



Datenhoheit in der Cloud – Voraussetzungen, Potenzial und Herausforderungen

RESEARCH VON:



Matthias Zacher
Senior Consulting Manager
IDC Deutschland



Lynn-Kristin Thorenz
Associate VP Research & Consulting
IDC Deutschland



Elena Georg
Consultant
IDC Deutschland





In diesem White Paper navigieren

Klicken Sie auf den Titel oder die Seitenzahl, um zu den einzelnen Abschnitten zu gelangen.

Einführung	3
Cloud Computing – Modernisierungsfaktor Nummer 1 für die IT	4
Dank Datenhoheit schneller zur umfassenden Digitalisierung	12
Den Weg in die Cloud zielgerichtet optimieren	18
Kunden müssen Anforderungen an Provider klar kommunizieren	23
Fazit und Ausblick	25
Empfehlungen	26
Methodik	27
Interview mit plusserver	28

Einführung

Digitalisierung und Innovation zählen zu den entscheidenden Erfolgsfaktoren im harten globalen Wettbewerb. Technologie und Datenhoheit sind aktuell besonders kritische Faktoren für die effiziente Umsetzung digitaler Geschäftsmodelle und digitaler Services. So wie das Business ist auch die IT kein statisches Element und einem kontinuierlichen Wandel unterworfen. Mit der technologischen Weiterentwicklung der Angebote und den Betriebsmodellen der Cloud Services Provider entstehen neue Herausforderungen und Fragen, die es zu beantworten gilt. Neben der Auswahl der geeigneten Workloads, der Umsetzung von Compliance, Sicherheit und Agilität haben sich Souveränität und Datenhoheit zu zentralen Fragestellungen entwickelt. Der Informationsbedarf ist hoch: Welche Maßnahmen sind erforderlich, um Datenhoheit zu erreichen? Wo liegen die Gemeinsamkeiten und Unterschiede bei Datenhoheit, Datenschutz und Datensicherheit? Was ist die souveräne Cloud? Und nicht zuletzt: Welche Anforderungen stellen Entscheider an Provider mit Blick auf Datenhoheit?

Diese Fragestellungen greift das vorliegende IDC White Paper auf. Es stellt die Datenhoheit als zentrale Anforderung für sicheres Cloud Computing in den Mittelpunkt der Betrachtungen und klärt die Frage, inwieweit die uneingeschränkte Verfügungsgewalt über die Daten der Kern jedes erfolgreichen wirtschaftlichen Handelns ist.

Um diese Punkte näher beleuchten zu können, gilt es zu klären: Wo stehen die Unternehmen bei ihrer IT-Modernisierung und welche Projekte stehen auf der Agenda? Welche Deployment-Modelle bevorzugen Unternehmen in Deutschland? Aus Sicht von IDC ist es ebenfalls erforderlich, sich gezielt mit Workloads, Cloud Security und Nachhaltigkeit zu befassen. Nur dann ist es möglich, einen umfassenden Blick auf Datenhoheit in der Cloud zu erhalten.

Das Paper zeigt Ihnen Ansätze zur Implementierung umfassender Datenhoheit in einer modernisierten und cloudbasierten IT. Dazu hat IDC im September 2022 eine Befragung von 150 IT-Entscheidern aus Deutschland durchgeführt. Alle Befragten treffen oder beeinflussen in ihren Unternehmen Entscheidungen über den Einsatz von Cloud-Technologie und Cloud Services.



Cloud Computing – Modernisierungsfaktor Nummer 1 für die IT

Aktuelle Modernisierungstrends

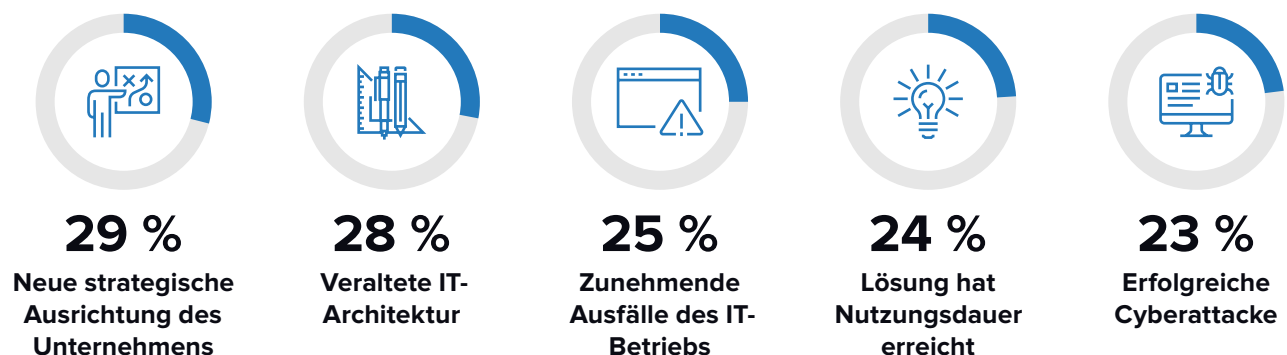
Die Geschwindigkeit und Intensität der wirtschaftlichen Veränderungen sind enorm. Cloud Computing hat in einer Welt des Wandels hinreichend bewiesen, dass moderne cloudbasierte Informationstechnologie aktuell sowohl technologisch als auch konzeptionell der effizienteste Weg ist, den wirtschaftlichen Erfolg langfristig zu sichern und die digitale Transformation voranzutreiben. Viele Entscheider stehen aber noch nicht dort, wo sie mit Blick auf die Steigerung der Prozessgeschwindigkeit mit IT hinwollen, denn die Erneuerung und Optimierung der IT-Landschaft ist hochkomplex. Die Schritte in die Cloud müssen sorgfältig gewählt werden und in Modernisierungsvorhaben eingebettet sein. Für viele Unternehmen stellt sich die Frage: „Wo beginnen?“ Das ist nachvollziehbar, denn die Zahl der Lösungsansätze ist groß und jedes Unternehmen hat seine spezifische Historie und seine individuellen Anforderungen.

IT-Modernisierung umfasst alle Maßnahmen und Schritte zur Verringerung der Komplexität von IT-Umgebungen und zur Erhöhung der Prozessgeschwindigkeit.

Der Druck auf die IT-Abteilungen ist hoch und steigt fast täglich. *Für knapp ein Drittel der befragten Teilnehmer erfüllt die vorhandene IT längst nicht mehr die Anforderungen eines sich permanent verändernden Business.* Sie ist häufig veraltet, d. h., die Server sind zu langsam im digitalisierten Tagesgeschäft und ihre Wartung und Pflege ist zu aufwändig und zu teuer. Das gilt auch dann, wenn die IT funktionale Anforderungen noch erfüllt. Legacy-Lösungen binden zudem Ressourcen, die für Innovation und Digitalisierung fehlen, und sie sind ein potenzielles Risiko für Cyberattacke und den Datenschutz. Eine breit gefasste parallele Einführung neuer IT-Lösungen und -Systeme ist für viele IT-Organisationen aber schlicht nicht leistbar. Ohne eine Priorisierung der Aufgaben geht es also nicht.

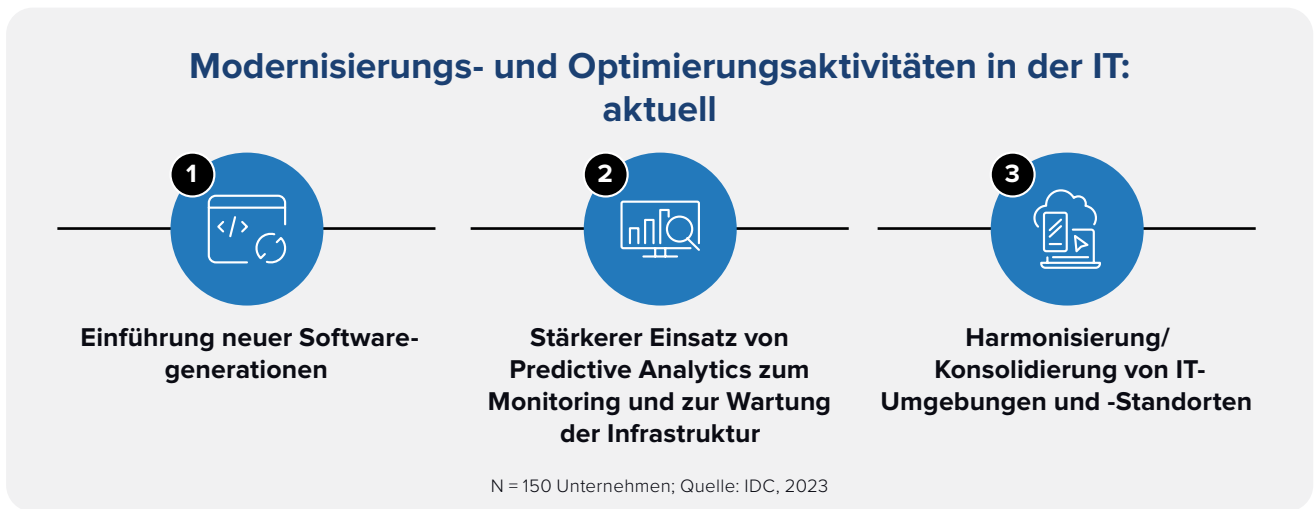
Abbildung 1

Top-5-Gründe für die Modernisierung der IT-Infrastruktur



N = 150 Unternehmen, Mehrfachnennungen, Abbildung gekürzt; Quelle: IDC, 2023
 F.: Was sind die wichtigsten Gründe für die Modernisierung der IT-Infrastruktur?

Der Blick auf **aktuelle Projekte** zeigt, dass in einem Drittel der Organisation die Einführung einer neuen Softwaregeneration auf der Agenda steht. Businessanwendungen laufen immer häufiger vollständig oder teilweise in der Cloud, um geschäftliche Anforderungen schneller und agiler abzubilden. Das bringt aber auch neue Anforderungen an die Datensicherheit und die Datenhoheit mit sich. Knapp ein Drittel setzt auf Monitoring für mehr Transparenz über die IT-Infrastruktur. Monitoring schafft nicht nur in komplexen Prozessen wie einem ERP-Upgrade einschließlich Infrastruktur umfassende Transparenz. Sie ist überall erforderlich, denn Abhängigkeiten zwischen Prozessen bestehen in allen Bereichen der IT. Unternehmen, die jetzt mit der Cloud starten oder ihre Cloud-Reise beschleunigen möchten, können von vielen Modernisierungsprojekten ihrer Branche profitieren und dort gesammelte Erfahrungen nutzen. Aus Sicht von IDC ist die IT-Infrastruktur ein sinnvoller Startpunkt: Gemeinsam mit der IT-Architektur wird dort die Basis für den effizienten Einsatz der Anwendungen gelegt, um das primäre Ziel, eine engere Verzahnung von Business und Technologie, zu erreichen.

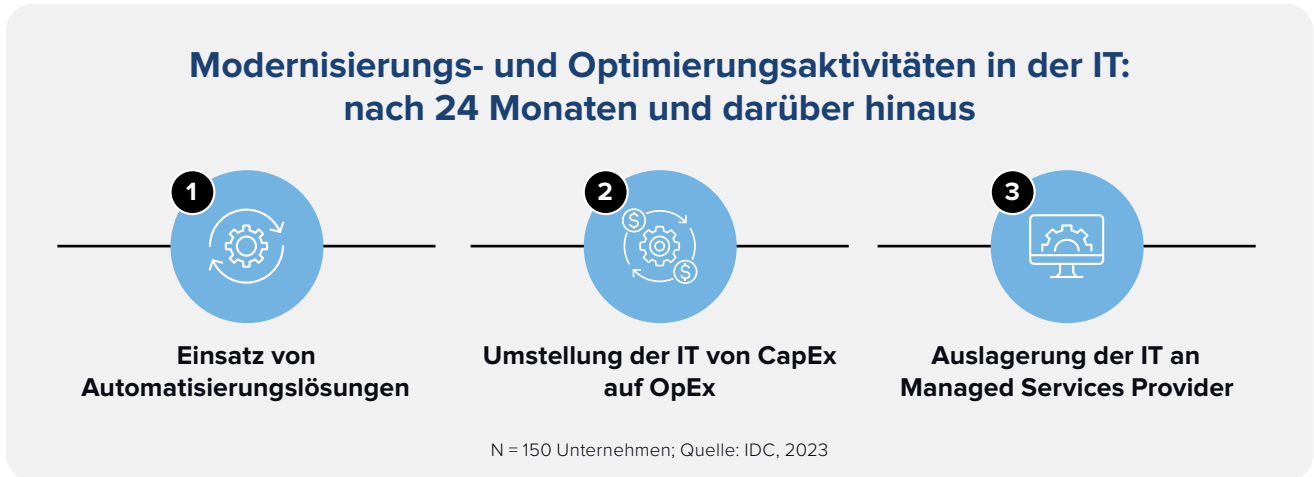


Die Konsolidierung und Harmonisierung von IT-Umgebungen und -Standorten ist ein erster erforderlicher Schritt und **mittelfristig** die häufigste Initiative. *IDC beobachtet gegenwärtig eine signifikante Reduzierung der Zahl der Serverräume, Rechenzentren und IT-Lokationen, um die IT kostengünstiger und effizienter zu machen.* Hand in Hand mit der Konsolidierung geht die Einführung von unternehmensweitem Enterprise Service Management. Der Trend zur Serviceorientierung ist seit Jahren sichtbar, aber noch lange nicht abgeschlossen und weiter sinnvoll, da die Strukturierung der Angebote der IT-Organisation für die Fachbereiche den Bezug von Cloud Services erheblich vereinfacht.



Getrieben von einer höheren Serviceorientierung, anhaltender Standardisierung und der Nutzung von Cloud Services wird langfristig das Thema Automatisierung die Liste der Modernisierungsinitiativen anführen.

Cloud Computing und Standardisierung sind in diesem Zusammenhang ganz entscheidende Enabler für die Automatisierung von Prozessen und Prozessketten und somit für eine höhere Prozessgeschwindigkeit sowie schnelleres und sicheres Business. Zugleich wird sich die Auslagerung der IT an Managed Services Provider beschleunigen und damit eine Umstellung der IT von CapEx auf OpEx verstärken und die Nutzung automatisierter Prozesse erhöhen.



Wir haben die Modernisierung der IT zügig und konsequent vorangetrieben. Nicht zuletzt auch durch die Auslagerung der Server in die Cloud. Das hat unsere IT sehr stark entlastet, weil wir kein eigenes Rechenzentrum mehr betreiben müssen.



