

Ryzyko według cennika

Pioneer Pekao Investment Management S.A. wspólnie z firmą ISCG sp. z o.o. przeprowadził kompleksową analizę czynników ryzyka, oraz ich wpływu na ciągłość działania i wyniki spółki. W efekcie powstała szczegółowa mapa współzależności systemów informatycznych na tle procesów biznesowych. Ostatecznym rezultatem projektu są kompletne procedury reagowania w sytuacjach, które zagrażają ciągłości procesów firmy lub jej wynikom finansowym.

Pioneer Pekao Investment Management S.A. (PPIM) należy do europejskiej grupy bankowo-finansowej **UniCredit**, w skład której wchodzi m.in. **Grupa Pekao S.A.** Firma działa w Polsce od 1992 r. i jest obecnie w krajowej czołówce firm inwestycyjnych, zarówno na rynku usług dla klientów indywidualnych, jak i instytucjonalnych. Na ofertę PPIM S.A. składa się kilkadziesiąt produktów, dostosowanych do różnych oczekiwań klientów w dziedzinie ryzyka inwestycyjnego i perspektyw inwestowania. Firma zarządza aktywami wszystkich funduszy Pioneer Pekao TFI S.A., największego – pod względem zarządzanych aktywów – towarzystwa funduszy inwestycyjnych w Polsce. Większość spośród osób zatrudnionych w PPIM S.A. pracuje w siedzibie głównej firmy w Warszawie.

Szersza definicja ryzyka

Kilkanaście lat działalności PPIM obfitowało w zmiany. Rozwój rynku stymulował tworzenie nowych produktów, dla których rozbudowywano istniejące lub tworzono całkiem nowe systemy informatyczne. W połączeniu ze zmianami w przepisach prowadziło to do komplikacji środowiska aplikacyjnego PPIM, a zatem wzrostu ryzyka operacyjnego.

Oczywiście, firma posiadała solidne zabezpieczenia sprzętowe i sieciowe dla wszystkich ważniejszych aplikacji i zasobów. Utrzymywała także aktualną dokumentację środowisk i procedur ich odtwarzania, które były testowane przynajmniej raz do roku.

„Zarząd PPIM zdawał sobie jednak sprawę, że prawdziwym celem wszelkich

działań zapobiegawczych nie jest tylko sprawność technologiczna, lecz przede wszystkim biznesowa” – mówi Tomasz Orlik Wiceprezes Zarządu COO.

Uruchomienie „Programu utrzymania ciągłości działania” umożliwiło kompleksową analizę czynników mających wpływ na nieprzerwane funkcjonowanie PPIM.

„Od dłuższego czasu przymierzaliśmy się do analizy wpływu awarii systemów na ciągłość procesów biznesowych, a nawet szerzej – na wyniki finansowe. Musieliśmy jednak wcześniej szczegółowo zamodelować procesy, uwzględniając strategię firmy w średnim okresie. Przygotowanie definicji procesów za pomocą narzędzi Aris zajęło nam kilka miesięcy” – opowiada Piotr Kalbarczyk, Dyrektor Zespołu ds. Infrastruktury Informatycznej w Pioneer Pekao Investment Management S.A.

Intencją zarządu PPIM było także rozszerzenie analiz ryzyka na czynniki nie związane z technologiami.

„W dotychczasowych analizach skupialiśmy się głównie na informatyce, zasilaniu i katastrofach. Tym razem chcieliśmy uwzględnić także ryzyka biznesowe, związane z rynkami inwestycyjnymi, kluczowymi partnerami i klientami, otoczeniem regulacyjnym i prawnym, a także nasze wewnętrzne ryzyka organizacyjne. Chcieliśmy w ten sposób dostosować nasze plany do wytycznych zawartych w Drugiej Umowie Bazylejskiej, a także do zmian na rynku” – wyjaśnia Marcin Wróbel, Dyrektor ds. Zarządzania Ryzykiem w Pioneer Pekao Investment Management S.A.

