dr Jan Madej
Katedra Informatyki
Wydział Zarządzania, Uniwersytet Ekonomiczny w Krakowie

Strategie analizy ryzyka w opracowywaniu polityki bezpieczeństwa systemu informatycznego

WSTĘP

Problem bezpieczeństwa systemów informatycznych (SI) nabrał obecnie szczególnego znaczenia. Wysoki stopień uzależnienia od technologii informatycznej (TI) oraz powszechne występowanie zagrożeń z nią związanych sprawiły, że do osiągnięcia odpowiedniego poziomu bezpieczeństwa SI w przedsiębiorstwie nie wystarczą już incydentalne działania, ale konieczne jest kompleksowe zarządzanie bezpieczeństwem systemu informatycznego.

Przyjmuje się, że zarządzanie bezpieczeństwem SI to szereg działań mających na celu uzyskanie i utrzymanie odpowiedniego poziomu bezpieczeństwa systemów informatycznych w przedsiębiorstwie. Część z tych działań może zachodzić równolegle, jednak niektóre wymagają realizacji w ściśle określonej kolejności i muszą być poprzedzone opracowaniem polityki bezpieczeństwa systemu informatycznego. To z kolei wymaga wcześniejszego przeprowadzenia analizy ryzyka według odpowiednio wybranej strategii.

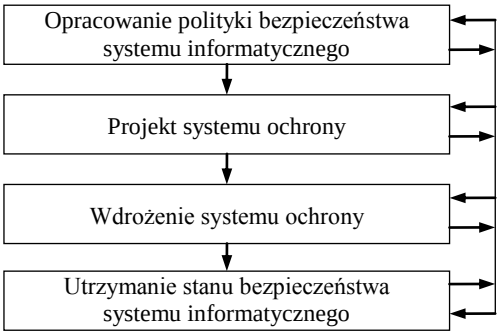
Celem niniejszego artykułu jest przedstawienie dostępnych strategii analizy ryzyka, które mogą być wykorzystane na pierwszym etapie procesu zarządzania bezpieczeństwem systemu informatycznego i dzięki którym możliwe jest opracowaniu właściwej polityki bezpieczeństwa SI.

ZARZĄDZANIE BEZPIECZEŃSTWEM SI

Lektura publikacji z zakresu bezpieczeństwa informatycznego pozwala stwierdzić, że proces zarządzania bezpieczeństwem SI – według autorów tych publikacji – składa się z różnej liczby etapów i przedstawiany jest na różnym poziomie szczegółowości[1]. Jest to efekt występowania różnych sposobów zarzą-

[1] Por. np.: BSI – *IT Baseline Protection Manual*, Bundesamt für Sicherheit in der Informationstechnik, 2009 [w:] *Bundesamt für Sicherheit in der Informationstechnik*, http://www.bsi.de/english/; A. Barczak, T. Sydoruk., *Bezpieczeństwo systemów informatycznych zarządzania*, Dom Wydawniczy Bellona, Warszawa 2003; D. Gaudyn, *Model zarządzania bezpieczeństwem informacji w organizacji ubezpieczeniowej*, rozprawa doktorska, Akademia Górniczo-Hutnicza, Kraków 2001; A. Grzywak (red.), *Bezpieczeństwo systemów komputerowych*, Wydawnictwo Pracowni

dzania bezpieczeństwem oraz różnych rozmiarów i struktur przedsiębiorstw. Jednak pomimo różnic, ważne jest to, że we wszystkich opracowaniach można wyróżnić podobne etapy tego procesu, które polegają na zaplanowaniu i opracowaniu polityki bezpieczeństwa, zaprojektowaniu i wdrożeniu systemu ochrony oraz utrzymaniu stanu bezpieczeństwa systemu (rysunek 1).



Rysunek 1. Etapy zarządzania bezpieczeństwem systemów informatycznych
Źródło: opracowanie własne.

Ważnym elementem są sprzężenia zwrotne, które mogą zachodzić pomiędzy dowolnymi etapami, a oznaczają potrzebę modyfikacji etapu wcześniejszego na skutek wykrycia (na etapie późniejszym) jego braków.

