

Der Netzwerk Insider

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Cloud nutzen oder Cloud aufbauen?

von Dr. Behrooz Moayeri



Dr.-Ing. Behrooz Moayeri hat viele Großprojekte mit dem Schwerpunkt standortübergreifende Kommunikation geleitet. Er gehört der Geschäftsleitung der ComConsult Beratung und Planung GmbH an und betätigt sich als Berater, Autor und Seminarleiter.

Kein Zweifel: Unser IT-Zeitalter wird von Cloud geprägt. Die Cloud-Strategie jedes Unternehmens ist eine Mischung aus der Nutzung bestehender Clouds und dem Aufbau einer eigenen Cloud. Dieser Beitrag befasst sich mit beiden Komponenten einer solchen Strategie.

Definition der Cloud

In 2011 veröffentlichte das US-amerikanische National Institute of Standards and Technology (NIST) eine Definition von Cloud Computing, die in der Begriffsklärung Maßstäbe setzt.

Nach dieser Definition sind die wesentlichen Merkmale von Cloud Computing die folgenden:

- **Selbstbedienung:** Der Kunde kann ohne Intervention eines Mitarbeiters des Diensteanbieters automatisch die notwendigen Ressourcen in Betrieb nehmen.

- **Nutzbarkeit über das Netz:** Die Cloud-Ressourcen sind über das Netz und standardisierte Schnittstellen nutzbar.
- **Gemeinsame Nutzung:** Verschiedene Kunden teilen sich die Nutzung von Cloud-Ressourcen, wobei die Ressourcen nach Bedarf der Kunden diesen dynamisch zur Verfügung gestellt werden. Dem jeweiligen Kunden bleibt verborgen, an welchem Standort sich die von ihm genutzten Cloud-Ressourcen wie Prozessor und Speicher befinden.
- **Schnelle Skalierbarkeit:** Eine Cloud ist in der Lage, auf den kurzfristig wechselnden Bedarf der Kunden so zu reagieren, dass dem Kunden die Cloud-Ressourcen als unendlich vorkommen.
- **Messbarkeit:** Die Nutzung der Cloud ist messbar. Zur Messbarkeit gehören die Überwachbarkeit, die Steuerung der Nutzung und das Reporting über die Ressourcennutzung.

Dasselbe Dokument unterscheidet zwischen verschiedenen Diensttypen, die sich darin unterscheiden, welche Art Service der Kunde in Anspruch nehmen kann:

- **Software as a Service (SaaS):** Der Kunde kann Applikationen nutzen, die in der Cloud laufen. Der Kunde muss sich nicht mit der Infrastruktur in der Cloud befassen. Dem Kunden bleibt verborgen, auf der Basis welcher Netze, Server, Betriebssysteme und Speicher die Applikationen in der Cloud ausgeführt werden. Häufig ist ein Browser die einzige auf der Kundenseite notwendige Software-Komponente zur Nutzung von SaaS.
- **Platform as a Service (PaaS):** Der Kunde kann seine selbst mitgebrachten Anwendungen unter Nutzung der Cloud-Infrastruktur nutzen, welche auch Programmiersprachen, Software-Bibliotheken und Software-Werkzeuge umfassen können. Der Kunde hat keinen Einfluss auf die Cloud-Infrastruktur einschließlich

Jetzt Leser werden! Wenn Sie aktuelle Artikel kostenlos und zeitnah erhalten möchten, können Sie den Netzwerk-Insider hier abonnieren: www.comconsult-research.de/insider/

Der Netzwerk Insider

Systematische Weiterbildung für Netzwerk- und IT-Professionals

der Netze, Server, Betriebssysteme und Speicher, hat aber volle Kontrolle über seine eigene Applikation.

doch verschiedene Cloud-Typen, zum Beispiel um die Last kurzfristig auf erweiterte Ressourcen verteilen zu können.

Sinnvolle Nutzung von Public Clouds

Den IT-Verantwortlichen, die aus der Welt geschlossener, ausschließlich von der eigenen Organisation genutzten IT-Ressourcen kommen, kann der Übergang ins Cloud-Zeitalter schwer fallen. Die Vorbehalte gelten vor allem der Public Cloud. Für viele IT-Abteilungen von Unternehmen und Organisationen ist es schlicht und ergreifend unvorstellbar, mit der Nutzung von Public Clouds die Kontrolle über ihre Daten und Applikationen ein Stück weit aufzugeben. Oft werden Sicherheitsvorbehalte geltend gemacht und Fragen gestellt wie: Was passiert, wenn unsere vertraulichen Daten über die Public Cloud in falsche Hände geraten? Wie können wir sicher sein, dass der Public Cloud Provider die notwendigen Maßnahmen zum Schutz unserer Daten ergreift? Wird der Provider uns mitteilen, dass unsere Daten kompromittiert worden sind?

Bedenken werden auch hinsichtlich der Verfügbarkeit von Public Clouds geäußert, etwa in der Art folgender Fragen: Was machen wir, wenn die Public Cloud, auf die wir uns verlassen, nicht verfügbar ist? Sind die allgemeinen Service Level Agreements (SLAs) für die Cloud für uns überhaupt geeignet? Können Vertragsstrafen bei SLA-Verstößen überhaupt die Schäden kompensieren, die wir durch die Nichtverfügbarkeit von Clouds erleiden?

