Zygmunt Ryznar

RYZYKO DECYZJI W ZAKRESIE KOMPUTERYZACJI BANKU
(dekalog grzechów komputeryzacji)

Wstęp

W podejmowanym cyklu artykułów prezentowane będzie podejście odwrotne do tak zwanej propagandy sukcesu , przy czym odwrotności tej nie należy brać dosłownie , gdyż nie chodzi tutaj o propagowanie błędów, lecz raczej odstraszanie (lub zniechęcanie) od ich popełniania .

Tak się składa, że wskutek bezkrytycznej mody na komputery albo chęci uniknięcia miana konserwatysty, niewielu specjalistów [1] mówi się o skutkach błędnych decyzji w zakresie komputeryzacji. W środowisku bankowym ryzyko stanowi ważny element decyzyjny, lecz odnosi się to do takich spraw jako ryzyko stóp procentowych, ryzyko waluty, ryzyko kraju, ryzyko kredytowe itp.

Tymczasem *prawidłowe działanie systemu informatycznego ma niebagatelny wpływ na jakość i ryzyko usług bankowych*. Zapewnienie bezbłędnego działania wielu programów w krytycznych warunkach przetwarzania , a więc wywoływanych w trybie czasu rzeczywistego przez tysiące terminali rozproszonych w sieci oraz ryzyko finansowe prawie każdej transakcji bankowej, stanowią wyzwanie nieporównywalne do tradycyjnych aplikacji komputerowych typu systemy płacowe i gospodarka materiałowa.
W tej sytuacji pisanie o niedociągnięciach może mieć większe znaczenie, niż mówienie o sukcesach. Być może dzięki takiemu "przewrotnemu spojrzeniu" łatwiej i pełniej można zrozumieć co leży u podstaw sukcesu komputeryzacji. Uczenie się poprzez cudze błędy jest bardziej efektywne, gdyż własne są zbyt kosztowne i często nienaprawialne . Ponadto rozważania i wnioski zawarte w tej publikacji są prawdopodobnie pouczające nie tylko dla banków, lecz również dla każdej organizacji-instytucji działającej w dowolnej branży w warunkach konkurencji rynkowej. Podejmowanie decyzji komputeryzacyjnych jest wyjątkowo trudne, gdyż odbywa się pod presją czasu ("konkurenci już podjęli decyzje") , w warunkach ciągłego postępu technicznego i zmiennych potrzeb informacyjnych.

W niniejszej publikacji omawiane będą następujące rodzaje ryzyka:

1. Ryzyko niewydolności i zawodności sprzętu
2. Ryzyko niezrealizowanych potrzeb informacyjnych kierownictwa banku
3. Ryzyko nieoperowalności systemu
4. Ryzyko niedostatecznego bezpieczeństwa systemu
5. Prototyp jako ryzyko wyboru nowości
6. Ryzyko dezintegracji informacji i organizacji
7. Ryzyko przekroczenia budżetu komputeryzacji
8. Ryzyko bankructwa dostawcy systemu lub nie wywiązania się z zobowiązań
9. Ryzyko uzależnienia od dostawcy lub typu komputera
10. Ryzyko największe: *brak decyzji komputeryzacji*

Wykaz powyższy może być nazwany dekalogiem grzechów komputeryzacji. Czasem grzechy od dobrych uczynków dzieli niewiele, a bywa tak że łączą je dobre intencje. Czasem bowiem mając dobre intencje popełnia się złe czyny , ale jest to analogia wybiegająca zbyt daleko poza rozważania zawodowe.

1.Ryzyko niewydolności i zawodności sprzętu

Komputer może być komputerowi nierówny w takim stopniu , że nie zmieści się to na żadnej skali porównawczej i nie chodzi tylko o szybkości zegarów ani magiczne liczby milionów czy miliardów operacji na sekundę , jakie może wykonać jednostka centralna komputera. Zadania jakie wykonuje system przetwarzania danych są - mimo prostoty matematycznej - bardzo złożone i wymagają zaangażowania całego potencjału (w tym stosunkowo powolnych pamięci dyskowych) obliczeniowego do wywoływania i współbieżnej realizacji wielu programów (do obsługi wielu równocześnie napływających transakcji, zapytań, tworzenia śladów audytowych , aktualizacji wielu pól danych znajdujących się we wzajemnej relacji, tworzenia raportów, obsługi poczty elektronicznej itp.), co wymaga nie tylko przesyłania ogromnych ilości danych finansowych lecz również koordynacji wielu procesów tworzonych automatycznie przez system operacyjny komputera.

---

1 Do napisania niniejszego opracowania skłoniło mnie moje własne ponad 30-letnie doświadczenie zawodowe pracy w charakterze analityka, projektanta i programisty oraz konsultanta . *Sformułowane w nim tezy i wnioski nie odnoszą się ani do aktualnych ani poprzednich moich pracodawców* , lecz są wyrazem wiedzy i prywatnych poglądów , ukształtowanych jako "summa summarum" całego mojego życia zawodowego.

Problem wydajności systemu nie może być rozpatrywany teoretycznie w oderwaniu od skali zastosowań. Ten sam komputer, który jest wystarczający jako tzw. serwer (umownie określmy go tutaj jako komputer centralny) dla małego banku spółdzielczego , może okazać się niewystarczający jako inteligentna stacja robocza pracująca w trybie GUI (Graphic User Interface -*Graficzne łącze użytkownika*) w zaawansowanym systemie dla dużego banku.

Pojęcie dużego banku też wymaga zdefiniowania, aczkolwiek potocznie w naszych krajowych warunkach za taki uważany jest każdy bank z tzw. dziewiątki banków komercyjnych. Z punktu widzenia przetwarzania danych przyjmiemy dla potrzeb ilustracji problemu, że typowy duży bank posiada 1 milion klientów , prowadzi 2 miliony rachunków, w tzw. szczycie przetwarza 100 tysięcy transakcji na godzinę oraz występuje w nim 1000 użytkowników (dilerów i stanowisk dysponencko-kasowych) mających dostęp do systemu w czasie rzeczywistym . Zapotrzebowanie na pamięć dyskową w takim systemie sięga powyżej 100 GigaBajtów (miliardów znaków) , gdyż obejmuje ono nie tylko informacje o klientach i rachunkach ale również archiwum transakcji (w skali co najmniej 1 roku) , składowanie wydruków użytkowych, tzw. dziennikowanie danych (journalizing) do potrzeb odzyskiwania danych, ślady audytowe oraz oprogramowanie.

Systemowi takiemu stawia się zwykle następujące wymagania wydajnościowe:

- kilkadziesiąt transakcji bankowych na sekundę
- 4-6 godzinny czas zamykania dnia
- kilkusekundowy czas odpowiedzi przy pracy w trybie rzeczywistym
- zdolność aktualizacji sald rachunków w czasie rzeczywistym (czyli natychmiast po zaakceptowaniu transakcji).

Przyczyną niewydolności może być niedostateczna wydajność komputera (lub sieci komputerowej) lub przyjęta w systemie bankowym technologia przetwarzania nie dostosowana do wielkości baz danych:

Na niską wydajność sprzętu składają się:
- niedostateczne parametry techniczne (za wolne procesory, brak wieloprocesorowości, niedostateczna pojemność pamięci operacyjnej i dyskowej)
- nieefektywny system operacyjny komputerów i sieci

Wydajność komputerów w zakresie przetwarzania transakcyjnego oceniana jest poprzez testy wydajnościowe zwane benchmarkami, wykonywane wg standardów opracowanych przez Transaction Processing Performance Council (TPC) . Od strony sprzętowej w testach uczestniczą komputery pracujące w architekturze klient/serwer z dołączoną dużą ilością terminali (np.tysiąc) emulowanych lub pracujących w sieci rozległej (WAN - Wide Area Network). Od strony software'owej występuje monitor przetwarzania transakcji, system zarządzania bazą danych oraz symulator sesji i generator transakcji aplikacyjnych. Transakcje aplikacyjne powinny stanowić odpowiednią "mieszankę", wykorzystującą wszechstronnie zasoby komputerowe (w szczególności dyskowe) w zakresie przeszukiwania, aktualizacji i dopisywania nowych pozycji, oraz zachowującą proporcje występujące podczas rzeczywistej eksploatacji Wyniki pomiarów wyrażane są w liczbie transakcji na sekundę (tps) oraz stosunku ceny do transakcji ($/tps) .

Technologia przetwarzania powinna być odpowiednia dla zadań i wolumenu danych, niezależnie od charakterystyk wydajnościowych komputerów. W przeciwnym razie technologia odpowiednia dla baz megabajtowych (zawierających miliony znaków) może okazać się katastrofą dla baz gigabajtowych (zawierających miliardy znaków) , nie mówiąc o bazach terabajtowych (biliony znaków).

Odpowiednio dobrana technologia powinna gwarantować właściwe proporcje pomiędzy zakresem przetwarzania natychmiastowego (w czasie rzeczywistym) i wsadowego. Czasem zwiększając zakres czasu rzeczywistego (np.włączając do niego generowanie księgowań) można skrócić wsadowe zamykanie końca dnia.

Zakres czasu rzeczywistego obejmuje zwykle aktualizację limitów, aktualizację informacji w kartotece klientów (łącznie z utrzymywaniem tzw.pozycji klientów) , zakładanie rachunków i aktualizację ich sald oraz generowanie księgowań. Same księgowania w księdze głównej (szczególnie liczącej ponad 50 tysięcy pozycji)

dokonywane są zwykle wsadowo nawet na największych mainframe'ach między innymi ze względu na dużą maszynochłonność przetwarzania, spowodowaną koniecznością sporządzenia wielu raportów. To samo dotyczy też raportowania przepływów pieniężnych, w tym symulowanych do przodu, wymagających sięgnięcia do transakcji aby pobrać z nich m.i. kody transakcji, kwoty , stopy odsetkowe, efektywne daty walut itp.

W aktualnym trendzie rozwojowym systemów bankowych pojawiła się **technologia OLAP** stosowana w przypadku hurtowni danych (Data Warehouse) w zastosowaniach typu DSS (Decision Support System). Termin OLAP oznacza *On Line Analytical Processing* i utworzony został początkowo jako przeciwieństwo w stosunku do przetwarzania transakcyjnego OLTP (On-Line Transaction Processing), W praktyce odnosi się zarówno do przetwarzania danych analitycznych w relacyjnych bazach danych) jak i na skonsolidowanych (zagregowanych) danych historycznych opartych na technologii wielowymiarowych hurtowni danych .

Hurtownie (magazyn) danych przechowują zwykle zbiorcze informacje na poziomie instytucji na takim analitycznym i zagregowanym poziomie oraz w tak długim horyzoncie czasowym aby można było je wyszukiwać w wielu wymiarach (czasowych, geograficznych, wg klientów, wg produktów itp.) . Instalowanie magazynów danych dla tego typu historycznych informacji ma na celu odciążenie operacyjnych baz danych od maszynochłonnego przetwarzania (które może znacznie wydłużyć czas odpowiedzi przy równocześnie odbywającej się ladowej obsłudze klienta) ukierunkowanego na wspomaganie kierownictwa. Magazyny danych mogą być traktowane jako przedsięwzięcie integracyjne w skali organizacji, gdyż są scaloną "zbiornicą" danych zasilaną (zwykle w trybie partiowym) przez różne bazy danych lub służą do przechowywania tzw. metadanych będących opisem struktury wspólnych danych ,

Ryzyko niewydolności systemu można zmniejszyć weryfikując przed zakupem specjalizowane narzędzia zawierające w nazwach postępowo "brzmiące" terminy typu OLAP lub Data Warehouse, a być może oferujące stare technologie w nowym opakowaniu. Niezawodną metodą weryfikacji jest sprawdzenie oferowanej technologii u dotychczasowych użytkowników o podobnym wolumenie danych na podobnej konfiguracji sprzętowej

Uzycie technologii OLAP w stosunku do relacyjnych baz danych zakłada użycie nowych technik skracających czas przetwarzania , np. próbkowania statystycznego do analizy trendów a nie tradycyjnego przeglądania całych baz danych
Efektywna obsługa dużych hurtowni danych (o wolumenie wielu gigabajtów) wymaga wykorzystania "zrównoleglonego" przetwarzania wykorzystującego konstrukcje wieloprocesorowe oraz 64 bitową adresację pamięci, umożliwiającą operowanie na praktycznie nieograniczonej pamięci operacyjnej. Dzięki temu można nawet kilkasetkrotnie skrócić czas przetwarzania.