Takie przedstawienie zarządzania bezpieczeństwem SI chociaż charakteryzuje się dużą prostotą, oddaje jednak ideę samego procesu, bez względu na wielkość i charakter przedsiębiorstwa oraz budowę jego systemu informatycznego.

W miarę potrzeb, schemat można odpowiednio dostosować uszczegóławiając kolejne etapy. Taki właśnie, rozbudowany proces zarządzania bezpieczeństwem SI przedstawiony został na rysunku 2. Uwzględniono i wykorzystano w nim m.in. zalecenia norm ISO/IEC TR 13335[2], ISO/IEC 17799[3], metody ochrony podstawowej BSI[4] oraz – klasyczne już – zalecenia NIST[5].

Komputerowej Jacka Skalmierskiego, Gliwice 2000; A. Koweszko, *Zarządzanie bezpieczeństwem*, 2005 [w:] *Stowarzyszenie do spraw audytu i kontroli systemów informatycznych – ISACA* (Information Systems Audit and Control Association), http://www.isaca.org.pl/.

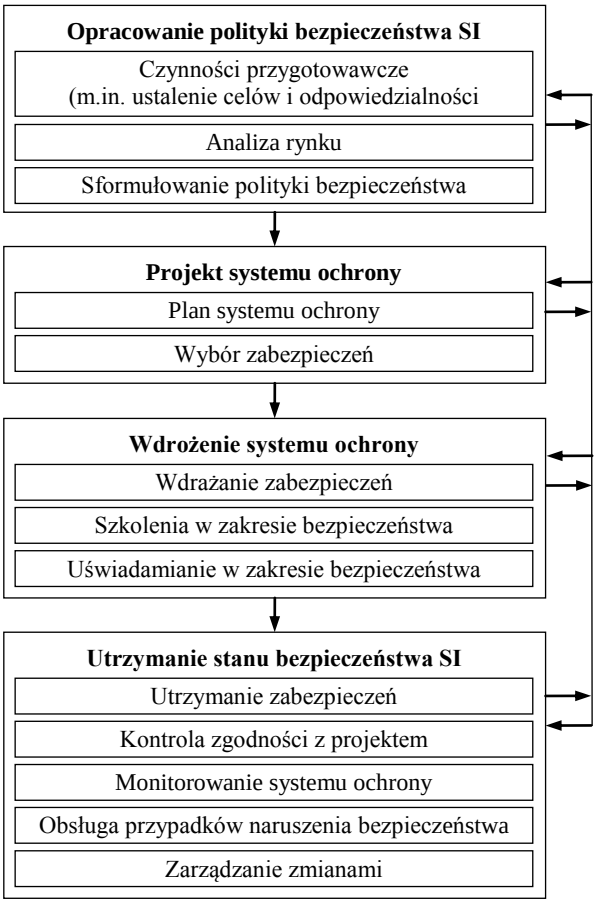
[2] Polska Norma PN-I-13335-1:1999, *Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele bezpieczeństwa systemów informatycznych*, Polski Komitet Normalizacyjny, Warszawa 1999.

[3] Polska Norma PN-ISO/IEC 17799:2003, *Technika informatyczna – Praktyczne zasady zarządzania bezpieczeństwem informacji*, Polski Komitet Normalizacyjny, Warszawa 2003.

[4] BSI – *IT Baseline Protection Manual*, Bundesamt für Sicherheit in der Informationstechnik, 2009, (w:) Bundesamt für Sicherheit in der Informationstechnik, serwis internetowy, http://www.bsi.de/english/.

[5] NIST – *An Introduction to Computer Security: The NIST Handbook*, NIST Special Publication 800-12, 1996 [w:] National Institute of Standards and Technology – Computer Security Resource Center, http://csrc.nist.gov/.

Na szczególną uwagę w całym procesie zarządzania bezpieczeństwem zasługuje pierwszy etap, czyli opracowanie polityki bezpieczeństwa SI, w skład którego wchodzi analiza ryzyka.



Rysunek 2. Etapy zarządzania bezpieczeństwem systemów informatycznych
Źródło: opracowanie własne.

