consol
Wir unternehmen IT

Cloud-Migration für kleinere und mittlere Unternehmen (KMU)

ConSol Leitfaden

INHALT

Einführung

Einleitung – Immer mehr KMU entdecken die Cloud

Die digitale Transformation nutzen viele Unternehmen für eine strategische Neuausrichtung und für eine Neu- oder Weiterentwicklung ihres Geschäftsmodells. Eine Frage, die sich die Firmen innerhalb dieses Prozesses sehr häufig stellen: „Bleiben wir On-Premise oder ziehen wir in die Cloud?“ 83 Prozent der deutschen Großunternehmen nutzten laut Umfrageergebnissen von Bitkom Research (Quelle: Cloud Monitor 2018) schon 2017 Cloud-Dienste.

Doch auch die kleinen und mittleren Unternehmen legen nach. Aufgrund der großen Nähe zu ihren Kunden legen zukunftsorientierte KMU noch mehr Wert auf Vernetzung, Agilität und kurze Reaktionszeiten. Die dazu notwendigen, digitalisierten Unternehmensprozesse sorgen zwar für mehr Effizienz, gleichzeitig entstehen aber neue Anforderungen an die IT.

Hier kommen Cloud-Lösungen für KMU ins Spiel, weil sie die erhöhten Leistungsanforderungen aufgreifen, IT-Abteilungen damit deutlich entlasten und beweglicher machen. IT-Ressourcen und -Services stehen damit jederzeit, von überall nutzbar und skalierbar zur Verfügung. Zu den Grundservices können nach und nach Funktionalitäten zugekauft werden, so dass auch die Kosten kalkulierbar sind: ‚Pay as you go‘ und ‚Pay as you grow‘ sind hier die geltenden Prinzipien, nach denen man genau die Angebote bezahlt, die man nutzt und diese nach Bedarf erweitern kann. Eine eigene IT-Operations-Abteilung oder große Investitionen in Hard- und Software sind mit der Cloud somit nicht mehr zwingend notwendig.

In diesem Leitfaden stellen wir Ihnen grundsätzlich die verschiedenen Arten und Vorteile des Cloud Computings vor und gehen die Schritte durch, die Sie bei einer Migration in die Cloud beachten sollten.

Schichtenmodelle – Was soll die Cloud für Sie leisten?

Das Cloud Computing stellt Services auf verschiedenen Ebenen und in unterschiedlichem Umfang zur Verfügung. Grundsätzlich unterscheidet man drei Schichtenmodelle (IaaS, PaaS und SaaS), die sich unter dem Oberbegriff „Anything as a Service“ zusammenfassen lassen. Doch was bedeuten die Begrifflichkeiten genau?

- **Anything as a Service (XaaS)** beinhaltet alle Services bzw. Leistungen innerhalb einer Cloud, die Benutzer über das Internet bestellen und nutzen können. Die im Folgenden erklärten Modelle Software as a Service (SaaS), Platform as a Service (PaaS) und Infrastructure as a Service (IaaS), sind damit Hauptbestandteile von **XaaS**.

- **Infrastructure as a Service (IaaS)** bedeutet, dass ein Provider mietbare Infrastruktur-Komponenten wie Server, Desktops, Archivierungssysteme oder auch Speicherplatz zur Verfügung stellt.
    - **Zielgruppe:** IT-Administratoren, Architekten
    - **Mehrwert:**
        - Kein Besitz von Hardware mehr nötig, trotzdem volle Kontrolle über die eigene IT
        - Bessere Skalierung (= Anpassung an höhere oder niedrigere Anforderungen)
        - Mehr Sicherheit *(siehe „Security“ ab Seite 7)*
    - **Anwendungsbeispiele:**
        - Migration von Legacy Software (= etablierte Unternehmenssoftware), etwa um Performance-Engpässe zu beheben und/oder globaler agieren zu können, da diese nun von überall aus verfügbar ist
        - Individuallösungen wie die Migration oder Entwicklung von Spezialsoftware, die auf ein bestimmtes Betriebssystem angewiesen ist
        - Filesharing zum Austausch von Dateien unterschiedlichster Art

- **Platform as a Service (PaaS)** ist eine Kombination aus Hardware und Software, die den Anwendern als Plattform zur Verfügung gestellt wird. Auf dieser können User selbst Applikationen und Software entwickeln sowie bestehende Software darauf integrieren oder als Service (SaaS) laufen lassen.
    - **Zielgruppe:** System-Architekten und Entwickler z.B. für Containertechnologie
    - **Mehrwert:**
        - Anwendungsentwicklung in passender Entwicklungsumgebung
        - Schnellere Entwicklung
        - Weniger Infrastruktur-Know-how erforderlich
        - Skalierung
    - **Anwendungsbeispiel:**
        - Entwicklung und Bereitstellung eigener Unternehmensapplikationen

- **Software as a Service (SaaS)** ist ein Vertriebsmodell für Software über das Internet. Hierüber können User, die den Service meist über ein Abonnement beziehen, auf Angebote des Providers zugreifen. Beispiele für KMU sind Customer Relationship Management-Module (CRM) oder Office-Anwendungen wie etwa ein E-Mail-Client.
    - **Zielgruppe:** Endanwender auf Graphical User Interfaces (GUI = Benutzeroberfläche)
    - **Mehrwert:**
        - Nur Daten und Zugangsrechte sind in der Verantwortung der User, der Rest liegt beim Cloud Provider. Dies bedeutet weniger internen Verwaltungsaufwand.
        - Keine Installation notwendig
        - Keine Wartung/Updates und damit auch kein eigener Techniker notwendig
        - Aktivierung der Mitarbeiter durch mobile Lösungen und flexible Handhabung der Services
        - Skalierung

