Cloud-Szenarien für den Mittelstand

Zukunftssichere IT trotz hoher Anforderungen

BW.Tech

2025
www.bw.tech

Inhaltsverzeichnis

Executive Summary

Digitalisierung ist entscheidend für Unternehmen, um wettbewerbsfähig zu bleiben und an den Chancen moderner Technologien zu partizipieren. Ein populäres Beispiel ist die **künstliche Intelligenz**, die ohne die richtigen infrastrukturellen Weichenstellungen gar nicht genutzt werden kann.

Mit **Cloud Computing** können mittelständische Unternehmen Wertschöpfungsketten nachhaltig digitalisieren und automatisieren. So lassen sich Kosten senken und gleichzeitig komplexe IT-Projekte realisieren.

Finanzielle Einschränkungen und der Mangel an qualifiziertem IT-Personal und rechtliche Unsicherheiten erschweren den Weg in die Cloud. Dennoch gibt es Strategien und Lösungen, die diesen Hindernissen effektiv begegnen.

Eine gut durchdachte **Cloud-Strategie** kann nicht nur die digitale Transformation unterstützen, sondern auch die langfristige Wettbewerbsfähigkeit und Innovationskraft des Unternehmens stärken.

Jedes **Cloud-Computing-Modell** hat seine Vor- und Nachteile. Als Unternehmen gilt es abzuwägen, welche Lösung den individuellen Anforderungen am meisten gerecht wird.

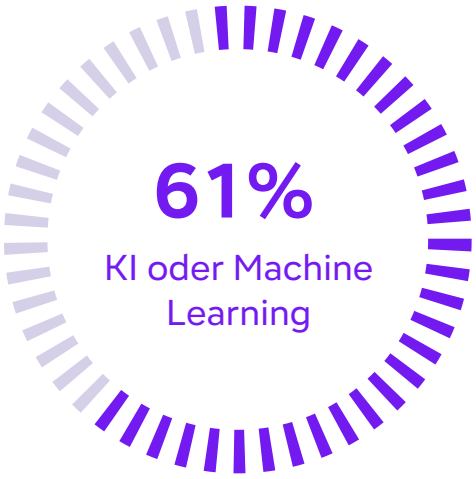
Mittelständische Unternehmen müssen bei der Wahl ihrer **Cloud-Hosting-Option** zwischen Sicherheitsanforderungen und Skalierbarkeit abwägen – eine Universallösung gibt es nicht. Auch Faktoren wie IT-Ressourcen und -Kompetenz, branchenspezifische Anforderungen und die Art der Workloads fließen in die Entscheidung ein.

1. Digitalisierung ist eine Chance

Der Digitalisierungsgrad ist für Unternehmen heute so entscheidend wie nie zuvor. Denn neue digitale Applikationen, wachsende Datenmengen und optimierte Produktions- und Arbeitsabläufe können nur in eine IT-Infrastruktur integriert werden, die den digitalen Anforderungen gewachsen ist. Wer hier nicht mithalten kann, leidet früher oder später unter massiven Wettbewerbsnachteilen. Ein mittlerweile altbekanntes Problem, zu dem nun ein neues hinzu kommt: Digitalisierung ist eine Voraussetzung für den Einsatz künstlicher Intelligenz.

Digitalisierung als Grundvoraussetzung für die Nutzung moderner Technologien

Laut aktueller Umfrageergebnisse der DIHK nutzen 61% der Unternehmen KI oder Machine Learning oder planen deren Einsatz in den nächsten Jahren.[1] Eine Steigerung um 24% zum Vorjahr, deren Trend sich in Zukunft fortsetzen wird.[2]



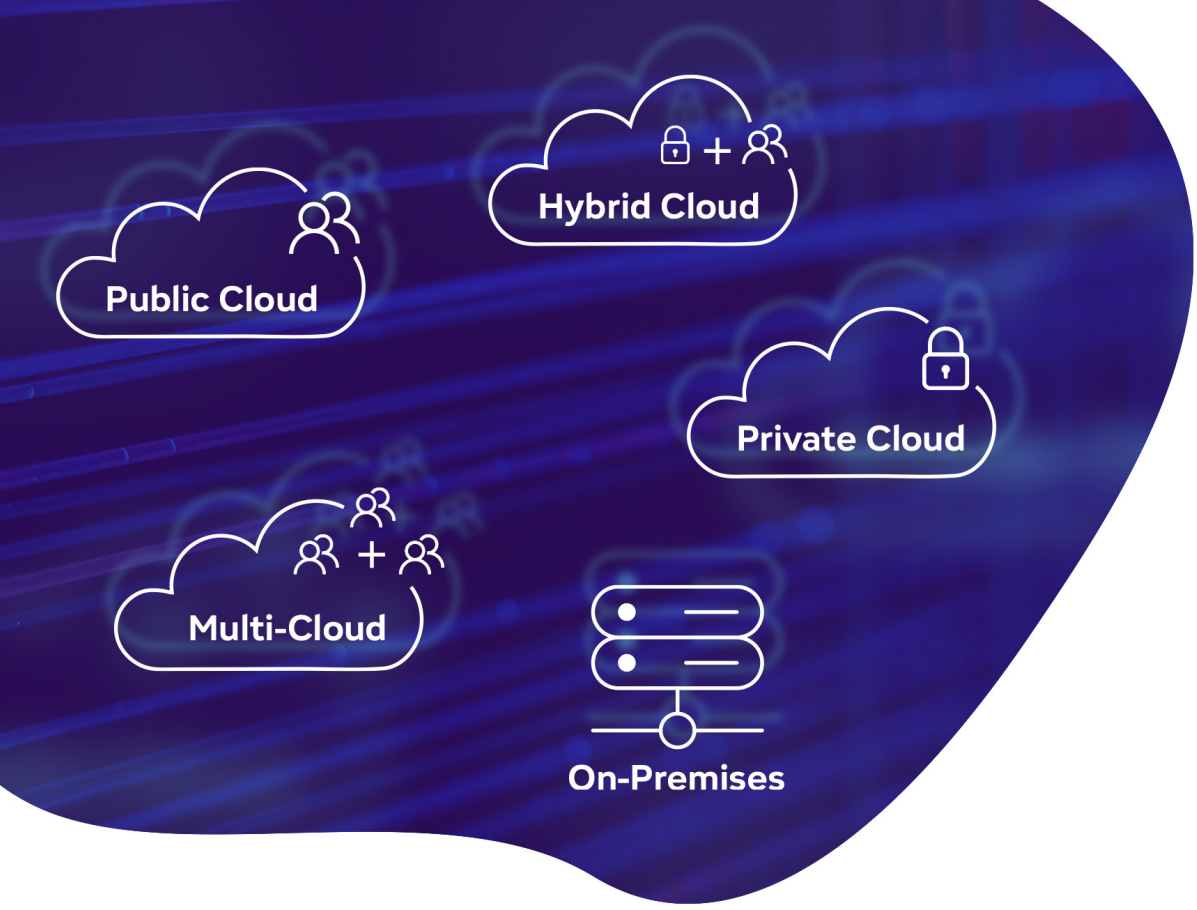
Im Umkehrschluss bedeuten diese 61% aber auch, dass viele Branchen derzeit noch das Potenzial verschenken, das der Einsatz künstlicher Intelligenz birgt – darunter vor allem **im Bau, aber auch im Handel und der Industrie.**[3] Grund dafür ist oft weniger das Wollen als das Können. Vielen Unternehmen fehlt es schlichtweg an einer IT-Infrastruktur, die den neuen Anforderungen standhält.

