EXOSCALE
member of | A1 Digital

Cloud-Computing: Wie Unternehmen den richtigen Cloud-Anbieter finden

Rechtliche, betriebswirtschaftliche und technische Auswahlkriterien für den Cloud-Einsatz

Cloud-Computing: Wie Unternehmen den richtigen Cloud-Anbieter finden

Rechtliche, betriebswirtschaftliche und technische Auswahlkriterien für den Cloud-Einsatz

Cloud-Computing ist mittlerweile auch in Deutschland angekommen. Im Jahr 2016 erklärten noch 17 Prozent der Teilnehmer an der jährlich erscheinenden „Cloud Monitor"-Studie von Bitkom Research und KPMG, die Cloud sei für sie kein Thema. Im Jahr 2022 waren es hingegen nur noch drei Prozent[1]. Skeptischer sind deutsche Unternehmen allerdings nach wie vor, wenn es um öffentliche Cloud-Ressourcen in einer sogenannten Public Cloud geht (Begriffsdefinition siehe Kasten auf Seite 6). Nach aktuellen Zahlen des Digitalverbands Bitkom nutzen erst 55 Prozent der Befragten dieses Bereitstellungsmodell, weitere 29 Prozent planen oder diskutieren den Einsatz[2].

Die Zurückhaltung ist verständlich, denn gerade in mittelständischen Unternehmen will der Schritt in die Public Cloud wohlüberlegt und gut geplant sein. Es gibt viele Fragen zu klären, etwa die nach Datenschutz und -souveränität, Rechtskonformität und Sicherheit. Oft schrecken auch komplexe Angebote, hohe Einstiegshürden und intransparente Preisgestaltungen von der Nutzung ab. Es besteht jedoch kein Zweifel daran, dass es der digitalen Transformation ohne die Public Cloud an Geschwindigkeit mangelt. Die Analysten der Förderbank KfW beklagen regelmäßig das schleppende Digitalisierungstempo im Mittelstand[3]. Wie eine aktuelle Studie von KfW Research zeigt, leiden vor allem Unternehmen mit ambitionierten Wettbewerbsstrategien unter Digitalisierungshemmnissen[4].

Dieses Whitepaper unterstützt Mittelständler dabei, schnell und erfolgreich in die Public Cloud zu starten und gibt Entscheidungshilfen für die Auswahl des richtigen Cloud-Anbieters an die Hand. Dabei finden rechtliche, betriebswirtschaftliche und technische Aspekte ebenso Berücksichtigung wie die spezifischen Herausforderungen im Mittelstand.

---

[1] https://kpmg.com/de/de/home/themen/2022/06/cloud-monitor-2022.html

[2] https://www.bitkom.org/sites/main/files/2023-05/230516Bitkom-ChartsCloud-Reportfinal.pdf

[3] https://www.kfw.de/%c3%9cber-die-KfW/KfW-Research/Digitalisierung.html

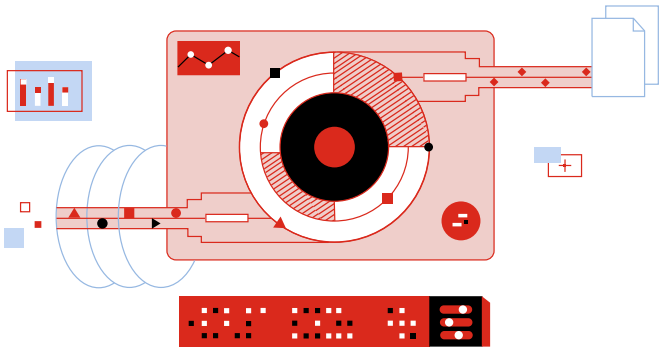
[4] https://www.kfw.de/PDF/Download-Center/Konzernthemen/Research/PDF-Dokumente-Fokus-Volkswirtschaft/Fokus-2023/Fokus-Nr.-432-Juli-2023-Digihemmnisse-Strategie.pdf

