10 Überlegungen, die bei Cloud-Beschaffungen eine Rolle spielen

März 2017

Hinweise

Dieses Dokument wird nur zu Informationszwecken zur Verfügung gestellt. Es stellt das aktuelle Produktangebot und die Verfahren von AWS zum Ausstellungsdatum dieses Dokuments dar. Änderungen vorbehalten. Kunden sind für ihre eigene unabhängige Einschätzung der Informationen in diesem Dokument und jedwede Nutzung der AWS-Services verantwortlich. Jeder Service wird „wie besehen“ ohne Gewähr und ohne Garantie jeglicher Art, weder ausdrücklich noch impliziert, bereitgestellt. Dieses Dokument gibt keine Garantien, Gewährleistungen, vertraglichen Verpflichtungen, Bedingungen oder Zusicherungen von AWS, seinen Partnern, Zulieferern oder Lizenzgebern. Die Verantwortung und Haftung von AWS gegenüber seinen Kunden werden durch AWS-Vereinbarungen geregelt. Dieses Dokument ist weder ganz noch teilweise Teil der Vereinbarungen von AWS mit seinen Kunden und ändert diese Vereinbarungen auch nicht.

Inhalt

Zweck

Amazon Web Services (AWS) stellt skalierbare und kosteneffiziente Cloud-Services bereit. Kunden im öffentlichen Sektor können mit ihrer Hilfe geltende Auflagen erfüllen, Kosten reduzieren, die Effizienz steigern und Innovationen beschleunigen.

Die Beschaffung einer Infrastructure-as-a-Service (IaaS)-Cloud unterscheidet sich vom Kauf einer herkömmlichen Technologie. Herkömmliche Ansätze für Beschaffung und Auftragsvergabe im öffentlichen Sektor, die für den Kauf von Produkten, beispielsweise Hardware und zugehörige Software, konzipiert wurden, sind möglicherweise nicht für Cloud-Services (wie IaaS) geeignet. Eine fehlende Modernisierung von Ansätzen für Beschaffung und Auftragsvergabe kann den Wettbewerber-Pool reduzieren und die Fähigkeit von Kunden einschränken, Cloud-Technologien einzuführen und zu nutzen.

Zehn Überlegungen, die bei Beschaffungen eine Rolle spielen

Die Cloud-Beschaffung ist eine Gelegenheit, bestehende Beschaffungsstrategien neu zu bewerten, um ein flexibles Akquisitionsverfahren zu entwickeln, mit dem Organisationen im öffentlichen Sektor die Vorteile der Cloud voll ausschöpfen können. Die folgenden Überlegungen zu Beschaffungen sind zentrale Komponenten, die als Grundlagen einer umfassenderen Strategie für die Cloud-Beschaffung im öffentlichen Sektor dienen können.

1. Informieren Sie sich über die Unterschiede zwischen Cloud Computing und anderen Technologien

Anbieter hyperskalierter Cloud-Services (Cloud Service Providers, CSPs) bieten für alle Kunden kommerzielle Cloud-Services im großen Maßstab und auf die gleiche Weise an. Kunden profitieren von standardisierten, kommerziellen Services, die auf Anforderung verfügbar sind. Sie zahlen nur für das, was sie tatsächlich nutzen.

Das standardisierte kommerzielle Bereitstellungsmodell des Cloud Computings unterscheidet sich grundlegend vom herkömmlichen Modell für Käufe lokaler IT-Technologien, die hochgradig anpassbar und möglicherweise nicht kommerziell verfügbar sind. Wenn Sie diesen Unterschied verstehen, können Sie ein effizienteres Beschaffungsmodell entwickeln. IaaS-Cloud-Services beseitigen die Notwendigkeit für Kunden, eigene physische Komponenten kaufen zu müssen. Zurzeit findet ein Wechsel vom Kauf physischer Komponenten hin zu Infrastruktur-Services statt, die ähnlich wie Versorgungsleistungen auf Anforderung verfügbar sind. Einrichtungen im öffentlichen Sektor sollten verstehen, wie diese standardisierten, ähnlich wie Versorgungsleistungen funktionierenden Services veranschlagt, beschafft und verwendet werden. Auf dieser Grundlage sollten sie eine Strategie für die Cloud-Beschaffung entwickeln, die sich bewusst von der Beschaffung herkömmlicher IT-Technologien unterscheidet und darauf ausgerichtet ist, die Vorteile des Cloud-Bereitstellungsmodells zu nutzen.