Myślę, że powyższe przykłady są odpowiedzią dlaczego klasyczne komputery osobiste nie są odpowiednim sprzętem dla dużych banków.

System bankowy musi być więc dobraną kombinacją sprzętu, technologii i walorów funkcjonalnych. Komputery stosowane w systemach bankowych powinna charakteryzować skalowalność , co oznacza możliwość zmiany konfiguracji sprzętowej (dodanie procesorów, zwiększenie pamięci operacyjnej nawet do wielu GB, dodanie macierzy dysków itp.) stosownie do wzrastającego wolumenu danych i nowych właściwości funkcjonalnych systemu aplikacyjnego.
Przepustowość sieci stanowi istotny czynnik rzutujący na wydolność systemu (w tym szczególnie na czas odpowiedzi) . W celu zmniejszenia wolumenu danych przepływającego przez sieć od strony systemu bankowego należy - w warunkach architektury klient/serwer - dążyć do maksymalnego rozproszenia (a ściśle rzecz biorąc replikowania z zasobów centralnych w określonych interwałach czasowych) po serwerach oddziałowych oprogramowania obsługi transakcji kasjerskich oraz takich względnie statycznych danych jak tablice i ekrany. Stworzy to równocześnie warunki do pracy oddziału w trybie off-line czyli w przypadku zerwania łączności z serwerem centralnym . Ponadto należy ograniczyć zakres danych generowanych w oddziałach (np.księgowania tworzone powinny być w serwerze centralnym na podstawie transakcji). Zmniejszenie wolumenu danych uzyskać można również poprzez kompresję danych.
Szybkość transmisji w stosunku do klasycznych rozwiązań można zwiększyć na przykład poprzez zastosowanie okablowania strukturalnego oraz technologii ATM (Asynchronous Transfer Mode), lecz wymaga to poniesienia znacznych wydatków.

Przy określaniu potrzebnej przepustowości sieci należy wziąć pod uwagę, że obsługiwać ona będzie nie tylko transakcje klientowskie bankowe, lecz też takie zadania jak:
·przesyłanie transakcji biura maklerskiego stowarzyszonego z bankiem, (tutaj szczytowe ranne godziny

mogą nakładać się na szczyty bankowej obsługi okienkowej),
·rozsyłanie oprogramowania użytkowego i definicji produktów z centrali do oddziałów (w zakresie dotyczącym oddziałów),
·rozsyłanie wyciągów i raportów przeznaczonych dla oddziałów,
·przesyłanie z centrali replikacji danych lokalnych zabezpieczających pracę off-line,
·przesyłanie z oddziałów zaległych transakcji off-line'owych umożliwiających wznowienie pracy on-line,
·inne aplikacje sieciowe (np.Lotus Notes)
·poczta elektroniczna ogólnego przeznaczenia itp.
·dane operacyjne przebiegające pomiędzy biurami maklerskimi i giełdą
·dane operacyjne przebiegające pomiędzy bankami i repozytoriami papierów wartościowych (Global Custody) m.i. dla transakcji pozagiełdowych
·.komunikaty systemu zarządzania siecią (m.i. rozsyłanie "wejściówek" -tickets, tokens- do sieci przypisanych do poszczególnych logowań, rejestracja przepływu komunikatów pomiędzy komponentami sieci , rejestracja zakłóceń , rejestracja zdalnych wywołań programowych RPC -Remote Procedure Call- , itp.)

Drugim (po wydolności) nieodłącznym atrybutem sprzętu w zastosowaniach bannkowych jest **niezawodność techniczna** . Powinna ona wynosić co najmniej 99% potencjalnego czasu użytkowania w skali roku.

Wysoką niezawodność techniczną osiąga się między innymi poprzez tzw. architekturę tolerującą błędy (fault tolerant architecture), umożliwiającej pracę mimo uszkodzenia komponentu. Ogólnie znane jest tego typu rozwiązanie dla dysków (w postaci macierzy dyskowych typu RAID, kiedy nawet fizyczne wyjęcie pojedynczego dysku nie powoduje "padnięcia" systemu). W przypadku jednostek centralnych stosuje się środowiska wieloprocesorowe np.w technologii SMP (Symmetric Multi Processing).

Dla tzw.krytycznych zastosowań (jak to ma miejsce w systemach całkowicie scentralizowanych) niektóre zachodnie banki stosują bliźniacze instalacje sprzętowe oddalone od siebie , które wykonują pełne równoległe (dublujące)przetwarzanie w dwóch ośrodkach obliczeniowych połączonych rozległą siecią (WAN) lub też automatycznie w określonych odstępach czasu wykonują backup na drugi komputer.
W łączności najprostszą metodą zwiększenia niezawodności i wydolności jest zwielokrotnienie linii, stosowanie obejść (tzw."bajpasowanie") itp.

Skutki podjęcia błędnej decyzji sprzętowej mogą być poważne.
·może wystąpić konieczność zmiany platformy sprzętowej i ewentualnie nowego oprogramowania (jeśli było ono zależne od platformy sprzętowej), co wymagać będzie ponownego wydania ogromnych środków (na przykład kilkunastu milionów dolarów) na co większości banków naszych po prostu nie stać.
·z powodu przestojów awaryjnych klienci będą rezygnować z usług finansowych banku , przy czym zagrożenie to jest wyjątkowo poważne w systemach całkowicie scentralizowanych (gdzie awaria komputera oznacza przestój wszystkich oddziałow banku)
·nastąpi skrócenie godzin obsługi klientów wskutek przedłuzonego czasu tzw. zamykania dnia .

(koniec części pierwszej)

Zygmunt Ryznar

RYZYKO DECYZJI W ZAKRESIE KOMPUTERYZACJI BANKU (dekalog grzechów komputeryzacji)

część 2:

Ryzyko niezrealizowanych potrzeb informacyjnych kierownictwa banku

(ryzyko zawiedzionych nadziei kierownictwa banku)

przyczyny:
- *nieprawidłowa architektura systemu : brak integracji informacji*
brak odpowiednich modułów funkcjonalnych

poziom nowoczesności:
kiedyś decydowały o tym szbd a teraz narzędzia opracowywania informacji
-brak narzędzi opracowywania danych dla kierownictwa
narzędzia dla kierownictwa : business view (czas, produkty, klienci) a nie computer view (klucze)
zapewnienie dostępu zarówno dla info analitycznych jak i zagregowanych\
łatwe przechodzenie od danych zagregowanych do analitycznych:
np. sumaryczne wyniki finansowe banku wg lat
banku wg regionów
regionu x wg oddziałów
oddziału x wg filii
filii x wg produktów

DSS - analiza trendów na podstawie próbkowania statystycznego
OLAP data warehouse data-minign (drilling)

źródło ryzyka tkwi już w momencie zawierania kontraktu “obiecanki-cacanki”.
Szczególne trudności mogą wystąpić w przypadku zakupu systemu stanowiącego "luźną sklejkę" pakietów pochodzących od różnych autorów. Uzyskanie faktycznej integracji takiego systemu wymaga konsekwentnego i stałego nacisku na dostawców, niezależnie od odpowiednich klauzul terminowych i finansowych w kontrakcie.

Na co zwracać uwagę aby ograniczyć stopień ryzyka wyboru złej architektury:

zestawy informacji posiadające podstawowe znaczenie dla decyzji bankowych lub konieczne ze względu na bezpieczeństwo systemu:
:

1.pozycja klienta
2.pozycja waluty
3.pozycja banku
4.cash flow
5.bilans księgowy
6.ślady audytowe (audit-trial journal).
7. utrzymywanie limitów

Wymieniona wyżej obsługa informacyjna *jak nić przewodnia oplata system bankowy , przechodząc przez wiele modułów aplikacyjnych* . Nienależyte uwzględnienie któregokolwiek z tych elementów mocno obniża jakość systemu. Na przykład w niewielu systemach występuje możliwość definiowania transakcji i stowarzyszonych z nimi księgowań.W innych nie ma obsługi limitów ,albo zawężone one są tylko do poszczególnych produktów.

Limity dotyczą kraju, regionu, branży ,klienta (limit globalny - management limit - dla klienta i ew. jego

macierzystej organizacji, limity przyznane - granted limits - dla kredytów, akredytyw, ujemnego salda na rachunku ror, itp) ,dilera, waluty, typów transakcji (forex,rynek pieniężny,papiery wartościowe ...). Przy okazji uwaga, iż suma limitów przyznanych może być większa od limitu globalnego, zaś limitów wykorzystanych powinna być mniejsza od niego. List limitów w systemie powinno być wiele,aby można było spełnic róznorodne wymagania banków. Limity powiązane są z zabezpieczeniami w tym blokowaniem depozytów ,papierów wartościowych itp. .

Obsługa limitów polega m.i. na :
- sygnalizacji przekroczeń limitów podczas wprowadzania transakcji ,
- bieżącej aktualizacji ich sald (w układzie limitów ustalonych, wykorzystanych i dostępnych), raportowaniu przekroczeń i wykorzystania limitów (na jakie cele zostały użyte),
- dostarczaniu analitycznych informacji do analizy przekroczeń limitów (wykaz wszystkich dokonanych transakcji wg podmiotu limitu , oddziałów , dilerów),
- raportowaniu limitów które tracą ważność itp.

Raporty (lub odpowiedzi na zapytania) powinny być uporządkowane wg bankowców (opiekunów), klientów itp.

.

Waluta i klient oraz czas stanowią nieodłączny atrybut prawie każdego zdarzenia w systemie. Obliczanie pozycji klientów i walut wymaga ustalenia w architekturze systemu "ścieżek " dotarcia do wszystkich transakcji finansowych (czyli do wnętrza modułów aplikacyjnych).

Wprowadzenie zmian projektowych dotyczących tych obiektów jest wobec tego bardzo pracochłonne i odpowiedzialne.
Dlatego kupując system trzeba ocenić na ile zaawansowana jest architektura systemu w zakresie orientacji na klienta, wielowalutowość , wielorakość limitów, definiowalność transakcji itp.

System robi wszystko ale nie tak jak spodziewa się uzytkujący go bank

Na przykład:
- obsługuje salda debetowe na rachunkach ROR bez zróżnicowanego liczenia ujemnych odsetek (w zależności od okresu zalegania ze spłatą skredytowanego salda)
- podaje przepływ pieniężny metodą memoriałową a nie kasową
- nie ma algorytmu procentowego liczenia opłat transakcyjnych naliczanych w momencie wprowadzania transakcji
- wielowalutowość systemu sprowadza się do tzw. walutowości dualnej
- nie dopuszcza się wybierania odsetek po kapitalizacji (np.w ciągu X dni)
- nie ma reklasyfikacji rachunków przypadku obniżenia salda poniżej minimum przewidzianego dla danej waluty
- obsługuje transakcje dilerskie ale nie prowadzi limitów dla poszczególnych dilerów i walut
-

Podstawowym zadaniem mid-office jest dostarczanie (w czasie rzeczywistym lub pseudorzeczywistym tj. na żądanie lub w określonych interwałach czasowych) **informacji o pozycji finansowej banku**

OBSŁUGA POTRZEB INFORMACYJNYCH KIEROWNICTWA

- *Przewidywanie wyników finansowych banku*

a. "Projekcje" do przodu przepływu gotówki, strategie finansowe w zakresie inwestycji kapitałowych i zasilania finansami (funding operations) m.i. dostarczanie informacji do decyzji w zakresie wyboru krótko- lub - długoterminowych długów albo wierzytelności , prezentacja stop procentowych niwelujących rozwarcie (tzw.break-even rate) i działań niezbędnych dla polepsze-nia płynności finansowej typu czy pożyczać pieniądze od kogoś czy udzielać wiecej kredytów .
b. Raportowanie typu "co stanie się jeśli " , np. jeśli zmieni się stopa procentowa

dla kredytów komercyjnych albo rozwarcie (gap) zwiększy się o 1 % .

