Współczesna Gospodarka

Contemporary Economy
Electronic Scientific Journal
www.wspolczesnagospodarka.pl

Vol. 1 Issue 1 (2010) 1-11
ISSN 2082-677X

NORMY, STANDARDY, MODELE I ZALECENIA W ZARZĄDZANIU BEZPIECZEŃSTWEM INFORMACJI

Karol Kreft

Streszczenie

Informacja jest obszarem, który decydować może o potencjale i wartości rynkowej przedsiębiorstwa. Wzrost wartości kapitału intelektualnego organizacji opierającej swoją działalność na informacji wymusza potrzebę stworzenia skutecznego sytemu zarządzania bezpieczeństwem. Przedsiębiorstwa coraz częściej tworzą systemy zarządzania bezpieczeństwem informacji w oparciu o sprawdzone modele. W artykule przedstawiono główne problemy zarządzenia bezpieczeństwem informacji. Opisano modele bezpieczeństwa i analizę ryzyka w zarządzeniu bezpieczeństwem informacji.

Słowa kluczowe: informacja, sytem zarządzania bezpieczeństwem, analiza ryzyka, modele bezpieczeństwa

Wstęp

W dobie rozwoju technologii informacyjnych, globalizacji oraz konsolidacji najcenniejszą wartością w prowadzeniu działalności gospodarczej stała się informacja. Szybki rozwój nowych technologii informacyjnych i tempo wdrażania pionierskich rozwiązań w gospodarce opartej na wiedzy, przekłada się na powstawanie nowych globalnych zagrożeń istotnych z punktu widzenia przedsiębiorstw wykorzystujących systemy informatyczne.

Można zaryzykować stwierdzenie, że nie ma przedsiębiorstwa, które nie doświadczyło strat związanych z utratą ważnych informacji. Nieliczna grupa przedsiębiorstw rozumie wagę posiadanych informacji i opracowuje skuteczny system zarządzania bezpieczeństwem.

1. Problemy zarządzania bezpieczeństwem informacji

Bezpieczeństwo informacji to nie tylko zabezpieczenia informatyczne czy fizyczne, to także przeszkolony i świadomy zagrożeń personel. Bezpieczeństwo informacji to proces i jak każdy proces wymaga ciągłego doskonalenia.

Ilość i wartość danych gromadzonych w systemach informacyjnych nieustannie narasta. Rośnie także liczba zagrożeń związanych z przechowywaną i przetwarzaną informacją. Reakcją na wzrost liczby zagrożeń jest nieustanne podnoszenie poziomu bezpieczeństwa informacji. W tym wypadku podnoszenie poziomu bezpieczeństwa związane jest z zapewnieniem niezakłóconego funkcjonowania systemu informatycznego podczas realizacji wyznaczonych zadań.

Wyniki Światowego Badania Bezpieczeństwa Informacji przeprowadzone przez Ernst&Young na ponad 1300 organizacjach z 55 krajów pokazały, że duża grupa przedsiębiorstw nie zarządza odpowiednio bezpieczeństwem informacji. Jedna piąta respondentów (21%) nie zajmuje się tą kwestią, a jedna trzecia (33%) stosuje nieformalne metody.

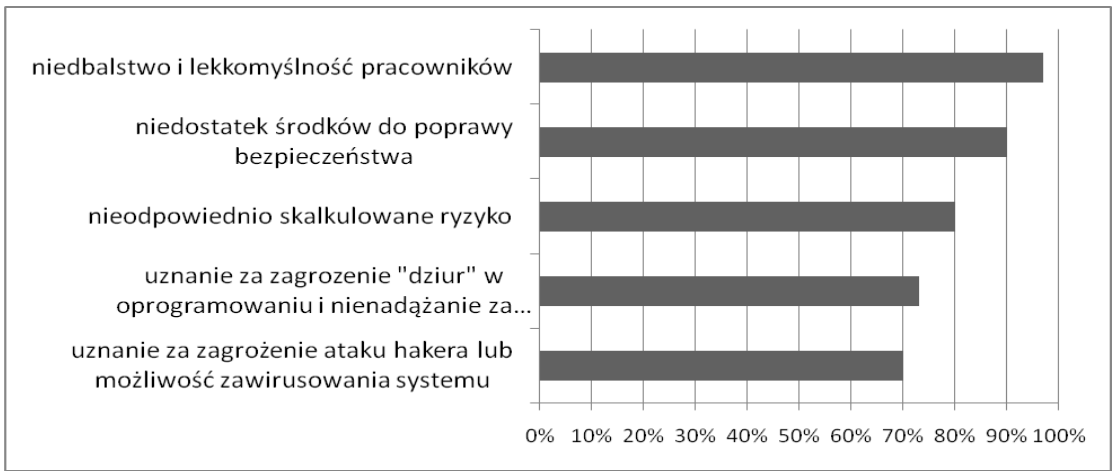
Certyfikaty bezpieczeństwa informacji, takie jak BS 7799, ISO 17790, CobIT, ITIL wdrożono tylko w około 25% przedsiębiorstw, kolejne 30% przedsiębiorstw planuje takie wdrożenia.