- **Anwendungsbeispiele:**
  - Customer Relationship Management
  - E-Commerce
  - E-Mail
  - Microsoft Office 365, Google G-Suite oder Amazon WorkMail

- **Dies gilt es zu beachten:**
  - Betriebszeiten der gewählten Services festlegen (man spricht hier von Service-Level-Agreements, kurz SLA)
  - Integrierbarkeit der Applikationen überprüfen, um zum Beispiel Datenschnittstellen zu schaffen
  - Schlagwort General Data Protection Regulation (GDPR): Wo liegen Ihre Daten und wie werden sie vom Cloud Provider gehandhabt? *(siehe hierzu S. 7-9)*

Einen Überblick über die gängigsten und umfassendsten SaaS-Lösungen für kleine und mittlere Unternehmen erhalten Sie in diesem Artikel.

- **Serverless Computing** lässt die vollkommene Abwesenheit eines Servers vermuten, meint aber etwas anderes: Ein Server existiert, doch hat der Anwender bzw. Entwickler bei diesem Modell keinen Konfigurations- oder Wartungsaufwand mehr und kann sich voll auf die Erstellung und Ausführung seiner Applikation konzentrieren. Die Funktion der entwickelten Applikation steht im Vordergrund, weswegen das Modell Function as a Service (FaaS) ein Beispiel des Serverless Computings ist. Ebenso können aber auch Datenbanken oder Speicherkapazität serverless angeboten werden.
  Für einen Vergleich der verfügbaren Services zwischen den Marktführern, ob serverless, PaaS oder IaaS, lohnt sich ein Blick auf http://comparecloud.in/.

Public, Private, Hybrid oder Multi – Was ist das richtige Bereitstellungsmodell für Sie?

- Mit der **Public Cloud** lassen sich IT-Ressourcen und Applikationen bei Service-Providern wie Amazon Web Services (AWS), Microsoft Azure oder Google Cloud über das Internet anmieten. Die Kunden haben dabei Zugriff auf ganz unterschiedliche Services wie IaaS, PaaS oder SaaS, die flexibel nach Nutzung oder auch über Abonnements abgerechnet werden können.

  Ihre Vorteile: Die Nutzung einer Public Cloud entlastet IT-Abteilungen und Anwender. Die Wartung und Verwaltung der Hardware sowie der zur Verfügung gestellten Anwendungen verbleibt beim Provider. Je nach Bedarf sind die angemieteten Leistungen quasi endlos skalierbar. Eine Public Cloud hilft außerdem, Ressourcen optimal zu verwerten, da in der Regel nur Dienste bezahlt

werden, die der Kunde tatsächlich nutzt (Pay as you go).

- Anders als bei der Public Cloud besitzt das Unternehmen bei der **Private Cloud** die Hardware in der Regel selbst. Zwar lindert das die Skalierungseffekte und die globale Verfügbarkeit bleibt aus, doch bietet dieses Modell die vollständige Kontrolle über das System.
  Ihre Vorteile: Durch die erhöhte Steuerbarkeit der Cloud und die physische Abschirmung der Private Cloud wird sie oft dann eingesetzt, wenn absolute Kontrolle über sensible Daten gefordert ist.

- Eine **Hybrid Cloud** ist ein Mix aus den oben beschriebenen Cloud-Modellen Public und Private. Doch was bedeutet das konkret? Mit einer hybriden Cloud-Architektur können Unternehmen Services sowohl aus einer Private als auch aus einer Public Cloud beziehen. Dabei können Kunden die Private Cloud entweder selbst betreiben oder auf einen Drittanbieter zurückgreifen.
  Ihre Vorteile: Damit haben Unternehmen beides – Freiheit und Sicherheit. Sollten sich Anforderungen an eine IT-Infrastruktur kurzfristig erhöhen, bietet die Public Cloud hochverfügbare und skalierbare Ressourcen und ist meist auch kostengünstiger als eine On-Premise-Lösung. Gleichzeitig können Firmen datenschutzkritische oder sehr spezifische Prozesse in eine Private Cloud auslagern.

- Die **Multi Cloud** ist zunächst eine Strategie. Als Teil dieser Ausrichtung setzen Kunden bzw. Unternehmen nicht nur auf einen, sondern auf mehrere Cloud-Anbieter. So kann man etwa IaaS bei AWS, PaaS bei Microsoft Azure und SaaS bei der Google Cloud nutzen. Innerhalb der Multi Cloud können die beiden Modelle Private und Public Cloud kombiniert sein, je nach Bedarf. Wichtig ist, dass die Cloud-Dienste der verschiedenen Anbieter für die Anwender unter einer einzigen großen Cloud vereint sind und von dort (an-)gesteuert werden können.

  Ihre Vorteile: „Multi Cloud is all about Choice" heißt es im Blog Cloud Health und damit ist der größte Vorteil auf den Punkt gebracht. Unternehmen haben die Wahl, welche Services sie wann, von wo und wie nutzen wollen – und das unabhängig vom Provider. Unternehmen picken sich das jeweils beste Angebot eines Anbieters heraus, passend zu ihren Bedürfnissen. Somit sind sie agiler, beschleunigen ihre Geschäftsprozesse und können schneller auf Marktanforderungen reagieren.

