Problematyka zapewnienia ciągłości działania w bankach spółdzielczych

Część 1: Zagrożenia

Ekspert: Krzysztof Maderak

Problematyka zapewnienia ciągłości działalności biznesowej organizacji nabrała w początku XXI wieku szczególnego znaczenia.

Uzależnienie od technologii, dostawców zewnętrznych, outsourcingu oraz wzrastające zagrożenie terrorystyczne i społeczne generują zwiększone ryzyko utraty możliwości prowadzenie działalności w obecnych warunkach otoczenia biznesowego.

Powszechność i złożoność zastosowania technologii informatycznej w działalności bankowej powoduje, że IT staje się centralnym sposobem komunikacji z klientami, zaś zależność od innych firm w ramach „wirtualnej gospodarki" wprowadza nowe wyzwanie w wypełnianiu zobowiązań.

Problemy z wydajnością systemów IT, awarie kluczowych aplikacji lub chociażby tylko niektórych składników elementów procesów biznesowych są natychmiast zauważane przez klientów, bank natomiast często nie ma możliwości natychmiastowej reakcji na degradację wydajności lub kompletną awarię w infrastrukturze partnerów. Problemy te dotyczą również banków spółdzielczych, które często działają na terenie charakteryzującym się słabą infrastrukturą techniczną, szczególnie w zakresie telekomunikacji szerokopasmowej.

Zakłócenia funkcjonowania organizacji związane są z zagrożeniami, które stanowią integralny składnik otaczającej nas rzeczywistości. Zagrożenia mogą być wynikiem zarówno działania sił przyrody, jak i oddziaływania człowieka na otoczenie. Z punktu widzenia zapewnienia ciągłości biznesowej kluczowe znaczenie ma oddziaływanie człowieka na środowisko naturalne oraz otoczenie technologiczne, ekonomiczne i społeczne.

Zdarzenia stanowiące zagrożenie dla ciągłości działania będące wynikiem oddziaływania człowieka mają swoje źródła w środowisku biznesowym, technicznym i społecznym. W środowiskach tych do zarządzania zagrożeniami stosuje się odpowiednio Business Continuity Management – BCM, teorię niezawodności i teorię zarządzania kryzysowego.

Zagrożenie ma postać i cechy mierzalne i charakterystyczne dla siebie. Ma swoje źródło i przyczyny powstania. Ogół przyszłych zagrożeń charakteryzują cztery rodzaje niepewności. Niepewność co do:

1. faktu wystąpienia zagrożenia;
2. momentu wystąpienia zagrożenia;
3. miejsca realizacji zagrożenia;
4. skutków materializacji zagrożenia.

Zagrożenia można podzielić – ze względu na poziom ich losowości – na trzy kategorie:

1. Zamierzone, czyli związane z działaniami wykonywanymi z premedytacją,
2. Losowe wewnętrzne, do których można zaliczać: niezamierzone błędy ludzkie, defekty sprzętu i oprogramowania, zniekształcenia lub zagubienie informacji na skutek błędów w dokumentacji,
3. Losowe zewnętrzne, do których należą między innymi negatywne oddziaływania środowiska naturalnego, wypadki, katastrofy itp.

Podobnie na trzy kategorie można podzielić zagrożenia ze względu na czynnik sprawczy. Pierwotnym źródłem zagrożeń mogą być czynniki środowiskowe – siły przyrody, czynniki społeczne i czynniki techniczne. Poniższa tabela przedstawia wybrane, kluczowe zagrożenia funkcjonowania organizacji ze względu na czynnik sprawczy.

Siły przyrody	Techniczne	Społeczne
Trzęsienie ziemi	Pożar	Wybuch bomby
Powódź	Katastrofa budowlana	Alarm bombowy
Huragan	Awaria zasilania	Terroryzm
Oblodzenia	Awaria wodociągowa	Sabotaż
Piorun	Awaria kluczowego sprzętu	Wandalizm
Gradobicie	Usterka programowa	Przestępstwo
Zamieć śnieżna	Awaria łączności	Hacking/cracking
Insekty	Awaria klimatyzacji	Kradzież
Szczury	Awaria sieci LAN/WAN	Strajk
	Awaria systemu backupu	Epidemia
	Przypadkowe włączenie systemu gaśniczego	Błąd człowieka

Powyższe czynniki powodujące zaburzenia w funkcjonowaniu firmy nie wyczerpują listy możliwych zagrożeń. Zagrożenia te są pochodną egzogenicznych i endogenicznych zmian w otoczeniu środowiskowym, technicznym i społecznym i podlegają szybkim zmianom.

Nikt nie ma bezpośredniej kontroli nad zagrożeniami i niewiele więcej można zrobić w związku z nimi samymi niż spróbować je zrozumieć. Można jedynie wdrożyć zabezpieczenia i systemy monitorowania tak, aby chronić się nimi.