2. Planen Sie rechtzeitig, um die gesamten Vorteile der Cloud nutzen zu können

Ein wichtiges Element einer erfolgreichen Cloud-Strategie ist die frühzeitige Einbeziehung aller wesentlichen beteiligten Stellen (Abteilungen für Beschaffung, Rechtsfragen, Budget/Finanzen, Sicherheit und IT sowie die geschäftliche Führungsebene). Diese Einbeziehung stellt sicher, dass die beteiligten Stellen verstehen können, wie sich die Einführung der Cloud auf die vorhandenen Verfahren auswirken wird. Sie bietet eine Möglichkeit, die Erwartungen hinsichtlich der Veranschlagung für IT, Risikomanagement, Sicherheitsmaßnahmen und Compliance neu zu definieren. Die Förderung einer Kultur der Innovation und die Schulung von Mitarbeitern hinsichtlich der Vorteile der Cloud und der Verwendung der Cloud-Technologie helfen Mitarbeitern mit institutionellem Wissen, die Cloud zu verstehen. Darüber hinaus wird so auch eine schnellere Akzeptanz der Cloud erreicht.

3. Vermeiden Sie zu strenge Vorgaben

Personen im öffentlichen Sektor, die an der Cloud-Beschaffung beteiligt sind, sollten die richtigen Fragen stellen, um die besten Lösungen zu erhalten. Im Cloud-Modell werden physische Komponenten nicht gekauft, sodass herkömmliche Beschaffungsanforderungen für Rechenzentren nicht länger relevant sind. Die fortgesetzte Wiederholung von Fragen, die im

Zusammenhang mit Rechenzentren relevant sind, werden unweigerlich zu Rechenzentrumslösungen führen. In diesem Fall können CSPs möglicherweise keine Angebote abgeben oder, was noch schlimmer ist, es werden schlecht gestaltete Verträge abgeschlossen, die Kunden aus dem öffentlichen Sektor hindern, die Möglichkeiten und Vorteile der Cloud zu nutzen.

Erfolgreiche Strategien für die Cloud-Beschaffung haben ihren Schwerpunkt auf leistungsbasierten Anforderungen auf Anwendungsebene und betrachten Arbeitslasten und Ergebnisse als Priorität, anstatt die zugrunde liegenden Methoden, Infrastrukturmodelle oder Hardwarekomponenten vorzugeben, die zur Einhaltung der Leistungsanforderungen verwendet werden. Kunden können die vorhandenen bewährten Methoden eines CSP für den Rechenzentrumsbetrieb nutzen, da der CSP über die nötigen detaillierten Kenntnisse und Erfahrungen hinsichtlich sicherer, hyperskalierter IaaS-Cloud-Services verfügt. Es ist nicht notwendig, angepasste Spezifikationen für Geräte, Betrieb und Verfahren vorzugeben (z. B. Racks, Servertypen und Entfernungen zwischen Rechenzentren). Durch die Nutzung kommerzieller Branchenstandards und bewährter Methoden für die Cloud (einschließlich branchenweit anerkannter Akkreditierungen und Zertifizierungen) vermeiden Kunden, die von ihnen genutzten Services unnötig einzuschränken, und stellen den Zugriff auf innovative und kosteneffektive Cloud-Lösungen sicher.

4. Trennen Sie Cloud-Infrastruktur (nicht verwaltete Services) und verwaltete Services

Es gibt einen Unterschied zwischen der Beschaffung einer Cloud-Infrastruktur (IaaS) und der Beschaffung von Arbeitskraft, um eine Cloud-Infrastruktur oder verwaltete Services, beispielsweise eine Software as a Service (SaaS)-Cloud, zu nutzen. Erfolgreiche Cloud-Beschaffungen machen einen Unterschied zwischen Cloud-Infrastruktur und „praktischen“ Services, Arbeitskraft und anderen verwalteten Services. Cloud-Infrastruktur auf der einen Seite und Services wie Arbeitskräfte für Planung, Entwicklung, Ausführung und Wartung von Cloud-Migrationen und -Arbeitslasten auf der anderen Seite können von CSP Partnern (oder anderen Drittanbietern) in Form einer umfassenden Lösung bereitgestellt werden. Eine Cloud-Infrastruktur sollte jedoch als eigener „Service“ mit andersartigen Rollen und Verantwortlichkeiten, Service Level Agreements (SLAs) und Bedingungen betrachtet werden.

