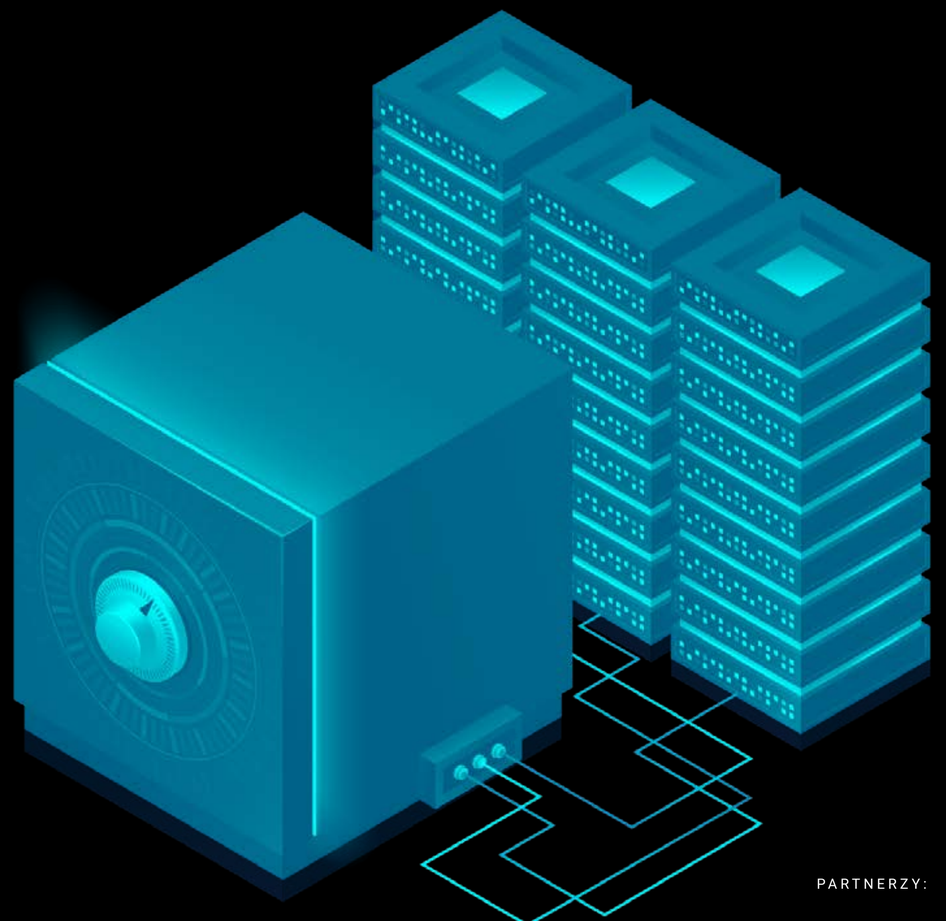
Disaster Recovery,
czyli jak nie stracić danych

Poradnik dla biznesu i IT



OPRACOWANIE MERYTORYCZNE:

beyond.pl

PARTNERZY:

vmware

ARROW

Spis treści

Wprowadzenie

Specjaliści ds. bezpieczeństwa mówią wprost: każda firma prędzej czy później straci dostęp do swoich danych. Pytanie tylko, gdy to się wydarzy, czy będzie w stanie sprawnie i skutecznie je odzyskać oraz czy udźwignie to finansowo.

Do niedawna kwestie zabezpieczenia przed awariami i zapewnienie ciągłości biznesowej były kluczowe głównie dla firm, które były uzależnione od nieprzerwanego dostępu do systemów informatycznych oraz danych przez nie wytwarzanych i przechowywanych. Jednak zmiany technologiczne w ostatnich latach (coraz większe uzależnienie firm od rozwiązań IoT, machine learning, sztucznej inteligencji itd.), dodatkowo pandemia COVID-19 ten krajobraz diametralnie zmieniła. Coraz więcej przedsiębiorstw jest uzależnionych od sprawnego działania systemów, a te które do tej pory funkcjonowały wyłącznie w świecie offline, zostały zmuszone w 2020 roku do przeniesienia biznesu i pracy w tryb online.

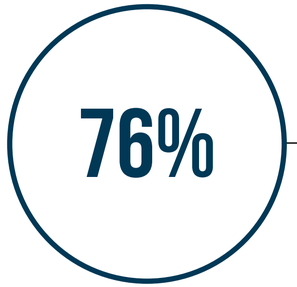
To wszystko sprawiło, że dziś firmy muszą pogłębić swoją wiedzę na temat bezpieczeństwa informatycznego i wybrać model odpowiedni dla swoich potrzeb biznesowych. Brak zabezpieczeń w tym obszarze generuje wiele zagrożeń. Nawet kilkuminutowa przerwa w działalności operacyjnej może nieść ze sobą poważne konsekwencje w postaci zmniejszenia sprzedaży, zakłócenia łańcucha dostaw oraz strat wizerunkowych. Niekiedy oznacza to nawet zagrożenie dla zdrowia i życia, ponieważ wstrzymanie przetwarzania danych grozi w fabrykach na przykład niepoprawną działalnością systemów zabezpieczeń gazowych czy termicznych, a w szpitalach może spowodować brak dostępu do informacji o dotychczasowym leczeniu pacjenta.

Co zrobi Twoja firma, jeśli nagle straci dostęp do danych w wyniku awarii sprzętu, zasilania, cyberataku lub pożaru? Czy masz plan jak odtworzyć dane po awarii? Czy regularnie go testujesz? Czy masz pewność, że jest on na tyle skuteczny, by Twoja firma mogła działać bez większych problemów?

E-book ekspertów Beyond.pl to wprowadzenie do zagadnienia Disaster Recovery. Znajdziesz w nim odpowiedzi na najważniejsze pytania dotyczące odtwarzania danych po awarii i praktyczne wskazówki jaki model Disaster Recovery wybrać dla swojej organizacji.

Zapraszamy do lektury.

Ile kosztuje awaria infrastruktury IT?