Die Umgebung, die einst ausreichte, um die täglichen Abläufe zu bewältigen, gerät mit zunehmender Digitalisierung, Automatisierung und Optimierung an ihre Grenzen. Eine Lösung muss her, die die aktuellen Anforderungen erfüllt und auch die zukünftige Entwicklung des Unternehmens unterstützt.

Doch wie kann dieser Weg realisiert werden, ohne dabei übermäßige Kosten und Komplexität zu verursachen?

Die Antwort liegt – wie so oft – in der Cloud.

[1] "Digitalisierung weiter eher Werkzeug als Innovationsmotor. Die DIHK-Digitalisierungsumfrage 2023", Deutsche Industrie- und Handelskammer, Berlin 2023; [2] ebd.; [3] ebd.



Cloud-Lösungen heute so relevant wie nie

Die Cloud ist unabdingbar – aber nicht als eine universelle Lösung, sondern als variables Werkzeug. Dabei geht es darum, Kosten zu sparen und Prozesse zu automatisieren, aber auch darum, eine IT-Umgebung zu schaffen, die flexibel, skalierbar und zukunftssicher ist.

Für mittelständische Unternehmen stehen zahlreiche Cloud-Hosting-Optionen zur Verfügung – von **Public Cloud über Private Cloud bis hin zu Hybrid- und Multi-Cloud-Lösungen**. Doch welche Option ist die beste für Ihr Unternehmen?

Eine pauschale Antwort darauf gibt es nicht, denn jedes Unternehmen hat individuelle Anforderungen, die individuelle Lösungen erfordern. **Die Wahl des richtigen Weges in die Cloud ist jedoch entscheidend und erfordert die Auswahl des optimalen Architektur- und Infrastrukturkonzepts, das den individuellen Herausforderungen und Anforderungen begegnet.**

Dieses Whitepaper soll deshalb einen Überblick geben, welche **Cloud-Hosting-Optionen** in mittelständischen Unternehmen zum Einsatz kommen können und wie Sie den Weg in die Cloud erfolgreich gestalten. Der Vergleich zwischen den Lösungen soll Ihnen dabei die Chance geben, die **ideale Cloud-Umgebung für Ihre individuellen Bedürfnisse zu finden**.

2. Herausforderungen und Anforderungen im Mittelstand

Auf dem Weg zu einer zukunftssicheren IT-Infrastruktur mit Cloud Computing stehen gerade mittelständische Unternehmen vor zahlreichen Herausforderungen. Doch hierfür gibt es Lösungen, die Modernisierung dennoch möglich machen. Wichtig ist nur, die Herausforderungen zu kennen, ihnen zu begegnen und Wege zu finden, diese zu meistern.

Finanzielle und personelle Hürden erschweren Digitalisierung

Die Digitalisierungsumfrage[4] und der Digitalisierungsindex 2023[5] verdeutlichen, dass viele Unternehmen in ihrer Entwicklung durch einen Mangel an finanziellen und personellen Mitteln[6] gebremst werden. Insbesondere fehlt es an qualifizierten Fachkräften, wie das Kompetenzbarometer des IW zeigt und eine Verstärkung des Problems bis 2027 prognostiziert.[7] Dieser Fachkräftemangel erschwert es vor allem kleinen und mittleren Unternehmen, moderne digitale Technologien zu integrieren.[8]

Kosteneffiziente, sichere und flexible Infrastrukturlösungen sowie der gezielte Einsatz von Fachkräften sind daher entscheidend, um die digitale Transformation erfolgreich voranzutreiben und die Wettbewerbsfähigkeit des Unternehmens langfristig zu sichern. Hier kann die Auslagerung an externe Anbieter sinnvoll sein, da diese zeitintensive Prozesse besonders in Hinblick auf Wartung, Sicherheit und Updates übernehmen.