Etap ten jest punktem wyjścia do skonstruowania odpowiedniego systemu ochrony, a tym samym do uzyskania zamierzonego poziomu bezpieczeństwa. Analiza ryzyka pełni na tym etapie kluczową rolę. W publikacjach z zakresu bezpieczeństwa SI właśnie ten etap wykazuje największe zróżnicowanie, wynikające ze wspomnianego już dopasowania do charakteru przedsiębiorstwa[6].

[6] Por. np.: A. Koweszko, *Zarządzanie…*; K. Liderman, *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Wydawnictwo Naukowe PWN, Warszawa 2008; A. Sadowski, *Czym jest polityka bezpieczeństwa organizacji?,* „Bezpieczeństwo IT" – miesięcznik internetowy, 2006, http://www.bezpieczenstwoit.pl/.

OPRACOWANIE POLITYKI BEZPIECZEŃSTWA SYSTEMU INFORMATYCZNEGO

Polityka bezpieczeństwa systemu informatycznego przedsiębiorstwa to zasady, zarządzenia i procedury, które określają, jak zasoby powinny być zarządzane, chronione i dystrybuowane w SI. Jej opracowanie wymaga wykonania szeregu czynności (m.in. określenia celów i potrzeb bezpieczeństwa, zidentyfikowania zasobów, zagrożeń i ryzyka ich wystąpienia), a następnie zdefiniowania zbioru zasad, zarządzeń i procedur, których przestrzeganie ma zapewnić bezpieczeństwo systemu. Wszystkie zasady, zarządzenia i procedury powinny zostać spisane i mieć postać formalnego, obowiązującego dokumentu, zwanego dokumentem polityki bezpieczeństwa.

Realizacja polityki bezpieczeństwa wymaga doboru oraz wdrożenia odpowiednich i spójnych zabezpieczeń (fizycznych, technicznych, organizacyjnych, personalnych oraz procedur ochronnych i awaryjnych), które utworzą tzw. system ochrony[7]. Poza systemem ochrony, polityka bezpieczeństwa powinna uwzględniać także m.in.: szkolenia, działania awaryjne, kontrole, monitoring i aktualizację zabezpieczeń.

Podczas opracowywania polityki bezpieczeństwa systemu informatycznego można wyróżnić następujące etapy:

- przeprowadzenie czynności przygotowawczych, podczas których należy:
  - uzyskać bezwzględne poparcie kierownictwa,
  - wyznaczyć osoby odpowiedzialne za opracowanie i realizację polityki bezpieczeństwa,
  - ustalić cele polityki bezpieczeństwa,
- przeprowadzenie analizy ryzyka,
- sformułowanie polityki i opracowanie dokumentu polityki bezpieczeństwa SI.

Etapy te scharakteryzowane zostały poniżej.

CZYNNOŚCI PRZYGOTOWAWCZE DO OPRACOWANIA POLITYKI BEZPIECZEŃSTWA SYSTEMU INFORMATYCZNEGO

Bardzo ważną sprawą dla całego procesu zarządzania bezpieczeństwem SI jest odpowiednie zaangażowanie kierownictwa wszystkich szczebli przedsię-

[7] Przy czym należy zdawać sobie sprawę z tego, że nie jest celowe (a często także nie jest możliwe) jednoczesne zastosowanie wszystkich dostępnych zabezpieczeń, gdyż w praktyce absolutne bezpieczeństwo systemu, tak czy inaczej, jest nieosiągalne, a funkcjonowanie zbyt rozbudowanego systemu ochrony zmniejsza efektywność działania i zwiększa koszty eksploatacji. Jednak przeoczenie bądź zbagatelizowanie realnego zagrożenia może okazać się katastrofalne w skutkach. Należy więc projektować i wdrażać optymalny system ochrony kierując się odpowiednio zdefiniowaną polityką bezpieczeństwa, dobraną do charakteru działalności przedsiębiorstwa.

biorstwa. Bez jego poparcia osiągnięcie zamierzonego poziomu bezpieczeństwa jest trudne, a czasami wręcz niemożliwe. Dlatego ważne jest, aby działania osób zajmujących się bezpieczeństwem SI poparte były odpowiednią postawą i zaangażowaniem kierownictwa, od którego oczekuje się m.in.:

- zrozumienia potrzeb w zakresie bezpieczeństwa SI,
- demonstrowania zaangażowania w sprawy bezpieczeństwa SI,
- odpowiedniego poziomu świadomości w zakresie bezpieczeństwa SI,
- gotowości do zaspokojenia potrzeb wynikających z zarządzania bezpieczeństwem SI (np. przydzielanie środków finansowych i zasobów na rzecz działań w tym zakresie).

