Internationaler Hauptsitz: 5 Speen Street, Framingham, MA 01701 USA T.508.872.8200 F.508.935.4015 www.idc.com

WHITE PAPER

Die wichtigsten Kriterien bei der Auswahl eines dauerhaften Cloud-Backup-Providers

Gesponsert von: EMC Mozy

Liz Conner Laura DuBois

Mai 2013

INFORMATIONEN IN DIESEM WHITE PAPER

Cloud-Dienste bewirken in den heutigen IT-Organisationen eine Transformation. Sie verändern nicht nur den Aufbau, die Beschaffung und den Einsatz von IT, sondern auch wie und von wem die IT-Infrastruktur bereitgestellt wird. Datenspeicherung ist eine Branche, die große Störungen erfährt, während Verbraucher und Unternehmen ihre Speicherkapazität und Storage-Funktionen von öffentlichen Cloud-Service-Anbietern beziehen. An der Spitze des nachhaltigen und erfolgreichen Einsatzes eines öffentlichen Cloud-Speicherdienstes steht jedoch die ausführliche Wertfeststellung des Cloud-Providers. Dieses Dokument führt wichtige Kriterien auf, die Unternehmen bei der Bewertung eines dauerhaften Cloud-Service-Providers beachten sollten. Es zeigt auch auf, wie Mozy von EMC diese Anforderungen erfüllt und über 100.000 gewerblichen und Millionen von Einzelkunden zuverlässigen Mozy Cloud-Service zum Schutz und zur Wiederherstellung ihrer Daten anbietet.

SITUATIONSÜBERBLICK

Das Wachstum der Cloud und ihr Einfluss

Cloud-Services sowie Mobilität, Big Data/Analysen und soziale Medien gehören zu den vier führenden Transformationstechnologien, die neue Geschäfts- und IT-Strategien befähigen. Cloud-Services haben die Art und Weise revolutioniert, auf die gewisse Anwendungen entwickelt und große Teile der IT-Infrastruktur erworben, verwaltet und eingesetzt werden. Unternehmen können bestimmte Abschnitte ihrer Rechen-, Speicher- und/oder Datenbedürfnisse auslagern und durch geringere Kapitalauslagen und Betriebskosten ihre stark beanspruchten IT-Budgets entlasten. Dank der Cloud-Dienste können Organisationen nur das kaufen, was sie benötigen, und durch einfacher aktualisierbare Dienste profitieren, wodurch keine zusätzliche Hardware für zukünftiges Wachstum in Betracht gezogen werden muss. Die Pflege der IT-Infrastruktur darf auch nicht übersehen werden. Die fortlaufende Überwachung, Fehlerbehebung und Wartung der Infrastruktur und der Anwendungen kann von internen Betriebsteams auf den Cloud-Provider abgewälzt werden.

Der Datenspeicherungs-Aspekt geht voran, während Cloud Computing zunehmend größer wird. Seit 2006, als IDC seine Cloud-Forschung einleitete, wird die öffentliche Cloud hauptsächlich zur Datenspeicherung genutzt. Eine 2012 von IDC durchgeführte CloudTrack-Befragung von 493 IT-Fachleuten ergab, dass an zweiter Stelle nach der E-Mail am wahrscheinlichsten die Speicherung und Archivierung in die öffentliche Cloud

verlegt werden würde. Woran liegt das? Für Organisationen, die schnelle Bereitstellung erweiterter Speicher oder Desktop/Laptop-Backups innerhalb der Grenzen ihrer festgelegten Betriebsbudgets (OPEX) benötigen, bieten die öffentlichen Cloud-Speicherdienste relativ mühelosen, externen Speicher, der nach Bedarf und Wachstum bezahlt werden kann. Diese Einsatzart der öffentlichen sowie Hybrid-Clouds wird hauptsächlich zur Sicherung, Speicherung und Notfallwiederherstellung verwendet. Durch Sicherung in der Cloud können Organisationen, die Investitionsansätzen gegenüber negativ eingestellt sind, Geld sparen, weil sie keinen physikalischen Backup-Speicher einrichten oder verwalten müssen. Die Sicherung umfasst außerdem eine Notfallwiederherstellung, falls in dem Hauptdatenzentrum vor Ort etwas vorfällt.

Zwar bevorzugen die meisten IT-Organisationen weiterhin ihre vertrauten Speicher vor Ort (NAS, SAN usw.), doch IDC ist der Ansicht, dass Sicherung und Notfallwiederherstellung für kritische Bedürfnisse, wie beispielsweise Speicher für virtuelle Geräte, Datenbanken und Transaktionsanwendungen, nach wie vor wichtige Faktoren beim Wachstum des Cloud Computing sind. Eine Umfrage über Disk-basierten Datenschutz, die IDC im März 2012 durchführte und an der 163 IT- und Speicherfachleute teilnahmen, ergab, dass ca. 64,5 % der Firmen eine Sicherungsstrategie in einer öffentlichen Cloud nutzen oder planen. Dieselbe Umfrage hob hervor, dass die 38 %, die derzeit die öffentliche Cloud zur Datensicherung verwenden, nur einen relativ kleinen, jedoch wachsenden Prozentsatz ihrer gesamten Datenmenge dort speichern.