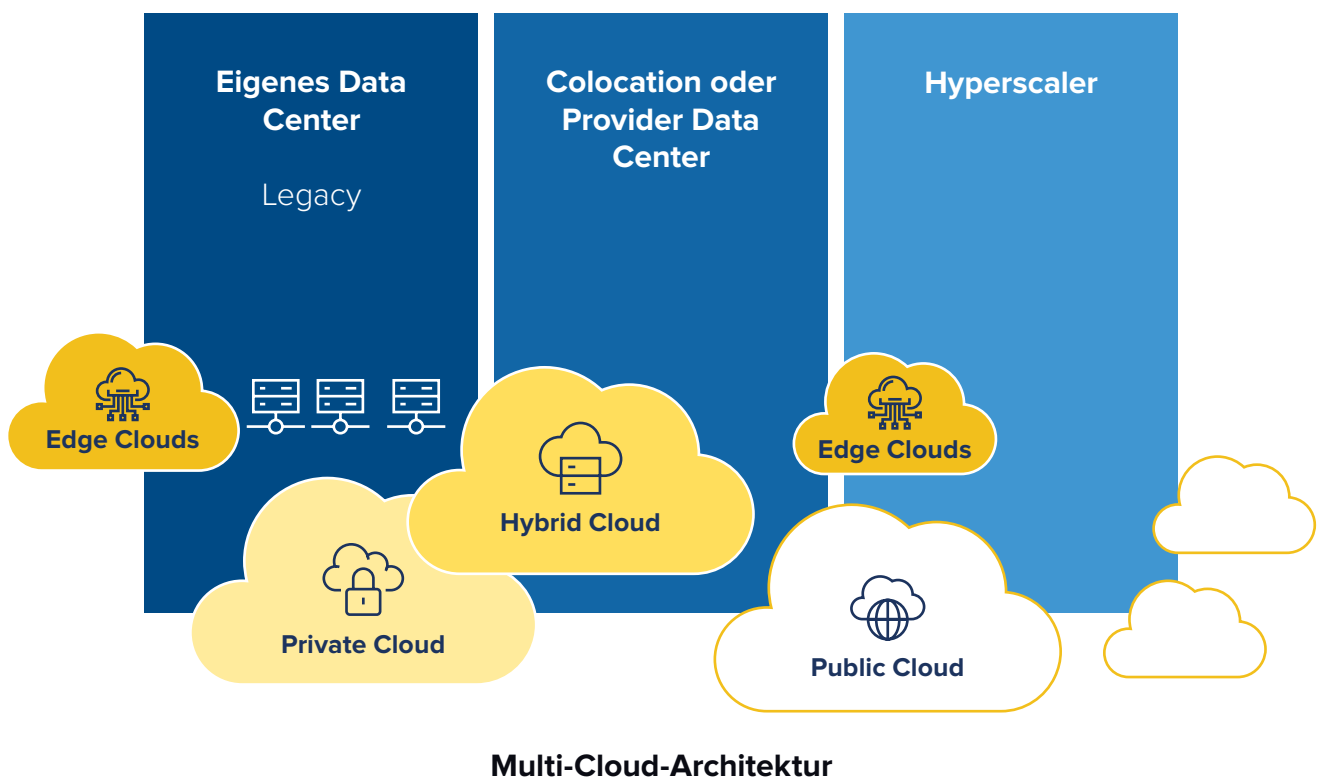
Thomas Janzen, Leitung IT, Dr. Dienst & Partner



Cybersecurity und Standards treiben die Nutzung von Cloud Computing

Die Befragungsergebnisse und zahlreiche IDC Studien bestätigen, dass sich Clouds in der Unternehmens-IT etabliert haben. Dieser Trend wird sich in den kommenden Jahren weiter verstärken, allerdings nicht ad hoc, sondern schrittweise. Die verschiedenen Deployment-Modelle ermöglichen den Entscheidern, individuelle Anforderungen umzusetzen (siehe Abbildung 2).

Abbildung 2
Cloud-Deployment-Modelle

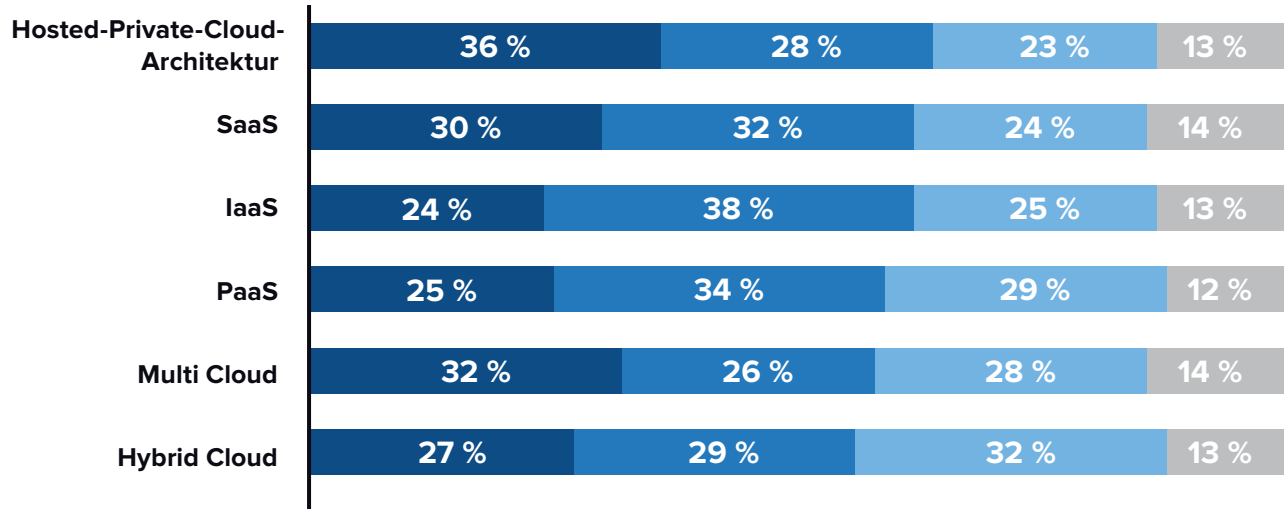


Quelle: IDC, 2023

Am häufigsten – implementiert von knapp zwei Dritteln der befragten Unternehmen – kommen Hosted Private Clouds zum Einsatz. Bei der Evaluierung der künftigen Cloud-Nutzung steht mit 32 Prozent der Nennungen die Hybrid Cloud an erster Stelle, gefolgt von Multi Clouds, wie Abbildung 3 zeigt.

Abbildung 3

Nutzung von Cloud Services und Cloud-Technologie



Umfassende Nutzung (mehr als 2 Workloads bzw. durch alle Nutzer einer Domain)

Begrenzte Nutzung (1 oder 2 Workloads) **Evaluieren wir**

Nutzen wir nicht und keine Pläne

N = 150 Unternehmen, Mehrfachnennungen; Quelle: IDC, 2023

F.: In welchem Umfang nutzt Ihr Unternehmen Cloud Services bzw. Cloud-Technologie oder planen Sie die Nutzung von Clouds?

Die Vielfalt und die Weiterentwicklung der Cloud-Deployment-Modelle und Cloud-Technologien seitens der Hersteller vereinfacht und beschleunigt die Infrastruktur- und Anwendungsmodernisierung. Zahlreiche IT-Modernisierungen basieren mittlerweile sogar auf einer Cloud-first- oder Cloud-only-Strategie.

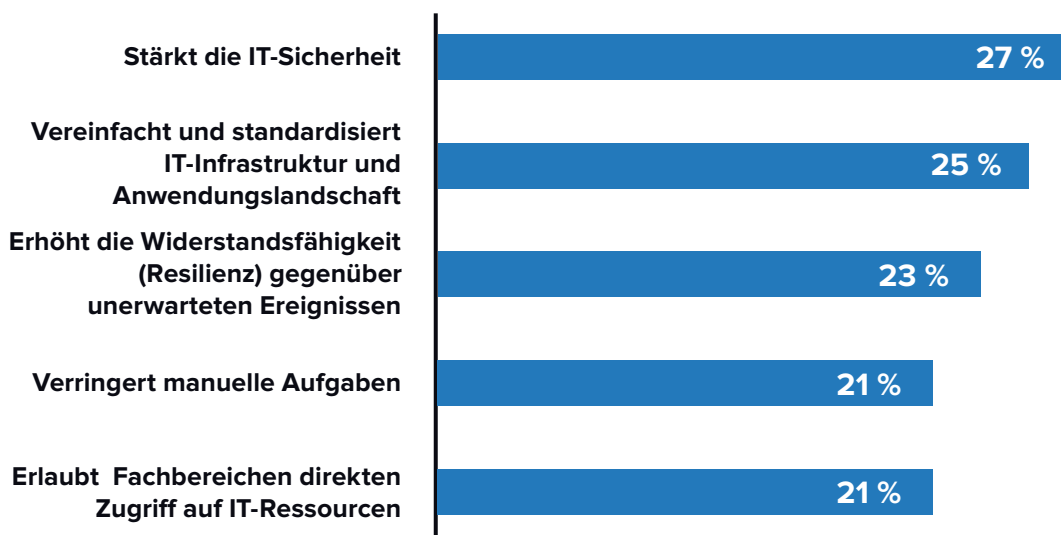
Aus Sicht von IDC versetzt nur eine digitale Architektur mit der Cloud als Kernelement IT-Organisationen in die Lage, die Fachbereiche und deren Businessziele optimal zu unterstützen und zu digitalisieren.

61 Prozent der Befragten planen mittel- und langfristig eine intensivere Nutzung von Cloud Services als bisher. Das ist ein klares Statement. Die CIOs und IT-Leiter sind also davon überzeugt, dass ihnen die Cloud am besten dabei helfen wird, die Anforderungen der Fachentscheider zu erfüllen. Dafür sprechen vielfältige Gründe, wie Abbildung 4 zeigt:

- ▶ *So sieht mehr als ein Viertel seine IT-Sicherheit durch die Cloud gestärkt.* Hier sind viele externe Rechenzentren sehr gut aufgestellt: Sie verwenden moderne Cybersecurity-Tools und bieten eine physische Sicherheit von Hardware und von Daten auf Basis von IT-Industrie-Best-Practices in den Rechenzentren der Provider, die die meisten Unternehmen selbst schlichtweg nicht realisieren könnten.
- ▶ *Eine der größten Stärken von Cloud Computing ist für 25 Prozent der Befragten die Etablierung von Standards in der IT-Infrastruktur und der Anwendungslandschaft. Standards erleichtern den IT-Betrieb erheblich.* Das gilt nicht nur für die Integration von Lösungen, die Beseitigung von Silos oder die Vereinfachung durch Automatisierung, sondern auch für die Transparenz der Abläufe. Wenn diese Aspekte in Angriff genommen werden, sind Unternehmen viel besser in der Lage, neue digitale Geschäftsmodelle und Innovationen umzusetzen.
- ▶ Ein weiterer Grund, in die Cloud zu gehen, hat einen hochgradig aktuellen Bezug. *Für 23 Prozent der Entscheider ist Cloud Computing ein geeignetes Tool zur Steigerung ihrer Widerstandsfähigkeit (Resilienz).* Ein robuster Geschäftsbetrieb ist vor dem Hintergrund unsicherer Märkte und Ökosysteme ein Muss und somit erfährt das Konzept Widerstandsfähigkeit mehr Aufmerksamkeit als bisher.

Abbildung 4

Top-5-Gründe für die Nutzung von Cloud Services und Cloud-Technologie



N = 150 Unternehmen, Mehrfachnennungen, Abbildung gekürzt; Quelle: IDC, 2023
F.: Welche sind die wichtigsten Gründe für die Nutzung von Cloud Services und Cloud-Technologie?

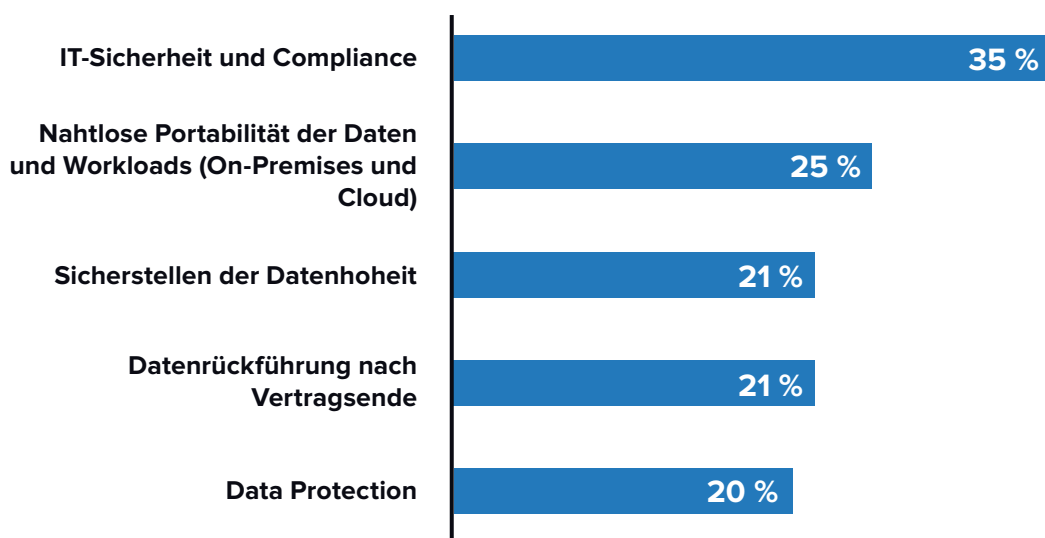
Darüber hinaus gibt es noch weitere Argumente für die Cloud, wie eine höhere Businessagilität, Datenhoheit, Skalierbarkeit der IT und die schnellere Bereitstellung von Businessfunktionalitäten. Cloud Computing ist nicht die alleinige Lösung aller Probleme in der IT, aber sie kann einen beträchtlichen Mehrwert liefern. Vor allem die befragten Spezialisten aus den operativen Bereichen und dem IT-Betrieb sehen einen hohen Nutzen in diesem Lösungsansatz.

Zugleich bringen die Komplexität der Cloud und die Vielfalt möglicher Lösungsansätze aber auch zahlreiche **Herausforderungen** (Abbildung 5) mit sich. Das Bewältigen der Herausforderungen entscheidet immer über den Erfolg oder Misserfolg eines Projekts.

- ▶ *IT-Sicherheit und Compliance gelten nach wie vor als größte Herausforderung. Vorbehalte bestehen also weiterhin. Das ist nicht überraschend, denn das komplexe Thema Cloud Security erfordert Wissen, das häufig fehlt.* Zudem wird Cloud Security mit der fortschreitenden Umsetzung der Digitalisierung und der umfassenderen Verwendung von Cloud Services und Cloud-Technologie wichtiger.
- ▶ *Daten und Workloads souverän in die Cloud und aus der Cloud heraus zu bewegen, bleibt eine Grundsatzfrage in der Entscheidung für Cloud Computing und ist gleichzeitig ganz zentral für Datenhoheit.* Das ist keineswegs nur eine technische Frage, sondern umfasst auch immer Kosten- und Vertragsthemen.
- ▶ Die Datenhoheit ist zweifellos nach wie vor ein unterschätzter Aspekt, denn die vollständige Verfügungsgewalt über die Daten ist ein Grundparadigma der Informationstechnologie. Hier stehen aktuell interessante Lösungsansätze zur Verfügung, wie im folgenden Kapitel gezeigt wird.
- ▶ Des Weiteren müssen alle Fragen rings um Data Protection mit Blick auf Business Continuity beantwortet werden. Aus Sicht von IDC bietet Cloud Computing bei Data Protection eher Chancen, insbesondere bei Backup und Recovery sowie der Archivierung von Daten beim Provider, und damit die Möglichkeit, Business Continuity mit nicht infizierten Images zu realisieren.