- *Zarządzanie ryzykiem*
  a. Analiza dochodowości i ryzyka sali dilerskiej (m.i. poprzez rewaluację operacji typu forward i swap); arbitrażu i zabezpieczeń (hedging) ,
  b. Analiza udzielanych kredytów (pod kątem stopnia spłacalności i zdolności kredytowej klientów),
  c. Analiza wykorzystania (w tym przekroczen) limitów .
  d. Sygnalizacja kredytów, dla których zabezpieczenie spadło poniżej wymaganego poziomu (np.w przypadku gdy zabezpieczeniem były lokaty dewizowe i nastąpił spadek kursów w stosunku do waluty kredytu lub waluty bazowej albo lokalnej).
  e. Raportowanie zabezpieczeń, których termin ważności upłynął lub upłynie w ciągu najbliższych dni.

Informacje dla kierownictwa prezentowane być powinny zarówno na ekranie jak i na raportach , również w postaci graficznej .
Podstawą sprawnej obsługi informacyjnej kierownictwa jest zaawansowany moduł zarządzania

Nie tylko obsługa działalności operacyjnej
Integracja bankowości hurtowej i detalicznej następować powinna poprzez stosowanie wspólnych zbiorów (klientów, banków, rachunków Nostro,walut,kursów wymiany, stóp procentowych, itp) dzięki czemu wyeliminować można operacje przeformatowań oraz importu/eksportu danych pomiędzy modułami (podsystemami). Operacje importu/eksportu danych powinny dotyczyć jedynie transakcji, a nie baz danych (dostęp do nich powinien być realizowany bezpośrednio). (Podobne problemy powstają w przypadku eksploatowania poszczególnych modułów na różnych platformach sprzętowych i/lub pod różnymi systemami operacyjnymi).

Oba rodzaje bankowości różnią się również technologią przetwarzania danych.

Jak wiadomo, bankowość hurtowa charakteryzuje się dużą złożonością algorytmów (np.w ocenie ryzyka , obliczaniem rewaluacji dla transakcji forward), zmiennością instrumentów finansowych (np.powstawanie nowego typu derywatyw) i stosunkowo małą liczbą transakcji i klientów.

Każda transakcja w tej bankowości stanowi przedmiot takiego samego "zainteresowania" jak pozycja bazy danych (np.lokata) w bankowości detalicznej i do jej obsługi stawiane są ostre wymagania czasu rzeczywistego , np. dla transakcji dilerskich . Transakcja jak i osoba ją wykonująca (diler) oraz waluta mogą być przedmiotem rachunku strat i zysków.

W przypadku bankowości detalicznej liczba transakcji i klientów jest bardzo znaczna i tradycyjnie większość zadań przetwarzania wykonuje się podczas zamykania dnia, podczas gdy dla bankowości komercyjnej w związku z mniejszym obciążeniem możliwe jest zwiększenie zakresu funkcjonalnego w trybie on-line. W związku z niewielkim rozmiarem baz danych system obsługujący bankowość komercyjną może posiadać specyficzną metodę alokacji (podczas przetwarzania, z późniejszym automatycznym backupem na dyski) ich w pamięci operacyjnej, co w zasadzie nie wchodzi w grę w przypadku bankowości detalicznej. Zlikwidowanie podziału na dwie "specjalizacje" wymaga więc wydajnego systemu przetwarzania danych, będącego w stanie obsłużyć powyższe krańcowo różne wymagania. Dlatego tak trudno jest spotkać system, który równie dobrze działa w obu tych obszarach.

W warunkach zachodnich nie jest to poważną przeszkodą , gdyż często występuje tam specjalizacja oddziałów (albo jeden typ działalności albo drugi) i banków np. w USA zwykle oddzielne banki prowadzą działalność detaliczną (retail), komercyjną (corporate) i inwestycyjną. Należy w tym miejscu podkreślić znaczenie działalności komercyjnej (w szczególności dilerskiej) na Zachodzie, gdzie znaczna większość (np.w Szwajcarii ponad 90%, Niemczech 80%, W.Brytanii 50%) codziennych operacji finansowych polega na operacjach międzywalutowych (wymiany walut).

W systemach bankowych dużych banków komercyjnych architektura klient server z serwerem centralnej bazy danych wydaje się być rozwiązaniem najbardziej pożądanym z docelowego punktu widzenia

Z punktu widzenia bankowego za scentralizowanym rozwiązaniem przemawiają następujące racje:

- W centralach wykonywana jest większość operacji zagranicznych i tzw. komercyjnych (kredyty dla przedsiębiorstw , inwestowanie na rynku kapitałowym itp.) . Do ich obsługi niezbędny jest dostęp do transakcji, baz danych klientów i rachunków.

- Zarządzanie bankiem polega nie tylko i nie tyle na obsłudze poszczególnych rachunków klientowskich (do czego lokalne bazy danych są wystarczające), ile na wyborze określonej strategii dobywania i inwestowania kapitału. do tego celu niezbędna jest całość informacji dotycząca banku czyli centralne bazy danych stowarzyszone z plikami transakcyjnymi .

Przykładowo , do zarządzanie skarbowością (Treasury Management) niezbędne są dane w zakresie pozycji klientów (w tym banków,będących klientami danego banku) oraz w zakresie tzw. pozycji banku (w tym cash flow projection) , do uzyskania których niezbędne są dane analityczne w postaci transakcji !!

Skonsolidowany bilans księgowy na szczeblu centrali (możliwy do uzyskania na podstawie bilansów oddziałowych) jest być może wystarczajacy dla standardowych raportów, lecz nie do takich zadań jak np. zarządzanie ryzykiem (rynkowym np.rozwarcie stóp procentowych ., kredytowym,płynnościowym itp.) wymagającym nie tylko informacji księgowych..

- scentralizowane rozwiązanie wydaje się być łatwiejsze do wdrożenia gdyż głównie odbywa się w centrali : tam odbywa się definiowanie produktów, utrzymywanie baz danych , zamykanie dnia itp.
- scentralizowana baza danych bardziej dostosowana jest do obsługi bankomatów oraz swobodnego trybu obsługi klientów (brak uzależnienia operacji od oddziału, w którym klient posiada rachunek).

W systemie w pełni scentralizowanym (w oddziałach istnieją tylko terminale lub komputery osobiste z emulatorami terminali) łatwiej jest utrzymywać bazy danych, gdyż znajdują się one tylko w ośrodku obliczeniowym centrali i są dostępne z terminali . Ilość danych przesyłanych po liniach telekomunikacyjnych jest wtedy stosunkowo niewielka (poza przypadkami przesyłania wydruków), gdyż są to głównie dane wprowadzane z klawiatury terminali (typ transakcji,identyfikator klienta, kwota) oraz pojedyncze informacje zwrotne (np.nazwisko, saldo dostępne) a nie całe rekordy.

Teletransmisji nie powinny podlegać formatki (maski) ekranów, które tworzone mają być lokalnie..

Sformowanie pełnego ciągu operacji z wygenerowaniem transakcji księgowych oraz liczenie odsetek odbywa się już w centralnym komputerze.

prawdopodobnie najlepsze rozwiązanie:
scentralizowane bazy danych z pewnym stopniem rozproszenia danych

Do ważnych decyzji strategicznych należy odpowiedź na pytanie: centralne bazy danych czy rozproszone ?

W systemach bankowych dużych banków komercyjnych centralne bazy danych wydają się być rozwiązaniem pożądanym z docelowego punktu widzenia. Przemawiają za tym poniższe racje.

W centralach wykonywana jest większość operacji zagranicznych i tzw. komercyjnych (kredyty dla przedsiębiorstw , inwestowanie na rynku kapitałowym itp.) . Do ich obsługi niezbędny jest

dostęp do transakcji, baz danych klientów i rachunków.

Zarządzanie bankiem polega nie tylko i nie tyle na obsłudze poszczególnych rachunków klientowskich (do czego lokalne bazy danych są wystarczające), ile na wyborze określonej strategii zdobywania i inwestowania kapitału. do tego celu niezbędna jest całość informacji dotycząca banku.

Przykładowo , do zarządzanie skarbowością (Treasury Management) niezbędne są dane w zakresie pozycji klientów (w tym banków,będących klientami danego banku) oraz w zakresie tzw. pozycji banku (w tym cash flow projection), do uzyskania których niezbędne są dane analityczne w postaci transakcji !! Skonsolidowany bilans księgowy na szczeblu centrali (możliwy do uzyskania na podstawie bilansów oddziałowych) jest być może wystarczajacy dla standardowych raportów, lecz nie do takich zadań jak np. zarządzanie ryzykiem (rynkowym np.rozwarcie stóp procentowych ., kredytowym,płynnościowym itp.) wymagającym nie tylko informacji księgowych..
Scentralizowane rozwiązanie wydaje się być łatwiejsze do wdrożenia gdyż głównie odbywa się w centrali : tam odbywa się definiowanie produktów, utrzymywanie baz danych , zamykanie dnia itp.
Scentralizowana baza danych bardziej dostosowana jest do obsługi bankomatów oraz swobodnego trybu obsługi klientów (brak uzależnienia operacji od oddziału, w którym klient posiada rachunek).

W systemie w pełni scentralizowanym (w oddziałach istnieją tylko terminale lub komputery osobiste z emulatorami terminali) łatwiej jest utrzymywać bazy danych, gdyż znajdują się one tylko w ośrodku obliczeniowym centrali i są dostępne z terminali . Ilość danych przesyłanych po liniach telekomunikacyjnych jest wtedy stosunkowo niewielka (poza przypadkami przesyłania wydruków), gdyż są to głównie dane wprowadzane z klawiatury terminali (typ transakcji,identyfikator klienta, kwota) oraz pojedyncze informacje zwrotne (np.nazwisko, saldo dostępne) a nie całe rekordy. Teletransmisji nie powinny podlegać formatki (maski) ekranów, które tworzone mają być lokalnie..

Sformowanie pełnego ciągu operacji z wygenerowaniem transakcji księgowych oraz liczenie odsetek odbywa się już w centralnym komputerze.

W scentralizowanym systemie przyjęta jest zwykle zasada priorytetu centralnych baz danych nad lokalnymi bazami i wtedy te ostatnie stanowią jakby "wyciąg" z tych pierwszych przeznaczony wyłącznie do pracy awaryjnej.

Czasem transakcjami aktualizowane są tylko centralne bazy danych , zaś w oddziałach pozostają po transakcjach jedynie dzienniki transakcji i lokalne bazy danych wg stanu z poprzedniego dnia..

Wówczas występuje potrzeba partiowego (batchowego) rozsyłania danych z centralnych baz danych do lokalnych baz w celu zabezpieczenia tego samego stanu informacji .

W celu odciążenia linii teletransmisyjnych w większości systemów lokalne bazy danych są przesyłane do oddziałów (jako tzw. strip file) tylko raz dziennie w godzinach nocnych po zamknięciu dnia . Lokalne bazy dotyczą głównie rachunków klientów oraz stałych danych (takich jak zbiór walut, parametry produktów zdefiniowane dla danego oddziału itp.) . Na poziomie oddziału mogą być również lokalizowane dane stałe dotyczące klientów , którymi opiekuje się dany oddział (oczywiście z replikacją tych danych w bazie centralnej).

Im wyższy stopień rozproszenia danych , tym większy może być wolumen przesyłanych danych i stawiane są wyższe wymagania liniom teletransmisji danych.

Jeszcze większe obciążenie sieci wystąpi w przypadku całkowicie zdecentralizowanego

umiejscowienia danych w oddziałach przy zachowaniu obsługi klienta w dowolnym oddziale . Występuje bowiem wówczas konieczność bezpośredniego komunikowania się oddziałów ze soba, w celu uzyskania wszelkich informacji o kliencie (w tym o saldzie), przesłania zrealizowanej transakcji itp., albo utrzymywania w czasie rzeczywistym tylko zbioru sald na rachunkach i replikowania (na bieżąco - lub partiowo - w zależnosci od przepustowości linii) danych oddziałowych w centrali .

W kwestii wyboru pomiędzy systemem scentralizowanym i rozproszonym pomocny może być wniosek, iż w przypadku centralizacji najważniejszym czynnikiem staje się wysoka niezawodność sieci, zaś przy rozproszeniu - jej duża przepustowość.

Scentralizowany charakter przetwarzania, w tym centralny sposób dystrybucji produktów bankowych , zmienia rolę oddziałów banku..

