



Unternehmen auf das Zeitalter der Cloud vorbereiten

Erkenntnisse aus fünf Jahren Cloud-Migration

UNTERNEHMEN AUF DAS ZEITALTER DER CLOUD VORBEREITEN

Unternehmen verlassen sich beim Betrieb ihrer Workloads immer seltener ausschliesslich auf selbstbetriebene IT-Umgebungen im eigenen Rechenzentrum. Stattdessen setzen sie zunehmend auf die Cloud – in Europa ebenso wie im Rest der Welt. Cloud Services sind für Unternehmen und deren Anwendungsstrategie mittlerweile grundlegend geworden. Damit steigen auch die Anforderungen: Unternehmen benötigen einen sicheren, hochperformanten und kosteneffektiven Zugang zu Public Clouds wie Microsoft Azure, Amazon Web Services (AWS) und zu den vielen SaaS-Anbietern.

Mitten in diesem Umbruch wollen die Unternehmen das Beste aus beiden Welten für sich herausholen. Einerseits haben sie den Anspruch, ihre sensiblen Daten zu schützen und selbst die volle Kontrolle darüber zu behalten. Sie müssen regulatorische Auflagen erfüllen und wollen ihre Anwendungen mit der gewünschten Performance betreiben, also mit geringer Latenz und verlässlichen Verbindungen in die Public Cloud. Andererseits haben die Unternehmen mit weiter sinkenden IT-Budgets und Fachkräftemangel zu kämpfen, wodurch die Connectivity mit dem öffentlichen Internet eine interessante Option verspricht. Bestenfalls ist und bleibt diese aber nur eine Teillösung.

In den vergangenen fünf Jahren konnten wir sehen, wie Unternehmen unterschiedliche Ansätze ausprobiert haben, um diese Kluft zu überbrücken. Als erfolgreichste Strategie erwies sich dabei, Teile des Unternehmensnetzwerks in ein neutrales Colocation-Rechenzentrum zu verlagern. Zudem werden Anwendungen nicht länger in einer „On-Premise-Lösung“ im eigenen Rechenzentrum betrieben, sondern intelligent mit Colocation-Rechenzentren und Cloud-Infrastrukturen kombiniert. Die Vorteile dieser Strategie sind eine hohe Performance und sichere Verbindungen zu Public Cloud und zu SaaS Services, wodurch die digitale Transformation vorangetrieben wird. Unternehmen, die auf diese Strategie setzen, können ihr Netzwerk und ihre Anwendungen zentral managen und gleichzeitig Daten, falls erforderlich, in einer privaten und selbst verwalteten Infrastruktur behalten.





Der Schock des Neuen

Unternehmen stehen vor der Herausforderung, sehr komplexe Umgebungen verwalten zu müssen, in denen bereits vorhandene Anwendungen auf neue Anwendungen treffen, die speziell für die Cloud entwickelt wurden. Zudem verwalten sie einige Teile ihrer IT nach wie vor selbst, während sie das Management anderer Teile ausgelagert haben. An diesen Umständen wird sich voraussichtlich für mindestens weitere zehn Jahre auch nichts ändern. Konzerne, Service Provider und Systemintegratoren möchten sich zunehmend mit den verschiedenen cloudbasierten Angeboten verbinden, doch diverse Herausforderungen machen einen anderen Ansatz erforderlich. Die Qualität der Internetverbindungen schwankt oft und ist wenig transparent. Die Orchestrierung der vielfältigen Services ist schwierig. Zudem werden die Grenzen des Netzwerks unübersichtlicher, was neue Herangehensweisen in puncto Sicherheit erfordert.

Um den Herausforderungen zu begegnen, haben sich in den vergangenen fünf Jahren viele Unternehmen darauf spezialisiert, Konzernen auf dem Weg in die Cloud zu helfen – sei es mit Application Performance Management, Cloud Service Deployment and Monitoring, Distributed Security Services oder mit einer Fülle anderer Dienstleistungen. Es sind so viele neue Anbieter kritischer Services auf den Markt gekommen, dass die Komplexität der Aufgabe, die sie zu lösen versprechen, ironischerweise eher zu- als abgenommen hat: Die Unternehmen müssen eine Möglichkeit finden, diese Services zu integrieren und die nötigen Mittel bereitstellen, um sie ganzheitlich zu managen.

