Disaster Recovery in der Cloud

Sven Böttcher
Apps Associates
Dortmund

Schlüsselworte

Disaster Recovery, Cloud, Amazon Web Services

Einleitung

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 schnellst möglich wieder hergestellt 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 (Hardware und Software) können die verschiedensten Gründe haben. Häufig werden hiermit Naturkatastrophen oder schwere Gebäudebeschädigungen, z.B. durch einen Brand, in Verbindung gebracht. Während diese Ereignisse meistens zu den schwersten Schäden führen, sind die häufigsten Ausfallgründe menschliche Fehler1. 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-Infrastrukturausfall zunächst dazu, dass die täglichen Geschäftsprozesse in einem Unternehmen nur beeinträchtigt oder überhaupt nicht mehr durchgeführt werden können. Ein produktives Arbeiten ist damit zumeist nicht mehr möglich. Des Weiteren führt ein die IT-Infrastruktur betreffender Unglücksfall häufig zu einem Verlust von Daten. Je nach Unglücksfall und Unternehmen kann es so sowohl zu einem beträchtlichen monetären Schaden als auch zu einem Imageschaden 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 dabei, 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 (DR) Architekturen (vgl. Abbildung 1) die benötigte IT-Infrastruktur in der Regel an einem oder mehreren ausreichend räumlich getrennten Orten (Disaster Recovery 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 befinden sich die Hardware im DR-Rechenzentrum im Stand-By Modus. Eine Ausnahme bildet solche Hardware, die für die kontinuierliche Datensicherung benötigt wird. Im Notfall werden alle Komponenten im DR-Rechenzentrum hochgefahren, sodass diese die Aufgaben der lokalen IT-Infrastruktur übernehmen.

[1] Quelle: The Acronis Global Disaster Recovery Index: 2012

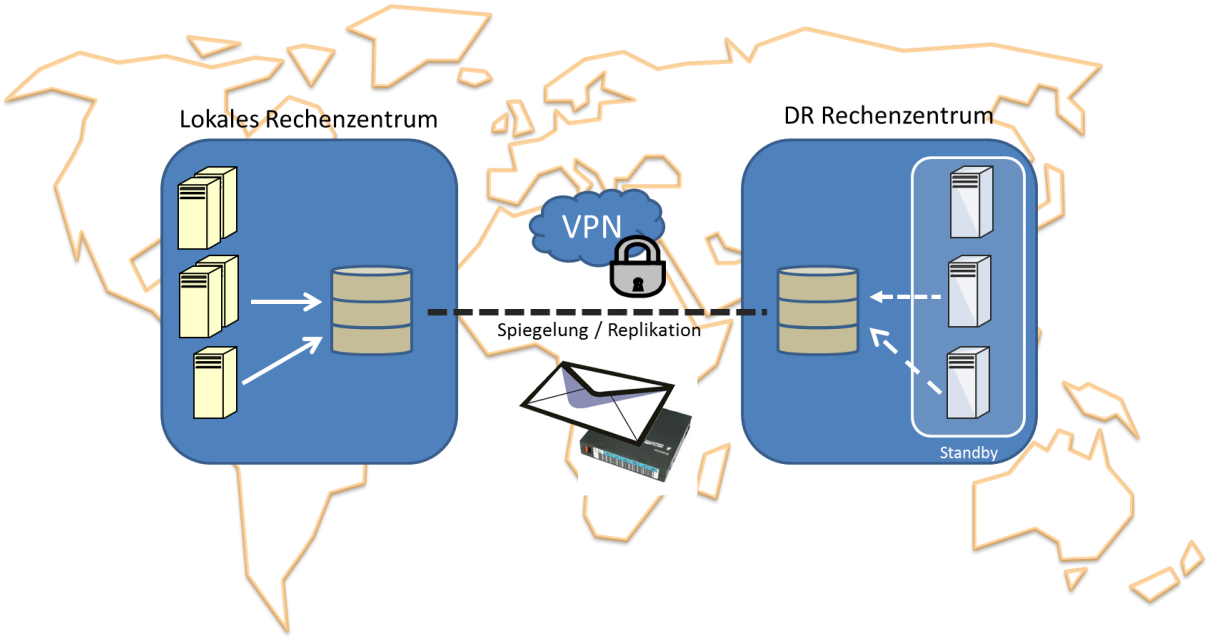

Abb 1: Traditionelle Disaster Recovery Architektur

Häufig wird aus Kostengründen jedoch für den Notfallbetrieb weniger bzw. nicht so leistungsfähige Hardware wie für den Regelbetrieb vorgehalten. Dies bedingt, dass die Geschäftsprozesse eines Unternehmens im Notfallbetrieb ggf. nur eingeschränkt ausgeführt werden 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, durch welchen viele der Probleme und Nachteile von traditionellen DR-Architekturen vermieden werden, stellt das Cloud Computing dar.

