JUST DO IT
HÖHERE ABTEILUNG FÜR
INFORMATIONSTECHNOLOGIE

tgm
Die Schule der Technik

Ausarbeitung
Synchronisierung & Konsistenz

SYT
5BHIT 2015/16

Erik Brändli & Michael Weinberger

Version 1.0
Begonnen am 6. November 2015
Beendet am 23.02.2016

Inhaltsverzeichnis

1 Disaster Recovery

1.1 Grundlagen & Definitionen [1] [2] [3] [4] [5]

Disaster Recovery (dt. auch Katastrophenwiederherstellung), im Folgenden auch *DR* genannt, beschreibt die Vorbereitung und Reaktion auf sogenannte Katastrophen, die abgespeicherte Daten und Lauffähigkeit eines IT-Systems betreffen. In diesem Bereich der Sicherheitsplanung ist mit negativen Ereignissen all das gemeint, was den Betrieb eines Unternehmens gefährdet. Hierzu gehören Cyberattacken, Infrastrukturausfälle ebenso wie Naturkatastrophen. DR umfasst beispielsweise Schritte zur Wiederherstellung von Server oder Mainframes mit Backups oder ferner die Bereitstellung von LANs für die unmittelbaren geschäftlichen Bedürfnisse.

Anhand einiger Beispiele von Oxford Knowledge wird die Sinnhaftigkeit der Technologie bewiesen:

- 93% der befragten Firmen, die ihre Datenzentren für 10 oder mehr Tage aufgrund eines Desasters nicht erreichen konnten, mussten innerhalb eines Jahres nach dem erstmaligen Auftreten Konkurs anmelden.
- Im Vereinigten Königreich wurden 70% der befragten Firmen, die einen großen Datenverlust verzeichneten innerhalb von 18 Monaten geschlossen.
- 29% der befragten Firmen hatten bereits mit Systemausfällen und korrumpierten Daten zu tun.
- 52% der befragten Firmen wurden bereits Opfer einer (gelungenen/nicht gelungenen) Cyberattacke.

1.1.1 Disaster Recovery Plan

In dessen Folge dokumentiert ein Disaster Recovery Plan, im Folgenden auch DRP genannt, dann konkret Richtlinien, Verfahren und Maßnahmen, um die Störung eines Unternehmens im Falle eines Desasters zu begrenzen, und möglichst innerhalb eines bestimmten Zeitrahmens wieder zurück zum Normalzustand überzugehen. Wie bei einer Katastrophe macht das Ereignis die Fortführung des normalen Geschäftsbetriebs unmöglich. Genannter Plan sollte ein Teil eines jeden Standard-Projektmanagementsprozess sein.
Falls ein DRP besteht, kann das Unternehmen die Auswirkungen des Desasters minimieren und ihre geschäftskritischen Prozesse schnell fortführen. Die Disaster-Recovery-Planung beinhaltet in der Regel eine Analyse der Geschäftsprozesse und des Bedarfs. Sie kann auch einen Schwerpunkt zur Prävention beinhalten. Disaster Recovery ist ein wichtiger Aspekt von Enterprise-Computing. Die Unterbrechung des Dienstes oder der Verlust von Daten kann sich schwerwiegend auf die Finanzen auswirken, sei es direkt oder durch den etwaigen darauffolgenden Imageverlust.
Die internationale Norm für Sicherheitsmanagement erlangt immer mehr Aufmerksamkeit, da viele größere Organisationen ihre IT-Service-Provider **ISO27001**-konform machen.

1.1.2 Business Continuity

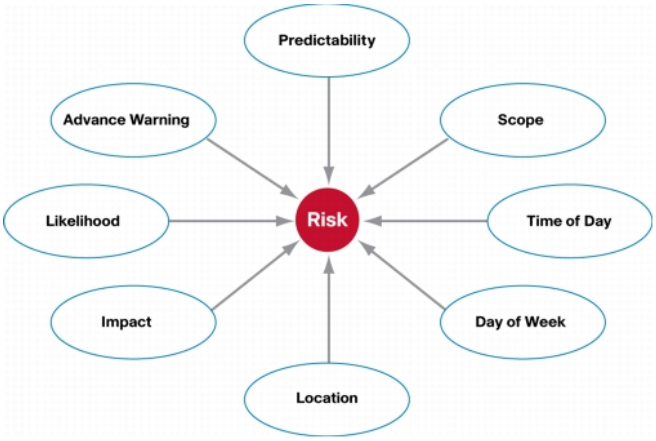
Business Continuity, dt. Betriebliches Kontinuitätsmanagement, beschreibt Prozesse und Verfahren eines Unternehmens, die die Weiterführung von wichtigen Geschäftsprozessen während und nach einem Desaster sichern sollen. Dabei liegt der Schwerpunkt mehr auf der Aufrechterhaltung der Geschäftstätigkeit als bei der Infrastruktur. Business Continuity und Disaster Recovery sind eng verbunden, sodass beide Begriffe manchmal kombiniert werden.
Die aufkommende internationale Norm für Business Continuity Management ist die **BS25999**.