1 Rechtliche Aspekte der Cloud-Wahl: Datenschutz, IT-Sicherheit, Compliance

a) Datenschutz

Seit Mai 2018 gilt in der Europäischen Union die Datenschutzgrundverordnung (DSGVO)[5]. Sie soll in allen Mitgliedsstaaten ein einheitliches und hohes Datenschutzniveau schaffen. Firmen dürfen personenbezogene Daten nur mit Zustimmung der Betroffenen erfassen und verwenden. Bei der Zusammenarbeit mit IT-Dienstleistern oder einem Cloud-Provider ist das auftraggebende Unternehmen für die Einhaltung der Bestimmungen verantwortlich. Zuwiderhandlungen können Geldbußen bis zu 20 Millionen Euro oder vier Prozent des weltweiten Jahresumsatzes nach sich ziehen. Werden personenbezogene Daten, die unter die Bestimmungen der DSGVO fallen, in Drittstaaten transferiert, müssen diese ein der Europäischen Union vergleichbares Datenschutzniveau bieten. Das ist zum Beispiel in Island, Liechtenstein und Norwegen der Fall, da diese Länder die Datenschutzgrundverordnung in ihr nationales Recht übernommen haben. Auch Japan und die Schweiz gelten als Staaten mit angemessenem Datenschutzniveau.

Rechtlich problematisch ist dagegen die Übermittlung an einen US-Provider. Der 2018 in Kraft getretene CLOUD Act (Clarifying Lawful Overseas Use of Data)[6] verpflichtet amerikanische Firmen, Kundendaten an US-Behörden herauszugeben – selbst dann, wenn diese nicht in den USA gespeichert sind. Die Betroffenen erfahren nicht, dass ihre Daten kompromittiert wurden, weil die US-Behörden die Provider durch eine sogenannte „Gagging Order“ zum Stillschweigen verpflichten können. Der Europäische Gerichtshof (EuGH) hat deshalb mehrfach festgestellt, dass in den USA kein angemessenes Datenschutzniveau herrscht. In einem Urteil vom Juli 2020 (Schrems II)[7] kippte er das zwischen der EU und den USA vereinbarte Privacy Shield, das einen datenschutzkonformen Datenaustausch ermöglichen sollte. Ein legaler Austausch personenbezogener Daten mit den USA war danach ohne zusätzliche Garantien nicht mehr möglich.



Seit Juli 2023 gilt der Nachfolger des Privacy Shields, das EU-US Data Privacy Framework (EU-US DPF)[8]. Es stellt einen sogenannten „Ange-

[5] https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=de

[6] https://www.justice.gov/criminal/cloud-act-resources

[7] https://www.bfdi.bund.de/SharedDocs/Downloads/DE/EU_UN/Kernaussagen-Schrems-II.pdf?__blob=publicationFile&v=4

[8] https://ec.europa.eu/commission/presscorner/detail/de/qanda_23_3752

messenheitsbeschluss“ dar, in dem die Europäische Kommission den USA ein mit der EU vergleichbares Datenschutzniveau attestiert. Das EU-US DPF beschränkt sich allerdings auf zertifizierte US-Organisationen, die sich zur Einhaltung der Datenschutzrichtlinien verpflichtet haben. Näheres dazu findet sich in den Anwendungshinweisen der Datenschutzkonferenz[9], einem Gremium der deutschen Datenschutzaufsichtsbehörden.

Ob das EU-US DPF einer rechtlichen Überprüfung durch den EuGH standhält, ist fraglich. Schließlich hat sich am Grundproblem nichts geändert. US-Behörden können nach wie vor auf Daten europäischer Unternehmen und Bürger zugreifen. Organisationen, die personenbezogene Daten mit US-Providern austauschen, gehen deshalb weiterhin rechtliche Risiken ein.

