

“Disaster: Backup & Recovery” – metodologia projektu

Jarosław Łagowski

IBM Polska

e-mail: j.lagowski@pl.ibm.com

Abstrakt

Trudno sobie wyobrazić współczesną organizację (przedsiębiorstwo lub urząd), która nie używa technologii informatycznej w celu przetwarzania danych związanych z jej działalnością. Co więcej, znaczna część tych organizacji jest zależna od tego typu przetwarzania danych. Zależność taka oznacza, że w przypadku braku możliwości elektronicznego przetwarzania danych, organizacja nie może działać. Czas przestoju w przetwarzaniu danych określany jako dopuszczalny jest różny dla różnych organizacji. Dla jednych może to być 1 godzina dla innych 1 tydzień. Tak czy inaczej, po przekroczeniu dopuszczalnego czasu, kiedy występuje brak możliwości przetwarzania danych, organizacja staje w obliczu zawieszenia działalności.

Wyodrębnić możemy dwie kategorie przyczyn przestoju w przetwarzaniu danych, biorąc pod uwagę możliwy sposób rozwiązania problemu: awaria systemu i katastrofa. Awaria systemu oznacza problem, który można usunąć w ramach podstawowej instalacji w czasie dopuszczalnym. Przykładem awarii może być uszkodzenie dysku. Rozwiązaniem problemu może być odtworzenie danych (np. z wykonanych wcześniej kopii taśmowych) na dysku zapasowym. Katastrofa oznacza problem, który nie może być usunięty w ramach instalacji podstawowej w czasie dopuszczalnym. Powodem może być na przykład pożar lub powódź, ale również problem wspomniany w poprzednim akapicie (awaria dysku), jeżeli nie może być on rozwiązany w czasie dopuszczalnym. Każda organizacja musi zdecydować, jaki czas przestoju jest dla niej dopuszczalny i tym samym w niektórych przypadkach to spodziewany czas odtwarzania będzie rozstrzygał o tym, czy problem jest awarią czy katastrofą.

Na podstawie 57 przypadków z całego świata zbadanych od roku 1988 przez Contingency Planning Research Inc. można powiedzieć, że spośród firm, które spotkała bezpowrotna utrata danych umieszczonych w systemie informatycznym (katastrofa, której nie dało się naprawić) tylko 6% przetrwało. Wśród pozostałych, 43% nigdy nie wznowiło działalności a 51% upadło po dwóch latach. Dane nie obejmują skutków zamachu z 11 Września 2001. Referat jest próbą odpowiedzi jak należy przygotować i wdrożyć strategię "Disaster: Backup & Recovery", aby znaleźć się wśród ww. 6%.

Przedstawione będzie sześć etapów przygotowania i implementacji tej strategii. W dalszej części artykułu projekt "Disaster: Backup & Recovery" nazywany będzie w skrócie DBR.

1. Etapy projektu DBR

Bardzo rzadko realizacja projektu informatycznego jest jednym, ciągłym procesem. Najczęściej proces dzielony jest na etapy, realizowane po kolei lub współbieżnie, z możliwością iteracji poszczególnych etapów lub ich grup. Nie inaczej jest w przypadku projektu DBR. Poniżej przedstawione zostaną w skrócie etapy projektu DBR. W następnych punktach zostaną omówione będą nieco dokładniej pierwsze, cztery etapy. Pełne omówienie wykracza poza ramy kilkunastostronicowego artykułu.

1.1. Etap I. Określenie wymagań funkcjonalnych (*business requirements*)

Jest to podstawowe zadanie do realizacji. Musimy tutaj dokonać analizy ryzyka katastrofy (*risk analysis*) i analizy wpływu katastrofy na funkcjonowanie organizacji (*impact analysis*). Podstawowe informacje, które musimy zdobyć to:

- jakie zadania nie mogą być realizowane bez systemu informatycznego,
- jak długa przerwa jest dopuszczalna dla takich procesów,
- jakie zadania realizowane normalnie za pomocą systemu informatycznego mogą być realizowane *off-line* i po odtworzeniu systemu wprowadzone do niego,
- jaki wolumen danych lub czas przetwarzania *off-line* jest dopuszczalny

Wynikiem tego etapu powinno być również oszacowanie kosztów przestoju systemu informatycznego oraz lista priorytetów odtwarzania poszczególnych funkcji systemu. Rezultat analizy powinien określić:

- minimalny zestaw zadań organizacji, które muszą być realizowane przez system,
- maksymalny czas odtworzenia tego zestawu po katastrofie,
- maksymalny czas pracy systemu przy użyciu tylko minimalnego zestawu,
- priorytety (kolejność i czasy) udostępnienia funkcji organizacji do realizacji w systemie.

1.2. Etap II. Określenie wymagań przetwarzania danych (*data processing requirements*)

Realizacja tego kroku zakłada wcześniejsze wykonanie zadań przewidzianych w kroku pierwszym. Celem jest wykonanie mapowania wymagań funkcjonalnych na język systemu informatycznego, zrozumiały dla inżyniera systemowego. Wynikiem końcowym tego kroku powinna być tabela pokazująca dla każdej aplikacji (lub modułu oprogramowania lub zestawu danych):

- maksymalny czas odtworzenia,
- maksymalny czas utraconych danych (wyrażony np. w minutach przed katastrofą),
- minimalną potrzebną moc przetwarzania,
- potrzebne zasoby dyskowe,
- zależności od innych aplikacji

1.3. Etap III. Projekt rozwiązania DBR (*design*)

Projekt rozwiązania oznacza ogólny opis przyjętej strategii oraz głównych elementów rozwiązania. Chodzi tutaj o określenie raczej funkcji, jakie musi spełnić konfiguracja systemowo-sprzętowa przeznaczona do realizacji strategii, niż o dokładne zdefiniowanie potrzebnego sprzętu i oprogramowania.

1.4. Etap IV. Wybór produktów / narzędzi realizujących zaprojektowane rozwiązanie (*select products to match the design*)

Bardzo często już na etapie projektowania dokonywana jest preselekcja produktów. Bywa, też tak, że projekt przygotowany jest pod kątem dostępnych narzędzi. Na tym etapie, musimy szczegółowo określić, które produkty wybieramy do realizacji rozwiązania. Pod pojęciem produktu lub narzędzia rozumiemy tutaj:

- oprogramowanie i sprzęt wspierające proces backupu,
- oprogramowanie i sprzęt wspierające proces odtwarzania,
- oprogramowanie i sprzęt potrzebny dla instalacji zapasowej,
- oprogramowanie i sprzęt komunikacyjny,
- inny potrzebny sprzęt i materiały (np. taśmy)

Specyfikacja produktu musi być pełna to znaczy określać wszystkie jego parametry (np. liczbę i rodzaj licencji dla oprogramowania, rozmiar i rodzaj pamięci masowej itp.).

