Piotr ZASKÓRSKI

INFORMACYJNO-BIZNESOWA CIĄGŁOŚĆ DZIAŁANIA FIRMY

Streszczenie

W artykule prezentowane są problemy zapewniania biznesowej ciągłości działania organizacji ze szczególnym uwzględnieniem uwarunkowań informacyjnych. Identyfikacja ciągłości działania związana jest z analizą ryzyka i kryteriami jego oceny w aspekcie integralności, dostępności i spójności danych. Te czynniki mają bezpośredni wpływ na poziom bezpieczeństwa informacyjnego. Główne aspekty zapewniania informacyjnej ciągłości działania zawierają się w procedurach biznesowej, całościowej ciągłości działania organizacji. Cały artykuł eksponuje problem bezpieczeństwa organizacji.

Abstract

The article presents assumptions for modeling of organization contingency, emphasizing threats for its critical infrastructure. Identification rules and criteria for risk assessment in the aspect of accessibility, confidentiality and integrity of information resources including rules for defining strategic organization resources, which influence its contingency and performance in a threat or damage state has been defined. Main aspects of organization procedures creation, which are integral part of contingency plan has been presented. Whole article has been summarized by a debate of system approach to organization security.

1. WPROWADZENIE

Współczesne uwarunkowania biznesowe stają się coraz bardziej wymagające i niestabilne. W związku z tym coraz większego znaczenia nabiera problem zapewniania ciągłości działania. Biorąc pod uwagę czynnik czasu, obserwuje się przechodzenie od zarządzania wg modelu *ex-post* do modelu *ex-ante*, ukierunkowanego głównie na organizację wielopodmiotowo realizowanych procesów. Ma to na celu przede wszystkim podnoszenie wartości każdej organizacji przy ograniczonym dostępie do różnych zasobów. Zjawisko to nierozerwalnie łączy się z koniecznością prowadzenia właściwej gospodarki informacyjnej. Determinowane jest zwłaszcza przez wewnętrzne relacje i dynamiczne powiązania w strukturach organizacyjnych

(sieciowych, wirtualnych i procesowych). Ważnym problemem staje się tutaj bezpieczeństwo zasobów (w tym informacyjnych) [1] zwłaszcza w kontekście przepływu danych[2] pomiędzy poszczególnymi uczestnikami procesów biznesowych.

Zasoby informacyjne uzyskują status zasobów strategicznych a w określonych sytuacjach kryzysowych – zasobów krytycznych i pojawia się zjawisko asymetrii informacyjnej, która często jest konsekwencją celowej działalności podmiotów gospodarczych. Asymetria informacyjna zawiera w sobie zarówno pozytywną jak i negatywną wartość. Pozytywna wartość polega na świadomym udostępnianiu swoich zasobów innym podmiotom na zasadzie zaufania lub współdziałania w realizacji wybranego przedsięwzięcia, dostosowując jej zakres do faktycznych potrzeb. Stąd też wielkość udostępnianych zasobów oraz ich szczegółowość nie musi być prostym odbiciem symetrycznie pozyskiwanych z otoczenia informacji. Asymetria informacyjna ma również wartość negatywną, rozumianą jako celowe zawężanie lub zniekształcanie albo udostępnianie w sposób słabiej eksponowany – informacji istotnej dla odbiorcy. Może to mieć miejsce nie tylko w systemach biznesowych, ale i w innych obszarach działań człowieka.

2. ISTOTA CIĄGŁOŚCI DZIAŁANIA ORGANIZACJI

Organizacja biznesowa jest podmiotem działania, który ma zdefiniowaną misję i realizuje określone cele oraz zadania w warunkach wyznaczonych przez otoczenie. Każdy rodzaj organizacji posiada określoną strukturę, która warunkuje sposób osiągania zamierzonego celu[3]. Sposób i poziom realizacji celu jest determinowany zachowaniem odpowiednich procedur bezpieczeństwa, a w tym ciągłości działania. Wyznaczony program i metody osiągania zamierzonego celu oraz potencjał organizacji, w tym dostępność do właściwych informacji – określają sprawność i skuteczność działań biznesowych. Podnoszenie bezpieczeństwa organizacji może następować przez wdrażanie struktur procesowych, których funkcjonowanie uwarunkowane jest dostępem on-line do odpowiednich zasobów informacyjnych zwykle w architekturze sieciowej. Procesy stają się obiektem organizacyjnym, a proces gromadzenia i przetwarzania danych zyskuje status procesu strategicznego w organizacji. Bezpieczeństwo informacyjne jest więc składową bezpieczeństwa całej organizacji i dotyczy wszystkich obszarów jej działalności podstawowej a infrastruktura krytyczna organizacji wiąże się

[1] Pod pojęciem bezpieczeństwo zasobów informacyjnych należy rozumieć przede wszystkim ochronę podstawowych atrybutów danych: integralności, dostępności i poufności.

[2] Pojęć: dane, informacja, wiedza, mądrość nie należy traktować jako synonimy. Według założeń modelu Wirth'a są to kolejne poziomy paradygmatu wiedzy w organizacji.

[3] Bieniok H. i inni: *Metody sprawnego zarządzania,* Placet, Warszawa 1999 r.

z zapewnieniem możliwości wypełniania przez nią funkcji podstawowych w różnych stanach zagrożeń i kryzysów na odpowiednim poziome[4].

Zintegrowane Systemy Informatyczne scalają szerokie spektrum zasobów informacyjnych w skali całej organizacji przy założeniu zapewniania poufności, integralności i dostępności zasobów informacyjnych dla uprawnionych użytkowników,[5.] Są to zarazem podstawowe kryteria ciągłości informacyjnej, szczególnie w warunkach asymetrii informacyjnej. Założenia te prowadzą również do zapewnienia szeroko pojętej zgodności[6] (ang. *compliance*) i wtedy różne kategorie danych podlegających unormowaniom prawnym (np. dane osobowe) wymagają silnych mechanizmów ochrony i bezpieczeństwa, co warunkuje ciągłość działań biznesowych. Szczególnego znaczenia nabierają zagrożenia dla infrastruktury krytycznej, przez którą rozumie się systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty determinujące sprawne działanie tej organizacji i wypełnianie przez nią statutowych funkcji w obszarze działalności podstawowej. Dotyczy to również dostępu do odpowiednich zasobów informacyjnych własnych i podmiotów kooperujących.