Wenn die beste Lösung mehr Aufwand bedeutet

In ihren Anfangszeiten wurde die Cloud-Adaption weniger geplant als vielmehr von frustrierten Anwendern vorangetrieben. Oft stellten diese Mitarbeiter über das öffentliche Internet Verbindungen in die Cloud her, die ausserhalb der Kontrolle der IT-Abteilungen lagen. Zu Recht warnten damals viele Experten vor den Gefahren einer „Schatten-IT“ oder der „Consumerisation der IT“.

Seit diesen frühen Tagen hat sich einiges getan. Inzwischen sind viele dieser Cloud Services in Unternehmen ein grundlegender Bestandteil der offiziellen IT-Infrastruktur. Die IT-Abteilungen unterstützen sie weitgehend und haben sie reglementiert, um die Gefahr von Verstössen gegen die Sicherheit und regulatorische Auflagen zu minimieren. Allerdings haben wir festgestellt, dass die Evolution der Netzwerkarchitektur in den Konzernen nicht immer Schritt gehalten hat. Sie berücksichtigt häufig nicht die Sensibilität der Vorgänge, die mit derartigen Services abgewickelt werden. Im Durchschnitt sind heute in Konzernen zwischen drei und fünf IaaS/PaaS-Anbieter mit dem Thema Managed IT Connectivity betraut. Dem gegenüber stehen nicht weniger als 15 bis 20 SaaS-Anbieter.

Nutzen wir das Internet privat zu Hause, ist die Performance der benötigten Services unserer Erfahrung nach grundsätzlich relativ zuverlässig und gut. Wir führen Videotelefonate via Skype, geniessen Netflix in 4K, Gaming und Online-Banking. Im Unternehmensumfeld ist die Internetnutzung jedoch etwas vollkommen anderes. Wenn es hier um geschäftskritische Daten und Anwendungen geht, sind die Anforderungen sehr viel höher. Das gilt besonders dann, wenn Anwendungen sowohl ein Rechenzentrum (selbst betrieben oder neutrale Colocation) als auch die Cloud benötigen.

Latenzen mindern die Performance von Clustern nicht linear, sondern exponentiell, sodass selbst kleine Latenzschwankungen Anwendungen spürbar beeinflussen können. Das merken auch diejenigen, die mit ihnen arbeiten müssen. Für viele ISPs nimmt dabei der Traffic Grössenordnungen an, die nicht mehr zu bewältigen sind. Schlimmstenfalls können abbrechende Verbindungen, grosse Latenzen oder unzureichender Durchsatz dazu führen, dass Daten nicht mehr korrekt synchronisiert werden. Es kommt zum „Split Brain“, also verschiedenen Datensätzen, die an unterschiedlichen Orten gespeichert werden. Das lässt sich oft nur mit hohem Aufwand beheben und kann immense Kosten verursachen. Unseren Erkenntnissen zufolge benötigen Konzerne daher eine sehr viel zuverlässigere und sicherere Verbindung als sie das öffentliche Internet planmässig bieten kann. Aus diesem Grund sind für sie private Verbindungen in die Cloud so interessant.

Sicher und geschützt

Noch vor fünf Jahren war Netzwerksicherheit für Cloud Connectivity ein eher nachgeordnetes Thema. Die vorherrschende Meinung lautete, dass IPSec oder SSL-Verschlüsselung für die in der Cloud betriebenen Anwendungen und Workloads ausreichen. Im Jahr 2018 ist die Lage eine ganz andere. Heute werden auch kritische Anwendungen teilweise oder vollständig in der Cloud betrieben. Sensible Daten, personenbezogen und/oder geschäftlich, werden ständig zwischen privaten und öffentlichen Umgebungen ausgetauscht. Deshalb müssen Cloud-Umgebungen als integraler Bestandteil des Netzwerks angesehen werden, mit allen einhergehenden Konsequenzen für die Nachverfolgbarkeit, Sichtbarkeit und Verwaltung.