1.5. Etap V. Implementacja przyjętego rozwiązania DBR (*implementation*)

Ten krok powinien być realizowany jako regularny projekt bazujący na specyfikacji przygotowanej w wyniku kroków poprzednich. Należy określić zasoby ludzkie, oraz systemowo-sprzętowe dla realizacji tego projektu. Niezbędny jest oczywiście harmonogram projektu obejmujący tak podstawowe rzeczy jak:

- terminy dostaw potrzebnego sprzętu i oprogramowania,
- terminy i zasoby ludzkie przeznaczone do instalacji dostarczonego sprzętu i oprogramowania,
- określenie faz projektu, terminów ich realizacji, wzajemnej zależności oraz przydzielonych zasobów ludzkich.

Ten krok powinien zostać zakończony pomyślnymi testami przyjętego rozwiązania DBR.

1.6. Etap VI. Utrzymanie i aktualizacja rozwiązania (*maintenance*)

Systemy informatyczne podlegają ciągłym zmianom, są rozwijane, uaktualniane itd., dlatego pomyślnie zakończenie kroku 5. nie oznacza końca prac dla rozwiązania DBR. Istotne jest ustalenie procedur i wyznaczenie ludzi (zespołu) odpowiedzialnych za:

- aktualizację rozwiązania, jeżeli wymaga tego rozwój systemu,
- okresowe testy rozwiązania, w szczególności procedury odtwarzania,
- ciągłe monitorowanie wykonania procedury backupu.

Oczywiście kroki zaprezentowane powyżej podlegają iteracji, to znaczy, że w wyniku realizacji danego kroku może okazać się konieczne powtórne wykonanie kroku poprzedniego lub przynajmniej jego części. Co więcej, wykonanie kolejnych kroków może odbywać się równolegle. Na przykład, po określeniu części wymagań funkcjonalnych (krok 1) możemy już zacząć mapować je na wymagania przetwarzania danych (krok 2), Zawsze należy pamiętać o celu nadrzędnym, jakim jest po prostu zapewnienie działalności organizacji po katastrofie systemu informatycznego.

2. Określenie wymagań funkcjonalnych

Istnieją dwa, podstawowe zagadnienia, które muszą być objęte analizą:

- Jakie są potencjalne przyczyny (zagrożenia) katastrofy systemu informatycznego?
- Jak długo, organizacja może działać bez systemu informatycznego, który uległ katastrofie?

Dużą pokusą jest stwierdzenie, że każdy rodzaj zagrożenia musi tak samo wzięty pod uwagę oraz, że wszystkie funkcje przedsiębiorstwa realizowane przez system są równie ważne. Takie określenie wymagań funkcjonalnych przenosi się następnie na duże koszty zabezpieczenia, które musi zapewnić odporność na wszelkie zagrożenia i ciągłość pracy całego systemu. Dlatego, też warto przeprowadzić analizę nieco dokładniej, aby stwierdzić jak jest naprawdę.

2.1. Analiza ryzyka katastrofy

Najważniejsze obszary analizy ryzyka dotyczą:

- **Zabezpieczenia fizyczne:** odporność budynku na pożar, zalanie, wybuch gazu itp.
- **Zabezpieczenia danych:** procedury dostępu do danych, zabezpieczenie integralności danych w systemie itp.
- **Regulaminy dla pracowników:** procedury poruszania się po budynku, dostępu do pomieszczeń ze sprzętem pracującym dla systemu informatycznego, dostęp osób trzecich itp.
- **Procedury lokalnego backupu i odtwarzania:** chodzi tutaj o sprawdzenie ryzyka sytuacji, kiedy problem, który powinien być obsłużony jako awaria może stać się katastrofą.
- **Infrastruktura:** awaryjne urządzenia zasilające, stabilizatory napięcia, bezpieczniki, stan instalacji gazowej, elektrycznej i wodnej, awaryjne urządzenia telekomunikacyjne.
- **Umiejscowienie serwerowni:** znając potencjalne zagrożenia możemy ocenić umiejscowienie i zabezpieczenie serwerowni (np. jeżeli wysokie jest ryzyko powodzi, serwerownia nie powinna znajdować się w piwnicach)
- **Krytyczne kwalifikacje:** należy rozpoznać kwalifikacje personelu niezbędne do zabezpieczenia i odtworzenia w razie katastrofy, wskazane powinny być osoby tzw. “niezastąpione”, aby jak najprędzej zapewnić “dublerów”

Wynikiem powinien być ranking potencjalnych przyczyn katastrofy.

2.2. Analiza wpływu na funkcjonowanie organizacji

Tutaj należy określić:

- jakie procesy przedsiębiorstwa (*business processes*) zależne są od systemu,
- które z tych procesów są krytyczne,
- koszt zatrzymania procesów przedsiębiorstwa na jednostkę czasu,
- maksymalny czas zatrzymania danego procesu,
- zależności między procesami,
- priorytet odtwarzania procesów,
- dopuszczalny poziom utraty danych dla procesu.

Istotne jest oczywiście ogólne spojrzenie na system informatyczny. Jeżeli skala systemu pozwala odtworzyć pełny system w akceptowalnym czasie, nie warto wtedy przeprowadzać pełnej analizy wpływu. W takim przypadku należy przyjąć, iż system będzie odtwarzany jako całość, czyli wszystkie procesy organizacji obsługiwane przez system będą dostępne w tym samym czasie po katastrofie.

Dla oceny istotności procesów organizacji może posłużyć się poniższą, ogólną klasyfikacją:

- **Procesy Krytyczne:** zapewniają codzienną pracę organizacji, zwykle muszą być odtworzone przed upływem 24 godzin po katastrofie.

- **Procesy Ważne:** mogą być odwleczone w czasie, ale ze ściśle określonym opóźnieniem (np. nie dłużej niż tydzień), zwykle muszą być odtworzone przed upływem 48 godzin po katastrofie
- **Procesy Drugorzędne:** mogą być odwleczone w czasie, bez określonego opóźnienia lub ze znacząco długim okresem opóźnienia

Istotne jest zrozumienie, iż ważność procesu jest funkcją czasu. Zatem procesy ważne, nie odtworzone po upływie kilku dni mogą stać się krytyczne. Dodatkowo, ocena ważności procesu może zależeć od daty, kiedy wystąpiła katastrofa. Np. pewne procesy mogą być realizowane tylko w określonym okresie roku (raz na kwartał) lub miesiąca (na koniec miesiąca). Zatem, jeżeli katastrofa wystąpi na początku miesiąca, proces, który jest realizowany na zakończenie miesiąca jest drugorzędny. Ale ten sam proces, w przypadku katastrofy mającej miejsce pod koniec miesiąca, staje się krytyczny. Analiza wpływu musi uwzględniać zmianę priorytetów odtwarzania procesów w zależności od daty wystąpienia katastrofy i aktualnego stanu przedsiębiorstwa.