Znaczenie biznesowych, a w konsekwencji również społecznych skutków materializacji zagrożeń mających wpływ na funkcjonowanie instytucji finansowych dość długo nie znajdowało odbicia w aktach normatywnych czy rekomendacjach nadzorów krajowych i organizacji międzynarodowych. Dopiero dwadzieścia lat temu, w 1987 roku, brytyjski Banking Act nałożył na tamtejsze banki obowiązek posiadania aktualnych planów ciągłości działania. Później działania te kontynuowała Financial Services Agency i rozciągnęła powyższe wymagania na wszystkie firmy brytyjskie z sektora finansowego.

Kiedy w 1993 roku podłożono bombę pod World Trade Center w Nowym Jorku, prawie 50 proc. przedsiębiorstw, które miały tam swoją siedzibę zbankrutowało. Można przypuszczać, że duża cześć

tych upadłości spowodowana była nieistnieniem scenariuszy działań, które mogłyby sprostać takiej sytuacji.

Najbardziej spektakularnym dowodem na konieczność holistycznego planowania awaryjnego w celu zapewnienia ciągłości działania oraz odtwarzania po katastrofie był atak terrorystyczny na Word Trade Center z 11 września 2001 roku. Na podkreślenie zasługuje fakt, że poza utratą majątku trwałego firm mieszczących się w budynkach, danych o operacjach bieżących i części danych archiwalnych, w wyniku ataku terrorystycznego przedsiębiorstwa utraciły znaczną część kluczowych pracowników, których zastąpienie nie było możliwe w krótkim i średnioterminowym horyzoncie czasowym.

Wielu amerykańskich specjalistów ds. bezpieczeństwa i ciągłości działania analizowało zachowania firm, które utraciły przejściowo lub całkowicie zdolność prowadzenia działalności w wyniku ataku terrorystycznego z 11 września 2001 roku, pod kątem przydatność planów odtwarzania po katastrofie. We wnioskach, które opracowano, zwracano uwagę na kilka kluczowych problemów. Duża część planów awaryjnych nie przewidywała tak szerokiego zakresu katastrofy, obejmując swoim zasięgiem tylko zniszczenie jednej z wież WTC. Wiele firm podkreślało, że ich plany awaryjne były o wiele zbyt szczegółowe, ale nie tak skuteczne, jak tego oczekiwano.

Problematyczne okazały się również plany awaryjne przygotowywane przez specjalistów zewnętrznych, którzy nie byli związani bezpośrednio z organizacją. Rozwiązania proste, przygotowane przez własnych specjalistów okazały się skuteczniejsze niż rozbudowane plany, charakteryzujące się długim i skomplikowanym procesem aktualizacji. Wskazano, że decydującymi czynnikami sukcesu w zapewnieniu ciągłości działania było właściwe określenie szczegółowości planów awaryjnych, zapoznanie z nimi wyższego i średniego kierownictwa, a także regularne testowanie. Podkreślono ponadto, że procedury zachowania ciągłości działania powinny obejmować także ryzyko kadrowe. Firma powinna dążyć do takiego ukształtowania swojej struktury organizacyjnej i planów szkoleniowych, aby możliwa była czasowa kumulacja zadań na wszystkich stanowiska pracy. Kumulacja taka musi jednakże uwzględniać wymogi prawne, np. Prawa bankowego, dotyczące rozdziału obowiązków, kontroli wewnętrznej itp.

Strategiczną podstawą planowania awaryjnego jest konieczność zapewnienia wysokiej dostępności dla systemów obsługujących kluczowe procesy biznesowe w organizacji.

Wysoka dostępność jest zdolnością systemu do zabezpieczaniu go przez drobnymi przestojami i odtwarzania w krótkim czasie w dużej mierze w zautomatyzowany sposób.

Dostępność usług w trybie 24/7 jest aktualnie kluczowym elementem funkcjonowania nowoczesnego banku na rynku usług finansowych. Szczególnie w obecnej chwili, kiedy relacje pomiędzy klientami i bankiem wykorzystują kanały telekomunikacyjne, call centres, pocztę elektroniczną i internet, a kanały te zastępują tradycyjne formy obsługi bezpośredniej. Znaczenie tych kanałów komunikacji dla kontaktu z klientem i poziomu jakości usług będzie rosło w kolejnych latach przede wszystkim ze względu na ich łatwość dostępu i wysoką efektywność. Rosnące zagrożenia i niespecyficzne ryzyka powodują, że organizacje finansowe są jeszcze bardziej zależne od złożonej techniki i wraz ze wzrostem znaczenia internetu dla realizacji transakcji klienta i kontaktu z nim, stają się coraz bardziej nietolerancyjne na przestój.

