DR-Konzept Detailanalyse

Übersicht

Das folgende Schema soll eine Hilfestellung bei Erstellung eines Desaster Recovery Konzept für ein kleines oder mittleres Unternehmen bieten. Die konzeptionellen Grundlagen für diese Vorgehensweise finden sich auf http://sicherheitskultur.at/Notfallplanung.htm

---

Betrachtete Szenarien:

1. Ausfall von einer oder mehrerer Komponenten im Rechnerraum (z.B. auch Switches, etc.)
2. Ausfall oder Verlust des gesamten Rechnerraums (z.B. durch Wassereinbruch)
3. Gebäude kann nicht betreten werden oder ist verloren (z.B. durch Feuer, Wasser, Quarantäne oder Sicherheitsmaßnahme nach Straßenunfall)

Verfügbarkeitsanforderungen in Bezug auf Arbeitsplätze für Szenarien 2 und 3

Wie viele Mitarbeiter aus jeder Abteilung müssen nach welcher Zeit wieder arbeiten können?
(die Antwort darauf bestimmt die Anforderungen bzgl. Zahl alternativer Arbeitsplätze, aber auch vieler anderer Kapazitäten, wie z.B. Zahl der nötigen Kapazitäten der (Ersatz-)Server)

Abteilung, Funktion	Nach 1 Tag	Bereits möglich	3 Tage	1 Woche	1 Monat

A. Anwendungen (Pro Standort der betrachtet werden soll)

(die vorgegebenen Antworten in „Details“ geben nur Beispiel an, die oft auftreten und die berücksichtigt werden sollten. Diese Antworten müssen in jedem Unternehmen individuell recherchiert werden)

System / Anwendung	RTO[1]	RPO[2]	Details	To do
Warenwirtschaftssystem, Lagerhaltung	1 d	minimal	Abhängig von DB- Server, Remotezugriff von außen?	
EDI-SW	2 w		Kann weitgehend durch Fax erledigt werden	
CAD-System	3 d	1d	Abhängig von Fileservern, evtl. offline möglich, Datenverfügbarkeit und andere Voraussetzungen prüfen	
MIS	1 w		Abhängig von DB- Server, Remotezugriff von außen?	
Zeiterfassung	> 1 w	1 d	Unkritisch, Einfluss auf Gehaltszahlungen ?	
Personal Informationssystem	> 1 w		Abhängig von DB- Server, Remotezugriff von außen?	
Gehalt	> 1 w			
Bank (MBS)-System	> 1 w	1 d		

[1] **RTO:** (Recovery Time Objective) maximale Zeit vom Eintritt des Ausfalls bis zur Wiederaufnahme des Betriebs

[2] **RPO:** (Recovery Point Objective) maximaler zeitlicher Abstand zwischen letzter gesicherter Transaktion vor einem Ausfall und dem Ausfall (d.h. tolerierter Datenverlust)

B. Basis-Infrastruktur (pro Standort der betrachtet werden soll)

(die DR-Anforderungen an die Basis-Infrastruktur ergeben sich u.a. aus den DR-Anforderungen für die Business-Anwendungen, die von dieser Infrastruktur abhängen. Die vorgegebenen Antworten in „Details“ geben nur Beispiel an, die oft auftreten und die berücksichtigt werden sollten. Diese Antworten müssen in jedem Unternehmen individuell recherchiert werden)

System / Anwendung	RTO	RPO	Details	To do
Telefonanlage	2 d	N/A	Alternative Routing-Lösungen (z.B. zu Handys) sind zusammen mit dem Provider zu untersuchen. Dabei ist zu unterscheiden zwischen Fall a) nur dieses Unternehmen betroffen und b) Ausfall des Verteilers des Providers	
Fax		N/A	Faxserver, Faxgeräte. Eingang und Ausgang separat betrachten. Alternative Software-Lösungen per Software auf Laptop sind zu untersuchen. Alternative Routing-Lösungen sind mit Provider zu klären	
Internes Netz (Router, Switches, etc.)	< 1 h f. Server-zugriff Szen. 1 ½ d f. Arbeitspl. Szen. 1	N/A	Szenario 1: Priorität 1 ist der Zugriff der Außenstellen auf Anwendungen und für den Fluss von Email. Für die Vernetzung der Server und lokalen Workstations muss ein Konzept vorliegen, das entweder Redundanzen oder eine schnelle Wiederherstellung in Fällen eines einzelnen Geräteausfalls ermöglichen würde. Die Angaben links gelten für dieses Szenario. Szenario 2 u. 3: für diesen Fall ist zu entscheiden ist auch, wie eine reduzierte Konfiguration aussehen könnte. Serverzugriff ist bei diesen Szenarien nach 1 d, Arbeitsplätze siehe separate Tabelle	
Alternative Arbeitsplätze für Szenario 3	Siehe separate Tabelle	N/A	Dies beinhaltet Arbeiten von zu Hause oder in einem Internetcafé. Zu klären ist, wie viele Arbeitsplätze nach 1 Tag, 3 Tagen oder 1 Woche aktiv sein müssen (siehe Tabelle am Ende des Dokuments). Daraus ergeben sich Auswirkungen auf mögliche Citrix-	