Aber auch strategische Überlegungen spielen bei der Abneigung gegen Public Clouds eine Rolle. Macht man sich von einem Provider nicht zu abhängig, wenn man seine Cloud-Dienste nutzt? Kann der Provider, sobald wir von seinen Diensten abhängig sind, nicht seine Bedingungen diktieren? Gibt es überhaupt einen Markt mit vergleichbaren Diensten, in dem ich bei Bedarf von einem zum anderen Provider wechseln kann?

Auch wenn solche Bedenken oft übertrieben werden, haben sie im Kern ernst zu nehmende Fragen zum Gegenstand, die von jeder Cloud-Strategie beantwortet wer-

den müssen.

Den Bedenken stehen oft übersehene Vorteile in verschiedener Hinsicht gegenüber. Einige dieser Vorteile sind wie folgt:

- **Infrastructure as a Service (IaaS):** Der Dienstleister stellt dem Kunden Ressourcen in Bereichen wie Prozessor, Speicher und Netz zur Verfügung. Der Kunde ist in der Lage, auf diesen Ressourcen beliebige Software einschließlich Betriebssysteme und Anwendungen zum Laufen zu bringen. Der Kunde erhält die Steuerung von Betriebssystem, Speicher, Anwendungen und unter Umständen bestimmte Netzkomponenten wie Host Firewalls.

NIST unterscheidet folgende Typen von Clouds:

- **Private Cloud:** Die Cloud-Infrastruktur dient der exklusiven Nutzung durch eine bestimmte Organisation, die verschiedene Organisationseinheiten umfassen kann. Die Organisation selbst, ein Auftragnehmer oder eine Kombination davon betreibt die Cloud. Die Cloud-Ressourcen befinden sich am Standort der Organisation oder an anderen Standorten.
- **Community Cloud:** Eine Community Cloud bedient Organisationen mit ähnlichen Interessen oder Aufgaben, zum Beispiel die kommunalen Verwaltungen einer bestimmten Region. Der Betrieb obliegt einer oder mehreren der Nutzerorganisationen oder einer Drittinstanz. Die Ressourcen befinden sich an den Standorten der Gemeinschaft oder an anderen Standorten.
- **Public Cloud:** Die Cloud steht der Nutzung der Allgemeinheit offen. Der Betreiber kann ein Unternehmen oder eine andere private oder staatliche Organisation sein. Die Ressourcen der Cloud befinden sich an Standorten des Eigners bzw. Betreibers.
- **Hybrid Cloud:** Die Cloud-Infrastruktur basiert auf einer Kombination von mindestens zwei der anderen hier genannten Typen (Private, Community, Public). Die Hybrid Cloud stellt sich für die Nutzer als eine Einheit dar, kombiniert je-

- Die Verfügbarkeit einer Public Cloud kann sogar höher als die Verfügbarkeit der eigenen IT sein, wenn man bedenkt, dass ein Cloud-Anbieter qua Masse über mehr RZ-Standorte und dichter verknüpfte Netze zwischen diesen Standorten verfügt.

- Public Clouds können sogar sicherer als die eigene IT sein, denn Sicherheit ist das Ergebnis der harten Arbeit von Experten, von denen ein Cloud-Anbieter wiederum dank seiner Größe mehr beschäftigen kann als ein Unternehmen mit einem beliebigen anderen Aufgabenbereich.

- Oft sind Cloud Services in der Gesamtkostenrechnung preiswerter als selbst aufgebaute und betriebene IT-Dienste eines Unternehmens, das die Fixkosten nicht auf so viele verschiedene Nutzer umlegen kann wie ein Cloud Provider.

- Der Aufbau einer IT-Umgebung ist in Public Clouds oft viel schneller möglich als in der eigenen IT. So kann auf kurzfristig entstehende Anforderungen der Nutzer häufig durch Cloud-Nutzung schneller reagiert werden als wenn man alles, von Prozessor, Netz, Speicher bis zu Software selbst aufbauen müsste.

- Die Abhängigkeit vom Betreiber kann in der Cloud sogar geringer sein als in der eigenen Organisation. Clouds unterliegen einem größeren Standardisierungszwang als eigene IT-Umgebungen. Nicht selten ist der Verlust eines eigenen IT-Mitarbeiters schmerzhafter als der Wechsel von einem zum anderen Service Provider.