Instytucje finansowe i ubezpieczeniowe są z punktu widzenia wykorzystania informacji podmiotami szczególnymi. Z jednej strony informacja i przetwarzające ją systemy są dla nich aktywami o żywotnym znaczeniu, z drugiej skala wykorzystywania technologii IT, w tym zaawansowanych środków technicznych i procedur bezpieczeństwa, jest tu największa, co determinuje wysoce restrykcyjne podejście do bezpieczeństwa informacji i zapewnienia ciągłego dostępu do niej.

Określenie kosztów czasu przestoju jest decydujące dla oszacowania nakładów niezbędnych do wdrożenia procedur odtwarzania po katastrofie. Kalkulacja kosztów związanych z utratą krytycznych funkcji jest procesem złożonym, obejmującym zarówno koszty wymierne, takie jak utracona wydajność, utracone dochody, koszty sądowe, kary za opóźnienia i inne opłaty, oraz koszty niematerialne, jak reputacja, utracone przychody, strata pracowników.

Ze względu na scentralizowaną strukturę banków zagrożeniem mającym decydujący wpływ na czas przestoju jest awaria w obrębie łączności korporacyjnej jak i połączeń z systemami rozliczeń międzybankowych czy sieci bankomatowej.

Racjonalne podejście do problematyki zapewnienia ciągłości działania wymaga wdrożenia w instytucji finansowej strategii i procedur postępowania w sytuacjach kryzysowych.

Business continuity management jest procesem przewidywania incydentów, które mogą dotyczyć krytycznych dla organizacji funkcji i procesów i upewniania się, że organizacja reaguje na jakikolwiek incydent w planowany i przygotowany sposób.

Wszystkie procesy biznesowe, nie tylko IT, muszą być antycypowane, adaptowane i odporne w obliczu pojawiających się problemów. Dlatego business continuity management jest nie tylko celem, ale staje się narzędziem, które skupia się na procesach biznesowych i ich stałym ulepszaniu. □

Zagadnienia związane z zarządzaniem ciągłością działania są określone w międzynarodowych i krajowych normach, standardach i metodykach, takich jak:

NFPA 1600 - standard został wprowadzony przez National Fire Protection Association[1] i dotyczy zarządzania kryzysowego oraz programów ciągłości biznesu. W standardzie przedstawiono szereg wymagań pozwalających na przygotowanie się, właściwą reakcję i przywrócenie działalności po katastrofie wywołanej przez człowieka, technologię lub czynniki naturalne. Standard przedstawia ustandaryzowane podstawy do planowania zarządzania kryzysowego i budowania programów ciągłości działania biznesu zarówno w sektorze prywatnym, jak i publicznym, dzięki wspólnym elementom, technikom i procesom. Został zatwierdzony jako American National Standard w 2004 roku.

BS 25999 – seria standardów opracowana przez British Standards Institute[2] i dotyczy obszaru zarządzania ciągłością działania. Standard zastąpił specyfikację PAS-56, która została jednocześnie wycofana. Seria BS 25999 składa się z dwóch standardów. Pierwszy – BS 25999-1:2006 jest zbiorem wytycznych, które wprowadzają procesy, zasady i terminologię. Drugi – BS 25999-2 jest standardem, w oparciu o który może być przyznany certyfikat zgodności. Określa on wymagania do wdrożenia środków kontroli ciągłości działania. Standard wprowadza systemowe podejście do zarządzania ciągłością działania w oparciu o dobre praktyki, może być wykorzystywany przez organizacje każdej wielkości w sektorach przemysłowym, handlowym, publicznym i non profit.

ISO/IEC 27001:2005[3] - międzynarodowa norma ISO 27001 określa wymagania związane z ustanowieniem, wdrożeniem, eksploatacją, monitorowaniem, przeglądem, utrzymaniem i doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji – SZBI. PKN opracował polskie tłumaczenie tej normy – PN-ISO/IEC 27001:2007. Norma ISO 27001 oparta jest na podejściu procesowym i wykorzystuje model Planuj – Wykonuj – Sprawdzaj – Działaj (PDCA, tj. Plan – Do – Check - Act), który jest stosowany dla całej struktury procesów SZBI.

Norma składa się z części podstawowej oraz załączników. Część podstawowa normy definiuje wymagania związane z ustanowieniem i zarządzaniem SZBI, wymaganą dokumentacją, odpowiedzialnością kierownictwa, wewnętrznymi audytami SZBI, przeglądami SZBI oraz ciągłym doskonaleniem SZBI. Wszystkie wymagania zdefiniowane w części podstawowej powinny być spełnione. Podstawą ustanowienia oraz utrzymania SZBI jest określenie metody oraz przeprowadzenie analizy ryzyka.

[1] więcej http://www.nfpa.org/assets/files/pdf/nfpa1600.pdf
[2] więcej http://www.bsi-global.com
[3] więcej http://www.iso.org, www.pkn.pl