Abbildung 5

Top-5-Herausforderungen bei der Cloud-Nutzung



N = 150 Unternehmen, Mehrfachnennungen, Abbildung gekürzt; Quelle: IDC, 2023
F.: Welche Aspekte sind eine Herausforderung bei der Cloud-Nutzung?

Neben vielfältigen Fragen rund um die IT-Sicherheit hat ein Viertel der Befragten Bedenken bei der Portabilität der Daten und Workloads in die Cloud und aus der Cloud. Zu weiteren Herausforderungen zählen die Stärkung der Cybersecurity, die Verringerung des Kostendrucks und im Kontext der engeren Verzahnung von Business und IT die Umsetzung widerstandsfähiger digitaler Businessmodelle.

Fast alle der genannten Gründe für die Cloud sowie auch die Herausforderungen berühren das Thema Datenhoheit direkt oder indirekt. Die Relevanz von Datenhoheit für den IT-Betrieb und den geschäftlichen Alltag ist bereits heute sehr hoch und das proaktive Umsetzen dieses Konzepts bringt jedem Unternehmen einen hohen Mehrwert.

Uns haben verschiedene Gründe in die Cloud geführt. Zunächst hatten wir einen hohen Administrationsaufwand mit dem eigenen Rechenzentrum. Auch die Ausfallsicherheit war ein Thema. Ein zweites Rechenzentrum war zwar in der Diskussion, um Redundanzen zu ermöglichen, würde aber wiederum enorme Personalressourcen verschlingen. Zusätzlich kam die Investitionsthematik dazu. Wir haben jetzt einen monatlichen Fixbetrag und so gut wie keine einmaligen großen Investitionen mehr. Das gibt uns Planungssicherheit.



Thomas Janzen, Leitung IT, Dr. Dienst & Partner

Unser Weg in die Cloud wurde im Wesentlichen durch unsere Kunden angestoßen und getrieben. Unsere Vorurteile gegenüber der Cloud, insbesondere bei Sicherheitsthemen, fielen dann recht schnell. Wir sehen einen großen Nutzen in der Cloud. Cloud Computing reduziert den Wartungsaufwand für uns erheblich, denn wir können nicht mehr alles selbst hosten und administrieren. Das ist einfach zu aufwendig.

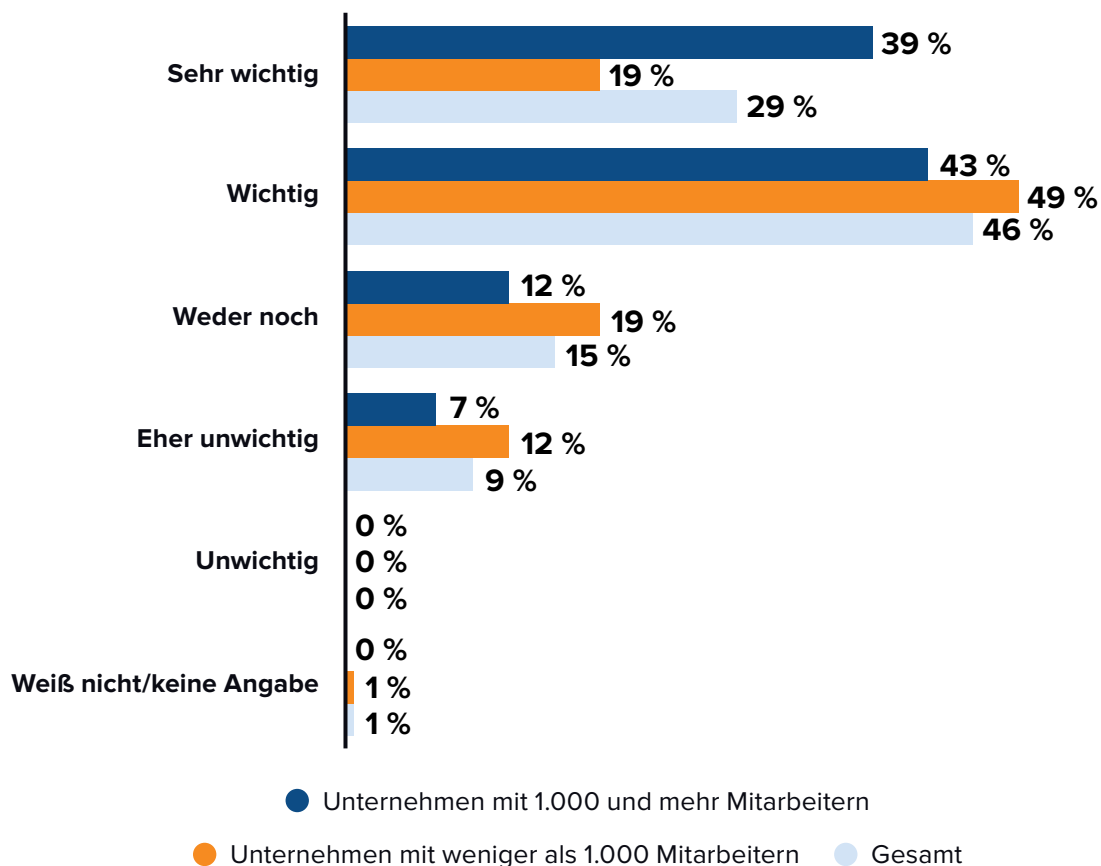


Hanno van den Boogaard, Regional Manager, Global IT, Valtech

Dank Datenhoheit schneller zur umfassenden Digitalisierung

Die Daten sind das wichtigste Asset jedes Unternehmens. Ihre sichere und souveräne Nutzung ist die Basis für ein erfolgreiches Tagesgeschäft und die Entwicklung neuer, vor allem digitaler Produkte, Dienstleistungen und Geschäftsmodelle. Das sichere Speichern und Verwenden der Daten on-premises stellt bereits hohe Anforderungen an den Datenschutz und die Datensicherheit. In der Cloud kommt mit der Datenhoheit eine weitere kritische Komponente hinzu. *Zwar ist das Thema noch recht neu, aber bereits 29 Prozent der befragten Unternehmen schätzen Datenhoheit als sehr wichtig für ihre Cloud-Strategie ein und weitere 46 Prozent betrachten sie als wichtig.* Die Awareness für Datenhoheit steigt rasch und wird weiterwachsen, je intensiver die Digitalisierung vorangetrieben wird und Cloud Computing in den Mittelpunkt digitaler Architekturen rückt. Große Unternehmen schätzen die Datenhoheit deutlich häufiger als der Mittelstand als „Sehr wichtig“ ein. Dafür sprechen zwei Gründe: Die Masse der großen Unternehmen verfügt über umfangreiche Erfahrungen mit Cloud Computing und hat Datenhoheit als sehr wichtigen Punkt erkannt. Darüber hinaus verfügen sie aufgrund großer IT-Organisationen und spezialisierter IT-Fachkräfte über das Potenzial, datenrelevante Themen granularer zu bearbeiten als mittelständische IT-Abteilungen. Damit sind sie in der Lage, Datenhoheit bei der Verlagerung von IT-Infrastruktur und Anwendungen zum Provider von Anfang an bei der Projektplanung und Umsetzung zu berücksichtigen. Das ist eine Anforderung, die jedes Unternehmen berücksichtigen sollte.

Abbildung 6
Wichtigkeit von Datenhoheit für Cloud Computing



N = 150 Unternehmen; Quelle: IDC, 2023

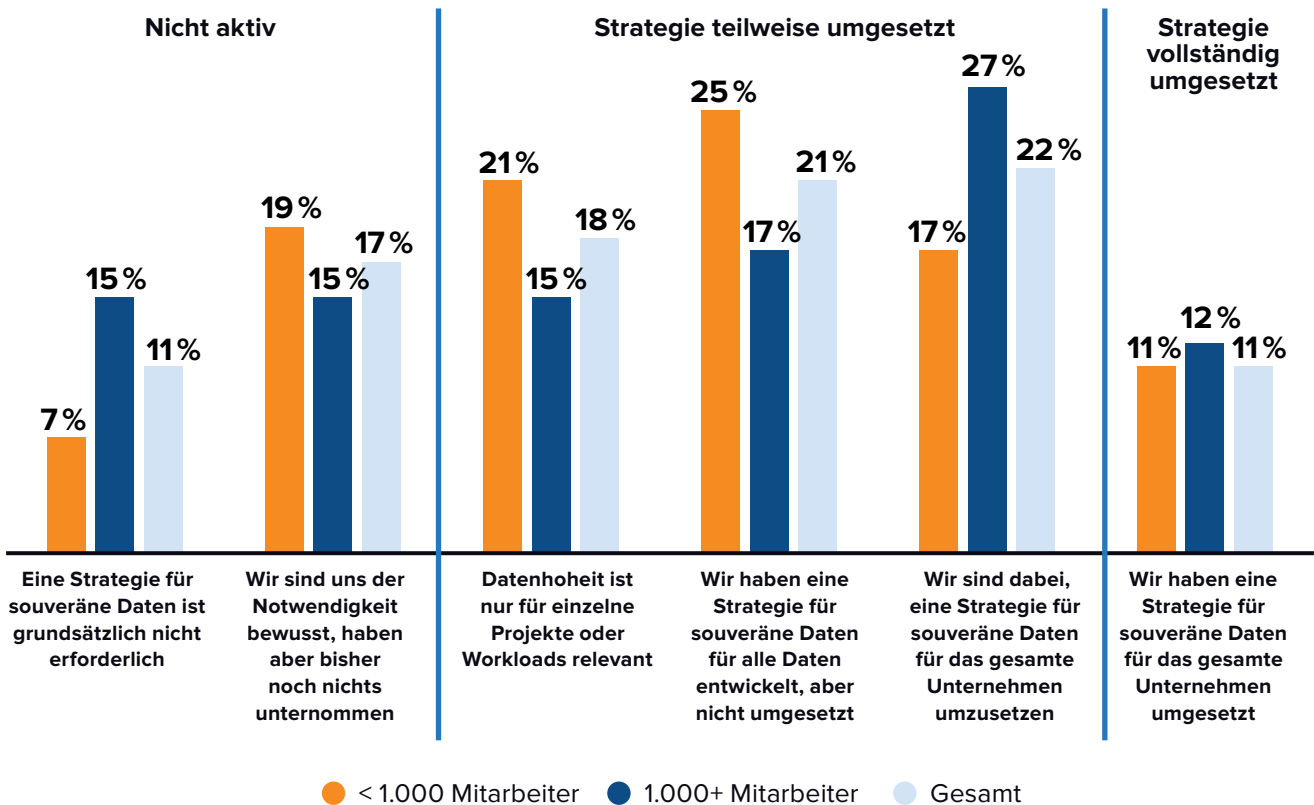
F.: Wie wichtig ist die Datenhoheit für die Cloud-Strategie Ihres Unternehmens?

Die Wichtigkeit von Datenhoheit wird von den meisten Unternehmen erkannt (Abbildung 6). Dieses Erkennen mündet aber nicht direkt in die erforderlichen umfassenden Aktivitäten. *Datenhoheit ist erst bei 11 Prozent der Unternehmen umfassend operationalisiert, d. h., sie arbeiten auf Basis einer Strategie für souveräne Daten (Abbildung 7). Die Mehrzahl der Unternehmen ist bei der Datenhoheit noch nicht so weit fortgeschritten, wie es eigentlich möglich und nötig wäre. Immerhin 61 Prozent sind zumindest in Teilschritten aktiv.*

Unternehmen, die die Digitalisierung als ihre Top-Business-Herausforderung verstehen und angehen, sehen den Zusammenhang und die Dringlichkeit von Datenhoheit und Cloud-Strategie. Für knapp 50 Prozent dieser Unternehmen ist Datenhoheit sehr wichtig für ihre Cloud-Strategie.

Aber 28 Prozent haben noch keine Schritte unternommen bzw. betrachten Datenhoheit sogar als nicht relevant. Hierzu zählen überdurchschnittlich häufig die Branchen Industrie und Financial Services mit einem hohen Anteil an Inhouse- und Legacy-IT. Aber auch in diesen Branchen besteht ein dringender Handlungsbedarf für die Weiterentwicklung und Umsetzung einer Strategie für Datenhoheit, denn die Reise in die Cloud hat dort ebenfalls längst begonnen. Große Unternehmen liegen bei der Umsetzung einer Strategie für Datenhoheit vor dem Mittelstand. Die Abstände sind aber geringer als erwartet. Somit sind mittelständische Unternehmen gleichermaßen bestrebt, bei der Umsetzung von Datenhoheit voranzukommen.

Abbildung 7
Umsetzung einer Strategie für Datenhoheit



N = 150 Unternehmen; Quelle: IDC, 2023

F.: Welche der folgenden Aussagen beschreibt die Position Ihres Unternehmens in Bezug auf Datenhoheit am besten?

In der Vergangenheit wurde Datenhoheit in Deutschland vorrangig unter dem Aspekt Datenschutz/Datenschutz-Grundverordnung (DSGVO) betrachtet. Das greift mittlerweile zu kurz. Heute ist die Sicht darauf breiter gefächert und der souveräne Umgang mit Daten erfordert eine granulare Betrachtung des Themas. IDC beobachtet dabei immer wieder, dass die Begriffe digitale Souveränität, Datensouveränität bzw. Datenhoheit, Datensicherheit und Datenschutz mitunter synonym genutzt werden. Das kann im Geschäftsalltag zu Unklarheiten bei der Benutzung der Begriffe, beispielsweise in der Kommunikation zwischen der IT, den Fachbereichen und der Unternehmensführung oder in der Kommunikation mit Geschäftspartnern, führen. Ein einheitliches Verständnis innerhalb des Unternehmens und über die Unternehmensgrenzen hinaus zu schaffen, ist essenziell.

DEFINITIONEN

Datenhoheit bzw. Datensouveränität beschreibt die vollständige Verfügungsgewalt bzw. selbstbestimmte Kontrolle von Unternehmen und Personen bei der Erhebung, Speicherung, Nutzung und Verarbeitung eigener Daten.

Datensicherheit umfasst technische Maßnahmen und Prozesse zum Schutz von Daten. Ziel ist die Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit.

Datenschutz beschreibt den Schutz vor der missbräuchlichen Verarbeitung personenbezogener Daten sowie das Recht auf informationelle Selbstbestimmung.

Digitale Souveränität ist ein Begriff, der auf politischer und gesellschaftlicher Ebene verwendet wird.