Rechtliche Unsicherheiten und Datennutzung

Rechtliche Unsicherheiten bezüglich der Datennutzung und Cyberangriffe stellen zusätzliche Risiken dar. Unternehmen müssen sich intensiv mit Datenschutz und Cybersicherheit auseinandersetzen, um ihre Daten und Systeme zu schützen und gesetzliche Vorgaben und Compliance, insbesondere der DSGVO zu gewährleisten.

Um den rechtlichen Unsicherheiten und Cyberbedrohungen zu begegnen, sollten Unternehmen Zugang zu klaren rechtlichen Rahmenbedingungen und robusten Sicherheitslösungen haben. Auch hier können Beratungsdienste und spezialisierte Sicherheitslösungen, wie etwa Managed Security Services hilfreich sein.

[4] "Digitalisierung weiter eher Werkzeug als Innovationsmotor. Die DIHK-Digitalisierungsumfrage 2023", Deutsche Industrie- und Handelskammer, Berlin 2023; [5] "Digitalisierung der Wirtschaft in Deutschland. Digitalisierungsindex 2023", Bundesministerium für Wirtschaft und Klimaschutz (BMWK) (Hrsg.), Berlin 2024; [6] "Digitalisierung der Wirtschaft in Deutschland. Digitalisierungsindex 2023", Bundesministerium für Wirtschaft und Klimaschutz (BMWK) (Hrsg.), Berlin 2024; [7] "Digitalisierung der Wirtschaft in Deutschland. Kompetenzbarometer: Fachkräftesituation in Digitalisierungsberufen – Beschäftigungsaufbau und Fachkräftemangel bis 2026", Institut der deutschen Wirtschaft, Alexander Burstedde (Hrsg.), o.O 2022; [8] ebd

Datenschutz

gilt dem Schutz personenbezogener Daten.

Relevanz:
Unternehmen müssen sicherstellen, dass sie geltende Datenschutzgesetze einhalten (z. B. DSGVO), um rechtliche Konsequenzen zu vermeiden.

Herausforderung:
Rechtliche Unsicherheiten bei der Datennutzung.

Datensicherheit

ist der Schutz von Daten vor unberechtigtem Zugriff, Manipulation und Verlust.

Relevanz:
Systeme müssen gegen Bedrohungen geschützt werden. Dies ist entscheidend, um Datenverluste und Betriebsunterbrechungen zu verhindern.

Herausforderung:
Zunehmende Cyberangriffe erfordern umfassende Sicherheitsmaßnahmen.

Datensouveränität

meint die Kontrolle und Selbstbestimmung über die eigenen Daten.

Relevanz:
Unternehmen müssen in der Lage sein, ihre Daten effektiv zu verwalten und zu nutzen.

Herausforderung:
Heterogene Legacy-Systeme und inkonsistente Daten erschweren die Verwaltung und Nutzung.

3. Mit Cloud-Computing zum Ziel

Rechtliche Unsicherheiten und fehlende IT-Ressourcen machen es schwer, die Digitalisierung weiter voranzutreiben. Durch die fehlenden Fachkräfte ist es für viele mittelständische Unternehmen beinahe unmöglich, die immer komplexeren IT-Systeme intern zu managen. Cloud-Computing mit der Möglichkeit, Managed Services Provider mit einzubeziehen, bietet vielversprechende Perspektiven insbesondere für mittelständische Unternehmen.

Kosten senken ohne Überlastung

Für den Mittelstand sind Lösungen notwendig, die es ermöglichen, Digitalisierungsprojekte umzusetzen, ohne die vorhandenen Ressourcen zu überlasten. Cloud-basierte Dienste bieten vielversprechende Ansätze, um diese Herausforderungen zu meistern. Zumal Cloud-Lösungen oft über eine höhere Datensicherheit und besseren Datenschutz verfügen als On-Premises-Applikationen. Unterschiede finden sich in der Art des Cloud-Hosting.

Kurzüberblick über Hosting-Optionen

On-Premises

Die IT-Infrastruktur wird vollständig im eigenen Rechenzentrum des Unternehmens gehostet.

Eine Remote-Infrastruktur, die exklusiv für ein einzelnes Unternehmen genutzt wird, entweder im eigenen oder in einem externen Rechenzentrum.

IT-Ressourcen werden über das Internet von Drittanbietern bereitgestellt.

Eine Kombination aus On-Premises, Private und Public Cloud-Lösungen, die miteinander integriert sind.

Gleichzeitige Nutzung mehrerer Public-Cloud-Anbieter, um spezifische Vorteile der jeweiligen Anbieter zu nutzen. Eine Integration untereinander ist nicht notwendig.

4. Die ideale Cloud-Hosting-Option für Ihr Unternehmen

Jedes Cloud-Computing-Modell hat seine Vor- und Nachteile. Als Unternehmen gilt es abzuwägen, welche Lösung den individuellen Anforderungen am meisten gerecht wird. Dieser Überblick über die Vor- und Nachteile der einzelnen Optionen soll Ihnen die Entscheidung erleichtern.

Die Private Cloud wird im unternehmensinternen Rechenzentrum oder exklusiv in einem externen Rechenzentrum gehostet. Sie steht für einen begrenzten Benutzerkreis über ein Intranet oder ein privates internes Netzwerk (VPN) bereit.

Vor allem für Unternehmen, die strenge Sicherheitskriterien erfüllen müssen und sensible Daten verwalten müssen, ist die Private Cloud die richtige Wahl. Durch die Exklusivität erfüllt sie hohe Sicherheits- und Datenschutzstandards und gewährleistet eine vollständige Kontrolle über die Daten. Außerdem lässt sich die Private Cloud jederzeit an spezielle Unternehmensanforderungen und IT-Ressourcen anpassen. Grundsätzlich lassen sich vier Hosting-Situationen von Private Clouds unterscheiden.