W ścianie firmowej serwerowni pęka rura z wodą, a Twoi pracownicy zostają odcięci od maili i systemów, na których pracują z domu. Czy Twoja firma posiada plan reagowania w takim przypadku? Ile kosztuje dzień lub tydzień przestoju? Czy odzyskasz wszystkie dane? Odpowiedzi na te pytania powinien znać każdy przedsiębiorca, bo jak wynika z danych Gartnera, 76% respondentów w ciągu ostatnich dwóch lat doświadczyło sytuacji, która wymagała uruchomienia planu odzyskiwania danych po awarii IT[1]. Jednocześnie ponad 50% badanych zgłosiło co najmniej dwa incydenty z obszaru utraty danych.

Wraz z rozwojem technologii i przenoszeniem się firm oraz konsumentów do świata online rośnie liczba zagrożeń, które trzeba brać pod uwagę. Dobrym przykładem może być sieć O2, która w 2018 roku uległa awarii i poniosła gigantyczne straty z nieswojej winy.

30 milionów klientów straciło dostęp do Internetu, ponieważ dostawcy infrastruktury, z której korzystał operator wygasł... certyfikat bezpieczeństwa[2].

[1] Gartner, Inc. “Survey Analysis: IT Disaster Recovery Trends and Benchmarks.” Jerry Rozeman, Ron Blair. April 30, 2020.

[2] https://www.bbc.com/news/business-46464730

Ile kosztuje awaria infrastruktury IT?

Coraz większym wyzwaniem jest też zabezpieczenie się przed cyberatakami. W 2019 roku 52% decydentów zajmujących się bezpieczeństwem sieci korporacyjnych doświadczyło co najmniej jednego naruszenia poufnych danych[3]. Jedną z ofiar działalności cyberprzestępców stało się miasto Baltimore. W maju 2019 wirus spowodował, że urzędnicy stracili dostęp do maili, danych finansowych, informacji na temat miejskiej infrastruktury, w tym szpitali, portów lotniczych, bankomatów itd. Miasto podjęło bardzo odważną decyzję. Nie zapłaciło hakerom 76 tys. dolarów okupu, ale zdecydowało się zainwestować 10 mln dolarów w budowę systemu zabezpieczeń. Atak był jednak na tyle druzgocący, że powrót do normalnej aktywności zajął miastu kilka miesięcy. Straty obliczono na 8 mln dolarów[4].

Z raportu VMware Carbon Black wynika, że niemal każda globalna firma (92%) doznała takiego ataku w trakcie pandemii COVID-19. Aż 91% oceniło, że wraz z przejściem na pracę zdalną cyberprzestępcy szturmem rzucili się na firmowe sieci i systemy, zwiększając zarówno skalę, jak i częstotliwość ataków[5].

92%

W takiej sytuacji warto zadać sobie pytanie o koszty potencjalnych awarii. W przypadku Amazona „zaledwie" 49-minutowy brak dostępu do strony internetowej i aplikacji mobilnej kosztował 5 mln dolarów[6]. Jak to możliwe? Taki przychód Amazon generował w tym czasie ze sprzedaży online.

Do 10 mln dolarów straciła z kolei linia Delta Air Lines, najstarszy przewoźnik w Stanach Zjednoczonych, obsługujący ponad 120 mln pasażerów rocznie. Brak dostępu do danych sprawił, że linia musiała odwołać około 1 tys. lotów[7].

[3] Forrester. "Top Cybersecurity Threats In 2020." Josh Zelonis, Sandy Carielli, Joseph Blankenship, Elsa Pikulik, Benjamin Corey, Madison Bakalar. January 24, 2020.

[4] https://www.nytimes.com/2019/05/22/us/baltimore-ransomware.html

[5] https://www.carbonblack.com/resources/global-threat-report-extended-enterprise--under-attack/

[6] https://venturebeat.com/2013/08/19/amazon-website-down/

[7] https://www.computerweekly.com/news/450302155/IT-failure-grounds-Delta-flights-worldwide

Polskie firmy tracą z powodu awarii

Szacuje się, że w przypadku 86% organizacji godzinny brak dostępu do danych kosztuje ponad 300 tys. dolarów. W przypadku 34% organizacji jedna godzina awarii przekłada się na od 1 do nawet ponad 5 mln dolarów strat. Tylko 2% firm przyznaje jednocześnie, że jedna godzina awarii kosztowała je mniej niż 100 tys. dolarów.

Źródło: Information Technology Intelligence[8]

Awarie i straty wynikające z braku dostępu do danych dotyczą oczywiście nie tylko zagranicznych firm. Awaria u jednego z polskich dostawców hostingu sprawiła, że przepadły nie tylko wszystkie dane, ale także ich kopie zapasowe. W efekcie klienci, wśród których znajdowało się również wiele e-sklepów, de facto stracili dostęp do skrzynek mailowych i firmowych baz danych.

W 2020 r. z awariami mierzyło się też wiele banków. Na przykład klienci Pekao, Alior Banku czy ING Banku Śląskiego mieli problem z logowaniem się na stronę banku i stracili możliwość dokonywania przelewów.

[8] https://itic-corp.com/blog/2019/05/hourly-downtime-costs-rise-86-of--firms-say-one-hour-of-downtime-costs-300000-34-of-companies-say-one--hour-of-downtime-tops-1million/

Ile może kosztować awaria? Analiza na przykładzie producenta z branży mięsnej

Firma produkcyjna wytwarza około 28 000 ton mięsa i jego przetworów miesięcznie (336 000 ton rocznie, 1 300 ton dziennie). Przy średniej cenie kosztów sprzedaży na poziomie około 20,00 zł/kg, średni dzienny przychód wynosi 26 mln zł.

Wszystkie obszary działalności firmy (skup surowca, przetwarzanie, sprzedaż, logistyka, utrzymanie, finanse i księgowość, administracja) opierają się na wykorzystaniu systemów informatycznych lub automatyki przemysłowej. Dywersyfikacja geograficzna kilku zakładów wymusza permanentne wykorzystanie systemów IT.