b) IT-Sicherheit

Cybergefahren gelten als Risiko Nummer eins für die wirtschaftliche Existenz von Unternehmen[10]. Sie gefährden aber auch zunehmend die Sicherheit und Versorgung der Bevölkerung – zahlreiche Gesundheitseinrichtungen, Kommunen und Städte wurden bereits gehackt. Zu den aktuellsten Fällen gehören Ransomware-Angriffe auf das Uniklinikum Frankfurt im Oktober 2023[11] und den kommunalen IT-Dienstleister Südwestfalen-IT im November 2023[12]. Die Gesetzgeber auf nationaler und europäischer Ebene erlassen deshalb immer strengere Vorgaben, die vor allem, aber nicht nur die Betreiber sogenannter kritischer Infrastrukturen (KRITIS) betreffen. Zu nennen sind etwa das IT-Sicherheitsgesetz 2.0 (ITSIG), das seit Mai 2021 in Deutschland gilt, sowie die EU-Richtlinie für Netzwerk- und Informationssicherheit NIS 2[13], die im Januar 2023 in Kraft trat und bis Mitte Oktober 2024 in nationales Recht umgesetzt werden muss.

Bei der Cloud-Wahl spielt vor allem die in NIS 2 vorgeschriebene Lieferkettensicherheit eine Rolle. Betroffene Unternehmen müssen nicht nur selbst alle Vorschriften

[9] https://datenschutzkonferenz-online.de/media/ah/230904_DSK_Ah_EU_US.pdf

[10] https://www.allianz.com/de/presse/news/studien/230117_Allianz-Risk-Barometer-2023.html

[11] https://www.heise.de/news/Angriffsversuch-durch-Hacker-Uniklinikum-Frankfurt-offline-9328925.html

[12] https://www.heise.de/news/Nach-Ransomware-Angriff-Suedwestfalen-IT-und-Kommunen-lehnen-Loesegeldzahlung-ab-9386564.html

[13] https://eur-lex.europa.eu/eli/dir/2022/2555/oj

einhalten, sondern auch nachweisen, dass sämtliche Lieferanten und Dienstleister ein den Anforderungen entsprechendes Sicherheitsniveau aufweisen.

c) Compliance

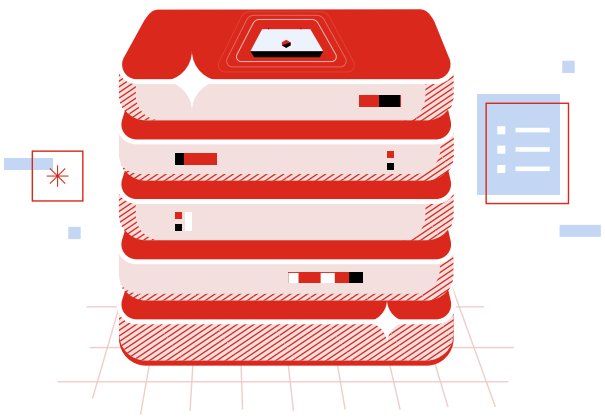
Gesetzesverstöße können erhebliche wirtschaftliche Folgen nach sich ziehen. Nicht nur die DSGVO sieht bei Zuwiderhandlung hohe Geldbußen vor, auch in der NIS-Novelle wurde der Strafrahmen deutlich ausgeweitet. Die Maximalstrafe beträgt hier nun zehn Millionen Euro. Bei strafrechtlich relevanten Tatbeständen wie Untreue, Verletzung von Buchführungspflichten oder Umweltdelikten drohen den Verantwortlichen sogar Haftstrafen. Verstöße gegen Wettbewerbs-, Verbraucher- oder Arbeitnehmerrechte führen darüber hinaus regelmäßig zu Abmahnungen, Bußgeldern oder Schmerzensgeld.

Firmen müssen deshalb Maßnahmen etablieren, die ein regel- und rechtskonformes Verhalten von Geschäftsführung und Belegschaft sicherstellen, zusammengefasst unter dem Begriff Compliance. Organisationen sollten zudem sicherstellen, dass auch bei Dienstleistern und Zulieferern alle Compliance-Aspekte Berücksichtigung finden.

Empfehlungen für die Cloud-Provider-Wahl aus Sicht von Datenschutz, Gesetzgebung und Compliance

1 Die Zusammenarbeit mit einem US-Provider birgt auch nach Verabschiedung des EU-US Data Privacy Frameworks hohe rechtliche Risiken. Unternehmen sollten lieber einen Provider wählen, der seinen Firmensitz in Europa hat und auch seine Rechenzentren in der EU betreibt. Das gewährleistet die Einhaltung aller DSGVO-Vorschriften.