Unterschiede in der Umsetzung des Cloud-Computing mit Private Cloud

Interne Private Cloud:

Das Unternehmen hostet und managt die IT-Infrastruktur intern im unternehmenseigenen Rechenzentrum.

Managed Private Cloud:

Die IT-Infrastruktur inklusive des Rechenzentrums wird intern gehostet. Allerdings übernimmt hier ein externer Cloud-Provider das Management der Cloud und gewährleistet einen reibungslosen Ablauf und Sicherheitsvorkehrungen.

Hosted Private Cloud:

Die Hosting-Infrastruktur befindet sich in einem externen Rechenzentrum. Der Provider verwaltet die Cloud, stellt den Nutzern die entsprechenden Anwendungen zur Verfügung und übernimmt den Betrieb inklusive Netzwerkkonfiguration und Wartung.

Community Cloud:

Bei dieser Sonderform der Private Cloud nutzen mehrere Unternehmen gemeinsam eine Private Cloud. Gründe für den Zusammenschluss können ein gemeinsamer Konzern oder ähnliche, branchenspezifische Anforderungen sein.

Unternehmen in hochregulierten Branchen benötigen maximale Kontrolle über ihre Daten und höchste Sicherheitsstandards, um gesetzlichen Vorgaben und Compliance-Anforderungen gerecht zu werden. Eine Private Cloud bietet ihnen genau das: Flexibilität, Datenschutz und maßgeschneiderte Lösungen für ihre spezifischen Bedürfnisse.

Frank Böttcher
CEO BW-Tech

Mit der Exklusivität und Individualität der Private Cloud gehen jedoch höhere Kosten im Vergleich zu anderen Cloud-Lösungen einher. Das komplexe System erfordert spezialisiertes IT-Personal für Aufbau, Wartung und Verwaltung, insbesondere wenn es sich um eine intern gehostete Private Cloud handelt. Je mehr Services auf externe Anbieter ausgelagert werden, desto stärker wird die interne IT entlastet. Bei der Frage, welche Private-Hosting-Situation die richtige ist, gilt es deshalb vor allem zu klären, inwieweit Prozesse mit den vorhandenen Ressourcen intern übernommen werden können. Je knapper die IT aufgestellt ist, desto sinnvoller ist es, einzelne Aspekte an Externe abzugeben.

Wird die Cloud von einem externen Provider gehostet oder gemanagt, sollte in diesem Punkt jedoch ein erhebliches Augenmerk auf die Cybersicherheitsstrategien des Anbieters gelegt werden. Bei der Auswahl eines Rechenzentrums sind DSGVO-Konformität und ein deutscher Serverstandort besonders bei der Verwaltung sensibler Daten wichtige Auswahlkriterien.

+

- **Sicherheit**
  durch exklusive Infrastruktur
- **Volle Kontrolle**
  über die Infrastruktur und Daten
- **Anpassung**
  an spezifische Bedürfnisse und Anforderungen

−

- **Hohe Kosten**
  für die Anschaffung und Wartung der Hardware
- **Bedingte Skalierbarkeit**
  im Vergleich zu anderen Lösungen
- **Wartung und Updates**
  müssen eventuell intern durchgeführt werden
- **Komplexität,**
  die spezialisierte IT-Ressourcen fordert

Schutz gegen Cyberangriffe gehört an die Tagesordnung

Cybersicherheit ist mit wachsendem Digitalisierungsgrad so wichtig wie nie zuvor. Denn Cyberangriffe sind Unternehmensalltag. Laut DIHK-Digitalisierungsumfrage war 2022 im Schnitt **jedes fünfte Unternehmen von mindestens einem Cyberangriff betroffen**.[9]

Die kontinuierliche Arbeit an einer soliden Sicherheitsarchitektur erfordert Kenntnisse und Ressourcen in der IT-Abteilung, die vor allem in mittelständischen Unternehmen und im Kontext des Fachkräftemangels rar sind.

Durch das Auslagern bestimmter Aspekte an externe Anbieter wird die IT-Abteilung auch in puncto Cybersicherheit entlastet. Bei Managed oder Hosted Private Clouds übernehmen die externen Anbieter, wie sichere Rechenzentren und Cloud-Provider, einen erheblichen Teil der Sicherheitsvorkehrungen. Seriöse Provider garantieren dabei ein hohes Maß an Sicherheitsstandards, die insbesondere für mittelständische Unternehmen mit begrenzten IT-Ressourcen beinahe unmöglich selbst umzusetzen sind.

[9] "Digitalisierung der Wirtschaft in Deutschland. Digitalisierungsindex 2023", Bundesministerium für Wirtschaft und Klimaschutz (BMWK) (Hrsg.), Berlin 2024

Im Gegensatz zur Private Cloud teilen sich im Public-Cloud-Hosting-Modell mehrere Nutzer die Ressourcen einer Cloud-Infrastruktur. Da der Zugriff nicht über ein Intranet oder ein privates internes Netzwerk sondern über das Internet erfolgt, ist er überall und on demand möglich.

Für mittelständische Unternehmen finden sich zahlreiche Anwendungsbereiche für Public Clouds, vor allem in den Bereichen des Filesharing, Dokumentenmanagement und dem Betrieb von Kollaborationsplattformen. Hybride Zusammenarbeit ist mit Public Clouds schnell und kosteneffizient realisierbar. Denn dank Pay-as-you-go-Modell wird Leerlauf vermieden und Rechenkapazität kann bei Bedarf einfach hinzugebucht werden. Dies bietet eine hohe Skalierbarkeit und Flexibilität. Hinzu kommt, dass bei der Nutzung von Public Clouds keine eigene Hardware gestellt werden muss, was eine schnelle und einfache Realisierung möglich macht.