Während das Cloud Computing und damit Cloud-Backup immer populärer werden, beginnen sich jedoch Unterschiede zwischen den verschiedenen Typen von Sicherungsdiensten und -anbietern abzuzeichnen, da Zulieferer neue Zielmärkte erschließen und verschiedene Gruppen von ihrem Cloud-Backup andere Eigenschaften verlangen.

- **Verbraucher gg. Unternehmen:** Es gibt offensichtliche Unterschiede zwischen den Bedürfnissen von Verbrauchern und den Anforderungen von Unternehmen. Diese Unterschiede machen sich in der benötigten Speicherkapazität und dem erforderlichen Anwendungs-Support bemerkbar sowie bei dem Bedarf an administrativen Tools und Funktionalität, Bandbreitenverfügbarkeit für die entsprechende Datenmenge, Anzahl der Nutzer, erforderlichen Sicherheitsfunktionen, Kundendienst, Betriebszeit und Zahlungsmodellen (kostenloses „Freemium“ bzw. gebührenpflichtiges Abonnement). Obwohl die Anforderungen des Verbrauchers nicht auf die leichte Schulter genommen werden dürfen, brauchen gewerbliche Kunden einen Anbieter, der sich im Umgang mit den besonderen Bedürfnissen von Unternehmen auskennt. Die besonderen Ansprüche von Unternehmen umfassen üblicherweise Anforderungen an die Datensicherheit, Datenschutz und Standort, Anwendung/Kundenunterstützung, effektive Handhabung großer Datenmengen und Support-Dienste, die über ein gemeinsames oder privates Punkt-zu-Punkt-Netz ausgeführt werden können.

- **Neuanbieter gg. etablierte Anbieter:** Cloud-Dienste stellen das Wachstum der IT-Branche dar und bieten innovativen, neuen Unternehmen relativ niedrige Eintrittshürden. Als Ergebnis bedienen kleine Aufsteiger Nischenmärkte, die derzeit nicht bedient werden, oder sie versuchen, individuelle/neue Dienste, Preismodelle,

 ©2013 IDC

Funktionen usw. anzubieten. Um die Anfangskosten gering zu halten, nutzen viele die Infrastruktur eines Drittanbieters für den Service, anstatt ihre eigene Hardware aufzubauen. Daher kann ein Cloud-Dienst von einem Drittanbieter abhängig sein, um die SLA (Service-Level-Vereinbarung) zu erfüllen, und die Fehlerbehebung wird folglich kompliziert. Andererseits tendieren etablierte Cloud-Provider dazu, ihre eigenen Clouds aufzubauen und zu bedienen. Sie zielen auf den Verbraucher bzw. die Geschäfts-/Unternehmenswelt im Allgemeinen ab oder in manchen Fällen auch auf beides. Etablierte Cloud-Provider haben sich erfolgreich einem Zertifizierungs- und Prüfverfahren unterzogen, und sie verfügen über wertvolle Erfahrung bei der Bereitstellung und Verwaltung der Cloud-Infrastruktur. Sie bieten möglicherweise auch umfangreichere SLAs, mehr maßgeschneiderte Angebote und eine geschäftliche und finanzielle Tragfähigkeit an, die Aufsteiger nicht bieten können.

Öffentliches Cloud-Backup ist ein zunehmend integrierter Teil der Unternehmens-IT geworden. Beim Vergleich der verschiedenen Anbieter müssen viele verschiedene Faktoren beachtet werden. Nach der Cloud-Prognose von IDC soll der Markt der öffentlichen Cloud-Backup-Dienste 2013 schätzungsweise über 2 Milliarden Dollar an Ausgaben und von 2010 bis 2015 eine durchschnittliche jährliche Wachstumsrate (CAGR) von 33 % erreichen. Die Gesamtausgaben sollen bis 2015 auf über 3,6 Milliarden Dollar wachsen. Mit erheblichen Investitionen in öffentliche Cloud-Dienste für die Datensicherung, die die bescheidene jährliche Wachstumsrate von 4,8 % des traditionellen Softwaremarktes für die Datensicherung am Standort deutlich übersteigen, ist die Wahl des richtigen Dienstanbieters wichtiger denn je, speziell mit einer Funktion wie der Datensicherung, die bezüglich Daten, Format und Fußabdruck notorisch langlebig ist.

KRITERIEN BEI DER AUSWAHL EINES CLOUD BACKUP-PROVIDERS

Damit große Unternehmen entscheiden können, welcher Cloud-Backup-Provider für ihre Bedürfnisse am besten geeignet ist, müssen gewisse Kriterien festgelegt werden, die ein potenzieller Anbieter erfüllen muss. Folgende Kriterien sind die entscheidenden Merkmale, die bei der Auswahl des Cloud-Backup-Anbieters beachtet werden müssen. Unternehmen können diese Kriterien bei der sorgfältigen Prüfung der Dienstanbieter, ihres Angebots und der Vertragsbedingungen verwenden.