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 „der Cloud“ sind das Speichern von Fotos, Musik oder anderen Daten im World Wide Web. Solche Dienste werden vor allem im privaten Endanwenderbereich in Anspruch genommen. Zu den bekanntesten Cloud Diensten gehören Apples 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 im Allgemeinen zwischen den Dienst- bzw. 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 Softwarelizenz und die Installation der entsprechenden Software auf lokaler Hardware. Stattdessen wird im Allgemeinen vom Anbieter eine nutzungsbezogene Gebühr für die Inanspruchnahme der jeweiligen Software erhoben. IaaS Anbieter bieten dagegen komplette Infrastrukturdienste an, durch die es theoretisch möglich ist, gesamte

Rechenzentren in „die Cloud“ auszulagern. Auch hier erfolgt die Abrechnung im Allgemeinen nutzungsbezogen, so dass nur für die tatsächlich in Anspruch genommene Infrastruktur gezahlt werden muss (pay-per-use). Einer der größten IaaS Anbieter ist der Online-Versandhandel Amazon. Amazon bündelt die zur Verfügung gestellten IaaS Dienste unter dem Namen Amazon Web Services (AWS). Diese Dienste umfassen beispielsweise eine nach Kundenanforderungen anpassbare Rechenkapazität (Elastic Compute Cloud – EC2), eine Datenspeicherinfrastruktur zum Speichern beliebiger Daten (Simple Storage Service – S3) und einen Load Balancing Dienst. Über den EC2 Dienst lassen sich benötigte Rechenressourcen bedarfsgesteuert in sehr kurzer Zeit zur Verfügung stellen oder bestehende Ressourcen anpassen, wodurch sowohl eine horizontale als auch eine vertikale Skalierung erreicht werden kann. Letzteres ist sogar voll automatisch möglich. Gerade in Verbindung mit Cloud Diensten kommt immer wieder die Frage der Datensicherheit auf. AWS bietet hier zahlreiche Sicherheitsstandards, die für viele Unternehmen nur schwer oder nur mit einem hohen Aufwand realisiert werden können. Zum Beispiel befinden sich die AWS Rechenzentren grundsätzlich in unauffälligen Gebäuden, der Zugang zu den Gebäuden ist strikt reglementiert und es kommt eine mindestens zweimalige 2-Faktor-Authentifizierung zum Einsatz. Des Weiteren ist AWS nach verschiedenen Standards wie zum Beispiel ISO 27001,SOC 1, SOC2 und SOC3 zertifiziert. Zudem kann der Kunden 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, so dass auch hinsichtlich gesetzlicher Rahmenbedingungen das Cloud Computing eine echte Alternative zu lokaler Hardware darstellen kann.

Fallbeispiel Disaster Recovery in der Cloud

Das eine (Amazon) Cloud basierte Notfallwiederherstellung funktioniert, konnte Apps Associates bereits für ihren Kunden Passkey zeigen. Passkey2 ist ein führender Anbieter von webbasierten Hotelbuchungstechnologien für Gruppenveranstaltungen. Die implementierte DR-Architektur ist schematisch in Abbildung 2 dargestellt. Als wichtigste Infrastrukturkomponenten 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 Infrastrukturkomponenten wurden gleichermaßen in einem (von anderen AWS Kunden) isolierten Bereich in der Amazon Cloud eingerichtet. Dieser Bereich wird als Virtual Private Cloud (VPC) bezeichnet. Die Datenbank- und Applikationsserver befinden sich in einem privaten Subnetz, welches vor direkten Zugriffen über das Internet geschützt ist. Ein direkter Zugriff auf diese Komponenten ist lediglich von bestimmten IP-Adressen aus dem öffentlichen Subnetz der VPC und über eine VPN-Verbindung aus dem lokalen Rechenzentrum bzw. dem Firmennetzwerk möglich. Diese VPN Verbindung wird unter anderem für die Golden Gate basierte Datenbanksynchronisation verwendet. Im öffentlichen und über das Internet erreichbaren Subnetz wurden neben zwei Webservern eine Network Address Translation (NAT) Instanz sowie ein Monitoringdienst (Nimsoft) eingerichtet. Durch die NAT Instanz erhalten die Komponenten im privaten Subnetz 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. Diese Komponenten 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 (Abbildung 3). Jegliche Anfragen werden dann durch den Route 53 Dienst auf die Webserver in der Amazon Cloud weitergeleitet.

