseinandersetzen – und entsprechende Vorkehrungen treffen. Das reicht von der Definition der Cloud-Strategie über die Ausgestaltung der Umsetzung bis hin zum laufenden Betrieb. Wer den „Weg in die Cloud“ antreten will, für den bietet die Norm für Informationssicherheits-Managementsysteme ISO / IEC 27001 optimale Orientierung; sie leitet in diesem Zusammenhang zu allen wichtigen Fragen, die Unternehmen sich vor „Reisebeginn“ beantworten müssen. Doch damit nicht genug, sie hilft auch bei der im Zweifel entscheidenden Providerauswahl. Denn mit einer entsprechenden Zertifizierung demonstrieren Cloudanbieter, dass sie dem Thema IT-Sicherheit eine hohe Bedeutung beimessen. Die ISO / IEC 27001 spielt auch im Cloudumfeld die zentrale Rolle.

Wir bieten ein breites Portfolio an IT-Sicherheitsservices und leisten damit einen wichtigen Beitrag für eine IT-Infrastruktur, auf die sich Kunden, Partner und Mitarbeiter unserer Kunden verlassen können. Mit unseren Zertifizierungen der IT-Sicherheit legen Unternehmen ein belastbares Fundament für eine sichere und verlässliche IT und langfristiges Vertrauen ihrer Kunden, Lieferanten und Mitarbeiter.

100-prozentige Sicherheit gibt es nicht: IT-Sicherheit ist ein permanenter und kontinuierlicher Prozess. Wir unterstützen Unternehmen dabei als neutraler und herstellerunabhängiger Partner. IT-Sicherheit muss von Beginn an mitgedacht, umgesetzt und kontinuierlich verbessert werden. Durch unser Engagement als Mitglied der Charter of Trust, der 2018 von Siemens und weiteren Industriepartnern initiierten weltweiten Kooperation für Cybersicherheit, sind wir an der Gestaltung von Industrieanforderungen und -standards von Anfang an beteiligt.

UNSER PORTFOLIO UMFASST UNTER ANDEREM:

- Zertifizierung Ihres Informationssicherheits-Managementsystems nach ISO / IEC 27001, der international führenden Norm für Informationssicherheits-Managementsysteme
- Zertifizierung Ihres (IT) Service Managements nach ISO / IEC 20000-1 – für hohe Qualität und einen effizienten Einsatz von Zeit und Ressourcen
- Zertifizierung nach IT-Sicherheitskatalog – für Betreiber von Strom- und Gasnetzen entsprechend den Vorgaben der Bundesnetzagentur
- KRITIS – Nachweis über angemessene IT-Sicherheit nach §8a BSIG für Betreiber kritischer Infrastrukturen (z.B. Gesundheit, Finanz- und Versicherungswesen, Energie u.a.)
- TISAX® – der zentrale Nachweis für IT-Sicherheit in der Automobilbranche, mit dem Lieferanten und Dienstleister erheblich Zeit und Kosten sparen

Eine detaillierte Übersicht des IT-Sicherheit Portfolios der TÜV SÜD Management Service gibt es unter **www.tuvsud.com/cyber-security-zertifizierungen**

TÜV SÜD Management Service GmbH
Marcello Walz, Global Business Line Manager IT
marcello.walz@tuvsud.com
Ridlerstraße 57
80339 München
Telefon +49 89 5791-2500
www.tuvsud.com/cyber-security-zertifizierungen

uniscon GmbH – Ihr Trusted Cloud Plattform Provider

Hochsichere Business-Cloud-Lösungen für sensible Daten und Anwendungen

Ob hochsicherer Datentransfer oder Hosting von SaaS-Angeboten: Die Lösungen von uniscon bieten höchste Sicherheit für vertrauliche Daten und Applikationen auf Basis der international patentierten *Sealed Cloud Technologie*.

Die uniscon GmbH ist ein Münchner Anbieter von DSGVO-konformen Cloud- und Datenraum-Lösungen für Unternehmen und einer der führenden Secure-Cloud-Provider in Europa. Die Produkte von uniscon greifen Hand in Hand: uniscons Business-Cloud *idgard®* sichert die digitale Kommunikation und den Datenaustausch mit Partnern, Kunden und Kollegen auf höchstem Niveau ab und vereinfacht sie darüber hinaus: Agenturen und Makler nutzen den web-basierten File-Sharing-Dienst für den Austausch großer Datenmengen, Wirtschaftsprüfer und Berater setzen *idgard®* als virtuellen Projekt- und Datenraum mit ihren Klienten ein, und Industriebetriebe schätzen die anwenderfreundliche Cloud als professionelles Tool für die Vorstandskommunikation. Apps für iOS und Android ermöglichen außerdem den sicheren mobilen Datenzugriff.