Bez zapewnienia rozwiązań klasy Disaster Recovery awaria w skrajnym przypadku doprowadziłaby do przestoju całej firmy, który kosztowałby 26 mln PLN w ciągu doby – tylko z tytułu nieosiągniętych korzyści, bez uwzględnienia kosztów stałych oraz innych strat. Zatrzymanie linii produkcyjnej może skutkować m.in. utratą jakości produktu końcowego, co może oznaczać utratę całej partii produktu, a w konsekwencji spadek zaufania klienta końcowego, jeżeli taki produkt zostanie dopuszczony do sprzedaży.

Analiza na przykładzie fikcyjnej firmy

Czy Twoja firma potrzebuje Disaster Recovery?

Badania dotyczące realnej ochrony danych pokazują, że często za deklaracjami nie stoją działania. Pomimo powszechnej świadomości zagrożenia awariami sieci, aż 75% firm nie posiada planu odzyskiwania danych. Tylko 39% ma plan na wypadek utraty kluczowych informacji. Jednak dopiero prawdziwy kryzys może zweryfikować czy wdrożone praktyki są skuteczne. W myśl taktyki treningu sportowców: „Im więcej potu na treningu, tym mniej krwi w boju" (Howard E. Wasdin).

Źródło: Raporty State of Salesforce Data Protection i Ponemon 2018 Cost of a Data Breach Study

Z badania Computerworld „Backup w firmie"[9] wynika, że polskie organizacje zasadniczo wiedzą, że muszą mieć procedury odzyskiwania danych. 75% uczestników deklaruje, że w ich firmach wdrożono schematy działania na wypadek awarii. Jeśli jednak przyjrzymy się głębiej dostępnym danym, to zauważymy duży rozdźwięk pomiędzy deklaracjami, a faktycznym przygotowaniem firm na nagłe awarie.

Choć zagrożeń, które mogą negatywnie wpłynąć na ciągłość działania jest coraz więcej, część firm nie wdraża rozwiązań Disaster Recovery. Dlaczego? Poniżej przedstawiamy najczęściej pojawiające się błędne przekonania, które stawiają pod znakiem zapytania bezpieczeństwo biznesu.

Mit pierwszy

Rozwiązanie Disaster Recovery nie jest dla mnie. Mój biznes nie jest zagrożony.

Rzeczywistość:

Każda firma wykorzystująca w swojej działalności systemy informatyczne jest zagrożona. Niezależnie od branży, wielkości przedsiębiorstwa, niekiedy wystarczy brak prądu lub zwykły ludzki błąd, by biznesowa ciągłość działania stanęła pod znakiem zapytania na długie godziny. Z danych CSO Online[10] wynika, że 70% osób doświadczyło utraty danych z powodu ich przypadkowego usunięcia, wirusów, błędów systemu, etc.

Doświadczenia pokazują, że firma powinna myśleć o Disaster Recovery zawsze wtedy, gdy:

- nie multiplikuje swoich serwerów w różnych lokalizacjach np. wykonuje backupy, ale przechowuje je w tej samej serwerowni, co systemy podstawowe
- jeśli przerwa dłuższa niż godzina w dostępie do danych po prostu się nie opłaca,
- infrastruktura oparta jest na sprzęcie starszym niż 3 lata (wraz z czasem eksploatacji - rośnie również ryzyko utraty danych)

[10] With the Bigger Dangers of Data Loss and Some Statistics, the Value of Backups is Becoming Prominent," Kwiecień 2018

Mit drugi

Moja firma przetrwa, jeśli dojdzie do awarii.

Rzeczywistość:

Nie każda awaria prowadzi do upadku firmy, ale każda niesie ze sobą określone konsekwencje, w tym finansowe. Z badań wynika m.in., że:

- średnio 68 dni roboczych tracą pracodawcy w skali roku z powodu przestojów IT[11],
- 43% firm nigdy nie wraca do działalności w następstwie awarii[12].

Zawsze świadomie należy ocenić ryzyko braku dostępu do danych i utraty ciągłości działania. W przypadku każdej większej firmy, nawet krótki przestój oznacza nie tylko brak możliwości sprzedaży produktu, ale niesie ze sobą straty wizerunkowe. Negatywne opinie w mediach czy na internetowych forach mogą istotnie wpłynąć na wyniki giełdowe i ogólną kondycję firmy.

[11] ERS Solutions, "The Costs of IT Downtime & Other Computer Downtime Statistics," 2019

[12] McGladrey and Pullen

Mit trzeci

Posiadamy plan Disaster Recovery.

Rzeczywistość:

Większość nowoczesnych firm ma wdrożone plany odtwarzania po awarii. Jednakże nie jest to równoznaczne z dostępem do technologii pozwalającej odtworzyć dane. Disaster Recovery zapewnia ciągłość biznesową przedsiębiorstwa dzięki dostępowi do niezależnego infrastrukturalnie centrum przetwarzania danych w przypadku awarii. Warto mieć to na uwadze, bo termin Disaster Recovery jest niekiedy niewłaściwie rozumiany. Po drugie, wiele planów Disaster Recovery jest przestarzałych i niedostosowanych do bieżących potrzeb. Raporty VMware Carbon Black wskazują na poważne braki w planowaniu awaryjnym Disaster Recovery:

- 84% firm wskazuje na brak procedur w razie awarii;
- 70% nie ma narzędzi do nadzoru bezpieczeństwa sieci i aplikacji;
- prawie 50% badanych przyznało, że ma braki kadrowe w IT;
- 48% przyznało, że ich braki są poważne;
- tylko 38% czuje się bardzo dobrze przygotowanych na sytuacje kryzysowe.

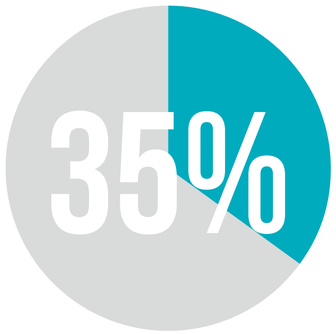
[13] https://itic-corp.com/blog/2019/05/hourly-downtime-costs-rise-86-of-firms-say-one-hour-of-downtime-costs-300000-34-of-companies-say-one-hour-of-downtime-tops-1million/

Co więcej, firmowe serwerownie nie gwarantują zachowania ciągłości biznesowej. Amerykańska firma konsultingowa ITIC wskazuje, że aż

85% firm dla utrzymania ciągłości biznesu potrzebuje dostępności do cyfrowych informacji na poziomie 99,99% dla krytycznych zasobów.