Badanie „The State of Information Security" zostały przeprowadzone na ponad 7,5 tysiąca respondentów w 54 krajach na sześciu kontynentach. Z analizy udzielonych odpowiedzi wynika, że przedsiębiorstwa dopiero stawiają pierwsze kroki w dziedzinie skutecznego i nowoczesnego podejścia do zarządzania bezpieczeństwem informacji.

Badania „The State of Information Security" wykazały ciekawe i zastanawiające fakty:

- Zwiększane znacząco wydatki na bezpieczeństwo nie przyniosły odczuwalnego skutku w postaci zmniejszenia liczby włamań do systemu.
- Ogromna większość ujawnionych incydentów to wydarzenia stosunkowo mało groźne, trwające krótko i kosztujące niewiele.
- Respondenci, którzy najbardziej ucierpieli w wyniku naruszeń bezpieczeństwa, średnio dwa razy częściej niż pozostali planowali – o dziwo – zmniejszenie wydatków na bezpieczeństwo. Prawdopodobnie poniesione wydatki na bezpieczeństwo zainwestowano w mało skuteczne zabezpieczenia lub chroniono niewłaściwe zasoby.
- Najbardziej poszkodowani respondenci uznali szkolenie pracowników jako priorytetowe.
- Co czwarty respondent nie mierzył, ani nie sprawdzał skuteczności prowadzonych działań w zakresie bezpieczeństwa.

Według raportu Unisys, który badał CISO (CISO – chief information security officers) do podstawowych zagrożeń należy lekkomyślność i niedbalstwo pracowników. Problemem jest także niedostatek środków potrzebnych do skutecznej poprawy bezpieczeństwa.

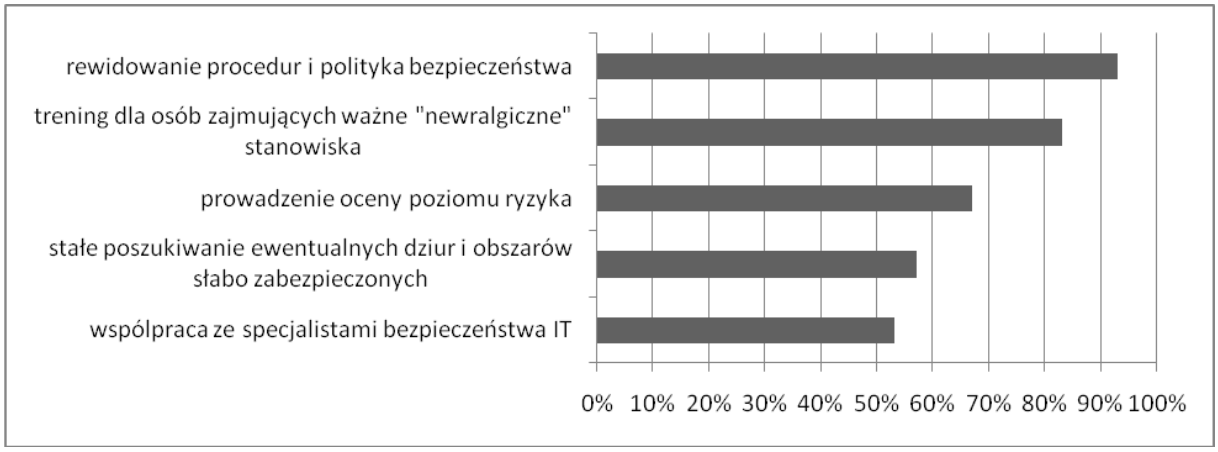


Rysunek 1. Zagrożenia wg ankiety przeprowadzonej przez Unisys

Źródło: opracowanie własne.