3. Określenie wymagań przetwarzania danych

Po określeniu wymagań funkcjonalnych wykonać należy mapowanie procesów przedsiębiorstwa wyznaczonych do odtwarzania po awarii na aplikacje i w konsekwencji zbiory danych systemu informatycznego. Pamiętać należy, że jedna aplikacja realizować może wiele procesów przedsiębiorstwa oraz, że niektóre procesy mogą być realizowane przez wiele aplikacji. Z mapowania wynikać będzie dla każdej aplikacji:

- maksymalny, akceptowalny czas przestoju,
- maksymalna akceptowalna utrata danych,

Dodatkowo, dla każdej aplikacji musimy określić:

- wymagania sprzętowe dla instalacji zapasowej (moc procesora, dyski, inne),
- wymagania sieciowe dla utrzymania zdolności odtworzenia w zadanym czasie i zadaną utratą danych,
- poziom usług świadczony przez aplikację po odtworzeniu po katastrofie

3.1. Katalog procesów

Zebrane informacje na temat procesów organizacji, realizowanych przez system informatyczny powinny być zebrane w katalog procesów. Katalog procesów może być przedstawiony w formie tabel. Uproszczony przykład katalogu aplikacji prezentujemy poniżej:

Rysunek 3.1 Katalog Procesów

	Istotność	Maks. Czas przestoju	Maks. Utrata danych	Aplikacje / Zbiory Danych
Proces1	Krytyczny	6 godzin	Bez utraty danych	Aplikacja1 / ZD1, ZD2
Proces2	Krytyczny	2 godziny	2 godziny	Aplikacja 1 / ZD2 Aplikacja 2 / ZD2
Proces3	Ważny	2 dni	1 tydzień	Aplikacja 3 / ZD3
Proces4	Drugorzędny	Uruchomienie 1/miesiąc	Bez utraty danych	Aplikacja 4 / ZD1, ZD3
...
Procesn	Drugorzędny	Uruchomienie 1/kwartał	1 miesiąc	Aplikacja 4 / ZD4

3.2. Katalog aplikacji

Kolejnym celem określenia wymagań przetwarzania danych jest katalog aplikacji (*application inventory*). Katalog aplikacji może być przedstawiony w formie dwóch tabel: tabeli funkcji i tabeli wymagań. Poniżej zaprezentujemy uproszczony przykład ilustrujący katalog aplikacji.

Rysunek 3.2 Katalog Aplikacji – tabela funkcji

	Maks. Czas od- tworzenia	Zbiory Danych	Maksymalna Utrata danych	Aplikacje, od których jest za- leżna	Aplikacje zależne
Aplikacja1	2 godziny	ZD1, ZD2	Bez utraty danych		Aplikacja 2
Aplikacja2	2 godziny	ZD2	2 godziny	Aplikacja 1	Aplikacja 4
Aplikacja3	2 dni	ZD3	1 tydzień		
Aplikacja4	Do końca miesiąca	ZD4	1 miesiąc	Aplikacja 2	
...
Aplikacjan	Do końca kwartału	ZDn	1 miesiąc		

Rysunek 3.3 Katalog Aplikacji – tabela wymagań

	Jednostki wydaj- ności procesora	Pamięć (MB)	Dyski (GB)	Sieć (Kbs)	Inne
Aplikacja1	10	512	100	19,2	Drukarka A3 – 300 stron papieru
Aplikacja2	8	256	50	2 * 64	Skaner 600 dpi
Aplikacja3	4	1024	500	9,6	???
Aplikacja4	10	1024	500	256	
...
Aplikacjan	12	2048	400	4,8	

3.3. Wynik analizy

Analiza przygotowanych katalogów procesów i aplikacji powinna doprowadzić do ostatecznego rozstrzygnięcia następujących zagadnień:

- Lista aplikacji odtwarzanych po katastrofie
- Lista aplikacji odtwarzanych częściowo (np. tylko dla wybranych danych)
- Lista aplikacji nie odtwarzanych po katastrofie
- Kolejność i maksymalne czasy odtwarzania aplikacji po katastrofie
- Sumaryczne wymagania systemowo – sprzętowe dla odtwarzania po katastrofie

Analiza musi być wynikiem kompromisu pomiędzy potrzebami a dostępnymi środkami.

4. Projekt rozwiązania DBR

Wymagania przetwarzania danych, przygotowane na poprzednim etapie, dają podstawy do rozpoczęcia fazy projektowania rozwiązania DBR. Gotowy projekt powinien określać:

- Zakres odtwarzania

- Strategię testów
- Procedury backupu i odtwarzania
- Zarządzanie instalacją zapasową
- Opis konfiguracji

4.1. Zakres odtwarzania

Na tym etapie, musimy jasno i ostatecznie zdefiniować:

- Jakie typy katastrofy są przewidziane i obsłużone przez rozwiązanie a jakie nie
- Kolejność odtwarzania aplikacji
- Maksymalny czas odtworzenia dla każdej aplikacji
- Jakie dane są odtwarzane dla kolejnych aplikacji
- Spodziewana aktualność danych po odtworzenia dla różnych grup danych

4.2. Strategia testów

W fazie projektowania, przed ostatecznym wyborem narzędzi i produktów nie jesteśmy w stanie zdefiniować szczegółowych planów testów. Należy natomiast odpowiedzieć na podstawowe pytania:

- Gdzie będą odbywać się testy?
- Jakie zasoby są potrzebne do wykonania testów?
- Czy testy mogą zakłócić przetwarzanie produkcyjne?
- Czy można testować przetwarzanie produkcyjne na instalacji zapasowej?

4.3. Procedury backupu i odtwarzania

Ponieważ sposób wykonania backupu determinuje sposób odtworzenia powinniśmy myśleć o procedurach backupu i odtwarzania jako całości. Punktem wyjścia powinny być cele odtwarzania. Procedury odtwarzania powinny być tak przygotowane, aby mogły być spełnione cele odtwarzania. Dopiero w drugim kroku powinniśmy opracować taki sposób backupu, aby ustalone sposoby odtwarzania były możliwe do realizacji. Rozważmy, jakie elementy powinniśmy wziąć pod uwagę mówiąc o procedurach backupu i odtwarzania.

Sprzęt i infrastruktura

Przygotowanie sprzętu i infrastruktury dla rozwiązania DBR jest czynnością zasadniczo jednorazową. Zmiany w tych elementach podlegają planowaniu przez zespół opiekujący się rozwiązaniem.