Dauerhaftes Dienstanbieter-Angebot

Angesichts der Beschaffenheit eines Cloud-Backups sollte ein Cloud-Backup-Provider zukunftsfähig sein. Auch wenn Neuunternehmen und sogar etablierte Anbieter anfängliche Einsparungen oder andere einmalige Angebote vorstellen, stellen sie für ihre potenziellen Kunden ein großes Risiko dar, sollten sie die nächsten 5 Jahre nicht überleben. Wenn eine Firma Server- oder Speicher-Hardware am eigenen Standort nutzt und der IT-Lieferant sein Geschäft aufgibt, haben die Kunden keinen Anbieter für Wartung/Kundendienst mehr und müssen ihre Anwendungen oder gespeicherten Daten schließlich auf ein anderes System verlegen. Dieser Übergang kann jedoch nach Bedarf und ohne Datenverlust beim Austritt einer Speicher-Hardware-Firma ausgeführt werden, sofern die Datenmigration erfolgreich ist. Dasselbe gilt jedoch nicht für Cloud-Provider. Wenn ein Cloud-Provider aus dem

Markt ausscheidet, dann besteht die Gefahr, dass auch die Daten der Kunden verloren gehen, was ein potenzielles Sicherheitsrisiko, Datenverlust und die Visibilität der Interessengruppen des Unternehmens zur Folge hat. Um sicherzustellen, dass ein Cloud-Provider auf lange Sicht erhalten bleibt, sollten potenzielle Kunden folgende Kategorien sorgfältig prüfen.

- **Finanzielle Stabilität:** Wenn der Cloud-Provider keine profitable, finanzielle Position einnimmt oder noch versucht, ein erfolgreiches Geschäftsmodell und/oder einen Kundenstamm aufzubauen, dann besteht ein hohes Risiko, dass es ein Verlustgeschäft wird und sich nicht halten kann. Die folgenden Fragen können zur Klärung der finanziellen Stabilität eines Providers herangezogen werden (die Antworten können im Rahmen einer unterzeichneten NDA erteilt werden):

  - Erzielen Sie heute schon Profite? Falls nicht, zu welchem Zeitpunkt werden Sie voraussichtlich die Gewinnschwelle erreichen?
  - Wie ist Ihre Liquiditätslage?
  - Wie fällt derzeit Ihre Bonitätsbeurteilung aus?
  - Können Sie bitte eine unterschriebene Kopie Ihrer letzten geprüften Finanzberichte bereitstellen?
  - Hat Ihr Unternehmen Gläubigerschutz beantragt? Wann? Warum?

- **Bewährte Infrastruktur:** Obwohl innovative Technologie und Hardware eine Branche optimieren oder bei der Gründung neuer Branchen helfen können, muss es sich bei der vom Cloud-Provider eingesetzten Infrastruktur im Falle eines Cloud-Backups um bewährte Systeme handeln, bevor der Enterprise-Kunde ihr seine kritischen Unternehmensdaten anvertrauen kann. Wie zuvor erwähnt verlassen sich viele Cloud-Backup-Dienste auf Fremd-IaaS und befinden sich daher in einer Abhängigkeit bei der Erfüllung von SLAs sowie bei der Fehlerbehebung. Stellen Sie folgende Fragen, um festzustellen, ob der Serviceanbieter eine bewährte Infrastruktur verwendet:

  - Verfahren Sie nach einem Buy-and-Operate-Modell oder sind Sie von IaaS-Providern abhängig?
  - Wie lauten jeweils die SLAs für die Verfügbarkeit des Service, Zuverlässigkeit, Sicherungserfolg, Sicherungszeiten, Wiederherstellungszeit u.s.w.?
  - Sind die SLAs dokumentiert und veröffentlicht?
  - Fragen Sie diejenigen Serviceanbieter, die statt ihrer eigenen Infrastruktur gewerbliche Hard- und Software verwenden, welche Hard- und Software-Infrastruktur verwendet wird.
  - Wie lange wird diese Infrastruktur schon produziert?

 ©2013 IDC

- **Etablierter Kundenstamm:** Bei der Suche eines Providers ist es hilfreich zu wissen, welche anderen Unternehmen seine Dienste bereits in Anspruch nehmen. Ein kleiner Kundenstamm weist – selbst wenn er wächst – eher auf ein neugegründetes Unternehmen hin. Ein Verlust des Kundenstamms würde darauf hinweisen, dass es Probleme gibt, die die Kunden dazu veranlassen, abzuwandern. Stellen Sie sicher, dass sich Dienstanbieter, die Tausende oder Millionen von Kunden angeben, auf gewerbliche Kunden beziehen, nicht nur auf Verbraucher. Viele Dienstanbieter beginnen mit einem Fokus auf Verbrauchern oder KMU, sind jedoch noch keine etablierten Enterprise-Provider. Um das Risiko zu verringern, suchen Sie sich einen Anbieter mit einer großen Enterprise-Kundschaft. Nutzen Sie Ihr internes oder Peer-Netzwerk, um mit den Kunden eines bestimmten Anbieters zu sprechen. Stellen Sie u. a. folgende Fragen:

  - Wie viele Kunden nutzen derzeit Ihre Dienste? Handelt es sich um „Freemium"- oder zahlende Kunden?
  - Wie viele Unternehmen nutzen derzeit Ihren Service? Handelt es sich um KMU oder Enterprise-Kunden?
  - Welches Wachstum weisen die Geschäftssegmente in den letzten 12 oder 24 Monaten auf?
  - Wie lange bedienen Sie bereits Enterprise-Kunden?
  - Gibt es Kunden, für die sich Ihr Service nicht eignet? Welche? Warum?