Podjęcie przez kierownictwo decyzji o zarządzaniu bezpieczeństwem SI powinno także oznaczać wyznaczenie osoby lub zespołu osób odpowiedzialnych za opracowanie i realizację polityki bezpieczeństwa systemu informatycznego. Polityka bezpieczeństwa systemu informatycznego musi mieć swojego „właściciela", który odpowiada za jej opracowanie, wdrożenie i późniejszą realizację. Zazwyczaj pełni on funkcję tzw. kierownika ds. bezpieczeństwa[8].

Należy jednak zaznaczyć, że właściciel polityki nie musi być jej autorem (choć sytuacja taka byłaby bardzo korzystna). W praktyce, niewiele przedsiębiorstw ma wystarczające zaplecze personalne i zatrudnia do opracowania polityki odpowiednich specjalistów.

Po wyznaczeniu osoby odpowiedzialnej za realizację polityki bezpieczeństwa kierownictwo musi wraz z nią ustalić główne cele polityki.

Punktem wyjścia jest jasne ustalenie głównych celów przedsiębiorstwa dotyczących bezpieczeństwa jego systemu informatycznego. Cele te muszą wynikać z celów nadrzędnych (np. celów biznesowych) i w efekcie prowadzić do celów polityki bezpieczeństwa systemów informatycznych, którymi najczęściej są:

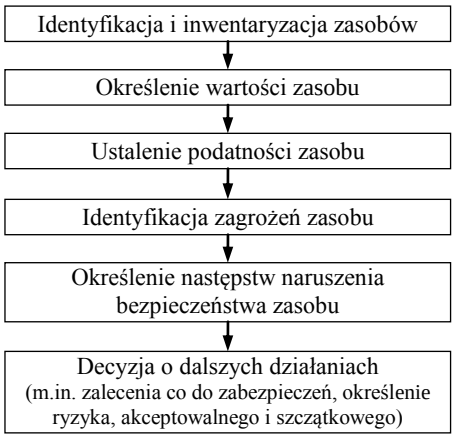
- zagwarantowanie prawnych wymagań ochrony informacji (np. ochrona danych rachunkowych, ochrona danych osobowych, ochrona informacji niejawnych),
- zagwarantowanie bezpieczeństwa zasobów systemu, a w szczególności przetwarzanej informacji (tzn. zagwarantowanie jej poufności, integralności i dostępności),
- zagwarantowanie bezpieczeństwa publicznego i prestiżu przedsiębiorstwa,
- zagwarantowanie ciągłości funkcjonowania przedsiębiorstwa,
- osiągnięcie redukcji kosztów.

Po wykonaniu tego etapu można przejść do kolejnego, którym jest przeprowadzenie analizy ryzyka.

[8] Zgodnie z wymogami ustawy o ochronie informacji niejawnych jest to funkcja inspektora bezpieczeństwa teleinformatycznego, a zgodnie z przepisami o ochronie danych osobowych – administratora bezpieczeństwa informacji.

ANALIZA RYZYKA I JEJ STRATEGIE

Analiza ryzyka w kontekście bezpieczeństwa systemów informatycznych składa się z analizy wartości zasobów, ich zagrożeń i podatności[9]. Jest ona bardzo ważnym elementem zarządzania bezpieczeństwem, ponieważ od sposobu jej przeprowadzenia zależy ocena sytuacji w zakresie bezpieczeństwa i późniejszy wybór zabezpieczeń. Przebieg pełnej analizy ryzyka składa się zazwyczaj z kilku etapów (zob. rysunek 3).



Rysunek 3. Etapy analizy ryzyka

Źródło: opracowanie własne.

Jednak, w zależności od przyjętej strategii, niektóre etapy analizy mogą być zredukowane. Analiza może być przeprowadzana nie tylko podczas tworzenia nowego systemu, ale także w dowolnym momencie życia już funkcjonującego systemu[10].