2 Von NIS 2 betroffene Firmen dürfen in Zukunft nur noch mit Dienstleistern zusammenarbeiten, die ein entsprechend hohes Sicherheitsniveau aufweisen. Sie sollten daher einen Provider wählen, der die Anforderungen erfüllt und dies anhand geeigneter Zertifikate nachweisen kann. Dazu gehören beispielsweise die Sicherheitsnormen ISO/IEC 27001[14], ISO/IEC 27017 und ISO/IEC 27018, der vom Bundesamt für Sicherheit in der Informationstechnik



[14] https://www.iso.org/standard/27001

herausgegebene Cloud-Computing Compliance Criteria Catalogue (BSI C5)[15] und das SOC-2 Framework[16] (Trust Services Criteria Compliance).

3 Unternehmen müssen jederzeit einen Überblick über ihren Compliance-Status haben und mögliche Risiken schnell erkennen können. Ein guter Cloud-Provider stellt alle dafür notwendigen Informationen übersichtlich und zentral an einer Stelle zur Verfügung.

Cloud-Computing-Formen

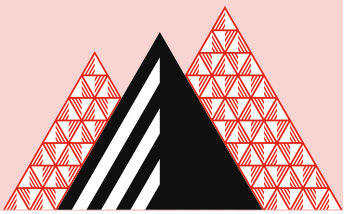
Nach der häufig verwendeten Definition des NIST (National Institute of Standards and Technology) existieren folgende Cloud-Computing-Formen:

Private Cloud: Die Cloud-Infrastruktur steht einem Unternehmen oder einer Abteilung zur exklusiven Nutzung zur Verfügung. Die Ressourcen können sich im eigenen Rechenzentrum, bei einem Hosting-Anbieter oder einem Provider befinden. Auch virtuelle Private-Cloud-Angebote innerhalb einer Public Cloud sind möglich.

Community Cloud: Organisationen mit gemeinsamen Interessen, Strukturen oder Sicherheitsanforderungen greifen auf eine gemeinsame Cloud-Infrastruktur zu. Diese kann von einem Provider, einem speziellen Dienstleister oder einer der beteiligten Organisationen betrieben werden.

Public Cloud: Die Cloud-Infrastruktur ist öffentlich über das Internet zugänglich. Sicherheit und Vertraulichkeit werden durch Verschlüsselung der Daten bei Transport und Speicherung gewährleistet.

Hybrid Cloud: Eine Mischform, bei der typischerweise Public-Cloud-Ressourcen mit lokalen IT-Infrastrukturen kombiniert werden, um Lastspitzen abzufangen oder das Serviceangebot zu erweitern.



[15] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html

[16] https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html

2 Betriebswirtschaftliche Aspekte der Cloud-Wahl: Kosten, Datensouveränität, Nachhaltigkeit

a) Kosten

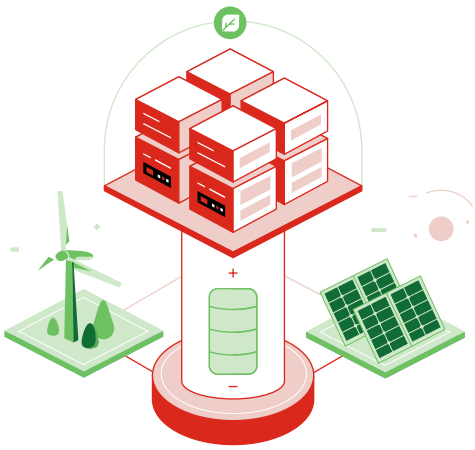
Cloud-Computing gilt als preiswerte Alternative zum IT-Betrieb im eigenen Rechenzentrum. Tatsächlich lassen sich besonders neue Ressourcen und Testumgebungen in der Cloud viel schneller und kostengünstiger aufbauen als in einem lokalen Datacenter. Der Kostenvorteil kann sich jedoch ins Gegenteil verkehren: Die nutzungsabhängige Abrechnung in der Cloud bringt es mit sich, dass ein hoher Bedarf auch die Kosten in die Höhe treibt. Entwickelt sich die Nachfrage unerwartet stark, führt das eventuell zu unangenehmen Überraschungen.

