MAIN

ABC Disaster Recovery

Poznaj technologie i procesy, które pozwolą
Twojej firmie utrzymać ciągłość działania

MAIN to polska firma specjalizująca się w budowie środowisk chmurowych. Nasze usługi opieramy na sieci własnych ośrodków Data Center w Warszawie. Oferujemy rozwiązania Private i Hybrid Cloud, uzupełnione konteneryzacją i Disaster Recovery, oraz świadczymy wszystkie poziomy administracji środowiskami fizycznymi i wirtualnymi.

Pomagamy zabezpieczać systemy IT, zapewniając przedsiębiorstwom wysoki poziom Business Continuity. Korzystamy ze sprawdzonych technologii (m.in. VMware i HPE), a każde rozwiązanie dopasowujemy do potrzeb firm oraz specyfiki ich infrastruktury.

MAIN jest częścią Grupy EIP.

Spis treści

Przecież moje systemy są bezpieczne...

Czyli dlaczego warto zapoznać się z naszym ebookiem

Nagłe przestoje, utrata danych, czy cyberataki są realnymi zagrożeniami, które **każdej sekundy dotykają firmy w Polsce** i na całym świecie. Jak wskazuje raport Veeam Data Protection Trends 2022:

98%

firm w regionie EMEA doświadczyło nieoczekiwanych przestojów w ciągu ostatnich 12 m-cy

85%

firm tworzy kopie zapasowe zbyt rzadko dla swoich potrzeb biznesowych

69%

przedsiębiorstw w Europie Wschodniej doświadczyło minimum jednego przypadku ransomware w ciągu ostatnich 12 m-cy

32%

danych utraconych w wyniku ataków ransomware nie odzyskano

Dlatego warto zadać sobie poniższe pytania związane z naszymi danymi firmowymi:

- Czy nasze dane są stale dostępne?
- Czy mamy zabezpieczenia przed utratą danych?
- Czy nasze kopie zapasowe są nie tylko łatwo dostępne, ale i bezpieczne?
- Czy mamy możliwość szybkiego przywrócenia działania w przypadku awarii serwera, zasilania lub braku dostępu do Internetu?

Jeśli odpowiedź na chociaż jedno z tych pytań brzmi “nie”, **cyberataki, klęski żywiołowe, pożary** i wiele innych zagrożeń może pozbawić Twoją firmę dostępu do kluczowych danych oraz spowodować przerwy w jej działaniu.

Każda minuta takiego przestoju to poważne koszty, na które składają się m.in.:


Utrata danych


Straty materialne


Straty wizerunkowe


Przywracanie działania

Niezadowolenie klientów

Mając świadomość zagrożeń możesz zawczasu przygotować się na nie.

Otwierając ten ebook robisz już pierwszy krok. Nie zatrzymuj się – zapoznaj się z przedstawionymi w nim możliwościami zabezpieczenia swojej firmy, wypełnij kwestionariusz sprawdzający odporność i działaj dalej na rzecz ciągłości działania swojej firmy.

Podejmij się opracowania **Planu Disaster Recovery (DRP)** – wsparcie w jego tworzeniu zapewniają również profesjonalni dostawcy usług Data Center.

Na ratunek - Disaster Recovery

Skuteczna odpowiedź na awarie, przestoje i zdarzenia losowe

Disaster Recovery to dedykowane technologie, procesy, polityki i procedury wdrożone w celu zminimalizowania wpływu nieprzewidzianych zdarzeń na działalność firmy. Pozwala jak najszybciej przywrócić do działania kluczowe systemy i aplikacje w sytuacji awarii, nieplanowanego przestoju lub utraty danych.

Dzięki Disaster Recovery firmy mogą uniknąć strat finansowych, spowodowanych przestojami czy karami administracyjnymi (związanymi np. z RODO), oraz długofalowych strat wizerunkowych, które często mają bezpośredni wpływ na płynność finansową firmy.

Usługi Disaster Recovery upowszechniają się w miarę jak obniżają się ceny rozwiązań. Możliwości dostępne dotychczas jedynie w najdroższych rozwiązaniach (klasy Enterprise) są już oferowane w tych bardziej przystępnych cenowo.

