Die Top-5-Gründe für ein Disaster Recovery in der Cloud

Sven Böttcher, Apps Associates GmbH

Die meisten Geschäftsprozesse eines Unternehmens basieren heutzutage auf einem oder mehreren IT-Systemen. Kommt es zu einem Ausfall der IT-Infrastruktur, kann dies schwerwiegende Folgen haben. Um auf Notfallsituationen vorbereitet zu sein, sollten Maßnahmen getroffen werden, durch die der Regelbetrieb schnellstmöglich wiederhergestellt wird. Doch solche Maßnahmen sind im traditionellen Sinn häufig mit hohen Kosten verbunden. In diesem Artikel wird die „Cloud" als kostengünstige Alternative für die Notfallwiederherstellung (Disaster Recovery) vorgestellt.

Ausfälle der IT-Infrastruktur (Hard- und Software) können die verschiedensten Gründe haben. Häufig stehen Naturkatastrophen oder schwere Gebäudebeschädigungen, etwa durch einen Brand, damit in Verbindung. Während diese Ereignisse meistens zu den schwersten Schäden führen, sind die häufigsten Ausfallgründe menschliche Fehler (Quelle: The Acronis Global Disaster Recovery Index, 2012).

Der Ausfall der IT-Infrastruktur kann für ein Unternehmen schwerwiegende Folgen haben. Da in der heutigen Zeit die meisten Geschäftsprozesse in irgendeiner Weise von einem oder auch mehreren IT-Systemen abhängen, führt ein IT-Infrastruktur-Ausfall zunächst dazu, dass die täglichen Geschäftsprozesse beeinträchtigt oder überhaupt nicht mehr durchgeführt werden können. Ein produktives Arbeiten ist damit zumeist nicht mehr möglich.

Darüber hinaus führt ein die IT-Infrastruktur betreffender Unglücksfall häufig zu einem Verlust von Daten. Je nach Unglücksfall und Unternehmen kann es dabei sowohl zu einem beträchtlichen monetären als auch zu einem Image-Schaden kommen. Unternehmen treffen daher Maßnahmen, um die IT-Infrastruktur und die Daten des Unternehmens im Ernstfall möglichst schnell wiederherzustellen, damit zumindest die wichtigsten Geschäftsprozesse wieder ausgeführt werden können. Von zentraler Bedeutung ist, wie schnell die unternehmenskritischen Prozesse nach dem Eintreten eines Unglücksfalls wieder ausführbar sind (Recovery Time Objective – RTO) und wie viele Daten zwischen der letzten Datensicherung und einem solchen Ereignis höchstens verloren gehen dürfen (Recovery Point Objective – RPO).

Um für den Ernstfall gewappnet zu sein, halten Unternehmen in traditionellen Disaster-Recovery-Architekturen (DR, siehe *Abbildung 1*) die benötigte IT-Infrastruktur in der Regel an einem oder mehreren ausreichend räumlich getrennten Orten (DR-Rechenzentren) redundant vor. Die Sicherung der Daten vom lokalen Rechenzentrum in ein DR-Rechenzentrum kann beispielsweise auf physikalischen Datenträgern oder über ein Virtual Private Network (VPN) erfolgen.

Im Allgemeinen ist die Hardware im DR-Rechenzentrum im Stand-by-Modus. Eine Ausnahme bildet Hardware, die für die kontinuierliche Datensicherung erforderlich ist. Im Notfall werden alle Komponenten im DR-Rechenzentrum hochgefahren, sodass diese die Aufgaben der lokalen IT-Infrastruktur übernehmen.

Häufig wird jedoch aus Kostengründen für den Notfallbetrieb weniger beziehungsweise nicht so leistungsfähige Hardware wie für den Regelbetrieb vorgehalten. Dies bedingt, dass die Geschäftsprozesse eines Unternehmens im Notfallbetrieb gegebenenfalls nur eingeschränkt erfolgen können. Auch wenn für den Notfallbetrieb nur ein Teil der im Regelbetrieb zur Verfügung stehenden IT-Infrastruktur vorgehalten wird, sind die Anschaffungskosten und der anfallende zeitliche Aufwand für die Administration dennoch sehr hoch. Ein vielversprechender Ansatz, der viele der Probleme und Nachteile von traditionellen DR-Architekturen vermeidet, ist das Cloud Computing.