Firmen können sich aber auch anderweitig Preisnachteile einhandeln, wenn sie den Bedarf falsch einschätzen. Viele Cloud-Anbieter verlangen eine längerfristige Bindung oder die Buchung großer Kontingente vorab. Gerade am Anfang fällt es jedoch schwer, die Cloud-Nutzung einzuschätzen. Überschätzt man den Bedarf, zahlt man für Ressourcen, die man gar nicht nutzt. Ist das gebuchte Kontingent zu klein, muss oft zu hohen Preisen nachgeordert werden.

Auch versteckte Kosten können zu unangenehmen Überraschungen führen. Viele Provider bieten beispielsweise einen kostenlosen Datentransfer in ihre Cloud an, verlangen aber für die Gegenrichtung hohe Preise. Wenn Organisationen den Provider wechseln wollen oder regelmäßig große Datenmengen aus der Cloud beziehen, kann das viel Geld kosten.

b) Datensouveränität

Nach der Definition des Kompetenzzentrums Öffentliche IT[17] ist digitale Souveränität „die Summe aller Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können.“ Für Organisationen bedeutet dies vor allem, dass Geschäftsgeheimnisse gewahrt und im Unternehmen entstehende Daten selbst wirtschaftlich verwertet und vor fremdem Zugriff geschützt werden können. Auch die freie Entscheidung darüber, wo und in welcher Form die Speicherung von Geschäftsdaten erfolgt, gehört zur Datensouveränität.



[17] https://www.oeffentliche-it.de/documents/10181/14412/Digitale%20Souver%C3%A4nit%C3%A4t

Beim Datentransfer in die Cloud besteht die Gefahr, diese Souveränität zu verlieren. Wenn die Informationen unverschlüsselt übertragen und gespeichert oder die Schlüssel vom Cloud-Provider verwaltet werden, kann es zum Verlust der Datensouveränität kommen. Auch unter dem Aspekt der Datensouveränität ist die Nutzung US-amerikanischer Cloud-Angebote daher problematisch, denn diese sind dazu verpflichtet, Kundendaten an Behörden herauszugeben. Ob diese Befugnisse nur zur Strafverfolgung verwendet oder auch zur Industriespionage missbraucht werden, lässt sich aus europäischer Sicht nicht herausfinden.

c) Nachhaltigkeit

Das energieeffiziente und ressourcenschonende Wirtschaften spielt eine immer wichtigere Rolle. Neben Kostenaspekten und Klimawandel verpflichten besonders auch rechtliche Vorgaben zum nachhaltigen Handeln. Im Januar 2023 trat die Corporate Sustainability Reporting Directive (CSRD)[18] in Kraft, die Organisationen zum Reporting ihrer Nachhaltigkeitsinitiativen verpflichtet. Sie gilt zunächst für Unternehmen mit mehr als 500 Angestellten, der Kreis der Betroffenen wächst aber bis 2028 erheblich.

Betroffene Betriebe müssen in einem jährlichen Bericht Rechenschaft über ihre nichtfinanziellen Aktivitäten ablegen, der den European Sustainability Reporting Standards (ESRS) entspricht. Dabei müssen sie nicht nur alle relevanten Aktivitäten innerhalb des Unternehmens dokumentieren, sondern auch nachweisen, dass sich ihre Lieferanten und IT-Dienstleister ebenfalls an Nachhaltigkeits- und Sozialstandards halten.

Empfehlungen für die Cloud-Provider-Wahl aus Sicht von Kosten, Datensouveränität und Nachhaltigkeit

1 Unternehmen sollten bei der Wahl des Providers auf eine faire, sekundengenaue Abrechnung ohne versteckte Kosten, lange Vertragsbindung und komplizierte Abnahmekonstrukte achten.