***idgard®* erfüllt höchste Anforderungen an Sicherheit & Datenschutz – das wissen auch uniscons Kunden:** Mehr als 1.250 Unternehmen vertrauen bereits auf den Dienst, darunter IT- und Kommunikationsanbieter (z.B. T-Systems), Unternehmensberatungen (u.a. Baker Tilly) sowie diverse Anbieter von Finanzdienstleistungen (z.B. Sparkassen und Volksbanken). Auch Behörden sind überzeugt: Das IT-Dienstleistungszentrum des Freistaats Bayern nutzt für den internen und externen Datenaustausch die *SecureBox Bayern*, die ihrerseits auf *idgard®* basiert.

Nicht nur sensible Daten, sondern auch Applikationen mit höchstem Anspruch an IT-Sicherheit finden in der Cloud eine vertrauenswürdige Heimat – auf uniscons *sealed platform®*. Die einzigartige Zero-Trust-Architektur schützt Daten und Anwendungen vor unbefugten Zugriffen, sodass selbst privilegierter Zugriff ausgeschlossen ist. Durch die Unterstützung von Docker und Kubernetes kann nahezu jede Anwendung das extrem hohe Sicherheitsniveau der *sealed platform®* für sich nutzen.

Was uniscons Lösungen gemeinsam haben? Sie werden alle nach dem Grundsatz „Privacy by Design" entwickelt und basieren auf der international patentierten *Sealed Cloud Technologie*. Diese stellt mit einer Reihe innovativer und ineinandergreifender technischer Maßnahmen sicher, dass jeglicher Zugriff auf unverschlüsselte Serverdaten technisch ausgeschlossen ist. Durch die hermetische Versiegelung der Infrastruktur wird ein vertrauliches Rechenzentrum geschaffen, das eine wesentlich höhere Anwendungs- und Datensicherheit gewährleistet als herkömmliche Systeme. Im Gegensatz zu anderen Cloud-Lösungen hat hier niemand, auch nicht der Betreiber der Cloud, Datenzugriff.

Dieses einzigartig hohe Sicherheitsniveau gewährleistet die Einhaltung selbst strenger Datenschutzbestimmungen. Die Dienste, die auf der *Sealed Cloud Technologie* basieren

- sind DSGVO-konform und gewähren die Einhaltung des EU-Datenschutzrechts bei der Verarbeitung personenbezogener Daten
- schützen Inhalte und Metadaten
- eignen sich auch für Daten, die der beruflichen oder behördlichen Geheimhaltung unterliegen.

uniscon wurde 2009 gegründet und ist seit 2017 Teil der Digitalisierungsstrategie von TÜV SÜD. TÜV SÜD ist ein weltweit führendes technisches Dienstleistungsunternehmen mit über 150 Jahren branchenspezifischer Erfahrung und heute mehr als 24.000 Mitarbeitern an etwa 1.000 Standorten in 54 Ländern. In diesem starken Verbund kann uniscon die Entwicklung seiner Technologie weiter vorantreiben und ist in der Lage, mit der *Sealed Cloud* und ihren Produkten internationale Großprojekte in den Bereichen IoT, SaaS und Industrie 4.0 zuverlässig zu realisieren.

Weitere Informationen zum Unternehmen und den Lösungen finden Sie unter **www.idgard.de** und **www.uniscon.com**.

uniscon GmbH
Ridlerstr. 57 (Newton)
80339 München
Germany
contact@uniscon.de

uniscon
SEALED CLOUD TECHNOLOGIES

A member of TÜV SÜD

Glossar

Definition und Erläuterung
der wichtigsten Fachbegriffe
zum Studienthema

Cloud Security 2021

Advanced Persistent Threat (APT)
Englisch für „fortgeschrittene andauernde Bedrohung“: ein komplexer, zielgerichteter, effektiver Angriff auf kritische IT-Infrastrukturen und vertrauliche Daten von Behörden, Groß- und Mittelstandsunternehmen aller Branchen, welche aufgrund ihres Technologievorsprungs potenzielle Opfer darstellen oder als Sprungbrett auf solche Opfer dienen können. Das Ziel eines APT ist es, dass die Angreifer möglichst lange handlungsfähig bleiben, um über einen längeren Zeitraum sensible Informationen auszuspähen oder anderweitig Schaden anzurichten, ohne dass der Angegriffene davon etwas merkt.