- **Geografisch verteilte Datenzentren:** Wie Hurricane Sandy 2012 bewies, ollte sich das Cloud-Datenzentrum, in dem Ihre Backup-Dateien gespeichert sind, in mindestens 40 km Entfernung zur Küste befinden (wenn ein Unglück geschieht). Geografisch verteilte Datenzentren sind für die Gewährleistung einer Ausfallsicherung wichtig, wenn konstante Betriebszeit vorgeschrieben ist und ein unvorhergesehenes Problem im Hauptdatenzentrum auftritt, in dem die Daten gespeichert sind. Der Standort ist wichtig für die Risikostreuung, insbesondere im Fall von Naturkatastrophen, aber auch, um den regionalen, rechtlichen Anforderungen für Datenspeicherorte zu entsprechen. So gelten beispielsweise an manchen geografischen Standorten Bestimmungen, dass Daten die regionalen Grenzen nicht verlassen dürfen. Dies macht es erforderlich, dass der Service-Provider physikalische Einrichtungen in dieser Region betreibt. Die Einhaltung des lokalen Datenverarbeitungsgesetzes durch den Cloud-Anbieter ist zwar ein wichtiges Kriterium, doch ist der Support des Anbieters von geeigneten Verschlüsselungsniveaus für diese Daten und deren gesicherten Datenschutz die wichtigere Maßnahme der Datensicherheitsfunktionen. Dies wird im Bereich „Service, der auf führenden Sicherheits- und Datenschutzmaßnahmen aufgebaut ist" beschrieben. Stellen Sie u. a. folgende Fragen:

  - Sind Ihre Datenzentren geografisch verteilt und verfügen Sie über Datenzentren außerhalb der USA, z. B. für Kunden aus Europa oder Asien/Pazifik?
  - Können Sie gewährleisten, dass meine Daten an ein bestimmtes Datenzentrum gesendet werden?

- Wie sieht Ihre Notfallplanung im Falle eines Standort- oder Betriebsausfalls aus?

- **Validierung und Akkreditierung durch Dritte:** Regelmäßige, erfolgreiche Prüfungen der Sicherheitsmaßnahmen eines Cloud-Backup-Providers sind wichtig, um zu gewährleisten, dass der Cloud-Anbieter die Kundendaten sicher und zuverlässig verarbeitet und hostet. SSAE 16 ist ein weithin anerkannter Prüfstandard des „American Institute of Certified Public Accountants (AICPA)“ (Institut amtlich zugelassener Buch- und Rechnungsprüfer der USA), anhand dessen festgestellt wird, ob die Kontrollziele und -maßnahmen eines Dienstunternehmens eingehend geprüft wurden, um die sichere und zuverlässige Bearbeitung und Aufbewahrung von Kundendaten zu gewährleisten. Außerdem legt die Zertifizierung ISO 27001 fest, dass ein potenzieller Anbieter internationale Normen zur Messung der Sicherheitsverwaltungssysteme erfüllen muss. ISO 27001 umfasst mehrere Anforderungen und bewährte Praktiken für einen systematischen Ansatz zur Verwaltung von Unternehmens-/Kundeninformationen basierend auf regelmäßigen Risikobewertungen, die sich den ständig im Wandel befindlichen Bedrohungen anpassen. Welche Antworten hat Ihr Dienstanbieter auf die folgenden Fragen?

  - Haben Sie sich während der vergangenen 24 Monate einer Fremdprüfung unterzogen? Wann und durch wen?

  - Bitte legen Sie uns die Ergebnisse dieser Prüfungen vor.

  - Verfügt Ihr Unternehmen über ISO 27001 oder ISO 27002, SSAE 16, PCI DSS, HIPAA oder andere Zertifizierungen?

- **SLA-Bedingungen und Ausführung:** Etablierte SLA-Bedingungen und ihre Ausführung sind nicht nur für die Feststellung der Verarbeitungs- und Hosting-Art der Kundendaten wesentlich, sie bieten auch die erforderliche Transparenz für den Dienstgrad, die der Kunde vom Cloud-Anbieter verlangen kann. Dadurch wird ein gewisser Erwartungsgrad sowie das Dienstleistungsniveau festgelegt. Stellen Sie Ihrem Dienstanbieter u. a. folgende Fragen:

  - Wie und von wem werden SLAs überwacht und bemessen?

  - Gibt es Geschäftsunterbrechungen, die die SLAs nicht abdecken? Beschreiben Sie sie.