W scentralizowanych systemach oddział staje tylko technicznym pośrednikiem , którego rola ogranicza się do rejestracji zlecenia klienta, gdyż mechanizmy działania produktów definiowane są centralnie . W przypadku zastosowania inteligentnych bankomatów (działających nie tylko jako tzw.cash dispensers , lecz również służących np. do przekazywania zleceń płatniczych) oddziały zostają całkowicie pominięte od strony organizacyjno-funkcjonalnej i jedyny ich ślad w systemie polega na zaewidencjonowaniu operacji w przekroju tzw. centrów kosztów/dochodów. Aktywna rola oddziałow będzie sprowadzać się do marketingu produktów bankowych oraz obsługi produktów negocjowalnych (a więc głownie kredytowych).

Systemy scentralizowane nie muszą (a można nawet powiedzieć - że nie powinny) funkcjonować w czystej formie, lecz mogą być uzupełniane przez *lokalne bazy danych* w oddziałach, między innymi w celu skrócenia czasu odpowiedzi oraz wykorzystywania w przypadku awarii łączy telekomunikacyjnych.

Ze względów technicznych i kosztowych istnieje potrzeba zachowania pewnych proporcji pomiędzy stopniem centralizacji i decentralizacji .

W systemie w pełni scentralizowanym (w oddziałach istnieją tylko terminale lub komputery osobiste z emulatorami terminali) łatwiej jest utrzymywać bazy danych, gdyż znajdują się one tylko w ośrodku obliczeniowym centrali i są dostępne z terminali . Ilość danych przesyłanych po liniach telekomunikacyjnych jest wtedy stosunkowo niewielka (poza przypadkami przesyłania wydruków), gdyż są to głównie dane wprowadzane z klawiatury terminali (typ transakcji,identyfikator klienta, kwota) oraz pojedyncze informacje zwrotne (np.nazwisko, saldo dostępne) a nie całe rekordy. Teletransmisji nie powinny podlegać formatki (maski) ekranów, które tworzone mają być lokalnie..

Sformowanie pełnego ciągu operacji z wygenerowaniem transakcji księgowych oraz liczenie odsetek odbywa się już w centralnym komputerze.

W scentralizowanym systemie przyjęta jest zwykle zasada priorytetu centralnych baz danych nad lokalnymi bazami i wtedy te ostatnie stanowią jakby "wyciąg" z tych pierwszych przeznaczony wyłącznie do pracy awaryjnej.

Czasem transakcjami aktualizowane są tylko centralne bazy danych , zaś w oddziałach pozostają po transakcjach jedynie dzienniki transakcji i lokalne bazy danych wg stanu z poprzedniego dnia..

Wówczas występuje potrzeba partiowego (batchowego) rozsyłania danych z centralnych baz danych do lokalnych baz w celu zabezpieczenia tego samego stanu informacji .

W celu zmniejszenia obciążenia linii teletransmisyjnych w większości systemów lokalne bazy danych są przesyłane do oddziałów (jako tzw. strip file) tylko raz dziennie w godzinach nocnych po zamknięciu dnia . Lokalne bazy dotyczą głównie rachunków klientów oraz stałych danych (takich jak zbiór walut, parametry produktów zdefiniowane dla danego oddziału itp.) . Na poziomie oddziału mogą być również lokalizowane dane stałe dotyczące klientów , którymi opiekuje się dany oddział (oczywiście z replikacją tych danych w bazie centralnej).

Im wyższy stopień rozproszenia danych , tym większy może być wolumen przesyłanych danych i stawiane są wyższe wymagania liniom teletransmisji danych.

Jeszcze większe obciążenie sieci wystąpi w przypadku całkowicie zdecentralizowanego umiejscowienia danych w oddziałach przy zachowaniu obsługi klienta w dowolnym oddziale . Występuje bowiem wówczas konieczność bezpośredniego komunikowania się oddziałów ze sobą, w celu uzyskania wszelkich informacji o kliencie (w tym o saldzie), przesłania zrealizowanej transakcji itp., albo utrzymywania w czasie rzeczywistym
tylko zbioru sald na rachunkach i replikowania (na bieżąco - lub partiowo - w zależności od przepustowości linii) danych oddziałowych w centrali .

W kwestii wyboru pomiędzy systemem scentralizowanym i rozproszonym pomocny może być wniosek, iż w przypadku centralizacji najważniejszym czynnikiem staje się wysoka niezawodność sieci, zaś przy rozproszeniu - jej duża przepustowość.

Scentralizowany charakter przetwarzania, w tym centralny sposób dystrybucji produktów bankowych , zmienia rolę oddziałów banku. W miarę upowszechniania się bankomatów, bankowych usług telefonicznych (phone banking) i terminalowych (home banking) , coraz mniej klientów będzie osobiście zgłaszać się w obsłudze okienkowej. Rola oddziałów będzie sprowadzać się do marketingu produktów bankowych oraz obsługi produktów negocjowalnych (a więc głownie kredytowych).
Nie należy przesadzać z rozbudową architektury klient-serwer, w tym lokalnych baz danych . gdyż spowodować to może wzrost obciążenia sieci zadaniami w zakresie konsolidacji (replikacji) centralnej i lokalnych baz danych oraz stworzy problemy z utrzymaniem integralności systemu i bezpieczeństwem danych. Systemy zawierające przewagę cech scentralizowanych są w literaturze zachodniej określane mianem “cooperative processing” coi na język polski można niezgrabnie przetłumaczyć jako “współdziałające przetwarzanie”.

System bankowy oparty na zasadach współdziałania nie powinien implikować całkowitej centralizacji oprogramowania aplikacyjnego, gdyż kopiowanie do stacji roboczych elementów oprogramowania , danych , wyników - przy każdym wywołaniu - byłoby równie obciążające sieć jak przesyłanie danych.
Wykorzystując zasady architektury klient-serwer w oddziałach powinny działać serwery aplikacyjne z własnym oprogramowaniem i centralnie definiowanymi parametrami , zaś w centrali banku serwer scentralizowanej bazy danych . Dla serwera bazy danych klientami są aplikacje oddziałowe.
Aby utrzymymać jednolitość oprogramowania w skali banku niezbędny jest mechanizm automatycznej dystrybucji programów i definicji typowych produktów po oddziałach.

Skutki podjęcia błędnej decyzji przez kierownictwo banku

- w zakresie elastyczności - utrata klientów wskutek niemożności nadążania za potrzebami klientów i brakiem konkurencyjności w stosunku do innych banków
- w zakresie zasilania informacjami zarządczymi
- w zakresie algorytmow działania systemu -system robi "wszystko" może oznaczać równie dobrze,że robi "wszystko i nic" (robi wszystko ale nie tak jak spodziewa się kupujący).

(koniec cz.2)

Zygmunt Ryznar

RYZYKO DECYZJI W ZAKRESIE KOMPUTERYZACJI BANKU (dekalog grzechów komputeryzacji)

cz.3 RYZYKO NIEOPEROWALNOŚCI SYSTEMU

Przez operowalność systemu rozumiemy łatwość utrzymywania oprogramowania i baz danych, podatność modułów aplikacyjnych na ntegrację z pakietami pochodzącymi od innych wytwórców, przejrzystość funkcjonalną oraz łatwość dostosowania czynności (menu) do obsługi poszczególnych stanowisk pracy w służbach bankowych.

System bankowy zasługuje więc na miano nieoperowalnego, gdy jego użytkownicy bankowcy będą mieć kłopoty ze zrozumieniem funkcjonalności programów, zaś informatycy nie będą w stanie właściwie administrować systemu wskutek jego zawiłej i nie udokumentowanej architektury.

1. Niewłaściwa lub nieprzejrzysta architektura aplikacji

Przed zakupem systemu kompleksowego w banku zwykle działa szereg (np. kilkadziesiąt) autonomicznych aplikacji będących przeważnie wynikiem przypadkowych (z tzw. "konieczności" chwili) zakupów wąsko specjalizowanych aplikacji na komputerach osobistych . W aplikacjach tych następuje z reguły znaczne dublowanie danych, zaś ewentualne powiązanie można osiągać poprzez obustronne konwersje danych związane z przeformatowaniem. Ponieważ nie korzystają one ze wspólnych baz danych. prowadzi to do rozbieżności pomiędzy takimi samymi informacjami znajdującymi się w różnych miejscach. Operowalność takiego systemu jest praktycznie żadna. Każdy pakiet rządzi się wlasnymi prawami, związanymi z określonym środowiskiem technologicznym (na które składa się język programowania, typ bazy danych, system operacyjny) i upodobaniami programistów tworzących programy (w zakresie wprowadzania danych, obsługi memu etc.). Wypada współczuć bankowym informatykom obsługującym takie róznorodne kolekcje programów "od sasa do lasa".

Systemu kupionego jako kompleksowy nie można idealizować i z góry zakładać, iż nie posiada żadnych wad zmniejszających operowalność systemu. Na przyklad, mogą wystąpić trudności w zrozumieniu funkcjonalności systemu, gdy występuje w nim wiele funkcji o podobnym przeznaczeniu lub niestowalnych w danym banku. System jest wówczas nimi "zaśmiecony" , lecz autorzy boją się je usunąć z oprogramowania ze względu na ewentualne nieudokumentowane powiązania z innymi funkcjami.

Jednym z wymogów operowalnosci jest kontrolowalność spójności systemu. Im większa złożoność systemu i głębsza jego parametryzacja, dokonywana przez administratorów i przez samych użytkowników, tym bardziej system powinien być wyposażony w mechanizmy automatycznego wykrywania ewentualnych wewnętrznych sprzeczności, braku obligatoryjnych tablic itp. Bez takiego podparcia trudno jest system przetestować w pełni na etapie wdrożenia i gwarantować jego bezbłędność podczas przetwarzania (gdy np. pojawią się nietestowane kombinacje parametrów lub nietestowane funkcje). Pożądane jest dla stabilności systemu , aby na przykład w ramach procedur otwierania dnia uruchamiany był specjalny przebieg testujący spójność systemu (aby nieoczekiwane "run-time errors" nie pojawiały się w trakcie obsługi klientów).

2.Nieudokumentowanie systemu

Im bardziej skomplikowana jest architektura systemu, tym większa występuje potrzeba posiadania dokumentacji eksploatacyjnej , obejmującej opisy modułów, produktów, struktury katalogów w pamięci dyskowej, funkcji programów, postępowania w przypadku pojawienia się błędów przetwarzania lub utraty danych , administrowania bazami danych itp. Istotnymi częściami takiej dokumentacji są instrukcje dla końcowego użytkownika (głównie dysponenta i kasjera) w zakresie obsługi poszczególnych typów rachunków oraz instrukcje tzw.zamykania/otwierania dnia.

Do najbardziej istotnych zagadnień rzutujących na operowalność należy technologia utrzymywania baz danych (uwzględniając ich stopien rozproszenia czy też replikacji) i elektronicznego archiwum

operacyjnego (np. na dyskach optycznych), pracy oddziałów w warunkach zerwania łączności teletransmisyjnej, oraz technologia zamykania dnia. W przypadku baz danych chodzi o reorganizacje w przypadku zmniejszenia efektywności przetwarzania (np.wskutek zbytniej fragmentacji), procedury "odzyskiwania" danych w przypadku awarii oraz przełączania pracy na ośrodek rezerwowy , okresowe "czyszczenia", naprawy spójności itp.. W procedurach zamykania dnia należy przewidzieć możliwości przetwarzania z datami wstecznymi, cofania przetwarzania (do określonych tzw.kroków) w przypadku wystąpienia błędów lub awarii.

3. Brak pomiaru i kontroli ryzyka bankowego w stosunku do produktów

Brak elastyczności systemu bankowego jest kłopotliwy , ale w pewnych warunkach jej nadmiar może okazać się szkodliwy , gdyż przy łatwej technice generowania typów produktów łatwo można utracić nad nimi kontrolę .Kontrola polega nie tylko na ustanowieniu określonych praw dostępu do funkcji definiowania produktów, lecz również na *kontroli ryzyka finansowego.*

W architekturze systemu niezbędny jest więc moduł oceny ryzyka kredytowego. *W warunkach zachodnich moduły zarządzania ryzykiem opracowywane są często siłami własnymi banków , gdyż można wtedy uwzględnić lepiej specyfikę "indywidualnych" (np.derywatywowych) instrumentów finansowych danego banku i łatwiej zintegrować z istniejącymi aplikacjami*.

Jak wiadomo, ryzyko jest to niebezpieczeństwo poniesienia straty lub nieosiągnięcia spodziewanego zysku założonego przy podejmowaniu decyzji o zawarciu transakcji bankowej .W podstawowym układzie klasyfikacyjnym wyróżnia się ryzyko rynku, ryzyko operacyjne, ryzyko kredytowe,ryzyko utraty płynności, ryzyko prawne itp.