Celem analizy ryzyka jest dostarczenie m.in.:

- informacji o wartości i wymaganiach ochronnych analizowanych zasobów,
- informacji o podatności zasobów,
- informacji o potencjalnych zagrożeniach zasobów i ich poziomie ryzyka,
- informacji o następstwach naruszenia bezpieczeństwa zasobów,
- zaleceń co do ryzyka akceptowalnego i ryzyka szczątkowego[11] danych zasobów,

[9] W nieco innym przekroju analizę ryzyka traktuje się jako część większego procesu zwanego zarządzaniem ryzykiem, które polega na porównywaniu określonego ryzyka z zyskami i kosztami ochrony, oraz na wyborze i wdrożeniu zabezpieczeń.

[10] K. Liderman, *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Wydawnictwo Naukowe PWN, Warszawa 2008.

[11] Ryzyko, które świadomie nie jest w żaden sposób ograniczane, ponieważ zostało zaakceptowane – określa się mianem ryzyka akceptowalnego. Ryzyko szczątkowe jest to ryzyko, które

- zaleceń co do wyboru zabezpieczeń,
- informacji o korzyściach wynikających z wdrożenia zabezpieczeń.

Zalecenia i informacje dostarczone przez analizę ryzyka powinny być przyjęte i zatwierdzone przez kierownictwo przedsiębiorstwa, jako punkt wyjścia do dalszych działań (m.in. opracowania planu systemu ochrony).

Jednak poddanie analizie wszystkich zasobów systemu informatycznego jest bardzo kosztowne i czasochłonne. Ponadto, nie zawsze istnieje potrzeba przeprowadzenia tak szczegółowej analizy.

O tym, jak dokładna i na czym oparta powinna być analiza ryzyka, decyduje przede wszystkim planowany poziom bezpieczeństwa systemu oraz inne czynniki (np. wielkość, charakter i rodzaj działalności przedsiębiorstwa). Dlatego w praktyce występują różne rodzaje analizy ryzyka, określane mianem strategii.

Najczęściej wykorzystywane strategie analizy ryzyka to:

- strategia podstawowego poziomu bezpieczeństwa,
- nieformalna analiza ryzyka,
- szczegółowa analiza ryzyka,
- strategia mieszana.

Porównanie ich podstawowych cech zawiera tabela 1.

Tabela 1. Porównanie strategii analizy ryzyka

	Strategia podstawowego poziomu bezpieczeństwa	Nieformalna analiza ryzyka	Szczegółowa analiza ryzyka	Strategia mieszana
czas przeprowadzania analizy	krótki / średni	krótki	długi	średni
koszt analizy	mały / średni	mały	wysoki	średni
zaangażowanie zasobów	małe / średnie	małe	wysokie	średnie
zasoby podlegające identyfikacji	wybrane	brak	wszystkie	wybrane
poziom bezpieczeństwa	podstawowy	niski	wysoki	podstawowy

Źródło: opracowanie własne.

pozostaje po wdrożeniu zabezpieczeń. W praktyce ryzyko takie zawsze istnieje, gdyż żaden system nie jest całkowicie bezpieczny, co więcej, pewne zasoby pozostają celowo niechronione w najlepszy dostępny sposób (np. z powodu niskiego ryzyka wystąpienia zagrożenia lub wysokich kosztów zabezpieczeń). Ważne jest jednak, aby osoby decydujące o wyborze zabezpieczeń miały świadomość istnienia ryzyka szczątkowego i ryzyko to akceptowały. Możliwa powinna być tylko albo akceptacja ryzyka, albo zastosowanie dodatkowych zabezpieczeń, które zredukują to ryzyko do akceptowanego poziomu, co na ogół wiąże się z dodatkowymi kosztami. Niedopuszczalna jest sytuacja, w której ryzyko szczątkowe nie jest akceptowane, ale np. z braku środków kierownictwo nie robi nic, aby je zmniejszyć.

Według powszechnie uznanych standardów i norm (np. BSI, ISO/IEC TR 13335, ISO/IEC 17799, ISO/IEC 27001) oraz doświadczeń praktycznych, dla przedsiębiorstw, które nie mają wysokich wymagań bezpieczeństwa, wystarczającą metodą analizy ryzyka jest strategia podstawowego poziomu bezpieczeństwa lub nieformalna analiza ryzyka.