Oprogramowanie

Oprogramowanie może ulegać zmianom, które jednak wraz z „dojrzewaniem” systemu będą coraz rzadsze. Tym niemniej zmiany oprogramowania są ściśle określone przez zespół opiekujący się systemem. Z tego powodu niezmiernie ważna jest komunikacja między zespołem utrzymującym rozwiązanie DBR a zespołem zajmującym się rozwojem systemu.

Dane

Zasadniczym podmiotem procedur backupu i odtwarzania są dane. Dane są najbardziej zmiennym elementem zarówno, jeżeli chodzi o rozmiar jak i o zawartość. W porównaniu z danymi, inne elementy, takie jak sprzęt, oprogramowanie, infrastruktura są niemal statyczne. Z tego powodu, to właśnie dane będą zasadniczym przedmiotem procedur backupu i odtwarzania.

4.3.1 Kategorie danych

W celu uporządkowania dalszych rozważań wprowadzimy trzy, ogólne kategorie danych.

Dane Systemowe

Ta kategoria obejmuje zbiory danych potrzebne do uruchomienia systemu operacyjnego. Dane dotyczą konkretnej konfiguracji systemowo – sprzętowej. Te dane zmieniane są rzadko.

Dane Konfiguracyjne

Ta kategoria (nazywana czasem meta – danymi) obejmuje zbiory konfiguracyjne podsystemów potrzebnych do działania aplikacji. Dane dotyczą konfiguracji baz danych, autoryzacji, monitorowania itp. Ten typ danych można nazwać danymi systemowymi zmiennymi: pod kątem aplikacji, przez aplikację lub, od których aplikacja jest zależna. Dane Konfiguracyjne mogą zmieniać się znacznie częściej niż Dane Systemowe.

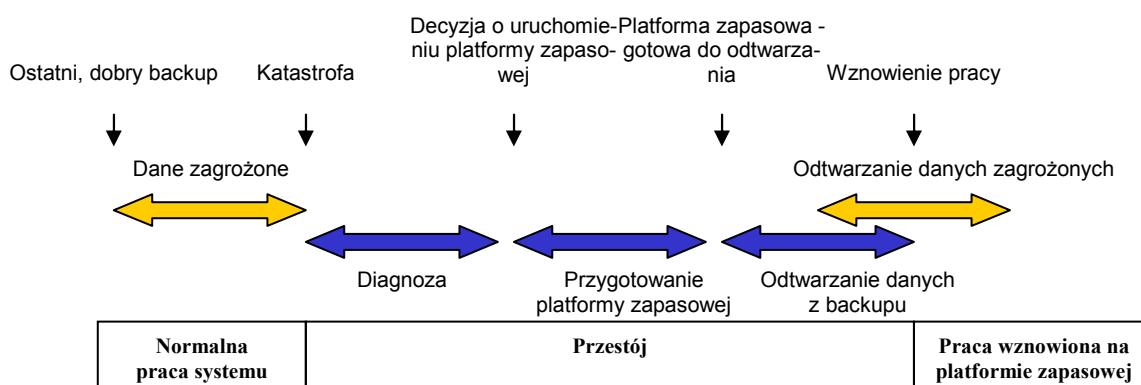
Dane Aplikacji

Ta kategoria obejmuje zbiory należące do aplikacji: bazy danych, programy, pliki robocze itp. Generalnie są to zbiory, poza dwoma, wymienionymi wyżej kategoriami, bez których aplikacja nie może działać. Kluczową grupą danych wśród Danych Aplikacji są bazy danych. O ile pozostałe grupy danych można odtworzyć bądź instalując na nowo (programy) bądź tworząc ich nowe instancje (pliki robocze), o tyle bazy danych jako zmieniane nieustająco w wyniku przetwarzania, muszą być odtworzone z backupu.

Projekt rozwiązania DBR powinien uwzględnić zaprezentowaną wyżej różnorodność danych z zastosowaniem najwyższego priorytetu dla baz danych.

4.3.2 Status danych w kontekście katastrofy

Rysunek 4.1 Dane i sekwencja zdarzeń w przypadku katastrofy i odtwarzania



Dane niezabezpieczone

Dopóki dane znajdują się w lokalizacji głównej nie możemy uznać ich za zabezpieczone. Dane niezabezpieczone możemy sklasyfikować jako:

- nie przenaszalne : dane produkcyjne nie skopiowane na taśmę, dysk zapasowy lub inne urządzenie pozwalające przenieść dane poza lokalizację główną bez zakłócenia pracy systemu,
- przenaszalne: kopia danych produkcyjnych, przygotowana do transferu na platformę zapasową.

Dane zabezpieczone

Dane przeniesione poza lokalizację główną możemy uznać za zabezpieczone. Dane zabezpieczone możemy sklasyfikować jako:

- dane przeniesione: dane są przetransportowane do umiejscowienia zapasowego, ale nie są jeszcze gotowe do użycia na platformie zapasowej (np. taśmy zostały przewiezione, ale jeszcze nie są odtworzone),
- dane zaaplikowane: dane są odtworzone na platformie zapasowej i gotowe do użycia

Dane zagrożone

Dane wprowadzone do systemu pomiędzy ostatnim, poprawnie wykonanym backupem a katastrofą określamy jako zagrożone (*orphan data*). Dane zagrożone odtwarzane są po odtworzeniu danych zachowanych w backupie. Sposób odtwarzania danych zagrożonych może obejmować tak różne możliwości jak ponowne, „ręczne” wprowadzenie danych czy wykorzystanie dziennika zmian, który jest duplikowany w instalacji zapasowej. W zależności od wybranego sposobu zabezpieczenia danych zagrożonych, należy się liczyć z określoną utratą danych zagrożonych.

Dane utracone

Dane utracone w wyniku katastrofy mogą obejmować zarówno planową utratę danych (wynikającą z przyjętego rozwiązania) jak i przypadkową utratę danych (wynikającą z błędu przyjętego rozwiązania lub z błędnego wykonania rozwiązania).

Dane buforowane

Jeżeli organizacja zachowuje możliwość jakiegokolwiek działania w czasie przestoju to może się to wiązać z wygenerowaniem danych, które trzeba będzie wprowadzić do systemu po wznowieniu działania. Takie dane nazywać będziemy danymi buforowanymi – oczekującymi na wprowadzenie do systemu po odtworzeniu.

4.3.3 Zależności między danymi

Ze względu na rozmiar danych, które mają być kopiowane a co za tym idzie, czas trwania backupu, często kopiowanie odbywa się etapami. To znaczy, że poszczególne partie backupu są przesunięte względem siebie w czasie. Projektując rozwiązanie, DBR, musimy wziąć pod uwagę konieczność uzyskania spójnych danych po odtworzeniu.

