

Jak Commerzbank odtworzył operacje IT po 11 września 2001

Autor: Joseph Walton

7 września 2001, po zakończeniu implementacji rozwiązań back-upowych, pracownicy Commerzbank w Nowym Jorku nie mogli przewidzieć zdarzeń, które wstrząsnęły światem zaledwie cztery dni później. Krytyczne dane banku zostały zabezpieczone niedługo po tragedii World Trade Center, dzięki kombinacji działań przygotowawczych, odrobinie szczęścia i ludziom gotowym do poświęceń.

Jednym z kluczowych celów dla 16 pod względem wielkości banku na świecie było uzyskanie zdolności odtworzeniowej tak szybko, jak to możliwe w przypadku przerwy w działalności ich nowojorskiej siedziby. Choć giełdzie na Wall Street ponowne uruchomienie notowań zajęło niemal tydzień, zabezpieczone informacje Commerzbanku były dostępne nawet zanim pracownicy firmy zdołali zebrać się w zapasowej lokalizacji oddalonej o 50 km od nowojorskiego centrum finansowego. Dane Commerzbanku były replikowane z głównej siedziby w budynku Two World Financial Center –zaledwie o 100 metrów od wież World Trade Center– do ośrodka zapasowego w Rye, N.Y.

Mimo, iż budynek Commerzbanku nadal stał, podmuch eksplozji wybił setki okien a popiół pokrył biura i znajdujący się w nich sprzęt.

Oprogramowanie do replikacji danych wdrożone w Commerzbanku uratowało jego dane i umożliwiło ich natychmiastowe udostępnienie w ośrodku zapasowym. Transakcje klientów, bazy danych finansowych, poczta elektroniczna i inne krytyczne aplikacje były zabezpieczone.



Nowy Jork, 21 września 2001 – budynek w pobliżu World Trade Center został poważnie uszkodzony w wyniku ataku terrorystycznego. Zdjęcie: Michael Rieger/ FEMA News Photo

"Zanim uruchomiliśmy naszą nową infrastrukturę składowania danych, swój back-up opieraliśmy na taśmach. Przy stosowaniu rozwiązania back-up'u na nośnikach magnetycznych, nasze dane były narażone na wysokie ryzyko," przyznał Gene Batan, wiceprezes Commerzbank ds. technologii informatycznych na terenie Ameryki Północnej. "W przypadku katastrofy, integralność naszych informacji całkowicie zależała od tego, kiedy ostatnio wykonywano kopie zapasowe, a czas odtworzenia zajęłoby nam co najmniej kilka dni. Nasz dostawca pamięci masowych zapewnił nam replikację w czasie rzeczywistym i skrócił czas odtworzenia od kilku dni do kilku minut."

Szybkość i pewność są jednakowo ważne dla firmy, która obsługuje codziennie transakcje o wartości 30 miliardów USD. Menadżerowie IT używają terminu "fail-over" na określenie sytuacji, w której jeden system ulega awarii a sieć przenosi dane lub inne zasoby na rozwiązanie zapasowe. Commerzbank posiadał zdolność natychmiastowego failover'u dla swej sieci pamięci masowej (SAN), która wspierała wszystkie środowiska Unix'owe i Windows 2000. Commerzbank mirrorował swoją sieć SAN na dedykowany system pamięci masowej w ośrodku zapasowym poza miastem, tworząc standardowe, natychmiast dostępne i funkcjonalne środowisko dla swych krytycznych danych.

"Gdyby nasze platformy Unix'owe i Windows 2000 nadal polegały na taśmowych rozwiązaniach back-up'owych, całkowite odtworzenie danych zajęłoby nam tygodnie," mówi Alban Bramble, zastępca wiceprezesa Commerzbank odpowiedzialny za platformy Unix'owe i Windows 2000. "Tymczasem, dzięki zastosowanemu oprogramowaniu SRDF [Symmetrix Remote Data Facility], natychmiast uzyskaliśmy w pełni zmirrorowane dane w ośrodku zapasowym. Nasze środowiska Unix'owe i Windows 2000 pozostały nietknięte i bezpieczne, umożliwiając nam skupienie się na innych problemach, które wyniknęły wskutek kryzysu z 9 września."