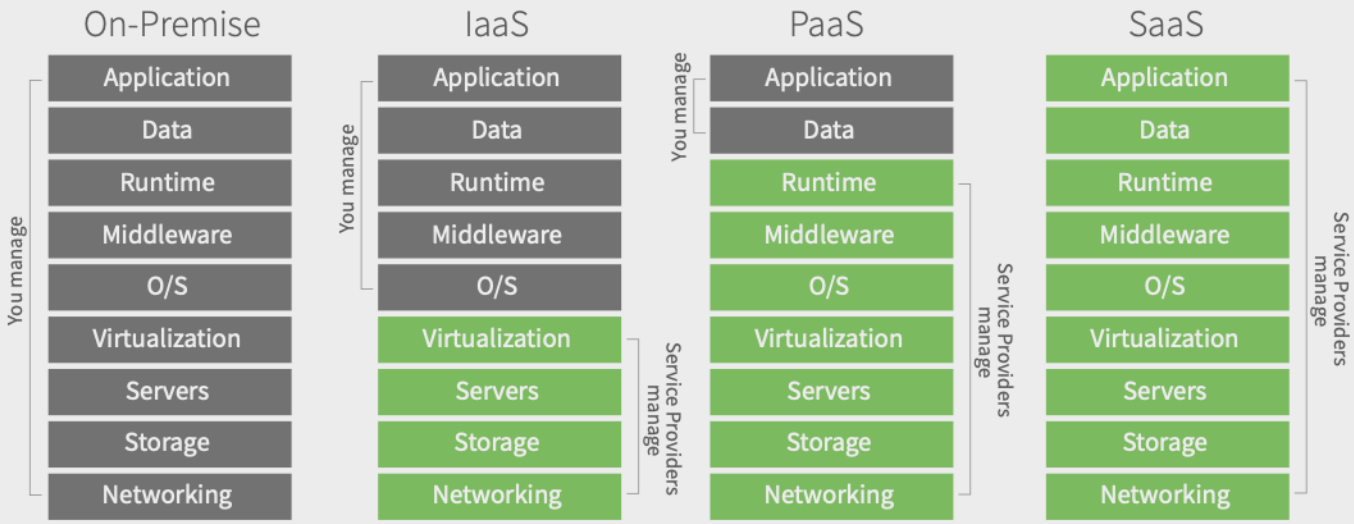
Security

Sicherheit im Cloud-Umfeld

Das Thema Sicherheit ist weiterhin auf Platz eins, wenn es um Kritikpunkte an der Public Cloud geht. Dabei werden gerne Beispiele angeführt, bei denen Fotos von Prominenten, Passwörter oder sogar Kontodaten gestohlen wurden. Auch scheint es von einem technischen Standpunkt her gefährlich zu sein, mehrere virtuelle Server auf einem realen Server laufen zu lassen – schließlich teilt man sich hier Ressourcen mit anderen Unternehmen, die theoretisch aus ihrer virtualisierten Isolation ausbrechen und so Dienste unterbrechen oder Daten stehlen könnten. Und dann bleibt noch die Frage, was mit den Daten überhaupt passiert, beispielsweise wenn eine ausländische Regierungsbehörde diese von dem dort ansässigen Cloud Provider einfordert. Und wem gehören die Daten eigentlich, wenn sie in der Cloud sind, dem Unternehmen oder doch dem Cloud Provider?

Gemeinsame Verantwortung in Cloud-Projekten

Um Sicherheit in Public Cloud Projekten zu gewährleisten, ist es notwendig zu verstehen, welchen Teil man selbst dazu beitragen muss. Im Cloud-Bereich spricht man hier von einem Shared Responsibility Model, also einem Modell der gemeinsamen Verantwortung. Wenn man sich wieder auf das Schichtenmodell beruft, sieht die Verantwortungsverteilung aus wie in nebenstehender Abbildung. Je weiter oben man sich in den Schichten befindet, desto weniger obliegt der Punkt Sicherheit dem Nutzer und desto mehr dem Cloud Provider. Man unterscheidet also die Sicherheit der bereitgestellten Cloud (Security of the Cloud) und der Sicherheit in der Cloud, also dem, was der Nutzer selbst konfigurieren kann und muss (Security in the Cloud).



Die Modelle der gemeinsamen Verantwortung in den Ausführungen der einzelnen Provider:

Microsoft	http://aka.ms/sharedresponsibility
Amazon	https://aws.amazon.com/compliance/shared-responsibility-model/
Google	https://cloud.google.com/files/PCI_DSS_Shared_Responsibility_GCP_v32.pdf

Sicherheit der Cloud

Cloud Provider sind die wohl am meisten von Cyber Attacken betroffenen Unternehmen. Allein durch ihre Größe stellen sie für Angreifer ein interessantes Ziel dar. Umgekehrt sind dadurch aber besonders die Sicherheitsmaßnahmen der großen Cloud Provider besonders gefestigt. Es ist also nicht verwunderlich, dass die führenden Public Cloud Anbieter weitaus mehr sicherheitsrelevante Zertifizierungen haben, als viele der regionalen Dienstleister. Besonders interessant ist dabei gerade in Deutschland die GDPR, die mitunter über das C5-Zertifikat abgedeckt wird. Hier wird beispielsweise sichergestellt, dass die Daten sicher und nur in durch den Kunden festgelegten Rechenzentren innerhalb Deutschlands oder der EU gespeichert werden.

Übersicht über die Zertifizierungen der führenden Cloud Anbieter:

https://www.microsoft.com/en-us/trustcenter/Compliance/C5
https://aws.amazon.com/de/compliance/services-in-scope/
https://cloud.google.com/security/compliance/#/

Was die eingangs beschriebenen Angriffe über die Virtualisierungsschicht angeht, die gerne als Argument benutzt werden, nicht in die Public Cloud zu migrieren, sind bis heute nur zwei – äußerst komplizierte – Methoden bekannt: Spectre und Meltdown. Hierbei können komplexe Algorithmen im Prozessor ausgenutzt werden, um theoretisch auf fremde virtuelle Server auf dem gleichen physischen Server zuzugreifen. Dieses Risiko ist verschwindend gering, trotzdem wurde schnell gehandelt. Diese Sicherheitslücke ist jetzt geschlossen.