Angesichts dieser Vorteile nutzen mittlerweile viele Unternehmen die Möglichkeiten von Public Clouds. Nachfolgend seien ohne Anspruch auf Vollständigkeit und auf der Basis der Beobachtungen des Autors einige Beispiele genannt:

Der Netzwerk Insider

Systematische Weiterbildung für Netzwerk- und IT-Professionals

- Für ein Medienunternehmen, dessen Kerngeschäft die Veröffentlichung von Nachrichten, Reportagen, Kommentaren, Bildern usw. zum aktuellen Geschehen ist, ist der Wert der Daten sehr zeitabhängig. Daten, die heute geheim sind, sind morgen schon öffentlich. Das mit der Kompromittierung der Daten eingehende Risiko ist gut kalkulierbar und auf eine kurze Zeitspanne vom Beginn der Bearbeitung eines Beitrags bis zur Veröffentlichung begrenzt. Diesem Risiko stehen die Vorteile der Nutzung von Public Clouds gegenüber. Zum Beispiel können weltweit agierende Korrespondenten des Unternehmens in der Regel einfacher und schneller auf eine Public Cloud zugreifen als auf die unternehmenseigene IT.
- Mitarbeiter des Vertriebs sind häufig mobile Mitarbeiter. Um solchen Mitarbeitern alle Werkzeuge zur Verfügung zu stellen, die sie für ihre tägliche Arbeit benötigen, sind große Anstrengungen erforderlich, von Infrastrukturen für den Zugriff mobiler Clients bis zu oft teuren Lizenzen für Anwendungen wie Customer Relationship Management (CRM). CRM-Angebote in der Cloud-Ausprägung gibt es schon lange. Das Risiko, dass zum Beispiel die Historie der Geschäfte eines Unternehmens mit einem bestimmten Kunden über die Cloud in falsche Hände gerät, ist zwar nicht von der Hand zu weisen, jedoch auch gut kalkulierbar.
- Weltweit agierende Unternehmen haben oft große Schwierigkeiten, ihren Mitarbeitern einen leistungsfähigen und zugleich sicheren Zugriff auf das Internet zu ermöglichen. Zentralisiert man den Zugang, weil man die Sicherheitsinfrastruktur wie Proxies und Content Security nur an einer Stelle realisieren will, müssen zum Beispiel Mitarbeiter in Asien über Europa auf Inhalte in Asien zugreifen. Als Alternative stehen Internet Security Clouds zur Verfügung. Einige Firmen betreiben weltweit verteilte Netze von Web Security Gateways (WSG) und bieten die Nutzung solcher Gateways kommerziell an. Die Nutzung solcher Gateways über das Internet entlastet die oft teuren Ressourcen des privaten Wide Area Network (WAN) des Unternehmens. Diese Ent-

lastung kann erheblich sein, denn nach den Beobachtungen des Autors ist die Webnutzung nicht selten für mehr als die Hälfte der Last in Unternehmensnetzen verantwortlich.

- Public Clouds können gut zu Testzwecken genutzt werden. Viele Unternehmen legen darauf wert, vor der Einführung jeder Anwendung diese zu testen. Eine Testumgebung unter Nutzung einer Public Cloud ist häufig schneller realisierbar als eine Testumgebung, die man selbst aufbaut.
- Beinhaltet eine Anwendung die starke Verschlüsselung der Daten und die Möglichkeit, das Schlüsselmanagement in der eigenen Hand zu behalten, können Unternehmen sogar vertrauliche Daten in der Cloud halten und dabei die Vorteile der Public Clouds nutzen.

Wozu eine Private Cloud?

Auch wenn es viele Beispiele für die sinnvolle Nutzung von Public Clouds gibt, führt die Risikoabwägung sowie eine umfassende Betrachtung der Vor- und Nachteile der Cloud-Nutzung und des Eigenbetriebs oft zu dem Ergebnis, dass zumindest ein Teil der Anwendungen und Daten im eigenen Hause zu behalten sind. Bleibt für solche Anwendungen und Daten im Cloud-Zeitalter alles beim Alten?

Die Antwort ist meistens nein. Die IT-Abteilung jedes Unternehmens muss sich heutzutage mit der Wirtschaftlichkeit, Agilität und Flexibilität messen lassen, die man von Clouds kennt. Nutzer werden immer weniger bereit sein, für ähnliche Aufgaben schlechtere Rahmenbedingungen bei der Nutzung der unternehmenseigenen IT zu akzeptieren als bei der Cloud-Nutzung. Auf zunehmendes Unverständnis stößt eine Unternehmens-IT, wenn sie für die Einrichtung einer neuen Applikation Wochen braucht.

So werden die Eigenschaften von Clouds auch für die internen IT-Abteilungen der Organisationen zum Maß aller Dinge:

- Selbstbedienung
- Nutzbarkeit über das Netz

- Gemeinsame Nutzung
- Schnelle Skalierbarkeit
- Messbarkeit

Im Folgenden wird auf diese Aspekte bezüglich Private Clouds eingegangen:

Selbstbedienung

Was bei der Selbstbedienung durch Kunden von Public Clouds selbstverständlich ist, erweist sich in Private Clouds aus verschiedenen technischen und organisatorischen Gründen als schwierig.

Die Management-Werkzeuge für Virtualisierung und Betriebssysteme, die bei IT-Abteilungen der Organisationen etabliert sind, eignen sich gut für die Einrichtung von IT-Diensten durch Administratoren und IT-Experten, sind jedoch nicht dafür geschaffen, dass ein Anwender seine Umgebung selbst konfiguriert. Eine Übertragung der Werkzeuge aus Public Clouds auf Private Clouds ist nicht einfach. Erstens gehen die Betreiber der Public Clouds mit solchen Werkzeugen oft als Betriebsgeheimnisse um. Zweitens müssen die Public Cloud Provider oft nur standardisierte und relativ einfach gestrickte Umgebungen einrichten lassen. Die IT-Wirklichkeit in den Unternehmen ist komplexer. Viele Anwendungen sind mit anderen Anwendungen verknüpft. Die Einrichtung gekoppelter Applikationen ist wesentlich komplexer als die Realisierung einer in sich geschlossenen Standardanwendung.