Szybkie odtworzenie

Proces przywracania operacji można nazwać „odtworzeniem”, ale gdy w grę wchodzi miliardy dolarów w transakcjach, każda minuta opóźnienia jest bardzo kosztowna. Zamiast „odtworzenia” firmy chcą „ciągłości działania”, licząc od chwili wystąpienia awarii. Trzeba zacząć działać jak najszybciej. Jeśli się to

nie uda, zamówienia, e-maile, zapytania, faktury i faksy zaczynają się piętrzyć, powodując opóźnienia, których być może nigdy nie da się nadrobić.

Po 11 września ośrodek zapasowy Commerzbanku stał się, z konieczności, głównym ośrodkiem przetwarzania. Natychmiast zjawili się pracownicy techniczni, by wesprzeć proces odtwarzania danych banku, których nie udało się odzyskać i zapewnić, że infrastruktura informatyczna jest zabezpieczona. W procesie tym brało udział 8 osób, pracujących w systemie zmianowym (1 zmiana trwała 24h).



Fot: FEMA News

Najwyższym priorytetem dla Commerzbanku stało się odtworzenie z taśm tych krytycznych informacji, które nie były objęte replikacją danych. Niektóre dane zachowane na taśmach znajdowały się początkowo na wielu platformach pochodzących od różnych dostawców, ale w chwili katastrofy do akcji ruszył zespół firmy EMC. Commerzbank potrzebował wielu terabajtów dodatkowej pojemności w swym ośrodku zapasowym, aby odtworzyć taśmy z krytycznymi informacjami.

EMC zdołało dostarczyć nowe produkty, skonfigurować środowisko i w pełni odtworzyć informacje Commerzbanku w czasie krótszym niż 36 godzin. Pojemność systemów w ośrodku zapasowym szybko została podwojona, podczas gdy same dane zostały zabezpieczone dodatkową kopią.

"W ciągu 24 godzin mieliśmy wypożyczony cały niezbędny sprzęt," wspomina Batan. "Tyle czasu wystarczyło, by zrobić to, co konieczne. Gdy w ośrodku zapasowym brakowało nam dysków, serwis sprowadził je samochodem z Bostonu w czasie, kiedy jeszcze wstrzymany był ruch powietrzny. Zapewnili nam techników i pracowników pomocniczych, którzy zastępowali naszych ludzi pracujących w nieludzkim wymiarze czasu."

"Sukces naszego planu ciągłości działania zawdzięczamy technologii i ogromnemu wsparciu ze strony serwisu. Jego pracownicy utrzymywali stabilne środowisko, a był to skomplikowany projekt," dodaje Bramble. "Ludzie są najważniejsi. To oni sprawiają, że technologia działa."

Ważna lekcja

Działy IT w firmach takich, jak Commerzbank wyciągnęły lekcję na przyszłość ze zdarzeń 11 września. Poniżej znajdują się najważniejsze wnioski.

Wniosek 1: Odległość ma kluczowe znaczenie.

Kto mógł przypuszczać, że mosty i tunele mogą stanowić słabe ogniwo w infrastrukturze IT? 11 września zmienił krajobraz demonstrując, że dostęp do ośrodka zapasowego może być ograniczony. Fizyczna skala katastrofy może dalece wykraczać poza lokalną siedzibę, odcinając ludzi i kanały komunikacji między lokalizacjami. Wiele osób nie było w stanie dostać się do ośrodka zapasowego z powodów trudnych do przewidzenia – wiele ulic, mostów, tuneli i wszystkie porty lotnicze zostały zamknięte.

Wniosek 2: Taśmy nie są skuteczne.

Stało się oczywistym, że poleganie na taśmach jako na nośniku kopii zapasowych i rozwiązaniu awaryjnym sprawia, że organizacje są nadal podatne na ryzyko. Specjaliści IT, którzy kiedyś wierzyli, że taśmy są "zupełnie wystarczające" odkryli, że dostęp do nich może być ograniczony lub wręcz niemożliwy. Czas odtworzenia może okazać się zbyt długi dla efektywnego wznowienia procesów biznesowych. Nawet, gdy można było odzyskać i odtworzyć pliki zachowane na taśmach, wiele z nich okazywało się uszkodzonych lub niewiarygodnych. Czas odtworzenia często wynosił pięć dni – a proces ten zwykle wymagał co najmniej jednego powtórzenia. Należy wziąć pod uwagę także fakt, iż taśma jest podatna na działanie błędu ludzkiego. W wielu przypadkach informacje nie były back-up'owane lub okazywało się, że kopie zapasowe były niespójne.

Wniosek 3: Wszystkie aplikacje mogą być krytyczne.

