Dane to paliwo współczesnego biznesu

Rozmowa z **Januszem Gocałkiem**, Prezesem Zarządu firmy Talex SA

Michał Koralewski: Panie Prezesie, po co chronić cyfrowe dane?

Janusz Gocałek: Dane to jeden z krytycznych elementów, decydujących o osiągnięciu sukcesu w biznesie. Pozwalają analizować wyniki finansowe, wnioskować o poziomie inwestycji, monitorować rynek i budować strategię na kolejne lata. Transformacja cyfrowa, której jesteśmy uczestnikami, spowodowała zmianę modeli biznesowych przedsiębiorstw, w których coraz częściej kluczową rolę odgrywa przechowywanie i przetwarzanie danych. Bez danych współczesne firmy są ślepe, niezdolne do funkcjonowania – nie mówiąc już nawet o próbie konkurowania na rynku. Coraz więcej przedsiębiorców zdaje sobie sprawę, że dane cyfrowe są jednym z najcenniejszych zasobów jakie posiadają, a ich utrata, wyciek, kradzież może decydować o konieczności zamknięcia biznesu. Skoro od bezpieczeństwa danych zależy „być albo nie być" firmy, to procesem zupełnie naturalnym staje się poszukiwanie miejsca, w którym te cyfrowe dane będą bezpieczne przez 24 godziny na dobę. Odpowiedzią na te poszukiwania są tzw. data center – centra przetwarzania danych.

M.K.: W Polsce działa ponad 100 komercyjnych centrów przetwarzania danych. Jak wybrać takie, któremu można powierzyć swój biznes?

J.G.: To zależy od tego, jakie są potrzeby przedsiębiorcy i jakimi danymi operuje. Dla jednej firmy kryterium będzie cena, dla innej bezpieczeństwo i dostępność. Niektóre dane można przechowywać na serwerach publicznych, inne wymagają szyfrowania, specjalnych procedur dostępu i niezależnych węzłów energetycznych itp. Inne potrzeby ma sprzedawca w małym e-sklepie, a zupełnie inne instytucja finansowa, taka jak bank. Tam, gdzie rośnie ryzyko kradzieży danych i negatywnych konsekwencji takiego zdarzenia, tam rośnie także konieczność poszukiwania takiego centrum przetwarzania danych, któremu można zaufać, powierzając swoje najcenniejsze zasoby.

M.K.: Instytucje finansowe zapewne mogą weryfikować serwerownie, opierając się na posiadanych przez nie certyfikatach jakości. Na które z nich warto zwrócić uwagę?

J.G.: Serwerownie dla instytucji finansowych muszą charakteryzować się wysokim poziomem bezpieczeństwa i niezawodności, potwierdzonym przez procesy certyfikacji przeprowadzane przez firmy audytorskie. W tej chwili liczą się trzy standardy: standard amerykańskiej organizacji Uptime Institute, standard ANSI TIA-942 oraz najbardziej kompleksowy i spójny standard EN 50600, opracowany przez Europejski Komitet Normalizacyjny Elektrotechniki, a następnie ratyfikowany i przyjęty przez kraje Unii Europejskiej jako oficjalny standard UE (ISO/IEC TS 22237 Series). Wymagania tych trzech standardów wobec centrum przetwarzania danych są różne i nie każdy z nich jednoznacznie określa reguły klasyfikacji. Dlatego warto zwrócić szczególna uwagę na ten ostatni standard, bo – jak mówiłem – podchodzi do zakresu jakości, bezpieczeństwa i dostępności w sposób najbardziej kompleksowy i szczegółowy.

M.K.: Talex SA, jako pierwsza firma w Polsce i jedyna w Europie Środkowo-Wschodniej, posiada dwa ośrodki centrum przetwarzania danych z certyfikatem standardu EN 50600 w najwyższej, czwartej klasie. O czym mówi ten standard?