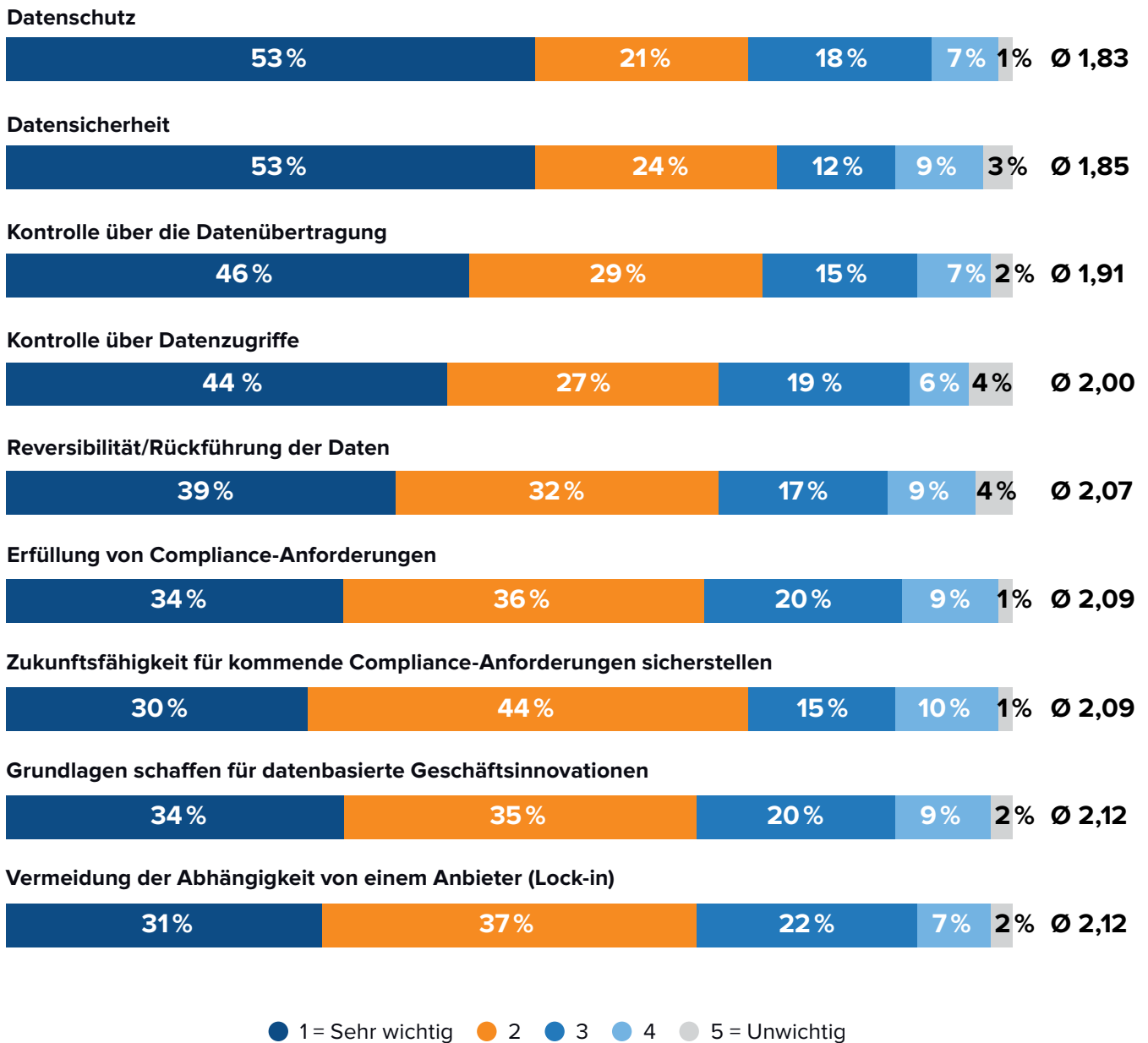
Die Gewährleistung von Datensouveränität bzw. Datenhoheit, Datensicherheit und Datenschutz ist eine Basisanforderung im Tagesgeschäft jedes Unternehmens und muss sowohl in der IT als auch in den Fachbereichen umgesetzt werden. Die Themen stehen in enger Wechselbeziehung und bedingen einander. Somit ist es wenig zielführend, sich nur auf einen Aspekt zu konzentrieren und die anderen zu vernachlässigen. Nur wenn Datenhoheit, Datenschutz und Datensicherheit koordiniert vorangetrieben werden, ist ein umfassender Schutz möglich. Das ist ohne Frage eine anspruchsvolle Aufgabe, die sich nur schrittweise lösen lässt.

Datenschutz und Datensicherheit basieren auf etablierten Anforderungen und Prozessen, die seit vielen Jahren erprobt sind. Für jeweils 53 Prozent der Befragten sind beide Aspekte besonders wichtig, wie die Abbildung 8 zeigt. Aufgrund der DSGVO hat jede Organisation Lösungen und Prozesse für den Schutz personenbezogener Daten eingeführt. Datensicherheit ist in den meisten Organisationen durch Tools zur Abwehr der Cyberangriffe und der Ransomware-Attacken abgedeckt. Allerdings variiert der Umsetzungsgrad stark.

Datenhoheit ist als Begriff und Konzept noch nicht so stark etabliert. Die Anforderungen, die hinter Datenhoheit stehen, sind aber bereits seit mehreren Jahren hochrelevant. Hierbei handelt es sich um die Kontrolle der Datenübertragung, die Kontrolle der Datenzugriffe und die Reversibilität der Daten. Die Nennungen lassen erkennen, dass Unternehmen als Konsequenz der Erfahrungen aus ihrem Tagesgeschäft Schritte in Richtung Datenhoheit gehen.

Datenhoheit hat zudem den Anspruch, im Rahmen der digitalen Transformation datenbasierte Geschäftsinnovationen, z. B. in dafür geschaffenen Datenräumen, zu unterstützen. Dieser Ansatz verfolgt das Ziel, Services, Daten, Applikationen oder Kapazitäten gemeinsam in der Cloud zu nutzen, in neuen Leistungsbündeln zu kombinieren oder darauf basierend neue Angebote zu entwickeln. Aus Sicht von IDC besteht hier ein hohes Potenzial, das in den kommenden Jahren erschlossen werden wird.

Abbildung 8
Wichtigkeit von Lösungsansätzen für Datenhoheit in der Cloud

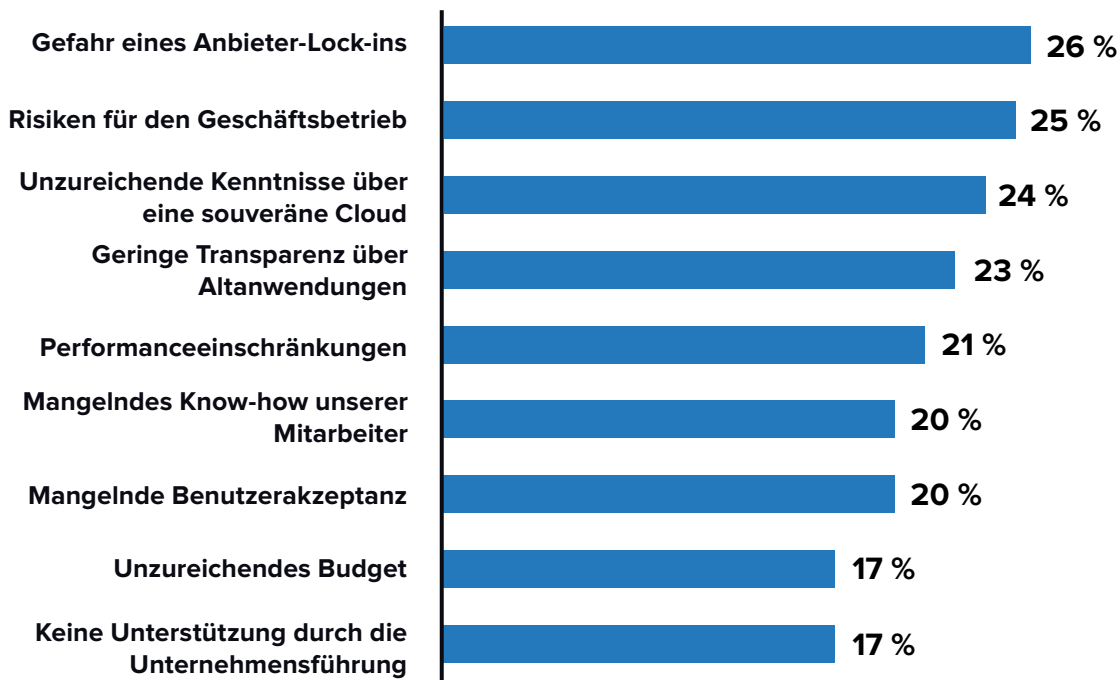


N = 137 Unternehmen, Mehrfachnennungen; geordnet nach Durchschnittsnote; Quelle: IDC, 2023
 F.: Wie wichtig sind für Ihr Unternehmen folgende Aspekte von Datenhoheit bei der Nutzung von Cloud-Lösungen?

Für die gezielte Umsetzung von Datenhoheit in der Cloud sind einige Herausforderungen zu lösen (Abbildung 9). Die Komplexität der Herausforderungen ist neben der Neuartigkeit des Begriffs und Konzepts der Hauptgrund für die aktuell geringe Umsetzungsrate. Gut ein Viertel der Befragungsteilnehmer sieht in diesem Kontext die Gefahr eines Anbieter-Lock-ins. Das Risiko ist dann gegeben, wenn das Konzept der Datenhoheit nicht konsequent verfolgt wird. Es wächst dann mit der Zahl der bezogenen anbieterspezifischen Services. Einen wesentlichen Einfluss auf die Tiefe des Anbieter-Lock-ins haben die Vertragsgestaltung einschließlich der Kosten für die Datenrückführung und die Technologie, die der Anbieter einsetzt.

Abbildung 9

Herausforderungen bei der Umsetzung von Datenhoheit in der Cloud



N = 150 Unternehmen, Mehrfachnennungen, Abbildung gekürzt; Quelle: IDC, 2023
 F.: Welche Herausforderungen sehen Sie bei der Umsetzung von Datenhoheit in einer Cloud?

Im Kontext der Datensouveränität lässt sich der Lock-in beherrschen und abschwächen, wenn der Service Provider neben der Datenhoheit auch technologische und operative Souveränität garantiert. Ein weiteres Viertel sieht Risiken für den Geschäftsbetrieb. Diese Sichtweise berührt grundsätzliche Fragen über die Datenhoheit und erfordert eine genaue Betrachtung der potenziellen Risiken. 24 Prozent der Befragten haben unzureichende Kenntnisse über eine souveräne Cloud und weitere 20 Prozent sehen grundsätzlich ein mangelndes Wissen ihrer Mitarbeiter bei diesem Thema.

Die **souveräne Cloud und der Sovereign Cloud Stack (SCS)** reduzieren auf Basis von Open Source und offenen Standards die Lock-in-Effekte. Aus Sicht von IDC verfügt eine souveräne Cloud über folgende Merkmale:

- **Datensouveränität/Datenhoheit:** sichert die vollständige Verfügungsgewalt bzw. selbstbestimmte Kontrolle bei der Erhebung, Speicherung, Nutzung und Verarbeitung eigener Daten.
- **Operative Souveränität:** transparente Kontrolle der Abläufe von der Bereitstellung und dem Management der Lösungen und Services bis hin zur Überwachung des physischen und digitalen Zugriffs auf die Infrastruktur.
- **Technologische Souveränität:** basiert auf Open Source bzw. allgemein verfügbarer standardisierter Technologie und ermöglicht Transparenz und Nachvollziehbarkeit der Datenverarbeitung und der eingesetzten Softwarekomponenten (Betriebssystem und Anwendungen).

Die Wertungen in Abbildung 9 zeigen, dass noch zahlreiche Herausforderungen bei der Datenhoheit existieren. Bei neuen Konzepten und Lösungen gilt es stets, eine Vielzahl an Unklarheiten zu beantworten. Die Anforderungen, die im Kontext Datenhoheit diskutiert werden, sind aber nicht neu und sind somit eher geringe Hürden für die Umsetzung von Datenhoheit. Mit Schulungs- und Trainingsmaßnahmen können Wissenslücken geschlossen und die meisten Fragen geklärt werden.

Wir treiben die digitale Souveränität aktiv voran. Aus unserer Perspektive sollten Unternehmen Herr ihrer Daten und Infrastruktur sein und digital souverän agieren können. Es ist ein großes Problem sich von einem Anbieter abhängig zu machen. Dadurch hat man wenig Möglichkeiten, auf künftige Entwicklungen zu reagieren und agil zu handeln.



Stefan Gohmann, COO, Univention

Datenklassifizierung und sensible Daten im Kontext Datenhoheit

Die Klassifizierung der Daten, also die Zuordnung sensibler Daten zu verschiedenen Stufen bzw. Kategorien, unterstützt Datenhoheitskonzepte wirkungsvoll. *Die Bewertung der Daten nach ihrer Schutzwürdigkeit vereinfacht die Auswahl der Speicherorte On-Premises, Private Cloud und Public Cloud. Sie schafft gleichzeitig Transparenz über die Rolle und den Wert unterschiedlicher Daten in den einzelnen Geschäftsprozessen und beschleunigt damit Prozessschritte signifikant.* Aufgrund der DSGVO haben die meisten Unternehmen ihre Daten klassifiziert. Immerhin 48 Prozent der Befragten haben ihre Daten vollständig und weitere 41 Prozent teilweise klassifiziert. Bestehende Lücken sollten zügig geschlossen werden, denn eine hohe Datenqualität einschließlich der Datenklassifizierung erleichtert die Nutzung der verschiedenen Cloud-Deployment-Modelle. Daten und insbesondere sensible Daten sind für Angreifer von besonders großem Interesse. Unabhängig davon, ob sie extern oder intern gespeichert und verarbeitet werden, gehört das Management der Daten in professionelle Hände.