> *Według raportu Veeam 'Trendy w ochronie danych 2021', popularność rozwiązań Disaster Recovery wzrosła o 19% w ciągu dwóch lat. Technologie te szybko, wydajnie oraz skutecznie pozwalają przywrócić działalność firmy po awarii i tym samym znacznie podnieść poziom jej ciągłości biznesowej.*

Adam Markowski,
Head of Sales, MAIN

W dalszej części poznasz dostępne rozwiązania Disaster Recovery – ich cechy, zalety oraz praktyczne zastosowania.

Kopie zapasowe (backup)

Podstawowe zabezpieczenie, o którym nie można zapominać

Posiadanie kopii zapasowych (ang. backup) to najpopularniejszy sposób zabezpieczenia firmy przed utratą danych. Niestety backup pokrywa jedynie część ryzyk, na które narażone są dziś przedsiębiorstwa. Może również wprowadzać złudne poczucie bezpieczeństwa, gdy:

Backup znajduje się w tej samej lokalizacji, co dane

Niektóre firmy przechowują kopie zapasowe w tej samej lokalizacji, a nawet na tym samym serwerze, co backupowane dane. W takiej sytuacji, jeśli dojdzie np. do uszkodzenia lub zaszyfrowania sprzętu, na którym się znajdują, przedsiębiorstwo traci dostęp zarówno do danych, jak i backupu.

Stosowane są przestarzałe technologie

Metody wykonywania backupu starzeją się z biegiem lat – wydłuża to czas tworzenia kopii oraz odzyskiwania danych, które mogą też zostać częściowo uszkodzone. W takiej sytuacji kopie nie spełnią swojego zadania – w przypadku utraty danych, ich całkowite odzyskanie będzie niemożliwe.

Zasada 3-2-1

Zgodnie z najlepszymi praktykami (tzw. zasada 3-2-1) firmy powinny posiadać trzy kopie danych, używać dwóch różnych technologii do ich przechowywania (backup w chmurze, zewnętrzny dysk twardy, taśma, etc.), a jedna z nich powinna znaleźć się w zewnętrznej lokalizacji.

W tym celu firmy mogą stworzyć dedykowane repozytoria danych lub umieścić kopie zapasowe w zewnętrznym centrum danych. Ta druga opcja:

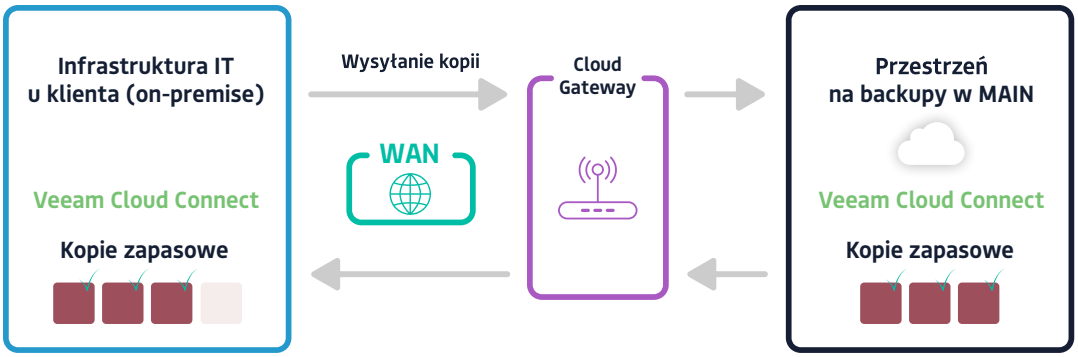
- Pozwala spełnić wymagania dotyczące przechowywania backupu poza siedzibą firmy;
- Umożliwia optymalizację kosztów;
- Nie wymaga utrzymania własnej przestrzeni, mediów, sprzętu i dodatkowego personelu;
- Kopie zapasowe w zewnętrznym Data Center są chronione przed atakami ransomware i wyzwaniami związanymi z bezpieczeństwem w sieci.