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Deutsche Bundesoberbehörde im Geschäftsbereich des Bundesministeriums des Innern mit Sitz in Bonn, die für Fragen der IT-Sicherheit zuständig ist.

Cloud Access Security Broker (CASB)
Service oder Anwendung, die Cloud-Applikationen absichert. Kann lokal installiert oder ebenfalls in der Cloud gehostet sein. Befindet sich zwischen Cloud-Service-Benutzern und Cloud-Anwendungen, überwacht alle Aktivitäten und setzt Sicherheitsrichtlinien durch.

Cloud Security Posture Management (CSPM)
Technologie, um Risiken in Cloud-Infrastrukturen – egal ob Infrastructure as a Service (IaaS), Software as a Service (SaaS) oder Platform as a Service (PaaS) – automatisiert zu identifizieren und zu beheben. CSPM-Tools visualisieren und bewerten Cloud-Risiken, helfen bei der Reaktion auf Vorfälle, überwachen Compliance-Richtlinien und können auch für die Integration von DevOps verwendet werden. Zudem unterstützen sie dabei, Best Practices für die Cloud-Sicherheit einheitlich auf hybride, Multicloud- und Container-Umgebungen anzuwenden.

EU Cloud Scheme (EUCS)
Sich noch im Abstimmungsstadium befindliches Zertifizierungs-Framework, das die Cybersicherheit von Cloud-Diensten EU-weit sicherstellen soll. Der Entwurf des EUCS-Kandidatenschemas (European Cybersecurity Certification Scheme for Cloud Services) wurde Ende 2020 durch eine Arbeitsgruppe der ENISA (Agentur der Europäischen Union für Cybersicherheit) veröffentlicht.

EU-DSGVO
Die EU-Datenschutz-Grundverordnung (Englisch: GDPR für „General Data Protection Regulation“) ist eine Verordnung der Europäischen Union, mit der die Regeln zur Verarbeitung personenbezogener Daten durch die meisten Datenverarbeiter, sowohl private wie öffentliche, EU-weit vereinheitlicht werden. Dadurch soll einerseits der Schutz personenbezogener Daten innerhalb der Europäischen Union sichergestellt, und auch andererseits der freie Datenverkehr innerhalb des Europäischen Binnenmarktes gewährleistet werden.

Intrusion Detection System (IDS)
System zur Erkennung von Angriffen, die gegen ein Computersystem oder Rechnernetz gerichtet sind. Das IDS kann eine Firewall ergänzen oder auch direkt auf dem zu überwachenden Computersystem laufen und so die Sicherheit von Netzwerken und Computersystemen erhöhen. Erkannte Angriffe werden meistens in Log-Dateien zusammengetragen und dem Benutzer oder Administrator mitgeteilt.

Intrusion Prevention System (IPS)
System zur Erkennung und automatisierten Verhinderung von Angriffen, die gegen ein Computersystem oder Rechnernetz gerichtet sind. In Abgrenzung zum IDS, das erkannte Angriffe nur protokolliert, stellt ein IPS Funktionen bereit, um einen entdeckten Angriff aktiv abwehren zu können.

ISO / IEC 20000-1
International anerkannte Norm zum IT Service Management (ITSM). Eine Zertifizierung ist für Organisationseinheiten möglich. Ein erworbenes Zertifikat muss alle drei Jahre erneuert werden.

ISO / IEC 27001
Internationale Norm, die die Anforderungen für Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten Informationssicherheits-Managementsystems unter Berücksichtigung des Kontexts einer Organisation spezifiziert.

ISO / IEC 27701
Datenschutzerweiterung der ISO / IEC 27001. Ziel des Standards ist, das bestehende Information Security Management System (ISMS) um zusätzliche Anforderungen zu erweitern, um ein Privacy Information Management System (PIMS) einzurichten, zu implementieren, aufrechtzuerhalten und kontinuierlich zu verbessern.