Poczta elektroniczna stała się jednym z najbardziej krytycznych środków komunikacji korporacyjnej. Gdy zagrożone są kanały komunikacji, zagrożony jest też biznes. 11 września, wiele firm odkryło, że opracowywane oferty, umowy handlowe i dokumenty potwierdzające zawarcie transakcji były przechowywane wyłącznie w ich systemach poczty elektronicznej. Chodzi jednak o coś więcej niż e-mail. Dziś, w przeważającej większości, operacje i aplikacje są współzależne. Jeśli utracona zostanie zawartość zasobów informacyjnych znajdujących się w aplikacjach wspomagających, strata ta często ma wpływ na pierwszoplanowe aplikacje takie, jak CRM lub ERP.

Wniosek 4: Niespójne kopie zapasowe są bezużyteczne.

Przed 11 września tworzenie kopii zapasowych traktowane było jako uciążliwy obowiązek, nie zawsze wykonywany z wystarczającą precyzją lub regularnością. Dziś, stało się ono imperatywem. Różne harmonogramy i strategie back-up'owania dla różnych aplikacji oznaczają, że informacja niezbędna do podtrzymania procesów biznesowych nie może być poddawana żadnym

przybliżeniom. Niespójne kopie zapasowe także znacznie wydłużają sam proces odtworzenia.

Wniosek 5: Składanie wszystkiego na barki ludzi nie wystarczy.

W katastrofie o rozmiarach tej z 11 września ludzie myślą przede wszystkim o swoich rodzinach. Nawet, jeśli pracownicy byli gotowi do pracy, wielu spośród nich nie mogło dostać się do ośrodka zapasowego z powodu zamkniętych dróg i ze względów bezpieczeństwa. W największym stopniu sprawdziły się te systemy informatyczne, które były zdolne do odtworzenia w sposób automatyczny i eliminowały konieczność interwencji człowieka oraz ręcznych działań takich, jak transport i wkładanie taśm. Co więcej, zmęczeni, zestresowani pracownicy łatwo popełniają błędy, które wydłużają proces odtworzenia.

Wniosek 6: Dwie lokalizacje to za mało.

Nawet te firmy, które posiadały ośrodek zapasowy pozostały całkowicie bezbronne wskutek katastrofy – ich procesy biznesowe polegały teraz na pojedynczej lokalizacji. Biorąc pod uwagę kumulację pracy u dostawców usług, firmy te zmuszone były funkcjonować poniżej ustalonych poziomów polityki bezpieczeństwa i ciągłości działania przez długi czas. Oczywistym jest więc fakt, że należy zastosować nowe sposoby rozproszenia informacji i kluczowych zasobów.

Wniosek 7: Firmy, które polegały na taśmach lub zewnętrznym dostawcy, miały w wielu wypadkach trudności w dotrzymaniu czasów odtworzenia.

Powód? Dostawcy usług disaster recovery zakładają, że tylko niewielki procent ich klientów będzie potrzebował wsparcia w tym samym czasie. W związku z wielką katastrofą skoncentrowaną pod względem geograficznym, wystąpiło nagłe, jednoczesne i masowe zapotrzebowanie na ich ograniczone zasoby.

Wniosek 8: Ludzie są niezastąpieni - podobnie jak informacja.

Powierzchnię można wynająć. Telefony komórkowe mogą zastąpić telefonię stacjonarną. Jednak dla każdej firmy, ciągłość działania zależy od dostępności kluczowych pracowników oraz krytycznych informacji i systemów. Gdy ludzie byli już bezpieczni, to właśnie informacja okazała się jednym z tych zasobów firmy, której nie można było zastąpić wystarczająco szybko – a bez niej, większość pracowników nie była w stanie odtworzyć działalności biznesowej.

Wniosek 9: Wszystkie scenariusze są prawdopodobne.

Katastrofa 11 września i kolejne zdarzenia wzmogły znaczenie posiadania planów ciągłości działania. Menedżerowie IT stoją w obliczu konieczności utrzymania delikatnej równowagi pomiędzy potrzebą zapewnienia odpowiedniego poziomu bezpieczeństwa firmie a korporacyjną rzeczywistością finansową i dostępnymi zasobami.

Nowa era w BCP

Firmy takie, jak Commerzbank rozszerzają swą definicję krytyczności. W obliczu konieczności uruchomienia działalności po katastrofie, firmy nauczyły się na własnej skórze, które aplikacje są krytyczne dla podstawowych procesów biznesowych.

