Cloud Computing – Chance oder Risiko?

Lösungen für eine zuverlässige Gewährleistung der Geschäftskontinuität

Kroll Ontrack

Einleitung

Fragen Sie einen durchschnittlichen Computernutzer nach der Cloud, und er wird Sie verständnislos ansehen oder anfangen, über das Wetter zu reden. Zwar haben es Marketingteams geschafft, dass Internetnutzer von der Existenz des Cloud Computing wissen, doch können nur wenige Anwender erklären, was die Cloud genau ist oder wofür sie genutzt werden kann. Fast alle Internetnutzer haben bereits mit Cloud-Technologien zu tun gehabt – oft ohne es zu wissen. Haben Sie schon einmal eine Website für das Hosten von Fotos genutzt? Dann haben Sie einen Speicher in der Cloud verwendet. Nutzen Sie interaktive soziale Medien oder Office-Anwendungen über einen Webbrowser? Dann verwenden Sie Cloud-Software.

Die Cloud-Computing-Branche wird zunehmend erwachsen und kann Unternehmen, die Investitionen in neue Technologien und Kosten gering halten möchten, effiziente Lösungen anbieten. Als Grundlage für alle Cloud-Computing-Leistungen dient die Virtualisierung – also Software, die für die Emulation von Computerhardware sorgt.

Mit dem Cloud Computing lassen sich drei verschiedene Services bereitstellen: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) und Infrastructure-as-a-Service (IaaS). Infrastructure-as-a-Service (IaaS) ist der etablierteste Cloud Service, da er Unternehmen die Möglichkeit bietet, ausschließlich benötigte Ressourcen für ihre Computersysteme zu nutzen. Mit IaaS können Kunden zum Beispiel auf externe virtualisierte Computer zugreifen, ohne die Kosten für Hardware und Anlagen tragen zu müssen.

SaaS ist der am einfachsten zugängliche Cloud Service, da er alle Anwendungsfunktionen über eine webbasierte Schnittstelle bereitstellt. Die Zahl der Anwendungen, die für Webbrowser entwickelt wurden, ist immens. So gibt es umfassende Anwendungen für mehr Produktivität im Büro, auf die bequem über einen Webbrowser und eine Internetverbindung zugegriffen werden kann.

PaaS eignet sich für die rasche Entwicklung von Anwendungen und basiert auf den beiden oben beschriebenen Cloud Services. Stellen Sie sich PaaS als Bindeglied zwischen SaaS und IaaS vor. Dieser Cloud Service wird sich möglicherweise früher als gedacht durchsetzen[1], da er mehr SaaS-Funktionen ermöglicht.

Gartner Research berichtet, dass Cloud-basierte Infrastructure-as-a-Service (IaaS)-Lösungen auf dem Markt immer beliebter werden. So schätzt Gartner den Markt für Cloud-Lösungen im Jahr 2011 auf 3,7 Milliarden USD und im Jahr 2014 bereits auf 10,5 Milliarden USD – ein beeindruckendes Wachstum in den kommenden drei Jahren.[2]

Die Kundenakzeptanz von Cloud Services bei Anwendungen mobiler Telefone zeigt, dass die Technologie ein Modell darstellt, in das immer mehr Unternehmen investieren. Laut comScore, Inc., einem Analyseunternehmen für digitale Geschäfte in den USA, besitzen 69,5 Millionen US-Amerikaner ein Smartphone. Ende 2010 griff über die Hälfte dieser Menschen mit ihren mobilen Geräten auf Bank- und Kreditkartenkonten oder Aktiendepots zu.[3]

SLAs und vertragliche Verpflichtungen bieten Cloud-Nutzern bei Betriebsstörungen keineswegs immer umfassende Sicherheit. So ist es riskant, in den Vertrag mit dem Cloud-Anbieter keine Klausel zur Datenrettung aufzunehmen.

[1] http://www.businesswire.com/news/home/20110314006630/en/Gartner-2011-Year-Platform-Service
[2] http://www.businesswire.com/news/home/20110407005575/en/Gartner-Maps-Rapidly-Evolving-Market-Cloud-Infrastructure
[3] http://www.comscore.com/Press_Events/Press_Releases/2011/4/comScore_Reports_February_2011_U.S._Mobile_Subscriber_Market_Share; http://www.creativedepartment.com/news/mobile/use-mobile-banking-apps-rose-sharply-fourth-quarter-183600

Die Cloud – hält auch Stürmen stand

Jason Baker, Chief Technology Officer bei Visi, Inc., einem Anbieter von IaaS- und Hosting-Diensten für Rechenzentren, merkt an, dass die Cloud-Technologie dank inhärenter Redundanz und Verteilungsfunktionen „auch Ausfälle übersteht". Baker erläutert, dass „Anwendungen bislang ... über den Webserver, Anwendungsserver und Datenbankserver bereitgestellt worden sind. Mit dem Cloud Computing werden diese Komponenten überflüssig, und Unternehmen können sich auf die web-orientierte bzw. Anwendungsschicht konzentrieren." Die physische Schicht – die Hardware – wird mithilfe von Virtualisierungstechnologie bereitgestellt.