System / Anwendung	RTO	RPO	Details	To do
			Konfiguration und –Lizenzen (zusätzlich zum derzeitig realisierten Zugriffen). Zugriff muss auf Haupt- oder Ausfall-RZ möglich sein.	
Unterlagen, die derzeit nur auf Papier vorliegen	Siehe separate Tabelle	Siehe separate Tabelle	Szenario 3 setzt voraus, dass alle Informationen oder Unterlagen in elektronischer Form vorliegen. Hier ist ein Archivierungskonzept erforderlich, das alle notwendigen Unterlagen elektronisch anbietet (siehe Tabelle am Ende des Dokuments)	
Plattenspeicher am 2. Standort			Zu klären sind die notwendigen Kapazitäten. Aus den Anforderungen bezüglich toleriertem Datenverlust und Wiederherstellungszeiten ergeben sich mögliche Anbindungsoptionen (Bandbreiten) und Technologien mit sehr unterschiedlichen Preispunkten (so ist ohne Breitbandvernetzung eine Wiederherstellung in < 12 h kaum möglich). Zu klären sind auch Anforderungen an Bandeinheiten und die Duplizierung der Inhalte im Bandsilo. Für den Fall eines längeren Betriebs des 2. Standorts (Verlust des Gebäudes) ist dort auch eine vollständige Datensicherung vorzusehen (Backup-Server)	
Internetanbindung 2. Lokation, Standleitungen	½ d f. Email-Routing 1 d für Zugriff Anwend.	N/A	Der 2. Standort muss eine ausreichende Internetanbindung haben, die vom 1. Standort unabhängig ist. Dazu gehören auch Firewall, Virenschutz, VPN-Server. Separate Anforderung ist die Umkonfigurierung der Workstations auf 2. Gateway an 2. Lokation	
Netzwerkkonzept 2. Lokation		N/A	Zu bedenken sind hierbei der Wechsel des Zugriffs der bestehenden und interim Arbeitsplätze, lokal oder außen auf die Systeme im anderen Netz, Namensauflösung, etc.	
VPN	½ d f. Szenar. 1	N/A	Hier sind IPSec-VPN und SSL-VPN separat zu betrachten. Dazu gehören auch Authentisierung (d.h. Zugriff auf LDAP/AD, Token-Server Safeword), End-Point-Security Unterstützung	

System / Anwendung	RTO	RPO	Details	To do
DHCP, Domain Controller, DNS, LDAP/AD	1 d ½ d f. LDAP	1 d	Um die Workstations starten zu können und für die Benutzerauthentisierung werden diese Komponenten benötigt. Ebenso zu berücksichtigen sind Abhängigkeiten von Startup-Skripts auf Fileservern. Die Workstations müssen im Bedarfsfall möglichst einfach auch auf die 2. Lokation zugreifen können (automatisch oder manuell)	
Terminalserver (Citrix)	1 d	1 w	Zahl der Clients nach 1 Tag, 3 Tagen oder 1 Woche siehe separate Tabelle. Zu klären sind Abhängigkeiten von Nfuse, End-Point-Security; Appsense ist nicht im Einsatz	
Lizenzserver für	1 w	N/A	Citrix kann z.B. für eine bestimmte Zeit ohne Lizenzen arbeiten, jede Anwendung ist separat zu klären	
Fileserver	Siehe sep. Tabelle	½ d, bzw. 1 d	Zu differenzieren sind Fileserver, die für den Workstation Startup benötigt werden, Office Dokumente, Dateien, die von Anwendungen benötigt werden. Möglicherweise ebenfalls relevant sind Antivirus-Server	
Externer Webserver	3 d	1 w	Zu klären ist, ob er kritische Anwendungen oder lokal veränderte Daten enthält (im ersten Fall wird Hochverfügbarkeit benötigt, im 2. Fall eine ausreichende Sicherung der Daten). Es muss auf jeden Fall sichergestellt sein, dass die Webserver-Inhalte auch im DR-Fall wiederhergestellt werden können (Themen wie Load Levelling, Application Server und Reverse Proxy sind bei Bedarf zu betrachten)	
Intranetserver	3 d	1 d	Frage, ob in kritischen Anwendungen eingesetzt, Sharepoint ist ein weiteres mögliches Thema	
Drucker, Spezialpapier		N/A	Es muss eine Möglichkeit bestehen auch in Szenario 3 zu drucken. Aber auch im Normalbetrieb ist zu klären ob eine Abhängigkeit von einem zentralen Printserver besteht. Benötigte Spezialpapiere sollten auch außerhalb des Gebäudes vorliegen. Thinprint ist dabei evtl. zu berücksichtigen	
Plotter	1 m	N/A	Frage ob geschäftskritisch	

System / Anwendung	RTO	RPO	Details	To do
E-Mail	1 d f. Zugriff Postfächer ½ d f. Routing		Dies betrifft alle Mailserver, Spam- und Virenschutz. Zu berücksichtigen ist MSE und der POP-Server und mögliche Authentisierungsanforderungen. Werden eingehende Mails bei Ausfall der Mailfunktionalität extern vorgehalten (wie lange? Benachrichtigungsmöglichkeit für Empfänger?) Zugriff auf Adressbücher als separates Thema	
Webmail	3 d	N/A		
Blackberry	3 d	1 d	Auch Blackberry-Printing (?)	
VoIP	3 d	N/A	Zu berücksichtigen sind Server- und Client-Anforderungen	
System-Überwachung	1 d	1 w	Optimalerweise werden die Systeme am 2. Standort kontinuierlich überwacht, d.h. die Systemüberwachung sollte auch redundant möglich sein	
Patch-Management	> 1 w	N/A		
Datensicherung			Für 1. und 2. Standort, auch der Fall, dass nur der Datensicherungsserver oder Bandkomponente am 1. Standort ausgefallen ist	
Virenschutz	1 d f. Schutz 1 w f. Patternvert.	N/A	Verteilung der Virenpattern, entweder über lokalen Server oder durch Umkonfigurieren auf Internetzugriff	

Verfügbarkeitsanforderungen in Bezug auf Material, das derzeit nur auf Papier vorliegt

Abteilung, Funktion	Art der Unterlagen	RTO	RPO