**Überblick**

Um Disaster Recovery zu verstehen, benötigt man einiges an Theorie. Da das Thema u.a. im Projektmanagement beheimatet ist, ist sehr viel eher beschreiben als praktisch.

**Grundlagen & Definitionen**

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 Servern** oder ferner die **Bereitstellung** von **Infrastruktur** für die **rasche Wiederaufnahme** der Geschätsfähigkeit.

Beispiele, wieso das ganze?:

93% der Firmen, Datenzentren Ausfall 10 oder mehr Tage mussten innerhalb 1 Jahr Konkurs anmelden.

UK, 70% der Firmen mit großem Datenverlust mussten innerhalb von 18 Monaten zusperren

**Disaster Recovery Plan**

In dessen Folge dokumentiert ein **Disaster Recovery Plan** 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. Eine **Katastrophe** macht den **Geschäftsbetrieb** **unmöglich**. Genannter **Plan sollte ein Teil** eines jeden **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.

**Business Continuity**

**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**.

**Was ist eigentlich eine Katastrophe?**

Kann vielerlei Ausmaß haben, jede davon **primäre und sekundäre** Auswirkungen, schlägt sich nieder in direkte Schäden, korrumpierte oder unzugängliche Daten. Das eigene IT-Netzwerk ist **verschiedensten Gefahren** ausgesetzt, in den schlimmsten **Fällen ohne jegliche Vorwarnung**

Das kann sein: Feuer, Wasserrohrbruch, Naturkatastrophen (besonder bei hoher Sicherheitsstufe!) Sicherheitsprobleme, Viren, Cyberattacken, Datendiebstahl, SW- und HW-Ausfälle, Stromausfall

**Alle für die Umgebung wichtigen Faktoren** müssen berücksichtigt werden. **Kleinere** Disaster treten immer **häufiger** bzw. mit einer **größeren Wahrscheinlichkeit** auf. **Naturkatastrophen** haben wenn sie auftreten die **verheerendste** Auswirkung.

Grafik, Risikoanalyse, alle Faktoren spielen eine Rolle, Extrembeispiel Erdbeben, Ansicht, was alles passieren kann

**Problem der Downtime, Kosten, max. Häufigkeit**

Beispiel Facebook 1. August 2014 großteils nicht erreichbar, hunderte amerikanische Nutzer riefen Polizei an. Downtime von knapp **20 Minuten** soll eine **halbe Million Dollar** gekostet haben. Dies wurde aus den Werbeeinnahmen berechnet, die einen Profit von immerhin 22.000 $ pro Minute ausmachen. Die **geschätzten Kosten** eine solchen Ausfalls liegen jedoch weit höher. Heikel ist auch der Ruf des Unternehmens, **Nutzer und Werbetreibende** **bauen auf dessen Zuverlässigkeit**. Jeder User, der nicht darafu zugreifen kann bedeutet ein verlorenes Mitglied der 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**, spiegeln jedoch wider,wieso **Disaster Recovery,** oder im **weitesten Sinne Hochverfügbarkeit** an sich **so wichtig** ist.

**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**, wo **nicht jeder Fehler** zu einem **schwerwiegenden Problem** werden darf, **hohe Toleranz** hat jedoch auch **hohe Kosten**.

**Aufstellen eines DRP**

Ein Disaster Recovery Plan muss **Desasteridentifikation, Kommunikationsrichtlinien, das Koordinieren der Prozesse**, etwaige **Ausweichmöglichkeiten**, Prozesse, um **so schnel wie möglich** wieder zum **Normalzustand** zurückzukehren. Es empfiehlt sich außerdem ein eigenes Disaster Response-Team auszuweisen. 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 (24/7, oder weniger?). 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.

**Cluster und deren Vorteile**

Wenn Systeme 24/7 verfügbar sein müssen, wird oft eine Clusterlösung herangezogen, welche sich in **2 Kategorien** teilt. 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**.** Es gibt es **in der Theorie 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.s

**Wieso 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.

**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.

Auf jeden Fall sollte in eine Unterbrechungsfreie Stromversorgung (USV) investiert werden**. Fehlende Elektrizität** ist nämlich die wohl wichtigste, weil **häufigste** Fehlerursache. Die USV hält die Infrastruktur **lang genug am Leben**, um Files zu **speichern** und die Server **sicher herunterzufahren**

Eine regelmäßige Backup-Routine (täglich oder mehr) gewährleistet erfolgreiche Katastrophenwiederherstellung, Teil des Backups sollte außerhalb des eigenen Netzes aufbewahrt werden.

Redundanz 🡪 **RAID**, ist ein zuverlässiger Schutz bei Datenträgerausfall   
Die besten Umsetzungen erlauben sogar **Hot-Swapping**, damit ein **Ersatz** eingefügt werden kann, **ohne** dass das System eine **Downtime** erleidet. RAID bietet auch einen schnellen Zugriff auf Daten

**Traditional Disaster Recovery**

Stufensystem, von Userzusammenschluss **SHARE** bzw. IBM gefestigt und etabliert. Reicht zurück bis in die späten 1980-er Jahre, ist in überarbeiteter Form (Stufe 7 nachträglich) gültig bis heute.