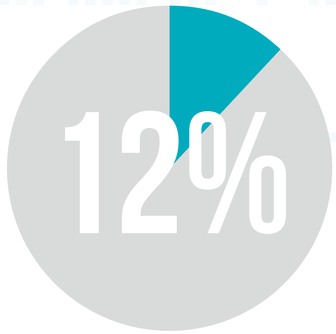
To oznacza maksymalnie 52 minuty przerwy w dostępie do danych w skali roku.[13] Taki poziom dostępności zapewnia niewiele serwerowni firmowych i tylko niektóre niezależne obiekty data center w kraju i zagranicą. Większość centrów danych posiada na ogół standard Rated 3 (99.982%) lub niższy. W Unii Europejskiej jedynie spółka Beyond.pl z obiektem Data Center 2 z Poznania przeszła niezależny audyt, na podstawie którego otrzymała najwyższy poziom bezpieczeństwa ANSI/TIA-942 Rated 4. Oznacza to poziom dostępności do danych na poziomie 99,995%, co jest równoznaczne z ograniczeniem niedostępności usługi do maksymalnie 26 minut w ciągu roku.

Co na to prawo?



Tylko 35% firm jest przekonanych, że ich infrastruktura i realizowane procesy odzyskiwania danych są zgodne z wymaganiami prawnymi.

Źródło: Dell EMC Global Data Protection Index



12% firm, które utraciły dane lub miały do czynienia z awarią na przestrzeni roku przyznało, że musiało zapłacić w związku z zaistniałą sytuacją kary.

W Polsce przykładem sektora, w którym prawnie wymagane jest wdrożenie rozwiązań technologicznych z obszaru Disaster Recovery jest bankowość. Banki są zobowiązane do posiadania systemu zarządzania ciągłością działania (business continuity), w tym planów utrzymania ciągłości działania oraz planów awaryjnych zapewniających nieprzerwane działanie banku (Rekomendacja 11 „M" KNF dotycząca zarządzania ryzykiem operacyjnym). Zgodnie z Rekomendacją D KNF dotyczącą zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, banki powinny też posiadać sformalizowane zasady dotyczące zarządzania infrastrukturą teleinformatyczną, w tym jej architekturą, poszczególnymi komponentami, wydajnością i pojemnością oraz dokumentacją, zapewniającymi właściwe wsparcie działalności banku oraz bezpieczeństwo przetwarzanych danych. Ma to ograniczyć możliwość powstawania awarii i incydentów.

Modele
Disaster Recovery – porównanie

Zdecydowana większość menedżerów IT zdaje sobie sprawę, że posiadanie planu Disaster Recovery jest niezbędne, by zachować ciągłość biznesową. Niestety, zdarza się, że trudno pozyskać zgodę ze strony biznesu na wdrożenie takich rozwiązań. W rezultacie wiele organizacji idzie na kompromis i nie otrzymuje takiego poziomu ochrony, jakiego wymagają aplikacje o znaczeniu krytycznym. Często firmy, które nie są zobligowane prawnie do posiadania planu Disaster Recovery ograniczają się do wyboru podstawowych rozwiązań w obszarze bezpieczeństwa danych, np. backupu. O ile jednak tworzenie kopii zapasowych danych jest pewnego rodzaju obowiązkową polisą OC, to Disaster Recovery jest formą polisy AC. I podobnie jak z polisą komunikacyjną, wybierając rozwiązanie Disaster Recovery należy znaleźć równowagę między ceną, potrzebami, a poziomem bezpieczeństwa.

Do niedawna firmy miały do dyspozycji w zasadzie tylko dwie możliwości. Mogły stworzyć własną zapasową lokalizację centrum danych (Disaster Recovery Center on-premise), bądź skorzystać z tej usługi od zewnętrznego dostawcy (Disaster Recovery Center off-premise). Obecnie te rozwiązania można uzupełnić lub zastąpić usługą odtwarzania danych w chmurze w modelu Disaster Recovery as a Service (DRaaS).

Przyjrzyjmy się rozwiązaniom dostępnym na rynku oraz ich wadom i zaletom.

Backup danych

Disaster Recovery Center w modelu on-premise (własne DRC)

Disaster Recovery Center w modelu off-premise (DRC od zewnętrznego dostawcy)

Disaster Recovery as a Service (DRaaS)

Modele
Disaster Recovery – porównanie

Backup danych

To najprostszy sposób zabezpieczania danych. W przypadku takiego rozwiązania kopiuje się dane do drugiej lokalizacji utrzymywanej lokalnie lub w chmurze. Jest to rozwiązanie stosunkowo powszechne, ale nie pozbawione wielu ograniczeń. Backup wykonuje się rzadko, na przykład raz na dobę. W przypadku awarii samo przywrócenie danych będzie niewystarczające i uruchomienie poprawnie działającego systemu może zająć długie godziny, a niekiedy tygodnie. Dodatkowo okresy pomiędzy backupami są „utracone.” Często popełnianym błędem w tym modelu jest przechowywanie backupu lokalnie tzn. we własnej serwerowni. Oznacza to, że Twoje dane i systemy nie są w żaden sposób zabezpieczone. W przypadku awarii, firma traci dostęp zarówno do infrastruktury podstawowej, jak i backupu.

Opieranie Disaster Recovery wyłącznie na kopiach zapasowych danych naraża organizacje na długie przestoje. Backup może być za to dobrym rozwiązaniem dla firm, które muszą archiwizować dane ze względów prawnych. Jednak dla zapewnienia ciągłości biznesowej, firmy muszą połączyć backup z innymi narzędziami do odtwarzania po awarii.