Service, der auf führenden Sicherheits- und Datenschutzmaßnahmen aufgebaut ist

Die Hauptbedenken des Cloud-Backups sind Datensicherheit und Datenschutz. Unternehmen sorgen sich um den illegalen Zugriff von außen (oder Hacking) auf ihre Daten und um potenzielle Beschlagnahmung der Hardware des Cloud-Anbieters durch Regierungsbehörden sowie um unbefugten Zugriff des Cloud-Anbieters auf die Daten zum Sammeln von Statistiken oder um Daten zu verkaufen. Da die Backup-Daten sich nicht unter der physischen Aufsicht des Unternehmens befinden, steht die Sorge um Sicherheits- und Datenschutzbelange für die IT-Abteilung von Unternehmen stets an erster. Daher ist es von höchster Wichtigkeit, dass Cloud-

 ©2013 IDC

Provider die besten Sicherheits- und Datenschutzfunktionen anbieten. Wichtige Sicherheitsfunktionen für Enterprise-Kunden umfassen u. a.:

- **AES-Verschlüsselung mit persönlichem Schlüssel:** Eine Funktion, mit der Kunden ihre eigenen, persönlichen Verschlüsselungscodes einrichten und pflegen können, die sie selbst und nicht der Provider kontrollieren. AES gilt als Standard in der Verschlüsselung von Daten. Er wird von verschiedenen Regierungsbehörden verwendet und ist FIPS-zertifiziert. Noch wichtiger ist allerdings, dass der Cloud-Backup-Provider die Dateien des Kunden selbst unter gesetzlichem Druck nicht entschlüsseln kann, wenn der Kunde seine eigenen Verschlüsselungscodes setzen und verwalten kann.

  - Verfügt Ihre Organisation über ein formelles, dokumentiertes, vorgeschriebenes und unternehmensweites Sicherheitsprogramm, einschließlich Sicherheitsrichtlinien, Standards und Verfahren? Bitte bereitstellen.

  - Müssen die Daten bei der Sicherung verschlüsselt werden? Welchen Verschlüsselungsgrad verwenden Sie?

- **Verschlüsselung während der Übertragung und in gespeichertem (Ruhe-) Zustand:** Gewährleistung, dass die Daten während der Übertragung sowie im Cloud-Backup-Speicher des Anbietersystems (Ruhezustand) verschlüsselt sind. Durch die gemeinsame Nutzung dieser beiden Verschlüsselungsarten werden die Daten besser gesichert, als wenn nur eine davon verwendet wird. Natürlich muss die Verschlüsselung in effektiver Übereinstimmung mit effizienten Speicherstrategien ausgeführt werden, z. B. Komprimierung und Deduplizierung.

- **Verwaltung/Handhabung der Verschlüsselung:** Festlegen, wer die Kontrolle über die Verschlüsselungscodes hat, ob die Verwaltung/Kenntnis der Verschlüsselung beim Provider oder beim Kunden liegt. Wenn der Kunde die Verwaltung der Verschlüsselung selbst vornimmt, muss der Anbieter über einen Prozess verfügen, um sicherzustellen, dass der Verschlüsselungscode örtlich beim Kunden gespeichert wird und nicht auf dem System des Providers. Um verschiedene Kundenbedürfnisse zu erfüllen, sind auch verschiedene Verwaltungsstufen der Verschlüsselung wünschenswert.

  - Bitten Sie Ihren Anbieter, die Infrastruktur zur Handhabung von Verschlüsselungscodes in seiner Organisation zu beschreiben.

  - Bitten Sie den Anbieter, die Optionen zur Handhabung von Verschlüsselungscodes in seiner Organisation zu beschreiben.

- **Dokumentiertes, vorgeschriebenes und überwachtes Sicherheitsprogramm:** Achten Sie darauf, dass der Cloud-Provider über ein gut dokumentiertes Sicherheitsprogramm verfügt, das allen Vorschriften entspricht. Dies hilft bei der Bestimmung der Glaubwürdigkeit des Anbieters bzgl. der Sicherheit.

  - Sind die Sicherheitsrichtlinien dokumentiert?

  - Verfügt der Service-Provider über eine dedizierte Sicherheitsorganisation?

  - Wurde eine Schwachstellenprüfung durch ein anerkanntes Fremdunternehmen durchgeführt? Können die Ergebnisse eingesehen werden?

Im Folgenden sehen Sie wichtige Datenschutzfunktionen, die Unternehmen bei der Auswahl eines potenziellen Cloud-Backup-Providers beachten sollten.

- **Dokumentierte, vorgeschriebene und überwachte Datenschutzrichtlinien:** Enterprise-Kunden möchten sichergehen, dass Cloud-Backup-Anbieter über Richtlinien verfügen, die sämtliche Datenschutzbelange abdecken. Dies stärkt die Glaubwürdigkeit des Cloud-Providers, da er sich die Zeit genommen hat, Datenschutzrichtlinien zu erarbeiten und zu dokumentieren. Fragen, die Sie dem Cloud-Provider stellen sollten, sind u. a.:

  - Verfügen Sie über eine veröffentlichte Datenschutzrichtlinie, die dem Personal zugänglich ist? Wurde sie von einem Verwaltungsrat geprüft und genehmigt?