System może zmniejszać ryzyko poprzez takie *techniki* jak zabezpieczenia (hedging) operacji kapitałowych, arbitraż i zarządzanie limitami (klientów,walut,krajów,dilerów ...), prognozowanie zmian stóp procentowych i kursów wymiany walut, rating banków i kredytobiorców, ryzyko ukształtowania się niekorzystnej struktury bilansowej, scenariusze co jeśli (if-what), symulowanie przepływu pieniężnego, prezentację produktowo-terminowej struktury stóp procentowych, modelowanie ryzyka (np.w oparciu o modele kowariancji) itp. .

4. Zbyteczna nadmiarowość

Pewna nadmiarowość systemu jest niezbędna w celu zabezpieczenia elastyczności poprzez wybór jednej z wielu opcji już istniejących w systemu. Nadmiarowość systemu nie powinna być jednak za duża (np. pozostawienie produktów typowych dla warunków Zachodnich - rachunków ESCROW, rachunków emerytalnych IRA-Individual Retirement Account , itp.), gdyż wówczas złożoność systemu może przeszkadzać w zrozumieniu jego funkcjonalnosci i odbić się ujemnie na eksploatacji systemu (zwiększone pole błędów wskutek występowania zbyt wielu czynności menu , nadmierne angazowanie zasobów pamięciowych itp.).

5. Brak elastyczności

Brak elastyczności jest katastrofą, gdyż niemożliwe się staje dostatecznie szybkie dostosowanie systemu do potrzeb klientów, zmieniającego się profilu usług bankowych, zmieniających się wymagań banku centralnego itp..
Ponieważ pojęcie elastyczności systemu bankowego może być rozmaicie interpretowane, określimy je co najmniej jako:
- definiowanie planu kont i księgowań
- definiowanie (parametryzacja) typy produktow i transakcji
- definiowanie zakresu pozycji klienta,waluty,banku
- generowanie menu indywidualnego dla każdej klasy użytkowników (grupy stanowisk pracy)
- możność zmian struktur danych i generowanie ekranów odzwierciedlających te zmiany
- stosowanie generatorów raportów (opartych na słowniku danych)

6. działania zmniejszające ryzyko nieoperowalności systemu

Przed utratą operowalności systemu bank może się zabezpieczać poprzez:

- zagwarantowanie w kontrakcie dokumentacji eksploatacyjnej dla końcowych uzytkowników oraz administratorów systemu
- dokładne rozgraniczenie w systemie - np.poprzez prawa dostępu - elementów rdzenia systemu (w zasadzie zmienianych jedynie przez autorów), elementów kastomizowalnych i zasad konstrukcji elementów , które mogą być swobodnie dodawane przez bank uzytkujący)
- usunięcie z systemu nadmiarowości funkcjonalnej o ktorej z góry wiadomo, że nie znajdzie zastosowania w ogóle (z powodu różnic systemu konstytucyjno-prawnego) lub w ciągu najbliższych kilku lat
- zastosowanie organizacyjnych i funkcjonalnych środków definiowania produktów bankowych oraz pomiaru ich ryzyka bankowego

Ryzyko dezintegracji informacji i organizacji

1. Komputeryzacji nie należy nakładać na dotychczasowe struktury organizacyjne

Na uwagę zasługuje teza, że komputeryzacji nie należy nakładać na dotychczasowe struktury organizacyjne i metody działania, gdyż wzajemne niedopasowanie grozi albo niewydolnością organizacyjną w zakresie obsługi nowych produktów bankowych, albo niewykorzystaniem zalet komputeryzacji. Ryzyko takich sytuacji może szczególnie wystąpić w przypadku, jeśli zmienia się radykalnie typ systemu informacyjnego (np. z trybu zdecentralizowanego przechodzi się do rozwiązania scentralizowanego) i wymaga to zmiany procedur decyzyjnych.

Oddziaływania systemu informacji i systemu organizacji są dwukierunkowe np. *dezintegracja informacji wzmacniać będzie dezintegrację organizacji.* Dezintegracja informacji ma miejsce na przykład w przypadku funkcjonowania informatycznego systemu jako zestawu autonomicznych pakietów oprogramowania, nie powiązanych ze sobą, dedykowanych do obsługi potrzeb określonego zespołu czy departamentu. Możliwa jest wówczas sytuacja, że zakresy informacyjne pakietów zachodzą na siebie , ale żaden z nich nie zbiera informacji całościowej w skali banku. Syntetyczne informacje są niemożliwe do uzyskania poprzez sumowanie baz cząstkowych z powodu dublowania danych. W tym przypadku nawet nie pomogą ewentualne łącza importowo-eksportowe pomiędzy pakietami.

Jeśli do rozproszenia informacji dochodzi jeszcze rozproszenie terytorialne jednostek organizacyjnych (np. departamentów centrali) to w przypadku braku jednolitego sieciowego systemu zapewniającego wspólne dane i płynny rozpływ informacji po komórkach organizacyjnych banku wzrasta również ich izolacja organizacyjna.

2.Projektowanie hurtowni danych jako okazja do uporządkowania zasobów informacyjnych

Okazją do uporządkowania zasobów informacyjnych banku jest projektowanie hurtowni danych (data warehouse), obejmującego m.i. sporządzenie specyfikacji informacji wspólnych (zwanych meta-danymi) , które będą wykorzystywane w skali całej instytucji, oraz zaprojektowanie wielowymiarowych baz danych , przeznaczonych nie tylko dla sprawozdawczosci finansowej lecz również dla kierownictwa banku .

Jeśli w banku stosowane są odrębne systemy dla bankowości detalicznej i bankowości komercyjnej hurtownia danych może stać się platformą integrującą je w kontekście informacji syntetycznych (natomiast pozostanie problem integracji na poziomie transakcyjnym np.w zakresie rachunków nostro, pozycji klientów , biezącej pozycji waluty itp.).

Brak kompleksowości jest jedną z typowych wad systemów bankowych. Nie można jednakże stawiać tutaj postulatu "wszystko albo nic !" (albo obejmuje całość działalności bankowej albo nie kupowac) , gdyż tak na prawdę, nie ma (lub prawie nie ma) systemów naprawdę kompleksowych , pochodzących od jednego wytwórcy .Przedsięwzięcia integracyjne są szczególnie złożone w przypadku pakietów pochodzących od różnych autorów. całkowicie autonomicznych, tzn. posiadających komplet swoich własnych danych (klientów, banków, walut, kont księgowych) i nie wyposażonych w odpowiednie łącza do innych aplikacji .Integracja ich jest jeszcze bardziej utrudniona ,jeśli przetwarzane są na różnych komputerach lub pod różnymi systemami operacyjnymi lub też używają różnych systemów zarządzania bazami danych.

Stosowanie autonomicznych pakietów do potrzeb poszczególnych służb, departamentow czy oddziałów utrwala dezintegrację organizacyjną banku , dając im „siłę" w postaci "własnych" źródeł informacji

3. Potrzeba nowego podejścia organizacyjnego przy komputeryzacji banku

Radykalną metodą dostosowania systemu organizacji do systemu informatycznego (odwrotne podejście może miejsce chyba tylko wówczas gdy istnieje konieczność wymiany rozwiązań informatycznych) jest metoda BPR (Business Process Reengineering) , polegająca nie na ulepszaniu aktualnie stosowanych procedur , lecz na zaprojektowaniu ich „od nowa" pod kątem zwiększenia efektywności biznesu, wykorzystując wszelakie możliwości elektronicznego przepływu informacji po sieci komputerowej i nowe możliwości przetwarzania danych (po wprowadzeniu technologii klient-serwer , hurtowni danych, itp.). W ramach BPR rozważane są m.i. kwestie orientacji schematów organizacyjnych instytucji na układ poziomy (płaski) lub hierarchiczny , problemowy (zadaniowy), technika pokonywania oporu wobec wprowadzanych zmian itp.

Inną metodą ponownej konstrukcji (tak chyba można nazwać „reengineering") systemu jest IE/CASE (Information Engineering and CASE tools) , którego przedmiotem są szeroko (tak pod względem techniki jak i kultury działania) pojęte procedury działania, podporządkowane naczelnym zasadom jakości (tzw. TQM principles - Total Quality Management) i wspomagane przez narzędzia komputerowe do generowania oprogramowania (stąd w nazwie CASE-computer Aided Software Engineering). Do naczelnych zasad jakości zalicza się m.i. przywództwo (od lidera grupy zależy wiele), kontrola jakości produktów i obsługi (Quality Assurance of Products and Services) oraz satysfakcja klienta.

Przykładem podejścia BRP może być przyjęcie procesów stowarzyszonych z produktami bankowymi jako kryterium płaskiej struktury organizacyjnej. Korzyści z przyjęcia takiej struktury są znane, a więc mniej biurokracji (krótka droga decyzyjna, szybki dostęp do „źródłowych" pracowników bezpośrednio mających kontakt ze zmiennym rynkiem usług bankowych) oraz działania ukierunkowane na dobrze określone cele. Struktura działa w ten sposób, że gdy zgodnie ze strategią finansową banku zapada decyzja wprowadzenia nowego typu produktu powołuje się - na prawach komórki organizacyjnej - zespół interdyscyplinarny produktu, który go nie tylko wdraża i modyfikuje lecz również prowadzi badania marketingowe (poszukiwanie nowych klientów, działania mające na celu zachowanie klientów dotychczasowych rynkowe, badanie relacji produktu w stosunku do podobnych produktów innych banków, parametryzację produktu (tworzenie podproduktów) stosownie do wymaganej dochodowości oraz zachowań rynku, badanie stopnia ryzyka produktów itp.

Gdy typ produktu jest wycofywany członkowie rozwiązywanego zespołu zgodnie ze swoimi specjalnościami są przydzielani do innych zespołów .W ten sposób bank podlega ciągłej restrukturyzacji - ta "niestabilność" organizacyjna może być frustrująca z powodów ogólnoludzkich, lecz jeśli w danej organizacji istnieją dobre stosunki międzyludzkie i doceniany jest wkład pracy, pracownicy uzyskują szansę awansu zgodnie z kwalifikacjami i o wiele częściej niż dzieje się to w tradycyjnych strukturach (aż kierownicy zostaną wysłani na emerytury itp.)

Wniosek

Wdrożenie systemu informatycznego to nie tylko instalacja oprogramowania na komputerach i przeszkolenie uzytkowników, lecz również stworzenie odpowiedniego środowiska organizacyjnego w banku.

Zygmunt Ryznar

Zygmunt Ryznar

Dekalog grzechów komputeryzacji

cz.4 Ryzyko niedostatecznego bezpieczeństwa systemu

(tam gdzie chodzi o pieniądze wszystko jest mozliwe)

Ze względu na finansowy charakter transakcji bankowych, wysoki stopień złożoności i ogromne ilości danych systemy bankowe powinny być zabezpieczane w sposób wyjątkowo staranny i pełny. Źródła zagrożeń są rozmaite. Wg miarodajnego źródła (DataPro Information Service) statystyka zagrożeń w systemach informatycznych wygląda następująco: 5 % spowodowanych jest przez wirusy i zawodowych włamywaczy, 15 % stanowi zagrożenie fizyczne, 20 % zalicza się na konto nieetycznych działań pracowników, zaś aż 60 % stanowią błędy i przeoczenia personelu firmy uzytkujacej system.

1.Błędy i przeoczenia personelu

Mylenie się jest naturalnym atrybutem człowieka (“errare humanum est”), co potwierdza wyżej podana statystyka zagrożeń. Do tego typu przewinień zaliczyć można przypadkowe ujawnienie informacji wskutek błędu operatorskiego (np. przesłanie danych do niewłaściwego klienta, wyświetlenie informacji poufnych na wszystkich terminalach, wyrzucenie “ważnego” raportu do kosza na śmieci, itp.). W warunkach pracy pod systemem operacyjnym MSDOS zdarzyć się może przypadkowe sformatowanie dysku lub usunięcie katalogu albo pliku, zmiana atrybutu pliku z ukrytego na jawny itp. Do najczęstszych uchybień należą błędy palcowania na klawiaturze, np. po zmianie systemu na jednej z giełd elektronicznych uległa zmianie kolejność pól i zdarzało się często, że ilość akcji wpalcowywana była przez maklera w pośpiechu do pola “cena akcji” zamiast “ilość akcji” (co doprowadziło pewnego dnia nawet do zawieszenia pracy giełdy z powodu “dziwnych” wyników finansowych), za tego typu błąd można też uznać dodanie jednego zera za dużo w długich liczbach itp.). Ryzyko tych zagrożeń zależy od organizacji pracy, cech psychofizycznych pracowników oraz wrażliwości systemu informatycznego na przypadkowe błędy.