Modele
Disaster Recovery – porównanie

Disaster Recovery Center w modelu on-premise (własne DRC)

Stworzenie oddzielnej i niezależnej, zapasowej lokalizacji przechowywania infrastruktury w modelu on-premise gwarantuje pełną kontrolę nad procesem odzyskiwania danych po awarii. Jednak na ten model mogą sobie pozwolić głównie największe organizacje. Stworzenie własnego ośrodka zapasowego jest czasochłonne i wymaga znaczących inwestycji w infrastrukturę, oprogramowanie oraz utrzymanie. Dodatkowo takie rozwiązanie jest nieefektywne. Zapasowa lokalizacja wykorzystywana jest bowiem tylko w sytuacjach awaryjnych, gdy główne centrum danych nie funkcjonuje tak jak powinno. Co więcej, nawet po wdrożeniu rozwiązania Disaster Recovery Center (DRC) wiele organizacji staje przed wyzwaniami związanymi ze skalowaniem tego modelu wraz ze wzrostem liczby danych i aplikacji. Firmy muszą poświęcić znaczną ilość czasu na planowanie, negocjowanie warunków z dostawcami, konfigurację sieci, dostosowywanie zasad bezpieczeństwa oraz testowanie.

Zdarza się, podobnie jak w przypadku tworzenia kopii zapasowych, że firmy budują ośrodek zapasowy w tej samej lokalizacji, w której funkcjonuje infrastruktura podstawowa (np. fabryka, centrala firmy). Takie działanie nie gwarantuje firmie żadnego bezpieczeństwa. W takim scenariuszu awaria w postaci braku prądu, zalania serwerowni lub błędu ludzkiego dotknie zarówno lokalizację podstawową, jak i Disaster Recover Center. DRC obligatoryjnie musi być oddalone geograficznie od podstawowej serwerowni, ale jednocześnie powinno być bardzo dobrze skomunikowane z punktu widzenia czasu przesyłu danych (niskie opóźnienia). Powinno też gwarantować odpowiednio wysokie standardy z punktu widzenia bezpieczeństwa fizycznego i infrastrukturalnego (np. zasilanie, chłodzenie). W praktyce, firmowe DRC nie może być obiektem o niższym standardzie niż podstawowa lokalizacja.

Warto też pamiętać o kwestiach personalnych. Nie każdy specjalista IT potrafi tworzyć i zarządzać planami Disaster Recovery, a na działach IT często spoczywa zbyt wiele obowiązków operacyjnych. To sprawia, że skuteczne planowanie i odtwarzanie po awarii często jest dużym wyzwaniem. Sytuację utrudnia dodatkowo bardzo duża rotacja na stanowiskach związanych z utrzymaniem IT.

Brak korzyści „tu i teraz” sprawia, że wiele firm rezygnuje z budowy Disaster Recovery Center we własnym zakresie.

Modele
Disaster Recovery – porównanie

Disaster Recovery Center w modelu off-premise (DRC od zewnętrznego dostawcy)

Wdrożenie centrum zapasowego w zewnętrznym centrum danych znacząco zmniejsza nakład pracy niezbędny do wdrożenia Disaster Recovery. W przypadku awarii firma może sprawnie przełączyć swoje systemy informatyczne i swobodnie działać z innej lokalizacji bez konieczności ponoszenia inwestycji we własne zapasowe centrum danych. Oczywiście, wybierając data center warto pamiętać o tym, że nie każdy obiekt jest w stanie świadczyć usługi DRC. Analizując wybór ośrodka zapasowego trzeba zwrócić uwagę na poziom jego odporności na awarie. Wybrane data center musi spełniać co najmniej takie standardy w obszarze bezpieczeństwa fizycznego i infrastrukturalnego oraz łączności, jak podstawowe centrum danych lub wyższe. Stąd istotny jest wybór partnera, którego zaplecze gwarantuje najwyższą dostępność potwierdzoną niezależnymi certyfikacjami (np. ANSI/TIA) oraz świadczy SLA na wymaganym przez firmę poziomie. Warto też zwrócić uwagę na kwestię łączności. Komunikacja musi być redundantna i obsługiwana na bieżąco, a czas przesyłu danych między DRC, a firmą powinien być jak najkrótszy.

W przypadku outsourcingu DRC u zewnętrznego dostawcy, ogromną zaletą tego modelu jest to, że nie musimy martwić się o dostęp do specjalistów utrzymujących fizyczne urządzenia. DRC off-premise gwarantuje stały dostęp do kompetencji Disaster Recovery. Dodatkowo, koszty osobowe są rozłożone na wielu klientów, którzy korzystają z tej usługi.

Co więcej, dzięki wsparciu kompetencyjnemu, operator razem z klientem wypracowuje procedury akceptowalne w przypadku potrzeby wdrożenia planu awaryjnego. To pozwala zdecydowanie szybciej uruchomić niezbędne kroki, by zminimalizować skutki awarii i zapewnić ciągłość działania biznesu.

Disaster Recovery Center od dostawcy występuje w dwóch wariantach:

- z kolokacją
- z dzierżawą infrastruktury (Infrastructure as a Service).

W przypadku IaaS firma nie ponosi jednorazowych kosztów zakupu sprzętu, co wpływa dodatkowo na optymalizację rozłożenia wydatków w czasie.

Model Disaster Recovery Center u dostawcy jest więc pod wieloma względami lepszy od modelu on-premise. Jest efektywniejszy kosztowo, zapewnia bardzo wysoki poziom bezpieczeństwa i jest optymalny dla krytycznych systemów IT.

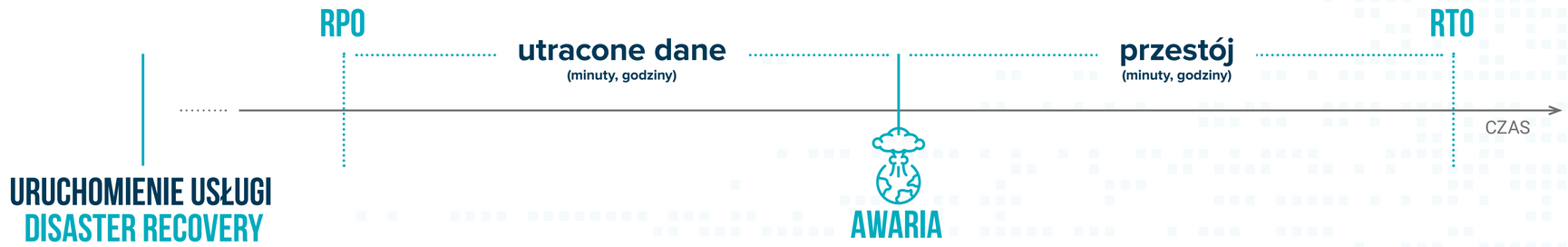
Modele
Disaster Recovery – porównanie

Disaster Recovery as a Service (DRaaS)

W obecnej sytuacji wiele firm skłania się ku modelowi usługowemu (DRaaS), który opiera się na skopiowaniu całego firmowego środowiska (nie tylko samych danych) i przechowywaniu go w chmurze (prywatnej lub publicznej). De facto jest to substytut zapasowego centrum danych (DRC).