Backup w chmurze (Backup-as-a-Service)

Nowoczesne, skalowalne kopie zapasowe

BaaS (Backup-as-a-Service) to backup danych w chmurze, który jest uruchamiany na zlecenie klienta i zgodnie z umowami SLA (Service Level Agreement). Umożliwia odzyskanie danych utraconych w wyniku awarii, uszkodzenia lokalnego repozytorium, a także przypadkowego lub celowego usunięcia kopii zapasowych.

Za usługę backupu i przywracania odpowiada dostawca - utrzymuje niezbędny sprzęt i aplikacje oraz odpowiada za zarządzanie nimi. Po stronie klienta instaluje się tylko oprogramowanie (tzw. agentów backupu), niekiedy tylko urządzenie backupowe.



Schemat działania chmurowego backupu

Do pozostałych zalet backupu w chmurze należą:

- Zautomatyzowanie backupu danych, który jest wykonywany w określonych odstępach czasu;
- Wysoka skalowalność zasobów - możliwe jest korzystanie z większej lub mniejszej przestrzeni w zależności od bieżących potrzeb.

Wybór Backup-as-a-Service nie musi oznaczać rezygnacji z lokalnego backupu. Jeśli dotychczas używane rozwiązanie do tworzenia kopii zapasowych sprawdza się w niektórych obszarach, a w innych nie, można go nadal używać, uzupełniając niedostatki usługą BaaS.

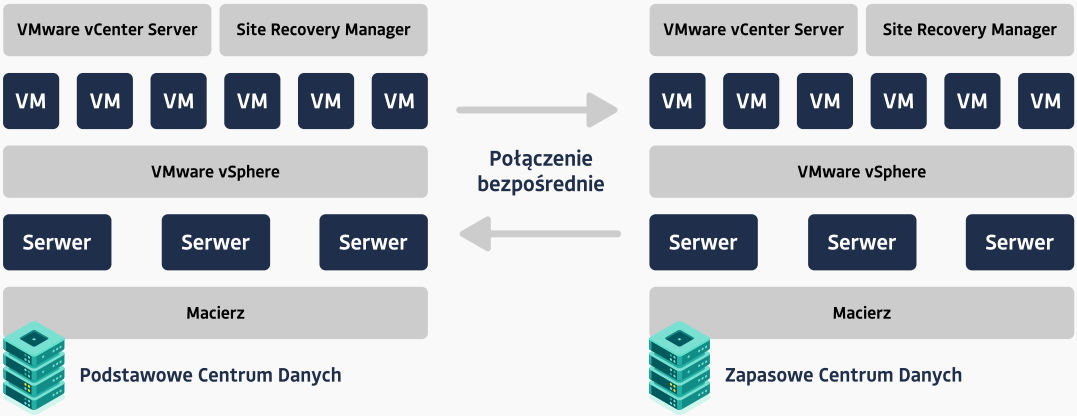
Replikacja do Zapasowego Centrum Danych

Nowoczesne rozwiązanie nawet dla najbardziej wymagających

Oprócz wysokiej jakości kopii zapasowych, które stanowią podstawowe zabezpieczenie, warto zainwestować w bardziej zaawansowane usługi Disaster Recovery. Do takich należy replikacja do Zapasowego Centrum Danych (tzw. Disaster Recovery Center).

Jak działa replikacja?

Replikacja pozwala na utworzenie gotowej do pracy, aktualnej kopii głównego środowiska firmowego lub jego wybranej części w zewnętrznej lokalizacji (tzw. Zapasowym Centrum Danych). Dzięki temu nawet w przypadku całkowitej awarii głównego środowiska, pracę można kontynuować po przełączeniu się na zapasowe. Po przeprowadzeniu naprawy, dane z dodatkowego ośrodka są kopiowane z powrotem do podstawowego, zapewniając jak najmniejsze zakłócenia w pracy.



Schemat replikacji z wykorzystaniem rozwiązań VMware

Replikacja może odbywać się do środowiska fizycznego – dzierżawionych lub kolokowanych w zewnętrznym centrum danych własnych serwerów. Drugą, popularniejszą opcją, jest wykorzystanie środowiska zapasowego opartego o chmurę prywatną bądź publiczną (tzw. Disaster Recovery as a Service – DRaaS).

