Jak zabezpieczyć dane, by zachować ciągłość działania biznesu?

Michał Jakś
Chief Security Officer, Talex SA
Mariola Bąk
Koordynator projektów, Talex SA

Wg raportu IDC FutureScape cyfrowa transformacja jest najważniejszym elementem strategii biznesowej przedsiębiorstw w końcówce tej dekady. Aby sprostać wymaganiom rynku i oczekiwaniom klienta szeroko rozumianej branży usługowej, a zwłaszcza dynamicznie rozwijających się usług e-commerce, firmy logistyczne wdrażają zaawansowane rozwiązania technologiczne. Dużym zainteresowaniem cieszą się nowoczesne systemy ERP, SCM i WMS. Ci najbardziej innowacyjni próbują rozwiązań opartych na uczeniu maszynowym, sztucznej inteligencji, Internecie rzeczy. Wszystko po to, by redukować koszty, ograniczać opóźnienia, eliminować ryzyko i budować przewagę konkurencyjną.

Skuteczność działania w logistyce zależy przede wszystkim od efektywnego przepływu informacji. Ilość danych przetwarzanych w czasie rzeczywistym wymaga od firm posiadania nie tylko zaawansowanych systemów, ale także niezawodnego i wydajnego środowiska IT o wysokiej dostępności. Niestety wiąże się to z wysokimi kosztami. Liczy się bowiem nie tylko zakup i wdrożenie najnowocześniejszego oprogramowania, sprzętu, zatrudnienie specjalistów, utrzymanie środowiska. Istotnym elementem staje się bezpieczeństwo informacji oraz ciągłość działania organizacji.

Zarządzający organizacją muszą zadać sobie kluczowe pytanie: Co się stanie, gdy podstawowa infrastruktura IT, wspierająca funkcjonowanie firmy, przestanie nagle działać – przez godzinę, dzień lub dłużej? Jaki będzie koszt utraty danych lub przerwania ciągłości działania na skutek awarii sprzętu, katastrof naturalnych jak powódź, pożar, czy tylko przez nieuwagę pracownika, który jednym kliknięciem lub niewłaściwą komendą usunie lub uszkodzi dane produkcyjne? Do tego dochodzą coraz większe zagrożenia związanie z cyberbezpieczeństwem, jak choćby działanie złośliwego oprogramowania, ataków ransomware szyfrującego nasze dane itp.

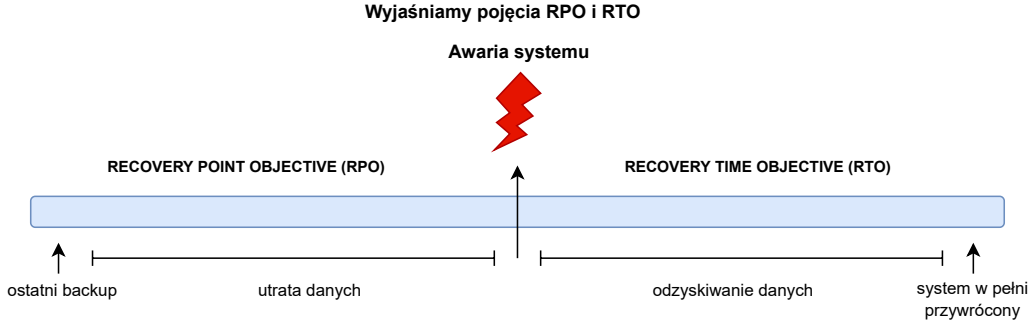
Firma analityczna IDC szacuje średni koszt przestoju na 200 000 USD na godzinę. Gartner obliczył, że firmy tracą średnio 5600 USD za każdą minutę przestoju. Oprócz strat finansowych zostaje mocno nadszarpnięty wizerunek organizacji czy marki. Klienci tracą zaufanie, które trzeba będzie długo i kosztownie odbudowywać. Dla niektórych skutki mogą okazać się wręcz katastrofalne. Wg szacunków IDC 80% firm, które nie mają planów usuwania skutków awarii, upadnie w razie takiego zdarzenia.

Także przepisy prawa wymuszają na organizacjach działania związane z bezpieczeństwem danych. RODO w artykule 32 pkt. 1 c, wyraźnie wskazuje konieczność zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

Nieodzowne w każdej firmie staje się więc wdrożenie odpowiednich strategii przetrwania i rozwiązań zapewniających ciągłość biznesu (planów awaryjnych, planów ciągłości działania), które uwzględnią zabezpieczenie danych i ciągłości pracy krytycznych dla firmy systemów w Zapasowym Centrum Przetwarzania Danych – czyli rozwiązania typu DRC (*Disaster Recovery Center*).