Ochrona infrastruktury krytycznej jest zespołem przedsięwzięć często związanych z szybkim odtworzeniem jej stanu poprzedniego na wypadek zagrożeń, awarii, ataków oraz innych zdarzeń zakłócających jej skuteczne funkcjonowanie[7]. Bezpieczeństwo infrastruktury krytycznej jest jedną z głównych składowych bezpieczeństwa organizacji i może oznaczać stopień uzasadnionego zaufania, że nie zostaną poniesione potencjalne straty w obszarze jej znaczących elementów. Stąd też ważne staje się określenie wymagań dla systemu bezpieczeństwa ze szczególnym uwzględnieniem założeń związanych z modelowaniem, projektowaniem i wdrażaniem systemów zapewniających ciągłość procesów informacyjnych w wybranych systemach działania.

Nieodłączną cechą systemową związaną z każdym działaniem jest ryzyko, które stanowi zwykle miarę start ponoszonych przez organizację w przypadku zaistnienia zagrożeń szczególnie dla jej ciągłości działania. Częstość wystąpienia zagrożenia

---

[4] Procesy strategiczne, które są związane z planowaniem i ustalaniem celów strategicznych oraz raportowaniem zarządczym (wspierane przez rozwiązania klasy MIS (ang. Management Information Systems), BW (ang. Business Warehouse), czy DSS (ang. Decision Support Systems);
Główne procesy operacyjne (wspierane przez zintegrowane systemy informatyczne typu ERP II (Enterprise Resuorces Planning) w zakresie logistyki, dystrybucji, kadr, finansów i tp.).

[5] *Strategies for Meeting*, New Internal Control Reporting Challenges: A White Paper—The Sarbanes-Oxley Act of 2002. New York, NY: PricewaterhouseCoopers, 2002

[6] Debreceny R., Gray G., Jun-Jin Ng J., Siow-Ping Lee K., Woon-Foong Yau, *Embedded Audit Modules in Enterprise Resource Planning Systems: Implementation and Functionality*, Journal of Information Systems, vol. 19, No.2, 2005, s. 7-27

[7] Kośla R., *Ochrona infrastruktury krytycznej w Polsce – aktualny stan prac*. Referat z konferencji SECURE 2002. Warszawa.

i jego charakter są zaledwie miarą statystyczną danego zjawiska. Połączenie częstości zagrożenia i jego skutków daje obraz poziomu ryzyka. W ocenie ryzyka przyjmuje się zagrożenia zewnętrzne związane z celowym, szkodliwym działaniem lub też będącego skutkiem wynikającym z działania sił natury. Ważnym zagrożeniem dla organizacji może być tzw. wymuszona asymetria informacyjna. Wtedy skutki ryzyka mają charakter negatywny i mierzone są wielkością strat.

$$RY = P \times S \times \mathrm{B} \times \mathrm{E} \tag{1}$$

gdzie:

RY – ryzyko

P – poziom częstości występowania zagrożenia

S – poziom/wartość strat

B – podatność na zagrożenie/poziom bezpieczeństwa

E – współczynnik ekspozycji zagrożenia

Splot różnych zdarzeń i ich skutków może prowadzić do eksponowania niektórych realizacji, co może oznaczać, że wybrana częstość wystąpienia pewnego typu zdarzeń i jego skutków może być dla organizacji szczególnie ważna (wzór 1). Można więc stwierdzić, że bezpieczeństwo organizacji jest dopełnieniem uogólnionego (unormowanego) poziomu ryzyka. Bezpieczeństwo organizacji i jej ciągłość działania może oznaczać stopień uzasadnionego (np. analizą ryzyka i przyjętymi metodami postępowania z ryzykiem) zaufania, że nie zostaną poniesione potencjalne straty. Ochronę infrastruktury krytycznej – również w wymiarze zasobów informacyjnych – należy interpretować jako proces składający się z przedsięwzięć organizacyjnych i technologicznych realizowanych w celu szybkiego odtworzenia możliwości działania na wypadek zagrożeń.

Funkcjonowanie współczesnych, zaawansowanych technologicznie organizacji, będących często strukturami procesowymi (płaskimi, sieciowymi, sieciocentrycznymi, wirtualnymi), uzależnione jest w dużym stopniu od informacji przetwarzanej, przechowywanej i przesyłanej w systemach teleinformatycznych. Sfałszowanie informacji lub destrukcja procesu przetwarzania – powodują straty, które mogą osiągnąć poziom nieodtwarzalny. Poziom ciągłości informacyjnej może być więc determinowany stopniem uzasadnionego (np. analizą ryzyka i przyjętymi metodami postępowania z ryzykiem) zaufania, że nie zostaną poniesione potencjalne straty wynikające z niepożądanego (przypadkowego lub świadomego) działania na szkodę organizacji w zakresie ujawnienia, modyfikacji, zniszczenia lub uniemożliwienia przetwarzania informacji przechowywanej, przetwarzanej i przesyłanej w określonym systemie obiegu informacji. Jak wynika z zapisów ustawy o zarządzaniu kryzysowym (art.3. pkt.2) w skład systemów infrastruktury

krytycznej[8] wchodzą systemy łączności i sieci teleinformatyczne na równi z systemami energetycznymi, komunikacyjnymi i logistycznymi. Stąd też te same zagrożenia mogą powodować różne straty w zależności od typu obiektu i powstaje wówczas możliwość oceny poziomu ciągłości informacyjno-biznesowej. Wszystkie zagrożenia skierowane przeciwko systemom sterowania i nadzoru infrastruktury oraz bazom danych związanych z eksploatacją infrastruktury krytycznej prowadzić mogą do utraty ciągłości działania.