[2] Passkey wurde 2014 von Lanyon, einem führenden Anbieter für Meeting und Eventplanungssoftware, übernommen.

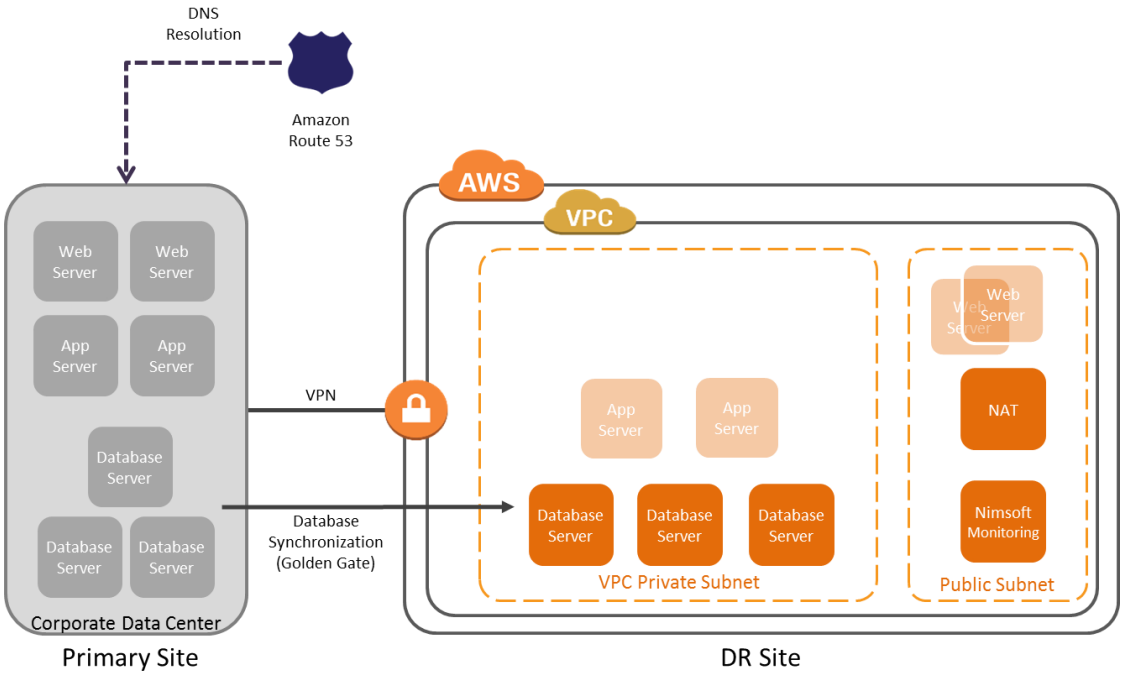

Abb 2: Lokale und DR-Infrastruktur in der AWS Cloud (Regelbetrieb)