Możliwie mała utrata danych w przypadku katastrofy lub poważnej awarii oraz akceptowalnie dla biznesu niskie czasy przywrócenia usług wymagają przede wszystkim stworzenia profesjonalnej koncepcji Disaster Recovery, dostosowanej do potrzeb i charakteru działalności organizacji. Wymaga to zwykle przeprowadzenia analizy różnych obszarów IT funkcjonujących w firmie, czego efektem jest oprócz ustalenia stanu obecnego, opis wymaganych zmian i zagrożeń, i przede wszystkim wskazanie stanu docelowego – czyli propozycja udoskonaleń oraz wdrożeń sprawdzonych i standardowo stosowanych rozwiązań, wraz z oszacowanie ich kosztów. Niezbędne jest też określenie optymalnych wartości **RTO** (*Recovery Time Objective*) - czasu odtwarzania aplikacji i procesów po wystąpieniu awarii oraz **RPO** (*Recovery Point Objective*) - czyli akceptowalnego poziomu utraty danych (zobacz rysunek poniżej).

Dobrze przygotowana koncepcja powinna uwzględniać zagadnienie cyklicznego testowania funkcji odtwarzania po katastrofie, ponieważ tylko rutynowe i dobrze przećwiczone procedury



oraz specjalizowane systemy automatyzacji DR (ang. *Disaster Recovery Automation*) pozwalają na zachowanie gotowości i dużej skuteczności przełączenia systemów w sytuacji kryzysowej. Warto też uwzględnić porównanie i możliwość wyboru pomiędzy tradycyjnym Disaster Recovery Center budowanym w ramach własnej infrastruktury klienta i dostawcy usługi z coraz bardziej popularnym rozwiązaniem chmurowym, czyli DRaaS (Disaster Recovery as a Service).

Jak wybrać dostawcę usług

Kiedy już zdecydujemy się na outsourcing naszego systemu recovery, postanowimy przekazać swoje dane i systemy w ręce profesjonalistów, w głowie każdego menadżera rodzą się kolejne pytania. Czy dostawca, którego wybrałem nie zawiedzie mnie w chwili, kiedy pojawią się trudności? Największych, najbardziej renomowanych dostawców, spotykają przecież zdarzenia, powodujące znaczne przerwy w dostępności usług, czy wręcz doprowadzają do utraty danych klientów.

Przy wyborze dostawcy usług DRC przede wszystkim należy brać pod uwagę:

- doświadczenie – Partner, który ma nas wesprzeć musi mieć ugruntowaną pozycję i doświadczenie, tu z pomocą przychodzą informacje o certyfikatach technologicznych oraz referencje.
- certyfikację ośrodka – Posiadanie certyfikatu, takiego jak np. EN 50600 wiąże się z budową ośrodka o infrastrukturze spełniającej restrykcyjne normy w zakresie dostępności, bezpieczeństwa fizycznego oraz efektywności energetycznej. Certyfikaty tego typu są potwierdzane przez niezależne jednostki certyfikujące a dany ośrodek podlega okresowym audytom zgodności z normą.
- certyfikację procesów – np. wdrożony standard ISO 27001 - system zarządzania bezpieczeństwem informacji, który obejmuje m.in. procedury dotyczące zarządzania ciągłością działania oraz zarządzanie incydentami związanymi z bezpieczeństwem informacji.

Disaster Recovery Center
Udostępnienie przez dostawcę infrastuktury IT w bezpiecznym Data Center, na której mogą działać najważniejsze systemy i procesy biznesowe Klienta. W razie przerwy w działaniu lub niedostępności ośrodka podstawowego, działalność operacyjna zostaje przełączona do ośrodka zapasowego w czasie zapewniającym zmniejszenie potencjalnych skutków do akceptowalnego poziomu strat finansowych i wizerunkowych. W niektórych wypadkach korzystnym rozwiązaniem dla Klienta jest mozliwość świadczenia takiej usługi w chmurze jako Disaster Recovery as a Service.

Biura Zapasowe
W przypadku jakiejkolwiek awarii czy zdarzenia uniemożliwiającego kontynuowanie pracy w lokalizacji podstawowej, klient na każde żądanie ma do dyspozycji niezbędną powierzchnię biurową, infrastrukturę oraz sprzęt IT oraz urządzenia biurowe gotowe do użytku, a także pomieszczenia socjalne oraz osobne miejsca parkingowe.

Michał Jakś

CSO, Talex SA

Odpowiedzialny za zachowanie ciągłości działania i bezpieczeństwa systemów informatycznych. Jako pierwszy w Polsce wdrażał wymagania normy EN50600 w dwóch ośrodkach Data Center w Talex SA Od 2005 r. zajmuje się utrzymaniem Systemu Bezpieczeństwa Informacji.