**Tier 0**

Haben keinen Disaster Recovery Plan, **keine Backups**, Zeit um wiederherzustellen **unvorhersehbar**, wenn nicht sogar **unmöglich**

**Tier 1**

Erhalten **regelmäßiges Backup**, lagern diese an einem **sicheren Ort**, der sich **außerhalb** des eigenen **Hauses**. 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**

Ebenso **regelmäßige** Sicherungen**, langlebige Speichermedien** wie z.B. **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**

Baut auf Tier 2 auf, hinzufügend dazu werden **kritische Daten elektronisch abgekapselt.** Die **Abgekapselten** sind üblicherweise **aktueller** **als** die Daten, die via **PTAM** abgelegt werden. Als Ergebnis ist hier **weniger Dateiverlust  
Beispiel zur Implementierung:**    
IBMs Peer-to-Peer TotalStorage Virtual Tape Server oder Oracles VMS Clustering

**Tier 4**Hoher Wert auf **Datenkorrektheit** und **schnellerer Wiederherstellung**. Statt Auslagern von Tapes werden **vorranging Disks** als Sicherungsmedium verwendet. Immer noch sind **mehrere Stunden Datenverlust** möglich, jedoch ist es **einfacher** jeweils zu einem **festgelegten Zeitpunkt** **Backups** zu **erstellen** als Tape-Sicherungen, sogar wenn elektronisch gekapselt.

**Tier 5**

Tier 5 wird verwendet, wenn es **zwingend erforderlich** ist, dass **Daten** **konsistent** sind zwischen Produktivsystem und dem Wiederherstellungs-Remoteserver. Bei einem solchen Aufbau kommt es **zu kaum bis gar keinem Datenverlust**, aber die Verfügbarkeit dieser **Funktionalität** ist **stark abhängig** von der verwendeten **Implementierung**.

**Tier 6**

Tier 6 hält das **höchste Maß an Datenrichtigkeit** aufrecht. Dieser Ansatz wird eingesetzt von **Systemen**, in denen **wenig oder gar kein Datenverlust vertretbar** ist, und wo **Daten** für den **weiteren** **Gebrauch** **schnell wiederhergesellt** werden müssen. Tier 6 erfordert eine Form von Disk Mirroring zu einem Remoteserver, hierfür gibt es verschiedenste synchrone oder asynchrone Implementierungen von namhaften Herstellern.

**Tier 7**

Übernimmt **Tier 6, Automatisierung**  
**Datenkonsistenz**, die bei Tier 6 gegeben ist. Desaster werden **automatisch erkannt** von Geräten **außerhalb** des eigenen **Computersystems**.  
Außerdem wird die **Wiederherstellung automatisch ausgeführt**, was sozusagen den kompletten Wiederherstellungsprozess bei System und Anwendungen **beschleunigt**, und diese **schneller** und **zuverlässiger** laufen lässt **als** es überhaupt möglich wäre durch **händische** Prozeduren. Die Ausfälle belaufen sich auf **wenige Minuten oder Sekunden**.

***OPTIONAL***

((((((

**Recovery Objectives**

*Evaluierung nach RTO/RPO*

Recovery Time Object 🡪 Wann Funktion spätestens wiederhergestellt sein sollen

Recovery Point Objective 🡪 Zeit, die es maximal brauchen darf, bis genug Daten wiederhergestellt sind, um den Unternehmensprozess fortführen zu lassen.

Es sind **viele Lösungen** verfügbar, die **richtige** auszuwählen **bedarf** einer **Kosteneinschätzung** sowie auch hier die **vertretbare Downtime** und das **Maß an Datenverlust** abzuwägen.   
Es gibt keine Eine-für-alle-Lösung, der beste Ansatz ist vielleicht eine Mischung der oben genannten Stufen. Auf diesem Wege kann günstig das richtige Level an Schutz umgesetzt werden.

)))))

**DraaS**

Oft auch nur **Recovery as a service** genannt, ist DRaaS eine **Unterkategorie des Cloud Computings** und eine **zuverlässige Form des Disaster Recovery**. Es **grenzt** sich von **cloudbasierten** **Backups** ab, indem es auch **bestimmte Daten schützt** und **auf Abruf Rechenkapazität** bereitstellt, um die Wiederherstellung zu **beschleunigen** und als **Failover** zu dienen. Als Teil des Cloud Computing-Modells folgt es dem Prinzip, dass **nur das bezahlt** werden muss, was man auch verwendet hat. Damit kommt klar der Vortei zu tragen, dass traditionelle **’Warm Site’**- oder **’Hot Site’**-Aufbauten **wesentlich ineffizienter** sind, da **sie ständig laufen** und **bezahlt** werden müssen.  
Es gibt auch die **Sandboxes**, wo die komplette Funktionalität getrennt vom Netzwerk überprüft werden kann.

**Architektur**

To-Cloud RaaS 🡪 Die **Zielanwendung** befindet sich im **privaten** Datencenter, und die **Cloud** wird als **Backup- und Recovery-Target** verwendet.

In-Cloud RaaS 🡪 Bedeutet, dass sowohl **Zielanwendung** **als auch Recovery-Sites** in der **Cloud** angesiedelt sind

From-Cloud RaaS 🡪 Die **Primärdaten** liegen in der **Cloud**, und das **Backup-Target** liegt im **privaten** Datencenter.

**Namhafte Anbieter:**

**Vmware, Zerto, Amazon AWS, Bluelock, Microsoft Azure,** **Preis** selbst verhandelbar nach Größe!