LCLOUD

7 kroków DO SKUTECZNEGO DISASTER RECOVERY W AWS

Praktyczny przewodnik dla firm,
które chcą zminimalizować ryzyko przestojów.

powered by aws

1 ZIDENTYFIKUJ KRYTYCZNE SYSTEMY I DANE

Każda firma posiada zasoby, bez których jej codzienne funkcjonowanie staje się niemożliwe. Dlatego pierwszym krokiem w tworzeniu planu Disaster Recovery jest **precyzyjne określenie, które systemy, aplikacje i dane są absolutnie kluczowe dla ciągłości działania biznesu.**

Najlepszym sposobem jest sporządzenie listy usług, których niedostępność natychmiast wpływa na przychody, obsługę klienta lub realizację procesów wewnętrznych. Do najczęściej wskazywanych należą: platforma do przyjmowania zamówień, system zgłoszeń serwisowych, sklep internetowy i jego zaplecze operacyjne, system CRM.

Przy analizie infrastruktury AWS warto szczególną uwagę zwrócić na: instancje Amazon EC2 obsługujące aplikacje kluczowe, bazy danych: Amazon RDS, Amazon Aurora, Amazon DynamoDB, przechowywane dane w usługach Amazon S3 oraz Amazon EFS oraz zasoby zależne od konkretnych regionów AWS, w których operuje Twoja firma.

Im dokładniejsza identyfikacja na tym etapie, tym skuteczniejszy będzie cały plan DR dostosowany do realnych potrzeb, a nie hipotetycznych zagrożeń.

WZÓR TABELI DO OKREŚLENIA KRYTYCZNYCH SYSTEMÓW

System / usługa	Typ zasobu w AWS, odpowiedzialny za utrzymanie/serwowanie systemu	Znaczenie dla biznesu	Czy objęte DR? (✓/✗)	Notatki
E-commerce frontend	Amazon EC2 / Amazon S3	Kluczowy kanał sprzedaży	✓	
CRM	Amazon RDS	Kluczowy dla obsługi klienta	✓	
Pliki klientów	Amazon S3	Dane osobowe / RODO	✓	

2 ZIDENTYFIKUJ KRYTYCZNE SYSTEMY I DANE

Drugim, ważnym krokiem w planie awaryjnym jest odpowiedź na dwa proste pytania:

- **Jaki jest akceptowalny czas przywrócenia systemu do działania? Jak długo maksymalnie możesz czekać na przywrócenie systemu?**

  Czas ten możemy wyrazić jako RTO - Recovery Time Objective. Określa maksymalny akceptowalny czas, przez jaki system może być niedostępny, zanim zacznie to poważnie wpływać na biznes.
  Na przykład: jeśli Twoja aplikacja do obsługi pacjentów w klinice przestanie działać rano, możesz nie przyjąć kilkunastu osób i całkowicie zablokować pracę rejestracji. Warto zatem zastanowić się jakie RTO jesteś w stanie zaakceptować. Czy może wynosić 1 godzinę? to maksymalny czas, w którym oczekujemy, że system powinien wrócić do działania.

- **Ile danych możesz stracić, zanim to naprawdę zrujnuje Twój biznes?**

  To z kolei określa parametr RPO – Recovery Point Objective. Określa, jak „świeża" musi być ostatnia kopia danych, aby firma mogła normalnie funkcjonować po awarii.
  Na przykład: jeśli kopia danych finansowych systemu księgowego wykonywana jest raz dziennie wieczorem, a awaria nastąpi przed końcem następnego dnia operacyjnego, możesz utracić wszystkie faktury i transakcje z ostatnich kilkunastu godzin. RPO wynosi w tym przypadku 24 godziny – ale skrócenie tego czasu do 1–2 godzin może znacząco zmniejszyć ryzyko i koszty.

To szczególnie ważne, bo dzięki temu dowiadujemy się, które systemy należy chronić najbardziej i jak często je zabezpieczać.

Aby określić te wartości, należy przeanalizować wpływ przestoju lub utraty danych na operacje firmy i oszacować realne granice tolerancji.

System	RTO	RPO
Sklep internetowy	30 minut	10 minut
CRM / system obsługi klienta	2 godziny	1 godzina
Dashboard zarządczy / BI	3 godziny	2 godziny
Repozytorium faktur / archiwum	24 godziny	12 godzin

Im niższe wartości RTO i RPO, tym większe wymagania wobec infrastruktury IT i procedur odtwarzania. Dla systemów sprzedażowych i obsługi klienta najczęściej stosuje się RTO < 2h i RPO < 1h. Dla systemów wspierających granice mogą być wyższe, zależnie od potrzeb firmy.

2 ZIDENTYFIKUJ KRYTYCZNE SYSTEMY I DANE

WZÓR TABELI DO OKREŚLENIA RTO I RPO

System / usługa	Akceptowalne RTO	Akceptowalne RPO	Uzasadnienie biznesowe
CRM - system obsługi klienta	30 minut	15 minut	Wsparcie klienta musi działać niemal ciągle. Opóźnienia utrudniają obsługę reklamacji i kontakt.
Baza danych użytkowników	20 minut	10 minut	Krytyczne dla aplikacji. Wysoka dostępność i minimalna utrata danych ograniczają ryzyko niezadowolenia.

