Standortunabhängig auf Anwendungen und Dokumente zugreifen

Arbeiten mit der Wolke

Cloudcomputing wird von der ICT-Industrie seit Jahren als Megatrend propagiert. Aber was ist das, wie funktioniert es und welches sind die Vorteile und Risiken?

Der Begriff Cloud (Wolke) umschreibt standardisierte IT-Infrastruktur, die den Nutzern über ein Netzwerk zur Verfügung steht. Der genaue Aufbau und die Spezifikationen bleiben den Anwendern weitgehend verborgen, und so scheint sie fern und undurchsichtig, wie von einer «Wolke» verhüllt. Dabei umfasst Cloudcomputing das gesamte ICT[1]-Spektrum und beinhaltet Infrastruktur (Server, Storage), Plattformen (Betriebssystem, Datenbank) und Software (Versichertenverwaltung, Buchhaltung, Archivsoftware).

Cloudcomputing ist in erster Linie durch die Idee entstanden, Skaleneffekte zu generieren, wie sie beispielsweise für die Dienste von Google, Microsoft und Co. unverzichtbar sind. Hinzu kommen Ausfallsicherheit sowie Standort- und Clientunabhängigkeit. Attribute, von denen Prozessoptimierer seit jeher träumen.

Aufbau und Servicemodelle

Cloudcomputing besteht aus drei Schichten respektive Servicemodellen (siehe auch Grafik, Seite 9):

– Infrastruktur (IaaS)
– Plattform (PaaS)
– Anwendung (SaaS)

Infrastructure as a Service (IaaS)

Mit Hilfe von Virtualisierungssoftware werden zunächst Server, Storage und Netzwerk zusammengefasst und bedarfsgerechte virtuelle Server bereitgestellt. Je nach Verwendungszweck verfügen diese virtuellen Server über mehr oder weniger Ressourcen (Prozessoren, Arbeits- und Festplattenspeicher). Diese Art virtualisierter Hardware ist als «Infrastructure as a Service» (IaaS) erhältlich. Eine Aufstockung der Ressourcen im laufenden Betrieb ist jederzeit möglich. Um die Ausfallsicherheit zu gewährleisten, muss die physische Hardware redundant vorhanden sein (zum Beispiel Server mit 2 Netzteilen und 2 Netzwerkkarten). Benutzer von IaaS sind für die Administrierung der Server ab der Betriebssystemebene selbst verantwortlich.

Platform as a Service (PaaS)

Auf den einzelnen virtuellen Servern werden dann in einem nächsten Schritt die benötigten Serverbetriebs- und Datenbanksysteme installiert. Die Trennung der einzelnen Serverdienste, sprich für jeden Dienst wird ein separater virtueller Server aufgesetzt (zum Beispiel Applikationsserver, Datenbankserver, AD-Server, Webserver), gilt heute als «Best Practice». Entsprechende virtuelle Server inklusive der Betriebssoftware bieten Provider als «Platform as a Service» (PaaS) an. Wer PaaS nutzt, installiert nur noch die Fachapplikationen, möchte aber mit dem Administrieren der Systeme nichts mehr zu tun haben.

Software as a Service (SaaS)

Schliesslich werden die einzelnen Server so eingerichtet und konfiguriert, dass die jeweiligen Nutzergruppen client- und standortunabhängig auf ihre Anwendungen zugreifen können. Durch Verwendung von «Multi-factor Authentication» wird unbefugter Zugriff verhindert. Mittels Whitelisting werden Zugriffe von aussen und ausführbare Anwendungen beschränkt, um die Infrastruktur vor Viren und Schadsoftware zu schützen. Durch die Verteilung der Dienste auf verschiedene Server sind auch sehr heterogene Installationen kein Problem. Analog zu den physischen Teilen müssen auch die virtuellen Komponenten redundant vorhanden sein, um eine hohe Verfügbarkeit respektive Ausfallsicherheit zu garantieren. Unter «Software as a Service» (SaaS), auch als «Software on Demand» bezeichnet, bieten Provider eine speziell auf die jeweilige Kundengruppe zugeschnittene Auswahl von Software an, die auf ihrer Infrastruktur läuft. Bei SaaS bringt der Benutzer weder seine Applikationen in die Cloud, noch muss er sich um Datenhaltung kümmern. Er nutzt die bestehenden Softwareanwendungen, die ihm der Cloudanbieter bereitstellt.