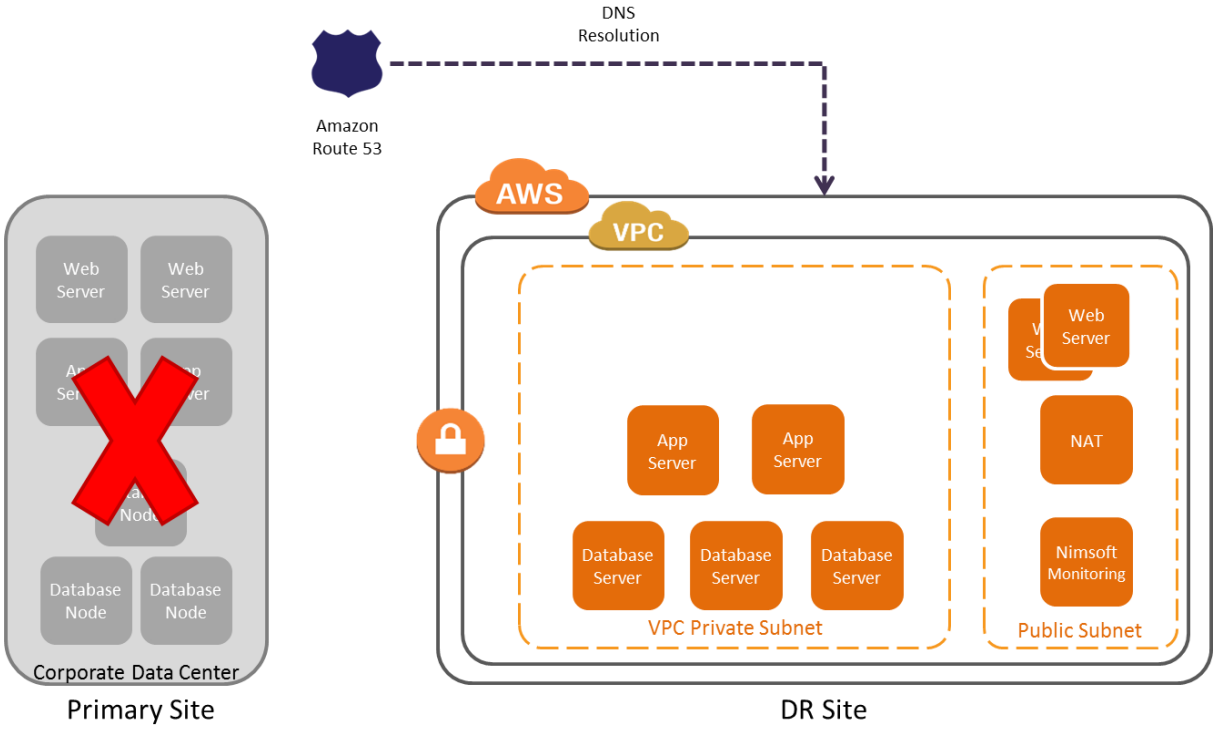

Abb 3: Lokale und DR-Infrastruktur in der AWS Cloud (Notfallbetrieb)

Gründe für ein Disaster Recovery in der Cloud

Einer der Hauptgründe, warum 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. Durch eine Cloud basierte DR-Strategie ist weder der Kauf der benötigten Hardware notwendig, noch muss ein Rechenzentrum für den Betrieb aufgebaut werden. Durch die bedarfsgesteuerte Bereitstellung der IT-Infrastruktur durch einen entsprechenden Anbieter reduzieren sich 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. Es fallen weder laufende Kosten für den Betrieb eines Rechenzentrums an, noch müssen beispielsweise kostenintensive Supportverträge für die zugrundeliegende Hardware abgeschlossen werden. Damit gewährleistet werden kann, 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. Dadurch wird ein effizienteres und auch häufigeres Testen der IT-Infrastruktur ermöglicht. Die oben erwähnten Kennzahlen RTO und RPO sind für die Planung einer DR-Strategie von zentraler Bedeutung. In traditionellen DR-Architekturen liegt das RTO häufig bei ein bis zwei Tagen und das RPO bei 24 bis 48 Stunden. Im Rahmen des oben dargestellten Fallbeispiels konnte gezeigt werden, dass ein RTO von 4 Stunden und ein RPO von weniger als 30 Minuten möglich ist. Entsprechend können im Ernstfall bei einer Cloud basierten Lösung die Geschäftsprozesse in einem Unternehmen deutlich schneller und bei einem geringeren Datenverlust wieder aufgenommen werden. Wie bereits beschrieben, wird für den Notfallbetrieb häufig nur Teil der im Regelbetrieb zur verfügungsstehenden IT-Infrastruktur vorgehalten. Dies führt dazu, dass im Notfallbetrieb unter Umständen mit Einschränkungen bei der täglichen Arbeit gerechnet werden muss, wodurch ggf. ein monetärer Nachteil entsteht. Durch die Skalierbarkeit von Cloud basierten Lösungen lassen sich Infrastrukturkomponenten bedarfsgesteuert hinzuschalten. Diese Eigenschaft wird häufig auch als „Elastizität“ bezeichnet. In Zeiten hoher Nachfrage können so zusätzliche und vorkonfigurierte IT-Infrastrukturkomponenten, wie Webserver oder Datenbankserver, eingeschaltet werden. Durch die pay-per-use basierten Dienste erhöhen sich die laufenden Kosten nur für diese Zeiträume. Sinkt die Anfrage wieder oder wird der Regelbetrieb wieder aufgenommen, können alle nicht benötigten Komponenten wieder abgeschaltet werden, was mit einer Kostenreduzierung einhergeht.

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 ersten Einblick in das Cloud basierte Disaster Recovery zu erhalten, bietet Apps Associates unter der Adresse http://www.appsassociates.com/awslabs/dr-registration.php ein kostenloses online Praktikum zu diesem Thema an.

Kontaktadresse:

Sven Böttcher

Apps Associates

Flughafenring ,11

44319 Dortmund

Telefon:	+49 (0) 231-2222 79 34
Fax:	+49 (0) 231-2222 79 79
E-Mail	sven.boettcher@appsassociates.com
Internet:	www.appsassociates.de