Auf der anderen Seite besteht eine ständige Abhängigkeit von Drittanbietern, die bis hin zu einem Vendor Lock-in führen kann. Außerdem ist die Kontrolle über die Infrastruktur begrenzt, denn sie wird vom Provider als Service-Paket vorgegeben. Da zudem Sicherheits- und Datenschutzbedenken bei Public-Cloud-Anbietern durchaus begründet sind, muss die Wahl des passenden Cloud-Providers gut überlegt sein.

Vendor Lock-in im Cloud-Computing

Ein Vendor Lock-in (auch Cloud Lock-in) bezeichnet eine Situation, in der der Kunde eines Anbieters (Vendor) so stark von dessen Dienstleistungen, Produkten oder Technologien abhängig ist, dass ein Wechsel zu einem anderen Anbieter sehr schwierig, kostspielig oder sogar unmöglich wird.

+

Kosteneffizienz
dank Pay-As-You-Go und Verzicht auf Hardware

Skalierbarkeit
basierend auf den Anforderungen

Zugänglichkeit
von überall mit einer Internetverbindung

Schnelle Realisierung, Updates und Wartung
durch den Cloud-Anbieter
Optionen

—

Sicherheitsbedenken
da Daten außerhalb des Unternehmens gelagert werden

Weniger Kontrolle
über die Infrastruktur

Abhängigkeit
von Drittanbietern mit Risiko für Vendor lock-in

Worauf sollten Sie bei der Auswahl des Public-Cloud-Anbieters achten?

Die eigenen, mitunter sensiblen Daten einem externen Provider anzuvertrauen, kann Sicherheitsbedenken hervorrufen. Diese Angst ist nicht unbegründet, wie vergangene Hackerangriffe auf Cloud-Dienstleister zeigen. In der Regel verfügen Cloud-Anbieter jedoch über ein ausgeklügeltes Sicherheitssystem, um sich vor unberechtigtem Zugriff zu schützen. Die Sicherheitsmaßnahmen des potenziellen Cloud-Anbieter müssen jedoch im Vorhinein gründlich geprüft werden. Daneben sollten die Kosten, der Support, die Reputation und die Vertragskonditionen überprüft werden, um eine Abhängigkeit vom Anbieter zu vermeiden (Vendor Lock-in).

Wichtige Sicherheitskriterien für die Auswahl des Public-Cloud-Anbieters können sein:

- Serverstandort des Rechenzentrums
- Unternehmensstandort des Cloudbetreibers
- DSGVO-Konformität
- Verschlüsselung
- Zugangskontrollen
- Regelmäßige Sicherheitsprüfungen

Die Hybrid Cloud zeichnet sich dadurch aus, dass mehrere On-Premises, Private- oder Public-Cloud-Lösungen integriert werden. Integration ist notwendig, um die jeweiligen Vorzüge der Lösung ohne Datenmigration zwischen den Modellen zu nutzen. Unterschieden werden Hybrid-Cloud-Lösungen in der Art der Zusammenstellung.

1. Public und Private Cloud kombinieren

Die Kombination von Public und Private Cloud ist besonders für Unternehmen relevant, die zwischen sensiblen und weniger kritischen Daten unterscheiden können.

Besonders sensible Daten können in der sicheren Private Cloud verbleiben. Gleichzeitig bietet die Public Cloud die Möglichkeit, schnell und flexibel auf sich ändernde Geschäftsanforderungen zu reagieren, da sie schnelle Skalierungen und kurze Latenzzeiten ermöglicht.

Durch die Integration können Daten je nach Bedarf zwischen verschiedenen Umgebungen verlagert werden. Allerdings bringt das auch Herausforderungen mit sich: Nicht nur ist die Verwaltung und Integration mehrerer Plattformen komplex, sie erfordert auch exakte Übergaberegeln, um die Sicherheit der Daten zu gewährleisten. Darüber hinaus kann die Nutzung verschiedener Plattformen zu höheren Kosten führen.

2. On-premises und Cloud kombinieren

In manchen Unternehmen gibt es Szenarien, die aus Sicherheits- oder Komplexitätsgründen einen lokalen Betrieb erfordern. Bei besonders kritischen Anwendungen steht so eine lokale Alternative zur Cloud bereit. Die Integration von Legacy-Systemen in eine Hybrid-Cloud-Architektur ermöglicht es, bestehende Systeme zu erhalten und gleichzeitig die Handlungs- und Innovationsfähigkeit zu gewährleisten.

Die Herausforderung bei dieser Hybrid-Lösung besteht darin, genau zu bestimmen, welche Anwendungen sich für die Cloud eignen und welche nicht. Es erfordert eine präzise Analyse der Sicherheitsanforderungen, Leistungsanforderungen und Komplexität der einzelnen Anwendungen, um optimale Entscheidungen zu treffen. Zudem müssen Unternehmen sicherstellen, dass die Integration reibungslos verläuft und sowohl Cloud- als auch On-Premise-Systeme nahtlos zusammenarbeiten.

+

Flexibilität und Kostenoptimierung
durch individuelle Kombinationen

Skalierbarkeit
durch die Nutzung der Public Cloud
für Spitzenlasten

Sicherheit
durch Private Cloud bzw. On-Premises

—

Komplexität
durch die Verwaltung und Integration
mehrere Umgebungen

Hohe Kosten
für die Implementierung und Verwaltung

Sicherheitsmaßnahmen
für Schutz und Übergabe der Daten
notwendig

Im Gegensatz zur Hybrid-Cloud-Infrastruktur, die unterschiedliche Cloud-Typen mischt, werden bei einer Multi-Cloud-Hosting-Lösung unterschiedliche Clouds desselben Typs verwendet, meist mehrere Public Clouds. Private Clouds können in diesem Konzept ebenfalls enthalten sein, sind aber nicht zwingend erforderlich. Die Multi-Cloud ist demnach eine Weiterführung der Hybrid Cloud.