Verbindungen mit dem öffentlichen Internet können geschützt werden. Schwieriger ist der Umgang mit der Visibility und der Verwaltung von internetbasierten Tunneln. Zumal die Zahl der zu sichernden Endgeräte ausufert und für Unternehmen einen höheren Verwaltungs- und Kostenaufwand bedeutet als ursprünglich angenommen. Sicherheit und Performance gehen dabei Hand in Hand: Bandbreite zu garantieren und Apps mit ausreichend Durchsatz auszustatten, ohne dabei die nötigen Sicherheitsmassnahmen zu beachten? Das ist heute nicht mehr akzeptabel.

Die Netzwerkränder befinden sich immer öfter in Colocation-Rechenzentren

Die wahrscheinlich grösste Wachstumsgeschichte der vergangenen fünf Jahre ist in diesem Zusammenhang, dass immer mehr Unternehmen die Schlüsselfunktionen der Randbereiche ihrer Netzwerke in Cloud- und Carrier-neutrale Colocation-Rechenzentren verlagern. Parallel dazu werden auch Hybrid-Cloud-Lösungen immer erfolgreicher; dabei werden Anwendungen teils in einer privaten – teils in einer öffentlichen Umgebung betrieben und von den in Colocation-Rechenzentren betriebenen Teilen des Netzwerks unterstützt. Dieser Ansatz beseitigt die Bedenken bezüglich der Performanceprobleme, die das öffentliche Internet mit sich bringen kann: Im Colocation-Rechenzentrum sind Unternehmen nur noch Millisekunden von den führenden Cloud-Service-Providern entfernt.

Für viele Unternehmen begann die Integration der Cloud-Plattformen in ihre Umgebungen mit der Nutzung von Fläche und Strom für Enterprise Edge Services. Im nächsten Schritt vergrösserten sie ihre Flächen, um auch private und interne Anwendungen in die Colocation-Umgebung verlagern zu können. Damit einher ging die vollständige Migration in die neue Hybrid-Umgebung, gefolgt vom Abschalten der veralteten Infrastruktur im firmeneigenen Rechenzentrum.

Bei dieser Vorgehensweise kommt es nicht nur auf ein hohes Mass an Connectivity an, sondern auch auf die Qualität und die Reichhaltigkeit des Traffics. Colocation-Rechenzentren bieten Zugang zu vielen verschiedenen Connectivity-Anbietern und eine von hohem Wettbewerb geprägte Umgebung. Unternehmen können hier bestehende Verträge mit Carriern und Providern nachverhandeln oder schnell neue Partner finden, die kosteneffektivere Alternativen bieten. Neben der deutlich verbesserten Connectivity ermöglichen es Colocation-Rechenzentren ihren Kunden zudem, die Kosten und den Bandbreitenbedarf zu reduzieren, den sie für den Betrieb ihrer eigenen Rechenzentren benötigen – sofern diese Rechenzentren nicht ohnehin schon überflüssig geworden sind.



Die wahrscheinlich grösste Wachstumsgeschichte der vergangenen fünf Jahre ist in diesem Zusammenhang, dass immer mehr Unternehmen die Schlüsselfunktionen der Randbereiche ihrer Netzwerke in Cloud- und Carrier-neutrale Colocation-Rechenzentren verlagern.



Im Durchschnitt sind heute in Konzernen zwischen **drei und fünf** IaaS/PaaS-Anbieter mit dem Thema Managed IT Connectivity betraut. Dem gegenüber stehen nicht weniger

...als

15-20

SaaS-Anbieter

Das Beispiel eines Kunden von Interxion zeigt, wie ein solcher Prozess in den vergangenen fünf Jahren typischerweise ablief:

Unser Kunde, ein grosser Konzern, betrieb drei private Rechenzentren und nutzte einen Carrier, um mehr als 50 Zentralen und 2.000 Filialen in ganz Europa über ein privates IP-Netzwerk miteinander zu verbinden.

Um Anwendungen zu aktualisieren und Kosten zu senken, entwickelte der Kunde einen langfristig angelegten Plan. Ziel sollte sein, die privaten Rechenzentren zu schliessen und die Kosten für den Netzwerkbetrieb zu reduzieren. Zudem wollte der Konzern Zugang zu einer grösseren Auswahl an IT-Serviceanbietern erhalten und ein Netzwerk, das ein deutlich höheres Mass an Individualisierung ermöglicht.