3 WYBIERZ STRATEGIĘ TWORZENIA KOPII ZAPASOWEJ

Nie wystarczy mieć backup. Musisz wiedzieć jakie dane dokładnie są kopiowane, jak często, gdzie kopie zapasowe są przechowywane, kto ma do nich dostęp i jak szybko da się je przywrócić. Bez tych informacji backup może być bezwartościowy.

Dobrym punktem odniesienia jest zasada 3-2-1:

3 kopie danych, na 2 różnych nośnikach, z 1 kopią przechowywaną poza środowiskiem produkcyjnym. To prosty model, który realnie zwiększa odporność biznesu na awarie.

W środowisku AWS warto korzystać z narzędzi takich jak:

- AWS Backup – do centralnego zarządzania kopiami wielu usług,
- Amazon EBS Snapshots – do szybkiego przywracania maszyn wirtualnych,
- Amazon S3 Versioning + Lifecycle – by chronić dane przed przypadkowymi usunięciami lub nadpisaniem,
- Manual Snapshots – do ręcznego tworzenia kopii zapasowych baz danych Amazon RDS, pozwalających na ich przechowywanie bez limitu czasu i kopiowanie między regionami lub kontami w celu zwiększenia bezpieczeństwa.

WZÓR TABELI DO OKREŚLENIA STRATEGII KOPII ZAPASOWEJ

Zasób	Narzędzie backupowe (np. AWS Backup, snapshot)	Częstotliwość wykonywania kopii	Lokalizacja (region)	Kto odpowiada za tworzenie kopii zapasowej?
AWS EC2	AWS EBS Snapshots	Codziennie	Frankfurt	Inżynier XYZ

4 ODPOWIEDNIO PRZYGOTOWANE PROCEDURY

Nie przewidzisz wszystkiego, ale możesz przygotować się na najbardziej prawdopodobne zagrożenia. Dobry plan Disaster Recovery powinien zawierać konkretne scenariusze i gotowe procedury działania w przypadku różnych typów incydentów.

Najczęstsze zagrożenia to:

- **Błąd człowieka**

  Ilość problemów może być naprawdę duża. Jedną z nich może być przypadkowe usunięcie bazy danych.

  Rozwiązaniem danej sytuacji jest odzyskanie danych z backupu zarządzanego przez AWS Backup, snapshotu w Amazon Elastic Block Store (Amazon EBS) lub wersjonowania w Amazon Simple Storage Service (Amazon S3).

- **Atak złośliwy (np. ransomware)**

  Cyberataki mogą skutkować m.in. zaszyfrowaniem danych, utratą kontroli nad kontami użytkowników czy całkowitym paraliżem systemu. Jednym z najgroźniejszych scenariuszy jest nieautoryzowany dostęp i zaszyfrowanie danych przez złośliwe oprogramowanie.

  Rozwiązaniem jest korzystanie z backupów offline lub kopii z ograniczonym dostępem – przechowywanych w izolowanym środowisku, np. w oddzielnej Amazon Virtual Private Cloud (Amazon VPC), do której nie ma bezpośredniego dostępu z zewnątrz. Takie podejście znacząco ogranicza ryzyko rozprzestrzenienia się ataku i umożliwia szybkie przywrócenie systemów.

- **Awarie infrastruktury AWS**

  W przypadku usług chmurowych również mogą wystąpić przestoje – najczęściej związane z niedostępnością wybranego regionu. Przykładem może być awaria w regionie eu-central-1 (Frankfurt), która uniemożliwi działanie systemów uruchomionych wyłącznie w tej lokalizacji.

  Rozwiązaniem jest przełączenie ruchu do zapasowego regionu lub wcześniejsze przygotowanie środowiska w alternatywnej lokalizacji, z wykorzystaniem replikacji między regionowej.

Każdy z tych scenariuszy powinien mieć przypisaną jasną sekwencję kroków, osoby odpowiedzialne i kryteria przywrócenia działania.

4 ODPOWIEDNIO PRZYGOTOWANE PROCEDURY

WZÓR TABELI DO OKREŚLENIA PROCEDUR

Typ awarii	Opis	Procedura działania	Czas odzyskiwania (est.)	Link do procedury
Błąd użytkownika	usunięcie bazy danych	przywrócenie snapshotu RDS z 1h	45 min	
Awarie AWS	niedostępność regionu	przełączenie do regionu zapasowego	2h	
Atak (ransomware)	zaszyfrowanie danych	przywrócenie z kopii offline, wymiana kluczy	3h	

5 OPRACUJ PLAN KOMUNIKACJI

Awarie są sytuacjami kryzysowymi, które trzeba sprawnie i jasno komunikować swojemu zespołowi. Brak jasnych zasad komunikacji może pogłębić chaos i negatywnie wpłynąć na jej naprawienie.

Kto powinien być przygotowany:

- Zespół techniczny – musi wiedzieć, co i kiedy należy zrobić.
- Zarząd – musi być informowany na bieżąco o skali problemu i postępie działań.
- Klienci oraz Partnerzy – powinni otrzymać jasny komunikat o sytuacji i przewidywanym czasie przywrócenia usług.