Wem die Daten in der Cloud gehören ist eindeutig, wenn auch nicht jedem bekannt. Daten, die man als Nutzer oder Unternehmen in angemieteten Cloud Services ablegt, gehören immer dem Kunden.

Wichtig ist auch, dass Regierungsbehörden nicht auf die Daten von Nutzern der Public Cloud zugreifen können und dürfen. Das garantiert – zumindest für amerikanische Unternehmen – der sogenannte CLOUD Act. Hierin ist ganz klar festgelegt, dass nur bei Verdacht auf kriminelles Verhalten und auch nur in gerichtlich abgesicherter Form Daten von Cloud Providern an die Regierung übergeben werden müssen und das auch nur dann, wenn es nicht den national gültigen Gesetzen widerspricht, also zum Beispiel den deutschen.

Mehr hierzu in „Don't get spooked by the Cloud Act", IDC UK, Martin Whitworth, November 2018.

Sie interessieren sich für detaillierte Informationen zum Thema Cloud Security? **Melden Sie sich jetzt schon für die Zusendung unseres nächsten Whitepapers an!**

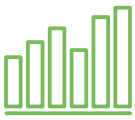
Kosten

Ist die billige Cloud ein Mythos?

Noch vor wenigen Jahren meinte man, die Cloud wäre die Wunderlösung, um IT-Kosten zu senken. Inzwischen hat sich gezeigt, dass die Cloud kein Wundermittel ist und die Kosten nur mit guter Planung gesenkt werden können.

Die Aussage, dass man sich durch die Cloud hohe Investitionskosten sparen würde, ist kritisch zu betrachten. Hierbei muss man zwischen den Betriebsmodellen unterscheiden. Diese Aussage ist wahr für die Public Cloud – hier bezieht man Rechenleistung wie den Strom aus der Steckdose. Nicht zutreffend ist die Behauptung bei einer Private Cloud. Denn hier muss man die Hardware in der Regel selbst beschaffen. Ein weiterer hoher Invest ist die Ausbildung von Fachkräften und gegebenenfalls eine initiale Migration von Daten und Applikationen. Allerdings erhalten Kunden dafür eine nie dagewesene Skalierbarkeit und Agilität. Computing-Ressourcen werden effektiver genutzt und viele Prozesse werden sowohl schneller als auch kostengünstiger.

Vorab: Kostenkalkulation



Wie errechnen sich die Kosten bei Public Cloud Providern und wie kann am Ende gespart werden? Im Bereich SaaS sind die Modelle meist recht einfach. Hier abonnieren Nutzer einen fertigen Service. Mehr User oder mehr Speicher sind gleichbedeutend mit mehr Kosten, wodurch diese für einzelne Produkte gut planbar sind.

Komplizierter wird es in allen anderen Bereichen, denn hier zahlt man für die tatsächlich genutzten Ressourcen. In erster Linie zahlt man in der Cloud für drei Dinge: Rechenleistung, Speicher und Netzwerk. Und bereits hier sollte man sich Gedanken machen, wie die fertige Architektur auszusehen hat. Denn höhere Flexibilität kostet. Wenn man beispielsweise auf Abruf (On Demand) Rechenleistung benötigt, wird das weit teurer als wenn User entsprechende Instanzen vorausschauend reservieren. Dasselbe gilt für den Speicher. Ein sogenannter Cold Storage, der für Datenarchivierung gedacht ist, ist billiger als permanent verfügbare Daten mit IO-Garantien. Auch der Einsatz von VPN oder Verschlüsselung kosten extra.

Je genauer man die eigenen Anforderungen kennt, desto mehr lässt sich in der Public Cloud tatsächlich planen und somit sparen.

Preisrechner

Ein guter Indikator für die anfallenden Preise eines Projekts sind die Preisrechner der einzelnen Anbieter. Azure (1), Google (2), AWS (3)(4) und auch andere Anbieter stellen Rechner bereit, in denen man die einzelnen Services und den erwarteten Nutzen konfigurieren kann. Die Ergebnisse können als grobe Richtlinie für den Preis gelten. Wichtig ist, dass sich der tatsächliche Nutzen durch die Dynamik der Cloud nie vorab bestimmen lässt. Es kommt gerne vor, dass Load Balancer und Ähnliches in der Konfiguration übersehen werden. Ebenso müssen User beachten, dass Anbieter nicht exakt dieselben Services bereitstellen. So kann eine virtuelle Maschine bei zwei Anbietern zwar dieselbe Spezifikation haben, durch die darunterliegende Virtualisierungstechnologie und auch die Anbindung ans Rechenzentrum können sich beide aber trotzdem unterschiedlich verhalten. Am Ende lassen sich genaue Kosten nur durch reale Tests für einzelne Use Cases bestimmen. Doch als grobe Richtlinie sind diese Tools sehr nützlich.