W infrastrukturze krytycznej można wyróżnić elementy konstrukcyjne oraz nadzorczo-sterujące, warunkujące właściwe zarządzanie i sterowanie procesami wykonawczymi. Wprowadza się więc pojęcie bezpieczeństwa elementów konstrukcyjnych oraz bezpieczeństwa związanego z eksploatacją systemów nadzorczo-sterujących. W szczególności do zagrożeń dla samych systemów informatycznych (komputerowych) można zaliczyć umieszczanie złośliwego oprogramowania, fizyczne niszczenie elementów technicznych a także zakłócanie działania i zniekształcanie danych, czyli tzw. wymuszoną asymetrię informacyjną. Techniczne, organizacyjne oraz programowe środki ochrony stanowią faktyczny obraz poziomu bezpieczeństwa zasobów informacyjnych organizacji. Każdy typ organizacji koncentruje się na wypełnianiu swej funkcji statutowej w różnych uwarunkowaniach zewnętrznych i wewnętrznych. Stąd też ważna jest systemowa identyfikacja i ewaluacja zagrożeń oraz szacowanie poziomu ryzyka dla skutecznego przeciwdziałania wymuszonej asymetrii informacyjnej.

Ochrona zasobów informacyjnych organizacji przez wykorzystanie świadomie sterowanej asymetrii informacyjnej wiąże się z zapewnianiem poufności, integralności i dostępności informacji przetwarzanej w systemach teleinformatycznych (w tym w systemach nadzorczo-sterujących), co może wzmacniać ciągłość biznesową.

3. UWARUNKOWANIA CIĄGŁOŚCI BIZNESOWO-INFORMACYJNEJ

Wielostronnie korzystne działania z wyliczeniem wzrostu wartości dodanej własnych działań (w tym wspólnych transakcji) przez wykorzystanie zjawiska synergii – tworzą tzw. łańcuch wartości dodanej. Asymetria informacyjna może przerwać ciągłość działania organizacji o gorszym dostępie do wybranych, niezbędnych do działania zasobów informacyjnych. Może to być ważne źródło ryzyka prowadzące

[8] Różne systemy wchodzące w skład infrastruktury krytycznej (transportu, komunikacji, magazynowe, produkcji) podlegają stałemu nadzorowi (sterowaniu lub wręcz realizacji) za pomocą tzw. sieci przemysłowych (ang. Industrial Control System – ICS), na które składają się sieci SCADA, DCS (ang. Distributed Control Systems) oraz ich elementy składowe w postaci sterowników programowalnych PLC (ang. Programmable Logic Controllers). Oznacza to, że należy uwzględniać zagrożenia, które polegają na uszkadzaniu elementów poszczególnych systemów.

do strat wymiernych i niewymiernych organizacji o gorszym dostępie do informacji. Negatywne skutki asymetrii informacyjnej nie są możliwe do całkowitego wyeliminowania. Zawsze będą funkcjonować podmioty świadomie kreujące zjawisko asymetrii informacyjnej, bazującej na lepszym dostępie do informacji.

Asymetria informacyjna może być często ukrywana przez organizację o lepszym dostępie do informacji. Dotyczyć to może ukrywania informacji niekorzystnych dla funkcjonowania całych organizacji i pojedynczych kontrahentów. Powstaje wówczas zjawisko przerzucania ryzyka na stronę współdziałającą lub ograniczanie poziomu ryzyka własnego metodą jego kompensowania przez inny podmiot o statusie całego systemu działania lub podmiotu fizycznego. Asymetria informacyjna może być ukrywana przez organizację również o gorszym dostępie do informacji. Celem może być uczestnictwo w priorytetowym procesie (w tym dokonanie korzystnej transakcji). Po dokonaniu tej transakcji organizacja o gorszym dostępie do informacji może rozpocząć niwelowanie asymetrii informacyjnej i świadome podnoszenie swej pozycji rynkowej. Ukrywanie informacji, zniekształcanie lub podawanie błędnych informacji oraz jej uzewnętrznianie w sposób ukrywający jej wartość (tzw. „przemycanie", aby odbiorca nie zwrócił na to uwagi) może mieć na celu nie tylko realizację celów cząstkowych ale również celów strategicznych. Asymetrię informacyjną można widzieć nie tylko w kontekście jakości i dostępności infrastruktury teleinformatycznej, ale również w kontekście formy i treści informacji, co może determinować szybkość i zakres dostępu do pożądanych zasobów informacyjnych.

Asymetria informacyjna o wartości pozytywnej polega przede wszystkim na identyfikacji i wydzieleniu względnie autonomicznych grup użytkowników zasobów informacyjnych oraz kontrolowaniu ich przepływów – zarówno w ramach określonej struktury (hierarchicznej, procesowej) jak i w relacjach z otoczeniem zewnętrznym. Tym samym powinno nastąpić kompleksowe zdefiniowanie dostępu do grup zasobów na odpowiednim poziomie repozytoriów danych w całej organizacji. Asymetria jest zatem ściśle powiązana z prawami dostępu poszczególnych klas końcowych użytkowników zasobów informacyjnych. Złożoność struktury organizacyjnej sprzyja wzrostowi poziomu asymetrii, co utrudnia zarządzanie dostępem do danych. Warto zauważyć w tym miejscu, że struktury płaskie (w tym organizacje procesowe) charakteryzują się niższym wskaźnikiem asymetrii niż struktury hierarchiczne. Zjawisko asymetrii informacyjnej postrzegane jest dość powszechnie, na co wskazują nawet lokalne badania ankietowe[9]. Warto jednak zauważyć, że zdaniem większości respondentów najczęściej występującym kryterium warunkującym

[9] J. Woźniak, WAT 2010, badania ankietowe: (zdaniem 68% respondentów w ich organizacjach występuje zjawisko asymetrii informacyjnej, a tylko w opinii 25% badanych – nie dostrzegany jest taki problem). Trudno jednak powiedzieć, jak wartościują to zjawisko.

asymetrię informacyjną w różnych organizacjach/przedsiębiorstwach jest kryterium wynikające z kompetencji opisanych na strukturze organizacyjnej. Wartościowanie poziomu asymetrii uwzględnia więc pozytywny aspekt selekcji informacji.