Mit der zunehmenden Cloud-Nachfrage werden Cloud-Dienste und -Anwendungen zu standardisierten Produkten. Für Cloud-Kunden werden jedoch die Leistungsfähigkeit und der Ruf des Anbieters eine wichtige Rolle spielen. „Anbieter von Cloud Services müssen in den nächsten Jahren ganz auf den Aufbau von Vertrauen setzen", erklärt Harold Moss, Chief Technology Officer für die Cloud-Sicherheitsstrategie von IBM. „Die Zahl der Anbieter wird zunächst wachsen, um dann wieder abzunehmen. Überleben werden nur jene Anbieter, die bereits jetzt komplette Lösungen bereitstellen können." Moss berichtet, dass manche Service Provider eigene Dienste an einen anderen Service Provider auslagern, um preislich wettbewerbsfähig zu bleiben. So entsteht ein „zusammengefasstes Service Level Agreement", meint Moss. Der Wert des Gesamtservice sinkt, da der Anbieter selbst die Cloud nutzt, um Rechenressourcen zur Verfügung zu stellen. Die Einhaltung von SLAs hängt dabei von den Leistungen anderer Anbieter ab.

Mit der zunehmenden Nachfrage werden Cloud-Dienste und -Anwendungen zu standardisierten Produkten. Für Cloud-Kunden werden jedoch die Leistungsfähigkeit und der Ruf des Anbieters eine wichtige Rolle spielen.

Regen in der Cloud

Kunden erwarten von Cloud-Anbietern die vollständige Einhaltung von Compliance-, Sicherheits- und Governance-Richtlinien. Leider zeigen Zertifikate und Prüfberichte nicht, wie ein Anbieter von Cloud Services mit Störungen umgehen kann.[4]

Regen in der Cloud kann für Endbenutzer fatale Folgen haben. Dies macht das Beispiel eines kanadischen IT-Service Providers deutlich. Der Anbieter nutzte eine NetApp® Filer-Appliance mit 40 TB, die virtuelle LUNs bzw. in der NetApp-Volume-Schicht iSCSI-Dateien umfasste. In diesen iSCSI-Dateien befanden sich VMware® ESX-Volumes. In den ESX-Volumes waren die Dateien der virtuellen Laufwerke enthalten, die für Server des IT-Service Providers und für virtuelle IaaS-Maschinen einiger Kunden genutzt wurden. Der Sturm, der auf das Unternehmen zukam, war interner – und nicht externer – Art.

Ein aufgebrachter Mitarbeiter verwendete auf der Ebene der Speichereinheiten den Befehl „Volumes löschen". Die betroffene Speichereinheit wies die Block-Snapshot-Technologie von NetApp auf. Das allein hätte genügt, um die Daten zu retten, wenn der Mitarbeiter nicht noch einen Schritt weiter gegangen wäre. Er wusste leider, wie die Snapshot-Funktion der Filer-Appliance funktioniert. Kurz vor dem Löschen der NetApp-Volumes setzte er die Systemuhr der Filer-Appliance eine Stunde zurück, so dass bei der Snapshot-Replikation die Metadaten der leeren Volumes kopiert wurden. Anschließend setzte der Mitarbeiter die Systemuhr der Filer-Appliance wieder eine Stunde vor, bevor er das Rechenzentrum des Unternehmens verließ. Die NetApp Filer-Appliance erstellte weiterhin wie geplant Snapshots der

[4] Im Sinne dieses Artikels sind Betriebsstörungen Vorfälle, die die Erledigung der täglichen Aufgaben behindern. Hierzu gehören Stromausfälle, gestörte Telefonleitungen usw. Als Datenverluste gelten Daten, die beschädigt sind oder sich nicht mehr aufrufen lassen. Somit gehören auch Datenverluste zur Kategorie Betriebsstörung.

Volumes. Dabei füllte sich die gesamte Snapshot-Liste jedoch mit leeren Blöcken. Als andere Administratoren die Katastrophe erkannten, gab es schon keinen gültigen Wiederherstellungspunkt mehr.