Unisys zaproponował także zestaw najlepszych praktyk z zakresu bezpieczeństwa informatycznego:

- Integracja zarządzania bezpieczeństwem z innymi działaniami w ramach tworzenia i weryfikacji wewnętrznych przepisów przedsiębiorstwa.
- Bezpośrednie sprawozdania CISO do członków zarządu.
- Wzmocnienie pozycji menadżerów ds. bezpieczeństwa informacji.
- Stworzenie najlepszego do zrealizowania, w danych warunkach, systemu treningu personelu w kwestiach bezpieczeństwa.
- Stałe monitorowanie procesu zarządzania bezpieczeństwem.



Rysunek 2. Jak przedsiębiorstwa zarządzają ryzykiem wg ankiety Unisys

Źródło: opracowanie własne.

2. Standardy, normy dotyczące bezpieczeństwa informacji

Przedsiębiorstwa coraz częściej tworzą systemy zarządzania bezpieczeństwem informacji w oparciu o sprawdzone modele. Bezpieczeństwo informatyczne możemy interpretować jako zespół procesów zmierzających do osiągnięcia i utrzymania założonego poziomu następujących atrybutów : poufności, autentyczności, dostępności, integralności, rozliczalności oraz niezawodności.

Tablica 1. Określenia atrybutów bezpieczeństwa wg PN-1-13335-1

Nazwa atrybutu	Określenie
Poufność	Własność zapewniająca, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, pomiotom lub procesom
Autentyczność	Własność zapewniająca, że tożsamość podmiotu lub zasobu jest taka jak deklarowana; dotyczy użytkowników, procesów, systemów lub nawet instytucji; autentyczność jest związana z badaniem, czy ktoś lub coś jest tym lub czymś za kogo lub za co się podaje
Dostępność	Własność bycia dostępnym i możliwym do wykorzystania na żądanie w założonym czasie przez kogoś lub coś, kto lub coś ma do tego prawo

Integralność danych	Własność zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany
Integralność systemu	Własność polegająca na tym, że system realizuje swoje zamierzone funkcje w nienaruszony sposób, wolny od nieautoryzowanej manipulacji celowej lub przypadkowej
Integralność	Integralność danych oraz integralność systemu
Rozliczalność	Własność zapewniająca, że działanie podmiotu może być jednoznacznie przypisane tylko temu podmiotowi
Niezawodność	Własność oznaczająca spójne, zamierzone zachowania i skutki

Źródło: opracowanie własne.

Zarządzanie bezpieczeństwem obejmuje zespół procesów zmierzających do osiągnięcia i utrzymania w systemie informacyjnym ustalonego poziomu wyżej wymienionych atrybutów bezpieczeństwa.

Normalizacja wprowadziła podstawowe definicje związane z bezpieczeństwem:

System zarządzania bezpieczeństwem informacji (ISMS – Information Security Management System) - część całościowego systemu zarządzania instytucji, oparta na podejściu wynikającym z ryzyka biznesowego i odnosząca się do ustanawiania, wdrażania, monitorowania, utrzymania oraz doskonalenia bezpieczeństwa informacji. (PN-I-07799-2)

Polityka bezpieczeństwa informacji - udokumentowany zbiór zasad, praktyk i procedur, w którym dana organizacja określa, w jaki sposób chroni aktywa systemu informatycznego oraz przetwarzanie informacji. (PN ISO/IEC 17799)