Analiza: wyzwanie organizacyjne

Rozszerzenie zakresu analizowanych ryzyk oraz przyjęcie w analizach perspektywy biznesowej (dodatkowe koszty, kary, utracone przychody, reputacja itd.) wymagało rozległych konsultacji z osobami odpowiedzialnymi za poszczególne procesy, systemy i obszary biznesu. W praktyce oznaczało to konieczność przeprowadzenia skoordynowanej akcji ankietowej wśród kilkudziesięciu osób ze wszystkich departamentów PPIM, przygotowania merytorycznego ankiet, jak również mechanizmów scalających ich wyniki. Równolegle należało przeprowadzić analizę faktycznych współzależności systemów informatycznych na tle opisanych procesów biznesowych, a jej wyniki scalić z wynikami ankiet. Zarówno ankiety, jak i analizy PPIM zlecił doświadczonej firmie zewnętrznej, ISCG sp. z o.o. (ISCG). Jej rola miała także polegać na przygotowaniu ostatecznego kształtu procedur oceny ryzyk i scenariuszy postępowania w wypadku wystąpienia zagrożeń.

„Projekt dotyczyć miał bezpośrednio dwóch kluczowych zasobów firmy: pracowników merytorycznych oraz systemów informatycznych. W przypadku pracowników wyzwaniem było zdobycie rzetelnych i wyczerpujących informacji od ludzi, którzy na co dzień absolutnie nie mają na to czasu. Na nasze szczęście, ISCG miała do tego własne, gotowe narzędzie, co sprowadziło proces pozyskiwania informacji do niezbędnego minimum. W przypadku zasobów, chodziło o kompetencje i doświadczenie z heterogeniczną infrastrukturą systemową i aplikacyjną w branży finansowej, co akurat dla ISCG jest chlebem powszednim” – motywuje wybór partnera **Piotr Kalbarczyk**.

Tropem współzależności

Aby sprawnie zgromadzić dane, ISCG udostępniła pracownikom PPIM dedykowaną aplikację portalową, składającą się z sekcji informacyjnej i formularzowej. Pracownicy merytoryczni PPIM mieli wskazać w ankietach, które systemy są według nich krytyczne dla ciągłości procesów biznesowych, a także jakie konsekwencje operacyjne i finansowe niesie

ze sobą niedostępność określonego systemu lub osoby przez określony czas: godzinę, dwie, dzień itd. Przy okazji mieli również wskazać, w jakich godzinach konkretne systemy muszą być dostępne, a w jakich ich dostępność nie jest absolutnie konieczna.

Po zapoznaniu się z częścią informacyjną, w części formularzowej użytkownicy wprowadzili dane do formularzy InfoPath. Dane były zapisywane w bazie, skąd później były pobierane do analizy. Wszystkie dane źródłowe i wyniki zapisywane były w formacie XML, aby można je łatwo przenosić do dokumentów procedur. W tym celu wykorzystano portal SharePoint Server 2007, formularze InfoPath 2007 i inne aplikacje pakietu Microsoft Office 2007. To skróciło i uprościło cały proces, na czym PPIM bardzo zależało.

Dane wprowadzone przez użytkowników zostały porównane z wynikami analizy systemów i aplikacji, przeprowadzonej równolegle. Wyniki tych porównań były miejscami zaskakujące.

„Dzięki dwutorowej analizie dowiedzieliśmy się, że faktyczne współzależności systemów są znacznie większe, niż wynikałoby to z dokumentacji samych systemów. Wyszło to zarówno podczas analizy konfiguracji infrastruktury, jak i z opisów użytkowników. Krótko mówiąc, systemy nie muszą być zintegrowane, by być od siebie zależne. Wystarczy, że do wykonania operacji w jednej aplikacji trzeba zajrzeć do innej” – podkreśla **Paula Januszkiewicz**, Audytor Bezpieczeństwa IT w ISCG Sp. z o.o. Ujawniono także inne okoliczności.

„Z analizy ankiet wynikało, że w firmie istnieją zasoby, których nie można po prostu zastąpić innymi. Przykładowo, jedna osoba doskonale zna się na jakiejś dziedzinie, a osoby z nią pracujące znają się na tym już tylko częściowo. Na co dzień to normalne, wszyscy to znamy, ale w sytuacji kryzysowej rodzi to pewne konsekwencje, a zatem trzeba z tym faktem coś zrobić. Odkrywanie takich rzeczy było jednym z kluczowych celów analizy” – mówi **Paula Januszkiewicz**.

