



Jak technologia może uratować biznes

Jak podaje IDC, awaria sprzętu lub oprogramowania jest największym i najczęściej pojawiającym się zagrożeniem dla utrzymania ciągłości biznesowej współczesnych firm. Może ona dotknąć każdego, nawet gigantów rynku, a co najgorsze – narazić firmy na bardzo duże koszty. Z powodu zatrzymania działalności i braku dostępu do informacji biznesowych przedsiębiorcy tracą rocznie nawet 800 milionów dolarów, a 80% firm, które straciły dane w wyniku awarii, kończy działalność w ciągu zaledwie 13 miesięcy od tego zdarzenia. Jak radzić sobie w ekstremalnych warunkach katastrofy IT i minimalizować straty po stronie firmy?



Najczęściej niedostępność danych jest spowodowana awarią sprzętu lub oprogramowania, a nieprzewidywalnych zagrożeń dla systemów IT nie brakuje. Oczywiście w ekstremalnych przypadkach awarię i paraliż całej firmy mogą wywołać: cyberatak, pożar czy klęska żywiołowa, ale najczęściej dochodzi do nich po prostu z powodu ludzkiego błędu. Zdaniem 81% menedżerów, to właśnie ludzie są najsłabszym ogniwem, jeżeli chodzi o kwestie bezpieczeństwa systemów IT. Wskazuje na to między innymi raport „Security Trends 2015”, opracowany przez Microsoft i EY.

„Za tworzenie rozwiązań IT i zarządzanie nimi odpowiadają ludzie, którym zdarza się popełniać błędy. Firmy nie są w stanie uchronić się w 100% przed awariami takich systemów. Można jednak zminimalizować ryzyko i zapewnić firmie technologiczne zabezpieczenie” – komentuje Łukasz Polak, wiceprezes Beyond.pl, polskiego centrum danych i dostawcy rozwiązań IT dla biznesu.

WALKA O DOSTĘPNOŚĆ 24/7/365

Pojawiają się niekiedy głosy sceptyczne, co do realnego zagrożenia katastrofą IT,

Nieco ponad połowa badanych firm ma udokumentowany plan zachowania ciągłości działania na wypadek awarii systemów IT. Około 14% planuje stworzenie takiego dokumentu, zaś co czwarta z badanych firm po prostu go nie ma. Gdy bezpieczeństwem zajmuje się niezależna komórka lub zewnętrzna firma, odsetek ten rośnie. Aż 73% takich organizacji ma plany działania na wypadek zaistnienia nieprzewidzianych okoliczności.

Wynika z raportu „Polska dla Biznesu, bezpieczeństwo, ryzyko, dostępność”, przygotowanego przez firmę HP.

Jednak wystarczy spojrzeć na miniony rok, kiedy to duże awarie IT rzeczywiście się zdarzały, nie omijając nawet największych firm. W 2015 roku mieliśmy do czynienia chociażby z awarią systemu informatycznego jednego z wiodących producentów samochodów, która spowodowała paraliż magazynu i spore opóźnienia w dostawach części zamiennych. W minionym roku doszło też do awarii IT firmy znanego operatora komórkowego, przez którą abonenci tej sieci stracili na pewien czas możliwość wykonywania i odbierania połączeń oraz dostęp do Internetu. W obu przypadkach nastąpiła utrata ciągłości biznesowej. To niesłychanie istotne, bo wg raportu EY to właśnie ciągłość działania jest głównym priorytetem polskich i zagranicznych firm. Z drugiej strony jest ważna także dla klientów. Bez względu na wszystko oczekują oni od firmy dostępności usług w systemie 24/7/365, dlatego szefowie działów IT stoją przed wyzwaniem, jakim jest stworzenie planu awaryjnego, który podtrzyma ciągłość dostępu do danych, aplikacji oraz wykonywania pracy operacyjnej.

BEZPIECZEŃSTWO IT W FIRMACH DZIŚ I JUTRO

Polscy przedsiębiorcy mają już świadomość znaczenia bezpieczeństwa systemów informatycznych. 78% menedżerów wskazuje, że bezpieczeństwo IT jest szczególnie ważne dla funkcjonowania ich firm – wynika z raportu „Polska dla Biznesu, bezpieczeństwo, ryzyko, dostępność”, przygotowanego przez firmę HP. Skłonność do inwestowania w rozwiązania, które to bezpieczeństwo zapewniają, rośnie wraz ze skalą przedsiębiorstwa. Aż 40% organizacji zatrudniających powyżej 200 osób deklaruje chęć podniesienia nakładów w tym roku. Najczęściej deklaracje takie składają firmy, które mają wyłącznie klientów B2B.