Usługa DRaaS jest często traktowana jako polisa ubezpieczeniowa, z której korzystamy w czasie „katastrofy". Chmura, podobnie jak tradycyjne DRC, zapewnia łatwe zarządzanie, elastyczny czas odzyskiwania sprawności systemu (RTO) i pozwala łatwo uruchomić proces odzyskania danych z poziomu panelu zarządzania. Stała replikacja w chmurze i zautomatyzowane procesy pozwalają osiągnąć czas odtwarzania (RTO) na poziomie kilku minut (a nawet mniej). Dodatkowo środowisko zapasowe w chmurze eliminuje problemy i koszty związane z budową centrum danych i zakupu dodatkowej infrastruktury.

RPO i RTO. Odtwarzanie po awarii.



Modele
Disaster Recovery – porównanie

Disaster Recovery as a Service (DRaaS)

Czas realizacji projektu Disaster Recovery redukuje się do absolutnego minimum tj. usługa może zostać uruchomiona w zaledwie 1 dzień od podpisania umowy. Dzięki migracji z modelu CAPEX do OPEX firmy mogą liczyć na niższy inwestycyjny próg wejścia w rozwiązania Disaster Recovery. Skalowalność i elastyczność usługi DRaaS przekłada się na niskie koszty utrzymania (opłata miesięczna za dostępność i płatność wyłącznie za wykorzystane zasoby) oraz możliwość rezygnacji w dogodnym momencie.

Usługa może być świadczona w modelu chmury publicznej, prywatnej i hybrydowej, gdzie np. strategiczne dane finansowe replikuje się w chmurze prywatnej, a pozostałe w chmurze publicznej.

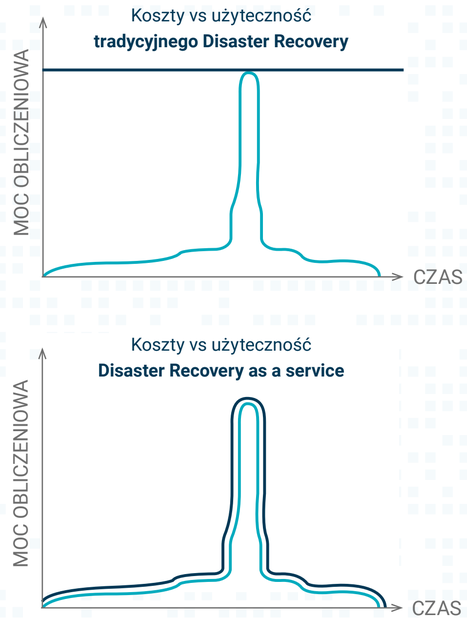
Dzięki temu z perspektywy kosztowej można zoptymalizować rozwiązanie dla firm o dowolnej wielkości i o różnorodnych potrzebach.

Firma Markets and Markets szacuje, że globalny rynek usług DRaaS wzrośnie z 5,1 mld USD w 2020 roku do 14,6 mld USD w 2025[14].

Brak nakładów inwestycyjnych indywidualne dopasowanie do klienta, optymalizacja kosztów operacyjnych przy zachowaniu wymaganego poziomu bezpieczeństwa sprawiają, że **usługi DRaaS zyskują na popularności.**

[14] https://www.marketsandmarkets.com/Market-Reports/recovery-as-a-service--market-962.html

Porównanie tradycyjnego DR i DRaaS



Modele
Disaster Recovery – porównanie

Kwestie organizacyjne

	DRC on-premise	DRC off-premise z kolokacją	DRC off-premise z IaaS	DRaaS
Lokalizacja sprzętu	Zasoby własne	Dostawca usługi	Dostawca usługi	Dostawca usługi
Właściciel sprzętu	Firma	Firma	Dostawca usługi	Dostawca usługi
Utrzymanie infrastruktury sprzętowej, budowlanej oraz źródeł zasilania pod potrzeby Disaster Recovery	Firma	Dostawca usługi	Dostawca usługi	Dostawca usługi
Infrastruktura Disaster Recovery	Dedykowana	Dedykowana	Dedykowana	Współdzielona lub chmura prywatna

Kwestie technologiczne

	DRC on-premise	DRC off-premise z kolokacją	DRC off-premise z IaaS	DRaaS
Licencjonowanie Disaster Recovery	Firma	Firma	Firma	Dostawca usługi
Upgrade produktów Disaster Recovery	Firma	Firma	Firma	Dostawca usługi
Utrzymanie infrastruktury systemowej Disaster Recovery	Firma	Firma	Firma	Dostawca usługi
Skalowanie Disaster Recovery adhoc	⊗	⊗	⊗	✓

Koszty Disaster Recovery

	DRC on-premise	DRC off-premise z kolokacją	DRC off-premise z IaaS	DRaaS
CAPEX	✓	✓ / ⊗	✓ / ⊗	⊗
Identyczne koszty w przypadku utrzymania w gotowości i użycia Disaster Recovery	✓	✓	✓	⊗
Inwestycyjny próg wejścia (najwyższy 4, najniższy 1)	4	3	2	1

Na co zwrócić uwagę przy wyborze rozwiązań Disaster Recovery?