  - Würden Sie die Prüfung Ihrer Datenschutzverfahren durch ein unabhängiges Unternehmen zulassen?

- **Richtlinie für Werbung/Datamining:** Cloud-Provider müssen transparente Richtlinien bzgl. der Nutzung der Kundendaten haben – hat der Cloud-Provider zu Werbezwecken und/oder Datamining darauf Zugriff oder ist der Datenzugriff strikt und ausschließlich dem Kunden vorbehalten? Unternehmen haben unterschiedliche Ansätze bezüglich der Nutzung für Werbung/Datamining, doch Cloud-Backup-Anbieter müssen in ihren Richtlinien im Hinblick auf die Nutzung von Kundendaten direkt und transparent sein.

  - Bitte erklären Sie Ihre Richtlinien bzgl. der Nutzung von Kundendaten für Werbezwecke und Datamining für finanziellen Gewinn.

- **Praktiken zum Schutz vertraulicher oder sensibler Informationen:** Manche Daten sind noch vertraulicher oder sensibler als alle anderen. Diese Datentypen erfordern zusätzliche Datenschutzprotokolle. Cloud-Anbieter müssen über feste Praktiken für zusätzliche Sicherheitsmaßnahmen für sensibles Material verfügen.

  - Setzen Sie Verfahren ein, um zu gewährleisten, dass Mitarbeiter und Vertragspartner den Schutz und die Vertraulichkeit Ihrer Daten wahren? Bitte erläutern.

 ©2013 IDC

Ein Service, der führende Datenmanagement-Prozesse ermöglicht

Eine weitere Eigenschaft, die zusätzlich zu den Sicherheits- und Datenschutzbedenken beachtet werden sollte, ist ein Service, der mit Datenmanagement von Weltklasse errichtet wird. Merkmale erfolgreichen Datenmanagements umfassen unter anderem folgendes:

- **Zentralisiertes Management-Rahmenkonzept.** Administratoren oder nicht-technische Mitarbeiter sollten dazu in der Lage sein, einen von einem Service-Provider bereitgestellten Cloud-Service zentral zu verwalten, darüber zu berichten und diesen zu überwachen. Dies sollte auch die Verteilung von Berichten umfassen.

- **Bereitstellung von Support für verschiedene Kunden und Anwendungen.** Kunden fangen oft mit einer bestimmten Anwendung oder mit einem Satz von Kunden an und erweitern diese dann zum Schutz anderer Systeme. Anstatt für jede Assetklasse in unterschiedliche Cloud-Services zu investieren, sollte es für einen Cloud-Service ein besonderes Anliegen sein, verschiedene Daten aus unterschiedlichen Systemen zu schützen und wiederherzustellen.

- **Integration von Active Directory (AD) oder LDAP.** Unterstützung für AD oder LDAP ist für effiziente unternehmensweite Bereitstellungen von wesentlicher Bedeutung. Die Integration mit Benutzer- und Gruppenkonten ermöglicht das verhältnismäßig nahtlose Hinzufügen und Entfernen von Benutzern in einem Cloud-Service.

- **Ermöglichung verschiedener Services.** Kunden beginnen zwar oft mit einem Backup, doch wird ihnen häufig klar, dass sie auch andere Bedürfnisse haben. Benutzer verlangen möglicherweise nach Funktionen wie Dateisynchronisierung und Wiederherstellung. Die Möglichkeit, eine Reihe von Funktionen mit einer einzelnen Service-Bereitstellung zu unterstützen, ermöglicht Einsparungen bei den Betriebskosten sowie Kapitaleinsparungen.

- **Datenbestückung.** Die Verteilung des Erst-Backups eines Kunden durch Vorbelegung eines Storage-Systems, das zum Cloud-Provider geschickt wird, ist für die Reduktion von Bandbreiten-Nutzung, Zeit und Kosten von maßgeblicher Bedeutung.

- **Hybrid-Cloud.** Die Bereitstellung einer Option für lokales Backup zusätzlich zu dem Cloud-Backup für geschäftsrelevante Daten hilft Cloud-Providern dabei, schnellstmögliche Wiederherstellungszeiten für essenzielle Daten zu gewährleisten.

WARUM UNTERNEHMEN SICH FÜR MOZY CLOUD BACKUP ENTSCHEIDEN

Bei der Beurteilung der Anbieter von Cloud-Backups steht Mozy in der engeren Auswahl an erster Stelle. Das vom Storage-Führer EMC unterstützte Unternehmen Mozy wurde 2005 gegründet und ist ein bewährter, führender Anbieter von Cloud-Speicher für Backups. Mozys Angebot ist auf die breite Kundenbasis zugeschnitten und richtet sich an eine Vielzahl unterschiedlicher Kunden, die von individuellen Endkunden bis zu Fortune 100-Unternehmen reichen. Für Unternehmenskunden bietet Mozy einfach zu verwaltendes Cloud-Backup, die Möglichkeit zur Skalierung über Multiuser-Umgebungen, zahlreiche Sicherheitsmerkmale (einschließlich einer Auswahl von Verwaltungsmöglichkeiten für AES-Schlüssel) sowie Software-Storagefunktionen für Unternehmen wie Snapshots, die eine umfassende Datenspeicherung ermöglichen.