ISO / IEC 27017
Internationaler Sicherheitsstandard, der für Anbieter und Nutzer von Cloud-Diensten entwickelt wurde, um eine sichere cloudbasierte Umgebung zu schaffen und das Risiko von Sicherheitsproblemen zu reduzieren.

ISO / IEC 27018
Internationaler Sicherheitsstandard, der Cloud-Service-Anbieter bei der Verarbeitung von personenbezogenen Daten, der Risikobewertung und der Implementierung von Kontrollen zum Schutz personenbezogener Daten unterstützen soll. Es war der erste internationale Standard über den Datenschutz bei Cloud-Computing-Diensten, der von der Industrie gefördert wurde.

Managed Security Service Provider (MSSP)
Dienstleister, der Netzwerksicherheitsdienste bereitstellt und meist auf Basis eines Outsourcing-Vertrags auch betreibt.

On-Premises / On-Prem
Lokales Nutzungs- und Lizenzmodell für serverbasierte Computerprogramme. Der Lizenznehmer erwirbt oder mietet Software und betreibt diese in eigener Verantwortung auf eigener Hardware beziehungsweise in einem eigenen Rechenzentrum oder auf gemieteten Servern in einem fremden Rechenzentrum.

Security by Default
Bezeichnung für Software-Konfigurationseinstellungen, die in ihrem ursprünglichen beziehungsweise standardmäßigen Zustand (Default-Einstellungen) die höchstmögliche Sicherheit gewährleisten. Jegliche Veränderung / Anpassung dieser Einstellungen durch den Nutzer oder Administrator der Software reduzieren die Sicherheit.

Security by Design
Bezeichnung für ein Leitbild in der Softwareentwicklung, bei dem die Sicherheit von Beginn an mit einbezogen wird. Unter anderem werden schon zu Beginn eines Softwareentwurfs solche Sicherheitstaktiken und -muster ausgewählt und integriert, die am besten geeignet sind, später ein sicheres Produkt zu gewährleisten.

Security Operations Center (SOC)
Sicherheitsleitstelle, die sich um den Schutz der IT-Infrastruktur eines Unternehmens oder einer Organisation kümmert. Um diese Aufgabe leisten zu können, integriert, überwacht und analysiert das SOC alle sicherheitsrelevanten Systeme wie Unternehmensnetzwerke, Server, Arbeitsplatzrechner oder Internetservices. Unter anderem werden die Log-Dateien der einzelnen Systeme gesammelt, analysiert und nach Auffälligkeiten untersucht.

Studiendesign

Alle wissenswerten Informationen
zu Aufbau, Methodik
und Stichprobe der Studie

Cloud Security 2021

Studienpartner

Gold-Partner:

PlusServer GmbH
Hohenzollernring 72
50672 Köln
Telefon: +49 (0) 2203 1045–3500
E-Mail: beratung@plusserver.com
Web: www.plusserver.com

Silber-Partner:

Arvato Systems GmbH
An der Autobahn 200
33333 Gütersloh
Telefon: +49 (0) 5241 80–70770
E-Mail: CyberCare@arvato-systems.de
Web: arvato-systems.de/security

Ergon Informatik AG
Merkurstrasse 43
CH-8032 Zürich
Telefon: +41 (0) 44 268–8700
E-Mail: info@airlock.com
Web: www.airlock.com

TÜV SÜD Management Service GmbH
Ridlerstr. 57
80339 München
Telefon +49 (0) 89 5791–2500
E-Mail: ms-anfragen@tuvsud.com
Web: www.tuvsud.com/tms

uniscon GmbH
Ridlerstr. 57 (Newton)
80339 München
Web: www.idgard.de,
www.uniscon.com

Gesamtstudienleitung

Matthias Teichmann
Director Research
IDG Research Services
Telefon: +49 (0) 89 36086–131
mteichmann@idg.de

Projektmanagement

Simon Hülsbömer
Senior Project Manager
IDG Research Services
Telefon: +49 (0) 89 36086–177
shuelsboemer@idg.de

Armin Rozsa
Junior Project Manager
IDG Research Services
Telefon: +49 (0) 89 36086–184
arozsa@idg.de