Warto przygotować wcześniej:

- szablony e-maili i komunikatów do różnych grup odbiorców,
- scenariusze wypowiedzi publicznych lub informacji prasowych,
- listę osób odpowiedzialnych za komunikację w każdej grupie,
- zasady eskalacji i kolejność informowania w zależności od rodzaju awarii.

WZÓR TABELI DO OKREŚLENIA PLANU KOMUNIKACJI

Rola / Osoba	Zakres komunikacji	Forma (e-mail, tel, system alertów)	Szablon komunikatu?
CTO	Zarząd	Mail + status meeting	[TAK / NIE]
Marketing	Klienci	E-mail, social media	[TAK / NIE]
PM/Operations	Partnerzy	Telefon / status	[TAK / NIE]

6 TESTUJ ODZYSKIWANIE DANYCH REGULARNIE

„Backup, którego nie przetestowano, nie istnieje." To jedno z najważniejszych założeń skutecznego planu Disaster Recovery. Nawet najlepiej zaplanowany system kopii zapasowych musi zostać sprawdzony w praktyce – zanim naprawdę będzie potrzebny.

Co warto przetestować:

- odzyskiwanie danych w kontrolowanym środowisku testowym,
- czas potrzebny na przywrócenie systemów – i czy mieści się w założonym RTO,
- spójność i kompletność danych po odtworzeniu,
- gotowość zespołu do działania pod presją i zgodnie z procedurami.

Regularne testy pozwalają zidentyfikować luki w procedurach, usprawnić działania zespołu i potwierdzić, że inwestycje w backup realnie zwiększają bezpieczeństwo. To także sposób na ograniczenie ryzyka zaskoczenia w sytuacji kryzysowej.

WZÓR TABELI DO TESTÓW ODZYSKIWANIA DANYCH

Data testu	Typ testu	Zakres (co testowane)	Wnioski / działania po teście
6 maj 2025	Pełne odzyskiwanie	Przywracanie całej bazy danych produkcyjnej	produkcyjnej Czas odtworzenia przekroczył RTO o 20 minut, decyzja o optymalizacji planu backupów.
29 maj 2025	Przywrócenie plików	Pojedyncze pliki konfiguracyjne aplikacji	Brak spójności wersji w backupie, wdrożenie dodatkowej walidacji kopii.

7 WDRÓŻ MONITORING I WSPARCIE 24/7

Nawet najlepiej przygotowany plan Disaster Recovery nie zadziała, jeśli nikt nie zauważy, że coś przestało działać. Dlatego niezbędnym elementem skutecznego zabezpieczenia jest ciągłe monitorowanie infrastruktury i gotowość do reakcji przez całą dobę, 7 dni w tygodniu.

Co powinno działać bez przerwy?

- monitorowanie usług i aplikacji przy użyciu narzędzi takich jak Amazon CloudWatch, Datadog czy AWS CloudTrail,
- automatyczne alerty i powiadomienia o przekroczeniu progów bezpieczeństwa, błędach systemowych i awariach,
- gotowość operacyjna zespołu Network Operations Center (NOC), który natychmiast reaguje na incydenty – niezależnie od pory dnia.

Stały monitoring i wsparcie 24/7 dają pewność, że kluczowe systemy są pod nadzorem nie tylko w godzinach pracy, ale również nocą, w weekendy i święta. To podstawa realnego bezpieczeństwa - szczególnie w środowiskach produkcyjnych, które muszą działać bez przerwy.

WZÓR TABELI DO OKREŚLENIA MONITORINGU 24/7

Zakres monitoringu	Narzędzie (np. Amazon CloudWatch)	Osoba / zespół	Czas reakcji (SLA)
Awarie EC2	Amazon CloudWatch alarmy	Zespół NOC	do 15 min
Błędy RDS	Amazon CloudWatch + SNS	Admin DB	do 1h

POTRZEBUJESZ WSPARCIA?

Budowanie skutecznego planu Disaster Recovery w AWS to nie jednorazowe zadanie, ale przemyślany proces, który wymaga doświadczenia, znajomości narzędzi chmurowych i stałej opieki nad środowiskiem.

Jeśli chcesz mieć pewność, że Twoje systemy są gotowe na każdy scenariusz awaryjny, warto powierzyć je specjalistom. **Jesteśmy gotowi przejąć Twoje środowisko w chmurze pod kompleksową opiekę, zapewniając pełne wsparcie i monitoring 24/7.**

Dzięki temu nie tylko zabezpieczysz swoją infrastrukturę przed awariami, ale też zyskasz spokój, wiedząc że czuwamy nad kopiami zapasowymi, planami przywracania i szybkim reagowaniem w razie incydentu.

Jeśli chcesz dowiedzieć się więcej, skontaktuj się z nami i porozmawiajmy o tym, jak możemy wspólnie podnieść bezpieczeństwo i stabilność Twojej infrastruktury.

Skontaktuj się z nami i umów bezpłatną konsultację.

KONTAKT@LCLOUD.PL

+48 22 355 23 55