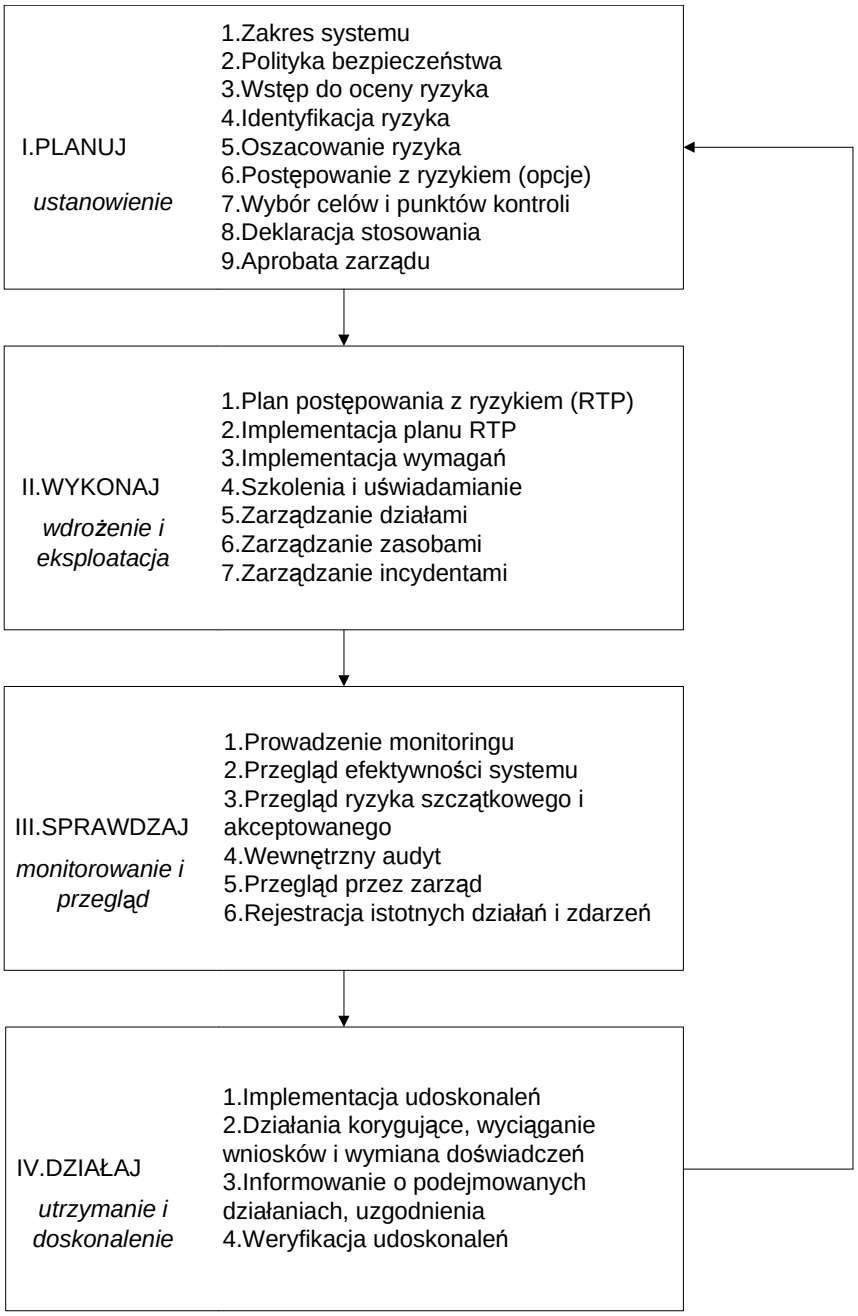
Zarządzanie ryzykiem – skoordynowane działania kierowania i kontrolowania organizacji z uwzględnieniem ryzyka. (ISO Guide 73:2002).

System zarządzania bezpieczeństwem to także zespół elementów o charakterze technicznym, proceduralnym i behawioralnym. Poszczególne elementy sytemu przedstawione zostaną na przykładzie zagrożenia związanego z przejęciem hasła użytkownika systemu informatycznego. W tym przypadku możemy zastosować następujące środki:

- Techniczne – oprogramowanie szyfrujące transmisje, wprowadzenie uwierzytelniania metodami biometrycznymi, zabezpieczenie okablowania strukturalnego przed dostępem osób nieupoważnionych.
- Proceduralne – konfiguracja systemu odrzucająca hasła krótkie i zawierające tylko litery, procedury wymuszające okresową zmianę hasła, procedury przechowywania i udostępniania hasła.
- Behawioralne – szkolenie pracowników w zakresie bezpiecznego logowania się do systemu, kształtowanie świadomości o występowaniu zagrożenia związanego z socjotechnicznymi metodami wyłudzania hasła.

Warunkiem skuteczności systemu zarządzania bezpieczeństwem jest podejście strategiczne całościowo obejmujące wszystkie elementy zabezpieczeń. Pominiecie jednego z elementów pozastawia lukę, której wykorzystanie przez osoby niepowołane może zniweczyć całe nakłady przeznaczone na bezpieczeństwo. Zatem system zarządzania bezpieczeństwem to także zespół zasad i procedur umożliwiających całościową skuteczną ochronę systemu informacyjnego przedsiębiorstwa.

W krajach Unii Europejskiej norma brytyjska BS 7799 jest uważana za wiodący dokument w zakresie zarządzania bezpieczeństwem.



Rysunek 3. Schemat zarządzania bezpieczeństwem informacji według normy BS 7799

Źródło: opracowanie własne.