Poprzednio, pojęcie "krytyczny" oznaczało, które aplikacje i informacje nie mogą, w żadnym wypadku zostać utracone. Teraz, określenie "krytyczny" zostało ponownie zdefiniowane i poszerzone tak, by zawierało także te aplikacje i informacje, które są konieczne do natychmiastowego uruchomienia obsługi klienta. Aplikacje takie, jak poczta elektroniczna stały się "krytyczne" w oparciu o ich znaczenie dla funkcjonowania firmy.



Nowy Jork, NY, 20 września 2001 – Kurz pokrył biuro w budynku obok World Trade Center.
Fot.: Andrea Booher/ FEMA News Photo

Zrewidowano także kwestie dotyczące personelu. Musi istnieć zespół zapasowy dla ludzi odpowiedzialnych za pierwszą reakcję na zdarzenie – zarówno w odniesieniu do odtwarzania danych, jak i w przypadku każdego długotrwałego projektu. Menedżerowie muszą uświadomić sobie długoterminową potrzebę zapewnienia nowych talentów. Czasem najtrudniejsze zadania będą wykonywane po wielu dniach lub tygodniach od wystąpienia katastrofy i nikt nie chce stracić i tak już przepracowanych najlepszych specjalistów IT.

Według Batana, redundantne systemy komunikacji mogą być równie ważne jak moc obliczeniowa systemów back-up'owych i pamięci masowych. Posiadanie sieci VPN lub połączeń typu dial-in umożliwiających pracę ludziom rozproszonym w wyniku katastrofy jest nie do przecenienia. Oznacza to, że firmy szukają sprzętu back-up'owego w postaci telefonów satelitarnych, przenośnych generatorów i usług całodobowego wsparcia technicznego.

Planowanie ciągłości działania musi być traktowane jako integralna część procesu produkcji i wdrożenia oprogramowania. Mimo, iż konieczność kompleksowego rozwiązania zapasowego jest oczywistością wśród menedżerów IT, chcą oni wiedzieć jak mogą stworzyć rozwiązanie, które stanie się aktywnym zasobem firmy. Poprzednio, wiele zapasowych ośrodków stało opustoszałych w oczekiwaniu na katastrofę, spełniając rolę specyficznej polisy

ubezpieczeniowej – beзуżyteczne dopóki coś się nie wydarzy. Teraz, firmy zwracają się ku "produktywnym zabezpieczeniom" - środowiskom, które umożliwiają wykorzystanie ośrodków zapasowych do testowania aplikacji, kontroli integralności baz danych, backup'ów i do innych codziennych zadań, które zapewniają zwrot z inwestycji.

"Jeżeli używamy tych zasobów każdego dnia, kluczowe staje się znaczenie sieci pamięci masowej, zdolnej elastycznie wspierać praktycznie dowolną platformę systemową," twierdzi Batan. *"Nikt nie może przewidzieć, kiedy uderzy w nas katastrofa, ani jak długo firma będzie musiała działać z ośrodka zapasowego."*

"Jesteśmy zdecydowani rozbudowywać swój system pamięci masowej i wzmacniać sieć SAN. Ze względu na nasze doświadczenia, naprawdę musimy posiadać aktywne centra przetwarzania danych w obu lokalizacjach, niż bierny ośrodek wykorzystywany wyłącznie do działań odtworzeniowych. Musimy przyznać, że nasze wdrożenie zostało zakończone w samą porę."

"Posiadanie skoordynowanego zestawu produktów z pewnego źródła w połączeniu z najwyższej jakości usługami sprawiło, że firmy takie, jak Commerzbank mogą przetrwać katastrofę o skali porównywalnej z atakami z 11 września," przyznaje. *"Niczego nie wolno nam zostawiać przypadkowi."*

Od czasu wydarzeń z 11 września, Commerzbank zdecydował przenieść większość swych zasobów informacyjnych i aplikacji na model replikacji opartej na dyskach i znacząco zwiększa wartość oraz stopień wykorzystania swego ośrodka zapasowego.

Commerzbank wykorzystuje możliwości, jakie daje zdalna replikacja i oprogramowanie do zarządzania pamięcią masową, do prowadzenia działalności w obu lokalizacjach jednocześnie, za pośrednictwem jednego centrum zarządzania i bez jakichkolwiek przerw.

O autorze: Joseph Walton jest wiceprezesem EMC Corporation, dostawcy systemów pamięci masowych, oprogramowania i usług.