2 In puncto Datensouveränität sollten Firmen einen Provider bevorzugen, der seinen Firmensitz in Europa hat und seine Rechenzentren dort betreibt.

3 Der Provider sollte nachweisen können, dass er nachhaltig und energieeffizient wirtschaftet. Die Daten sollten so bereitstehen, dass Kundenunternehmen sie leicht in ihre eigenen Nachhaltigkeitsreport übernehmen können.

[18] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2464

3 Technische Aspekte der Cloud-Wahl: Servicebreite, Komplexität, Support

a) Servicebreite

Neben der klassischen Einteilung in IaaS, PaaS und SaaS (siehe Kasten auf Seite 10) differenziert sich das Angebot an Cloud-Services immer weiter aus. Für mittelständische Kunden ist vor allem die richtige Balance zwischen Servicebreite und Übersichtlichkeit entscheidend. Fehlen wichtige Services, hindert dies das Unternehmen an der Weiterentwicklung. In einem übergroßen, unübersichtlichen Angebot gehen dagegen viel Zeit und Mühe mit dem Vergleich der Leistungen und der Auswahl passender Services verloren.

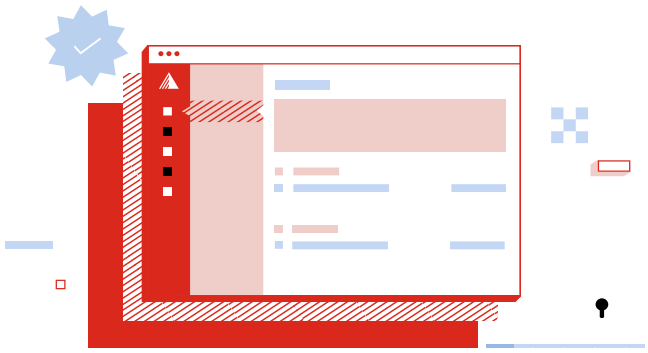
b) Komplexität

In der Informationstechnologie fehlen Fachkräfte. Laut dem Institut der deutschen Wirtschaft IW in Köln gab es im Jahr 2022 34.000 Stellen für IT-Fachpersonal, die nicht besetzt werden konnten. Im Mittelstand ist der Mangel an IT-Fachkräften besonders ausgeprägt, wie der European SME Survey zeigt[19].

Viele Cloud-Angebote erfordern jedoch einen hohen Grad an Expertenwissen und eine intensive Einarbeitung. Nicht selten beschäftigen große Unternehmen mehrere Cloud-Architekten, die sich mit nichts anderem beschäftigen als dem Design der Cloud-Umgebung. Für Mittelständler kommt die Beschäftigung von eigenen Cloud-Architekten in der Regel nicht infrage. Geeignete Fachkräfte sind teuer und kaum zu finden. Kosten und Aufwand wären für den Einstieg in das Cloud-Computing viel zu hoch. Deshalb verwundert es nicht, dass der Mangel an qualifiziertem Personal laut dem Bitkom Cloud Report 2023 das am häufigsten genannte Cloud-Hindernis darstellt[20].

c) Support

Cloud-Computing zeichnet sich durch hohe Verfügbarkeit aus und ist relativ robust gegenüber Fehlern. Dennoch kommt es auch in der Cloud immer wieder zu Ausfällen, beispielsweise 2021 beim Cloud-Provider Amazon Web Services[21] und Anfang 2023 in



[19] https://op.europa.eu/en/publication-detail/-/publication/12f499c0-461d-11ee-92e3-01aa75ed71a1/language-en

[20] https://www.bitkom.org/sites/main/files/2023-05/230516Bitkom-ChartsCloud-Reportfinal.pdf

[21] https://www.heise.de/hintergrund/Die-technischen-Hintergruende-von-Amazons-AWS-Ausfall-6293942.html

der Microsoft-Cloud Azure[22]. Vor allem kleine und mittelständische Kunden erhalten bei solchen Ereignissen oft wenige oder gar keine Informationen und werden mit den entstandenen Schäden wie Umsatzeinbußen oder Kundenverlusten allein gelassen.