1.1.3 Was ist eigentlich eine Katastrophe?

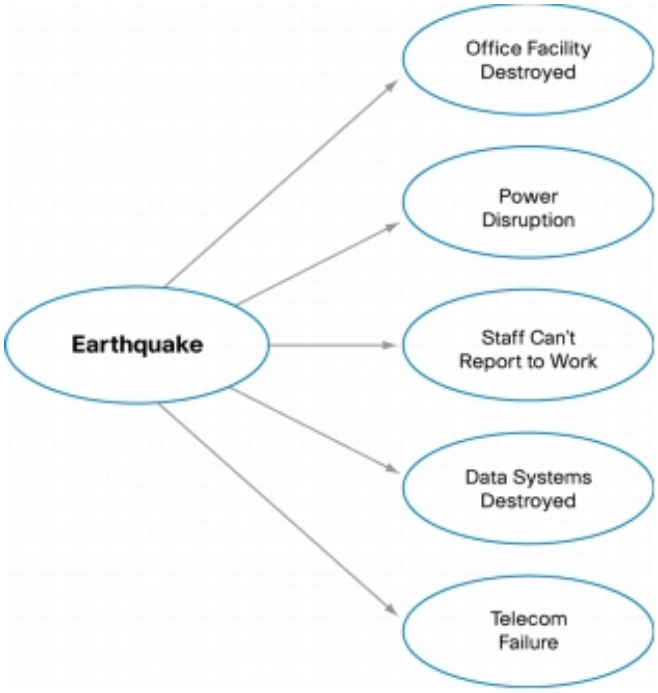
Wie bereits kurz erwähnt, eine Katastrophe kann vielerlei Ausmaß haben. Jede einzelne davon hat primäre und sekundäre Auswirkungen, die sich in direkte Schäden, korrumpierte oder unzugängliche Daten niederschlägt. Das eigene IT-Netzwerk ist verschiedensten Gefahren ausgesetzt, die in den schlimmsten Fällen auch ohne jegliche Vorwarnung auftreten können.
Einige Beispiele:

- Feuer, Brand im Serverraum, Wasserrohrbruch
- Sonstige Naturkatastrophen
  Sind ebenso zu berücksichtigen, speziell bei hoher Sicherheitsstufe!
- Sicherheitsprobleme, Viren, Cyberattacken, Datendiebstahl
- Hardware- und Softwareausfälle
- Stromausfall
- ...

Die Liste könnte noch weiter fortgeführt werden, wichtig ist, dass möglichst alle wichtigen und für die Umgebung relevanten Faktoren berücksichtigt werden. Kleinere Disaster treten immer häufiger bzw. mit einer größeren Wahrscheinlichkeit auf.
So fern es sich anhört, Naturkatastrophen haben wenn sie auftreten die verheerendste Auswirkung. Unter einer Aktiv/Aktiv-Konfiguration versteht man in diesem Zusammenhang, dass die so gesicherte Ressource, also zum Beispiel eine Datenbank, auf allen Clusterknoten aktiv ist. Wenn ein Knoten ausfällt, übernehmen die übrigen Knoten die Prozesse des ausgefallenen Knotens, es gibt praktisch keinerlei Ausfallzeiten, eventuell jedoch starke Einbußen in der Performance, da die gleiche Last nun von weniger Systemen übernommen werden muss.