W tym miejscu należy zaznaczyć, że strategia podstawowego poziomu bezpieczeństwa i analiza nieformalna proponują od razu pewne rozwiązania w zakresie zabezpieczania zasobów. Oznacza to, że nachodzą one częściowo na następny etap zarządzania bezpieczeństwem, czyli projektowanie systemu ochrony (por. rysunek 2).

Strategia podstawowego poziomu bezpieczeństwa – polega na doborze grupy zabezpieczeń, które pozwalają osiągnąć podstawowy poziom bezpieczeństwa systemu informatycznego w przedsiębiorstwie. Podczas jej realizacji należy najpierw sporządzić listę zasobów systemu (w oparciu o katalog modułów wzorcowych), a następnie zapoznać się z ich potencjalnymi zagrożeniami (w oparciu o katalog zagrożeń).

Kolejnym krokiem jest przypisanie wymagań ochronnych do poszczególnych zasobów, a na zakończenie – wybór zestawu zabezpieczeń odpowiednich dla zasobów i ustalonego dla nich poziomu bezpieczeństwa (w oparciu o katalog zabezpieczeń). Wzorcowe katalogi zasobów, zagrożeń i zabezpieczeń dostępne są w publikacjach poświęconych wykorzystaniu podstawowego poziomu bezpieczeństwa[12]. Można także skorzystać z doświadczeń innych przedsiębiorstw, podobnych do analizowanego pod względem celów, wielkości, rodzaju działalności i budowy systemu informatycznego.

Do zalet strategii podstawowego poziomu zalicza się m.in.:

- redukcja czasu i wysiłku poświęconego na wybór zabezpieczeń,
- niewielkie zaangażowanie zasobów systemu,
- łatwa przenośność rozwiązań pomiędzy różnymi systemami,
- łatwa porównywalność rozwiązań przyjętych w różnych przedsiębiorstwach.

Do wad tej strategii zalicza się m.in.:

- nieodpowiednia (niewystarczająca lub zbyt restrykcyjna) ochrona zasobów systemu w przypadku błędnego ustalenia ich wymagań ochronnych,
- ewentualne trudności z zarządzaniem bezpieczeństwem w przypadku istotnych zmian w systemie (np. jego rozwoju lub aktualizacji).

Nieformalna analiza ryzyka – nie jest oparta na metodach strukturalnych, ale przeprowadzana jest przez osobę, która wykorzystując swoją wiedzę i doświadczenie potrafi określić wartość zasobów, ich podatność oraz zidentyfikować ryzyko, na jakie są one narażone. Jeżeli osoba taka nie jest zatrudniona w przedsiębiorstwie, to analiza może być przeprowadzona przez konsultantów zewnętrznych.

[12] BSI – *IT Baseline Protection…*; Polska Norma PN-ISO/IEC 17799:2003; *Technika…*

Do zalet nieformalnej analizy ryzyka należą przede wszystkim:

- oszczędność czasu potrzebnego na przeprowadzenie analizy,
- niewielki koszt analizy (w porównaniu np. z analizą szczegółową).

Do jej wad należą:

- większe prawdopodobieństwo nieuwzględnienia niektórych rodzajów ryzyka oraz pominięcia zasobów,
- duży wpływ subiektywnych poglądów i nastawienia osoby analizującej na wynik tejże analizy,
- brak szczegółowego uzasadnienia wyboru konkretnych zabezpieczeń,
- trudności w zarządzaniu bezpieczeństwem w przypadku istotnych zmian w systemie (np. jego rozwoju lub aktualizacji), które mogą spowodować konieczność przeprowadzenia powtórnej analizy.

Jednak pomimo swoich wad nieformalna analiza ryzyka jest często wystarczająca dla małych przedsiębiorstw.

Szczegółowa analiza ryzyka – musi być przeprowadzona dla całego systemu informatycznego przedsiębiorstwa. Wymaga ona identyfikacji i określenia wartości wszystkich zasobów oraz oceny ich podatności i zagrożeń. Informacje te służą do określenia poziomu ryzyka, wyboru zabezpieczeń oraz przyjęcia ryzyka akceptowalnego.