Ein besonderer Schwerpunkt liegt für Mozy in der Bereitstellung von Funktionen, die im Bereich des Cloud-Backups für Unternehmenskunden von besonderer Bedeutung sind.

Mozy bietet auf dem Cloud-Backup-Markt eine Reihe von Schlüsselmerkmalen (siehe Tabelle 1), aufgrund derer sich das Unternehmen von der Konkurrenz abheben kann.

TABELLE 1

Checkliste für wichtige Cloud-Backup-Funktionen

	Mozys Merkmale
Dauerhaft	
Finanzielle Stabilität	Mozy ist ein Cloud-Service von EMC, einem öffentlich gehandelten Unternehmen im Wert von 47 Milliarden Dollar.
Bewährte Infrastruktur	Der Mozy-Cloud-Service ist seit über acht Jahren in Produktion. Die starke Backup-Infrastruktur umfasst 90 PB verwalteter Cloud-Daten.
Etablierter Kundenstamm	Mozy hat über 100.000 gewerbliche Kunden und mehr als 6 Millionen Endverbraucher. Mozy bietet seinen Enterprise-Kunden seit 2008 Cloud-Backup-Dienste an.
Geografisch verteilte Datenzenter-Standorte	Mozy verfügt über ein Netz geografisch verteilter Datenzentren – darunter Datenzentren in Amerika und EMEA für Kunden und Partner in diesen Regionen.
Zertifikate	Mozy ist ISO 27001 zertifiziert und hält sich an das Safe Harbor-Abkommen.
Erfolgreiche Prüfungen	Mozy schloss die SSAE 16 Typ II Prüfung erfolgreich ab.
SLA-Bedingungen und Ausführung	Mozy stellt 99,9 % Serviceverfügbarkeit bereit.
Sicherheit	
AES-Verschlüsselung mit	Mozy bietet private AES-Verschlüsselung mit seinem privaten und Enterprise-

 ©2013 IDC

TABELLE 1

Checkliste für wichtige Cloud-Backup-Funktionen

	Mozys Merkmale
privatem Schlüssel	Kundenschlüssel.
Verschlüsselung beim Senden und im Ruhezustand	Alle Daten werden während der Sicherung, beim Senden über eine verschlüsselte SSL-Verbindung und im Ruhezustand für vollständigen und umfassenden Datenschutz verschlüsselt.
Verwaltung/Handhabung der Verschlüsselung	Mozy bietet drei Stufen der Schlüsselverwaltung an: eine Standardverschlüsselung über Blowfish, die von Mozy verwaltet wird, ein privater Schlüssel mit AES, der vom Kunden direkt verwaltet wird und ein Enterprise-Kundenschlüssel mit AES, den ebenfalls der Kunde selbst verwaltet.
Personalschutz	Mozy verfügt über ein persönliches Sicherheitsprogramm, das Hintergrundprüfungen, Zugangsverwaltung und Prüfung umfasst.
Dokumentiertes, vorgeschriebenes und überwachtes Sicherheitsprogramm	Mozy verfügt auch über ein ISO Sicherheitsmanagementsystem.
Sicherheitsrichtlinien	Mozy verfügt über ein dediziertes Cloud-Sicherheitsteam, das umfangreiche physische und digitale Sicherheitsrichtlinien ausarbeitet und pflegt. Die Sicherheitsrichtlinien von Mozy können nach Bedarf an die Kunden weitergegeben werden.
Penetrationstests und Schwachstellenbewertungen	Die Schwachstellenbewertung wird vierteljährlich oder nach Bedarf durchgeführt. Penetrationstests werden vom Mozy-Sicherheitsteam nach Bedarf in Verbindung mit dem Schwachstellenbewertungs¬programm durchgeführt.
Datenschutz	
Dokumentierte, vorgeschriebene und überwachte Datenschutzrichtlinien	Die Mozy Datenschutzrichtlinie ist auf der Mozy-Website einzusehen (verfügbar unter mozy.com/privacy).
Richtlinie für Nutzerwerbung/Vereinbarung gegen Datamining zu Werbezwecken	Mozy verkauft oder vermarktet keine Nutzerdaten und sieht auch keine Endverbraucher-Backup-Daten ein.
Praktiken zum Schutz vertraulicher und sensibler Informationen	Mozy verfügt über Richtlinien zur Datenklassifizierung und -bearbeitung sowie zu Informamtionsbearbeitungsverfahren und den mit diesen Stufen verbundenen Kontrollen.
Einhaltung der regionalen und örtlichen Datenschutzbestimmungen	Mozy hält sich an die Safe Harbor-Vereinbarung und bietet ein Netzwerk geografisch verteilter Datenzentren an.