Cloud Computing

Cloud Computing oder auch einfach „die Cloud" ist ein Begriff, der heutzutage aus der IT-Welt nicht mehr wegzudenken ist. Die gängigsten Anwendungen und die damit verbundenen Vorstellungen von „Cloud" sind das Speichern von Fotos, Musik oder anderen Daten im World Wide Web. Solche Dienste werden vor allem von privaten Endanwendern in Anspruch genommen. Zu den bekanntesten Cloud-Diensten gehören die Apple iCloud und Microsofts OneDrive.

Auch wenn diese Dienste heutzutage für die meisten Endanwender ausreichend sind und täglich millionenfach in Anspruch genommen werden, haben Unternehmen gänzlich andere Anforderungen an das Cloud Computing, um ihre täglichen Geschäftsprozesse effizienter und kostengünstiger zu gestalten. Im professionellen Bereich wird in Bezug auf Cloud Computing normalerweise zwischen den Dienst- beziehungsweise Geschäftsmodellen „Software as a Service" (SaaS), „Platform as a Service" (PaaS) und „Infrastructure as a Service" (IaaS) unterschieden, je nachdem, was der Anbieter zur Verfügung stellt.

Beim SaaS-Dienstmodell wird beispielsweise Software für die Benutzung über das Internet angeboten. Durch dieses Dienstmodell entfallen der klassische Kauf einer Software-Lizenz und die Installation der entsprechenden Software auf lokaler Hardware. Stattdessen wird vom Anbieter meistens eine nutzungsbezogene Gebühr für die Inanspruchnahme der jeweiligen Software erhoben.

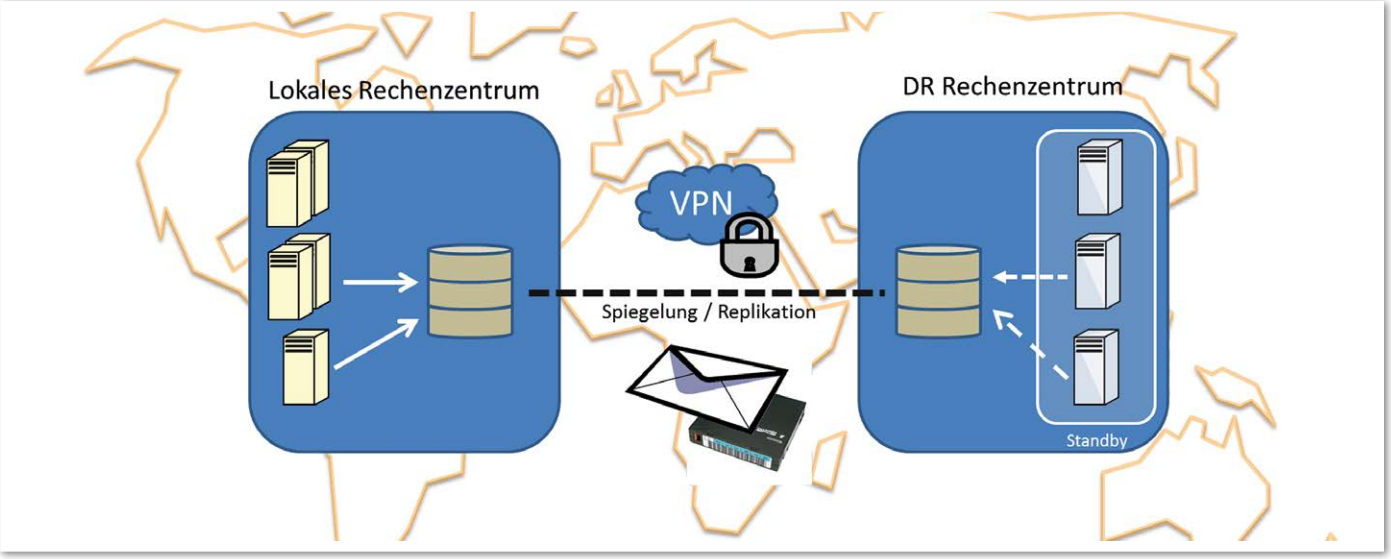

Abbildung 1: Traditionelle Disaster-Recovery-Architektur

IaaS-Anbieter bieten dagegen komplette Infrastruktur-Dienste an, durch die es theoretisch möglich ist, gesamte Rechenzentren in die Cloud auszulagern. Auch hier erfolgt die Abrechnung im Allgemeinen nutzungsbezogen, sodass nur für die tatsächlich in Anspruch genommene Infrastruktur gezahlt werden muss („pay per use").