(a) Risikofaktoren [9]



(b) Extrembeispiel Erdbeben [10]

Abbildung 1: Katastrophe & Auswirkung, Risikoabschätzung

1.1.4 Problem der Downtime, Kosten, max. Häufigkeit

Das Beispiel des Webblogs 'Interxion' zeigt mögliche Kosten bei einem internationaln Marktführer wie etwa Facebook:
Als Facebook am 1. August 2014 großteils nicht erreichbar war, riefen hunderte amerikanischer Nutzer ihren nächstgelegenen Polizeiposten an. Die Downtime dauerte zwar nur 20 Minuten, soll das Unternehmen aber immerhin 500.000$ gekostet haben. Berechnet hat dies "The Wireäufgrund der Werbeeinnahmen von Facebook, die im Jahr 2,91 Milliarden$ betragen – oder 22.453$ pro Minute. Es wird geschätzt, dass die wahren Kosten eines solchen Ausfalls weit höher liegen. Heikel dabei ist der Ruf des Unternehmens: Nicht nur Nutzer, auch diejenigen, die den Dienst finanzieren – die Werbetreibenden – bauen auf dessen Zuverlässigkeit. Jeder Nutzer, der wegen einer Downtime Facebook unfreiwilig den Rücken kehrt, bedeutet für die Werber ein verlorenes Mitglied ihrer Zielgruppe. In einer aktuellen Studie schätzen Unternehmen ihre Kosten für eine Stunde Ausfallzeit auf mindestens 20.000 $, 20% der Unternehmen auf über 100.000 $. Natürlich spielt es eine Rolle, in welcher Branche das Unternehmen tätig ist, und wieviele Zugriffe auf Ihre Services erfolgen. Die Kostenberechnung für eine Server-Downtime ist ein komplexes Unterfangen – nur den Verlust der Werbeinnahmen in Betracht zu ziehen, wie es im Fall Facebook gemacht wurde, greift sicher noch zu wenig weit.

1.1.5 Fehlertoleranz

Jeder, der mit IT-Systemen arbeitet wurde auch schon Zeuge eines Ausfalls einer Komponente oder eines Service, wichtig ist auch, auf den Begriff Fehlertoleranz zu achten. *Fehlertoleranz* ist die Möglichkeit des Systems, selbstständig und automatisch auf verschiedenste Bedingungen zu reagieren und dementsprechend auszugleichen. Durch das selbsständige Vorgehen reduziert die Fehlertoleranz die Auswirkungen auf das System. Das System, das Programm, der Prozess wird weiterlaufen, vollkommen unbewusst, das ein Problem aufgetreten ist. Abhängig des Fehlertoleranzgrads des eingesetzten Systems müsste ein DRP in der Theorie gar nicht nötig sein, die Praxis spiegelt jedoch ein anderes Bild wieder. Wichtige Systeme haben einen höheren Fehlertoleranzgrad als weniger wichtige, wo nicht jeder Fehler zu einem schwerwiegenden Problem werden darf. Hohe Fehlertoleranz ist jedoch auch mit hohen Kosten verbunden.

1.2 Aufstellen eines DRP [6]

Ein Disaster Recovery Plan muss Desasteridentifikation, Kommunikationsrichtlinien, das Koordinieren der Prozesse, etwaige Ausweichmöglichkeiten, Prozesse, um so schnel wie möglich wieder zum Normalzustand zurückzukehren und einen Feldtest des Plans sowie Wartungsroutinen beinhalten. Es muss kurz ein funktioneller Plan sein, der alle Prozessketten richtig adressiert, um die Systeme wiederherzustellen, inkl. eines Zuständigen zur stetigen Wartung des Plans. Es empfiehlt sich außerdem ein eigenes Disaster Response-Team auszuweisen, abhängig von den gegebenen Anforderungen. Wenn der Plan entworfen wird, ist es wichtig eine Priorisierung aufzustellen, welche Infrastruktur bzw. Systeme für den Erhalt der Einsatzfähigkeit zwingend nötig sind. Ein erstes Maß ist die Wiederherstellung der voraussetzenden Umgebungen, etwa ein funktionierendes internes Netzwerk. Ein zweiter Punkt ist die auferlegte nötige Uptime für jedes System. Diejenigen, die eine 24/7-Uptime erreichen sollen sind den weniger prioren vorzuziehen. Es ist auch zu bedenken, dass bestimmte Workarounds effektiv laufen sollen, ohne noch größere Probleme zu verursachen. Der Ersteller des Plans muss möglichst viele Daten sammeln über alle verwendeten Systeme, sowie Abhängigkeiten untereinander abbilden und miteinander in Konflikt stehende, gleichrangige Priorisierungen klären. Ein DRP wird nicht automatisch ausgeführt, sondern händisch, angepasst an den Bedarfsfall.