Sandra Baumgarten
Junior Project Manager
IDG Research Services
Telefon: +49 (0) 89 36086–116
sbaumgarten@idg.de

Sales-Team

Regina Hermann
Account Manager Research
IDG Research Services
Telefon: +49 (0) 89 36086–384
rhermann@idg.de

René Krießban
Account Manager Research
IDG Research Services
Telefon: +49 (0) 89 36086–322
rkriessan@idg.de

Bastian Wehner
Account Manager Research
IDG Research Services
Telefon: +49 (0) 89 36086–169
bwehner@idg.de

Impressum

**Studienkonzept/
Fragebogenentwicklung:**
Simon Hülsbömer,
Matthias Teichmann

**Endredaktion/
CvD Studienberichtsband:**
Simon Hülsbömer

Analysen/Kommentierungen:
Oliver Schonschek, Bad Ems

**Kommentierungen
CIO-Agenda 2021:**
Simon Hülsbömer

**Hosting/Koordination
Feldarbeit:**
Armin Rozsa

Artdirector & Grafik:
Daniela Petrini, Reutte

Umschlaggestaltung unter
Verwendung eines Farbfotos von
© shutterstock.com/mipan

Lektorat:
Elke Reinhold, München

Druck:
Peradruck GmbH
Hofmannstr. 7 b
81379 München

Ansprechpartner:
Matthias Teichmann
mteichmann@idg.de

Herausgeber:

IDG Business Media GmbH

Anschrift:
Lyonel-Feininger-Str. 26
80807 München
Telefon: +49 (0) 89 36086–0
Fax: +49 (0) 89 36086–118
E-Mail: info@idg.de

Vertretungsberechtigter:
Jonas Triebel, Geschäftsführer

Registergericht:
Amtsgericht München, HRB 99187

Umsatzsteueridentifikationsnummer:
DE 811 257 800

**Weitere Informationen unter:
www.idg.de**

Studiensteckbrief

Herausgeber	COMPUTERWOCHE, CIO, TecChannel und ChannelPartner
Studienpartner	**Gold-Partner:** PlusServer GmbH **Silber-Partner:** Arvato Systems GmbH Ergon Informatik AG (Airlock) TÜV SÜD AG uniscon GmbH
Grundgesamtheiten	Oberste (IT-)Verantwortliche von Unternehmen in der DACH-Region: strategische (IT-)Entscheider im C-Level-Bereich und den Fachbereichen (LoBs), IT-Entscheider und IT-Spezialisten aus dem IT-Bereich, IT-Security-Spezialisten
Teilnehmergenerierung	Stichprobenziehung in der IT-Entscheider-Datenbank von IDG Business Media sowie zur Erfüllung von Quotenvorgaben über externe Online-Access-Panels; persönliche E-Mail-Einladungen zur Umfrage
Gesamtstichprobe	383 abgeschlossene und qualifizierte Interviews
Untersuchungszeitraum	1. bis 15. März 2021
Methode	Online-Umfrage (CAWI)
Fragebogenentwicklung	IDG Research Services in Abstimmung mit den Studienpartnern
Durchführung	IDG Research Services
Umfragesoftware	Tivian