Noch gravierender als die technischen sind die organisatorischen Hindernisse. Selbst wenn die Selbstbedienung technisch ermöglicht wird, stellt sich die Frage, wer im Unternehmen berechtigt ist, durch Selbstbedienung Ressourcen in der Private Cloud zu belegen. Eine weitere Frage ist, ob es durchsetzbar ist, Dienste und Applikationen auf Zeit einzurichten und nach Ablauf der Zeit diese zu automatisch deaktivieren zu lassen. Kaum jemand möchte die Verantwortung dafür übernehmen, eine laufende Applikation zu deaktivieren.

Ein Kompromiss kann darin bestehen, dass die Selbstbedienung nicht allen Nutzern in der Organisation ermöglicht wird, sondern Administratoren, die ohne Hil-

Der Netzwerk Insider

Systematische Weiterbildung für Netzwerk- und IT-Professionals

fe anderer Administratoren alle erforderlichen Schritte für die Einrichtung einer Anwendung durchführen können. Dann kann der Durchlauf der Einrichtung, die wegen der Einteilung der IT-Organisation in Sparten wie Server, Virtualisierung, Storage und Netz langwierig sein kann, beschleunigt werden.

Somit ist die Suche nach der geeigneten Tool-Landschaft für die Automatisierung der Einrichtung von Diensten und Applikationen zum Fokus vieler IT-Abteilungen geworden. Das Ziel besteht darin, dass möglichst aus demselben Tool aus bisher ganz verschiedene Ressourcen wie Server, Speicher und Netz für eine bestimmte Anwendung bereitgestellt werden. (siehe Abbildung 1)

Verschiedene Anbieter versuchen, mit ihren Produkten diesem Bedarf der IT-Abteilungen gerecht zu werden. Zu diesen Anbietern gehören die folgenden:

- Anbieter von Lösungen für die Virtualisierung
- Hersteller von Netzkomponenten
- Server-Hersteller

Nach Einschätzung des Autors ist eine Lösung für Virtualisierung die für die Bündelung der Automatisierung am meisten ge-

eignete Komponente der IT-Umgebung. Ein heutiger Hypervisor erlaubt nicht nur die Einrichtung virtueller Server, sondern auch die Zuordnung von Speicher und die Konfiguration eines virtuellen Netzes. Die Hersteller von Lösungen für die Virtualisierung haben in den letzten Jahren ihre Produkte um Automatisierungswerkzeuge erweitert.

Aber auch einige Netzhersteller versuchen, im Markt für RZ-Automatisierung Fuß zu fassen. Ihre Stärken liegen natürlich im Netzbereich. Was die Konzepte dieser Hersteller, zum Beispiel aus dem Bereich Software Defined Networking (SDN), oft vermissen lassen, ist der gesamtheitliche Ansatz, der die Automatisierung nicht nur im Netzbereich, sondern auch im Server- und Speicherumfeld ermöglicht.

Auch Serverhersteller haben in den letzten Jahren die Automatisierungsfunktionen für ihre Produkte verbessert. Das Unified Computing System (UCS) von Cisco beispielsweise ermöglicht das sogenannte Stateless Computing. Gemeint ist die zentrale Speicherung von normalerweise hardwaregebundenen Konfigurationsdaten, so dass physikalische Server ausgetauscht werden können, ohne dass die Ersatzhardware aufwändig konfiguriert werden muss. Diese Funktion ergänzt die Virtualisierung. Während die Automatisierungsfunk-

tion der Virtualisierung dafür sorgt, dass auf der Basis vorhandener Server-, Netz- und Speicherhardware virtuelle Ressourcen definiert werden, ist die Automatisierung der Server-Hardware dafür zuständig, dass neue Hardware möglichst effizient und schnell hinzugefügt werden kann, zum Beispiel um festgestellte Engpässe zu beheben. (siehe Abbildung 2)

Nutzbarkeit über das Netz

Schon lange vor dem Cloud-Zeitalter haben Unternehmen ihre IT-Ressourcen vernetzt. Insofern ist die Eigenschaft „Nutzbarkeit über das Netz“ für IT-Abteilungen nichts Neues. Die Frage ist aber, über welches Netz. Was ist das passende Netz zur Cloud?

Man könnte auf dem Standpunkt stehen, mit der Private Cloud ändere sich im Unternehmensnetz nichts. Es gibt nach wie vor ein RZ-Netz, möglicherweise bestehend aus einem Ethernet- und einem Fibre-Channel-Teil, und dann das unternehmensinterne Netz, das sich über verschiedene Standorte, Campusnetze, Gebäudenetze etc. erstreckt. Das Ethernet im RZ folgt anderen Regeln als das Netz außerhalb der Rechenzentren und muss zum Beispiel Layer-2-Domänen zwischen verschiedenen Standorten ermöglichen.