Amazon stellt noch einen weiteren Kostenrechner zur Verfügung (5), der bei der Entscheidung behilflich sein kann, ob man von einem lokalen Rechenzentrum in die Public Cloud migrieren möchte. Zunächst gibt man die benötigten Ressourcen an, wie virtuelle Maschinen oder Datenbanken. Im Anschluss erhält man eine Schätzung, wie viele Kosten sich durch die Migration auf AWS sparen lassen würden. Unter dem Report findet man sehr gut aufgelistet, welche Schätzungen AWS hierbei vorgenommen hat. Diese reichen von Hardware über Lizenzen bis hin zu den Gehältern der Administratoren. Aber Vorsicht: Das Model ist bewusst vereinfacht und bezieht sich auf durchschnittliche Workloads. Es wird immer Ausnahmen geben, die eher für den Betrieb einer Private Cloud sprechen.

(1) https://azure.microsoft.com/de-de/pricing/calculator/
(2) https://cloud.google.com/products/calculator/
(3) http://calculator.s3.amazonaws.com/index.html
(4) https://calculator.aws
(5) https://awstcocalculator.com/

Versteckte Kosten

Um die realen Kosten für ein Projekt zu berechnen, erfordert es die genaue Kenntnis der Leistungen, die Nutzer aus der Cloud beziehen wollen. Oftmals kommt es während der Entwicklung oder im laufenden Projekt zu unnötigen Kosten, die relativ einfach zu umgehen sind.

Die häufigste Ursache unnötiger Kosten ist die mangelnde Sorgfalt der Entwickler und Administratoren. In der Cloud ist es einfach, sich per Self-Service Ressourcen zu aktivieren, allerdings besteht so auch schnell die Gefahr, den Überblick zu verlieren. Dann passiert es, dass zu viele ungenutzte Ressourcen aktiv sind und Kosten verursachen. Zuständigkeiten müssen klar definiert und Ressourcen eindeutig Personen und Teams zugewiesen werden. Dies lässt sich über die Accountstruktur und Namens-Tags abbilden. Alle nicht mit Tags versehenen Ressourcen können regelmäßig gelöscht werden. Darüber hinaus ist es ratsam, Entwicklungssysteme nachts und über die Wochenenden über automatische Skripte abzuschalten. Gerne wird auch überprovisioniert, wenn Kunden noch nicht wissen, welche Lasten sie konkret benötigen. Doch in der Cloud lassen sich Ressourcen jederzeit nach oben skalieren: Es schadet also nicht, klein anzufangen.

Versteckte Kosten finden sich oft auch im Netzwerk. Zwar kostet es für gewöhnlich nichts, wenn die Daten im Netzwerk des Cloud Providers bleiben. Allerdings werden manche Services über das öffentliche Internet geleitet. Bei der Anbindung externer Systeme gilt es, besonders auf das Netzwerk zu achten – insbesondere im Kontext der Multi Cloud.

Anfänglich entstehen die höchsten Kosten durch die Einarbeitung der Mitarbeiter. Es ist also stets wichtig, diesen Prozess im Auge zu behalten und durch Schulungen oder gegebenenfalls die Beratung durch externe Firmen zu beschleunigen.

Rabattmodelle

Generell ähneln sich die Rabattmodelle der großen Anbieter. Die Nutzung der gleichen Ressourcen in größerem Umfang reduziert die Kosten, ebenso die Vorab-Reservierung von Ressourcen. Außerdem kann man zusätzlich sehr preiswert virtuelle Maschinen mieten, die vom Cloud Provider aktuell nicht benötigt werden. Zu beachten ist, dass man Instanzen nur auf ein oder drei Jahre reservieren kann. Wirklich nützlich ist das bei einer planbaren Grundlast, doch dann lassen sich tatsächlich bis zu 70 Prozent der Kosten einsparen. Damit sichergestellt ist, dass die gleichen Ressourcen für möglichst viele Szenarien genutzt werden können, man also gewissermaßen Mengenrabatt bekommt, kann es helfen, Richtlinien zu definieren, die nur den Einsatz freigegebener Maschinentypen erlauben. Über die temporär ungenutzten Ressourcen der Cloud-Anbieter lassen sich vor allem Kosten einsparen, wenn man sie für unkritische Berechnungen einsetzt, oder als temporäre Unterstützung für Cluster mit lang andauernden Berechnungen.

Organisatorisches

Cloud Readiness evaluieren

Wie bereit sind Sie für die Cloud? Um diesen Weg erfolgreich zu gehen, ist es wichtig einzuschätzen zu können, wo man aktuell steht.

Diesen Ist-Zustand beschreibt man im Allgemeinen als Cloud-Readiness. Kennzahlen hierfür sind unter anderem die bestehenden Skills und Prozesse im Unternehmen sowie Security-, aber auch Business-Verständnis für die Cloud.

Die führenden Anbieter haben zu dieser Thematik diverse Frameworks herausgegeben, die dem Kunden dabei helfen, von ihrer langjährigen Migrations- und Betriebserfahrung zu profitieren. Dabei hat jeder Hersteller zwar eine leicht andere Definition und damit andere Kategorien, die eine Cloud Readiness beschreiben, alle Hersteller decken jedoch die wichtigsten Punkte ab.

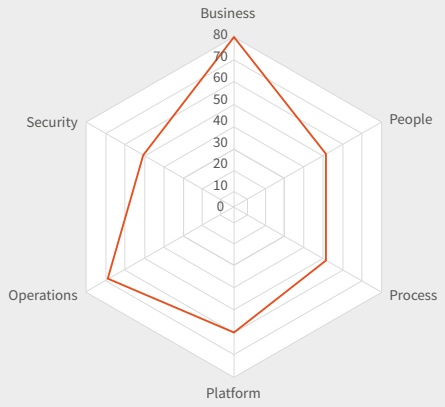
Das AWS Cloud Adaption Framework (1) dient als Tool, den bisherigen Wissensstand im Unternehmen zu erfassen, wodurch gezielt aufgezeigt werden kann, an welchen Punkten für eine erfolgreiche Cloud-Migration bzw. -Transformation gearbeitet werden muss. Das Tool bedient sich hierzu sechs verschiedener

Blickwinkel auf das Unternehmen und dessen Fokusbereiche. Es wird beispielsweise beschrieben, welche Rolle der CIO in dem Prozess einnehmen könnte und was er zu beachten hat. Dasselbe gilt für Human Ressources und Security-Beauftragte.