5. Integrieren Sie ein Preismodell ähnlich Preismodellen für Versorgungsleistungen

Um die Vorteile des Cloud Computings zu nutzen, müssen Sie über den allgemein akzeptierten Ansatz hinausdenken, bei dem Aufträge zu festen Preisen vergeben werden. Um einen Vertrag für die Cloud abzuschließen, der eine fluktuierende Nachfrage berücksichtigt, muss dieser eine nutzungsabhängige Bezahlung der Services vorsehen.

Die CSP-Preise sollten:

- Auf einem Pay-as-you-Go-Modell ähnlich Versorgungsleistungen basieren, bei dem Kunden am Ende des Monats lediglich die tatsächliche Nutzung bezahlen.
- Abhängig von den Marktpreisen fluktuieren dürfen, damit Kunden die Vorteile der dynamischen und wettbewerbsorientierten Gestaltung der Cloud-Preise nutzen können.

Es CSPs zu ermöglichen, Pay-as-you-Go- oder flexible nutzungsbasierte Preise anzubieten, erlaubt Kunden die Kosten der Nutzung einzuschätzen, statt Vermutungen zu zukünftigen Anforderungen anzustellen und die Beschaffung zu umfangreich zu dimensionieren. CSPs sollten öffentlich verfügbare, aktuelle Preise und Tools bereitstellen, mit denen Kunden ihre Preise bewerten können, vergleichbar dem AWS Einfacher Monatsrechner: http://aws.amazon.com/calculator. Zusätzlich sollten CSPs Kunden die nötigen Tools bereitstellen, mit denen sie detaillierte und anpassbare Abrechnungsberichte generieren können, um geschäftliche und Compliance-Anforderungen zu erfüllen.

Darüber hinaus sollten CSPs auch Funktionen bereitstellen, die Kunden die Analyse der Cloud-Nutzung und -Ausgaben ermöglichen, damit Kunden Warnungen integrieren können, mit denen sie benachrichtigt werden, wenn sie sich den Nutzungsgrenzen und projizierten/veranschlagten Kosten nähern. Anhand solcher Warnungen können Organisationen ermitteln, ob die Nutzung reduziert werden muss, um übermäßige Ausgaben zu vermeiden, oder ob zusätzliche Mittel bereitgestellt werden müssen, um Kosten abzudecken, die das projizierte Budget überschreiten.

6. Nutzen Sie Drittanbieter-Akkreditierungen für Sicherheit, Datenschutz und Überwachung

Die Nutzung bewährter Methoden der Branche hinsichtlich Sicherheit, Datenschutz und Überwachung stellt sicher, dass effektive physische und logische Sicherheitskontrollen vorhanden sind. Dies verhindert übermäßig aufwändige Prozesse und duplizierte Genehmigungs-Workflows, die häufig nicht durch echte Risiken und Compliance-Anforderungen begründet sind. Es gibt zahlreiche Sicherheits-Frameworks, bewährte Methoden, Audit-Standards und standardisierte Kontrollen, die in Cloud-Verträgen aufgeführt werden können, wie:

- Federal Risk and Authorization Management Program (FedRAMP)
- Service Organization Controls (SOC) 1/American Institute of Certified Public Accountants (AICPA): AT 801 (zuvor Statement on Standards for Attestation Engagements [SSAE] No. 16)/International Standard on Assurance Engagements (ISAE) 3402 (zuvor Statement on Auditing Standards [SAS] No. 70), SOC 2, SOC 3
- Payment Card Industry Data Security Standard (PCI DSS)
- International Organization for Standardization (ISO) 27001, ISO 27017, ISO 27108, ISO 9001
- Department of Defense (DoD) Security Requirements Guide (SRG)
- Federal Information Security Management Act (FISMA)
- International Traffic in Arms Regulations (ITAR)
- Family Educational Rights and Privacy Act (FERPA)
- Information Security Registered Assessors Program (IRAP) (Australien)
- IT-Grundschutz (Deutschland)
- Federal Information Processing Standard (FIPS) 140–2

7. Seien Sie sich bewusst, dass Sicherheit eine übergreifende Verantwortung ist

Da Cloud Computing-Kunden Systeme auf einer Cloud-Infrastruktur aufbauen, werden die Sicherheits- und Compliance-Verantwortlichkeiten zwischen