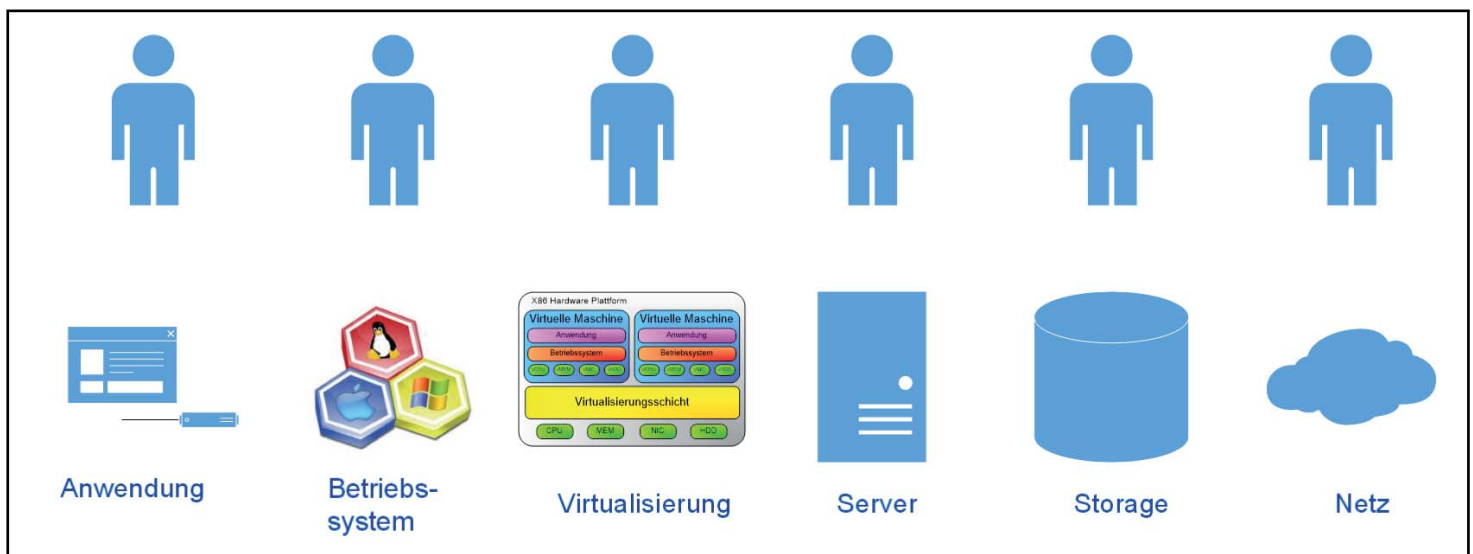


Abbildung 1: Automatisierung muss verschiedene Felder abdecken

Jetzt Leser werden! Wenn Sie aktuelle Artikel kostenlos und zeitnah erhalten möchten, können Sie den Netzwerk-Insider hier abonnieren: www.comconsult-research.de/insider/