Spójność zbiorów danych

Tutaj, ponownie, najistotniejsze są zbiory baz danych. Dzieje się tak, dlatego, iż często, informacja na temat jednego obiektu rzeczywistego (np. pracownika) uzyskiwana jest z wielu zbiorów (tablic) bazy danych. Inny przykład, kiedy spójność zbiorów bazy danych jest zagrożona to niezgodność tablicy i jej indeksów. Jeżeli kopiowanie zbiorów przechowujących tablicę i jej indeksy jest rozciągnięte w czasie, to może się zdarzyć, że kopia indeksu wskazuje na obiekt nieistniejący lub inny niż powinna. Nie istnieje mechaniczny sposób sprawdzenia spójności

zbiorów w zaprezentowanym wyżej znaczeniu. Spójność musi być zapewniona na poziomie kopiowania określonych grup zbiorów bazy danych razem, a następnie sprawdzana po odtworzeniu w sposób programowy.

Spójność transakcji biznesowych

Bardzo często, zmiany w systemie informatycznym są potwierdzane lub inicjowane dokumentami zewnętrznymi. Np. wystawienie faktury jest rejestrowane w systemie i jednocześnie tworzona jest faktura na papierze, przekazywana w odpowiedniej ilości kopii do zainteresowanych stron. System informatyczny, odtworzony po katastrofie może zawierać stan transakcji niespójny z faktycznie zakończonymi transakcjami biznesowymi. Rozwiązanie DBR musi zaproponować sposób doprowadzenia do spójności transakcji biznesowych i systemu.

4.3.4 Typy backupu

Cele i ograniczenia rozwiązania DBR często wymuszają zastosowanie różnych typów backupu dla poszczególnych kategorii czy typów danych.

Kopie *point-in-time*

Tego typu kopia prezentuje stan danych na określony punkt w czasie. Tradycyjnie, wykonanie kopii tego typu, wymaga wstrzymania zapisu do kopiowanych zbiorów w celu zapewnienia spójności. Tego typu kopia może następnie służyć do odtworzenia gotowego do użycia systemu ze stanem, jaki miał miejsce w momencie wykonania kopii. Może też być punktem startu do odtworzenia bardziej aktualnego stanu systemu przez zastosowanie zachowanego dziennika zmian. Kopie *point-in-time* można podzielić na dwie, zasadnicze grupy.

Kopie Logiczne: Tworzony jest „ekstrakt” zawartości zbiorów danych bez odwzorowania ich fizycznej struktury. Tego typu kopia pozwala na bardziej elastyczne odtworzenie (z zastosowaniem innej struktury fizycznej). Z reguły jednak, czas odtworzenia z kopii logicznej jest wybitnie dłuższy niż odtworzenie z kopii fizycznej.

Kopie Fizyczne: Kopiowane są zbiory danych na poziomie ich reprezentacji i struktury fizycznej. Jest to z reguły szybszy sposób wykonania kopii niż kopia logiczna. Zdecydowanie natomiast szybsze jest odtwarzanie z wykorzystaniem kopii fizycznej. Należy jednak pamiętać, że odtworzenie z kopii fizycznej wymaga określonego środowiska, jak najbardziej identycznego ze środowiskiem pierwotnym.

Kopie *on-line*

Backup powinien być wykonany przy minimalnym przestoju środowiska pierwotnego lub, jeżeli to możliwe, bez takiego przestoju. Niektóre bazy danych zapewniają możliwość wykonania backupu bez zatrzymywania przetwarzania. Tak wykonana kopia jest z założenia niespójna i wymaga dodatkowych czynności (aplikacji dziennika zmian) w celu uzyskania spójnego stanu bazy danych. Wadą takiego rozwiązania dla dużych wolumenów danych jest duże przesunięcie w czasie pomiędzy pierwszym a ostatnim kopiowanym zbiorem i co za tym idzie długi, często nie akceptowalny czas uspoźniania kopii. Innym rozwiązaniem jest wykonanie backupu „prawie” *on-line*. Jest to możliwe poprzez sprzęgnięcie mechanizmów systemowo – sprzętowych z backupem bazy danych. Możliwe jest wtedy krótkie wstrzymanie pracy bazy danych na czas zainicjowania backupu zbiorów danych. Mechanizm systemowo – sprzętowy wykona kopie spójnego stanu zbiorów posługując się własnymi kopiami zmienianych obszarów danych.

Kopie przyrostowe

Kopie przyrostowe zawierają jedynie dane zmieniane od czasu poprzedniej kopii. Tego typu kopie są użyteczne tylko w zestawieniu z wcześniej wykonaną pełną kopią systemu. Odtwarzanie przy użyciu kopii przyrostowych wymaga sekwencyjnego odtworzenia najpierw kopii peł-

nej potem kolejnych kopii przyrostowych. Czas odtwarzania jest wybitnie dłuższy od czasu odtwarzania z kopii pełnej. Korzyścią z wykonania kopii przyrostowych może być krótszy czas wykonania kopii oraz jej mniejsza objętość. Należy jednak pamiętać, że jeżeli od poprzedniej kopii zmianom uległa większość danych, kopia przyrostowa może trwać nawet dłużej niż kopia pełna (narzut porównania).

Kopie dziennika zmian

Systemy zarządzania bazą danych, (DBMS) generują specjalny dziennik zmian przechowujący zapisy wszystkich operacji zmieniających stan bazy danych. Dziennik taki (zbiór danych) ma zwykle ograniczoną pojemność. Po zapełnieniu bieżącego dziennika, DBMS rozpoczyna zapis do nowego dziennika. Zapełniony dziennik zmian może być skopiowany. Nazywamy go wtedy dziennikiem archiwalnym. Skopiowany ciąg dzienników archiwalnych może następnie posłużyć po odtworzeniu bazy danych z backupu do powtórzenia operacji, które miały miejsce w bazie danych po wykonaniu backupu.

4.3.5 Transport i składowanie kopii danych

Wykonana kopia danych powinna jak najszybciej, w sposób bezpieczny zostać przetransportowana do lokalizacji zapasowej. W przypadku wykonania kopii na taśmę oznacza to fizyczne przetransportowanie nośnika (np. samochodem) do lokalizacji zapasowej. Naraża to kopię danych na utratę w trakcie transportu oraz stawia problemy natury organizacyjnej (ludzie, środek transportu, czas).

Lepszym rozwiązaniem jest elektroniczne przesyłanie kopii danych do lokalizacji zapasowej. Wymaga to jednak odpowiedniej infrastruktury: sieci, technologii zdalnego kopiowania. Korzyścią jest szybszy i prostszy transport danych do lokalizacji danych. Jednocześnie, możliwe jest, szybsze niż w przypadku kopii na taśmy, wychwycenie błędu w kopii danych.