Als weitere Hilfestellung bietet AWS ein Cloud Adoption Readiness Tool an (2), das den Nutzer mit strukturierten Fragen durch den Prozess führt und am Ende einen Readiness Report erzeugt. Dieser Report enthält unter anderem das hier abgebildete Chart (3), das aufzeigt, an welchen Bereichen künftige Cloud-Nutzer nachbessern müssen.

(1) https://pages.awscloud.com/rs/112-TZM-766/images/a-practical-guide-for-cloud-migration-readiness.pdf
(2) https://cloudreadiness.amazonaws.com/#/cart
(3) https://cloudreadiness.amazonaws.com/bfd2391ccfbac30513c6cc8b5c40e3ae.pdf

Microsoft lehnt sich bei der Cloud Readiness sehr nah an seine Produkte an und erläutert vieles von einem technischen Standpunkt aus (1). Zusätzlich findet man in der Online-Dokumentation (2) den Migrationsprozess der von Microsoft-Tutorials bekannten fiktiven Firma Contoso und die für den Prozess eingesetzten Tools, die auf einem sehr technischen Level beschrieben sind. Wer Azure als Strategie gesetzt hat oder technische Einblicke in den Prozess möchte, ist hier an der richtigen Stelle.



(1) https://azure.microsoft.com/mediahandler/files/resourcefiles/d817c644-5dac-442f-8839-7d704e828809/Azure_Strategic_Implementation_Guide_for_IT_Organizations.pdf
(2) https://azure.microsoft.com/de-de/migration/get-started/

Google führt in seinem Adaption Framework eine zwölfteilige Cloud Maturity Scale ein, die dem Leser hilft, sich einfach im Ist-Zustand wiederzufinden und künftige Schritte hin zu einer wahren Cloud Company zu planen. Das Paper betont bewusst, dass man damit selbstständig arbeiten kann und es auch übertragbar auf andere Cloud Provider ist. Wer sich also noch nicht entschieden hat, findet hier den einfachsten Einstieg.

https://services.google.com/fh/files/misc/adoption_framework_whitepaper_nov12_final.pdf

Bei allen Frameworks hat Wissensaufbau oberste Priorität, und zwar für alle Beteiligten. Neben Schulungen wird eine Vorgehensweise klar empfohlen: experimentieren, migrieren, dann transformieren.

Dass das nicht ohne eine klare Linie in der Führungsebene des Unternehmens möglich ist, wird auch mehrfach betont. Diese Tipps treffen zwar auf jede neue Technologie zu. Aber gerade im Cloud-Bereich mit seiner großen, transformativen Wirkung kann man diese Hinweise nur noch einmal ans Herz legen.

Use Cases definieren

Wenn man sich für die Cloud-Transformation entscheidet, stellt sich stets die Frage, wo und wie man beginnen soll. Hierfür gibt es generelle Regeln, die dabei helfen, die richtigen Applikationen zu finden. Um geeignete Migrations-Kandidaten zu identifizieren, sollten zunächst die vorhandenen Anwendungen gelistet und kategorisiert werden.

Applikationen, die leicht zu migrieren sind, zeichnen sich dadurch aus, dass sie möglichst wenige Abhängigkeiten zu anderen Systemen haben, nicht business-kritisch sind und sich ohne allzu große Anpassungen in die Cloud heben lassen. Wenn Applikationen identifiziert werden können, die untereinander sehr ähnlich sind, ist auch das ein guter Startpunkt, da man so schneller voranschreiten kann. Der Return on Invest sollte nicht aus den Augen gelassen werden. Auch wenn der initiale Invest durch die eingesetzten Aufwände zunächst hoch erscheint, relativiert sich diese erste Phase ganz klar durch den progressiven Wissensaufbau im Unternehmen. Denn auch hier gilt: experimentieren, migrieren und dann transformieren. Die großen und letztlich entscheidenden Applikationen sollten nicht ohne die nötige Erfahrung in die Cloud migriert werden.

Migrationsart festlegen

Je nach Use Case wird ein anderer Bereich aus dem eingangs vorgestellten Schichtenmodell eingesetzt. Soll eine bisherige Server-Applikation ohne Änderungen in der Cloud weiterlaufen, spricht man von "lift and shift". Hierbei befinden wir uns im Bereich IaaS. Die Migrationsart des "lift and reshape" zählt ebenso zu IaaS, teilweise auch zu PaaS. Die Applikation wird zwar in die Cloud gehoben, aber doch etwas angepasst oder modernisiert. Von "reshape and decouple" spricht man, wenn die Applikation modernisiert und gleichzeitig in losere Komponenten zerlegt wird, was dem Cloud-Gedanken und dem Gedanken von Microservices näher kommt. Soll die komplette Anwendung neu geschrieben werden, setzt man auf moderne Container-Technologien. Der "complete rewrite" ist in der PaaS-Schicht angesiedelt. Möchte man seine Software in Zukunft als Service beziehen, muss diese nur eingekauft werden, was als "rebuy" bezeichnet wird.