W obu przypadkach ważne jest, aby ośrodki podstawowe jak i zapasowe znajdowały się w różnych położeniach geograficznych – stanowi to zabezpieczenie nawet na wypadek katastrofalnej awarii w ośrodku podstawowym.

W zależności od wybranego rozwiązania Disaster Recovery dostawca udostępnia w ośrodku zapasowym miejsce w szafie dla zasobów obliczeniowych i storage wraz z dedykowaną infrastrukturą sieciową, która zapewnia wysoką jakość, szybkość i bezpieczeństwo połączenia.

Michał Kaczorowski,
Solution Architect, MAIN

Replikacja w praktyce – case study z branży fintech

Przykładem wdrożenia Disaster Recovery jest środowisko stworzone w MAIN dla ProService Finteco. Sektor finansowy, dla którego przedsiębiorstwo świadczy usługi, wymaga szczególnie wysokiego poziomu ochrony oraz dostępności danych i systemów. Dlatego firma ProService Finteco wybrała najbardziej zaawansowane rozwiązanie – replikację do Zapasowego Centrum Danych.

Najważniejsze korzyści, jakie zyskało przedsiębiorstwo:

- Wysoki poziom Business Continuity dzięki stworzeniu zapasowego środowiska w zewnętrznym Data Center;
- Bezpieczeństwo i łączność między ośrodkami zapewnione przez prywatne, szyfrowane połączenie DWDM;
- Większa odporność środowiska na awarie dzięki wiodącemu oprogramowaniu VMware – Site Recovery Manager i vSphere Replication, które odpowiadają za uruchomienie i nadzór asynchronicznej replikacji maszyn oraz danych;
- Odporność na awarie sprzętu sieciowego, jak i ewentualne problemy z dostępem do internetu;
- Spełnienie norm KNF oraz ISO.

Disaster Recovery Plan – plan odzyskiwania po awarii

Jak go stworzyć i na co zwrócić szczególną uwagę

Disaster Recovery Plan umożliwia skuteczne i szybkie działanie w razie awarii lub utraty danych. Obejmuje on **wszystkie działania minimalizujące skutki przestoju**, tak aby firma mogła kontynuować działalność lub szybko wznowić funkcje krytyczne.

Pierwszym krokiem w tworzeniu Disaster Recovery Plan jest przeprowadzenie **analizy ryzyka (Risk Assessment)** i zbadanie **wpływu awarii na działanie firmy** – Business Impact Analysis. Analizy te pozwolą zidentyfikować systemy IT, które wspierają kluczowe dla działalności naszej firmy procesy.

Pozwala to odtworzyć w pierwszej kolejności te dane, które stanowią o „przeżyciu" firmy. Decydując o tym, które aplikacje i serwery zostaną odtworzone jako pierwsze, ustalamy typowe dla systemów Disaster Recovery metryki – RTO i RPO.

Recovery Time Objective (RTO) określa w czasie, jak dużo danych możemy stracić, aby nie zagroziło to sprawnemu funkcjonowaniu firmy. Czy mogą to być dane z ostatniej godziny, czy może zaledwie z ostatnich 15 minut?

Z kolei **Recovery Point Objective (RPO)** to akceptowalny poziom utraty danych wyrażony w czasie.

Co powinno się znaleźć w Disaster Recovery Planie?

Kluczowy personel

Pracownicy odpowiedzialni za opracowanie, testowanie oraz wdrożenie planu, a także nadzorowanie procesu odzyskiwania danych i systemów. W tym punkcie warto zadać sobie poniższe pytania:

- Kto będzie podejmować szybkie decyzje w sytuacjach awaryjnych?
- Jakie obowiązki mają pracownicy odpowiedzialni za DRP?
- Kto posiada i autoryzuje dostęp do kluczowych systemów?