Należy zwrócić uwagę także na normę ISO/IEC TR 133335 Guidelines for the Management of IT Security, która składa się z następujących części:

- ISO/IEC TR 13335-1 Wytyczne do zarządzania bezpieczeństwem systemów informatycznych.
  (terminologia, związki miedzy pojęciami, podstawowe modele)
- ISO/IEC TR 13335-2 Technika informatyczna – Planowanie i zarządzanie bezpieczeństwem systemów informatycznych.
  (prowadzenie analizy ryzyka, plany zabezpieczeń, organizacja bezpieczeństwa, działania uświadamiające, szkolenia)

- ISO/IEC TR 13335-3 Techniki zarządzania bezpieczeństwem systemów informatycznych.
  (zrządzanie bezpieczeństwem, trójpoziomowa polityka bezpieczeństwa, analiza ryzyka, implementacja planu zabezpieczeń, czynności powdrożeniowe, monitorowanie bezpieczeństwa, reagowanie na incydenty).
- ISO/IEC TR 13335-4 Wybór zabezpieczeń.
  (klasyfikacja i charakterystyka zabezpieczeń, dobór zabezpieczeń ze względu na rodzaj zagrożeń i specyfikę systemu).
- ISO/IEC TR WD 13335-5 Zabezpieczenia dla połączeń z sieciami zewnętrznymi.
  (dobór zabezpieczeń na styku systemów instytucji z siecią zewnętrzną).

Niezależną organizacją skupiającą specjalistów z zakresu bezpieczeństwa informacyjnego z ponad stu krajów jest Information Systems Audit and Control Association (ISACA). Głównym celem ISACA jest opracowanie i rozpowszechnienie standardów dotyczących audytu bezpieczeństwa. W grupie dokumentów opublikownych przez ISACA najważniejszy jest standard Control Objectives for Information and Related Technology (COBIT). W metodyce COBIT zarządzanie procesami teleinformatycznymi podzielono na cztery domeny:

PO – Planowanie i organizacja (Planning and Organisation)
(definiowanie planu strategicznego dla teleinformatyki, definiowanie architektury informatycznej, ustalenie kierunku technologicznego, określenie organizacji i relacji na styku teleinformatyka-biznes, zarządzanie inwestycjami teleinformatycznymi, przedstawianie celów i kierunków rozwoju, zarządzanie zasobami ludzkimi, zachowanie zgodności z wymogami zewnętrznymi, ocena ryzyka, zarządzanie projektami, zarządzanie jakością)

AI – Nabywanie i wdrażanie (Acquisition and Implementation)
(identyfikowanie zautomatyzowanych rozwiązań, nabywanie i utrzymywanie oprogramowania użytkowego, nabywanie i utrzymywanie infrastruktury technologicznej, rozwiązywanie i utrzymanie procedur dotyczących teleinformatyki, instalowanie i akredytowanie systemów, zarządzanie zmianami)

DS – Dostarczanie i wspieranie (Delivery and Support)
(definiowanie poziomu usług, zarządzanie usługami zewnętrznymi, zarządzanie wydajnością, zapewnienie ciągłości usług, zapewnienie bezpieczeństwa systemów, identyfikowanie i rozliczanie kosztów, szkolenie użytkowników, wspomaganie i doradztwo dla klientów, zarządzanie konfiguracją, zarządzanie problemami i incydentami, zarządzanie danymi, zarządzanie infrastrukturą, zarządzanie operacjami)

M- Monitorowanie
(monitorowanie procesów, monitorowanie wydajności, raportowanie, ocena adekwatności kontroli wewnętrznej, zapewnienie niezależnego audytu)

Dzięki wspieraniu przez jedną z najsilniejszych organizacji (ISACA) COBIT jest jednym z najbardziej wszechstronnych, kompleksowych i powszechnie stosowanych standardów.

Na podstawie normy BS 7799 Komitet Techniczny nr 182 do spraw „Ochrony informacji w Systemach Teleinformatycznych" PKN opracował polską normę PN-ISO/IEC 17799: Technika informatyczna – Praktyczne zasady zarządzania bezpieczeństwem informacji.

Ważniejsze zalety normalizacji z zakresu bezpieczeństwa informacji to:

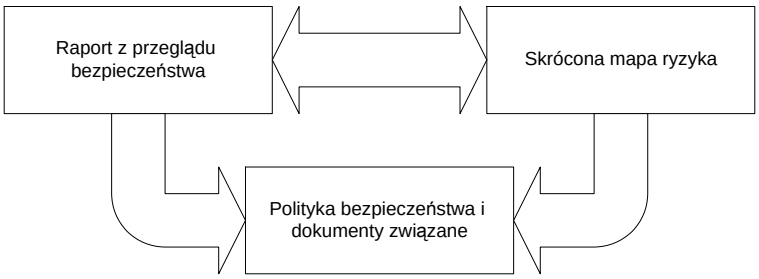
- systematyzacja procesu oceny systemu zabezpieczeń,
- ustalenie wspólnej platformy odniesienia pozwalającej uzyskać powtarzalność procesu oceny bezpieczeństwa i porównywalność wyników,
- ułatwienie formułowania zasad przeprowadzenia audytu bezpieczeństwa,
- wspomaganie procesu projektowania i tworzenia systemów informacyjnych mających spełniać wysoką jakość pozwalającą na uzyskanie założonego certyfikatu bezpieczeństwa.