Rollen bestimmen

Zum einen braucht es für eine erfolgreiche Cloud Migration einen Sponsor. Dabei handelt es sich um ein Mitglied der Führungsebene, das von dem Projekt überzeugt ist. Die Aufgabe dieser Person besteht darin, den Teams Hindernisse aus dem Weg zu räumen und menschliche sowie finanzielle Ressourcen zu garantieren. Ohne einen Sponsor besteht die Gefahr, dass das Projekt zu sehr gegen Bürokratie und bestehende Systeme anrennt und damit das eigentliche Ziel aus dem Fokus gerät.

Es muss ein zentrales Expertenteam geben, ein sogenanntes Center of Excellence. Dieses Team unterstützt die gesamte Firma, komplexe und wiederkehrende Probleme zu lösen und dient als Wissensmultiplikator: eine Funktion, die essentiell für den Projekterfolg ist.

Zu guter Letzt müssen alte Gewohnheiten über Board geworfen werden – eine der schwierigsten Unternehmungen. Hier kann ein Cloud-Evangelist helfen, der seine ansteckende Begeisterung für die

Technologie und den damit verbundenen Umschwung im Unternehmen verbreitet. So lässt sich verhindern, dass Mitarbeiter die disruptive Technologie verschmähen und das Cloud-Vorhaben frühzeitig scheitert.

Krisenvorbereitung

Was tun, wenn schlagartig keine neuen Cloud Ressourcen mehr aktiviert werden können? Wie ist das möglich in einer Public Cloud, die eigentlich endlos skaliert? Die meisten Anbieter schützen ihre Kunden vor unbeabsichtigten Kosten, indem sie Ressourcen limitieren. Das kann die Anzahl der zu Verfügung stehenden Prozessoren (CPUs) oder auch die Anzahl gleichzeitiger Zugriffe auf einen Service sein. Über den Support lassen sich diese Limitierungen problemlos erhöhen. Diese Stolpersteine können das Projekt unnötig verzögern, daher sollten Cloud-Nutzer von Anfang an möglichst präzise abschätzen, welche Kapazitäten sie später benötigen.

Die finale Frage ist die Frage nach der Exit-Strategie. Was passiert zum Beispiel, wenn der Cloud-Provider einen zentralen Service einstellen sollte, die Preise unverhältnismäßig erhöht oder gar den gesamten Dienst einstellt? Bei den Marktführern ist dies eher unwahrscheinlich. Setzt man aber bewusst auf kleinere Anbieter oder will auch bei den großen Providern auf Nummer sicher gehen, bleiben aktuell zwei Möglichkeiten. Die eine besteht darin, nur Services zu verwenden, die alle Provider anbieten. Besonders empfehlenswert sind an der Stelle Open Source-Projekte wie Kubernetes. Gleichzeitig muss klar sein, dass die proprietären Lösungen eines Dienstleisters gezielt aufeinander abgestimmt sind. Sie stellen Support bereit und die Entwicklung mit ihnen läuft meist schneller. Die zweite Möglichkeit, dem sogenannten Vendor-Lock-in* zu entgehen, ist eine Multi Cloud-Strategie, mit der man nicht nur auf einen einzigen Provider angewiesen ist.

*Wenn ein Kunde oder Cloud-Nutzer einen Service nicht ohne Weiteres durch den Dienst eines alternativen Anbieters ersetzen kann, spricht man von Vendor-Lock-in.

Software migrieren – Anwendungsbeispiele

Backup

Das Backup von Daten ist in einer digitalen Welt unabdingbar. Daher gibt es bereits viele gute Backup-Lösungen, die man sich ohne großen Aufwand selbst ins Büro stellen kann. Allerdings bleibt immer das Restrisiko, dass auch diese Hardware versagt oder die gesamte Infrastruktur etwa durch Brand oder Diebstahl abhandenkommen kann.

Abhilfe schaffen Backup-Lösungen aus der Cloud. Dazu wird lokal eine Software installiert, mit der sich steuern lässt, welche Daten wie oft ins Backup geschoben werden sollen. Gleichzeitig ist es dem Nutzer auch möglich, Daten aus dem Backup wiederherzustellen. Statt die Hardware zu kaufen, beziehen Kunden einen Service, den sie monatlich nach Speichermenge und Speicherklasse bezahlen. Speicherklassen sind hierbei hot, warm und cold. Hot sind Speicher, auf die schnell und kurzfristig zugegriffen werden muss, wie das Backup vom gestrigen Tag. Dagegen steht der „kalte“ Langzeitspeicher. In welchem Speicher sich die

Daten befinden, lässt sich einfach regeln. Das gilt von kleinen Terabyte-Lösungen bis hin zu Lasten, wie man sie aus dem Rechenzentrum kennt.

Neben der einfachen Bereitstellung, dem geringen administrativen Aufwand und der Skalierbarkeit ist besonders die hohe Verfügbarkeit ein Argument, Backup-Lösungen aus der Cloud zu beziehen. In wenigen Fällen ist das Backup aus der Cloud allerdings auch mit Nachteilen verbunden. Bei einer langsamen Internetverbindung oder bei sehr großen Datenmengen kann ein Backup aus der Cloud natürlich länger dauern. Eine Lösung sind hybride Systeme, bei denen die aktuellste Sicherung zusätzlich lokal vorgehalten wird, ein Duplikat und ältere Sicherungen allerdings in der Cloud liegen. Wenn man seine gesamten gesammelten Backups und Daten in die Cloud heben möchte und es sich dabei um mehrere Terabytes bis Petabytes handelt, Hardware-Appliances der Anbieter zusenden lassen. Das spart Zeit und Transferkosten. Die Appliances werden lokal angeschlossen, mit den Daten befüllt und zurück an den Provider gesandt, der sie schließlich direkt auf seinen Speicher überspielt und somit in der Cloud verfügbar macht.