Einer der größten IaaS-Anbieter ist der Online-Versandhandel Amazon. Er bündelt die zur Verfügung gestellten IaaS-Dienste unter dem Namen „Amazon Web Services" (AWS). Sie umfassen beispielsweise eine nach Kunden-Anforderungen anpassbare Rechenkapazität (Elastic Compute Cloud – EC2), eine Datenspeicher-Infrastruktur zum Speichern beliebiger Daten (Simple Storage Service – S3) und einen Load-Balancing-Dienst. Dieser kann benötigte Rechen-Ressourcen bedarfsgesteuert in sehr kurzer Zeit bereitstellen oder bestehende Ressourcen anpassen, wodurch sowohl eine horizontale als auch eine vertikale Skalierung erreicht werden kann. Letzteres ist sogar voll automatisch möglich.

Die Sicherheit steht im Vordergrund

Gerade in Verbindung mit Cloud-Diensten kommt immer wieder die Frage nach der Datensicherheit auf. AWS bietet hier zahlreiche Sicherheits-Standards, die für viele Unternehmen nur schwer oder nur mit einem hohen Aufwand realisiert werden können. Zum Beispiel sind die AWS-Rechenzentren grundsätzlich in unauffälligen Gebäuden, der Zugang zu den Gebäuden ist strikt reglementiert und es kommt eine mindestens zweimalige Zwei-Faktor-Authentifizierung zum Einsatz.

Zudem ist AWS nach verschiedenen Standards wie ISO 27001, SOC1, SOC2 und SOC3 zertifiziert. Der Kunden kann auswählen, wo sich die in Anspruch genommene IT-Infrastruktur befindet und wo die eigenen Daten gespeichert werden sollen. In diesem Jahr wurde ein AWS-Rechenzentrum in Frankfurt eröffnet, sodass auch hinsichtlich gesetzlicher Rahmenbedingungen das Cloud Computing eine echte Alternative zu lokaler Hardware darstellen kann.

Fallbeispiel Disaster Recovery in der Cloud

Dass eine (Amazon-)Cloud-basierte Notfall-Wiederherstellung funktioniert, konnte das Unternehmen des Autors bereits für seinen Kunden Passkey zeigen. Passkey, im Jahr 2014 von Lanyon, einem führenden Anbieter für Meeting und Eventplanungssoftware, übernommen, ist ein großer Anbieter von webbasierten Hotelbuchungs-Technologien für Gruppenveranstaltungen. *Abbildung 2* zeigt schematisch die implementierte DR-Architektur.

Als wichtigste Infrastruktur-Komponenten stehen im Regelbetrieb Webserver, Applikationsserver sowie Datenbankserver zur Verfügung. Jegliche Kundenanfragen werden über den AWS-DNS-Dienst „Route 53" auf die lokalen Webserver geleitet. Diese Infrastruktur-Komponenten wurden gleichermaßen in einem (von anderen AWS-Kunden) isolierten Bereich (Virtual Private Cloud – VPC) in der Amazon-Cloud eingerichtet. Die Datenbank- und Applikationsserver befinden sich in einem privaten Sub-Netz, das vor direkten Zugriffen über das Internet geschützt ist.

Ein direkter Zugriff auf die Komponenten ist lediglich von bestimmten IP-Adressen aus dem öffentlichen Sub-Netz der VPC und über eine VPN-Verbindung aus dem lokalen Rechenzentrum beziehungsweise aus dem Firmen-Netzwerk möglich. Diese VPN-Verbindung kommt unter anderem für die Golden-Gate-basierte Datenbank-Synchronisation zum Einsatz.

Im öffentlichen und über das Internet erreichbaren Sub-Netz wurden neben zwei Webservern eine Network-Address-Translation-Instanz (NAT) sowie ein Monitoring-Dienst (Nimsoft) eingerichtet. Über die NAT-Instanz bekommen die Komponenten im privaten Sub-Netz Zugriff auf das Internet.

