JUST DO IT
HÖHERE ABTEILUNG FÜR
INFORMATIONSTECHNOLOGIE

tgm
Die Schule der Technik

Ausarbeitung

Synchronisierung & Konsistenz

SYT
5BHIT 2015/16

Erik Brändli & Michael Weinberger

Version 0.1
Begonnen am 6. November 2015
Beendet am ??.??.2016

Inhaltsverzeichnis

1 Disaster Recovery

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

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.
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.

 Erik Brändli & Michael Weinberger

1.1.2 Business Continuity

Business Continuity 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, so dass beide Begriffe manchmal kombiniert werden.
Die aufkommende internationale Norm für Business Continuity Management ist die **BS25999**.

1.1.3 Arten von Katastrophen

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.
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.

1.1.4 Problem der Downtime, Kosten, max. Häufigkeit

1.2 Aufstellen eines DRP

1.2.1 Vorbereitende Schritte

1.2.2 Datenanalyse, Risikoanalyse

1.3 Schaffung eines zuverlässigen Systems

1.4 Disaster Recovery-Techniken

 Erik Brändli & Michael Weinberger

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 disaster recovery. `http://www.oxford-knowledge.com/services/it-projects-consultancy/backup-disaster-recovery/#.Vs0h2PnhCUk`. zuletzt besucht: 24.02.2016.

Listings

Abbildungsverzeichnis

 Erik Brändli & Michael Weinberger