Migration von Altsoftware

In den meisten Unternehmen findet sich Software, die seit Jahren läuft und gewissermaßen zum Inventar gehört. Sie abzulösen scheitert häufig am mangelnden Funktionsumfang konkurrierender Software oder an der Akzeptanz der Mitarbeiter, die ihre Arbeitsabläufe, sei das jetzt gut oder schlecht, der Software angepasst haben. Möchte man diese Software in die Cloud heben, dann ist dafür ein Lift-and-Shift-Projekt am geeignetsten.

Das bedeutet, dass die bestehende Software, die vermutlich auf einem Windows- oder Linux-Server läuft, künftig auf einer Virtuellen Maschine mit ähnlicher Leistung in der Cloud laufen wird. Statt bei seiner internen IT oder einem Zulieferer physisch einen Server stehen zu haben, mietet man ihn sich in der Cloud als Infrastructure as a Service an.

Bei einem Lift-and-Shift-Projekt besteht nur wenig Anpassungsbedarf und die Software sieht am Ende für den Nutzer aus wie bisher. Vorhandene Applikationen lassen sich auf diese Weise in kurzer Zeit in die Cloud migrieren. Trotzdem gibt es einiges zu beachten. Was die Sicherheit angeht, wissen wir ja, dass die "Security of the Cloud" vom Anbieter abgedeckt ist. Man muss sich also keine Gedanken darüber machen, ob es Stromausfälle gibt, oder ein Einbrecher den physischen Server stielt. Entscheidend ist die Frage, wie sich Nutzer in Zukunft bei der Anwendung authentifizieren. Sind Nutzername und Passwort in einer Datenbank hinterlegt? Gibt es ein zentrales Active Directory? Die Datenbank in der Cloud muss natürlich auch gesichert werden. Die Provider stellen selbstverständlich Möglichkeiten hierfür bereit, beispielsweise Verschlüsselung, Nutzer- und Rollenverwaltung. Diese müssen aber zunächst verstanden und eingerichtet werden.

Sinnvoller ist es oft, die Nutzerverwaltung als Service zu beziehen. Sie lässt sich mit dem lokalen Identitätsdienst, zum Beispiel Active Directory, verbinden. Nun sollten keine Unbefugten mehr auf die Software zugreifen können. Trotzdem ist die Angriffsfläche der Software zunächst wesentlich größer als bei einem lokalen, physischen Server im Firmennetzwerk, denn die Cloud ist aus dem gesamten Internet erreichbar. Auch hierfür gibt es verschiedene Lösungen. Zum einen lassen sich die benötigten Netzwerke und Subnetze in der Cloud so konfigurieren, dass sie nur von bestimmten IP-Adressen aufgerufen werden können. Zum anderen gibt es die Möglichkeit, ein VPN oder auch eine teurere, aber schnellere direkte

Verbindung zum Cloud Provider aufzubauen. Ein weiterer, wichtiger Punkt ist die Verbindung der Software zu anderen Systemen.

Die meisten Applikationen benötigen eine Datenbank. Nun wird man im Rahmen der Cloud-Migration nicht mehr seine lokale Datenbank einsetzen, sondern sich auch hier aus dem Portfolio der Cloud-Anbieter bedienen. Da verschiedene Datenbanken und Abrechnungsmodelle angeboten werden, sollten Nutzer ihre reale Last kennen. Dabei kommt es auf Größe, Anzahl der Zugriffe und Zugriffsgeschwindigkeiten an. Zusätzlich gibt es eine Reihe von Möglichkeiten, Datenbanken zu nutzen: als serverless Datenbank, als konfigurierbaren Service, oder doch selbst installiert auf virtuellen Servern, falls man zum Beispiel zusätzliche Plugins für die Datenbank benötigt. Wenn die Software noch andere Verbindungen benötigt werden diese für gewöhnlich über das Netzwerk an die benötigten Endpunkte weitergeleitet. Diese können sich zunächst on Premise befinden und später migriert werden.

Fazit

Immer mehr kleine und mittlere Unternehmen wollen den Schritt in die Cloud wagen. Da es in den KMU aufgrund der Unternehmensgröße oftmals keine eigene IT-Abteilung gibt, sind die Unternehmer auf externes Know-how angewiesen.

In diesem Leitfaden haben wir zunächst viele grundsätzliche Informationen zu den unterschiedlichen Cloud- und Service-Modellen zur Verfügung gestellt. Ein besonderes Augenmerk haben wir anschließend auf die Aspekte Kostenkalkulation, Cloud Readiness und Datensicherheit gelegt – gerade das Thema Security sorgt bei den meisten Unternehmen noch für große Verunsicherung.

Kein Wunder also, dass das Top-Kriterium für die Auswahl eines Cloud-Providers seine Konformität mit der DSGVO ist (Quelle: Bitkom Research). Aufgrund der hohen Nachfrage zu diesem Thema wird es in Kürze einen weiteren Leitfaden speziell zu **Cloud Security** geben. Melden Sie sich jetzt schon an für Teil 2 unserer Cloud-Reihe!

ConSol
Consulting & Solutions Software GmbH

St.-Cajetan-Straße 43
D-81669 München
Tel.: +49-89-45841-100
vertrieb@consol.de
www.consol.de
Folgen Sie uns auf Twitter: @consol_de

ConSol
Austria Software GmbH

Maysedergasse 2/25
A-1010 Wien, Österreich
Tel.: +43-1-9971392
info-austria@consol.com
www.consol-software.at
Folgen Sie uns auf Twitter: @consol_at