Beim Umsetzen des Plans richtete der Konzern im ersten Schritt Points of Presence (PoPs) in vier Rechenzentren von Interxion ein. Diese PoPs befanden sich an den vier für den Konzern wichtigsten Standorten. Dadurch erhielt er Zugang zu einer hohen Zahl an regionalen und lokalen ISPs und konnte seine lokale Connectivity deutlich steigern. Die Verbindungen zwischen Zentralen und Filialen und auch die Anbindung der Mitarbeiter im Aussendienst oder in Home-Offices waren nun sehr viel besser. Dabei wurden die Ränder des Unternehmensnetzwerks neu definiert. Zusätzlich schuf der Konzern zwei private Verbindungen zu AWS für seine Dev/Ops-Umgebung, um seine Cloud-Migrationen zu unterstützen.

Über mehrere Jahre hinweg galt nun die Devise „Cloud First“. Workloads wurden migriert, wobei zunächst genau analysiert wurde, welche Anwendungen es im Netzwerk gab, in welche davon künftig weiter investiert werden soll – und welche durch SaaS-basierte Alternativen ersetzt werden. Bei dieser Analyse identifizierte der Kunde etliche bestehende Anwendungen und Workloads, die zwar weiter benötigt wurden, aber künftig näher an der Public und/oder Private Cloud betrieben werden sollten. Er verfolgte dabei einen hybriden Ansatz und das Ziel, Daten und Anwendungen stets so nahe aneinander wie möglich zu betreiben.

Im Laufe der Zeit identifizierte der Konzern geeignete SaaS-Anbieter und ging die Integration in AWS an. Zudem fiel die Entscheidung, künftig auf Office 365 und Skype for Business zu setzen. Dafür wurden zwei weitere private Verbindungen zu Microsoft eingerichtet, die unmittelbar zu einer deutlich besseren Qualität, vor allem bei Skype-Anrufen, führten. Dank des positiven Effekts nahmen die Mitarbeiter des Konzerns den neuen Service sehr schnell an.

Ein weiterer wichtiger Schritt im Projekt war die Umstrukturierung von Edge-Netzwerkfunktionen, einschliesslich Network Security, Network Performance Management und Remote Access Integration, aus der eigenen IT-Umgebung heraus und in die Rechenzentren von Interxion. Dadurch konnte der Konzern seinen Bedarf an „Tromboning“ – dem Umleiten von Traffic in alternative, günstigere Netze – in beide Richtungen deutlich reduzieren. Bestehende interne Anwendungen konnten beinahe vollständig an zwei strategisch wichtige Interxion Standorte ausgelagert werden, wo die Netzwerk-PoPs und die privaten Verbindungen in die Clouds zum Tragen kommen. Heutiger Stand ist: Der Konzern konnte bereits eines seiner eigenen Rechenzentren ausser Betrieb nehmen. Die beiden verbleibenden eigenen Rechenzentren sollen 2020 abgeschaltet werden.



Wenn sich Unternehmen für diesen Colocated-Hybrid-Cloud-Ansatz entscheiden, werden sie agiler und optimieren ihre Netzwerkstrategien, da Interconnections zwischen Netzwerken, Cloud-Plattformen, Kunden- und Partner-Communities alle an einem Ort eingerichtet werden können. Kombiniert mit den Cloud-Plattformen ihrer Wahl ist das Colocation-Modell für ihre IT-Infrastruktur der Schlüssel für bessere Workload Performance, die bestmögliche Connectivity und eine durch SLAs abgesicherte Verfügbarkeit des Netzwerks von 99,999 Prozent.

Interxion Cloud Connect ist in allen 13 Ländern verfügbar, in denen Interxion tätig ist. Die Plattform bietet Unternehmen Any-to-Any Connectivity, also die Möglichkeit, sich von jedem beliebigen Standort aus mit jedem beliebigen anderen Standort und den dort ansässigen Kunden und Cloud Service Providern zu verbinden. Unternehmen, Carrier und IT-Service Provider, die sich mit einem ganz bestimmten Cloud Service Provider oder einer ganz bestimmten Region verbinden müssen, nutzen dieses europaweite Netzwerk immer häufiger entweder über eine einzige Verbindung oder über zwei redundante Verbindungen. Ein Kunde hat auf der Plattform fast 50 Verbindungen zu Cloud-Angeboten im Einsatz.