J.G.: EN 50600 to grupa norm, które w sposób kompleksowy odnoszą się do centrów przetwarzania danych. Opisuje w sposób szczegółowy wszystkie elementy infrastruktury obiektu: od konstrukcji budynku, poprzez system dystrybucji zasilania, zarządzania działaniem centrum, systemy zapewniające bezpieczeństwo, infrastrukturę telekomunikacyjną aż po elementy kontroli środowiska data center. Wszystko po to, aby zapewnić jasne wymagania dotyczące konstrukcji i funkcjonowania takich centrów i by w efekcie stworzyć niezawodne i godne zaufania miejsce, w którym można bezpiecznie przechowywać i przetwarzać dane – paliwo współczesnego biznesu. Nasze centra przetwarzania danych w Poznaniu i Wrocławiu uzyskały ten certyfikat i zostały zaklasyfikowane na najwyższym poziomie we wszystkich kategoriach podlegających ocenie, tj. klasie 4 dostępności, klasie 4 zabezpieczeń i najwyższym poziomie efektywności energetycznej. Wdrożenie standardu zweryfikowała niezależna firma audytorska, austriacki CIS - Certification & Information Security GmbH.

Chcąc utrzymać certyfikat standardu EN 50600 w najwyższej klasie, zobowiązaliśmy się do ciągłej weryfikacji i modernizacji naszego centrum przetwarzania danych. Mało tego, bazując na naszym doświadczeniu i praktyce sami modernizujemy niektóre elementy data center, wybiegając myślą poza zapisy normy, narzucając sobie rygor zapewnienia naszym klientom jeszcze większej jakości.

M.K.: Dziękuję za rozmowę

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.

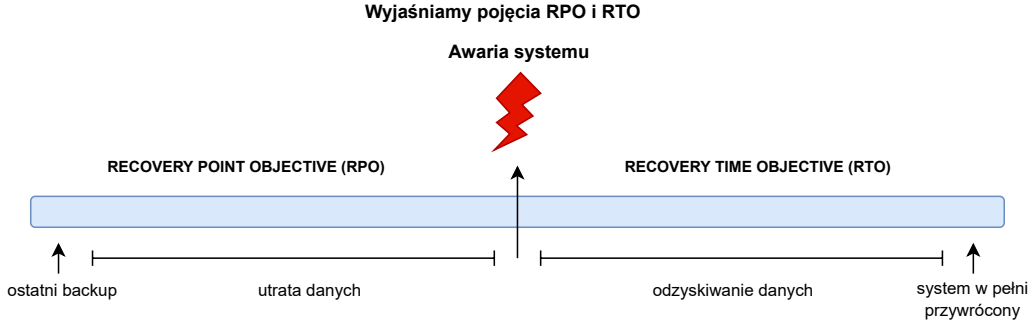
Firma analityczna IDC szacuje średni koszt przestoju na 200 000 USD na godzinę. Gartner obliczył, że firmy tracą średnio 5600 USD za każdą minutę przestoju. Oprócz strat finansowych zostaje mocno nadszarpnięty wizerunek organizacji czy marki. Klienci tracą zaufanie, które trzeba będzie długo i kosztownie 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.

TALEX S.A.

www.talex.pl

IT Support & Consulting | Cloud Services | Software Development

Talex od 30 lat realizuje kompleksowe usługi integratorskie dla biznesu. Oferujemy optymalne rozwiązania i zaawansowane technologie dla najbardziej wymagających klientów. Naszą domeną są usługi z zakresu szeroko pojętego wsparcia IT, doradztwa, usług chmurowych, tworzenie oprogramowania autorskiego oraz na zamówienie klienta.

Swoje usługi świadczymy w Talex Data Center – zaawansowanym centrum przetwarzania danych. Jako jedyna firma w Europie Środkowo-Wschodniej dysponujemy dwoma ośrodkami Data Center z certyfikatami EN-50600 najwyższej, czwartej klasy.

2 500
projektów IT

100
zaimplementowanych aplikacji

400
pracowników IT

2 000 m²
powierzchni biur zapasowych

1 000
przeanalizowanych procesów biznesowych

1 000
wdrożeń infrastruktury informatycznej

TALEX S.A., ul. Karpia 27d, 61-619 Ponań,
tel. 61 827 55 00, biuro@talex.pl