Identyfikacja krytycznych zasobów i ocena ryzyka

Analiza zasobów oraz najbardziej prawdopodobnych zagrożeń dla IT lub organizacji jako całości. Wpływ każdego z zagrożeń na ciągłość biznesową (w tym szacowana długość przestoju, koszty, wpływ na inne krytyczne procesy itp.).

Odzyskiwanie danych i systemów

Konkretne kroki, które należy podjąć w celu wznowienia działalności oraz zapasowe plany, zasoby, sprzęt i lokalizacje, które mogą być wykorzystane do kontynuowania działań, jeśli podstawowe zasoby są niedostępne. Należy zawrzeć tutaj m.in.:

- Procesy tworzenia kopii zapasowych,
- Technologie potrzebne do szybkiego przywrócenia danych, sieci i fizycznej infrastruktury IT

Komunikacja

Sposoby komunikacji pracowników odpowiedzialnych za odzyskiwanie danych po awarii między sobą, z zainteresowanymi stronami oraz z całym pozostałym personelem. Znajdują się tu odpowiedzi na takie pytania, jak:

- W jaki sposób pracownicy będą się komunikować w przypadku awarii tradycyjnych sposobów komunikacji?
- Czy niektórzy pracownicy powinni mieć dostęp do dodatkowych telefonów komórkowych?
- W jaki sposób pracownicy będą otrzymywać informacje z firmy?

Oprócz technologii dobry dostawca usług Data Center zapewni **konsultacje i pomoc w opracowaniu Planu Disaster Recovery** oraz doborze rozwiązania na podstawie szczegółowej analizy firmowego środowiska IT. Dodatkowo po wdrożeniu usługi zadba o jej regularne testowanie oraz wsparcie techniczne.

Teraz Twoja kolej

Podejmij kolejne kroki, żeby zabezpieczyć swoją firmę

Zależało nam, aby w przybliżyć Ci rozwiązania, które pozwolą utrzymać ciągłość biznesową.

Co warto zrobić dalej?

- Wypełnij kwestionariusz ciągłości biznesowej (str. 13);
- Przeprowadź analizę ryzyka i oceń własną infrastrukturę IT;
- Wybierz rozwiązanie Disaster Recovery, które najlepiej spełnia potrzeby Twojej firmy;
- Stale monitoruj stan zabezpieczeń i ulepszaj je w razie potrzeby.

A co najważniejsze - **pamiętaj, że nie jesteś w tym sam/a.**
Wsparcie w każdym z powyższych kroków otrzymasz
od profesjonalnych dostawców rozwiązań Disaster Recovery.

Podejmujesz kolejny krok? A może masz dodatkowe pytania?
Odezwij się do nas. Rozwiejemy wątpliwości, doradzimy
przy analizie, wyborze i utrzymaniu rozwiązania Disaster Recovery.

ask@main.pl www.main.pl +48 (22) 339 18 98

Wolisz poczekać z rozmową?
Obserwuj nas w mediach społecznościowych.

Stawiamy na partnerskie podejście
„Pokaż nam, co masz, a zaproponujemy Ci najlepsze rozwiązania".

Ty wypełniasz, my pomagamy

Sprawdź, czy Twoja firma jest dobrze zabezpieczona

Odpowiedz na pytania poniżej i dowiedz się, czy Twoje przedsiębiorstwo jest gotowe na utrzymanie ciągłości biznesowej w razie nieprzewidzianych zdarzeń. Im więcej odpowiedzi “tak”, tym lepiej!