TABELLE 1

Checkliste für wichtige Cloud-Backup-Funktionen

	Mozys Merkmale
Ein Dienst mit Datenverwaltung der Weltklasse	
Zentralisierte Verwaltung	Mozy bietet eine Web-basierte, mandantenfähige Admin-Konsole zur Kontenverwaltung durch administratives und sub-administratives Personal. Die Mozy Software kann über die Admin-Konsole konfiguriert, eingesetzt und zentral verwaltet werden, wodurch umfassende, benutzerdefinierte Konfigurationssteuerung möglich ist.
Unterstützter Kunden- und Anwendungsbereich	Mozy unterstützt eine Reihe von Anwendungen, darunter Netzwerkfreigaben, alle Versionen von SQL und Exchange, SharePoint, Active Directory, COM+ Dienste, SYSVOL Verzeichnisfreigabe und Windows Registry-Datenbanken.
Active Directory-Integration	Mozy bietet Active Directory-Integration, die automatisch die Erstellung, Organisation und Entfernung von Nutzern in MozyEnterprise auslöst.
Leistungsangebot	Mozy bietet verbraucherbasiertes Cloud-Backup, gewerbliches Cloud-Backup (Endverbraucher und Server) sowie Enterprise Cloud-Backup.
Richtlinien für Sicherung und Speicherung	MozyEnterprise bietet eine 90-Tage Datenspeicherungsrichtlinie.
Datenbestückung: Erste Sicherung	Mozy bietet Mozy Data Shuttle an, eine Funktion zur Bestückung der ersten Sicherung in der Mozy Cloud.
Hybridoption zur schnellsten, örtlichen Wiederherstellung	Mit Mozy 2xProtect können Sie die örtliche Sicherung zusätzlich zum Cloud-Backup auf einem USB- oder externen Laufwerk durchführen. Außerdem stehen optimierte kostenlose, örtliche BRS-Backup-Lösungen für das Hybrid-Cloud-Backup bereit.

Quelle: IDC 2013

HERAUSFORDERUNGEN/CHANCEN

Über die Jahre hat sich Mozy als führender Cloud-Backup-Anbieter für Verbraucher und Enterprise-Kunden etabliert. Mozy hat gewissenhaft die wichtigsten Bedenken aller Kunden bzgl. öffentlicher Cloud, Datenschutz und Sicherheit angesprochen. Die Einführung von Funktionen wie z. B. AES-Verschlüsselung, private Schlüsselverwaltung, Zugang und Protokollierung, Audit-Trails, ISO 27001 Zertifizierung, SSAE 16-Prüfung und mehrerer Datenzentrum-Standorte half Mozy dabei, sich einen starken Ruf unter den Cloud-Anbietern zu machen.

Der nächste maßgebliche Unterschied kommt mit der Verfeinerung der effizienten Verschiebung, Speicherung und Wiederherstellung der Daten. Die Auseinandersetzung mit der Größe des Datenumfangs in Relation zum Datenkanal, der für die Verschiebung verwendet wird, wird den Bedarf für effiziente Speichertechnologien betonen. Ein weiteres Problem zeigt sich bei verschiedenen Workloads, die möglicherweise andere Wiederherstellungsoptionen für die

 ©2013 IDC

wirksamste Datenwiederherstellung erfordern. Hierfür müssten verschiedene Optionen eingesetzt werden. Durch die Lösung dieser Punkte hat Mozy die Gelegenheit, wertvolle Dienste anzubieten, die von vielen anderen nicht berücksichtigt werden, und somit einmal mehr zu zeigen, warum das Unternehmen beim Cloud-Backup führend ist.

SCHLUSSFOLGERUNG

Während Enterprise-Organisationen ihre Datenzentren auf die kostengünstigste und wirksamste Art und Weise optimieren, erwachsen neue Gelegenheiten für Cloud-Backup-Dienste. Um die Kosten für Datenzentren zu reduzieren – vor allem Speicher-Hardware, Gebäudefläche sowie Strom- und Kühlungskosten – wenden sich die Unternehmen für ausgelagerte Datensicherung und Notfallwiederherstellungsdienste den öffentlichen Cloud-Anbietern zu. Und während das Interesse der Unternehmen am Cloud-Backup wächst, steigt auch der Bedarf für kompetente Cloud-Provider. Durch den erhöhten Fokus auf unternehmensspezifische Bedürfnisse, wie beispielsweise umfassende Datenschutz- und Sicherheitsfunktionen, einfache Kontenverwaltung und Multiuser-Administration, 24-Std.-Support und Skalierbarkeit, setzt sich Mozy als branchenführender Cloud-Backup-Provider ab, den jedes größere Unternehmen in die engere Wahl ziehen sollte.

Urheberrechtshinweis

Externe Veröffentlichung von IDC-Informationen und -Daten – Sämtliche IDC-Informationen, die in Anzeigen, Pressemitteilungen oder Werbematerial verwendet werden sollen, erfordert die vorherige schriftliche Genehmigung des zuständigen IDC Vice President oder Country Manager. Ein Vorentwurf des geplanten Dokuments sollte gemeinsam mit dem Antrag eingereicht werden. IDC behält sich das Recht vor, die Genehmigung der externen Nutzung des Materials nach eigenem Ermessen abzulehnen.

Copyright 2013 IDC. Kopie und Vervielfältigung sind ohne schriftliche Genehmigung strengstens untersagt.