Dieser Vorfall entwickelte sich zu einer richtiggehenden Katastrophe, da nicht nur einige der IaaS-Systeme von Kunden nicht mehr funktionierten, sondern der Service Provider nicht einmal mehr über seine eigenen Betriebsdaten verfügte. Zudem standen keine Sicherungskopien der ursprünglichen Daten zur Verfügung.

Der Service Provider hatte seinen Kunden für Rechenzentrums- und wichtige Tier-1-Internetverbindungen eine Verfügbarkeit von 99,99 Prozent versprochen. Während der Störung konnten die Systemverfügbarkeit sowie die blitzschnellen Verbindungen aufrechterhalten und somit die vereinbarten SLAs eingehalten werden. Wie diese Cloud Service-Kunden jedoch bald feststellen konnten, sind Systemverfügbarkeit und Konnektivität etwas anderes als die Verfügbarkeit von Daten.

Das kanadische IT-Unternehmen musste den Datenrettungsservice eines externen Anbieters in Anspruch nehmen, um die eigenen Daten zu retten und die virtuellen IaaS-Systeme seiner Kunden wiederherzustellen. Während der Störung kümmerte sich das Unternehmen so gut es ging um seine Kunden. Manchen Kunden wurde jedoch mitgeteilt, dass sie zur Rettung ihrer Daten den gleichen Anbieter für Datenrettungsservices beauftragen und bezahlen müssten, da sie keine zusätzliche Replikationslösung gekauft hatten und somit über keinerlei Sicherungskopien ihrer Daten verfügten. Für Kunden, die davon ausgegangen waren, dass ihre SLAs auch für die Verfügbarkeit von Daten gelten würden, war dies ein Schock.

Dieses Beispiel zeigt, dass SLAs und vertragliche Verpflichtungen Cloud-Nutzern bei Störungen nicht immer ausreichend Schutz bieten. So ist es riskant, in den Vertrag mit dem Cloud-Anbieter keine Klausel zur Datenrettung aufzunehmen. Ein zu großes Vertrauen in die Selbstheilungskräfte oder 100-prozentige Redundanz von Speicherausrüstung ist naiv und kann Unternehmen teuer zu stehen kommen. Eine synchrone Datenreplikation ist kostspielig und schützt nicht vor menschlichen Fehlern oder der mutwilligen Zerstörung von Daten.

Systemverfügbarkeit und Konnektivität sind etwas anderes als die Verfügbarkeit von Daten.

Ein Regenschirm für die Cloud

Anfang 2011 tobten mehrere Stürme, die bei bekannten Anbietern von Cloud Services zu Ausfällen führten.[5] Die Stürme traten unabhängig voneinander auf. Die Störungen führten jedoch zu ausgefallenen oder deaktivierten Websites und unzufriedenen Internetanwendern. Benutzer der Services sahen sich mit der folgenden Meldung konfrontiert: „Der Dienst ist vorübergehend nicht verfügbar." Da Cloud Services noch relativ neu sind, lernen viele Kunden die Einschränkungen ihrer SLA-Verträge erst dann kennen, wenn es zu einer Betriebsstörung kommt. Welche Kompensation oder Gutschrift bieten SLAs für Ausfälle? Wie sorgt der Cloud-Anbieter für die Wiederherstellung der ausgefallenen Services? Manche Cloud-Kunden bemerken zu spät, dass ihre Cloud-Verträge strengere Bedingungen zur Ausfallsicherheit beinhalten sollten.[6]

[5] http://www.computerworld.com/s/article/9216064/Amazon_gets_black_eye_from_cloud_outage, http://www.pcmag.com/article2/0,2817,2384214,00.asp, http://www.computerworld.com/s/article/9211798/Update_Google_Gmail_outage_leaves_thousands_of_users_without_e_mail_, http://news.cnet.com/8301-31001_3-20046091-261.html

[6] Im Sinne dieses Artikels sind Betriebsstörungen Vorfälle, die die Erledigung der täglichen Aufgaben behindern. Hierzu gehören Stromausfälle, gestörte Telefonleitungen usw. Als Datenverluste gelten Daten, die beschädigt sind oder sich nicht mehr aufrufen lassen. Somit gehören auch Datenverluste zur Kategorie Betriebsstörung.