Stichprobenstatistik

Branchenverteilung*	Land- und Forstwirtschaft, Fischerei, Bergbau	5,7 %
	Energie- und Wasserversorgung	8,4 %
	Chemisch-pharmazeutische Industrie, Life Science	12,5 %
	Medizin- und Labortechnik	9,7 %
	Metallerzeugende und -verarbeitende Industrie	4,7 %
	Maschinen- und Anlagenbau	9,9 %
	Automobilindustrie und Zulieferer	10,4 %
	Herstellung von elektrotechnischen Gütern, IT-Industrie	11,2 %
	Konsumgüter-, Nahrungs- und Genussmittelindustrie	4,7 %
	Medien, Papier- und Druckgewerbe	5,5 %
	Baugewerbe, Handwerk	5,5 %
	Groß- und Einzelhandel (inkl. Online-Handel)	11,0 %
	Banken und Versicherungen	15,1 %
	Transport, Logistik und Verkehr	11,7 %
	Dienstleistungen für Unternehmen	11,2 %
	Hotel- und Gastgewerbe, Tourismus	4,4 %
	Öffentliche Verwaltung, Gebietskörperschaften, Sozialversicherung	7,3 %
	Schule, Universität, Hochschule	3,4 %
	Gesundheits- und Sozialwesen	3,9 %
	Andere Branchengruppe	5,5 %
Unternehmensgröße deutschlandweit	Weniger als 10 Beschäftigte	0,8 %
	10 bis 99 Beschäftigte	5,2 %
	100 bis 499 Beschäftigte	28,7 %
	500 bis 999 Beschäftigte	25,3 %
	1.000 bis 9.999 Beschäftigte	27,4 %
	10.000 Beschäftigte und mehr	12,5 %
Umsatzklasse deutschlandweit	Weniger als 20 Millionen Euro	8,1 %
	20 bis 49 Millionen Euro	14,9 %
	50 bis 99 Millionen Euro	19,1 %
	100 bis 999 Millionen Euro	30,8 %
	1 Milliarde Euro und mehr	19,8 %
	Weiß ich nicht / keine Angabe	7,3 %
Jährliche Aufwendungen in IT-Systeme	Weniger als 1 Million Euro	16,7 %
	1 bis 10 Millionen Euro	34,7 %
	10 bis 100 Millionen Euro	25,3 %
	100 Millionen Euro und mehr	9,9 %
	Keine Angabe / weiß nicht	13,3 %

*** Mehrfachnennungen möglich**

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 Hannover Messe, dmexco 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 Video-Interviews tragen dazu bei, dass die IDG-Studien mittlerweile auf großes Interesse stoßen.

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.

Round Table Moderation

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.

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.

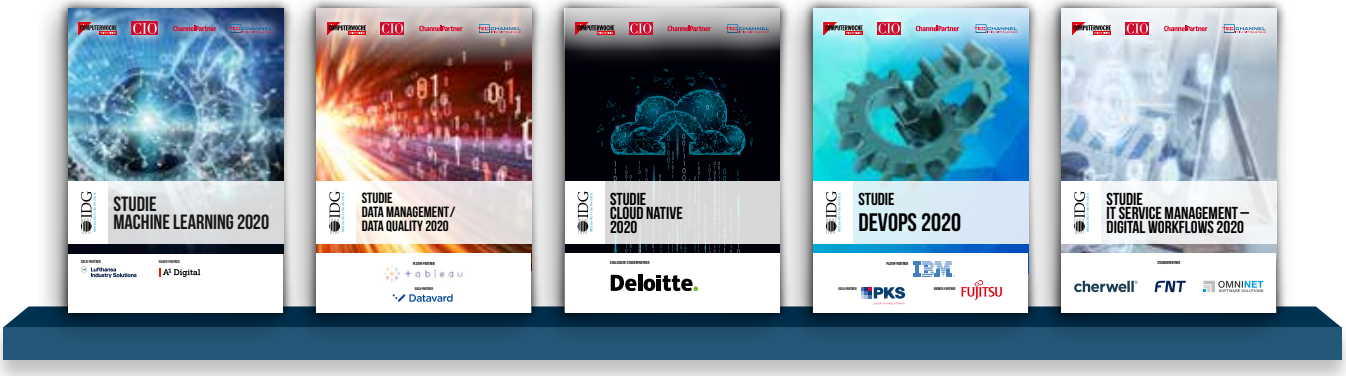
Jürgen Hill:
Chefreporter Future Technologies
Thematisch befasst sich der studierte Diplom-Journalist und Informatiker mit allen Facetten rund um Digitalisierung, KI/ML, IoT und Industrie 4.0.

Protokoll

Iris Lindner, Edling
Oliver Schonschek, Bad Ems
Florian Stocker, München

IDG INSIGHTS INTENT & ENGAGEMENT

Unsere Studienreihe



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

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

Für Rückfragen zu demnächst kommenden Studien:
research@idg.de

Für regelmäßige Infos:
https://www.idg.de/media/research-services/

Oder folgen Sie uns gern auf Twitter: https://twitter.com/IDGResearch_DE

oder auf LinkedIn: https://www.linkedin.com/showcase/idg-research-services-germany/

IDG
RESEARCH SERVICES

plusserver

arvato
BERTELSMANN
Arvato Systems

AIRLOCK®
SECURE ACCESS HUB

TÜV
SÜD

uniscon
SEALED CLOUD TECHNOLOGIES
A member of TÜV SÜD