Der Netzwerk Insider

Systematische Weiterbildung für Netzwerk- und IT-Professionals

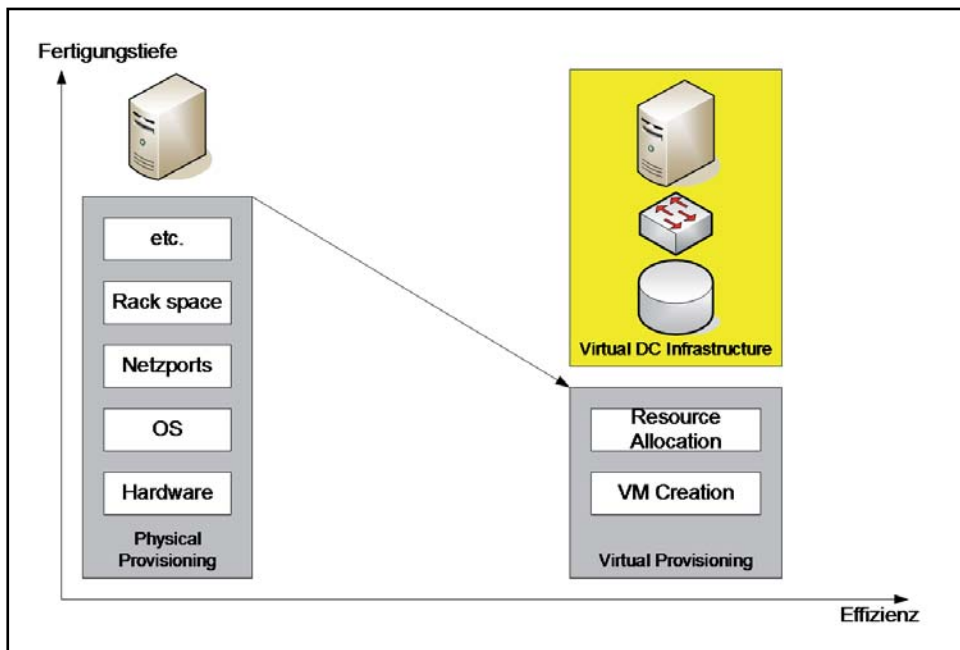


Abbildung 2: Effizienz durch Virtualisierung

Die Realität ist aber leider etwas komplexer. Mit „Nutzbarkeit über das Netz“ im engeren Sinne ist zunehmend auch die Nutzbarkeit über das Internet gemeint. Denn immer mehr mobile Mitarbeiter greifen über das Internet auf Clouds – öffentliche wie private – zu und erwarten eine komfortable, unkomplizierte und zugleich sichere Möglichkeit der Cloud-Nutzung. Klassische Konzepte, bei denen solchen mobilen Mitarbeitern nur ein zentraler VPN-Zugang zur Verfügung steht, der möglicherweise über sehr lange interkontinentale Verbindungen zu nutzen ist, stoßen immer wieder auf Performance- und Akzeptanz-Probleme.

Überlegungen in vielen Unternehmen gehen daher schon so weit, dass das „Intranet“ im Sinne des weltweit verteilten „in-ternen“ Netzes abgeschafft wird. Diese Überlegungen sind darin begründet, dass angesichts der zunehmenden Nutzerzahl und Vielfalt der über das Internet zu realisierenden Zugänge ein separates Intranet, in dessen Sicherheit große Anstrengungen investiert werden müssen, immer stärker an Sinnfälligkeit verliert. Ausnahmen können zum Beispiel räumlich ohne-

hin geschlossene Lokationen sein, zum Beispiel Produktionsstandorte. Aber der normale Büroarbeitsplatz verlagert sich immer mehr in die mobile Welt. Ein solcher Arbeitsplatz hat als Netzzugang das Internet zur Verfügung. Für solche Nutzerzenarien sind Sicherheitskonzepte auszuarbeiten. Wenn dies ohnehin zu leisten ist, kann gleich die Nutzerzahl erhöht werden und alle Nutzer umfassen, die einen normalen Büroarbeitsplatz benötigen.

In solchen Überlegungen ist das Internet das Netz des Cloud-Zeitalters. Und dann spielt es für einen Arbeitsplatz keine große Rolle, ob der Service, den er nutzt, in einer öffentlichen oder einer privaten Cloud realisiert ist.

Gemeinsame Nutzung

Die Mandantenfähigkeit der IT-Infrastruktur ist natürlich im Falle der öffentlichen Clouds nicht nur eine Forderung der Kunden, sondern auch ein Gebot der Gesetzgebung und Regulierung. Aber auch private Clouds müssen die gemeinsame Nutzung derselben physika-

lischen Infrastruktur durch Anwendungen und Nutzergruppen ermöglichen, die aus Sicherheitsgründen voneinander zu trennen sind. Viele Unternehmensnetze bestehen jetzt schon aus verschiedenen Zonen, auf die verschiedene Schutzniveaus oder auch verschiedene Benutzergruppen abgebildet werden, die voneinander zu trennen sind.

Die technische Basis für die Mandantenfähigkeit der IT-Infrastrukturen der Unternehmen ist die Virtualisierung auf verschiedenen Ebenen. Die Zeiten, in denen jegliche Trennung auch eine physikalische Trennung sein musste, sind endgültig vorbei. Erstens wäre dies in den meisten Umgebungen nicht oder nicht wirtschaftlich realisierbar. Zweitens wäre eine physikalische Trennung mit anderen Cloud-Eigenschaften wie Automatisierung nicht vereinbar. Drittens ist die Virtualisierung mittlerweile so ausgereift und erprobt, dass das notwendige Vertrauen in die Wirksamkeit der durch die Virtualisierung ermöglichten logischen Trennung geschaffen worden ist.

Virtualisierung schafft nämlich die logische Trennung auf verschiedenen Ebenen:

- Der Hypervisor trennt die Virtuellen Maschinen (VMs) voneinander und gibt ihnen zugleich die Möglichkeit, dieselbe Physik zu nutzen.
- Virtual Local Area Networks (VLANs) und Virtual Private Networks (VPNs), auf welcher Ebene sie auch immer realisiert werden, sorgen für die logische Trennung im Netz.
- Diverse Verfahren sind für die logische Trennung von Speicher verfügbar, von klassischen Verfahren auf der Basis der Trennung der Logical Units (LUNs) und Zoning im SAN bis zu systeminternen Mechanismen für die Bildung von logischen Volumes.

Die technischen Möglichkeiten sind also da. Eine Herausforderung besteht aber darin, das passende Zonenkonzept für die Cloud zu finden. Das Zonenkonzept darf sich nicht mit jeder neuen Anwendung ändern. Jede neue Anwendung muss mög-