Im Regelbetrieb werden nur die für die Datensicherung und den Betrieb wichtigsten Komponenten betrieben; die Applikations- und Webserver sind nicht aktiv. Sie liegen als Abbild (Amazon Machine Image – AMI) in einem Speicherbereich in der Amazon-Cloud vor und können im Ernstfall einfach und schnell (über das Internet) instanziiert werden *(siehe Abbildung 3)*. Jegliche Anfragen werden dann durch den „Route 53"-Dienst auf die Webserver in der Amazon-Cloud weitergeleitet.

Disaster Recovery in der Cloud

Einer der Hauptgründe, aus denen Unternehmen gänzlich auf eine DR-Strategie verzichten, sind die in der Regel sehr hohen Kosten. Insbesondere die anfänglichen Kosten für die Anschaffung der zusätzlichen IT-Infrastruktur und für den Aufbau der benötigten Rechenzentren stellen für viele Unternehmen eine unüberwindbare Hürde dar.

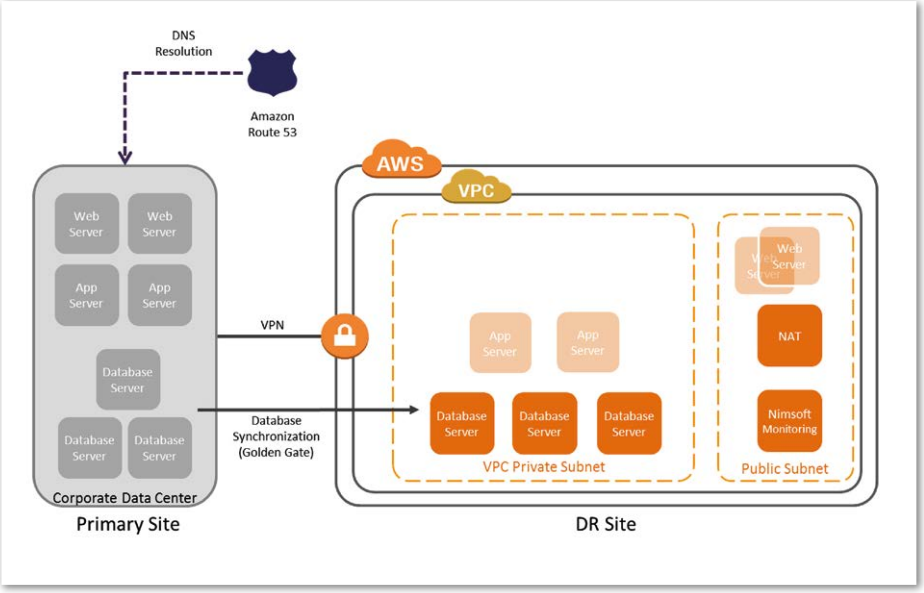

Abbildung 2: Lokale und DR-Infrastruktur in der AWS-Cloud (Regelbetrieb)

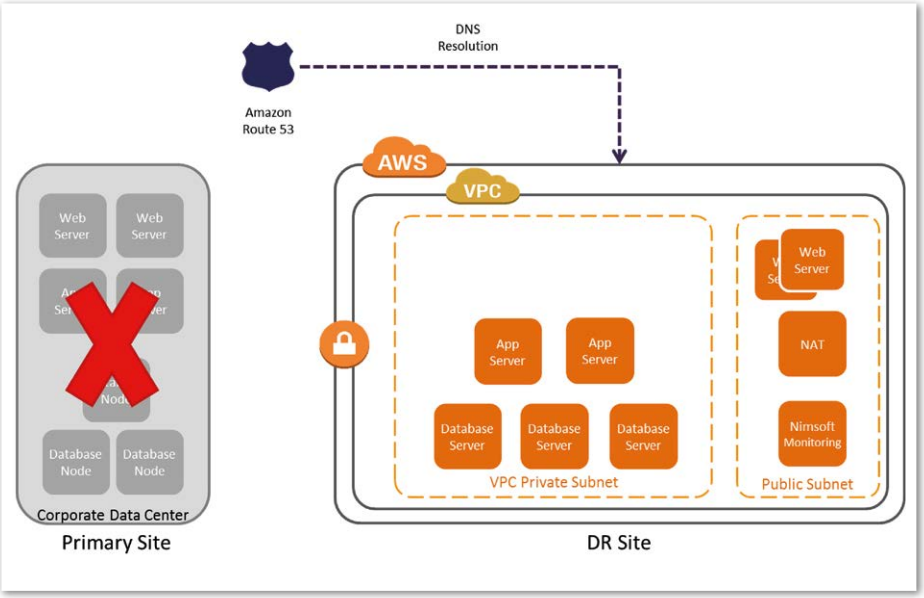

Abbildung 3: Lokale und DR-Infrastruktur in der AWS-Cloud (Notfall-Betrieb)