Es muss aber gar kein Cloud-Ausfall sein, der guten Support schmerzlich vermissen lässt. Wenn Fragen zu Produktdetails oder Einstellungen ins Leere laufen und IT-Mitarbeiter bei Fehlern und Problemen nur in der Warteschleife oder bei einem Chatbot landen, leidet nicht nur die Nutzererfahrung, sondern auch die Sicherheit. Schließlich gehören Fehler bei der Konfiguration von Cloud-Ressourcen zu den größten Risiken im Cloud-Computing[23]. Ein schneller, persönlicher Support gilt deshalb als wichtiges Kriterium für die Cloud-Wahl.

DIE DREI EBENEN DER CLOUD-BEREITSTELLUNG

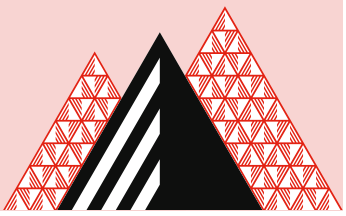
Cloud-Services lassen sich prinzipiell in drei Bereitstellungsmodelle unterteilen:

Infrastructure as a Service (IaaS): Der Provider stellt Server-, Storage- und Netzwerkkomponenten zur Verfügung, auf deren Basis Unternehmen eigene Betriebssysteme und Applikationen installieren und betreiben können. Die Komponenten liegen in der Regel virtualisiert vor, es gibt aber auch sogenannte Bare-Metal-Angebote, die einen direkten Zugriff auf Hardware-Ressourcen ermöglichen.

Platform as a Service (PaaS): Der Cloud-Anbieter stellt eine Plattform mit Betriebssystem, Middleware und Entwicklungswerkzeugen zur Verfügung. Firmen können darauf eigene Anwendungen entwickeln und betreiben.

Software as a Service (SaaS): In diesem Bereitstellungsmodell werden Applikationen als Service zur Verfügung gestellt. Der Zugriff erfolgt in der Regel geräteunabhängig über einen Browser.

Quelle: National Institute of Standards and Technology (NIST)



[22] https://www.heise.de/meinung/Kommentar-zum-Cloud-Ausfall-bei-MS-Ist-der-Patient-schon-tot-oder-nur-laediert-7484066.html

[23] https://cloudsecurityalliance.org/blog/2022/08/22/top-threat-3-to-cloud-computing-misconfiguration-and-inadequate-change-control/

Empfehlungen für die Cloud-Provider-Wahl aus Sicht von Servicebreite, Komplexität und Support

1 Der Cloud-Anbieter der Wahl sollte alle Services anbieten, die das Unternehmen benötigt. Als Vorteile erweisen sich eine klare, übersichtliche Struktur und eine Konzentration auf das Wesentliche. Ein übermäßig ausdifferenziertes Angebot überfordert schnell.

2 Für den Einstieg in das Cloud-Computing empfehlen sich einfache, leicht zu verstehende und zu bedienende Services. Idealerweise unterstützt der Cloud-Provider den Einstieg mit Informations- und Schulungsangeboten.

3 Erst im Fall von Problemen oder Fragen zeigt sich die Kundenfreundlichkeit eines Providers. Für weltweit tätige Konzerne sind mittelständische Kundenunternehmen häufig nur eine Nummer, die mit Chatbots und anderen automatisierten Angeboten abgespeist werden. Firmen sollten auf einen Support auf Augenhöhe achten und Provider bevorzugen, die schon beim First-Level-Support persönliche Ansprechpartner zur Verfügung stellen.

Fazit: Die erfolgreiche Reise in die Cloud braucht den richtigen Partner

Cloud-Computing ist ein unverzichtbarer Bestandteil jeder Digitalisierungsstrategie, auch in mittelständischen Unternehmen. Rechtliche Vorgaben, knappe Budgets sowie der Mangel an IT-Fachkräften erschweren es jedoch, die notwendige Geschwindigkeit zu erreichen. Unternehmen benötigen deshalb einen Cloud-Partner wie Exoscale, der alle oben genannten Kriterien erfüllt und sie bei der Reise in die Cloud optimal unterstützt. Mit seinem Firmensitz in der Schweiz und seinen europäischen Rechenzentren ist der Provider hundertprozentig DSGVO-konform und erfüllt alle oben genannten Sicherheitskriterien. Über das Compliance Center von Exoscale können Unternehmen einfach per Knopfdruck die Rechtskonformität ihrer Cloud-Nutzung jederzeit nachweisen.