Durch die Multi-Cloud-Strategie wird die Abhängigkeit von einem Anbieter reduziert. So sind im Falle einer Datenpanne bei einem Anbieter nicht alle Unternehmensbereiche betroffen und Vendor-Lock-in wird vermieden. Diese zusätzliche Sicherheit ist aber auch mit einem nicht zu unterschätzenden Mehraufwand im Hinblick auf Koordination und Steuerung verbunden. Diese Strategie bietet sich, wie auch die Hybrid-Cloud-Strategie an, wenn innerhalb der Prozesse auch sensible Daten verarbeitet werden. Der Hauptvorteil einer Multi-Cloud-Strategie besteht zusätzlich darin, dass die spezifischen Stärken verschiedener Cloud-Anbieter genutzt werden. Denn kein Anbieter kann die individuellen Bedürfnisse eines Unternehmens gezielt abdecken. Mit der Multi Cloud sind die Cloud-Ressourcen optimal an die Bedürfnisse des Unternehmens angepasst.

Die Orchestrierung der Cloud-Dienste kann sich jedoch als sehr komplex gestalten und erfordert ein gutes Management. So werden Fehler an den zusätzlichen Schnittstellen vermieden. Hierfür sind Management-Tools unerlässlich, die in die Kosten einkalkuliert werden müssen. Zudem kann es zwischen den verschiedenen Anbietern zu Verzögerungen und Fehlern im Datenaustausch kommen und auch die unterschiedlichen Sicherheitskonzepte der Anbieter müssen beachtet werden.

+

Flexibilität
dank der Nutzung der besten Funktionen verschiedener Anbieter

Ausfallsicherheit
durch Verteilung der Dienste über mehrere Clouds

Vermeidung von Abhängigkeit
von einem einzelnen Anbieter

Optimierung der Kosten
durch die Nutzung der günstigsten Optionen

—

Komplexität
da mehrerer Cloud-Anbieter verwaltet werden müssen

Sicherheit
muss über mehrere Plattformen hinweg gewährleistet werden

Datenintegration und -synchronisation
kann zu Latenz führen

Höhere Kosten
durch Nutzung verschiedener Anbieter und zusätzlicher Management-Tools möglich

5. Sicherheit vs. Skalierbarkeit: Eine Abwägung

Die Wahl zwischen Sicherheit und Skalierbarkeit sollte keine entweder-oder Entscheidung sein. Oft haben Unternehmen schlichtweg nicht die Möglichkeit, frei zu entscheiden, auf welches Modell die Wahl fällt, da für ihre Prozesse ein bestimmter Grad an Skalierbarkeit notwendig ist. Sicherheitsaspekte sollten jedoch unabhängig von den individuellen Anforderungen immer gewahrt werden.

Fällt die Entscheidung also zugunsten der Skalierbarkeit auf einen Public-Cloud-Provider, Managed- oder Hosted-Services oder ein externes Rechenzentrum, sollten DSGVO-Konformität, ein deutscher Serverstandort und weitere Sicherheitsmaßnahmen elementaren Einfluss auf die Wahl des Anbieters nehmen. So müssen Unternehmen nicht an Sicherheit einbüßen, können aber dennoch Ressourcen effizient nutzen, da nach Bedarf abgerechnet wird.

Nein zu US-Providern – Warum das?

Der **CLOUD Act** gibt US-Behörden **seit 2018** das Recht, auf Daten zuzugreifen, die von US-Unternehmen oder deren Tochtergesellschaften gespeichert werden, unabhängig davon, ob die Daten in den USA oder im Ausland gespeichert sind. Dies bedeutet, dass selbst Daten, die in Europa oder anderen Regionen gespeichert sind, von US-Behörden angefordert werden können.

Der **CLOUD Act** steht damit in direktem Konflikt mit der **DSGVO**, die die Übermittlung personenbezogener Daten in Länder verbietet, die nicht das gleiche Datenschutzniveau wie die EU gewährleisten. Wenn Daten auf Anforderung von US-Behörden herausgegeben werden, kann dies also einen Verstoß gegen die DSGVO darstellen und zu erheblichen rechtlichen Konsequenzen für das betroffene Unternehmen führen.

Deshalb sollte die Wahl beim Hosting kritischer Unternehmensdaten immer auf einen **Cloud-Anbieter aus dem europäischen Raum** fallen, da so die DSGVO-Konformität gewährleistet wird.

Unternehmen in regulierten Branchen wie Finanzdienstleistungen oder Gesundheitswesen müssen mitunter sehr hohe Sicherheitsstandards erfüllen. Aber auch für Unternehmen abseits dieser Branchen, die mit sensiblen Kundendaten oder immateriellen Vermögenswerten agieren, können **Public-Cloud-Provider** nicht das nötige Maß an Compliance gewährleisten.

Hier sind Daten und Workflows besser On-Premises oder in der Private Cloud aufgehoben – zumindest teilweise. Denn gerade in Zeiten von Hybrid und Multi Cloud ist, sofern es die eigenen Ressourcen zulassen, auch für diese Unternehmen eine Koexistenz von Sicherheit und Skalierung im Cloud-Computing möglich.

Die Wahl der richtigen Hosting-Strategie ist niemals pauschal. Jedes Unternehmen hat individuelle Anforderungen, ob es um Skalierbarkeit, Sicherheit oder Performance geht. Der Schlüssel liegt darin, die spezifischen Bedürfnisse genau zu verstehen und darauf basierend eine maßgeschneiderte Cloud-Lösung zu entwickeln.