Do zalet tej analizy zaliczyć można m.in.:

- określenie poziomu bezpieczeństwa dla każdego zasobu SI,
- dostarczenie dodatkowych informacji dla innych procesów w przedsiębiorstwie (np. zarządzania zmianami).

Główne jej wady to:

- wysoki koszt wynikający m.in. z jej dużej czaso- i pracochłonności,
- konieczność posiadania przez osoby przeprowadzające analizę szczegółowej wiedzy o konkretnych rozwiązaniach występujących w systemie.

Strategia mieszana – jej przeprowadzenie poprzedzone jest wyodrębnieniem części systemu informatycznego przedsiębiorstwa o wysokim stopniu ryzyka lub zawierającej zasoby krytyczne. Następnie dla tej części przeprowadzana jest szczegółowa analiza ryzyka w celu osiągnięcia odpowiedniego poziomu ochrony, a dla reszty systemu realizowana jest strategia podstawowego poziomu bezpieczeństwa lub analiza nieformalna.

Główną zaletą strategii mieszanej, w porównaniu z analizą szczegółową całego systemu, jest mniejszy koszt i krótszy czas jej realizacji. Wadą tej strategii jest nieodpowiedni dobór analizy dla części systemu w przypadku niewłaściwego wyodrębnienia obszarów systemu o wysokim stopniu ryzyka.

Strategia ta, ze względu na mniejsze koszty i porównywalną skuteczność, może być z powodzeniem wykorzystana zamiast analizy szczegółowej. Jest ona zalecana w większości przedsiębiorstw, dla których strategia podstawowego poziomu bezpieczeństwa jest niewystarczająca.

SFORMUŁOWANIE POLITYKI I OPRACOWANIE DOKUMENTU POLITYKI BEZPIECZEŃSTWA SI

Przeprowadzenie analizy ryzyka powinno dostarczyć osobom odpowiedzialnym za bezpieczeństwo systemu informatycznego niezbędnej wiedzy na temat ryzyka, na jakie narażone są zasoby systemu oraz możliwości jego zaakceptowania lub sposobów jego ograniczenia i wyeliminowania. Na jej podstawie kierownictwo przedsiębiorstwa musi opracować i przyjąć treść polityki bezpieczeństwa.

Na etapie opracowywania (podczas zebrań, posiedzeń i spotkań) ma ona kształt roboczy (często w postaci raportów, sprawozdań, propozycji, notatek, itd.), ale musi zostać sformalizowana i przyjąć postać dokumentu polityki bezpieczeństwa.

Dokument polityki bezpieczeństwa systemu informatycznego to wszystkie spisane zasady, rozporządzenia i procedury stanowiące politykę bezpieczeństwa SI. Powinien on być zatwierdzony przez kierownictwo oraz opublikowany i udostępniony w odpowiedni sposób wszystkim pracownikom[13].

Zalecane jest, aby dokument ten zawierał m.in.:

- definicję bezpieczeństwa SI oraz ogólne cele, zakres i znaczenie bezpieczeństwa,
- przyjętą hierarchię ważności zasobów (np. strategiczne, krytyczne, autoryzowane, powszechnie dostępne) i klasyfikację wymagań ochronnych zasobów (np. bardzo wysokie, wysokie, umiarkowane, brak),
- wyjaśnienie polityki bezpieczeństwa, zasad, standardów i wymagań zgodności,
- oświadczenie o intencjach kierownictwa i ich poparciu dla realizowanej polityki,
- określenie ogólnych i szczegółowych obowiązków oraz odpowiedzialności w zakresie zarządzania bezpieczeństwem, a także konsekwencje naruszenia polityki bezpieczeństwa,
- odsyłacze do dokumentacji uzupełniającej politykę (np. do procedur ochronnych).

W tym miejscu należy raz jeszcze podkreślić rolę sprzężeń zwrotnych, które występują na każdym etapie zarządzania bezpieczeństwem oraz podczas formalizowania polityki bezpieczeństwa. Ostateczny kształt dokumentu polityki, a przede wszystkim opracowanie szczegółowych procedur postępowania i obsługi zabezpieczeń systemu informatycznego, możliwe jest dopiero po ich wyborze i wdrożeniu.