Materiały normalizacyjne można pogrupować według podejścia do problematyki bezpieczeństwa, każda norma przedstawia inną metodykę, ma swoje wady i zalety. Czasami proponowane rozwiązanie jest niekompletne i nie pokrywa w pełni potrzeby danej organizacji. Tworząc system bezpieczeństwa należy niezależnie od przyjętej bazy normalizacyjnej zapewnić harmonię między poszczególnymi elementami zabezpieczeń.

3. Modele bezpieczeństwa i analiza ryzyka w zarządzaniu bezpieczeństwem informacji

Modele bezpieczeństwa i analiza ryzyka odgrywają kluczową rolę w procesie tworzenia systemu bezpieczeństwa instytucji. Metodyki postępowania różnią się w zależności od skali systemu informacyjnego. Niecelowe wydaje się stosowanie skomplikowanych i trudnych do realizacji modeli do małych systemów informacyjnych. Uproszczenie modelu obniża koszty budowy systemu bezpieczeństwa, co przyczynia się do zachowaniu opłacalności całego przedsięwzięcia.

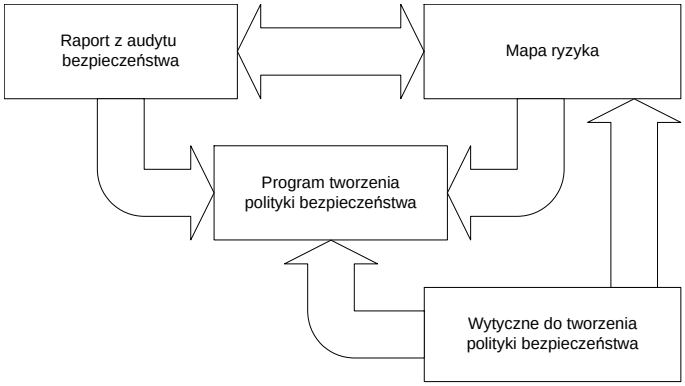
CERT(Computer Emergency Response Team) opracował trzy modele bezpieczeństwa



Rysunek 4. Model dedykowany małym organizacjom

(minimalne nakłady finansowe)

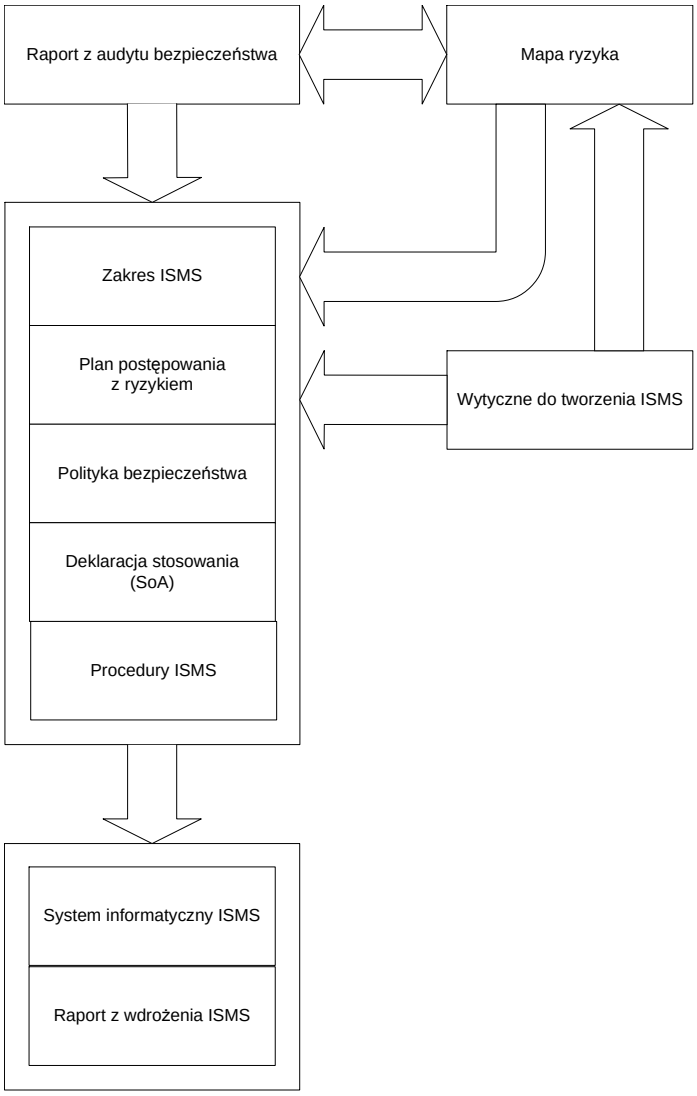
Źródło: opracowanie własne.