Auch in betriebswirtschaftlicher Hinsicht überzeugt Exoscale: Die Kostenabrechnung erfolgt sekundengenau und fair, ohne Vertragsbindung oder komplizierte Tarifstrukturen. Der Datentransfer aus der Cloud kostet bis zu einem Volumen von einem Terabyte pro Instanz und pro Monat nichts. Alle Daten liegen in europäischen Rechenzentren, Unternehmen behalten die volle Souveränität über ihre Ressourcen. Exoscale hat sich außerdem zu einem nachhaltigen und klimaschonenden Wirtschaften verpflichtet und berichtet jährlich über den ESG-Report (Environmental, Social, Governance) der Muttergesellschaft A1 über seine Aktivitäten. Bis 2025 will der Provider zu hundert Prozent er-

neuerbare Energien nutzen. Alle Nachhaltigkeitszertifikate lassen sich jederzeit über das bereits erwähnte Compliance Center einsehen.

Schließlich bietet Exoscale auch aus technischer Sicht viele Vorteile. Der Provider führt alle für den Mittelstand relevanten Leistungen im Portfolio, ohne sein Angebot mit Hunderten oder Tausenden Services zu überfrachten. Der Einstieg ist einfach, bei Problemen oder Fragen erhalten Kundenunternehmen schon im First-Level-Support direkten Kontakt zu den Entwicklern. Die Exoscale Academy bietet zudem kostenlose Schulungs- und Zertifizierungsangebote.

Jetzt Exoscale kostenlos und unverbindlich testen >

Checkliste

Diese Fragen sollten Unternehmen dem Provider stellen

- ✓ Befinden sich die Rechenzentren in der Europäischen Union? Ist die Datenhaltung DSGVO-konform? Können fremde Behörden Zugriff auf die Daten erzwingen?
- ✓ Kann der Provider nachweisen, dass er alle Rechtsvorschriften erfüllt? Welche Sicherheitszertifikate bietet er?
- ✓ Wie können Kundenunternehmen dokumentieren, dass die Nutzung der Cloud-Angebote alle Compliance-Anforderungen abdeckt?
- ✓ Wie sieht die Kostenstruktur aus? Ist sie einfach und leicht zu verstehen – oder gibt es komplizierte Tarife und versteckte Kosten? Gelingt ein schneller Einstieg? Oder erfordert er hohe Vorabinvestitionen und eine lange Vertragsbindung?
- ✓ Achtet der Provider auf ein nachhaltiges, klimafreundliches Wirtschaften? Wie dokumentiert er seine Nachhaltigkeitsinitiativen?
- ✓ Bietet die Cloud-Plattform alle notwendigen Services, ohne überfrachtet und kompliziert zu sein? Wie einfach ist der Einstieg in die Nutzung?
- ✓ Welche Supportangebote bietet der Provider? Gibt es bei Problemen bereits im First-Level-Support einen menschlichen Ansprechpartner oder nur Kontakt zu einem Chatbot?
- ✓ Wie unterstützt der Provider Kunden beim Onboarding? Welche Schulungs- und Zertifizierungsangebote gibt es?

EXOSCALE

Einfach, sicher, skalierbar. Als europäischer Cloud-Provider unterstützt Exoscale seit mehr als 10 Jahren Unternehmen und Engineers ihre Workloads und Anwendungen sicher in der Cloud zu betreiben. Mit der benutzerfreundlichen, zuverlässigen und performanten Cloud-Plattform ist Exoscale der ideale Partner für Cloud-native Anwendungen. Unser Fokus auf Sicherheit und Datenschutz ermöglichet zudem eine reibungslose und DSGVO-konforme Nutzung der Cloud.

Kontakt >

EXOSCALE
member of | A1 Digital