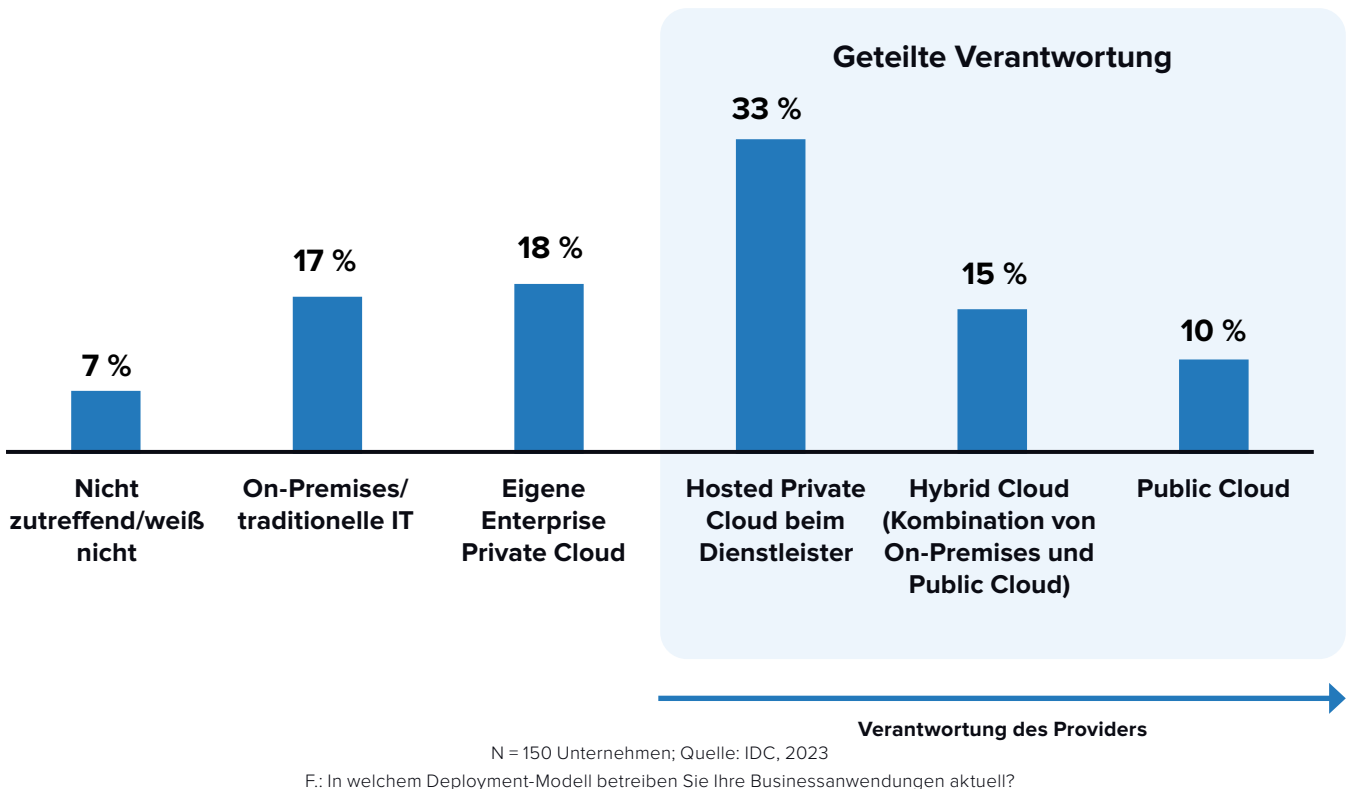
Den Weg in die Cloud zielgerichtet optimieren

Vielfalt der Deployment-Modelle mit hohem Nutzwert

Für erste oder weitere Schritte in die Cloud ist ein klares Verständnis darüber notwendig, welcher Workload mit welchem Ziel optimiert werden soll und welche Maßnahmen mit Blick auf die Datenhoheit zu berücksichtigen sind. Jedes Unternehmen verfügt über eine mindestens zweistellige Zahl an Workloads, die potenziell in der Cloud laufen können. Hierzu zählen u. a. Businessanwendungen, Collaboration Tools, Virtual-Desktop-Infrastruktur, Edge Computing, App/Dev/Test-Tools, Media und Streaming, Datenbanken, Künstliche Intelligenz/Machine Learning oder Backup, Archivierung und Disaster Recovery. Nicht alle der genannten Lösungen sind aktuell für jedes Unternehmen relevant, ihre Zahl wird aber generell in jeder Organisation wachsen. Businessanwendungen, wie ERP und CRM, benötigt jedes Unternehmen, um die betriebswirtschaftlichen Prozesse zu erfassen und zu steuern und damit auch geschäftskritische Daten, wie Finanzdaten und Kundendaten, zu verwalten. Sie werden in unterschiedlichen Deployment-Modellen betrieben und Datenhoheit muss permanent gewährleistet sein.

Datenhoheit ist immer dann relevant, wenn der Provider ganz oder teilweise die Verantwortung für den Betrieb einschließlich Datenhaltung übernimmt. Abbildung 10 zeigt die von links nach rechts steigende Verantwortung des Cloud-Anbieters auf.

Abbildung 10
Aktuelle Deployment-Modelle von Businessanwendungen



In der Hosted Private Cloud übernimmt der Anbieter die Wartung und Maintenance für die Infrastruktur der Businessanwendungen und damit eine Teilverantwortung für den Schutz und die Integrität der Daten. Der Umfang der Verantwortung für die Daten erhöht sich für den Provider mit der Übernahme weiterer Komponenten der Kunden-IT. 15 Prozent der Befragten betreiben ihre Businessanwendungen in einer Hybrid Cloud. [Die Kontrolle](#)

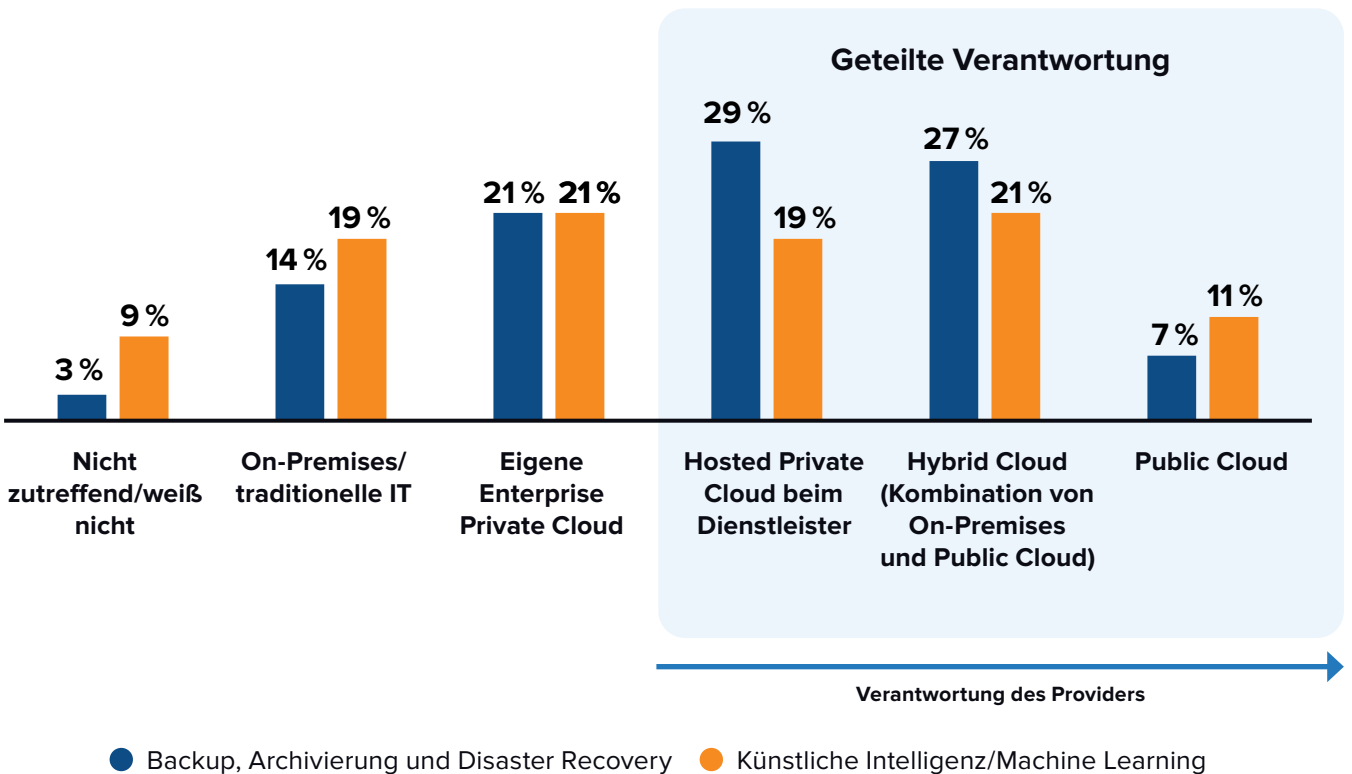
über die Daten erfordert eine hohe Aufmerksamkeit, da die Aufgaben und Rollen der Vertragspartner sehr detailliert definiert sein müssen. Weitere 10 Prozent nutzen ein reines Public-Cloud-Modell. Datenhoheit ist hier ebenfalls sehr kritisch, da die Verantwortlichkeiten für den Betrieb der Infrastrukturen und Anwendungen vollständig beim Provider liegen. Wie Daten, Anwendungen, Schnittstellen, Codes und Dienste Dritter gehandhabt werden, kann je nach Angebot variieren. Aus diesem Grund ist eine umfassende Transparenz umso wichtiger für eine konfliktfreie Geschäftsbeziehung mit dem IT-Partner.

Das gilt ebenso für weitere Workloads, hier dargestellt anhand von „Backup, Archivierung und Disaster Recovery“ und „Künstliche Intelligenz/Machine Learning (KI/ML)“. Beide Beispiele verdeutlichen ergänzend zu den Businessanwendungen, dass sich Deployment-Modelle von Workload zu Workload unterscheiden und sich damit die Anforderungen an Cloud Provider ändern. Eine große Bandbreite von Clouds erhöht jedoch die Komplexität beim Provider-Management und bei der Datenhoheit und Datensicherheit:

- ▶ Backup, Archivierung und Disaster Recovery ist ein etabliertes Thema und besonders mit Blick auf Resilience und Cybersecurity wichtig. Fragen rund um die Datenhoheit für Lösungen in der Public Cloud und beim Dienstleister müssen sehr detailliert besprochen werden, um Business Continuity nach einem erfolgreichen Cyberangriff sicherzustellen.
- ▶ KI/ML wird als relativ junges Thema häufig in Pilotprojekten erprobt. Seine Relevanz wächst stetig und rasch, um Datenanalysen für die Verbesserung der Prozesse in der IT und in den Fachbereichen zu nutzen, die Digitalisierung voranzutreiben und datengetriebene Geschäftsmodelle zu entwickeln und zu optimieren. Datenhoheit ist hier wegen der Verwendung verschiedener interner und externer Datenquellen hochkomplex und muss sowohl bei den Piloten als auch im Realbetrieb gewährleistet sein.

Abbildung 11

Aktuelle Deployment-Modelle von Backup, Archivierung und Disaster Recovery sowie KI/ML



N = 150 Unternehmen; Quelle: IDC, 2023

F.: In welchem Deployment-Modell betreiben Sie folgende Workloads aktuell?

Die bereits in Abbildung 10 getroffenen Aussagen zur Verantwortung des Providers gelten auch für die in Abbildung 11 dargestellten Lösungen. Jeder CIO und IT-Leiter muss in Absprache mit den Fachbereichen die Workloads und ihre Deployment-Modelle individuell betrachten. Dies führt häufig zu der Frage nach der Zahl der Cloud Provider. Die IDC Empfehlung lautet hier, die Zahl der Cloud Provider so niedrig wie möglich zu halten. Für mittelständische Unternehmen könnte das beispielsweise ein Provider für die Kernapplikation sein, ergänzt um einige SaaS-Partner. In diesem Modell müssen Entscheider genauer hinsehen. Einige Player bieten ihre Services und Lösungen auf einer eigenen Plattform, in die zahlreiche Partnerangebote integriert sind. Diese Plattform basiert typischerweise auf einer Anbieter-Multi-Cloud. Die Komplexität solcher Plattformen ist hoch und der Anbieter steht in der Pflicht, umfassende Transparenz bei Datenschutz, Datensicherheit und Datenhoheit zu liefern.

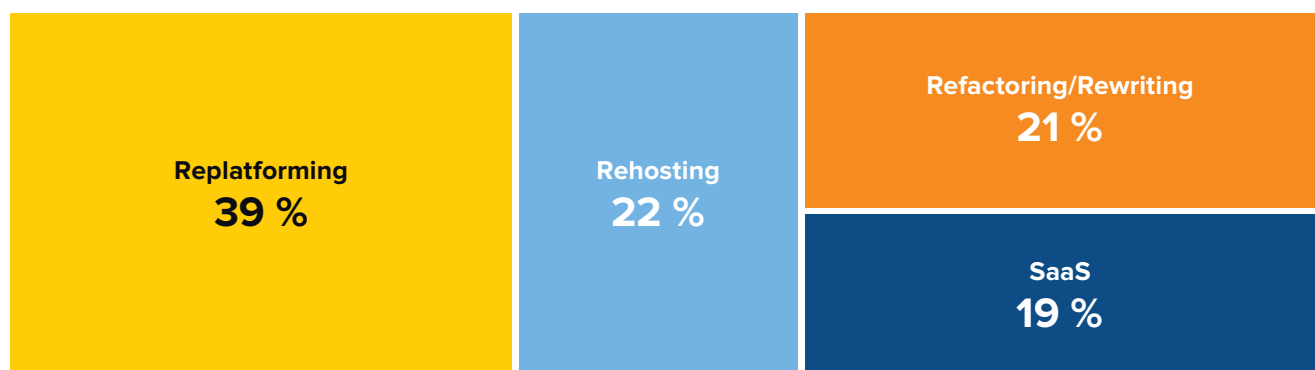
Migrationspfade zielgerichtet nutzen

Wie bereits in Kapitel 1 aufgezeigt, wird sich Cloud Computing zum dominierenden IT-Paradigma entwickeln. Laut IDCs europäischer Befragung zum Thema Multi Cloud verfügen bereits mehr als 80 Prozent der Unternehmen in Deutschland über eine Cloud-Strategie. *Aktuell wächst die Zahl der Businessanwendungen, die in die Cloud migriert werden, denn es gibt längst nicht mehr nur „den einen Weg“ in die Cloud.* Die Migrationspfade sind vielfältiger geworden und werden aktiv genutzt, wie Abbildung 12 zeigt.

- ▶ „**Lift und Shift**“, also das externe Rehosting der Lösung ist häufig der Start einer umfassenden IT-Modernisierung und damit ein wichtiger Schritt, um sich von der eigenen Legacy-Hardware zu lösen.
- ▶ Ein wichtiger Pfad ist das **Replatforming** von Lösungen, d. h. der Betrieb einer modernisierten Anwendung beim Provider. Durch die Nutzung von Cloud-Diensten des Providers nutzt die Anwendung einige Cloud-Attribute, ist aber nicht cloudnativ.
- ▶ Bisher weniger sichtbar sind das Refactoring von Code oder ein umfassendes **Neuschreiben/Rewriting** der Lösung auf Basis von PaaS. Letzteres ermöglicht das umfassende Berücksichtigen von Cloud-Native-Attributen und -Funktionalitäten wie CI/CD, DevOps, Microservices, Containern sowie Orchestrierung. Die Schritte zur digitalen Transformation werden damit erheblich beschleunigt.

Für ihre Businessanwendungen nutzen 64 Prozent der Befragten mittelfristig eines der verschiedenen Cloud-Modelle, wie die nächste Abbildung zeigt. Das ist ein bereits signifikanter Anteil, der die Anforderungen an Datenhoheit und Cloud Security steigen lässt.