Niezależnie od elektronicznego przesyłania danych powinna istnieć kopia danych na taśmach. Daje to możliwość powrotu do poprzednich wersji danych oraz stanowi dodatkowe zabezpieczenie w przypadku jednoczesnej katastrofy ośrodka głównego i zapasowego. W przypadku elektronicznego przesyłania danych, kopia danych na taśmy może być wykonana w ośrodku zapasowym i zabezpieczona na miejscu lub przewieziona to trzeciej lokalizacji.

4.3.6 Gotowość instalacji zapasowej

Mówiąc o procedurach DBR musimy wziąć pod uwagę zakładany poziom gotowości instalacji zapasowej. Pierwsze rozróżnienie może dotyczyć wyposażenia instalacji zapasowej.

Przygotowane umiejscowienie (*cold site*)

Przygotowane umiejscowienie oznacza, że jest gotowa lokalizacja (pomieszczenie), zasilanie, klimatyzacja, łącza sieciowe i być może minimalny zestaw systemowo – sprzętowy. Określone są też wymagania rozbudowy instalacji zapasowej w przypadku katastrofy. Takie rozwiązanie oznacza minimalne koszty przygotowania i ekstremalnie długi czas odtwarzania – najpierw trzeba doposażyć ośrodek a potem dopiero przystąpić do odtwarzania. W tym przypadku, oczywiście, nośnikiem kopii zapasowej mogą być tylko taśmy.

Przygotowana instalacja (*hot site*)

Przygotowana instalacja oznacza w pełni wyposażony ośrodek dysponujący zasobami potrzebnymi do przejęcia pracy od instalacji podstawowej.

Oczywiście, zaprezentowany wyżej podział jest dość ogólny. Często istnieją rozwiązania pośrednie – instalacja zapasowa jest wyposażona tak, aby podjąć tylko krytyczne przetwarzanie. Inne

procesy będą obsługiwane w miarę wyposażania instalacji zapasowej lub z założenia nie będą obsługiwane w instalacji zapasowej.

Jeżeli mówimy o instalacji typu *hot site* to warto rozważyć poziom gotowości do przejęcia pracy na wypadek katastrofy.

Bez przygotowania

Kolejne backupy są tylko gromadzone i na wypadek katastrofy musi nastąpić odtwarzanie z wybranego (najczęściej najnowszego backupu)

Odtwarzanie cykliczne

Kolejne backupy są odtwarzane w instalacji zapasowej. Instalacja zapasowa po odtworzeniu jest gotowa do użycia prezentując stan systemu z momentu wykonania backupu.

Gotowość do aktualizacji stanu systemu (*ready to roll forward*)

Oprócz backupów odtwarzanych cyklicznie, gromadzone są w ośrodku zapasowym dzienniki zmian systemu głównego. Na wypadek awarii stan instalacji zapasowej może być zaktualizowany poprzez zastosowanie dzienników zmian.

Aktualizacja stanu systemu (*roll forward*)

Dzienniki zmian odebrane z instalacji podstawowej są aplikowane na instalacji zapasowej. Aktualizacja stanu systemu może odbywać się cyklicznie (np. raz na dobę aplikowane są wszystkie zgromadzone dzienniki) lub w sposób ciągły, natychmiast po otrzymaniu kolejnego dziennika zmian z systemu podstawowego. Należy uwzględnić problem liniowości aplikacji dzienników zmian w systemie zapasowym, podczas, gdy zmiany w systemie podstawowym generowane są równolegle. W konsekwencji może to oznaczać, że czas aplikacji dziennika zmian w instalacji zapasowej jest dłuższy niż czas jego powstawania w instalacji podstawowej. W takim przypadku poziom gotowości *roll-forward* nie może być zastosowany.

Stan systemu zawsze aktualny (*realtime remote update*)

Ten poziom gotowości jest możliwy do osiągnięcia tylko przy zastosowaniu techniki utrzymywania zdalnej kopii lustrzanej (*mirror copy*) zbiorów danych. Kopia taka oznacza, że zmiana zbiorów w systemie głównym jest potwierdzona tylko wtedy, kiedy jednocześnie udała się zmiana w zbiorach instalacji zapasowej.

Podobnie jak w przypadku kategorii wyposażenia instalacji zapasowej, tak i przypadku kategorii gotowości instalacji zapasowej mogą istnieć kategorie pośrednie lub dla różnych zbiorów danych może być przejęta inna kategoria gotowości. I tak na przykład dane krytyczne mogą być utrzymywane w stanie zawsze aktualnym przez zastosowanie *realtime remote update*, dane ważne mogą być gotowe do aktualizacji a dane drugorzędne mogą być odtwarzane z ostatniego backupu.

4.4. Zarządzanie instalacją zapasową

4.4.1 Opcje zarządzania instalacją zapasową

Instalacja „uśpiona”

W tej opcji decydujemy się na nie wykonywanie żadnych operacji bieżących. Działanie instalacji zapasowej (oprócz prac przygotowawczych) rozpoczyna się w momencie katastrofy instalacji podstawowej.

Instalacja zarządzana zdalnie

W tej opcji, większość operacji na instalacji zapasowej prowadzona jest zdalnie. Daje to możliwość redukcji personelu obsługującego tylko instalację zapasową do niezbędnego minimum. Generuje natomiast dodatkowe zadania dla administratorów instalacji podstawowej. Dodatkowo, wymaga dodatkowej konfiguracji umożliwiającej zdalne zarządzanie.

Instalacja zarządzana lokalnie

W tej opcji, mówimy o pełnym składzie personelu zarządzającego dla instalacji zapasowej. Ten wybór zapewnia najprostsze i najszybsze odtwarzanie na wypadek katastrofy.

4.4.2 Zadania zarządzania instalacją zapasową

Wybór opcji zarządzania instalacją zapasową rzutuje w konsekwencji na sposób realizacji zadań zarządzania instalacją zapasową. Poniżej przedstawimy generalną klasyfikację tych zadań.

Operacje podstawowe

Operacje podstawowe to start, zamknięcie i restart systemu.

Obsługa konsoli

To zadanie polega na odczytywaniu i interpretacji komunikatów pojawiających się na konsoli systemu. W konsekwencji operator powinien podjąć odpowiednie akcje lub przekazać informacje odpowiedniej osobie.

Obsługa taśm

Obsługa taśm w zależności od przyjętego rozwiązania może być realizowana:

- tylko w ośrodku podstawowym,
- tylko w ośrodku zapasowym,
- w obydwu ośrodkach w odpowiednim zakresie,
- w wydzielonym ośrodku obsługi taśm

Planując obsługę taśm należy brać pod uwagę ilość zabezpieczanych danych a co za tym idzie ilość nośników, na których będą odbywać się operacje oraz czas ich odczytu i zapisu. W przypadku dużej ilości danych, niezbędna może okazać się automatyzacja obsługi taśm (roboty taśmowe).