Asymetria informacyjna ma istotne znaczenie w procesie zarządzania bezpieczeństwem zasobów informacyjnych w organizacjach procesowych z uwzględnieniem zarówno korzyści, jak i potencjalnych zagrożeń. Podstawowym wyznacznikiem funkcjonowania struktur procesowych jest integracja projektowania, wdrażania i realizacji określonych kategorii procesów[10]. Na tej podstawie można stwierdzić, że struktury procesowe noszą znamiona organizacji uczących się, nastawionych na właściwe i sprawne zarządzanie informacja i wiedzą (rys.1.). W związku z tym kluczowe znaczenie odgrywa system ochrony określonych kategorii procesów i danych jako determinantów pozycji rynkowej organizacji wkomponowanej w łańcuch wartości dodanej[11]. Jednak zestawiając tego typu działania z polityką bezpieczeństwa danych w przedsiębiorstwie, szczególnego znaczenia nabiera określenie jednocześnie najefektywniejszego i maksymalnie ograniczonego dostępu do informacji przy zachowaniu świadomie sterowanej asymetrii informacyjnej. Każdy uczestnik procesu może w pewnym zakresie kontrolować przepływ danych w trakcie realizacji procesu i wykrywać „nieszczelności" zabezpieczeń systemów teleinformatycznych[12]. Relacje wewnątrz-strukturalne opierają się w znacznej mierze na Internecie i Intranecie. Podstawowymi klasami zagrożeń dla ciągłości działań biznesowych mogą być wówczas awarie systemu, złośliwe oprogramowania, błąd ludzki i inne[13].

Coraz większego znaczenia w zabezpieczeniu ciągłości działalności biznesowej nabierają zintegrowane systemy informatyczne zarządzania[14], a w tym zarówno systemy analitycznego przetwarzania danych (OLAP, czyli On-Line Analyzing Processes)) i przetwarzania transakcyjnego (OLTP, czyli On-Line Transaction Processing). W tym środowisku są przechowywane, systematyzowane i analizowane dane o znaczeniu strategicznym dla wielu podmiotów działania, partycypujących w realizacji różnych, rozproszonych procesów (rys. 1). Tym samym zabezpieczenie

[10] Przykładowo, proces produkcji samochodu jest z zasady procesem wielopodmiotowym jako logicznie powiązany łańcuch kooperantów w wymiarze czasu i efektu. Stąd też wizja M. Hammera i J. Champy'ego, że „…w firmie ukierunkowanej na proces to proces, a nie funkcje czy geografia, będzie stanowił podstawę struktury organizacyjnej…"

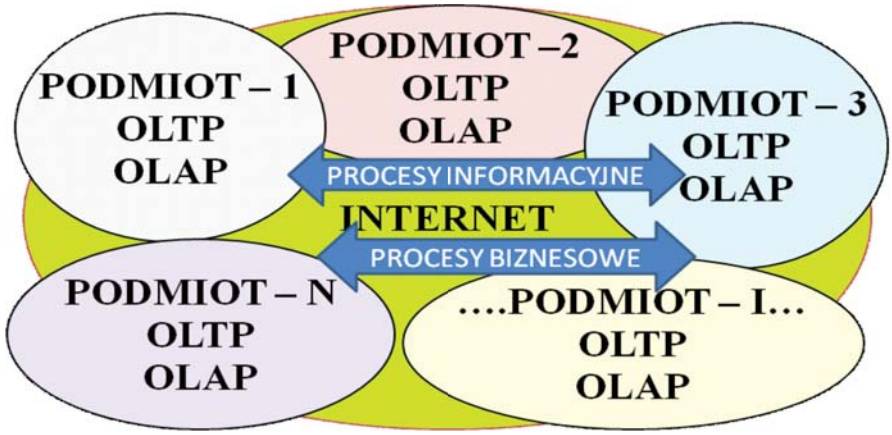
[11] Por. szerzej [w:] P. Zaskórski, J. Woźniak, *Ciągłość informacyjno-decyzyjna warunkiem bezpieczeństwa organizacji gospodarczej*, Ogólnopolska Konferencja Naukowa, Nowoczesne koncepcje i metody zarządzania. Teoria i praktyka, WAT, Warszawa 2009.

[12] Zazwyczaj jednak klienta wewnętrznego interesuje tylko wynik swojego poprzednika. Zatem ten rodzaj kontroli nie odgrywa znaczącej roli w procesie ochrony zasobów informacyjnych.

[13] Por. szerzej [w:] D.L. Pipkin, *Bezpieczeństwo informacji. Ochrona globalnego przedsiębiorstwa*, WNT, Warszawa 2002, s. 41-75.

[14] Przykładami rozwiązań są np. systemy: SAP/R3, BAAN, NAVISION, hurtownie danych.

ww. klas narzędzi informatycznych w znacznym stopniu warunkuje bezpieczeństwo zasobów informacyjnych, a tym samym ciągłość działań biznesowych. Tak więc wszelkie relacje[15] w strukturach procesowych mogą być źródłem ryzyka dla bezpieczeństwa zasobów informacyjnych w aspekcie niepożądanej asymetrii informacyjnej.



Rys. 1. Podstawowe kategorie zasobów informacyjnych w procesowych organizacjach biznesowych
Źródło: opracowanie własne

W przypadku struktur procesowych relacje z otoczeniem zewnętrznym stają się wręcz koniecznością. Należy wówczas uwzględniać sposób i zakres pozyskiwania zasobów informacyjnych a także formy i środki komunikacji. Każdy z wymienionych czynników w ściśle określony sposób determinuje jakość procesów biznesowych, co wiąże się z poziomem zabezpieczenia repozytoriów danych. Należy zauważyć, że to właśnie podmioty zewnętrzne są zarówno źródłem[16], jak i głównym beneficjentem zasobów informacyjnych[17]. Odwołując się do założeń koncepcji X-engineeringu, należy stwierdzić, że wdrażane organizacji procesowych bazuje na możliwościach Internetu[18]. Zawsze jednak problemem jest maksymalizacja poziomu bezpieczeństwa zasobów informacyjnych z uwzględnieniem świadomie sterowanej asymetrii informacyjnej i ograniczania skutków asymetrii wymuszonej przez otoczenie.