Abbildung 12
Cloud-Migrationspfade für Businessanwendungen



N = 96 Unternehmen; nur Unternehmen mit Migration in die Cloud; Quelle: IDC, 2023
F.: Welche Cloud-Migrationsstrategie plant Ihr Unternehmen für Businessanwendungen?

Bei der Migration kommt es natürlich zu Reibungen. Vor allem bei der Migration der ersten Systeme mussten wir Fehleranalysen betreiben und herausfinden, woran es liegt. Sind es Netzwerk-Bottlenecks oder hängt es mit der Belastung von einem Router oder Switch zusammen? Aus der Erfahrung empfehle ich, frühzeitig Know-how des Anbieters zu suchen, ansonsten verliert man zu viel Zeit.



Stefan Gohmann, COO, Univention

IT-Security stärken – darauf kommt es an

Ein umfassender Security-Ansatz deckt immer den gesamten Security Lifecycle von Prevention bis Disaster Recovery ab. Er muss als Prozess und nicht als Technologie betrachtet und risikobasiert etabliert werden, denn es geht um die Absicherung der verschiedenen Workloads. Datenschutz, Datensicherheit und Datenhoheit sind hier wichtige Elemente, grundsätzlich müssen aber auch weitere Security-Aspekte betrachtet werden. Im Kontext Cloud und Datenhoheit haben die befragten Unternehmen vielfältige Schutzmaßnahmen ergriffen, oft auch unter Einbindung externer Ressourcen. 23 Prozent der Befragten nutzen ein Security Operations Center (SOC), um Cybersecurity Incidents auf Basis aktueller Informationen zu lösen. Weitere Lösungen sind Cloud Data Protection zur Absicherung der Cloud Services und zur Gewährleistung von Compliance, beispielsweise der DSGVO, sowie Cloud Backups zur Sicherstellung von Disaster Recovery und Business Continuity. Zusätzlichen Schutz liefern u. a. Cloud Segmentation, Next Generation Firewalls sowie Multi-Faktor-Authentifizierung. IDC empfiehlt, stärker auf die Absicherung von Identitäten in der Cloud zu achten, da der Missbrauch digitaler Identitäten weiter wächst. Es überrascht nicht, dass gemäß der aktuellen IDC Studie zu Cybersecurity Cloud Security das derzeit häufigste strategische Sicherheitsthema ist, da mehr und mehr kritische Prozesse in der Cloud laufen. Die Beherrschung der Security-Komplexität ist die größte Herausforderung und der Fachkräftemangel ist eine akute Bedrohung für den Betrieb der Security-Lösungen sowie für präventive Maßnahmen. IDC sieht einen Trend zu integrierten Plattformen und Managed Security Services, denn ein effektiver Schutz gelingt nur durch die Kombination verschiedener Technologien und konsistenter Maßnahmen über On-Premises- und Cloud-Infrastrukturen hinweg. Die Komplexität des Themas IT-Security und insbesondere Cloud Security erfordert permanente Aufmerksamkeit und regelmäßiges Handeln, um die Lösungen und die Prozesse kontinuierlich aktuell zu halten. Das überfordert die Leistungsfähigkeit vieler IT-Organisationen. Aus diesem Grund nutzen sie Managed Security Services, um Lücken bei Security-Spezialisten und Know-how zu schließen.

Für 62 Prozent der Befragten muss bei der Nutzung von Cloud Computing die Sicherheitsarchitektur überarbeitet werden.

IT-Security und Datensicherheit sind für uns sehr wichtige Themen. Jedes Tool und auch jedes Add-on wird eingehend auf Legal-Aspekte, GDPR und aus Security-Sicht überprüft. Die Datenresidenz und der Datenzugriff spielen dabei eine wichtige Rolle. Für uns ist es essenziell, dass die Daten in Europa bleiben.



Hanno van den Boogaard, Regional Manager, Global IT, Valtech

Nachhaltigkeit – von der Marketingbotschaft zum Wirtschaftsfaktor

Das Thema Nachhaltigkeit prägt die unternehmerische Agenda deutlich stärker als noch vor einigen Jahren. Eine aktuelle IDC Data Center Studie zeigt, dass 21 Prozent der befragten Unternehmen bereits über eine unternehmensweite Nachhaltigkeitsstrategie verfügen. Nachhaltigkeit wird nach und nach zum Businessfaktor und langfristig auf der strategischen Ebene eine zentrale Rolle einnehmen. Die genannte Studie belegt klar, dass 77 Prozent der Befragungsteilnehmer an der Reduzierung ihres Stromverbrauchs arbeiten. Das Thema ist nicht neu. Kostenaspekte bei der Beschaffung von IT und beim Ressourcen- und Energieverbrauch spielen schon lange eine Rolle, die Diskussion um „Green Data Center“ wird seit vielen Jahren geführt.

Nachhaltigkeit wird nun allerdings viel breiter gesehen – getrieben von wirtschaftlichen Veränderungen, hohen Energiepreisen und einer breiten gesellschaftlichen Diskussion. Auch wenn Energiekosten aktuell vorrangig unter dem Aspekt Kostenreduzierung betrachtet werden, so ist eine Verschiebung der Perspektiven bereits sichtbar. *Hohes Potenzial sieht IDC vor allem in der Bereitstellung von nachhaltiger IT: nachhaltigere Hardware, die ressourceneffizient ist und über einen längeren Lebenszyklus verfügt, die regelmäßige Modernisierung der IT-Infrastruktur und Anwendungsumgebung oder eine nachhaltige Softwareentwicklung und -architektur.* All das kann die IT in den Unternehmen und damit die gesamte Organisation per se nachhaltiger machen.

Nachhaltigkeitsrelevante Aspekte werden künftig zunehmend in Ausschreibungen für Cloud Services vorhanden sein. Dabei schauen die Verantwortlichen auf zahlreiche Kriterien. Hierzu zählt für 37 Prozent der Befragten die Verwendung von Software-Tools für optimiertes Workload-Management – sowohl serverseitig als auch für Anwendungen und Container – durch den Provider. Des Weiteren erwarten die Unternehmen, dass die Provider noch umfassender automatisieren, Strom aus erneuerbaren Energiequellen nutzen und PUE-Messungen (Power Usage Effectiveness) vorlegen. Das sind wesentliche Maßnahmen, die aber auch für das eigene Unternehmen relevant sein sollten. Grundsätzlich wird es essenziell, Businessprioritäten insbesondere mit Blick auf Kosten, Effizienz und Nachhaltigkeit unter der Prämisse der digitalen Transformation voranzutreiben.

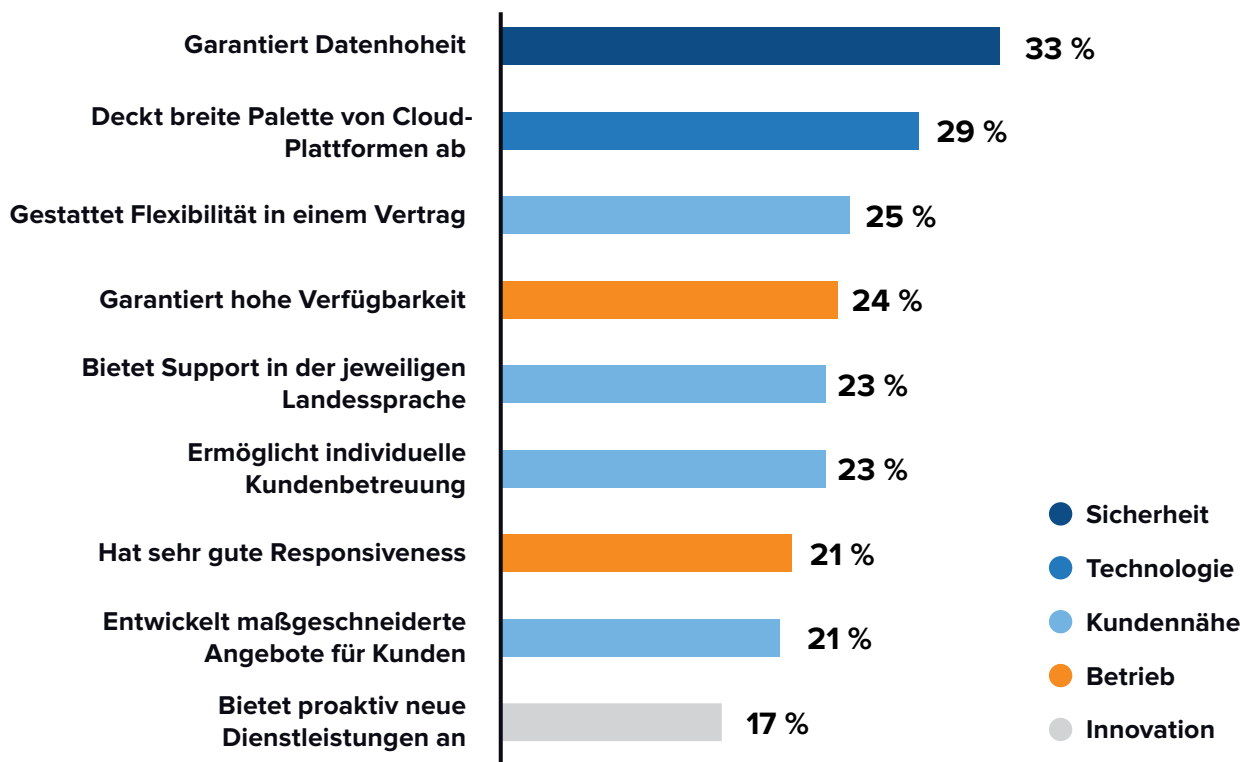


Kunden müssen Anforderungen an Provider klar kommunizieren

Die Wahl des Cloud-Anbieters hat einen starken Einfluss auf die Qualität der IT-Services für die Fachbereiche und letztendlich auf die Digitalisierung. Um aus den vielen Angeboten am Markt den passenden IT-Partner zu finden, müssen der Leistungskatalog und das Serviceangebot die spezifischen Anforderungen der Unternehmen erfüllen. Viele Anbieter befinden sich dabei auch selbst in einer anhaltenden Transformation. Aus diesem Grund ist es empfehlenswert, deren Roadmap zu kennen und zu wissen, welche Zukunftsthemen sie besetzt haben. Zudem muss die „vielbeschworene Chemie“ stimmen. Das klingt trivial, ist es aber nicht. Besonders wichtig in diesem Kontext und Fundament einer erfolgreichen geschäftlichen Partnerschaft: klare Zielsetzungen, präzise Anforderungen an den Provider und umfassende Transparenz der IT. Weil Cloud Services Provider Kunden mit unterschiedlichen Ansprüchen und Szenarien bedienen müssen, stellen sie sich technologisch und methodisch breit auf. Aber letztendlich lassen sich die Kundenanforderungen trotz aller Vielfalt in fünf Segmenten zusammenfassen: Sicherheit, Technologie, Betrieb, Kundennähe und Innovation, wie in Abbildung 13 dargestellt ist. Die farblichen Markierungen verdeutlichen, dass bei drei der fünf Segmente ein Kriterium genannt wurde und bei zwei Segmenten mehrere Aspekte. Unter den verschiedenen Kriterien für die Zusammenarbeit mit einem Cloud Provider liegt Datenhoheit an erster Stelle. Sie wird in Ausschreibungen künftig eine der zentralen Kriterien und Anforderungen sein. Flexibilität und Agilität für eine erfolgreiche digitale Transformation wird erst durch eine breite Palette an Cloud-Plattformen möglich. Kapitel 4 hat gezeigt, dass die Workloads je nach Anforderung auf unterschiedlichen Deployment-Modellen laufen. Anbieter müssen Veränderungen und Neuerungen im Cloud Computing zügig aufgreifen und in ihre Angebote übernehmen.

Abbildung 13

Zentrale Kriterien der Zusammenarbeit mit einem Cloud Provider



N = 150 Unternehmen, Mehrfachnennungen, Abbildung gekürzt; Quelle: IDC, 2023

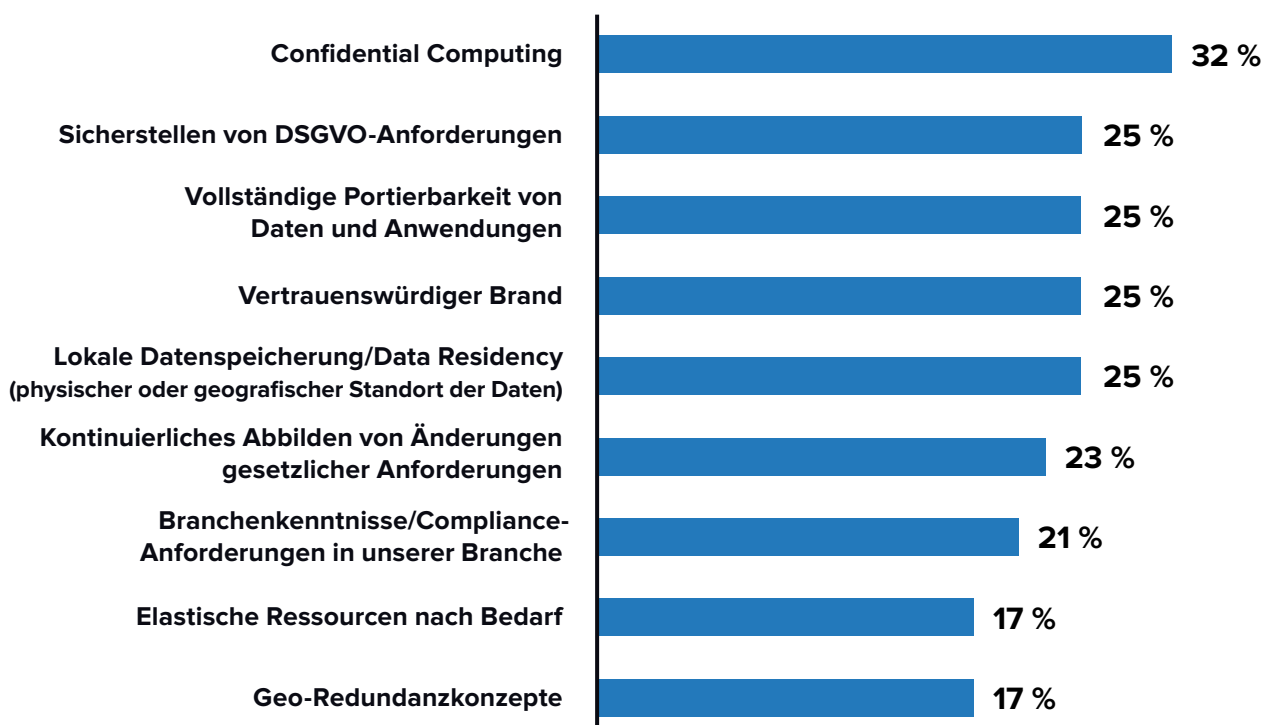
F.: Welche Eigenschaften sind für Sie bei der Zusammenarbeit mit einem Anbieter von Cloud Managed Services am wichtigsten?