Cloud Performance - fünf Jahre der Optimierung

Um die wachsenden Anforderungen an die Cloud zu erfüllen, müssen Unternehmen sich auf die Netzwerkperformance sowie die kluge Verteilung von Workloads konzentrieren. Zwar fließen immer grössere Teile der IT-Budgets von Konzernen in Cloud Services, aber ob diese Projekte wirklich erfolgreich sind, hängt zu grossen Teilen von dem Netzwerk ab, über das diese Services laufen. Das zeigen die Erfahrungen der vergangenen fünf Jahre beim Umsetzen von Cloud-Strategien in Unternehmen.

Es hat sich als unzureichend erwiesen, beim Zugang zu cloudbasierten Anwendungen auf das öffentliche Internet zu setzen. Die Performance des öffentlichen Internets reicht nicht aus, um als Basis für eine erfolgreiche Cloud-Transformation zu dienen. Besser agieren Unternehmen, die Interxion als Zentrum für eine Hybrid-Cloud-Strategie nutzen, denn sie können sichere Verbindungen in die Cloud herstellen und gleichzeitig ihre eigene, private Cloud-Infrastruktur und Network Edge Services in den hochsicheren Rechenzentren von Interxion betreiben. Damit verbunden sind weitere Vorteile, wie eine schnelle Bereitstellung, 99,999 Prozent Verfügbarkeit sowie ein zu 100 Prozent garantierter Durchsatz.

In den kommenden fünf Jahren stehen ohne Zweifel mindestens ebenso viele Änderungen an, wie wir sie in den vergangenen fünf Jahren erlebt haben. Wir freuen uns darauf, weiterhin eine entscheidende Rolle im Zentrum der Transformation der Unternehmens-IT spielen zu dürfen.

Um mehr darüber zu erfahren, wie Interxion Ihnen dabei helfen kann, Ihre Cloud-Infrastruktur für die maximale Performance auszurichten, lesen Sie unser Datenblatt [Colocated Hybrid Cloud](#).



Über Interxion

Interxion (NYSE: INXN) ist ein führender europäischer Anbieter von Cloud- und Carrier-neutralen Rechenzentrumsdienstleistungen für Colocation und betreibt insgesamt 50 Rechenzentren in 13 europäischen Städten verteilt auf 11 Länder. Interxions energieeffiziente Rechenzentren sind in einem standardisierten Design errichtet und bieten ein Höchstmass an Sicherheit und Verfügbarkeit zum Betrieb geschäftskritischer Anwendungen. Durch den Zugang zu mehr als 700 Connectivity-Anbietern, 21 europäischen Internetaustauschknoten und den führenden Cloud- und Media-Plattformen an seinen Standorten hat Interxion Hubs für Cloud, Content, Finance und Connectivity geschaffen, welche die Etablierung von Ökosystemen für Branchen-Cluster nachhaltig fördern. Weitere Informationen über Interxion finden Sie unter www.interxion.ch

Data Centre Services in ganz Europa



www.interxion.ch
customer.services@interxion.com



Interxion (Schweiz) AG
Tel.: +41 (0) 44 562 3000
Email: info.ch@interxion.com

European Customer Service Centre (ECSC)
Tel. Anrufe aus Europa (kostenfrei): + 800 00 999 222
Tel. Anrufe aus den USA (kostenfrei): 185 55 999 222
E-Mail: customer.services@interxion.com

Gründungsmitglied: Uptime Institute EMEA Chapter. **Gründungsmitglied:** European Data Centre Association. **Mitglied:** European Internet Exchange Association. **Mitglied:** EuroCloud. **Mitglied:** The Green Grid, aktiv im Technical Committee und im Advisory Council. **Mitglied:** Gemeinsamer Forschungsausschuss der Europäischen Kommission zur Nachhaltigkeit. **Mitglied:** Bundesverband Informationswirtschaft, Telekommunikation und Medien e.V. (BITKOM). Alle europäischen Geschäftsbereiche von Interxion entsprechen dem international anerkannten ISO/IEC-27001- (537141) Zertifikat für Informations-Sicherheits-Management-Systeme und dem ISO 22301 (BCMS 560099) -Zertifikat für Business-Continuity-Management. © Copyright 2018 Interxion. BP-ENT-HQ-REBUILD-HQ-de-10/18