In Kürze

> Die Pensionskasse kann entscheiden, wieviel Aufwand sie einem Anbieter in der Cloud überlassen will
> Um den Datenschutz zu gewährleisten, empfiehlt sich ein Anbieter mit Servern auf Schweizer Boden

Liefermodelle

Bei Cloudcomputing unterscheidet man zwischen vier Liefermodellen:

– Public Cloud
– Private Cloud
– Community Cloud
– Hybrid Cloud

Public Cloud

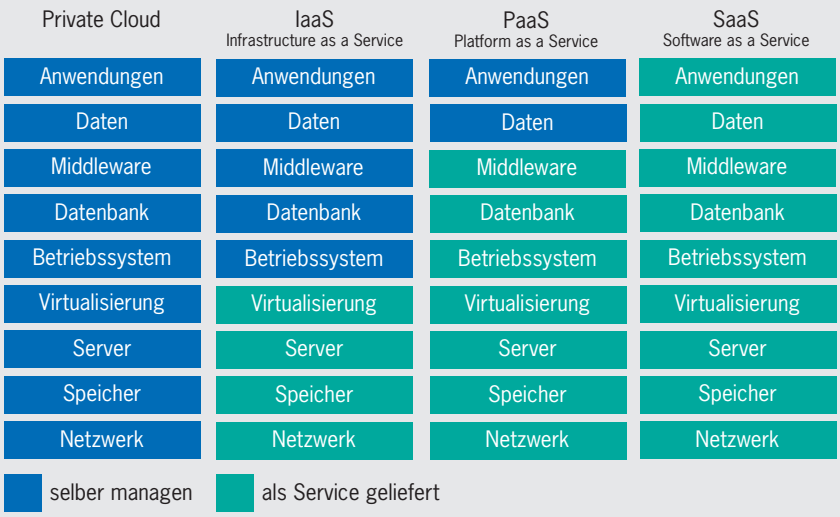
Als Public Cloud werden Dienste von Anbietern bezeichnet, die für eine breite

Autor

Roger Peduzzi
ICR Informatik AG,
Rotkreuz

[1] Information and Communication Technology.

Unterschiedliche Formen von Clouddiensten



Öffentlichkeit bestimmt sind. Folglich sind Public-Cloud-Anbieter so aufgestellt, dass ihre Nutzer die gewünschten Dienste selbständig aktivieren können. Zu Public-Cloud-Diensten gehören zum Beispiel: iCloud, SkyDrive, Microsoft 365, Windows Azure, Oracle Cloud oder Amazon Web Services.

Private Cloud

Bei der Private Cloud befinden sich sowohl Anbieter als auch Nutzer im selben Unternehmen. Das Wegfallen der Probleme im Zusammenhang mit der Datensicherheit wird oft als Hauptgrund angegeben, wenn die Wahl auf die Private Cloud fällt. In Tat und Wahrheit sind Firmen, die eine Private Cloud betreiben, einfach selber für die Datensicherheit verantwortlich und tragen auch die damit anfallenden Kosten und Risiken selber.

Community Cloud

Die Community Cloud ähnelt der Public Cloud. Sie ist jedoch für einen beschränkten Nutzerkreis (zum Beispiel Schweizer Vorsorgeeinrichtungen) bestimmt. Aufgrund der Einschränkung kann der Community-Cloud-Anbieter besser auf die branchenspezifischen Wünsche der Klientel eingehen. Exemplarisch kann die Auswahl der Software oder der Standort des Rechenzentrums genannt werden. Aufgrund des überschaubaren Nutzerkreises sind bei der Community Cloud weniger Systemadministratoren als bei der Public Cloud involviert. Folglich wird es auch einfacher, den Datenschutz und die Datensicherheit zu gewährleisten.

Hybrid Cloud

Von Hybrid Cloud spricht man, wenn für die benötigten Dienste verschiedene Liefermodelle zur Anwendung kommen. So ist es zum Beispiel denkbar, dass eine Vorsorgeeinrichtung eine Private Cloud betreibt, aber auf den Einsatz eines eigenen Exchange Servers für die Verwaltung der Outlookkonten verzichtet und stattdessen Exchange 365, einen Public-Cloud-Dienst von Microsoft, einsetzt. Und schon spricht man von einer Hybrid Cloud.