Jednak mimo wysokiej świadomości tego, jak ważne jest bezpieczeństwo i zachowanie ciągłości działania, w wielu przedsiębiorstwach brakuje procedur pozwalających przeciwdziałać zagrożeniom.

TECHNOLOGICZNE UBEZPIECZENIE

Rozwiązaniem, które takie zewnętrzne organizacje mogą zaoferować przedsiębiorstwom, jest na przykład Zapasowe Centrum Danych (Disaster Recovery Center). To zabezpieczenie pozwala uruchomić zasoby zgromadzone w zewnętrznym ośrodku zawsze, kiedy tylko zachodzi taka potrzeba, ograniczając do minimum ryzyko pojawienia się czasowej czy trwałej niedostępności danych. Rozwiązanie to zabezpiecza bowiem również przed ich utratą. Dzięki niemu w przypadku wystąpienia nieplanowanych przerw w funkcjonowaniu przedsiębiorstwa usługi i wszelka działalność operacyjna zostają zaledwie w ciągu kilku sekund przełączone do ośrodka zapasowego, a czas niedostępności usług zredukowany jest do minimum.

„Na początek każdy menedżer powinien zastanowić się, czy jego firma ma systemy informatyczne, których awaria lub brak mogą zakłócić jej ciągłość biznesową. Bywa, że utrata jednego systemu może spowodować zatrzymanie działalności całego przedsiębiorstwa, a co za tym idzie – milionowe straty, dlatego tak ważne jest wdrożenie w firmie Business Continuity, czyli planu utrzymania ciągłości działania” – podkreśla Łukasz Polak z Beyond.pl.

Jeszcze do niedawna odtwarzanie awaryjne wiązało się z dużymi wydatkami. Inwestycje były konieczne do stworzenia odrębnego środowiska informatycznego na potrzeb zapasowych systemów. Dziś przedsiębiorcy mają możliwość współpracy z zewnętrznym dostawcą usług: Data Center. Mogą korzystać



ŁUKASZ POLAK, wiceprezes Beyond.pl, polskiego centrum danych i dostawcy rozwiązań IT dla biznesu. Odpowiada m.in. za zarządzanie operacyjne i rozwój sprzedaży spółki na arenie międzynarodowej, współpracując z kluczowymi klientami. Z poziomu zarządu nadzoruje projekt budowy największego w Polsce Centrum Danych o wartości 150 milionów złotych.

„Za tworzenie rozwiązań IT i zarządzanie nimi odpowiadają ludzie, którym zdarza się popełniać błędy. Firmy nie są w stanie uchronić się w 100% przed awariami takich systemów. Można jednak zminimalizować ryzyko i zapewnić firmie technologiczne zabezpieczenie.

Każdy menedżer powinien zastanowić się, czy jego firma posiada systemy informatyczne, których awaria lub brak może zakłócić jej ciągłość biznesową. Bywa, że utrata jednego systemu może spowodować zatrzymanie działalności całego przedsiębiorstwa, a co za tym idzie – milionowe straty, dlatego tak ważne jest wdrożenie w firmie Business Continuity, czyli planu utrzymania ciągłości działania. Zamiast jednak tworzyć własną zapasową infrastrukturę, przedsiębiorcy mogą skorzystać z outsourcingu IT, czyli zdecydować się na zlecenie stworzenia kopii kluczowych danych zewnętrznemu ośrodkowi.

To rozwiązanie staje się powoli tak naturalne jak outsourcing takich kompetencji, jak: logistyka, rachunkowość i usługi kadrowo-płacowe. Zewnętrzny partner gwarantuje dostęp do najnowszych rozwiązań technologicznych i know-how, a co najważniejsze z punktu widzenia przedsiębiorców – pozwala zoptymalizować koszty”.

z Disaster Recovery Center w modelu outsourcingu. Plusów takiego rozwiązania można wymienić wiele. Najważniejszym z nich jest jednak możliwość korzystania z rezerwowych zasobów w wypadku nagłej potrzeby. „Outsourcing IT staje się powoli tak naturalny jak outsourcing usług logistycznych, rachunkowości czy usług kadrowo-płacowych. Zewnętrzny partner gwarantuje dostęp do najnowszych rozwiązań technologicznych i know-how, a co najważniejsze z punktu widzenia przedsiębiorców – pozwala zoptymalizować koszty” – podkreśla Łukasz Polak. ■