1.3 Schaffung eines zuverlässigen Systems [7]

1.3.1 Clustersysteme und deren Vorteile

Wenn Systeme 24/7 verfügbar sein müssen, wird oft eine Clusterlösung herangezogen. Hier unterscheidet man zwischen zwei Varianten, Failover-Clustering und 'echtem' Clustering. Bei der Failover-Technologie mit zwei oder mehreren Netzwerkdiensten übernimmt ein Zweitsystem bei einseitigem Ausfall des Primärsystems. Echtes Clustering, sprich ein Aktiv/Aktiv-Cluster, wird bezeichnet einen Rechnerverbund, in dem mehrere (meistens > 2) Nodes gleichzeitig aktiv sind. Computercluster werden neben der Verteilung der Rechenleistung auch u. a. zur Sicherstellung der Verfügbarkeit von diversen Ressourcen wie Netzwerke, Applikationen etc. verwendet. Unter einer Aktiv/Aktiv-Konfiguration versteht man in diesem Zusammenhang, dass die so gesicherte Ressource, also zum Beispiel eine Datenbank, auf allen Clusterknoten aktiv ist. Beide Herange-

hensweisen beinhalten keinen DRP. Da sie "100% der Zeit"verfügbar sind (aus Sicht des Kunden), gibt es per se keine Katastrophen, die die Business Continuity beeinträchtigen. Der einzige Nachteil: Solche Lösungen sind meistens sehr teuer in Aufbau und Wartung, und daher eher nur von großen Unternehmen mit großem Budget zu bewerkstelligen.

1.3.2 Wieso dann DR?

Für Systeme, die keine 100%-ige Verfügbarkeit benötigen, oder das Budget es nicht anders vorsieht, ist DR die bessere Wahl. Eine typische Lösung ist es ein identes System aufzubauen, es für etwaige Einsatzfälle zu warten und es als Failover zu verwenden. Der Wechsel auf dieses System verlangt einen Eingriff des Administrators, während dieser Zeit bis zur Inbetriebnahme 'steht der Betrieb'. Die Rückkehr auf den Normalzustand kann mithilfe dieser Methode relativ schnell wiedererlangt werden, und generiert weniger Kosten als eine vollständige Cluster-Lösung.
Die billigste Variante (aus Hardware-Sicht) ist es auf Fehler zu reagieren, nachdem sie passiert sind. Hier wird das gesamte System heruntergefahren bis der Fehler ausgebessert ist, der Betrieb kann nicht fortgeführt werden. Wenn z.B. die Festplatte ausfällt, steht die gesamte Infrastruktur still, bis einzig und allein die kaputte Festplatte ausgetauscht ist. Systemadministratoren können wie erwähnt Katastrophen nicht vollständig verhindern - sie können jedoch bestimmte Wahrscheinlichkeiten verringern und mit einem guten DRP komplette Wiederherstellungen gewährleisten mit einem Minimum an Zeit in einem geordneten Prozess.
Der Grad einer guten Absicherung hängt wie gesagt auch mit en Finanzen zusammen, in eine unterbrechungsfreie Stromversorgung (USV) sollte auf jeden Fall investiert werden. Die USV hält die Infrastruktur lang genug am Leben, um Files zu speichern und die Server sicher herunterzufahren, ein Strom-Backup ist wohl für kein System unwichtig. Fehlende Elektrizität ist nämlich die wohl wichtigste, weil häufigste Fehlerursache.
Eine regelmäßige Backup-Routine (täglich, wenn nicht sogar mehr) ist der Schlüssel zu einer erfolgreichen Katastrophenwiederherstellung. Ein Teil der Backups sollte an einem sicheren Platz abgelegt sein, wenn möglich außerhalb des eigenen Infrastruktur-Netzes.
Auch Redundanz spielt eine tragende Rolle beim Aufbau eines zuverlässigen Systems. Gute DR-Pläne sehen nicht vor, dass wichtige Daten jediglich auf einer Maschine liegen. Ohne diese Maßnahme wäre es nicht möglich, einen Failover-Server mit einer Kopie der kritischen Daten bereitzustellen. *RAID* (Redundant Array Of Independent Disks) ist eine gute Lösung, um dem entgegenzuwirken. Hier haben, je nach Modus, mehrere Festplatten dieselben Daten. RAID ist ein zuverlässiger Schutz bei Datenträgerausfall, der ja bekanntlich eine 100%-ige Wahrscheinlichkeit mit sich bringt. Die besten Umsetzungen erlauben sogar Hot-Swapping, damit ein Ersatz eingefügt werden kann, ohne dass das System eine Downtime erleidet. RAID bietet auch einen schnelleren Zugriff auf Daten, macht es u. a. effizient für Fileserver.