[13] Zalecane jest udostępnienie dokumentu polityki bezpieczeństwa w formie właściwej, dostępnej i zrozumiałej dla użytkowników, do których jest on adresowany.

ZAKOŃCZENIE

Celem niniejszego referatu było przedstawienie etapu opracowywania polityki bezpieczeństwa systemu informatycznego wraz z analizą ryzyka, jako pierwszego etapu zarządzania bezpieczeństwem systemu informatycznego. Przedstawiono w nim czynności konieczne do prawidłowego sformułowania dokumentu polityki bezpieczeństwa ze szczególnym uwzględnieniem analizy ryzyka.

Analiza ryzyka jest kluczowym elementem w całym procesie zarządzania bezpieczeństwem SI i – co ważne – może być przeprowadzana na różne sposoby. Prawidłowy wybór strategii analizy ryzyka decyduje nie tylko o poniesionych nakładach i ilości czasu potrzebnego do jej przeprowadzenia, ale także o zasadności przyjętych rozwiązań. Dlatego w opracowaniu przedstawiono zalety i wady najczęściej wykorzystywanych strategii analizy ryzyka.

LITERATURA

BSI – *IT Baseline Protection Manual*, Bundesamt für Sicherheit in der Informationstechnik, 2009 [w:] Bundesamt für Sicherheit in der Informationstechnik, serwis internetowy http://www.bsi.de/english/.

Barczak A., Sydoruk T., *Bezpieczeństwo systemów informatycznych zarządzania*, Dom Wydawniczy Bellona, Warszawa 2003.

Gaudyn D., *Model zarządzania bezpieczeństwem informacji w organizacji ubezpieczeniowej*, rozprawa doktorska, Akademia Górniczo-Hutnicza, Kraków 2001.

Grzywak A. (red.), *Bezpieczeństwo systemów komputerowych*, Wydawnictwo Pracowni Komputerowej Jacka Skalmierskiego, Gliwice 2000.

Koweszko A., *Zarządzanie bezpieczeństwem*, 2005 [w:] Stowarzyszenie do spraw audytu i kontroli systemów informatycznych – ISACA (Information Systems Audit and Control Association), serwis internetowy http://www.isaca.org.pl/.

Liderman K., *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Wydawnictwo Naukowe PWN, Warszawa 2008.

NIST – *An Introduction to Computer Security: The NIST Handbook*, NIST Special Publication 800-12, 1996 [w:] National Institute of Standards and Technology – Computer Security Resource Center, http://csrc.nist.gov/.

Polska Norma PN-ISO/IEC 17799:2003, *Technika informatyczna – Praktyczne zasady zarządzania bezpieczeństwem informacji*, Polski Komitet Normalizacyjny, Warszawa 2003.

Polska Norma PN-I-13335-1:1999, *Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele bezpieczeństwa systemów informatycznych*, Polski Komitet Normalizacyjny, Warszawa 1999.

Polska Norma PN-ISO/IEC 27001:2007, *Systemy zarządzania bezpieczeństwem informacji. Wymagania*, Polski Komitet Normalizacyjny, Warszawa 2007.

Sadowski A., *Czym jest polityka bezpieczeństwa organizacji?*, 2006, „Bezpieczeństwo IT" – miesięcznik internetowy, http://www.bezpieczenstwoit.pl/.

Streszczenie

Artykuł poświęcony jest zagadnieniu opracowywania polityki bezpieczeństwa systemu informatycznego ze szczególnym uwzględnieniem etapu analizy ryzyka. Celem artykułu jest przedstawienie dostępnych strategii analizy ryzyka (strategia podstawowego poziomu bezpieczeństwa, nieformalna analiza ryzyka, szczegółowa analiza ryzyka, strategia mieszana). W artykule przedstawiono etapy konieczne do prawidłowego sformułowania dokumentu polityki bezpieczeństwa oraz omówiono dostępne strategie analizy ryzyka.

Risk analysis strategies in the development of information system security policy

Summary

Article is devoted to the issue of development of information system security policy, with particular emphasis on risk analysis stage. The article presents the available risk analysis strategies (strategy of baseline protection, an informal risk analysis, detailed risk analysis, mixed strategy). The article presents the steps necessary to create a security policy document and discusses strategies for risk analysis.