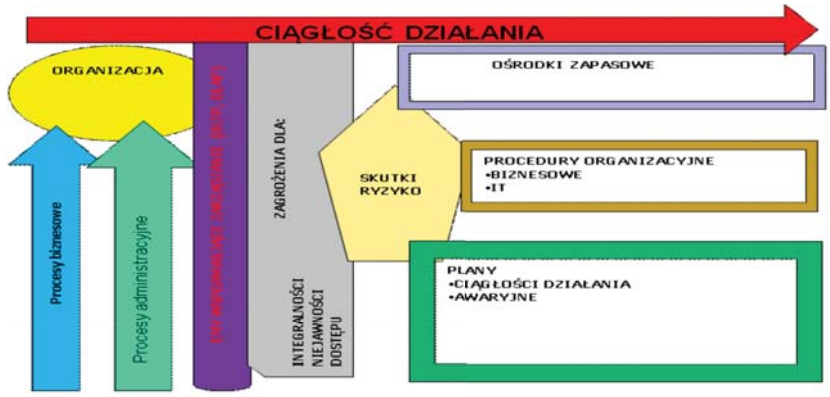
W Polsce jak i na świecie wprowadza się unormowania prawne związane z bezpieczeństwem zasobów informacyjnych[19]. Są to ważne wskazania zapewniające

[15] Oczywiście, wskazane zostały jedynie wybrane kategorie relacji wewnętrznych w organizacjach procesowych, które ze względu na swoją specyfikę generują najistotniejsze rodzaje zagrożeń.
[16] Innymi źródłami są m.in. wiedza generowana przez organizację i wiedza ukryta pracowników.
[17] W tym znaczeniu zasoby informacyjne należy rozumieć także np. jako know-how, B+R, analizę popytu, podaży, działań podejmowanych przez konkurentów, itp.
[18] K. Zimniewicz, Wyd. cyt., s 89-94.
[19] Dotyczy to głównie wdrażania norm ISO/IEC 13335, ISO/IEC 27002:2005 oraz PN-I-07799-2:2005.

poziom bezpieczeństwa zasobów informacyjnych udostępnianych, szczególnie w trybie on-line. Menedżerowie nie zawsze mają możliwość wdrażania określonych norm i standardów ochrony. Związane jest to bowiem ze znaczącymi nakładami inwestycyjnymi ponoszonymi na rozwój infrastruktury bezpieczeństwa (w przypadku modeli procesowych złożoność organizacji skutkuje wzrostem kosztów). Głównym przedsięwzięciem jest wówczas zbudowanie fundamentów własnej polityki bezpieczeństwa. Skutecznym rozwiązaniem staje się model bezpieczeństwa, który uwzględnia specyfikę i złożoność procesów biznesowych.

4. PLANOWANIE CIĄGŁOŚCI INFORMACYJNO-DECYZYJNEJ

Każda organizacja jako system działania realizuje procesy transformujące zdefiniowane wejście na określone wyjście. Stan i poziom zasobów decydują o potencjale organizacji. Wartość wyników działania (wartość wyjścia) jest pochodną wartości wejścia i stanu systemu. Wartość organizacji wyraża się także poziomem ryzyka związanego z przydatnością i dostępnością odpowiednich zasobów systemu. Ryzyko utraty określonych własności zasobów bezpośrednio wiąże się z poziomem ciągłości działania. Podstawowe kategorie strat mogą dotyczyć zarówno utraty jak również obniżenia wartości różnego typu zasobów (w tym informacyjnych). Straty mogą też powstać w wyniku zakłócenia kluczowych procesów gospodarczych lub administracyjnych[20].



Rys. 2. Uogólniony model bezpieczeństwa organizacji
Źródło: opracowanie własne

[20] W zarządzaniu bezpieczeństwem organizacji ważnym staje się bieżące monitorowanie stanu infrastruktury krytycznej, jej audyty oraz systemowa weryfikacja skuteczności mechanizmów jej ochrony w odniesieniu do prognozowanych nakładów. Efektywność systemu bezpieczeństwa jako kosztów osiągania jednego ze strategicznych celów organizacji jest ważnym wskaźnikiem jakości tego systemu.

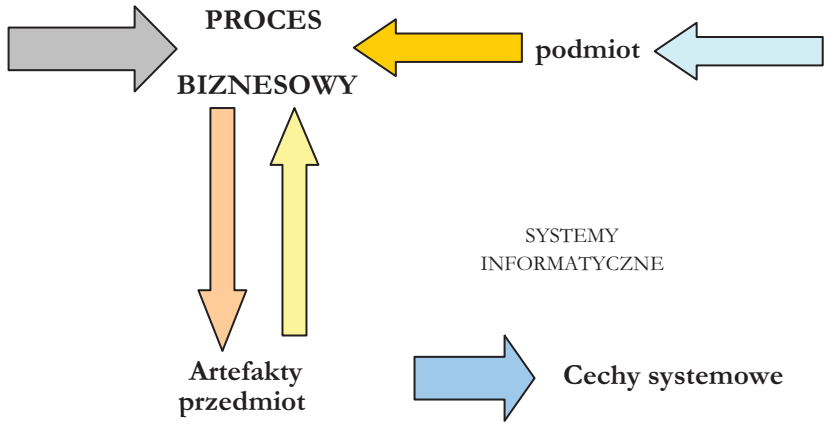
Ważną przesłanką do oceny oraz planowania zakresu i poziomu ochrony zasobów informacyjnych jest ich znaczenie dla organizacji. Przyjmuje się, że zasoby wpływające bezpośrednio na realizację strategii organizacji posiadają status zasobów strategicznych i podlegają szczególnej ochronie zarówno w aspekcie integralności jak i poufności oraz dostępności dla wybranych użytkowników. Do takich zasobów należą informacje analityczne, będące obrazem działania organizacji w dłuższym horyzoncie czasowym. Archiwizowanie i utrzymywanie zasobów historycznych, oczyszczonych i odpowiednio zagregowanych warunkuje realizację wieloprzekrojowych analiz i wspomagania decyzji w wyznaczonych horyzontach działania. Organizację takich zasobów zapewniają systemy hurtowni danych klasy OLAP wzbogacone o procedury odkrywania wiedzy (ang. *data mining*). Źródłami dla systemów OLAP są systemy klasy OLTP utrzymujące dane obrazujące bieżące działania organizacji. Ochrona tych zasobów może mieć wpływ na ciągłość działania organizacji również w wymiarze realizacji celów strategicznych. Poufność, integralność i dostępność tych danych może być zagrożona. Dane te mają zwykle charakter dziedzinowy i dotyczyć mogą zakresu tematycznego. W przypadku jednak tzw. systemów zintegrowanych – dane mogą być funkcjonalnie a nawet fizycznie scalone w postaci standardowej bazy danych. Wtedy mechanizmy replikacji i wielowarstwowa architektura tej klasy systemów umożliwiają utrzymywanie ich aktualności i zapewniają możliwości ich szybkiego odtwarzania w różnych Problem organizacji zasobów informacyjnych należy ujmować w aspekcie ich podatności na zagrożenia. Analiza i ocena ryzyka wiąże się z ustaleniem nie tylko źródeł zagrożeń dla poszczególnych komponentów całej organizacji, ale również z uświadomieniem ich odporności na zagrożenia, konsekwencji w aspekcie potencjalnych strat a także możliwości implementacji mechanizmów ochrony. Mechanizmy bezpieczeństwa dedykowane dla danej organizacji powinny uwzględniać fakt, że o skuteczności zabezpieczeń decyduje najsłabsze ogniwo systemu oraz zweryfikowany poziom zaufania.