2.Wirusy i zawodowi włamywacze

Mimo deklaracji producentów i firm software’owych o odporności niektórych systemów operacyjnych na zawirusowanie nie należy lekceważyć tego problemu i wdrożyć systematyczne badanie pamięci operacyjnej i dyskowej programami antywirusowymi (najlepiej rezydującymi na stałe w pamięci operacyjnej czyli typu TSR Terminate and Stay Resident). Poważniejszym problemem mogą być umyślne działania zawodowych włamywaczy komputerowych (tzw. intruderów, crackerów, hackerów) działających w sieciach rozległych, którzy po przechwyceniu komunikatów sieciowych (zawierających adresy sieciowe i dane), znając dokładnie mechanizmy systemów operacyjnych lub techniką "koni trojańskich" (np. fałszywy ekran aplikacji) przechwytują wejścia użytkowników (nazwa programu, identyfikatory i hasła użytkowników) uzyskując dostęp do aplikacji .

3.Nieetyczni pracownicy

Zagrożenia w tej grupie mogą być wielorakie, a ochrona przed nimi jest wyjątkowo trudna. W szczególności wymienić można :

- nadużycia popełniane w systemie przez pracowników banku , byłych pracowników banku i klientów systemu np. znających formaty elektronicznych dokumentów i stosowane zabezpieczenia (cyfry i sumy kontrolne) wprowadzających fałszywe elektroniczne dokumenty płatnicze lub popełniajacych nadużycia w systemie obsługi kart płatniczych , względnie wykorzystujących luki w prawie bankowym itp.
- niewłaściwie określony zakres dostępu dla użytkowników systemu (każda klasa użytkowników bankowych powinna mieć indywidualnie skonfigurowane menu, z którego jedynym wyjściem jest wylogowanie się z aplikacji (zabezpiecza to przed możliwością wykonywania np. komend systemu operacyjnego).
- dostęp do oprogramowania systemu i baz danych programistów banku, którzy mogą np. chwilowo zmieniać daty systemowe i czas (aby ukryć moment dokonania oszustwa), modyfikować algorytmy (np.sposób zaokrąglenia kwot z generowaniem transferu różnicy na inne rachunki bankowe) lub też zmieniać zawartość baz danych (np.salda na rachunkach) używając uniwersalnych narzędzi edycyjnych nie pozostawiających śladów audytowych.
- dostęp nieuprawnionych osób do pomieszczeń serwerów, dysków , taśm i wydruków itp.
- umyślne “psucie” baz danych np. poprzez dezorganizację relacji w bazach danych (pozostawienie rekordu typu “dziecko” bez rodzica itp.).

4.Zagrożenie fizyczne

Głównym zagrożeniem jest umyślne lub losowe unieruchomienie centrum obliczeniowego. Zwykle zabezpieczeniem przeciwko temu jest równolegle zasilany danymi awaryjny komputer zlokalizowany w innym miejscu - tzw. disaster recovery centre). Koszty takiego rozwiązania można zmniejszyć poprzez

długoterminowy kontrakt z firmą zewnętrzną na tzw. hot-site - obejmujący bieżący automatyczny backup na analogiczny komputer w stacjonarnym lub ruchomym (mobile) ośrodku obcym znajdującym się z reguły w pewnym terytorialnym oddaleniu (aby zabezpieczyć się przed zdarzeniami losowymi typu pożar, powódź itp.) i inicjację przetwarzania w przypadku awarii systemu macierzystego. Na świecie istnieje wiele firm specjalizujących się w świadczeniu tego typu usług , łącznie z odzyskiwaniem danych.

5.Poziomy zabezpieczeń

Realizacja zabezpieczeń następuje poprzez systemy operacyjne komputerów, sieciowe systemy operacyjne , systemy zarządzania bazami danych . oprogramowanie aplikacyjne oraz przedsięwzięcia organizacyjne.

A. system zarządzania sieciami komputerowymi i systemami rozproszonymi

Rola zabezpieczeń na tym poziomie wzrasta wraz z rozwojem sieci rozległych (np.internetowych) i stosowaniem architektury klient-serwer. Stosowanie tzw. otwartych (standardowych czyli ogólnie znanych) rozwiązań powinno być zrównoważone przez odpowiednie zabezpieczenia. O słabości całej sieci decydują nasłabsze jej ogniwa (przez nie można wprowadzić konia trojańskiego), każdy węzeł sieci musi podlegać tym samym rygorom, najlepiej zabezpieczać sieć już na poziomie terminali i stacji roboczych (czyli tam gdzie można wejść do systemu). Wśród zabezpieczeń najpopularniejsze staje się tworzenie ścian zaporowych (firewalls) mających na celu wykrycie nieuprawnionych użytkowników sieci oraz generowanie przez serwer sieciowy "biletów" użytkownika z hasłami ważnymi tylko na przeciąg jednej sesji. Rozwój łączności radiowej, satlitarnej stwarza szerokie możliwości omijania konieczności fizycznego podłączania się do okablowania sieci. W związku z tym podstawową metodą zabezpieczania pozostaje szyfrowanie (kryptografia) danych i złożone algorytmy "routowania" oraz ciągła weryfikacja wszystkich procesów pojawiających się w sieci. Metody szyfrowania danych stale ulegają doskonaleniu ze względu na ich "złamania" przez hakerów. Przykładowo, w 1994 roku złamano 129 bitowy publiczny klucz RSA, w związku z powyższym opracowane są klucze nawet ponad 1000 bitowe.

Architektura klient-serwer zwykle niesie ze sobą też pewne zagrożenia, wynikające z niedostatecznego zabezpieczenia aplikacji na poziomie sieci. Źródłem tych zagrożeń są na przykład protokoły sieciowe przenoszące adresy w ramkach komunikatów. Adresy te "biegają" po sieci i w pewnych warunkach mogą stać się łupem dowolnego użytkownika. Szczególnej ochronie podlegać powinny zdalne wywoływania procedur (RPC - Remote Procedure Call) , które już u klienta powinny podlegać zaszyfrowaniu zaś rozszyfrowywać powinien je dopiero serwer.

Należy przyznać, że z ubiegiem czasu wzrasta stopień zabezpieczenia sieciowego. Chociaż internet z definicji jest globalną ogólnodostępną siecią światową, wprowadzane są sieci zamknięte zwane intranetem ("wewnętrzny internet") łączące się z "zewnetrznym" internetem poprzez ściany zaporowe (firewall) i serwery kontrolne (authentication servers) z mechanizmami poświadczającymi autentyczność użytkownika, filtrującymi domeny i dostęp do serwerów internetowych, itp.

B . system operacyjny komputera

Rola zabezpieczenia pojedynczych komputerów maleje w przypadku aplikacji rozproszonych , a korzystających z zasobów całej sieci. W klasycznym przypadku (mainframe) zabezpieczenie na poziomie systemu operacyjnego obejmuje identyfikację i autentyfikację użytkowników,kontrolę dostępu, zabezpieczenie śladów audytowych oraz właściwe utrzymywanie zasobów systemowych. *Identyfikacja poza nazwą obejmuje również sprawdzanie* hasła , zaś *autentyfikacja sprawdza* lokalizację użytkownika *i autentyczność użytkownika poprzez* dodatkowy dialog sprawdzający. *Kontrola dostępu przebiega na poziomie katalogów,plików,programow-procesów itp.Ślady audytowe są szczegółową* rejestracją zdarzeń zachodzących w systemie. Na poziomie systemu operacyjnego dostęp do aplikacji kontrolowany jest poprzez hasło oraz prawa czytania, pisania, kopiowania, usuwania (itp) poszczególnych plików . Hasła powinny być zmienne, zaś ich ewidencja niezwykle staranna i prowadzona przez niewielką liczbę zaufanych osób. Do wykonywania niektórych operacji powinna być zabezpieczona możliwość stosowania haseł dwuczłonowych np.podzielonych pomiędzy np.dwie osoby (każda z nich zna część hasła - czyli do wykonania czynności niezbędna jest obecność obu tych osób). System powinien prowadzić ewidencję zmian haseł (kto i kiedy zmieniał hasło w danej klasie użytkowników).

C. system zarządzania bazą danych (SZBD)

SZBD może znacznie wzmocnić bezpieczeństwo danych poprzez zapewnienie ich integralności , pogłębioną kontrolę dostępu do informacji (np.schodząc do poziomu pól), prowadzenie własnego dziennikowania (journalizing) umożliwiającego odzyskanie danych itp.

D. aplikacja

Aplikacja powinna posiadać własne (niezależny od systemu operacyjnego) zabezpieczenia identyfikujące użytkowników i wprowadzające podział czynności wg klas użytkowników, ślady audytowe, wychwytywanie zmian wykonanych poza aplikacją, lokalne oprogramowanie oddziału znajdującego się w stanie off-line z

powodu awarii linii teletransmisyjnej itp. .

E . program

Zawiera dodatkowe zabezpieczenia specyficzne dla funkcjonalności danego programu np. uprawnienia kwotowe realizacji poszczególnych typów transakcji .

F. zabezpieczenie fizyczne

Obejmuje różnorodne przedsięwzięcia, takie jak podtrzymywanie zasilania w energię elektryczną, ośrodek zapasowy (disaster recovery centre), archiwium na niemodyfikowalnych dyskach optycznych (typu WORM) w celu zabezpieczenia danych historycznych przed zmianami.

G. zabezpieczenie organizacyjne

Głównym środkiem organizacyjnym jest podział oprogramowania aplikacyjnego na warstwy (projektowa, testowa, modelowa, produkcyjna, eksperymentalna) i całkowite oddzielenie programistów od warstwy produkcyjnej. *Każda z warstw powinna być w pełni izolowana*, to znaczy posiadać swoje klasy użytkowników, swoje definicje produktów, swoje oprogramowanie aplikacyjne i swoje bazy danych . Liczba warstw zależy od zakresu prowadzonych prac modyfikacyjnych i dostępnych zasobów dyskowych.

6.Zabezpieczenie na poziomie aplikacji

Wg amerykańskich standardów zawartych w tzw. księdze "pomarańczowej" (TCSEC-Trusted Computer System Evaluation Criteria Orange Book) lub księdze "lawendowej" (NCSC-National Computer Security Center) Lavender Book.

- grupa **D** (oznacza jedynie minimalne zabezpieczenie, np. hasło wejściowe przy logowaniu się)
- grupa **C** (np.C2 narzuca kontrolowany dostęp - poprzez nadanie uprawnień - do operacji np. select, update.. oraz do obiektów typu pliki danych)
- grupa **B** (wymaga wprowadzenia dodatkowych zabezpieczeń np. zróżnicowanego poziomu poufności MLS - Multilevel Security opartego na technice etykietowania - sensivity labels - informacji w bazie danych), MAC (Mandatory Access Control), aktywnego monitorowania administratora o narastaniu zdarzeń świadczących o intensyfikacji prób włamań do systemu i zmuszeniu go do podjęcia działań co najmniej przerywających podejrzane procesy itp.
- grupa **A** (oznacza najwyższy -top secret- stopień zabezpieczenia, zwykle weryfikowany formalnie wg specjalnych standardów).

W aplikacjach stosujących komunikaty EDIFACT (Electronic Data Interchange for Administration Commerce and Trade) należy przestrzegać określonych standardów komunikatów i bezpieczeństwa (głównie identyfikacji użytkownika np. poprzez podpis elektroniczny i szyfrowania informacji). Przykładowo w USA znajdują zastosowanie standardy ANSI X9.24 dla transakcji detalicznych - retail - oraz X9.26 i X.28 dla transakcji komercyjnych - wholesale.

W ramach aplikacji bankowej zabezpieczenie polegać może na dodatkowej kontroli (w stosunku do systemu operacyjnego) logowania się (sign-on) użytkowników oraz bardzo szczegółowym rozpisaniu (np.poprzez generowanie menu) dla poszczególnych użytkowników uprawnień wykonywania poszczególnych funkcji i dostępu do typów transakcji, uprawnień modyfikacji zawartości określonych pól itp. Ponadto na poziomie typów transakcji (do ich wprowadzania i autoryzacji) przydzielane są hasła i/lub limity kwotowe dla różnych grup personelu (kierowników, dysponentów , kasjerow i dilerów) . Przełamanie limitu możliwe powinno być jedynie poprzez akceptację uprawnionej osoby.