Cloud-Anbieter ohne interne oder externe Datenrettungs-experten, die bei der Behebung von Störungen helfen, können ihren Kunden nicht genügend Sicherheit bieten. Bei einem Ausfall arbeiten alle verfügbaren IT-Mitarbeiter fieberhaft an der Wiederherstellung der Services, Ersetzung von Ausrüstung, Wiederherstellung von Sicherungskopien, Durchführung einer Ursachenanalyse und Erledigung anderer investigativer Aufgaben, damit das Management verstehen kann, was den Ausfall ausgelös t hat. Cloud-Anbieter, die versuchen, alle Aufgaben intern zu lösen, erkennen schnell, dass ihre sowieso schon überlasteten IT-Teams bei Ausfällen endgültig überfordert sind.

Ursachen für Cloud-Ausfälle können Netzwerkstörungen, der Austausch von Hardware, externe Angriffe auf das Netzwerk oder Softwarefehler sein. Trotz der Fortschritte bei den Datenspeicherungstechnologien kommt es in der Cloud immer wieder zu Datenverlusten und Ausfällen. Anbieter von Datenrettungsservices stellen Daten von Speichergeräten wieder her, die ausgefallen sind, aufgrund menschlicher Fehler falsch verwaltet oder sabotiert wurden. Diese Anbieter sind jedoch nicht direkt in die gesamte Kette vom Speicher bis hin zum Kunden eingebunden. Speicherkunden geben Datenrettungsservices erst dann in Auftrag, wenn sie nicht mehr auf ihre Daten zugreifen können. Kein Unternehmen erwartet, jemals selbst von einem Speicherausfall oder Datenverlust betroffen zu sein. Tritt der Fall jedoch ein und hat ein Cloud-Anbieter (oder Kunde) seine Daten nicht unmittelbar vor dem Ausfall komplett gesichert, kann ein Anbieter von Datenrettungsservices für die Wiederherstellung der ursprünglichen Daten sorgen.

Die Virtualisierungstechnologie bei Cloud-Speichern erschwert eine Datenrettung. Das duale Dateisystem mit Host-Server- und virtuellen Computersystemen bringt eine doppelte Datenfragmentierung mit sich. Die Virtualisierungstechnologie dient als Grundlage für Cloud Services und ermöglicht ein skalierbares Wachstum. Die Speicherschicht kann zu einer Schwachstelle werden, da Virtualisierung hier eine zentrale Rolle spielt. Wenn Sie sich für die Nutzung von Cloud-Technologien entscheiden, besteht der beste Schutz vor Datenverlust darin, einen vertrauenswürdigen Full-Service-Anbieter von Datenrettungsservices als Partner zu wählen um im Ernstfall Ausfallzeiten minimieren.

Dabei geht es nicht nur darum, dass die Speicherung an externen Standorten, die synchrone bzw. asynchrone Replikation oder die Sicherung auf Band in die SLAs aufgenommen werden (diese Mindestanforderungen sollten alle Cloud-Anbieter erfüllen). Ein Cloud-Anbieter, der einen vertrauenswürdigen Anbieter von Datenrettungsservices als Partner hat, zeigt, dass die Datenverfügbarkeit mindestens genauso wichtig ist wie die Systemverfügbarkeit oder Gewährleistung des Zugriffs. Ein Cloud-Anbieter, der ein Datenrettungsunternehmen der Enterprise-Klasse als Partner hat, stärkt das Vertrauen seiner Kunden, indem er zum Schutz der Kundendaten einen umfassenden Plan für die Geschäftskontinuität entwickelt.

Dabei ist die Datenwiederherstellung beim Cloud Computing nur ein Aspekt. Auch die Datenvernichtung spielt eine wichtige Rolle. Bei der Suche nach einem geeigneten Cloud-Anbieter sollten Sie fragen, was mit Ihren Daten nach dem Ablauf des Cloud-Vertrags geschieht. Große Rechenzentren verfügen über OEM-Wartungsverträge zur Pflege der Speicherausrüstung sowie zur Vernichtung oder Entmagnetisierung ausgefallener Laufwerke, bevor diese entsorgt werden. Oftmals gehen Unternehmen davon aus, dass gelöschte Daten durch die wiederholten Schreibvorgänge späterer Speicherprozesse schnell genug überschrieben werden. Für eine vollständige Datenvernichtung müssen bestimmte Dateien jedoch einen richtigen Löschprozess durchlaufen.

Blauer Himmel in der Cloud

Um eine Cloud-Strategie erfolgreich umsetzen zu können, müssen Sie zunächst alle möglichen Hindernisse kennen. Manche dieser Hindernisse hängen mit dem Service Provider, andere mit der Projektstrategie und dem Budget zusammen. Sie müssen wissen, wo die Zuständigkeit des Service Providers endet und wo Ihre Verantwortung für die Datensicherheit beginnt, damit Ihre Infrastrukturen und Anwendungen Kunden jederzeit zur Verfügung stehen.