Rysunek 5. Model dedykowany organizacji o dowolnej wielkości

(optymalizacja nakładów finansowych)

Źródło: opracowanie własne.



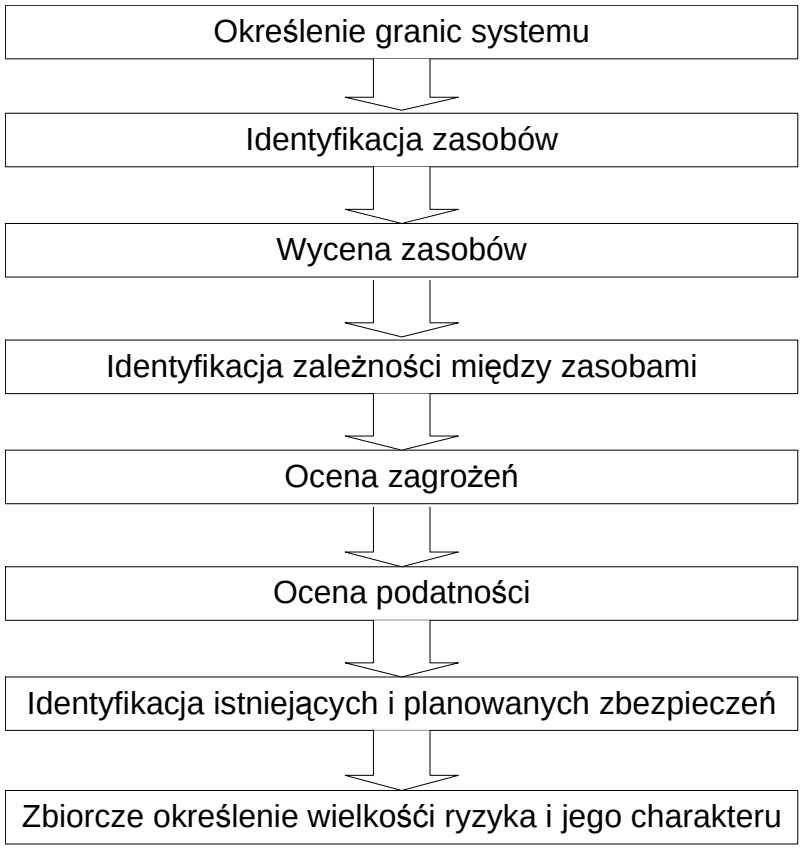
Rysunek 6. Model dedykowany organizacji o dowolnej wielkości

(certyfikat zgodności z normą PN-I-07799-2:2005)

Źródło: opracowanie własne.

W celu zapewnienia założonego poziomu bezpieczeństwa informacyjnego zaleca się okresowe przeprowadzanie analizy ryzyka – jej wyniki stanowią wytyczne dalszych działań modyfikujących system zabezpieczeń.

W normie BS7799 położono znaczy nacisk na zarządzanie ryzykiem.



Rysunek 7. Prowadzenie analizy ryzyka (BS7799)

Źródło: opracowanie własne.

Spotykane strategie zarządzania ryzykiem to:

- Ignorowanie istnienia ryzyka – przedsiębiorstwo odpowiedzialne nie powinno decydować się na taką strategię.
- Transfer ryzyka – ubezpieczenie się od ryzyka – po wniesieniu opłaty następuje przeniesienie ryzyka na instytucję ubezpieczającą, lecz bez obwarowań (zabezpieczeń redukujących ryzyko) uczynić tego nie można.
- Redukcja ryzyka przez stosowanie zabezpieczeń, wymaga ona oszacowania wielkości ryzyka.