Thomas Wuckel
CEO BW-Tech

6. Die Entscheidungsfaktoren im Überblick

Sicherheit und Skalierbarkeit sind häufig die Entscheidungsträger bei der Wahl des richtigen Cloud-Computing-Modells. Jedoch spielen auch eine Reihe weiterer Faktoren eine Rolle, die bei der Entscheidung berücksichtigt werden sollten.

Hier finden Sie gesammelt alle Fragen, die Sie sich bei der Auswahl der passenden Cloud-Hosting-Option stellen sollten, um die ideale Lösung für die Bedürfnisse und Anforderungen Ihres Unternehmens zu finden:

Sicherheit und Compliance:

- Welche Anforderungen an den Datenschutz werden benötigt?
- Welche Rolle spielen regulatorische Vorgaben? Ist ein deutscher Serverstandort notwendig?

Anwendungsfälle und Workloads:

- Welche Anwendungen und Workloads sollen gehostet werden?
- Kann zwischen kritischen und weniger kritischen Daten unterschieden werden?

Skalierbarkeit und Flexibilität:

- Müssen Ressourcen durch saisonale oder variierende Anforderungen oft angepasst werden?
- Ist ein schnelles Unternehmenswachstum absehbar?
- Werden Managed Services und Unterstützung durch Rechenzentrums-Services benötigt?

IT-Kompetenz und Ressourcen:

- Wie hoch sind die personellen Ressourcen der IT?
- Über welche Kompetenzen verfügt das IT-Personal?
- Hat das Team Erfahrung im Cloud-Betrieb?

Kosten:

- Welches Budget steht für Cloud Computing zur Verfügung?
- Wie hoch ist der Total Cost of Ownership?
- Welche Rolle spielt eine Kostenminimierung durch Pay-As-You-Go?

Branche:

- Muss dem Schutz geistigen Eigentums besonderer Schutz geboten werden?
- Welche branchenspezifischen gesetzlichen Standards müssen eingehalten werden?

7. Schritt-für-Schritt zur passenden Hosting-Situation

Die Auswahl der passenden Hosting-Situation ist ein vielschichtiger Prozess, der eine gründliche Analyse Ihrer Anforderungen, eine sorgfältige Bewertung der verfügbaren Optionen und eine detaillierte Planung der Implementierung umfasst. Indem Sie diese Schritte systematisch durchlaufen, können Sie sicherstellen, dass Ihre Hosting-Lösung optimal auf Ihr Unternehmen abgestimmt ist. Möglicherweise kann es sinnvoll sein, externe Dienstleister hinzuzuziehen, die den Migrationsprozess unterstützen.

Bedarfsanalyse und Zieldefinition

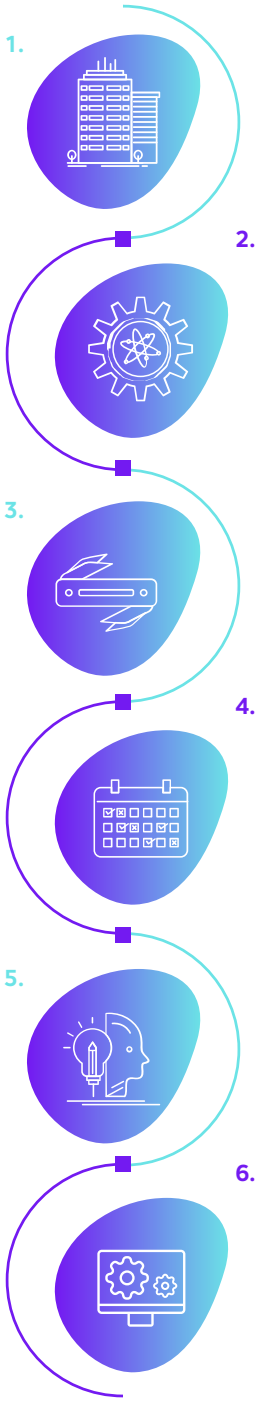
- Identifizieren Sie die Bereiche, die von der Cloud profitieren.
- Bestimmen Sie die Anforderungen Ihrer Anwendungen (z.B. Speicherplatz, Rechenleistung, Sicherheit und Datenschutz)

Sicherheits- und Compliance-Aspekte überprüfen

- Prüfen Sie, welche Sicherheitsprotokolle und Schutzmaßnahmen der Anbieter bietet (z.B. Verschlüsselung, Zugriffskontrollen).
- Stellen Sie sicher, dass der Anbieter relevante Compliance-Standards erfüllt.
- Analysieren Sie potenzielle Risiken (z.B. an Schnittstellen).
- Implementieren Sie Sicherheitsrichtlinien und legen Sie Übergaberegelungen fest.

Umfassende Implementierung

- Erstellen Sie einen detaillierten Plan zur Implementierung, einschließlich Zeitrahmen für die Migration von Daten und Anwendungen und Training der Mitarbeiter.
- Rollen Sie die Strategie schrittweise auf weitere Teile des Unternehmens aus.



Strategieentwicklung

- Legen Sie ein Budget für die laufenden Kosten (z.B. monatliche Gebühren) und mögliche Einmalkosten (z.B. Migration, Implementierung) fest.
- Evaluieren Sie, welches Cloud-Computing-Modell am besten zu den Unternehmensanforderungen passt.
- Führen Sie eine Anbieterbewertung durch und vergleichen Sie Kosten, Reputation, Support und Vertragskonditionen.

Testphase und Implementierung

- Führen Sie ein Pilotprojekt durch und starten Sie mit kleineren Projekten, um die Leistungsfähigkeit und Zuverlässigkeit der Lösung zu testen.
- Passen Sie die Strategie bei Bedarf an.

Überprüfung und Optimierung

- Überwachen Sie die Leistung nach der Implementierung und sammeln Sie Feedback von den Nutzern.
- Etablieren Sie Prozesse zur ständigen Überprüfung und Optimierung der Cloud-Nutzung.