Obsługa wydruków

Instalacja zapasowa musi być wyposażona, lub mieć dostęp do infrastruktury zapewniającej możliwość niezbędnych wydruków na wypadek katastrofy.

Monitorowanie otoczenia

To zadanie obejmuje obserwacje temperatury i wilgotności w serwerowni, kontrolowanie sprawności klimatyzacji, zagrożenia zalania wodą itp. Monitorowanie powinno być maksymalnie zautomatyzowane, trzeba jednak wyznaczyć personel odpowiedzialny za sprawdzenie wyników monitorowania i podjęcia odpowiednich kroków w razie zaobserwowanych odchyleń.

Dostęp do instalacji

Muszą istnieć przygotowane procedury zapewniające dostęp dodatkowego personelu w razie katastrofy.

4.4.3 Automatyizacja

Automatyizacja obsługi instalacji zapasowej a w szczególności procedur odtwarzania jest niezbędna. Chodzi tutaj zarówno o automatyzację w sensie operacji sterowanych przez oprogramowanie czy sprzęt jak i o automatyzację czynności operatora. Wymaga to przygotowania dokumentów – procedur postępowania operatora. W przypadku katastrofy, bardzo ważnym czynnikiem staje się stres. Tym samym rośnie ryzyko popełnienia błędu przez osobę realizującą zadania nieprecyzyjnie określone.

4.4.4 Kultura pracy z instalacją zapasową

Jeżeli wybrana została opcja zarządzania instalacją zapasową z pełną obsługą dla tej instalacji musimy pamiętać o kilku podstawowych zasadach:

- personel instalacji zapasowej musi na bieżąco poznawać i rozumieć zmiany zachodzące w instalacji podstawowej,
- pożądana jest okresowa wymiana personelu między instalacjami,
- należy utrzymywać aktualną dokumentację odnośnie procedur pracy,
- w szczególności, musi być dostępna aktualna kopia pełnego planu odtwarzania po awarii,
- ile to możliwe, instalacja zapasowa powinna obsługiwać część bieżącego przetwarzania danych.

4.4.5 Inne

Istnieje szereg dodatkowych warunków do spełnienia, aby instalacja zapasowa była w pełni funkcjonalna na wypadek katastrofy. Oto niektóre obszary wymagań dodatkowych:

- Pełen zestaw nośników instalacyjnych i dokumentacji
- Łatwo dostępne połączenia zewnętrzne: telefon, faks, Internet
- Wyposażenie biurowe dla personelu: komputery PC, drukarki, ksero, akcesoria biurowe
- Miejsca pracy przygotowane dla personelu dodatkowego w czasie odtwarzania po katastrofie
- Miejsca parkingowe dla dodatkowych samochodów
- Zaplecze socjalne: kuchnia, być może miejsca hotelowe

4.5. Konfiguracja

W tym punkcie projektu musimy określić wymagania systemowo – sprzętowe dla instalacji zapasowej jak i sposób komunikacji z instalacją podstawową.

4.5.1 Odległość pomiędzy instalacją główną i zapasową

Wraz ze wzrostem odległości między instalacjami wzrasta bezpieczeństwo danych (odporność konfiguracji na czynniki zewnętrzne), ale jednocześnie wzrasta koszt i stopień komplikacji łączności pomiędzy instalacjami. Najbardziej zalecany jest średni dystans: 5 – 30 km. Przy takim dystansie zachowujemy dużą odporność na czynniki zewnętrzne: pożar, akt terroru, awaria wodociągu. Jednocześnie, zaletami średniego dystansu pomiędzy instalacjami są:

- stosunkowo niski koszt budowy połączenia dwóch instalacji,

- możliwość wysoko przepustowego łącza,
- łatwość przemieszczenia personelu na wypadek katastrofy,
- możliwość wykorzystania instalacji zapasowej również do celów backupu lokalnego

Oczywiście, średni dystans może okazać się niewystarczający, np., jeżeli instalacja zasadnicza leży na obszarze obciążonym dużym prawdopodobieństwem powodzi lub trzęsienia ziemi.

4.5.2 Parametry instalacji zapasowej

Podstawowe parametry instalacji zapasowej wynikają wprost z określenia wymagań przetwarzania danych (patrz pt. 3.). Instalacja zapasowa musi być przygotowana pod kątem zasobów do odtworzenia procesów krytycznych w określonym w wymaganiach czasie. Odtworzenie procesów pozostałych może odbywać się w drugiej kolejności, i o ile pozwala na to specyfikacja czasów odtwarzania, może być poprzedzone wyposażeniem instalacji zapasowej w dodatkowy sprzęt.

4.5.3 Połączenie instalacji głównej i zapasowej

Sposób połączenia instalacji również wynika z wymagań przetwarzania danych oraz objętości odtwarzanych zbiorów. Wyróżnić możemy cztery, podstawowe typy połączenia instalacji.

Brak bezpośredniego połączenia

Brak bezpośredniego połączenia sieciowego oznacza, że instalacja zapasowa musi w celu odtworzenia posłużyć się taśmami zapisanymi w instalacji podstawowej i fizycznie przetransportowanymi do instalacji zapasowej. Bezwzględnie jest to najtańszy sposób połączenia, ale może być wykluczony, chociażby wtedy, jeżeli czas odtwarzania z taśm przekracza dopuszczalny czas podjęcia pracy po katastrofie.

Zestawione połączenie sieciowe

Wykorzystując zestawione połączenie sieciowe dane mogą być kopiowane zdalnie z instalacji podstawowej na zapasową. Minimalizuje to ryzyko utraty danych w czasie transportu danych. Ten typ połączenia stanowi podstawę do realizacji kolejnych poziomów wymienionych niżej.

Zdalny dostęp do urządzeń taśmowych

Kopia danych z instalacji podstawowej na taśmy odbywa się przez sieć bezpośrednio na urządzenia znajdujące się w instalacji zapasowej.

Zdalny dostęp do dysków

Dane z instalacji podstawowej są przechowywane na dyskach instalacji zapasowej jako kopia lustrzana odświeżana synchronicznie lub asynchronicznie. Jaki sposób odświeżania kopii lustrzanej zostanie wybrany, zależy od przepustowości sieci, ilości danych synchronizowanych i wpływu synchronizacji na wydajność przetwarzania danych

Sposób połączenia instalacji podstawowej i zapasowej może być oczywiście kombinacją wymienionych wyżej typów. Tym niemniej, bardzo rzadko udaje się osiągnąć wymagania przetwarzania danych bez zestawionego połączenia sieciowego.