Wyróżniamy strategie redukcji ryzyka, różniące się sposobem realizacji:

- Zastosowanie zabezpieczeń typowych dla określonych warunków, czyli ochrona podstawowa. Niezależnie od rzeczywistego ryzyka cały system traktowany jest w ten sam sposób. Nie bada się ryzyka, co prowadzi zwykle do przeszacowania nakładów na zabezpieczenia.
- Przyjęcie zabezpieczeń po przeprowadzeniu uproszczonej analizy ryzyka. Analiza koncentruje się na tych obszarach, które wydają się być najbardziej narażone.
- Przyjęcie zabezpieczeń wynikających ze szczegółowej analizy ryzyka. Całość systemu poddana jest dokładnej analizie ryzyka, często wykorzystywane jest specjalistyczne oprogramowanie.
- Metoda mieszana. W wyniku ogólnej analizy ryzyka określa się obszary systemu szczególnie narażone lub mające strategiczne znaczenie dla funkcjonowania przedsiębiorstwa, dla których zabezpieczenia dobiera się na podstawie szczególnej analizy ryzyka. W pozostałych obszarach systemu zastosowana jest ochrona podstawowa.

Zakończenie

Konieczne jest zatem opracowanie skutecznego systemu przetwarzania informacji, który będzie odporny na strategiczne zagrożenia. Działania kierownictwa przedsiębiorstwa powinny skoncentrować się na następujących zagadnieniach:

1. Stworzenie polityki bezpieczeństwa informacji, określenie zasad zabezpieczenia informacji, zapewnienie dostępności i integralności danych.
2. Alokacja zasobów i przydzielenie obowiązków pracownikom odpowiedzialnym za bezpieczeństwo, odpowiednio wykwalifikowane osoby będą dysponowały środkami do wdrażania i realizacji polityki bezpieczeństwa.
3. Ocena zagrożeń, identyfikacja zagrożeń, które mogą zakłócić prowadzenie działalności gospodarczej przedsiębiorstwa, opracowanie szczegółowej analizy zagrożeń dla każdego strategicznego elementu systemu informacyjnego.
4. Opracowanie planu w przypadku zaistnienia zagrożenia, określenie algorytmu postępowania, wyznaczenie konkretnych działań w odniesieniu do zasiniałych zagrożeń.
5. Rozwój i implementacja systemu zarządzania bezpieczeństwem informacji, postępowanie zgodne z dobrze dopracowanym projektem.
6. Analiza zaproponowanych środków kontrolnych jeszcze przed ich wdrożeniem.
7. Monitorowanie skuteczności zastosowanego systemu zarządzania bezpieczeństwem, systematyczne uaktualnianie elementów systemu.

Zarządzanie bezpieczeństwem informacji jest zbyt ważną rzeczą, by można było ograniczyć działania wyłącznie do zawodów związanych z technologiami komputerowymi.

Literatura

1. Amoroso E., *Wykrywanie intruzów*, Wydawnictwo READ ME, Łódź 2000
2. Białas A., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie,* Wydawnictwo Naukowo-Techniczne, Warszawa 2007
3. Lam K., LeBlanc D., Smith B., *Ocena bezpieczeństwa sieciowego*, Wydawnictwo Microsoft Press, Warszawa 2005
4. Lehitinen R., Russell D., Gangemi G., *Podstawy ochrony komputerów*, Wydawnictwo Helion, Gliwice 2007
5. Paluszynski W., *Systemy zarządzania bezpieczeństwem informacji,* materiały TI Trusted Information Consulting
6. Pietrzak J., Hardjono T., Seberry J., *Teoria bezpieczeństwa systemów komputerowych,* Wydawnictwo Helion, Gliwice 2003
7. Pipki D., *Bezpieczeństwo informacji Ochrona globalna przedsiębiorstwa,* Wydawnictwo Naukowo-Techniczne, Warszawa 2002
8. Reuvid J., *E-biznes bez ryzyka Zarządzanie bezpieczeństwem w* sieci, Wydawnictwo Helion, Gliwice 2007
9. http://ceo.cxo.pl
10. http://www.cert.pl
11. http://www.egospodarka.pl

NORMS, STANDARDS, MODELS AND RECOMMENDATIONS FOR INFORMATION SECURITY MANAGEMENT

Summary

Information is the factor which can decide about the potential and market value of a company. An increase in the value of intellectual capital of an information-driven company requires development of an effective security management system. More and more often companies develop information security management systems (ISMS) based on already verified models. In the article, the main problems with management of information security were discussed. Security models were described, as well as the risk analysis in information security management.

Keywords: information, security management systems, risk analysis, security models

dr Karol Kreft
Uniwersytet Gdański
Wydział Ekonomiczny
Instytut Transportu i Handlu Morskiego
ul. Armii Krajowej 119/121, 81-824 Sopot
krol@panda.bg.univ.gda.pl