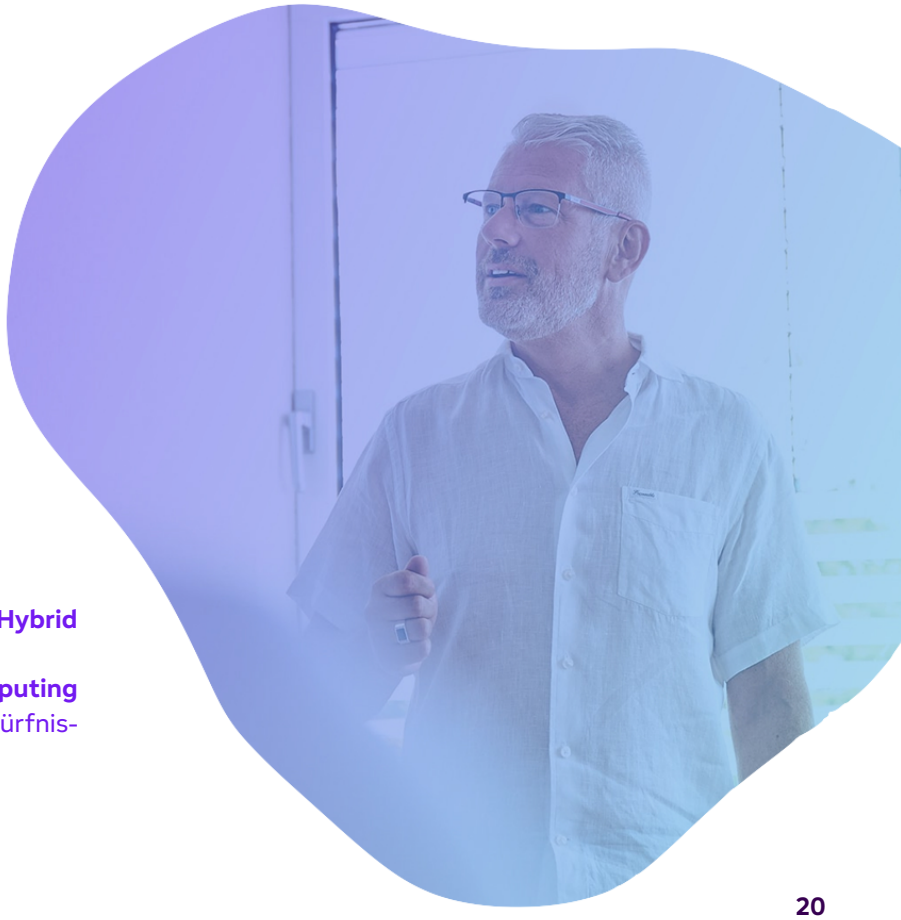
8. Die Cloud und Managed Services

Egal ob Public, Private, Multi oder Hybrid Cloud – Es gibt keine Universallösung. Die Wahl des richtigen Cloud-Computing Modells hängt von individuellen Bedürfnissen und Ressourcen ab. Lassen es die internen Mittel zu, so kann eine Private Cloud die sicherste Lösung für Ihr Unternehmen sein. Jedoch muss die Unternehmens-IT im Stande sein, komplexe Prozesse zu managen und dabei ein höchstes Maß an **Sicherheitsvorkehrungen** zu treffen. Andernfalls kann eine **private Cloud** weitaus gefährdender für die eigenen Daten sein, als es bei einer Auslagerung an **Dritte** der Fall wäre. Ein aufwendiges Unterfangen, für das gerade mittelständische Unternehmen oft nicht ausreichend aufgestellt sind. Externe können hier je nach Bedarf unter die Arme greifen und bieten meist höhere Sicherheitskonzepte als intern gehostete Private Clouds.

Managed Services können demnach als die Lösung für den Mittelstand gesehen werden, denn sie bieten **Sicherheit**, **Flexibilität**, **Skalierbarkeit** und **Compliance**. Je nach finanziellen Ressourcen und Bedarf an Skalierbarkeit können Managed Services Provider unterschiedlich stark eingebunden werden – sei es nur zum Management Ihrer Private Cloud oder in umfassenden Konzepten mit hybride, Multi- oder Public-Cloud-Lösungen. Insbesondere in Public-Cloud-Konzepten sollte jedoch die Abhängigkeit von einem Anbieter gering gehalten werden.

In jedem Falle muss die Wahl des **Cloud-Dienstleisters** unter Sicherheitsaspekten und hinsichtlich der technischen Performance erfolgen. Es ist empfehlenswert, dass der Provider seinen Stammsitz und seine Rechenzentren in der Europäischen Union hat und zertifiziert ist. Bei der Auslagerung in ein externes Rechenzentrum ist darauf zu achten, dass dieses **DSGVO**-konform ist.

Mit einer strukturierten Implementierung – bestenfalls mit einem externen Dienstleister, der den Migrationsprozess unterstützt – und einer kontinuierlichen Überwachung der Leistung nach der Implementierung kann eine zukunftsfähigen IT-Infrastruktur sicher gemeistert werden – trotz der zahlreichen Herausforderungen. Und der Weg für moderne Technologien, effiziente Wertschöpfungsketten und nachhaltiger Wettbewerbsfähigkeit ist geebnet.



BW.Tech Cloud by Design

Egal ob **Public**, **Private**, **Multi** oder **Hybrid Cloud** – Es gibt keine Universallösung.
Die Wahl des **richtigen Cloud-Computing Modells** hängt von individuellen Bedürfnissen und Ressourcen ab.

BW.Tech

IT-Service für Systemintegration und Datensicherheit

Albert-Bassermann-Strasse 31
68782 Brühl

Kontakt

Telefon: +49 (0) 6205 310 5500
E-Mail: info@bw-tech.de