Dla zapewnienia biznesowej ciągłości działania organizacji a przede wszystkim powiązania różnego typu zagrożeń ze skutkami w pierwszej fazie planowania jest potrzebna identyfikacja źródeł ryzyka w jej strukturze organizacyjnej. Przyjąć można, że inaczej rozkładać się będą akcenty dla organizacji hierarchicznych (wielopoziomowych), w tym dla organizacji administracji państwowej a inne akcenty dotyczyć będą organizacji gospodarczych (biznesowych) płaskich (sieciowych, macierzowych, hipertekstowych). Bezpieczeństwo organizacji i bezpieczny poziom (stan) zasobów informacyjnych, będących integralnym komponentem infrastruktury krytycznej wynikać powinny z możliwości zapewnienia ciągłości działania (rys. 2)

przez przeciwdziałanie zagrożeniom dla eksploatowanych rozwiązań informatycznych. Podstawą tworzenia uogólnionego modelu bezpieczeństwa może być identyfikacja poziomu bezpieczeństwa w aspekcie różnego typu zagrożeń[21], w której należy uwzględniać klasyfikację typów organizacji, strukturę organizacyjną i sposób uporządkowania realizowanych procesów a także istotę rozwiązań IT wspomagających funkcjonowanie danej organizacji, a w szczególności architekturę zasobów informacyjnych, ich kompleksowość i znaczenie oraz poziom sprzężenia z otoczeniem zewnętrznym i wewnętrznym. Na tym tle należy dokonać identyfikacji podstawowych klas skutków dla ważnych komponentów informacyjnej infrastruktury krytycznej przez wyeksponowanie istotnych zjawisk/procesów/obiektów wpływających na ogólne i informacyjne bezpieczeństwo organizacji. Główne zagrożenia dla poufności, dostępności i integralności danych utrzymywanych w systemach IT z uwzględnieniem ich kontekstowości powinny być poddane walidacji. Analiza ryzyka wg przyjętego modelu (metodyki) ewaluacji i walidacji zagrożeń, ich częstości oraz szacowanych strat może być istotną bazą do określenia procedur organizacyjnych, zapewniających ciągłość działania organizacji z uwzględnieniem oceny dynamiki zjawisk/procesów/przepływów (materialnych, finansowych, kadrowych jak również informacji i wiedzy). Szybkie i wielowariantowe opracowywanie planów ciągłości działania w zakresie dostępności, integralności i poufności zasobów informacyjnych przy uwzględnieniu typu/klasy infrastruktury teleinformatycznej i przy zachowaniu kryterium zapobiegania potęgowaniu się skutków negatywnych, wynikających z danego typu zagrożenia – staje się pomocnym mechanizmem przeciwdziałania wymuszonej asymetrii informacyjnej. Wiąże się to często z opracowywaniem doraźnych planów awaryjnych związanych z wybranymi typami zagrożeń, ich bieżącą oceną oraz możliwością oddziaływania otoczenia (wymuszania zachowań systemu) i jego elementów (obiektów) z uwzględnieniem podatności na te oddziaływania.

Zakłada się, że w procesie modelowania systemu bezpieczeństwa organizacji (rys. 3) podstawą jest identyfikacja źródeł i analiza ryzyka. Stąd też przyjmuje się, że źródeł ryzyka w procesach gromadzenia i przetwarzania informacji (i nie tylko) należy poszukiwać w naruszeniu relacji między procesami, ich wykonawcami oraz przedmiotem działania. Zagrożenia mogą więc wywołać negatywne skutki w zasobach technicznych i programowo-technologicznych przez destabilizację ich funkcjonowania. Zasoby te mogą być również zniekształcone w odniesieniu do poszczególnych artefaktów (zbiorów danych, obszarów działalności) oraz tracić adekwatność do metod działania (zasoby metadanych, doświadczenie).

[21] Zaskórski P.: Koncepcja informatyzacji systemu reagowania kryzysowego MON. AON, Warszawa 2002.



Rys. 3. Model holistycznego podejścia do identyfikacji źródeł ryzyka w procesach biznesowych
Źródło: opracowanie własne na podstawie BS 25999-1: 2006: Business continuity management. Code of practice, BS 25999-2: 2007: Specification for business continuity management

Procedury organizacyjne związane z ciągłością działania i całościowy model bezpieczeństwa powinny uwzględniać wszystkie typy zasobów warunkujące wypełnianie zadań z obszaru działalności podstawowej[22]. Główną przesłanką w zapewnianiu ciągłości informacyjno-biznesowej jest obiektywny wpływ otoczenia na poziom realizacji celów strategicznych w okresie mieszczącym się w przedziale czasu objętym wieloletnim lub krótkookresowym planem działania. Cele i zadania systemu bezpieczeństwa organizacji powinny być wyodrębnioną przedmiotowo, podmiotowo, przestrzennie, czasowo i proceduralnie – składową jej celu strategicznego. Procedury organizacyjne mają zapewniać ciągłość działań przez tworzenie zapasowych struktur lub zmiany w istniejących strukturach działania a także przez przesuwanie kompetencji, przemieszczanie zasobów i ogólnie tworzenie oraz realizację planów awaryjnych. Modele wzorców procedur organizacyjnych przeciwdziałania zagrożeniom dla informacyjnej ciągłości działania w różnych klasach organizacji mogą bazować na strukturach procesowych, strukturach zapasowych (ośrodkach, serwerowniach)[23] lub na okresowych usprawnieniach istniejących struktur działania. Warianty sce-