Service-Anbietern und Cloud-Kunden aufgeteilt. In einem IaaS-Modell kontrollieren Kunden sowohl die Architektur als auch den Schutz ihrer Anwendungen und Daten auf der Infrastruktur. Die CSPs sind für die Bereitstellung von Services über eine hoch sichere und kontrollierte Infrastruktur und für die Bereitstellung einer breiten Palette zusätzlicher Sicherheitsfunktionen verantwortlich. Die jeweiligen Verantwortlichkeiten des CSP und des Kunden sind vom verwendeten Cloud-Bereitstellungsmodell abhängig, IaaS, SaaS oder Platform-as-a-Service (PaaS). Kunden sollten sich ihrer Verantwortlichkeiten im Bereich Sicherheit in jedem Cloud-Modell klar bewusst sein.

8. Entwerfen und implementieren Sie eine Governance für Cloud-Daten

Organisationen sollen die vollständige Kontrolle und Eigentümerschaft über ihre Daten behalten und die Möglichkeit haben, die geografischen Standorte zu wählen, an denen ihre Daten gespeichert werden sollen. Der Zugriff auf die Infrastruktur und Daten der Kunden sollte dabei durch Identitäts- und Zugriffskontrollen des CSP geschützt werden. Kunden sollten sich ihrer Verantwortlichkeiten im Zusammenhang mit Speicherung, Verwaltung, Schutz und Verschlüsselung ihrer Daten klar bewusst sein. Ein großer Vorteil besteht darin, dass Cloud Computing im Vergleich zu herkömmlichen IT-Infrastrukturen haben Kunden die Flexibilität, um zu verhindern, dass herkömmliche Anbieter. Cloud-Kunden keine physischen Komponenten und CSPs bieten die Möglichkeit, den IT-Stack nach Bedarf, mit größerer Portabilität und Interoperabilität als das alte IT-Paradigma. Einrichtungen im öffentlichen Sektor sollten von CSPs Folgendes verlangen: 1) Zugriff auf Tools und Services für Cloud-Portabilität, mit denen Kunden nach Bedarf Daten in ihre und aus ihrer Cloud-Infrastruktur verschieben können, und 2) Verzicht auf Mindestverpflichtungen oder langfristige Verträge.

9. Spezifizieren Sie die Bedingungen für kommerzielle Elemente

Cloud Computing sollte als kommerzielles Element gekauft werden. Organisationen sollten sich überlegen, welche Bedingungen in diesem Kontext angemessen (und nicht angemessen) sind. Ein kommerzielles Element ist ein Element, das verkauft, gemietet, lizenziert oder auf andere Weise öffentlich zum Verkauf angeboten wird

und im Allgemeinen allen Benutzern/Kunden im kommerziellen und öffentlichen Sektor die gleiche Funktionalität bereitstellt. Die Bedingungen des IaaSCSP spiegeln die Funktionsweise eines Cloud-Service-Modells wider (d. h., kein Kauf physischer Komponenten und CSPs betreiben ihr Geschäft in großem Maßstab, um standardisierte kommerzielle Services bereitzustellen). Es ist von kritischer Bedeutung, dass die Bedingungen eines CSP integriert und im größtmöglichen Umfang genutzt werden.

10. Definieren Sie Bewertungskriterien für die Cloud

Die Cloud-Bewertungskriterien sollten sich auf Anforderungen hinsichtlich der Systemleistung konzentrieren. Wählen Sie einen geeigneten CSP aus einem bekannten Ressourcenpool aus, um die Vorteile der Elastizität, Kosteneffizienz und schnellen Skalierbarkeit der Cloud zu nutzen. Dieser Ansatz stellt sicher, dass Sie die besten Cloud-Services erhalten, um Ihre Anforderungen zu erfüllen, das beste Preis-Leistungs-Verhältnis für diese Services erzielen und die Fähigkeit erhalten, marktgetriebene Innovationen zu nutzen. Die Definitionen des National Institute of Standards and Technology (NIST) für Cloud-Vorteile sind ein ausgezeichneter Ausgangspunkt für die Festlegung von Cloud-Bewertungskriterien: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf.

Fazit

Tausende Kunden aus dem öffentlichen Sektor nutzen AWS, um schnell Services über einen effizienten, Cloud-basierten Beschaffungsvorgang zu starten. Wenn Sie diese zehn Schritte berücksichtigen, können Organisationen Services bereitstellen, die Bürgern und Besuchern von Bildungseinrichtungen noch größere Vorteile bieten und noch stärker missionsorientiert sind.