Technische Risiken – Überlegungen	Warum dies eine Rolle spielt
▪ Erfüllen die Sicherungssysteme und -verfahren Ihre internen Sicherungsstandards? ▪ Weist Ihr Cloud-Anbieter genügend technische Erfahrung auf, um Ihre Anforderungen zu erfüllen?	Verdächtige Hardware, fragmentierte Dateien und ungeeignete RAID-Level können die Datenverfügbarkeit beeinträchtigen.

Sicherheit in der Cloud – Überlegungen	Warum dies eine Rolle spielt
▪ Wie sicher sind Ihre Daten? Welche Maßnahmen hat der Anbieter ergriffen, um Probleme mit der Datensicherheit zu verhindern? Werden die Daten beispielsweise verschlüsselt? ▪ Wissen Sie, wer in Ihrem Unternehmen sowie beim Cloud-Anbieter auf Ihre Daten zugreifen kann? ▪ Wie sehen die Sicherheitsprüfungen für Mitarbeiter aus?	In Ihrem Unternehmen werden gängige Branchenvorgaben für Datensicherheit und Mitarbeiter angewendet. Wenn Sie wissen, wie Ihr Cloud-Partner mit seinen Mitarbeitern und Daten umgeht, können Sie einen Service wählen, der gut zu Ihren aktuellen Richtlinien passt.
▪ Dateneigentum – Sind Sie weiterhin der Eigentümer Ihrer Daten, wenn sich diese in der Cloud befinden? ▪ Sind Sie weiterhin der Eigentümer dieser Daten, wenn sie sich nicht mehr in Ihrem Besitz befinden? ▪ Werden Daten am Ende ihres Lebenszyklus von der gesamten Hardware gelöscht und entmagnetisiert? Wer zertifiziert die Löschung? Und wurden die Daten den Löschvorschriften Ihres Landes gemäß vernichtet?	Die jüngste Debatte über das Sicherheitskonzept eines beliebten sozialen Netzwerks zeigt, dass diese Fragen eine wichtige Rolle spielen.
Der Weg durch den Rechtsdschungel – Überlegungen	**Warum dies eine Rolle spielt**
▪ Bewahrt der Cloud-Anbieter Daten entsprechend der Aufbewahrungsrichtlinie Ihres Unternehmens für Dokumente auf? ▪ Kann Ihnen der Cloud-Anbieter zusichern, dass er alle Datenschutzbestimmungen einhält? ▪ Können Sie oder Ihr externer E-Discovery-Anbieter bei einem Gerichtsverfahren oder einer Untersuchung auf alle elektronisch gespeicherten Daten zugreifen und diese entweder extrahieren oder aufbewahren?	Bei Cyberkriminalität oder einer Verletzung des Datenschutzes sorgen Forensiker für die Sicherung des gesamten Speichers. Dabei können auch Ihre Daten erfasst werden. Wenn Daten in Cloud Services gemeinsam gespeichert werden, kann dies die Untersuchung erschweren und dazu führen, dass Sie und Ihre Kunden nicht mehr auf Speicher oder Anwendungen zugreifen können.
▪ Wo genau werden Ihre Daten gespeichert? ▪ Sind sie zusammen mit Daten anderer Unternehmen virtualisiert? ▪ An welchem geografischen Standort befindet sich das Rechenzentrum? ▪ Werden die Daten an einem Gerichtsstand gespeichert, an dem Dritte Zwangsmaßnahmen durchsetzen können? ▪ Wenn Sie den Vertrag mit dem Cloud-Anbieter beenden: Erhalten Sie Ihre Daten zurück? Wenn ja: In welchem Format? ▪ Wie können Sie sicher sein, dass alle Kopien Ihrer Daten nach der Beendigung des Vertrages zerstört werden?	Mandantenfähigkeit kann die Datenrettung sowie die Erstellung von Daten für Gerichtsverfahren oder Untersuchungen erschweren. Auch geografische Aspekte spielen eine Rolle, da Verzögerungen beim Datenabruf extrem teuer werden können. Für den Schutz und die Pflege der Daten Ihrer Kunden sind Sie verantwortlich – und nicht der Cloud-Anbieter. Wenn Sie die Probleme zuverlässig erkennen und beheben können, lassen sich juristische Debakel verhindern.

Kroll Ontrack

Mehr Informationen im Internet oder
über unsere kostenlose Hotline:

0800 10 12 13 14

www.krollontrack.de