Durch eine Cloud-basierte DR-Strategie ist weder der Kauf von Hardware erforderlich, noch muss ein Rechenzentrum für den Betrieb aufgebaut werden. Die bedarfsgesteuerte Bereitstellung der IT-Infrastruktur durch einen entsprechenden Anbieter reduziert die Investitionskosten („CapEx“) auf null.

Neben den Anschaffungskosten stellen für viele Unternehmen die Betriebskosten („OpEx“) einen weiteren Grund dar, komplett auf eine DR-Strategie zu verzichten. Auch diese Kosten lassen sich durch eine Cloud-basierte Lösung senken, da weder laufende Kosten für den Betrieb eines Rechenzentrums anfallen, noch beispielsweise kostenintensive Support-Verträge für die zugrunde liegende Hardware abgeschlossen sein müssen.

Damit gewährleistet ist, dass die für den Notfallbetrieb vorgehaltene IT-Infrastruktur auch im Notfall zuverlässig funktioniert, sind regelmäßige Tests notwendig. In traditionellen DR-Architekturen muss ein Mitarbeiter dafür in ein entferntes Rechenzentrum reisen und die entsprechenden Tests durchführen. Da in einer Cloud-basierten Lösung sämtliche IT-Infrastruktur über das Internet erreichbar ist und administriert werden kann, entfallen zeitaufwändige Reisen. Damit ist ein effizienteres und auch häufigeres Testen der IT-Infrastruktur möglich.

Die erwähnten Kennzahlen RTO und RPO sind für die Planung einer DR-Strategie von zentraler Bedeutung. In traditionellen DR-Architekturen liegen das RTO häufig bei ein bis zwei Tagen und das RPO bei 24 bis 48 Stunden. Im Rahmen des dargestellten Fallbeispiels konnte gezeigt werden, dass ein RTO von vier Stunden und ein RPO von weniger als einer halben Stunde möglich ist. Entsprechend können im Ernstfall bei einer Cloud-basierten Lösung die Geschäftsprozesse in einem Unternehmen deutlich schneller und bei einem geringeren Datenverlust wiederaufgenommen werden.

Wie bereits beschrieben, wird für den Notfallbetrieb häufig nur ein Teil der im Regelbetrieb zur Verfügung stehenden IT-Infrastruktur vorgehalten. Dies führt dazu, dass im Notfallbetrieb unter Umständen mit Einschränkungen bei der täglichen Arbeit gerechnet werden muss, wodurch gegebenenfalls ein monetärer Nachteil entsteht. Die Skalierbarkeit von Cloud-basierten Lösungen ermöglicht den bedarfsgesteuerten Einsatz der Infrastruktur-Komponenten. Diese Eigenschaft wird häufig auch als „Elastizität“ bezeichnet. In Zeiten hoher Nachfrage können so zusätzliche und vorkonfigurierte IT-Infrastruktur-Komponenten wie Webserver oder Datenbankserver eingeschaltet werden. Für die „pay per use“-basierten Dienste fallen laufende Kosten nur für diese Zeiträume an. Sinkt die Anfrage oder wird der Regelbetrieb wiederaufgenommen, können alle nicht benötigten Komponenten abgeschaltet werden, was mit einer Kostenreduzierung einhergeht.

Fazit

Zusammenfassend kann eine Cloud-basierte DR-Strategie als echte Alternative angesehen werden. Dieser Ansatz ist insbesondere für Unternehmen interessant, die bisher aufgrund der hohen Kosten gänzlich auf eine DR-Strategie verzichtet haben. Für Unternehmen, die bereits für den Notfall gerüstet sind, stellt der turnusmäßige Austausch der Infrastruktur einen guten Einstiegspunkt dar. Um einen Einblick in das Cloud-basierte Disaster Recovery zu erhalten, bietet Apps Associates unter *„http://www.appsassociates.com/awslabs/dr-registration.php“* ein kostenloses Online-Praktikum zu diesem Thema an.

Sven Böttcher
sven.boettcher@appsassociates.com