Der Netzwerk Insider

Systematische Weiterbildung für Netzwerk- und IT-Professionals

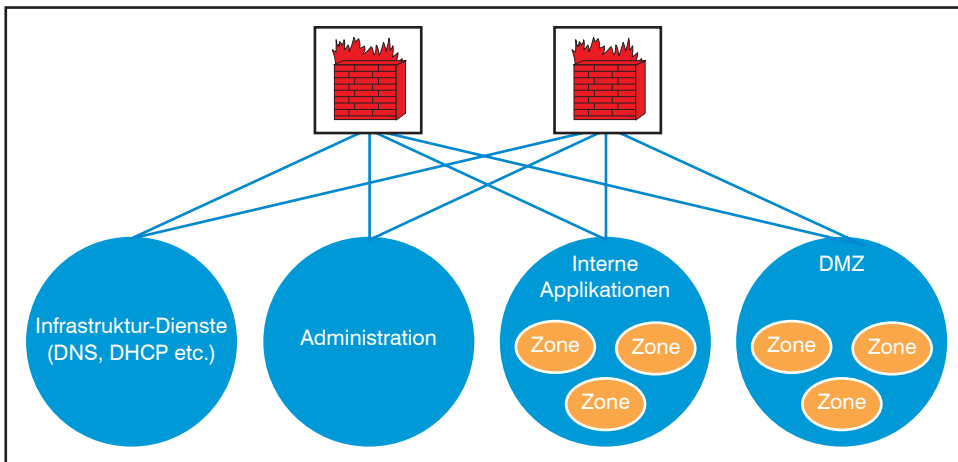


Abbildung 3: Idee für ein Zonenkonzept

lichst zu einer bestehenden Zone zuzuordnen sein. (siehe Abbildung 3)

Schnelle Skalierbarkeit

Eine Anekdote besagt, dass der Amazon-Chef bei einer Visite in einem Rechenzentrum der Firma auf die Idee gekommen sei, die auf Spitzenzeiten ausgelegte Infrastruktur von Amazon in der übrigen Zeit kommerziell zu vermarkten. Eine der Hauptideen hinter Cloud besteht darin, dass Synergieeffekte für die schnelle Skalierbarkeit genutzt werden, bis hin zu dem Eindruck, dass jedem Cloud-Nutzer die Ressourcen der Cloud unendlich vorkommen.

Damit dies funktioniert, muss jede Cloud stets für die zu erwartenden Neuzugänge an Nutzern und Applikationen ausreichend Reserve vorweisen. Eine Alternative hierzu wäre, IT-Ressourcen wie elektrische Leistung auf einem Umschlagplatz zu beziehen. Leider ist Letzteres im Moment zu sehr visionär, um von der Machbarkeit ausgehen zu können.

Insbesondere Private Clouds müssen daher nach dem Prinzip des kalkulierten Überangebots an Ressourcen arbeiten. Dies ist nur machbar, wenn möglichst viele Anwendungen des Unternehmens den in der Private Cloud gesetzten Standard nutzen und nach einem Profil gestrickt sind, das zur Private Cloud passt. Wenn viele Anwendungen aus der Reihe tanzen und nicht

in das Cloud-Ressourcenschema passen, werden Synergieeffekte immer spärlicher und die Umsetzung des Überangebotsprinzips immer unwirtschaftlicher.

Es gibt auch noch eine organisatorische Herausforderung. Viele IT-Vorhaben in Unternehmen werden projektorientiert geplant und finanziert. Eine Organisations-

einheit plant eine neue Anwendung und bringt das notwendige Geld mit, um sie zu realisieren. Nach diesem Finanzierungsschema kann Cloud nicht funktionieren. Die Sinnfälligkeit der Cloud steht und fällt damit, dass Investitionen in Hardware-Ressourcen von der Finanzierung einzelner Anwendungen entkoppelt werden. Eine Erweiterung um standardisierte Hardware darf nicht auf die Finanzierung durch ein Projekt warten müssen, sonst funktioniert die schnelle Skalierbarkeit nicht. Cloud-Ressourcen müssen wie Strom, Wärme, Klimatisierung, Wasser implementiert und zur Verfügung gestellt werden. Das steht nicht im Widerspruch zur verursachergerechten Finanzierung.

Messbarkeit

Nicht nur für die verursachergerechte Finanzierung muss die Nutzung von Cloud-Ressourcen messbar sein. Die Messbarkeit ist auch für die vorausschauende Planung erforderlich. Jeder Cloud-Betreiber muss stets darüber im Bilde sein, wie ausgelastet seine Prozessoren, Netze und Speicher sind, um bei drohendem Engpass rechtzeitig reagieren zu können.