1.4 Disaster Recovery: Techniken [8] [11]

1.4.1 Traditional Disaster Recovery

SHARE ist ein ehrenamtlicher Userzusammenschluss mit Fokus auf IBM-Systeme und -Technologien, und wurde bereits im Jahr 1955 gegründet. SHARE hat ursprünglich die *Seven tiers of disaster recovery* definiert, um verschiedene Herangehensweisen zu beschreiben, um eben auftragskritische Computersysteme wiederherzustellen, und wurde darin auch von IBM selbst unterstützt. Obwohl

das Originalkonzept bis in die späten 1980er-Jahre zurückreicht, verwenden DRP-Experten diesen Ansatz bis heute sehr häufig (Stand: Dez. 2015), um Möglichkeiten und Kosten darzustellen. Natürlich wurden die genauen Definitionen dementsprechend angepasst, um heutigen Standards besser zu entsprechen.
Das SHARE Technical Steering Committee in Zusammenarbeit mit IBM hat die Stufen (Tiers) auf die Zahlen 0 bis 6 festgelegt. Durch den technischen Fortschritt der vergangenen Jahrzehnte wurde eben eine 7. Stufe hinzugefügt, die mehrere auch geographisch voneinander unabhängige Systeme berücksichtigt, welches das höchste Maß an Verfügbarkeit darstellt.

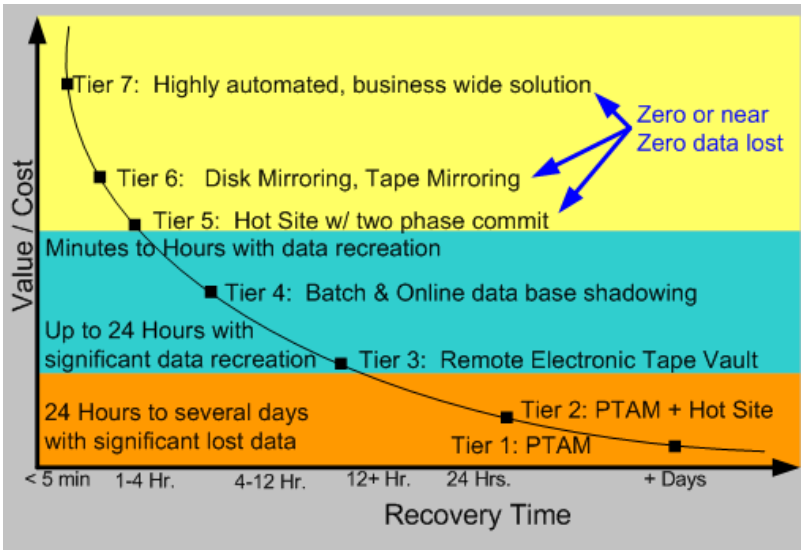


Abbildung 2: Seven tiers of disaster recovery [12]

- Tier 0: No off-site data – Possibly no recovery
  Unternehmen mit einer Tier 0-Lösung haben keinen Disaster Recovery Plan. Sie haben keine gespeicherten Informationen über das System, keine Dokumentation und auch keine Backups. Die Zeit, die benötigt wird um ein solches System wiederherzustellen ist unvorhersehbar, es kann sogar sein, dass es unmöglich ist zum Normalzustand zurückzukehren.

- Tier 1: Data backup with no hot site
  Tier 1-Systeme erhalten regelmäßig ein Backup, und lagern diese an einem sicheren Ort, der sich außerhalb des eigenen Hauses (der eigenen Infrastruktur) befindet. Dies ist notwendig, da vor einem Desaster auch Backups mit lokalem, nicht redundanten Speicherort nicht sicher sind. Diese Methode Backups zu transportieren heißt PTAM, ausgeschrieben 'Pick-up Truck Access Method'. Sprich, das Backup ist so schnell greifbar, wie der Transport vom Aufbewahrungsort dauert. Abhängig davon, wie oft Sicherungen gemacht und versendet werden müssen Unternehmen einige Tage bzw. Wochen Datenverlust inkaufnehmen, dafür sind die Sicherungsdateien geschützt außerhalb des Geländes aufbewahrt.