Identyfikacja użytkownika może polegać nie tylko na stosowaniu hasła lecz również dialogu typu "handshaking" polegającego na zastosowaniu sekwencji pytań i odpowiedzi (np. imienia najmłodszego dziecka, miejsca urodzenia czy roku ukończenia szkoły średniej).

System aplikacyjny powinien być bezwzględnie zabezpieczony przed "niezależnymi" (np.używając systemowych procedur lub edytorów poza aplikacją bankową) zmianami informacji, takimi jak korekta salda rachunku , usuwanie transakcji, zmiany w śladach audytowych , w tablicach systemowych ,"poprawianie " danych archiwalnych, itp. Zamiast usuwania transakcji należy stosować transakcje stornujące (rewersyjne).

Aplikacja powinna być wyposażona w . procedury odzyskiwania danych w przypadku awarii lub ich usunięcia .System zapewnić powinien pełne ślady błędów przetwarzania , umożliwiające identyfikację przyczyny błędu oraz miejsce jego wystąpienia (w jakim programie lub funkcji oraz linii lub instrukcji).

Podstawowym wymaganiem stawianym aplikacji jest tworzenie śladów audytowych oraz śladów logowania się w ramach aplikacji. Każdy rachunek oraz baza klientów powinny być stowarzyszone z pełną (na dowolny dzień roku bieżącego i ubiegłego - lub zależnie od dostępnych zasobów dyskowych) historią rachunków oraz zmian. Historia rachunków i zmian (wspomagane techniką dziennikowania - journalizing - systemu zarządzania bazą danych) powinny umożliwiać odtworzenie stanu baz danych na określony dzień w

przeszłości.Niezależnie od historii rachunków system powinien utrzymywać automatycznie dziennik wejść transakcyjnych ("śladów"-tzw.audit-trail), tworzony w trakcie wprowadzania (a nie po !) transakcji . Pełne ślady powinny obejmować co najmniej: datę wykonania, efektywną datę transakcji, terminal z którego dokonano transakcji, ID użytkownika, kwote, rodzaj transakcji, unikalny nr transakcji w danym dniu, oznaczenie statusu operacji (zrealizowana,anulowana, wycofana lub błędna). W przypadku operacji aktualizujących pliki i bazy danych ślad audytowy będzie zawierał informacje o poprzedniej i aktualnej zawartości zmienianych pól.

Atestowanie aplikacji bankowych na stopień bezpieczeństwa powinno być obowiązkową czynnoscią przed dopuszczeniem oprogramowania do eksploatacji. Atestacja taka może wymagać nawet udostępnienia kodu źródłowego, aby np. upewnić się, że znajdują się w nim mechanizmy stabilizujące integralność danych (np. tzw.rollback) lub też czy spełnia wymagania tzw. API (Application Program Interface) niezbędne do współdziałania z innymi programami oraz jakie ścieżki logiczne należy przede wszystkim testować . W procedurze astestowania używa się czasem specjalistycznego oprogramowania typu "reverse engineering" aby uzyskać dokładny obraz (np.w postaci schematu blokowego) działania programu i współdziałania podprogramów. Nie należy również zapominać o badaniu antywirusowym .
Problematyce wydawania atestów bezpieczeństwa dla oprogramowania aplikacyjnego nadaje się dużą wagę w USA i Wielkiej Brytanii.W obu krajach wdrażane są programy mające na celu wprowadzenie trybu formalnego testowania oprogramowania na stopień zabezpieczenia (w USA - Trusted Technology Assesment Program : TTAP, w W.Brytanii - Commercially Licensed Evaluation Facilities CLEF). Wyraźny postęp w tym kierunku stanowi tzw. biała księga (ITSEC White Book - ITSEC Information Technology Security Evaluation Criteria) , precyzująca poziomy (E0 do E6) oceny oprogramowania zwane TOE (Target Of Evaluation) oraz 10 klas zabezpieczenia , przyjęta przez W.Brytanię,Francję, Niemcy i Holandię i w 1991 akceptowana przez Wspólnotę Europejską.

Stosowanie metod sztucznej inteligencji do zwalczania nadużyć
Systemy z zakresu sztucznej inteligencji, w postaci systemów "neuronowych" lub ekspertowych, znajdują zastosowanie w tzw. środowisku słabo określonym lub nieokreślonym (np. w rozkładach liczb sprawiających wrażenie chaosu), w którym nie występują klasyczne algorytmy z dokładnie zdefiniowanymi zmiennymi i zależnościami arytmetycznymi. Wbrew powszechnemu odczuciu systemy te stosowane są od dawna, aczkolwiek nie tak masowo jak zwykłe systemy informatyczne. Przykładem pionierskiego złożonego systemu neuronowego był w połowie lat 80-tych system wykrywania bomb na lotnisku J.F.Kennedy'iego w Nowym Jorku i system analizy ryzyka kredytowego w AVCO Financial Services. Inną dziedziną zastosowań systemów neuronowych jest wykrywanie oszustw typu wyłudzanie odszkodowań z tytułu ubezpieczeń i tworzenie strategii inwestowania dla biur dilerskich (np. na Wall Street) oraz wykrywanie nadużyć w przypadku kart płatniczych (np. w Chase Manhattan Bank, Mellon Bank, Security Pacific).

Skutki braku zabezpieczenia systemu informatycznego mogą być dla banku róznorakie, począwszy od utraty zaufania ze strony klientów i przejscia ich do innych banków, skończywszy na utracie znacznej części własnego kapitału.

Zygmunt Ryznar

Zygmunt Ryznar

dekalog grzechów komputeryzacji

część 5. *Grzech* **6. Prototyp jako ryzyko wyboru nowości**

Zarządzający informatyką w instytucjach finansowych znajdują się pod stałą presją nowości. Dotyczą one komputerów (np.wieloprocesorowość), sieci (transmisja asynchroniczna, Internet), architektury przetwarzania (technologia klient-serwer), urządzeń bankowych (inteligentne karty płatnicze, homebanking poprzez telewizję kablową), zarządzania danymi (wielowymiarowe hurtownie danych) itp. Oprócz postępu technicznego dochodzą nowości w zakresie rozwoju samych aplikacji bankowych (obsługa nowych produktów bankowych, standardy EDIFACT w sieciach finansowych itp.).

Zakladając, iż cykl życia nowości wynosi 5-7 lat , należy tyle inwestować, ile zdoła się wdrożyć w ciągu 3-4 lat (gdyż po tym okresie rozpoczyna się etap decyzyjny wyboru następnej nowości). Podejmujący decyzje ponosi duże ryzyko, gdyż może inwestować w nowości, które zostaną zahamowane w wyniku walki konkurencyjnej, lub też są nimi tylko z nazwy ("stare" w nowym opakowaniu).

Decyzje inwestycyjne nalezy podejmować w stosownym zakresie i w odpowiednim czasie. Nie ma niestety gotowych reguł zapewniających takie postępowanie. Jeśli decyzje podjęte zostaną zbyt wczesnie lub bez dostatecznego rozeznania, istnieje większe ryzyko, iż nowość nie będzie nowoczesnym rozwiązaniem, natomiast jeśli zbyt późno - nie zdążymy jej wykorzystać, gdyż stanie się przestarzała.

To, co w zainwestowaliśmy, a przestaje być nowością, można starać się skierować do innych aplikacji. Na przykład w USA liczba bankomatów ma się zwiększać (a nie maleć jak w Europie), ale co piąty z liczących się banków planuje wykorzystywać bankomaty nie do tradycyjnych usług kasowych lecz do świadczenia usług ubezpieczeniowych , zaś co trzeci bankomat nie będzie związany z konkretnym oddziałem bankowym (lecz z centralą banku).

Przeradzanie się nowości w trwałą tendencję rozwojową stwierdzić można m.i. na podstawie zachowywania się potentatów komputerowych. Ponieważ "sparzyły się" one niejednokrotnie na nietrafionych pracach badawczo-rozwojowych, koncentrują się obecnie na wyłapywaniu "obcych" prototypów gotowych do szerokiego upowszechniania a opracowywanych przez małe firmy, dysponujące odpowiednim pomysłem i niedostatecznie dużym kapitałem. Przykładem tego typu działania w zakresie takiej nowości jak wielowymiarowe bazy danych są firmy ORACLE (wykupienie firmy IRI z pakietem Express) i Informix (przejęcie firmy Metacube). Wyraźnie zamierzają one radykalnie zmodernizować swoje relacyjne bazy danych (mające szczyt powodzenia za sobą) lub pójść ewentualnie w zupełnie nowym kierunku. Pewną nowością w najbliższych latach może być specjalizacja dużych komputerów typu "mainframe" w obsłudze bardzo dużych hurtowni danych.

Przykładem innej nowości, dopiero oczekującej na upowszechnienie, jest neuronowa technologia przetwarzania danych (wykorzystywana w bankowości do modelowania ryzyka finansowego, symulacji zachowania się klientów, przewidywania kursów giełdowych itp.).

Aby doprowadzić system bankowy od stanu prototypu do stabilnego stanu eksploatacyjnego trzeba nie tylko dysponować dużymi środkami finansowymi lecz odpowiednio to zorganizować poprzez komputerowo obsługiwaną kontrolę nad wprowadzanymi zmianami oraz testowanie systemu w wielu iteracjach (nawrotach) .

Może się zdarzyć, że zamiast systemu kupimy tylko jego szkielet i narzędzia projektowo-programistyczne. Wówczas ryzyko niepowodzenia jest jeszcze większe. Kupując gotowy (lub prawie gotowy) system zagraniczny dostajemy nie tylko ileś tam godzin pracy programistów , lecz przede wszystkim nową wiedzę bankową. Decydując się więc na opracowanie systemu własnymi siłami ryzykujemy to, iż nowoczesne narzędzia zastosujemy tylko do automatyzacji własnych przestarzałych produktów bankowych !.

Grzech 7. Ryzyko przekroczenia budżetu komputeryzacji

W przypadku kupna systemu bankowego istotną i trudną kwestią jest jego **cena**. Zwykle samo oprogramowanie aplikacyjne (zwykle jest to licencja a nie prawo własności) i sprzęt można wycenić mniej więcej precyzyjnie , lecz udział ich w sumie ogólnej może nie przekraczać 50% (a czasem

wynosi zaledwie 30%). Główną pozycją cenową stają się zwykle koszty wdrożenia (w tym kastomizacji i konsultacji) i tutaj dostawcy starają się - twierdząc, że ponoszą duże ryzyko - uzyskać najwięcej dochodu. Są też koszty o których się "zapomina": np.przeszkolenie personelu banku (czasem kilka- lub kilkanaście tysiecy osób), koszty konwersji danych z dotychczasowych systemów, koszty dublowania prac w początkowym okresie wdrożenia , koszty konsultacji dodatkowych (nie da się wszystkiego przewidzieć w kontrakcie) łącznie z kosztami podróży, zakwaterowania itp.
Konsultacje stanowią też ryzyko finansowe**.** Aby spełniły one swoją rolę niezbędna jest umiejętność formułowania zadań (trzeba wiedzieć czego się chce) i egzekwowania wyników. Inaczej zamiast konstruktywnej pomocy i rozwiązania konkretnych problemów możemy otrzymać ogólnikowe wykłady prowadzone przez ludzi od marketingu (nie od roboty lecz robienia tzw. dobrego wrażenia na klientach), ogólnodostępne zachodnie publikacje itp.
Największym zagrożeniem dla budżetu wydaje się być kastomizacja. W przypadku zachodniego systemu trwa w Polsce około. roku , zaś wdrożenie w banku wielooddziałowym zajmie następny rok. Są to poważne koszty utrzymania kilkudziesięcioosobowego zespołu , składającego się z własnych i obcych pracowników (ze strony zespołu autorskiego itp), koszty utrzymania sprzętu komputerowego koniecznego do rozwoju i testowania systemu itp..