Einige Cloud Services Provider fokussieren sich vorrangig auf Lösungen mit einer traditionellen Sicht auf die Cloud. In diesen Angeboten stehen Virtualisierungskonzepte im Mittelpunkt, ganz im Sinne einer „Legacy Cloud“. Immer mehr Dienstleister entwickeln Services auf Basis cloudnativer Infrastrukturen und Konzepte in Form einer „Cloud-Native Cloud“. *Aus Sicht von IDC bieten „Cloud-Native Clouds“ mittel- bis langfristig einen beträchtlichen Mehrwert mit Blick auf IT-Modernisierung. Oder prägnanter formuliert: Eine erfolgreiche Digitalisierungsstory lässt sich nur mit Cloud-Native-Konzepten effizient umsetzen.* Das sollten Entscheider bereits frühzeitig bedenken. Idealerweise sollten Anbieter in beiden Welten zuhause sein, um Anwender umfassend in ihrer Transformation unterstützen zu können. Dafür ist eine flexible Vertragsgestaltung, die individuelle Angebote, Agilität und Flexibilität bei der Bereitstellung von IT-Ressourcen ermöglicht, essenziell für Cloud User. Kundennähe in ihren unterschiedlichen Facetten und Ausprägungen hat ganz grundlegenden Einfluss auf die Qualität einer Geschäftsbeziehung bzw. Partnerschaft. Entscheider müssen aber berücksichtigen, dass der Individualisierung von Servicekonzepten aufgrund der Provider-Geschäftsmodelle Grenzen gesetzt sind. Das Einhalten der vereinbarten Kennzahlen im Betrieb versteht sich bei einer Zusammenarbeit von selbst.

Um die Souveränität der Kundendaten garantieren zu können, müssen Dienstleister jederzeit technische, prozessuale und organisatorische Maßnahmen treffen, diese permanent aktualisieren und ihre Umsetzung kommunizieren (Abbildung 14).

Abbildung 14

Anforderungen an Cloud Provider bei Datenhoheit



N = 150 Unternehmen, Mehrfachnennungen, Abbildung gekürzt; Quelle: IDC, 2023

F.: Was sind für Ihr Unternehmen die wichtigsten Kriterien, die Ihr Cloud Provider bei der Datenhoheit erfüllen muss?

Darauf sollten IT-Abteilungen achten. Immerhin knapp ein Drittel der Befragten legt in diesem Zusammenhang Wert auf Confidential Computing. Rechenzentren weisen damit nach, dass ihre Lösungen auch auf Prozessorebene und/oder über Softwareerweiterungen in der Betriebssystem-/Hypervisor-Umgebung vertrauenswürdig sind. Das ist ein Kernelement des Sovereign Cloud Stack. Volle Souveränität ist erst dann möglich, wenn eine souveräne Cloud zum Einsatz kommt und diese Cloud lokal verfügbar ist. Souveränität basiert auf geschäftlichen und rechtlichen Vereinbarungen sowie Vertrauen. Unternehmen bevorzugen in der Regel das „stimmige“ Gesamtpaket und lassen sich weniger als bisher auf Kompromisse mit dem Provider ein, wenn sich Alternativen bieten.

Fazit und Ausblick

Können Unternehmen im Jahr 2023 die Cloud und das Thema Datenhoheit für ihre IT-Modernisierung und für digitale Geschäftsmodelle und digitale Services noch ignorieren? Die Antwort ist eindeutig und lautet Nein.

Für IDC ist moderne cloudbasierte Informationstechnologie ein wesentlicher Faktor zur Sicherstellung des Tagesgeschäfts und ein wichtiger Enabler der digitalen Transformation. Sie ermöglicht auf Basis von Standards und offenen Technologien, auf die geopolitischen Herausforderungen und den hohen Wettbewerbsdruck proaktiv und vorausschauend zu reagieren.

Der Wert der Cloud wird durch Datenhoheit deutlich gesteigert, denn die Selbstbestimmung von Unternehmen in digitalen Ökosystemen stärkt die operative Excellence im geschäftlichen Alltag und die Innovationskraft, indem sie frei entscheiden können, welche Daten wie, wo und von wem digital verarbeitet werden.

Eine umfassende Souveränität ist aber erst mit einer souveränen Cloud gegeben. Ihr Mehrwert besteht neben der Umsetzung von Datenhoheit in einem souveränen Technologie-Stack und transparenten Betriebsmodellen in einer höheren Vertrauenswürdigkeit als Trusted Partner sowie geringeren Compliance-Hürden. Aus Perspektive der IT-Security verbessert eine souveräne Cloud die Autonomie und die Kontrolle über die eigenen Daten und externen Instanzen beim Provider.

Der Weg in die souveräne Cloud wird für viele Organisationen ein schrittweiser Prozess sein. Wichtig ist aus Sicht von IDC, Schritte zur Datenhoheit in der Cloud so zügig wie möglich zu gehen und die ersten Workloads dafür auszuwählen. Mittelfristig müssen die relevanten Anwendungen und Daten in die souveräne Cloud verlagert werden, um das Level an Souveränität zu erreichen, das Unternehmen im Wettbewerb benötigen.

Empfehlungen

1

Richten Sie Ihre IT-Modernisierung auf die digitale Transformation Ihres Unternehmens aus

Wählen Sie Modernisierungsansätze für Ihre IT, die langfristigen Nutzen statt schneller Vorteile bringen. Investieren Sie vorrangig in die IT-Infrastruktur und IT-Architektur, da hier die Grundlagen für den optimalen Einsatz flexibler und agiler Anwendungen gelegt werden. Schaffen Sie zunächst Transparenz über Ihre komplette IT-Ausstattung und Ihre IT-Prozesse, um die Defizite und den Nutzen zu erkennen. Priorisieren Sie, indem Sie ihre Systeme zunächst konsolidieren und harmonisieren und damit die Basis für eine digitale IT legen.

2

Fokussieren Sie sich auf Cloud Computing als Kern Ihrer zukunftsfähigen IT-Landschaft und IT-Architektur

Cloud Computing ermöglicht aufgrund von Standards und offenen Strukturen eine umfassende Automatisierung aller Abläufe und stärkt zugleich die Widerstandfähigkeit von Organisationen mit robusten Prozessen und Sicherheitsmechanismen der Provider. Prüfen Sie, welches Deployment-Modell – Hybrid Clouds, Multi Clouds, SaaS – Ihr Businessmodell am besten unterstützt. Evaluieren Sie den Wert von Cloud-Native-Architekturen. Sie steigern den Nutzwert und die Zukunftsfähigkeit einer nachhaltigen Cloud mit Orchestrierung, Microservices und verschiedenen Ops-Modellen erheblich.

3

Stellen Sie Datenhoheit in den Mittelpunkt Ihrer Cloud-Strategie

Da die Daten das Kernasset jeder Organisation sind, müssen Sie jederzeit die vollständige und souveräne Verfügungsgewalt über Ihre Daten besitzen. Entwickeln Sie eine Vorgehensweise zum Erreichen von Datenhoheit für die relevanten Workloads und Daten in der Cloud. Achten Sie bei der Speicherung Ihrer Daten auf die Kontrolle über den Datenzugriff und die Datenübertragung und die Portierbarkeit der Daten. Prüfen Sie, ob die etablierten Methoden des Datenschutzes und der Datensicherheit vollständig implementiert sind.

4

Betrachten Sie die souveräne Cloud als die aktuell umfassendste Form zum Schutz Ihrer Daten bei Providern

Datenhoheit ist ein zentrales, aber nicht das einzige Element einer souveränen Cloud. Aus diesem Grund empfiehlt IDC stärker als bisher, auf Provider zu achten, die souveräne Clouds auf Basis des Sovereigns Cloud Stack anbieten und ihre souveränen Clouds lokal zur Verfügung stellen. Prüfen Sie, ob Ihre Daten-Governance die Anforderungen einer souveränen Cloud erfüllt, und schulen Sie Ihre Mitarbeiter über den Nutzen einer souveränen Cloud.

5

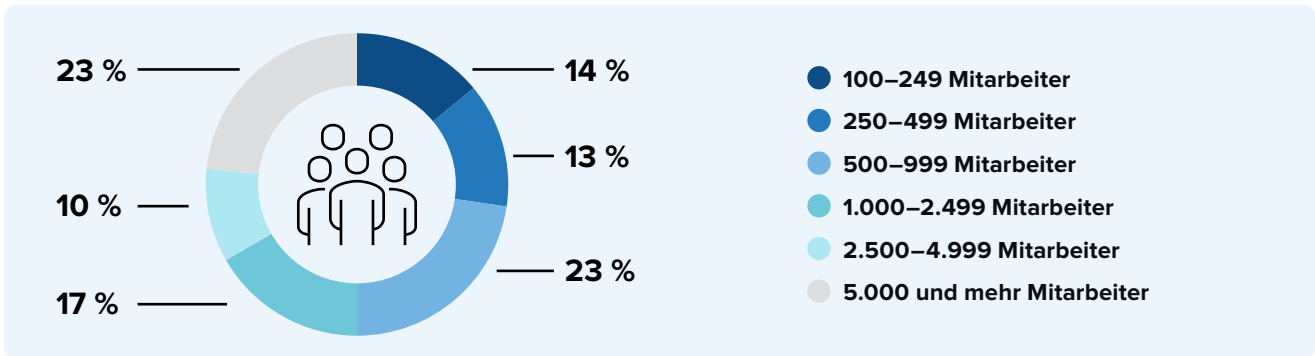
Achten Sie bei der Providerauswahl auf eine vertrauensvolle Geschäftsbeziehung und ein breites Angebot von Cloud Services, um immer mehr Workloads souverän betreiben zu lassen

Migration in die und das Management der souveränen Cloud sind wegen ihrer Komplexität schwierige Aufgaben. Da spezielles Know-how zur Bewertung der angebotenen und der erbrachten Leistungen benötigt wird, müssen Sie sich auf Ihren Provider verlassen können. Berücksichtigen Sie, dass Sie nach wie vor die rechtliche Verantwortung für die Nutzung der Services tragen. Zudem sollte der Anbieter unterschiedliche Cloud Services anbieten, damit Sie die Zahl der souverän betriebenen Workloads Ihren Businessanforderungen entsprechend rasch ausbauen können.

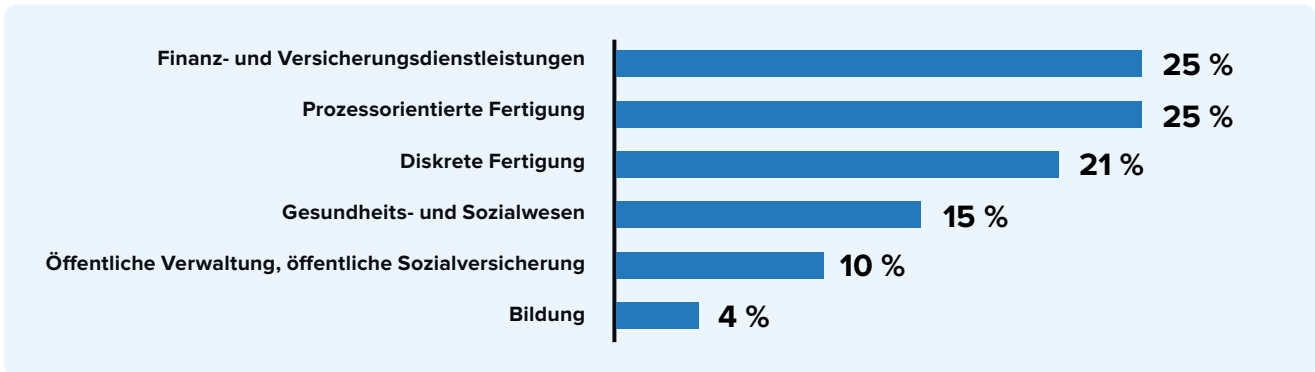
Methodik

Die Ergebnisse dieses White Papers basieren auf einer Befragung von 150 IT-Entscheidern von Unternehmen mit mehr als 100 Mitarbeitern aus Deutschland im September 2022. Alle Entscheider können in ihren Unternehmen über den Einsatz von Cloud-Technologie und Cloud Services entscheiden oder solche Entscheidungen beeinflussen.

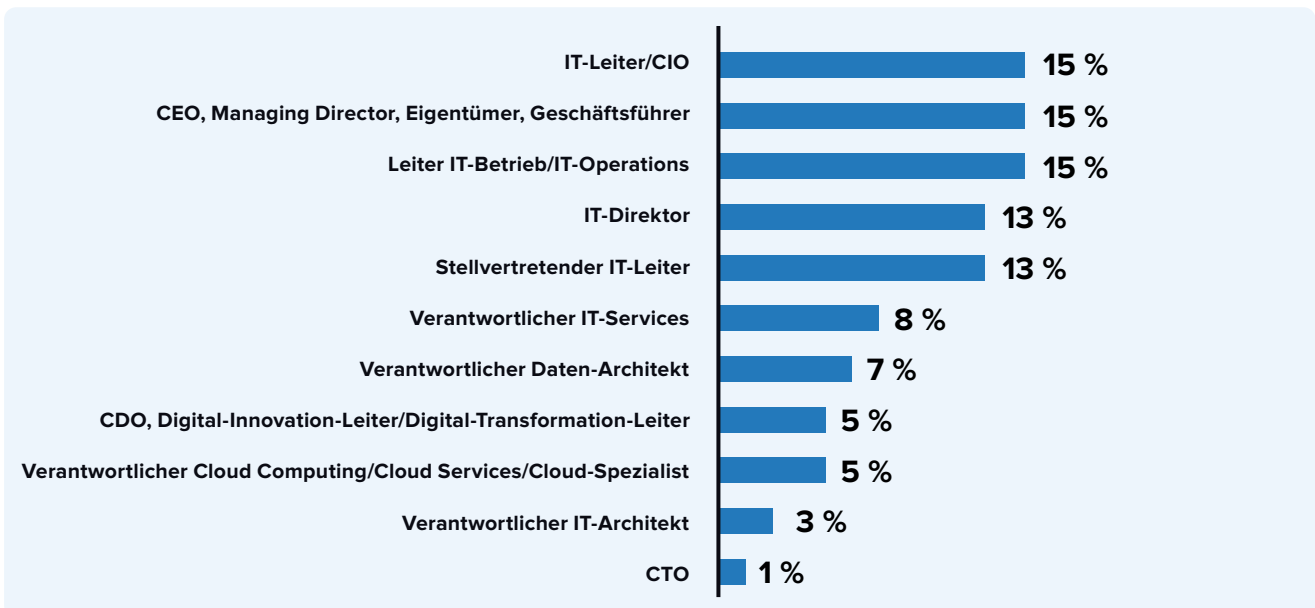
Unternehmensgrößenklassen



Branchen



Position der Entscheider



Interview

MIT:

Alexander Wallner
CEO plusserver



plusserver

IDC: Die Modernisierung der IT ist für viele Unternehmen eine dringliche Aufgabe. Warum ist das Thema augenblicklich so wichtig und was sind aus Ihrer Sicht die grundlegenden Themen der IT-Modernisierung, die Entscheider jetzt angehen müssen?