Ryzyko zmierzone i wycenione

W rezultacie projektu przeprowadzonego wspólnie z ISCG, PPIM dysponuje dziś pełną wiedzą o tym, które zasoby informatyczne są faktycznie krytyczne dla jej biznesu i jakie są finansowe konsekwencje spadku ich wydajności lub awarii.

„Dawniej wiedzieliśmy jedynie to, że awaria serwera oznacza niedostępność działających na nim aplikacji. Dziś, jeśli dojdzie do awarii, potrafimy natychmiast stwierdzić, jak wpływa to na procesy biznesowe.

Potrafimy też oszacować czas odtwarzania oraz wyliczyć straty i utracone przychody” – mówi **Piotr Kalbarczyk**.

Ponieważ ankiety wypełniane przez użytkowników biznesowych obejmowały pytania na temat ryzyk rynkowych, instytucjonalnych i organizacyjnych, PPIM ma dziś znacznie pełniejszy obraz ryzyka.

„Mamy całościowe spojrzenie na ryzyko, a jednocześnie szczegółowe zasady podstępowania w określonych przypadkach. Zbieranie takich informacji bez wsparcia narzędziowego byłoby długotrwałe i frustrujące dla wszystkich uczestników przedsięwzięcia. ISCG rzeczywiście bardzo nam pomogło – dane są przekrojowe i pochodzą bezpośrednio od zainteresowanych” – mówi **Marcin Wróbel**.

Zaangażowanie w projekt szerokiego grona osób miało też inne, pozytywne konsekwencje.

„Uczestnicząc w tym przedsięwzięciu pracownicy PPIM zyskali szersze spojrzenie na firmę i swoją własną pracę. To nowe spojrzenie to jest z pewnością bardziej realistyczne niż dotąd, bo okazało się, że nic nie dzieje się samo, i że wszystkie procesy, zasoby i ludzie w firmie są ze sobą ściśle powiązane. Ludzie dostrzegli też, jak bardzo ich oceny, szacunki i wyobrażenia mają wpływ na zasady funkcjonowania firmy, co z

pewnością było motywujące” – mówi **Jarosław Rosa** z zarządu ISCG.

W wyniku projektu PPIM dysponuje szczegółową mapą współzależności systemów – nie tylko w sensie formalnym, ale też faktycznym, włącznie z osadzeniem tych współzależności na osi czasu. Firma potrafi też bardzo dokładnie stwierdzić, jakie są konsekwencje finansowe pojawienia się określonych zagrożeń oraz różnych sposobów reagowania na nie.

„Tę wiedzę trudno przecenić. To najbardziej wiarygodna, a zarazem najbardziej użyteczna analiza ryzyka na potrzeby biznesu, z jaką miałem do czynienia w Polsce” – mówi **Marcin Wróbel**.

ISCG sp. z o.o.

ISCG to zespół uznanych w Polsce autorytetów, wypróbowanych w najbardziej wymagających projektach informatycznych, którzy zmieniają dział IT Klienta z ośrodka kosztowego w jednostkę generującą wartość dodaną dla biznesu Firmy. Czy to w zakresie optymalizacji infrastruktury, bezpieczeństwa, czy rozwiązań informatycznych wspierających działalność biznesową, ISCG udostępnia kompetencje najwyższej próby, aby inwestycje w IT przynosiły wymierną korzyść. ISCG adresujemy swoje rozwiązania do klientów korporacyjnych i średnich przedsiębiorstw działających na rynku polskim i międzynarodowym. Na liście klientów znajdują się największe światowe marki. Atutem ISCG jest wiedza i doświadczenie zespołu wykwalifikowanych certyfikowanych specjalistów. Jako jedna z niewielu firm wdrożeniowych ma w swoim gronie Inżynierów uhonorowanych tytułem MVP w kategorii Enterprise Security, aktywnie rozwijających wiedzę o technologach firmy Microsoft.