W przypadku podjęcia się przez bank opracowania systemu informatycznego własnymi siłami ryzyko finansowe jest bardzo duże. Trzeba przewidzieć wydatkowanie ok.100 ml USD na projekt i oprogramowanie zaawansowanego kompleksowego systemu bankowego, co wydaje się być sumą umiarkowaną , zakładając iż realizacja zadania potrwa ok.5 lat , czyli w warunkach dużej koncentracji kadrowej i sprawności organizacyjnej.Jest to wydatek, któremu mogą podołać tylko bardzo duże banki , zakładając , iż posiadają odpowiednio kwalifikowanych informatyków i bankowców o takim stanie wiedzy, który zapewni nowoczesność rozwiązania na wiele lat. Przykładem pomyślnego kompleksowego przedsięwzięcia informatycznego realizowanego przez bank może być system OURASI opracowany przez bank :Le Credit Agricole we Francji .

Ryzyko finansowe kastomizacji systemu własnymi siłami jest o wiele niższe, niż w przypadku budowy systemu, jednakże wymaga posiadania zdolnych programistów i prowadzenia sprawnego zarządzania zmianami (najlepiej wspomaganego komputerowo , począwszy od momentu sformułowania potrzeby zmiany, poprzez specyfikację, realizację zmiany w specjalnej warstwie rozwojowej, testowanie lokalne i systemowe, skończywszy na aktualizacji warstwy produkcyjnej).

Koszty eksploatacji systemu można zmniejszyć poprzez tzw. **outsourcing** czyli korzystanie z usług zewnętrznych. Nie tylko może to dotyczyć dzierżawy pamięci dyskowych i rezerwowania mocy komputera w firmie zewnętrznej zamiast własnego rezerwowego ośrodka obliczeniowego (disaster recovery centre), lecz również w ten sposób mogą być realizowane główne (bieżące, operacyjne) usługi obliczeniowe. Swiadczy o tym przykład banków szwajcarskich i ich umowa z Perrot Systems oraz banku włoskiego Credito Emiliano (Credem) z EDS .

Grzech 8. Ryzyko nie wywiązania się dostawcy systemu z zobowiązań

Zapewnienia firmy będącej integratorem iż dostarczy "rozwiązanie pod klucz" lub tzw. TOTAL SOLUTION, czyli wykona zadania kastomizacyjne i integracyjne oraz wdrożeniowe są wiarygodne tylko wówczas jeśli firma ta dysponuje wiedzą, ludźmi oraz środkami finansowymi do realizacji tej obietnicy i są wtedy egzekwowalne jeśli zostały w kontrakcie wyspecyfikowane zadania do wykonania oraz jeśli zadania te mają byc zrealizowane w ramach ryczałtowej kwoty (inaczej środki finansowe zostać mogą przedwcześnie wykorzystane bez realizacji całości zadań).

Wiarygodne informacje o dostawcy i wykonawcy kontraktu uzyskuje się przede wszystkim poprzez szczegółowo zaplanowane pobyty u nich na miejscu oraz u ich klientów. Przedmiotem wywiadów jest kapitał i dochodowość dostawcy, liczba specjalistów zatrudnionych w pracach projektowo-programistycznych, powiązania ze specjalistycznymi firmami software'owymi (gwarantującymi wykonawstwo złożonych zadań typu architektura klient-serwer), sposób kierowania rozwojem aplikacji oraz jej dokumentowania, proporcje zatrudnienia pracowników produkcyjnych w stosunku do pracowników marketingu i sprzedaży, dorobek wdrożeniowy i liczba pracowników zaagażowanych do prac wdrożeniowych, środki techniczne obsługi klientów (np.zdalny elektroniczny help-desk), informacje o szybkości reagowania na błędy aplikacji, skala podjętych prac badawczo-rozwojowych (oby nie za duża), obciązenie firmy w zakresie konserwacji systemów

już wdrożonych oraz zaangażowanie firmy w przetargach itp.

Istnieje zawsze pewne zagrożenie ryzykiem bankructwa firmy, wchłonięcia jej lub przejęcia pakietu kontrolnego akcji przez inną firmę. Swiadczy o tym chociażby przykład takich zasłużonych dla informatyki bankowej firm jak BIS, Kapiti, Winter Partners i Kindle.Chociaż w jakiś sposób firmy te (ich systemy) pozostały na rynku , to jednak zmiana ich statusu prawnego i finansowego oraz zwykle występujące przy tym zmiany personalne, utrudniają realizację poprzednich kontraktow. Bankructwo dostawcy groźniejsze jest w sytuacji gdy bank kupuje system wykonany na nieotwarte platformy komputerowe

9.Ryzyko uzależnienia od dostawcy lub platformy sprzętowej

Ryzyko uzależnienia się zmniejszone jest w przypadku zakupu tzw. systemów otwartych. Wymagania otwartości można formułować na poziomach sprzętu (komputerów i sieci), systemu operacyjnego, systemu zarządzania bazą danych oraz oprogramowania aplikacyjnego (architektury i poszczególnych programów). Podstawową zaletą systemów otwartych jest ich zdolność do łączenia się z innymi systemami applikacyjnymi, przenoszenia na inne platformy sprzętowe (co daje możność uniezależnienia się od dostawcy), akceptowania różnorodnych protokołów sieciowych itp.

Problemy otwartości systemów stanowią przedmiot działania kilku organizacji międzynarodowych, w tym stowarzyszenia X/Open (powołanego w połowie lat 80-tych) , UI (Unix International) oraz OMG (Object Management Group). Organizacje te opracowują standardy (np.POSIX), które określają m.i. zbiór funkcji korzystających w programach z podstawowych usług systemu operacyjnego, aby zapewnić przenaszalność na poziomie kodu źródłowego pomiędzy zupełnie różnymi systemami operacyjnymi , zasady pisania tzw.skryptów na poziomie powłoki (shell scripts) oraz podtrzymanie środowiska czasu rzeczywistego (real time environment support).
Jądro otwartego systemu operacyjnego nie powinno zawierać procedur zależnych od konkretnych platform sprzętowych zapewniając wtedy najlepszą przenaszalność począwszy od komputerów opartych na procesorach INTEL skończywszy na mainframe'ach.

Dotychczas za najbardziej otwarty system operacyjny uważany był UNIX.. W ostatnim okresie obserwuje się ekspansję systemu operacyjnego Windows NT w zastosowaniach bankowych, w szczególności na poziomie serwerów oddziałowych. W tym przypadku sprawa otwartosci ulega pewnemu uproszczeniu, gdyż występuje jeden producent (Microsoft) i system ten od “urodzenia” jest wieloplatformowy. Stopień otwartości operacyjnych systemów unixowych stanowi przedmiot dyskusji i walki konkurencyjnej. Uzyskiwanie "teoretycznej " zgodności ze standardami jeszcze nie stanowi dowodu na przenaszalność systemu pomiędzy platformami (niektóre - a może nawet większość powyższych systemów funkcjonuje tylko na jednej platformie lub tylko na komputerach jednej firmy). W ramach “otwartych” unixów stosowane są różne komendy a zdarza się często , że nawet te same komendy działają inaczej w każdym systemie.
Standardy otwartości obowiązuja również systemy zarżadzania bazami danych (np.SQLowe obowiązuje standard ISO 9075). Należy spodziewać się wejścia w życie standardów hurtowni danych.
Architektura klient/serwer budowana powinna jest wg standardów OSF - DCE (Open Software Foundation - Distributed Computing Environment) oraz OMG - CORBA (Object Management Group - Common Request Broker Architecture). Konkurentem tych standardów jest DCOM (Distributed Component Object Model) firmy Microsoft.
Na poziomie techniki programowania programy użytkowe powinny spełniać wymagania stawiane przez tzw.przemysłowe standardy (industry standards) API (Application Programs Interface), które m.i. definiują standardowe formaty danych, mechanizmy eksportu i importu danych, umożliwiając tym samym łączność z dowolnymi aplikacjami.

Uzależnienie od dostawcy wynikać może też z niemodyfikowalności systemu przez uzytkowników (w zakresie parametryzacji, raportowania , struktur danych itp.). Powoduje to, iż w warunkach zmiennych wymagań środowiska bankowego wzrastają znacznie nakłady na utrzymywanie systemu gdyż odbywa się to prawie wyłącznie poprzez dodatkowe zlecenia dla autorów systemu. Terminowość realizacji tych zleceń będzie daleka od ideału w przypadkach, gdy -przy ograniczonej “mocy przerobowej” - konserwują oni systemy w wielu bankach.

Czasem technologia przetwarzania jest “zbyt mocno” związana z konfiguracją sprzętową, gdy na przykład zaklada wczytywanie całej bazy danych do pamięci operacyjnej. Wtedy okazuje się, że system obsługujący sprawnie bank z kilkoma tysiącami klientów (np. specjalizujący się w bankowości komercyjnej, czyli ukierunkowany na przedsiębiorstwa) staje się niewydolny na danej platformie dla banków detalicznych , mimo

iż posiada obsługę funkcjonalną odpowiednich produktów bankowych.

Tak więc należy stwierdzić, iż w pełni otwarty system bankowy zapewnic powinien nabywcy niezależność od dostawcy sprzętu i autora oprogramowania oraz umożliwić rozwijanie systemu zarówno w od strony technicznej jak i aplikacyjnej.

10. Ryzyko największe: *brak strategii komputeryzacji* *(grzech główny)*

Brak odpowiednich decyzji komputeryzacji banku jest ryzykiem największym, gdyż pozbawia bank bardzo istotnego narzędzia usprawniania zarządzania i obsługi klienta , zmniejszając szanse przetrwania na wymagającym rynku bankowym. Ryzyko tkwi jednak **nie w tym czy** komputeryzować **ale jak** komputeryzować. *Grzechem jest więc brak strategii komputeryzacji czyli komputeryzacja "jak leci" poprzez nagromadzenie masy komputerów osobistych (najlepiej aby na każdym biurku "stał" komputer co będzie świadczyć o "nowoczesności" firmy) oraz wielu "najróżniejszych" programów w sumie nie stanowiących logicznej i technologicznej całości.*
Nie można budować systemu idąc na pozorną łatwiznę, czyli "sklejanie systemu" z pakietów pochodzących od różnych autorów. Mimo iż " małe jest piękne" to "duże będące ich sumą " może okazać się tworem pokracznym, nie spełniającym oczekiwań. Nakłady na ich integrację poprzez wspólne bazy danych (o ile będzie to możliwe) mogą byc wyższe od opłat licencyjnych za system kompleksowy, zaś to co otrzymamy będzie gorszej jakości (np.obniżenie wydajności przetwarzania wskutek pośrednictwa mechanizmów eksportu-importu danych). Nie oznacza to, że pakiety zewnętrzne w ogóle nie wchodzą w grę. Akceptować można niewielką ilość pakietów specjalizowanych, opartych na standardach międzynarodowych i przeznaczonych do realizacji wybranych funkcji bankowych, np.uzgodnień rachunków NOSTRO, potwierdzeń transakcji (confirmation matching) , obsługi akredytyw. Rdzeń (jądro) systemu musi pozostać produktem jednolitym, narzucającym nowoczesną architekturę systemu.

Brak właściwych decyzji wynikać może nie tylko z braku środków finansowych (na rynku bankowym istnieje wiele propozycji o bardzo zróżnicowanych cenach), lecz również wskutek tradycyjnie silnie zakorzenionego oporu przeciwko zmianom. Opór ten występuje w banku na wszystkich szczeblach. W naczelnym kierownictwie jest to opór przeciwko zmianom organizacyjnym oraz zmianie stylu pracy (niechęć uzywania nowych narzędzi w procesach decyzyjnych). W kierownictwie operacyjnym opór przejawia się poprzez wykazywanie zajętości uniemożliwiającej szkolenie w zakresie nowego systemu, bojaźn przed zmianami kadrowymi (zastąpienie przez młodszych i bardziej zaznajomionych z techniką komputerową), obawa niemożnosci kontroli i oceny personelu w nowych warunkach, irytacja wobec "zbyt szybkich" zmian organizacyjnych, itp. Personel wykonawczy wykazuje instynkt samozachowawczy w postaci bojaźni przed zwolnieniem z pracy i utratą dotychczasowych kwalifikacji oraz wobec nowej techniki ("czy poradzę sobie ?").
Skutki oporu są rozmaite. Przede wszystkim jest to odwlekanie decyzji (czasem do przysłowiowej emerytury) i tendencja do akcentowania ewentualnych wad przyszłego systemu przy równoczesnym pomijaniu zalet

Zygmunt Ryznar