4.5.4 Połączenia sieciowe

W kontekście instalacji zapasowej możemy mówić o dwóch typach połączenia sieciowego:

- połączenie pomiędzy instalacją główną i zapasową (mówione wyżej),
- połączenie umożliwiające pracę po katastrofie (np. podłączenie użytkowników)

Jeżeli jest to możliwe jedno, fizyczne łącze może być wykorzystane do obydwu typów połączenia. Warto zauważyć, że dane łącze nie będzie wykorzystywane do obydwu celów naraz. Parametry powinny być dopasowane do większych wymagań jednego z typów połączenia.

W celu łatwego lub wręcz automatycznego przełączenia pracy na instalację zapasową, należy rozważyć, aby wejście do sieci (*gateway*) było niezależne od obydwu ośrodków lub było zduplikowane.

4.5.5 Rozłożenie obciążenia pomiędzy instalacjami

Planując instalacje zapasową powinniśmy zdecydować jak wyglądać będzie jej codzienne obciążenie. Możliwe są trzy podstawowe modele:

- instalacja zapasowa tylko na potrzeby DBR,
- instalacja zapasowa obsługuje część niekrytycznego przetwarzania od instalacji podstawowej,
- działają dwie, równorzędne instalacje z równomiernie rozłożonym obciążeniem; w razie awarii jednej z nich druga przejmuje całość przetwarzania.

Pierwsza z propozycji stwarza najlepsze warunki odtwarzania na wypadek katastrofy. Ten model oznacza jednak, że kosztowne zasoby systemowo – sprzętowe są niewykorzystywane na bieżąco.

Drugi z modeli wydaje się najrozsądniejszą propozycją. Zwłaszcza, przy założeniu, że przetwarzanie niekrytyczne na instalacji zapasowej nie modyfikuje danych (raportowanie, analizy).

Trzecia możliwość stwarza konieczność przygotowania symetrycznych procedur DBR dla każdej z instalacji. Poza tym, równomierne rozłożenie obciążenia wymaga ścisłej współpracy z twórcami i administratorami aplikacji i w niektórych przypadkach nie jest możliwe.

4.5.6 Projektowanie aplikacji

Projektowanie rozwiązania DBR jest znacznie ułatwione, jeżeli aplikacja jest projektowana z myślą o takim rozwiązaniu. Podstawowe zasady pomagające w obsłudze aplikacji pod kątem rozwiązania DBR, (ale nie tylko) to:

Modularyzacja

Moduł aplikacji oznacza zbiór danych i programów realizujących określone procesy biznesowe. Moduł powinien być maksymalnie niezależny od innych modułów a jego powiązania – ściśle określone. Pozwala to łatwiej wykonać mapowanie procesów (w tym procesów krytycznych) na zbiory podlegające odpowiedniej procedurze DBR.

Spójna konwencja nazewnictwa

Spójna konwencja nazewnictwa wiążąca ze sobą wszystkie elementy modułu aplikacji (programy, wsady, obiekty bazy danych, zbiory) pozwala łatwiej zaimplementować procedury DBR dla wydzielonych fragmentów aplikacji (zbiorów procesów).

Transakcyjność

Transakcyjność oznacza logiczne grupowanie operacji przetwarzania danych oraz zapewnienie, że dana grupa operacji (transakcja) zostanie wykonana w całości lub nie wykona się żadna operacja z grupy. Dzięki transakcyjności dane zachowują zawsze spójny stan, co ułatwia odtworzenie pracy systemu po katastrofie.

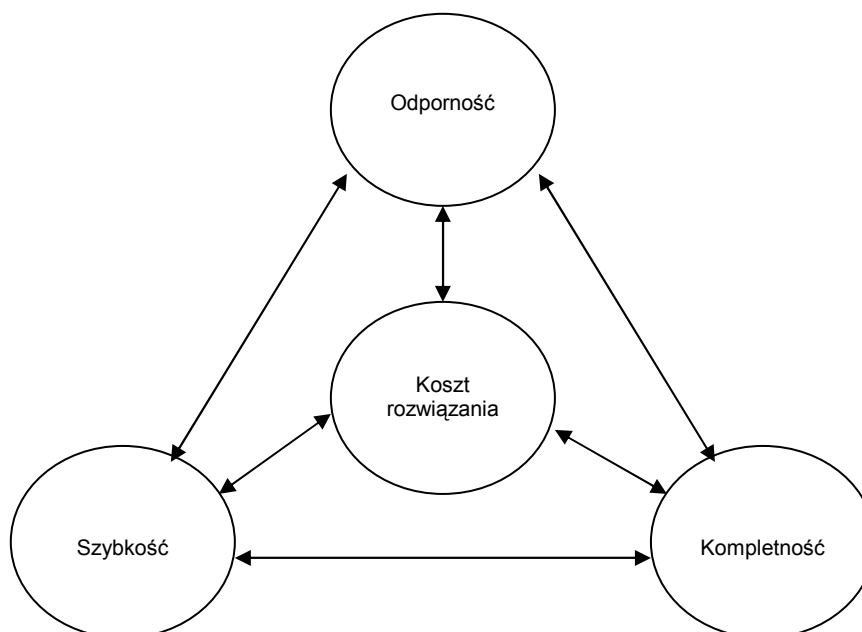
4.5.7 Kryteria wyboru

Ostateczny kształt rozwiązania DBR zależy od decyzji podjętych przez uprawnione do tego osoby (ośrodek decyzyjny). Podstawowe kryteria wyboru:

- Koszt rozwiązania
- Odporność na różne typy katastrof
- Szybkość odtwarzania
- Kompletność odtworzonego systemu

Poniżej prezentujemy graf przedstawiający kryteria wyboru. Powiązania między kryteriami oznaczają linie kompromisu.

Rysunek 4.2 Kryteria wyboru DBR



5. Podsumowanie

Przedstawiliśmy trzy z sześciu etapów projektu „Disaster: Backup & Recovery”. Jak widać, projekt taki, traktowany poważnie, może być procesem złożonym, dosyć skomplikowanym, czasochłonnym, kosztownym i wymagającym zasobów ludzkich i sprzętowych. Istotne jest, aby kierownictwo organizacji, która zależy od systemu informatycznego zrozumiało znaczenie pomyślnej realizacji takiego projektu. Pomyślnie zrealizowany projekt DBR jest swego rodzaju „ubezpieczeniem” systemu. Podobnie jak w przypadku ubezpieczania samochodu przed kradzieżą, może ono nigdy się nie przydać. Pewne jest jedno: za późno jest na zawarcie umowy po kradzieży.

Bibliografia

1. Fire in the Computer Room - What Now?, SG24-4211-01
2. Disaster Recovery Library S/390 Technology Guide, GG24-4210-01
3. Disaster Recovery Library Data Recovery, GG24-3994
International Technical Support Organization Bibliography of Redbooks, GG24-3070.
(www.redbooks.ibm.com)