Vorteile

Von der beschriebenen Funktionsweise sowie der weitgehend anerkannten Merkmale von Cloudcomputing wie Skalierbarkeit, Zuverlässigkeit und Ausfalltoleranz, Optimierung und Konsolidierung sowie Qualitätssicherung und Qualitätskontrolle lassen sich die folgenden Vorteile ableiten:

- Kostenersparnis durch Bezahlung nach Verbrauch
- Hohe Ausfallsicherheit
- Client- und standortunabhängiger Zugriff
- Keine oder kleinere Investitionen in Hard- und Software
- Kein oder weniger eigenes IT-Personal nötig
- Transparente und budgetierbare Kosten
- Verkürzte Projektlaufzeiten
- Schnellere Anpassung der Kapazitäten an den Bedarf
- Konzentration auf die Kernkompetenzen

Diese Vorteile gelten jedoch nur teilweise für die Private Cloud, weil bei dieser ja eigene IT-Infrastruktur angeschafft und betrieben wird, und so die Flexibilität und die Budgetierbarkeit der Gesamtkosten im Vergleich zu SaaS abnimmt.

Risiken

Die Risiken beschränken sich im Wesentlichen auf die Datensicherheit, den Datenschutz und auf die Abhängigkeit (Lock-in-Effekt) vom jeweiligen Cloudanbieter. Die Datensicherheit respektive das Risiko des unbefugten Zugriffs wird heute mithilfe von Verschlüsselung und «Multifactor Authentifizierung» gelöst.

Im Zusammenhang mit dem Datenschutz ist es wichtig, dass sensible Personendaten in der Schweiz gespeichert werden. Sonst gilt ausländisches Recht. Gerade die jüngere Zeit hat gezeigt, dass beispielsweise in den USA, wo sich über 90 Prozent der Cloudinfrastruktur befinden, die Behörden unter dem Vorwand des Patriot Acts die Herausgabe von Daten verlangen. Das geht sogar so weit, dass US-amerikanische Firmen gezwungen werden, auch Daten herauszugeben, die auf Servern gespeichert sind, die sich ausserhalb der USA befinden.

Auch dem Lock-in-Effekt, der Abhängigkeit zum Anbieter des Clouddiensts, muss Aufmerksamkeit geschenkt werden. Wenn der Softwarelieferant auch SaaS-Provider ist, erhöht sich die Abhängigkeit beim Wechsel in die Cloud nicht. Stattdessen ergeben sich Synergien, wodurch sich die Gesamtkosten reduzieren. Kritisch wird dieser Punkt jedoch dann, wenn eine spätere Abkehr vom Cloudanbieter respektive ein Insourcing nicht oder nur schwer möglich ist.

Fokus auf Kernkompetenzen

Schweizer Vorsorgeeinrichtungen sind gemessen an den Mitarbeiterzahlen kleine Organisationen mit relativ einheitlichen Bedürfnissen und daher prädestiniert für Community-Cloud-Dienste. Gerade bei SaaS können sie von Skaleneffekten profitieren, die ihnen die SaaS-Anbieter weitergeben. Zudem entfallen wiederkehrende Investitionen und Unterhalt für die IT-Infrastruktur und die SaaS-Kunden erhalten System- und Anwendersupport aus einer Hand. Dadurch können sie sich auf ihre Kernkompetenzen fokussieren. Für das Hosting der Applikationen und Daten sollte aus Datenschutzgründen ein Schweizer Anbieter mit Servern in der Schweiz gewählt werden. ■

Accéder aux applications et aux documents indépendamment de l'emplacement

Travailler sur un nuage

Le cloud computing est la coqueluche de l'ICT depuis des années. Mais qu'est-ce que c'est exactement, comment fonctionne ce «nuage» dont on nous dit qu'il est la «mégatendance de l'avenir», quels en sont les avantages et les risques?

Le terme cloud (de l'anglais nuage) désigne une infrastructure que les consommateurs peuvent utiliser via un réseau. L'utilisateur n'ayant aucune connaissance exacte ni de la composition ni des spécifications, l'ensemble lui paraît donc lointain et opaque, comme enveloppé d'un «nuage». Le cloud computing ou informatique en nuage englobe tout le spectre des ICT[1] et comprend des infrastructures, des plates-formes et du logiciel. Le cloud computing est avant tout né parce qu'on voulait générer des effets d'échelle qui sont indispensables pour des services tels que Google, Microsoft et compagnie. A cela s'ajoute la protection contre les défaillances, ainsi que l'indépendance d'un emplacement ou d'un client.

