Disaster Recovery Plan (DRP) – checklist

1. Cel DRP

Odzyskiwanie danych i przywrócenie dostępności oraz funkcjonowania systemu informatycznego jest najważniejszym zadaniem w planowaniu DRP.

1.1. W DRP należy zdefiniować:
1.1.1. co jest katastrofą,
1.1.2. jakie i gdzie zlokalizowane są zasoby cyfrowe i systemy, które mają być odzyskane w razie katastrofy,
1.1.3. czas przywracania danych i systemu.

Najczęściej katastrofa dotycząca systemów informatycznych jest spowodowana błędem ludzkim (np. przypadkowe wykasowanie bazy danych przez osobę z uprawnieniami administratora, zaszyfrowanie zasobów cyfrowych przez złośliwe oprogramowanie przypadkowo lub celowo uruchomione przez użytkownika systemu, fizyczne uszkodzenie lub zniszczenie nośnika, na którym przechowywane są dane i pliki aplikacji). Należy rozważyć także inne możliwe scenariusze, w szczególności ze względu na specyfikę działalności danego podmiotu.

1.2. Określając DRP należy także:
1.2.1. zidentyfikować krytyczne systemy dla działalności oraz kolejność, w jakiej powinny być odzyskiwane,
1.2.2. zdefiniować w jakich przypadkach proces odzyskiwania danych ma dotyczyć pojedynczych plików, czy konieczne jest odzyskanie całego system,
1.2.3. określić kiedy wystarczające jest odtworzenie danych z kopii zapasowych, a kiedy konieczne jest odzyskanie systemu,
1.2.4. określić maksymalny czas braku dostępu do systemu informatycznego / zasobów informacyjnych, który można zaakceptować.

2. Metody odzyskiwania danych i systemów informatycznych

2.1. Nie jest możliwe określenie konkretnej metody odzyskiwania danych i systemu informatycznego bez odniesienia się do konkretnej:
2.1.1. infrastruktury IT,
2.1.2. systemu operacyjnego,
2.1.3. pozostałego oprogramowania,
2.1.4 stosowanej metody tworzenia kopii zapasowych danych jak np. backup pełny, przyrostowy, różnicowy, syntetyczny, synchroniczna replikacja bazy danych, itp.

2.2. Przykładowe metody odzyskiwania danych i systemów informatycznych:

2.2.1. Odzyskiwanie plików / danych (file recovery)
Metoda odzyskiwania danych opartego na plikach wykorzystuje skrypt do tworzenia kopii zapasowych plików na maszynie wirtualnej. Skrypt ten jest zainstalowany na maszynie

Wersja 1.1
Opracowanie: Leadenhall Insurance S.A., Lloyd's coverholder, ul. Domaniewska 42, 02-672 Warszawa

wirtualnej zawierającej dane, które chcemy chronić. Rozwiązania polegające na tworzeniu kopii zapasowych plików nie zajmuje tyle pamięci dyskowej, co rozwiązanie polegające na tworzeniu kopii zapasowych na maszynach wirtualnych. Pozwala też na wybór danych, które mają podlegać kopiowaniu i przez to ochronie. Jest to też metoda bardzo precyzyjnego przywracania wskazanego zakresu danych (poszczególnych plików, folderów lub dysków).

2.2.2. Pełne odzyskiwanie całego systemu (system recovery)
Przygotowanie przywracania całego systemu polega na wykorzystywaniu narzędzi do wykonywania kopii niektórych plików systemowych i rejestru systemu operacyjnego oraz zapisywania ich jako tzw. punkty przywracania. W przypadku awarii lub uszkodzenia danych możliwe jest przywrócenie systemu do stanu roboczego bez konieczności ponownej instalacji całego systemu operacyjnego. Naprawiany jest system operacyjny przez przywracanie plików i ustawień, które zostały zapisane w punktach przywracania.

2.2.3. Odzyskiwanie maszyn wirtualnych (virtual machine recovery)
Maszyny wirtualne mają wiele zalet w porównaniu z maszynami fizycznymi. Te same narzędzia do odzyskiwania danych, które działają na maszynach fizycznych, mogą być również używane do odzyskiwania danych z maszyn wirtualnych.