Alexander Wallner: Die Modernisierung der Unternehmens-IT hat seit einiger Zeit oberste Priorität bei Entscheider:innen, und das über alle Branchen hinweg. Die Studie zeigt klar, wo der Nachholbedarf der Unternehmen am größten ist: Weniger als ein Viertel der befragten Unternehmen schätzen ihre Agilität als „Sehr hoch“ ein. Angesichts der geopolitischen und wirtschaftlichen Lage werden mehr Agilität sowie eine widerstandsfähige IT-Infrastruktur immer wichtiger für die Geschäftskontinuität. Neue Geschäftsmodelle und die steigenden Gefahren durch Cyberkriminalität machen der IT zu schaffen. Die Anforderungen an einen effizienten IT-Betrieb lassen sich oftmals mit den bestehenden Legacy-Strukturen nur schwer erfüllen und einen Stillstand beziehungsweise Ausfall der IT kann sich kein Unternehmen, das im globalen Wettbewerb steht, erlauben. Vor diesem Hintergrund sind die Antworten der befragten Entscheider:innen gut nachvollziehbar: Sie sehen mit 29 Prozent die neue strategische Ausrichtung ihres Unternehmens als Hauptgrund für die Modernisierung der IT. Weitere 28 Prozent nennen den hohen Verwaltungsaufwand für bestehende Systeme sowie ein Viertel die zunehmenden Ausfälle im IT-Betrieb als Hauptgründe für die Modernisierung der IT.

Diese Anforderungen sind zusammen mit den Auswirkungen der Corona-Pandemie maßgebliche Treiber der Cloud-Transformation, da die unzähligen Vorteile der IT in der Cloud immer deutlicher werden. Aus Agilitäts-, Kosten- als auch aus Energieeffizienzgründen macht der Umstieg Sinn. Die bestehende Legacy hält viele Unternehmen auf: Sie müssten massive Investitionen tätigen, um eigene Rechenzentren zu modernisieren, die Hardware zu aktualisieren und damit energieeffizient zu machen.

Der Weg in die Cloud ist aus meiner Sicht daher untrennbar mit der IT-Modernisierung verbunden, doch bei der Umsetzung gibt es verschiedene Ansätze. Hybrid Cloud, Public und Private Clouds haben alle ihre Stärken und Herausforderungen und es ist wichtig, dass Entscheider:innen sich mit den unterschiedlichen Konzepten intensiv beschäftigen, um die beste Lösung für die individuellen

Bedürfnisse ihres Unternehmens zu finden. Welche Lösung kostet mich wie viel? Welche Funktionen werden mir angeboten und ist der Betrieb meiner Applikationen überhaupt machbar in der Cloud? Und nicht zuletzt muss bei der IT-Modernisierung in der Cloud natürlich der Business Value im Blick behalten werden, der am Ende entsteht.

Damit einher geht das Thema „Datenstrategie“. Hier muss geklärt werden, welche Daten die Kernwertschöpfung des Unternehmens ausmachen und wo sich diese Daten jetzt beziehungsweise in Zukunft befinden. Dieses Fundament ist entscheidend und die Modernisierung der IT sollte stets mit diesen Fragen im Hinterkopf angegangen werden.

Zu guter Letzt bedarf es aus meiner Sicht einer Machbarkeitsprüfung: Wie steht es um die internen Kapazitäten und die Expertise? Letztere ist oftmals spärlich vorhanden, gerade wenn es um dedizierte Cloud-Lösungen geht. Entscheider:innen sollten sich also gut überlegen, ob sie diese Expertise intern aufbauen wollen und müssen oder ob die Zusammenarbeit mit einem externen Partner sinnvoller ist.

IDC: Datenhoheit ist ein kritischer Aspekt, der noch mehr Aufmerksamkeit benötigt als bisher. Warum ist Datenhoheit aus Ihrer Sicht wichtig?

Wallner: Datenhoheit ist das Kernelement für die Geschäftsmodelle der Zukunft – gleichzeitig zeigen die Studienergebnisse aber, dass erst 11 Prozent der deutschen Unternehmen eine Strategie für souveräne Daten umgesetzt haben. Um zu begreifen, was das heißt, muss man erst den Begriff verstehen: Datenhoheit bzw. Datensouveränität beschreibt die selbstbestimmte Kontrolle von Unternehmen und Personen bei der Erhebung, Speicherung, Nutzung und Verarbeitung eigener Daten. Es geht also kurz gesagt darum, dass ich zu jeder Zeit weiß, wo meine Daten gerade sind und ob sie dort sicher sind. Viele Unternehmen können im ersten Moment mit dieser Definition nichts anfangen – obwohl Daten heute der Wirtschaftstreiber Nummer eins sind.

Immerhin zeigen unsere Ergebnisse auch, dass 43 Prozent der Unternehmen bereits an einer Umsetzung der Datenhoheit arbeiten. Diese Umsetzung muss nun aber konsequent verfolgt werden und darf nicht auf die lange Bank geschoben werden. Denn im Kern ermöglicht Datenhoheit zwei grundlegende Unternehmensgrundsätze: sicheres Business und Innovation.

In einer immer stärker vernetzten Welt werden Kooperationen und die Zusammenarbeit – auch mit Wettbewerbern – zur Normalität. Die Cloud ermöglicht heute immer und überall, mit Geschäftspartnern und anderen Stakeholdern zu interagieren und Daten auszutauschen beziehungsweise auf Daten zuzugreifen. Gleichzeitig müssen Geschäftsgeheimnisse weiterhin geschützt werden und sensible Informationen, etwa personenbezogene Kundendaten, dürfen ohnehin nicht ohne explizites Einverständnis ausgetauscht werden.

Das Gleiche gilt, wenn Daten zum Geschäftsmodell werden: Wertschöpfung entsteht in der Datenökonomie, indem Daten angereichert und gewinnbringend eingesetzt werden können. Dafür beziehen Unternehmen schon heute Daten aus öffentlichen Quellen und geben sie auch selbst heraus, um Innovation zu fördern – etwa in Zusammenarbeit mit Start-ups. Unternehmen unterliegen in unterschiedlichen Teilen der Welt teils starken Kontrollen durch staatliche Akteure, die sie zur Herausgabe von Informationen zwingen können. Das bedeutet nicht, dass eine Zusammenarbeit mit solchen Unternehmen falsch wäre, es heißt nur, dass Datenhoheit in solchen Geschäftsbeziehungen noch stärker bewahrt werden muss, insbesondere wenn es sich um sensible Daten handelt.

Wenn man bedenkt, dass durchschnittlich 43 Prozent der Daten von den Befragten als hochsensibel eingestuft wurden und damit personenbezogene Daten, Produkt- und Produktentwicklungsdaten sowie Finanzdaten gemeint sind, wird klar, warum sich hier ein genauer Blick lohnt.

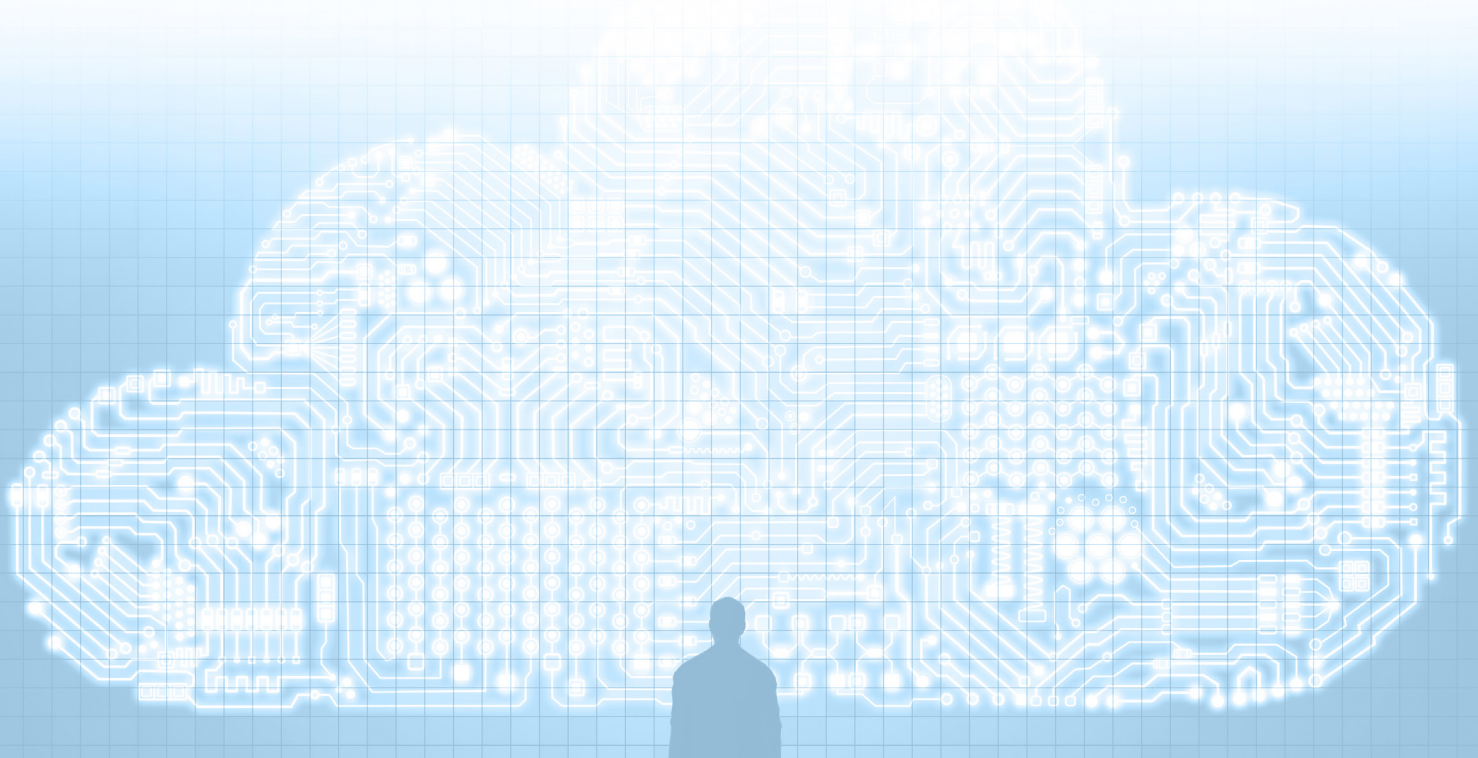
All diese Gegebenheiten untermalen, warum das Thema Datenhoheit so fundamental wichtig für Unternehmen ist. Beide Aspekte, die Datensicherheit und die Datenhoheit, spielen zusammen und dürfen in der oben erwähnten Datenstrategie auf keinen Fall fehlen.

IDC: Welche konkreten Schritte empfehlen Sie IT-Verantwortlichen und CIOs, um Cloud Computing als zentrales Element der IT-Modernisierung unter den Aspekten Datensicherheit, Datenhoheit und Nachhaltigkeit einführen und nutzen zu können?

Wallner: 61 Prozent der Befragten planen mittel- und langfristig eine intensivere Nutzung von Cloud Services als bisher. Wer heute Cloud Computing sicher und souverän nutzen möchte, um seine IT zu modernisieren und zukunftsfähig zu gestalten, der braucht eine entsprechende Strategie für den Weg in die Cloud und eine Datenstrategie für die Arbeit in der Cloud. Hier muss zunächst definiert werden, welche Daten ein besonders hohes Schutzniveau benötigen und ob diese Daten überhaupt in die Cloud dürfen. Dies gilt umso mehr beim Einsatz von Public-Cloud-Lösungen. Sensible Daten sollte man, soweit sie in der Cloud benötigt werden, stets in einer europäischen Cloud vorhalten. Hiermit schließt man Interessenkonflikte bei den Anbietern aufgrund rechtlicher Vorgaben – und damit eine gewisse Abhängigkeit vom politischen Willen – von vornherein aus.

Zudem sollte neben der Wahl der für das eigene Unternehmen „richtigen“ Cloud beziehungsweise Clouds – in einem Hybrid- oder Multi-Cloud-Setup – zunächst der Cloud-Readiness-Check im Mittelpunkt stehen: Hierbei lohnt sich ein umfangreiches Assessment der bestehenden IT-Infrastruktur, welches im Idealfall mithilfe von externen Expert:innen durchgeführt wird. Dabei geht es um die Frage, welche Daten und Prozesse in der Cloud vorgehalten beziehungsweise betrieben werden sollen – und damit von Anfang an um den Fokus auf Datenhoheit.

Daneben sollten sich CIOs mit interoperablen Lösungen beschäftigen, denn Datenhoheit bedeutet nicht nur, dass man jederzeit über den Ort und die Sicherheit der Daten informiert ist, sondern dass man frei über die Daten verfügt. Dazu gehört auch, dass man seine Informationen, Anwendungen und Systeme problemlos von einem Cloud-Anbieter zu einem anderen verschieben kann und eine providerübergreifende sichere Nutzung ohne das Risiko eines Vendor Lock-ins gegeben ist.



ÜBER IDC

IDC ist der weltweit führende Anbieter von Marktinformationen, Beratungsdienstleistungen und Veranstaltungen auf dem Gebiet der Informationstechnologie und der Telekommunikation. IDC analysiert und prognostiziert technologische und branchenbezogene Trends und Potenziale und ermöglicht ihren Kunden so eine fundierte Planung ihrer Geschäftsstrategien sowie ihres IT-Einkaufs. Durch das Netzwerk der mehr als 1100 Analysten in über 110 Ländern mit globaler, regionaler und lokaler Expertise kann IDC ihren Kunden umfassenden Research zu den verschiedensten Segmenten des IT-, TK- und Consumer-Marktes zur Verfügung stellen. Seit mehr als 50 Jahren vertrauen Business-Verantwortliche und IT-Führungskräfte bei der Entscheidungsfindung auf IDC.

Weitere Informationen sind auf unseren Webseiten unter www.idc.com oder www.idc.de zu finden.

COPYRIGHT-HINWEIS

Die externe Veröffentlichung von IDC Informationen und Daten – dies umfasst alle IDC Daten und Aussagen, die für Werbezwecke, Presseerklärungen oder anderweitige Publikationen verwendet werden – setzt eine schriftliche Genehmigung des zuständigen IDC Vice President oder des jeweiligen Country Managers bzw. Geschäftsführers voraus. Ein Entwurf des zu veröffentlichenden Textes muss der Anfrage beigelegt werden. IDC behält sich das Recht vor, eine externe Veröffentlichung der Daten abzulehnen.

Für weitere Informationen bezüglich dieser Veröffentlichung kontaktieren Sie bitte:

Lynn-Kristin Thorenz, Associate Vice President, Research & Consulting, IDC • E-Mail: lthorenz@idc.com



 @idc

 @idc

idc.com