Structuration et modèles de service

Le cloud computing se compose de trois niveaux ou modèles de service (voir aussi le graphique à la page 11):

Infrastructure as a Service (IaaS)

A l'aide d'un logiciel de virtualisation, on rassemble des serveurs, des mémoires et des réseaux et on les met à la disposition des consommateurs sous forme de serveurs virtuels adaptés à leurs besoins. Selon l'utilisation prévue, ces serveurs virtuels disposent de plus ou moins de ressources (processeurs, mémoire de travail et disque dur). Ce genre de matériel virtualisé peut être acquis au titre d'«infrastructure en tant que service» (Infrastructure as a Service, IaaS). Les ressources peuvent être étendues à tout moment et en pleine exploitation. Pour que la protection contre les défaillances soit garantie, le matériel physique doit être redondant (par exemple un serveur avec 2 unités d'alimentation et 2 cartes réseau). Les consommateurs d'IaaS sont eux-mêmes responsables de l'administration des serveurs à partir du niveau du système d'exploitation.

Platform as a Service (PaaS)

Une prochaine étape consiste à installer sur chaque serveur virtuel les systèmes d'exploitation et les bases de données nécessaires. La séparation des divers services de serveur, autrement dit, l'installation d'un serveur virtuel à part pour chaque service (par exemple serveur pour les applications, serveur pour les banques de données, serveur AD, serveur pour le Web), est aujourd'hui considérée comme meilleure pratique. Les fournisseurs proposent de tels serveurs virtuels, y compris le logiciel d'exploitation, sous forme de «plate-forme en tant que service» (Platform as a Service, PaaS). Le consommateur qui opte pour la PaaS installe encore les applications spécialisées, mais il ne veut plus devoir se soucier de l'administration des systèmes.

Software as a Service (SaaS)

Enfin, les différents serveurs sont installés et configurés de manière à ce que des groupes d'utilisateurs spécifiques puissent accéder à leurs applications indépendamment d'un client ou d'un emplacement. Des systèmes d'authentification d'identité multifactoriels évitent les accès non autorisés. A l'aide d'une «liste blanche» (white listing), on restreint les accès de l'extérieur et les applications exécutables afin de protéger l'infrastructure contre les virus et les logiciels nuisibles. Du fait de la répartition des services sur différents serveurs, même les installations hétérogènes ne présentent pas de problème. Par analogie aux éléments physiques, les composants virtuels doivent également être redondants afin que la disponibilité et la protection contre les défaillances soient garanties. Sous la désignation «logiciel en tant que service» (Software as a Service [SaaS] ou Software on demand), les fournisseurs proposent des logiciels customisés à certains groupes de clients qui fonctionnent sur leur infrastructure. Avec SaaS, l'utilisateur n'apporte pas ses applications dans le cloud et il ne doit pas se soucier de la gestion de données, il utilise le logiciel applicatif mis à sa disposition par le fournisseur du cloud.

En bref

> La caisse de pensions peut décider combien de travail elle veut confier au prestataire de services en nuage

> Pour garantir la protection des données, il est conseillé de choisir un fournisseur ayant ses serveurs sur sol suisse

Modèles de livraison

Il existent quatre modèles de livraison distincts dans le cloud computing:

Public Cloud

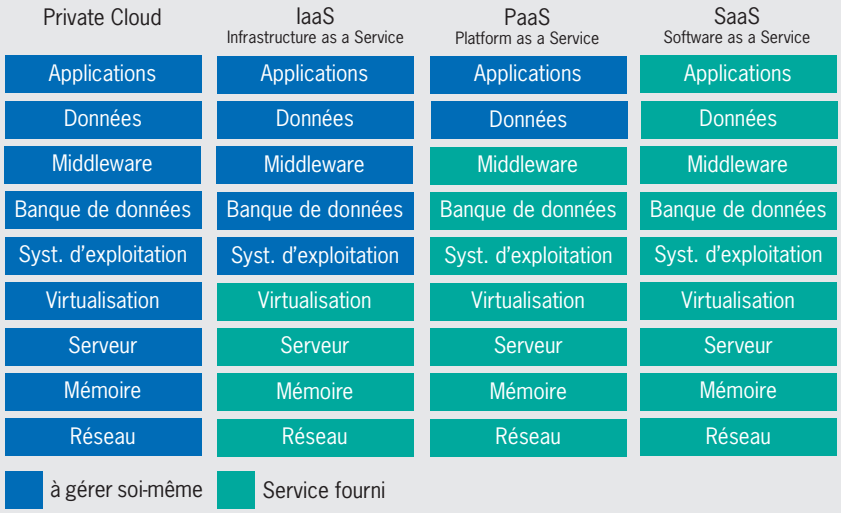
Un nuage public est un service destiné à un vaste public. Les fournisseurs de public clouds sont organisés de manière à ce que leurs utilisateurs puissent eux-mêmes activer les services désirés. Parmi les services offerts par le biais d'un nuage public, on peut citer iCloud, SkyDrive, Microsoft 365, Windows Azure, Oracle Cloud ou Amazon Web Services.