2.2.4. Bare metal recovery
Metoda ta polega na odtworzeniu środowiska systemowego po fizycznej awarii sprzętowej serwera podczas którego dotychczasowy serwer zastępowany jest nowym. Klasyczne podejście BMR oznacza ponowną instalację i konfigurację systemu operacyjnego oraz aplikacji na nowym serwerze a następnie ręczne lub za pomocą skryptów odtwarzanie wymaganych danych i plików. Bardzo często oznacza to także ręczne konfigurowanie podstawowych komponentów środowiska IT.

2.2.5. Zlokalizowane odzyskiwanie danych lub systemu (localised recovery)
Zlokalizowane odzyskiwanie dotyczy sytuacji, gdy system informatyczny jest odzyskiwany z innej lokalizacji, gdzie była przechowywana jego kopia. Metoda ta jest możliwa przede wszystkim w przypadku stosowania synchronicznej replikacji systemu w różnych lokalizacjach. Dostawcy usług chmurowych z reguły umożliwiają synchroniczną replikację systemów i danych w różnych lokalizacjach. W przypadku stosowania tego rozwiązania należy zwrócić uwagę na zgodną z obowiązującymi przepisami dopuszczalną rezydencję danych (np. wyłącznie UE).

2.2.6. Odzyskiwanie z chmury obliczeniowej (cloud recovery)
Odzyskiwanie z chmury obliczeniowej to proces przywracania utraconych, przypadkowo usuniętych lub uszkodzonych danych przez internet z systemu znajdującego się w chmurze obliczeniowej. Ten rodzaj przywracania systemu lub danych zazwyczaj obejmuje odzyskiwanie danych na komputer stacjonarny, pojedynczy serwer lub podłączony do sieci system pamięci masowej. Narzędzia do przywracania systemu z reguły są zapewniane przez dostawcę chmury. Odzyskiwanie w chmurze może polegać także na odzyskiwaniu danych (systemu) całkowicie w chmurze (z jednej lokalizacji do innej, gdzie następuje synchroniczna replikacja systemu i danych – patrz p. 2.2.5.)

3. Instrukcje zawarte w DRP

DRP powinien określić:

3.1. stosowane oprogramowanie do monitorowania pracy systemu (np. Pingdom, Nagios),

3.2. osobę (osoby) odpowiedzialną za reagowanie na zgłaszane problemy z dostępnością i funkcjonowaniem systemu oraz uruchomienie procedury DRP,

3.3. instrukcję przywracania danych lub systemu

Przykładowo: zaloguj się do panelu dostawcy serwisu X, przełącz się na lokalizację podstawową i jeżeli to możliwe zamknij wszystkie instancje, następnie przełącz się na lokalizację alternatywną i uruchom wszystkie zatrzymane instancje; operację wykonaj ręcznie w panelu dostawcy usługi; przetestuj funkcjonowanie przywróconego systemu i dostęp do danych; poinformuj użytkowników i jeżeli to potrzebne przekaż stosowne wytyczne dotyczące korzystania z systemu).

3.4. instrukcję rekonstrukcji systemu i danych w lokalizacji podstawowej z alternatywnej jeżeli lokalizacja podstawowa zostanie przywrócona i będzie stabilna (element opcjonalny - jeżeli dotyczy konkretnego scenariusza odtwarzania).

3. Testy DRP

Plan powinien zawierać harmonogram testowania odtwarzania systemu i danych, wykonywanie tych testów oraz zasady ich dokumentowania.

4. Analiza przyczyn katastrofy

W szczególności należy ustalić:

4.1. czy incydent jest ograniczony do jednego systemu, czy też dotyczy całej sieci?

4.2. czy jakieś pliki zostały uszkodzone lub usunięte?

4.3. czy któryś z systemów jest niedostępny?

4.4. czy incydent spowodował fizyczne uszkodzenia elementów systemu?

W wyniku analizy przyczyn należy określić, czy potrzebne jest wprowadzenie dodatkowych mechanizmów kontrolnych lub środków naprawczych dotyczących bezpieczeństwa systemu i danych.

5. Okresowy przegląd

DRP należy regularnie przeglądać, nie rzadziej niż raz w roku i dokumentować wykonanie przeglądu. W przypadku wystąpienia awarii i przywrócenia działalności należy zweryfikować, czy postępowano zgodnie z DRP i czy był on adekwatny do okoliczności zdarzenia i faktycznego przywrócenia działalności.