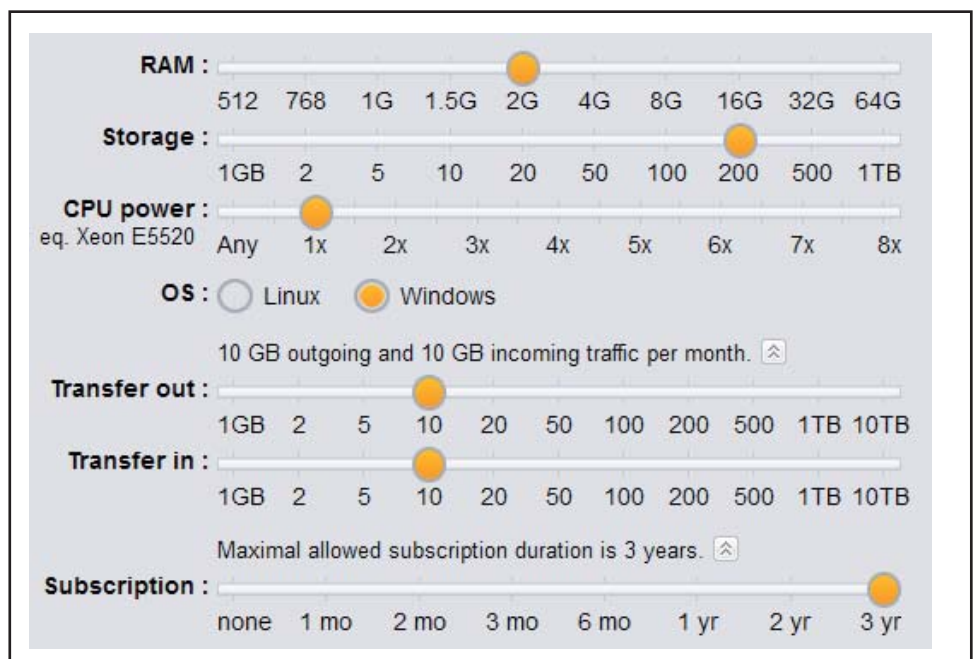


Abbildung 4: Idee für Abrechnungsmodell

Jetzt Leser werden! Wenn Sie aktuelle Artikel kostenlos und zeitnah erhalten möchten, können Sie den Netzwerk-Insider hier abonnieren: www.comconsult-research.de/insider/

Der Netzwerk Insider

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Der Komplexitätsgrad der Finanzierungsschlüssel muss sich natürlich in Grenzen halten. Gute Ideen kann man den kommerziellen Modellen der Public Cloud Provider abgewinnen, denn schließlich sind diese Modelle schon ein paar Jahre auf dem Markt und funktionieren offensichtlich. Ob man in den Finanzierungsschlüsseln nur statische Parameter wie Anzahl der VMs, Umfang des reservierten Speichers oder Anzahl und Typ der Netzports vorsieht oder auch dynamische Kennzahlen wie tatsächliche Netzlast, ist eine Frage des Aufwands, den man in die Abrechnung zu investieren bereit ist, sowie der Akzeptanz im eigenen Unternehmen.

Wenn die Kundschaft eher Planungssicherheit bevorzugt, sind statische Parameter zu empfehlen. Bestehen die „sparsamen“ Verbraucher auf genauere Abrechnung, können auch dynamische Kennzahlen herangezogen werden. Letzteres darf aber nicht dominieren, wenn man den Aufwand für die Abrechnung in Grenzen halten will. (siehe Abbildung 4)

Fazit

Kein Unternehmen kommt an der Nutzung und/oder dem Aufbau von Clouds vorbei. Nachdem man geklärt hat, welche Anwendungen und Daten in öffentlichen

Clouds gut aufgehoben sind und für welche man die private Cloud benötigt, kann man zum Aufbau der privaten Cloud die vorhandenen technischen Möglichkeiten sowie die Erfahrungen von Unternehmen nutzen, die schon Clouds betreiben. Die Wesensmerkmale der Cloud dürfen dabei nicht aus dem Blickfeld geraten, nämlich Automatisierung (in erster Linie für Administratoren und später vielleicht auch bis zur Selbstbedienung durch Anwender), Nutzbarkeit über das Netz und am besten über das Internet, Mandantenfähigkeit, Skalierbarkeit durch kalkuliertes Überangebot an Ressourcen sowie Messbarkeit der Cloud-Nutzung.

Kongress

ComConsult Netzwerk Forum 2015
20.04. - 22.04.15 in Königswinter

Netzwerke im Rechenzentrum
Netzwerk-Design: kommt eine neue Form von Netzwerk?
Betriebsoptimierung

Das ComConsult Netzwerk Forum 2015 stellt die momentan dominantesten Netzwerk-Themen in den Mittelpunkt der Veranstaltung: Netzwerke im Rechenzentrum, Netzwerk-Design und Betriebsoptimierung. Zwei Vortragstage und ein optionaler Vertiefungstag bilden den perfekten Rahmen um effizient und kompakt auf den neuesten Stand zu kommen.

Das ComConsult Netzwerk Forum 2015 ist die herausragende Veranstaltung im Jahr 2015. Wie immer ein Treffpunkt der Branche und schlicht der beste Ort um in kürzester Zeit auf den neuesten Stand zu kommen.

Die Veranstaltung kombiniert zum Vorteil der Teilnehmer:

- Unsere Auswahl der aktuellsten Themen der Netzwerk-Szene
- Top-Referenten
- Exklusive Präsentationen von ComConsult Research, die nur auf unseren Foren veröffentlicht werden
- Aktuelle Praxiserfahrungen aus laufenden Projekten

Moderation: Dr. Jürgen Suppan

Preis: Kongress mit Intensiv-Tag 20.04. - 22.04.15 - € 2.390,--
Kongress ohne Intensiv-Tag 20.04. - 21.04.15 - € 1.990,--
Intensiv-Tag am 22.04.15 - € 790,--



Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

Jetzt Leser werden! Wenn Sie aktuelle Artikel kostenlos und zeitnah erhalten möchten, können Sie den Netzwerk-Insider hier abonnieren: www.comconsult-research.de/insider/