Pytanie	Tak	Nie
Czy jesteś świadomy współczesnych zagrożeń (phishing, ransomware), które blokują/kradną dane?		
Czy masz świadomość kosztów krytycznej awarii IT?		
Czy zostały zidentyfikowane krytyczne systemy w firmie?		
Czy opracowano analizę wpływu awarii na biznes?		
Czy firma posiada politykę bezpieczeństwa IT?		
Czy został określony czas, w jakim musi nastąpić przywrócenie do działania krytycznych systemów IT?		
Czy kopie zapasowe krytycznych systemów IT są przechowywane poza siedzibą firmy?		
Czy firmowa serwerownia posiada gwarantowane zasilanie?		
Czy firmowa serwerownia posiada klimatyzację?		
Czy firmowa serwerownia znajduje się w dedykowanym pomieszczeniu?		
Czy firmowa serwerownia jest wyposażona w zabezpieczenia przeciwpożarowe?		
Czy firmowa serwerownia jest wyposażona w system monitoringu i bezpieczeństwa?		
Czy firmowa serwerownia posiada niezależne łącza telekomunikacyjne od więcej niż jednego dostawcy?		
Czy personel wsparcia IT nadzoruje infrastrukturę podstawową w trybie 24/7/365?		
Czy firma korzysta z centralnie zarządzanego systemu tworzenia backupów?		
Czy dane są składowane na współdzielonym systemie dyskowym?		
Czy kopie zapasowe są regularnie testowane?		
Czy firma posiada zwirtualizowane systemy?		
Czy firma korzysta z chmury?		

Zależy Ci na wysokim poziomie Business Continuity?
Szukasz porady lub dedykowanych rozwiązań?

Skontaktuj się z nami!

FAQ, czyli pytania, których boisz się zadać – ale już nie musisz!

Co to jest Disaster Recovery?

Disaster Recovery, inaczej “odzyskiwanie po awarii”, to wszystkie procesy, polityki, procedury i dedykowane technologie, które pozwalają oraz pomagają przywrócić działania krytycznej infrastruktury IT.

Jakie są rodzaje Disaster Recovery?

Do najważniejszych technologii zapewniających ciągłość działania należą kopie zapasowe (backup) oraz replikacja.

Jakie są korzyści z Disaster Recovery?

Rozwiązania Disaster Recovery pozwalają odzyskać dane w przypadku ich utraty oraz utrzymać ciągłość działania całych systemów IT, także w momencie poważnej awarii, cyberataku, pożaru, katastrofy naturalnej czy innego zdarzenia losowego.

W ten sposób umożliwia ochronę firmy od strat, a w wielu przypadkach – nawet bankructwa.

Dla kogo jest Disaster Recovery?

Aktualnie niemalże każda firma działa w oparciu o systemy informatyczne i dane, których na co dzień dotyka wiele zagrożeń. Disaster Recovery, które minimalizuje skutki utraty dostępu do danych czy awarii systemów IT jest więc ważnym rozwiązaniem dla każdego przedsiębiorstwa.

Jakie pytania zadać wybierając dostawcę usług Disaster Recovery?

- Jakie poziomy Service Level Agreement (SLA) oferuje?
- Gdzie przechowywane będą dane?
- Kto ma dostęp do danych?
- Jakie technologie zapewniają odseparowanie danych od danych innych klientów?
- Czy każdy dostęp jest rejestrowany?
- Jakie firma posiada zabezpieczenia, jakie odnotowała próby włamań?
- Czy dane w jakikolwiek sposób będą wykorzystywane, np. do celów marketingowych?
- Czy infrastruktura odpowiada wymogom i regulacjom prawnym?
- Jaką odpowiedzialność prawną przyjmuje na siebie dostawca chmury?
- Jakie rozwiązania zabezpieczają dane?

Czy Disaster Recovery jest drogie?

Nie. Koszt wdrożenia i utrzymania dobrze dobranych do potrzeb firmy rozwiązań Disaster Recovery jest znacznie niższy niż koszty związane z utratą dostępu do danych i systemów IT, do których należą, m.in.:

- koszty odzyskania danych,
- koszty odbudowy systemów,
- straty finansowe związane z przestojem,
- długofalowe straty wizerunkowe,
- kary administracyjne (np. RODO).

Jakie są rodzaje kopii zapasowych?

Wyróżniamy trzy główne rodzaje kopii zapasowych:

Pełna

polega na skopiowaniu wszystkich dostępnych plików. W przypadku błędu lub awarii możemy z niej przywrócić kompletny stan systemu sprzed zdarzenia. Jej wadą jest długi czas jej tworzenia oraz zajmowana powierzchnia dyskowa.