Private Cloud

Un nuage privé est un nuage où le fournisseur et l'utilisateur se trouvent dans

[1] Information and Communication Technology.

Les différentes formes de services en nuage



la même entreprise. Souvent, on vous explique que le nuage privé a été choisi pour éviter le problème de la sécurité des données. Or en réalité, les entreprises qui opèrent un nuage privé sont tout simplement elles-mêmes responsables de la sécurité des données et en endossent par conséquent les coûts et les risques.

Community Cloud

Le nuage communautaire ressemble fort au nuage public, sauf qu'il est destiné à un cercle d'utilisateurs restreint (par exemple les institutions de prévoyance suisses). Parce que le cercle d'utilisateurs est restreint, le fournisseur d'un nuage communautaire peut mieux tenir compte des désirs spécifiques à la clientèle d'un secteur donné. Ainsi par exemple, les clients pourront choisir le logiciel ou l'emplacement du centre de calcul. Parce que ce cercle restreint d'utilisateurs est facilement contrôlable, il y aura moins d'administrateurs du système dans un nuage communautaire et il sera donc aussi plus facile d'assurer la protection des données et d'en garantir la sécurité.

Hybrid Cloud

Un nuage est dit hybride lorsque les services consommés sont fournis de différentes manières. Ainsi, il serait pensable qu'une institution de prévoyance opère son nuage privé, mais qu'elle renonce à exploiter son propre serveur exchange pour la gestion des comptes Outlook et utilise au lieu de cela Exchange 365, un service public cloud proposé par Microsoft – et voilà déjà un nuage hybride.

Avantages

Du mode de fonctionnement décrit ainsi que des caractéristiques largement reconnues du cloud computing telles que l'élasticité, la fiabilité, la tolérance aux défaillances, l'optimisation et la consolidation, la sécurité et le contrôle de la qualité découlent les avantages suivants:

- économie de coûts grâce au paiement à la consommation
- protection élevée contre les défaillances
- indépendance du client et de l'emplacement
- pas ou peu d'investissements dans le matériel et le logiciel
- pas ou peu de personnel IT propre nécessaire
- coûts transparents et faciles à budgétiser
- temps plus court de mise en place de projets
- adaptation plus rapide des capacités aux besoins
- concentration sur les compétences clés

Cependant, ces avantages ne jouent que partiellement pour le nuage privé puisque là, on doit se procurer et opérer sa propre infrastructure IT. La flexibilité et la facilité de budgétisation des coûts globaux diminuent donc forcément en comparaison avec SaaS.

Risques

Les risques concernent avant tout la sécurité des données, la protection des données et la dépendance (effet lock-in) du fournisseur d'un cloud donné. La sécurité des données et le risque d'accès non autorisés sont aujourd'hui résolus à l'aide du cryptage et de l'authentification d'identité multifactorielle. Concernant la protection des données, il est important que les données personnelles sensibles soient stockées en Suisse, sinon, le droit de l'emplacement à l'étranger sera applicable. Aux Etats-Unis par exemple où se trouvent plus de 90% de l'infrastructure des nuages, il arrive que les autorités réclament des données au nom de la loi antiterroriste «Patriot Act». Elles vont même jusqu'à contraindre des entreprises américaines à livrer des données qui sont stockées sur des serveurs hors du territoire américain.

Il faut également être attentif à l'effet lock-in, autrement dit, la dépendance d'un fournisseur de services en nuage. Lorsque le fournisseur de logiciel est en même temps fournisseur SaaS, cette dépendance ne grandit pas quand on s'installe sur un nuage. Il se produit au contraire des synergies qui permettent de réduire les coûts globaux. La situation devient toutefois critique lorsqu'il est difficile, voire impossible de quitter un fournisseur de nuage ou de rapatrier des services.

Concentration sur les compétences clés

Compte tenu du nombre de collaborateurs, les institutions de prévoyance suisses sont des petites organisations avec des besoins relativement uniformes; de ce fait, elles sont prédestinées à ce service des nuages mutualisés. Notamment avec SaaS, elles peuvent profiter d'effets d'échelle qui sont répercutés par les fournisseurs. Elles peuvent également faire l'économie d'investissements récurrents et de frais d'entretien de l'infrastructure IT et les clients SaaS profitent d'un support système et utilisateur d'un seul tenant et peuvent donc se concentrer sur leurs compétences clés. Pour l'hébergement des applications et des données, il faudrait donner la préférence à des fournisseurs suisses avec des serveurs établis en Suisse par souci de protection des données. ■

Roger Peduzzi