Większość rozwiązań Disaster Recovery jest do siebie podobna, zwłaszcza jeśli chodzi o strukturę kosztów oraz tzw. Recovery Time Objective (RTO – szybkość odtworzeniowa). Natomiast już Recovery Point Objective (RPO – ilość utraconych danych, maksymalny akceptowalny czas pomiędzy wystąpieniem awarii, a backupem danych) różnicuje ofertę dostawców. Ale różnic jest więcej. Podpowiadamy na co zwrócić uwagę przy wyborze rozwiązań DR.

#1: Zidentyfikuj poziom RTO jaki zapewnia dostawca

Choć ochrona wszystkich firmowych danych jest możliwa, to może być bardzo kosztowna. Dlatego dobrym rozwiązaniem jest nadanie priorytetów aplikacji na podstawie ich znaczenia dla organizacji i czasu przywrócenia (RTO). Ten parametr określa dopuszczalny czas przywrócenia aplikacji do prawidłowego działania. Niektóre rozwiązania Disaster Recovery mają RTO określone w minutach, inne w godzinach, a jeszcze inne w dniach.

Potrzeby biznesowe narzucają różne poziomy RTO. Aplikacja, od której zależą przychody firmy nie może być niedostępna przez dłuższy czas. Na przykład dla zapewnienia poprawnego działania aplikacji do zarządzania transakcjami giełdowymi każda minuta może być na wagę złota.

W przypadku rozwiązań Disaster Recovery działa prosta zasada: im krótsze RTO, tym droższe jest odzyskiwanie aplikacji w wymaganym czasie. Dlatego organizacje powinny nadać krótszy poziom RTO dla krytycznych aplikacji biznesowych, a następnie odpowiednio dłuższy poziom aplikacjom niższego poziomu.

#2: Sprawdź gdzie przechowywane są Twoje dane

Aby zapewnić bezpieczeństwo np. w przypadku katastrofy naturalnej lub regionalnej awarii w dostępie do energii, zapasowa lokalizacja powinna znajdować się wystarczająco daleko od podstawowej, jednocześnie na tyle blisko, by zapewnić szybki transfer danych. Zapytaj w jakim centrum danych przechowywane są Twoje pliki, czy operator posiada jedną czy kilka serwerowni, jaki standard spełniają i ile wynoszą opóźnienia w transmisji danych (*latency*).

#3: Sprawdź jak wyglądają testy

Tworzenie planu odzyskiwania danych po awarii nie jest czynnością jednorazową. Centra danych nie są statyczne – istniejące aplikacje są aktualizowane, pojawiają się też nowe.

Organizacje muszą często testować swój plan odzyskiwania po awarii, a najlepsze praktyki sugerują realizację takich działań co najmniej raz na kwartał. Optymalna strategia Disaster Recovery powinna oferować klientom realizację obszernych, nieprzerwanych testów i dostarczać szczegółowe raporty nie wpływając przy tym na realizację bieżących zadań.

#4: Sprawdź niezawodność i doświadczenie dostawcy

Usługi DR oferuje na rynku wielu dostawców. Jednak skala, zakres ich działalności oraz poziom zaawansowania stosowanych rozwiązań jest różny. Ponieważ organizacje muszą polegać na rozwiązaniach Disaster Recovery w krytycznych momentach, gdy ich główne centra danych nie działają, niezawodność infrastruktury Disaster Recovery i doświadczenie dostawcy powinny być kluczowym czynnikiem przy wyborze usług.

Sprawdź jak szeroką gamę rozwiązań Disaster Recovery oferuje dostawca, jakie ma doświadczenie w tym zakresie, czy jest tylko resellerem czy operatorem, który w 100% odpowiada za bezpieczeństwo krytycznych systemów. Dowiedz się jaki poziom niezawodności infrastruktury jest w stanie zagwarantować w umowie SLA.

Disaster Recovery w Beyond.pl

Bez względu na potrzeby Twojej organizacji w zakresie Disaster Recovery, Beyond.pl zapewnia wsparcie w każdym modelu:

- backup, również w modelu Rapid Restore;
- Disaster Recovery Center (kolokacja lub wynajem infrastruktury);
- Disaster Recovery as a Service;

Co istotne, nasze cross-technologiczne kompetencje umożliwiają projektowanie i wdrażanie rozwiązań hybrydowych, które łączą model DRC dla systemów najbardziej krytycznych z modelem DRaaS dla aplikacji wspierających. Takie podejście optymalizuje finansowo inwestycję, a z drugiej strony zapewnia business continuity na właściwym poziomie.

Współpracując z Beyond.pl w obszarze Disaster Recovery nie trzeba iść na kompromisy – rozwiązanie jest dostosowane do potrzeb i oczekiwań, zarówno jeśli chodzi o gwarancje SLA na poziomie do 99,9999%, technologię, jak i parametry RTO oraz RPO. Kompleksowość oferty pozwala nam także doradzać klientom w wyborze modelu Disaster Recovery, tak by spełniał on ich potrzeby biznesowe oraz uwzględniał możliwości finansowe.

Co wyróżnia Beyond.pl jako dostawcę usług Disaster Recovery?

Najwyższy poziom bezpieczeństwa

Beyond.pl to centra przetwarzania danych typu core i hyper-edge o docelowej mocy 42MW. Spółka obsługuje dwa nowoczesne obiekty Data Center zlokalizowane w Poznaniu. Obiekt Data Center 2 jest jedynym centrum danych w Unii Europejskiej spełniającym rygorystyczne wymagania niezależnej certyfikacji ANSI/TIA-942 Rated 4 (design, build oraz operate). Certyfikat na najwyższym poziomie – Rated 4 – potwierdza standardy bezpieczeństwa dla data center w zakresie projektowania, mechaniki, zasilania i telekomunikacji gwarantując najwyższy poziom dostępności – do 99,995%.

Bezpieczeństwo fizyczne i infrastrukturalne obiektu, który ma pełnić funkcję zapasowej serwerowni musi być równie wysokie (lub wyższe) w porównaniu do obiektu podstawowego. W tym zakresie Data Center 2 Beyond.pl jest niekwestionowanym liderem.

Łączność

Oferujemy neutralność telekomunikacyjną i dostęp do globalnych operatorów – w tym dla dostawców klasy Tier 1, największego w Polsce punktu wymiany ruchu internetowego EPIX oraz do wielu regionalnych i lokalnych dostawców Internetu. Jesteśmy redundantni telekomunikacyjnie i otwarci na współpracę ze wskazanymi przez klientów dostawcami.