[22] Organizacja jest więc systemem zachowującym się racjonalnie, posiadającym w swojej strukturze podsystemy mające wspólne zamierzenia (cele), które zmuszają do wprowadzenia podziału pracy, a system informacyjny i komunikacyjny, umożliwia interakcje między podsystemami i pełni rolę regulacyjno-sterującą w całym systemie. W ten sposób wypełnia się zasada strukturalizmu i sterowalności. Uporządkowane części (podsystemy) przyczyniają się do powodzenia całości, a powodzenie całości jest istotnym warunkiem powodzenia jego składowych. Stąd też bezpieczeństwo systemu (organizacji) przekłada się na bezpieczeństwo poszczególnych jego elementów.
[23] NIST SP 800-34 : Typy zapasowych ośrodków obliczeniowych [Zimny (ang. Cold Site), Ciepły (ang. Warm Site), Gorący (ang. Hot Site), Lustrzany (ang. Mirrored Site) oraz Mobilny (ang. Mobile Site)].

nariuszy przyszłości stanowią pewną całościową, hipotetyczną wizję przyszłości a w tym przewidywane (możliwe) sytuacje krytyczne obejmujące dany obiekt wraz z wybranymi segmentami otoczenia. Scenariusze mogą mieć charakter eksploracyjny lub antycypacyjny (2). Scenariusze eksploracyjne – stanowią opis sekwencji zdarzeń prowadzących w sposób logiczny od sytuacji wyjściowej do możliwej przyszłości z uwzględnieniem tendencji dominujących, natomiast scenariusze antycypacyjne zawierają obraz przyszłości, określany jako pożądany przy założeniu zmian w funkcjonowaniu danej organizacji w określonych sytuacjach[24].

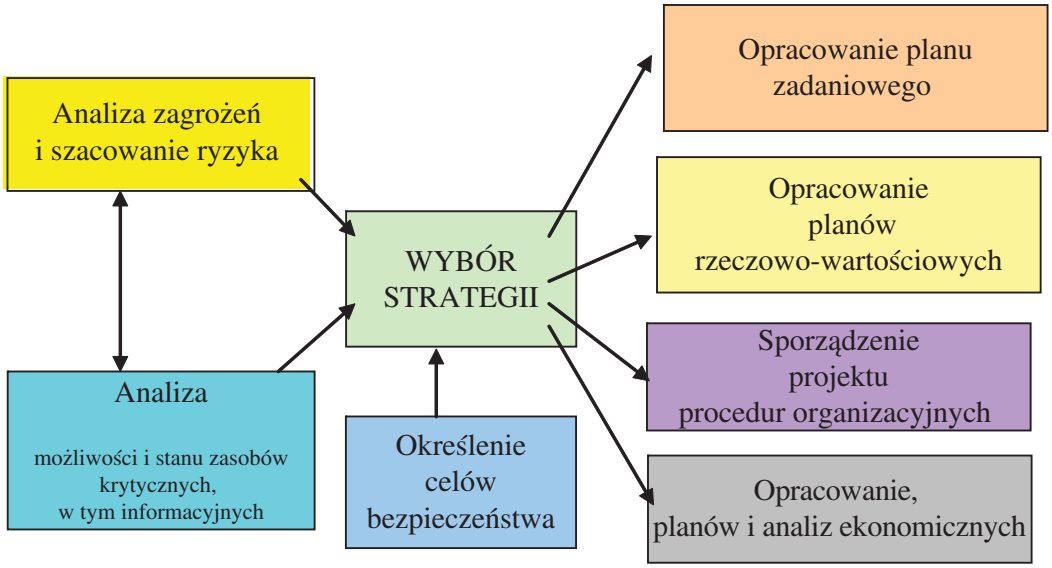
Często odwołujemy się do scenariuszy zachowań otoczenia, które mogą odgrywać ważną rolę w planowaniu skutków w danej organizacji. Scenariusze te pozwalają na przygotowanie zbioru reakcji i działań profilaktycznych w różnych horyzontach czasowych[25]. W modelowaniu ciągłości działania wykorzystuje się również scenariusze symulacyjne na podstawie listy istotnych czynników w otoczeniu, mających wpływ na bezpieczeństwo organizacji. Każdy czynnik powinien mieć określoną wagę (priorytet) w danym obszarze problemowym. W scenariuszach możliwych zdarzeń tworzy się opis rozwoju sytuacji w otoczeniu i projektuje odpowiednią reakcję organizacji. Szczególnego znaczenia nabierają wówczas procesy kluczowe lub krytyczne o dużym wpływie na bezpieczeństwo organizacji i wysokim prawdopodobieństwie zaistnienia. Najczęściej opracowuje się scenariusze dla niekorzystnego układu warunków funkcjonowania organizacji przy silnym ograniczeniu wartości zasobów.

Sporządzane różnymi metodami dokumenty planistyczne[26] (plany awaryjne) różnią się między sobą przeznaczeniem, zakresem przedmiotowym, stopniem szczegółowości i układem treści. Jest to zwykle zbiór analiz, prognoz i zamierzeń opisujących całą organizację z uwzględnieniem celu, przedmiotu działania i uwarunkowań działalności w aspekcie zaangażowanych zasobów finansowych, osobowych i rzeczowych, spodziewanych efektów finansowych i czynników ryzyka. Plan taki jest więc dokumentem, w którym na podstawie diagnozy sytuacji krytycznych (diagnozy wewnętrznej i zewnętrznej) określane są cele i kluczowe strategie oraz planowane działania (rys. 4).

[24] Opracowuje się zwykle wiele prawdopodobnych wersji biegu wydarzeń i do nich projektuje się różne sposoby zachowania organizacji (odmienne strategie, plany przedsięwzięć).