- Tier 2: Data backup with a hot site
  Bei Verwendung von Tier 2 werden ebenso regelmäßige Sicherungen vorgenommen, auf langlebigen Speichermedien wie etwa Tapes. Das wird kombiniert mit eigener Infrastruktur außerhalb des eigenen Geländes (genannt 'Hot Side'), von welchen die Backups rückgelesen

werden im Falle eines Desasters. Diese Lösung benötigt immer noch einige Stunden oder Tage zur Wiederherstellung, jedoch ist die Gesamtdauer besser vorhersehbar.

- Tier 3: Electronic vaulting
  Der Ansatz Tier 3 baut auf Tier 2 auf. Hinzufügend dazu werden kritische Daten elektronisch abgekapselt von den weniger prioren. Die Abgekapselten sind üblicherweise aktueller als die Daten, die via PTAM abgelegt werden. Als Ergebnis ist hier weniger Dateiverlust, sollte eine Katastrophe eintreten.
  Einrichtungen, die 'Electronic Remote Vaulting' bereitstellen, verfügen über Hochgeschwindigkeitsanbindungen und entweder physische oder virtuelle Sicherheitstape-Lesegeräte, mit automatisierter Sicherungsbibliothek beim entfernten Standort.
  Als praktischen Beispiel zur Implementierung dienen IBMs Peer-to-Peer TotalStorage Virtual Tape Server oder Oracles VMS Clustering.

- Tier 4: Point-in-time copies Tier 4-Lösungen werden oft von Unternehmen verwendet, die hohen Wert auf Datenkorrektheit und schneller Wiederherstellung legen als die unteren Stufen bereitstellen. Eher als das Auslagern von Speichertapes wie bei 0-3 gegeben, integriert diese Stufe Sicherungen auf Basis von Disks (also Festplatten). Immer noch sind mehrere Stunden Datenverlust möglich, jedoch ist es einfacher, point-in-time-Kopien (PiT, jeweils zu einem festgelegten Zeitpunkt)

1.4.2 Disaster Recovery as a service

1.4.3 Beispiel MySQL

Literaturverzeichnis

[1] Peter Gregory. *IT Disaster Recovery Planning for Dummies*. Wiley Publishing, Inc., 2008.

[2] Tech Target. Definition disaster recovery (dr). `http://www.searchsecurity.de/definition/Disaster-Recovery-DR`. zuletzt besucht: 24.02.2016.

[3] Tech Target. Definition disaster recovery plan (drp). `http://www.searchsecurity.de/definition/Disaster-Recovery-Plan-DRP`. zuletzt besucht: 24.02.2016.

[4] Oxford Knowledge. Backup and disaster recovery. `http://www.oxford-knowledge.com/services/it-projects-consultancy/backup-disaster-recovery/#.Vs0h2PnhCUk`. zuletzt besucht: 23.02.2016.

[5] Interxion. Server-downtime – kosten fuer unternehmen. `http://www.interxion.com/ch/blog/server-downtime--kosten-fur-unternehmen/`. zuletzt besucht: 23.02.2016.

[6] John R. Vacca. *Computer and Information Security Handbook*. Morgan Kaufmann, 2009.

[7] Terry Collings/Kurt Wall. *Red Hat Linux Networking and System Administration - Third Edition*. Wiley Publishing, Inc., 2005.

[8] International Journal of Innovative Research in Computer and Communication Engineering. Vol. 1, issue 6, august 2013. `http://ijircce.com/upload/2013/august/8_A%20Study.pdf`. zuletzt besucht: 23.02.2016.

[9] Cisco. Risikofaktoren. `http://www.cisco.com/en/US/technologies/collateral/tk869/tk769/images/white_paper_c11-453495-2.jpg`. zuletzt besucht: 23.02.2016.

[10] Cisco. Erdbeben. `http://www.cisco.com/en/US/technologies/collateral/tk869/tk769/images/white_paper_c11-453495-3.jpg`. zuletzt besucht: 23.02.2016.

[11] LLC Recovery Specialties. Business continuity: The 7-tiers of disaster recovery. `http://recoveryspecialties.com/7-tiers.html`. zuletzt besucht: 23.02.2016.

[12] LLC Recovery Specialties. Business continuity: The 7-tiers of disaster recovery. `http://recoveryspecialties.com/images/7-tier%20of%20DR%20generic.gif`. zuletzt besucht: 23.02.2016.

Abbildungsverzeichnis