Lokalizacja w strategicznym punkcie Europy – dokładnie 300 km od Warszawy i Berlina – gwarantuje optymalny czasu transferu danych. Latency do Warszawy czy Berlina to zaledwie 4ms, a Frankfurtu 10ms. W przypadku świadczenia usług Disaster Recovery gwarancja stabilnej łączności i szybki transfer danych jest jednym z kluczowych elementów wyboru dostawcy.

Sprawdzone technologie

Usługi Disaster Recovery oferowane przez Beyond.pl działają w oparciu o najlepsze technologie i infrastrukturę klasy premium: w tym oprogramowanie VMware Cloud Director Availability, macierze Pure Storage, infrastrukturę HPE oraz Dell, procesory Intel. Współpracujemy z najlepszymi na rynku, aby dostarczać najbezpieczniejsze usługi Disaster Recovery.

Kompleksowe portfolio usług

Klienci Beyond.pl mogą skorzystać z rozbudowanego portfolio uzupełniających usług, m.in. kolokacji, IaaS, chmury prywatnej i globalnej czy usług wspierających managed services optymalizujących koszty i zwiększających poziom bezpieczeństwa.

Usługi Disaster Recovery w Beyond.pl

Dla najbardziej wymagających Klientów Beyond.pl posiada ofertę Disaster Recovery Center w ramach której:

- RTO i RTO mogą wynosić poniżej 1s dzięki synchronicznej replikacji danych;
- Klienci mogą korzystać z najszybszych i najbezpieczniejszych pamięci masowych na rynku;
- gwarantowana jest dostępność do danych nawet przez 100% czasu;

Obok Disaster Recovery Center, Klienci Beyond.pl mogą skorzystać z usługi Disaster Recovery as a Service, którą charakteryzuje:

1. Bardzo szybkie uruchomienie usługi i łatwe zarządzanie

Usługa jest uruchomiona zaledwie w kilka godzin/1 dzień od podpisania umowy. W przypadku awarii zapasowe środowisko jest uruchamiane nawet w ciągu 1 minuty.

Jego udostępnienie wymaga:

- konfiguracji parametrów odtworzenia danych (częstotliwość replikacji, czas przywrócenia danych gwarantowany umową SLA, etc);
- uruchomienia wirtualnej maszyny u Klienta;
- instalacji oprogramowania;

Cały proces odbywa się przy minimalnym zaangażowaniu Klienta. Dodatkową zaletą usługi jest możliwość elastycznej zmiany konfiguracji w przypadku rozbudowy zasobów i dostęp do wszystkich funkcjonalności z poziomu jednej konsoli.

Usługi Disaster Recovery w Beyond.pl

2. Wiele wariantów

W ramach usługi DRaaS klient może skorzystać z 3 podstawowych pakietów określających wymagany poziom bezpieczeństwa, m.in. szybkość odtworzenia środowiska oraz częstotliwość replikacji danych. Dodatkowo ma możliwość konfiguracji środowiska zapasowego według własnych kryteriów i dopasowania go ściśle do własnych potrzeb.

	Standard	Medium	High
RPO*	12 H	8 H	15 MIN
Ilość zachowanych replikacji	2	7	14
Okres przechowywania replikacji	1 DOBA	3 DNI	1 TYDZIEŃ
Ilość darmowych testów w roku	1	1	1
RTO**	24 H	12 H	USTALANE INDYWIDUALNIE

Katalog polityk do umowy SLA

3. Elastyczny model rozliczeń

Beyond.pl oferuje 2 modele rozliczania usług chmurowych:

1. Model abonamentowy, gdzie klient płaci z góry za zarezerwowane zasoby stałą kwotę miesięczną;
2. Model elastyczny, w którym płaci jedynie za zużyte zasoby rozliczane godzinowo lub dobowo.

* Możliwość zapewnienia klientowi wymaganego RPO zależy od wielkości replikowanego środowiska oraz łącza internetowego klient-Beyond.

** Możliwość zapewnienia klientowi wymaganego RTO zależy od wielkości środowiska uruchamianego awaryjnie oraz bieżących możliwości Beyond.

Podsumowanie

Migracja firm do online i bardzo szybko rosnąca liczba gromadzonych i przetwarzanych danych sprawia, że z roku na rok rośnie znaczenie nieprzerwanego dostępu do cyfrowych zasobów. Wraz z nim rośnie też liczba zagrożeń, którym muszą sprostać przedsiębiorstwa. To nie tylko pożar, powódź, błąd ludzki czy awaria sprzętu, ale też coraz większa aktywność cyberprzestępców, które skutecznie mogą zagrozić stabilności przedsiębiorstwa.

Przez wiele lat rozwiązania Disaster Recovery gwarantujące ciągłość działania i szybkie odtworzenie danych w przypadku awarii były dostępne jedynie dla dużych organizacji. Musiały one dysponować odpowiednimi zasobami kapitałowymi i osobowymi, niezbędnymi do tego, by zaplanować, wdrożyć, a następnie utrzymać środowisko zapasowe na odpowiednim poziomie.

Wraz z rozwojem chmury obliczeniowej i modeli usługowych pojawiły się rozwiązania alternatywne, takie jak DRaaS. Nie tylko upraszczają one cały proces zarządzania ciągłością działania, ale zapewniają sprawne odtwarzanie danych po awarii. Co bardzo ważne – przy niskim koszcie i dużej elastyczności zarówno jeśli chodzi o dobór istotnych dla bezpieczeństwa parametrów, jak i skalowalność infrastruktury.

To sprawia, że rozwiązania Disaster Recovery są technologicznie i finansowo w zasięgu ręki niemal każdej organizacji. Dziś bardziej niż kiedykolwiek warto zainwestować w dobrą polisę AC dla danych i systemów, które wspierają działalność Twojego przedsiębiorstwa.

OPRACOWANIE MERYTORYCZNE:

beyond.pl

PARTNERZY:

vmware

ARROW

kontakt@beyond.pl +48 61 667 48 90