Przyrostowa

powielane są pliki utworzone lub zmodyfikowane od momentu wykonania poprzedniej kopii. Ich odzyskiwanie wymaga odtwarzania każdej kolejnej zapisanej kopii, aż do pierwszej pełnej.

Różnicowa

zasada działania jest podobna do kopii przyrostowej, z tą różnicą, że pliki już wcześniej umieszczone w kopii różnicowej, będą ponownie zarchiwizowane. Do odzyskania danych wystarczy więc ostatnia kopia różnicowa i pełna.

Słowniczek

Business Impact Analysis

analiza wpływu negatywnych czynników na biznes. Ma ona na celu określenie krytycznych procesów, maksymalnych możliwych strat oraz krytycznego czasu dla tych procesów.

Przeprowadzając analizę BIA, należy ustalić najgorszy scenariusz, najbardziej krytyczny dzień roku pod względem wydajności analizowanego procesu biznesowego.

Business Continuity

ciągłość biznesowa, czyli wszystkie działania zapewniające realizację kluczowych funkcji biznesowych firmy podczas zdarzeń kryzysowych, takich jak: katastrofy naturalne, cyberataki, awarie infrastruktury, pożar, etc.

Chmura

(chmura obliczeniowa, cloud, cloud computing) – zwirtualizowany fizyczny sprzęt (serwery, komputery), który zapewnia użytkownikom dostęp do zasobów z dowolnego urządzenia z dostępem do internetu.

Disaster Recovery

inaczej “odzyskiwanie po awarii”; to infrastruktura, procedury i procesy pozwalające utrzymać ciągłość biznesową w sytuacji awaryjnej oraz przywrócić/odtworzyć środowisko IT.

Disaster Recovery Center

Zapasowe Centrum Danych, w którym mogą znajdować się kopie zapasowe oraz gdzie znajdują się zapasowe środowiska utworzone w procesie replikacji.

Disaster Recovery Plan

plan obejmujący wszystkie działania minimalizujące skutki przestoju i umożliwiający skuteczne i szybkie działanie w razie awarii lub utraty danych. Tworzony jest w oparciu o analizę ryzyka (Risk Assesment) i wpływu awarii na działanie firmy (Business Impact Analysis).

Kopia zapasowa (backup)

dane, które mają służyć do odtworzenia oryginalnych danych w przypadku ich utraty lub uszkodzenia.

Ransomware

rodzaj złośliwego oprogramowania, które wykorzystywane jest do szyfrowania danych oraz systemów w celu wyłudzenia okupu.

Replikacja

narzędzie niezbędne do wykonania gotowego do pracy, zdublowanego systemu informatycznego firmy (lub jego części). Dzięki temu nawet w przypadku całkowitej awarii głównego środowiska, pracę można kontynuować po przełączeniu się na zapasowe.

Risk Assessment

ocena ryzyka określająca możliwe wypadki, ich prawdopodobieństwo i konsekwencje oraz odporność organizacji na takie zdarzenia. Jest nieodłączną częścią szerszej strategii zarządzania ryzykiem, która pomaga ograniczyć wszelkie potencjalne konsekwencje związane z ryzykiem.

RPO (Recovery Point Objective)

akceptowalna dla organizacji utrata danych w wyniku awarii.

RTO (Recovery Time Objective)

ilość czasu potrzebna do przywrócenia systemu po wystąpieniu awarii.

SLA

(Service Level Agreement) – umowa o poziomie usług jest zawierana pomiędzy klientem a dostawcą usług w chmurze (CSP) i definiuje, ile procent czasu w skali roku usługi mają być dostępne, jaki może być czas ich niedostępności oraz jak dostawca reaguje na zgłoszenia klienta.

Zasada 3-2-1

najlepsza praktyka tworzenia backupu, wg której należy mieć trzy kopie danych, używać dwóch różnych technologii do ich przechowywania, a jedna z nich powinna znaleźć się w zewnętrznej lokalizacji.

Czujesz głód wiedzy?

Więcej na temat Disaster Recovery (i nie tylko) znajdziesz w Strefie Eksperta MAIN.

Strefa Eksperta ›