[25] Metody scenariuszowe traktuje się przede wszystkim jako narzędzie planowania strategicznego, które nie dają dokładnego obrazu przyszłości, ale pobudzają do działań profilaktycznych, szczególnie w zarządzaniu bezpieczeństwem. Metody scenariuszowe zmuszają do przewidywania różnego rozwoju zdarzeń i analizy ich wpływu na zachowania danej organizacji. Do ważnych obszarów należą wśród nich scenariusze symulacyjne.

[26] NIST SP 800-34: Klasyfikacja planów zapewniania ciągłości działania



Rys. 4. Ogólna procedura budowy planów awaryjnych i ciągłości działania organizacji
Źródło: opracowanie własne na podstawie Liderman K.: Analiza ryzyka i ochrona informacji w systemach komputerowych. PWN

Proces przygotowania planu awaryjnego i planów ciągłości działania wiąże się z wyborem strategii działania oraz stworzeniem realnych planów ilościowo-wartościowych. Musi to być poprzedzone analizą podstawowych grup zasobów (infrastruktury krytycznej), którymi dysponuje wybrana organizacja (zasoby finansowe, rzeczowe, osobowe, organizacyjne, informacyjne), w układzie głównych funkcji i kompetencji (macierz zasoby/funkcje). Wyniki analizy potencjału organizacji są zazwyczaj prezentowane w formie analizy SWOT. Plany rzeczowe (nazywane też planami technicznymi) powinny określać ilość i strukturę zasobów rzeczowo-osobowych niezbędnych do realizacji planowanych przedsięwzięć oraz wyznaczać sposoby ich wykorzystania.

Przedmiotem ciągłego doskonalenia modelu zarządzania organizacją w sytuacjach krytycznych, zagrażających obniżeniu bezpieczeństwa organizacji w różnych jego aspektach (ekonomicznym, materialnym, energetycznym, informacyjnym) powinno być integracja zasobów informacyjnych. Informatyczne systemy wspomagające zarządzanie oraz systemy wspomagania podejmowania decyzji mogą zmienić model funkcjonowania organizacji przez wykorzystywanie wspólnej platformy Internetu (strategia X-engineeringu). Podstawą tych zmian są procesy i propozycje ich realizacji przy silnej partycypacji otoczenia z uwzględnieniem wymuszonej lub sterowanej asymetrii informacyjnej. Wzmocnienie potencjału organizacji może nastąpić

przez integrację współdziałania a przede wszystkim przez integrację procesów bieżącego informowania i monitorowania zdarzeń przy ustalonych wzorcach procedur działania.

5. PODSUMOWANIE

Rozwój technik i metod zarządzania organizacją daje możliwości wprowadzenia skutecznych zmian w każdej organizacji dla poprawy jej bezpieczeństwa wewnętrznego i zewnętrznego oraz zapewnienia ciągłości działania. Ciągłość biznesowa organizacji jest silnie warunkowana bezpieczeństwem zasobów informacyjnych, szczególnie we współczesnych warunkach wdrażania struktur procesowych, których funkcjonowanie bazuje na dostępie on-line do zasobów pochodzących z różnych źródeł. Procesy stają się obiektem organizacyjnym, a proces gromadzenia i przetwarzania danych zyskuje status procesu strategicznego w organizacji. Bezpieczeństwo informacyjne jest więc składową bezpieczeństwa całej organizacji i dotyczy wszystkich obszarów jej działalności podstawowej. Właściwa realizacja działań we wszystkich obszarach determinuje skuteczność realizacji procesów w każdej organizacji, niezależnie od jej struktury organizacyjnej. Infrastruktura krytyczna organizacji wiąże się z zapewnieniem możliwości wypełniania przez nią funkcji podstawowych na poziome procesów strategicznych i głównych procesów operacyjnych.

Systemy zintegrowane scalają szerokie spektrum zasobów informacyjnych w skali całej organizacji. Umożliwia to zapewnienie poufności, integralności i dostępności zasobów informacyjnych każdej organizacji. Założenia te prowadzą również do zapewnienia szeroko pojętej zgodności struktur informacyjnych i silnych mechanizmów bezpieczeństwa.

Literatura

1. BS 25999-1: *Business continuity management. Code of practice,* 2006.
2. BS 25999-2: *Specification for business continuity management,* 2007.
3. Grajewski P., *Organizacja procesowa*, PWE Warszawa 2007.
4. Kaczmarek T.T., Ćwiek G., *Ryzyko kryzysu a ciągłość działania*, Difin, Warszawa 2009.
5. Pipkin D.L., *Bezpieczeństwo informacji. Ochrona globalnego przedsiębiorstwa*, WNT, Warszawa 2002.
6. Komisja Wspólnot Europejskich: *Komunikat komisji w sprawie europejskiego programu ochrony infrastruktury krytycznej (*dnia 12.12.2006/KOM). Bruksela 2006.
7. Liderman K.*: Analiza ryzyka i ochrona informacji w systemach komputerowych*. PWN. Warszawa. 2008.
8. PN-IEC 62198: *Zarządzanie ryzykiem przedsięwzięcia – Wytyczne stosowania* 2005.

9. Zaskórski P., Żyto T., Pałka D.: *Risk in development and implementation of integrated systems.* VIII NATO Regional Conference on Military Communications and Information Systems. Gdynia 2006.
10. Zaskórski P., Suszek A.: *Zarządzanie procesami projektowo-wdrożeniowymi systemów bezpieczeństwa. V Międzynarodowa Konferencja Bezpieczeństwa.*" Zarządzanie kryzysowe". Gdynia 2007.
11. Zaskórski P., Woźniak J., *Ciągłość informacyjno-decyzyjna warunkiem bezpieczeństwa organizacji gospodarczej*, Ogólnopolska Konferencja Naukowa, Nowoczesne koncepcje i metody zarządzania. Teoria i praktyka, WAT, Warszawa 2009.
12. Zaskórski P., Woźniak J., *Asymetria informacyjna w zarządzaniu bezpieczeństwem organizacji gospodarczej*, Biuletyn IOIZ, WAT, Warszawa 2009.